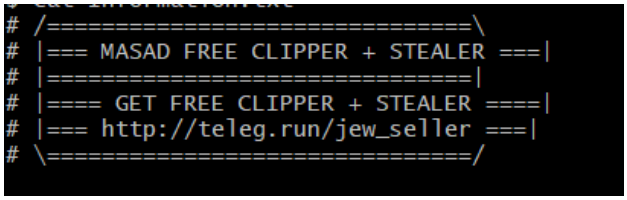
Masad Stealer: Exfiltrating using Telegram

blogs.juniper.net/en-us/threat-research/masad-stealer-exfiltrating-using-telegram

September 26, 2019



Juniper Threat Labs discovered a new Trojan-delivered spyware that uses Telegram to exfiltrate stolen information. Using Telegram as a Command and Control (C&C) channel allows the malware some anonymity, as Telegram is a legitimate messaging application with 200 million monthly active users.

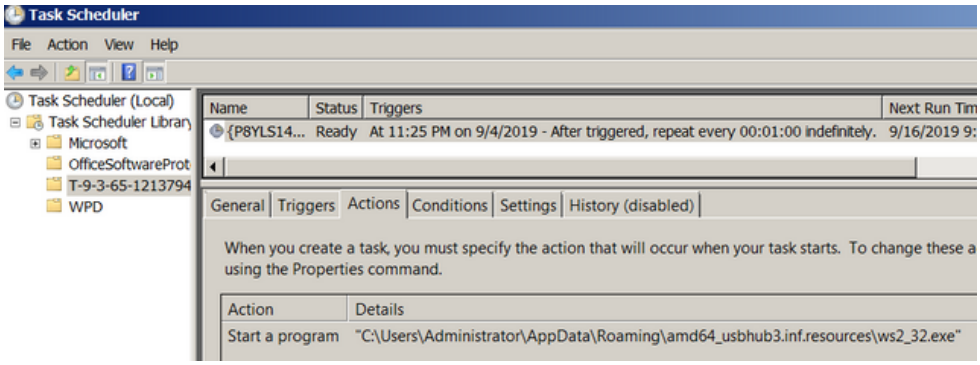
The malware is being advertised on black market forums as “Masad Clipper and Stealer.” It steals browser data, which might contain usernames, passwords and credit card information. Masad Stealer also automatically replaces cryptocurrency wallets from the clipboard with its own.

Masad Stealer sends all of the information it collects – and receive commands from – a Telegram bot controlled by the threat actor deploying that instance of Masad. Because Masad is being sold as off-the-shelf malware, it will be deployed by multiple threat actors who may or may not be the original malware writers.

What it does

This malware is written using Autoit scripts and then compiled into a Windows executable. Most samples we have seen are about 1.5 MiB in size, however, Masad Stealer can be found in larger executables as it is sometimes bundled into other software.

When Masad Stealer is executed, it drops itself in %APPDATA%\folder_name}\{file_name}, where folder_name and file_name are defined in the binary. Examples include amd64_usbhub3.inf.resources and ws2_32.exe, respectively. As a persistence mechanism, mMasad Stealer creates a scheduled task that will start itself every one minute.



Masad stealer using scheduled task as persistence mechanism

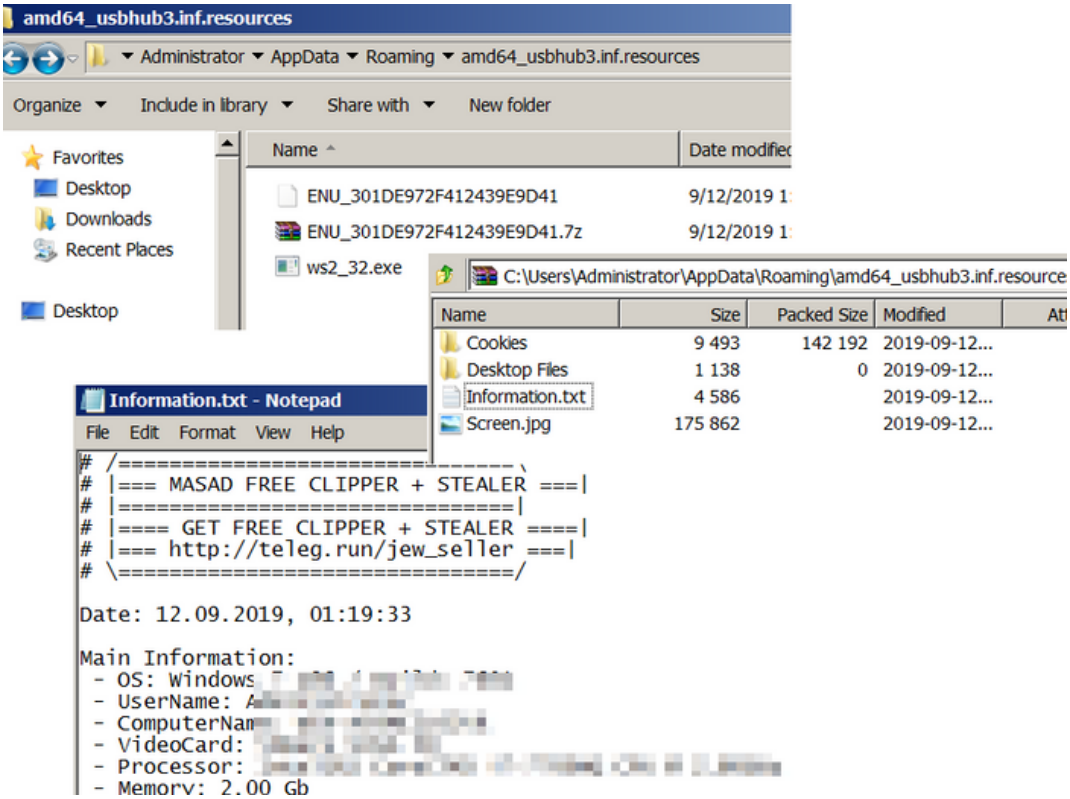
Stealing routine

After installing itself, Masad Stealer starts by collecting sensitive information from the system, such as:

- Cryptocurrency Wallets
- PC and system information
- Credit Card Browser Data
- Browser passwords
- Installed software and processes
- Desktop Files
- Screenshot of Desktop
- Browser cookies

- Steam files
- AutoFill browser fields
- Discord and Telegram data
- FileZilla files

It zips this information into a file using 7zip utility, which is bundled into the malware binary.



A screenshot of what this malware have exfiltrated on one test machine

The above screenshot is a view of what Masad Stealer tries to exfiltrate from a sandbox. But the data that it can exfiltrate can expand to the following list:

```
Content: @CRLF \1\Passwords.txt - Passwords
@CRLF \1\Information.txt - Information
@CRLF \1\Screen.jpg - Screen
@CRLF \1\AutoFills.txt - AutoFills
@CRLF \1\CreditCards.txt - Credit Cards
@CRLF \1\Cookies - Cookies
@CRLF \1\Desktop Files - Desktop Files
@CRLF \1\Discord - Discord
@CRLF \1\Telegram - Telegram
@CRLF \1\Steam - Steam
@CRLF \1\Exodus - Exodus
@CRLF \1\Jaxx - Jaxx
@CRLF \1\Electrum - Electrum
@CRLF \1\Wallets - Wallets
@CRLF \1\FileZilla - FileZilla
@CRLF \1\SDA - SDA
@CRLF \1\Passwords.txt
```

A list of information that this malware can steal

Using a hardcoded bot token, which is basically a way to communicate with the Command and Control bot, Masad Stealer sends this zip file using the **sendDocument** API.

