Fujitsu Threat Monitoring

Threat Advisory - Ransomware Outbreak

SOC Threat Advisory: **Ransomware Outbreak**
Threat Level: **SIGNIFICANT**

This is to reference the recent ransomware outbreak affecting countries worldwide. Initial infection appears to occur via an attachment supplied via email. Upon succesful infection of the recipient machine the malware uses multiple techniques to further propagate through the network.

shaping tomorrow with you

FUJITSU

Technical Threat

Ransomware initially believed to be a variant of Petya, has been observed infecting machines in multiple countries.

The attack follows the below process to infect victims. Various sources claim email delivers a malicious payload, as either a .doc/.rtf files. The victim executes the malicious dropper file causing the final payload to be downloaded.

Upon infection the malicious code has checks for Sandboxes, virtual environments and anti-virus. Credential theft is attempted via a modified version of Mimikatz. If credential theft is successful these credentials are then used to attempt to move laterally across a network, at this stage conditional behaviour enacts either PSEXEC or WMIC.

The ransomware can also spread using an exploit for previously patched SMB vulnerability CVE-2017-0144 (also known as EternalBlue), which was also exploited by WannaCrypt to spread to out-of-date machines. In addition, Petya also uses a second exploit for CVE-2017-0145 (also known as EternalRomance and fixed by the same bulletin).

A hard coded path of C:\windows was identified by Fujitsu CTI in this sample

The use of this path instead of using a given API function is commonly used by malware and is described here but as a result of this Windows installations outside of this path will remain unaffected.

Affected Systems and remediation

Machines that are patched against this exploit (with security update MS17-010) or have disabled SMBv1 are not affected by the method of propagation.

As this attack uses a more traditional ransomware encryption technique there is no 'killswitch', infected networks and machines will be targeted by the worm capabilities of this new threat.

Users should not open any document supplied via email. Documents using exploits can infect devices upon opening and do not require further interaction, such as, enabling macros.

Symantec currently classify this threat as

- Host IPS (OS Attack: Microsoft SMB MS17-010 Disclosure Attempt - Attack: Shellcode Download Activity)
- SEP 14 Machine Learning (Heur.AdvML.B – SEP 14 only (aka ML.Attribute.HighConfidence)
- SONAR behavioural analysis (SONAR.Module!gen3)

Further Information

» https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know