Enhanced Attack Report

Small Sieve

Generated on 2025-03-07

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 1
1. Command and Scripting Interpreter: Python as used by the malware (T1059.006)

Milestone 2
1. Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder as used by the malware (T1547.001)

Milestone 3
1. Obfuscated Files or Information as used by the malware (T1027)
2. Execution Guardrails as used by the malware (T1480)
3. Masquerading: Match Legitimate Name or Location as used by the malware (T1036)

Milestone 4
1. Application Layer Protocol: Web Protocols as used by the malware (T1071.001)
2. Data Encoding: Non-Standard Encoding as used by the malware (T1132.002)

Milestone 1

Pre-Conditions:

- The system has the necessary permissions to execute Python scripts.
- Tools: A Python interpreter and the necessary libraries and dependencies for Python.
- Connectivity: Network connectivity to access and execute Python scripts.
- Environment: A system with Python installed and a stable and secure environment to run Python scripts.
- The malware has access to a Python interpreter.
- The system has Python installed.

Post-Conditions:

- Logs of the group's use of the backdoor, including exit commands.
- The MuddyWater APT group has used new malware in global attacks against vulnerable infrastructure.
- The group has downloaded a URL and saved it to a provided filename using the Python urllib module.
- The group is known by multiple names, including MuddyWater, Earth Vetala, MERCURY, Static Kitten, Seedworm, and TEMP.Zagros.
- Low-quality products sent by the group to victims.
- Network connections made by the group, including connections to vulnerable infrastructure.
- WHOIS domain information showing the creation date of scam sites.
- Tracking numbers for non-existent shipments used by the group.
- The group has exploited the Office vulnerability CVE-2017-0199 for execution.
- Files created by the group's use of Virtual Basic Script (VBS), including POWERSTATS payload and macros.
- Logs of the group's activities, including cyber espionage and malicious campaigns.
- Fake or stolen images used by the group on their scam sites.
- The group has used a backdoor to exit, but does not remove persistence.
- The group has used developed tools in Python, including Out1.
- Startup folder entries used by the group to start Small Sieve.
- Secure payment methods used by the group, including bank transfers and cryptocurrency.
- Independent reviews of the group's activities, including reviews of scam sites.
- The group has used a PyInstaller-packed Python script called Small Sieve.
- The group has used JavaScript files to execute its POWERSTATS payload.
- Testimonials from seemingly real people who had a great experience with the group's scam sites.
- The group conducts cyber espionage and malicious campaigns targeting organizations in various sectors.
- Files created by the group, including malware, scripts, and backdoors.

Attack Step 1.1

==
Name: Command and Scripting Interpreter: Python as used by the malware
Description: The malicious functions of the malware, a PyInstaller-packed Python script, are executed utilizing the Python scripting language.

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 2

Pre-Conditions:

- The malware has the necessary permissions to modify the registry.
- The malware has the necessary code to execute the autostart.
- The system's registry has a Run key.
- The malware has been installed on the system.
- A Windows-based system.
- The system's registry is accessible.
- The system's registry and startup folder must be enabled.

Post-Conditions:

- Existence of the DLL file renamed as a legitimate filename, Goopdate.dll.
- Presence of the Python script Small Sieve in the system.
- Downloading and saving of files using the Python urllib module.
- Creation of a new connection to Telegram using the provided token.
- Installation of the backdoor binary index.exe in the user's AppData/Roaming directory.
- Existence of the executable, GoogleUpdate.exe.
- Storage of the updated token in the encoded MicrosoftWindowsOutlookDataPlus.txt file.
- Persistence of the backdoor in the system after reboot.
- Presence of the updated token in the encoded MicrosoftWindowsOutlookDataPlus.txt file.
- Existence of the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OutlookMicrosift.
- Termination of the original connection to Telegram.
- Creation of a new registry run key for the backdoor.

Attack Step 2.1

===
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. A new value is created within the HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key, often utilizing a name that resembles legitimate system processes or files. The value data associated with this new key directs to the full path of the malware's executable file. Upon user logon, Windows automatically processes the values within the Run key, resulting in the execution of the corresponding applications. This mechanism ensures the malware's execution with each user system startup.

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 3

Pre-Conditions:

- Connectivity: Connectivity to access the custom hex byte swapping encoding scheme and the obfuscated Base64 function.
- Data: Program strings and Telegram credentials to be protected.
- The malware has the necessary resources to perform the obfuscation.
- The malware has the necessary environment to execute the custom hex byte swapping encoding scheme and the obfuscated Base64 function.
- The malware has access to program strings and Telegram credentials.
- Connectivity to the command and control (C2) channel.
- The word "Platypus" is present in the command line.
- A bot identifier generated at startup (between 10,000,000 and 90,000,000).
- The Small Sieve payload is executed correctly.
- The system's local proxy settings are enabled.
- The malware with the necessary permissions.
- A local proxy server or settings.
- A Python interpreter with the urllib module.
- A system with a command line interface.
- The malware is running on a system with a command line interface.
- The malware has the necessary permissions to execute the payload.
- A system with a network connection.
- The malware has a list of legitimate names or locations to match.
- The malware has access to the system.
- Availability of necessary knowledge of Windows operating system.
- Availability of system files to modify.
- Tools: Malware with masquerading capabilities.
- Connectivity: Internet access for downloading necessary information.
- Environment: Windows operating system.
- Resources: System permissions, memory, and processing power.
- Availability of legitimate names or locations to match.
- Availability of Windows Defender filenames and Registry key names.
- Availability of necessary knowledge of malware development and operation.
- The malware has the necessary knowledge of Microsoft and Outlook filenames.
- Availability of Microsoft and Outlook filenames.

Post-Conditions:

- Experts first noticed a MuddyWater campaign in late 2017 hitting several targets in the Middle East.
- A new wave of spam emails is spreading worldwide, using the UNICEF name and a seemingly official email in an effort to persuade people to donate money for the victims of the Gaza conflict.
- Network connections to the Telegram Bot API and other hacking tools.
- The group conducts cyber espionage and malicious campaigns targeting organizations in sectors, such as defense, telecommunications, oil and natural gas, and local government in Europe, Africa, Asia, and North America.
- i-Soon also made money by training MPS employees to hack independently of i-Soon, offering a variety of specialized hacking tools advertised as “industry-leading offensive and defensive technology.”
- Logs of the malicious activities, including cyber espionage and malicious campaigns.