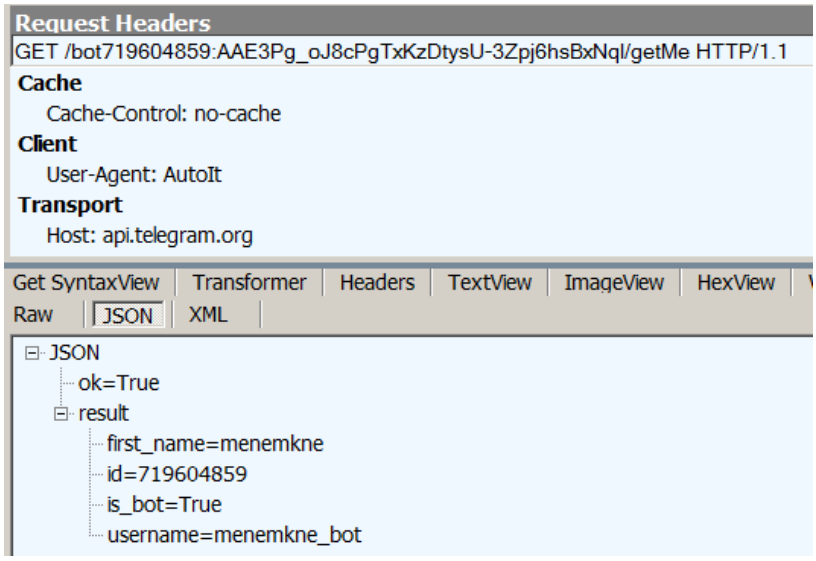
sendDocument

Use this method to send general files. On success, the sent Message is returned. Bots can currently send files of any type of up to 50 MB in size, this limit may be changed in the future.

Parameter	Type	Required	Description
chat_id	Integer or String	Yes	Unique identifier for the target chat or username of the target channel (in the format `@channelusername`)

A snip of sendDocument telegram bot API that this malware used to exfiltrate data

In order to communicate with the Command and Control bot, Masad Stealer first sends a getMe message using the bot token to be able to confirm that the bot is still active. Upon receiving this request, the bot replies with the user object that contains the username of the bot. This username object is useful for identifying possible threat actors related to this malware. This is an important consideration because of the off-the-shelf nature of this malware – multiple parties will be operating Masad Stealer instances for different purposes.



Initial request by the malware to the telegram bot to make sure it is active.

Where the bot's token is **"719604859:AAE3Pg_oJ8cPgTxKzDtysU-3Zpj6hsBxNql".**

Clipping Routine

This malware includes a function that replaces wallets on the clipboard, as soon as it matches a particular configuration. Below are the regular expressions and supported wallets that it matches against the clipboard data:

```
XMR2[1-9A-z]{105}
BCNDdzFFzCqrht[1-9A-z]{93}
ADA[48][1-9A-z]{94}
XMR2[1-9A-z]{94}
BCNG[1-9][1-9A-z]{93}
GRFTsteamcommunity[.]com/tradeoffer/new/[?]partner=[0-9]{9}&token=[A-z0-9_]{8}
Steam0x[0-9A-z]{40}
ETHq[a-z0-9]{41}
BCHt1[0-9A-z]{33}
ZCASH3P[1-9A-z]{33}
WAVES[13][1-9A-Z][1-9A-z]{32}
BTC[1][1-9A-Z][1-9A-z]{32}
BTC[3][1-9A-Z][1-9A-z]{32}
BTC3G[A-z][1-9A-z]{32}
BTGX[a-z][1-9A-z]{32}
DASH[LM][A-z][1-9A-z]{32}
LTCD[A-Z1-9][1-9A-z]{32}
DOGER[1-9a-z][1-9A-z]{32}
RDDB[1-9a-z][1-9A-z]{32}
BLKE[A-z][1-9A-z]{32}
EMCr[A-z][1-9A-z]{32}
XRPA[A-Z][1-9A-z]{32}
NEOS[A-z][1-9A-z]{32}
STRATQ[A-z][1-9A-z]{32}
QTUMV[a-z][A-z][1-9A-z]{31}
VIA[0-9]{20}
LLSK41001[0-9]{10}
Yandex MoneyR[0-9]{12}
WMRG[0-9]{12}
WMGZ[0-9]{12}
WMZH[0-9]{12}
WMHU[0-9]{12}
WMUX[0-9]{12}
WMX380[0-9]{9}
QIWI79[0-9]{9}
QIWIP[0-9]{9}
PAYEERP[0-9]{8}
```

