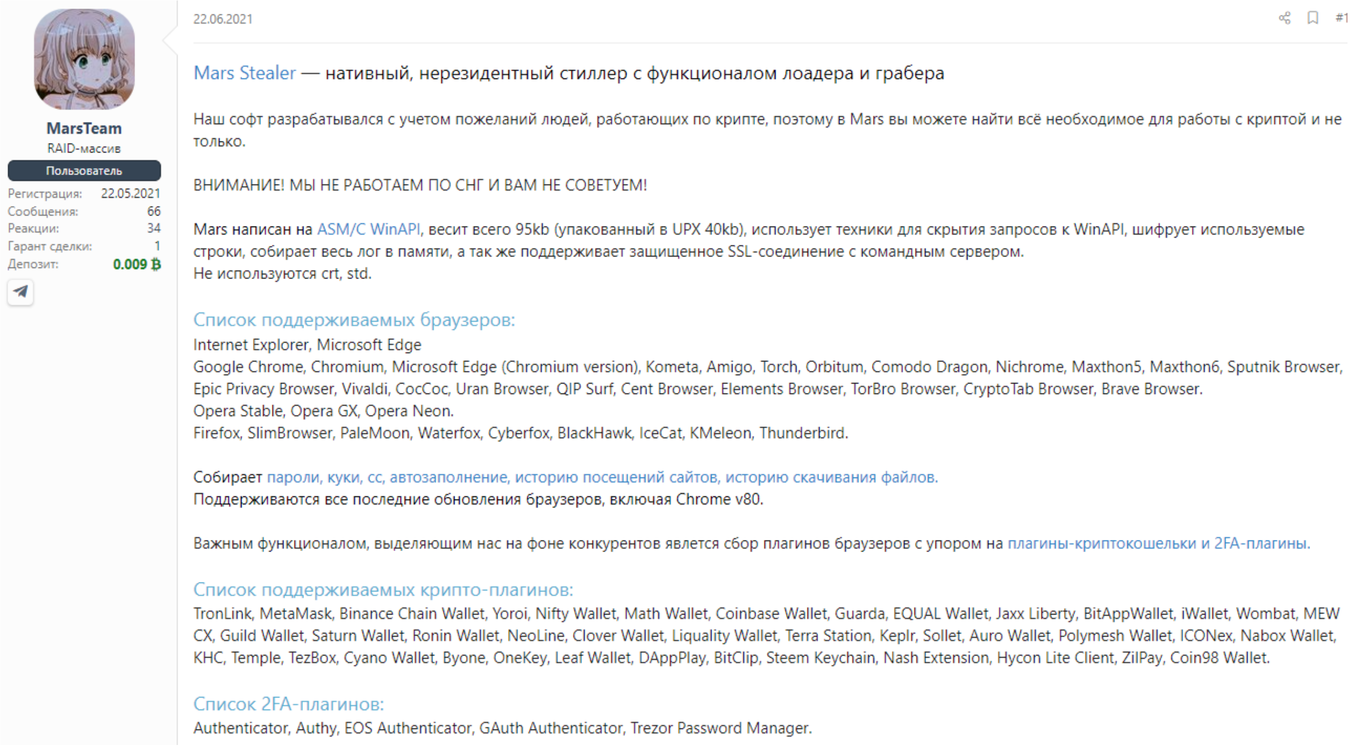
Exclusive Threat Research: Mars (Stealer) Attacks!

blog.morphisec.com/threat-research-mars-stealer

- Tweet
-

The Morphisec Labs team has conducted research on the new Mars infostealer. Mars is based on the older Oski Stealer and was first discovered in June 2021. The new Mars is available for sale on several underground forums and is reported to be under constant development. The Mars Stealer pilfers user credentials stored in various browsers, as well as many different cryptocurrency wallets. Mars Stealer is being distributed via social engineering techniques, malspam campaigns, malicious software cracks, and keygens. (For more about infostealers, read Morphisec's coverage of the Jupyter infostealer.)



MarsTeam

RAID-массив

Пользователь

Регистрация:	22.05.2021
Сообщения:	66
Реакции:	34
Гарант сделки:	1
Депозит:	0.009 ₿

22.06.2021 #1

Mars Stealer — нативный, нерезидентный стиллер с функционалом лоадера и грабера

Наш софт разрабатывался с учетом пожеланий людей, работающих по крипте, поэтому в Mars вы можете найти всё необходимое для работы с криптой и не только.

ВНИМАНИЕ! МЫ НЕ РАБОТАЕМ ПО СНГ И ВАМ НЕ СОВЕТУЕМ!

Mars написан на ASM/C WinAPI, весит всего 95kb (упакованный в UPX 40kb), использует техники для скрытия запросов к WinAPI, шифрует используемые строки, собирает весь лог в памяти, а так же поддерживает защищенное SSL-соединение с командным сервером.
Не используются crt, std.

Список поддерживаемых браузеров:
Internet Explorer, Microsoft Edge
Google Chrome, Chromium, Microsoft Edge (Chromium version), Kometa, Amigo, Torch, Orbitum, Comodo Dragon, Nichrome, Maxthon5, Maxthon6, Sputnik Browser, Epic Privacy Browser, Vivaldi, CocCoc, Uran Browser, QIP Surf, Cent Browser, Elements Browser, TorBro Browser, CryptoTab Browser, Brave Browser.
Opera Stable, Opera GX, Opera Neon.
Firefox, SlimBrowser, PaleMoon, Waterfox, Cyberfox, BlackHawk, IceCat, KMeleon, Thunderbird.

Собирает пароли, куки, сс, автозаполнение, историю посещений сайтов, историю скачивания файлов.
Поддерживаются все последние обновления браузеров, включая Chrome v80.

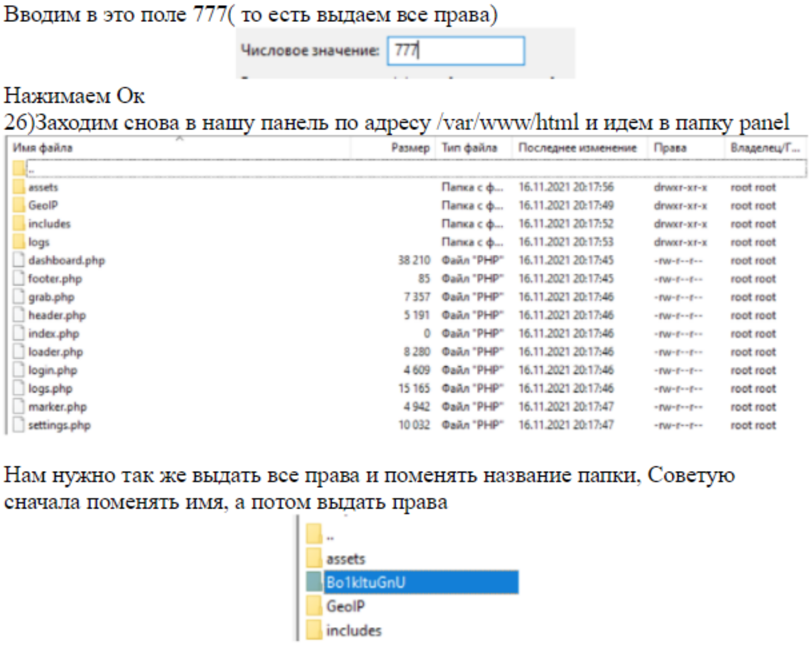
Важным функционалом, выделяющим нас на фоне конкурентов является сбор плагинов браузеров с упором на плагины-криптокошельки и 2FA-плагины.

Список поддерживаемых крипто-плагинов:
TronLink, MetaMask, Binance Chain Wallet, Yoroi, Nifty Wallet, Math Wallet, Coinbase Wallet, Guarda, EQUAL Wallet, Jaxx Liberty, BitAppWallet, iWallet, Wombat, MEW CX, Guild Wallet, Saturn Wallet, Ronin Wallet, NeoLine, Clover Wallet, Liquality Wallet, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh Wallet, ICONex, Nabox Wallet, KHC, Temple, TezBox, Cyano Wallet, Byone, OneKey, Leaf Wallet, DAppPlay, BitClip, Steem Keychain, Nash Extension, Hycon Lite Client, ZilPay, Coin98 Wallet.

Список 2FA-плагинов:
Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Trezor Password Manager.

Figure 1: Mars stealer post on hacking forums.

Not long after the Mars Stealer's release, a cracked version was released with an instruction document. This guide has some flaws. One flaw instructs users to set up full access (777) to the whole project, including the victims' logs directory.



Вводим в это поле 777(то есть выдаем все права)

Числовое значение: 777

Нажимаем Ок
26)Заходим снова в нашу панель по адресу /var/www/html и идем в папку panel

Имя файла	Размер	Тип файла	Последнее изменение	Права	Владелец/Г...
..					
assets		Папка с ф...	16.11.2021 20:17:56	drwxr-xr-x	root root
GeoIP		Папка с ф...	16.11.2021 20:17:49	drwxr-xr-x	root root
includes		Папка с ф...	16.11.2021 20:17:52	drwxr-xr-x	root root
logs		Папка с ф...	16.11.2021 20:17:53	drwxr-xr-x	root root
dashboard.php	38 210	Файл "PHP"	16.11.2021 20:17:45	-rw-r--r--	root root
footer.php	85	Файл "PHP"	16.11.2021 20:17:45	-rw-r--r--	root root
grab.php	7 357	Файл "PHP"	16.11.2021 20:17:46	-rw-r--r--	root root
header.php	5 191	Файл "PHP"	16.11.2021 20:17:46	-rw-r--r--	root root
index.php	0	Файл "PHP"	16.11.2021 20:17:46	-rw-r--r--	root root
loader.php	8 280	Файл "PHP"	16.11.2021 20:17:46	-rw-r--r--	root root
login.php	4 609	Файл "PHP"	16.11.2021 20:17:46	-rw-r--r--	root root
logs.php	15 165	Файл "PHP"	16.11.2021 20:17:46	-rw-r--r--	root root
marker.php	4 942	Файл "PHP"	16.11.2021 20:17:47	-rw-r--r--	root root
settings.php	10 032	Файл "PHP"	16.11.2021 20:17:47	-rw-r--r--	root root

Нам нужно так же выдать все права и поменять название папки, Советую сначала поменять имя, а потом выдать права

..
assets
Bo1kltuGnU
GeoIP
includes

Figure 2: Cracked Mars Stealer instruction guide.

Whoever released the cracked Mars Stealer without official support has led threat actors to improperly configure their environment, exposing critical assets to the world.

Infostealers Ecosystem

As Sophos explains, information stealers are used for a wide variety of identity theft. They enable attackers to harvest personally identifiable information (PII), including login data such as stored credentials and browser cookies that control access to web-based services. These credentials are then sold on criminal marketplaces.

Infostealers offer an accessible entry point to criminal activity. For example, only $160 gets you a lifetime subscription to Mars Stealer. You can purchase infostealers on Dark Web forums without any vetting, unlike more sophisticated tools such as ransomware, which require you to have a reputation amongst other cybercriminals. Infostealers empower novice cybercriminals to build a reputation they can leverage to acquire more powerful malware from more sophisticated actors.

Mars Stealer Statistics

With cryptocurrency use rising, more people will likely possess hot wallets in an unsecured environment. The crypto wallet MetaMask is the plugin most stolen using Mars Stealer.

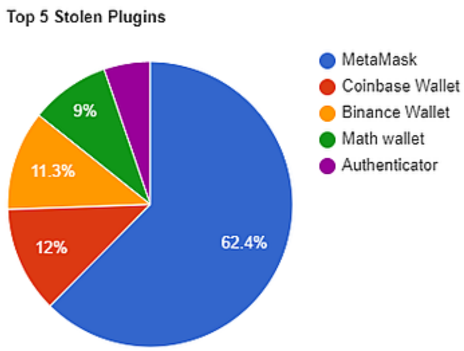
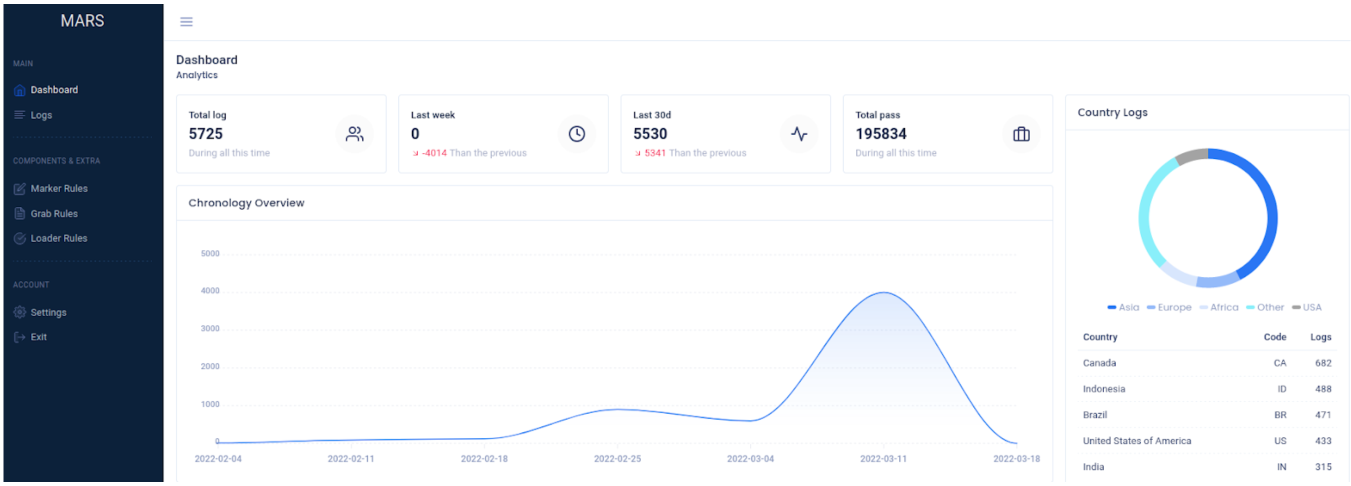


Figure 3: Top 5 stolen plugins

The Morphisec Labs Team compiled the below statistics while evaluating a single actor’s campaign last month. It includes targets by country, total stolen passwords, and so on. In addition, we found more than infected 50 domain users, compromising companies' domain passwords. The vast majority of victims are students, faculty members, and content makers looking for legitimate applications who end up with malicious ones instead. Aside from the listed credential types, Morphisec identified credentials which led to the full compromise of a leading healthcare infrastructure provider in Canada, and a number of high profile Canadian service companies. We have contacted and notified the companies and the authorities.



Dashboard
Analytics

Total log
5725
During all this time

Last week
0
↘ -4014 Than the previous

Last 30d
5530
↘ 5341 Than the previous

Total pass
195834
During all this time

Country Logs

Country	Code	Logs
Canada	CA	682
Indonesia	ID	488
Brazil	BR	471
United States of America	US	433
India	IN	315

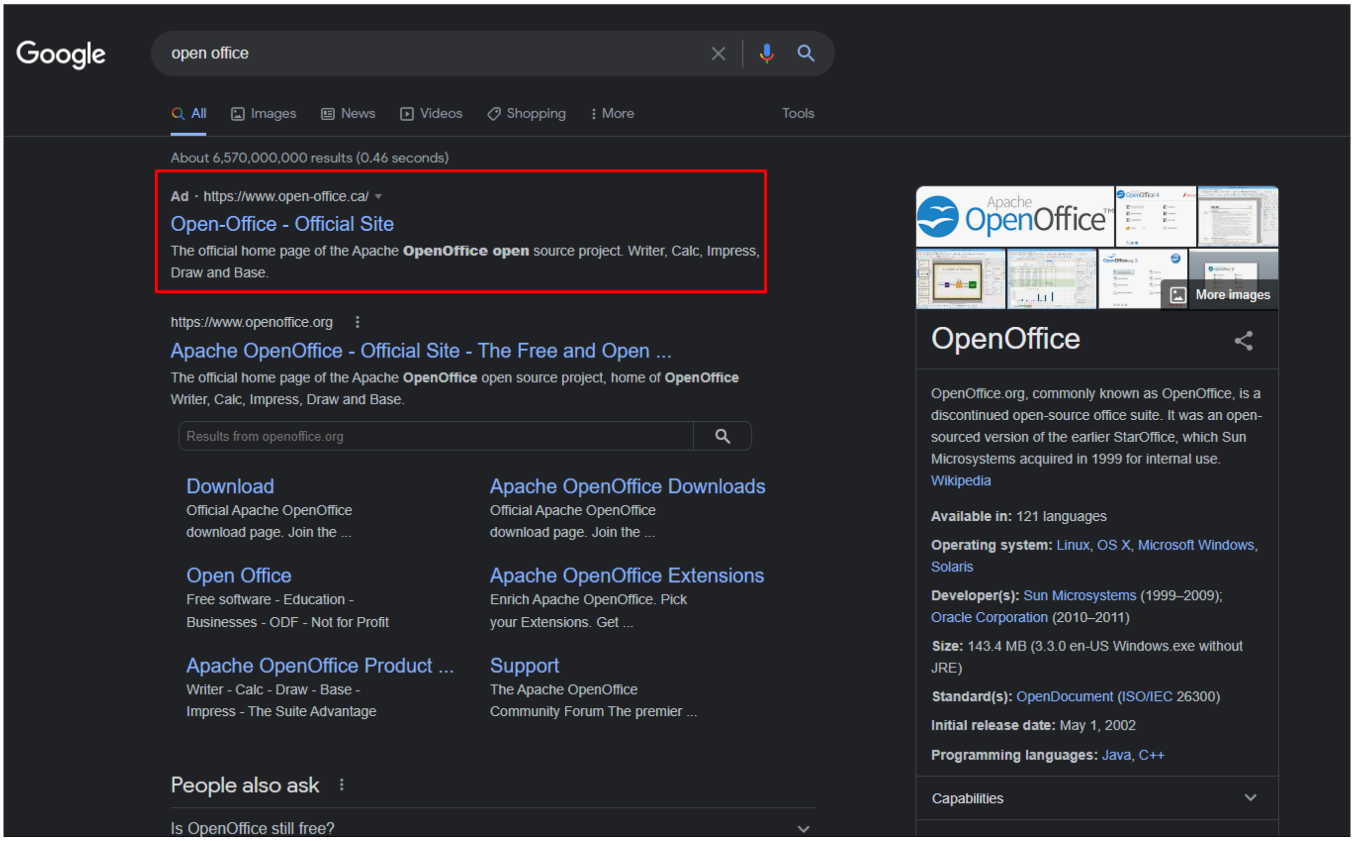
Figure 4: Mars admin panel

Operation Mars

Spam email is the most common distribution method for Mars Stealer, as a compressed executable, download link, or document payload. Creating a malicious website masquerading as pirated software is another common method for spreading this infostealer.

Initial access vector

In this campaign, the actor distributed Mars Stealer via cloned websites offering well-known software. They used the Google Ads advertising platform to trick victims searching for the original software into visiting a malicious site instead. The actor is paying for these Google Ads campaigns using stolen information (see figure 15). The example below is one of many demonstrating how the actor targets Canadians by using geographically targeted Google Ads.



About 6,570,000,000 results (0.46 seconds)

Ad · https://www.open-office.ca/

Open-Office - Official Site

The official home page of the Apache **OpenOffice open** source project. Writer, Calc, Impress, Draw and Base.

https://www.openoffice.org

Apache OpenOffice - Official Site - The Free and Open ...

The official home page of the Apache **OpenOffice** open source project, home of **OpenOffice** Writer, Calc, Impress, Draw and Base.

Results from openoffice.org

Download
Official Apache OpenOffice download page. Join the ...

Apache OpenOffice Downloads
Official Apache OpenOffice download page. Join the ...

Open Office
Free software - Education - Businesses - ODF - Not for Profit

Apache OpenOffice Extensions
Enrich Apache OpenOffice. Pick your Extensions. Get ...

Apache OpenOffice Product ...
Writer - Calc - Draw - Base - Impress - The Suite Advantage

Support
The Apache OpenOffice Community Forum The premier ...

People also ask

Is OpenOffice still free?

OpenOffice

OpenOffice.org, commonly known as OpenOffice, is a discontinued open-source office suite. It was an open-sourced version of the earlier StarOffice, which Sun Microsystems acquired in 1999 for internal use. Wikipedia

Available in: 121 languages

Operating system: Linux, OS X, Microsoft Windows, Solaris

Developer(s): Sun Microsystems (1999–2009); Oracle Corporation (2010–2011)

Size: 143.4 MB (3.3.0 en-US Windows.exe without JRE)

Standard(s): OpenDocument (ISO/IEC 26300)

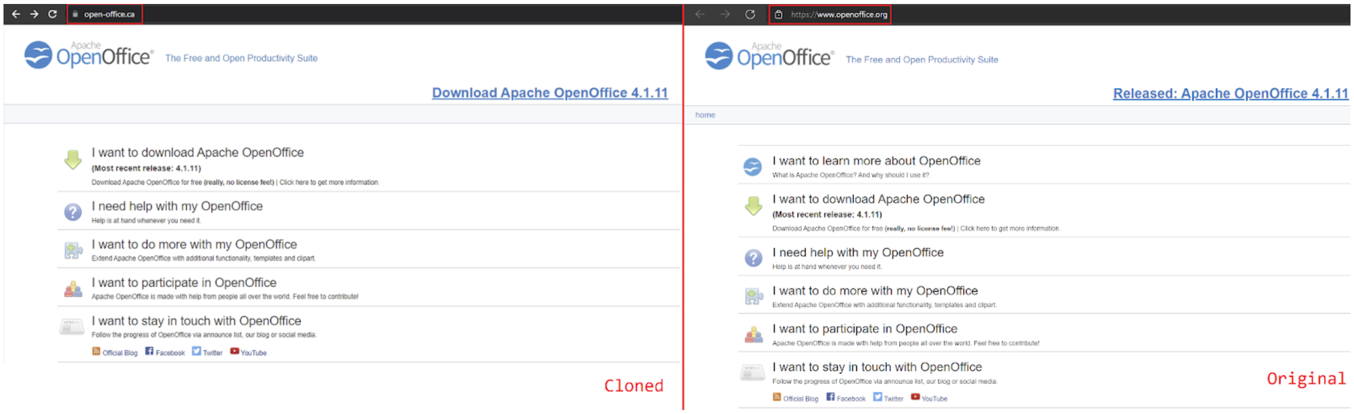
Initial release date: May 1, 2002

Programming languages: Java, C++

Capabilities

Figure 5: 'OpenOffice' Google search yields an actor's malicious website.

Below is a fully cloned website masquerading as the official openoffice.org website to lure victims to download the Mars Stealer.



Download Apache OpenOffice 4.1.11

I want to download Apache OpenOffice
(Most recent release: 4.1.11)
Download Apache OpenOffice for free **(really, no license fee!)** | Click here to get more information.

I need help with my OpenOffice
Help is at hand whenever you need it.

I want to do more with my OpenOffice
Extend Apache OpenOffice with additional functionality, templates and clipart.

I want to participate in OpenOffice
Apache OpenOffice is made with help from people all over the world. Feel free to contribute!

I want to stay in touch with OpenOffice
Follow the progress of OpenOffice via announce list, our blog or social media.
Official Blog Facebook Twitter YouTube

Cloned

https://www.openoffice.org
Apache OpenOffice
The Free and Open Productivity Suite

Released: Apache OpenOffice 4.1.11

home

I want to learn more about OpenOffice
What is Apache OpenOffice? And why should I use it?

I want to download Apache OpenOffice
(Most recent release: 4.1.11)
Download Apache OpenOffice for free **(really, no license fee!)** | Click here to get more information.

I need help with my OpenOffice
Help is at hand whenever you need it.

I want to do more with my OpenOffice
Extend Apache OpenOffice with additional functionality, templates and clipart.

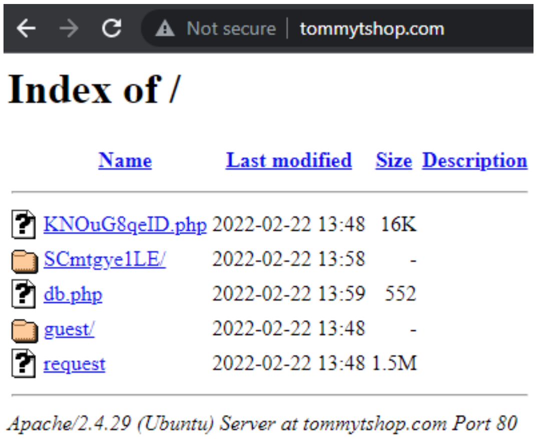
I want to participate in OpenOffice
Apache OpenOffice is made with help from people all over the world. Feel free to contribute!

I want to stay in touch with OpenOffice
Follow the progress of OpenOffice via announce list, our blog or social media.
Official Blog Facebook Twitter YouTube

Original

Figure 6: Cloned OpenOffice website leads to the Mars stealer.

The downloaded payload is an executable file, with a corresponding icon and name, packed with the Babadeda crypter or Autoit loader. We won't cover the Mars Stealer's technical details, which were thoroughly covered by 3xp0rt. During our investigation and research, we identified a C2—**tommytshop[.]com**—where the Mars admin panel is stored, which was still up and running at the time of publication.



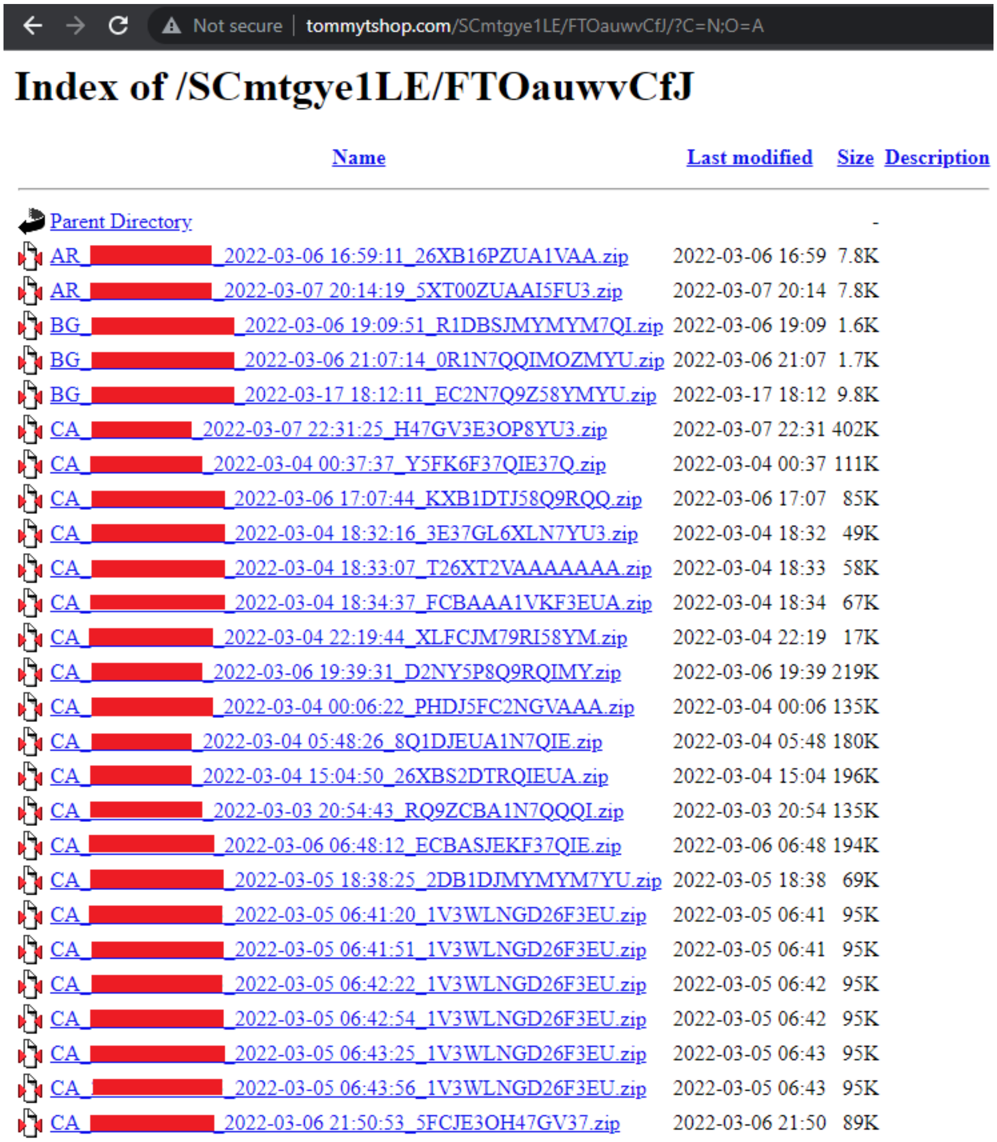
Index of /

Name	Last modified	Size	Description
KNOuG8qeID.php	2022-02-22 13:48	16K	
SCmtgye1LE/	2022-02-22 13:58	-	
db.php	2022-02-22 13:59	552	
guest/	2022-02-22 13:48	-	
request	2022-02-22 13:48	1.5M	

Apache/2.4.29 (Ubuntu) Server at tommytshop.com Port 80

Figure 7: C2 open directory

As mentioned earlier, surprisingly, the stolen information directory was improperly configured and left open. We immediately identified that the vast majority of compromised victims are from Canada (files that start with *CA_*).



Index of /SCmtgye1LE/FTOauwvCfJ

Name	Last modified	Size	Description
Parent Directory		-	
AR_[redacted]_2022-03-06 16:59:11_26XB16PZUA1VAA.zip	2022-03-06 16:59	7.8K	
AR_[redacted]_2022-03-07 20:14:19_5XT00ZUAAI5FU3.zip	2022-03-07 20:14	7.8K	
BG_[redacted]_2022-03-06 19:09:51_R1DBSJMYMYM7QI.zip	2022-03-06 19:09	1.6K	
BG_[redacted]_2022-03-06 21:07:14_0R1N7QQIMOZMYU.zip	2022-03-06 21:07	1.7K	
BG_[redacted]_2022-03-17 18:12:11_EC2N7Q9Z58YMYU.zip	2022-03-17 18:12	9.8K	
CA_[redacted]_2022-03-07 22:31:25_H47GV3E3OP8YU3.zip	2022-03-07 22:31	402K	
CA_[redacted]_2022-03-04 00:37:37_Y5FK6F37QIE37Q.zip	2022-03-04 00:37	111K	
CA_[redacted]_2022-03-06 17:07:44_KXB1DTJ58Q9RQQ.zip	2022-03-06 17:07	85K	
CA_[redacted]_2022-03-04 18:32:16_3E37GL6XLN7YU3.zip	2022-03-04 18:32	49K	
CA_[redacted]_2022-03-04 18:33:07_T26XT2VAAAAAAA.zip	2022-03-04 18:33	58K	
CA_[redacted]_2022-03-04 18:34:37_FCBAAA1VKF3EUA.zip	2022-03-04 18:34	67K	
CA_[redacted]_2022-03-04 22:19:44_XLFCJM79RI58YM.zip	2022-03-04 22:19	17K	
CA_[redacted]_2022-03-06 19:39:31_D2NY5P8Q9RQIMY.zip	2022-03-06 19:39	219K	
CA_[redacted]_2022-03-04 00:06:22_PHDJ5FC2NGVAAA.zip	2022-03-04 00:06	135K	
CA_[redacted]_2022-03-04 05:48:26_8Q1DJEUA1N7QIE.zip	2022-03-04 05:48	180K	
CA_[redacted]_2022-03-04 15:04:50_26XBS2DTRQIEUA.zip	2022-03-04 15:04	196K	
CA_[redacted]_2022-03-03 20:54:43_RQ9ZCBA1N7QQQI.zip	2022-03-03 20:54	135K	
CA_[redacted]_2022-03-06 06:48:12_ECBASJEKF37QIE.zip	2022-03-06 06:48	194K	
CA_[redacted]_2022-03-05 18:38:25_2DB1DJMYMYM7YU.zip	2022-03-05 18:38	69K	
CA_[redacted]_2022-03-05 06:41:20_1V3WLNGD26F3EU.zip	2022-03-05 06:41	95K	
CA_[redacted]_2022-03-05 06:41:51_1V3WLNGD26F3EU.zip	2022-03-05 06:41	95K	
CA_[redacted]_2022-03-05 06:42:22_1V3WLNGD26F3EU.zip	2022-03-05 06:42	95K	
CA_[redacted]_2022-03-05 06:42:54_1V3WLNGD26F3EU.zip	2022-03-05 06:42	95K	
CA_[redacted]_2022-03-05 06:43:25_1V3WLNGD26F3EU.zip	2022-03-05 06:43	95K	
CA_[redacted]_2022-03-05 06:43:56_1V3WLNGD26F3EU.zip	2022-03-05 06:43	95K	
CA_[redacted]_2022-03-06 21:50:53_5FCJE3OH47GV37.zip	2022-03-06 21:50	89K	

Figure 8: Stolen Information

Below is an example of stolen information extracted from one of the folders. It’s quite self-explanatory:

- **Autofill** - Stores browser autofill data

- **CC** - Stores credit card information
- **Plugins** - Stores browser extension data: Metamask, Coinbase wallet, Binance, etc.
- **System.txt** - Stores infected system information such as IP, country code, timezone, etc.

Figure 9: Stolen information content

Mapping the Attack Infrastructure

Fortunately, the actor compromised his own computer with the Mars Stealer while debugging. This allowed us a rare peek into an operation by looking at his own stolen information—screenshots, passwords, history, system information, etc. Below is an image we generated to summarize the actor’s most relevant activity details.

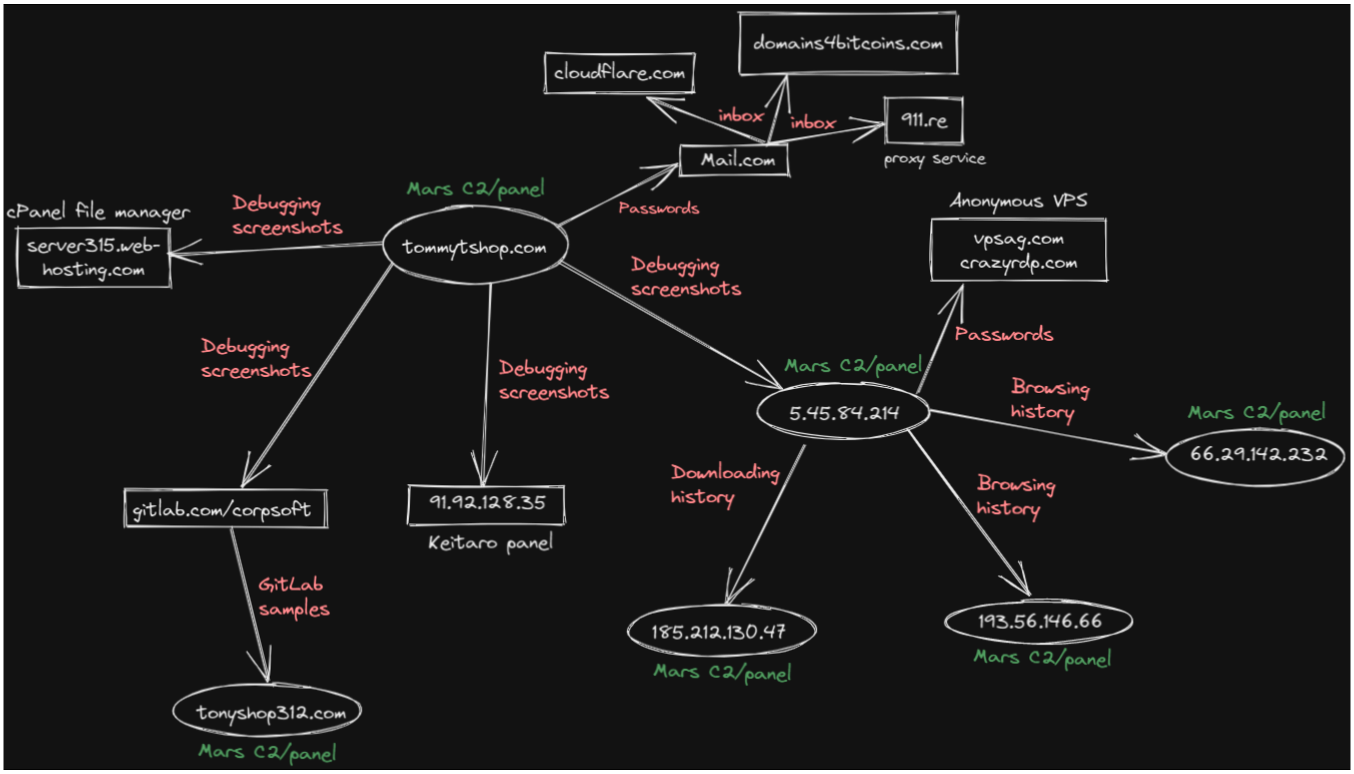
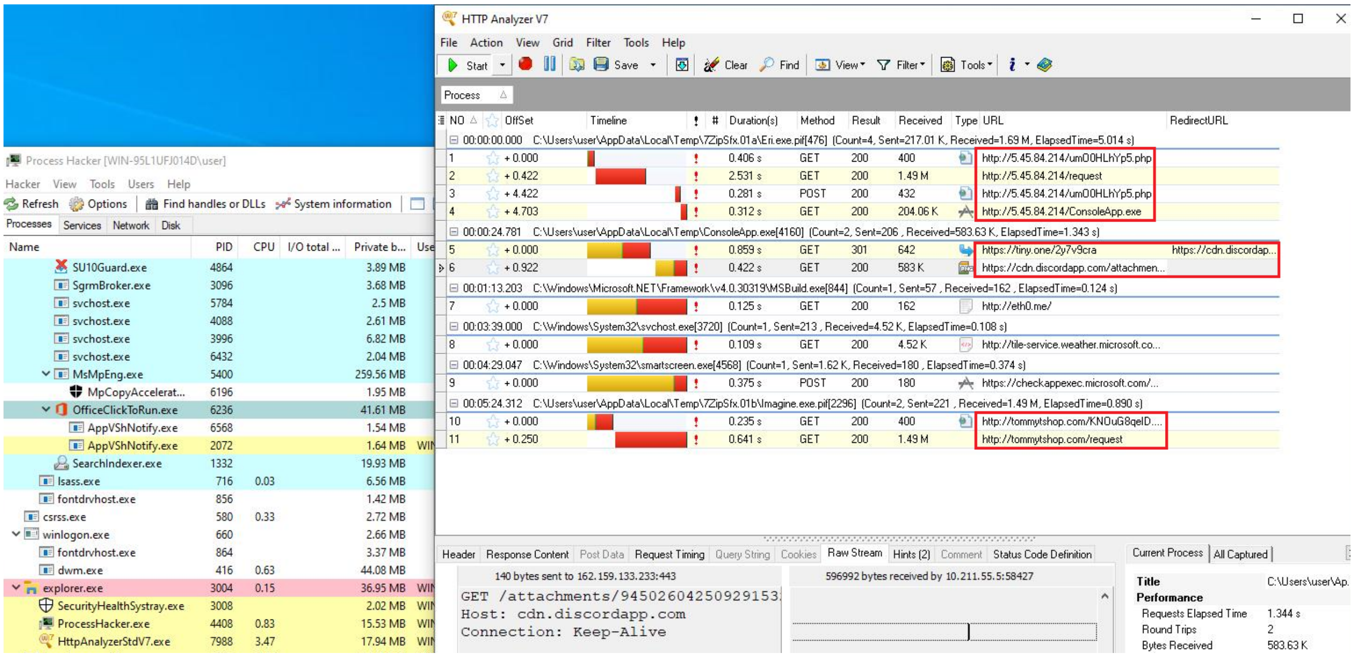


Figure 10: Recon diagram

We looked at the actor's screenshots and discovered they were debugging their Mars Stealer builds using HTTP Analyzer. This revealed their second Mars Stealer C2 - **http://5.45.84[.]214** which was improperly configured, similar to the first C2.



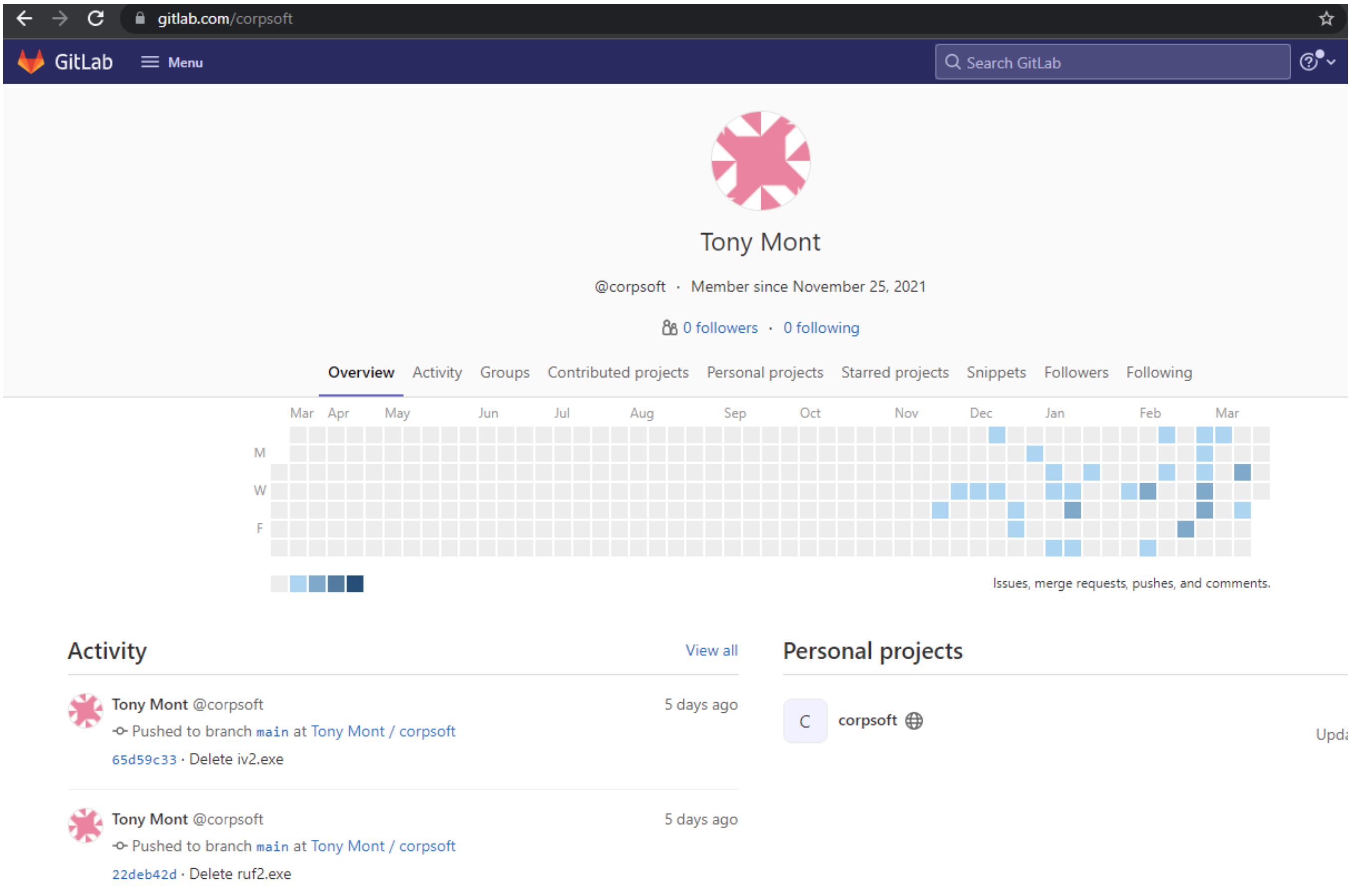
```
Process Hacker [WIN-95L1UFJ014D\user]

Name                        PID    CPU    I/O total ...   Private b...   Use
SU10Guard.exe               4864                          3.89 MB
SgrmBroker.exe              3096                          3.68 MB
svchost.exe                 5784                          2.5 MB
svchost.exe                 4088                          2.61 MB
svchost.exe                 3996                          6.82 MB
svchost.exe                 6432                          2.04 MB
MsMpEng.exe                 5400                          259.56 MB
  MpCopyAccelerat...        6196                          1.95 MB
OfficeClickToRun.exe        6236                          41.61 MB
  AppVShNotify.exe          6568                          1.54 MB
  AppVShNotify.exe          2072                          1.64 MB        WI
SearchIndexer.exe           1332                          19.93 MB
lsass.exe                   716    0.03                   6.56 MB
fontdrvhost.exe             856                           1.42 MB
csrss.exe                   580    0.33                   2.72 MB
winlogon.exe                660                           2.66 MB
  fontdrvhost.exe           864                           3.37 MB
  dwm.exe                   416    0.63                   44.08 MB
explorer.exe                3004   0.15                   36.95 MB       WI
  SecurityHealthSystray.exe 3008                          2.02 MB        WI
  ProcessHacker.exe         4408   0.83                   15.53 MB       WI
  HttpAnalyzerStdV7.exe     7988   3.47                   17.94 MB       WI
```

```
HTTP Analyzer V7

NO  OffSet   Duration(s)  Method  Result  Received  URL                                       RedirectURL
00:00:00.000  C:\Users\user\AppData\Local\Temp\7ZipSfx.01a\Eri.exe.pif[476]  (Count=4, Sent=217.01 K, Received=1.69 M, ElapsedTime=5.014 s)
1   + 0.000  0.406 s      GET     200     400       http://5.45.84.214/umOOHLhYp5.php
2   + 0.422  2.531 s      GET     200     1.49 M    http://5.45.84.214/request
3   + 4.422  0.281 s      POST    200     432       http://5.45.84.214/umOOHLhYp5.php
4   + 4.703  0.312 s      GET     200     204.06 K  http://5.45.84.214/ConsoleApp.exe
00:00:24.781  C:\Users\user\AppData\Local\Temp\ConsoleApp.exe[4160]  (Count=2, Sent=206 , Received=583.63 K, ElapsedTime=1.343 s)
5   + 0.000  0.859 s      GET     301     642       https://tiny.one/2y7v9cra                 https://cdn.discordap...
6   + 0.922  0.422 s      GET     200     583 K     https://cdn.discordapp.com/attachmen...
00:01:13.203  C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe[844]  (Count=1, Sent=57 , Received=162 , ElapsedTime=0.124 s)
7   + 0.000  0.125 s      GET     200     162       http://eth0.me/
00:03:39.000  C:\Windows\System32\svchost.exe[3720]  (Count=1, Sent=213 , Received=4.52 K, ElapsedTime=0.108 s)
8   + 0.000  0.109 s      GET     200     4.52 K    http://tile-service.weather.microsoft.co...
00:04:29.047  C:\Windows\System32\smartscreen.exe[4568]  (Count=1, Sent=1.62 K, Received=180 , ElapsedTime=0.374 s)
9   + 0.000  0.375 s      POST    200     180       https://checkappexec.microsoft.com/...
00:05:24.312  C:\Users\user\AppData\Local\Temp\7ZipSfx.01b\Imagine.exe.pif[2296]  (Count=2, Sent=221 , Received=1.49 M, ElapsedTime=0.890 s)
10  + 0.000  0.235 s      GET     200     400       http://tommytshop.com/KNOuG8qeID....
11  + 0.250  0.641 s      GET     200     1.49 M    http://tommytshop.com/request
```

```
140 bytes sent to 162.159.133.233:443
GET /attachments/94502604250929153
Host: cdn.discordapp.com
Connection: Keep-Alive

596992 bytes received by 10.211.55.5:58427

Title                    C:\Users\user\Ap.
Performance
  Requests Elapsed Time  1.344 s
  Round Trips            2
  Bytes Received         583.63 K
```

Figure 11: Actor's screenshot revealing additional C2

An additional screenshot led us to the actor's GitLab account, which was continuously updated with the latest Mars Stealer builds under the name of "Tony Mont," which has been active since late November 2021. We are assuming they do this for automation purposes.



Tony Mont

@corpsoft · Member since November 25, 2021

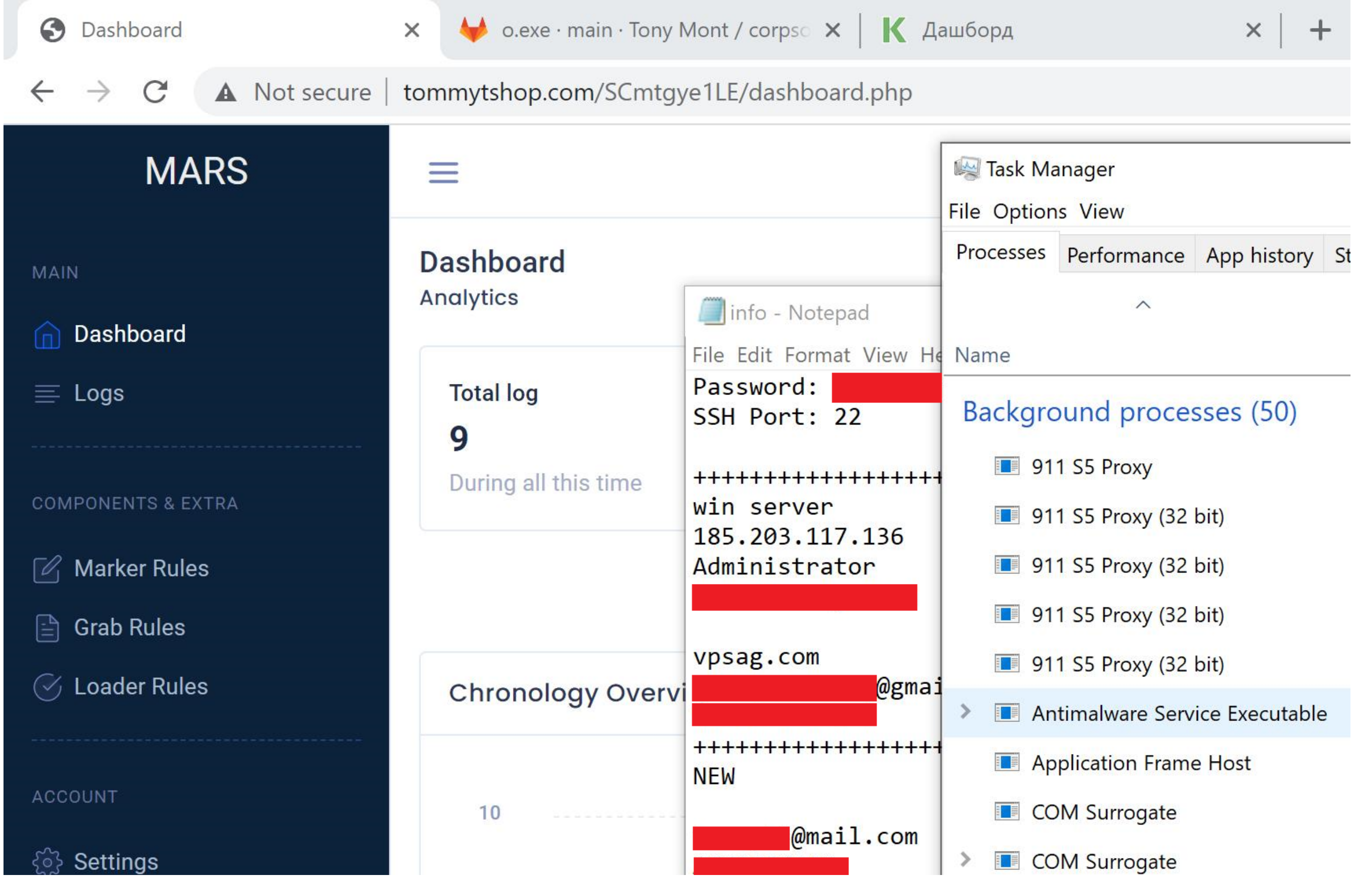
0 followers · 0 following

Tony Mont @corpsoft 5 days ago
Pushed to branch main at Tony Mont / corpsoft
65d59c33 · Delete iv2.exe

Tony Mont @corpsoft 5 days ago
Pushed to branch main at Tony Mont / corpsoft
22deb42d · Delete ruf2.exe

Figure 12: Actor's GitLab account

Another interesting screenshot revealed this actor stores their passwords in a plain text document for almost every service they're using.



Total log
9
During all this time

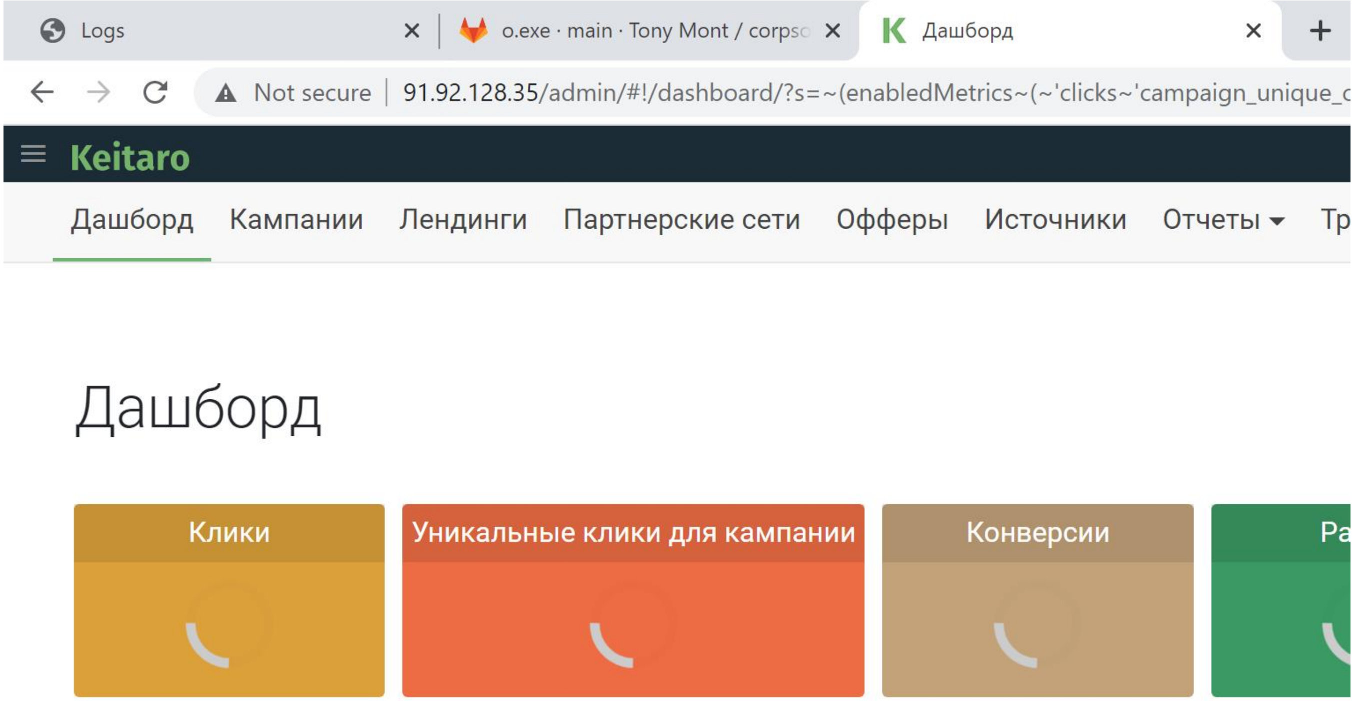
```
Password: [redacted]
SSH Port: 22

++++++++++++++++++
win server
185.203.117.136
Administrator
[redacted]

vpsag.com
[redacted]@gmai
[redacted]
++++++++++++++++++
NEW

[redacted]@mail.com
[redacted]
```

Background processes (50)

- 911 S5 Proxy
- 911 S5 Proxy (32 bit)
- 911 S5 Proxy (32 bit)
- 911 S5 Proxy (32 bit)
- 911 S5 Proxy (32 bit)
- Antimalware Service Executable
- Application Frame Host
- COM Surrogate
- COM Surrogate

Figure 13: Actor’s plain text passwords

The actor is also using Keitaro, a universal tracker for affiliate marketing. And the images below show the actor is a Russian speaker.



Logs
o.exe · main · Tony Mont / corpsc
Дашборд
Not secure
91.92.128.35/admin/#!/dashboard/?s=~(enabledMetrics~(~'clicks~'campaign_unique_c
Keitaro
Дашборд
Кампании
Лендинги
Партнерские сети
Офферы
Источники
Отчеты
Тр
Дашборд
Клики
Уникальные клики для кампании
Конверсии
Ра

Figure 14: Keitaro panel

The actor’s Google Ads platform page, paid for with stolen credentials.

