Enhanced Attack Report

Small Sieve

Generated on 2025-04-10

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: Small Sieve
Malware Description: Small Sieve is a simple â€“ possibly disposable â€“ Python backdoor which is distributed using an NSIS installer that performs persistence. It provides basic functionality required to maintain and expand a foothold in victim infrastructure using custom string and traffic obfuscation schemes together with the Telegram Bot API to avoid detection.

Quick Overview

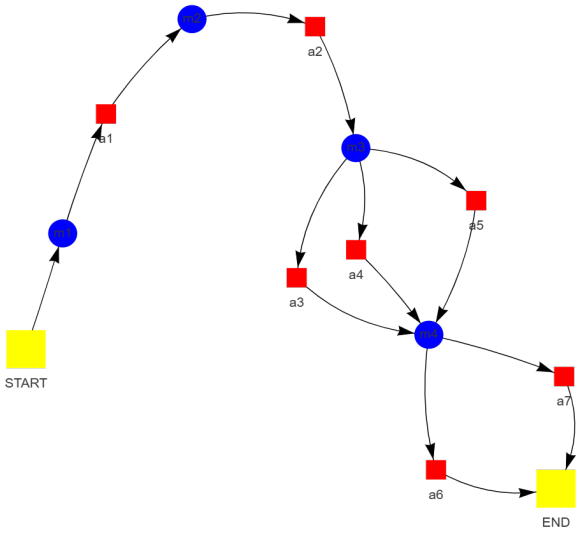
Milestone m1
a1. Command and Scripting Interpreter: Python as used by the malware (T1059.006)

Milestone m2
a2. Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder as used by the malware (T1547.001)

Milestone m3
a3. Obfuscated Files or Information as used by the malware (T1027.013)
a4. Execution Guardrails as used by the malware (T1480.001)
a5. Masquerading: Match Legitimate Name or Location as used by the malware (T1036.005)

Milestone m4
a6. Application Layer Protocol: Web Protocols as used by the malware (T1071.001)
a7. Data Encoding: Non-Standard Encoding as used by the malware (T1132.002)

Attack Graph



Milestone *m1*

Attack Step *a1*

==========

Name: Command and Scripting Interpreter: Python as used by the malware
Description: The MuddyWater Small Sieve backdoor is implemented as a Python script packaged using PyInstaller. This packaging process results in an executable file capable of execution on systems independent of a pre-installed Python interpreter.

Pre-Conditions:

- A Python interpreter is available on the target system.
- Access for the malware to execute Python scripts.

Post-Conditions:

- Compromised system with persistent access for attackers.
- Modified system startup settings for persistent access.
- Execution of malicious scripts and payloads.
- Base64 encoded data and JSON files related to C2 communication.
- Logs from the NSIS installer used for distribution.

- Data exfiltration from the victim system.
- Python scripts and associated files ("Small Sieve" backdoor).
- Web service logs showing communication with compromised websites.
- New files created with .old extension containing DLLs.
- Potential modification of system settings and configurations.
- PowerShell scripts and logs indicating execution of malicious code.
- Registry keys modifications (HKLM\Software \NFC\IPA and HKLM\Software \NFC\(Default)).
- Modified Office documents containing exploits (CVE-2017-0199).
- Network connections to command and control (C2) servers.

MITRE Technique

ID: T1059.006
Name: Command and scripting interpreter: python
Description: Adversaries may abuse Python commands and scripts for execution. Python is a very popular scripting/programming language, with capabilities to perform many functions. Python can be executed interactively from the command-line (via the python.exe interpreter) or via scripts (.py) that can be written and distributed to different systems. Python code can also be compiled into binary executables.
More info: https://attack.mitre.org/techniques/T1059/006

Indicators

No indicators found.

Milestone *m2*

Attack Step *a2*

==========
Name: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder as used by the malware
Description: Persistence is established by the malware through the addition of a registry run key under the HKCU\Software\Microsoft\Windows\CurrentVersion\Run subkey. A new entry, designated as "SystemTextEncoding" or potentially "OutlookMicrosift", is created with the path to the malicious binary as its value. This configuration results in the automatic execution of the malware upon each system boot or user logon.

Pre-Conditions:

- A Windows operating system with administrative privileges.
- The ability to write to the registry.
- The malware code itself.
- The malware has access to the registry.
- The target system is running a supported operating system.

Post-Conditions:

- Python script (Small Sieve) packed with PyInstaller.
- Backdoor binary index.exe installed in the user's AppData/Roaming directory.
- Log entries related to PowerShell script execution and backdoor activity.

