Threat actors use copyright infringement phishing lure to deploy infostealers

By Joey Chen

THURSDAY, OCTOBER 31, 2024 09:37

THREATS THREAT SPOTLIGHT

- Cisco Talos has observed an unknown threat actor conducting a phishing campaign targeting Facebook business and advertising account users in Taiwan.
- The decoy email and fake PDF filenames are designed to impersonate a company's legal department, attempting to lure the victim into downloading and executing malware.

- This campaign abuses Google's Appspot[.]com domains, a short URL and Dropbox service, to deliver an information stealer onto the target's machine to avoid network security product detections.
- Talos also observed the threat actor using multiple techniques to evade antivirus detection and sandbox analysis, such as code obfuscation, shellcode encryption, hiding malicious code in resource data to expand the file size to over 700 MB, and embedding LummaC2 or Rhadamanthys information stealers into legitimate binaries.

Phishing email campaign targets Taiwan

Talos observed an unknown threat actor conducting a malicious phishing campaign targeting victims in Taiwan since at least July 2024. The campaign specifically targets victims whose Facebook accounts are used for business or advertising purposes.

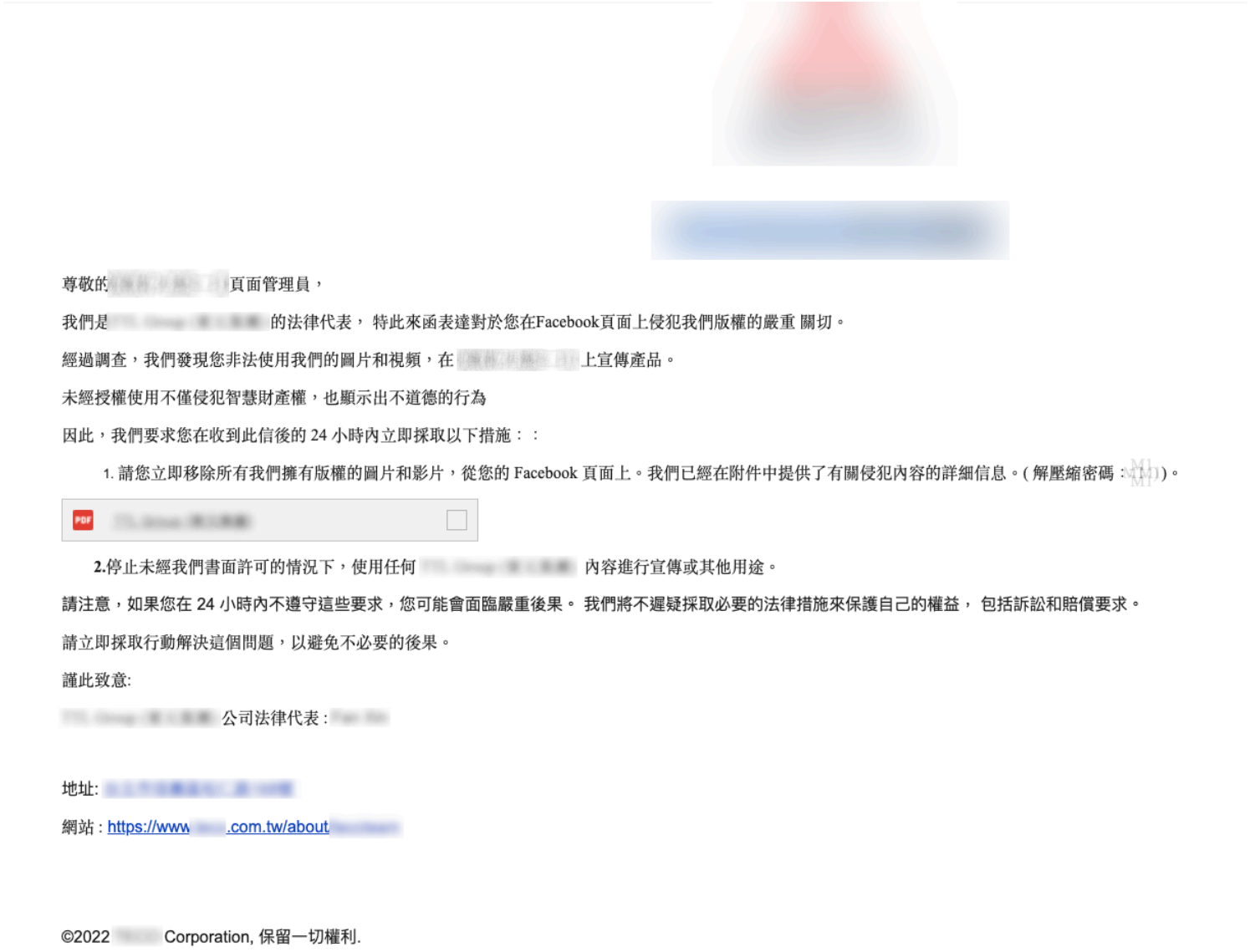
The initial vector of the campaign is a phishing email containing a malware download link. The phishing email uses traditional Chinese in decoy templates and the fake PDF files, suggesting the target is likely traditional Chinese speakers. Some of the fake PDF filenames that we observed during our analysis are:

- IMAGE COPYRIGHTED.exe
- [Redacted] 的影片內容遭到侵犯版權.exe (translates to “[Redacted]'s video content has been copyright infringed.exe”)
- 版權侵權信息- [Redacted] Media Co Ltd.exe (translates to “Copyright Infringement Information - [Redacted] Media Co Ltd.exe”)
- 版權侵權信息- [Redacted] Media Group Inc.exe (translates to “Copyright Infringement Information - [Redacted] Media Group Inc.exe”)
- 版權侵權信息- [Redacted] Technology Group.exe (translates to “Copyright Infringement Information - [Redacted] Technology Group.exe”)
- 版權侵權信息- [Redacted] Co. Ltd.exe (translates to “Copyright Infringement Information - [Redacted] Co. Ltd.exe”)
- [Redacted] Online -宣布侵權.exe (translates to “[Redacted] Online - declare infringement.exe”)

The decoy email and fake PDF filenames are designed to impersonate a company's legal department, attempting to lure the victim into downloading and executing malware. Another observation we found is that the fake PDF malware uses the names of well-known technology and media companies in Taiwan and Hong Kong. This provides strong evidence that the threat actor conducted thorough research before launching this campaign.

