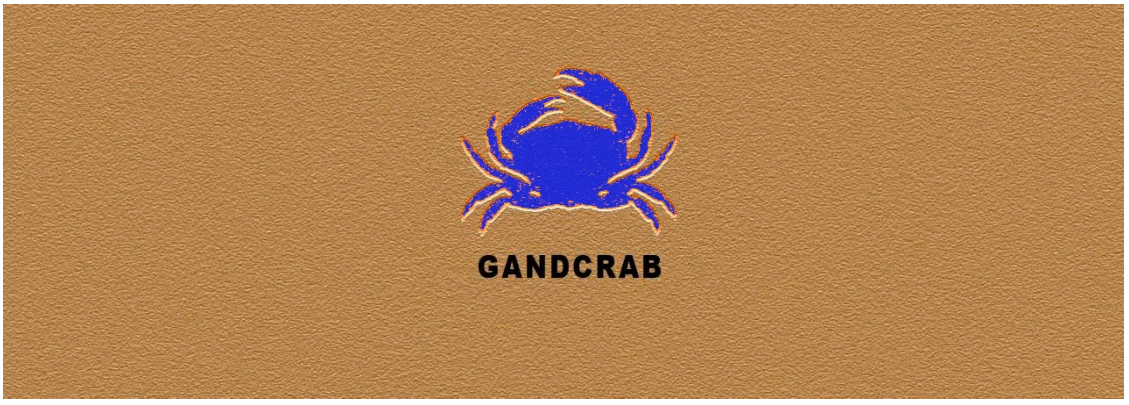
GandCrab Operators Use Vidar Infostealer as a Forerunner

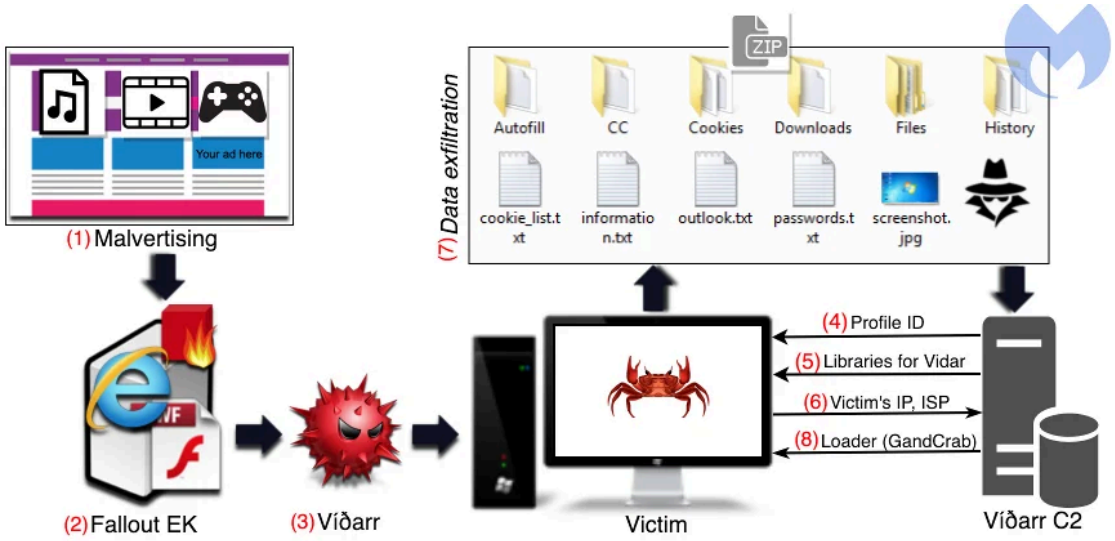
By Ionut Ilascu

Published: 2019-01-07 · Archived: 2026-04-05 14:18:23 UTC



Cybercriminals behind GandCrab have added the infostealer Vidar in the process for distributing the ransomware piece, which helps increase their profits by pilfering sensitive information before encrypting the computer files.

Following the trails of a malvertising campaign targeting users of torrent trackers and video streaming websites, malware researchers found that Fallout Exploit Kit was used to spread a relatively new infostealer called Vidar, which doubled as a downloader for GandCrab.




DIE LINKE.
0:00

Visit Advertiser website[GO TO PAGE]

Using a rogue advertising domain, the threat actor triaged by geolocation the visitors of the compromised websites and redirected them to an exploit kit (EK).

Fallout was the most active, says Jérôme Segura of Malwarebytes, adding that it pushed Vidar - a commercial threat available for $700 specifically built for stealing passwords and forms from web browsers.

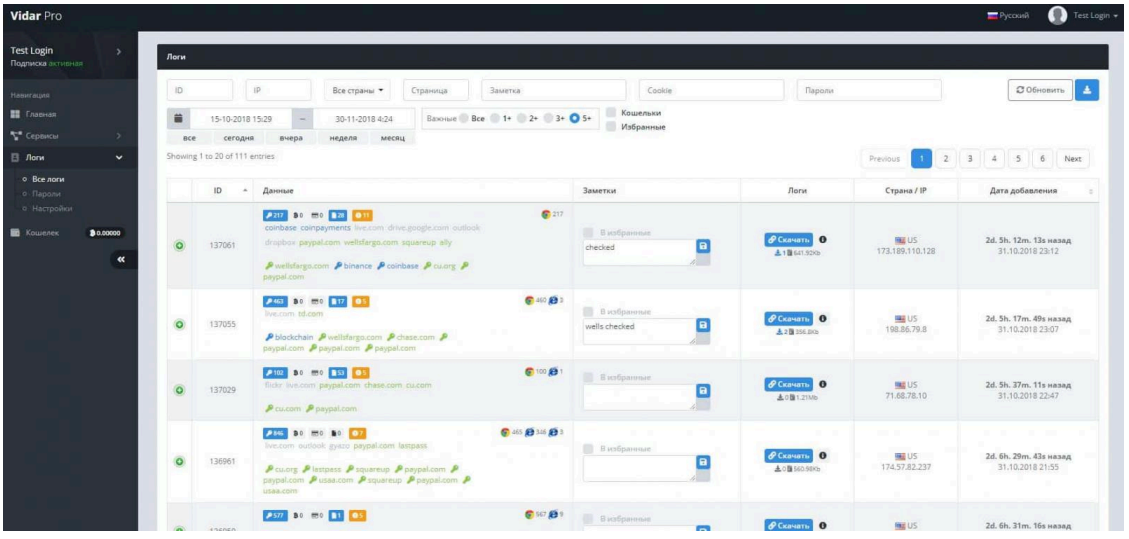
It can be configured to grab specific information, like payment card numbers or credentials stored in various applications. The variant examined by Malwarebytes included scraping capabilities for details from "an impressive selection of digital wallets."

```
HTTP/1.1 200 OK
Date: [redacted]
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip
Server: Pro-Managed

1,1,1,1,1,1,0,1,1,1,250,Desktop;%DESKTOP%
\;*.txt:*.dat:*wallet*.*:*2fa*.*:*backup*.*:*code*.*:*password*.*:*auth*.*:*google*.*:*utc
*.*:*UTC*.*:*crypt*.*:*key*.*:*upbit*.*:*bcex*.*:*bithimb*.*:*hitbtc*.*:*bitflyer*.*:*kuco
in*.*:*huobi*.*:*poloniex*.*:*kraken*.*:*okex*.*:*binance*.*:*bitfinex*.*:*gdax*.*:*ethere
um*.*:*jaxx*.*:*exodus*.*:*metamask*.*:*myetherwallet*.*:*electrum*.*:*bitcoin*.*:*blockch
ain*.*;500;true;movies:music:mp3;documents;%DOCUMENTS%
\;*.txt:*wallet*.*:*2fa*.*:*backup*.*:*code*.*:*password*.*:*auth*.*:*google*.*:*utc*.*:*U
TC*.*:*crypt*.*:*key*.*:*upbit*.*:*bcex*.*:*bithimb*.*:*hitbtc*.*:*bitflyer*.*:*kucoin*.*:
*huobi*.*:*poloniex*.*:*kraken*.*:*okex*.*:*binance*.*:*bitfinex*.*:*gdax*.*:*ethereum*.*:
*jaxx*.*:*exodus*.*:*metamask*.*:*myetherwallet*.*:*electrum*.*:*bitcoin*.*:*blockchain*.*
```

Once it starts running, Vidar searches for data specified in its configuration along and delivers it to the command and control (C2) server as a ZIP archive, [notes] Segura.

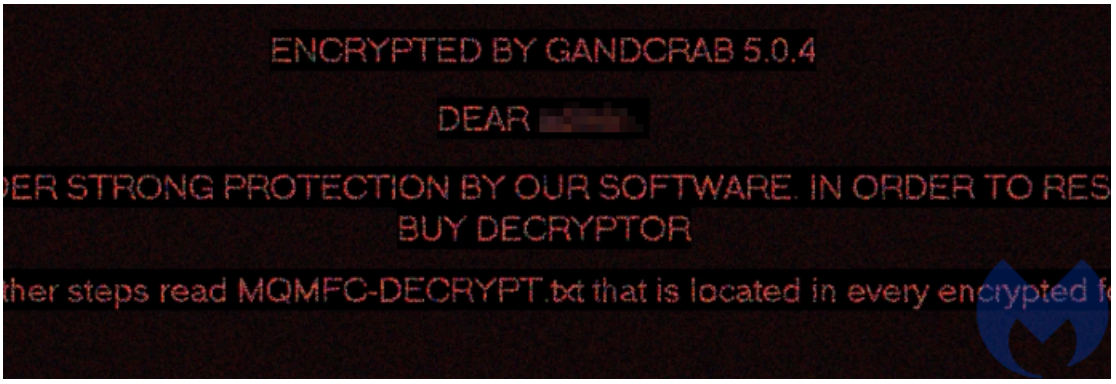
Its interface makes it easy for the operator to keep track of the victims, deliver instructions to the malware and check the type of data collected from each infected host.



Downloading GandCrab ransomware

Vidar can work as a malware dropper and in the case observed by Malwarebytes the second payload was GandCrab ransomware.

"Within about a minute after the initial Vidar infection, the victim’s files will be encrypted and their wallpaper hijacked to display the note for GandCrab version 5.04."



5.04 is the latest revision of the ransomware and at the moment there is no possibility to decrypt the files it touches without paying the ransom or getting the decryption key from the threat actor.

Users affected by earlier versions of the ransomware can recover their files with a free GandCrab decryption tool that works with v1, v4, and v5 up to v5.02 of the malware.

Running an infostealer before deploying the ransomware ensures some money for the adversary even if the victim does not pay the ransom. Even if the cybercriminals do not use the stolen data themselves, they can sell it on underground forums.

Users with computer files locked by GandCrab should now also consider changing the username/password combinations at least for the critical services and applicatons they're using.
