INTEL471

PrivateLoader

The malware behind a havoc-wreaking Pay-per-install service

Souhail Hammou
Malware Reverse Engineer

Agenda

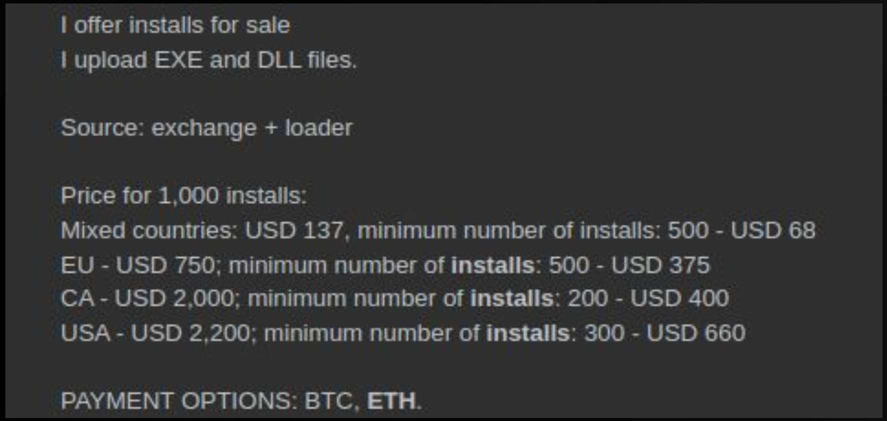
- Introduction to Pay-per-install (PPI) services
- Discovering PrivateLoader
- In-depth look at PrivateLoader
- Tracking PrivateLoader
- Conclusion

Introduction to underground PPI services

- PPI services monetize wide distribution of malware and PUAs.
- Providers offer geo-targeted installs (aka loads) in exchange for money.
- A malware operator purchases a number of installs and the service works to guarantee the same number of infected bots.
- Used mainly by low to mid-tier actors to distribute downloaders and information stealers.

Introduction to underground PPI services

- There exist public and private PPI services. Underground forums host ads for such services and provide escrow.

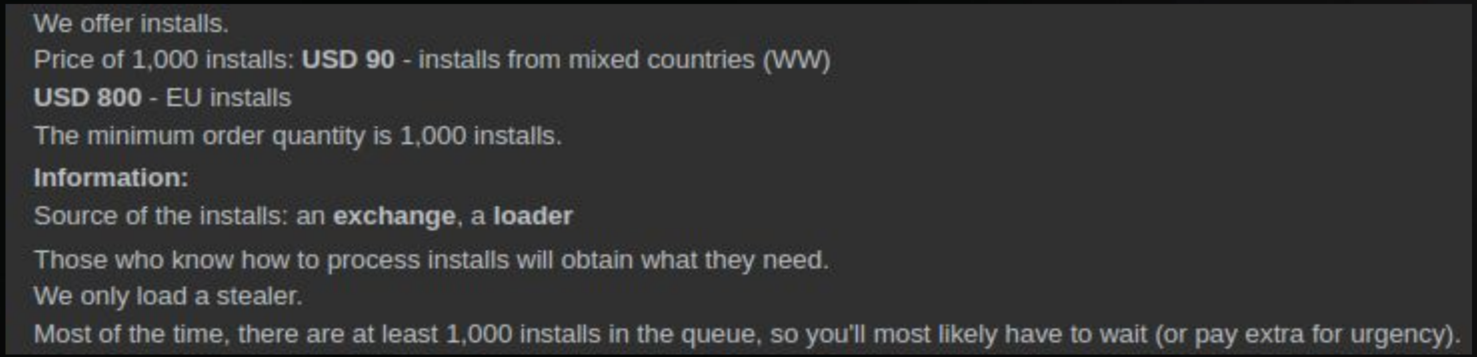


I offer installs for sale
I upload EXE and DLL files.

Source: exchange + loader

Price for 1,000 installs:
Mixed countries: USD 137, minimum number of installs: 500 - USD 68
EU - USD 750; minimum number of **installs**: 500 - USD 375
CA - USD 2,000; minimum number of **installs**: 200 - USD 400
USA - USD 2,200; minimum number of **installs**: 300 - USD 660

PAYMENT OPTIONS: BTC, **ETH**.



We offer installs.
Price of 1,000 installs: **USD 90** - installs from mixed countries (WW)
USD 800 - EU installs
The minimum order quantity is 1,000 installs.
Information:
Source of the installs: an **exchange**, a **loader**
Those who know how to process installs will obtain what they need.
We only load a stealer.
Most of the time, there are at least 1,000 installs in the queue, so you'll most likely have to wait (or pay extra for urgency).

Custom loaders of PPI services

- Most PPI services use custom loaders for payload delivery.
- Methods of distribution deliver the custom loader to victims.
- The loader connects to a C2 server to retrieve the payloads to install.
- The loader communicates information back to confirm the installs as proof.
- An infected bot can be re-used multiple times. This creates a clutter of malware on victim machines (tens to hundreds of malicious payloads).

A typical PPI transaction

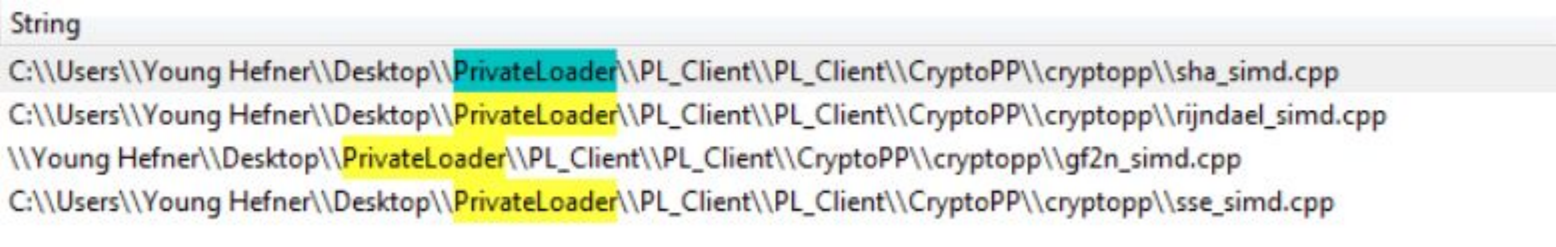
- Malware operators provide:
  - Payment in cryptocurrency.
  - Malicious payloads to distribute.
  - Number of installs.
  - Geo-targeting preferences e.g. EU, Mixed geo etc.
- PPI Service operators provide:
  - Payload distribution: Bot masters, affiliates, PPI etc.
  - Payload delivery to infected hosts.

Methods of distribution

- Bot masters:
  - Monetize their large botnets by using infected bots for PPI installs.
  - Bot masters offer PPI services for direct payload delivery in underground forums.
- Affiliate programs:
  - PPI services can outsource malware delivery to affiliates.
  - Affiliates get paid to distribute a custom PPI loader.
  - The sky's the limit with delivery methods: phishing, bundleware etc.
- Other PPI services:
  - A PPI service can deliver its custom loader using better PPI services.
  - Example: GCleaner using PrivateLoader for delivery.

