THE UNITED REPUBLIC OF TANZANIA

TANZANIA COMMUNICATIONS REGULATORY AUTHORITY

ISO 9001:2015 CERTIFIED

SECURITY NOTICE

"PHOBOS" RANSOMWARE ATTACK

1. Introduction

One month ago, Tanzania Computer Emergency Team (TZ-CERT) published a security notice on spreading of ransomware detailing its propagation method, impacts and remedial measures that organizations and individuals can take to better manage and respond to its attacks.

Furthermore, TZ-CERT has observed a new and sophisticated techniques that ransomware actors are currently using to infect targeted victims across the globe. The ransomware actors have launched a new variant of ransomware known as **"Phobos"** reported to take advantage of an open or poorly secured Remote Desktop Port (RDP) from a victimized computer system as well as exploitation of human weaknesses through use of social engineering methods.

Similar to other ransomware attacks, phobos malware encrypts data from infected systems and keeps it hostage until a ransom is paid in bitcoin cryptocurrency. Upon taking control of the affected systems, phobos renames encrypted files in "dot phobos" file extension bearing victim's unique identity (ID) and email address.

Pursuant to section 6(i) of the Electronic Postal Communications (CERT) Regulations 2018, TZ-CERT is mandated to issue guidelines, advisory and vulnerability notes relating to information on security practices, procedures, prevention, response and reporting of cyber threats.

In view of the above, TZ-CERT wishes to inform its constituents and stakeholders on existance of **phobos malware** and share security best practises to help mitigate and better respond to its attacks.

2. Impacts

The impact of a successful **"phobos"** attack may result to loss of access to data, systems or interruption of critical business operations. 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 “phobos” malware is infected into targeted systems through: -

3.1. Spam email containing effected link/attachment i.e. by opening/clicking email attachments or links infected with **phobos malware**. Opening/clicking these attachments/links allows installation of the **phobos malware** or other high-risk viruses into host’s machines;

3.2. Use of an open or poorly secured Remote Desktop Port (RDP) port.

3.3. Fake software updates; downloading and installation of malicious software and application updates. i.e. downloading contaminated updates from criminals sites;

3.4. Download and installation of unlicensed software i.e. Phobos actors use untrustworthy software download sources such as freeware download websites, free file hosting websites, and peer-to-peer networks) to disseminate malicious files; and

3.5. Exploit bugs/flaws of an outdated software or applications.

4. Symptoms of “Phobos” infections

The infection of “phobos” malware may include following symptoms: -

4.1. Display of a ransom note on desktop demanding payment of funds in bitcoins cyptocurrency for “phobos” actors to unlock encrypted files;

4.2. Computer resources that were previously usable are rendered inaccesible i.e. denied user’s access to her/his stored data or computer system; and

4.3. Change of files names and extensions i.e. infected files are renamed in **“dot phobos”** file extension bearing victim's unique identity (ID) and email address.

Figure 1: Screenshot of phobos’s notification after infecting a victim.

All your files are encrypted
*To decrypt your files, contact us using this e-mail: Cadillac.407@aol.com Please set topic 'Encryption ID: ********'.*
We offer free decryption of your test files as a proof. You can attach them to your e-mail and we'll send you decrypted ones.
Decryption price increases over time, hurry up and get discount.
Decryption using third parties may lead to scam or increased price.

Figure 2: Text presented by phobos's malware after infecting a victim.

