
# PRECURSOR ANALYSIS REPORT: SQL SLAMMER WORM INFECTION OF DAVIS-BESSE NUCLEAR POWER PLANT 2003

Cybersecurity for the Operational Technology Environment (CyOTE)

**31 MARCH 2023**

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

**INL/RPT-23-71941**

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

This *paper* is the product of *research* conducted by the Cybersecurity for the Operational Technology Environment (CyOTE) program and was funded by the Department of Energy Office of Cybersecurity, Energy Security and Emergency Response (DOE CESER). No updates have been made since the date of publication and no further funding has been approved.

# TABLE OF CONTENTS



# FIGURES



# TABLES

# PRECURSOR ANALYSIS REPORT: SQL SLAMMER WORM INFECTION OF DAVIS-BESSE NUCLEAR POWER PLANT 2003

## 1. EXECUTIVE SUMMARY

The SQL Slammer Worm Infection of Davis-Besse Nuclear Power Plant 2003 Precursor Analysis Report leverages publicly available information about Davis-Besse's 2003 cyber attack and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

On 25 January 2003, the SQL Slammer worm infected more than 90% of vulnerable hosts and crashed the internet in 10 to 15 minutes, making it one of the fastest spreading worms in history. SQL Slammer is a fileless, memory-resident worm that remotely exploits a stack-based buffer overflow vulnerability on local hosts to intensively scan and rapidly self-propagate across the internet. The worm infected approximately 300,000 unpatched hosts running Microsoft Structured Query Language (SQL) Server 2000 or Microsoft Desktop Engine (MSDE) 2000 with SQL Server Resolution Service.

The SQL Slammer worm indirectly infected FirstEnergy's Davis-Besse nuclear power plant by first infecting a consultant's company network server and then propagating through an external misconfigured connection into Davis-Besse's site network. The infection caused major network congestion, slow performance, data overloads, and the inability of local hosts to communicate with each other, which eventually caused a loss of availability and a loss of view when the Safety Parameter Display System (SPDS) and Plant Process Computer (PPC) crashed. At the time of the infection, the plant was already offline, the digital monitoring systems had redundant analog backups, and the plant control and safety functions were not affected, so there were no concerns of a safety breach. However, this incident resulted in many lessons learned and spawned important discussions about cybersecurity's role in nuclear safety and electric power reliability regulation, policy, and guidance.

Researchers and analysts identified 10 unique techniques utilized during the attack with a total of 640 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Eight of the identified techniques used during Davis-Besse cyber attack were precursors to the triggering event. Analysis identified 596 observables associated with these precursor techniques, 428 of which were assessed to have an increased likelihood of being perceived in the 331 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack. Asset owners and operators can use these products if they experience similar observables or to prepare for comparable scenarios.

# 2. INTRODUCTION

The Cybersecurity for the Operational Technology Environment (CyOTE) program developed capabilities for energy sector organizations to independently identify adversarial tactics and techniques within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), CyOTE is a partnership with energy sector owners and operators whose goal is to tie the impacts of a cyber attack to anomalies in the OT environment to determine whether the anomalies have a malicious cyber cause.

## 2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1, applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. The program utilizes MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) as a common lexicon to assess triggering events. By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables, which could represent a faint signal of an attack requiring investigation. CyOTE can assist organizations in prioritizing their OT environment visibility investments.

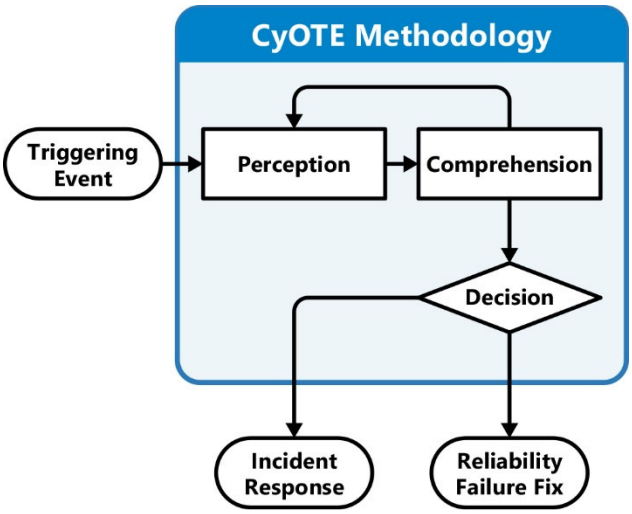



***Figure 1. CyOTE Methodology***

Historical case studies such as this one support continued learning through analysis of incidents that have impacted OT. This precursor analysis report is based on publicly available reports and provides examples of how key concepts in the CyOTE methodology appear in the real world, providing insights on how similar novel attacks could be detected earlier and therefore mitigated. The analysis enables OT personnel to independently identify observables associated with techniques known to be indicators of attack within OT environments. The identified observables highlight anomalous events for further investigation, which could enhance comprehension of malicious activity.

A timeline of events based on the CyOTE methodology portrays the attack-related observables associated with the precursor analysis report cyber attack. The timeline includes assessed dates, the triggering event, and comprehension of malicious activity by the organization. The point on this timeline when each technique appears is critical to the organization's ability to perceive and comprehend the associated malicious activity. Perception of techniques early in the timeline is critical, since halting those techniques will generally have greater potential to limit additional attack vectors using other techniques, defeat the cyber attack, and limit damage to operations.

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for personnel to detect those observables. If a technique includes

effects which personnel may detect, such as deletion or modification of system files or required user execution, then the technique would be more perceivable.

Differences in infrastructure and system configurations may present different challenges and opportunities for observable detection. For example, architecture-wide endpoint monitoring is likely to improve the perceivability of techniques which modify host files, such as the Data Destruction technique (T0809) for Inhibit Response Function and Theft of Operational Information technique (T0882) for Impact. Network monitoring and log analysis capabilities are likely to improve perceivability of techniques which create malicious network traffic, such as the Standard Application Layer Protocol technique (T0869) for Command and Control, External Remote Services technique (T0822) for Initial Access, and Connection Proxy technique (T0884) for Command and Control. Alternatively, enhancing the monitoring parameters of system files would increase the perceivability of techniques such as Data from Information Repositories technique (T0811) for Collection and the Service Stop technique (T0881) for Inhibit Response Function.

Comprehension can be further enhanced by technique artifacts created when adversaries employ certain attack techniques. The CyOTE program provides organizations with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack.

## 2.2. BACKGROUND ON THE ATTACK

The SQL Slammer worm infected more than 90% of vulnerable hosts and crashed the internet in 10 to 15 minutes in late January 2003, making it one of the fastest spreading worms in history.[1,2] SQL Slammer is a fileless, memory-resident worm that remotely exploits a stack-based buffer overflow vulnerability (CVE-CAN-2002-0649)[3] on local hosts to intensively scan and rapidly self-propagate.[4,5,6] The worm infected approximately 300,000 unpatched hosts running Microsoft Structured Query Language (SQL) Server 2000 or Microsoft Desktop Engine (MSDE) 2000 with SQL Server Resolution Service over User Datagram Protocol (UDP) Port 1434.[7] At certain points in the worm's spread, more than 55 million hosts were scanned every second, with replicated hosts doubling every 8.5 seconds.[8,9] The global recovery cost is estimated at $1 billion, and the global cost of lost productivity is estimated at $1.2 billion.[10]

Among SQL Slammer's victims was FirstEnergy's Davis-Besse nuclear power plant in Ottawa County, Ohio. At 9:00 AM (M-470) on 25 January 2003 (D-0), users on Davis-Besse's enterprise network noticed slow performance, which was about the same time SQL Slammer started infecting internet-connected networks across the world.[11,12]

At the time of the SQL Slammer infection, Davis-Besse was offline and in a safely defueled condition because a large cavity had been found in the Reactor Pressure Vessel (RPV) head, which averted any major safety issues.[13]

A timeline of adversarial techniques is shown in Figure 2. The timeline includes the estimated number of days prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.[a]

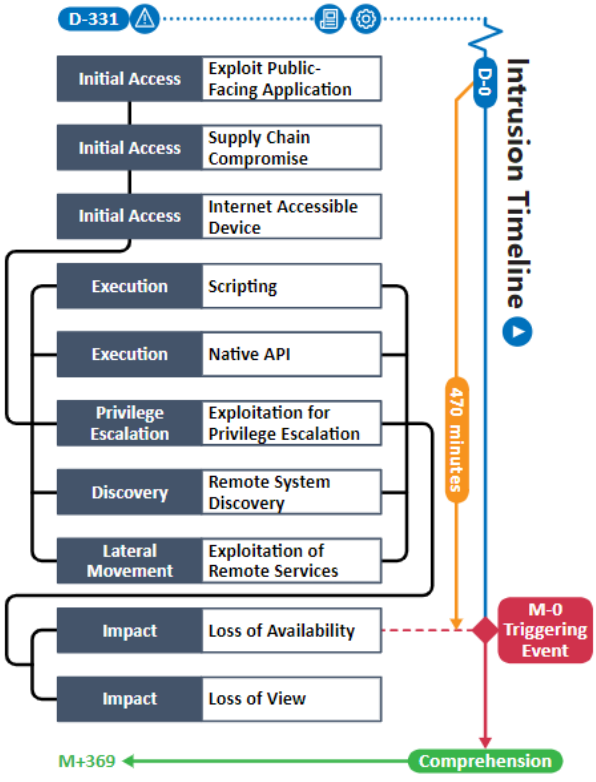



***Figure 2. Intrusion Timeline***

A critical factor in Davis-Besse's infection was the failure of plant personnel to perform a critical software update that was released months earlier. On 10 July 2002 (D-199), Microsoft released a critical security patch/update for Microsoft SQL Server 2000.[14] On 24 July (D-185), Microsoft published Security Bulletin MS02-039[15] informing system administrators running Microsoft SQL Server 2000 of a critical buffer overflow vulnerability (CVE-CAN-2002-0649)[16], found to be exploitable in SQL Server Resolution Service over UDP Port 1434, which the available critical security patch/update would fix.[17] Davis-Besse's IT personnel and plant computer engineers were not aware of the critical security patch/update or bulletin, which directly applied to vulnerable SQL Server 2000 hosts the plant employed in both the enterprise network and operations networks.[18,19]

The SQL Slammer worm indirectly infected Davis-Besse's site network by first infecting a consultant

[a] "M" events correspond to minutes prior to (M-) or after correspond to days prior to (D-) or after (D+) the triggering event (D-0).

company's network server, which was using UDP Port 1434 for data transfers, and then propagating through an external misconfigured Transmission System 1 (T1) connection into Davis-Besse's site network.[b,20] The consultant company accessed the plant's site network via the T1 connection, which itself was implemented behind Davis-Besse's external-facing enterprise firewall, bypassing the firewall's access control policy and ruleset configured to block UDP Port 1434. At least some Davis-Besse IT personnel were aware of this misconfigured connection.[21]

In February 2002 (D-331), the Nuclear Regulatory Commission (NRC) issued a security order alerting licensees about external connections that bypass network boundary protections.[22] Davis-Besse's IT personnel addressed the fulfillment of the NRC's security order; however, the external T1 connection used by the consultant, bypassing the external-facing enterprise firewall, remained in place and misconfigured. The relevant plant computer engineers were not informed of the external T1 connection's placement nor the IT personnel's decision to address the NRC's security order.[23]

Davis-Besse's enterprise network was interconnected with the operations network, with no firewall segregating traffic passing into the operations network, so the worm had unobstructed access to saturate bandwidth and infect vulnerable Microsoft SQL Server 2000 hosts that had UDP Port 1434 open within the enterprise network and operations networks.[24,25] The resulting intense network scanning and flood of packet clones from SQL Slammer into the network can cause performance issues, increased latency and packet loss, network outages, denial of service, and system crashes.[26,27,28]

After infecting Davis-Besse's enterprise network, the worm spread to an unpatched SQL Server 2000 host in the operations network, with plant personnel noticing slow performance by 4:00 PM (M-50).[29,30] At 4:50 PM (M-0), the network congestion caused by SQL Slammer's intensive scanning crashed the Safety Parameter Display System (SPDS), which is the plant's computerized display panel that relays critical plant safety parameters to plant operators and the NRC Operations Center in real time.[c] Even though the plant was offline at the time of the infection, many of the safety measures still require diligent monitoring. At 5:13 PM (M+23), the Plant Processing Computer (PPC), which is a plant-wide input/output (I/O) information system for consolidated analog and digital data acquisition and transfer, crashed.[31,32,33] However, the SPDS and the PPC had redundant analog backups that were unaffected by the worm, and plant control and safety functions were not affected.