Additionally, we observed two phishing emails masquerading as notices from a well-known industrial motor manufacturer and a famous online shopping store in Taiwan. The emails claim that the company’s legal

representatives have issued a notice to a Facebook page administrator alleging copyright infringement due to the unauthorized use of their images and videos for product promotion. The emails demand the removal of the infringing content within 24 hours, cessation of further use without written permission, and warn of potential legal action and compensation claims for non-compliance. Last but not least, with these two emails, we can easily identify that the threat actor uses the same template with minor modifications, such as changing the company name, legal department information, address, and website.



尊敬的[redacted]頁面管理員，

我們是[redacted]的法律代表， 特此來函表達對於您在Facebook頁面上侵犯我們版權的嚴重 關切。

經過調查，我們發現您非法使用我們的圖片和視頻，在[redacted]上宣傳產品。

未經授權使用不僅侵犯智慧財產權，也顯示出不道德的行為

因此，我們要求您在收到此信後的 24 小時內立即採取以下措施：：

1. 請您立即移除所有我們擁有版權的圖片和影片，從您的 Facebook 頁面上。我們已經在附件中提供了有關侵犯內容的詳細信息。(解壓縮密碼：[redacted])。

PDF [redacted]

2.停止未經我們書面許可的情況下，使用任何[redacted]內容進行宣傳或其他用途。

請注意，如果您在 24 小時內不遵守這些要求，您可能會面臨嚴重後果。 我們將不遲疑採取必要的法律措施來保護自己的權益， 包括訴訟和賠償要求。

請立即採取行動解決這個問題，以避免不必要的後果。

謹此致意:

[redacted]公司法律代表：[redacted]

地址: [redacted]

網站 : https://www[redacted].com.tw/about[redacted]

©2022 [redacted] Corporation, 保留一切權利.

Phishing email impersonating a well-known industrial motor manufacturer.

首頁

尊敬的 頁面管理員 ·

我們是 的法律代表 · 特此來函表達對於您在Facebook頁面上侵犯我們版權的嚴重 關切 ·

經過調查 · 我們發現您非法使用我們的圖片和視頻 · 在 上宣傳產品 ·

未經授權使用不僅侵犯智慧財產權 · 也顯示出不道德的行為

因此 · 我們要求您在收到此信後的 24 小時內立即採取以下措施 : :

1. 請您立即移除所有我們擁有版權的圖片和影片 · 從您的 Facebook 頁面上 · 我們已經在附件中提供了有關侵犯內容的詳細信息 · (解壓縮密碼 :) ·

PDF

2.停止未經我們書面許可的情況下 · 使用任何 內容進行宣傳或其他用途 ·

請注意 · 如果您在 24 小時內不遵守這些要求 · 您可能會面臨嚴重後果 · 我們將不遲疑採取必要的法律措施來保護自己的權益 · 包括訴訟和賠償要求 ·

請立即採取行動解決這個問題 · 以避免不必要的後果 ·

Phishing email impersonating a famous online shopping store.

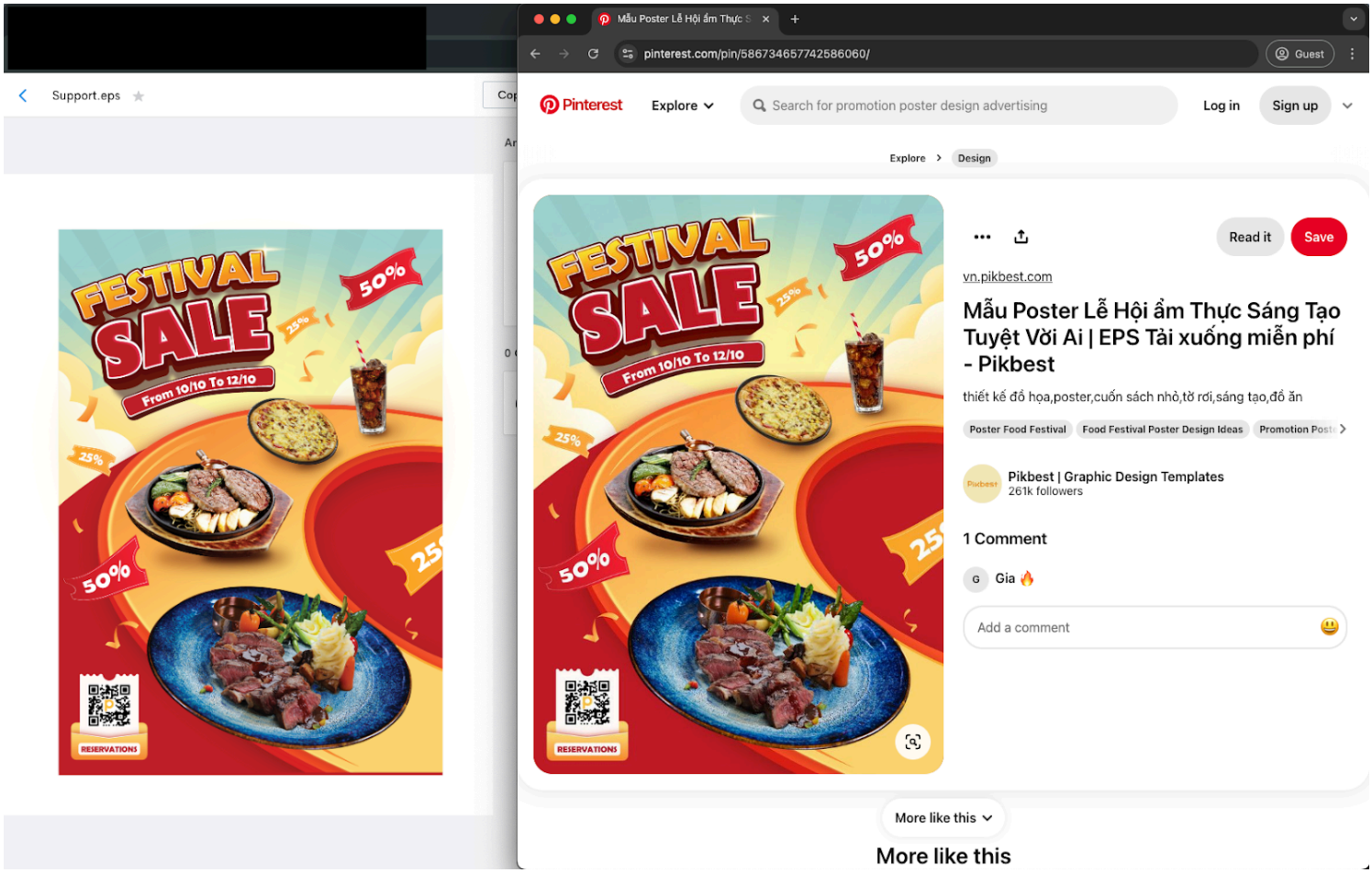
Attribution

Talos observed an unknown image printing file within the encrypted archive, with the filename "Support." Based on the file name and file size, it is likely that all encrypted archives we found on VirusTotal, which we have not been able to decrypt, contain the same EPS files inside. Pivoting off the EPS file metadata and its preview image on a search engine, we found an identical image with the same file name on a Vietnamese-language website. However, there is no strong evidence that it was created by an author from that region.

Support

```
ÐÐÓÆ NULNULNULWe4BSNULNULNULNULNULNULNULNULwe4BS7BSONULÿÿNULNUL%!PS-Adobe-3.1 EPSF-3.0
%ADO_DSC_Encoding: Windows Roman
%%Title: Awesome Creative Food Festival Poster Template Ai.eps
%%Creator: Adobe Illustrator(R) 23.0
%%For: ACER
%%CreationDate: 5/9/2023
%%BoundingBox: 0 0 1809 2363
%%HiResBoundingBox: 0 0 1808.6401 2362.9849
%%CropBox: 0 0 1808.6401 2362.9849
%%LanguageLevel: 2
%%DocumentData: Clean7Bit
%ADOBeginClientInjection: DocumentHeader "AI11EPS"
%%AI8_CreatorVersion: 23.0.0
%AI9_PrintingDataBegin
%ADO_BuildNumber: Adobe Illustrator(R) 23.0.0 x530 R agm 4.7767 ct 5.4352
%ADO_ContainsXMP: MainFirst
%AI7_Thumbnail: 100 128 8
%%BeginData: 19342 Hex Bytes
%000033000066000099000CC00330000333300336600339900 33CC0033FF
%006600006633006666006699006 6CC0066FF009900009933009966009999
%0099CC0099FF00CC0000CC3300CC6600CC9900CCCC00CCFF00FF3300FF66
%00FF9900FFCC330000330033330066330099330 0CC3300FF333300333333
%3333663333993333CC3333FF33660033663333666633669933 66CC3366FF
%339900339933339966339999339 9CC3399FF33CC0033CC3333CC6633CC99
```

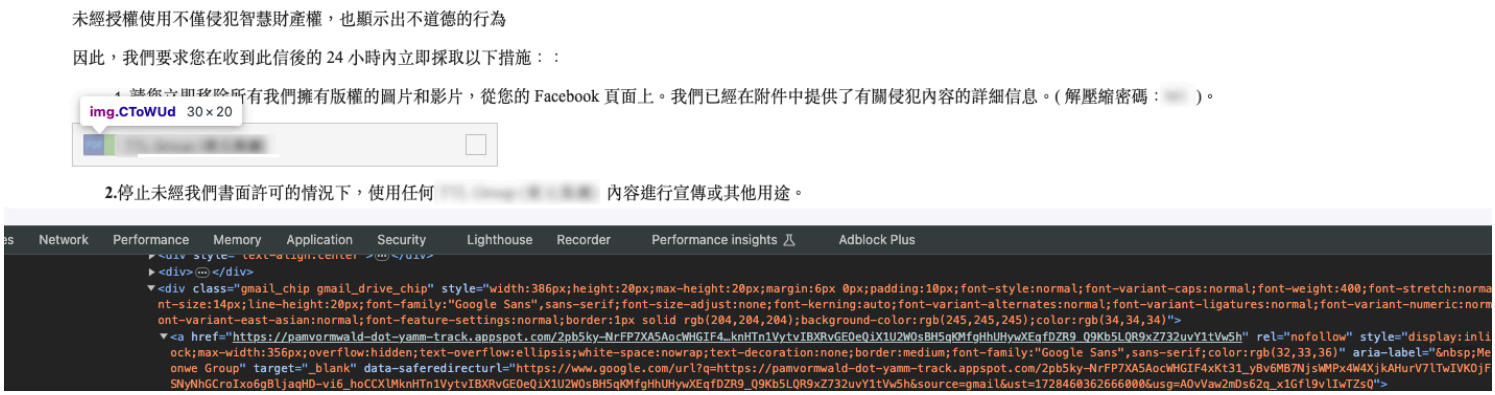
Support EPS file metadata.



The support EPS file preview image in this campaign (left) and the image we found from the internet (right).