PrivateLoader

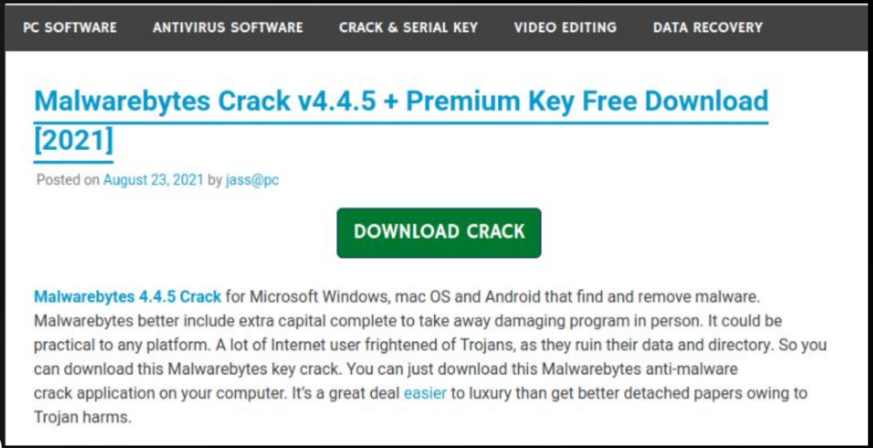
- Intel 471 became aware of PrivateLoader in late July 2021. We believe it has been active since at least May 2021.
- Private PPI service: service and operators are unknown.
- The variety and large amount of payloads it was dropping in a single run caught our attention.
- Programmed in C++, uses HTTP for C2 communication and is actively maintained. In early August 2021 it underwent changes to become modular.



```
String
C:\\Users\\Young Hefner\\Desktop\\PrivateLoader\\PL_Client\\PL_Client\\CryptoPP\\cryptopp\\sha_simd.cpp
C:\\Users\\Young Hefner\\Desktop\\PrivateLoader\\PL_Client\\PL_Client\\CryptoPP\\cryptopp\\rijndael_simd.cpp
\\Young Hefner\\Desktop\\PrivateLoader\\PL_Client\\PL_Client\\CryptoPP\\cryptopp\\gf2n_simd.cpp
C:\\Users\\Young Hefner\\Desktop\\PrivateLoader\\PL_Client\\PL_Client\\CryptoPP\\cryptopp\\sse_simd.cpp
```

Distribution method

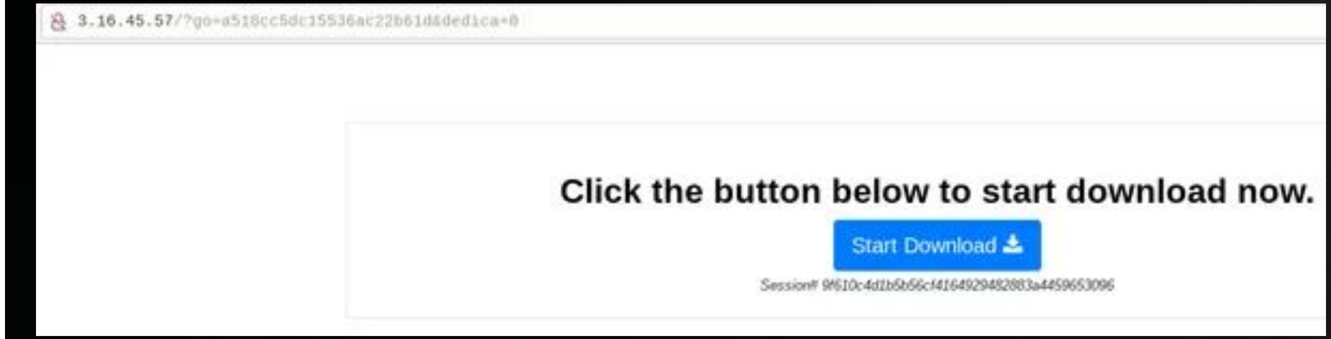
- Network of malicious websites of fake cracked software.
- SEO optimized.
- “Download Crack” button is retrieved from a remote server.
- User is redirected to download password-protected archive.
- Researchers from SophosLabs tied some of the infrastructure to an affiliate PPI service called **InstallUSD**. Affiliates host download links on websites and get paid for installs.
- Main distribution method.



Malwarebytes Crack v4.4.5 + Premium Key Free Download [2021]

Posted on August 23, 2021 by jass@pc

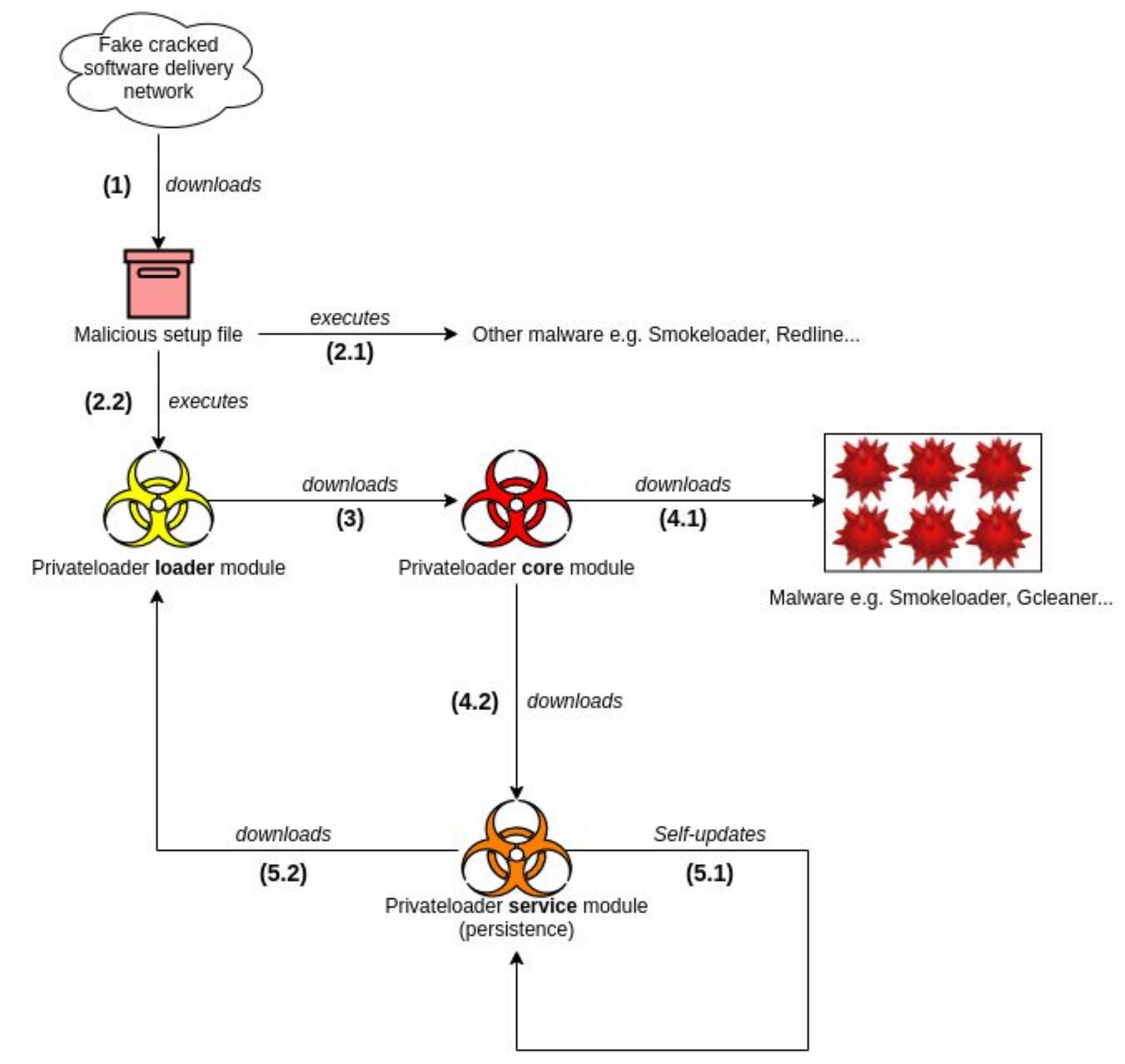
Malwarebytes 4.4.5 Crack for Microsoft Windows, mac OS and Android that find and remove malware. Malwarebytes better include extra capital complete to take away damaging program in person. It could be practical to any platform. A lot of Internet user frightened of Trojans, as they ruin their data and directory. So you can download this Malwarebytes key crack. You can just download this Malwarebytes anti-malware crack application on your computer. It's a great deal easier to luxury than get better detached papers owing to Trojan harms.



Click the button below to start download now.

Session# 9f610c4d1b5b56cf4164929482883a4459653096

Life cycle of a PrivateLoader infection

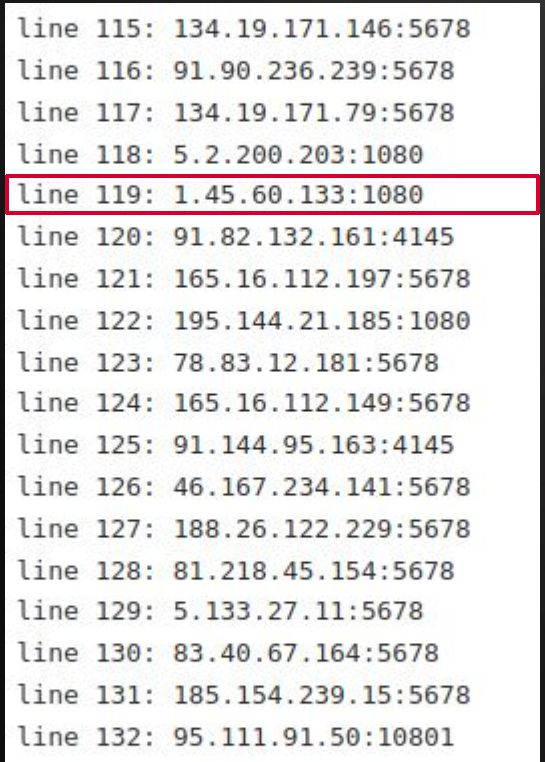

Fake cracked software delivery network
(1)
downloads
Malicious setup file
executes
(2.1)
Other malware e.g. Smokeloader, Redline...
(2.2)
executes
Privateloader **loader** module
downloads
(3)
Privateloader **core** module
downloads
(4.1)
Malware e.g. Smokeloader, Gcleaner...
(4.2)
downloads
downloads
(5.2)
Privateloader **service** module
(persistence)
Self-updates
(5.1)

Loader module

- The first stage payload in a PrivateLoader infection.
- Contains multiple loader C2s used to retrieve the main C2 configuration.
- The loader module includes multiple URLs that are requested (GET request):
    - /proxies.txt
    - /server.txt
    - /api/setStats.php
- The resulting responses can contain an encoded, encrypted or plaintext main C2 configuration.
    - HOST:45.133.1.60

Loader module: Example of /proxies.txt

- Example: hxxp://45.133.1[.]182/proxies.txt
- The response is a multiline text file with an IP address and a port in each line.
- The main C2 IP address is always encoded in line 119 of this file.
- The port is discarded and the IP is rearranged.
- 1.45.60.133 becomes 45.133.1.60.



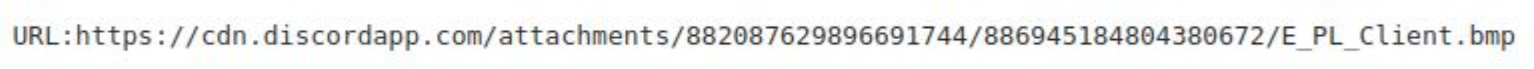
```
line 115: 134.19.171.146:5678
line 116: 91.90.236.239:5678
line 117: 134.19.171.79:5678
line 118: 5.2.200.203:1080
line 119: 1.45.60.133:1080
line 120: 91.82.132.161:4145
line 121: 165.16.112.197:5678
line 122: 195.144.21.185:1080
line 123: 78.83.12.181:5678
line 124: 165.16.112.149:5678
line 125: 91.144.95.163:4145
line 126: 46.167.234.141:5678
line 127: 188.26.122.229:5678
line 128: 81.218.45.154:5678
line 129: 5.133.27.11:5678
line 130: 83.40.67.164:5678
line 131: 185.154.239.15:5678
line 132: 95.111.91.50:10801
```

Excerpt with line numbers

Loader module: Downloading the core module

- Loader uses the main C2 address to query this URL:
  - Example: hxxp://45.133.1[.]60/base/api/statistics.php
- The response is encrypted with a 1-byte XOR key hardcoded in the sample.
- The decrypted response is a download config for the encrypted core module.

  Frequently stored on the Discord CDN.



```
URL:https://cdn.discordapp.com/attachments/882087629896691744/886945184804380672/E_PL_Client.bmp
```

Loader module: Executing the core module

- Decrypts and reflectively loads the core module DLL.
- Builds a parameter buffer that it supplies to the core module's entrypoint.

Buffer offset	Argument	Size
0x00	Region code integer hardcoded into the loader module e.g. 2	4 bytes
0x04	Termination byte set to 1 by the core module before it terminates	1 byte
0x05	The main C2 host	variable
0x120	Unknown integer as a string	variable

INTEL471

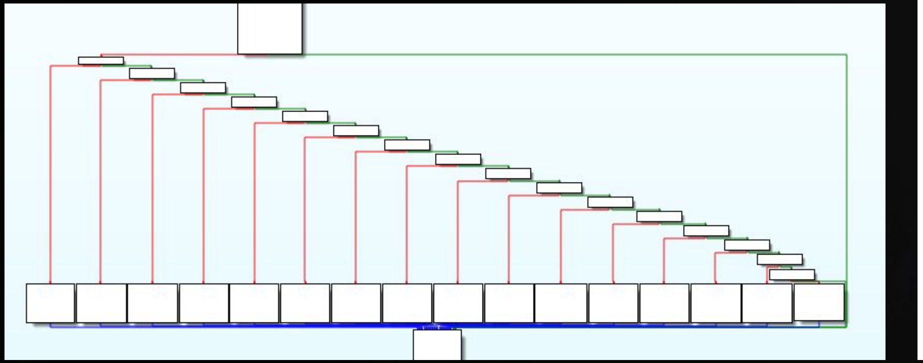
Core module

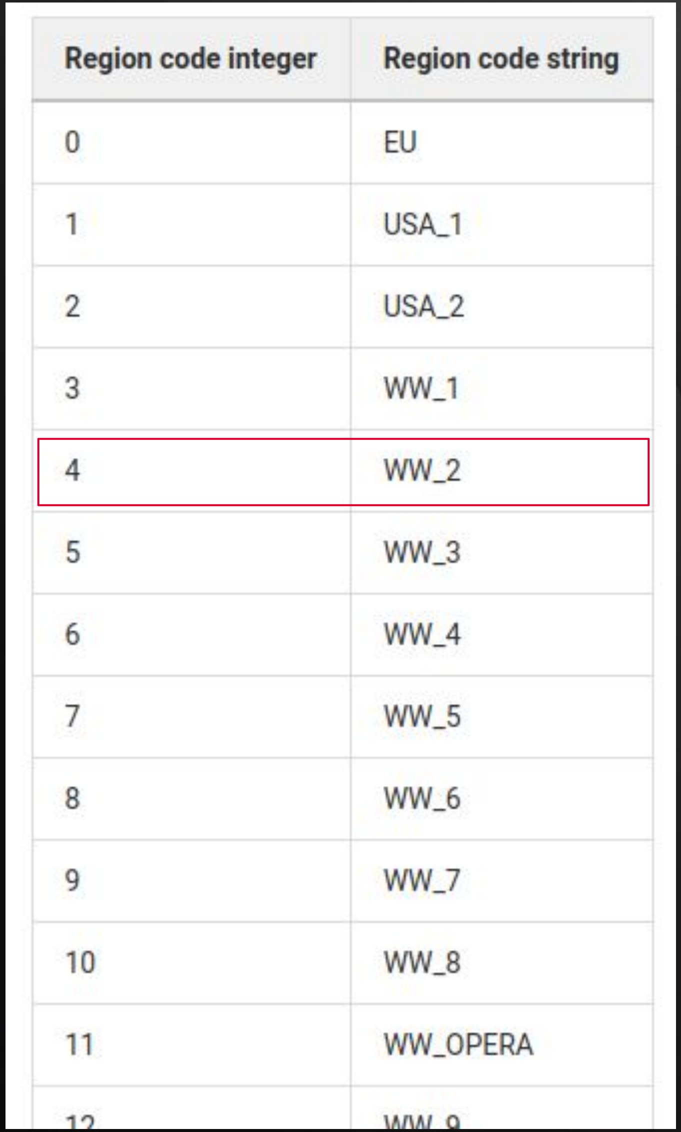
- Uses Windows 10 UAC bypass to elevate privileges. Relies on widely documented technique involving ComputerDefaults.exe
- Disables Windows Defender by writing to the registry.

Registry key	Values
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender	- DisableAntiSpyware - DisableRoutinelyTakingAction
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	- DisableBehaviorMonitoring - DisableOnAccessProtection - DisableScanOnRealtimeEnable - DisableRealtimeMonitoring - DisableIOAVProtection - DisableRawWriteNotification

Core module: Region code

- Reads its configuration from the parameter buffer passed by the loader module.
- The region code integer is mapped to a string using a conversion table.
- Frequently updated. 32 region codes in current samples.

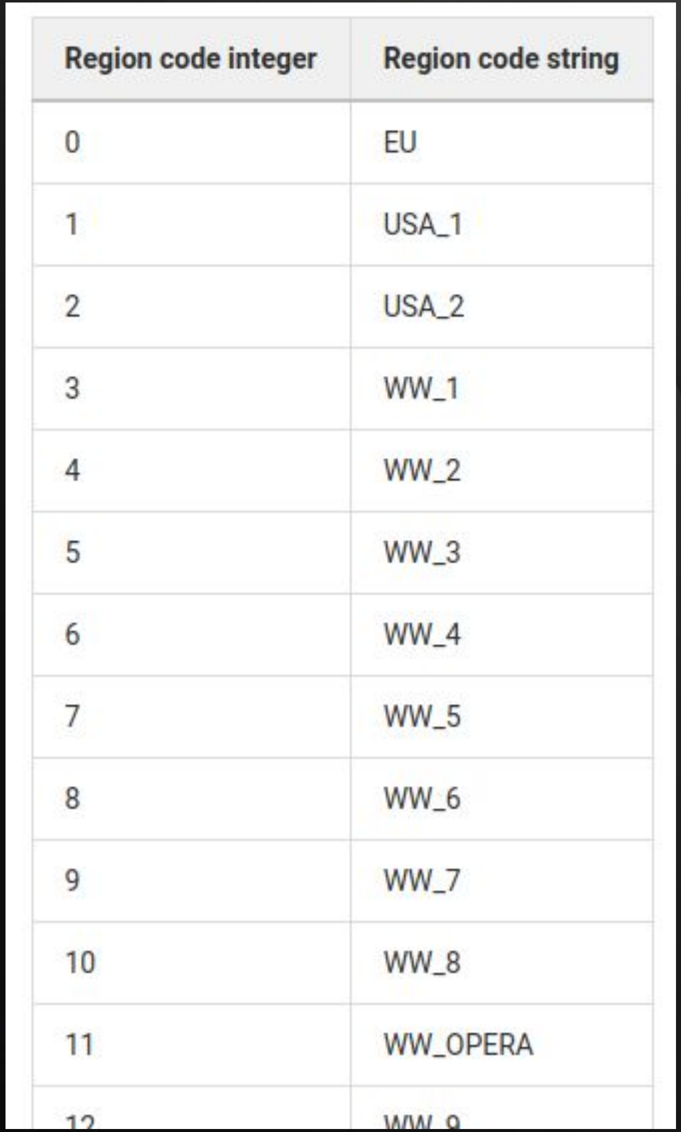




Region code integer	Region code string
0	EU
1	USA_1
2	USA_2
3	WW_1
4	WW_2
5	WW_3
6	WW_4
7	WW_5
8	WW_6
9	WW_7
10	WW_8
11	WW_OPERA
12	WW_9

Core module: Region code

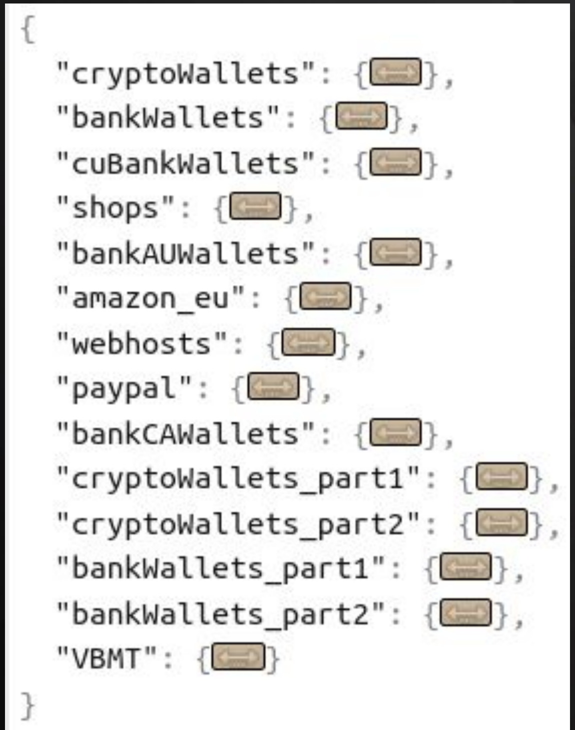
- Since this region code is hardcoded in the loader, we believe that the proper samples are funneled to targeted geo-locations by the delivery network distributing PrivateLoader.
- Region code defines which payloads to deliver to bots.



Region code integer	Region code string
0	EU
1	USA_1
2	USA_2
3	WW_1
4	WW_2
5	WW_3
6	WW_4
7	WW_5
8	WW_6
9	WW_7
10	WW_8
11	WW_OPERA
12	WW_9

Core module: Target fingerprinting

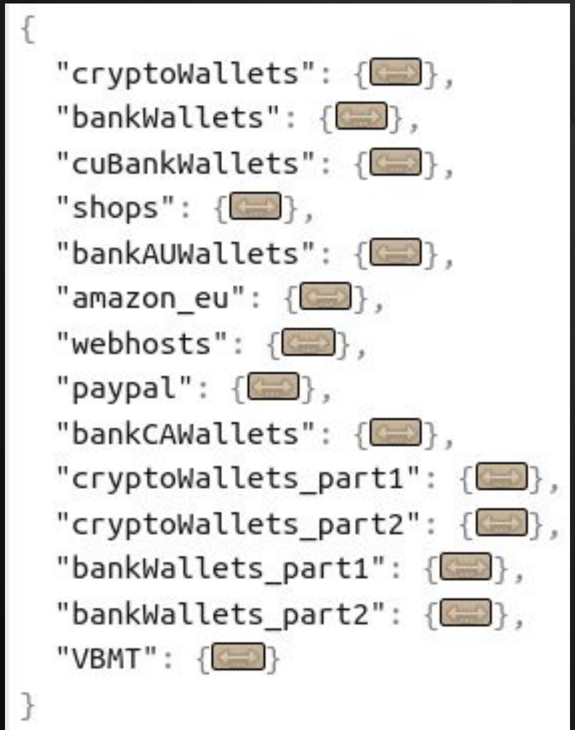
- Searches for cryptocurrency wallet software and browser login data for multiple websites related to banking, cryptocurrency and e-commerce.
- Searches are grouped by category each with specific targets e.g. cold wallets, browser wallets, banking websites etc.



```
{
  "cryptoWallets": {↔},
  "bankWallets": {↔},
  "cuBankWallets": {↔},
  "shops": {↔},
  "bankAUWallets": {↔},
  "amazon_eu": {↔},
  "webhosts": {↔},
  "paypal": {↔},
  "bankCAWallets": {↔},
  "cryptoWallets_part1": {↔},
  "cryptoWallets_part2": {↔},
  "bankWallets_part1": {↔},
  "bankWallets_part2": {↔},
  "VBMT": {↔}
}
```

Core module: Target fingerprinting

- When a target in a category identified, the category is marked as present.
- Operators can set an option to serve payloads only when a target for a certain category was identified on the infected host.

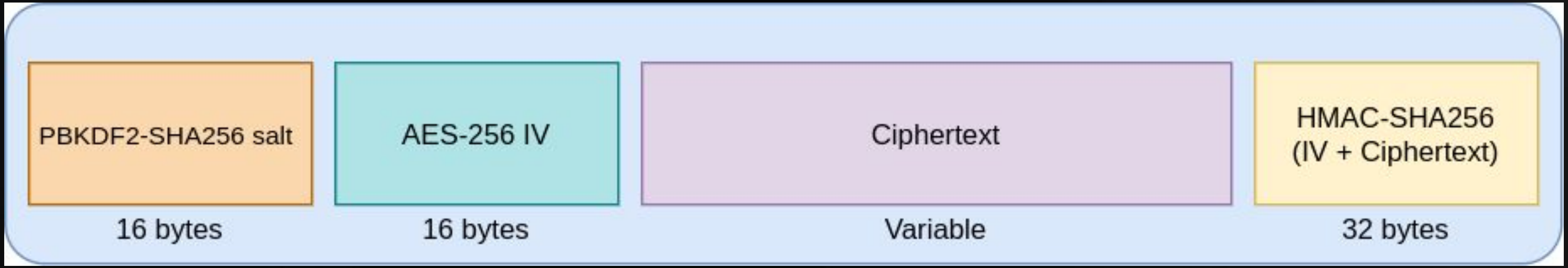


```
{
  "cryptoWallets": {↔},
  "bankWallets": {↔},
  "cuBankWallets": {↔},
  "shops": {↔},
  "bankAUWallets": {↔},
  "amazon_eu": {↔},
  "webhosts": {↔},
  "paypal": {↔},
  "bankCAWallets": {↔},
  "cryptoWallets_part1": {↔},
  "cryptoWallets_part2": {↔},
  "bankWallets_part1": {↔},
  "bankWallets_part2": {↔},
  "VBMT": {↔}
}
```

INTEL471

Core module: Communication protocol

- Communication is done using HTTP POST requests.
  - Endpoint: /base/api/getData.php
- Relies on a more robust algorithm to encrypt request and response messages.
  - PBKDF2-SHA512 + AES-256 CBC + HMAC-SHA256.
  - The password used in PBKDF2 is: **Snowman+under_a_sn0wdrift_forgot_the_Snow_Maiden**
  - PBKDF2 is used to generate AES-256 and HMAC keys.
- Resulting packet is base64 encoded.



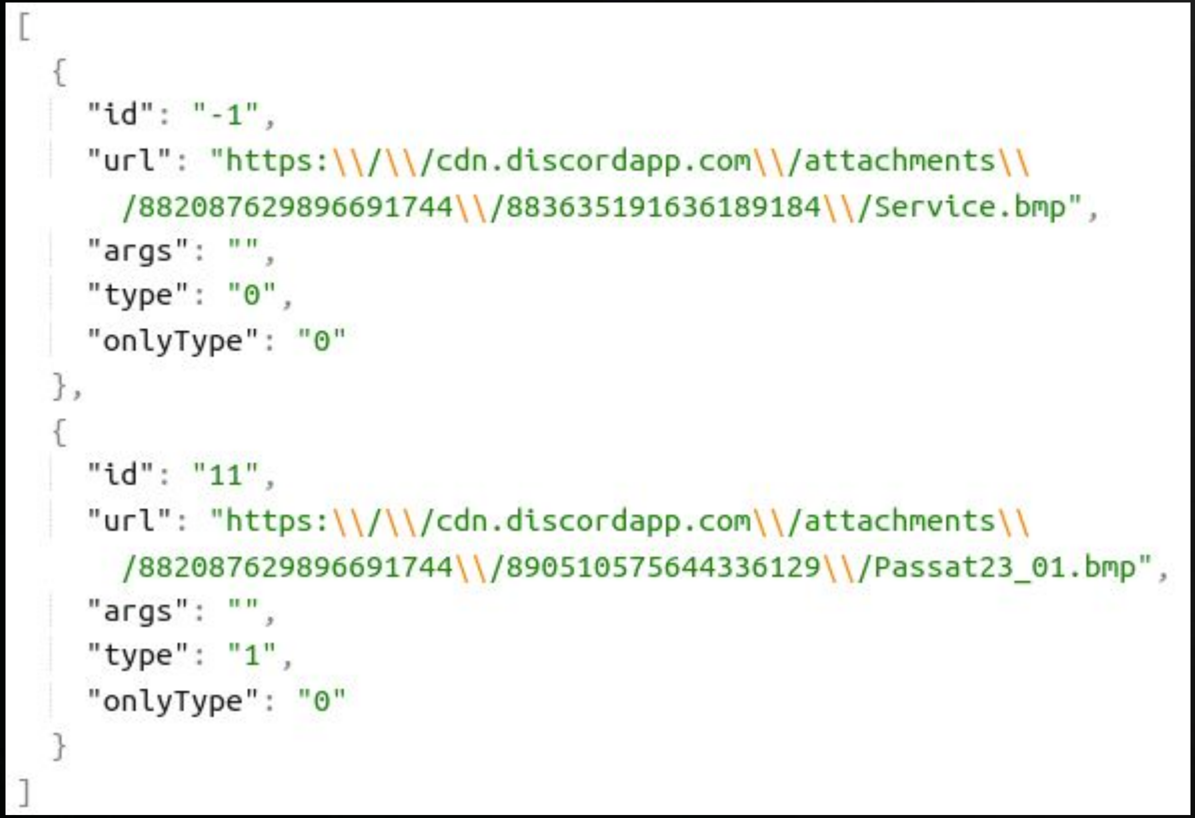
PBKDF2-SHA256 salt	AES-256 IV	Ciphertext	HMAC-SHA256 (IV + Ciphertext)
16 bytes	16 bytes	Variable	32 bytes

Core module: Retrieving payloads

- PrivateLoader supports deployment of:
  - Windows .EXE executables.
  - Browser extensions on most Chromium browsers silently.
- Request messages to retrieve the download URLs:
  - GetExtensions|{REGION_CODE}|{BOT_COUNTRY}|10
  - GetLinks|{REGION_CODE}|{BOT_COUNTRY}|10

Core module: Executable payloads

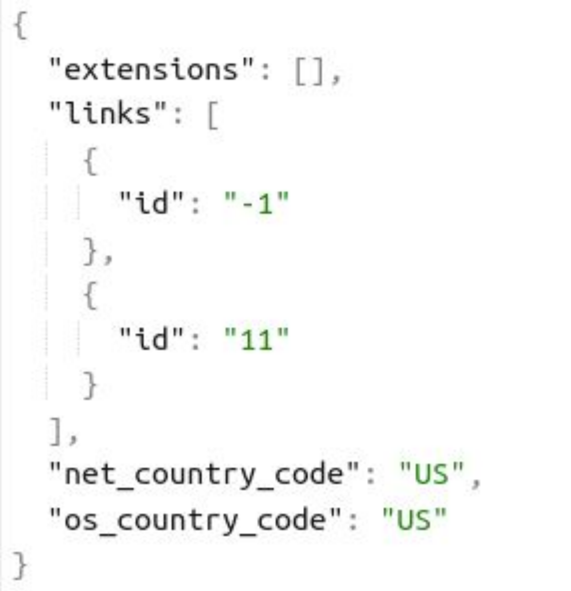
- Example request to get loader links
  - GetLinks|WW_8|US|10
- Example response:



```
[
  {
    "id": "-1",
    "url": "https:\\/\\/cdn.discordapp.com\\/attachments\\
      /882087629896691744\\/883635191636189184\\/Service.bmp",
    "args": "",
    "type": "0",
    "onlyType": "0"
  },
  {
    "id": "11",
    "url": "https:\\/\\/cdn.discordapp.com\\/attachments\\
      /882087629896691744\\/890510575644336129\\/Passat23_01.bmp",
    "args": "",
    "type": "1",
    "onlyType": "0"
  }
]
```

Core module: PPI logs

- The core module must relay information regarding installed payloads back to the C2.
- AddLoggerStat|{"extensions":[],"links":[{"id":"-1"},{"id":"11"}],"net_country_code":"US","os_country_code":"US"}



```
{
  "extensions": [],
  "links": [
    {
      "id": "-1"
    },
    {
      "id": "11"
    }
  ],
  "net_country_code": "US",
  "os_country_code": "US"
}
```

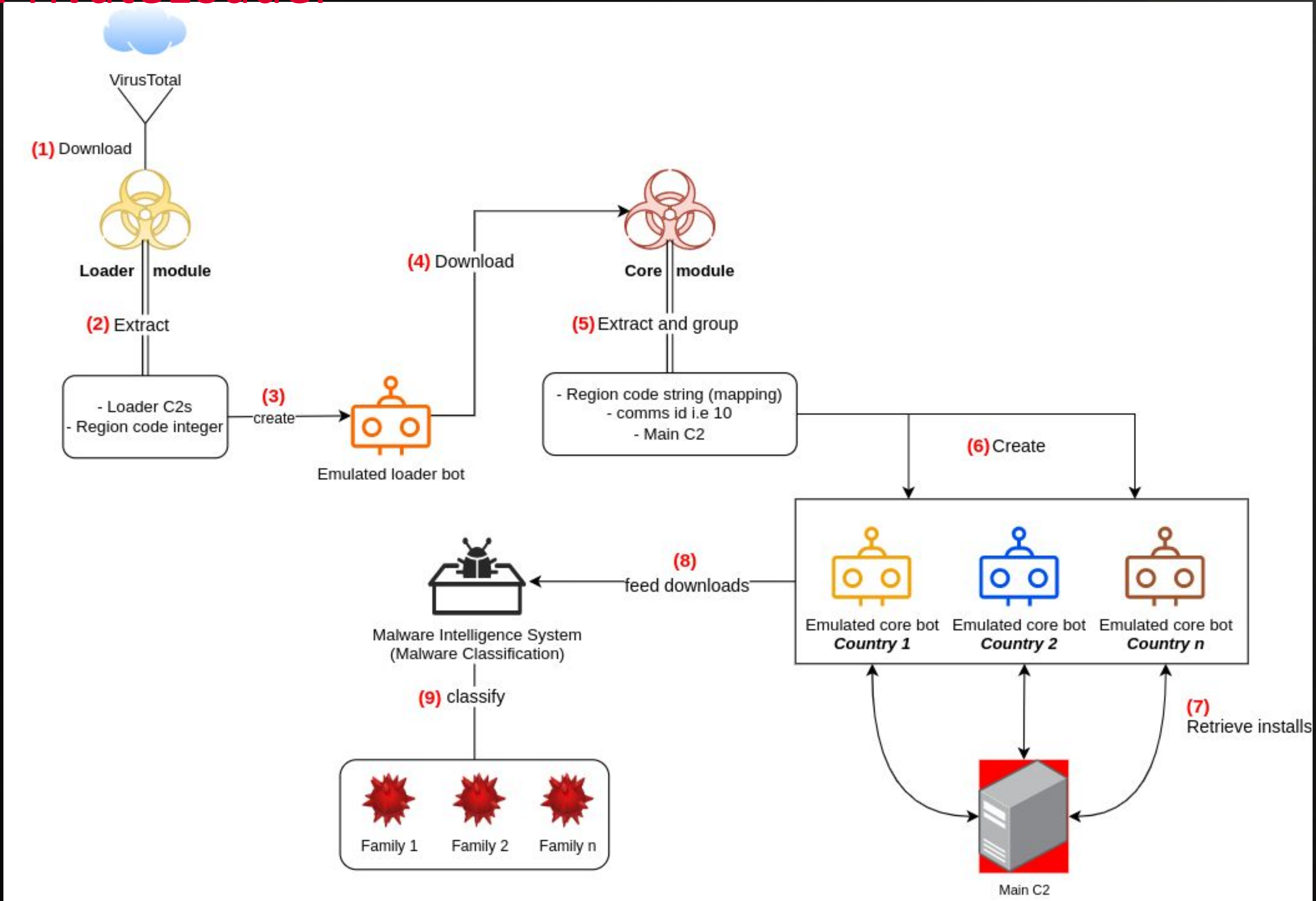
Service module

- Ensures persistence:
  - Persisted to run at logon:
    - Windows service.
    - Scheduled task.
  - Runs every hour thanks to a scheduled task.
  - C:\Program Files (x86)\PowerControl\PowerControl_Svc.exe
- Communicates with the main C2:
  - /service/communication.php
- Updates itself.
- Receives a download URL to execute a loader module.

Tracking PrivateLoader

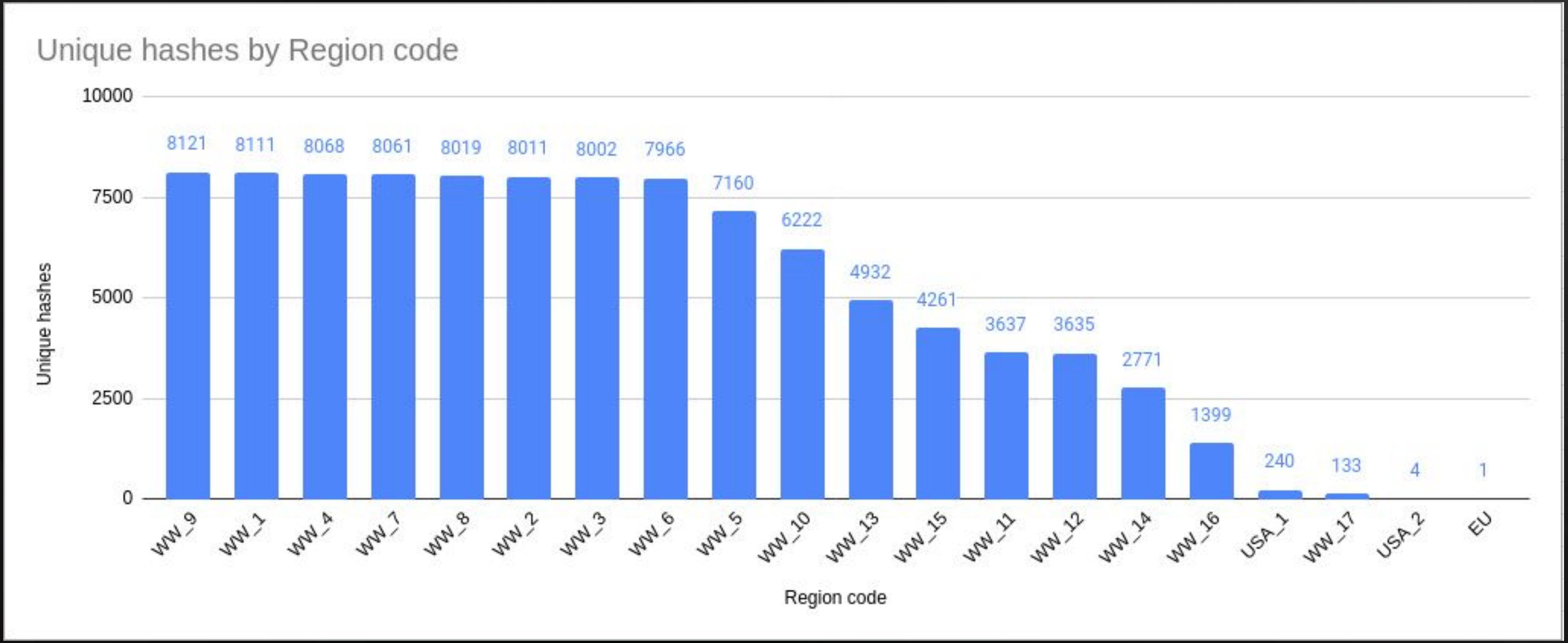
- Intel 471 started tracking PrivateLoader in early September 2021.
- Automate the whole life-cycle of an infection for each sample.
    - From a loader component to getting installs.
- Replicate using config extractors + network protocol emulation.
- Create bots from various countries.
- Passive bots to avoid raising alarms.
- Classify as many malware families as we can.

Tracking PrivateLoader



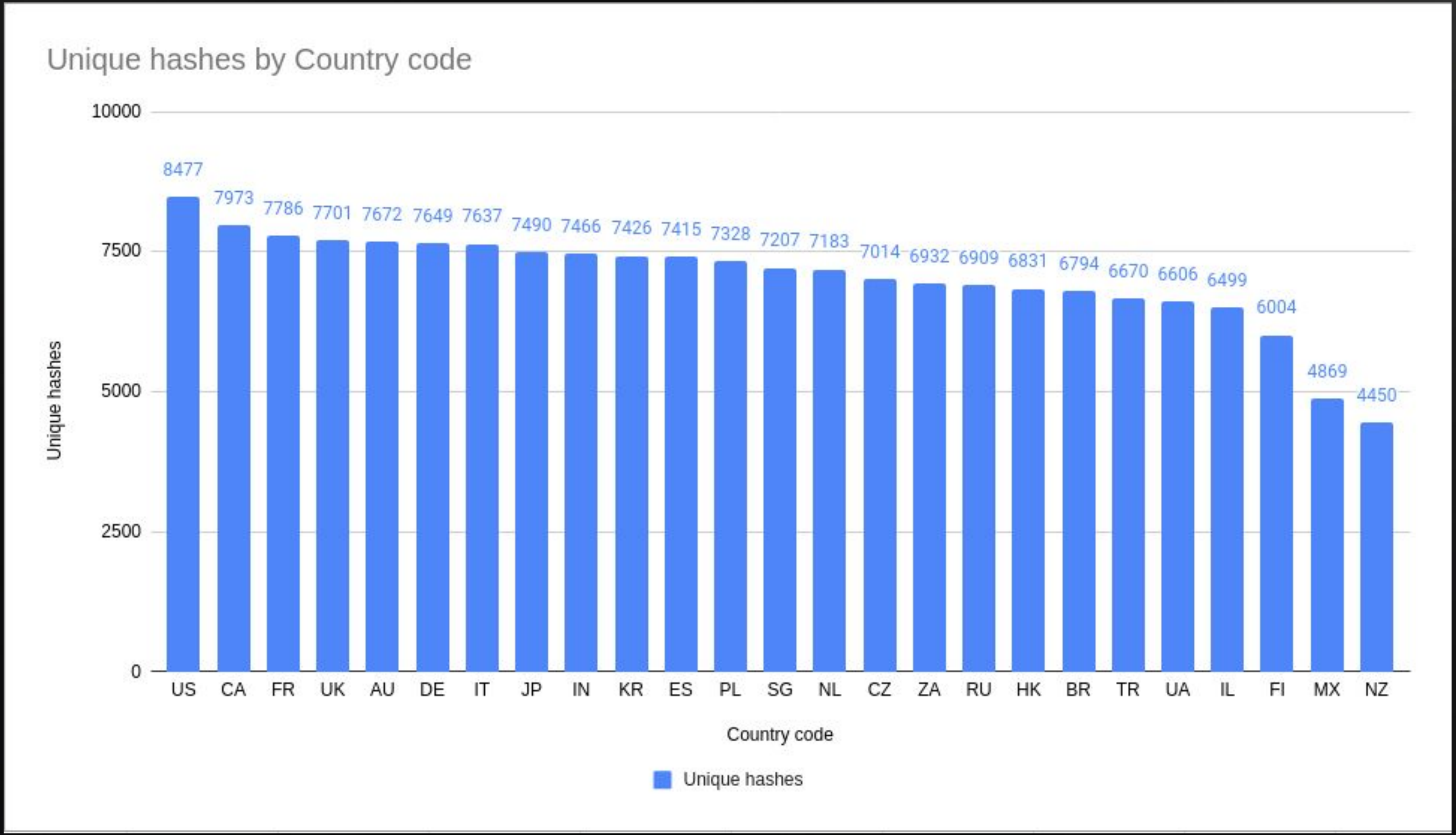
INTEL471

Tracking PrivateLoader: Bot stats

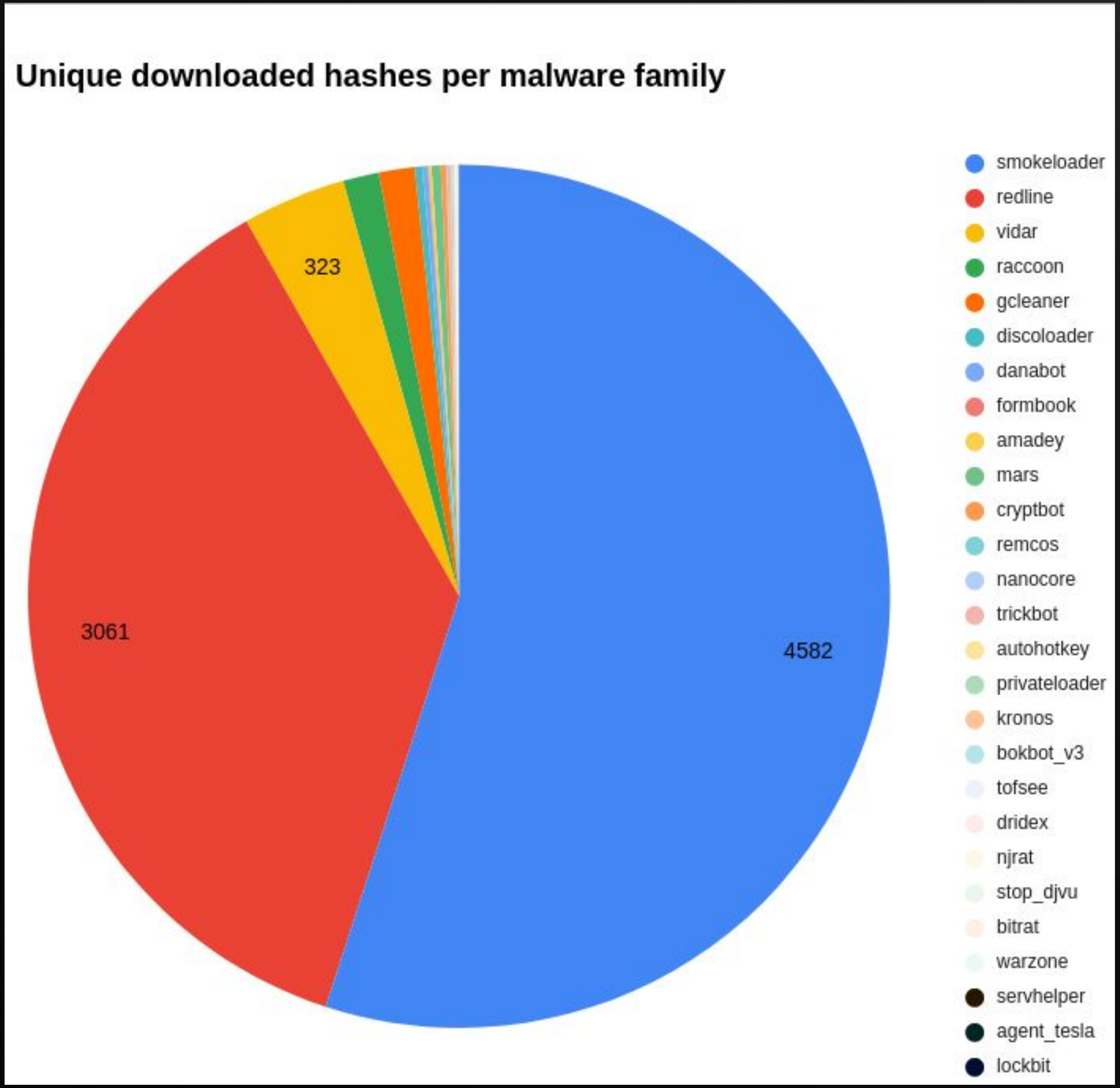


INTEL471

Tracking PrivateLoader: Bot stats



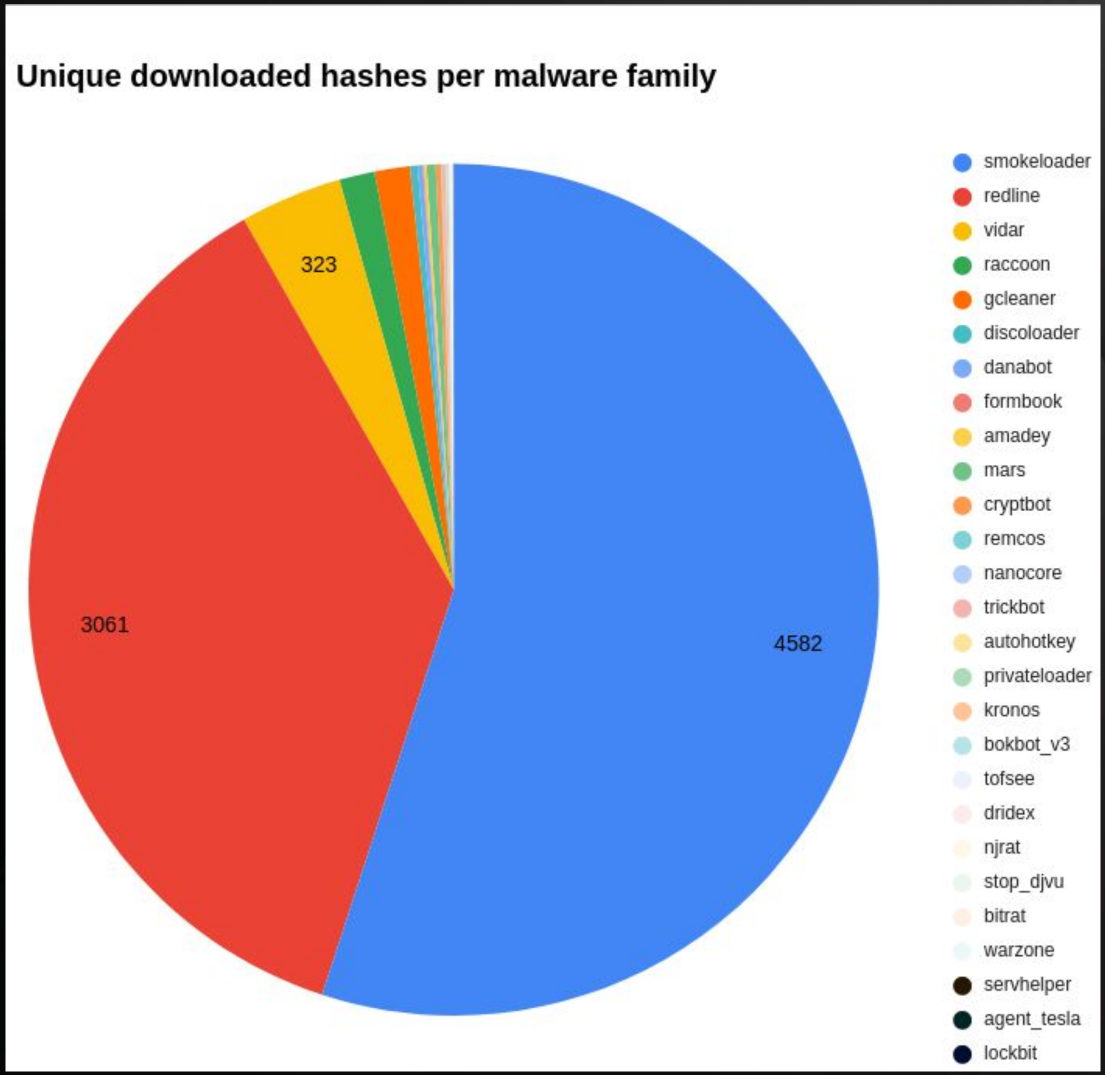
Tracking PrivateLoader: Malware families



INTEL471

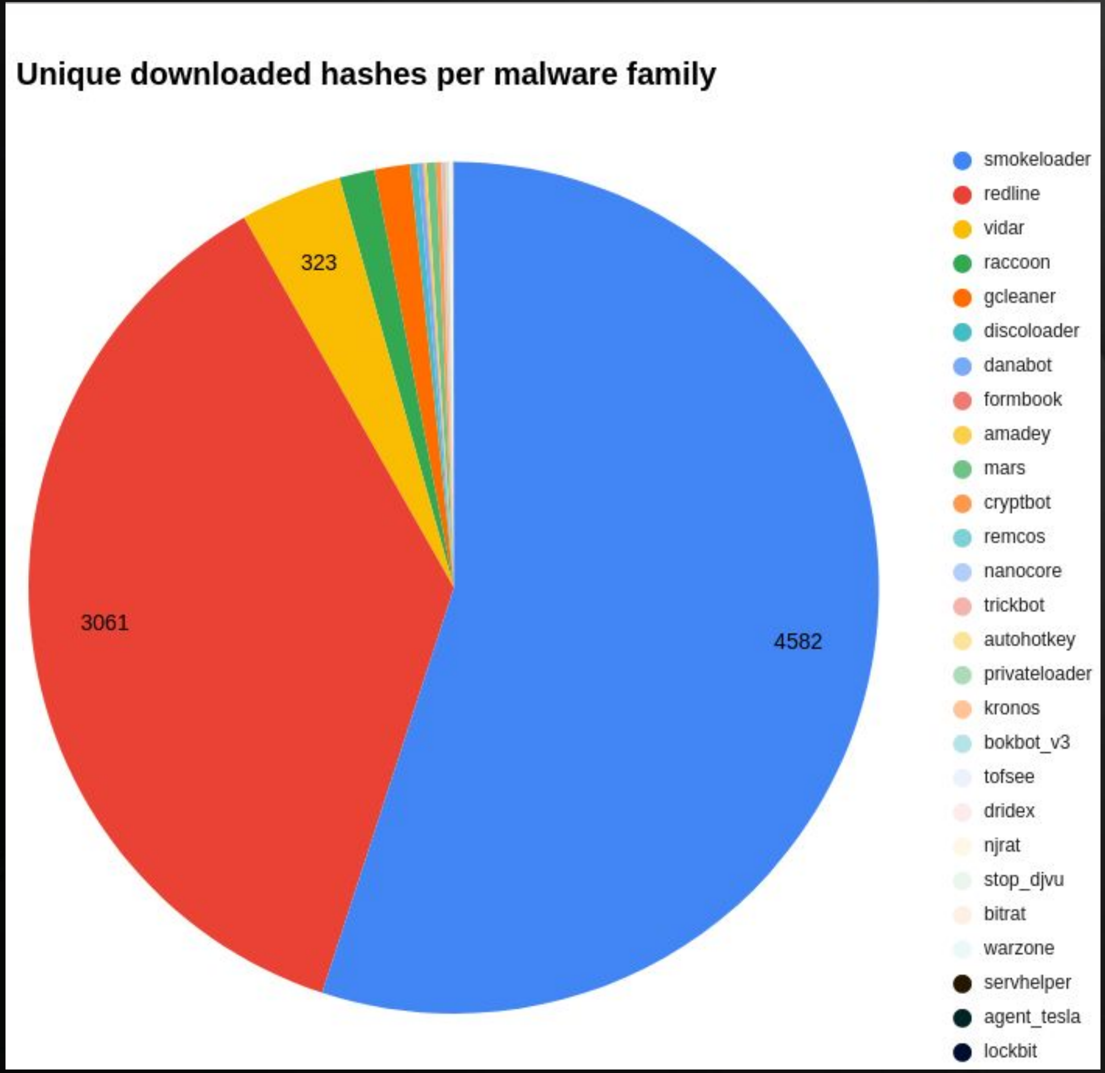
Tracking PrivateLoader: Banking Trojans

- On Oct. 22, 2021, a Smokeloader sample delivered the Qbot banking trojan. Revealed the new botnet ID star01.
- On Oct. 31. PrivateLoader dropping:
  - ➢ Kronos.
- On Nov. 1. Privateloader dropping:
  - ➢ Danabot: affiliate ID 40.
  - ➢ Dridex: 10444 botnet.
  - ➢ Trickbot: lip*, tot*, top* gtags.
- Danabot, Dridex and Trickbot were often bundled together.


Unique downloaded hashes per malware family

Tracking PrivateLoader: Banking Trojans

- On Nov. 14, started dropping Danabot with affiliate ID 4 for a day.
- Starting late February 2022, new version of the Danabot banking trojan pushed by affiliate ID 5.

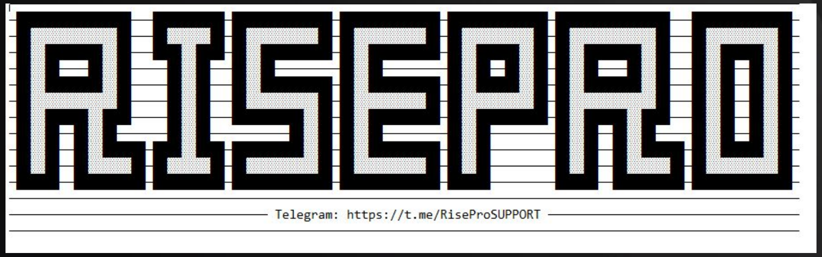


Tracking PrivateLoader: Ransomware

- PPI services advise against deploying ransomware.
- Ransomware seen from PrivateLoader:
    - Lockbit
    - STOP Djvu

Tracking PrivateLoader: Some new families

- RisePro stealer
  - Information stealer in C++ appeared in December 2021.
  - From the same developers of Privateloader.
  - Download and execute functionality: miners.



RISEPRO

Telegram: https://t.me/RiseProSUPPORT

- Discoloader
  - .NET loader
  - Hosts payload on the Discord CDN

Conclusion

- PPI services have been around for a long time.
- Accessible and affordable to offload malware delivery.
- PPI services often overlooked when it comes to installed payloads.
- Privateloader as an example.

Thank you !

Contact: shammou@intel471.com

Website: www.intel471.com

Twitter: @Dark_Puzzle