Enhanced Attack Report

COLDSTEEL

Generated on 2025-04-04

Disclaimer

This report has been generated automatically and should be used for informational purposes only. To generate this report, Large Language Models (LLMs) were used to analyze the provided data. This technology is not perfect and may generate incorrect or misleading results. The results should be reviewed by a human expert before taking any action based on the information provided.

Definitions

Pre-Conditions: Conditions that must be true to execute the attack steps in the milestone.

Post-Conditions: Traces that an attacker leaves behind after executing the attack steps in the milestone.

Attack Steps: Steps that an attacker would take to achieve the goal of the milestone.

MITRE Technique: Techniques from the MITRE ATT&CK; framework that are relevant to the milestone.

STIX

Malware Name: COLDSTEEL
Malware Description: â€¢ COLDSTEEL provides interactive desktop & command line invocation, functionality including the ability to copy files, take screenshots and simulate user input. â€¢ COLDSTEEL persists as a Windows service. â€¢ COLDSTEEL communicates with the C2 server using a raw TCP connection.

Quick Overview

Milestone 1
1. Exploit Public-Facing Application as used by the malware (T1190)

Milestone 2
1. Command and Scripting Interpreter: Windows Command Shell as used by the malware (T1059.003)
2. System Services: Service Execution as used by the malware (T1569.002)

Milestone 3
1. Create or Modify System Process: Windows Service as used by the malware (T1543.003)

Milestone 4
1. Obfuscated Files or Information: Software Packing as used by the malware (T1027.002)
2. Modify Registry as used by the malware (T1112)
3. Indicator Removal: File Deletion as used by the malware (T1070.004)
4. Access Token Manipulation: Create Process with Token as used by the malware (T1134.002)

Milestone 5
1. System Information Discovery as used by the malware (T1082)
2. File and Directory Discovery as used by the malware (T1083)
3. Process Discovery as used by the malware (T1057)

Milestone 6
1. Non-Application Layer Protocol as used by the malware (T1095)

Milestone 1

Attack Step 1.1

==
Name: Exploit Public-Facing Application as used by the malware
Description: The malware family designated as COLDSTEEL exhibits obfuscation techniques, including potential log blending strategies to obscure malicious activities. Functionality variations are observed across different COLDSTEEL variants, with notable distinctions in Windows 10 compatibility and the utilization of ObRegisterCallbacks for process handle permission manipulation. Exploitation of publicly accessible applications is strongly implied as a primary method of initial access for COLDSTEEL variants. This suggests potential exploitation of vulnerabilities such as Log4j to gain entry into systems. Following successful exploitation, malicious payloads are executed, potentially delivered through the compromised application. Subsequently, techniques like ObRegisterCallbacks are employed to escalate privileges within compromised systems. Persistence mechanisms, including registry entries and scheduled tasks, are likely implemented by COLDSTEEL to ensure continued presence on compromised machines even after system reboots. Data theft, aimed at sensitive information such as credentials and financial data, is a probable objective of the malware. Communication with a remote Command and Control (C2) server controlled by its creators is anticipated for receiving further instructions or exfiltrated data.

Pre-Conditions:

- A public-facing application exists with a known vulnerability.
- A network connection exists between the compromised system and the target application server.
- The malware is capable of identifying and targeting the vulnerable application.

Post-Conditions:

- dll, 1.bat)
- Network traffic analysis revealing communication with C2 servers
- Registry modifications
- PowerShell execution logs

MITRE Technique

ID: T1190
Name: Exploit public-facing application
Description: Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.
More info: https://attack.mitre.org/techniques/T1190/

Indicators

- The file name is "newdev.dll".
- The path includes "AppData\Roaming\newdev.dll".

Milestone 2

Attack Step 2.1

===
Name: Command and Scripting Interpreter: Windows Command Shell as used by the malware
Description: The malware variant COLDSTEEL exhibits capabilities for command execution leveraging the Windows Command Shell (cmd.exe). Certain variants obfuscate this activity by copying cmd.exe to dllhost.exe, thereby mimicking legitimate system processes and potentially evading detection by security software. This inherent ability to execute arbitrary commands grants COLDSTEEL significant operational latitude, enabling actions such as file manipulation, modification of system configurations and registry entries, data exfiltration to a command-and-control server, and potential lateral movement within a network infrastructure. For instance, COLDSTEEL can utilize cmd commands to enumerate active processes and gather details regarding running applications, potentially compromising sensitive information.

