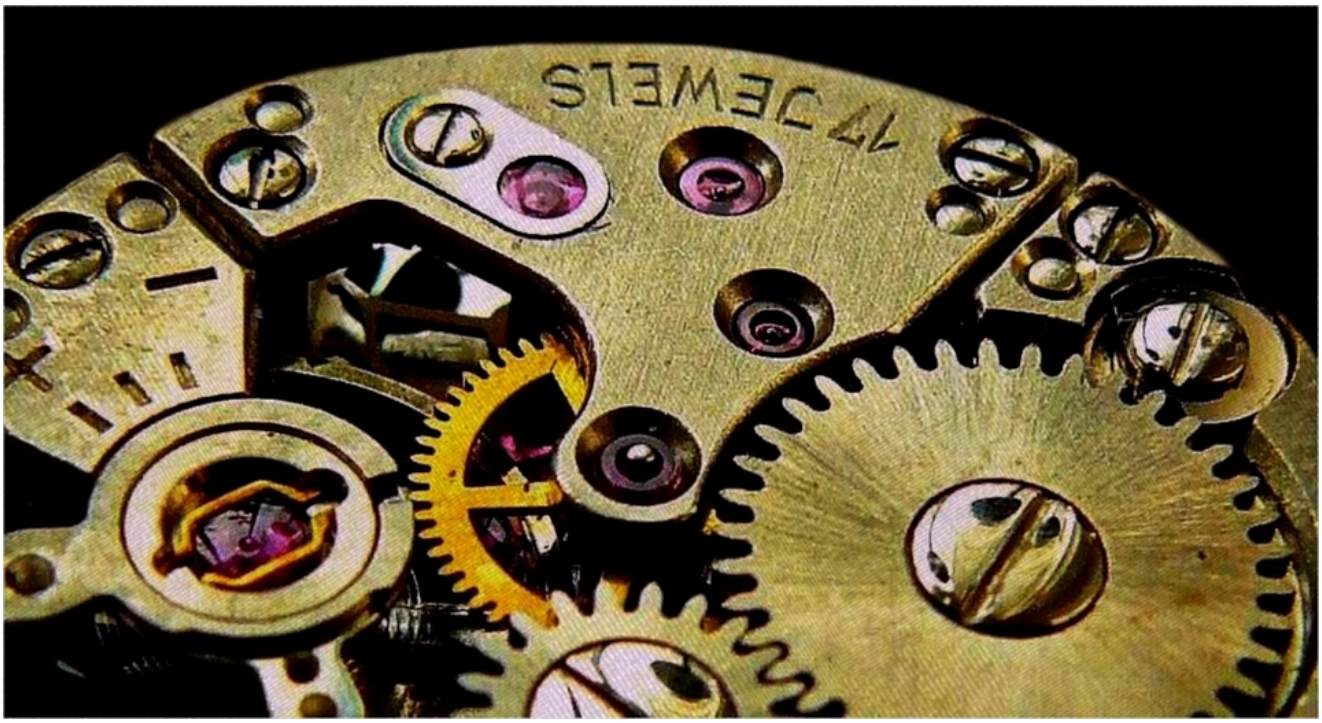
A deeper look at Tofsee modules

cert.pl/en/news/single/a-deeper-look-at-tofsee-modules/



Tofsee is a multi-purpose malware with wide array of capabilities – it can mine bitcoins, send emails, steal credentials, perform DDoS attacks, and more. All of this is possible because of its modular nature.

We have already published about Tofsee/Gheg a few months ago – https://www.cert.pl/en/news/single/tofsee-en. Reading or at least skimming it is probably required to fully understand this post. Note that it is meant as an extension of that research, focusing on plugin functionality that we previously ignored. We will shortly summarize each plugin and highlight its most important features.

The post is rather long – for the impatient, list of hashes and table of contents in one:

Resource Id	DLL name	DLL MD5 hash
1	ddosR.dll	fbc7eebe4a56114e55989e50d8d19b5b
2	antibot.dll	a3ba755086b75e1b654532d1d097c549
3	snrpR.dll	385b09563350897f8c941b47fb199dcb
4	proxyR.dll	4a174e770958be3eb5cc2c4a164038af
5	webmR.dll	78ee41b097d402849474291214391d34

Resource Id	DLL name	DLL MD5 hash
6	protect.dll	624c5469ba44c7eda33a293638260544
7	locsR.dll	2d28c116ca0783046732edf4d4079c77
10	hostR.dll	c90224a3f8b0ab83fafbac6708b9f834
11	text.dll	48ace17c96ae8b30509efcb83a1218b4
12	smtp.dll	761e654fb2f47a39b69340c1de181ce0
13	blist.dll	e77c0f921ef3ff1c4ef83ea6383b51b9
14	miner.dll	47405b40ef8603f24b0e4e2b59b74a8c
15	img.dll	e0b0448dc095738ab8eaa89539b66e47
16	spread.dll	227ec327fe7544f04ce07023ebe816d5
17	spread2.dll	90a7f97c02d5f15801f7449cdf35cd2d
18	sys.dll	70dbbaba56a58775658d74cdddc56d05
19	webb.dll	8a3d2ae32b894624b090ff7a36da2db4
20	p2p.dll	e0061dce024cca457457d217c9905358

1. ddosR.dll

Original filename: p:\cmf5\small2\plugins\plg_ddos\ddos.cpp

This plugin can perform DDOS attacks. Implemented attacks are not very complicated, for example request spamming (HTTP Flood):

Or plain old SYN flood (using PassThru driver, aka grabb module).

We haven't observed any DDoS activity from Tofsee yet, so this plugin is probably not used by the botmaster.

Configuration from the C&C for this plugin is very simple:

The binary contains a lot of strings, what simplifies analysis greatly:

2. antibot.dll

Original filename: z:\cmf5\small2\plugins\plg_antibot\plugin.cpp

Now, this is an interesting plugin, because it removes other malware from victim's computer.

It can:

- enumerate processes and kill ones that may be dangerous (search by configured names)
- search SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects registry branch, and remove bad browser helper objects
- enumerate mutexes and kill processes that own them (search by mutex names).

List of browser helper objects removed by this module (downloaded from C&C):

3. snrpR.dll

Original filename: p:\\cmf5\\small2\\plugins\\plg_sniff\\sniff.cpp

Related config section:

Communication is sniffed and replaced using PassThru driver (accessible through named pipe “\\\\.\\PassThru”)

- **mail.sniff** enables stealing mail addresses from incoming e-mails. Mail addresses are stolen from “From” and “To” fields. It also looks for entities “%40″,”#64″,”#064” in content (looking for “@” char).

- **ftp.sniff** and **pop.sniff** enables POP3 and FTP credentials stealing. The plugin is looking for “user” and “pass” protocol commands, gets authentication data and sends through Passthru driver.

- **mail.replace** functionality replaces incoming e-mails using a specified template (stored in ‘mailbody’ key of config)

Template example that we received (despite this function being turned off right now):

It leaves original “From” and “To” headers (%FROM_LINE, %TO_LINE), has the ability to leave original subject (%SUBJ, %_SUBJ), and original timestamps (%DATE, %P5DATE, %M5DATE).

4. proxyR.dll

Original filename: p:\\cmf5\\small2\\plugins\\plg_proxy\\plugin.cpp

This plugin listens for TCP connections on 0.0.0.0:1080 and provides multithreaded SOCKS proxy server. The sample we analyzed identifies itself in Proxy-Agent HTTP header as WinRoute Pro/4.1.

Traffic is redirected to addresses specified at a proxy_cfg section, separately for each region.

Addresses are specified as a reference to a work_srv list or directly.

In proxy_cfg we can also find some defined timeouts for a socket.

When any value is missing in configuration, binary has some sane defaults inside.

