



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.



Phishing email impersonating a well-known industrial motor manufacturer.



Facebook 首頁

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])。



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。

Phishing email impersonating a famous online shopping store.

Attribution

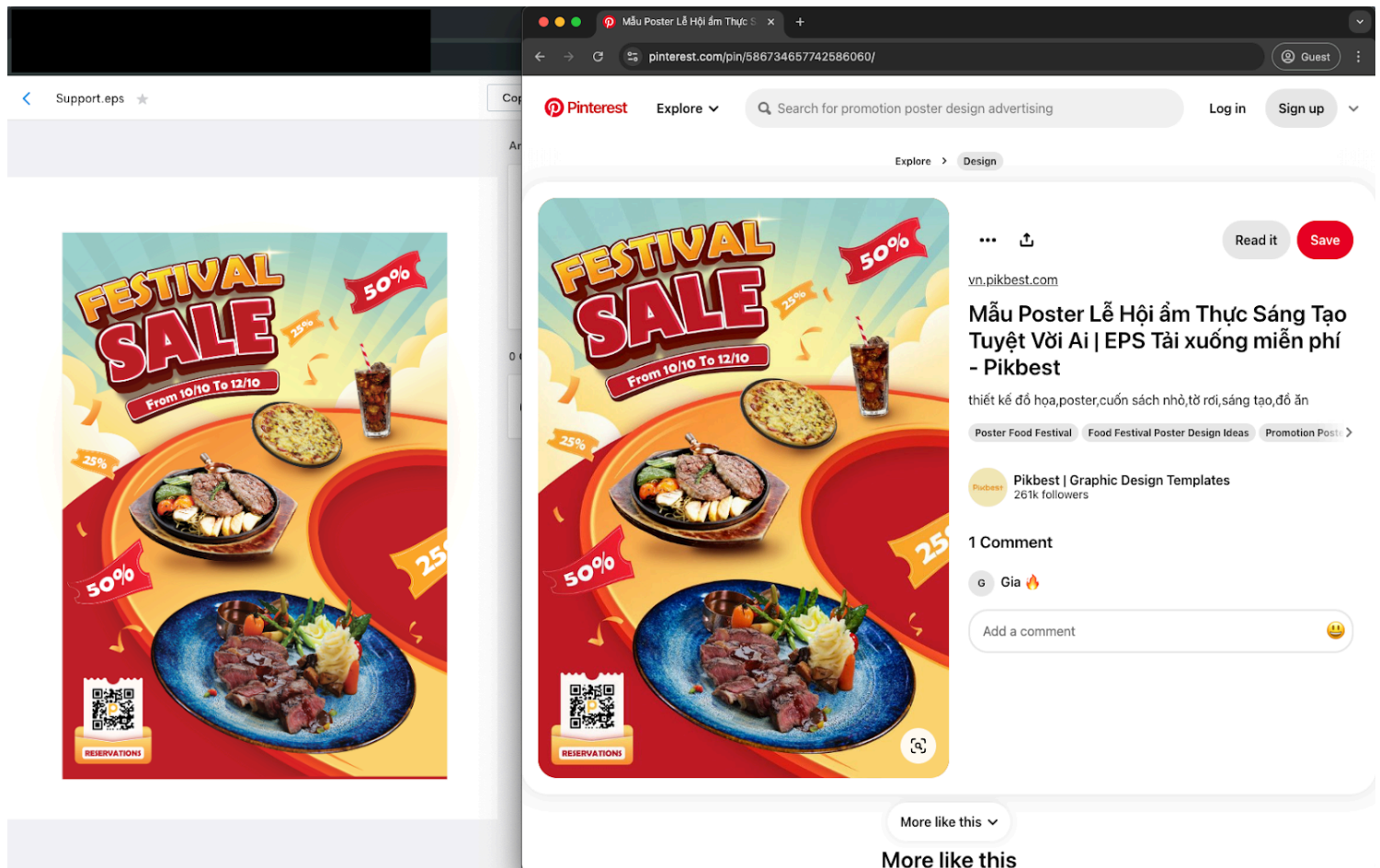
Talos observed an unknown image printing file within the encrypted archive, with the filename "Support." Based on the file name and file size, it is likely that all encrypted archives we found on VirusTotal, which we have not been able to decrypt, contain the same EPS files inside. Pivoting off the EPS 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 x
1  %ADOE  NUBNUBNUBwe4BSNUBNUBNUBNUBNUBNUBNUBNUBNUBNUBwe4BS7BSNUBNUBNUBNUBNUBNUBNUBNUBNUBNUB!PS-Adobe-3.1 EPSF-3.0
2  %%ADO_DSC_Encoding: Windows Roman
3  %%Title: Awesome Creative Food Festival Poster Template Ai.eps
4  %%Creator: Adobe Illustrator(R) 23.0
5  %%For: ACER
6  %%CreationDate: 5/9/2023
7  %%BoundingBox: 0 0 1809 2363
8  %%HiResBoundingBox: 0 0 1808.6401 2362.9849