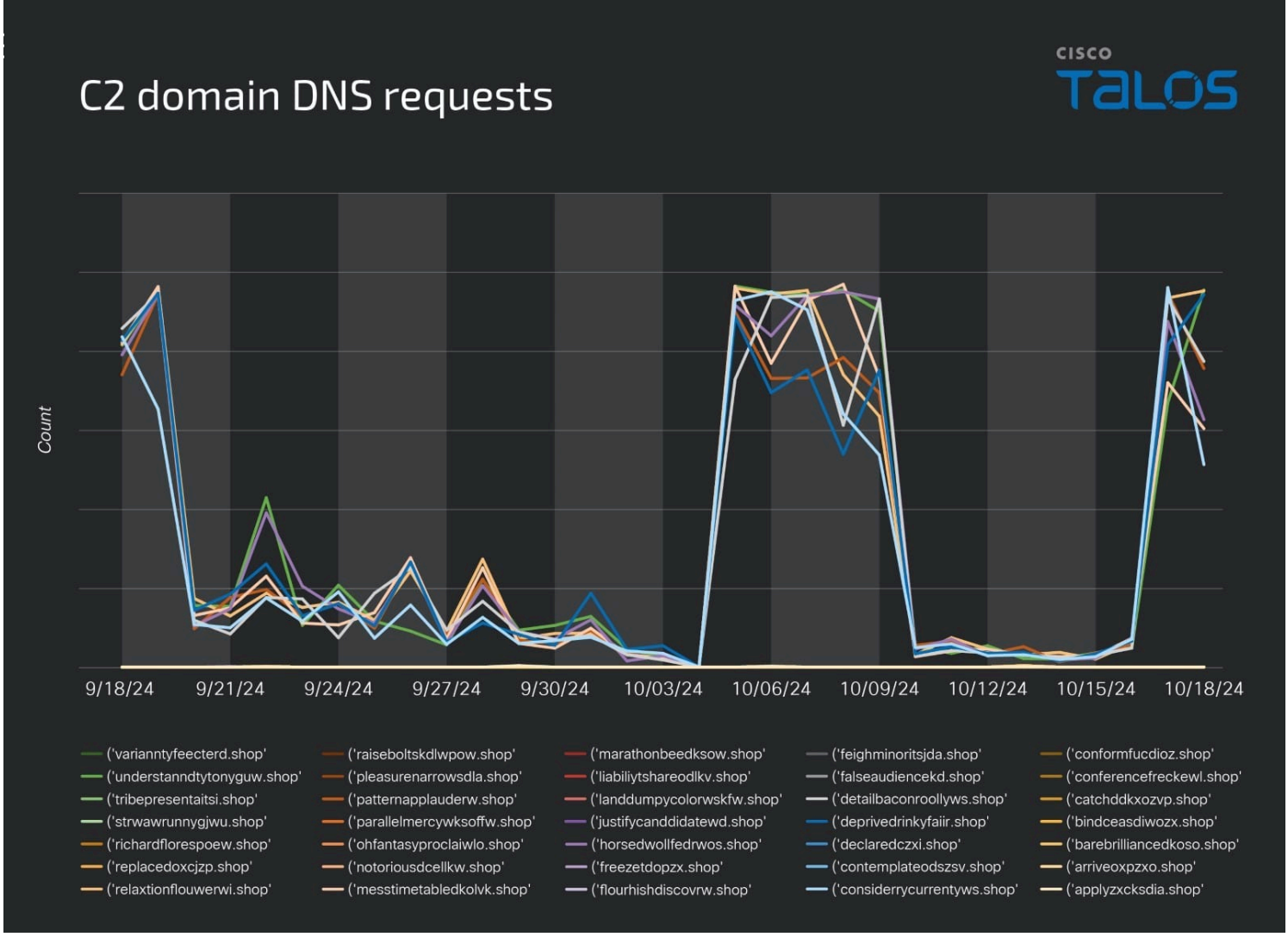
Actor infrastructure

The threat actor is abusing Google's Appspot.com domains, a short URL and Dropbox service, to deliver an information stealer onto the target's machine. Appspot.com is a cloud computing platform for developing and hosting web applications in Google-managed data centers. When the victim clicks on the download link, it initially connects to Appspot.com, then redirects to a short URL created by a third-party service, and finally redirects to Dropbox to download the malicious archive. The actor is using the third-party data storage service as a download server to deceive network defenders.



Malware download link.

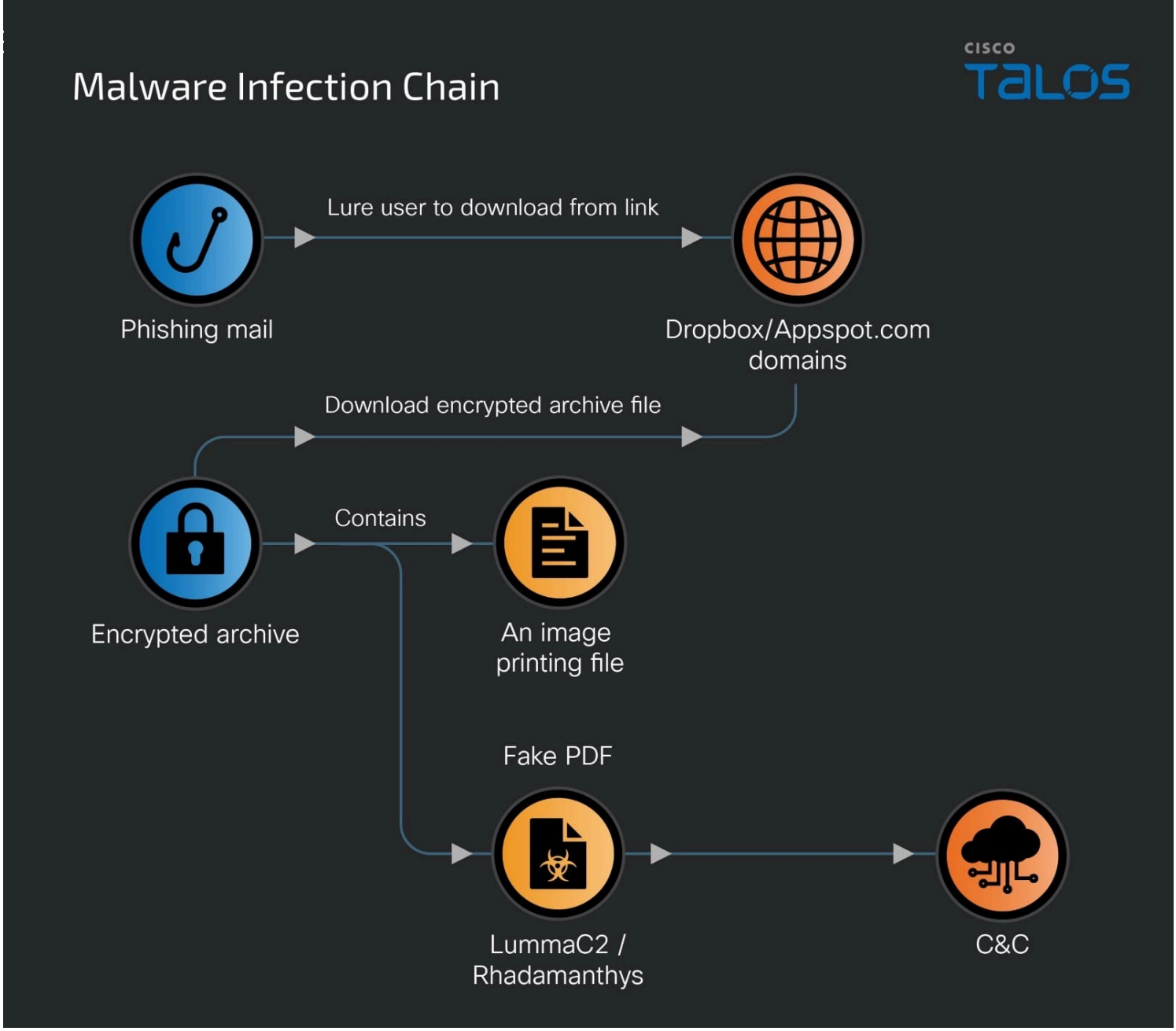
We also discovered that the actor is using multiple command and control (C2) domains in the campaign. The DNS requests for the domains during our analysis period are shown in the graph, indicating the campaign is ongoing.



