THE UNITED REPUBLIC OF TANZANIA

TANZANIA COMMUNICATIONS REGULATORY AUTHORITY

ISO 9001:2015 CERTIFIED

SAMSAM-RANSOMWARE NOTICE

1. Introduction:

Tanzania Computer Emergency Team (TZ-CERT) part of Tanzania Communication Regulatory Authority (TCRA) is informed of malicious software family of ransomware known as **SamSam-ransomware**. Similar to WannaCry-ransomware, SamSam has a tendency to encrypt files on the compromised systems and demands from victims a ransom in crypto-currency to decrypt them.

The SamSam actors target Information and Communication Technology (ICT) systems and services specifically of organisations. Based on statistics provided by Symantec, SamSam-ransomware attacks have hit nearly seventy (70) institutions in the United States earlier this year. The Federal Bureau Investigation (FBI) estimates that the SamSam group has received $6 million in ransom payments to date and caused over $30 million in losses to victims.

2. Mode of propagation:

The findings revealed that unlike WannaCry-ransomware which invades computer systems by exploiting Microsoft Windows Server Messaging Block (SMB) vulnerabilities, SamSam-ransomware uses a wide range of exploits or brute force techniques. Its actors exploit exposed Remote Desktop Protocol (RDP) from vulnerable Microsoft Windows Operating Systems through use of brute force attacks or stolen login credentials to gain access to a network and infect accessible host machines. Detecting RDP intrusions can be challenging since the malware enters through an approved access point, thus detection of RDP intrusion is not straight forward.

Initially, in early 2016, the SamSam actors used to exploit vulnerable web-based **JBoss Applications,** a proprietary open source Java platform developed by JBoss (a division of Red Hat Inc.) used to build, deploy and host highly transactional applications and services by means of **JexBoss Exploit Kit,** a kit with tools for testing and exploiting vulnerable Java application server and other Java platform, framework, application etc. Until now, the SamSam actors have discovered different approaches to infect targeted systems with SamSam-ransomware. Aside from JBoss Applications and RDP, SamSam actors can also

exploit vulnerabilities in Java-based web-servers, file transfer protocol (FTP), Virtual Networking Computing (VNC) and other remote desktop applications.

3. Phases of Executing SamSam Attacks:

Launch of an attack on the targeted system, might involve following approaches: -

3.1 **Scanning** for exposed Remote Desktop Protocol (RDP), VNC, and other vulnerable services to identified potential vulnerabilities. In this stage the actors employ different vulnerability scanning tools such as Nmap to identify exposed and vulnerable systems on the internet. According to the research conducted by SecureWorks Team, **over 3.2 million** hosts globally have RDP exposed.

For the case of Tanzania, **496 hosts** were found with RDP exposed based. Source: Different Threats Intelligence Systems for the month of September, 2018.

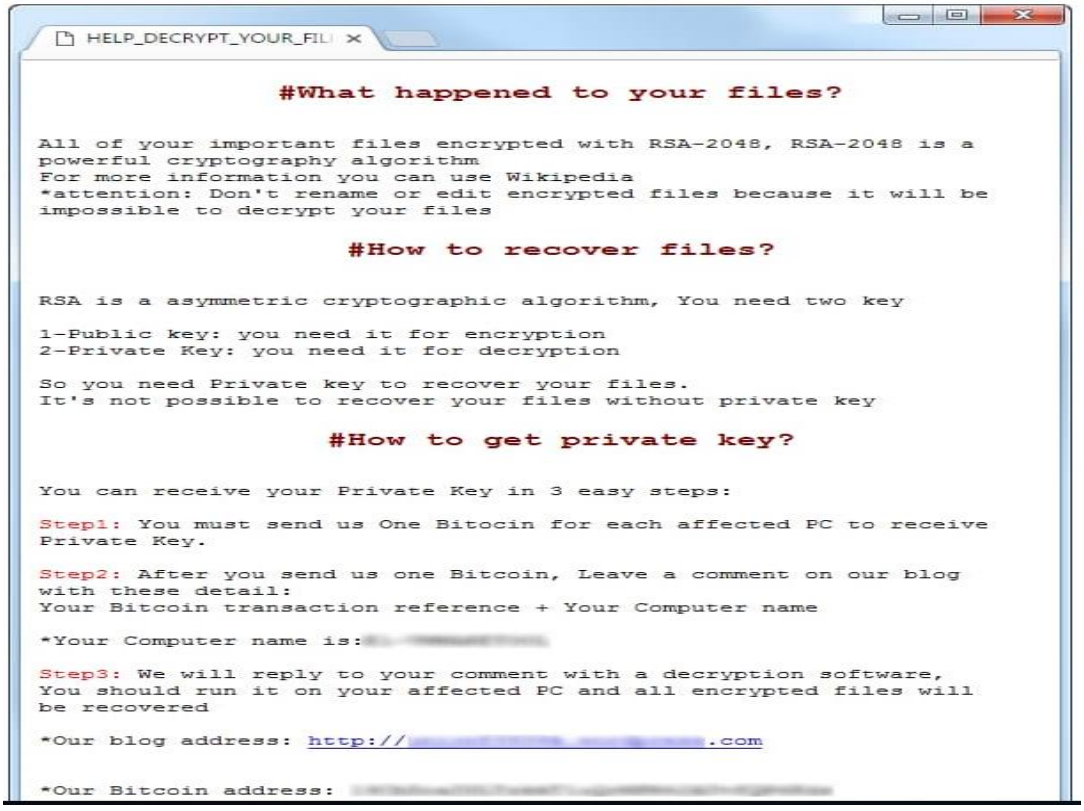
3.2 **Exploitation of vulnerabilities** - Earlier, the SamSam actors used to engage **JexBoss Exploit Kit**. Recent findings uncovered a wide range of other applications being used to exploit vulnerable systems, among them are "Mimikatz", "reGeorg", "PsExec", "RDPWrap", "NLBrute" etc.

3.3 **Elevation of privilege –** For the case of RDP, once the SamSam actor have access to the compromised systems via RDP, escalates privileges for administrator's by utilizing the credential harvesting tool such as Mimikatz, NLBrute and other similar tools.

3.4 **Deployment of SamSam-ransomware -** With administrative rights, SamSam-ransomware is deployed on the compromised host as executable file by utilizing batch scripts in combination with legitimate remote process execution tools like PsExec, Windows Management Instrumentation (WMI via Wmiexec.py) and RDP.

3.5 **Execution of SamSam-ransomware –** After deployment, SamSam encrypts files from compromised system and thereafter drops ransom notification to demand for payment in crypto-currency (Bitcoin) for the private decryption keys to be able to recover the files.

Figure No.1: Ransom Notification Page



4. Mitigation Measures:

Users and system administrators are urged to implement below control measures to mitigate the impacts of SamSam-ransomware attacks:

1. Scan your network to identify systems that use RDP for remote communication and disable the service if not needed.

2. Always keep your patch levels up-to-date, especially on computers that host public services and accessible for internet services, such as HTTP, FTP, mail, and DNS services.

3. Verify cloud-based virtual machine instances accessed over the internet have no open RDP ports, especially port 3389, unless there is a necessity of keeping the ports open.

4. Consider placing systems with an open RDP port behind a firewall and require users to use a Virtual Private Network (VPN) to access the internal systems.

5. Enforce strong passwords and account lockout policies to defend against brute force attacks; and where possible apply two-factor authentication.

6. Maintain a good back-up strategy.

7. Restrict permission to users connected to Local Area Network (LAN) to install and run unwanted software applications.

8. Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.

9. Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats such as .vbs, .bat, .exe, .pif and .scr files.

10. Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives; and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.

11. If Bluetooth is not required for mobile devices, it should be turned off. If needed, ensure that the device's visibility is set to "Hidden" to prevent from being scanned by other Bluetooth devices. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.

5. Important to System Administrators:

It's recommended for administrators to review the following SamSam Malware Analysis reports of four different malware variants for more information: -

1. MAR-10219351.r1.v2 – SamSam1
2. MAR-10166283.r1.v1 – SamSam2
3. MAR-10158513.r1.v1 – SamSam3
4. MAR-10164494.r1.v1 – SamSam4

6. Reference:

1. https://blog.barkly.com/what-is-samsam-ransomware-2018
2. https://www.us-cert.gov/ncas/alerts/AA18-337A
3. https://github.com/joaomatosf/jexboss
4. https://www.technopedia.com/definition/3525/jboss-application-server-jboss-as
5. https://www.us-cert.gov/security-publications/Ransomware.
6. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/how-to-mitigate-samsam/
7. https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks