

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.

<input type="checkbox"/>	Build	Date	Country	IP	Cookies	Passwords	Cards	Wallets	
<input type="checkbox"/>	zumafrank	2021-04-13 02:57:38	Germany	15.██████████	1118	22	0	0	download
<input type="checkbox"/>	zumafrank	2021-04-07 10:00:06	Germany	18.██████████	243	1	0	0	download
<input type="checkbox"/>	zumafrank	2021-04-12 20:19:52	United States	212.██████████	0	1	0	0	download
<input type="checkbox"/>	zumafrank	2021-04-13 08:03:54	Germany	87.██████████	207	1	0	0	download
<input type="checkbox"/>	zumafrank	2021-04-09 18:42:15	United States	144.██████████	285	0	0	0	download
<input type="checkbox"/>	zumafrank	2021-04-12 06:25:27	China	139.██████████	194	0	0	0	download

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

Serious Warning!
Scanning on distributing websites like (Virus Total, jotti, MetaDefender, VirSCAN.org) is NOT allowed, and is a direct BAN don't say I wasn't warned.

Dont use Internet Download Manager When downloading your crypted file.

File ID	Filename	Upload Date	File Status	Action
INnQ2JvW9uNBvjW	zumafrank.exe	04/09/2021 06:36 PM	In Queue	N/A
mr2FXpg9SdlexB3	BNLBIN.exe	04/09/2021 02:24 PM	Encrypted	Deleted
o8CBni04ESwfj55	bin.exe	04/09/2021 01:27 PM	Encrypted	Deleted
1GcOg5625FG1UHL	ELObin.exe	04/09/2021 01:17 PM	Encrypted	Deleted
YGgprNBSHjflTQ7	bin.exe	04/09/2021 01:14 PM	Encrypted	Deleted
luxC7LQx9BIMLal	ELObin.exe	04/09/2021 06:26 AM	Encrypted	Deleted
OKhSBefeGGSKAjJ	ELObin.exe	04/09/2021 02:29 AM	Encrypted	Deleted
RrWATHmUx6vY0i2	ELObin.exe	04/09/2021 02:26 AM	Encrypted	Deleted
sSSNw0NeCSAQOWa	bin.exe	04/09/2021 02:22 AM	Encrypted	Deleted
cjvQQM6PplqYHvi	bin.exe	04/09/2021 02:16 AM	Failed	N/A

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](#) open on a new tab, 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](#) open on a new tab. 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).