Ultimately, the infection of Davis-Besse's site network caused major network congestion, slow performance, data overloads, the inability of local hosts to communicate with each other, and system crashes.[34,35] It took four hours and 50 minutes to recover the SPDS (M+290) and six hours and nine minutes to recover the PPC (M+369). As the SQL Slammer worm is memory-resident, infected servers were shut down to remove the worm, isolated from the network to prevent reinfection, updated with the available critical security patch/update, and reconnected to the site network. Though there were no concerns of a safety breach, this incident resulted in many lessons learned and spawned important dialogs about cybersecurity's role in nuclear safety and electric power reliability regulation, policy, and guidance.[36,37]

Analysis identified 10 unique techniques in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

[b] The "site network" refers to the entirety of the Davis-Besse network.
[c] At the time, any SPDS outage lasting eight hours or more required that the NRC be notified.

***Table 1. Techniques Used in the SQL Slammer Worm Infection of Davis-Besse Nuclear Power Plant 2003***


***Table 2. Precursor Analysis Report Quantitative Summary***

| Precursor Analysis Report Quantitative Summary | Totals |
|---|---|
| **MITRE ATT&CK® for ICS Techniques** | **10** |
| **Technique Observables** | **640** |
| **Precursor Techniques** | **8** |
| **Precursor Technique Observables** | **596** |
| **Highly Perceivable Precursor Technique Observable** | **428** |

# 3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist organizations in identifying malicious cyber activity earlier and more effectively. The following techniques and observables were compiled from publicly available sources and correlated with expert analysis.

## 3.1. EXPLOIT PUBLIC-FACING APPLICATION TECHNIQUE (T0819) FOR INITIAL ACCESS

At about 9:00 AM on 25 January 2003, the SQL Slammer worm remotely exploited CVE-CAN-2002-0649 on a consultant's public-facing company network server and on unpatched SQL Server 2000 hosts within Davis-Besse's site network.[38,39,40] This vulnerability allowed a deliberately designed packet, remotely sent to SQL Server Resolution Service over UDP Port 1434, to overwrite portions of system memory, granting remote execution of arbitrary, memory-injected code at an elevated privilege.[41,42,43] IT personnel and plant computer engineers were not aware of the critical security patch/update, available six months before the infection.[44,45]

The central exploit of SQL Slammer is the first byte of the UDP packet being a 0x04 flag.[46,47] Any bytes after the 0x04 flag are input to the Sprintf() function during the SQL Server Monitor thread process of generating a registry key to open. The Sprintf() function takes the input and formats it as output into a fixed-sized destination buffer on the stack frame. The Sprintf() function does not verify nor limit the input sent to write to or overwrite the fixed-sized buffer, and there is no presence of a 0x00 flag byte as an end indicator within the packet, enabling SQL Slammer's code to write outside of the fixed-sized buffer's bounds and perform a stack-based buffer overflow.[48,49]

IT Staff, IT Cybersecurity, and Support Staff personnel may have been able to observe a critical security patch/update, a Microsoft Security Bulletin, and a Carnegie Mellon Vulnerability Note.

A total of 102 observables were identified with the use of the Exploit Public-Facing Application technique (T0819). This technique is important for investigation because it provides initial access into a public-facing, vulnerable network. This technique appears early in the technique timeline and responding to it will halt all future remote exploitative code execution on hosts with the CVE-CAN-2002-0649 vulnerability. Responding to the critical security patch/update or the Microsoft Security Bulletin would have prevented the SQL Slammer worm from propagating to Davis-Besse's site network. Terminating the chain of techniques at this point would have effectively eliminated the SQL Slammer worm's root means of exploitation for infection.

Of the 102 observables associated with this technique, 74 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** (See Appendix B) | A total of 55 artifacts could be generated by the Exploit Public-Facing Application technique |
| **Technique Observers**[d] | IT Staff, IT Cybersecurity, Support Staff |

[d] Observer titles are adapted from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster. CyOTE products utilize these job categories rather than organizational titles to both support comprehensive analysis and preserve anonymity within the victim organization. A complete list of potential observers can be found in Appendix C.

## 3.2. SUPPLY CHAIN COMPROMISE TECHNIQUE (T0862) FOR INITIAL ACCESS

The SQL Slammer worm propagated to Davis-Besse's site network by first infecting an unnamed consultant's unsecure company network via exploiting a public-facing, unpatched company network server using UDP Port 1434 for data transfers.[50,51] The worm then propagated through an external misconfigured T1 connection used by the consultant, which bridged the consultant's unsecure company network with Davis-Besse's enterprise network, to further exploit and infect hosts within Davis-Besse's enterprise and operations networks. The T1 connection was used by the consultant to provide application software that ran on a server in Davis-Besse's site network.

IT Staff, IT Cybersecurity, and Support Staff personnel may have been able to observe the presence of an anomalous T1 connection and unmonitored network traffic. Potential observers may have also been able to observe anomalous system behavior on the host with the T1 connection and on the local area network gateway linking the host with the T1 connection to other networks.

A total of four observables were identified with the use of the Supply Chain Compromise technique (T0862). This technique is important for investigation because it provides initial access into a vulnerable network through an indirect route. This technique appears early in the timeline and responding to it would have limited all future SQL Slammer scanning and propagation from the consultant's company network to Davis-Besse's site network. Terminating the chain of techniques at this point would have effectively eliminated SQL Slammer's point of origination into Davis-Basse's site network.

All four observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts (See Appendix B)** | A total of 31 artifacts could be generated by the Supply Chain Compromise technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, Support Staff |

## 3.3. INTERNET ACCESSIBLE DEVICE TECHNIQUE (T0883) FOR INITIAL ACCESS

The misconfigured T1 connection used by the consultant, bridging the consultant's unsecure company network with Davis-Besse's enterprise network, provided a backdoor from the internet to the plant's enterprise network in an unmonitored and unsegregated manner.[52,53] The T1 connection was implemented behind Davis-Besse's external-facing enterprise firewall, bypassing the external-facing enterprise firewall's access control policy and ruleset configured to block UDP Port 1434. The misconfigured T1 connection caused vulnerable hosts within Davis-Besse's site network to be directly internet reachable. At least some employees of the plant's IT department were aware of the T1 connection, but when the T1 connection was implemented is unknown. The plant's relevant computer engineers were not informed of the external T1 connection's placement nor the decision to address the NRC security order, available 11 months before the infection.[54] Davis-Besse's enterprise network was interconnected with the operations network, and no firewall was segregating traffic passing into the operations network.[55] Once the worm infected the enterprise network, it had unobstructed access to saturate bandwidth and pseudo-randomly infect vulnerable Microsoft SQL Server 2000 hosts in the operations network that had Port 1434 open.[56]

IT Staff, IT Cybersecurity, Engineering, and Support Staff personnel may have been able to observe the presence of an anomalous NRC security order, T1 connection, and unmonitored network traffic. Potential observers may have also been able to observe anomalous system behavior on the host with the T1 connection and on the local area network gateway linking the host with the T1 connection to other networks.

A total of five observables were identified with the use of the Internet Accessible Device technique (T0883). This technique is important for investigation because it provides initial access into a vulnerable network through a path that bypasses network boundary protection devices. This technique appears early in the timeline and responding to it would have limited additional SQL Slammer scanning and propagation from the consultant's company network to Davis-Besse's site network. Properly responding to the NRC's security order would have entirely prevented the SQL Slammer worm from infecting Davis-Besse's site network. Terminating the chain of techniques at this point would have effectively eliminated SQL Slammer's open path into Davis-Besse's site network.

All five observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** (See Appendix B) | A total of 23 artifacts could be generated by the Internet Accessible Device technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, Engineering, Support Staff |

## 3.4. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

SQL Slammer is a Windows-based worm pre-written in x86 assembly code, and it accomplishes the steps of "Get Inside", "Reprogram the Machine", "Choose Victims at Random", "Replicate", and "Repeat" on every vulnerable host that is reachable and infected by the pseudo-random flood of single 376-byte UDP packets (404-byte packets with the requisite headers) that successive SQL Slammer infections generate.[57,58,59] The structure of the simple 376-byte packet containing the SQL Slammer worm code is comprised of the enabling vulnerability (CVE-CAN-2002-0649), the propagation mechanism, and the payload.[60]

SQL Slammer's code did not carry a directly malicious payload, but rather had the unintended effect of performing denial of service (DoS) attacks due to its rapidly propagated packets saturating available bandwidth.[61,62] SQL Slammer's packet content is disguised as a routine query request for SQL Server Resolution Service; however, the packet actually contains a string that is too long for SQL Server Monitor to properly handle.[63,64] This too-long UDP request string will act on a stack-based buffer overflow to overwrite portions of the system memory with deliberate data as a means to execute arbitrary code in the security context of the domain or SYSTEM level privileges of the SQL Server service account.[65,66,67] This arbitrary code execution remains in the infected host's memory and propagates a high volume of SQL Slammer clones by pointing at its own code as the data to send, in 376-byte one-way UDP packets, to hosts with an IP address generated by the worm's pseudo-random scan cycle instance. If the packet is sent to a vulnerable machine, the machine is infected, and the worm begins to propagate from the newly infected host.[68]

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe anomalous network traffic over UDP Port 1434, network traffic over TCP Port 179, UDP packet contents, and system behavior on local hosts.

A total of 97 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because it provides the automated, self-propagating means of deploying and executing a worm. This technique appears midway in the technique timeline and responding to it will limit all future scripted exploitation and propagation techniques on hosts with the CVE-CAN-2002-0649 vulnerability. Terminating the chain of techniques at this point would limit SQL Slammer's outward propagation, rapid replication rate, and bandwidth saturation.

Of the 97 observables associated with this technique, 69 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** (See Appendix B) | A total of 12 artifacts could be generated by the Scripting technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Cybersecurity |

## 3.5. NATIVE API TECHNIQUE (T0834) FOR EXECUTION

SQL Slammer is a Windows-based worm pre-written in x86 assembly code; as such, SQL Slammer interacts with the Windows operating system (OS) native application programming interfaces (API) to further access and utilize SYSTEM level functions throughout the entirety of the exploitation and propagation steps.[69,70] Native APIs provide a means of calling low-level hardware, memory space, and process services within the Windows Kernel. This functionality is accessible by user-mode applications and libraries. Native APIs are normally for boot and for carrying out standard tasks and requests, but SQL Slammer uses native APIs to carry out malicious tasks and requests associated with its exploitation and propagation steps.

SQL Slammer's ability to perform the exploit lies within the first byte of the packet, which is a 0x04 byte, and the Sprintf() function passing too much data to the fixed-size destination buffer, which allows arbitrary code to be written to and executed in memory.[71] SQL Slammer's ability to import functions from the SQLsort.dll, ws2_32.dll, and kernel32.dll libraries lies within the LoadLibrary() function, along with get handles referring to the libraries that functions are imported from.[72] SQL Slammer's ability to create pseudo-random IP addresses with a starting point value lies within the GetProcAddress() and GetTickCount() functions. The GetTickCount() function will seed each linear congruent pseudo-random number generator (PRNG) scan cycle instance with the number of milliseconds on the CPU's system clock since the system was last booted, and then interpret this number as an IP address.[73,74] SQL Slammer's ability to create a socket to connect two host nodes lies within the Socket() function. SQL Slammer utilizes this function to send packet clones to the PRNG incremented IP addresses over UDP Port 1434.[75]

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe anomalous network traffic over UDP Port 1434, network traffic over TCP Port 179, UDP packet contents, and system behavior on local hosts.

A total of 97 observables were identified with the use of the Native API technique (T0834). This technique is important for investigation because it is the lowest-level means of execution to call to hardware, memory space, and process services for OS-based worms. This technique appears midway in the technique timeline and responding to it will limit all future scripted exploitation and propagation techniques on hosts with the CVE-CAN-2002-0649 vulnerability. Terminating the chain of techniques at this point would limit SQL Slammer's outward propagation, rapid replication rate, and bandwidth saturation.

Of the 97 observables associated with this technique, 69 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** (See Appendix B) | A total of 25 artifacts could be generated by the Native API technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Cybersecurity |

## 3.6. EXPLOITATION FOR PRIVILEGE ESCALATION TECHNIQUE (T0890) FOR PRIVILEGE ESCALATION

Once a SQL Slammer clone has been sent to a vulnerable SQL Server 2000 host, arbitrary code is executed in memory, outside of the allocated fixed-size destination buffer reserved for the SQL Server Resolution Service Request.[76,77,78] SQL Server 2000 runs in the security context chosen by the administrator at the time of installation: by default it runs as a domain user, but it also could run as a local SYSTEM user.[79] Therefore, depending on the SQL Server 2000 host that is infected, the arbitrary code will execute outside of the fixed-size destination buffer with domain level or SYSTEM level privileges.