A list of wallet and corresponding regular expressions that it monitors on the clipboard

Below is a list of coins/wallet it tries to clip:

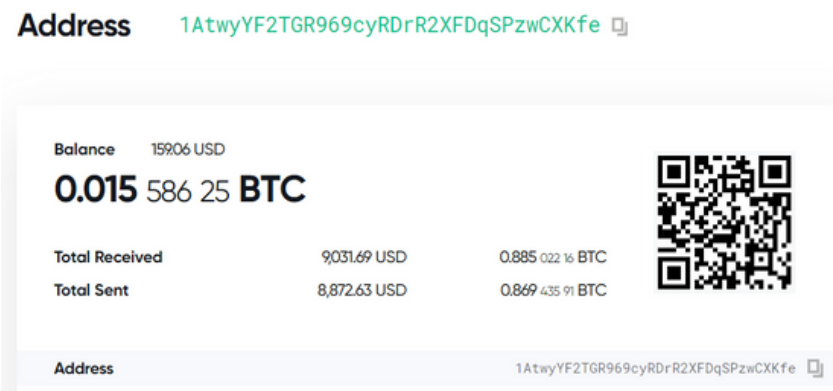
Monero	Bitcoin Cash	Litecoin	Neo	Web Money
ADA	ZCASH	DogeCoin	Stratis	QIWI Pay
Bicond	Waves	Reddcoin	Qtum	Payeer
Bytecoin	Bitcoin	Black Coin	VIA	
Steam Trade Link	Bitcoin Gold	Emercoin	Lisk	
Ethereum	Dash	Ripple	Yandex Money	

If the clipboard data matches one of the patterns coded into Masad Stealer, the malware replaces the clipboard data with one of the threat actors' wallets, which are also found in its binary. Below are the bitcoin and monero wallets found in one of the samples:

Bitcoin: 1AtwyYF2TGR969cyRDrR2XFDqSPzwCXKfe

Monero: 42Mm9gjuUSmPNr7aF1ZbQC6dcTeSi1MgB1Tv41frv1ZRFWLn4wNoLH3LDAGn9Fg2dhJW2VRHTz8Fo9ZAit951D2pDY8ggCR

Below is a snapshot of the bitcoin wallet transaction, as of this writing. This wallet has already received around $9,000 USD equivalent of bitcoins (as of Sept 15, 2019), which may or may not come from the activity of this malware.



A sample fraudulent bitcoin wallet found on one of the sample

Attack Vector

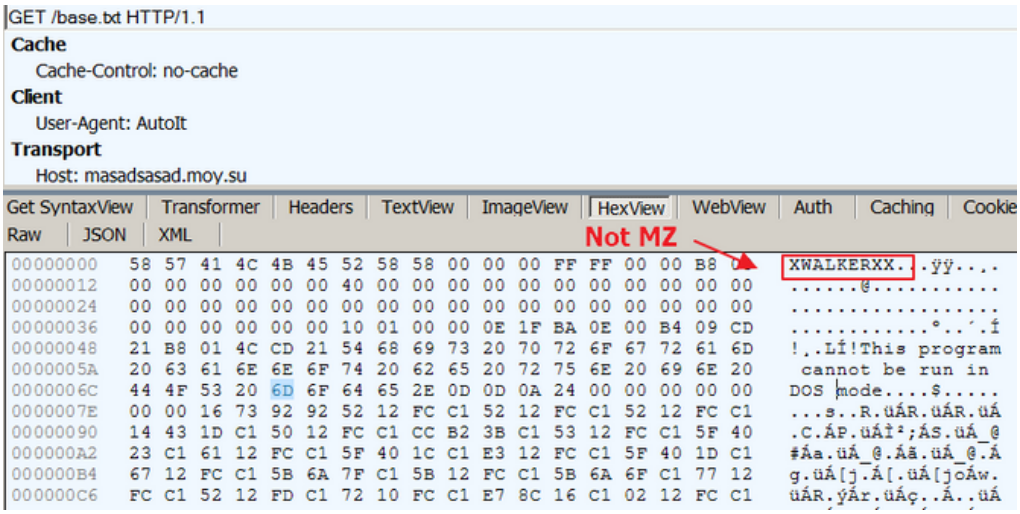
Based on our telemetry, Masad Stealer's main distribution vectors are masquerading as a legitimate tool or bundling themselves into third party tools. Threat actors achieve end user downloads by advertising in forums, on third party download sites or on file sharing sites. Below are the currently known list of software that Masad Stealer has been seen mimicking:

