Bad Rabbit Ransomware: Technical Analysis

Introduction

On Oct 24, 2017, a few organisation in Ukraine, Russia, Turkey and Germany had reported of disruptions attributing to ransomware. Based on initial information received, a new variant of WannaCry and NotPetya ransomware known as Bad Rabbit are responsible for the incidents. Further analysis of the ransomware has been carried out and details of the ransomware is explained below. National Cyber Coordination and Command Centre is currently monitoring closely for any signs of infection or propagation in Malaysia.

Impact

Encrypt user files and demand ransom to decrypt the files for 0.05 worth of Bitcoin.

System Affected

All Windows Operating System

Brief Description

A new strain of ransomware nicknamed “Bad Rabbit” has been found spreading since yesterday. To-date, the malware has affected systems at three Russian websites, an airport in Ukraine and an underground railway in the capital city, Kiev.

According to Kaspersky Lab, most of the victims targeted by these attacks are located in Russia but there are also attacks reported in Ukraine, Turkey and Germany. Based on initial analysis, Bad Rabbit has the same characteristic of WannaCry and NotPetya that is exploiting the SMB vulnerability for propagation once a computer is infected.

The distribution method of Bad Rabbit is via drive-by download in which popular websites are compromised and JavaScript were injected in their HTML body or .js file. Once infected, users will receive a popup asking to download an update for Adobe Flash Player.

Once “Install” button is clicked, a download of an executable file from 1dnscontrol[.]com is initiated. This executable file, install_flash_player.exe is the dropper for Win32/Filecoder.D and once installed the computer will be encrypted and a ransom note asking for 0.05 bitcoin will appear.

Recommendation:

1. Patch your Windows Operating System with MS17-010 Microsoft Security bulletin;
2. Patch your computers with the latest Windows Security Updates. Users are strongly recommended to turn on the 'Automatic Updates' features in Windows OS to ensure that security patches and updates are applied as soon as they are released;
3. Back up your important files and data to an external drive;
4. Update and run your computer with antivirus that has the latest anti-malware signatures;
5. Block SMB ports (139, 445) from all accessible hosts. If the SMB service is required, please ensure that the required patch (MS17-010) has been applied;
6. Update Windows Defender with the latest update from Microsoft;
7. To prevent getting infected by Bad Rabbit, users are advised to create these two files in C:\windows and remove all permissions – C:\windows\infpub.dat and C:\windows\cscc.dat
8. Advise your users not to click any popup window regarding updating Adobe Flash without informing the IT department;
9. Report any incidents related to this attack to NC4.

Reference:

1. Microsoft Security Bulletin MS17-010 – Critical
   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

2. Bad Rabbit: Not-Petya is Back With Improved Ransomware
   https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

3. Cybereason Researcher Discovers Vaccine For Bad Rabbit Ransomware
   https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomware

4. Bad Rabbit: A new ransomware epidemic is on the rise
   https://www.kaspersky.com/blog/bad-rabbit-ransomware/19887/

5. Ransom - Win32Tibbar A –
   https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Tibbar.A