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe anomalous network traffic over UDP Port 1434, network traffic over TCP Port 179, UDP packet contents, and system behavior on local hosts.

A total of 97 observables were identified with the use of the Exploitation for Privilege Escalation technique (T0890). This technique is important for investigation because it provides malicious, exploitative code the ability to run at an elevated privilege. This technique appears midway in the technique timeline and responding to it will limit all future scripted exploitation and propagation techniques on hosts with the CVE-CAN-2002-0649 vulnerability. Terminating the chain of techniques at this point would limit SQL Slammer's outward propagation, rapid replication rate, and bandwidth saturation.

Of the 97 observables associated with this technique, 69 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts (See Appendix B)** | A total of 16 artifacts could be generated by the Exploitation for Privilege Escalation technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Cybersecurity |

## 3.7. REMOTE SYSTEM DISCOVERY TECHNIQUE (T0846) FOR DISCOVERY

SQL Slammer rapidly scans, discovers, propagates to, and infects vulnerable hosts simultaneously, as packets are sent to a loop of pseudo-randomly generated IP addresses.[80,81] Because single SQL Slammer worm packets are sent over UDP port 1434 and carry the potential to exploit vulnerable SQL Server 2000 hosts, the worm broadcasts its UDP scans without requiring responses from potential victim hosts, thus making it quicker and more effective.[82] This pseudo-random infinite IP loop for packet spraying, causing a flood of outbound UDP packets, is what led to the unintended consequence of performing denial of service attacks, with rapidly propagating packets saturating available bandwidth: SQL Slammer scans as fast as the infected host or network can transmit the packets.

SQL Slammer's scanning entails socket setups, followed by the start of an infinite loop of PRNG IP addresses (pseudo-randomly generated IP addresses) that create and send a packet copy of itself to the cycled PRNG IP addresses over UDP Port 1434.[83] In generating an infinite loop of IP addresses, SQL Slammer uses a linear congruent PRNG algorithm, where the GetTickCount() function seeds each PRNG scan cycle instance with the number of milliseconds on the CPU's system clock since the system was last booted, and then interprets this number as an IP address.[84,85] After the PRNG scan cycle is seeded with GetTickCount(), the algorithm will infinitely increment and cycle according to the algorithm's increment value. The specific PRNG scan cycle utilized by SQL Slammer resulted in approximately 74,856 distinct IP addresses being infected across many domains and geographic locations. Though it did not limit SQL Slammer's spread much, several errors made by the author within the PRNG algorithm left out many IP addresses within the internet address space. Despite this, the algorithm generated public, private, broadcast, and multicast IP addresses.[86,87,88]

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe anomalous network traffic over UDP Port 1434, network traffic over TCP Port 179, UDP packet contents, and system behavior on local hosts.

A total of 97 observables were identified with the use of the Remote System Discovery technique (T0846). This technique is important for investigation because it provides exploitative worms with a means to simultaneously scan, discover, propagate to, and infect vulnerable hosts with single UDP packets. This technique appears midway in the timeline and responding to it will limit all future scripted exploitation and propagation techniques on hosts with the CVE-CAN-2002-0649 vulnerability. Terminating the chain of techniques at this point would limit SQL Slammer's bandwidth saturation.

Of the 97 observables associated with this technique, 69 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** (See Appendix B) | A total of 43 artifacts could be generated by the Remote System Discovery technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Cybersecurity |

## 3.8. EXPLOITATION OF REMOTE SERVICES TECHNIQUE (T0866) FOR LATERAL MOVEMENT

SQL Slammer's successive infections and outward propagation is due to a vulnerability in SQL Server 2000 Resolution Service. CVE-CAN-2002-0649 allowed a deliberately designed packet, remotely sent to SQL Server 2000 Resolution Service over UDP Port 1434, to overwrite portions of system memory, granting remote execution of arbitrary, memory-injected code at an elevated privilege.[89] The remote execution of SQL Slammer's code triggers an infinite exploitation and propagation loop, which sends SQL Slammer packet clones to pseudo-randomly selected, PRNG IP addresses within a worm's scan cycle instance.[90,91] The flood of requests is just meaningless network traffic until a single SQL Slammer packet reaches a vulnerable host. SQL Slammer's infinite exploitation and propagation loop routine will continue until the infected host is rebooted or crashes, as it remains solely in memory.[92]

When SQL Server 2000 Resolution Service receives a SQL Slammer packet starting with a 0x04 byte, followed by many 0x01 bytes, the 0x01 bytes are inputted into the Sprintf() function and SQL Server Monitor thread generates a registry key to open with a long name of 'A' characters and causes a buffer overflow of the fixed-sized destination buffer.[93] This results in overwrites of key areas of memory with SQL Slammer's propagation code, while also gaining control over the SQL Server process.

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe anomalous network traffic over UDP Port 1434, network traffic over TCP Port 179, UDP packet contents, and system behavior on local hosts.

A total of 97 observables were identified with the use of the Exploitation of Remote Services technique (T0866). This technique is important for investigation because it is the mechanism by which an adversary can continually spread exploitative, self-propagating worms to vulnerable networks. This technique appears midway in the timeline and responding to it will limit all future scripted exploitation and propagation techniques on hosts with the CVE-CAN-2002-0649 vulnerability. Terminating the chain of techniques at this point would limit SQL Slammer's outward propagation, rapid replication rate, and bandwidth saturation.

Of the 97 observables associated with this technique, 69 are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** (See Appendix B) | A total of 31 artifacts could be generated by the Exploitation of Remote Services technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Cybersecurity |

## 3.9. LOSS OF AVAILABILITY TECHNIQUE (T0826) FOR IMPACT

At about 9:00 AM on 25 January, users on Davis-Besse's enterprise network noticed slow performance.[94] By 4:00 PM, plant personnel noticed slow performance on the operations network. Then at 4:50 PM, the network congestion caused by SQL Slammer's intensive scanning crashed the SPDS. At 5:13 PM, the PPC crashed. Though operators had lost their digital monitoring systems, the SPDS and the PPC had redundant analog backups that could not be affected by the worm, and the plant control and safety functions were not affected.

The unintended payload of SQL Slammer is its scanning/propagation mechanism, as each successive SQL Slammer infection competes for bandwidth and scans as fast as the infected host or network transmits packets.[95] Due to SQL Slammer's bandwidth saturation with its scanning, it causes major network congestion, slow performance, data overloads, increased latency, increased packet loss, denial of services, network outages, the inability of internal hosts to communicate with other internal hosts, and system crashes.[96,97]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe anomalous system behavior on local hosts.

A total of 22 observables were identified with the use of the Loss of Availability technique (T0826). This technique is important for investigation because it prevents organizations from delivering products or services. This technique appears late in the timeline and represents the triggering event. Responding to it has the potential to limit the extent of SQL Slammer's propagation within the internal network and saturation of available host and network bandwidth. Terminating the chain of techniques at this point would not have prevented Davis-Besse from being infected by the SQL Slammer worm.

All 22 observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** **(See Appendix B)** | A total of eight artifacts could be generated by the Loss of Availability technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management |

## 3.10. LOSS OF VIEW TECHNIQUE (T0829) FOR IMPACT

The SQL Slammer infection caused Davis-Besse's SPDS and PPC to crash.[98] The SPDS is the plant's computerized display panel that relays critical plant safety parameters to plant operators and the NRC Operations Center in real time. The SPDS monitors crucial safety measures such as coolant system sensor readouts, core temperature sensor readouts, and external radiation sensor readouts. Even though the plant was offline at the time of the SQL Slammer infection, many of the safety measures still require diligent monitoring. The PPC is a plant wide I/O information system for consolidated analog and digital data acquisition and transfer.[99,100,101]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe loss of view for various systems.

A total of 22 observables were identified with the use of the Loss of View technique (T0829). This technique is important for investigation because it causes a sustained loss of view of the digital monitoring systems. This technique appears late in the timeline and responding to it will not limit SQL Slammer's propagation within the internal network and saturation of available host and network bandwidth. Terminating the chain of techniques at this point would not prevent Davis-Besse from being infected by the SQL Slammer worm.

All 22 observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

| CyOTE Capabilities for Technique Perception and Comprehension | |
|---|---|
| **Artifacts** (See Appendix B) | A total of four artifacts could be generated by the Loss of View technique |
| **Technique Observers** | IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management |

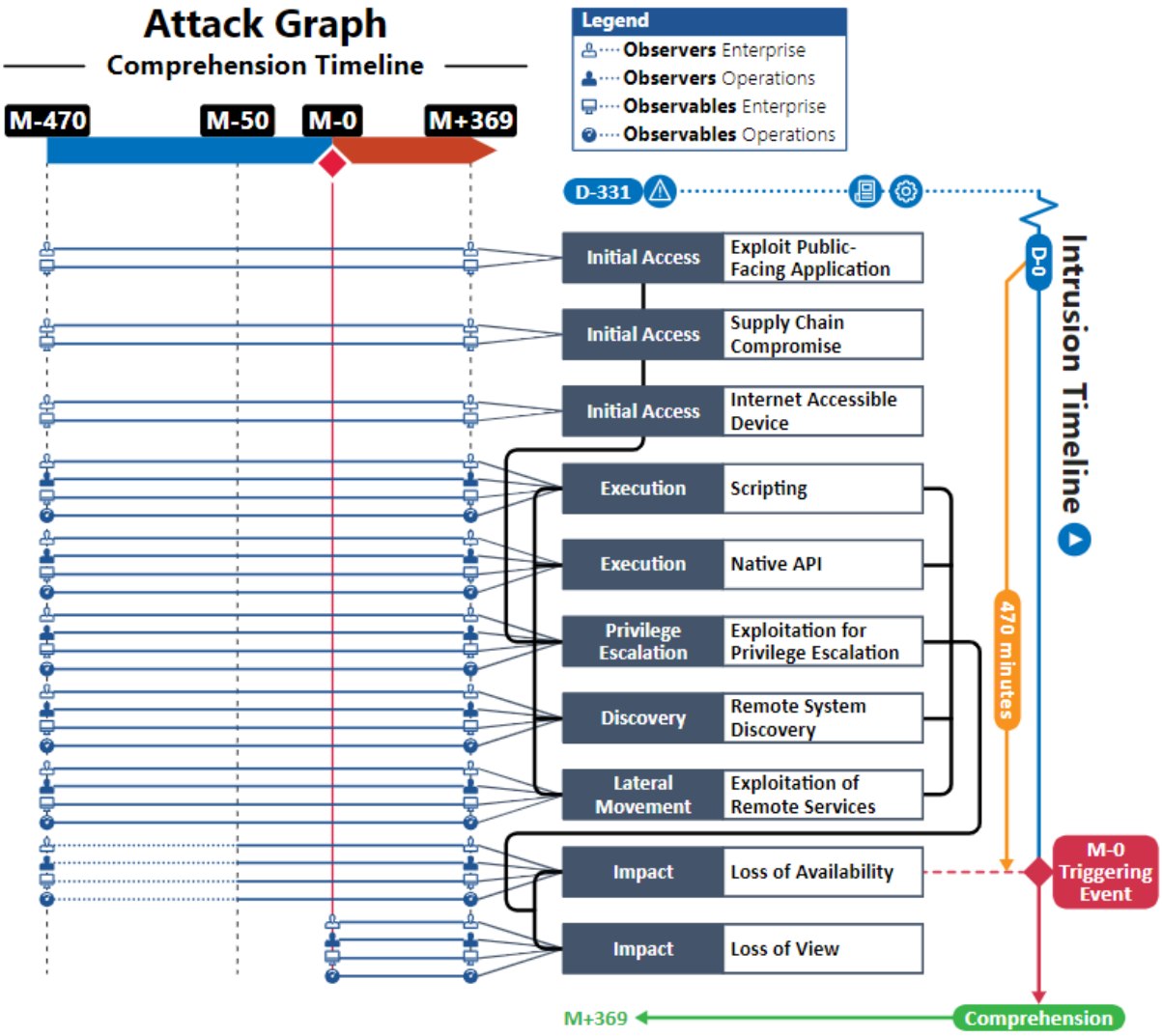



***Figure 3. Attack Graph***

# APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| **Observable 1 †** | *Presence of Vulnerability on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Critical Security Patch/Update* |
| **Observable 2 †** | *Presence of Vulnerability on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Microsoft Security Bulletin MS02-039 - Critical: Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875): CVE-CAN-2002-0649: Microsoft SQL Server 2000 Resolution Service Buffer Overflow Vulnerability* |
| **Observable 3 †** | *Presence of Vulnerability on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Carnegie Mellon University Software Engineering Institute CERT Coordination Center: CA-2002-22: Multiple Vulnerabilities in Microsoft SQL Server: Vulnerability Note VU#484891: CAN-2002-0649: Microsoft SQL Server 2000 Contains Stack Buffer Overflow in SQL Server Resolution Service* |
| **Observable 4 †** | *Presence of Vulnerability on Local Host: Microsoft Structured Query Language (SQL) Server 2000: CERT Advisory CA-2003-04 MS-SQL Server Worm* |
| **Observable 5 †** | *Presence of Vulnerability on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Microsoft Statement on the "Slammer" Worm Attack* |
| **Observable 6 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets with No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 7 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 8 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 9 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| **Observable 10 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 11 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 12 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 13 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 14 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 15 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 16 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Public-Facing Hosts: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 17 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Inbound Sources: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 18 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| **Observable 19 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 20 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 21 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 22 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 23 †** | *Anomalous Network Traffic: Between External Edge Routers and Internal Edge Routers: Over TCP Port 179: Border Gateway Protocol (BGP) Requests: Routing Update Messages: BGP Routing Table Updates* |
| **Observable 24 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 25 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 26 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 27 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 28 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| | *2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 29 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 30 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 31 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 32 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 33 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 34 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 35 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 36 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 37 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| | *2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 38 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 39 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 40 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 41 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 42 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 43 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 44 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 45 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 46 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way* |