- ProxySwitcher (legitimate version here: https://www.proxyswitcher.com/)
- CCleaner.exe (legitimate version here: https://ccleaner.com/)
- Utilman.exe (legitimate version comes with Windows)
- Netsh.exe (legitimate version comes with Windows)
- Iobit v 1.7.exe (legitimate version here:https://www.iobit.com/)
- Base Creator v1.3.1 [FULL CRACK].exe (there is no legitimate version)
- EXEA HACK CRACKED (PUBG,CS GO,FORTNITE,GTA 5,DOTA).exe (there is no legitimate version)
- Icacls.exe (legitimate version comes with Windows)
- WSManHTTPConfig.exe (legitimate version comes with Windows)
- RADMIR CHEAT MONEYY.exe (there is no legitimate version)
- Tradebot_binance.exe (legitimate version here: https://tradesanta.com/en)
- Whoami.exe (legitimate version comes with Windows)
- Proxo Bootstrapper.exe (this is actually a reasonably popular form of malware)
- Fortniteaimbot 2019.exe (there is no legitimate version)
- Galaxy Software Update.exe (https://www.samsung.com/us/support/answer/ANS00077582/)

Download additional malware

Some samples of Masad Stealer have the capability to download additional malware. We have seen samples that download other malware, usually a miner, from these URLs:

- https://masadsasad[.]moy.su/base.txt (miner)
- https://zuuse[.]000webhostapp.com/mi.exe (miner)
- http://37[.]230.210.84/still/Build.exe
- http://37[.]230.210.84/still/SoranoMiner.exe
- http://187[.]ip-54-36-162.eu/steal.exe
- http://bgtyu73[.]ru/22/Build.exe



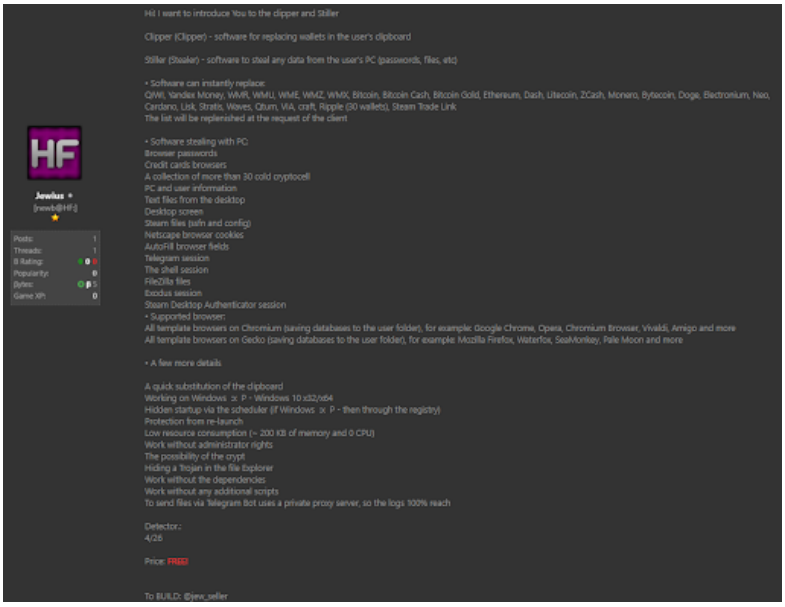
Masad stealer downloading a miner via HTTPS and with modified header

The figure above is a response from the request to https://masadsasad[.]moy.su/base.txt. This response contains an executable file with modified header. In addition to connecting via TLS, the modified header is an added trick by the malware to hide itself.

