VulnerabilityAlert

AlertNo:AVA170513

Date:5/13/2017 6:05 AM

Multiple Ransomware Spreading Rapidly –High Alert

Overview

Currently by two major ransomware, with the use of known Microsoft vulnerabilities are targeting the entire world with millions of phishing emails.

Description / Impact

- Massive ransomware attack spreading through the globe, It has been identified as a variant of ransomware known as WannaCry (also known as 'Wana Decrypt0r,' 'WannaCryptor' or 'WCRY'). Furthermore, it was observed that "WannaCry" Ransomware started spreading since last night.

- Current research shows that this is ransomware being distributed through a phishing attack and then infecting the victim network through an auto-propagating worm utilizing an SMB exploit (MS17-010).

- The second ransomware from the Necurs botnet is spreading a "Jaff," file-encrypting ransomware very similar to the infamous Locky ransomware.

- The ransomware is spreading via emails are attached with an attached PDF document, which if clicked, opens up an embedded Word document with a malicious macro script to downloads and execute the "Jaff" or "WannaCry" , ransomware.

Risk Reduction Recommendations

Immediate Actions to be taken:

- The effected PCs should be immediately disconnected from the network.
- Contact your virus guard providers/ Security Vendors for necessary actions.
- As an immediate action, email attachments should be blocked relating to following files but not limited to .pdf (encapsulating a .js– javascript)/*.hta/.doc macro based Microsoft word) or related executables.

Prevention:

- Have all files backed up in a completely separate system.
- This ransomware targets all versions of Windows including Windows XP, Windows Vista, Windows 7, Windows 8 and Windows 10.
- Clients should ensure that they are patched on MS17-010.
- Disable the outdated protocol SMBv1.
- Isolate unpatched systems from the larger network

Recovery:

- As of now, there are no know recovery methods available. Do not try to pay the ransom.

Disclaimer

The information provided here in is on "as is" basis, without warranty of any kind.

FinancialSectorComputerSecurityIncidentResponseTeam,SriLanka
Hotline:+94112039777
Reportincidenttoincident@fincsirt.lk