9  %%CropBox: 0 0 1808.6401 2362.9849
10 %%LanguageLevel: 2
11 %%DocumentData: Clean7Bit
12 %%ADOBEGINCLIENTINJECTION: DocumentHeader "AI11EPS"
13 %%AI8_CreatorVersion: 23.0.0
14 %%AI9_PrintingDataBegin
15 %%ADO_BuildNumber: Adobe Illustrator(R) 23.0.0 x530 R agm 4.7767 ct 5.4352
16 %%ADO_ContainsXMP: MainFirst
17 %%AI7_Thumbnail: 100 128 8
18 %%BeginData: 19342 Hex Bytes
19 %0000330000660000990000CC0033000033330033660033990033CC0033FF
20 %0066000066330066660066990066CC0066FF009900009933009966009999
21 %0099CC0099FF00CC0000CC3300CC6600CC9900CCCC00CCFF00FF3300FF66
22 %00FF9900FFCC3300003300333300663300993300CC3300FF333300333333
23 %3333663333993333CC3333FF3366003366333366663366993366CC3366FF
24 %3399003399333399663399993399CC3399FF33CC0033CC3333CC6633CC99
25 %33CCCC33CCFF33FF0033FF3333FF6633FF9933FFCC33FFFF660000660033

```

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.

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：

4 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：)。

img.CToWUd 30x20

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。

Network Performance Memory Application Security Lighthouse Recorder Performance insights Adblock Plus

<div style="text-align:center"></div>

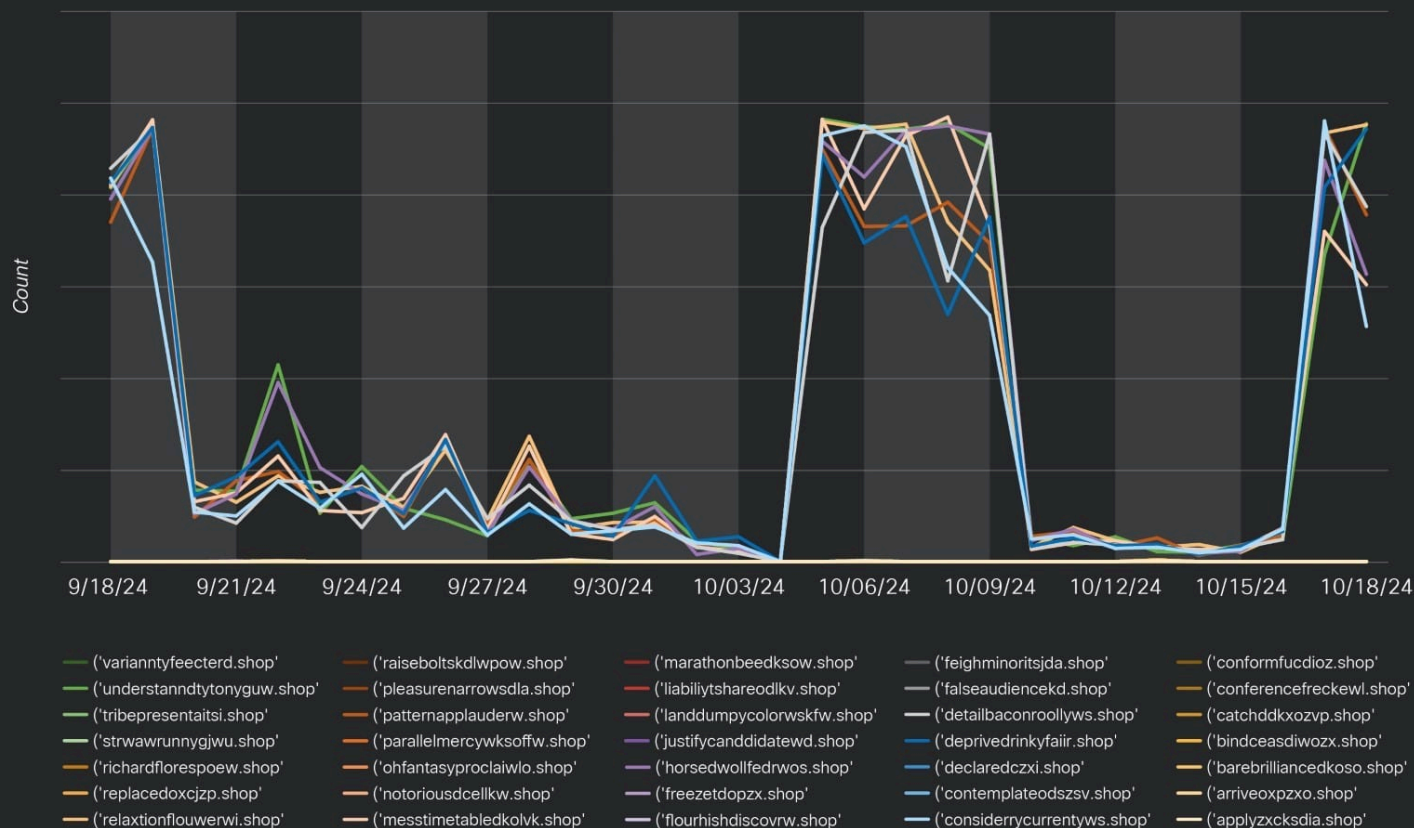
<div></div>

<div class="gmail_chip gmail_drive_chip" style="width:386px;height:20px;max-height:20px;margin:6px 0px;padding:10px;font-style:normal;font-variant-caps:normal;font-weight:400;font-stretch:normal;font-size:14px;line-height:20px;font-family:"Google Sans",sans-serif;font-size-adjust:none;font-kerning:auto;font-variant-alternates:normal;font-variant-ligatures:normal;font-variant-numeric:normal;font-variant-east-asian:normal;font-feature-settings:normal;border:1px solid rgb(204,204,204);background-color:rgb(245,245,245);color:rgb(34,34,34)">

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

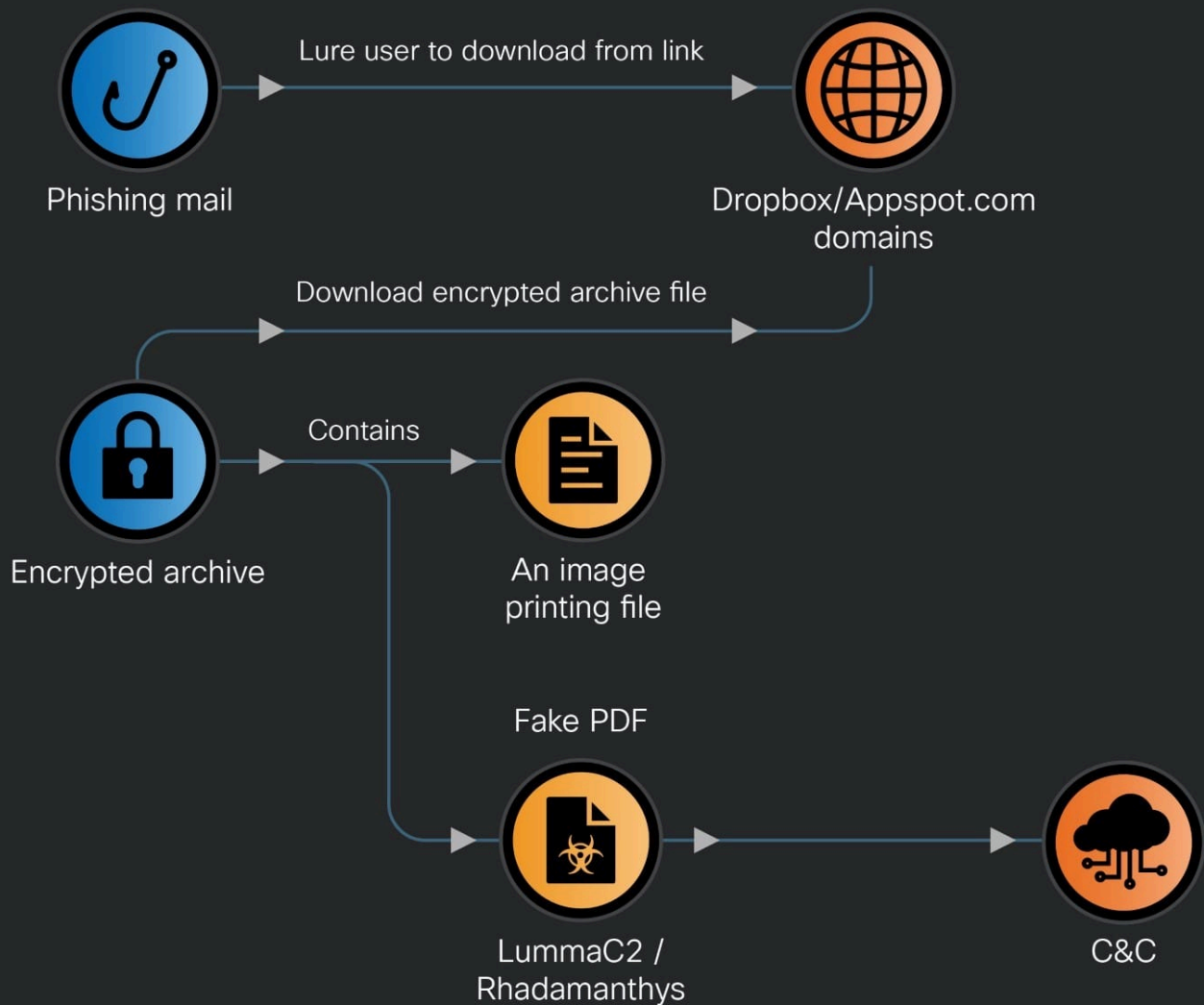


C2 domain DNS requests.

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.

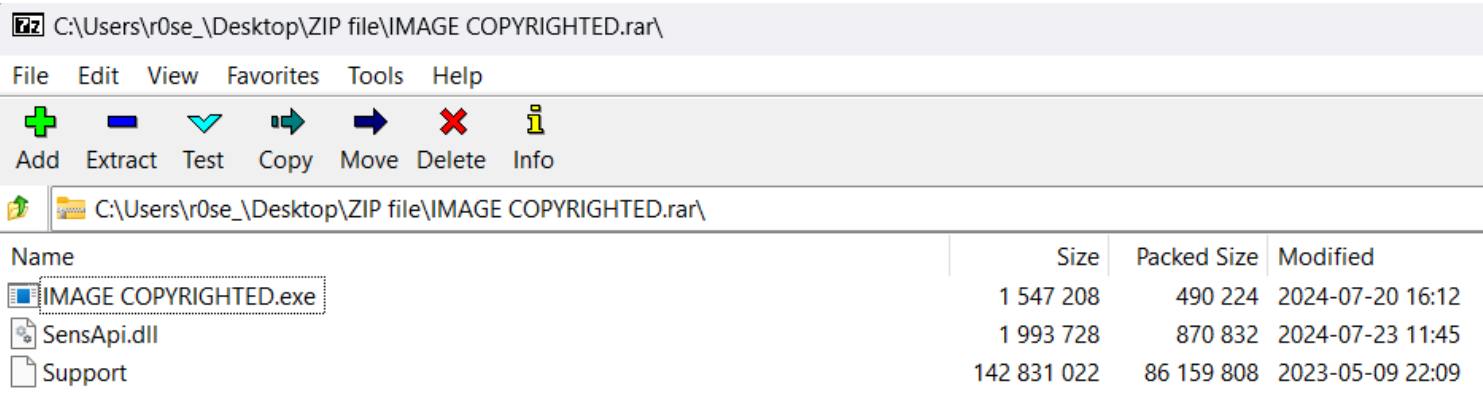
Malware Infection Chain



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.

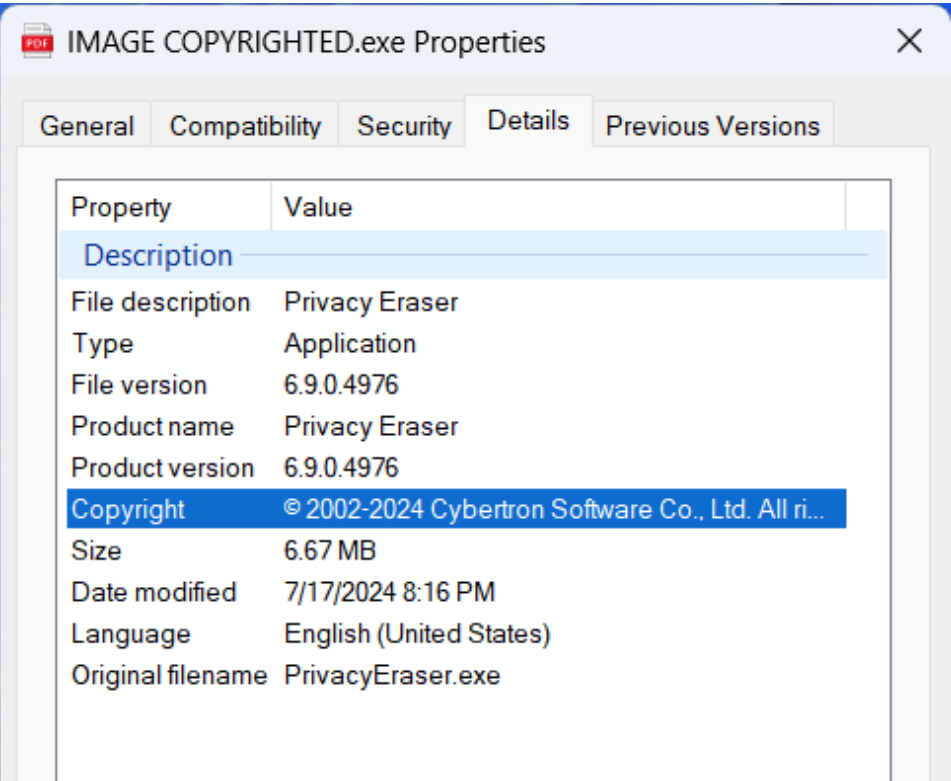
C:\Users\r0se_\Desktop\IMAGE COPYRIGHTED.rar\			
File Edit View Favorites Tools Help			
Add Extract Test Copy Move Delete Info			
C:\Users\r0se_\Desktop\IMAGE COPYRIGHTED.rar\			
Name	Size	Packed Size	Modified
IMAGE COPYRIGHTED.exe	7 001 600	4 360 544	2024-07-17 20:16
Support	142 831 022	86 107 040	2023-05-09 22:09

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.

005E4F88 85C0 test eax, eax
 005E4F88 74 02 je aa.5E4F8C
 005E4F8C C3 jmp eax
 005E4F8D 55 ret
 005E4F8E 8BEC push ebp
 005E4F8F 53 mov ebp, esp
 005E4F90 53 push ebx

eax=02D20000

.text:005E4F8A aa.exe:\$1E4F8A #1E438A

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

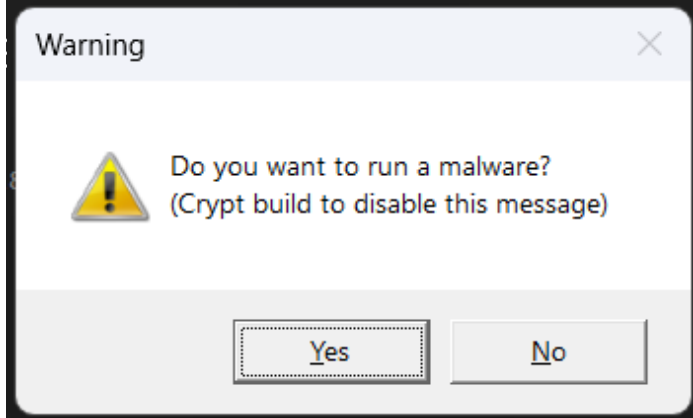
Address	Hex	ASCII
02D20000	0B 1D 99 BE 7E 00 03 35 3C BF 7E 00 F7 D2 C1 C3	...%...5<~.÷0AA
02D20010	0E 81 F0 AF CB E9 EC 43 41 33 DD 03 F2 33 35 84	..ð-EéiCA3Y.ò35.
02D20020	BE 7E 00 81 F1 68 F5 A0 5C 40 89 35 D3 BD 7E 00	%~..ñhõ \@.50%~.
02D20030	48 81 F1 68 F5 A0 5C 2B F2 33 DD 49 4B 81 F0 AF	H.ñhõ \+ò3YIK.ð-
02D20040	CB E9 EC C1 CB 0E F7 D2 BF 4C 03 05 00 4E 81 C0	ÉéiAÉ.÷0L...N.A
02D20050	EE DE A7 69 33 3D 26 BF 7E 00 87 D0 F7 DA C1 C7	îp\$î3=&~..ð÷ÚÁÇ
02D20060	14 03 35 F1 BE 7E 00 33 C7 31 0D E5 BD 7E 00 F7	..5ñ%~.3Ç1.â%~.÷
02D20070	D7 C1 CA 03 03 1D 67 BF 7E 00 01 35 95 BD 7E 00	xÁÉ...g~..5.%~.
02D20080	F7 D9 C1 CE 17 2B 35 76 BE 7E 00 C1 C3 10 03 15	÷ÚÁî.+5v%~.AA...
02D20090	F5 BE 7E 00 29 0D 07 BD 7E 00 01 15 9D BD 7E 00	õ%~..).%~...%~.
02D200A0	C1 CB 10 C1 C6 17 F7 D9 09 05 28 BD 7E 00 C1 C2	ÁÉ.ÁÉ.÷Û..(%~.AA
02D200B0	03 F7 D7 33 C7 C1 CF 14 F7 DA 87 D0 81 E8 EE DE	.÷x3CÁî.÷Û.ð.èîp
02D200C0	A7 69 46 87 C2 C1 C2 19 81 2D 5A BD 7E 00 0E 5C	\$îF.ÁÁÁ..-Z%~.. \
02D200D0	4A 3D 4B 33 D7 4A 81 25 21 BD 7E 00 40 E3 A3 AF	J=K3xJ.%!%~..@ãf
02D200E0	21 15 A2 BD 7E 00 33 D6 4E 87 C1 87 C1 46 33 D6	!.Ç%~.3ÖN.A.ÁF3Ö
02D200F0	81 2D FD BC 7E 00 16 29 38 6F 42 33 D7 43 C1 CA	..ý%~..)8oB3xCÁÉ
02D20100	19 81 C2 FB 03 00 00 F7 D0 03 15 74 BF 7E 00 81	..ÂÛ...÷Ð..t~..

Jump code to shellcode block.

02D203EE	03D0	add ebx,ebp	02D203EE	03D0	add ebx,ebp
02D203F0	46	inc esi	02D203F0	46	inc esi
02D203F1	48	dec eax	02D203F1	48	dec eax
02D203F2	83EF 04	sub edi,4	02D203F2	83EF 04	sub edi,4
02D203F5	0F85 0CFDFFFF	jne 2D20107	02D203F5	0F85 0CFDFFFF	jne 2D20107
