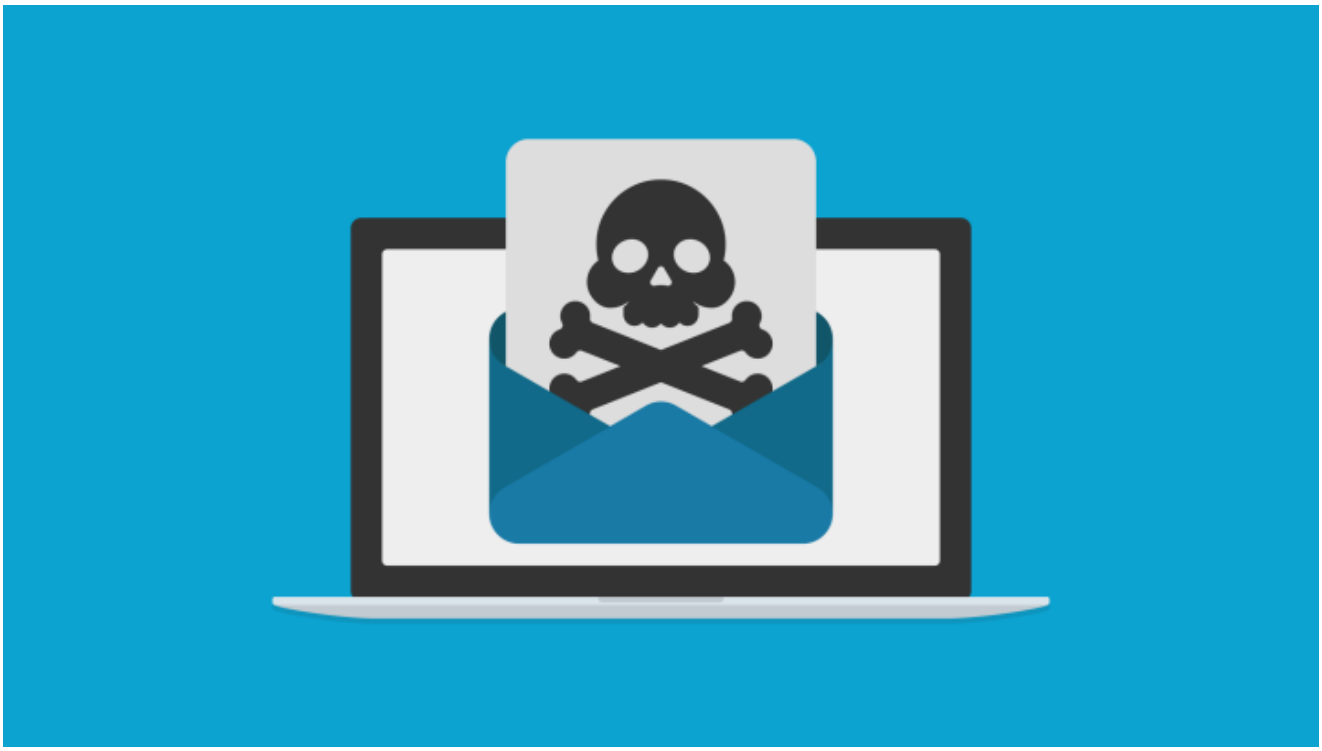
Tofsee Botnet: Proxying and Mining

bitsight.com/blog/tofsee-botnet-proxying-and-mining

Written by André Tavares March 27, 2023 Share Facebook Twitter LinkedIn



Key findings

- 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.

Old bot, new tricks (not really)

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.

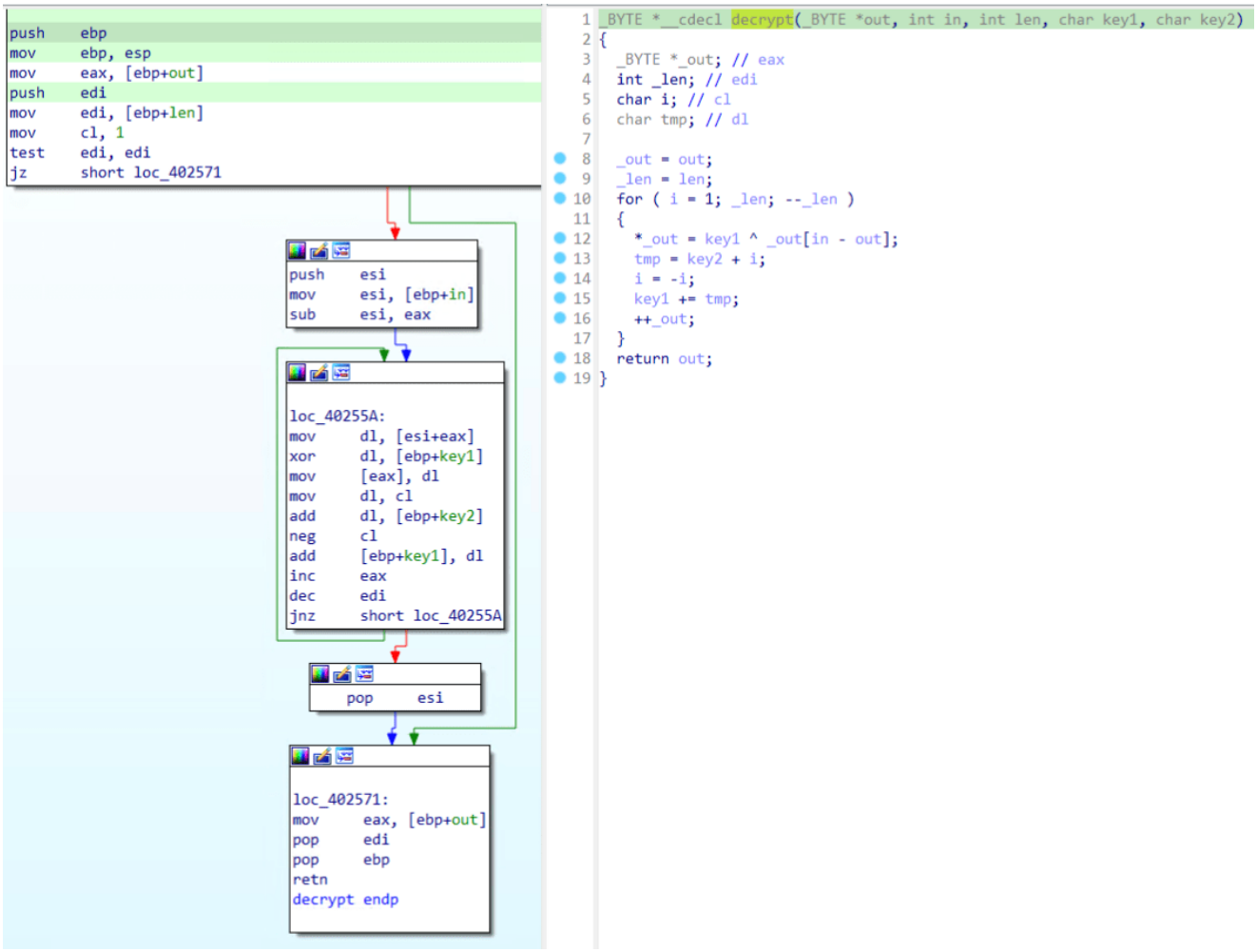


Figure 1 - Tofsee string decryption function.

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.

Proxying web traffic

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.

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.

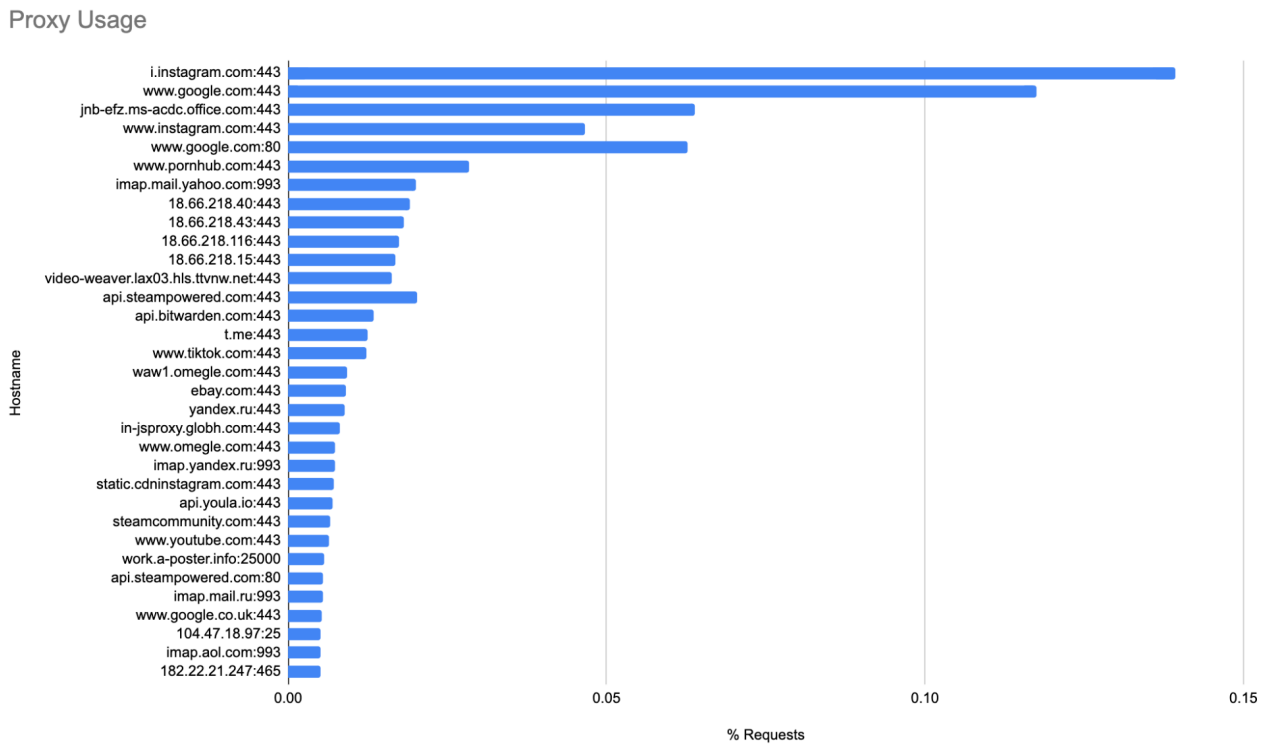


Figure 2 - Most requested HOST:PORT pairs.
While looking through the traffic, we spotted an interesting pattern. Around **3%** of the requests were HTTP POST with the URI ending in "**.php**" and, in many cases, starting with "**/wp-**", to random websites that appear legitimate. Each request's payload 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.

Mining Masari

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.

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)

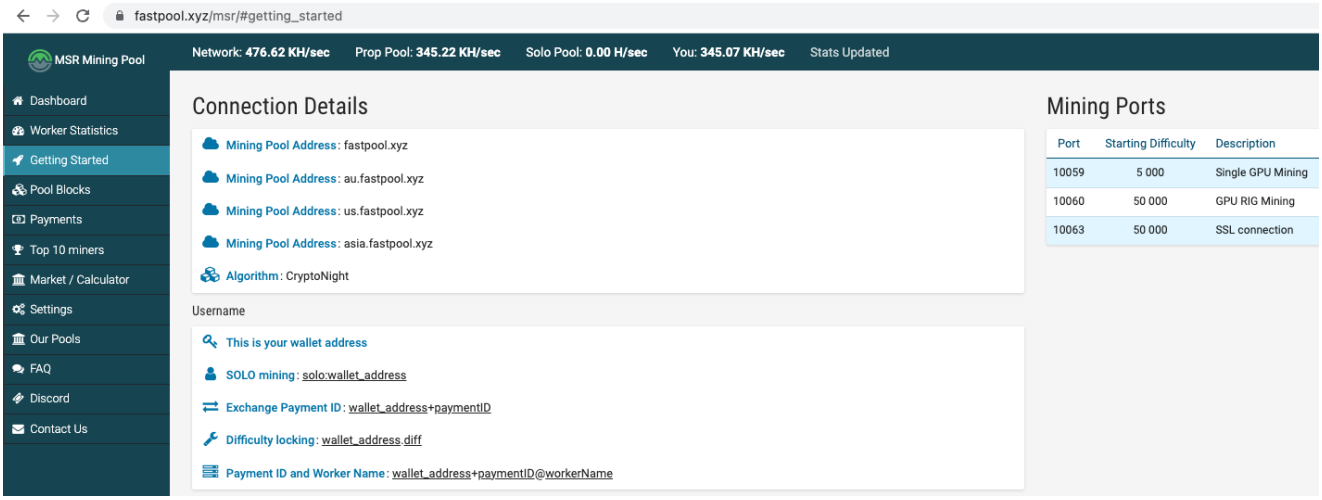


Figure 3 - MSR mining pool documentation
The mining pool website has some statistics on the botnet's mining work (Fig. 4). In total so far, to this address, Tofsee botnet was able to mine ~200 000 MSR, which currently corresponds to ~1500$. By searching for the wallet address on Google, the first reference is from June 2022.

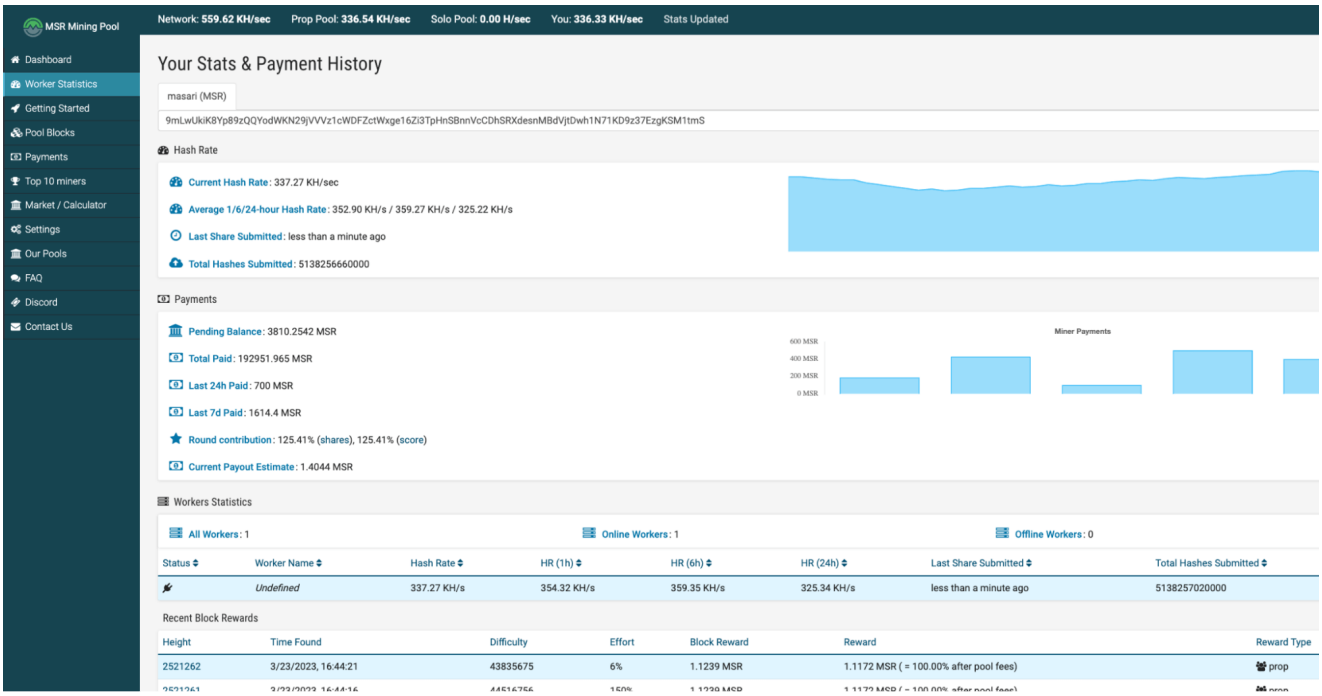


Figure 4 - MSR mining pool documentation

Tracking the botnet

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.

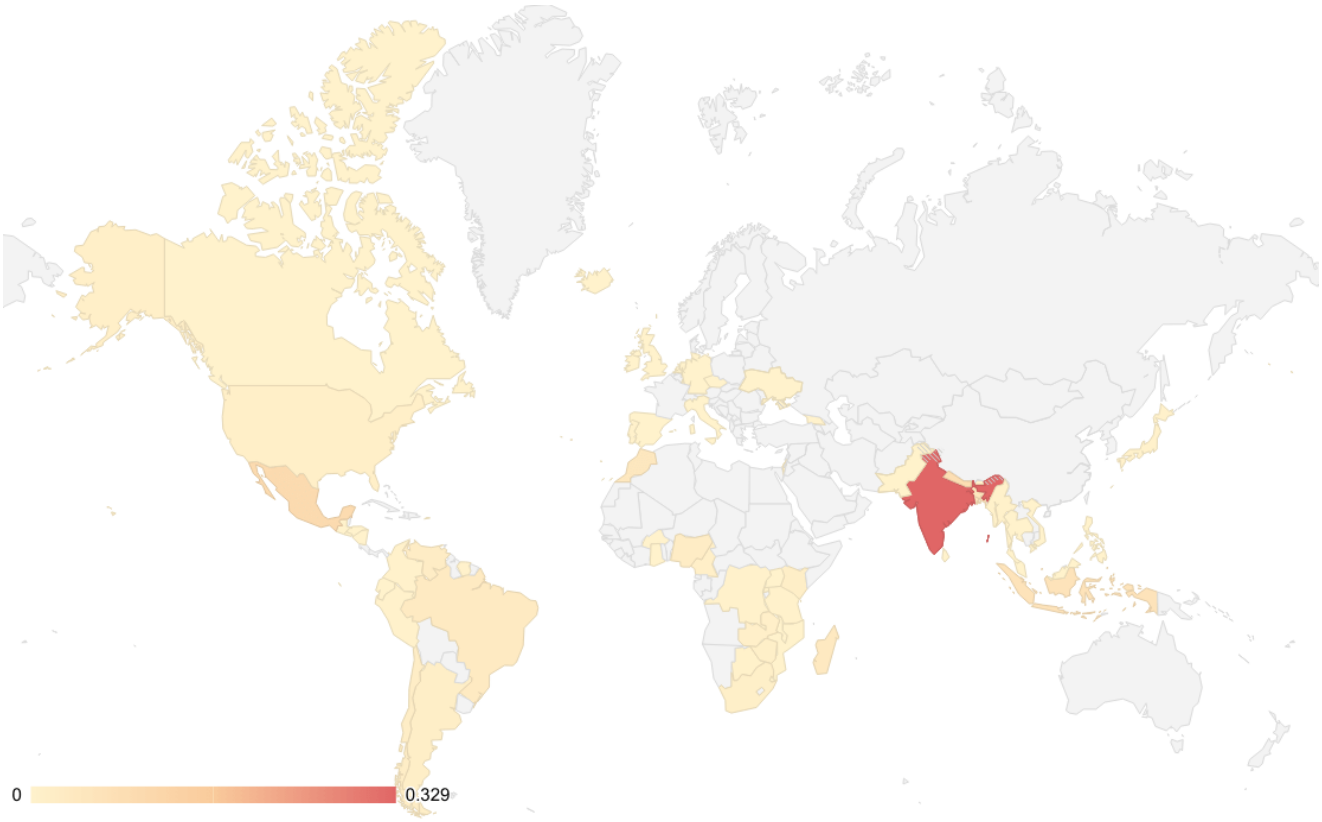


Figure 5 - Approximation of Tofsee botnet distribution in March 2023.
The data used to populate this map is sampled, which means that the actual geographical distribution of Tofsee may be closer to this one but not exactly what this map suggests.

Wrap-up

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.

IOCs & Signatures

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:

String decryption function in Python:

Suricata rule:

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

Note: Both rules need to trigger in order for an alert to be generated.

More at https://github.com/bitsight-research/threat_research