PrivateLoader: The first step in many malware schemes

intel471.com/blog/privateloader-malware

Pay-per-install (PPI) malware services have been an integral part of the cybercrime ecosystem for a considerable amount of time. A malware operator provides payment, malicious payloads and targeting information, and those responsible for running the service outsource the distribution and delivery. The accessibility and moderate costs allow malware operators to leverage these services as another weapon for rapid, bulk and geo-targeted malware infections.

By understanding how these services proliferate, defenders can better recognize these campaigns and stop them from wreaking havoc on their organization's IT stack. This report focuses on the PrivateLoader modular downloader programmed in the C++ programming language connected to an unidentified PPI service. PrivateLoader sits at the front of this operation and communicates with its back-end infrastructure to retrieve URLs for the malicious payloads to "install" on the infected host. As is the case with downloaders tied to PPI services, PrivateLoader communicates a variety of statistics such as which payloads were downloaded and launched successfully.

Distribution campaigns generally rely on a network of search engine optimization (SEO) enhanced websites that lure unsuspecting victims searching for warez aka pirated software to download and execute malware. A password-protected archive typically is delivered that contains a setup file that embeds and executes multiple malicious payloads on the infected host such as GCleaner, PrivateLoader, Raccoon, Redline, Smokeloader and Vidar malware. We assess these campaigns started to incorporate PrivateLoader since at least May 2021.

This report investigates the PPI service behind it and methods operators employ to obtain "installs" and presents details about the malware families the service delivers.

How PrivateLoader works

The service behind this PrivateLoader PPI campaign and its operators are unknown, as it was not possible to connect the downloader to a specific underground PPI service at the time of this report. However, we observed PrivateLoader's main command and control (C2) servers also host the administration panel, which is based on the AdminLTE 3 dashboard template. The image below shows the authentication page:

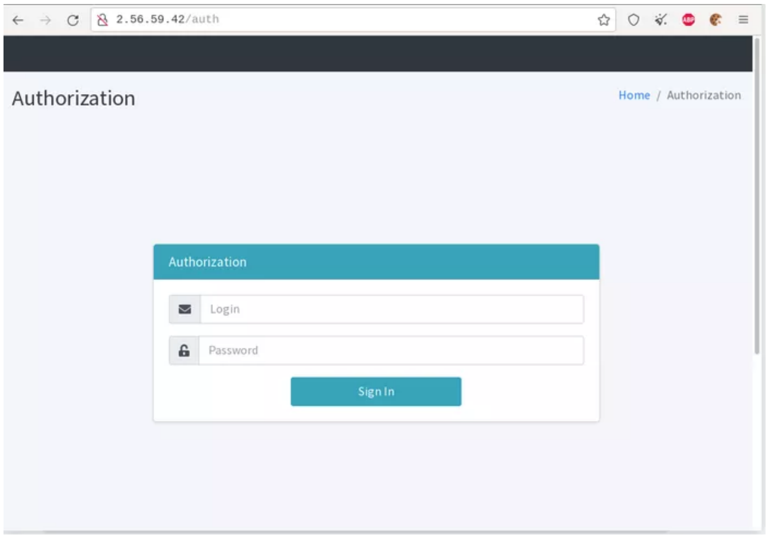


Image 1: This image depicts the PrivateLoader authentication page.

The front-end script, which uses the Javascript library app.js, appears to expose functionalities offered to panel users. The table below describes interesting JavaScript functions in the script:

