New Panda Stealer Targets Cryptocurrency Wallets

trendmicro.com/en_us/research/21/e/new-panda-stealer-targets-cryptocurrency-wallets-.html

May 4, 2021

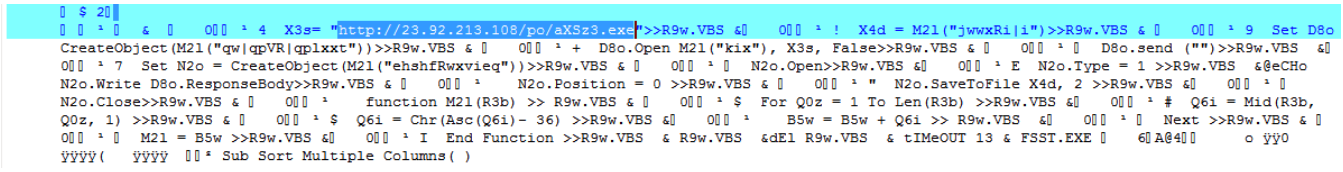

Figure 1. The macros script that downloads the Panda Stealer loader

The other infection chain involves an attached .XLS file containing an Excel formula that utilizes a PowerShell command (Figure 2) to access paste.ee, a Pastebin alternative, that accesses a second encrypted PowerShell command (Figure 3).

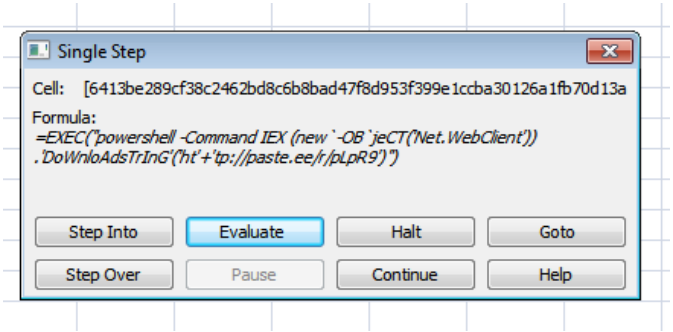

Figure 2. Excel formula accessing a paste.ee URL via PowerShell command

Figure 3. Encoded and decoded PowerShell script from a paste.ee URL

Decoding these PowerShell scripts revealed that they are used to access paste.ee URLs for easy implementation of fileless payloads. The CallByName export function in Visual Basic is used to call the load of a .NET assembly within memory from a paste.ee URL. The loaded assembly, obfuscated with an Agile.NET obfuscator, hollows a legitimate MSBuild.exe process and replaces it with its payload: the hex-encoded Panda Stealer binary from another paste.ee URL.

Once installed, Panda Stealer can collect details like private keys and records of past transactions from its victim's various digital currency wallets, including Dash, Bytecoin, Litecoin, and Ethereum. Not only does it target cryptocurrency wallets, it can steal credentials from other applications such as NordVPN, Telegram, Discord, and Steam. It's also capable of taking screenshots of the infected computer and exfiltrating data from browsers like cookies, passwords, and cards.

It drops files under %Temp% folder that stores stolen information under randomized file names, which are then sent to a command-and-control (C&C) server. Further analysis of its C&C server leads to a login page for "熊猫Stealer," which translates to "Panda Stealer" (Figure 4), but more domains have been identified with the same login page (Figure 5). Another 14 victims were discovered from the logs of one of these servers.

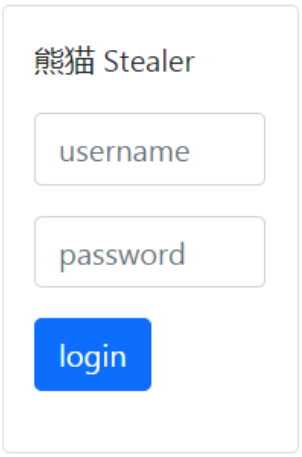

Figure 4. Possible login page for Panda Stealer

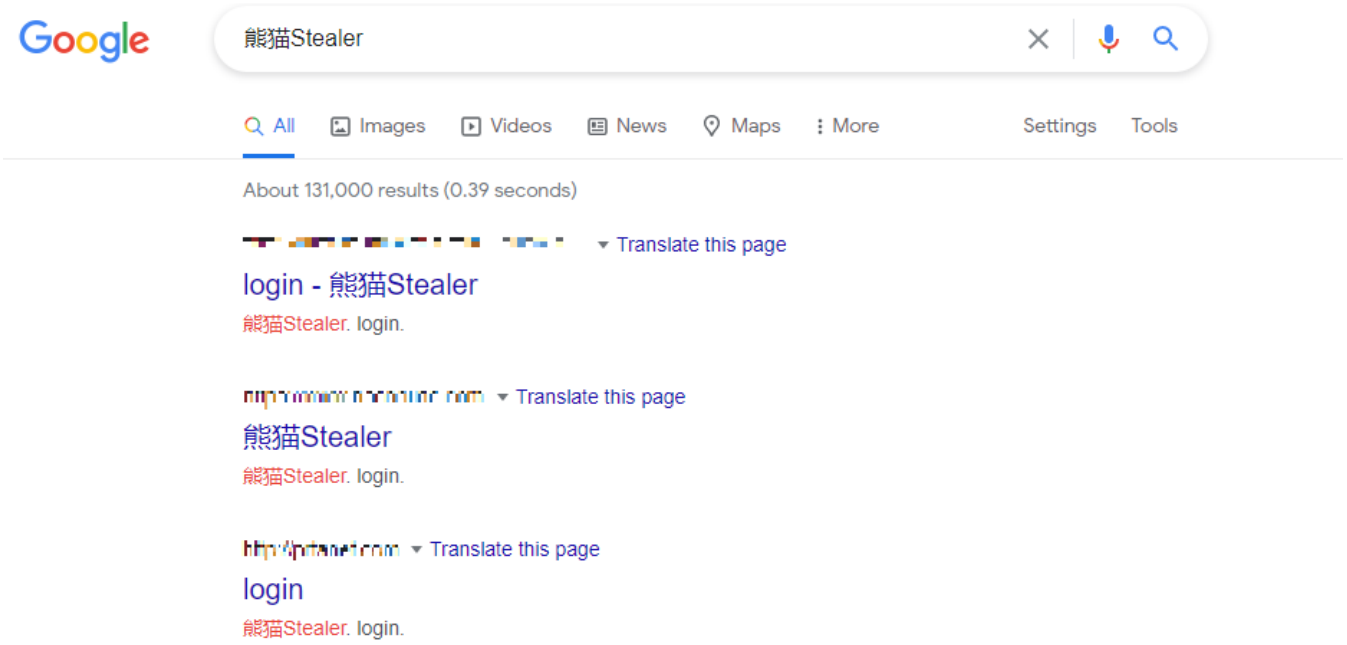

Figure 5. Other login pages called "熊猫Stealer"

Another 264 files similar to Panda Stealer were found on VirusTotal. More than 140 C&C servers (Table 1) and over 10 download sites were used by these samples. Some of the download sites were from Discord, containing files with names such as "build.exe," which indicates that threat actors may be using Discord to share the Panda Stealer build.

Some of the aforementioned download sites are listed below:

- hxxp://23.92.213.108/po/tai1.exe
- hxxp://83.220.175.66/build.exe
- hxxps://bingoroll2.net/chirik.exe
- hxxp://bingoroll2.net/chirik.exe

- hxxp://cryptojora.club/sosi.exe
- hxxp://f0522235.xsph.ru/build.exe
- hxxp://f0522235.xsph.ru/build2.exe
- hxxp://f0522235.xsph.ru/build.exe
- hxxp://micromagican.com/chirik.exe
- hxxp://repairyou.com/henry.exe
- hxxp://traps.ml/build.exe
- hxxp://tydaynsosi.ru/loader/23/1kwo.txt
- hxxp://tydaynsosi.ru/loader/23/1tgk.txt

C&C servers	Occurrence per unique file
hxxp://cocojambo.collector-steal.ga/collect.php	73
hxxp://f0522235.xsph.ru/collect.php	4
hxxp://guarantte.xyz/collect.php	3
hxxp://f0527189.xsph.ru/collect.php	3
hxxp://f0527703.xsph.ru/collect.php	2
hxxp://j1145058.myjino.ru/collect.php	2
hxxp://1wftyu121cwr24v3hswa1234g.tk/collect.php	2
hxxp://f0527262.xsph.ru/collect.php	2
hxxp://steammd0.beget.tech/collect.php	2

Table 1. The top C&C servers used by files that are similar to Panda Stealer

Attribution

Based on one of the active C&C servers (Figure 6), we have identified an IP address that we believe was used by the threat actor. We believe that this address is assigned to a virtual private server (VPS) rented from Shock Hosting, which the actor infected for testing purposes. The VPS may be paid for using cryptocurrency to avoid being traced and uses the online service Cassandra Crypter (Figure 7). We have reported this to Shock Hosting, and they confirmed that the server assigned to this IP address has been suspended.