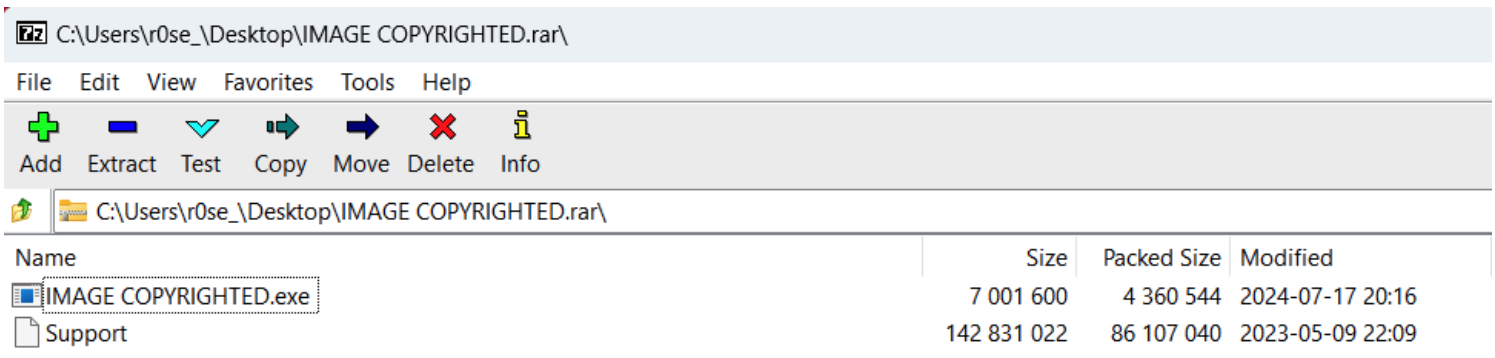
C2 domain DNS requests.

Malware infection summary

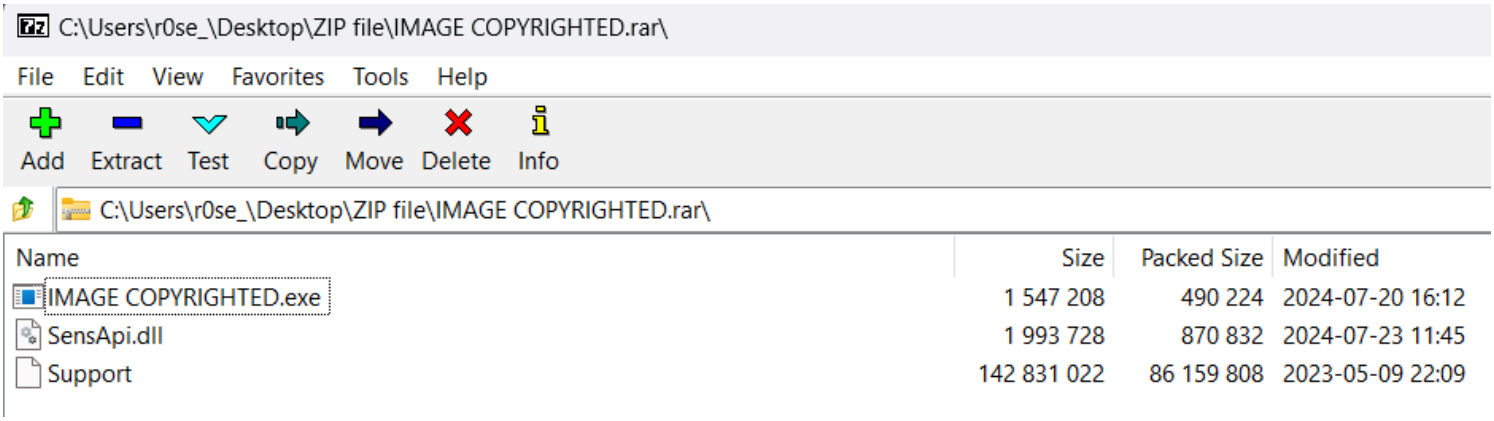
The infection chain begins with a phishing email containing a malicious download link. When the victim downloads the malicious RAR file, they will need a specific password to extract it, revealing a fake PDF executable malware and an image printing file. Once the malware is decrypted and the fake PDF executable is run, it will execute the embedded LummaC2 or Rhadamanthys information stealer, which then collects the victim's credentials and data, sending them back to the C2 server.



The malicious RAR file usually contains a fake PDF executable malware and an image printing file, but we observed a few malicious RAR files that contain an additional DLL file. However, without the correct password, we are not able to extract the malicious RAR file and analyze it.

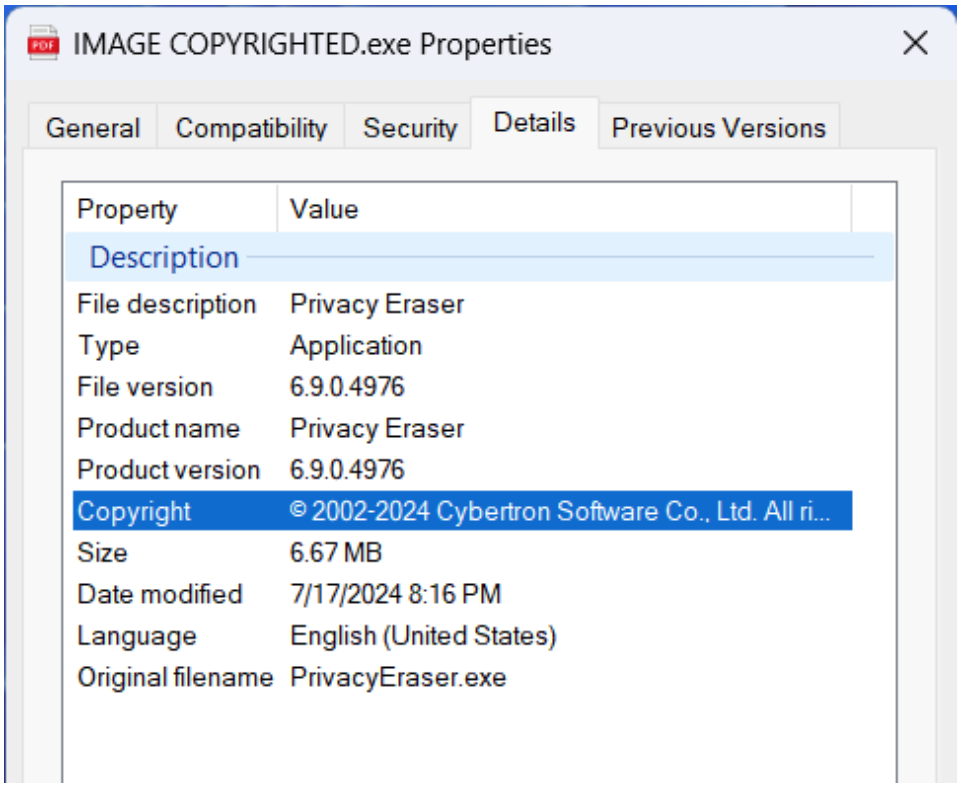


The RAR file contains a fake PDF and an image printing file.



The RAR file contains a fake PDF, an image printing file, and additional DLL file.

The fake PDF executable malware variant was delivered as a payload in this campaign. This malware will embed LummaC2 or Rhadamanthys information stealers into legitimate binary and the legitimate binary including iMazing Converter, foobar2000, Punto Switcher, PDF Visual Repair, LedStatusApp, and PrivacyEraser. Below shows one of the file details of the fake PDF executable.



Fake PDF file detail information.

LummaC2 stealer and its loader

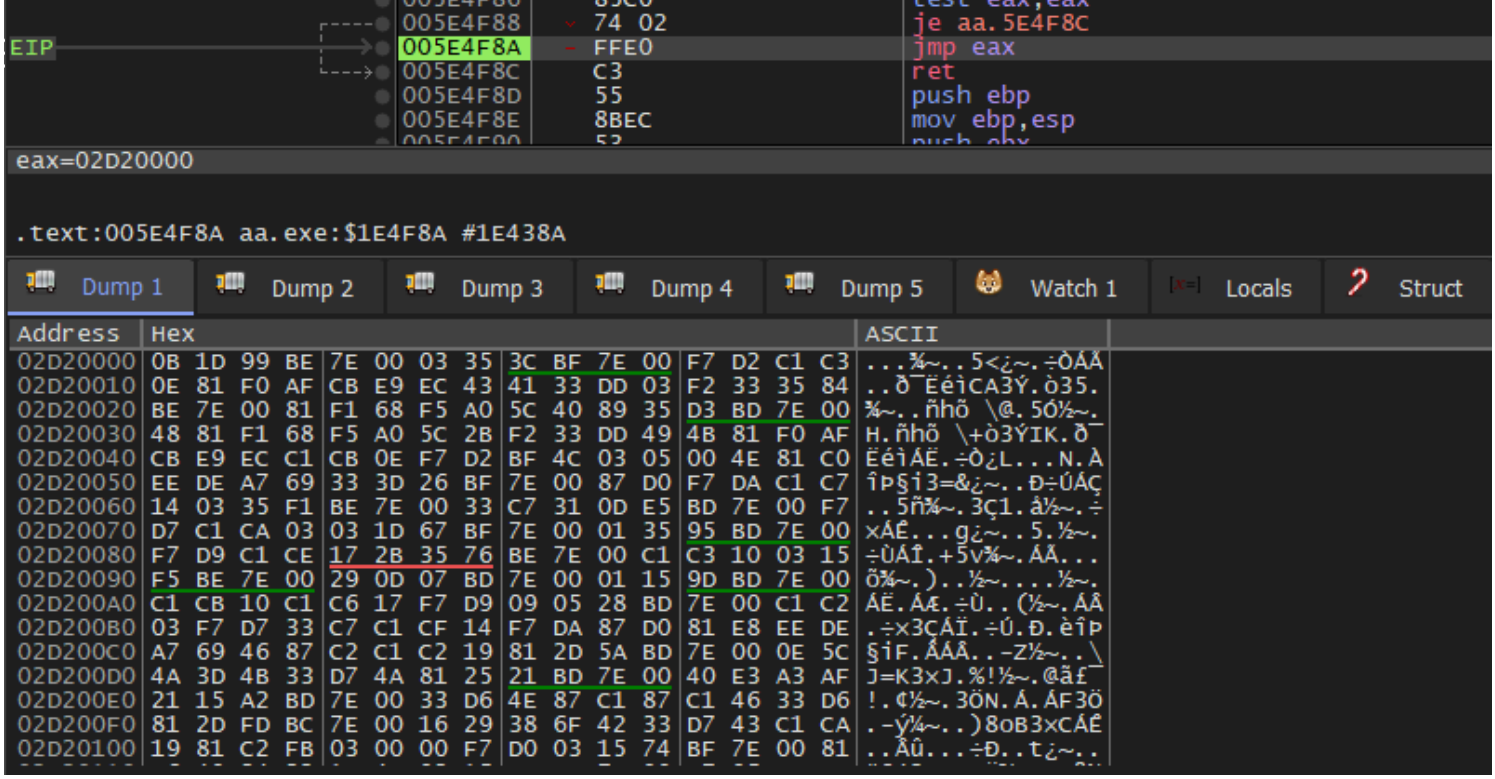
LummaC2 Stealer is a type of malware designed to exfiltrate sensitive information from compromised systems. It can target system details, web browsers, cryptocurrency wallets, and browser extensions. Written in C, this malware is sold on underground forums. To avoid detection and analysis, it employs various obfuscation methods. The malware connects to a C2 server to receive instructions and transmit the stolen data.