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| | *Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 47 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 48 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 49 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 50 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 51 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 52 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 53 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 54 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Private Addresses* |
| **Observable 55 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| | *2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Broadcast IPs* |
| **Observable 56 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Multicast IPs* |
| **Observable 57 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 58 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 59 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 60 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 61 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 62 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 63 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 64 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Service Process* |
| **Observable 65 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Resolution Service Process* |
| **Observable 66 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Monitor Process* |
| **Observable 67 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| **Observable 68 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways* |
| **Observable 69 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways* |
| **Observable 70 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Microsoft Structured Query Language (SQL) Server 2000 Hosts* |
| **Observable 71 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Local Area Network Gateways* |
| **Observable 72 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Wide Area Network Gateways* |
| **Observable 73** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() |
| **Observable 74** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: LoadLibrary() |
| **Observable 75** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetProcAddress() |
| **Observable 76** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetTickCount() |
| **Observable 77** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Socket() |
| **Observable 78** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: ws2_32handle |
| **Observable 79** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: kernel32handle |
| **Observable 80** | Anomalous System Behavior on Local Host: Anomalous Socket Setup: Microsoft Structured Query Language (SQL) Server 2000 |
| **Observable 81** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Generate Registry Key: Registry Key With Long Name |
| **Observable 82** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion |
| **Observable 83** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server |

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| **Observable 84** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer\CurrentVersion |
| **Observable 85** | Anomalous System Behavior on Local Host: Anomalous Allocation of Memory Space: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes |
| **Observable 86** | Anomalous System Behavior on Local Host: Anomalous Memory Writes: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes: Sprintf() Function Overwrites Destination Buffer With Too-Long String |
| **Observable 87 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: Domain User* |
| **Observable 88 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: SYSTEM User* |
| **Observable 89** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Load the Address of a JMP ESP Instruction |
| **Observable 90** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77F8313C |
| **Observable 91** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77E89B18 |
| **Observable 92** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: ws2_32.dll |
| **Observable 93** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: kernel32.dll |
| **Observable 94** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EBX Register |
| **Observable 95** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EAX Register |

| Observables Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| **Observable 96** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77f8313c |
| **Observable 97** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77e89b18 |
| **Observable 98** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77ea094c |
| **Observable 99** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Disuse of Adding 1 in the Twos Complement Negation |
| **Observable 100** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of ADD Instead of SUB to Compensate for the Resulting Negative Number |
| **Observable 101** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: 25th and 26th Bits in the Scanned IP Addresses Remain Constant |
| **Observable 102** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: Certain /16 Address Blocks not Included in Scanning Cycle: Last Two Bits of First Address Byte Never Change |

| Observables Associated with Supply Chain Compromise Technique (T0862) | |
|---|---|
| **Observable 1 †** | *Anomalous System Behavior on Local Host: Initial Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Host: Increase in Local Host Throughput Associated with Scanning: Over UDP Port 1434: Local Host with Consultant Transmission System 1 (T1) Connection: Server Running Consultant's Application Software* |
| **Observable 2 †** | *Anomalous System Behavior on Local Host: Initial Increase in System Resource Utilization: Local Area Network Gateway: Increase in Local Host Throughput Associated with Scanning: Over UDP Port 1434: Local Area Network with Consultant Transmission System 1 (T1) Connection: Local Corporate Network* |
| **Observable 3 †** | *Anomalous Installation of Data Communications Line: From External Corporate Entity to Local Environment: Transmission System 1 (T1) Line: Bridging Consultant Company Network to Local Corporate Network: Connected behind External-Facing Firewall: Used by Consultant* |
| **Observable 4 †** | *Presence of Unmonitored Network Traffic: From External Corporate Entity to Local Environment: Over UDP Port 1434: Not Routed Through Local Corporate Network Gateway: Bypasses External-Facing Firewall's Access Control Policy and Ruleset* |

| Observables Associated with Internet Accessible Device Technique (T0883) | |
|---|---|
| **Observable 1 †** | *Presence of Vulnerability on Local Host: Regulatory Body Provides Notification of Alert: Issuance of Anomalous Nuclear Regulatory Commission (NRC) Security Order: Alert for External Network Connections Bypassing Network Boundary Protections* |
| **Observable 2 †** | *Anomalous System Behavior on Local Host: Initial Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Host: Increase in Local Host Throughput Associated with Scanning: Over UDP Port 1434: Local Host with Consultant Transmission System 1 (T1) Connection: Server Running Consultant's Application Software* |
| **Observable 3 †** | *Anomalous System Behavior on Local Host: Initial Increase in System Resource Utilization: Local Area Network Gateway: Increase in Local Host Throughput Associated with Scanning: Over UDP Port 1434: Local Area Network with Consultant Transmission System 1 (T1) Connection: Local Corporate Network* |
| **Observable 4 †** | *Anomalous Installation of Data Communications Line: From External Corporate Entity to Local Environment: Transmission System 1 (T1) Line: Bridging Consultant Company Network to Local Corporate Network: Connected behind External-Facing Firewall: Used by Consultant* |
| **Observable 5 †** | *Presence of Unmonitored Network Traffic: From External Corporate Entity to Local Environment: Over UDP Port 1434: Not Routed Through Local Corporate Network Gateway: Bypasses External-Facing Firewall's Access Control Policy and Ruleset* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 1 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 2 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 3 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 4 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 5 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 6 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 7 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 8 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000:* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| | *Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 9 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 10 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 11 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Public-Facing Hosts: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 12 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Inbound Sources: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 13 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 14 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 15 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 16 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 17 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 18 †** | *Anomalous Network Traffic: Between External Edge Routers and Internal Edge Routers: Over TCP Port 179: Border Gateway Protocol (BGP) Requests: Routing Update Messages: BGP Routing Table Updates* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 19 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 20 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 21 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 22 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 23 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 24 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 25 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 26 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| | *2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 27 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 28 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 29 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 30 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 31 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 32 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 33 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 34 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 35 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 36 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 37 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 38 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 39 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 40 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 41 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 42 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 43 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 44 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| | *2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 45 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 46 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 47 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 48 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 49 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Private Addresses* |
| **Observable 50 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Broadcast IPs* |
| **Observable 51 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Multicast IPs* |
| **Observable 52 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 53 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 54 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 55 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 56 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 57 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 58 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 59 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Service Process* |
| **Observable 60 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Resolution Service Process* |
| **Observable 61 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Monitor Process* |
| **Observable 62 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 63 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways* |
| **Observable 64 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways* |
| **Observable 65 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Microsoft Structured Query Language (SQL) Server 2000 Hosts* |
| **Observable 66 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Local Area Network Gateways* |
| **Observable 67 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Wide Area Network Gateways* |
| **Observable 68** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() |
| **Observable 69** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: LoadLibrary() |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 70** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetProcAddress() |
| **Observable 71** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetTickCount() |
| **Observable 72** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Socket() |
| **Observable 73** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: ws2_32handle |
| **Observable 74** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: kernel32handle |
| **Observable 75** | Anomalous System Behavior on Local Host: Anomalous Socket Setup: Microsoft Structured Query Language (SQL) Server 2000 |
| **Observable 76** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Generate Registry Key: Registry Key With Long Name |
| **Observable 77** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion |
| **Observable 78** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server |
| **Observable 79** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer\CurrentVersion |
| **Observable 80** | Anomalous System Behavior on Local Host: Anomalous Allocation of Memory Space: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes |
| **Observable 81** | Anomalous System Behavior on Local Host: Anomalous Memory Writes: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes: Sprintf() Function Overwrites Destination Buffer With Too-Long String |
| **Observable 82 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: Domain User* |
| **Observable 83 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000:* |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| | *Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: SYSTEM User* |
| **Observable 84** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Load the Address of a JMP ESP Instruction |
| **Observable 85** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77F8313C |
| **Observable 86** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77E89B18 |
| **Observable 87** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: ws2_32.dll |
| **Observable 88** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: kernel32.dll |
| **Observable 89** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EBX Register |
| **Observable 90** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EAX Register |
| **Observable 91** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77f8313c |
| **Observable 92** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77e89b18 |
| **Observable 93** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77ea094c |

| Observables Associated with Scripting Technique (T0853) | |
|---|---|
| **Observable 94** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Disuse of Adding 1 in the Twos Complement Negation |
| **Observable 95** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of ADD Instead of SUB to Compensate for the Resulting Negative Number |
| **Observable 96** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: 25th and 26th Bits in the Scanned IP Addresses Remain Constant |
| **Observable 97** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: Certain /16 Address Blocks not Included in Scanning Cycle: Last Two Bits of First Address Byte Never Change |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| **Observable 1 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 2 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 3 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434* |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| | *Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 4 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 5 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 6 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 7 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 8 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 9 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 10 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 11 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning:* |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| | *Public-Facing Hosts: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 12 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Inbound Sources: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 13 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 14 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 15 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 16 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 17 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 18 †** | *Anomalous Network Traffic: Between External Edge Routers and Internal Edge Routers: Over TCP Port 179: Border Gateway Protocol (BGP) Requests: Routing Update Messages: BGP Routing Table Updates* |
| **Observable 19 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 20 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 21 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434* |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| | *Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 22 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 23 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 24 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 25 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 26 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 27 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 28 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 29 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| | *2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 30 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 31 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 32 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 33 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 34 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 35 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 36 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 37 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 38 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 39 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-* |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| | *byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 40 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 41 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 42 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 43 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 44 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 45 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 46 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 47 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| | *2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 48 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 49 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Private Addresses* |
| **Observable 50 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Broadcast IPs* |
| **Observable 51 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Multicast IPs* |
| **Observable 52 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 53 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 54 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 55 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 56 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 57 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 58 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| **Observable 59 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Service Process* |
| **Observable 60 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Resolution Service Process* |
| **Observable 61 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Monitor Process* |
| **Observable 62 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 63 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways* |
| **Observable 64 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways* |
| **Observable 65 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Microsoft Structured Query Language (SQL) Server 2000 Hosts* |
| **Observable 66 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Local Area Network Gateways* |
| **Observable 67 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Wide Area Network Gateways* |
| **Observable 68** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() |
| **Observable 69** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: LoadLibrary() |
| **Observable 70** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetProcAddress() |
| **Observable 71** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetTickCount() |
| **Observable 72** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Socket() |
| **Observable 73** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: ws2_32handle |
| **Observable 74** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: kernel32handle |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| **Observable 75** | Anomalous System Behavior on Local Host: Anomalous Socket Setup: Microsoft Structured Query Language (SQL) Server 2000 |
| **Observable 76** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Generate Registry Key: Registry Key With Long Name |
| **Observable 77** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion |
| **Observable 78** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server |
| **Observable 79** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer\CurrentVersion |
| **Observable 80** | Anomalous System Behavior on Local Host: Anomalous Allocation of Memory Space: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes |
| **Observable 81** | Anomalous System Behavior on Local Host: Anomalous Memory Writes: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes: Sprintf() Function Overwrites Destination Buffer With Too-Long String |
| **Observable 82 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: Domain User* |
| **Observable 83 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: SYSTEM User* |
| **Observable 84** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Load the Address of a JMP ESP Instruction |
| **Observable 85** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77F8313C |
| **Observable 86** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77E89B18 |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| **Observable 87** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: ws2_32.dll |
| **Observable 88** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: kernel32.dll |
| **Observable 89** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EBX Register |
| **Observable 90** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EAX Register |
| **Observable 91** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77f8313c |
| **Observable 92** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77e89b18 |
| **Observable 93** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77ea094c |
| **Observable 94** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Disuse of Adding 1 in the Twos Complement Negation |
| **Observable 95** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of ADD Instead of SUB to Compensate for the Resulting Negative Number |
| **Observable 96** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: |

| Observables Associated with Native API Technique (T0834) | |
|---|---|
| | Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: 25th and 26th Bits in the Scanned IP Addresses Remain Constant |
| **Observable 97** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: Certain /16 Address Blocks not Included in Scanning Cycle: Last Two Bits of First Address Byte Never Change |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Observable 1 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 2 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 3 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 4 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 5 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Observable 6 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 7 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 8 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 9 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 10 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 11 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Public-Facing Hosts: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 12 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Inbound Sources: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 13 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 14 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Observable 15 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 16 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 17 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 18 †** | *Anomalous Network Traffic: Between External Edge Routers and Internal Edge Routers: Over TCP Port 179: Border Gateway Protocol (BGP) Requests: Routing Update Messages: BGP Routing Table Updates* |
| **Observable 19 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 20 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 21 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 22 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 23 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Observable 24 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 25 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 26 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 27 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 28 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 29 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 30 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 31 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 32 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Observable 33 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 34 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 35 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 36 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 37 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 38 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 39 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 40 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 41 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-* |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| | *byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 42 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 43 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 44 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 45 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 46 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 47 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 48 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 49 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Private Addresses* |
| **Observable 50 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| | *2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Broadcast IPs* |
| **Observable 51 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Multicast IPs* |
| **Observable 52 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 53 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 54 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 55 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 56 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 57 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 58 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 59 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Service Process* |
| **Observable 60 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Resolution Service Process* |
| **Observable 61 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Monitor Process* |
| **Observable 62 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Observable 63 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways* |
| **Observable 64 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways* |
| **Observable 65 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Microsoft Structured Query Language (SQL) Server 2000 Hosts* |
| **Observable 66 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Local Area Network Gateways* |
| **Observable 67 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Wide Area Network Gateways* |
| **Observable 68** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() |
| **Observable 69** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: LoadLibrary() |
| **Observable 70** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetProcAddress() |
| **Observable 71** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetTickCount() |
| **Observable 72** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Socket() |
| **Observable 73** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: ws2_32handle |
| **Observable 74** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: kernel32handle |
| **Observable 75** | Anomalous System Behavior on Local Host: Anomalous Socket Setup: Microsoft Structured Query Language (SQL) Server 2000 |
| **Observable 76** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Generate Registry Key: Registry Key With Long Name |
| **Observable 77** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion |
| **Observable 78** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Observable 79** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer\CurrentVersion |
| **Observable 80** | Anomalous System Behavior on Local Host: Anomalous Allocation of Memory Space: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes |
| **Observable 81** | Anomalous System Behavior on Local Host: Anomalous Memory Writes: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes: Sprintf() Function Overwrites Destination Buffer With Too-Long String |
| **Observable 82 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: Domain User* |
| **Observable 83 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: SYSTEM User* |
| **Observable 84** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Load the Address of a JMP ESP Instruction |
| **Observable 85** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77F8313C |
| **Observable 86** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77E89B18 |
| **Observable 87** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: ws2_32.dll |
| **Observable 88** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: kernel32.dll |
| **Observable 89** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EBX Register |
| **Observable 90** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EAX Register |

| Observables Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Observable 91** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77f8313c |
| **Observable 92** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77e89b18 |
| **Observable 93** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77ea094c |
| **Observable 94** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Disuse of Adding 1 in the Twos Complement Negation |
| **Observable 95** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of ADD Instead of SUB to Compensate for the Resulting Negative Number |
| **Observable 96** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: 25th and 26th Bits in the Scanned IP Addresses Remain Constant |
| **Observable 97** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: Certain /16 Address Blocks not Included in Scanning Cycle: Last Two Bits of First Address Byte Never Change |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| **Observable 1 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 2 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 3 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 4 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 5 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 6 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 7 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 8 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000:* |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| | *Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 9 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 10 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 11 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Public-Facing Hosts: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 12 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Inbound Sources: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 13 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 14 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 15 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 16 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 17 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 18 †** | *Anomalous Network Traffic: Between External Edge Routers and Internal Edge Routers: Over TCP Port 179: Border Gateway Protocol (BGP) Requests: Routing Update Messages: BGP Routing Table Updates* |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| **Observable 19 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 20 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 21 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 22 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 23 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 24 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 25 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 26 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| | *2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 27 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 28 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 29 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 30 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 31 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 32 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 33 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 34 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 35 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 36 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| **Observable 37 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 38 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 39 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 40 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 41 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 42 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 43 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 44 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| | *2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 45 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 46 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 47 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 48 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 49 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Private Addresses* |
| **Observable 50 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Broadcast IPs* |
| **Observable 51 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Multicast IPs* |
| **Observable 52 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 53 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 54 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| **Observable 55 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 56 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 57 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 58 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 59 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Service Process* |
| **Observable 60 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Resolution Service Process* |
| **Observable 61 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Monitor Process* |
| **Observable 62 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 63 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways* |
| **Observable 64 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways* |
| **Observable 65 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Microsoft Structured Query Language (SQL) Server 2000 Hosts* |
| **Observable 66 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Local Area Network Gateways* |
| **Observable 67 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Wide Area Network Gateways* |
| **Observable 68** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() |
| **Observable 69** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: LoadLibrary() |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| **Observable 70** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetProcAddress() |
| **Observable 71** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetTickCount() |
| **Observable 72** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Socket() |
| **Observable 73** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: ws2_32handle |
| **Observable 74** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: kernel32handle |
| **Observable 75** | Anomalous System Behavior on Local Host: Anomalous Socket Setup: Microsoft Structured Query Language (SQL) Server 2000 |
| **Observable 76** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Generate Registry Key: Registry Key With Long Name |
| **Observable 77** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion |
| **Observable 78** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server |
| **Observable 79** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer\CurrentVersion |
| **Observable 80** | Anomalous System Behavior on Local Host: Anomalous Allocation of Memory Space: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes |
| **Observable 81** | Anomalous System Behavior on Local Host: Anomalous Memory Writes: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes: Sprintf() Function Overwrites Destination Buffer With Too-Long String |
| **Observable 82 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: Domain User* |
| **Observable 83 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000:* |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| | *Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: SYSTEM User* |
| **Observable 84** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Load the Address of a JMP ESP Instruction |
| **Observable 85** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77F8313C |
| **Observable 86** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77E89B18 |
| **Observable 87** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: ws2_32.dll |
| **Observable 88** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: kernel32.dll |
| **Observable 89** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EBX Register |
| **Observable 90** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EAX Register |
| **Observable 91** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77f8313c |
| **Observable 92** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77e89b18 |
| **Observable 93** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77ea094c |

| Observables Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| **Observable 94** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Disuse of Adding 1 in the Twos Complement Negation |
| **Observable 95** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of ADD Instead of SUB to Compensate for the Resulting Negative Number |
| **Observable 96** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: 25th and 26th Bits in the Scanned IP Addresses Remain Constant |
| **Observable 97** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: Certain /16 Address Blocks not Included in Scanning Cycle: Last Two Bits of First Address Byte Never Change |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| **Observable 1 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 2 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 3 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434* |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| | *Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 4 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 5 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 6 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 7 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 8 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 9 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 10 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 11 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning:* |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| | *Public-Facing Hosts: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 12 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Inbound Sources: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 13 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 14 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 15 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 16 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 17 †** | *Anomalous Network Traffic: From Pseudo-random External Hosts to Internal Application Servers: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 18 †** | *Anomalous Network Traffic: Between External Edge Routers and Internal Edge Routers: Over TCP Port 179: Border Gateway Protocol (BGP) Requests: Routing Update Messages: BGP Routing Table Updates* |
| **Observable 19 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 20 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 21 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434* |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| | *Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 22 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 23 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 24 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 25 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 26 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 27 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 28 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 29 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| | *2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 30 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 31 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Public Addresses* |
| **Observable 32 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 33 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 34 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 35 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 36 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random External Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 37 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 38 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 39 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-* |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| | *byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 40 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 376-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 41 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: With First Byte 0x04* |
| **Observable 42 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Too-Long UDP Request for SQL Server Monitor: Without End Byte 0x00* |
| **Observable 43 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 44 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: SQL Server Resolution Service Requests: One-Way Single Packets With No Associated Response: Pseudo-random Flood of 404-byte UDP Packet Clones With Exploit Code: Sent to Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |
| **Observable 45 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Microsoft SQL Server 2000 Hosts* |
| **Observable 46 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 47 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server* |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| | *2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Local Area Network Gateways* |
| **Observable 48 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Increase in Network Traffic Associated With Scanning: Wide Area Network Gateways* |
| **Observable 49 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Unicast IPs: Private Addresses* |
| **Observable 50 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Broadcast IPs* |
| **Observable 51 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: Numerous New Outbound Destinations: 74,856 Distinctly Infected IP Addresses: Multicast IPs* |
| **Observable 52 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 \|; offset-0; depth-1"* |
| **Observable 53 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 68 6F 75 6E 74 68 69 63 6B \|"* |
| **Observable 54 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Containing "\| 04 01 01 01 01 01\|"* |
| **Observable 55 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Presence of First Flag Byte: 0x04 Flag Byte* |
| **Observable 56 †** | *Anomalous Network Traffic: From Internal Application Servers to Pseudo-random Internal Hosts: Microsoft Structured Query Language (SQL) Server 2000: Over UDP Port 1434: UDP Packet Contents: Absence of End Flag Byte: 0x00 Flag Byte* |
| **Observable 57 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Destination Unreachable* |
| **Observable 58 †** | *Anomalous System Behavior on Local Host: Hosts With Port 1434 Closed: Packet Drops From Unavailable Service: Internet Control Message Protocol (ICMP) Error Code Response: Request Timed Out* |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| **Observable 59 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Service Process* |
| **Observable 60 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Resolution Service Process* |
| **Observable 61 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: SQL Server Monitor Process* |
| **Observable 62 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances* |
| **Observable 63 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways* |
| **Observable 64 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways* |
| **Observable 65 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Microsoft Structured Query Language (SQL) Server 2000 Hosts* |
| **Observable 66 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Local Area Network Gateways* |
| **Observable 67 †** | *Anomalous System Behavior on Local Host: Saturation of Bandwidth: Wide Area Network Gateways* |
| **Observable 68** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() |
| **Observable 69** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: LoadLibrary() |
| **Observable 70** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetProcAddress() |
| **Observable 71** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: GetTickCount() |
| **Observable 72** | Anomalous System Behavior on Local Host: Anomalous Call to Windows API on Local Host: Microsoft Structured Query Language (SQL) Server 2000: Socket() |
| **Observable 73** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: ws2_32handle |
| **Observable 74** | Anomalous System Behavior on Local Host: Anomalous Usage of Get Handles: Microsoft Structured Query Language (SQL) Server 2000: kernel32handle |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| **Observable 75** | Anomalous System Behavior on Local Host: Anomalous Socket Setup: Microsoft Structured Query Language (SQL) Server 2000 |
| **Observable 76** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Generate Registry Key: Registry Key With Long Name |
| **Observable 77** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion |
| **Observable 78** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server |
| **Observable 79** | Anomalous System Behavior on Local Host: Anomalous Usage of Structured Query Language (SQL) Monitor Thread: Microsoft SQL Server 2000: Open Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer\CurrentVersion |
| **Observable 80** | Anomalous System Behavior on Local Host: Anomalous Allocation of Memory Space: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes |
| **Observable 81** | Anomalous System Behavior on Local Host: Anomalous Memory Writes: Microsoft Structured Query Language (SQL) Server 2000: Fixed Sized Destination Buffer on Stack Frame: 128 Bytes: Sprintf() Function Overwrites Destination Buffer With Too-Long String |
| **Observable 82 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: Domain User* |
| **Observable 83 †** | *Anomalous System Behavior on Local Host: Anomalous Remote Execution of Arbitrary Code: Microsoft Structured Query Language (SQL) Server 2000: Sprintf() Function Passes Too-Long SQL Server UDP Request String: Using SQL Server Service Permissions: SQL Server Service Account: SYSTEM User* |
| **Observable 84** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Load the Address of a JMP ESP Instruction |
| **Observable 85** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77F8313C |
| **Observable 86** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: SQLsort.dll: Call to SqlSort Import Address Table (IAT): Uses Salt Value as Increment Pointer: 0x77E89B18 |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| **Observable 87** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: ws2_32.dll |
| **Observable 88** | Anomalous System Behavior on Local Host: Presence of Anomalous Library Imports: Microsoft Structured Query Language (SQL) Server 2000: kernel32.dll |
| **Observable 89** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EBX Register |
| **Observable 90** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: PRNG Seed: GetTickCount(): EAX Register |
| **Observable 91** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77f8313c |
| **Observable 92** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77e89b18 |
| **Observable 93** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of OR Instead of XOR to Clear the Value of EBX: 0x77ea094c |
| **Observable 94** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Disuse of Adding 1 in the Twos Complement Negation |
| **Observable 95** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: Use of ADD Instead of SUB to Compensate for the Resulting Negative Number |
| **Observable 96** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: |