Another infected machine was discovered with a history of visiting a Google Drive link, which is also mentioned in a discussion about AZORult log extractor on an underground forum. The same link and unique cookie were observed on both the log dumps and the forum, therefore the user who posted on the forum must also have access to that log file.

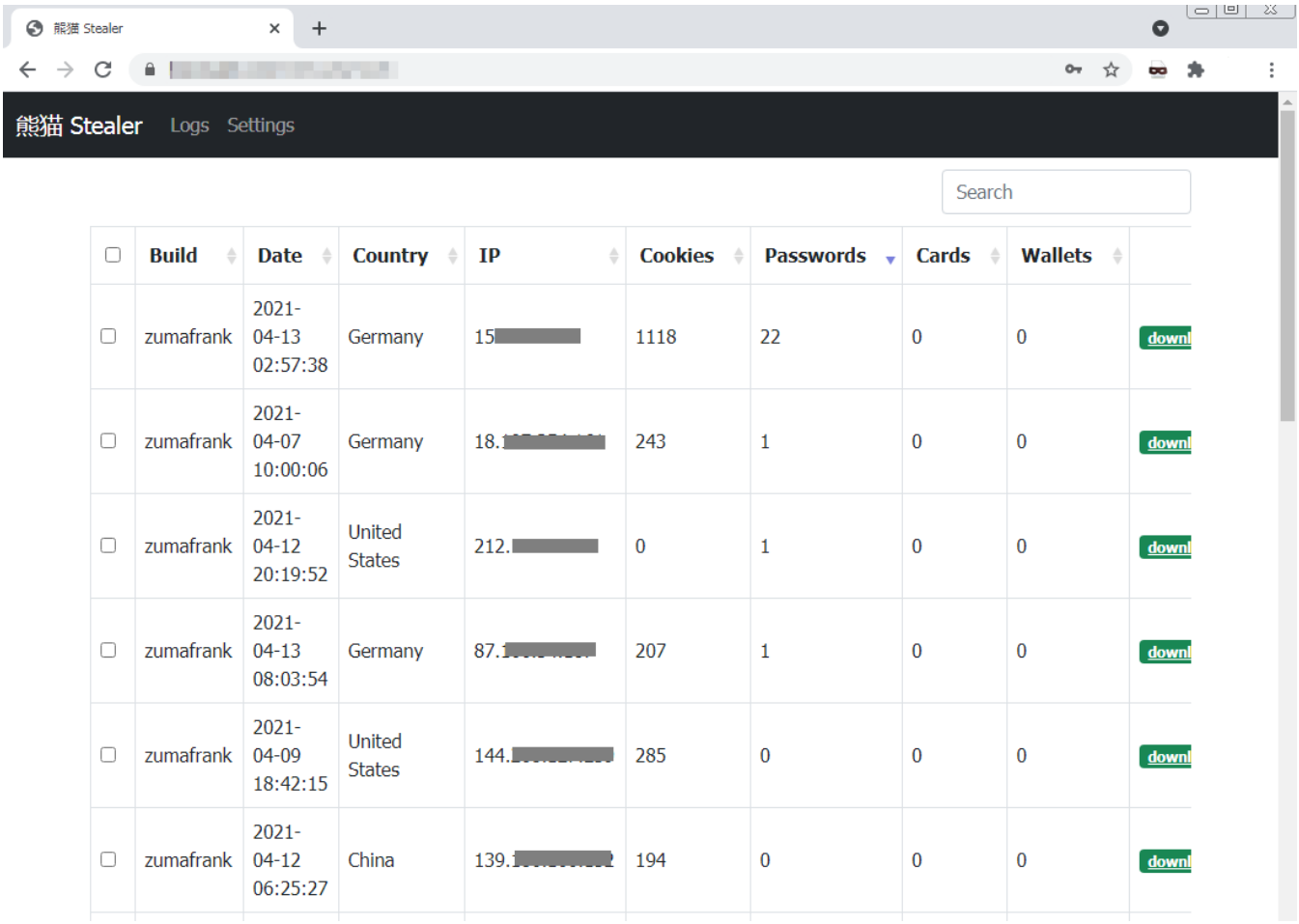

Figure 6. Control panel of an active C&C server

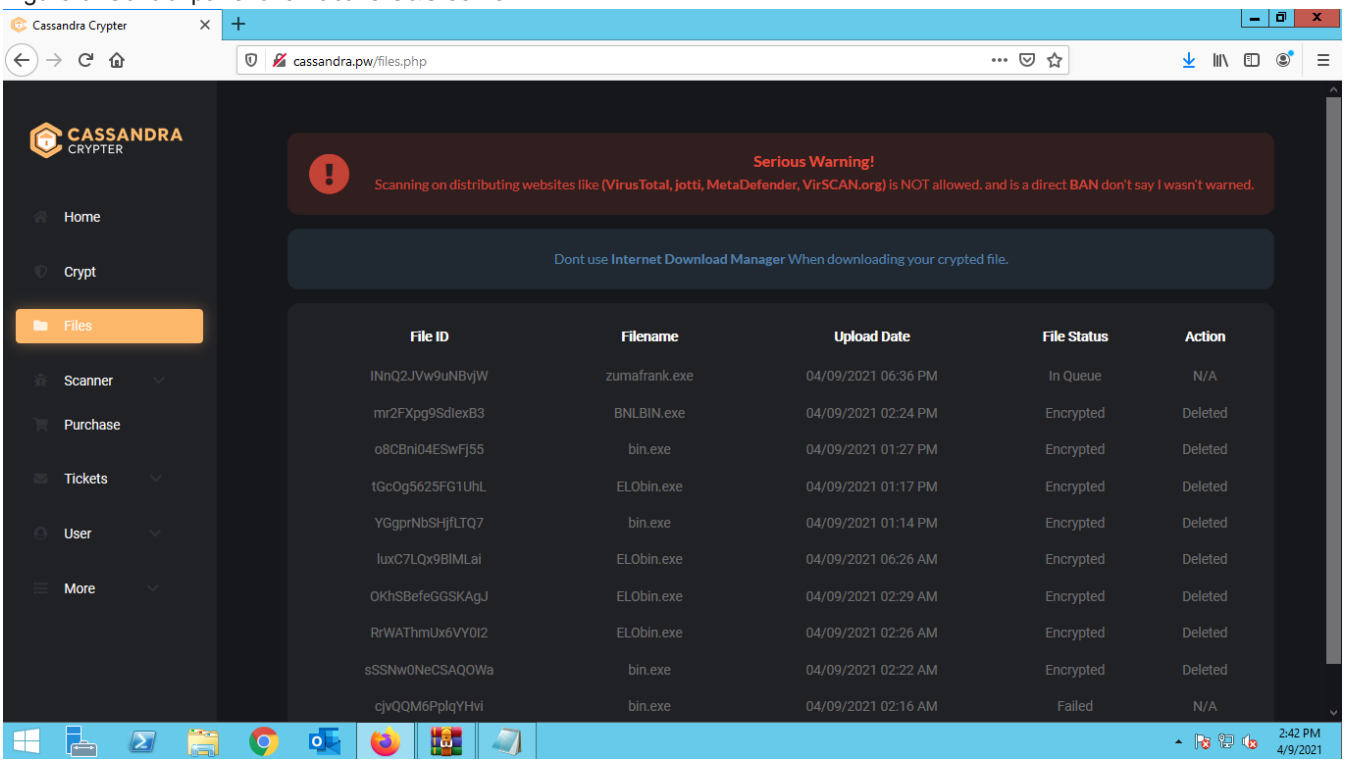

Figure 7. Screenshot taken of the threat actor using Cassandra Crypter

Similarities with other stealers

Panda Stealer was found to be a variant of Collector Stealer, which has been sold on some underground forums and a Telegram channel (Figure 8). Collector Stealer has since been cracked by a Russian threat actor called NCP, also known as su1c1de. Comparing the compiled executables of the cracked Collector Stealer and Panda Stealer shows that the two behave similarly, but have different C&C URLs, build tags, and execution folders (Figure 9). Like Panda Stealer, Collector Stealer exfiltrates information like cookies, login data, and web data from a compromised computer, storing them in an SQLite3 database. It also covers its tracks by deleting its stolen files and activity logs after its execution (Figure 10).

