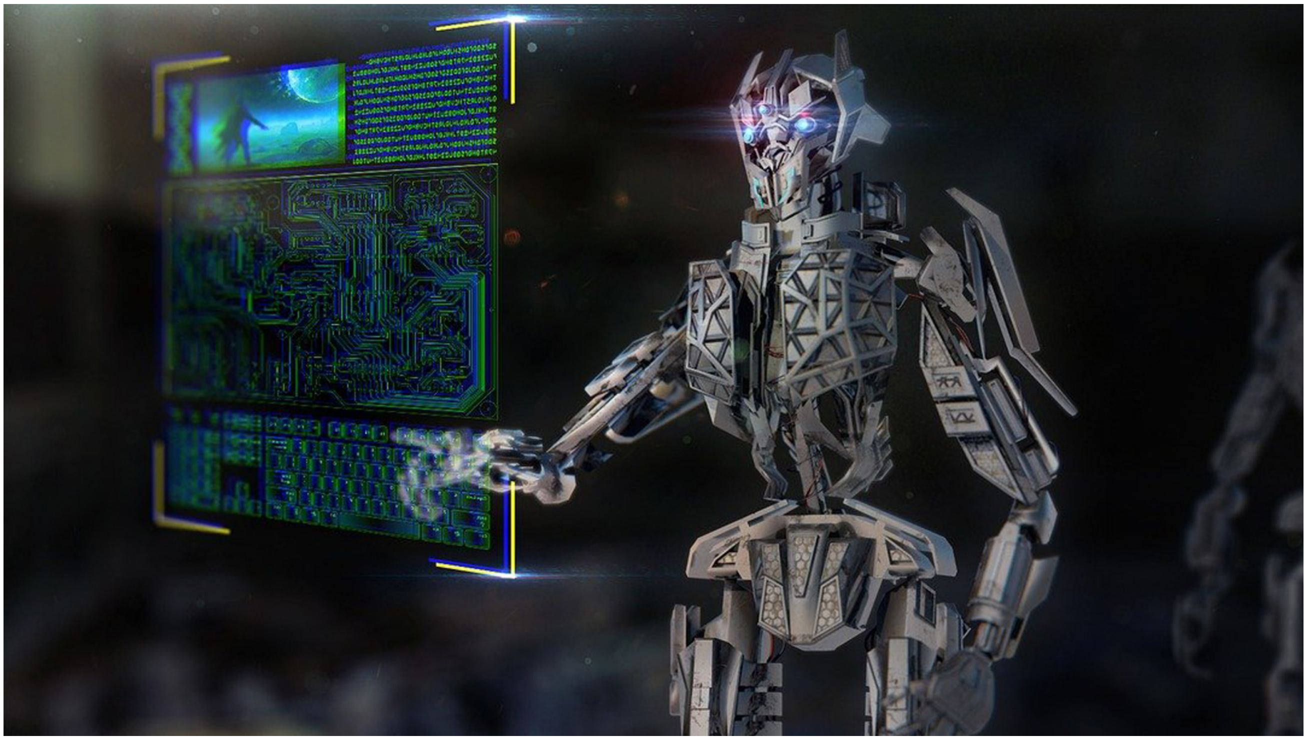
Revamped CryptBot malware spread by pirated software sites

bleepingcomputer.com/news/security/revamped-cryptbot-malware-spread-by-pirated-software-sites/

Bill Toulas

By
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.

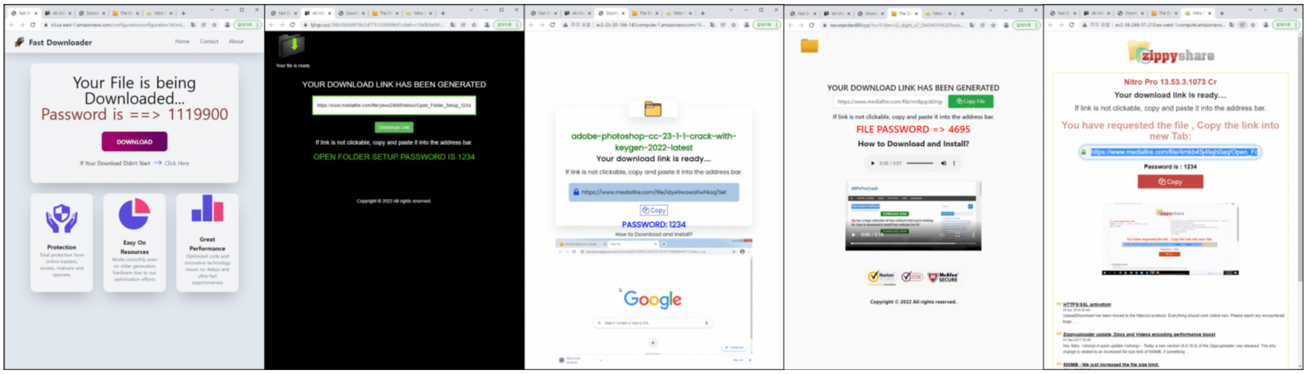
Security analysts at Ahn Lab reported that the threat actors are constantly refreshing their C2, dropper sites, and the malware itself, so CryptBot is currently one of the most shifting malicious operations.

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.



Fast Downloader

Your File is being Downloaded...
Password is ==> 1119900

DOWNLOAD

If Your Download Didn't Start → Click Here

Protection
Total protection form online trackers, viruses, malware and spyware.

Easy On Resources
Works smoothly even on older generation hardware due to our optimization efforts

Great Performance
Optimized code and innovative technology insure no delays and ultra-fast responsiveness

Your file is ready

YOUR DOWNLOAD LINK HAS BEEN GENERATED

https://www.mediafire.com/file/yewx29d95ntstwz/Open_Folder_Setup_1234

Download Link

If link is not clickable, copy and paste it into the address bar.

OPEN FOLDER SETUP PASSWORD IS 1234

Copyright © 2022 All rights reserved.

adobe-photoshop-cc-23-1-1-crack-with-keygen-2022-latest
Your download link is ready....
If link is not clickable, copy and paste it into the address bar.

https://www.mediafire.com/file/idye9wowa6wf4oq/Set

Copy

PASSWORD: 1234
How to Download and Install?

YOUR DOWNLOAD LINK HAS BEEN GENERATED

https://www.mediafire.com/file/rm8pqok0ng

Copy File

If link is not clickable, copy and paste it into the address bar.

FILE PASSWORD => 4695

How to Download and Install?

Copyright © 2022 All rights reserved.

Nitro Pro 13.53.3.1073 Cr
Your download link is ready....
If link is not clickable, copy and paste it into the address bar.

You have requested the file , Copy the link into new Tab:

https://www.mediafire.com/file/4mkb45j4tejh0aq/Open_Fo

Password is : 1234

Copy

HTTPS/SSL activation

Zippyuploader update, Docs and Videos encoding performance boost

500MB - We just increased the file size limit.

s3.sa-east-1.amazonaws.com/configurationconfiguration14/ind...
Home
Contact
About
kjhgv.xyz/?68c5fd3d9f38c2d7753336fd9b91cda8+c1fa0b9e041...
ec2-23-20-166-143.compute-1.amazonaws.com/?6...
Google
newstandard09.xyz/?u=518m=(2_digit)_u7_DAEMON%20Tools...
AllPcProCrack
Norton
McAfee SECURE
ec2-34-244-37-210.eu-west-1.compute.amazonaws...
zippyshare

Some of the websites used recently for CryptoBot 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 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

"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."

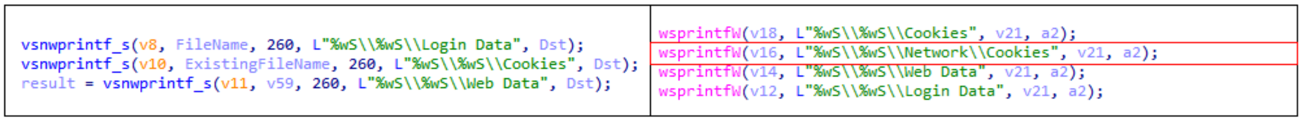
Another feature the CryptBot’s authors have scrapped is the screenshot function and the option of collecting data on TXT files on the desktop, which were too risky and perhaps easily detected during exfiltration.

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, 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.



```
vsnwprintf_s(v8, FileName, 260, L"%wS\\%wS\\Login Data", Dst);
vsnwprintf_s(v10, ExistingFileName, 260, L"%wS\\%wS\\Cookies", Dst);
result = vsnwprintf_s(v11, v59, 260, L"%wS\\%wS\\Web Data", Dst);
```

```
wsprintfW(v18, L"%wS\\%wS\\Cookies", v21, a2);
wsprintfW(v16, L"%wS\\%wS\\Network\\Cookies", v21, a2);
wsprintfW(v14, L"%wS\\%wS\\Web Data", v21, a2);
wsprintfW(v12, L"%wS\\%wS\\Login Data", v21, a2);
```

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:

Fake Windows 10 updates infect you with Magniber ransomware

New ChromeLoader malware surge threatens browsers worldwide

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Popular Python and PHP libraries hijacked to steal AWS keys

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

- Cracks
- CryptBot
- Malware
- Pirated Software
- Search Engine
- Warez

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: