

New ransomware, old techniques: Petya adds worm capabilities

By Microsoft Defender Security Research Team

Published: 2017-06-28 · Archived: 2026-04-05 21:36:00 UTC

On June 27, 2017 reports of a [ransomware](#) infection began spreading across Europe. We saw the first infections in Ukraine, where more than 12,500 machines encountered the threat. We then observed infections in another 64 countries, including Belgium, Brazil, Germany, Russia, and the United States.

(Note: We have published a follow-up blog entry on this ransomware attack. We have new findings from our continued investigation, as well as platform mitigation and protection information: [Windows 10 platform resilience against the Petya ransomware attack](#).)

The new ransomware has worm capabilities, which allows it to move laterally across infected networks. Based on our investigation, this new ransomware shares similar codes and is a new variant of [Ransom:Win32/Petya](#). This new strain of ransomware, however, is more sophisticated.

To protect our customers, we released cloud-delivered protection updates and made updates to our signature definition packages shortly after. These updates were automatically delivered to all Microsoft free antimalware products, including [Windows Defender Antivirus](#) and Microsoft Security Essentials. You can download the latest version of these files manually at the [Malware Protection Center](#).

Windows Defender Advanced Threat Protection ([Windows Defender ATP](#)) automatically detects behaviors used by this new ransomware variant without any updates. To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, [sign up for a free trial](#).

Delivery and installation

Initial infection appears to involve a software supply-chain threat involving the Ukrainian company M.E.Doc, which develops tax accounting software, MEDoc. Although this vector was speculated at length by news media and security researchers—including Ukraine’s own Cyber Police—there was only circumstantial evidence for this vector. Microsoft now has evidence that a few active infections of the ransomware initially started from the legitimate MEDoc updater process. As we highlighted previously, [software supply chain attacks](#) are a recent dangerous trend with attackers, and it requires advanced defense.

We observed telemetry showing the MEDoc software updater process (*EzVit.exe*) executing a malicious command-line matching this exact attack pattern on Tuesday, June 27 around 10:30 a.m. GMT.

The execution chain leading to the ransomware installation is represented in the diagram below and essentially confirms that *EzVit.exe* process from MEDoc, for unknown reasons, at some moment executed the following command-line:

```
C:\Windows\system32\rundll32.exe | "C:\ProgramData\perfc.dat",#1 30
```

The same update vector was also mentioned by the Ukraine Cyber Police in a public list of indicators of compromise (IOCs) , which includes the MEDoc updater.

A single ransomware, multiple lateral movement techniques

Given this new ransomware's added lateral movement capabilities it only takes a single infected machine to affect a network. The ransomware spreading functionality is composed of multiple methods responsible for:

- stealing credentials or re-using existing active sessions
- using file-shares to transfer the malicious file across machines on the same network
- using existing legitimate functionalities to execute the payload or abusing SMB vulnerabilities for unpatched machines

In the next sections, we discuss the details of each technique.

Lateral movement using credential theft and impersonation

This ransomware drops a credential dumping tool (typically as a .tmp file in the %Temp% folder) that shares code similarities with [Mimikatz](#) and comes in 32-bit and 64-bit variants. Because users frequently log in using accounts with local admin privileges and have active sessions opens across multiple machines, stolen credentials are likely to provide the same level of access the user has on other machines.

Once the ransomware has valid credentials, it scans the local network to establish valid connections on ports *tcp/139* and *tcp/445*. A special behavior is reserved for Domain Controllers or servers: this ransomware attempts to call *DhcpEnumSubnets()* to enumerate DHCP subnets; for each subnet, it gathers all hosts/clients (using *DhcpEnumSubnetClients()*) for scanning for *tcp/139* and *tcp/445* services. If it gets a response, the malware attempts to copy a binary on the remote machine using regular file-transfer functionalities with the stolen credentials.

It then tries to execute remotely the malware using either PSEXEC or WMIC tools.

The ransomware attempts to drop the legitimate *psexec.exe* (typically renamed to *dllhost.dat*) from an embedded resource within the malware. It then scans the local network for *admin\$* shares, copies itself across the network, and executes the newly copied malware binary remotely using PSEXEC.

In addition to credential dumping, the malware also tries to steal credentials by using the *CredEnumerateW* function to get all the other user credentials potentially stored on the credential store. If a credential name starts with "TERMSRV/" and the type is set as 1 (generic) it uses that credential to propagate through the network.

This ransomware also uses the Windows Management Instrumentation Command-line (WMIC) to find remote shares (using *NetEnum/NetAdd*) to spread to. It uses either a duplicate token of the current user (for existing connections), or a username/password combination (spreading through legit tools).

