

Oski Stealer : A Credential Theft Malware

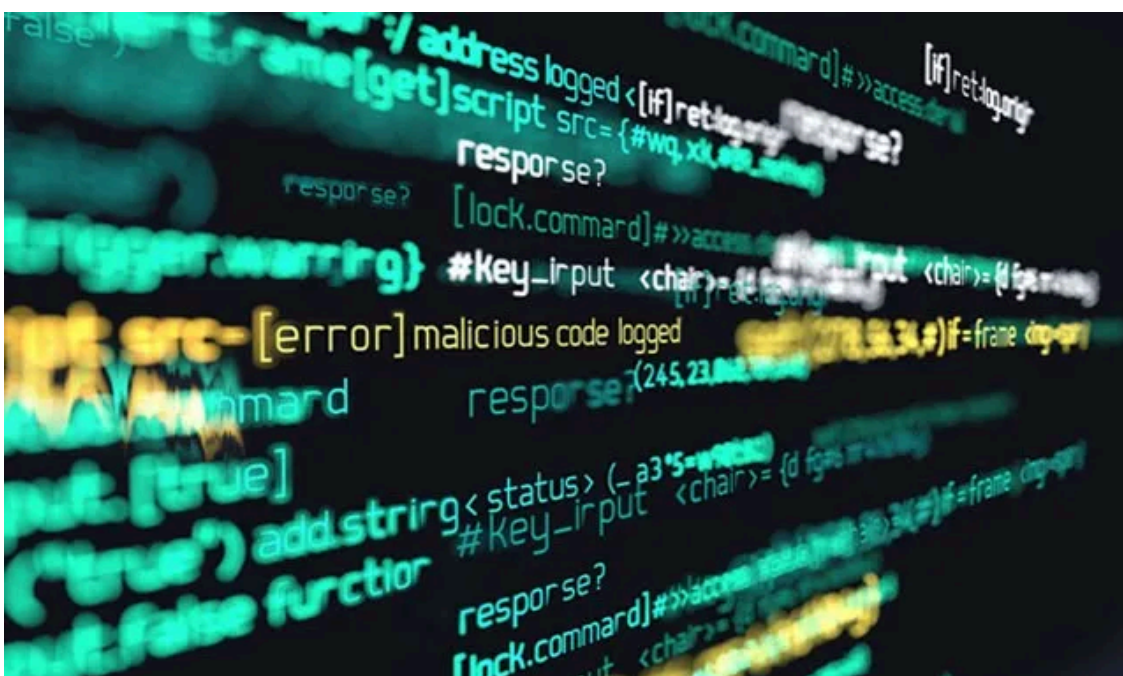
By Isha Kudkar

Published: 2021-01-16 · Archived: 2026-04-05 22:40:28 UTC



4 min read

Jan 16, 2021



Credential theft malware continues to be one amongst the foremost prevalent sorts of malware employed in cyber attacks. The most objective of nearly all credential theft malware is to assemble the maximum amount of confidential and sensitive information, like user credentials and financial information, as possible.

The Oski stealer is a malicious information stealer, which was first introduced in November 2019. The Oski stealer steals personal and sensitive credentials from its target so the attackers responsible can misuse it to get revenue in various ways. Research shows that this information stealer is distributed through deceptive websites that are opened because of hijacked router DNS settings.

Oski is currently being sold on Russian underground hacking forums at a low price of \$70-\$100.

Press enter or click to view image in full size

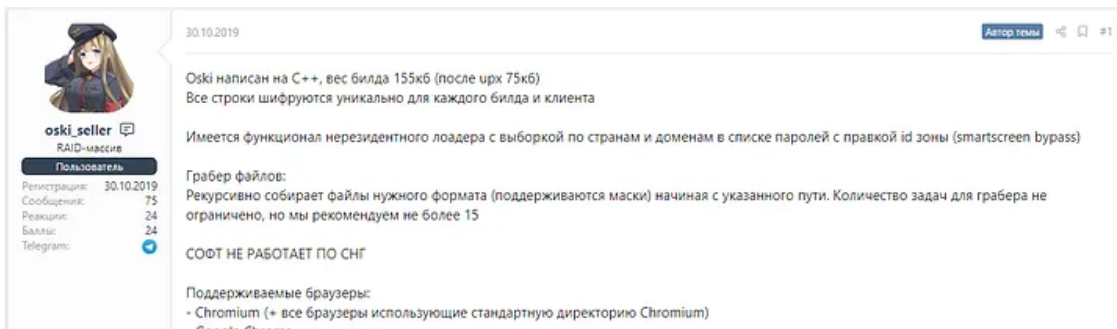


Fig. 1 Forum Thread for selling Oski Stealer

Researchers at ‘CyberArk’ have analyzed the newest malware samples they may get their hands on and report on the complete list of Oski’s capabilities. Written in C++, the malware can steal the subsequent things:

- Login credentials from different applications
- Browser information (cookies, autofill data, and credit cards)
- Crypto wallets
- System information
- Capture Screenshots
- Different user files

The code of the malware is super clean and indicates that the author is knowledgeable, ensuring reliable operation. However, Oski doesn’t have any sophisticated obfuscation, anti-analysis, or anti-debugging tricks under its sleeve yet, but this will always be added later. The very fact that the code basis is neatly done creates the setting to figure on this tool further and add more features within the future.

Press enter or click to view image in full size

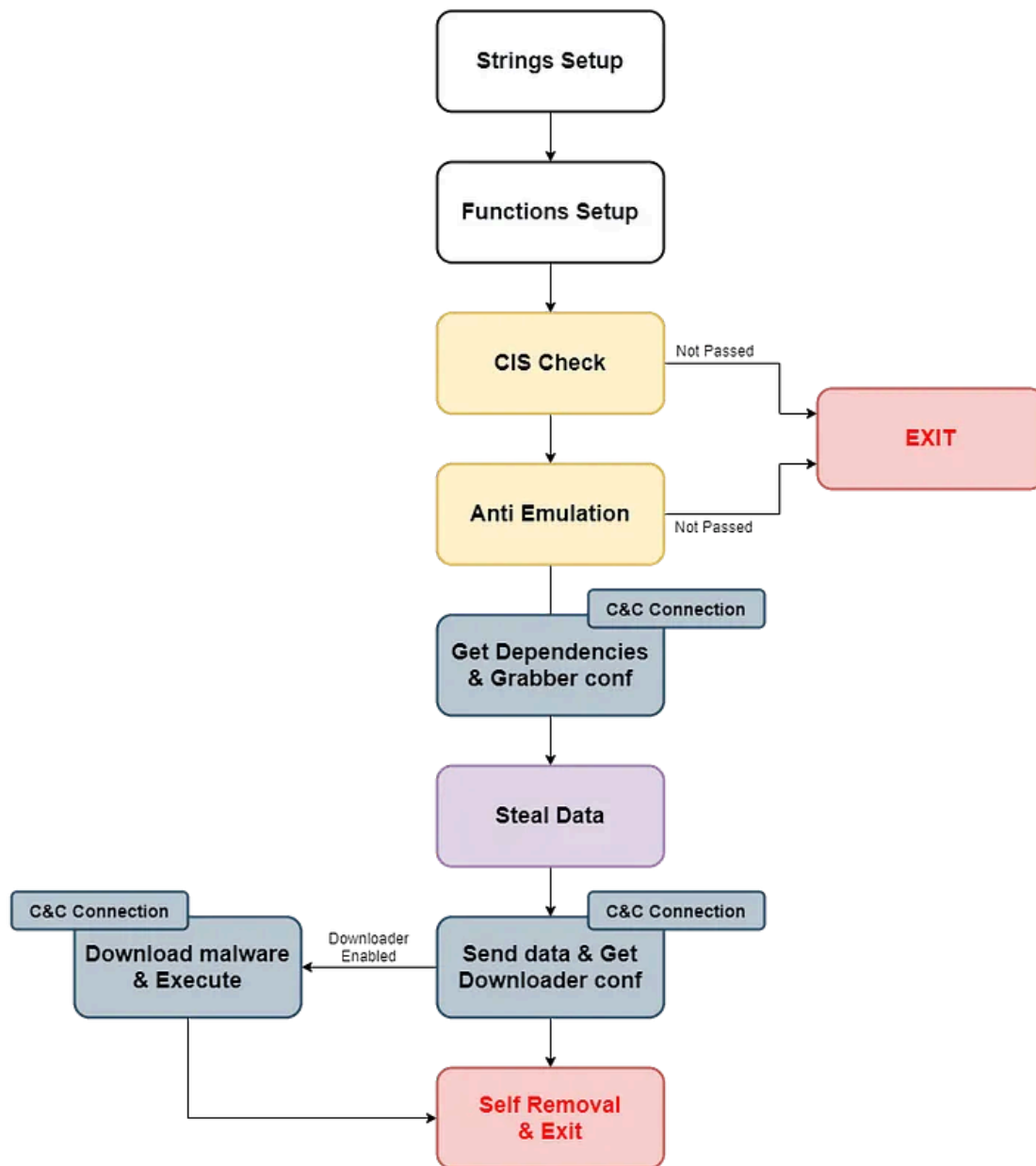


Fig. 2 Malware Flow

Attackers try to trick users into installing Oski by hijacking router DNS settings in order that browsers then open corrupted pages and pop-ups. This motivates visitors to put in an application designed to deliver the latest information referring to the COVID-19. In fact, the file that's downloaded through these malicious sites installs Oski, a trojan horse capable of stealing sensitive information. It targets data from browsers like cookies and browsing history, autofill data, and saved login credentials. It also attempts to steal databases that contain two-factor authentication data, cryptocurrency wallets, and word files, and might take screenshots of the victim's screen and perform other dubious actions. Attackers behind Oski are able to hijack various accounts, including social media, email, cryptocurrency trading accounts, and so on.

Get Isha Kudkar's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Furthermore, they could be capable of hijacking accounts that have an extra layer of protection beyond passwords. Cyber criminals misuse stolen accounts to create fraudulent purchases and transactions, spread spam campaigns, trick other users into paying money to them, steal identities, etc. They may additionally be able to access text and documents files containing lead, take screenshots when victim's open them, or capture other computing activities. Victims of Oski attacks might thus suffer monetary loss, have their identities stolen, experience problems regarding online privacy, browsing safety and other serious issues. Therefore, this malware must be far from infected systems immediately.

Other Harmful Features of Oski Stealer:

Oski Stealer modifies the default registry settings by making vicious entries in it which allows the virus to be automatically activated on every occasion the machine is started. It messes with important system files that are efficient for smooth computer functioning and prevents many installed apps similarly as drivers from working in an appropriate manner. It displays bogus security warnings, error messages, updates notification etc. and tries to force you into installing bogus software. This nasty trojan keeps performing malicious acts within the background all the time which consumes enormous amounts of memory resources and degrades the PC performance severely. It causes the device to reply in a very very slow manner and take over usual time to finish any task. It assists remote criminals to urge access to your system and contribute malevolent deeds inside for his or her delicate welfare. viewing these hazards, you're strongly recommended to delete Oski Stealer from the PC without wasting any time. And to prevent this, you must only choose reliable or official websites and direct links to download any application and avoid using unofficial domains and other third-party downloaders, peer-to-peer networks, freeware download pages etc.

To remove Malware :

If you're concerned that malware or PC threats like Oski Stealer may have infected your computer, we recommend you begin an in-depth system scan with SpyHunter. SpyHunter is a complicated malware protection and remediation application that provides subscribers a comprehensive method for safeguarding PCs from malware, additionally to providing one-on-one technical support service.

Link to download — <https://www.spyhunter.com/2Qk6Q2N/>

Source: <https://medium.com/shallvhack/oski-stealer-a-credential-theft-malware-b9bba5164601>