02D203FB	F6C4 D6	test ah,D6	02D203FB	55	push ebp
02D203FE	22A0 70C4A349	and ch,byte ptr ss:[ebp+49A3C470]	02D203FE	8BEC	mov ebp,esp
02D20404	A8 20	test al,20	02D20404	81EC 20010000	sub esp,120
02D20406	9F	lahf	02D20404	E8 A2050000	call 2D209AB
02D20407	49	dec ecx	02D20409	8945 FC	mov dword ptr ss:[ebp-4],eax
02D20408	50	push eax	02D2040C	6A FF	push FFFFFFFF
02D20409	3C DF	cmp al,DF	02D2040E	68 5588EC81	push 81EC8855
02D2040B	9D	popfd	02D20413	8B45 FC	mov eax,dword ptr ss:[ebp-4]
02D2040C	26	test	02D20416	50	push eax
02D2040D	C6	ret far	02D20417	E8 8F080000	call 2D20FAB
02D2040E	C8	ret far	02D2041C	8945 C4	mov dword ptr ss:[ebp-3C],eax
02D2040F	F6C4 D6	test ah,D6	02D2041F	E8 370D0000	call 2D21158
02D20412	22D0	and dl,al	02D20424	8945 C8	mov dword ptr ss:[ebp-38],eax
02D20414	13C7	adc eax,edi	02D20427	B9 C0D54400	mov ecx,aa.44D5C0
02D20416	D3B1 C9B9A349	shl dword ptr ds:[ecx+49A3B9C9],cl	02D2042C	81E9 00D04400	sub ecx,aa.44D000
02D2041C	C7	test	02D20432	894D B4	mov dword ptr ss:[ebp-4C],ecx
02D2041D	7F 5F	jg 2D2047E	02D20435	C785 60FFFFFF F00D00	mov dword ptr ss:[ebp-A0],DF0
