CERT-EU Security Advisory 2017-012

WannaCry Ransomware Campaign Exploiting SMB Vulnerability

May 12, 2017 — v1.0

History:

- *12/05/2017 — v1.0: Initial publication*

Summary

A large spear-phishing campaign has been observed over the last couple of weeks. The payload delivered is a variant of ransomware malware called **WannaCry**. As of today, May 12th, 2017, it appears that the delivery mechanism has been *improved* by adding a method to infect other computers in the local network through a recent SMB vulnerability in Microsoft Windows operating system [1, 2, 3] (CVE-2017-0143 through CVE-2017-0148).

The exploit (codenamed *EternalBlue*) has been made available on the Internet through the *ShadowBrokers* dump on April 14th, 2017 [6] and patched by Microsoft on March 14th, 2017 as part of MS17-010 [3]. Unfortunately, it appears that many organizations have not yet installed the patch. As of the time of writing this advisory, there were at least tens of thousands computers affected world-wide with some prominent organizations including Telefonica [4] in Spain and NHS hospitals in UK [5].

Technical Details

While there is only limited information available about the initial infection vector, first indications point mostly to a spear-phishing campaign delivering MS Office documents with malicious macros utilizing JavaScript or PowerShell to deliver the malware. While such campaigns are common and relatively wide-spread, it appears that the very high impact of this one was enhanced by including an exploit for a recent SMB protocol vulnerability in Microsoft Windows [1, 2, 3].

Once at least one computer in local network is infected, the malware will automatically spread using the SMB protocol and ports 137 and 138 UDP and ports 139 and 445 TCP. It is important to mention that **un-patched** computers and networks exposing SMB protocol (and the above-mentioned ports) 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.

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].

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`).

Products Affected

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

- 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
- Microsoft Windows 10
- Microsoft Windows Server 2016

It is unconfirmed at the moment, if the Microsoft Windows XP is also impacted by this vulnerability or not.

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.

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

- Update systems to latest version or patch as reported by manufacturer.
- For systems without support or patch available, it is recommended to isolate them from the network or shut down as the case may be.
- Isolate communication to ports 137 and 138 UDP and ports 139 and 445 TCP in organizations' networks.
- Discover which systems within the network may be susceptible to attack and isolate them, update, and/or shut down.

In case of infection/encryption of files, it is recommended to keep/backup the files that had been encrypted before disinfecting the machine, since it may be possible that a decryption key may become available at some point in the future. There are however no guarantees that this

will be possible. Also, it should be kept in mind that making the ransomware payment does not guarantee that the attackers send the decryption key.

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