Satan ransomware rebrands as 5ss5c ransomware

bartblaze.blogspot.com/2020/01/satan-ransomware-rebrands-as-5ss5c.html

The cybercrime group that brought us Satan, DBGer and Lucky ransomware and perhaps Iron ransomware, has now come up with a new version or rebranding named "5ss5c".

In a previous blog post, Satan ransomware adds EternalBlue exploit, I described how the group behind Satan ransomware has been actively developing its ransomware, adding new functionalities (specifically then: EternalBlue) and techniques with each run. Then, it appeared the group halted operations on at least the ransomware front for several months.

However, as it turns out, the group has been working on new ransomware - **5ss5c** - since at least November 2019.

The following tweet got my attention:

> 🧐Unknown #Ransomware captured tonight from #China, Encrypt only compressed files.
> Email：5ss5c@mail.ru
> ext：.5ss5c
> IP：61.186.243.2 58.221.158.90@demonslay335 @Amigo_A_ @GrujaRS @BleepinComputer @Rmy_Reserve @VK_Intel pic.twitter.com/dTdgnMfoLX
> — onion (@jishuzhain) January 12, 2020

After some quick checks, it appears this is a downloader for the 5ss5c ransomware, which is extremely reminiscent of how Satan ransomware operated:

Figure 1 - 5ss5c downloader

The malware will leverage certutil and even contains logging:

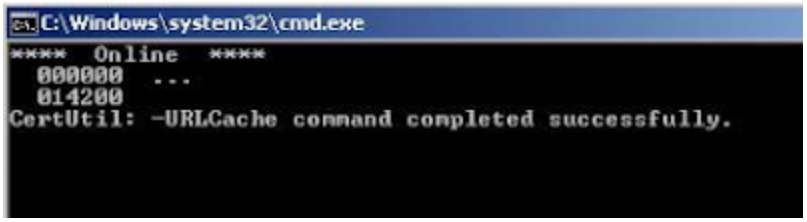

Figure 2 - certutil logging

It will download and leverage:

- Spreader (EternalBlue and hardcoded credentials);
- Mimikatz and what appears another password dumper/stealer;
- The actual ransomware.

The following hashes are relevant to this new variant:

Name: down.txt
URL: http://58.221.158[.]90:88/car/down.txt
Purpose: Downloader
MD5: 680d9c8bb70e38d3727753430c655699
SHA1: 5e72192360bbe436a3f4048717320409fb1a8009
SHA256: ddfd1d60ffea333a1565b0707a7adca601dafdd7ec29c61d622732117416545f
Compilation timestamp: 2020-01-11 19:04:24
VirusTotal report:
ddfd1d60ffea333a1565b0707a7adca601dafdd7ec29c61d622732117416545f

down.txt is, as mentioned, the downloader for the spreader module and for the actual ransomware:

Name: c.dat
URL: http://58.221.158[.]90:88/car/c.dat
Purpose: spreader
MD5: 01a9b1f9a9db526a54a64e39a605dd30
SHA1: a436e3f5a9ee5e88671823b43fa77ed871c1475b
SHA256: 9a1365c42f4aca3e9c1c5dcf38b967b73ab56e4af0b4a4380af7e2bf185478bc
Compilation timestamp: 2020-01-11 19:19:54
VirusTotal report:
9a1365c42f4aca3e9c1c5dcf38b967b73ab56e4af0b4a4380af7e2bf185478bc

Name: cpt.dat
URL: http://58.221.158[.]90:88/car/cpt.dat
Purpose: ransomware
MD5: 853358339279b590fb1c40c3dc0cdb72
SHA1: 84825801eac21a8d6eb060ddd8a0cd902dcead25
SHA256: ca154fa6ff0d1ebc786b4ea89cefae022e05497d095c2391331f24113aa31e3c
Compilation timestamp: 2020-01-11 19:54:25
VirusTotal report:
ca154fa6ff0d1ebc786b4ea89cefae022e05497d095c2391331f24113aa31e3c
Fun fact: file version information contains "**TODO: 5SS5C Encoder**".

The compilation times are sequential, which makes sense - the downloader has been developed (and compiled) first, then the spreader and the actual ransomware.

Note that **cpt.exe** as filename has already been observed in Satan ransomware.

Further indicators, such as hashes, URLs, file paths and so on will be posted at the end of this blog post.

5ss5c - still in development - and with oddities

There's quite some curiosities that indicate 5ss5c is still in active development and stems from Satan ransomware, for example:

- There are several logs created, e.g. there is a file "*C:\Program Files\Common Files\System\Scanlog*" that simply logs whether IPC SMB is open/available;
- Certutil logging (successful download or not);
- There are several Satan ransomware artefacts;
- Other Tactics, Techniques and Procedures (TTP) align with both Satan (and DBGer), and slightly overlap with Iron:

- One of these is, for example, the use of multiple packers to protect their droppers and payloads.
- This time however, they decided to use both MPRESS and Enigma, and even Enigma VirtualBox! (Note: Enigma and Enigma VirtualBox are not the same - the latter is a virtualised packer and also referred to as EnigmaVM.)

However, there are quite some curiosities, one of them being what appear to be hardcoded credentials:

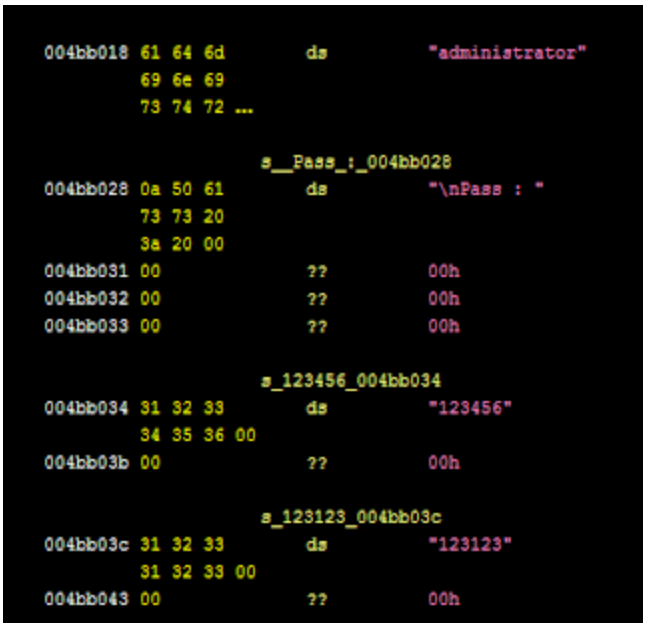

Figure 3 - Hardcoded creds

These hardcoded credentials will be leveraged in an attempt to connect to an SQL database with the **xp_cmdshell** command: https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/xp-cmdshell-transact-sql?view=sql-server-ver15

Curiously, we can identify the following data inside the ransomware in regards to the SQL database:

- ecology.url
- ecology.password
- ecology.user

Searching a bit further, we can discover a company named Finereport (https://www.finereport.com/en/company), which claims to be "*Top 1 in China's BI market share in IDC "China BI Software Tracker, 2018*". You guessed it - it uses SQL as database.

What else is new is, as mentioned before, the use of Enigma VirtualBox for packing an additional spreader module, aptly named **poc.exe**. This suggest they may be experimenting (**poc** often is an acronym for **p**roof **o**f **c**oncept).

This file will be dropped to **C:\ProgramData\poc.exe** and will run the following command:

> *cd /D C:\ProgramData&star.exe --OutConfig a --TargetPort 445 --Protocol SMB --Architecture x64 --Function RunDLL --DllPayload C:\ProgramData\down64.dll --TargetIp*

Now compare this to Satan ransomware's command:

> *cmd /c cd /D C:\Users\Alluse~1\&blue.exe --TargetIp & star.exe --OutConfig a --TargetPort 445 --Protocol SMB --Architecture x64 --Function RunDLL --DllPayload down64.dll --TargetIp*

Something looks similar here... :-)

5ss5c ransomware - how it operates

Back to the actual ransomware. It will create the following mutexes:

- **SSSS_Scan** (in previous iterations SSS_Scan has also been observed)
- **5ss5c_CRYPT**

Just like its predecessor, 5ss5c also has an exclusion list, where it will not encrypt specific files as well as files in the following folders:

