Tracking PrivateLoader: Malware Distribution Service

bitsight.com/blog/tracking-privateloader-malware-distribution-service

Written by André Tavares August 31, 2022

PrivateLoader is a loader from a pay-per-install malware distribution service that has been utilized to distribute info stealers, banking trojans, loaders, spambots, and ransomware on Windows machines. First seen in early 2021, being hosted on websites that claim to provide cracked software, the customers of the service are able to selectively deliver malware to victims based on location, financial activity, environment, and specific software installed. BitSight's partial visibility over its botnet of infected machines suggests that it's spread worldwide, with a significant percentage of infections in India and Brazil.

Infection chain

PrivateLoader was seen being distributed through SEO-optimized websites that claim to provide cracked software. Victims download a password-protected zip file (the password is in the file name) which contains an NSIS installer that executes many malicious payloads, including PrivateLoader. It's a multi-stage malware loader comprising at least three modules: the *loader*, the *core*, and the *service*.

In the first stage, the *loader* is executed, which downloads and executes the second stage, the core module. The *core* module's primary purpose is to download and execute more malware, including another PrivateLoader module named service. The *service* module takes care of persistence by creating a scheduled task and, not only self-updates but also downloads and executes the loader module. Figure 1 depicts the typical infection chain.

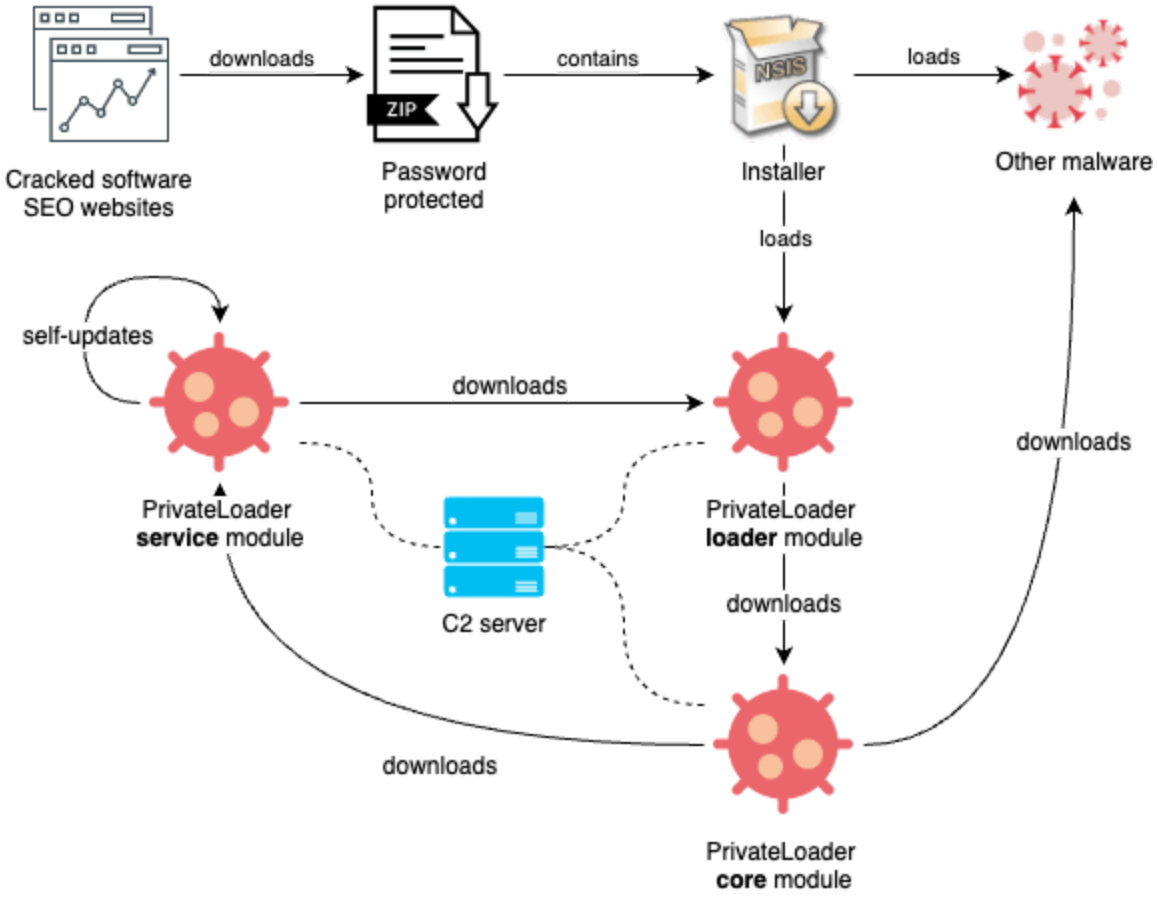

Fig. 1 - PrivateLoader infection chain.

Capabilities

The main purpose of PrivateLoader is to download and execute more malware. Moreover, both static and dynamic analysis (Fig. 3 and 2) suggest that the malware has additional capabilities, such as disabling Windows Defender, the discovery of user-sensitive data, and many anti-analysis techniques.

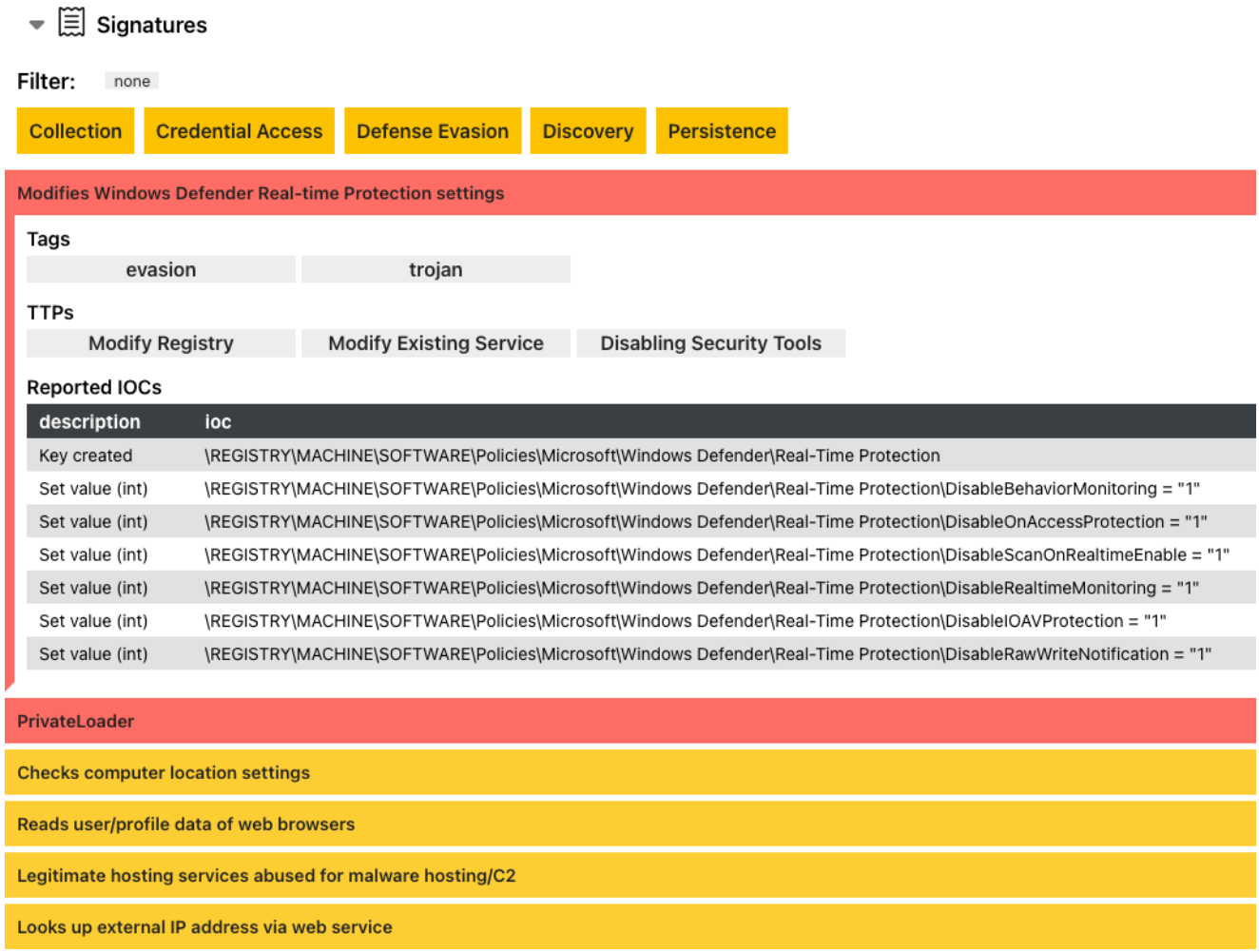

Fig. 2 - Automated dynamic analysis of the loader module.

