Old Bot in New Bottle: Amadey Botnet Back in Action Via Phishing Sites

thecyberexpress.com/amadey-botnet-back-via-phishing-sites/

An old botnet called Amadey that was discovered in 2018 has been found to be actively used to attack systems. Researchers at the Cyble Research and Intelligence Labs (CRIL) found gamers being victimized by phishing websites under the guise of offering gaming hacks and cheats.

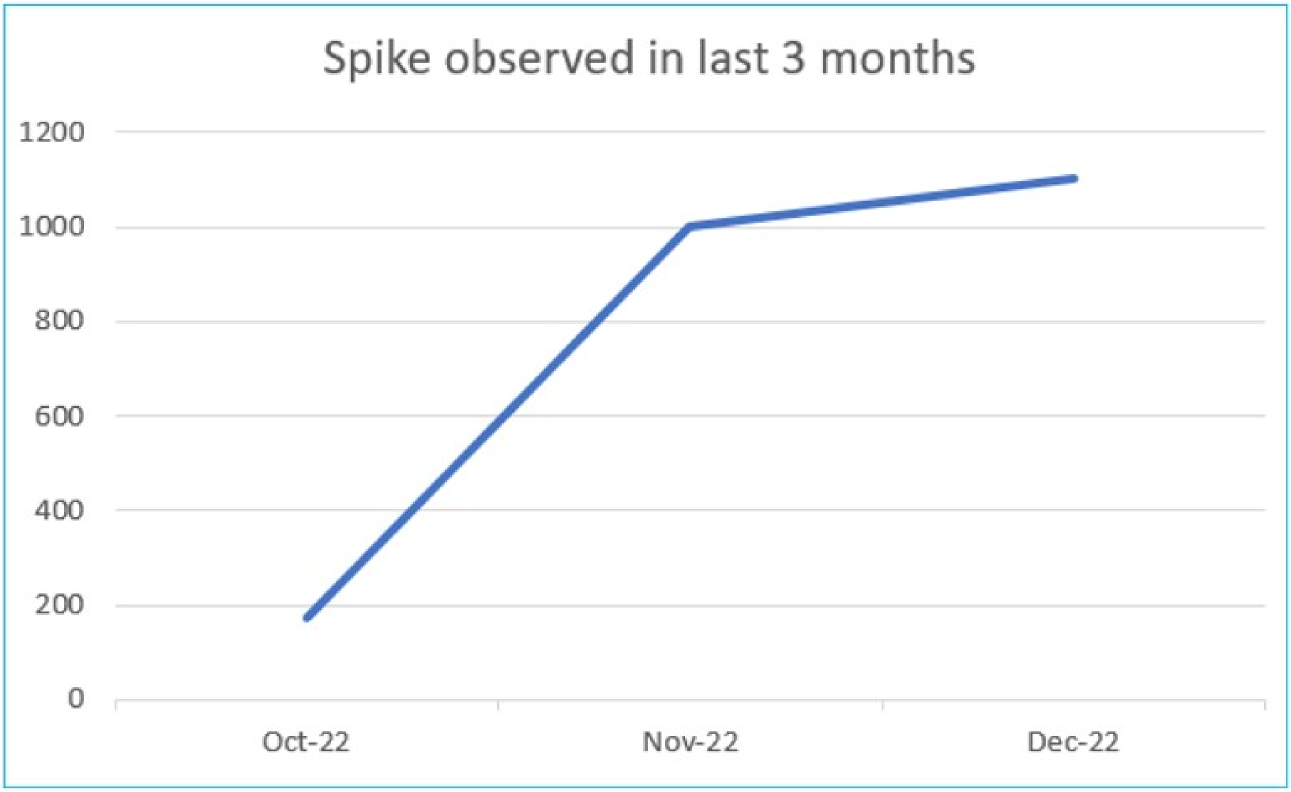
This info-stealing trojan can copy login details from several browsers and has been found to have infected devices in attacks launched by the LockBit ransomware group in 2022. The increase in its use was observed in the last 3 months of 2022.