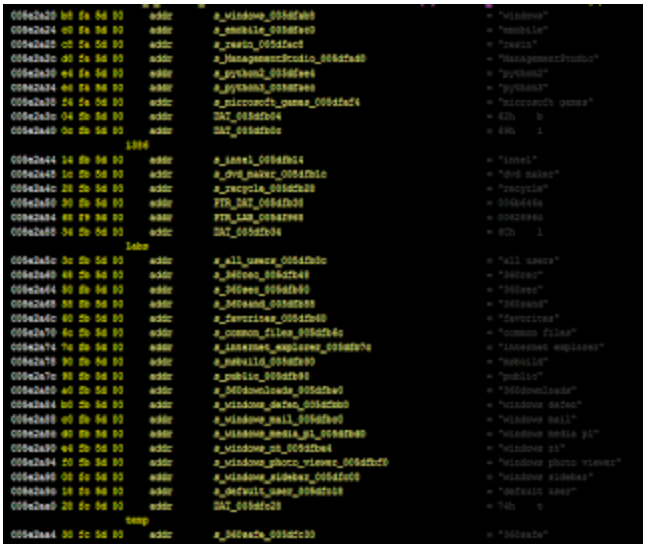

Figure 4 - Exclusion list

For example, the following folders belonging to Qihoo 360 (an internet security company based in China also offering antivirus) were already excluded in Satan and DBGer ransomware:

- 360rec
- 360sec
- 360sand

While these are new in 5ss5c ransomware:

- 360downloads
- 360safe

As in previous iterations, 5ss5c ransomware will stop database-related services and processes.

It will however only encrypt files with the following extensions:

> *7z, bak, cer, csv, db, dbf, dmp, docx, eps, ldf, mdb, mdf, myd, myi, ora, pdf, pem, pfx, ppt, pptx, psd, rar, rtf, sql, tar, txt, vdi, vmdk, vmx, xls, xlsx, zip*

This extension list is not like before, and includes mostly documents, archives, database files and VMware-related extensions such as *vmdk*.

The ransomware will then create the following URI structure to communicate with the C2 server (*61.186.243[.]2*):

- /api/data.php?code=
- &file=
- &size=
- &status=
- &keyhash=

It will also create a ransomware note on the **C:** drive as: **_如何解密我的文件_.txt** which translates to **_How to decrypt my file_.txt**. Example content is as follows:

Figure 5 - ransom note

The content reads:

> 部分文件已经被加密
> 如果你想找回加密文件,发送 (1) 个比特币到我的钱包
> 从加密开始48小时之内没有完成支付,解密的金额会发生翻倍.
> 如果有其他问题,可以通过邮件联系我
>
> 您的解密凭证是：
>
> Email:[5ss5c@mail.ru]

Translated:

> *Some files have been encrypted*
> *If you want to retrieve the encrypted file, send (1) Bitcoins to my wallet*
> *If payment is not completed within 48 hours from the start of encryption, the amount of decryption will double.*
> *If you have other questions, you can contact me by email*
> *Your decryption credentials are:*
>
> *Email: [5ss5c@mail.ru]*

Interestingly, the ransomware note does not contain a Bitcoin address. Additionally, the note only contains instructions in Chinese, not Korean nor English like previous iterations.
Is 5ss5c ransomware more targeted, or just actively being tested by the group/developers behind it?

Encrypted files will have the actor's email address prepended and a unique token with the ransomware's name will be appended, for example;
test.txt becomes
[5ss5c@mail.ru]test.txt.Y54GUHKIG1T2ZLN76II9F3BBQV7MK4UOGSQUND7U.5ss5c.

Prevention

- Enable UAC;
- Enable Windows Update, and install updates (especially verify if MS17-010 is installed);
- Install an antivirus, and keep it up-to-date and running;
- Install a firewall, or enable the Windows Firewall;
- Restrict, where possible, access to shares (ACLs);
- Create backups! (and test them)

More ransomware prevention can be found here.

Conclusion

Satan is dead, long live 5ss5c! It just doesn't sound as good, does it?

Whoever's behind the development of Satan, DBGer, Lucky and likely Iron ransomware, is back in business with the 5ss5c ransomware, and it appears to be in active development - and is trying to increase (or perhaps focus?) its targeting and spread of the ransomware.

It is recommended organisations detect and/or search for the indicators of compromise (IOCs) below, and have proper prevention controls in place. MITRE ATT&CK IDs can also be found below.