TLS streams are more difficult to inspect, helping to hide them from network-based security defenses. The modified header helps to hide the fact that the payload being downloaded is an executable from endpoint security products.

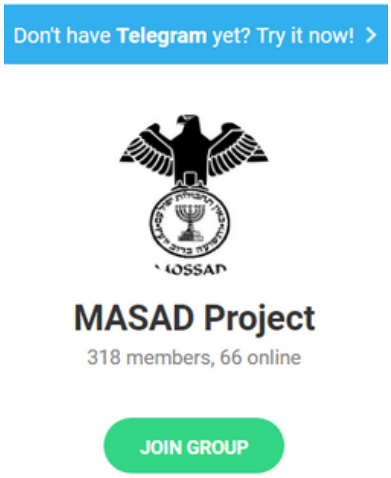
Threat Actors

This malware is being advertised in several hack forums as Masad Stealer. It starts with a free version and ladders up to versions asking up to $85, with each tier of the malware offering different features.



Sample Masad stealer ad found in hackforums

There is at least one dedicated website (masadproject[.]life) in existence to promote the sale of Masad Stealer. The developers have also created a Telegram group for their potential clients, and presumably to offer tech support. At time of writing, this group has more than 300 members.



Screenshot of a telegram group where one threat actor is operating

Of the more than 1,000 samples we identified to be variants of this malware, there where 338 unique Telegram Command and Control bot IDs. From this data, we can estimate the number of threat actors – or at least the number of different campaigns being run using the Masad Stealer malware – and the size of their operations. We used the getMe API, along with the bot token, to identify the usernames. Among the top bot IDs are as follows:

Telegram Bot ID	Telegram Bot Username	Unique Hashes
bot610711208	potterk_bot	45
bot830353220	reaper228bot	24
bot661438794	RanisYolo19_bot	23
bot796671289	dfsklnjfmkdvehfsf454sdfbot	22
bot870978042	dawdvwabot	20
bot753197414	korote_bot	14
bot823037532	NA/Inactive	13
bot699800942	RcbBots_Bot	13
bot831297312	xAmytBot	13
bot883608782	bichpaket777_bot	12
bot656889928	notius_bot	12
bot813438470	idontknowubot	12
bot911603667	Masat_bot	11
bot963764792	NA/Inactive	11
bot930786995	reborntodes_bot	9
bot884837464	istrong_bot	9
bot646596033	SkyDen_bot	9
bot865594389	gnoy199519bot]	8

Previous versions of this malware (or possibly a direct ancestor) are called “Qulab Stealer”.

How does Juniper Networks protect you against this?

Juniper Advanced Threat Protection products JATP and Sky ATP use machine learning to be able to accurately identify malware. The following images show the Sky ATP detecting multiple variations of this malware.

Threat level: High Medium Low None; clean

Threat level >= 4

File Hash (SHA-256)	Threat Level	Filename
eg. 123, 456		
848d76a227f4fe282b7ddfd82a6dfc4c25da2735a684462b42fe4e1c413d8e34	10	wevtutil.exe
44134b9d4b10d94f6381b446a1728b116d62e65c1a52db45235af12caf7e38c0	10	Build.exe
965a5949d8f94e17ebcd4cb6d0a7c19f49facbfc1b1c74111e5ceb83550d6c8f	10	Windows_Video_montager.exe
b763054180cd4e24c0a78b49055ad36dbc849f1a096cddf2db8cee0b9338c21d	9	Pictures.exe
3ba3c528d11d1df62a969a282e9e54534fb3845962672ad6d8bbc29cb6d062f5	10	Utilman.exe
ef623aadd50330342dc464a31b843b3d8b5767d62a62f5e515ac2b380b208fbe	9	Build.exe
c73675005a09008bc91d6bc3b5ad59a630ab4670dca6ac0d926165a3ecfd8d92	10	mmgaserver.exe
5b5ebe019806885bbaafe37bc10ca09549e41c240b793fd29a70690a5d80b496	10	dns-sd.exe
d01d40f33f10758c145d479823baee3739d7f2068351de40350b604298d2dbf1	9	ByNoBann.exe
6cff1249cc45b61ce8d28d87f8edc6616447e38168e610bed142f0b9c46ea684	10	lodctr.exe
0dcf547bd8f4074af97416d8b84ea64b2f3319064aa4bce64ad0c2e2d3957175	10	Build.exe
6bf6b1bde63cee9b81902efd187fdd56ecee5853754ce0a19d5ab5c3b0242988	10	Build.exe
b154151dc8ace5c57f109e6bb211a019db20c4f0127c4d13c7703f730bf49276	10	Build.exe
bf6083040ca51e83415f27c9412d9e3d700bd0841493b207bc96abf944ab0ca7	10	SMS-BOMBERINHO v26.exe
dfe3d0e95feaed685a784aed14d087b019ba2eb0274947a840d2bdbae4ae3674	10	C:\Users\<USER>\AppData\Roam
f030fb4e859ee6a97c50c973a73dced3640befe37f579cfd15367ce6a9bbede2	9	msdt.exe

Juniper Sky ATP’s detection of this malware family

The use of machine learning is critical to defending against this malware because of the number of rapid iterations it underwent throughout its development. Machine learning allows Juniper Connected Security to identify Masad Stealer variants as they emerge, helping to keep customers protected even before new strains have been identified.

Conclusion

Juniper Threat Labs believes that Masad Stealer represents an active and ongoing threat. Command and Control bots are still alive and responding as of this writing, and the malware appears to still be available for purchase on the black market.

In order to protect your organization, make sure that you have a next generation firewall (NGFW) with Advanced Threat Protection. NGFWs have the ability to identify the Telegram protocol and block it, if there is no legitimate business use, while Advanced Threat Protection products offer other methods to detect and counteract this malware.

Juniper Sky ATP, in conjunction with our SRX firewall will block any client infected with Masad Stealer from reaching out to the Command and Control bot master. It will also block the download of the Masad Stealer malware files in the first place, offering both remediation and prevention capabilities.