You might also like

Government Regulation of AI businesses: UK Competition Watchdog Launches Review

Password is Passé: Google Introduces Passkey Login

Researchers Find New KEKW Malware Variant in PyPI Packages

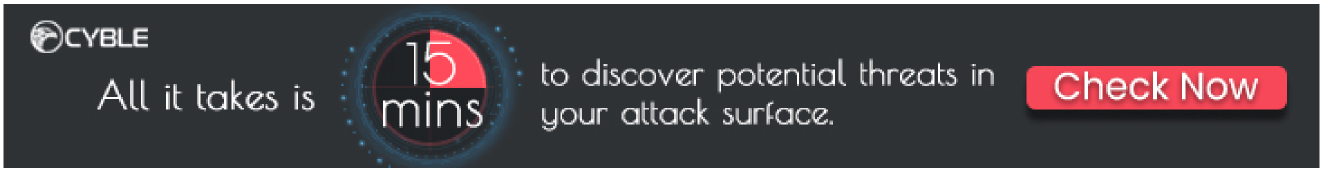


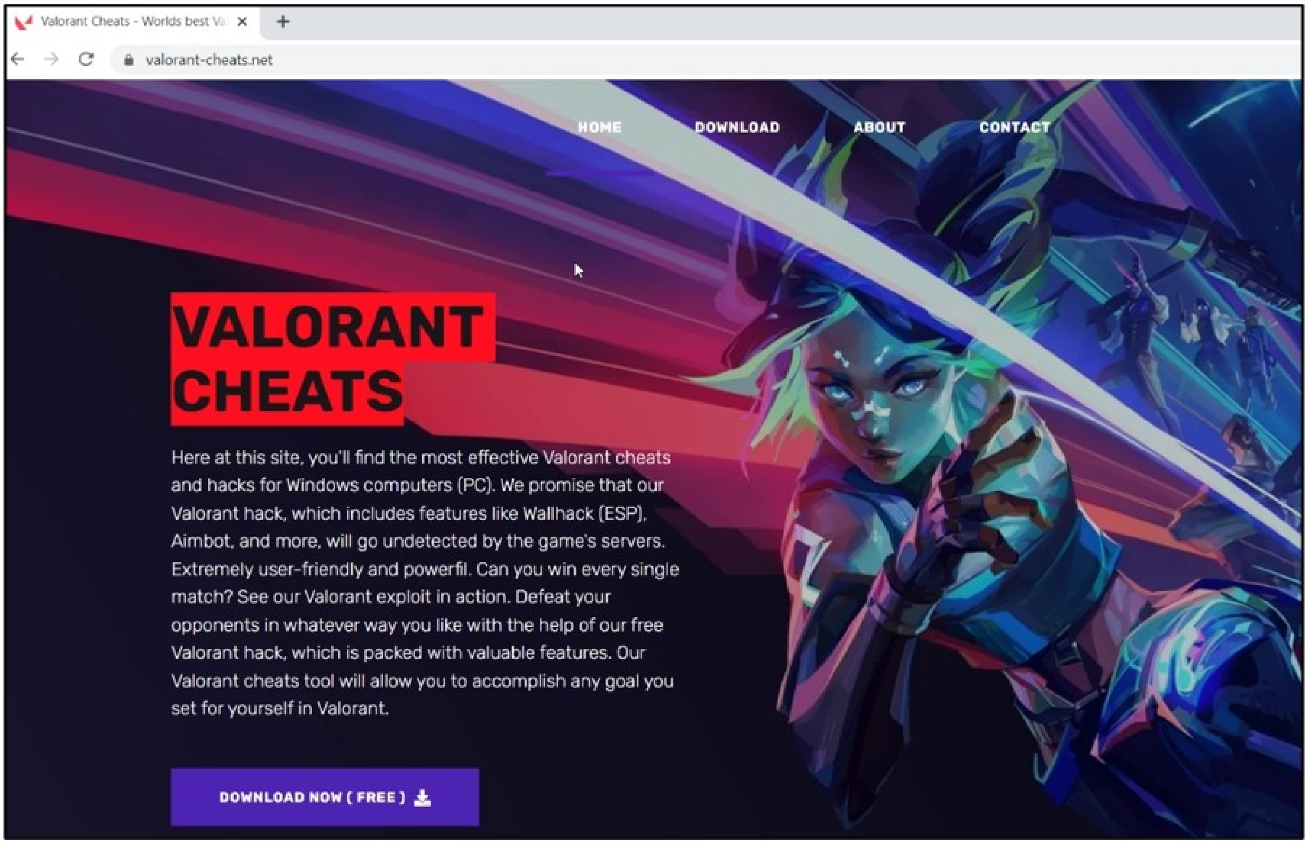
The increased use of the Amadey bot (Image: Cyble)