Lateral movement using EternalBlue and EternalRomance

The new ransomware can also spread using an exploit for the Server Message Block (SMB) vulnerability [CVE-2017-0144](#) (also known as EternalBlue), which was fixed in [security update MS17-010](#) and was also exploited by [WannaCrypt](#) to spread to out-of-date machines. In addition, this ransomware also uses a second exploit for [CVE-2017-0145](#) (also known as EternalRomance, and fixed by the same bulletin).

We've seen this ransomware attempt to use these exploits by generating SMBv1 packets (which are all XOR 0xCC encrypted) to trigger these vulnerabilities.

These two exploits were leaked by a group called [Shadow Brokers](#). However, it is important to note that both of these vulnerabilities have been fixed by Microsoft in [security update MS17-010](#) on March 14, 2017.

Machines that are patched against these exploits (with [security update MS17-010](#)) or [have disabled SMBv1](#) are not affected by this particular spreading mechanism. Please refer to our previous [blog](#) for details on these exploits and how modern Windows 10 mitigations can help to contain similar threats.

Encryption

This ransomware's encryption behavior depends on the malware process privilege level and the processes found to be running on the machine. It does this by employing a simple XOR-based hashing algorithm on the process names, and checks against the following hash values to use as a behavior exclusion:

- *0x6403527E* or *0x651B3005* – if these hashes of process names are found running on the machine, then the ransomware does not do SMB exploitation.
- *0x2E214B44* – if a process with this hashed name is found, the ransomware trashes the first 10 sectors of `\\.\PhysicalDrive0`, including the MBR.

This ransomware then writes to the master boot record (MBR) and then sets up the system to reboot. It sets up scheduled tasks to shut down the machine after at least 10 minutes past the current time. The exact time is random (`GetTickCount()`). For example:

```
schtasks /Create /SC once /TN "" /TR "<system folder>\shutdown.exe /r /f" /ST 14:23
```

After successfully modifying the MBR, it displays the following fake system message, which notes a supposed error in the drive and shows the fake integrity checking.

Only if the malware is running with highest privilege (i.e., with `SeDebugPrivilege` enabled), it tries to overwrite the MBR code.

This ransomware attempts to encrypt all files with the following file name extensions in all folders in all fixed drives, except for `C:\Windows`:

.3ds	.7z	.acddb	.ai
.asp	.aspx	.avhd	.back
.bak	.c	.cfg	.conf

.cpp	.cs	.ctl	.dbf
.disk	.djvu	.doc	.docx
.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			

It uses file mapping APIs instead of a usual *ReadFile()/WriteFile()* APIs.

Unlike most other ransomware, this threat does not append a new file name extension to encrypted files. Instead, it overwrites the said files.

The AES key generated for encryption is per machine, per fixed drive, and gets exported and encrypted using the embedded 2048-bit RSA public key of the attacker.

The unique key used for files encryption (AES) is added, in encrypted form, to the *README.TXT* file the threat writes under section “*Your personal installation key:*”.

Beyond encrypting files, this ransomware also attempts to infect the MBR or destroy certain sectors of VBR and MBR.

After completing its encryption routine, this ransomware drops a text file called *README.TXT* in each fixed drive.

This ransomware also clears the System, Setup, Security, Application event logs and deletes NTFS journal info.

Detection and investigation with Windows Defender Advanced Threat Protection

Windows Defender Advanced Threat Protection ([Windows Defender ATP](#)) is a post-breach solution and offers by-design detections for this attack without need of any signature updates. Windows Defender ATP sensors constantly monitor and collect telemetry from the endpoints and offers machine-learning detections for common lateral movement techniques and tools used by this ransomware, including, for example, the execution of *PsExec.exe* with different filename, and the creation of the *perfc.dat* file in remote shares (UNC) paths.

The second alert targets the distribution of the ransomware's .dll file over the network. This event provides helpful information during investigation as it includes the User context that was used to move the file remotely. This user has been compromised and could represent the user associated with patient-zero.

With Windows Defender ATP, enterprise customers are well-equipped to quickly identify Petya outbreaks, investigate the scope of the attack, and respond early to malware delivery campaigns.

Protection against this new ransomware attack

Keeping your [Windows 10 up-to-date](#) gives you the benefits of the latest features and proactive mitigations built into the latest versions of Windows. In Creators Update, we further [hardened Windows 10 against ransomware attacks](#) by introducing new next-gen technologies and enhancing existing ones.