Pre-Conditions:

- A computer running the Windows operating system is present.
- The malware has successfully infected the target computer.
- The malware has gained sufficient permissions to execute commands in the Windows Command Shell.

Post-Conditions:

- URLs: hxxp://104.223.34.[.]198/111.php, hxxp://104.223.34.[.]198/1dll.php, hxxp://104.223.34.[.]198/syn.php
- Malware delivery: The URLs might lead to sites hosting malware that could be downloaded and executed.
- 223.34.198, 103.224.80.76
- To determine the consequences and traces, I need more context about the specific actions being performed.
- What commands are being executed?
- Data exfiltration: The attacker might be trying to steal data from the targeted systems.
- What network connections are being established?
- Domain names: bd82563c72e6f72adff76bd8c6940c6037516a2a89c5fd0c23b8af622f0e91939b486e9db7faef192.95.36[.]61vpn2.smi1egate[.]comsvn1.smi1egate[.]comgiga.gnisoft[.]com
- What files are being accessed or modified?
- Web server exploitation: Attempting to access or exploit vulnerabilities on web servers at the given IP addresses.

MITRE Technique

ID: T1059.003
Name: Command and scripting interpreter: windows command shell
Description: Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via Remote Services such as SSH.

More info: https://attack.mitre.org/techniques/T1059/003

Indicators

- Path: C:\Users\\AppData\Roaming\newdev.dll: [file : name = ' newdev . dll ' A N D file : parent _ directory _ ref . path = ' C : \ \ Users \ \ < user > \ \ AppData \ \ Roaming ']

Attack Step 2.2

==
Name: System Services: Service Execution as used by the malware
Description: COLDSTEEL malware exhibits characteristics indicative of sophisticated functionality and behavior. Persistence is established through the utilization of a Windows service, enabling continuous operation even after system reboots. A comprehensive system survey is conducted upon establishment of persistence, gathering information pertaining to the target machine. The collected data is subsequently transmitted to a Command and Control (C2) server via raw TCP connections. Variations in functionality are observed across different COLDSTEEL variants. Older versions demonstrate limited support for Windows 10, potentially resulting in memory leaks during execution attempts. Newer variants are anticipated to address these limitations and incorporate enhanced capabilities. Communication with the C2 server is facilitated through potential server IP addresses such as 104.223.34[.]198 and protocols that may not adhere to standard web conventions. URLs ending in .smi1egate, .gnisoft, and .com are mentioned, potentially representing C2 infrastructure or additional malware components. Obfuscation techniques are employed by COLDSTEEL to conceal its true purpose and communication channels. This is evidenced by the presence of various IP addresses, URLs, and references to svn1, giga, dll, and syn. Exploitation of legitimate Windows service functionality is utilized by COLDSTEEL for executing malicious code under the guise of a legitimate system process. This tactic allows for circumvention of security measures, persistence, and stealthy operation. COLDSTEEL represents a sophisticated malware family characterized by capabilities encompassing persistence, information gathering, remote command execution, and communication obfuscation.

Pre-Conditions:

- Network connectivity to the C2 server is available.
- The malware code is loaded into memory.
- The malware has successfully infiltrated the target system.
- A Windows operating system is present.
- A running instance of a Windows service exists.