It can work on browsers including Chrome, Chedot, Microsoft Edge, CentBrowser, SputnikLab, and Opera Software among others. It also impacts cryptocurrencies including Bitcoin, Monero, Ethereum, and Litecoin.

Attack vector using the Amadey bot

Cybercriminals are using fraudulent websites with malicious links camouflaged as cheats for the multiplayer shooting video game Valorant. It asks users to download a .rar file from hxxps[:]//valorantcheatsboss[.]com/upload/boss/Bossmenu%20Setup[.]rar which starts the attack with capabilities including system reconnaissance, changing permissions, changing crypto transaction recipients, and adding more malware. The .rar file has a Seil.exe file that infects the system with the Amadey bot.





VALORANT CHEATS

Here at this site, you'll find the most effective Valorant cheats and hacks for Windows computers (PC). We promise that our Valorant hack, which includes features like Wallhack (ESP), Aimbot, and more, will go undetected by the game's servers. Extremely user-friendly and powerfil. Can you win every single match? See our Valorant exploit in action. Defeat your opponents in whatever way you like with the help of our free Valorant hack, which is packed with valuable features. Our Valorant cheats tool will allow you to accomplish any goal you set for yourself in Valorant.

Sample of a fraudulent gaming website used to infect devices (Image: Cyble)

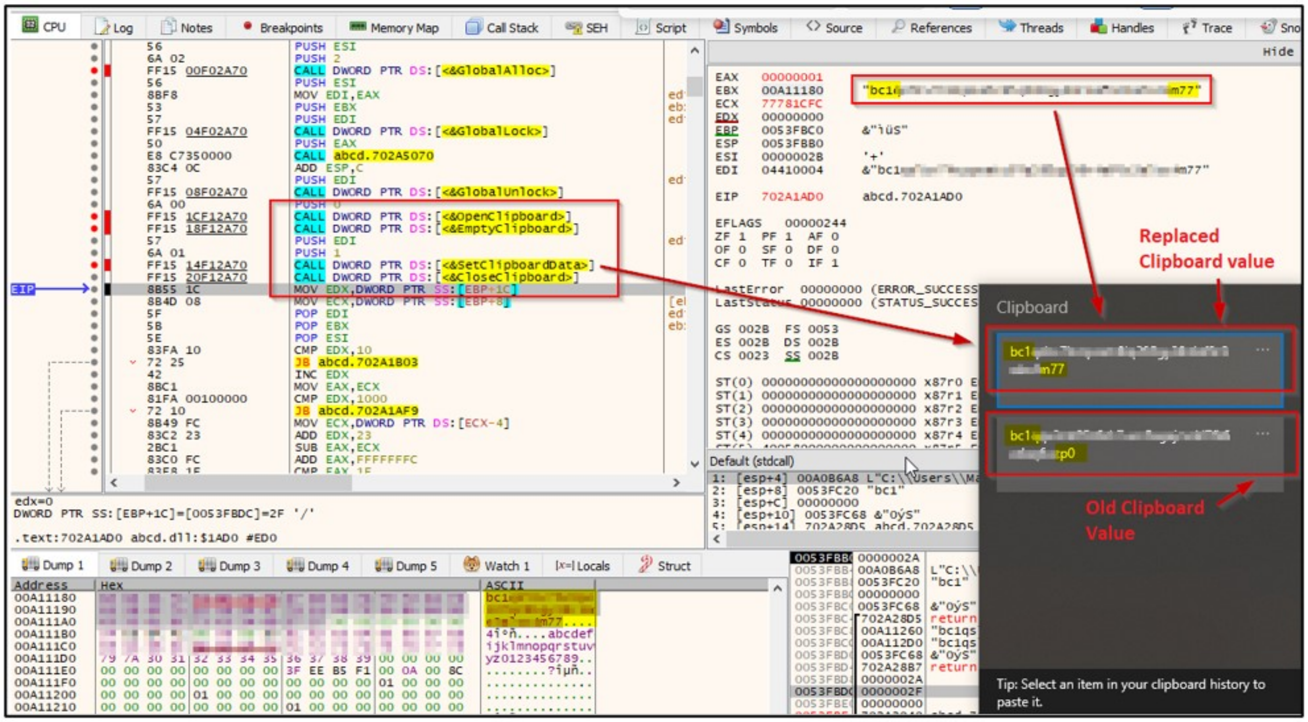
The above image offers several cheats however, misspells the word ‘powerful’ as powerfil which acts as a reminder that often fraudulent websites and phishing emails are not proofread. Amadey bot downloads other malware families including Redline and Manuscript.

Technical details of the Amadey bot attack

CRIL researchers examined a found sample hash (SHA256), b00302c7a37d30e1d649945bce637c2be5ef5a1055e572df9866ef8281964b65, a 32-bit VC++ compiled executable file and made the following observations:

- The Amadey bot creates a duplicate of itself and saves it in the %Temp% folder. It then gets executed using the ShellExecuteA() API.
- Following this, it creates a mutex to make sure only one instance of the bot is running in the system at one point. The mutex name was c1ec479e5342a25940592acf24703eb2
- It maintains persistence using the startup value in HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders registry key. With this, the malware executes every minute because it gets configured in the Task Scheduler.

- At this stage, the bot collects the machine's username and changes the permissions granted to the file nbveek.exe and folder 4b9a106e76. It gets the permission to read, write, and execute files using the 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*
- Now information collection begins which is sent to the cybercriminal's command and control (C&C) server using a POST request with specific field names. It includes id for collecting the victim's ID, vs for the version number of the bot, ar for the admin privilege status, etc.
- Two DLL files – cred64.dll and clip64.dll are downloaded and saved in *%appdata%*. These modules that steal credentials are executed using rundll32.exe. Cred64.dll is a 64-bit Microsoft Visual C/C++ DLL executable and is programmed to steal browser data and setting details.
- It further steals the crypto wallet data from the directories including *%appdata%\Armory\*. It was found to be capable of terminating the crypto wallet client process if it was denied access to sensitive data. The copied data was sent to *hxxp[:]//62[.]204[.]41[.]242/9vZbns/index[.]php*
- dll was a 32-bit VC++ compiled DLL file. It was a clipper module stealing cryptocurrency transaction data from the clipboard. It would replace the recipient's wallet address from it to itself so the amount reaches them instead of the intended account.



```
56                 PUSH ESI
6A 02              PUSH 2
FF15 00F02A70      CALL DWORD PTR DS:[<&GlobalAlloc>]
56                 PUSH ESI
8BF8               MOV EDI,EAX
53                 PUSH EBX
57                 PUSH EDI
FF15 04F02A70      CALL DWORD PTR DS:[<&GlobalLock>]
50                 PUSH EAX
E8 C7350000        CALL abcd.702A5070
83C4 0C            ADD ESP,C
57                 PUSH EDI
FF15 08F02A70      CALL DWORD PTR DS:[<&GlobalUnlock>]
6A 00              PUSH 0
FF15 1CF12A70      CALL DWORD PTR DS:[<&OpenClipboard>]
FF15 18F12A70      CALL DWORD PTR DS:[<&EmptyClipboard>]
57                 PUSH EDI
6A 01              PUSH 1
FF15 14F12A70      CALL DWORD PTR DS:[<&SetClipboardData>]
FF15 20F12A70      CALL DWORD PTR DS:[<&CloseClipboard>]
8B55 1C            MOV EDX,DWORD PTR SS:[EBP+1C]