MITRE Technique

ID: T1547.001
Name: Boot or logon autostart execution: registry run keys / startup folder
Description: Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.
More info: https://attack.mitre.org/techniques/T1547/001

Indicators

- Registry value name: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OutlookMicrosift
- Path: %AppData%\OutlookMicrosift\index.exe

Milestone *m3*

Attack Step *a3*

==========
Name: Obfuscated Files or Information as used by the malware
Description: The program strings and Telegram credentials employed by Small Sieve are subject to a two-stage obfuscation process. Initially, custom hexadecimal byte swapping is executed, rearranging the data's constituent bytes according to a predetermined pattern. Subsequently, an obfuscated variant of the Base64 encoding scheme is applied to the byte-swapped data, rendering it more resistant to direct interpretation and necessitating specialized decryption methodologies.

Pre-Conditions:

- An obfuscated Base64 function is available.
- Program strings and Telegram credentials exist within the malware.
- The malware Small Sieve is present in the environment.
- A custom hex byte swapping encoding scheme is available.

Post-Conditions:

- Compromised system with persistent access for attackers.
- PowerShell scripts used for maintaining persistent access.
- Data exfiltration from victim systems.
- Increased risk of further attacks and malware infections.
- Log entries indicating communication with the C2 server.
- Modified Registry Keys (HKLM\Software\NFC\IPA, HKLM\Software\NFC(Default)).
- Network traffic using HTTP over IPv4 or IPv6 to C2 server.
- Modified %LocalAppData%\MicrosoftWindowsOutlookDataPlus.txt file.
- Custom hex byte swapping encoding scheme applied to tasking traffic.
- Obfuscated program strings and Telegram credentials stored in memory.
- Potential disruption of normal system operations.
- New files with .old extensions containing obfuscated code.

MITRE Technique

ID: T1027.013
Name: Obfuscated files or information: encrypted/encoded file
Description: Adversaries may encrypt or encode files to obfuscate strings, bytes, and other specific patterns to impede detection. Encrypting and/or encoding file content aims to conceal malicious artifacts within a file used in an intrusion. Many other techniques, such as Software Packing, Steganography, and Embedded Payloads, share this same broad objective. Encrypting and/or encoding files could lead to a lapse in detection of static signatures, only for this malicious content to be revealed (i.e., Deobfuscate/Decode Files or Information) at the time of execution/use.
More info: https://attack.mitre.org/techniques/T1027/013

Indicators

- Small Sieve sample (Filename: gram_app.exe)
- Small Sieve sample (Filename: index.exe)

- Path: %LocalAppData%\MicrosoftWindowsOutlookDataPlus.txt
- Registry value name: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OutlookMicrosift
- Path: %AppData%\OutlookMicrosift\index.exe

Attack Step *a4*

==========
Name: Execution Guardrails as used by the malware
Description: The malware implements an "Execution Guardrail" technique utilizing a command-line argument requirement for payload activation. Successful execution of the Small Sieve payload is contingent upon the specific word "Platypus" being provided as a command-line argument. This mechanism serves to restrict unauthorized or accidental activation, ensuring that only authorized individuals possessing knowledge of this specific trigger can initiate the malware's full functionality.

Pre-Conditions:

- The ability to execute commands on the system.
- Command line interface access to the system.
- The word "Platypus" is present in the command line arguments.
- A system running the Small Sieve payload.

Post-Conditions:

- Logs indicating execution of PowerShell scripts and Python modules.
- Modified Registry Keys (HKLM\Software \NFC\IPA and HKLM\Software \NFC\(Default)).
- Compromised system with persistent backdoor access.
- Data exfiltration from compromised system.
- Network connections to C2 server using custom hex byte swapping encoding scheme.
- New files created with .old extension containing DLLs.
- Potential for further malicious activity on the compromised system.
- Modified system proxy settings.
- Telegram channel activity with bot ID and commands.

MITRE Technique

ID: T1480.001
Name: Execution guardrails: environmental keying
Description: Adversaries may environmentally key payloads or other features of malware to evade defenses and constraint execution to a specific target environment. Environmental keying uses cryptography to constrain execution or actions based on adversary supplied environment specific conditions that are expected to be present on the target. Environmental keying is an implementation of Execution Guardrails that utilizes cryptographic techniques for deriving encryption/decryption keys from specific types of values in a given computing environment.
More info: https://attack.mitre.org/techniques/T1480/001

Indicators

- Small Sieve sample (Filename: gram_app.exe)
- Small Sieve sample (Filename: index.exe)
- Path: %LocalAppData%\MicrosoftWindowsOutlookDataPlus.txt
- Registry value name: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OutlookMicrosift
- Path: %AppData%\OutlookMicrosift\index.exe

Attack Step *a5*

==========
Name: Masquerading: Match Legitimate Name or Location as used by the malware
Description: Filename manipulation is employed by the "Small Sieve" malware as a technique for obfuscation. Variations of legitimate file names, such as "Microsoft" (rendered as "Microsift") and "Outlook," are incorporated into its filenames. This practice aims to reduce the perceived suspiciousness during cursory file inspections, potentially facilitating evasion of detection by security personnel or users conducting superficial file name reviews.