The loader for LummaC2 changes the execution flow of the binary malware, causing it to invoke an unknown library to execute the malicious code functions. This strategic modification complicates detection and analysis efforts. Once these malicious functions are invoked, the malware utilizes the CreateFileMappingA API to write the payload into a mapped memory block, effectively hiding it within the system's memory. After successfully mapping the payload, the malware then executes it.

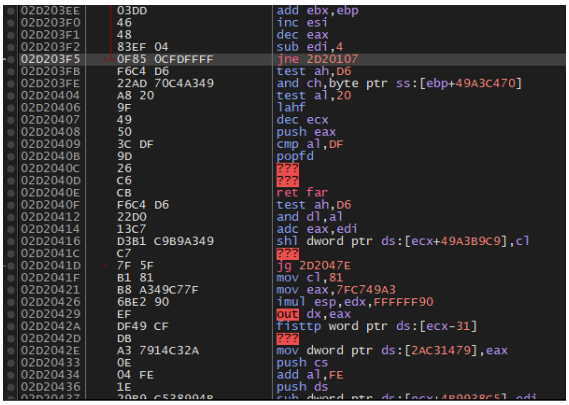
```
.text:0056F19A ; int __cdecl Lummac2_point_function(int)
.text:0056F19A Lummac2_point_function proc near        ; CODE XREF: sub_563703+5B↑p
.text:0056F19A                                         ; sub_569D29+2D↑p ...
.text:0056F19A
.text:0056F19A arg_0           = dword ptr  8
.text:0056F19A
.text:0056F19A                 push    ebp
.text:0056F19B                 mov     ebp, esp
.text:0056F19D                 push    [ebp+arg_0]
.text:0056F1A0                 call    unknown_libname_49 ; Microsoft VisualC 14/net runtime
.text:0056F1A5                 pop     ecx
.text:0056F1A6                 pop     ebp
.text:0056F1A7                 retn
.text:0056F1A7 Lummac2_point_function endp
```

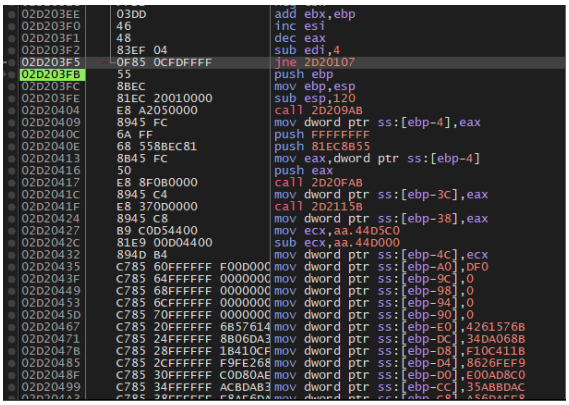
Call to an unknown library to execute the malicious code functions.

When the malware begins executing the shellcode in memory, it first decrypts the second half of the program block, which contains part of the shellcode loader and the LummaC2 malware execution file. Once the decryption is complete, it will call the VirtualAllocate API to allocate a memory block, write the information stealer's execution file to that block, and then execute it.



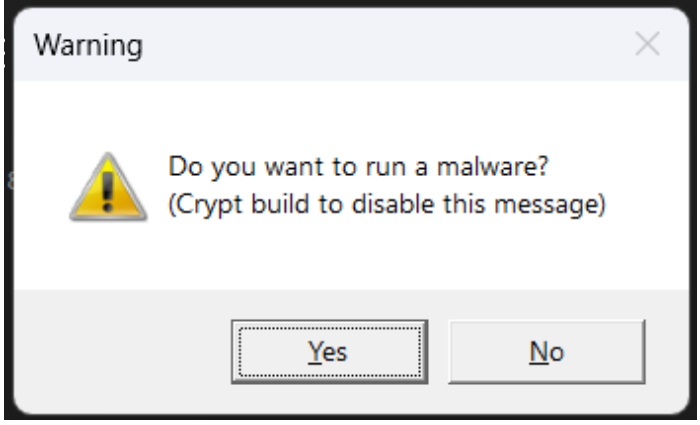
Jump code to shellcode block.



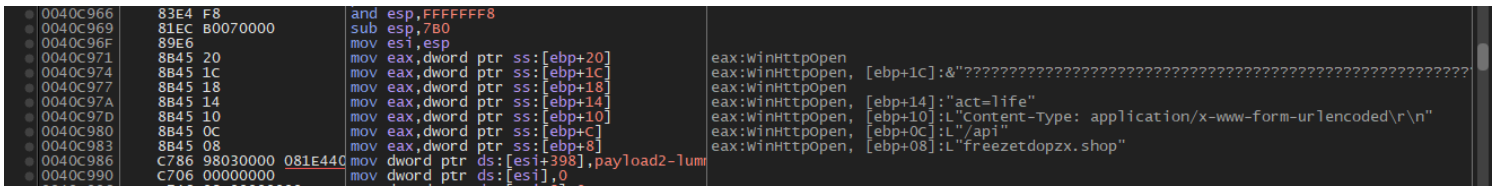


Encrypted shellcode (left side) and decrypted shellcode (right side).

We also collected all of the build IDs of the LummaC2 in this campaign and below are the screenshots of the LummaC2 stealer alert message box and its POST message.



Alert message shown to the user when executing LummaC2.



POST message with act=life and url path /api.

Build ID:

- sTDsFx--Socks
- iAIMAC--ghost

Rhadamanthys stealer and its loader

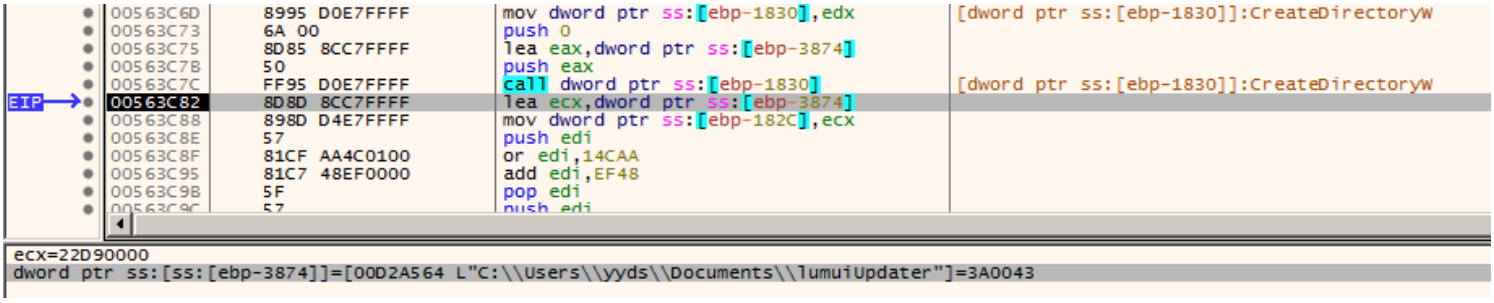
Rhadamanthys is a sophisticated information stealer that emerged in 2022 and is sold on underground forums. This comprehensive stealer malware is capable of gathering system information, credentials, cryptocurrency wallets, browser passwords, cookies, and data from various other applications. It employs numerous anti-analysis techniques, complicating analysis efforts and hindering its execution in sandbox environments.