8B4D 08            MOV ECX,DWORD PTR SS:[EBP+8]
5F                 POP EDI
5B                 POP EBX
5E                 POP ESI
83FA 10            CMP EDX,10
72 25              JB abcd.702A1B03
42                 INC EDX
8BC1               MOV EAX,ECX
81FA 00100000      CMP EDX,1000
72 10              JB abcd.702A1AF9
8B49 FC            MOV ECX,DWORD PTR DS:[ECX-4]
83C2 23            ADD EDX,23
2BC1               SUB EAX,ECX
83C0 FC            ADD EAX,FFFFFFFC
83F8 1F            CMP EAX,1F

edx=0
DWORD PTR SS:[EBP+1C]=[0053FBDC]=2F '/'

.text:702A1AD0 abcd.dll:$1AD0 #ED0
```

```
EAX  00000001
EBX  00A11180     "bc1[redacted]m77"
ECX  77781CFC
EDX  00000000
EBP  0053FBC0     &"ìüS"
ESP  0053FBB0
ESI  0000002B     '+'
EDI  04410004     &"bc1[redacted]m77"

EIP  702A1AD0     abcd.702A1AD0

EFLAGS   00000244
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS
LastStatus 00000000 (STATUS_SUCCES

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000 x87r0 E
ST(1) 00000000000000000000 x87r1 E
ST(2) 00000000000000000000 x87r2 E
ST(3) 00000000000000000000 x87r3 E
ST(4) 00000000000000000000 x87r4 E
```

```
1: [esp+4]  00A0B6A8 L"C:\\Users\\Ma
2: [esp+8]  0053FC20 "bc1"
3: [esp+C]  00000000
4: [esp+10] 0053FC68 &"oýS"
5: [esp+14] 702A28D5 abcd.702A28D5
```

```
Address   Hex                                              ASCII
00A11180  [redacted]                                       bc1[redacted]
00A11190  [redacted]                                       [redacted]
00A111A0  [redacted]                                       [redacted]m77....
00A111B0  [redacted]                                       4ì°ñ....abcdef
00A111C0  [redacted]                                       ijklmnopqrstuv
00A111D0  79 7A 30 31 32 33 34 35 36 37 38 39 00 00 00 00  yz0123456789..
00A111E0  00 00 00 00 00 00 00 00 3F EE B5 F1 00 0A 00 8C  ........?îµñ..
00A111F0  00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ..............
00A11200  00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  ..............
00A11210  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ..............
```

```
0053FBB0  0000002A
0053FBB4  00A0B6A8  L"C:\\
0053FBB8  0053FC20  "bc1"
0053FBBC  00000000
0053FBC0  0053FC68  &"oýS"
0053FBC4  702A28D5  return
0053FBC8  00A11260  "bc1qs
0053FBCC  00A112D0  "bc1qs
0053FBD0  0053FC68  &"oýS"
0053FBD4  702A28B7  return
0053FBD8  0000002A
0053FBDC  0000002F
0053FBE0  00000000
```

Clipboard

bc1[redacted]m77

bc1[redacted]p0

Amadey bot changing the clipboard data impacting the cryptocurrency transaction (Image: Cyble)

Amadey is being sold for about $500 on Russian-speaking hacker forums according to a report by malpedia. Amadey uses an infected system as a botnet and can launch a distributed denial of service attack on other systems.

Tags: Amadey botnetCRIL amadey botcryptocurrency name changing botgame cheat botThe Cyber ExpressThe Cyber Express News