FUNCTION	DESCRIPTION	ENDPOINT AND PARAMETERS

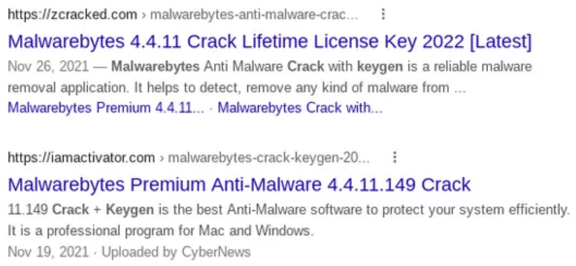
FUNCTION	**DESCRIPTION**	**ENDPOINT AND PARAMETERS**
AddNewUser	Adds a new user with a specific role.	/base/user_reg.php • login: User login. • password: User password. • role: User role as an integer.
saveUser	Modifies an existing user.	**/base/user_reg.php** • **user_id**: User identifier. • **login**: New user login. • **password**: New user password. • **role**: New user role as an integer. • **banned**: Banned status as an integer.
AddNewLink	Adds a loader link configuration to a payload to install.	**/base/link_add.php** • **link_url:** Download link to the payload to install. • **link_status**: Link status as an integer. • **link_geo:** Targeted geolocation as an integer. • **link_dmethod**: Link distribution method as an integer.
EditStatusLink	Updates the status of a loader link configuration.	**/base/link_edit.php** • **link_id**: Loader link identifier. • **link_status**: New status as an integer.
editUrlLink	Edits the URL for a loader link configuration.	**/base/link_url_edit.php** • **link_id**: Loader link identifier. • **link_url**: Updated download link.
removeLink	Removes a loader link configuration.	**/base/link_del.php** **link_id**: Loader link identifier.
EditGeoLink EditGeoLinkIdx	Updates the geolocation targeting for a loader link configuration.	**/base/link_edit_geo.php** • **link_id**: Loader link identifier. • **link_geo**: New targeted geolocation as an integer.
saveLinkInformation	Modifies an existing loader link configuration.	**/base/link_edit_info.php** • **link_id**: Loader link identifier. • **link_url**: Download link of the payload. • **link_status**: Status as an integer. • **link_geo**: Targeted geolocation as an integer. • **link_ftype**: Selected category identifier of the payload as an integer. • **link_countries**: Targeted countries as a string. • **link_arguments**: Arguments to pass to the payload as a string. • **link_onlybytype**: Integer that indicates to run the payload only if the category identifier matches. • **link_subgeo**: Subgeolocation as a string. • **link_dmethod**: Link distribution method as an integer.

FUNCTION	DESCRIPTION	ENDPOINT AND PARAMETERS
AddNewExtension	Adds a configuration to a browser extension to install.	**/base/extension_add.php** • **extension_url:** Download link to the browser extension to install. • **config_url**: Download link to the configuration of the browser extension. • **ext_status**: Extension status as an integer. • **ext_geo**: Targeted geolocation as an integer.
editUrlExtension	Edits the URL for a browser extension configuration.	**/base/extension_url_edit.php** • **extension_id**: Extension identifier. • **ext_url**: New link to the extension. • **cfg_url**: New link to the extension configuration.
removeExtension	Removes a browser extension configuration.	**/base/extension_del.php** **ext_id**: Extension identifier.
saveExtensionInformation	Modifies an existing browser extension configuration.	**/base/extension_edit_info.php** • **ext_id**: Extension identifier. • **ext_url**: Download link of the extension. • **cfg_url**: Download link of the extension configuration. • **ext_status**: Extension status as an integer. • **ext_geo**: Targeted geolocation as an integer. • **ext_countries**: Targeted countries as a string.
LoadFileToEncrypt	Encrypts a file. Possibly uses the byte substitution and XOR algorithm described in the Malware Report	**/base/file_crypt.php** Multipart form POST request with the file to encrypt.
CalculateAllLinksLoads	Returns the number of total and unique installed payloads for all link identifiers.	**/base/logger_counter.php** **ids**: All link identifiers.
CalculateCurrentLinksLoads	Returns the number of total and unique installed payloads for a link identifier.	**/base/logger_counter.php** **ids:** Single link identifier.

Delivering the PrivateLoader downloader

PrivateLoader is delivered through a network of websites that claim to provide “cracked” software, which is modified versions of popular legitimate applications that people commonly use. These websites are SEO optimized and usually appear at the top of search queries that contain keywords such as “crack” or “crack download,” preceded by the software name.

For example, a search for “Malwarebytes crack” returns the following websites as the fourth and fifth results:



https://zcracked.com › malwarebytes-anti-malware-crac...

Malwarebytes 4.4.11 Crack Lifetime License Key 2022 [Latest]

Nov 26, 2021 — **Malwarebytes** Anti Malware **Crack** with **keygen** is a reliable malware removal application. It helps to detect, remove any kind of malware from ...

Malwarebytes Premium 4.4.11... · Malwarebytes Crack with...

https://iamactivator.com › malwarebytes-crack-keygen-20...

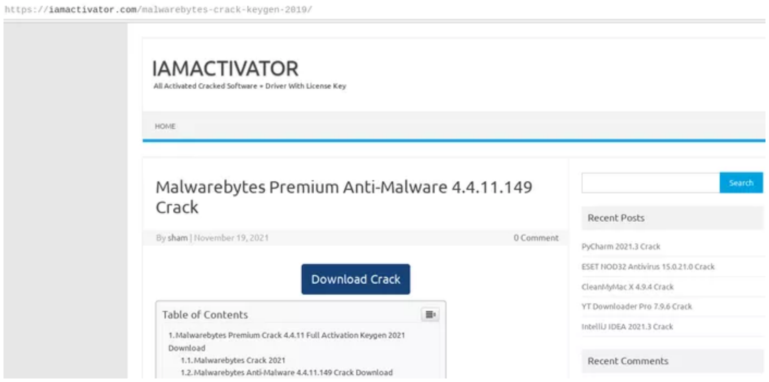
Malwarebytes Premium Anti-Malware 4.4.11.149 Crack

11.149 **Crack** + **Keygen** is the best Anti-Malware software to protect your system efficiently. It is a professional program for Mac and Windows.

Nov 19, 2021 · Uploaded by CyberNews

This image depicts "Malwarebytes crack" search results.

Visitors are lured into clicking a "Download Crack" or "Download Now" button to obtain an allegedly cracked version of the software. The JavaScript for the download button is retrieved from a remote server.



https://iamactivator.com/malwarebytes-crack-keygen-2019/

IAMACTIVATOR

All Activated Cracked Software + Driver With License Key

HOME

Malwarebytes Premium Anti-Malware 4.4.11.149 Crack

By sham | November 19, 2021 0 Comment

Download Crack

Table of Contents

1. Malwarebytes Premium Crack 4.4.11 Full Activation Keygen 2021 Download
   1.1. Malwarebytes Crack 2021
   1.2. Malwarebytes Anti-Malware 4.4.11.149 Crack Download

Search

Recent Posts

PyCharm 2021.3 Crack

ESET NOD32 Antivirus 15.0.21.0 Crack

CleanMyMac X 4.9.4 Crack

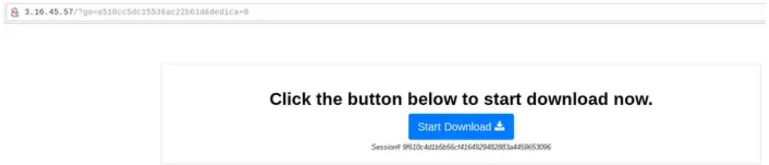
YT Downloader Pro 7.9.6 Crack

IntelliJ IDEA 2021.3 Crack

Recent Comments

This image depicts an option to allegedly download a cracked version of the software.

After a few redirections, the final payload is served to the user as a password-protected compressed (.zip) archive. The screenshot below shows the actual download page:



3.16.45.57/?go=a518cc5dc15536ac22b61d&dedica=0

Click the button below to start download now.

Start Download

Session# 9f610c4d1b5b56cf4164929482883a4459653096

This image depicts the download page.

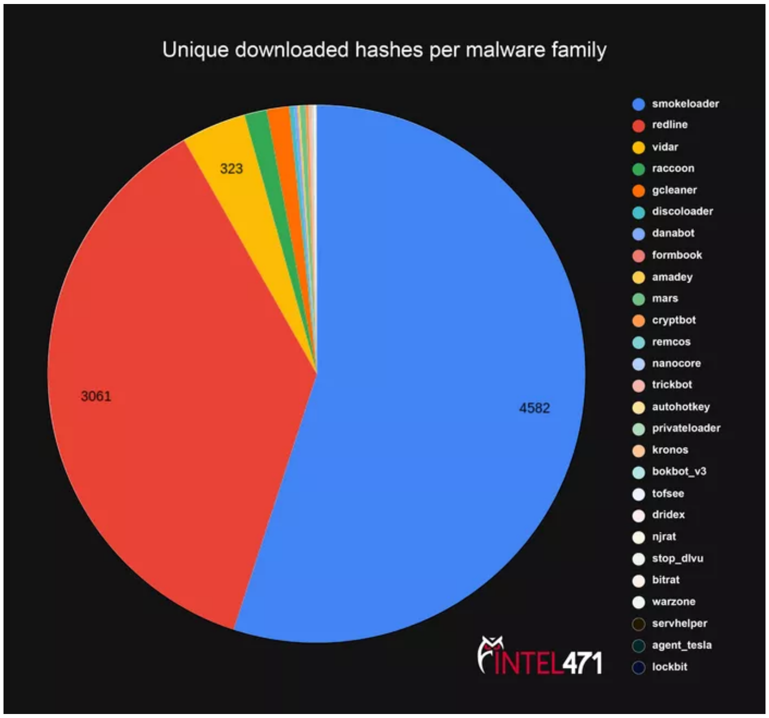
In our example, the archive served was named "PASSWORD_IS_324325_____Malwarebytes-Pr.zip." It contained a Nullsoft Scriptable Install System (NSIS) installer named "setup_x86_x64_install.exe," which embeds and executes numerous malicious payloads such as GCleaner, PrivateLoader and Redline.

Researchers from SophosLabs previously investigated this delivery network and tied some of its infrastructure to the InstallUSD PPI service.

Malware families dropped

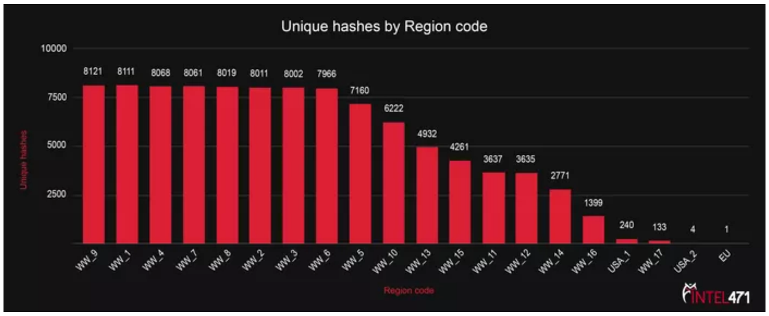
Automated malware coverage and tracking for PrivateLoader started in early September 2021. We have since gathered sizable amounts of data that helped us learn more about the service.

The following chart shows the number of unique hashes downloaded by PrivateLoader for each malware family our Malware Intelligence systems detected. The most popular families this PPI service distributed in descending order were Smokeloader, Redline and Vidar:



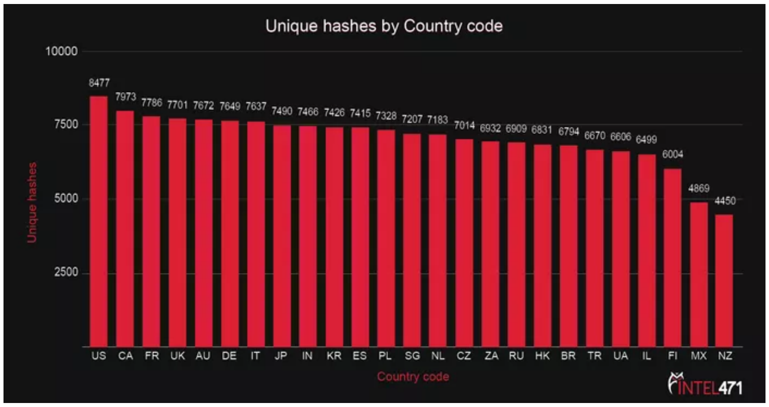
This chart shows the number of unique hashes downloaded by PrivateLoader for each malware family our Malware Intelligence systems detected.

Each PrivateLoader sample embeds a region code that is communicated to the C2 server and country of the bot. The chart below depicts the number of unique hashes downloaded per region code in the duration of coverage. We believe the "WW" prefix in these region codes stands for "worldwide," since it was most commonly found in samples. On the panel side, we suspect this code represents the "link_geo" parameter described in the previous table.



This chart depicts the number of unique hashes downloaded per region code.

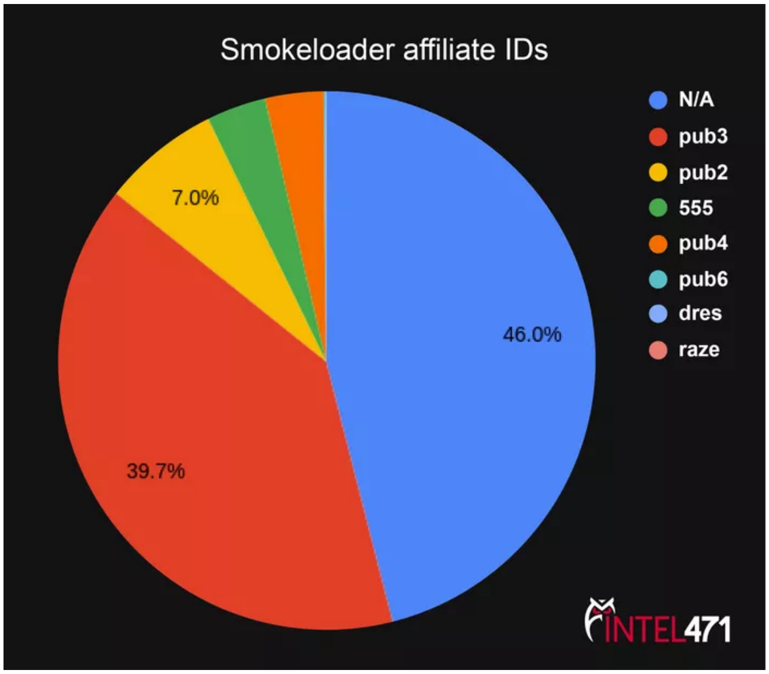
However, we observe a different distribution when querying the number of unique hashes by bots' country codes (see: chart below). This is expected since popular worldwide region codes encapsulate multiple countries.



This chart depicts the number of unique hashes downloaded per country code.

Smokeloader

Of the payloads we saw pushed by PrivateLoader, the most common was Smokeloader. The following chart shows the extracted affiliate IDs (or lack thereof) from all unique Smokeloader samples detected by our Malware Intelligence systems:



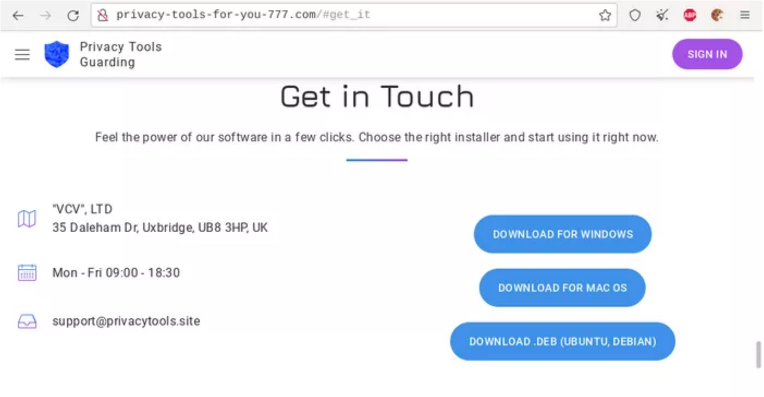
This chart shows the percentage of extracted affiliate IDs from all unique Smokeloader samples detected by our Malware Intelligence systems.

The top 10 detected domains used to deliver Smokeloader included:

HOST NAME	UNIQUE SAMPLES DOWNLOADED
privacytoolz123foryou[.]top	321
threesmallhills[.]com	296
privacy-toolz-for-you-5000[.]top	264
privacytoolzforyou-7000[.]top	231
privacytoolzforyou-7000[.]com	212
privacytoolzforyou7000[.]top	200
privacytoolzforyou-6000[.]top	179

HOST NAME	UNIQUE SAMPLES DOWNLOADED
privacy-toolz-for-you-403[.]top	177
privacy-tools-for-you-777[.]com	150
privacytoolzforyou6000[.]top	136

It’s apparent the operators running the “Privacy tools” domains heavily rely on PrivateLoader to deliver Smokeloader. An inspection of active distribution URLs showed these domains host a website that claims to offer “Privacy Tools.” This website likely is spoofing the real PrivacyTools[.]io website run by volunteers who advocate for data privacy.


privacy-tools-for-you-777.com/#get_it
Privacy Tools
Guarding
SIGN IN
DOWNLOAD FOR WINDOWS
DOWNLOAD FOR MAC OS
DOWNLOAD .DEB (UBUNTU, DEBIAN)

Get in Touch

Feel the power of our software in a few clicks. Choose the right installer and start using it right now.

"VCV", LTD
35 Daleham Dr, Uxbridge, UB8 3HP, UK

Mon - Fri 09:00 - 18:30

support@privacytools.site

This image depicts the landing page of one of the “Privacy tools” domains.

These websites host Smokeloader payloads as part of three categories named “pab1”, “pab2” and “pab3”. These are not necessarily linked to the analogous “pub*” affiliate IDs, since we have seen some “pab2” payloads with the “555” affiliate ID. While tracking PrivateLoader, we only received links to download the “pab2” payloads from these websites. It is likely these operators use other methods or PPI services to distribute the Smokeloader family.

On Oct. 22, 2021, a “pab2” Smokeloader sample downloaded by PrivateLoader from one of these websites delivered the Qbot banking trojan. This is an unusual distribution method for Qbot and revealed the new botnet ID star01.

Banking trojans

There are other actors throughout the underground that leverage PrivateLoader for banking trojan distribution.

On Oct. 31, 2021, PrivateLoader bots connecting from European countries were instructed to download and execute the Kronos banking trojan from the following URL:

```
hxxp://2.56.59[.]42/EU/Yandex1500[.]exe
```

The downloaded sample also executed the Vidar information stealer. The download and execute commands for this sample stopped the following day.

On Nov. 1, 2021, PrivateLoader bots downloaded Dridex samples tied to the 10444 botnet, and Danabot with the affiliate identifier 40. The same day, bots also downloaded Trickbot samples with the group tags (gtags) lip*, tot* and top*. In all cases, the delivered samples embedded other malware families such as other banking trojans, information stealers or ransomware.

SAMPLE HASH	MALWARE FAMILIES	FIRST SEEN (UTC)	LAST SEEN (UTC)	OTHER DETECTED FAMILIES
14e7cc2eadc7c9bac1930f37e25303212c8974674b21ed052a483727836a5e43	Trickbot: top142	Nanocore RAT Smokeloader Redline		

SAMPLE HASH	MALWARE FAMILIES	FIRST SEEN (UTC)	LAST SEEN (UTC)	OTHER DETECTED FAMILIES
4554dc95f99d6682595812b677fb131a7e7c51a71daf461a57a57a0d903bb3fa	Trickbot: tot160 Trickbot: top141 Dridex: 10444	Tofsee Redline		
4ed7609cbb86ea0b7607b8a002e7f85b316903c3b6801240c9576aae8b3052ff	Trickbot: lip143 Trickbot: top142	njRAT STOP Djvu Redline Vidar		
5adbe8d0375d6531f1a523085f4df4151ad1bd7ae539692e2caa3d0d73301293	Trickbot: lip142 Dridex: 10444	Remcos Tofsee		
6abbd89e6ab5e1b63c38a8f78271a97d19bafff4959ea9d5bd5da3b185eb61e6	Trickbot: top141	Redline		
929a591331bdc1972357059d451a651d575166f676ea51daaeb358aa2a1064b7	Dridex: 10444	Smokeloader Redline		
aae0553b761e8bb3e58902a46cd98ee68310252734d1f8d9fd3b862aab8ed5c9	Trickbot: lip142	Redline		
bf7b5f72b2055cfc8da01bb48cf5ae8e45e523860e0b23a65b9f14dbdbb7f4ee	Trickbot: lip141 Trickbot: top141 Trickbot: top142 Dridex: 10444 Danabot: affid 40	Redline QuasarRAT		
eef15f6416f756693cbfbfd8650ccb665771b54b4cc31cb09aeea0d13ec640cf	Trickbot: lip141 Trickbot: lip142 Trickbot: lip143 Trickbot: top141	Smokeloader Lockbit Redline		

SAMPLE HASH	MALWARE FAMILIES	FIRST SEEN (UTC)	LAST SEEN (UTC)	OTHER DETECTED FAMILIES
f9246be51464e71ff6b37975cd44359e8576f2bf03cb4028e536d7cfde3508fc	Trickbot: lip141 Trickbot: lip142	Redline		
fcc49c9be5591f241ffd98db0752cb9e20a97e881969537fba5c513adbd72814	Trickbot: lip142 Dridex: 10444	Redline		

The sample with the hash 929a591331bdc1972357059d451a651d575166f676ea51daaeb358aa2a1064b7 that embedded both Dridex and Smokeloader was downloaded from the following URL:

```
hxxp://privacytoolzfor-you6000[.]top/downloads/toolspab2.exe
```

In the previous subsection, we linked the “Privacy tools” websites to Smokeloader operators. It is unclear whether the operators behind these websites operated the Dridex 10444 botnet or only acted as a link in the delivery chain. However, we can assume the “Privacy tools” website was used for distribution since the same Dridex botnet identifier and controllers were seen across different hashes and delivery URLs during this period.

Seeing downloads for Danabot, Dridex, Kronos and Trickbot for the first time within the same time frame hardly can be regarded as a coincidence. Moreover, these trojans often were bundled with each other. Therefore, we assess a single entity likely operating these specific botnets was using the PrivateLoader PPI service at the time.

On Nov. 14, 2021, PrivateLoader bots started to download samples of the Danabot banking trojan with the affiliate ID 4 for a single day.

Based on these short outbursts that lasted no more than a day, we suspect the banking trojan operators were experimenting with this PPI service as another delivery mechanism for their malware.

Ransomware

Underground PPI services generally advise against deploying ransomware on target machines since it renders them unusable. However, cybercriminals have a reputation of not adhering to rules and deploy ransomware anyway.

The only time in which we detected ransomware samples downloaded by PrivateLoader was when it dropped banking trojans in early November 2021. The table in the previous subsection showed downloads for the LockBit and STOP Djvu ransomware families.

While analyzing payloads downloaded by PrivateLoader, we identified a new loader we dubbed Discoloader. Discoloader was written using the .NET framework and uses the Discord content delivery network (CDN) to host its payload. Although not directly from PrivateLoader, we observed samples of this family delivering Conti ransomware directly into infected hosts, which is an uncharacteristic delivery mechanism since this family typically only is deployed after total compromise of enterprise networks.

Conclusion

PPI services have been a pillar of cybercrime for decades. Just like the wider population, criminals are going to flock to software that provides them a wide array of options to easily achieve their goals. As we have detailed, criminals have used PrivateLoader to launch all kinds of schemes. By highlighting the versatility of this malware, we hope to give defenders the chance to develop unique strategies in thwarting malware attacks empowered by PrivateLoader.

MITRE ATT&CK techniques

This report uses the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework.

TECHNIQUE TITLE	ID	USE
Resource Development [TA0042]		

TECHNIQUE TITLE	ID	USE
Stage Capabilities: Upload Malware	T1608.001	PrivateLoader often hosts malicious payloads on the Discord CDN. We observed recent controllers downloading attachments from just the 891006172130345095, 905701898806493199 and 896617596772839426 IDs.
Persistence [TA0003]		
Create or Modify System Process: Windows Service	T1543.003	PrivateLoader can be persisted as a startup service and is installed with the following attributes: • Service name: PowerControl. • Service display name: "Power monitoring service for your device." • Service start type: At system startup. • Service binary path: C:\Program Files. (x86)\PowerControl\PowerControl_Svc.exe.
Scheduled Task/Job: Scheduled Task	T1053.005	The PrivateLoader service module always persists as a scheduled task that executes every hour. It also can be persisted as a logon scheduled task when a Windows service is not used.
Browser Extensions	T1176	PrivateLoader can download and silently install malicious browser extensions on Google Chrome and Microsoft Edge browsers.
Privilege Escalation [TA0004]		
Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002	The PrivateLoader core module uses a Windows 10 user account control (UAC) bypass technique to elevate privileges. The bypass uses a widely documented technique involving the ComputerDefaults.exe system executable (.exe) file, which has the auto-elevate option set.