Post-Conditions:

- System instability
- Firewall rule modifications
- Files downloaded from C2 server
- Potential for further malicious activity
- Modified system registry entries
- Process creation logs
- Data exfiltration
- Altered system configuration files
- New log files with suspicious activity
- Compromised system functionality

- Hidden or modified files
- Windows service installation
- Network traffic to C2 server

MITRE Technique

ID: T1569.002
Name: System services: service execution
Description: Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (services.exe) is an interface to manage and manipulate services. The service control manager is accessible to users via GUI components as well as system utilities such as sc.exe and Net.
More info: https://attack.mitre.org/techniques/T1569/002

Indicators

- Path: C:\Users\\AppData\Roaming\newdev.dll: [file : name = ' newdev . dll ' AND file : parent _ directory _ ref . path = ' C : \ \ Users \ \ < user > \ \ App Data \ \ Roaming ']
- IPv4: 192.95.36.61: [ipv4-addr:value = '192.95.36.61']

Milestone 3

Attack Step 3.1

==
Name: Create or Modify System Process: Windows Service as used by the malware
Description: A new autostart Windows service is created by COLDSTEEL malware to ensure persistence across system reboots. This service generation is accomplished through the utilization of the Create or Modify System Process technique, enabling automatic execution upon system startup. The malware's core functionality is subsequently loaded and executed as part of this persistent service. To evade detection, COLDSTEEL likely employs unique service names that resemble legitimate system processes. The executable file for the service is newdev.dll, demonstrating the malware's active modification of system processes for malicious purposes.

Pre-Conditions:

- A user account with sufficient privileges exists.
- A Windows operating system.
- An active internet connection for communication with the C2 server.
- Access to system resources, including file system and registry.
- The malware has access to the necessary files and directories.
- The system is running a supported version of Windows.
- The ability to execute code on the target system.

Post-Conditions:

- System instability
- Firewall rule modifications
- DNS queries to malicious domains
- Suspicious files in temporary directories
- Network connections to C2 servers
- Potential for further malware infections
- Loss of sensitive information
- Data exfiltration
- Unusual process activity logs
- Compromised system functionality
- Modified system registry settings
- New user accounts created
- Altered log files
- File transfers to and from external servers

MITRE Technique

ID: T1543.003
Name: Create or modify system process: windows service
Description: Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions. Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry.

More info: https://attack.mitre.org/techniques/T1543/003

Indicators

- file : name = 'newdev.dll'
- file : parent_directory_ref.path = 'C:\Users\\AppData\Roaming'

Milestone 4

Attack Step 4.1

==
Name: Obfuscated Files or Information: Software Packing as used by the malware
Description: Software packing techniques, specifically employing Themida, are utilized by the malware known as Milestone2017 to obfuscate its files or information. The process involves embedding and encrypting the malware's code within a larger executable file, presenting a facade of benignity. Themida is integrated into the malware development workflow, enabling the attackers to package the malicious code of Milestone2017 within a container file generated by Themida. Subsequently, the embedded malware code is encrypted by Themida, rendering it unreadable in its raw form. The container file is then compiled into a seemingly legitimate executable, concealing the encrypted and hidden Milestone2017 code. Upon execution of this packed file on a victim's system, Themida's internal mechanisms decrypt and extract the original Milestone2017 malware code. The decrypted malware subsequently executes, carrying out its malicious activities. The utilization of software packing techniques presents challenges for traditional antivirus solutions, which primarily rely on known malicious signatures. Themida's sophisticated encryption and embedding techniques effectively conceal the true nature of the malware until decryption and execution occur.

Pre-Conditions:

- The malware utilizes software packing techniques to obfuscate its code.
- Access to a system infected with the COLDSTEEL malware.
- Tools capable of analyzing malware and unpacking packed files.
- Knowledge of malware analysis techniques.

Post-Conditions:

- Unusual network traffic
- System compromise
- Persistence on the system
- Hidden or encrypted files containing malware
- Potential for further malicious activity
- Altered registry settings
- Log entries indicating suspicious activity
- DNS requests to malicious domains
- Data exfiltration
- File transfers to external servers
- Modified system files
- New processes and services running

MITRE Technique

ID: T1027.002
Name: Obfuscated files or information: software packing
Description: Adversaries may perform software packing or virtual machine software protection to conceal their code. Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory. Virtual machine software

protection translates an executable's original code into a special format that only a special virtual machine can run. A virtual machine is then called to run this code.
More info: https://attack.mitre.org/techniques/T1027/002

Indicators

- file : name = ' newdev . dll'
- file : hashes.sha256 = '...' (Replace with actual SHA256 hash)
- file : hashes.md5 = '...' (Replace with actual MD5 hash)

Attack Step 4.2

==
Name: Modify Registry as used by the malware
Description: Registry keys are directly modified by the COLDSTEEL malware to append a description to its Windows service.

Pre-Conditions:

- The malware possesses the necessary code modules for registry manipulation.
- The target system has a Windows operating system installed.
- The malware executable is loaded and running.
- The malware has successfully gained administrative privileges on the target system.

Post-Conditions:

- System instability
- Hidden files and folders
- Malware persistence
- Log files containing malicious activity
- Backdoor executables
- Modified registry keys
- Compromised system functionality
- Unusual process activity in event logs
- Data theft
- Altered system configurations
- Network connections to suspicious IP addresses

MITRE Technique

ID: T1112
Name: Modify registry
Description: Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.
More info: https://attack.mitre.org/techniques/T1112/

Indicators

- Path: C:\Users\\AppData\Roaming\newdev.dll: [file : name = ' newdev . dll ' A N D file : parent _ directory _ ref . path = ' C : \ \ Users \ \ < user > \ \ AppData \ \ Roaming ']

Attack Step 4.3

===
Name: Indicator Removal: File Deletion as used by the malware
Description: The provided textual analysis indicates potential malicious activity associated with a COLDSTEEL variant, possibly MileStone2017. This variant is hypothesized to leverage Windows services for persistence and communication. A custom DLL file (newdev.dll) located within the user's AppData directory is purportedly utilized by the malware to create a Windows service. The execution of this service triggers the ServiceMain export, which is believed to encompass the core functionality of the malware. Network communications employing identifiers such as "MileStone2017" are suggested to facilitate tracking and differentiation of variants. While file deletion is not explicitly stated as a primary action, inferences can be drawn from the context. The malware's deployment within the AppData directory, a common location for obfuscation and persistence, coupled with the existence of multiple variants indicative of active development, suggests a potential capability for file removal. This could encompass the deletion of temporary files or logs to obscure its presence and activities, or potentially target critical system files or user data for manipulation or theft. Further investigation into the ServiceMain function's code execution and the malware's network communications is recommended to provide a more comprehensive understanding of its capabilities.

Pre-Conditions:

- The malware has successfully executed.
- The files to be deleted exist on the system.
- File access permissions
- Malware execution environment
- Operating System

Post-Conditions:

- Potential for further attacks
- System compromise
- Malware persistence
- Network reconnaissance
- Access logs on compromised servers
- Email communication with attackers
- New files (e.g., malicious DLLs)
- Data exfiltration
- Firewall bypass attempts
- DNS queries to suspicious domains
- Registry changes
- Modified system files
- Unusual network traffic logs

MITRE Technique

ID: T1070.004
Name: Indicator removal: file deletion
Description: Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: Ingress Tool Transfer) may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

More info: https://attack.mitre.org/techniques/T1070/004

Indicators

- file : name = 'newdev.dll'
- file : parent_directory_ref.path = 'C : \ \ Users \ \ < user > \ \ AppData \ \ Roaming'

Attack Step 4.4

==

Name: Access Token Manipulation: Create Process with Token as used by the malware
Description: A sophisticated cyber attack employing malware exhibiting several concerning characteristics has been identified. Malware samples were digitally signed hours after compilation, suggesting a potentially evasive tactic to circumvent detection by security tools reliant on trusted signatures. The malware utilizes techniques such as ObRegisterCallbacks to manipulate process access rights within the Windows operating system. The specific action of "Access Token Manipulation: Create Process with Token as used by the malware" has been highlighted. This entails the creation of new processes while impersonating the user 'ANONYMOUS'. This action presents a significant risk due to the potential for elevated privileges associated with the 'ANONYMOUS' account, enabling more destructive actions. Furthermore, operating as 'ANONYMOUS' allows the malware to potentially conceal its true identity and intentions from security monitoring tools typically focused on known user accounts. Fortinet SolutionsFortiEDR (Endpoint Detection and Response) has been identified as a security product capable of detecting and blocking this malware. FortiEDR functions "out-of-the-box" without requiring specific configurations for this threat, leveraging pre-built threat intelligence.

