THE UNITED REPUBLIC OF TANZANIA

TANZANIA COMMUNICATIONS REGULATORY AUTHORITY

ISO 9001:2015 CERTIFIED

SECURITY NOTICE

RANSOMWARE OUTBREAK

1. Introduction

Recently, Tanzania Computer Emergence Response Team (TZ-CERT) has observed an increase in ransomware attacks across the globe.

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Principally, it encrypts files on the compromised systems and demands from victims a ransom in crypto-currency to decrypt them.

December last year, TZ-CERT published security notice on a variant of ransomware known as SamSam detailing mode of propagation, impacts and its control measures. Since then, however, there has been an evolution of threats landscape such that ransomware actors have discovered new and sophisticated techniques for attacking.

Pursuant to section 6(s) of Electronic and Postal Communication (Computer Emergency Response Team), TZ-CERT is responsible to proactively provide early warning on eminent cybersecurity incidents. As part of providing its proactive services to stakeholders, this notice has been prepared to share security strategies and best practices to help mitigating and effectively responding to ransomware attacks.

2. Impacts

The impact of a successful ransomware attack can be severe to a targeted organization or individuals. This may include loss of access to data, systems or leads to operational outages. The potential downtime, coupled with unforeseen expenses for restoration, recovery, and implementation of new security processes and controls can be devastating and always difficult to quantify in monetary terms.

3. Propagation

The ransomware infections are transmitted to targeted systems in mainly two ways:

3.1. Manual propagation

Upon getting access into victim's machine and obtain administrative privileges, the ransomware actor may execute either of the following: -

3.1.1. Manually run encryptors on targeted systems;

3.1.2. Deploy encryptors on a victim's machine using Windows batch files (mount C$ shares, copy the encryptor, and execute it with the Microsoft PsExec tool);

3.1.3. Deploy encryptors with Microsoft Group Policy Objects GPOs); or

3.1.4. Deploy encryptors with existing software deployment tools utilized by the victim organization.

3.2. Automated propagation

This may involve the following: -

3.2.1. Extract credential or Windows token from Hard disk (HDD) or memory;

3.2.2. Leverage trust relationships between systems such as Windows Management Instrumentation (WMI), Server Messaging Block (SMB), or PsExec to bind to systems and execute payload; and

3.2.3. Exploit unpatched Windows vulnerabilities (e.g. EternalBlue or MS17-010).

4. Security strategies combat ransomware

TZ-CERT encourages its constituents to take note of the following security best practices to help prevent, mitigate and recover from ransomware attacks: -

4.1. Preventive measures

Prevention is the most effective defence against ransomware and it is critical to take precautions for protection.

TZ-CERT recommends to take the following preventive measures against to protect their computer networks from falling victim to a ransomware infection: -

4.1.1. Raise awareness of ransomware and enhance appropriate technical expertise. End users are targets and cyber-actors are constantly exploiting human vulnerabilities, employees and individuals should be aware of ransomware threats.

4.1.2. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

4.1.3. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

4.1.4. Configure firewalls to block access to known malicious IP addresses;

4.1.5. Patch operating systems, software, and firmware on devices, consider using a centralized patch management system.

4.1.6. Set anti-virus and anti-malware programs to conduct regular scans automatically;

4.1.7. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;

4.1.8. Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

4.1.9. Scan and remove macro scripts from files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

4.1.10. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

4.1.11. Consider disabling Remote Desktop Protocol (RDP) if it is not being used;

4.1.12. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

4.1.13. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

4.1.14. Educate your personnel – Attacker often enter the organization by exploiting human vulnerabilities i.e. tricking users to disclose password or click on a virus-laden email attachment.

Keep on reminding users to never click unsolicited links or open unsolicited attachment in emails.

4.2. Business Continuity Considerations

4.2.1. Back up data regularly - verify the integrity of the backups and test the restoration process to ensure it is working;

4.2.2. Secure your backups - ensure backups are kept offline i.e. not connected permanently to the computers and networks they are backing up. Some instances of ransomware known as persistent synchronization, have the capability to lock cloud-based backups when systems continuously back up in real time.

Backups are critical in ransomware recovery and response; if infected, a backup may be the best way to recover your critical data; and

4.2.3. Perform vulnerability assessment and penetration test to systems and network infrastructure to uncover potential vulnerabilities for corrective measures to improve security posture of your organization.

4.3. Actions to recover if impacted

In case preventive measures fail, consider taking the following steps upon being hit by ransomware: -

4.3.1. Isolate the infected computer immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or shared computing resources;

4.3.2. Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware;

4.3.3. If possible, change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system.

4.3.4. Delete Registry values and files to stop the program from loading.

4.3.5. Report the incident to TZ-CERT for technical assistance.

5. Important to victims

TZ-CERT understands that falling victims of ransomware attacks can be frustrating and may necessitate expenditure of funds for payment of a ransom to recover valuable information that has been held hostage. However, it is important to consider the following security risks prior to pay the ransom;

5.1. Paying a ransom does not guarantee a victim to regain access to data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom;

5.2. Some victims who paid the demand have reported being targeted again by ransomware actors;

5.3. After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key; and

5.4. Paying could inadvertently encourage this criminal business model.

In principal, victims are urged to report any cybersecurity incident to TZ-CERT for immediate assistance and avoid meeting attackers' demands.

6. References

6.1. https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf

6.2. https://www.fireeye.com/blog/threat-research/2019/09/ransomware-protection-and-containment-strategies.html

6.3. https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf