TRUST IN GERMAN SICHERHEIT

G DATA
Whitepaper 2018 – paper 06

Analysis of

Win32.Trojan-Ransom.GandCrab.R

+

Extra: a look into a Ukrainian wholesale cybercrime business

G DATA Software AG | October 2018

Analysis by: https://twitter.com/RansomBleed

Contents

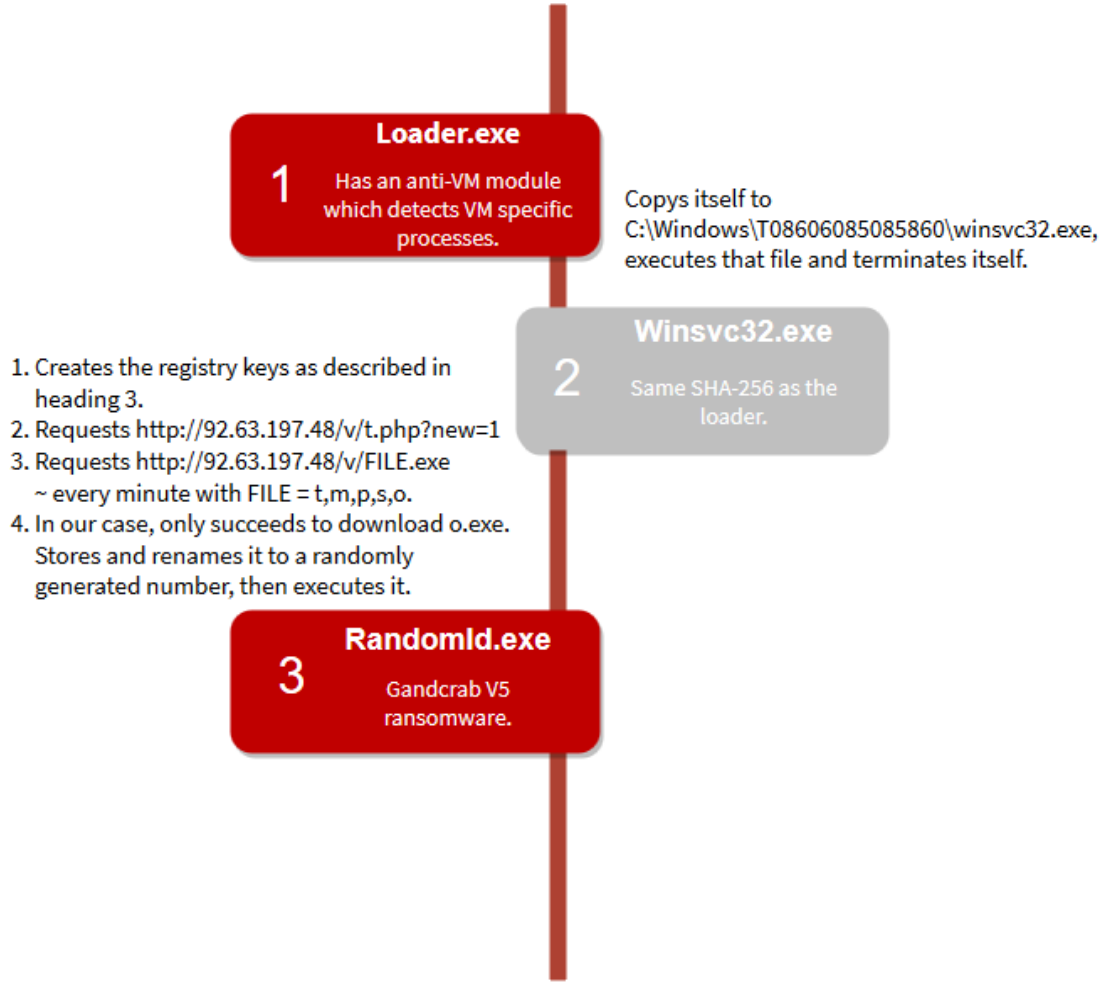
1

1. Introduction

Browsing the malc0de.com DB[1] led me to an interesting malware[2], which by the time of analyzing was in comparison to other samples yet not that much detected by AV solutions and the detection families weren't quite clear. That was a sign for me that I might have found a new and interesting sample to analyze!

Turns out that the file was a loader for the GandCrab v5 ransomware.

2. Overview



Note: The loader tries to move the file *4377357356* to *srhjtsjtsshtjsjs* and tries to delete the files *afiuegfuaeugfiaegf* and *246247357357357.* Also it tries to search for the window names *afiugefiegfiagef*, *eafeougaeoguoegf* and *aohefouaehoufaehfaehu.* If one of those names is found, the focus is then set to them (they receive the keyboard input) and the found window is set to the foreground. The sleep function is called between each operation.