Pre-Conditions:

- Network connectivity may be required for communication with command and control servers.
- A vulnerable system running a compatible operating system.
- A process is running.
- The malware has access to the current process's token.
- The malware code is present and loaded into memory.

Post-Conditions:

- Unusual log entries
- Hidden files and folders
- System compromise
- Backdoors or malware remnants
- Persistence on the system
- New user accounts
- Altered registry settings
- Data exfiltration
- Network traffic manipulation
- Modified system files
- Network connections to suspicious IPs

MITRE Technique

ID: T1134.002
Name: Access token manipulation: create process with token

Description: Adversaries may create a new process with an existing token to escalate privileges and bypass access controls. Processes can be created with the token and resulting security context of another user using features such as CreateProcessWithTokenW and runas.
More info: https://attack.mitre.org/techniques/T1134/002

Indicators

- Path: C:\Users\\AppData\Roaming\newdev.dll: [file : name = ' newdev . dll ' AND file : parent _ directory _ ref . path = ' C : \ \ Users \ \ < user > \ \ App Data \ \ Roaming ']
- IPv4: 192.95.36.61: [ipv4-addr : value = ' 192.95.36.61 ']

Milestone 5

Attack Step 5.1

===
Name: System Information Discovery as used by the malware
Description: System information discovery is a common tactic employed by malware such as COLDSTEEL to gather intelligence regarding the infected machine. The precise methods utilized by COLDSTEEL for system information collection are likely detailed within the comprehensive analysis provided. However, malware typically employs various techniques to acquire this data. Operating system details, including version, edition, and build number, are frequently extracted. Hardware information, such as processor type and speed, RAM size, motherboard model, and disk drive specifications, is also commonly targeted. Network configuration details, encompassing IP addresses, MAC addresses, network interfaces, and active connections, may be collected. Furthermore, malware often seeks to identify installed software, listing programs and their versions. User account information, including local user names and privileges, is another common target. System events, such as recent logon/logoff events and application activity, are also frequently monitored. File system information, encompassing file paths, names, sizes, and user folders, may be acquired. The transmission of this gathered system information back to a command-and-control (C&C;) server is typically accomplished through various methods, including HTTP/HTTPS, DNS tunneling, or other protocols such as SMTP, IRC, or custom protocols.

Pre-Conditions:

- The target machine has system information available.
- A running instance of the COLDSTEEL malware.
- Network connectivity may be required for some types of system information gathering.
- The malware is running on a target machine.

Post-Conditions:

- System instability
- System compromise
- Malware persistence
- Hidden or encrypted data files
- Modified system registry entries
- Indicators of compromise (IOCs) in security logs
- Network traffic to command-and-control servers
- Data exfiltration
- New files and directories created
- Backdoors or rootkits installed
- Altered system configurations
- Unusual process activity in logs
- Performance degradation

MITRE Technique

ID: T1082
Name: System information discovery

Description: An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
More info: https://attack.mitre.org/techniques/T1082/

Indicators

- file : name = ' newdev . dll'
- file : parent_directory_ref.path = ' C : \ \ Users \ \ < user > \ \ AppData \ \ Roaming '
- IPv4: 192.95.36.61: [ipv4-addr:value='192.95.36.61']
- IPv4: 103.224.80.76: [ipv4-addr:value='103.224.80.76']
- IPv4: 138.128.98.106: [ipv4-addr:value='138.128.98.106']
- IPv4: 1.9.5.38: [ipv4-addr:value='1.9.5.38']

Attack Step 5.2

==

Name: File and Directory Discovery as used by the malware
Description: File and directory discovery activities indicative of malicious behavior are observed within the provided context. URLs and IP addresses associated with potential command-and-control (C&C;) servers are listed. Suspicious file extensions, such as ".php," suggest the potential execution of scripts designed to gather file information. Malware employs various techniques to enumerate files and directories. These techniques include direct utilization of operating system functions like listdir() or GetFileInformationByHandle(), execution of shell commands such as "dir" or "ls," and transmission of network requests to C&C; servers for specific file or directory listings. The purpose of file and directory discovery by malware is multifaceted. It enables the identification of valuable files, facilitates the mapping of target filesystem structures to understand their organization and potential vulnerabilities, and aids in the expansion of malware's reach within networks by discovering shares, network drives, or connected systems.