Indicators of Compromise

Sha256

e968affb1fc7756deb0e29807a06681d09a0425990be76b31816795875469e3d

4b1ccf6b823ee82e400ba25b1f532cd369d7e536475a470e2011b77ffeaf7bb3

fc84d6636a34ad1a11dbaa1daec179e426bdcd9887b3d26dc06b202417c08f95

9ca15f15fbae58cb97b0d48a0248461e78e34e6d530338e3e5b91f209a166267

31f3a402c1662ed6adffbf2b1b65cf902d1df763698eb76d21e4e94b4c629714

8d9f124ddd69c257189f1e814bb9e3731c00926fc2371e6ebe2654f3950ca02e

a0923d7645604faaa864a079adeb741a5d6e65507a2819b2fee4835d396077d9

a19b790ea12f785256510dde367d3313b5267536a58ca0c27dbdac7c693f57e1

f030fb4e859ee6a97c50c973a73dced3640befe37f579cfd15367ce6a9bbede2

f01db6d77ac21211992ceae4e66e1e03c1cb39d61e03645b9369f28252ca7693

dfe3d0e95feaed685a784aed14d087b019ba2eb0274947a840d2bdbae4ae3674

bf6083040ca51e83415f27c9412d9e3d700bd0841493b207bc96abf944ab0ca7

b154151dc8ace5c57f109e6bb211a019db20c4f0127c4d13c7703f730bf49276

6bf6b1bde63cee9b81902efd187fdd56ecee5853754ce0a19d5ab5c3b0242988

0dcf547bd8f4074af97416d8b84ea64b2f3319064aa4bce64ad0c2e2d3957175

6cff1249cc45b61ce8d28d87f8edc6616447e38168e610bed142f0b9c46ea684

5b5ebe019806885bbaafe37bc10ca09549e41c240b793fd29a70690a5d80b496

103d87098c9702cab7454b52869aeeb6a22919f29a7f19be7509255ce2d8c83e

c73675005a09008bc91d6bc3b5ad59a630ab4670dca6ac0d926165a3ecfd8d92

ef623aadd50330342dc464a31b843b3d8b5767d62a62f5e515ac2b380b208fbe

3ba3c528d11d1df62a969a282e9e54534fb3845962672ad6d8bbc29cb6d062f5

b763054180cd4e24c0a78b49055ad36dbc849f1a096cddf2db8cee0b9338c21d

d5ce4b04b7eec6530a4a9d40510177468fadc235253e5a74530a8c9d990f3c50

965a5949d8f94e17ebcd4cb6d0a7c19f49facbfc1b1c74111e5ceb83550d6c8f

44134b9d4b10d94f6381b446a1728b116d62e65c1a52db45235af12caf7e38c0

848d76a227f4fe282b7ddfd82a6dfc4c25da2735a684462b42fe4e1c413d8e34

5ca0a957fe6c253827f344da4ba8692d77a4e21a1df4251594be2d27d87dd8ae

016fa511f6546ed439d2606c6db8821685a99f5a14ef3f710668b58dc89c6926

22be594fbfa878f631c0632f6c4d260b00918817ff66a1f9f15efe44c1a58460

f3571ec66288405dab43332ca03812617f85fb08832fbbe1f1d89901fe034b8a

04c949eca23103b1de05278b49f42c3ab6b06f4bf20aafa5f2faefaa84c16ecd

e968affb1fc7756deb0e29807a06681d09a0425990be76b31816795875469e3d

d6fc04acda8f33a6d35eb577c27754c2f2b4d6f4869576c7c4e11b2c5e9b0176

18c0bd4dd98008383fc52045ad896449fa7f0037593bb730ed1ef88aa547006d

4c9d5469e9095813418260045c2b11e499e4eaa0ffb25293f90f580c464157df

0b5f1fbc05dc8baca492b748adeb01fb4904e02723b59211ecde222f7b12d91e

31ad5c4547ceae4d0550c8460524c16a6105afc056760e872c4966656256c9dc

edb00a0e5ff70e899857549e3263c887a799416c8bbab43ab130ca1be9bbd78c

96f852b81760a425befaa11ea37c0cdea2622630bf2a0c94bb95042211ab614d

57fd171a5b1a88e9583b42439851a91a940eb31105ab29cb314846da2ed43b82

277018b2cc6226dca6c7678cac6718c8584f7231340ad8cd7c03477559fdf48b

1acf5a461ee16336eb8bbf8d29982c7e26d5e11827c58ca01adac671a28b52ad

290a1b89517dec10bfd9938a0e86ae8c53b0c78ed7c60dc99e4f8e5837f4f24a

7937a1068f130a90b44781eea3351ba8a2776d0fede9699ba8b32f3198de045b

87e44bca3cc360c64cc7449ec1dc26b7d1708441d471bf3d36cd330db3576294

cf97d52551a96dacb089ac41463d21cab2b004ba8c38ffc6cb5fb0958ddd34db

79aa23c5a25c7cdbaba9c6c655c918dac3d9823ac62ebed9d7d3e94e1eaafc07

03d703f6d341be258ac3d95961ff0a67d4bf792f9e896530e193b091dca29c2e

a368b6755e62e5c0ff79ea1e3bd146ee8a349af309b4acf0558a9c667e78293a

ba933cefbe9a8034f0ba34e7d18481a7db7451c8ef4b6172fb0cad6db0513a51

URLs:

https://masadsasad[.]moy.su/base.txt

https://zuuse[.]000webhostapp.com/mi.exe

http://37[.]230.210.84/still/Build.exe

http://37[.]230.210.84/still/SoranoMiner.exe

http://187[.]ip-54-36-162.eu/steal.exe

http://bgtyu73[.]ru/22/Build.exe