Plugin also adds port mapping using UPNP, disguising itself as Skype:

Strings from the binary give a little more insight about the purpose of this plugin:

6. protect.dll

Original filename: z:\cmf5\small2\plugins\plg_protect\plugin.cpp

This plugin downloads and installs malicious service in system:

Malicious service binary is obfuscated with “state-of-the-art encryption algorithm” – i.e. negating every byte:

Md5 of decrypted backdoor = 49642f1d1b1673a40f5fa6263a66d056. This file is protected by packer, and it’s the only packed binary that we observed during our analysis of Tofsee – it suggests that the binary could’ve been created by another actor and reused in Tofsee.

7. locsR.dll

Original filename: z:\cmf5\cmf5\small2\plugins\plg_locs\plg.cpp

This plugin steals network credentials for Microsoft Outlook:

After extracting them from the registry, they are decrypted and used to send more emails. Additionally, it generates email in form [computer name]@mail.ru and attempts to send emails using it (with raw SMTP protocol).

Strings from binary:

10. hostR.dll

This is HTTP server plugin. It masquerades as Apache/2.2.15 (Win32). It can serve files, probably for other bots.

It is able to blacklist some IPs – probably security analysts (for example Forcepoint and Google are banned).

Configuration for this module, fetched from the C&C:

11. text.dll

Original filename: p:\cmf5\small2\plugins\plg_text\plg_text.cpp

Very short plugin, it is able to process email templates downloaded from C&C.

12. smtp.dll

Very important module – it generates and sends emails. It's probably biggest module and code is rather complicated sometimes.

Most interesting thing about it is the fact that it uses its own dedicated scripting language for generating messages. Script example, received from C&C:

If someone recognizes this as a real scripting language, we'd be grateful for the information. We have never seen something like this, so we analyzed interpreter of this language.

The syntax is rather simple, but very assemblish and primitive. We hope that malware authors are generating this scripts from a higher level language because writing something like this must really hurt one's sanity ;].

A lot of opcodes are supported – take a look at this (simplified) parsing function for example:

We didn't reverse all of them, but few most important ones are:

- C ip:port – Connect
- L lbl – Create Label lbl.
- J lbl – Jump to label lbl.
- v name value – Create variable name and assign value value.
- W text – Write something to output – in this case to final email.
- I lbl condition – If condition is satisfied than jump to lbl

Additionally wrapping text in """ allows for newlines and escape sequences in it, and __v(XX)__ is a variable interpolation.

Again, few from the most interesting strings from that binary:

We thought that IfYouAreReadingThisYouHaveTooMuchFreeTime is an easter egg for us, malware analysts, but it turns out that it's just a strange quirk related to hotmail authentication.

Configuration for this module, fetched from C&C:

13. blist.dll

This plugin checks if a bot is listed as a spambot and blacklisted. In the config we observed following DNSBLs (DNS-based Blackhole Lists) were supplied:

DNSBL is a service based on DNS used for publishing IP addresses of spam senders. If spam server uses DNSBL filters, it will do a DNS request to DNSBL domain with each incoming SMTP connection. Technical details are outside of the scope of this post, but any interested reader can take a look at http://www.us.sorbs.net/using.shtml or https://en.wikipedia.org/wiki/DNSBL.

Checking DNSBL is implemented with gethostbyname:

Configuration for this module, fetched from C&C:

14. miner.dll

This is (as the name suggests) cryptocurrency miner. This plugin only coordinates the work, but it has few accompanying binaries, that perform the dirty work.

One binary, called grabb, is distributed straight from the C&C. Other binaries are downloadable through URLs specified in configs – in theory. In practice, servers distributing miners seem to be dead, so we were not able to download miners.

Miner "verifies" that has really downloaded right binary, but hashing was probably too difficult for malware creators to implement, so they settled on size verification – for example, they are check that cores_gt_1 binary has exactly 223744 bytes.

We didn't analyze it in-depth because crypto miners are boring enough, and strings from binary give enough information about inner workings anyway:

And the rest can be read from the configuration, fetched from C&C:

15. img.dll

This short plugin processes malicious attachments – encodes them with base64 and appends to emails.

Nothing interesting here, as can be seen in hardcoded strings:

Configuration for this module, fetched from the C&C:

16. spread.dll

First, it extracts xs, datr, c_user (and more) cookies.

Exact method depends on the browser, but generally plugin reads cookies stored on disk by the browser – for example cookies.sqlite from \Mozilla\Firefox\Profiles, for Firefox. Supported browsers are Chrome, IE, Firefox, Safari, and Opera.

After that, plugin uses that cookies to impersonate user in facebook API:

List of friends is downloaded through API and a message is sent to them. Format of message is stored in configuration, for example:

'fb.message1': '%SPRD_TEXT1|%LANG_ID| %SPRD_URL1'

Twitter is handled very similarly: cookies are stolen, followers are downloaded by API call to https://twitter.com/followers, and messages are sent.

VKontakte also seems to be supported, but that functionality is optional and held in another plugin. This module only checks if VK is enabled in config and calls handler (that can be initialized from another plugin), if it's defined. Malware creators usually don't like to attack Russia, so this function is disabled and VKontakte plugin is not distributed.

Plugin can also spread itself through Skype, but reverse engineering Skype protocol was clearly too hard for malware authors, so plugin waits until Skype is started, and then sends windows messages to Skype window:

The plugin has dozens of strings hardcoded, so analyzing it in disassembler is a breeze. Few more interesting groups:

References to the OCR plugin – to avoid captchas:

Facebook cookies:

Strings related to Facebook spread:

Strings related to cookie stealing:

Strings related to Skype hijacking:

Twitter cookies:

And Twitter spread:

Finally, things needed to send stolen cookies somewhere:

Rich functionality means rich configuration from the C&C:

17. spread2.dll

This plugin uses methods more than 15 years old, and tries to spread Tofsee through… infected USB drives! This doesn't sound like an effective idea for A.D. 2017, but despite that, the plugin is still enabled.

First it copies malicious binary into RECYCLER\<random_gibberish>.exe file on the USB drive, then sets READONLY and SYSTEM attributes on that file, and finally writes malicious autorun.inf file:

The malicious binary that will be spread is downloaded from the internet (see also sys.dll plugin and %FIREURL variable).

Nothing too interesting in hardcoded strings, except operation logs:

Configuration for this module, fetched from the C&C:

18. sys.dll

This plugin seems to be a downloader or rather an updater. It sends requests, depending on a value of the %FIREURL configuration variable.

Example values of the %FIREURL variable (one per line):

Variables are expanded recursively, and %SYS_RN means \r\n of course, so first possible value can be read as:

If we send this request to that IP address on port 80, we will get yet another malicious binary. Different requests lead to different binaries.

If a request is invalid, or not supported, following image is sent instead:

We appreciate the humor.

Nothing surprising in hardcoded strings:

Configuration for this module, fetched from the C&C:

Additionally the %FIREURL variable from config is used.

19. webb.dll

This plugin tries to locate iexplore.exe process. If this succeeds, it injects DLL file called IEStub.dll to this process.

IEStub.dll hooks a lot of functions from iexplorer. List of hooked functions:

Hooks intercept called functions and can change their parameters. We haven't analyzed hooks in depth, but most of them seem to be loggers intercepting "interesting" data from parameters – We haven't observed any web injects served by Tofsee.

For completeness, interesting hardcoded strings:

Configuration for this module, fetched from the C&C:

20. P2P.dll

Original filename: p:\cmf5\small2\plugins\plg_p2p\plg_p2p.cpp

This plugin is rather short. Despite promising name, it's rather boring – opening a port on a router and listening for connection is the most important thing it does. It doesn't implement any commands, this is left for the main module to handle.

Like almost every module, it logs to %TMP%\log_%s.txt, and when this fails falls back to C:\log.txt.

Also adds port mapping using UPnP, in the same way as plugin 4 (proxyR.dll).

Configuration for this module, fetched from the C&C:

Interesting strings: