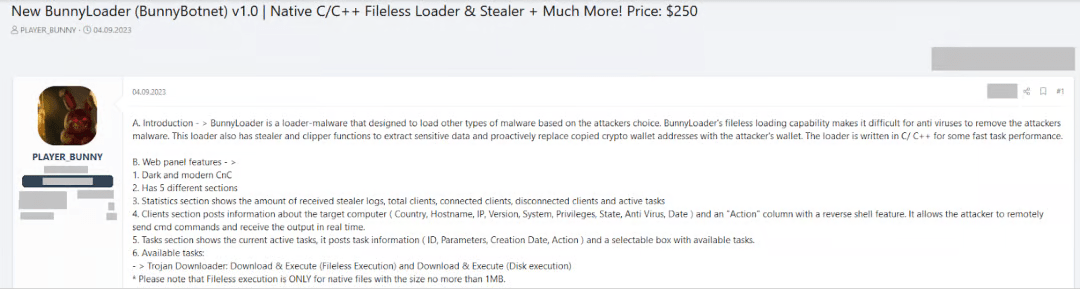
**A new malware-as-a-service called Bunnyloader was advertised in cybercrime forums.**



**A new malware-as-a-service (MaaS) named BunnyLoader has surfaced in the threat ecosystem, according to cybersecurity analysts.**

BunnyLoader is a new malware-as-a-service (MaaS) that has been marketed for sale in numerous cybercrime forums starting September 4, 2023, according to Zscaler ThreatLabz experts.



A lifetime license for the C/C++-coded BunnyLoader malware loader costs $250 on various forums. The authors are releasing several updates to integrate new features and correct errors, leading analysts to assume that the BunnyLoader is undergoing rapid development.

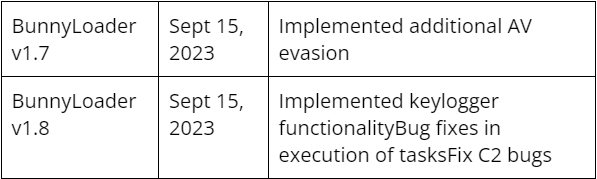
The malware can download and run a second-stage payload, log keys, steal sensitive data and cryptocurrency, and carry out remote orders. It also supports anti-sandbox tactics and evasion techniques.

"BunnyLoader offers a wide range of functionalities, including downloading and running a second-stage payload, stealing system information and browser credentials, and much more." reads the Zscaler report that was released. The cryptocurrency wallet addresses of the victim are replaced with actor-controlled cryptocurrency wallet addresses via BunnyLoader, which uses a clipper to monitor the victim's clipboard and record keystrokes as.

Additionally, it is claimed in the advertisement that BunnyLoader offers a fileless loader, which enables malware to download and run additional malware stages straight from memory.

Stolen information is compressed into a ZIP archive and sent to a C2 server.

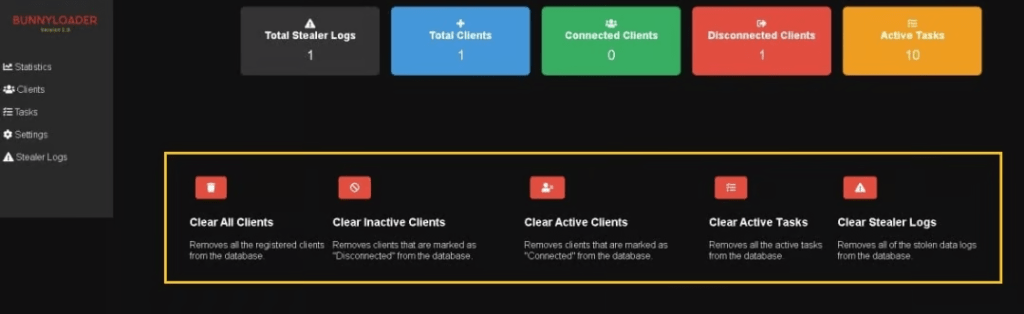
The authors released BunnyLoader v1.7 and v1.8 on September 15, 2023. These updates included keylogger capability and new AV evasion approaches, respectively, and solved bugs in task execution and C2.



Command-and-control (C2) was found to contain major SQL injection flaws on September 27, 2023, which may have been exploited by attackers to seize control of the C2 database.

Numerous functionalities are supported by the BunnyLoader panel, including:

* the act of obtaining and running more malware
* Keylogging and credential theft
* using a victim's clipboard to conduct remote commands on the compromised machine, collecting infection statistics, and stealing bitcoin
* showing all clients who are connected or disconnected at once
* observing ongoing tasks
* recording the actions of the thief



The researchers examined the malware's activities after it was executed, but they have not yet identified the malware's propagation method.

When the loader is executed, it conducts a series of anti-VM tactics and sets up persistence via the Windows Registry.

After sending the registration request to the C2 server, BunnyLoader executes the primary malicious operations if the C2 server's response is "Connected."

The malware has the ability to download and run subsequent software, operate keyloggers, and steal sensitive information, including information from online browsers and cryptocurrency wallets. Additionally, the spyware has the ability to steal data from VPN clients and chat apps.

“BunnyLoader is a new MaaS threat that is continuously evolving their tactics and adding new features to carry out successful campaigns against their targets.” continues the report.

Credits: -

<https://securityaffairs.com/151869/malware/bunnyloader-maas.html>