**CERT-EU Security Advisory 2017-012**

# WannaCry Ransomware Campaign Exploiting SMB Vulnerability

***May 22, 2017 — v1.6***

*History:*

- *12/05/2017 — v1.0: Initial publication*
- *13/05/2017 — v1.1: Additional information about ways to defend and new patches added*
- *15/05/2017 — v1.2: Additional variants discovered and a new tool published*
- *15/05/2017 — v1.3: Some wording changed*
- *16/05/2017 — v1.4: Additional variants with new killswitches discovered*
- *18/05/2017 — v1.5: Encryption key recovery sometimes possible*
- *22/05/2017 — v1.6: Better tool available for recovering encrypted files; other campaigns identified*

## Summary

A large ransomware campaign has been observed since Friday, May 12th, 2017. The payload delivered is a variant of ransomware malware called **WannaCry**. It appears to infect computers through a recent SMB vulnerability in Microsoft Windows operating system [1, 2, 3, 7, 12, 13] (CVE-2017-0145).

The exploit used – *EternalBlue* – has been made available on the Internet through the *Shadow-Brokers* dump on April 14th, 2017 [6], but already earlier patched by Microsoft on March 14th, 2017 as part of MS17-010 [3] for the supported versions of the Microsoft Windows operating system. Unfortunately, the patch was not available at that time for legacy Windows XP, Windows 8, as well as for Windows Server 2003 systems. Even in case of systems where the patch was available, it appears that many organizations have not installed it. There were more than 200 000 computers affected world-wide with some prominent organizations including Telefonica [4] in Spain and NHS hospitals in UK [5].

As of May 13th, 2017, due to the seriousness of the threat, **Microsoft has made available the patch MS17-010** [9] also for earlier (no longer supported) versions of Microsoft Windows operating system, such as **Windows XP**, **Windows 8**, and **Windows Server 2003**.

A tool called ***wanakiwi*** has been recently made available that **may make it possible to recover the encrypted files** on Windows XP, Windows 7, Windows Vista, Windows Server 2003 and 2008, if the system was not rebooted after the infection [16].

Other campaigns leveraging the tools leaked by the *ShadowBrokers* have been identified [18, 19]. While they do not deliver ransomware, they may be used for other purposes and represent a significant threat. The other campaigns share the same infection method – SMB. It is important to monitor network activity even if no ransomware cases have been observed.

## Technical Details

The campaign uses an exploit for a recent SMB protocol vulnerability in Microsoft Windows [1, 2, 3, 7]. According to [7], the ransomware perpetrators incorporated publicly-available exploit code for the patched SMB *EternalBlue* vulnerability, CVE-2017-0145, which can be triggered by sending a specially crafted packet to a targeted SMB server. It spreads initially through vulnerable computers exposing port 445 on the Internet, and then using the same technique propagating through the internal network.

Following [7], the threat arrives as a dropper that has the following two components:

- A component that tries to exploit the SMB *EternalBlue* vulnerability in other computers.
- Ransomware known as *WannaCry/WannaCrypt*.

The dropper – depending on the version – tries to connect to one of the following (*killswitch*) domains [7, 8, 10, 14]:

```
iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf[.]com
lazarusse.suiche.sdfjhgosurijfaqwqwqrgwea[.]com
```

These domains have been **sinkholed** by MalwareTech [8] and others. **If the connection is successful**, the threat **does not infect** the system further with ransomware or try to exploit other systems to spread; it simply stops execution. However, if the connection fails, the dropper proceeds to drop the ransomware and creates a service on the system. Hence, it is imperative to **enable access to this domain**, by either:

- enabling access to this domain on the Internet – the malware is not proxy-aware, so if a proxy use is required, this may fail;
- redirecting the requests to this domain (through local DNS or proxy re-writing, etc.) to a webserver that will respond with HTTP code 200 to any request.

In either case, it is worth to **monitor the requests** as the machines initiating these requests most likely had been infected with the WannaCray ransomware.

The threat creates a service named `mssecsvc2.0`, whose function is to exploit the SMB vulnerability in other computers accessible from the infected system. Once at least one computer in local network is infected, the malware will automatically spread using the SMB protocol on TCP port 445 [7]. It is important to mention that **unpatched** computers and networks exposing SMB protocol on the Internet may be directly infected without the need for any other delivery mechanism. It is sufficient that they are powered-up and accepting SMB protocol connections. Recent analysis [12, 13] also indicates that if a target system is infected with *DoublePulsar* backdoor, it will be automatically exploited. Also, once a new system is infected, *DoublePulsar* will be installed as well.

The malware used in the attacks encrypts the files and also drops and executes a decryptor tool. Then, the malware requests around $300 in Bitcoin for obtaining a decryption key. The decryption tool clearly supports multiple countries, as it provides the interface in several languages. For command and control, the malware extracts and uses Tor service executable with all necessary dependencies to access the Tor network. More analysis may be found in [2] and [7].

The file extensions that the malware is targeting contain certain clusters of formats including [2]:

- Commonly used office file extensions ( `.ppt` , `.doc` , `.docx` , `.xlsx` , `.sxi` ).
- Less common and nation-specific office formats ( `.sxw` , `.odt` , `.hwp` ).
- Archives, media files ( `.zip` , `.rar` , `.tar` , `.bz2` , `.mp4` , `.mkv` ).
- Emails and email databases ( `.eml` , `.msg` , `.ost` , `.pst` , `.edb` ).
- Database files ( `.sql` , `.accdb` , `.mdb` , `.dbf` , `.odb` , `.myd` ).
- Developers' sourcecode and project files ( `.php` , `.java` , `.cpp` , `.pas` , `.asm` ).
- Encryption keys and certificates ( `.key` , `.pfx` , `.pem` , `.p12` , `.csr` , `.gpg` , `.aes` ).
- Graphic designers, artists and photographers files ( `.vsd` , `.odg` , `.raw` , `.nef` , `.svg` , `.psd` ).
- Virtual machine files ( `.vmx` , `.vmdk` , `.vdi` ).

### Other Related Campaigns

Since the start of the *WannaCry* campaign, there has been a lot of interest and research performed. This allowed to also identify other campaigns exploiting the vulnerabilities published by the *ShadowBrokers*, such as *BlueDoom* [18] or *EternalRocks* [19], and others. Some of these campaigns have started prior to the *WannaCry*, and other later. They all share the same infection vector, but the differ in the activity performed after infection. Some are used to mine *Monero* cryptocurrency, others install backdoors that could be used later, but do not perform any additional visible actions for the moment. Most of these additional campaigns do not use any type of *killswitch*.

Since the initial infection for all these related campaigns appears to be using the same infection vector, it is important to monitor networks for activity related to *EternalBlue* even if no ransomware infections have been observed. There may be machines infected with any of the other campaigns. The following SNORT rules may be used to detect network activity related to *EternalBlue* [17]:

```
alert tcp $HOME_NET 445 -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo
  Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98
  07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|";
  distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218;
  rev:2;)

alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo
  Request (set)"; flow:to_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00
  18 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|";
  distance:0; flowbits:set,ETPRO.ETERNALBLUE; flowbits:noalert; classtype:trojan-activity;
  sid:2024220; rev:1;)

alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo
  Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98
  07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|";
  distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218;
  rev:1;)
```

## Products Affected

The following products known to be impacted if they are not patched [1, 3, 7]:

- Microsoft Windows Vista SP2
- Microsoft Windows Server 2008 SP2 and R2 SP1
- Microsoft Windows 7
- Microsoft Windows 8.1
- Microsoft Windows RT 8.1
- Microsoft Windows Server 2012 and R2

It has been recently confirmed [7] that the malware targets also earlier – no longer supported – version of the Microsoft operating system:

- Windows XP
- Windows 8
- Windows Server 2003

At the same time, Microsoft has confirmed [7] that Windows 10 is not impacted by this attack at the moment. It is important to realize however that the attack may evolve and future versions may also target unpatched versions of Windows 10.

## Recommendations

A patch for the SMB vulnerability is available as Microsoft Security Bulletin **MS17-010** for the supported Microsoft Windows operating system versions [3]. It is imperative that this patch is installed. Since the threat appears to evolve (new variants, new *killswitch* domains appearing), any measures relying on a specific characteristic of the variants currently used, should not be considered reliable.

Additionally, as of May 13th, 2017, due to the seriousness of the threat, **Microsoft has made available the patch MS17-010** [9] also for earlier (no longer supported) versions of Microsoft Windows operating system, such as **Windows XP**, **Windows 8**, and **Windows Server 2003**.

Additionally, the following measures should be taken as soon as possible [1, 7]:

- Update system with Microsoft patch MS17-010 or upgrade to Windows 10.
- Disable SMBv1 with the steps documented at Microsoft Knowledge Base Article 2696547.
- Consider adding a rule on the firewall to block incoming SMB traffic on port 445.
- Discover which systems within the network may be susceptible to attack and isolate them, update, and/or shut down.
- For systems without support or patch available, it is recommended to isolate them from the network or shut down as the case may be. As an option, there has been a tool published [11], which can block execution of the malware on vulnerable systems.
- In case of new infections, it is highly recommended to provide all workstations with access to the *killswitch* domains as mentioned in the Technical Details section of this advisory.

As a general rule, the best defense against ransomware-type attacks are frequent and reliable backups. If a recent backup is available, the affected systems may be easily restored from backups.

In case of infection/encryption of files, there may be a possibility to **recover the encrypted files** on Windows XP, Windows 7, Windows Vista, Windows Server 2003 and 2008, if the system was not rebooted after the infection [16]. The *wanakiwi* tool tries to recover the private user key

in memory by searching for the two prime numbers used to generate the RSA key-pair during the WannaCry encryption process. The primes extraction method is based on Adrien Guinet's *wannakey* [15], which consist of scanning the WannaCry process memory to recover the prime numbers that were not cleaned during `CryptReleaseContext()`.

Also, it should be kept in mind that making the ransomware payment does not guarantee that the attackers send the decryption key. Currently, there are no confirmed cases for this campaign indicating that paying the ransom actually allowed to decrypt the files.

## References


[1] https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html

[2] https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/

[3] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

[4] https://blog.gdatasoftware.com/2017/05/29751-wannacry-ransomware-campaign

[5] https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/

[6] https://support.kaspersky.com/shadowbrokers

[7] https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

[8] https://intel.malwaretech.com/botnet/wcrypt

[9] https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

[10] https://blog.comae.io/wannacry-new-variants-detected-b8908fefea7e

[11] https://www.ccn-cert.cni.es/en/updated-security/ccn-cert-statements/4485-nomorecry-tool-ccn-cert-s-tool-to-prevent-the-execution-of-the-ransomware-wannacry.html

[12] https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/

[13] https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis

[14] https://www.bleepingcomputer.com/news/security/wannacry-wana-decryptor-wanacrypt0r-info-and-technical-nose-dive/

[15] https://github.com/aguinet/wannakey

[16] https://github.com/gentilkiwi/wanakiwi

[17] https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/

[18] https://heimdalsecurity.com/blog/bluedoom-worm-eternablue-nsa-exploits/

[19] https://www.bleepingcomputer.com/news/security/new-smb-worm-uses-seven-nsa-hacking-tools-wannacry-used-just-two/