As another layer of protection, [Windows 10 S](#) only allows apps that come from the Windows Store to run. Windows 10 S users are further protected from this threat.

We recommend customers that have not yet installed security update [MS17-010](#) to do so as soon as possible. Until you can apply the patch, we also recommend two possible workarounds to reduce the attack surface:

- Disable SMBv1 with the steps documented at [Microsoft Knowledge Base Article 2696547](#) and as [recommended previously](#)
- Consider adding a rule on your router or firewall to block incoming SMB traffic on port 445

As the threat targets ports 139 and 445, you customers can block any traffic on those ports to prevent propagation either into or out of machines in the network. You can also disable remote WMI and file sharing. These may have large impacts on the capability of your network, but may be suggested for a very short time period while you assess the impact and [apply definition updates](#).

Aside from exploiting vulnerabilities, this threat can also spread across networks by stealing credentials, which it then uses to attempt to copy and execute a copy on remote machines. You can prevent credential theft by ensuring credential hygiene across the organization. [Secure privileged access](#) to prevent the spread of threats like Petya and to protect your organization's assets. Use [Credential Guard](#) to protect domain credentials stored in the Windows Credential Store.

Windows Defender Antivirus detects this threat as [Ransom:Win32/Petya](#) as of the [1.247.197.0 update](#). Windows Defender Antivirus uses cloud-based protection, helping to protect you from the latest threats.

For enterprises, use [Device Guard](#) to lock down devices and provide kernel-level virtualization-based security, allowing only trusted applications to run, effectively preventing malware from running.

Monitor networks with [Windows Defender Advanced Threat Protection](#), which alerts security operations teams about suspicious activities. Download this playbook to see how you can leverage Windows Defender ATP to detect, investigate, and mitigate ransomware in networks: [Windows Defender Advanced Threat Protection – Ransomware response playbook](#).

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, [sign up for a free trial](#).

Resources

MSRC blog: <https://blogs.technet.microsoft.com/msrc/2017/06/28/update-on-petya-malware-attacks/>

Next-generation ransomware protection with Windows 10 Creators Update:

<https://blogs.technet.microsoft.com/mmpc/2017/06/08/windows-10-creators-update-hardens-security-with-next-gen-defense/>

Download English language security updates: [Windows Server 2003 SP2 x64](#), [Windows Server 2003 SP2 x86](#), [Windows XP SP2 x64](#), [Windows XP SP3 x86](#), [Windows XP Embedded SP3 x86](#), [Windows 8 x86](#), [Windows 8 x64](#)

Download localized language security updates: [Windows Server 2003 SP2 x64](#), [Windows Server 2003 SP2 x86](#), [Windows XP SP2 x64](#), [Windows XP SP3 x86](#), [Windows XP Embedded SP3 x86](#), [Windows 8 x86](#), [Windows 8 x64](#)

MS17-010 Security Update: <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

General information on ransomware: <https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx>

Security for IT Pros: <https://technet.microsoft.com/en-us/security/default>

Indicators of Compromise

Network defenders may search for the following indicators:

File indicators

- 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
- 9717cfdc2d023812dbc84a941674eb23a2a8ef06
- 38e2855e11e353cedf9a8a4f2f2747f1c5c07fcf
- 56c03d8e43f50568741704aee482704a4f5005ad

Command lines

In environments where command-line logging is available, the following command lines may be searched:

- Scheduled Reboot Task: Petya schedules a reboot for a random time between 10 and 60 minutes from the current time
 - `schtasks /Create /SC once /TN "" /TR "<system folder>\shutdown.exe /r /f" /ST <time>`

- `cmd.exe /c schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST <time>`

This may be surfaced by searching for EventId 106 (General Task Registration) which captures tasks registered with the Task Scheduler service.

- Lateral Movement (Remote WMI)
 - `"process call create \"C:\Windows\System32\rundll32.exe |||\"C:\Windows\perfc.dat|||\" #1"`

Network indicators

In environments where NetFlow data are available, this ransomware's subnet-scanning behavior may be observed by looking for the following:

- Workstations scanning ports tcp/139 and tcp/445 on their own local (/24) network scope
- Servers (in particular, domain controllers) scanning ports tcp/139 and tcp/445 across multiple /24 scopes

Talk to us

Questions, concerns, or insights on this story? Join discussions at the [Microsoft community](#) and [Windows Defender Security Intelligence](#).

Follow us on Twitter [@WDSecurity](#) and Facebook [Windows Defender Security Intelligence](#).

Source: <https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/>