- Google will no longer prohibit advertisers from employing fingerprinting techniques starting from 16 February 2025.
- MuddyWater is also known as Earth Vetala, MERCURY, Static Kitten, Seedworm, and TEMP.Zagros.
- The DLL file is contained within an executable, GoogleUpdate.exe.
- A DLL file renamed as a legitimate filename, Goopdate.dll, to enable the DLL side-loading technique.
- Specialized hacking tools, such as the Automated Penetration Testing Platform, the Divine Mathematician Password Cracking Platform, and the Public Opinion Guidance and Control Platform (Overseas).
- Files created by the malicious activities, including the DLL file and the hacking tools.
- The malicious file impersonates a legitimate file that is signed as a Google Update executable file.
- Traffic to the Telegram Bot API is protected by TLS, but Small Sieve obfuscates its tasking and response using a hex byte shuffling algorithm.
- Small Sieve uses a custom hex byte swapping encoding scheme combined with an obfuscated base64 function to protect program strings and updated Telegram credentials.
- Fingerprinting techniques employed by advertisers starting from 16 February 2025.
- A hex byte shuffling algorithm used to obfuscate tasking and response.
- A network connection will be established with the Telegram Bot API.
- The original connection to Telegram will be terminated.
- The DLL side-loading technique will be enabled.
- A network connection will be established with the C2 server.
- A malicious file will impersonate a legitimate file that is signed as a Google Update executable file.
- The backdoor will exit, but persistence will not be removed.
- The updated token will be stored in the encoded MicrosoftWindowsOutlookDataPlus.txt file.
- The system's local proxy settings will be disabled or modified.
- A file named Small Sieve payload will be created with the custom hex byte swapping encoding scheme.
- The DLL file will be contained within an executable, GoogleUpdate.exe.
- A log entry will be created when the system's local proxy settings are disabled or modified.
- The Small Sieve payload will only execute correctly if the word "Platypus" is passed to it on the command line.
- The backdoor will reconnect to the Telegram Bot API using the provided token.
- Tasking requests will be dropped if they do not come from the specified channel.
- Small Sieve uses variations of Microsoft (Micrisift) and Outlook in its filenames to attempt to avoid detection during casual inspection.
- Google will no longer prohibit advertisers from employing fingerprinting techniques starting from 16 February 2025.
- The DLL file is contained within an executable.
- Logs of the fingerprinting techniques used by Google advertisers.
- Files created by the spam emails, including the email templates and sender information.
- The initial token used to authenticate each message to the Telegram Bot API is 2003026094: AAGoitvpcx3SFZ2_6YzIs4La_kyDF1PbXrY.
- A new wave of spam emails is spreading worldwide, using the UNICEF name and a seemingly official email in an effort to persuade people to donate money for the victims of the Gaza conflict.
- MuddyWater is also known as Earth Vetala, MERCURY, Static Kitten, Seedworm, and TEMP.Zagros.
- Files created by the malware, including the configuration files and communication logs.
- The malicious file impersonates a legitimate file that is signed as a Google Update executable file.
- Files created by the scam websites, including fake images and reviews.
- Experts first noticed a MuddyWater campaign in late 2017 hitting several targets in the Middle East.
- PowGoop consists of three components: a DLL file, an executable, and a legitimate filename.
- Logs of the malicious file impersonating a legitimate file.

- Logs of the malware used by MuddyWater, including the command and control protocols.
- Logs of the Small Sieve beacons using the Telegram Bot API.
- Network connections to the UNICEF website and other humanitarian organizations.
- Gaming laptop scams have grown more sophisticated, preying on unsuspecting buyers looking for deals.
- The group conducts cyber espionage and malicious campaigns targeting organizations in various sectors.

Attack Step 3.1

===
Name: Obfuscated Files or Information as used by the malware
Description: The program strings and updated Telegram credentials are protected by a two-pronged obfuscation technique employed by the malware. Hex byte order swapping, a custom encoding scheme, is utilized to obfuscate the data within the code, hindering direct interpretation and comprehension of its true meaning. Furthermore, a custom base64 encoding function is employed, likely involving additional transformations or manipulations before and after base64 encoding, to further obfuscate the data.

MITRE Technique

ID: T1027
Name: Obfuscated files or information
Description: Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.
More info: https://attack.mitre.org/techniques/T1027/

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 3.2

===
Name: Execution Guardrails as used by the malware
Description: The execution of the Small Sieve payload by MuddyWater is contingent upon the provision of the specific command-line argument "Platypus".

MITRE Technique

ID: T1480
Name: Execution guardrails
Description: Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary’s campaign. Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical

devices, files, joined Active Directory (AD) domains, and local/external IP addresses.
More info: https://attack.mitre.org/techniques/T1480/

Indicators

- Small Sieve sample (Filename: gram_app.exe)
- Small Sieve sample (Filename: index.exe)
- Path: %LocalAppData%\MicrosoftWindowsOutlookDataPlus.txt
- Path: %AppData%\OutlookMicrosift\index.exe

Attack Step 3.3

==
Name: Masquerading: Match Legitimate Name or Location as used by the malware
Description: Filename variations incorporating "Microsift" and "Outlook" are employed by the malware to facilitate concealment. This tactic aims to mimic legitimate Windows files, potentially evading detection by users through superficial filename examination. The subtle misspelling and association with prevalent software functionalities may contribute to a perception of reduced suspiciousness.