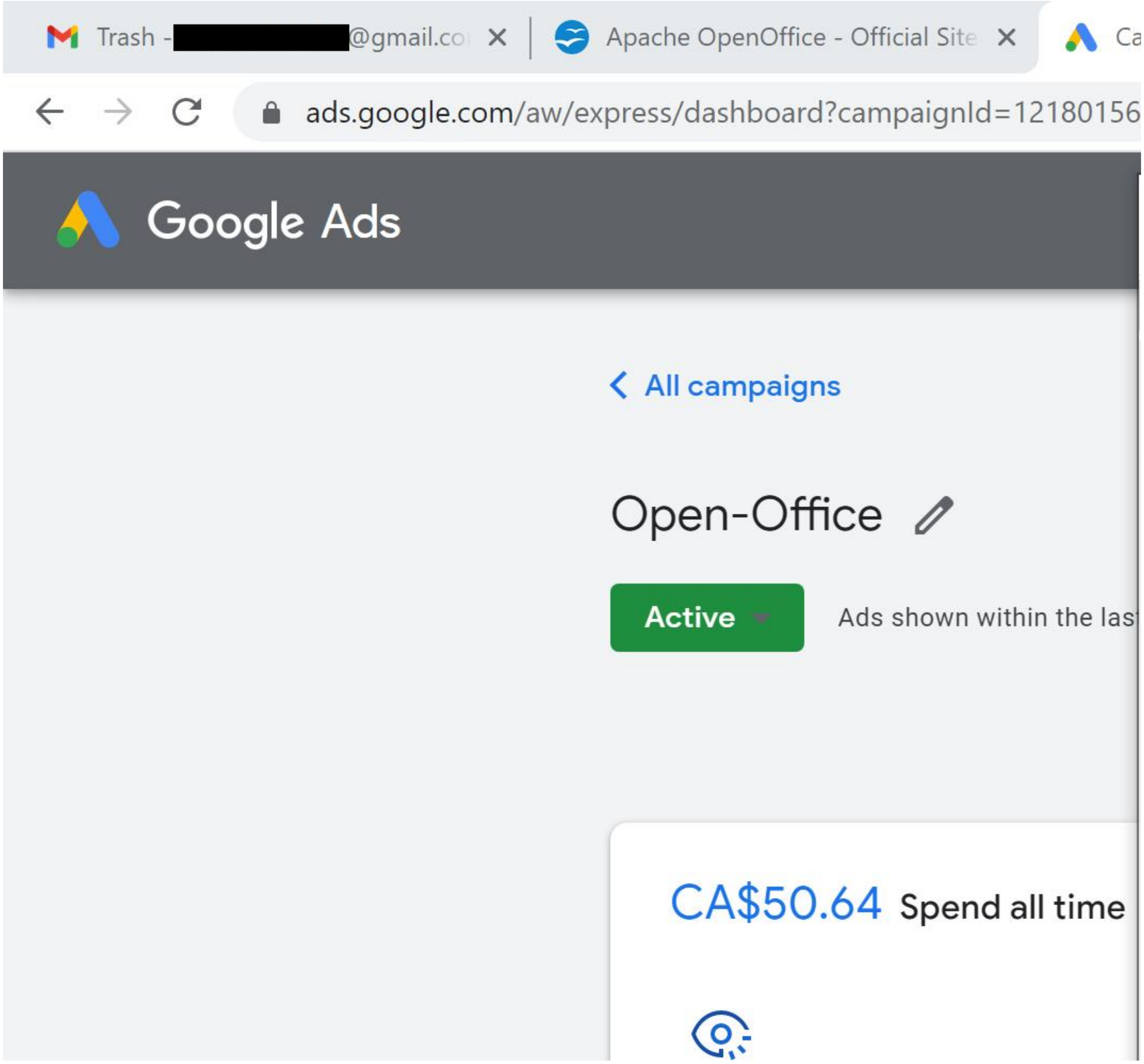

Trash - [redacted]@gmail.co
Apache OpenOffice - Official Site
Ca
ads.google.com/aw/express/dashboard?campaignId=12180156
Google Ads
All campaigns
Open-Office
Active
Ads shown within the las
CA$50.64 Spend all time

Figure 15: Actor’s Google Ads campaign

Attribution

We can safely attribute this actor as a Russian national by looking at the screenshots and keyboard details from the extracted **system.txt**.

Protect Yourself From Infostealers like Mars Stealer

Morphisec Labs will keep monitoring the Mars Stealer and provide updates when appropriate. Infostealers are used by a wide variety of cybercriminals, from novices to state-sponsored actors. They’re easy to acquire—and they work. Mars is currently being promoted in over 47 different underground forums, Darknet onion sites, and Telegram channels, and even has an official Telegram channel for purchasing through.

Morphisec protects against advanced attack chains such as those used in the Mars stealer. We do this with our patented Moving Target Defense (MTD) technology, which blocks advanced and zero-day attacks. MTD uses system polymorphism to hide application assets, operating system assets, and other critical assets from adversaries. This leads to unpredictable and dramatically reduced attack surfaces.

Gartner analysts call Moving Target Defense a “game-changer.” Learn more about Moving Target Defense and why Gartner cited this technology in its report: Emerging Trends and Technologies Impact Radar for Security.

Indicators of Compromise (IOCs)

Services

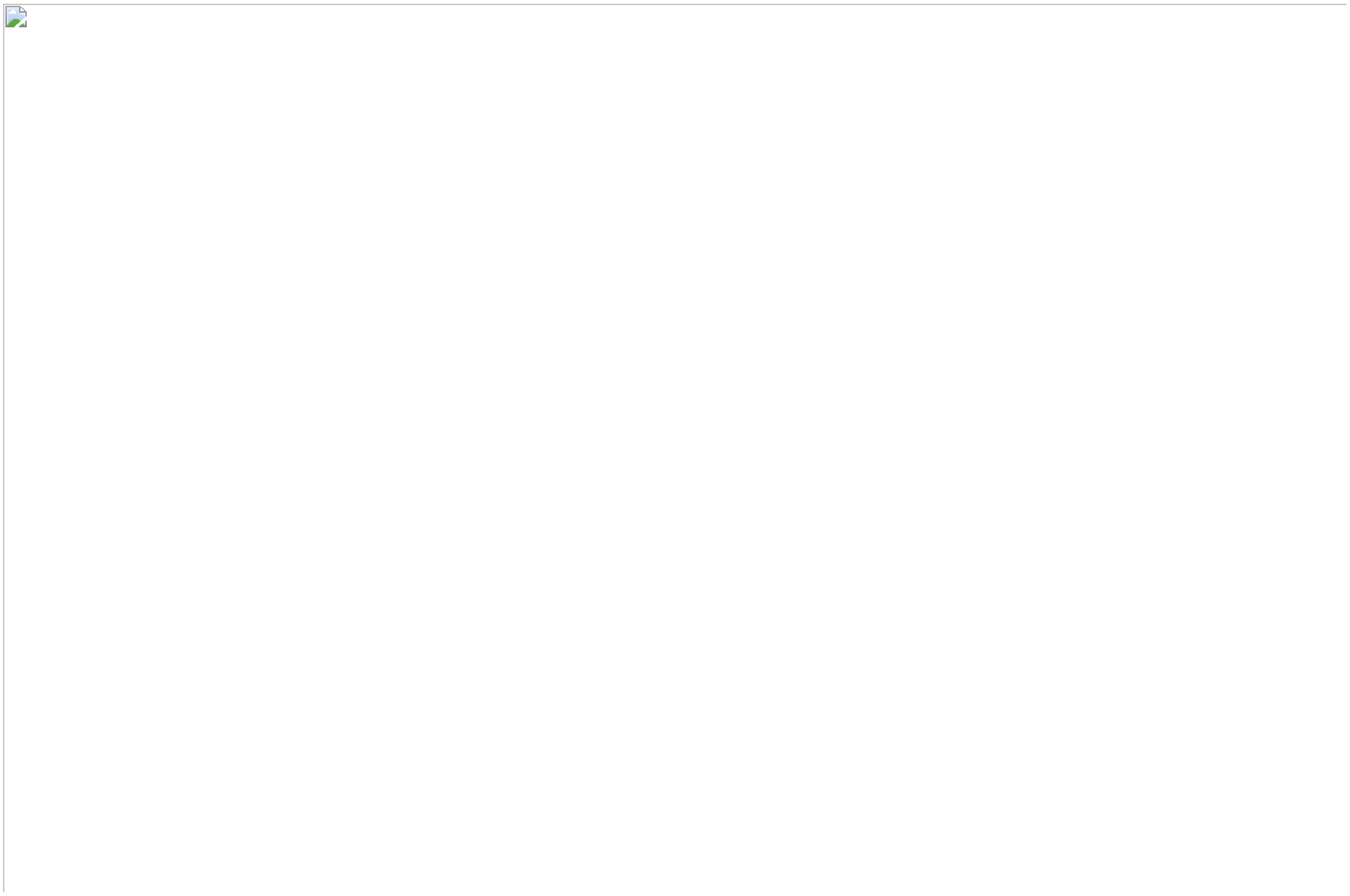
IP/URL	Service
91.92.128[.]35	Keitaro panel
https://gitlab.com/corpsoft	GitLab account
server315.web-hosting.com:2083	cPanel file manager

Mars C2

tommytshop[.]com
5.45.84[.]214
193.56.146[.]66
185.212.130[.]47
tonyshop312[.]com
66.29.142[.]232
telemeetrydata[.]cn

Samples (SHA256)

```
c48e5a61fd89ac5e950a37e1d81d2f733c16983d369dbedbb3a0c3e8c97f7b14
38807bc99d0f9a78480d3b12cfc96cdbfdb83bc277758595e77808b9b22ac087
bb48381955c8676b866760129db84ffce2e0b9c1fdd6a0179ab022dbf6fea708
cf1d4bf6b4a831d9664bbf0f40a609152a699f8d535c21e41ada406c47f63bfa
10731eea825c6bbcd5c543b2c98f4de384b36279cabba22fa247cda865c59093
af023cd8d2dcbeccfaf1970947217685931 54fc35019534a399563b011862a91
c26e405d1f07a9090e83454a7a978d5a89ef4764b00e7b354e6b2bb653e49378
9ed18a0b5e15bd4ecb73c5428e208b5d1b162274cfb0d6c62f7b5c3a04ec4d56
ab7e7d8594befb5a7137ec323db87a4aacfa64260327d61eee30626a760c3d5b
d5ee3a86821e452c33f178dc080aff7ca5054518a719ef74320909cbb55bb6c5
36613d674b4737da2b2986d9a49b48d06f1233cc7ea6aa7386bdb6d4bec90301
b15cb7537c9da026144ce35c70b21f72f81c8855b537c6ae987e785447e90f42
c3c1549bdd5613e9dbc3f09963cd1bd0f303b6f33bb4df62d9260590869cadec
8f925aa659cdab2466d2860dfc06d14d1c384c7a449683813db8d9219ed333c9
6929dae4d2bf6d2086bca0389e967f2c43bfb940da09b175b39df5fa1684a027
```



Contact SalesInquire via Azure