PTA CERT for Telecom Sector

Security Advisory-No: Ext:153-16

10, Sep 2018

Threat Classification: Malware (Ramsomware)

Name: SamSam

Source: Exploit vulnerabilities in Remote Desktop Protocol (RDP), Java-based web servers and File Transfer Protocol (FTP) servers to gain access to the victim's network.

Distribution: Through Malvertising and spam email campaigns.

Impact: Attacker first compromises the Remote Desktop Protocol (RDP) on a targeted system either by conducting brute force attack or by using stolen credentials Later, it deploy the SamSam ransomware throughout the network by exploiting vulnerabilities in system.

Scope:

- It encrypts victim's files and demand Bitcoins for decryption.
- It allows the attacker to select target and easily learn which computer has been encrypted.
- Due to manual attack, it poses no risk of spreading out or attracting unwanted attention.

Recommendations:

a. **<u>Mitigation Measures for End Users</u>**

1. All Window Operating Systems (Win XP, 7, 8, 8.1, 10, 2003 and 2008) are vulnerable; therefore, it is of paramount importance to update the windows operating systems using official update feature.
2. Disable "Turn on fast startup" feature in Windows 7, 8, 8.1 and 10 to properly install all updates.
3. Install and fully update reputable antivirus like Kaspersky, AVAST,_Avira, ESET etc.
4. Install and regularly update software firewall such as Comodo_Firewall or Zone alarm etc.
5. Limit Ike rate of password retries with the security policy editor.
6. Implement multi-factor authentication on the systems.
7. Update all third party applications with the latest patches.
8. Turn off a windows feature in control panel by un-checking "SMB 1.O/CIFS File Sharing Support" in "Program and Features" tool.
9. Do not open email attachments from un-trusted sources.

10. Restricted access to RDP (on port 3389).
11. Regularly maintain offline backups of critical data.

b. Recommendations for System Administrators

(1) Regularly install security updates of Windows Server.
(2) Disconnect' those systems from network that cannot be updated.
(3) Turn off a windows feature in control panel by un-checking "SMB 1.OICIFS File Sharing Support" in "Program and Features" tool if not required.
(4) Maintain offline backups of all the critical systems and sensitive data.
(5) Restrict users' permissions to install and run unwanted applications.
(6) Actively monitor and validate traffic, going in and out of the network.
(7) In case computer has been infected, disconnect it from the network to prevent the malware from spreading and apply the decryption tools available online such as WannaKiwi, WannaKey, PayBreak System, etc to decrypt files.
(8) Educate users on prevention against cyber threats specially phishing email having lucrative offers.
(9) In case of any incident, please report to this office.