PRODAFT

Threat Intelligence Insights

PrivateLoader

Pay-per-install (PPI) service used to spread the most popular malware around the world.

PrivateLoader is a downloader malware family first identified in early 2021. Its primary purpose is to distribute and deliver different malware on behalf of other threat actors in exchange for payment.

Many threat actors use the pay-per-install (PPI) malware distribution service to distribute ransomware, information stealers, banking trojans, downloaders, and other commodity malware, based on different victim attributes.

PrivateLoader will most likely be updated with new features to enhance its capabilities. The PTI team has been monitoring PrivateLoader for a while and has gathered valuable information.

Attack Highlights

Threat Type:
Botnet

Targets:
Egypt, Vietnam, Brazil

Primary motiavtion:
Pay-per-install gain

Active URLs:
28

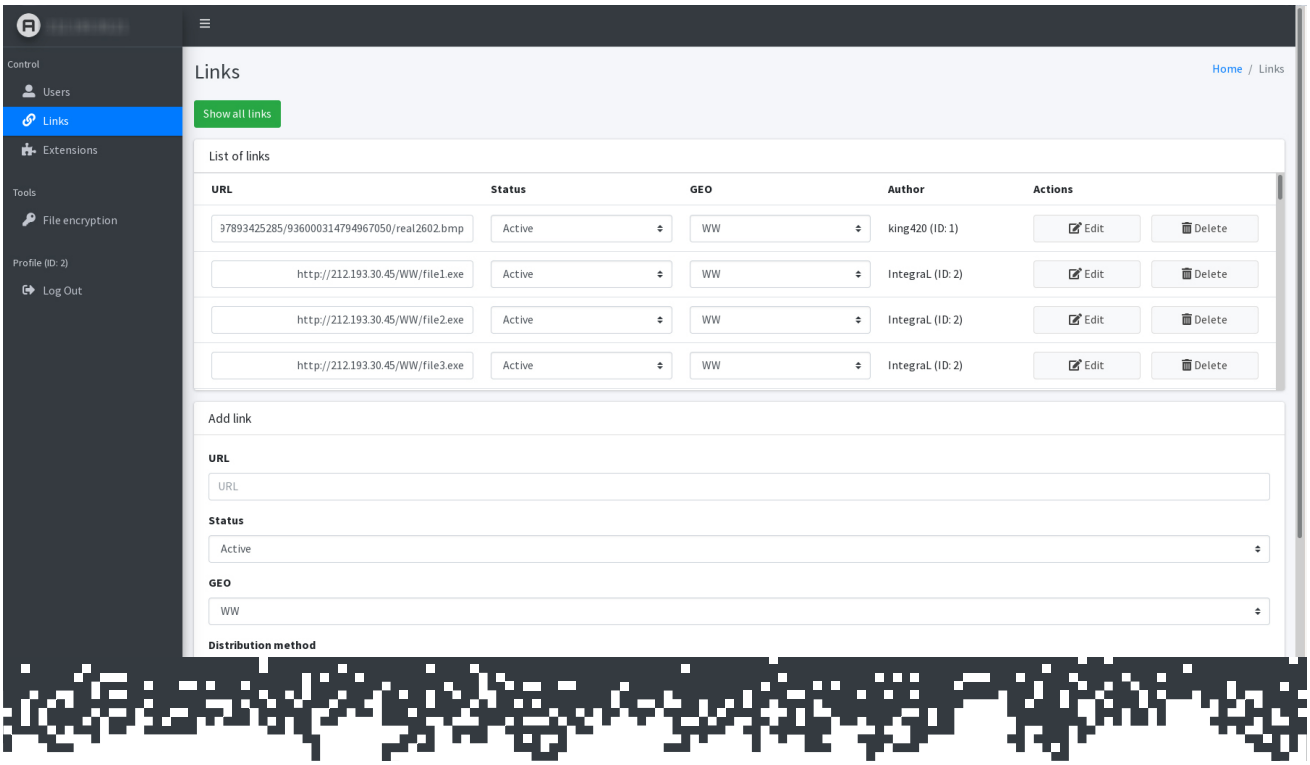
The Strategy

PrivateLoader is mostly delivered through SEO-optimized websites that claim to provide cracked versions of well-known software or privacy tools.

Once the victim has downloaded the tool on the website, the final payload is served to the victim as a password-protected zip file. The zip file embeds and executes numerous malicious payloads.

These payloads are delivered based on a variety of victim attributes, including but not limited to location, corporate network, cryptocurrency, and financial activity or installed software.

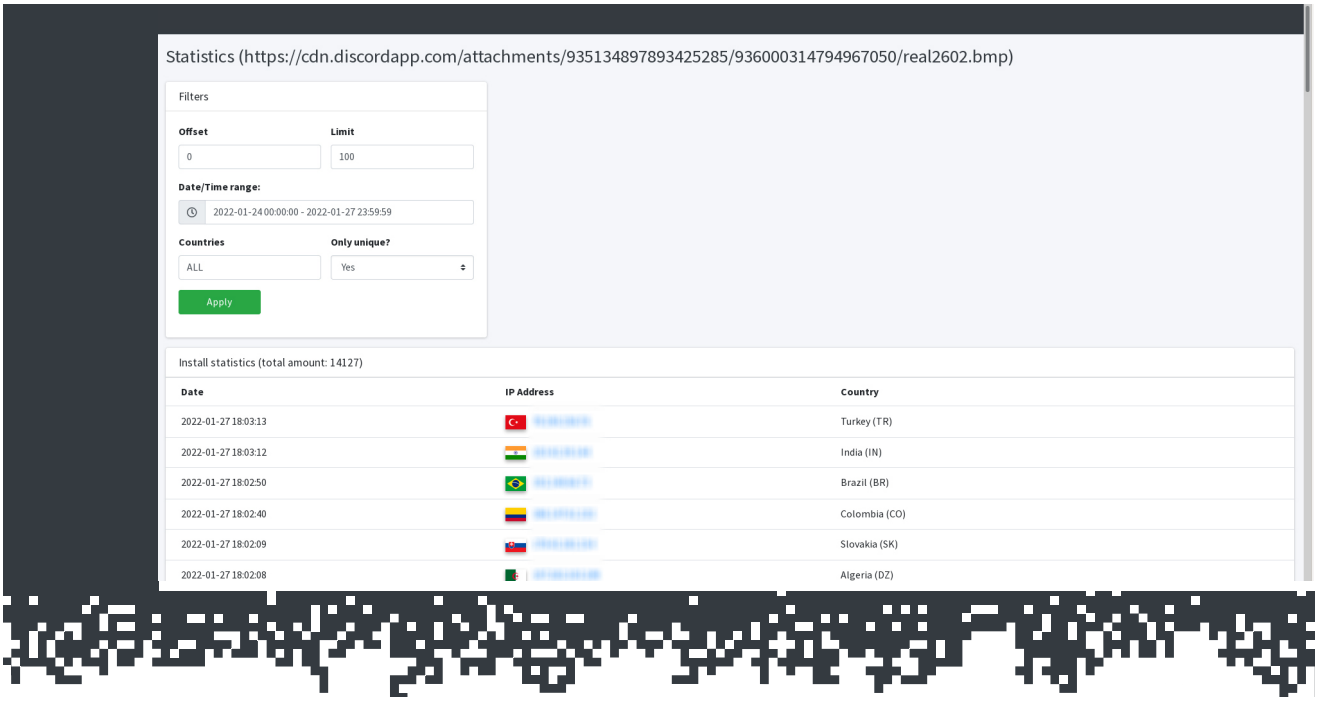
Below you can see a non-exhaustive list of active URLs to distribute the malware with a geo-fencing filter (WW=Worldwide).



A non-exhaustive list of active URLs to distribute the malware

The PrivateLoader pay-per-install distribution service is used to distribute some of the most popular malware families, such as SmokeLoader, RedLine Stealer, Vidar, Raccoon Stealer, GCleaner, LockBit, and many others.

Below you can see the victim information for a particular URL and the corresponding filtering options based on countries and installation date range.



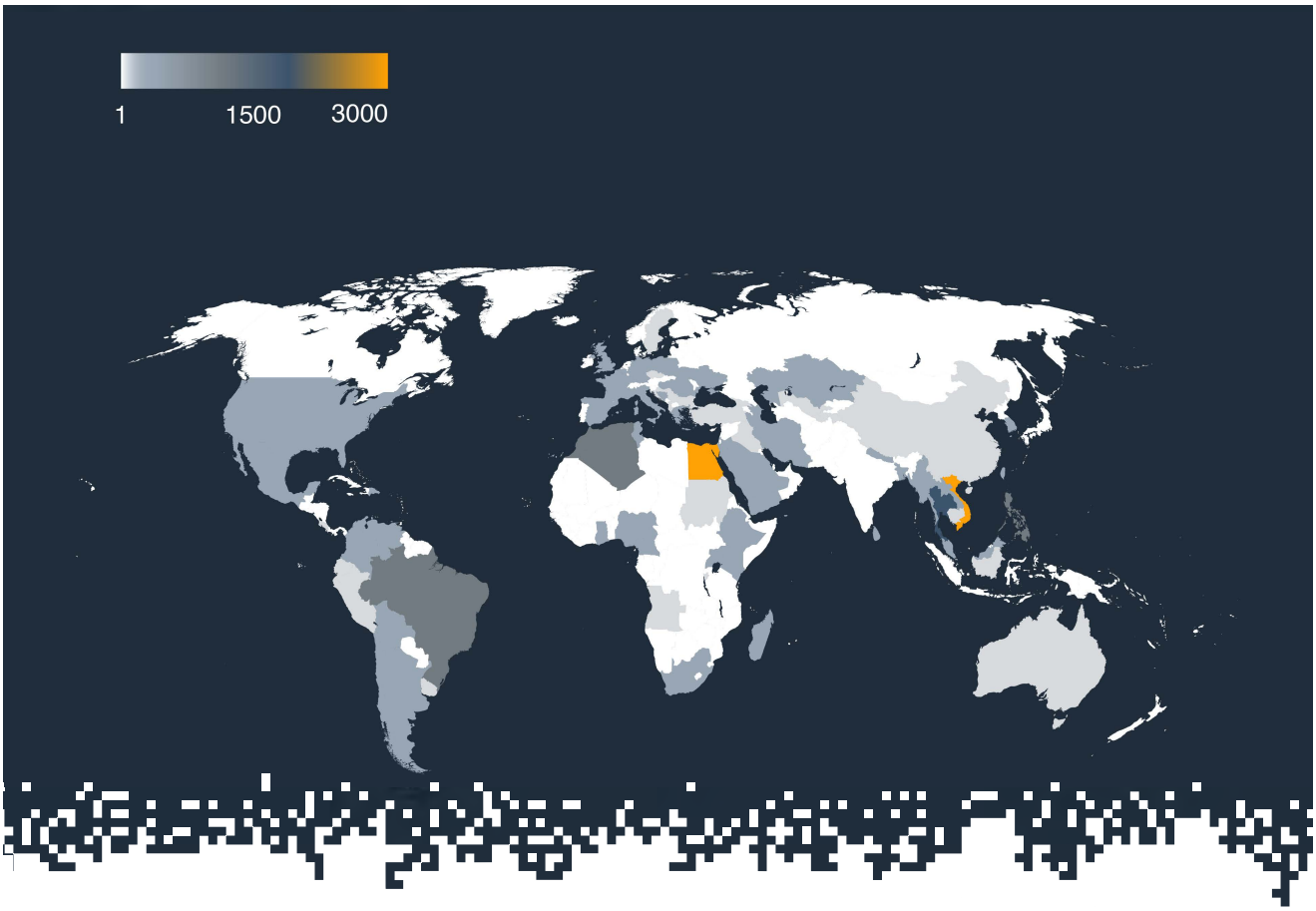
Victims' information for a specific URL

The Attacker

The exact attribution of the campaigns is unclear for now. However, one of the most common URLs that the threat actors use is vk.com which is known to be the most-used social media platform in Russia. Attackers use a publicly known open redirect vulnerability to forward the targets to the server where the malware is served.

The Findings

According to our findings, there are currently more than 25'000 victims worldwide. The visibility of our PTI team on PrivateLoader shows that the downloader malware is spread worldwide, with the most significant number of victims in Egypt, Vietnam, and Brazil. You can see the actual distribution of PrivateLoader victims below.



Spreading of PrivateLoader

Our visibility into their Command and Control C2 panel shows that there are 28 active URLs for distributing the malware and 138 inactive/suspended URLs.

Conclusion

The pay-per-install services provide an easy way for the threat actors to deploy and launch their malware at scale. PrivateLoader has been used to distribute ransomware, information stealers, banking trojans, downloaders, and other commodity malware.

Enterprise executives and their risk advisors need in-depth threat intelligence to mitigate these threats while minimizing the damage they cause. The work of our TI team is crucial to understanding the cybercrime landscape.

Our threat intelligence platform relies on dozens of intelligence collection tools that monitor thousands of different sources and detect security issues earlier and faster to meet the challenges of today's complex cyberattacks.

Proactive threat intelligence is key to identifying the factors contributing the cybercrime trends and preventing the threat actors from exploiting enterprise vulnerabilities.