| Observables Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| | Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: 25th and 26th Bits in the Scanned IP Addresses Remain Constant |
| **Observable 97** | Anomalous System Behavior on Local Host: Presence of Anomalous Pseudo-random Scan Cycle: Microsoft Structured Query Language (SQL) Server 2000: Scanning of Pseudo-random IP Addresses: Over UDP Port 1434: Usage of Linear Congruent Pseudo-random Number Generation (PRNG) Algorithm for Infinite IP Address Scan Cycle: mod $2^{32}$ addr' = (addr * 214013 + (-2531012 xor EBX)): 74,856 Distinctly Infected IP Addresses: Certain /16 Address Blocks not Included in Scanning Cycle: Last Two Bits of First Address Byte Never Change |

| Observables Associated with Loss of Availability Technique (T0826) | |
|---|---|
| **Observable 1 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Network Interface/Adapter Throughput: Bandwidth Cap* |
| **Observable 2 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Central Processing Unit (CPU) Utilization* |
| **Observable 3 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Memory Usage* |
| **Observable 4 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Network Interface/Adapter Throughput* |
| **Observable 5 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Central Processing Unit (CPU) Utilization* |
| **Observable 6 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Memory Usage* |
| **Observable 7 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Network Interface/Adapter Throughput: Bandwidth Cap* |
| **Observable 8 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways: Increase in Local Host Throughput* |

| Observables Associated with Loss of Availability Technique (T0826) | |
|---|---|
| | *Associated With Scanning: Over UDP Port 1434: Increase in Central Processing Unit (CPU) Utilization* |
| **Observable 9 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Memory Usage* |
| **Observable 10 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Network Interface/Adapter Throughput: Bandwidth Cap* |
| **Observable 11 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Central Processing Unit (CPU) Utilization* |
| **Observable 12 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Memory Usage* |
| **Observable 13 †** | *Anomalous System Behavior on Local Host: Anomalous Slow Performance* |
| **Observable 14 †** | *Anomalous System Behavior on Local Host: Anomalous Data Overload* |
| **Observable 15 †** | *Anomalous System Behavior on Local Host: Anomalous Bandwidth Saturation* |
| **Observable 16 †** | *Anomalous System Behavior on Local Host: Anomalous Increase in Latency* |
| **Observable 17 †** | *Anomalous System Behavior on Local Host: Anomalous Increase in Packet Loss* |
| **Observable 18 †** | *Anomalous System Behavior on Local Host: Anomalous Denial of Service* |
| **Observable 19 †** | *Anomalous System Behavior on Local Host: Anomalous Network Outage* |
| **Observable 20 †** | *Anomalous System Behavior on Local Host: Anomalous Inability of Internal Hosts to Communicate With Other Internal Hosts* |
| **Observable 21 †** | *Anomalous System Behavior on Local Host: Anomalous System Crashes: Safety Parameter Display System (SPDS)* |
| **Observable 22 †** | *Anomalous System Behavior on Local Host: Anomalous System Crashes: Plant Process Computer (PPC)* |

| Observables Associated with Loss of View Technique (T0829) | |
|---|---|
| **Observable 1 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Network Interface/Adapter Throughput: Bandwidth Cap* |
| **Observable 2 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Central Processing Unit (CPU) Utilization* |

| Observables Associated with Loss of View Technique (T0829) | |
|---|---|
| **Observable 3 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Microsoft Structured Query Language (SQL) Server 2000 Hosts: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Memory Usage* |
| **Observable 4 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Network Interface/Adapter Throughput* |
| **Observable 5 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Central Processing Unit (CPU) Utilization* |
| **Observable 6 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Hosts With IP Addresses Within Pseudo-random IP Generation Scan Cycle Instances: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Memory Usage* |
| **Observable 7 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Network Interface/Adapter Throughput: Bandwidth Cap* |
| **Observable 8 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Central Processing Unit (CPU) Utilization* |
| **Observable 9 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Local Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Memory Usage* |
| **Observable 10 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Network Interface/Adapter Throughput: Bandwidth Cap* |
| **Observable 11 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Central Processing Unit (CPU) Utilization* |
| **Observable 12 †** | *Anomalous System Behavior on Local Host: Increase in System Resource Utilization: Wide Area Network Gateways: Increase in Local Host Throughput Associated With Scanning: Over UDP Port 1434: Increase in Memory Usage* |
| **Observable 13 †** | *Anomalous System Behavior on Local Host: Anomalous Slow Performance* |
| **Observable 14 †** | *Anomalous System Behavior on Local Host: Anomalous Data Overload* |
| **Observable 15 †** | *Anomalous System Behavior on Local Host: Anomalous Bandwidth Saturation* |
| **Observable 16 †** | *Anomalous System Behavior on Local Host: Anomalous Increase in Latency* |

| Observables Associated with Loss of View Technique (T0829) | |
|---|---|
| **Observable 17 †** | *Anomalous System Behavior on Local Host: Anomalous Increase in Packet Loss* |
| **Observable 18 †** | *Anomalous System Behavior on Local Host: Anomalous Denial of Service* |
| **Observable 19 †** | *Anomalous System Behavior on Local Host: Anomalous Network Outage* |
| **Observable 20 †** | *Anomalous System Behavior on Local Host: Anomalous Inability of Internal Hosts to Communicate With Other Internal Hosts* |
| **Observable 21 †** | *Anomalous System Behavior on Local Host: Anomalous System Crashes: Safety Parameter Display System (SPDS)* |
| **Observable 22 †** | *Anomalous System Behavior on Local Host: Anomalous System Crashes: Plant Process Computer (PPC)* |

# APPENDIX B: ARTIFACTS LIBRARY

| Artifacts Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| **Artifact 1** | Logon Security Event |
| **Artifact 2** | Logon Timestamp |
| **Artifact 3** | Process Failure |
| **Artifact 4** | Process State Change |
| **Artifact 5** | Operational Data Modification |
| **Artifact 6** | Operational Data Corruption |
| **Artifact 7** | Open Platform Communication (OPC) Communication (COM) Objects |
| **Artifact 8** | Remote Connections |
| **Artifact 9** | External Network Connections |
| **Artifact 10** | Logon Event |
| **Artifact 11** | Prefetch |
| **Artifact 12** | Logon Event |
| **Artifact 13** | Administrator Logon |
| **Artifact 14** | External Network Connections |
| **Artifact 15** | Remote Connections |
| **Artifact 16** | Ransom Note |
| **Artifact 17** | Logon Timestamp After Hours |
| **Artifact 18** | MAC Address |
| **Artifact 19** | IP Address |
| **Artifact 20** | Process Ending |
| **Artifact 21** | HTTP Traffic Port |
| **Artifact 22** | External Industrial Protocol Connections |
| **Artifact 23** | Web Server Log |
| **Artifact 24** | Virtual Network Computing (VNC) Traffic Port |
| **Artifact 25** | Secure Shell (SSH) Traffic Port |
| **Artifact 26** | Logon Security Event |
| **Artifact 27** | Telnet Traffic |
| **Artifact 28** | Increase Number of Logon Attempts |
| **Artifact 29** | Trivial File Transfer Protocol (TFTP) Port |
| **Artifact 30** | File Transfer Protocol (FTP) Port |
| **Artifact 31** | Application Failure |
| **Artifact 32** | HTTPS Port |

| Artifacts Associated with Exploit Public-Facing Application Technique (T0819) | |
|---|---|
| **Artifact 33** | User Account |
| **Artifact 34** | Web Proxy Logs |
| **Artifact 35** | Application Log |
| **Artifact 36** | Process Creation |
| **Artifact 37** | Process Ending |
| **Artifact 38** | Source IP Address |
| **Artifact 39** | MAC Address |
| **Artifact 40** | Firewall Logs |
| **Artifact 41** | Transport Layer Security (TLP) Certificate |
| **Artifact 42** | .lnk Files |
| **Artifact 43** | File Transfer Protocol Secure (FTPS) Port |
| **Artifact 44** | Logon Alert for Default Password |
| **Artifact 45** | Process Creation |
| **Artifact 46** | Vendor Jump Host Logon |
| **Artifact 47** | Configuration Alert for Default Password |
| **Artifact 48** | Remote Connections |
| **Artifact 49** | Remote Desktop Protocol (RDP) Traffic Port |
| **Artifact 50** | VNC Traffic Port |
| **Artifact 51** | SSH Traffic Port |
| **Artifact 52** | Telnet Traffic |
| **Artifact 53** | HTTP Traffic |
| **Artifact 54** | Application Log |
| **Artifact 55** | RDP Traffic Port |

| Artifacts Associated with Supply Chain Compromise Technique (T0862) | |
|---|---|
| **Artifact 1** | MAC Address |
| **Artifact 2** | Link Layer Discovery Protocol (LLDP) Requests |
| **Artifact 3** | Usage of Vendor Maintenance Account |
| **Artifact 4** | Usage of Default Account |
| **Artifact 5** | Static Source IP Address |
| **Artifact 6** | Ping Echo Port |
| **Artifact 7** | HTTP Port |
| **Artifact 8** | Simple Network Mail Protocol (SNMP) Port |

| Artifacts Associated with Supply Chain Compromise Technique (T0862) | |
|---|---|
| **Artifact 9** | Server Message Block (SMB) Port |
| **Artifact 10** | Network Discover Protocols |
| **Artifact 11** | Domain Name |
| **Artifact 12** | Source IP Address |
| **Artifact 13** | Mismatched Software Hashes |
| **Artifact 14** | Domain Name System (DNS) Queries Traffic Port |
| **Artifact 15** | Inaccurate Delivery Based on Design Documents |
| **Artifact 16** | Destination IP Address |
| **Artifact 17** | Physical Defects to Hardware |
| **Artifact 18** | Factory Acceptance Test Failure |
| **Artifact 19** | Inconsistencies in Hardware Bill of Materials (HBOM) |
| **Artifact 20** | Inconsistencies in Software Bill of Materials (SBOM) |
| **Artifact 21** | Hardware Serial Number Missing |
| **Artifact 22** | Unscheduled Firmware Updates |
| **Artifact 23** | Domain Registrant Data |
| **Artifact 24** | Hardware Failed Site Acceptance Test |
| **Artifact 25** | Hardware Tampering Evidence |
| **Artifact 26** | Device Incompatibility Issues |
| **Artifact 27** | Device Failures |
| **Artifact 28** | Additional Hardware Inserted on Devices |
| **Artifact 29** | Domain Autonomous System Number |
| **Artifact 30** | Domain IP Resolution |
| **Artifact 31** | Manipulation of Signature on Digital Certifications |

| Artifacts Associated with Internet Accessible Device Technique (T0883) | |
|---|---|
| **Artifact 1** | Host Registry Entries |
| **Artifact 2** | HTTPS Traffic |
| **Artifact 3** | Suspicious Connections in Proxy Logs |
| **Artifact 4** | Timestamps |
| **Artifact 5** | Virtual Private Network (VPN) Logoff Events |
| **Artifact 6** | Suspicious Connections in Firewall Logs |
| **Artifact 7** | VPN Logon Events |
| **Artifact 8** | Systems Applications and Protocols (SAP) Traffic |