We observed the Rhadamanthys loader in this campaign contains 10 sections in its binary structure. Despite the presence of multiple sections, the threat actor specifically targets the .rsrc section to insert the malicious code. This section is heavily obfuscated to conceal the malicious activities and make analyses more challenging. The choice of the .rsrc section is strategic, as it is typically associated with resource data like icons and menus, making it less likely to raise immediate suspicion.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000A50E8	00001000	000A5200	00000400	00000000	00000000	0000	0000	60000020
.itext	00001668	000A7000	00001800	000A5600	00000000	00000000	0000	0000	60000020
.data	000037A4	000A9000	00003800	000A6E00	00000000	00000000	0000	0000	C0000040
.bss	00006778	000AD000	00000000	00000000	00000000	00000000	0000	0000	C0000000
.idata	00000F1C	000B4000	00001000	000AA600	00000000	00000000	0000	0000	C0000040
.didata	000001A4	000B5000	00000200	000AB600	00000000	00000000	0000	0000	C0000040
.edata	0000009A	000B6000	00000200	000AB800	00000000	00000000	0000	0000	40000040
.tls	00000018	000B7000	00000000	00000000	00000000	00000000	0000	0000	C0000000
.rdata	0000005D	000B8000	00000200	000ABA00	00000000	00000000	0000	0000	40000040
.rsrc	000FBD34	000B9000	000FBE00	000ABC00	00000000	00000000	0000	0000	40000040

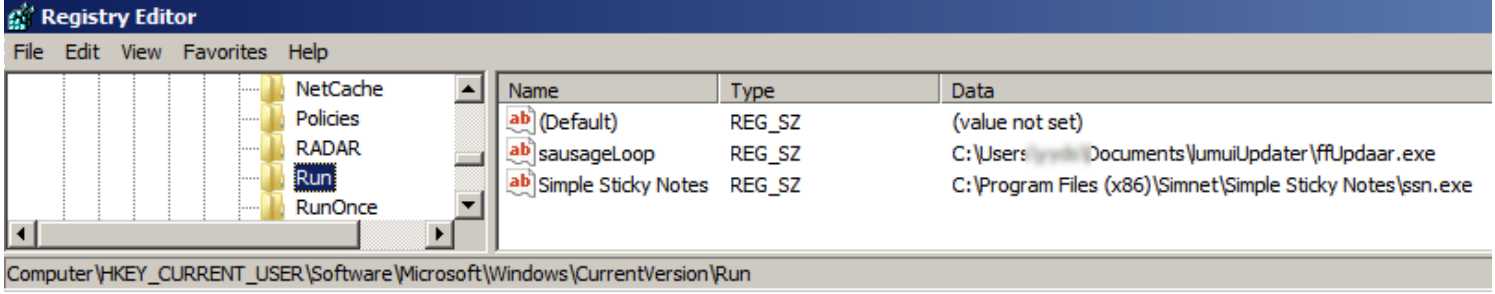
The loader of Rhadamanthys binary structure sections.

After analysis, we discovered that the Rhadamanthys loader employs several sophisticated techniques to ensure its persistence and evasion. Initially, the loader copies itself and writes the file to “C:\Users\[user]\Documents\lumuiUpdater\ffUpdaar.exe”. In order to avoid detection by antivirus programs and sandbox environments, it expands the file size to over 700 MB. This significant increase in file size is intended to bypass heuristic and signature-based detection mechanisms commonly used by security products, which may struggle to process such large files effectively.



The loader copies itself to the lumuiUpdater folder.

Furthermore, the loader is configured to start automatically by modifying the Windows Registry. It writes an entry to “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” and key name value “sausageLoop”, a registry key that specifies programs to be launched during the system startup. This registry modification ensures that the malicious loader is executed every time the victim's computer restarts, thereby maintaining its persistence on the infected system.



The loader is configured to start automatically.

Finally, the loader executes the legitimate system process "%Systemroot%\system32\dialer.exe" and injects Rhadamanthys' payload into it. This process injection technique allows the malware to run its malicious code within the context of a legitimate system process, further evading detection. Additionally, it uses mutex objects to ensure that only one instance of the malware runs on the infected host. Below is the list of mutex names we observed in this campaign, which has also been disclosed in previous reporting by other.

- Global\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
- Session\1\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
- Session\2\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
- Session\3\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
- Session\4\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
- Session\5\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
- Session\6\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
- Session\7\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
- Session\8\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}

Coverage

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**Cisco Secure Web Appliance (Web Security Appliance)**
✓	✓	✓	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protection with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. Snort SIDs for this threat are 64167-64169.

IOC

IOCs for this research can also be found at our GitHub repository here.

RELATED CONTENT

Exploring vulnerable Windows drivers

DECEMBER 19, 2024 06:04

This post is the result of research into the real-world application of the Bring Your Own Vulnerable Driver (BYOVD) technique along with Cisco Talos' series of posts about malicious Windows drivers.

Unwrapping the emerging Interlock ransomware attack

NOVEMBER 7, 2024 06:00

Cisco Talos Incident Response (Talos IR) recently observed an attacker conducting big-game hunting and double extortion attacks using the relatively new Interlock ransomware.

Threat actor abuses Gophish to deliver new PowerRAT and DCRAT

OCTOBER 22, 2024 06:00

Cisco Talos recently discovered a phishing campaign using an open-source phishing toolkit called Gophish by an unknown threat actor.