MITRE Technique

ID: T1036
Name: Masquerading
Description: Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.
More info: https://attack.mitre.org/techniques/T1036/

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

Milestone 4

Pre-Conditions:

- The malware has a configured Bot ID.
- The malware has a valid HTTPS connection.
- The malware has access to the host's IP address.
- The Telegram API is available.
- Resources: The malware requires computational resources to process the web protocols and communicate with the Telegram API and Bot API.
- Environment: A network environment with web protocols (HTTP and HTTPS) available.
- The system has the necessary resources, such as memory and processing power, to execute the malware.
- Tools: Small Sieve, Telegram API, and HTTP protocol.
- The system has the necessary configuration to enable the use of the Telegram API.
- The system has a network connection.
- Connectivity: A network connection to the Telegram Bot API.
- The system has the necessary configuration to enable the use of the HTTP protocol.
- The system has the necessary tools, such as Small Sieve, installed.
- Environment: A system with a network connection and the necessary tools, such as Small Sieve, installed.
- Permissions: The necessary permissions to execute the malware and access the Telegram API.
- The malware is present in the system.

Post-Conditions:

- Experts first noticed a MuddyWater campaign in late 2017 hitting several targets in the Middle East.
- The malware is controlled from behind a proxy network to obfuscate the C2 location.
- The original connection to Telegram is terminated.
- Small Sieve uses variations of Microsoft (Microsift) and Outlook in its filenames to attempt to avoid detection during casual inspection.
- The group conducts cyber espionage and malicious campaigns targeting organizations in various sectors.
- MuddyWater is also known as Earth Vetala, MERCURY, Static Kitten, Seedworm, and TEMP.Zagros.
- The DLL file is contained within an executable, GoogleUpdate.exe.
- Logs of the Small Sieve beacons and tasking.
- Proxy network logs.
- The updated token will be stored in the encoded MicrosoftWindowsOutlookDataPlus.txt file.
- C2 communication logs.
- System logs of the compromised systems.
- Small Sieve beacons using the Telegram Bot API, sending the configured Bot ID, the currently logged-in user, and the host’s IP address.
- The malicious file impersonates a legitimate file that is signed as a Google Update executable file.
- Files with variations of Microsoft (Microsift) and Outlook in their filenames.
- Files created by the malware, such as configuration files and logs.
- The backdoor will reconnect to the Telegram Bot API using the provided token.
- Logs of the Telegram Bot API connections.
- MuddyWater has used one C2 to obtain enumeration scripts and monitor web logs, but a different C2 to send data back.

- Small Sieve's beacons and taskings are performed using Telegram API over HTTPS.
- Malware files uploaded to the victim's machine.
- The group conducts cyber espionage and malicious campaigns targeting organizations in various sectors.
- Logs of the malicious file impersonating a legitimate file.
- MuddyWater has used malware that can upload additional files to the victim's machine.
- The DLL file is contained within an executable, GoogleUpdate.exe.
- Hex byte swapping encoding scheme logs.
- C2 server logs.
- Obfuscated Base64 function logs.
- Small Sieve payload logs.
- Logs of the tools used by MuddyWater, such as Small Sieve.
- The malicious file impersonates a legitimate file that is signed as a Google Update executable file.
- The tasking and beaconing data is obfuscated through a hex byte swapping encoding scheme combined with an obfuscated Base64 function.
- MuddyWater uses tools such as Small Sieve, which employ a custom hex byte swapping encoding scheme to obfuscate tasking traffic.
- MuddyWater has used tools to encode C2 communications, including Base64 encoding.

Attack Step 4.1

==
Name: Application Layer Protocol: Web Protocols as used by the malware
Description: The malware's command and control communications are conducted via the Telegram API over an HTTPS protocol.

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 4.2

==
Name: Data Encoding: Non-Standard Encoding as used by the malware
Description: The tasking traffic is obfuscated by a custom hex byte swapping encoding scheme implemented by the malware, designated as Small Sieve.

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.