| Artifacts Associated with Internet Accessible Device Technique (T0883) | |
|---|---|
| **Artifact 9** | Host Registry Entries HKEY_LOCAL_MACHINE\SYSTEM |
| **Artifact 10** | SQL Traffic |
| **Artifact 11** | Host Information in External Data Store or Website (SHODAN) |
| **Artifact 12** | HTTP 80 |
| **Artifact 13** | VNC Traffic Port 5800 |
| **Artifact 14** | Dialog Boxes Opened on Human Machine Interface (HMI) |
| **Artifact 15** | Application Authentication Events |
| **Artifact 16** | Internet Address in Memory Socket Data |
| **Artifact 17** | Remote Logins in OS Logs (Windows Event) |
| **Artifact 18** | Operational Database Connection to External Addresses |
| **Artifact 19** | Industrial Traffic from Internet Address |
| **Artifact 20** | Standard Traffic from Internet Address |
| **Artifact 21** | Internet Address in Application Logs |
| **Artifact 22** | Internet Address in OS Logs |
| **Artifact 23** | Internet Address in Command Line Record Data (netstat) |

| Artifacts Associated with Scripting Technique (T0853) | |
|---|---|
| **Artifact 1** | Startup Menu Modification |
| **Artifact 2** | OS Service Installation |
| **Artifact 3** | Registry Modifications |
| **Artifact 4** | Network Services Created |
| **Artifact 5** | External Network Connections |
| **Artifact 6** | Prefetch Files Created |
| **Artifact 7** | Executable Files |
| **Artifact 8** | System Processes Created |
| **Artifact 9** | OS Timeline Event |
| **Artifact 10** | System Event Log Creation |
| **Artifact 11** | Files Dopped into Directory |
| **Artifact 12** | Windows API Event Log |

| Artifacts Associated with Native API Technique (T0834) | |
|---|---|
| **Artifact 1** | Alert Generated |

| Artifacts Associated with Native API Technique (T0834) | |
|---|---|
| **Artifact 2** | System Resource Usage Management Changes |
| **Artifact 3** | .dll Modifications |
| **Artifact 4** | Imports Hash Changed |
| **Artifact 5** | Files Created |
| **Artifact 6** | Processes Initiated |
| **Artifact 7** | Services Initiated |
| **Artifact 8** | SYSMON Events Created |
| **Artifact 9** | Performance Degradation |
| **Artifact 10** | Blue Screen |
| **Artifact 11** | Configuration Change |
| **Artifact 12** | Command Execution |
| **Artifact 13** | Industrial Protocol Command Packet |
| **Artifact 14** | Host Device Failure |
| **Artifact 15** | Industrial Network Traffic |
| **Artifact 16** | Device Reads |
| **Artifact 17** | Device I/O Image Table Manipulated |
| **Artifact 18** | Device Failure |
| **Artifact 19** | Systems Calls |
| **Artifact 20** | Device Performance Degradation |
| **Artifact 21** | Device Memory Modification |
| **Artifact 22** | Device Alarm |
| **Artifact 23** | Device Live Data Changes |
| **Artifact 24** | Alter Process Logic |
| **Artifact 25** | Memory Corruption |

| Artifacts Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Artifact 1** | SYSMON Event 8 CREATEREMOTETHREAD Process Injection Detected |
| **Artifact 2** | Unexpected Process Crash |
| **Artifact 3** | Network Traffic Associated with Privilege Escalation Vulnerabilities (CVE-2014-4076 Sent a Specially Crafted TCP Packet to \\.\\ TCP Device Through DEVICEIOCONTROL Function |
| **Artifact 4** | Unusual Process Activity (Thread Suspension of Everything Except Thread Running in a Process Other Than Exploit Thread) |
| **Artifact 5** | Suspicious Files Written to Disk |

| Artifacts Associated with Exploitation for Privilege Escalation Technique (T0890) | |
|---|---|
| **Artifact 6** | Unusual Command Line History Associated with Known CVE Techniques (CVE-2019-5736 Privilege Escalation is Visible via Unusual Command Line Commands) |
| **Artifact 7** | Suspicious File Write to System Directory Followed by Privileged Execution of File |
| **Artifact 8** | Unusual or Unexpected KERBEROS Ticket Requests |
| **Artifact 9** | Suspicious Program Running Under SYSTEM or Other Elevated Account |
| **Artifact 10** | Driver Loaded (SYSMON Event) |
| **Artifact 11** | Network Traffic Matching Vulnerability (Snort, SURICATA) |
| **Artifact 12** | Abnormal Reads/Writes Between Processes |
| **Artifact 13** | Unusual Command Line Arguments to Application (lolbins) |
| **Artifact 14** | Artifacts Associated with Known Privilege Escalation CVES (PE Hard Coded Debug File Path for APT28 Malware Included Reference to CVE-2014-4076 Privilege Escalation) |
| **Artifact 15** | Unusual or Unexpected Child Process Running at Elevated Privileges |
| **Artifact 16** | Execution of a Suspicious File in the System32 or Windows Directory at Privileged Level |

| Artifacts Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| **Artifact 1** | Protocol Header Enumeration |
| **Artifact 2** | Protocol Content Enumeration |
| **Artifact 3** | VNC Port 5900 Calls |
| **Artifact 4** | TCP ACK Scan |
| **Artifact 5** | TCP XMAS Scan |
| **Artifact 6** | Recurring Protocol SYN Traffic |
| **Artifact 7** | TCP FIN Scans |
| **Artifact 8** | Device Failure |
| **Artifact 9** | TCP Reverse Ident Scan |
| **Artifact 10** | Sequential Protocol SYN Traffic |
| **Artifact 11** | Scans Over Industrial Network Ports with Target IPs |
| **Artifact 12** | Industrial Network Traffic Content Containing Logical Identifiers |
| **Artifact 13** | SMTP Port 25 Traffic |
| **Artifact 14** | Device Reboot |
| **Artifact 15** | Bandwidth Degradation |
| **Artifact 16** | Host Recent Connection Logs |

| Artifacts Associated with Remote System Discovery Technique (T0846) | |
|---|---|
| **Artifact 17** | IEC 101 Traffic to Serial Devices |
| **Artifact 18** | IEC 102 |
| **Artifact 19** | IEC 104 |
| **Artifact 20** | OPC Network Traffic |
| **Artifact 21** | Statistical Anomalies in Network Traffic |
| **Artifact 22** | DNS Port 53 Zone Transfers |
| **Artifact 23** | Industrial Network Traffic |
| **Artifact 24** | Common Network Traffic |
| **Artifact 25** | IEC 103 Traffic (For North America) |
| **Artifact 26** | IEC 61850 MMS |
| **Artifact 27** | Controller Proprietary Traffic |
| **Artifact 28** | Echo Type 8 Traffic |
| **Artifact 29** | ICMP Type 7 Traffic |
| **Artifact 30** | SNMP Port 162 Traffic |
| **Artifact 31** | SNMP Port 161 Traffic |
| **Artifact 32** | ARP Scans |
| **Artifact 33** | Operating System Queries |
| **Artifact 34** | TCP SYN Scans |
| **Artifact 35** | Industrial Network Traffic Content About Hostnames |
| **Artifact 36** | Polling Network Traffic from Unauthorized IP Sender Addresses |
| **Artifact 37** | NETBIOS Name Services Port |
| **Artifact 38** | LDAP Port |
| **Artifact 39** | Active Directory Calls |
| **Artifact 40** | Email Server Calls |
| **Artifact 41** | DNS Lookup Queries |
| **Artifact 42** | TCP Connect Scan |
| **Artifact 43** | Command Line Dialog Box Open |

| Artifacts Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| **Artifact 1** | SQL Protocol |
| **Artifact 2** | OPC Code Injection |
| **Artifact 3** | Vendor Specific Network Traffic |
| **Artifact 4** | Remote Network Traffic |

| Artifacts Associated with Exploitation of Remote Services Technique (T0866) | |
|---|---|
| **Artifact 5** | Common Network Traffic |
| **Artifact 6** | Absence of Alarm Events |
| **Artifact 7** | Alarm Events |
| **Artifact 8** | Application Logoff Event |
| **Artifact 9** | Safe Mode Reboot |
| **Artifact 10** | Blank Screens |
| **Artifact 11** | System Reboots |
| **Artifact 12** | Kernel Level Events |
| **Artifact 13** | Security Events Across Multiple Devices |
| **Artifact 14** | Host System Registry Changes |
| **Artifact 15** | Industrial Protocol Network Traffic |
| **Artifact 16** | Database Command Executions |
| **Artifact 17** | SMB Protocol |
| **Artifact 18** | Code Injection into the OS |
| **Artifact 19** | Application Logon Event |
| **Artifact 20** | Code Injections into Application |
| **Artifact 21** | Controller Failure |
| **Artifact 22** | Process Failure |
| **Artifact 23** | Misconfigurations of End Points |
| **Artifact 24** | Manipulation of Set Points |
| **Artifact 25** | Manipulation of Process |
| **Artifact 26** | Connection to Controller End Points |
| **Artifact 27** | Connection to Data Historian End Points |
| **Artifact 28** | Connection to EWS End Points |
| **Artifact 29** | Connection to HMI End Points |
| **Artifact 30** | Application Logs |
| **Artifact 31** | User Events Across Multiple Devices |

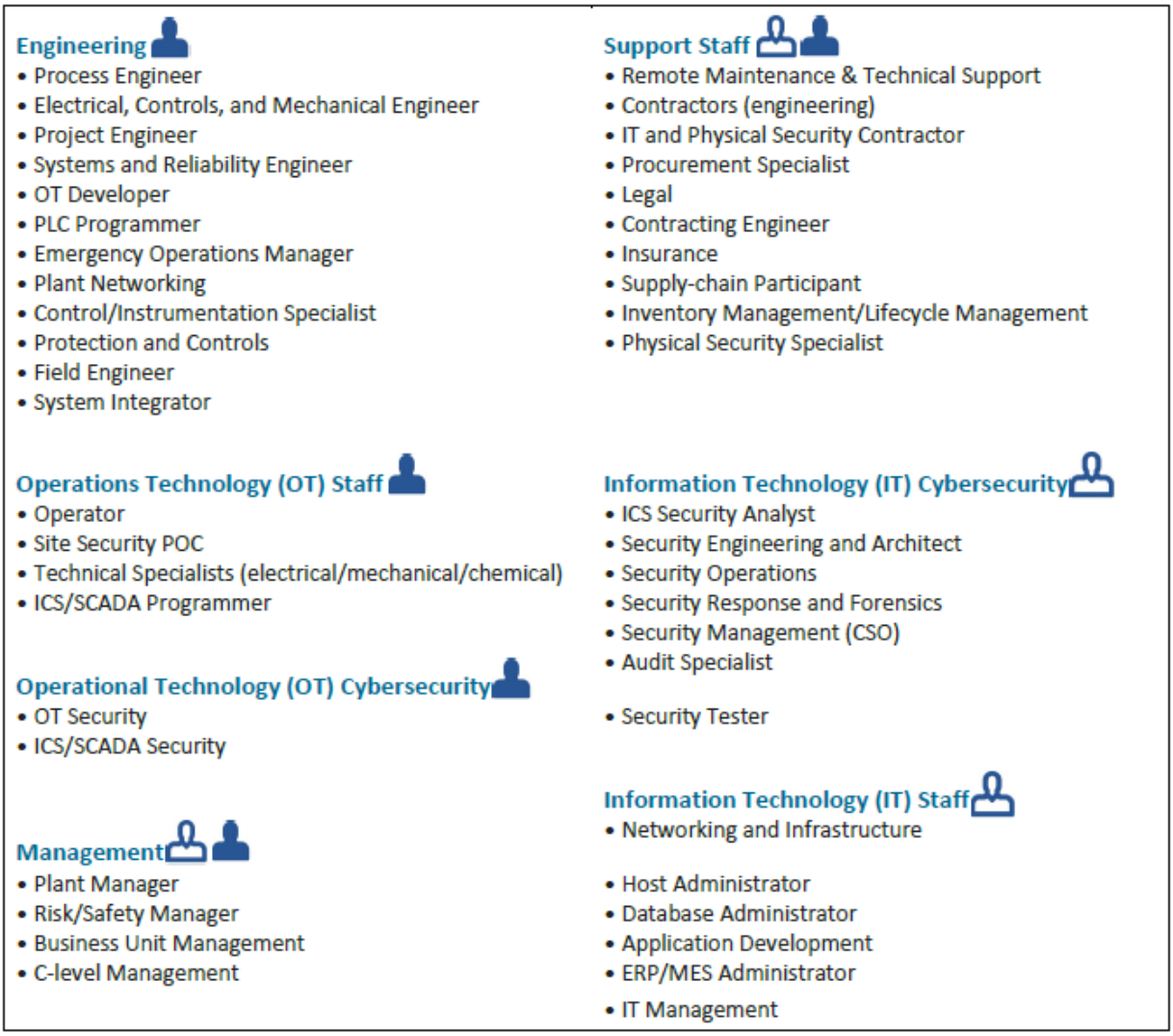
| Artifacts Associated with Loss of Availability Technique (T0826) | |
|---|---|
| **Artifact 1** | Process Failure Due to Loss of Required Network or System Dependency |
| **Artifact 2** | Unexplained Loss of User Data |
| **Artifact 3** | Changes In Network Routing or Usage of Redundant Control System Network Connection Due to Failed Network Path |

