

# Amadey Botnet Back in Action Via Phishing Sites

By theycyberexpress

Published: 2023-01-27 · Archived: 2026-04-06 00:22:00 UTC



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.

 Amadey Botnet

**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

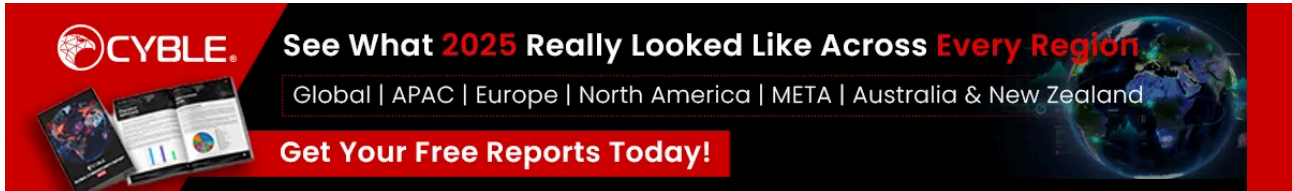
[Cybercriminals are using fraudulent](#) websites with malicious links camouflaged as cheats for the multiplayer shooting video game Valorant. It [asks users](#) to download a .rar file from `hxxps[:]//valorantcheatsboss[.]com/upload/boss/Bossmenu%20Setup[.]rar` which starts the attack with capabilities 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.

## Amadey Botnet

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.

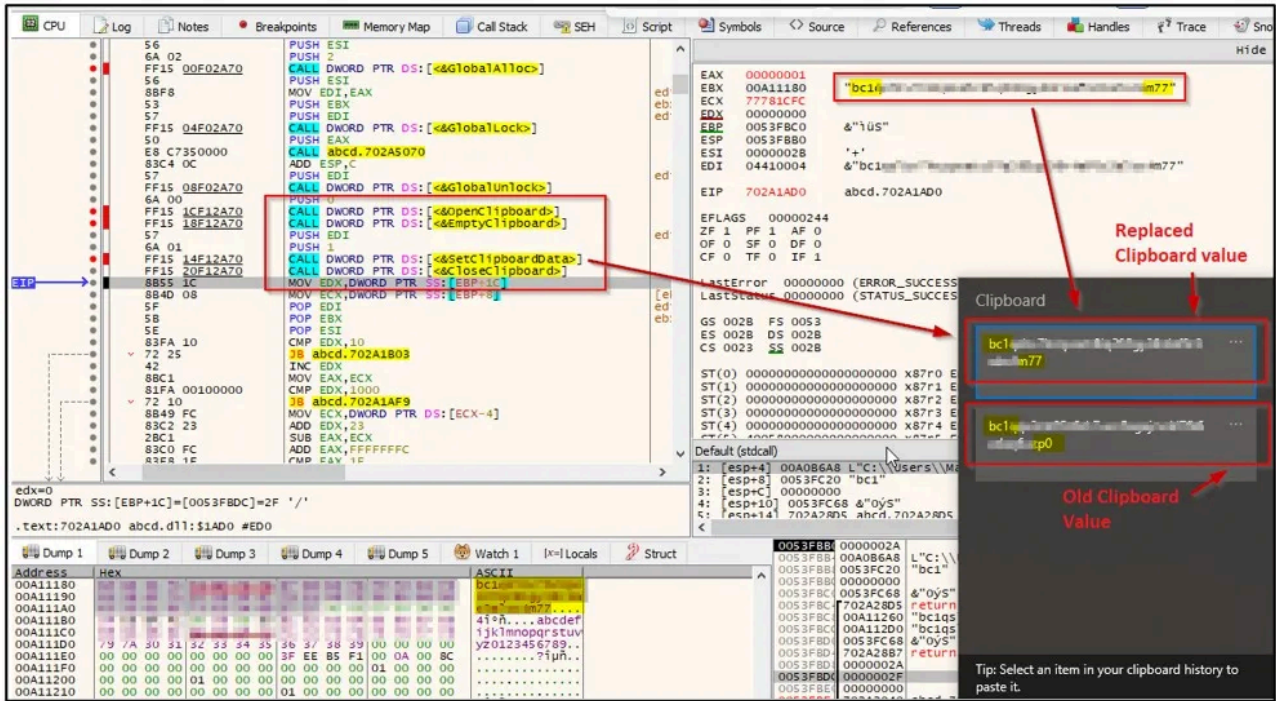
Technical details of the Amadey bot attack



[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.



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](#).

Source: <https://theyberexpress.com/amadey-botnet-back-via-phishing-sites/>