02D2041F	B1 81	mov cl,81	02D2043F	C785 64FFFFFF 00000000	mov dword ptr ss:[ebp-9C],0
02D20421	B8 A349C77F	mov eax,7FC749A3	02D20449	C785 68FFFFFF 00000000	mov dword ptr ss:[ebp-98],0
02D20426	6BE2 90	imul esp,edx,FFFFFFFF90	02D20453	C785 6CFFFFFF 00000000	mov dword ptr ss:[ebp-94],0
02D20429	EF	out dx,eax	02D2045D	C785 70FFFFFF 00000000	mov dword ptr ss:[ebp-90],0
02D2042A	DF49 CF	fsttp word ptr ds:[ecx-31]	02D20467	C785 20FFFFFF 6857614	mov dword ptr ss:[ebp-E0],42615768
02D2042D	D8	test	02D20471	C785 24FFFFFF 88060A3	mov dword ptr ss:[ebp-DC],34DA0688
02D2042E	A3 7914C32A	mov dword ptr ds:[2AC31479],eax	02D2047B	C785 28FFFFFF 18410CF	mov dword ptr ss:[ebp-D8],F10C4118
02D20433	0E	push cs	02D20485	C785 2CFFFFFF F9FE268	mov dword ptr ss:[ebp-D4],8626FEF9
02D20434	04 FE	add al,FE	02D2048F	C785 30FFFFFF C0D80AE	mov dword ptr ss:[ebp-D0],E00AD8C0
02D20436	1E	push ds	02D20499	C785 34FFFFFF ACDA83	mov dword ptr ss:[ebp-CC],35ABBDAC
02D20438	79D0 C538D049	sub dword ptr ds:[ecx+49D038C1],edi	02D204A3	C785 38FFFFFF 24760A3	mov dword ptr ss:[ebp-C8],35A90688

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.

```

0040C966 8B45 F8      and esp,FFFFFFF8
0040C969 81EC 80070000 sub esp,780
0040C96F 89E6        mov esi,esp
0040C971 8B45 20      mov eax,dword ptr ss:[ebp+20]
0040C974 8B45 1C      mov eax,dword ptr ss:[ebp+1C]
0040C977 8B45 18      mov eax,dword ptr ss:[ebp+18]
0040C97A 8B45 14      mov eax,dword ptr ss:[ebp+14]
0040C97D 8B45 10      mov eax,dword ptr ss:[ebp+10]
0040C980 8B45 0C      mov eax,dword ptr ss:[ebp+0C]
0040C983 8B45 08      mov eax,dword ptr ss:[ebp+08]
0040C986 C786 98030000 081E44C0 mov dword ptr ds:[esi+398],payload2-lumma
0040C990 C706 00000000      mov dword ptr ds:[esi],0

```

```

eax:winHttpopen
eax:winHttpopen, [ebp+1C]:&"????????????????????????????????????????????
eax:winHttpopen
eax:winHttpopen, [ebp+14]:"act=life"
eax:winHttpopen, [ebp+10]:L"Content-Type: application/x-www-form-urlencoded\r\n"
eax:winHttpopen, [ebp+0C]:L"/api"
eax:winHttpopen, [ebp+08]:L"freezetdopzx.shop"

```

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

Build ID:

- sTDsFx--Socks
- iAlMAC--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.

```

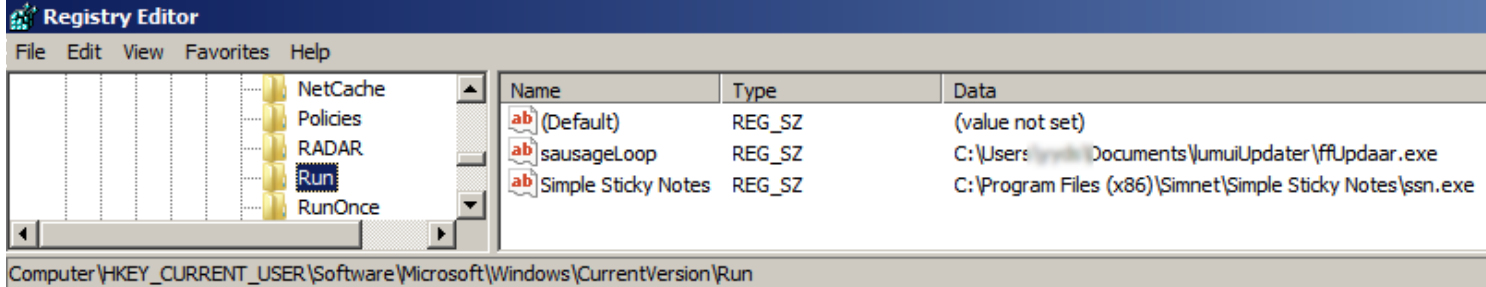
• 00563C6D 8995 D0E7FFFF mov dword ptr ss:[ebp-1830],edx [dword ptr ss:[ebp-1830]]:CreateDirectoryW
• 00563C73 6A 00 push 0
• 00563C75 8D85 8CC7FFFF lea eax,dword ptr ss:[ebp-3874]
• 00563C78 50 push eax
• 00563C7C FF95 D0E7FFFF call dword ptr ss:[ebp-1830] [dword ptr ss:[ebp-1830]]:CreateDirectoryW
EIP → 00563C82 8D8D 8CC7FFFF lea ecx,dword ptr ss:[ebp-3874]
• 00563C88 898D D4E7FFFF mov dword ptr ss:[ebp-182C],ecx
• 00563C8E 57 push edi
• 00563C8F 81CF AA4C0100 or edi,14CAA
• 00563C95 81C7 48EF0000 add edi,EF48
• 00563C9B 5F pop edi
• 00563C9C 57 push edi

ecx=22D90000
dword ptr ss:[ss:[ebp-3874]]=[00D2A564 L"C:\\Users\\yyds\\Documents\\lumuiUpdater"]=3A0043

```

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](#).

SHARE THIS POST

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.

INTELLIGENCE CENTER

- Intelligence Search
- Email & Spam Trends

VULNERABILITY RESEARCH

- Vulnerability Reports
- Microsoft Advisories

INCIDENT RESPONSE

- Emergency Support

SECURITY RESOURCES

- Open Source Security Tools
- Intelligence Categories Reference
- Secure Endpoint Naming Reference

MEDIA

Talos Intelligence Blog

Threat Source Newsletter

Beers with Talos Podcast

Talos Takes Podcast

Talos Videos

SUPPORT

Support Documentation

COMPANY

About Talos

Careers

Cisco Security

FOLLOW US

© 2024 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our [Privacy Policy](#).