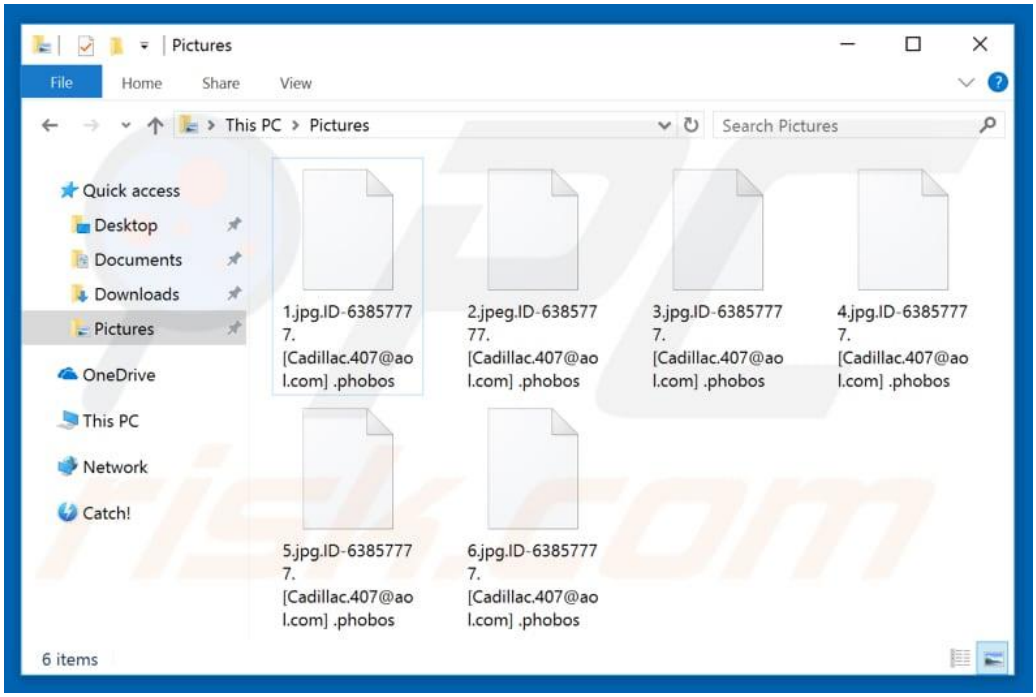

Figure 3: Screenshot of another variant of phobos ransomware pop-up window

5. Mitigation

Apart from remedial measures shared in the previous published ransomware security notice accessible on TZ-CERT's website, users/organizations are urged to take note of the following security best practises to avoid falling victims of "phobos" attacks:-

5.1. Avoid opening links/attachments presented in unsolicited emails. If you receive an email that contains an attachment (or web link) sent from an unknown/untrustworthy email address, do not open the attachment or click the presented link;

5.2. Always download software using official websites or other reliable sources and don't use third party downloaders or other dubious tools;

5.3. Use reputable anti-virus or anti-spyware software i.e. tools that can detect and eliminate various threats (computer infections) before they can do any damage to your computer;

5.4. Avoid installing unlicensed software and applications on your computer systems. Most cyber criminals do such software and applications as attack vectors to spread malicous programs and use to install a back door for launching cyber attacks;

5.5. If your computer is already infected with Phobos, it is recommended to run a scan with anti-spyware preferably **"SpyHunter"** to automatically eliminate the ransomware, or else manually remove the malware by refering steps in this link;

5.6. It is advisable to use official software updating tools to update your computer system i.e. use tools or implemented functions that are provided by official software developers only;

5.7. Properly configure Remote Desktop Port (RDP) or disable it if unusable;

5.8. Enable and properly configure firewall to detect and prevent malicious inbound network traffics;

5.9. Properly configure the mailserver to detect and prevent spams with malicious files extensions, links and attachments;

5.10. Properly configure the Local Area Network (LAN) to improve network performance and security i.e. controlling spreading of malware infections across the network;

5.11. Install and maintain reliable anti-malware software;

5.12. Check regularly for available software updates and apply them.

5.13. Disable macros in Microsoft office documents; and

5.14. Backup your data regularly and store it at a secure location.

6. Important

TZ-CERT is urging its constituents and stakeholders to report the incidents of phobos attacks for immediate technical assistance and also refer published ransomware security notice accessible on TZ-CERT's website to obtain more information on how to combat ransomware attacks and improve cybersecuirty posture.

7. References

7.1. https://www.pcrisk.com/removal-guides/14258-phobos-ransomware

7.2. https://bestsecuritysearch.com/completely-remove-phobos-virus-computer/