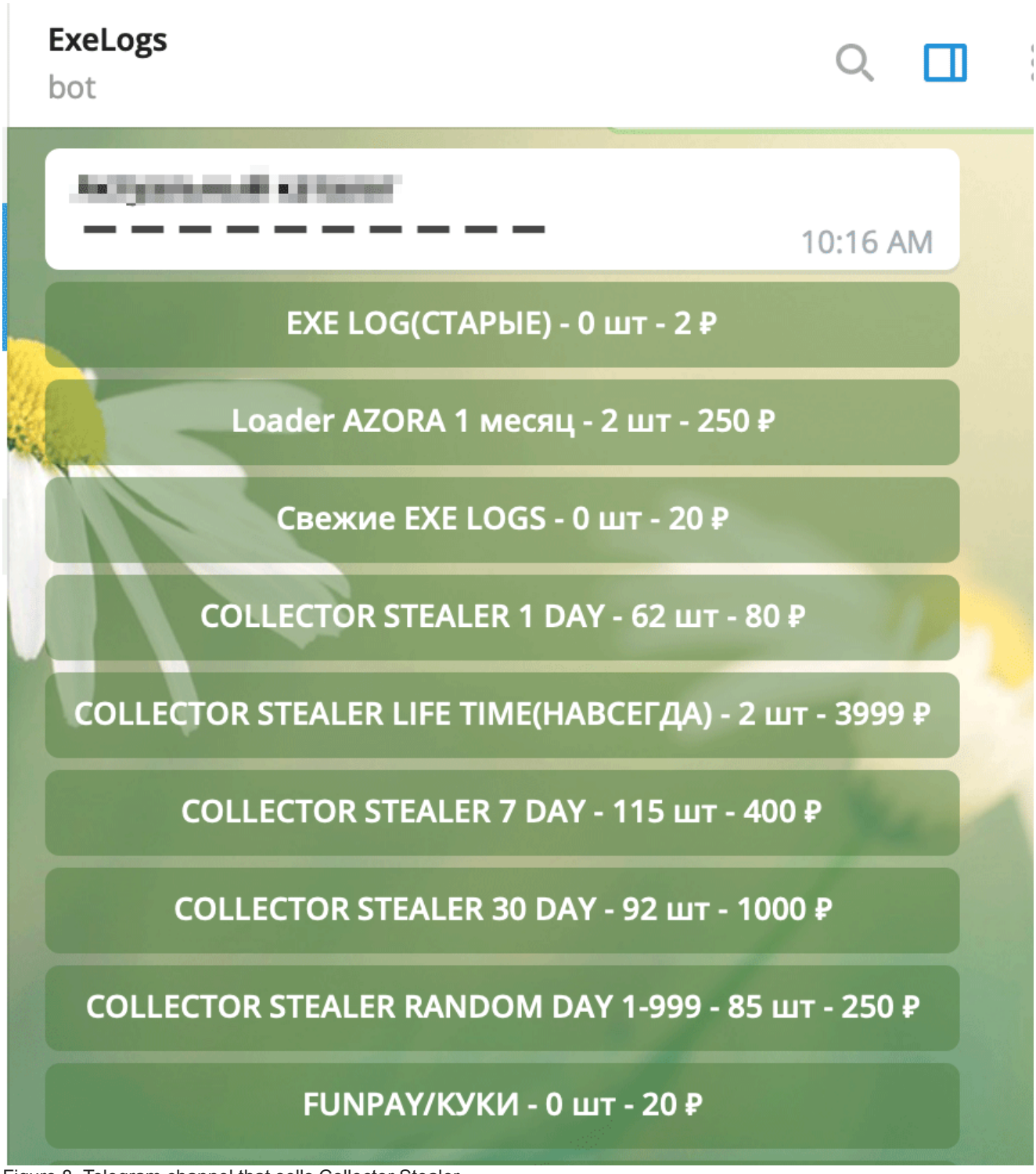

Figure 8. Telegram channel that sells Collector Stealer

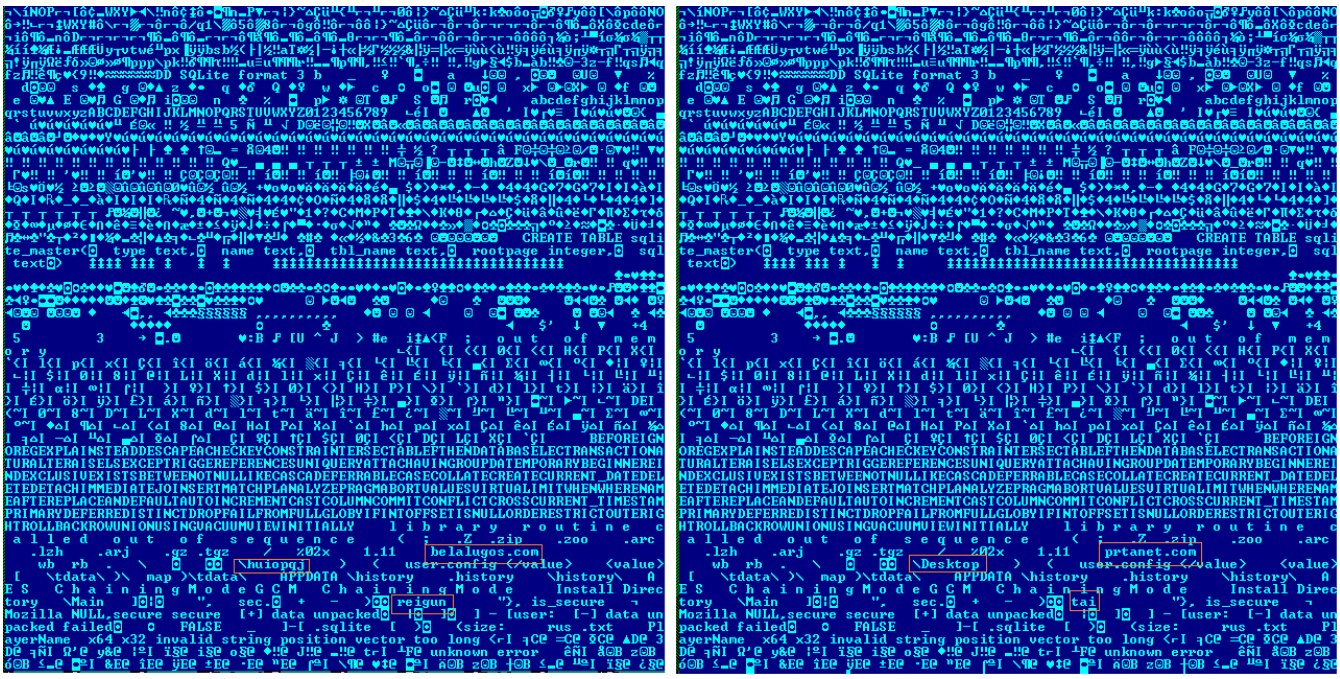

Figure 9. The compiled executable of the cracked Collector Stealer (left) and the Panda Stealer sample (right)

