

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT, CABINET DIVISION  
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
(NTISB-II)

No. 1-5/2003 (NTISB-II)

Islamabad 29 August, 2018

Subject: Advisory — Prevention Against Cyber Espionage (Advisory No 153)

1. Introduction. A new ransomware attack **SamSam** is being distributed by **malvertising** and **spam email campaigns**. **SamSam** uses vulnerabilities in **Remote Desktop Protocol (RDP)**, **Java-based web servers** and **File Transfer Protocol (FTP)** servers to gain access to the victims' network.

2. Technical Analysis.

a. Method of Infection. 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 deploys the **SamSam** ransomware throughout the network by exploiting **vulnerabilities in system**.

b. Capabilities of Malware.

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

Recommendations. Keeping in view the capability of malware; suggested security measures are as under:-

a. Mitigation Measures For End Users

- (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 system 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 **Zonealarm** etc.
- (5) Limit the rate of **password retries** with the **security policy editor**.
- (6) Implement **multi-factor authentication** on the systems.

DG IS&TD Diary No. 220  
PS TO CHIEF SECRETARY SINDH  
Diary No. 22267 18  
Dated 4.8.18  
Inward Date 3/9/2018  
Outward Date

*C/S*  
*Secy (I.T.) / GAC*

NO. PS/SECY/1.1/776  
Dated: 04/09/18  
*W*  
*4/9/18*

*DCI*  
*4.9.18*  
*[Signature]*

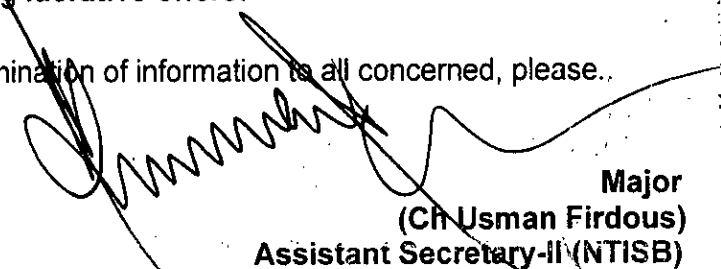
*[Signature]*  
*(2018/08/29)*

- (7) Update all **third party applications** with the latest patches.
- (8) **Turn off** a windows feature in control panel, by unchecking "**SMB 1.0/CIFS File Sharing Support**" in "Program and Features" tool.
- (9) Do not open email attachments from **untrusted 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 Unchecking "**SMB 1.0/CIFS File Sharing Support**" in "Program and Features" tool if not required.
- (4) Maintain Off line 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**.

4. Forwarded for perusal and dissemination of information to all concerned, please.

  
Major  
(Ch Usman Firdous)  
Assistant Secretary-II (NTISB)  
Ph# 051-9204560

**All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments**

Copy to :-

SPS to Cabinet Secretary, Cabinet Division, Islamabad  
PS to AS-III, Cabinet Division, Islamabad  
APS to Secretary, NTISB  
APS to Deputy Secretary, NTISB