Indicators of Compromise:

Type	Indicator
File	C:\Program Files\Common Files\System\Scanlog
File	C:\Program Files\Common Files\System\cpt.exe
File	C:\Program Files\Common Files\System\tmp
File	C:\ProgramData\5ss5c_token
File	C:\ProgramData\blue.exe
File	C:\ProgramData\blue.fb
File	C:\ProgramData\blue.xml

Type	Indicator
File	C:\ProgramData\down64.dll
File	C:\ProgramData\mmkt.exe
File	C:\ProgramData\poc.exe
File	C:\ProgramData\star.exe
File	C:\ProgramData\star.fb
File	C:\ProgramData\star.xml
Registry key	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\5ss5cStart
Command	C:\Windows\system32\cmd.exe /c cd /D C:\ProgramData&blue.exe --TargetIp
Command	star.exe --OutConfig a --TargetPort 445 --Protocol SMB --Architecture x64 --Function RunDLL --DllPayload C:\ProgramData\down64.dll --TargetIp
Mutex	SSSS_Scan
Mutex	5ss5c_CRYPT
Email	5ss5c@mail.ru
URL	http://58.221.158.90:88/car/down.txt
URL	http://58.221.158.90:88/car/c.dat
URL	http://58.221.158.90:88/car/cpt.dat
IP	58.221.158.90
IP	61.186.243.2
Hash	82ed3f4eb05b76691b408512767198274e6e308e8d5230ada90611ca18af046d
Hash	dc3103fb21f674386b01e1122bb910a09f2226b1331dd549cbc346d8e70d02df
Hash	9a1365c42f4aca3e9c1c5dcf38b967b73ab56e4af0b4a4380af7e2bf185478bc
Hash	af041f6ac90b07927696bc61e08a31a210e265a997a62cf732f7d3f5c102f1da
Hash	ca154fa6ff0d1ebc786b4ea89cefae022e05497d095c2391331f24113aa31e3c
Hash	e685aafc201f851a47bc926dd39fb12f4bc920f310200869ce0716c41ad92198
Hash	e5bb194413170d111685da51b58d2fd60483fc7bebc70b1c6cb909ef6c6dd4a9

Type	Indicator
Hash	ddfd1d60ffea333a1565b0707a7adca601dafdd7ec29c61d622732117416545f
Hash	ef90dcc647e50c2378122f92fba4261f6eaa24b029cfa444289198fb0203e067
Hash	47fa9c298b904d66a5eb92c67dee602198259d366ef4f078a8365beefb9fdc95
Hash	68e644aac112fe3bbf4e87858f58c75426fd5fda93f194482af1721bc47f1cd7
Hash	ea7caa08e115dbb438e29da46b47f54c62c29697617bae44464a9b63d9bddf18
Hash	23205bf9c36bbd56189e3f430c25db2a27eb089906b173601cd42c66a25829a7
Hash	a46481cdb4a9fc1dbdcccc49c3deadbf18c7b9f274a0eb5fdf73766a03f19a7f
Hash	cf33a92a05ba3c807447a5f6b7e45577ed53174699241da360876d4f4a2eb2de
Hash	8e348105cde49cad8bfbe0acca0da67990289e108799c88805023888ead74300
Hash	ad3c0b153d5b5ba4627daa89cd2adbb18ee5831cb67feeb7394c51ebc1660f41
Hash	de3c5fc97aecb93890b5432b389e047f460b271963fe965a3f26cb1b978f0eac
Hash	bd291522025110f58a4493fad0395baec913bd46b1d3fa98f1f309ce3d02f179
Hash	75d543aaf9583b78de645f13e0efd8f826ff7bcf17ea680ca97a3cf9d552fc1f
Hash	50e771386ae200b46a26947665fc72a2a330add348a3c75529f6883df48c2e39
Hash	0aa4b54e9671cb83433550f1d7950d3453ba8b52d8546c9f3faf115fa9baad7e
Hash	5d12b1fc6627b0a0df0680d6556e782b8ae9270135457a81fe4edbbccc0f3552

These indicators are also available on AlienVault OTX:
Satan ransomware rebrands as 5ss5c ransomware

MITRE ATT&CK techniques