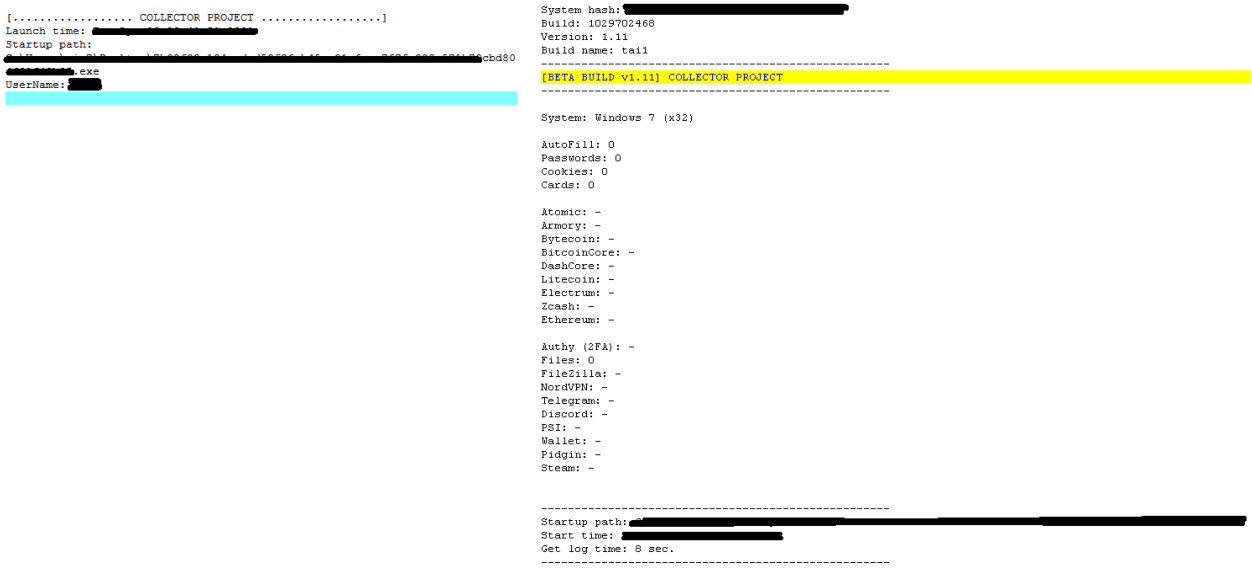

Figure 10. The activity logs of an earlier Collector Stealer version (left) and Panda Stealer (right)

Because the cracked Collector Stealer builder is openly accessible online, cybercriminal groups and script kiddies alike can use it to create their own customized version of the stealer and C&C panel. Threat actors may also augment their malware campaigns with specific features from Collector Stealer. We have also discovered that Panda Stealer has an infection chain that uses the same fileless distribution method as the "Fair" variant of Phobos ransomware to carry out memory-based attacks, making it more difficult for security tools to spot.

Protect your network from spammed threats

To protect systems against fileless threats that use spam emails as vectors, enterprises can use the Trend Micro endpoint solutions such as Trend Micro Smart Protection Suites and Worry-Free™ Business Security. Both solutions protect users and businesses from threats by detecting malicious files and spammed messages and blocking all related malicious URLs.

Indicators of compromise

There were numerous files, domains, and IP addresses that were involved in this attack. Trend Micro has provided detection for the malicious artifacts found in this investigation. A partial list of the notable items is detailed below:

SHA256	Trend Micro Detection Name

6413be289cf38c2462bd8c6b8bad47f8d953f399e1ccba30126a1fb70d13a733	Trojan.X97M.PANDASTEAL.AA
4ff1f8a052addbc5a0388dfa7f32cc493d7947c43dc7096baa070bfc4ae0a14e	Trojan.Win32.PHOBOS.B
0a9f466fb5526fd512dd48c3ba9551dbd342bdb314a87d5c6f730d3c80041da6	TrojanSpy.X97M.PANDASTEAL.THDABBA
05d38ac5460418b0aa813fc8c582ee5be42be192de10d188332901157c54287c	TrojanSpy.Win32.PANDASTEAL.THDABBA
1efa74e72060865ff07bda90c4f5d0c470dd20198de7144960c88cef248c4457	TrojanSpy.Win32.PANDASTEAL.THDABBA

URLs

- hxxp://23.92.213.108/po/aXSz3[.]exe
- hxxp://23.92.213.108/po/tai1[.]exe
- hxxp://prtboss.com/collect[.]php
- hxxp://biscosuae[.]com
- hxxp://prtanet[.]com
- hxxps://paste.ee/r/pLpR9
- hxxps://paste.ee/r/Qsowz
- hxxps://paste.ee/r/6toiY
- hxxp://cocojambo.collector-steal.ga/collect.php
- hxxp://f0522235.xsph.ru/collect.php
- hxxp://guarantte.xyz/collect.php
- hxxp://f0527189.xsph.ru/collect.php
- hxxp://f0527703.xsph.ru/collect.php
- hxxp://j1145058.myjino.ru/collect.php
- hxxp://1wftyu121cwr24v3hswa1234g.tk/collect.php
- hxxp://f0527262.xsph.ru/collect.php

Malware

In early April, we observed a new information stealer called Panda Stealer being delivered via spam emails. Based on Trend Micro's telemetry, United States, Australia, Japan, and Germany were among the most affected countries during a recent spam wave.

By: Monte de Jesus, Fyodor Yarochkin, Paul Pajares May 04, 2021 Read time: (words)