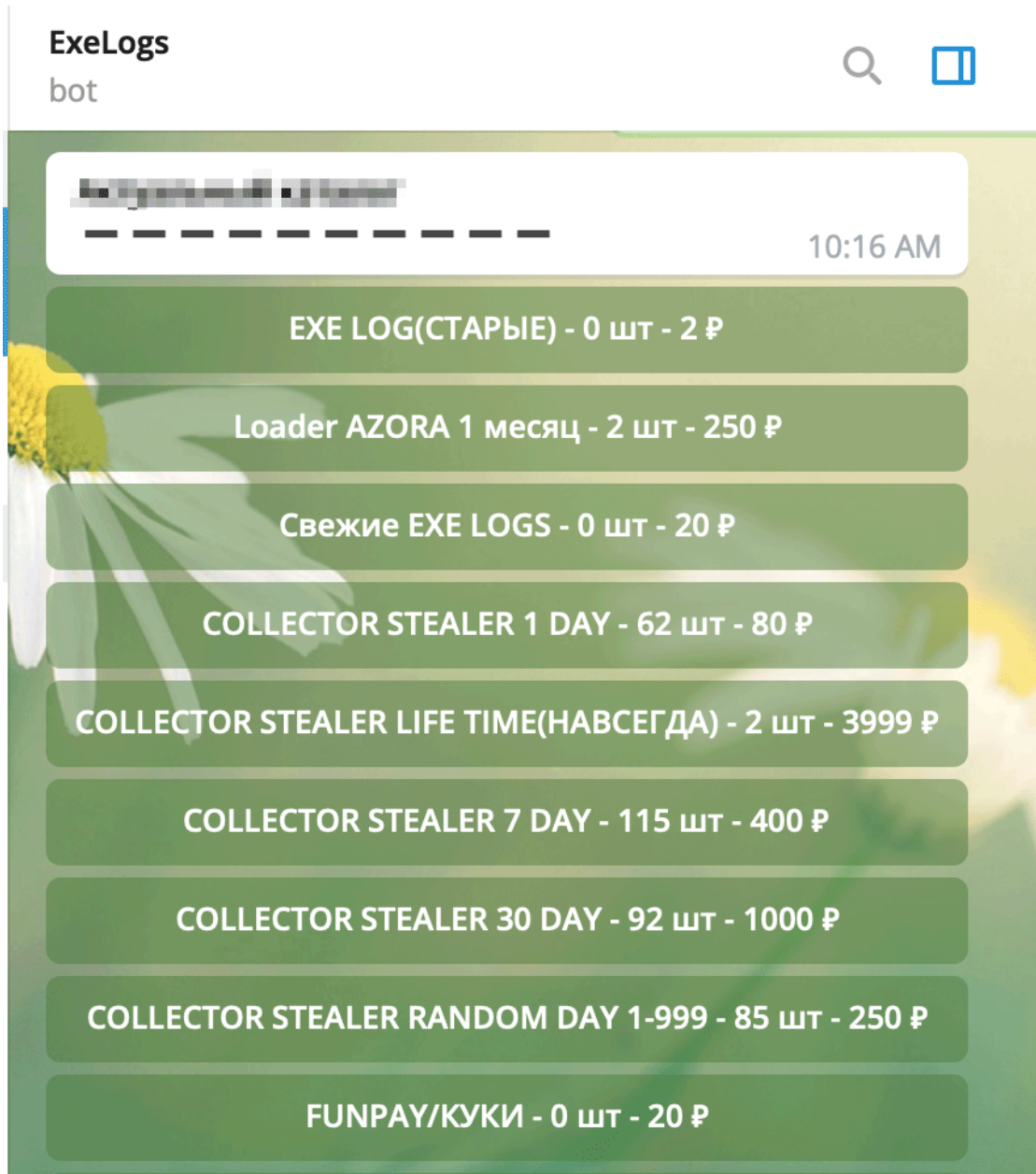


Figure 8. Telegram channel that sells Collector Stealer

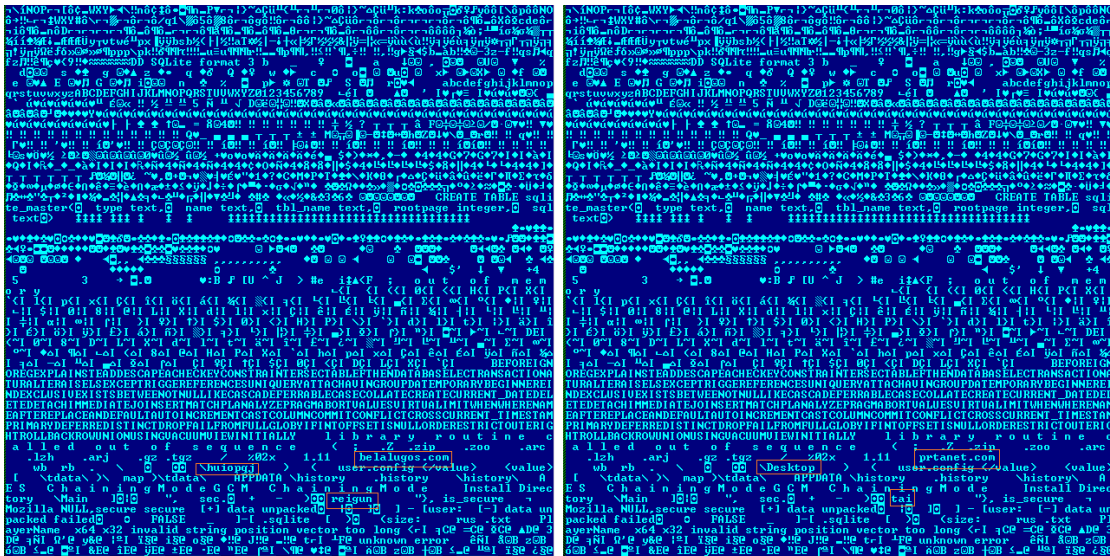


Figure 9. The compiled executable of the cracked Collector Stealer (left) and the Panda Stealer sample (right)

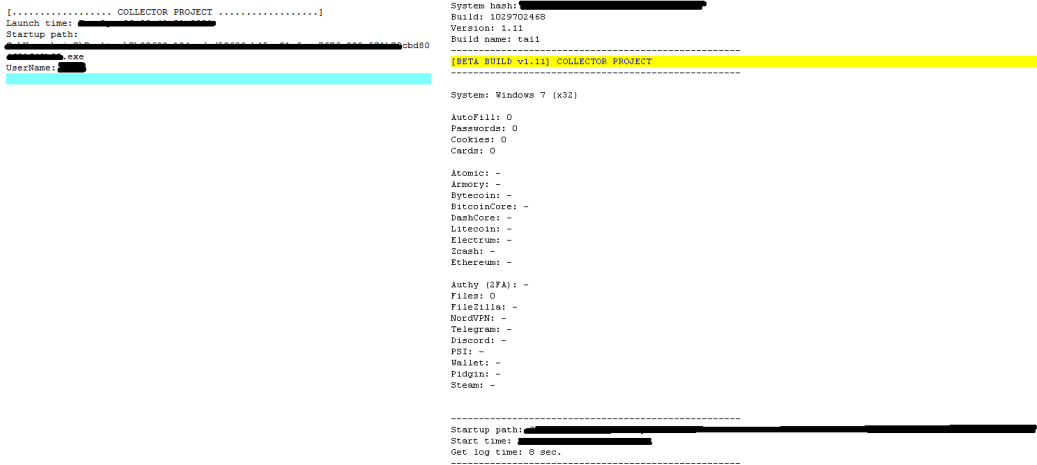


Figure 10. The activity logs of an earlier Collector Stealer version (left) and Panda Stealer (right)

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 [open on a new tab](#) 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](#) products 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.THADABBA
05d38ac5460418b0aa813fc8c582ee5be42be192de10d188332901157c54287c	TrojanSpy.Win32.PANDASTEAL.THADABBA
1efa74e72060865ff07bda90c4f5d0c470dd20198de7144960c88cef248c4457	TrojanSpy.Win32.PANDASTEAL.THADABBA

URLs

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

Tags

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