CAPABILITY	NAMESPACE
contain obfuscated stackstrings (2 matches)	anti-analysis/obfuscation/string/stackstring
get geographical location	collection
parse credit card information	collection/credit-card
reference Base64 string	data-manipulation/encoding/base64
encode data using XOR (7 matches)	data-manipulation/encoding/xor
encrypt data using AES via x86 extensions (2 matches)	data-manipulation/encryption/aes
reference AES constants	data-manipulation/encryption/aes
hash data with MD5	data-manipulation/hashing/md5
hash data using SHA256	data-manipulation/hashing/sha256
authenticate HMAC	data-manipulation/hmac
contain a resource (.rsrc) section	executable/pe/section/rsrc
get common file path	host-interaction/file-system
set current directory	host-interaction/file-system
delete file (2 matches)	host-interaction/file-system/delete
get file attributes	host-interaction/file-system/meta
set file attributes	host-interaction/file-system/meta
read file on Windows (5 matches)	host-interaction/file-system/read
write file on Windows (7 matches)	host-interaction/file-system/write
set registry value (2 matches)	host-interaction/registry/create
link function at runtime on Windows	linking/runtime-linking
linked against Crypto++	linking/static/cryptopp
inspect section memory permissions	load-code/pe
parse PE header (2 matches)	load-code/pe
resolve function by parsing PE exports (4 matches)	load-code/pe

Fig. 3 - Rule-based static analysis of the core module with CAPA.

Moreover, previous research on PrivateLoader shared a YARA rule to detect and hunt its samples based on its string decryption technique and also a python script to extract all of its strings, which contains valuable information when reversing the malware. Those strings can also be used for defense, hunting, and tracking purposes since the command and control servers (C2) and other configuration values are included in them. As an example, here are all of the strings from a loader module, a core module, and a service module.

Botnet tracking

Combining the mentioned sample hunting technique with previous research on how the bots communicate with their C2 servers allowed us to build a tracker that gives us visibility over what's being distributed by PrivateLoader.

We started tracking PrivateLoader in July 2022 and so far we've seen 1K+ URLs used to distribute 2K+ samples. As an example, this URL was used to distribute 4 samples of Redline malware. We've seen many URLs from Discord, VK, and Amazon CDNs, although domains and IPs are also often used.

Figure 4 shows the top malware distributed by PrivateLoader this past July and August. Most of them are stealers, Redline being by far the most common, but there are also banking trojans, loaders, spambots, and even ransomware.

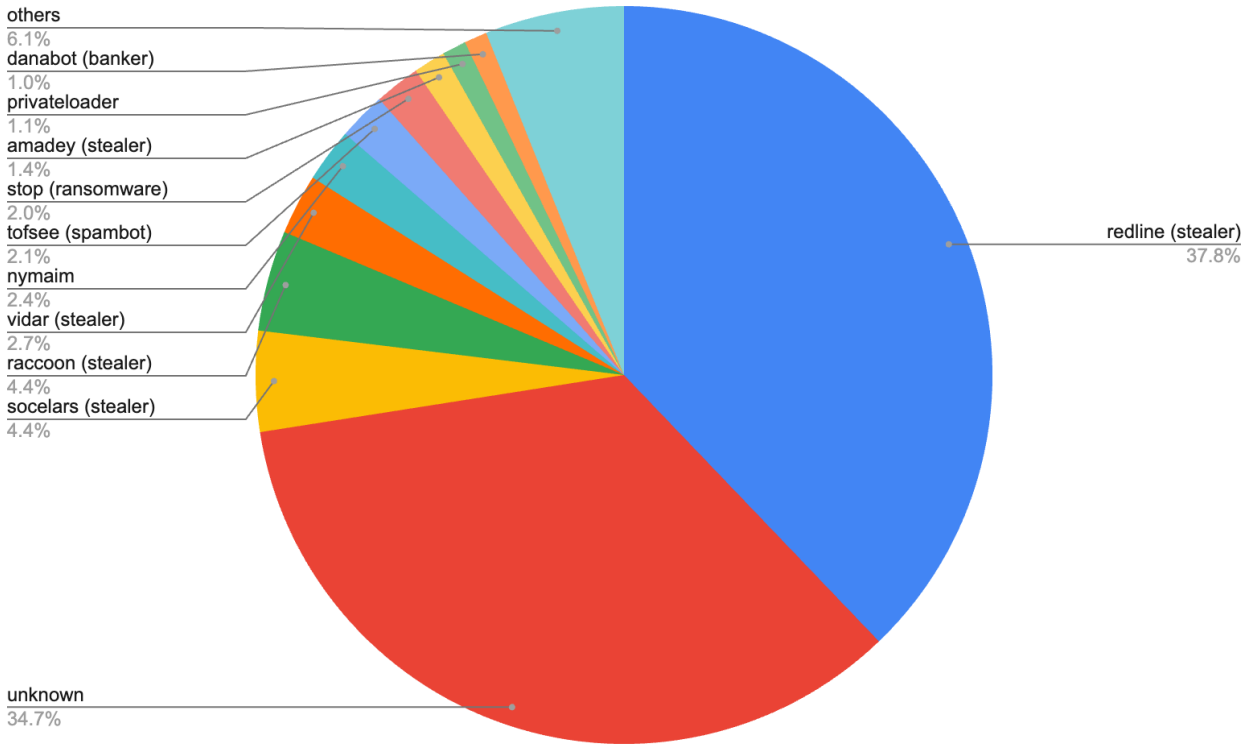

Fig. 4 - Top Malware Families Distributed by PrivateLoader in July and August 2022.

We were able to identify with high confidence 30 malware families being distributed by PrivateLoader. They are AgentTesla, Amadey, ArrowRAT, AsyncRAT, Azorult, Colibri, Danabot, DCRat, Eternity, Fabookie, Formbook, GCleaner, Glupteba, Gozi_ISFB, PseudoManuscrypt, Nitol, NetSupport, Nymaim, PrivateLoader, Qakbot, Raccoon, Redline, SmokeLoader, Socelars, STOP, Tofsee, Vidar, WarzoneRAT, XMRig, and YTStealer. For some of them, we only encounter a couple of samples, and so they are included in the "others" slice.

Regarding the unknown samples, since this classification was done in an automated way, some samples are harder to programmatically classify; some signatures probably need to be improved, but also some of them might be new unknown malware. By sampling and manually analyzing some of the unknown samples, we mainly identify Redline and SmokeLoader, although Fabookie, Vidar, Raccoon, and NekoStealer families were also observed.

BitSight's partial visibility over the geographical distribution of PrivateLoader in July 2022 suggests that it's spread worldwide, with a significant percentage of infections in India (21%) and Brazil (16%), as figure 5 shows.

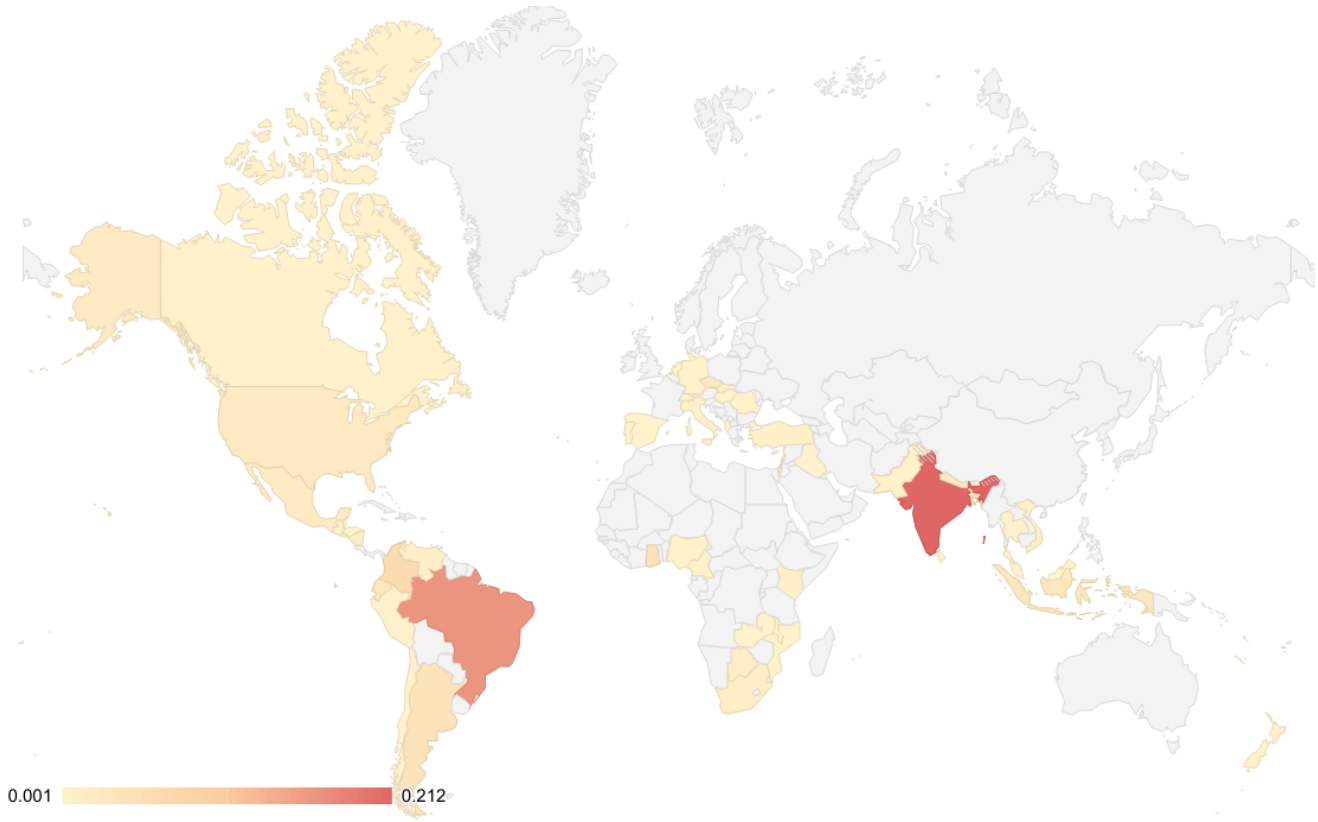

Fig. 5 - Approximation of botnet distribution in July 2022.
The data used to populate this map is sampled, which means that the actual geographic distribution of PrivateLoader may be closer to this one but not exactly what this map suggests.

Indicators of Compromise

0d7692792b4907f9470d3b1bb6ce8310 - NSIS installer
e8fe5a28d052a908573b49ab0a904ca4 - PrivateLoader loader module
5df119a002dcaf9b7ba82acfe35e4cb1 - PrivateLoader core module
45abb1bedf83daf1f2ebbac86e2fa151 - PrivateLoader service module

We are currently uploading our **live** PrivateLoader IoCs and dropped malware to abuse.ch:
- PrivateLoader samples by YARA hunting:
https://yaraify.abuse.ch/yarahub/rule/privateloader/
- PrivateLoader C2 servers: https://threatfox.abuse.ch/browse/malware/win.privateloader/
- Drop URLs obtained from the C2 server:
https://urlhaus.abuse.ch/browse/tag/PrivateLoader/
- Malware samples from drop URLs: https://bazaar.abuse.ch/user/86185858/

Threat Hunting Signatures

Yara rule

The following rule was tested with VirusTotal Retrohunt, which returned 1K+ samples within a one-year time period:

https://github.com/bitsight-research/threat_research/blob/main/privateloader/privateloader.yara

Suricata rule

The following rule was tested with a PCAP generated from a sandbox run of the loader module:

https://github.com/bitsight-research/threat_research/blob/main/privateloader/privateloader.rules

Get the Weekly Cybersecurity Newsletter

Subscribe to get security news and industry ratings updates in your inbox.

-
- *
  Read more
  By checking this box, I consent to sharing this information with BitSight Technologies, Inc. to receive email and phone communications for sales and marketing purposes as described in our privacy policy. I understand I may unsubscribe at any time.