Note #2: The steps 1-4 are only executed if winsvc32.exe is actually in the folder *C:\Windows\T08606085085860* as seen in the image above.

3. The registry keys

Debugging the loader led me to the following registry changes:

Registry key	Functionality
HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusOverride set to 1	Windows security center stops monitoring the status of an antivirus protection
HKLM\SOFTWARE\Microsoft\Security Center\UpdatesOverride set to 1	No clear documentation available but it seems like it disables the antivirus updates.
HKLM\SOFTWARE\Microsoft\Security Center\FirewallOverride set to 1	Turns of the firewall
HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusDisableNotify set to 1	Disables the antivirus notifications
HKLM\SOFTWARE\Microsoft\Security Center\AutoUpdateDisableNotify set to 1	Disables security center update notifications
HKLM\SOFTWARE\Microsoft\Security Center\FirewallDisableNotify set to 1	Disables firewall notifications
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\DisableSR set to 1	Disables system restore points
HKCU\SOFTWARE\Microsoft\CurrentVersion\Run set to *C:\Windows\T08606085085860\winsvc32.exe*	Creates an autostart entry

4. Spreading method

Winsvc32.exe gets a list of all available external drives as well as the network shares *\public_html, \\htdocs, \\httpdocs, \\wwwroot, \\ftproot, \\share, \\income* and *\\upload.*

It creates the directory _ and moves all data from the disks and copies itself as DeviceManager.exe inside that folder. An autorun.inf file with the following code is created.

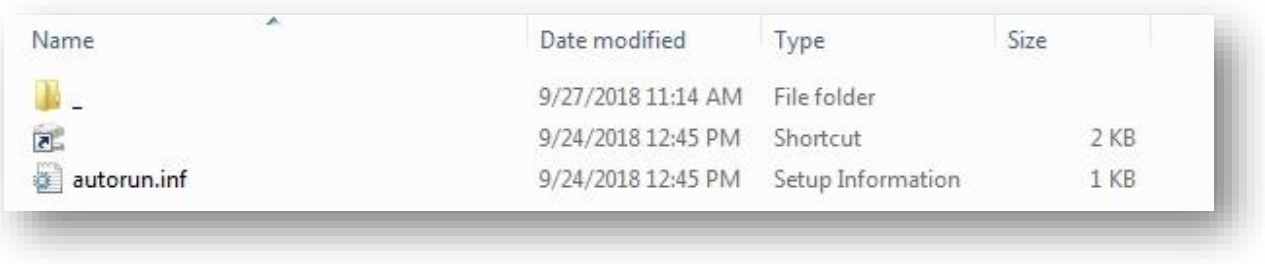
```
[AUTORUN]OPEN=_\DEVICEMANAGER.EXE

USEAUTOPLAY=1
```

A shortcut having an empty name and a disc icon with the following location is created.

%WINDIR%\SYSTEM32\CMD.EXE /C START _ & _\DEVICEMANAGER.EXE & EXIT

To visualize this behavior better, see the following picture of the final result.



A report about the GandCrab v5 ransomware is here[3].

5. Digging deeper

Checking the WHOIS entry of the IP address lead to very interesting results. The owner name is *"Fop Horban Vitalii Anatoliyovich"* who is apparently living at *"62408, Kharkiv Region, Elite Village, School Str. 25, Ap. 26"* according to myip.ms[4]. Google maps shows that this is the address of the local post office, which indicates that it is not the real address of the owner.

Looking at other services in the IP range 92.63.197.0-255 which are all owned by the same user lead to several websites.

6. Money related domains

Active domain Frim0ney.info

According to the website traffic analysis tool Similarweb.com, the main traffic source for the domain frim0ney.info are emails[5]. It's very likely that the author is using that domain for spam purposes as the website displays an offer which is very typical for spam. You can see a snippet of the offer below.

Inactive domains

Lucky-chances.com, earn-your-money.com, global-profits1.com, best-profits-here12.com

➔ Under construction

7. Dating related domains

Active domain Dating-future69.com, sewryus.xyz

No data from Similarweb.com is available unfortunately. When searching for the domain *dating-future69.com* in Google, all the spam report links suggest that this domain is about spam as well. Backlink entries from mostly Chinese Forms are also confirm this thought. In the image below you can see a few of those entries summed up in one picture.

Inactive dating domains

Dating-future69.com, 100sexual-partner-found.com, realflirtdating11.com, your-dating-now11.com,great-hookup-online.com, dating-hearts.com, yourdating-menus.com, hotdatingspot.com, datingsworld1.com, dating-opportunities.com, hot-kisses-finder.com, night-calldates.com, secret-flirtparadise.com

➔ under construction

findyour-dating1.com

➔ resolves a streaming site

myhookup-clubs.com

➔ resolves a warez site

8. Misc domains

Os-print.win

➔ Shows a casino offer

vrb-kontosicherheit.top

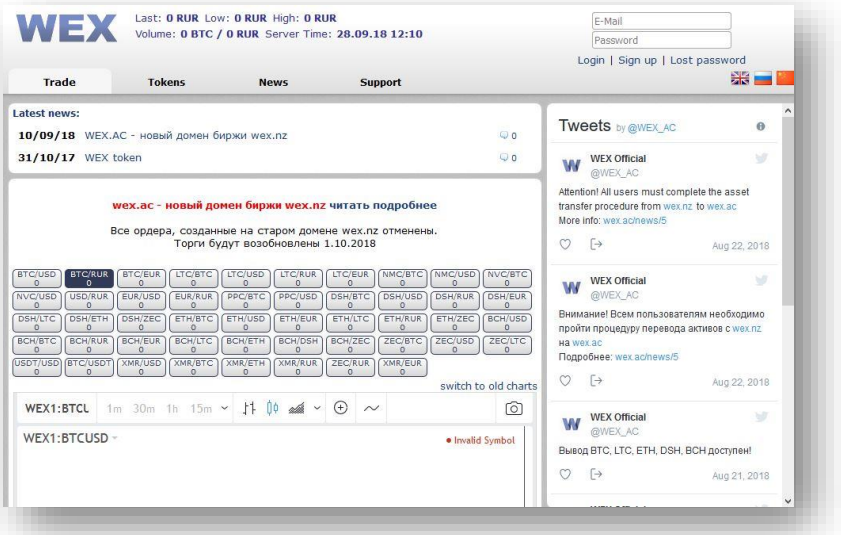
➔ ERR_CONNECTION_TIMED_OUT

enterwords.ru, improbablead.com, honeyindoc.ru, vivedoc.ru

➔ Empty page

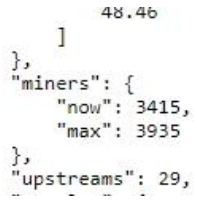
Wex.ac

The website running under that domain appears to be a cryptocurrency exchange. After seeing all of the domains before, I initially had no good feeling about this one as well and it turns out to be true. According to a Bitcointalk.com topic[6], the domain wex.ac just mirrors the original site wex.nz so that it looks real for possible victims. Furthermore, the site is used for phishing login data which is used by the criminals to log into the real exchange and possibly steal the money which is stored on the real exchange. Below you can see a screenshot from the fake website which looks almost identical to wex.nz.



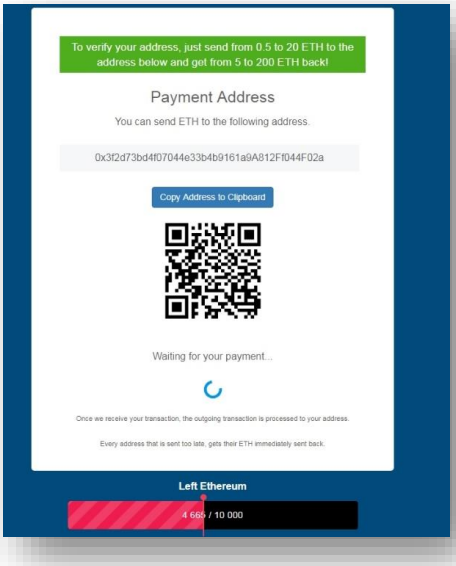
http://92.63.197.48:8080/

This host displays a JSON output which reveals that somewhere, eventually due to a download from Winsvc32.exe shown in the overview, cryptocurrency is mined. At the current time of writing there seem to be 3415 active infected devices.



http://92.63.197.127/

This website leads to a scam involving the cryptocurrency Ethereum which claims that if a victim sends 0.5 – 20 ETH, it will get 5 – 200 ETH in return.



9. File hashes and resources

[1] http://malc0de.com/database/

[2] 672feda122f91a12c5ff8b24db05dfac0d6677074aeeb933e72f1f753c100c39

[3] http://csecybsec.com/download/zlab/20181001_CSE_GandCrabv5.pdf

[4] https://myip.ms/view/web_hosting/729281/Fop_Horban_Vitalii_Anatoliyovich.html

[5] https://www.similarweb.com/website/frim0ney.info

[6] https://bitcointalk.org/index.php?topic=4906680

If you want to stay updated about malware, be sure to follow these accounts:

RansomBleed - My personal twitter account about the latest malware reports.

GDataSoftwareAG – G DATAs twitter company account.

Blog – The G DATA blog about all kinds of security-related news.