



Feel like you're
being watched?



Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)

> Security (<https://www.bleepingcomputer.com/news/security/>)

> Revamped CryptBot malware spread by pirated software sites

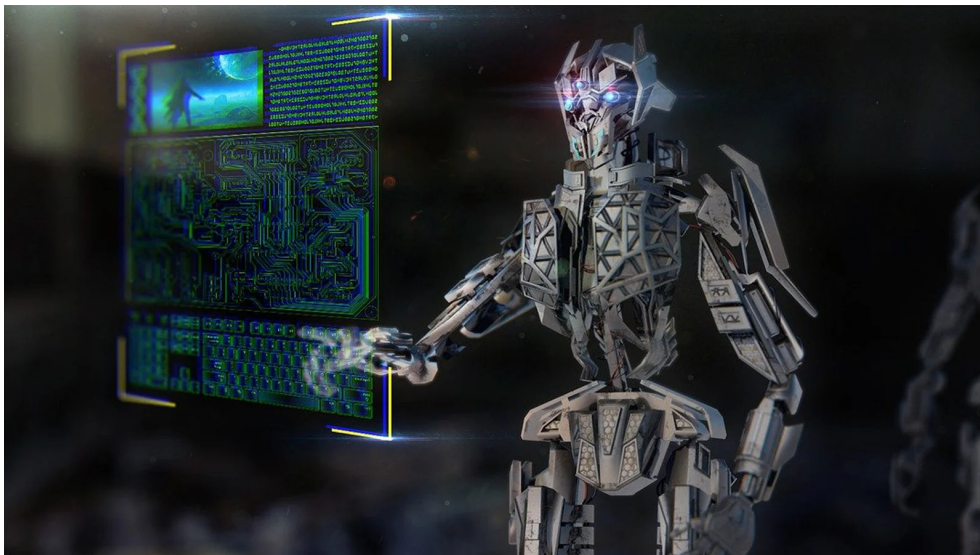
Revamped CryptBot malware spread by pirated software sites

By
Bill Toulas
(<https://www.bleepingcomputer.com/author/bill-toulas/>)

February 21, 2022

12:40 PM

0



A new version of the CryptBot info stealer was seen in distribution via multiple websites that offer free downloads of cracks for games and pro-grade software.

CryptBot is a Windows malware that steals information from infected devices, including saved browser credentials, cookies, browser history, cryptocurrency wallets, credit cards, and files.



The latest version features new capabilities and optimizations, while the malware authors have also deleted several older functions to make their tool leaner and more efficient.



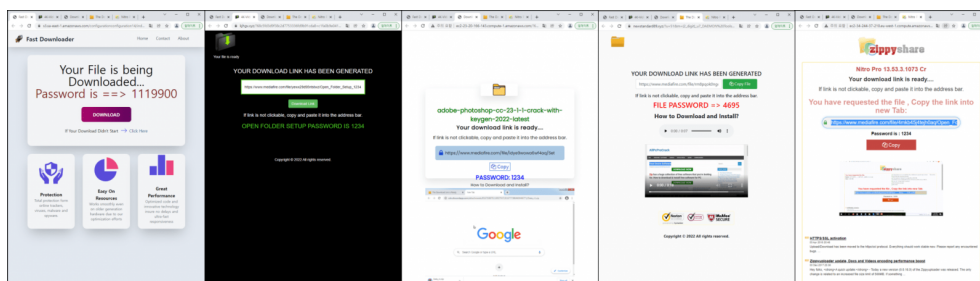
Security analysts at Ahn Lab reported that the threat actors are constantly refreshing their C2, dropper sites, and the malware itself, so CryptBot is currently one of the most shifting malicious operations.

Using search results for delivery

According to the Ahn Lab report, the CryptBot threat actors distribute malware through websites pretending to offer software cracks, key generators, or other utilities.

To gain wide visibility, the threat actors utilize search engine optimization to rank the malware distribution sites at the top of Google search results, providing a stable stream of prospective victims.

According to screenshots shared of the malware distribution sites, the threat actors use both custom domains or websites hosted on Amazon AWS.



Some of the websites used recently for CryptBot distribution

Source: Ahn Lab

The malicious websites are constantly being refreshed, so there's a wide variety of ever-shifting lures to draw users onto the malware distribution sites.

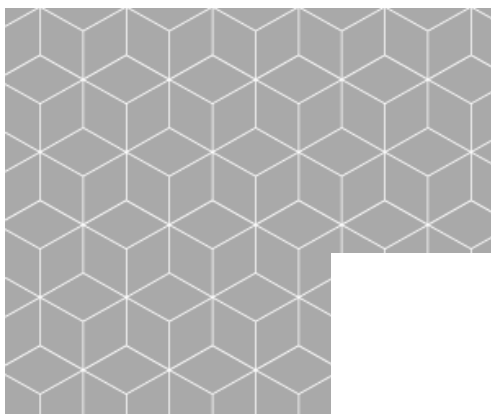


Visitors of these sites are taken through a series of redirections before they end up on the delivery page, so the landing page could be on a compromised legitimate site abused for SEO poisoning attacks.

We have seen the same malware operators using fake VPN sites (<https://www.bleepingcomputer.com/news/security/fake-vpn-site-pushes-cryptbot-and-vidar-info-stealing-trojans/>) to deliver CryptBot to victims in previous years, so search engine abuse isn't a new trick.

Features removed

Fresh samples of CryptBot indicate that its authors want to simplify its functionality and make the malware lighter, leaner, and less likely to be detected.



In this context, the anti-sandbox routine has been removed, leaving only the anti-VM CPU core count check in the newest version.

Also, the redundant second C2 connection and second exfiltration folder were both removed, and the new variant only features a single info-stealing C2.

"The code shows that when sending files, the method of manually adding the sent file data to the header was changed to the method that uses simple API. user-agent value when sending was also modified," explains ASEC's report (<https://asec.ahnlab.com/en/31802/>)

"The previous version calls the function twice to send each to a different C2, but in the changed version, one C2 URL is hard-coded in the function."

Another feature the CryptBot's authors have scrapped is the screenshot function and the option of collecting data on TXT files on the desktop, which were too risky and perhaps easily detected during exfiltration.

Works on all Chrome versions

On the other hand, the latest version of CryptBot brings some targeted additions and improvements that make it a lot more potent.

In previous versions (<https://www.bleepingcomputer.com/news/security/malicious-kmspico-installers-steal-your-cryptocurrency-wallets/>), the malware could only



successfully exfiltrate data when deployed against Chrome versions between 81 and 95.

This limitation arose from implementing a system that looked for user data in fixed file paths, and if the paths were different, the malware returned an error.

<pre>vsmprintf_s(v8, FileName, 260, L"%S\\%S\\Login Data", Dst); vsmprintf_s(v10, ExistingFileName, 260, L"%S\\%S\\Cookies", Dst); result = vsmprintf_s(v11, v50, 260, L"%S\\%S\\Web Data", Dst);</pre>	<pre>wsprintf(v18, L"%S\\%S\\Cookies", v21, a2); wsprintf(v16, L"%S\\%S\\Network\\Cookies", v21, a2); wsprintf(v14, L"%S\\%S\\Web Data", v21, a2); wsprintf(v12, L"%S\\%S\\Login Data", v21, a2);</pre>
---	---

Pathname discovery system comparison (new right) - ASEC

Now, it searches on all file paths, and if user data is found anywhere, it exfiltrates them regardless of the Chrome version.

Considering that Google rolled out chrome 96 in November 2021, CryptBot remained ineffective against most of its targets for roughly three months, so fixing this problem was well overdue for its operators.

As CryptBot primarily targets people searching for software cracks, warez, and other methods of defeating copyright protection, simply avoiding the downloading of these tools will prevent infection by this malware and many others.

Related Articles:

SEO poisoning pushes malware-laced Zoom, TeamViewer, Visual Studio installers (<https://www.bleepingcomputer.com/news/security/seo-poisoning-pushes-malware-laced-zoom-teamviewer-visual-studio-installers/>)

New Golang botnet empties Windows users' cryptocurrency wallets (<https://www.bleepingcomputer.com/news/security/new-golang-botnet-empties-windows-users-cryptocurrency-wallets/>)

Hackers slip into Microsoft Teams chats to distribute malware (<https://www.bleepingcomputer.com/news/security/hackers-slip-into-microsoft-teams-chats-to-distribute-malware/>)

FritzFrog botnet grows 10x, hits healthcare, edu, and govt systems (<https://www.bleepingcomputer.com/news/security/fritzfrog-botnet-grows-10x-hits-healthcare-edu-and-govt-systems/>)

Qbot needs only 30 minutes to steal your credentials, emails (<https://www.bleepingcomputer.com/news/security/qbot-needs-only-30-minutes-to-steal-your-credentials-emails/>)

Feel like you're being watched?