| Artifacts Associated with Loss of Availability Technique (T0826) | |
|---|---|
| **Artifact 4** | Significant Reduction or Increase in Network Traffic Due to Malware Propagation of Disappearance of Services |
| **Artifact 5** | Significant Logged Usage of Native Crypto Functions or Presence of Import of Crypto Functions in Binaries |
| **Artifact 6** | Operator or User Discovery of Encrypted or Inoperable Systems |
| **Artifact 7** | File System Modification Artifacts Might Be Associated with The Loss of Availability Might Be Present on Disk |
| **Artifact 8** | Unexplained Loss of Application Data |

| Artifacts Associated with Loss of View Technique (T0829) | |
|---|---|
| **Artifact 1** | Blocking Communications Paths and Channels (Comms, Network Infrastructure, Host Packet Routing) Might Occur via an OS or Device Modification |
| **Artifact 2** | Masked Reconfiguration of Alarm Thresholds or Other Configuration Settings Might Result in Unexpected Lack of Situational Awareness |
| **Artifact 3** | File System Modification Artifacts Might Be Associated with The Loss of View Attack Might Be Present on Disk |
| **Artifact 4** | Application Logic Hooks or Modifications Might Prevent Proper Reporting to/from an Industrial Application |

# APPENDIX C: OBSERVERS

This is a collection of standardized potential observers that work in operational technology organizations. It has been slightly modified by the CyOTE team from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster to communicate the categories of potential observers during cyber events.



# REFERENCES

[1] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[2] [Wired | Paul Boutin | “Slammed!” | https://www.wired.com/2003/07/slammer/ | 1 July 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[3] “NVD - CVE-2002-0649.” n.d. Nvd.nist.gov. Accessed December 13, 2023. https://nvd.nist.gov/vuln/detail/CVE-2002-0649#vulnCurrentDescriptionTitle.

[4] [Microsoft | “Win32/Slammer” | https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Win32%2FSlammer | 20 March 2009 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[5] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[6] [Carnegie Mellon University CERT Division | “2003 CERT Advisories” | https://resources.sei.cmu.edu/asset_files/WhitePaper/2003_019_001_496200.pdf | 25 January 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[7] [Cisco Systems, Inc. | “Combating Internet Worms “SQL Slammer”” | https://www.cisco.com/web/offer/powernow/docs/security/Slammer.pdf | 1 February 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[8] [Cisco Systems, Inc. | “Combating Internet Worms “SQL Slammer”” | https://www.cisco.com/web/offer/powernow/docs/security/Slammer.pdf | 1 February 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[9] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[10] [ZDNET | Robert Lemos | “Counting the cost of Slammer” | https://www.zdnet.com/article/counting-the-cost-of-slammer/ | 3 February 2003 | Accessed on 18 January 2023 | The source is publicly available information and does not contain classification markings]

[1111] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[12] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[13] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 |

Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[14] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[15] BetaFred. 2023. “Microsoft Security Bulletin MS02-039 - Critical.” Learn.microsoft.com. March 1, 2023. https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2002/ms02-039?redirectedfrom=MSDN.

[16] “NVD - CVE-2002-0649.” n.d. Nvd.nist.gov. https://nvd.nist.gov/vuln/detail/CVE-2002-0649#vulnCurrentDescriptionTitle.

[17] [Microsoft | “Microsoft Security Bulletin MS02-039 - Critical” | https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2002/ms02-039?redirectedfrom=MSDN | 24 July 2002 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[18] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[19] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[20] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[21] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[22] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[23] [United States Nuclear Regulatory Commission | Edward Markey | “EDO Principal Correspondence Control” | https://www.nrc.gov/docs/ML0329/ML032970134.pdf | 22 October 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[24] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[25] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[26] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[27] [Carnegie Mellon University CERT Division | “2003 CERT Advisories” | https://resources.sei.cmu.edu/asset_files/WhitePaper/2003_019_001_496200.pdf | 25 January 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[28] [The Register | John Leyden | “SQL worm slams the Net” | https://www.theregister.com/2003/01/27/sql_worm_slams_the_net/ | 27 January 2003 | Accessed on 18 January 2023 | The source is publicly available information and does not contain classification markings]

[29] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[30] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[31] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[32] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[33] [Westinghouse Nuclear | “Plant Process Computer System” | https://www.westinghousenuclear.com/Portals/0/operating%20plant%20services/automation/plant%20computer%20systems/NA-0029%20Plant%20Process%20Computers.pdf | 1 July 2017 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[34] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[35] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[36] [United States Nuclear Regulatory Commission | Edward Markey | “EDO Principal Correspondence Control” | https://www.nrc.gov/docs/ML0329/ML032970134.pdf | 22 October 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[37] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[38] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[39] [Microsoft | “Microsoft Security Bulletin MS02-039 - Critical” | https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2002/ms02-039?redirectedfrom=MSDN | 24 July 2002 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[40] [Microsoft | “Microsoft Statement on the “Slammer” Worm Attack | https://news.microsoft.com/2003/01/25/microsoft-statement-on-the-slammer-worm-attack/ | 25 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[41] [Carnegie Mellon University CERT Division | “2003 CERT Advisories” | https://resources.sei.cmu.edu/asset_files/WhitePaper/2003_019_001_496200.pdf | 25 January 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[42] [Carnegie Mellon University CERT Division | “2002 CERT Advisories” | https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_496196.pdf | 29 July 2002 | Accessed on 21 December 2002 | The source is publicly available and does not contain classification markings]

[43] [Carnegie Mellon University CERT Coordination Center | Allen Householder | “CERT Advisory CA-2003-04 MS-SQL Server Worm” | https://vuls.cert.org/confluence/display/historical/CERT+Advisory+CA-2003-04+MS-SQL+Server+Worm | 25 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[44] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[45] [Microsoft | “Microsoft Security Bulletin MS02-039 - Critical” | https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2002/ms02-039?redirectedfrom=MSDN | 24 July 2002 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[46] [Threat Post | David Litchfield | “The Inside Story of SQL Slammer” | https://threatpost.com/inside-story-sql-slammer-102010/74589/ | 20 October 2010 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[47] [National Institute of Standards and Technology | “National Vulnerability Database: CVE-2002-0649 Detail” | https://nvd.nist.gov/vuln/detail/CVE-2002-0649 | 12 August 2002 | Accessed on 21 December 2022 | The source is publicly available information and does not contain any classification markings]

[48] [Threat Post | David Litchfield | “The Inside Story of SQL Slammer” | https://threatpost.com/inside-story-sql-slammer-102010/74589/ | 20 October 2010 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[49] [Wired | Paul Boutin | “Slammed!” | https://www.wired.com/2003/07/slammer/ | 1 July 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[50] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[51] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[52] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[53] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[54] [United States Nuclear Regulatory Commission | Edward Markey | “EDO Principal Correspondence Control” | https://www.nrc.gov/docs/ML0329/ML032970134.pdf | 22 October 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[55] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[56] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[57] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[58] [Wired | Paul Boutin | “Slammed!” | https://www.wired.com/2003/07/slammer/ | 1 July 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[59] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[60] [Cisco Systems, Inc. | “Combating Internet Worms “SQL Slammer”” | https://www.cisco.com/web/offer/powernow/docs/security/Slammer.pdf | 1 February 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[61] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[62] [Symantec | Douglas Knowles | “W32.SQLExp.Worm” | https://web.archive.org/web/20061205015822/http:/sarc.com/avcenter/venc/data/w32.sqlexp.worm.html | 24 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[63] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[64] [Wired | Paul Boutin | “Slammed!” | https://www.wired.com/2003/07/slammer/ | 1 July 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[65] [Wired | Paul Boutin | “Slammed!” | https://www.wired.com/2003/07/slammer/ | 1 July 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[66] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[67] [Microsoft | “Microsoft Security Bulletin MS02-039 - Critical” | https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2002/ms02-039?redirectedfrom=MSDN | 24 July 2002 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[68] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[69] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[70] [MITRE | “Native API” | https://attack.mitre.org/techniques/T0834/ | 13 April 2021 | Accessed on 8 March 2023 | The source is publicly available information and does not contain classification markings]

[71] [Threat Post | David Litchfield | “The Inside Story of SQL Slammer” | https://threatpost.com/inside-story-sql-slammer-102010/74589/ | 20 October 2010 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[72] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[73] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[74] [Wired | Paul Boutin | “Slammed!” | https://www.wired.com/2003/07/slammer/ | 1 July 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[75] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[76] [Wired | Paul Boutin | “Slammed!” | https://www.wired.com/2003/07/slammer/ | 1 July 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[77] [Threat Post | David Litchfield | “The Inside Story of SQL Slammer” | https://threatpost.com/inside-story-sql-slammer-102010/74589/ | 20 October 2010 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[78] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[79] [Microsoft | “Microsoft Security Bulletin MS02-039 - Critical” | https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2002/ms02-039?redirectedfrom=MSDN | 24 July 2002 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[80] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[81] [University of California and USC Information Science Institute | Mohit Lad, Xiaoliang Zhao, and others | “Analysis of BGP Update Surge during Slammer Worm Attack” | 2003 | Accessed on 21 December 2002 | The source is publicly available and does not contain classification markings]

[82] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[83] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[84] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[85] [Caida | David Moore, Vern Paxson, and others | “The Spread of the Sapphire/Slammer SQL Worm” | https://archive.nanog.org/meetings/nanog27/presentations/worm.pdf | 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[86] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[87] [F-Secure | “Worm:W32/Slammer” | https://www.f-secure.com/v-descs/mssqlm.shtml | 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[88] [Caida | David Moore, Vern Paxson, and others | “The Spread of the Sapphire/Slammer SQL Worm” | https://archive.nanog.org/meetings/nanog27/presentations/worm.pdf | 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[89] [Carnegie Mellon University CERT Division | “2003 CERT Advisories” | https://resources.sei.cmu.edu/asset_files/WhitePaper/2003_019_001_496200.pdf | 25 January 2003 |

Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[90] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[91] [University of California and USC Information Science Institute | Mohit Lad, Xiaoliang Zhao, and others | “Analysis of BGP Update Surge during Slammer Worm Attack” | 2003 | Accessed on 21 December 2002 | The source is publicly available and does not contain classification markings]

[92] [F-Secure | “Worm:W32/Slammer” | https://www.f-secure.com/v-descs/mssqlm.shtml | 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[93] [Symantec | Jensenne Roculan, Sean Hittel, and others | “SQLExp SQL Server Worm Analysis” | https://web.archive.org/web/20170424202953/http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf | 28 January 2003 | Accessed on 21 December 2022 | The source is publicly available and does not contain classification markings]

[94] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[95] [IEEE Computer Society | David Moore, Vern Paxson, and others | “Inside the Slammer Worm” | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219056 | 11 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[96] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[97] [Cisco Systems, Inc. | “Combating Internet Worms “SQL Slammer”” | https://www.cisco.com/web/offer/powernow/docs/security/Slammer.pdf | 1 February 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[98] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[99] [The Register | Kevin Poulson | “Slammer worm crashed Ohio nuke plant net” | https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/ | 20 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[100] [United States Nuclear Regulatory Commission | “NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION ” | https://www.nrc.gov/docs/ML0324/ML032410430.pdf | 29 August 2003 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]

[101] [Westinghouse Nuclear | “Plant Process Computer System” | https://www.westinghousenuclear.com/Portals/0/operating%20plant%20services/automation/plant%20computer%20systems/NA-0029%20Plant%20Process%20Computers.pdf | 1 July 2017 | Accessed on 21 December 2022 | The source is publicly available information and does not contain classification markings]