Pre-Conditions:

- The malware has access to a list of legitimate file names and registry key names associated with Windows Defender.
- The ability to create and modify registry entries.
- The ability to create and modify files.
- Access to the target system's registry.
- Access to the target system's file system.

Post-Conditions:

- Data exfiltration from victim systems.
- Network connections to C2 servers using protocols like HTTPS and Telegram API.
- Altered system configurations and settings.
- Disruption of normal system operations.
- New files created with malicious code (e.g., index.exe, Goopdate.dll).
- Registry key modifications (HKLM\Software \NFC\IPA and HKLM\Software \NFC\(Default)).
- Potential for further malware infections and lateral movement within the network.
- Compromised systems with persistent access for attackers.
- Traces of data transfer between victim systems and C2 servers.
- Presence of backdoors and other malware within the compromised systems.
- Modified or added registry run keys for persistence.
- Logs containing suspicious activity related to file execution, network communication, and registry modifications.

MITRE Technique

ID: T1036.005
Name: Masquerading: match legitimate name or location
Description: Adversaries may match or approximate the name or location of legitimate files or resources when naming/placing them. This is done for the sake of evading defenses and observation. This may be done by placing an executable in a commonly trusted directory (ex: under System32) or giving it the name of a legitimate, trusted program (ex: svchost.exe). In containerized environments, this may also be done by creating a resource in a namespace that matches the naming convention of a container pod or cluster. Alternatively, a file or container image name given may be a close approximation to legitimate programs/images or something innocuous.
More info: https://attack.mitre.org/techniques/T1036/005

Indicators

- Path: %LocalAppData%\MicrosoftWindowsOutlookDataPlus.txt

- Registry value name: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OutlookMicrosift
- Path: %AppData%\OutlookMicrosift\index.exe

Milestone *m4*

Attack Step *a6*

==========
Name: Application Layer Protocol: Web Protocols as used by the malware
Description: The malware Small Sieve, attributed to the threat actor MuddyWater, utilizes the Telegram Bot API over HTTPS for both beaconing and task reception from its operators. HTTPS encryption is employed by Small Sieve to secure communications with Telegram Bot API servers, thereby obscuring the nature of the communication from network monitoring tools. Interaction with a designated Telegram bot via its API facilitates discreet communication, as the bot presents itself as a legitimate service within the Telegram platform. The confluence of HTTPS encryption and the Telegram Bot API effectively obfuscates Small Sieve's command and control (C2) communications, posing challenges for detection and analysis by security researchers and defenders.

Pre-Conditions:

- Access to the Telegram Bot API.
- The malware is active.
- An internet connection.
- A system infected with the Small Sieve malware.
- The malware has established a connection to the Telegram Bot API.

Post-Conditions:

- Logs of unusual activity
- Network infrastructure manipulation
- Presence of malware binaries
- Network traffic to C2 servers (HTTP, HTTPS, DNS tunneling)
- Telegram API interactions
- Altered system configurations
- Compromised systems
- System instability
- New files with suspicious names and extensions (.old)
- Proxy server logs
- JSON files containing C2 commands or results
- Modified registry keys
- Base64 encoded data
- Data exfiltration

MITRE Technique

ID: T1071.001
Name: Application layer protocol: web protocols
Description: Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
More info: https://attack.mitre.org/techniques/T1071/001

Indicators

No indicators found.

Attack Step *a7*

==========
Name: Data Encoding: Non-Standard Encoding as used by the malware
Description: The malware's tasking traffic is obfuscated through the utilization of a custom hex byte swapping encoding scheme. Data transmitted between the malware and its command and control (C2) server undergoes scrambling via an algorithm that reorders bytes within each data unit. This process impedes the decipherment of communication content by security tools.

Pre-Conditions:

- The malware is running.
- Access to the data to be encoded.
- A communication channel with the C2 server exists.
- The Small Sieve tool is available.

Post-Conditions:

- New files created in %LocalAppData%\ MicrosoftWindowsOutlookDataPlus.txt
- Logs containing suspicious activity related to the malware
- Presence of Base64 and JSON encoded data
- Small Sieve encoded data in network traffic
- Compromised system functionality
- Telegram API interactions
- Network connections to C2 servers using HTTP over IPv4 or IPv6
- Modified DLL file with .old extension
- System instability
- Increased security risks
- Modified registry keys (HKLM\Software \NFC\IPA and HKLM\Software \NFC\(Default))
- Data exfiltration

MITRE Technique

ID: T1132.002
Name: Data encoding: non-standard encoding
Description: Adversaries may encode data with a non-standard data encoding system to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a non-standard data encoding system that diverges from existing protocol specifications. Non-standard data encoding schemes may be based on or related to standard data encoding schemes, such as a modified Base64 encoding for the message body of an HTTP request.
More info: https://attack.mitre.org/techniques/T1132/002

Indicators

No indicators found.