Pre-Conditions:

- Operating system access.
- The malware is running on a victim machine.
- Potential network connectivity (for remote file/directory information).
- The victim machine is not in safe mode.

Post-Conditions:

- Masked network connections
- Hidden registry keys
- Hidden files and directories
- Network traffic logs with obfuscated destinations or content
- Concealed loader and backdoor files
- Modified system files (e.g., drivers)
- Registry entries with unusual values or timestamps
- Process creation events with altered names or descriptions
- Obfuscated process activity

MITRE Technique

ID: T1083
Name: File and directory discovery
Description: Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
More info: https://attack.mitre.org/techniques/T1083/

Indicators

- file: name = 'newdev.dll'
- file: parent_directory_ref.path = 'C:\Users\\AppData\Roaming'

Attack Step 5.3

==
Name: Process Discovery as used by the malware
Description: Process discovery is employed by the FBI20111024 malware to ascertain information pertaining to running processes on an infected system. This process is likely effectuated through the utilization of system calls provided by the operating system to query process lists and retrieve process details, such as names, identifiers, parent processes, and execution paths. Additionally, direct inspection of memory regions containing process information may be undertaken, requiring advanced comprehension of memory structures and potentially involving techniques such as reading specific process control blocks (PCBs). The transmission of gathered process information to a command-and-control (C&C;) server for subsequent analysis or instructions is suggested by the provided URLs.

Pre-Conditions:

- The target system has active network connections.
- The operating system must have specific builds that are compatible with the malware's DKOM techniques.
- The malware is running on a target system.
- Access to kernel objects and structures through Direct Kernel Object Modification (DKOM).

Post-Conditions:

- Unusual network traffic
- System instability
- Log file alterations
- New registry entries
- Malware propagation
- Evidence of DKOM usage
- Remote code execution
- Data breaches
- Loss of system control
- Hidden processes
- Suspicious DLLs
- Modified system files
- Altered system configurations

- Backdoor creation

MITRE Technique

ID: T1057
Name: Process discovery
Description: Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Administrator or otherwise elevated access may provide better process details. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
More info: https://attack.mitre.org/techniques/T1057/

Indicators

- The file name is "newdev.dll".
- The file path is "C:\Users\\AppData\Roaming\newdev.dll".
- The malware communicates with IPv4 addresses: 192.95.36.61, 103.224.80.76, 138.128.98.106, and 1.9.5.38.

Milestone 6

Attack Step 6.1

==

Name: Non-Application Layer Protocol as used by the malware
Description: Communication between the malware and its command and control (C2) server is facilitated through TCP sockets operating at a level below conventional applications, thereby characterizing it as a "Non-Application Layer Protocol." A custom message format is employed by the malware, deviating from standard protocols such as HTTP or FTP. This non-conformance to established network traffic patterns presents a challenge for detection mechanisms.

Pre-Conditions:

- Requirements:
- The malware is active on a target system.
- Pre-Conditions:
- The operating system supports the specific non-application layer protocol used by the malware.
- A network connection exists between the infected system and the command and control server.

Post-Conditions:

- Unauthorized access to sensitive information
- System instability
- Modified kernel objects
- Malware propagation
- Unusual network traffic patterns
- New files with suspicious names and extensions
- Backdoor connections established to external servers
- Data corruption
- Hidden processes and threads
- Log entries indicating unauthorized activity
- Altered system registry entries
- Performance degradation

MITRE Technique

ID: T1095
Name: Non-application layer protocol
Description: Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).
More info: https://attack.mitre.org/techniques/T1095/

Indicators

- IPv4: 192.95.36.61: is used by the malware.

- IPv4: 103.224.80.76: is used by the malware.
- IPv4: 138.128.98.106: is used by the malware.
- IPv4: 1.9.5.38: is used by the malware.