THE UNITED REPUBLIC OF TANZANIA

TANZANIA COMMUNICATIONS REGULATORY AUTHORITY

ISO 9001:2015 CERTIFIED

SECURITY NOTICE

"PHOBOS" RANSOMWARE ATTACK

1. INTRODUCTION

Ransomware infections has continued to spread and affect individuals and organizations of all sizes across the globe. Ransomware is a form of malware or a virus that prevents users from accessing their systems or data until a sum of money is paid. Ransomware actors have been using different attack vectors to infect targeted computer systems with malware. To date there are more than 1000 variants of ransomware with diverse attacking techniques.

As part of fulfilling its mandates, Tanzania Computer Emergency Team (TZ-CERT) part of Tanzania Communications Regulatory Authority (TCRA) published on its website - www.tzcert.go.tz ransomware security notice 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 technique that ransomware actors are currently using to infect targeted victims across the global with variant of ransomware known as **"Phobos"** reported to take advantage of an open or poorly secured **Remote Desktop Port (RDP)** from a 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.

2. IMPACTS

A successful phobos attack may result to loss of access to data, interruption of critical business operations and financial loss from payment of ransom in vain attempt to restore encrypted even though the potential downtime, coupled with unforeseen expenses for restoration, recovery, and implementation of new security processes and controls can be devastating and difficult to quantify in monetary terms.

3. PROPAGATION

It is either through clicking email attachments or links infected with **phobos malware**, exploitation of an open and poorly secure remote desktop protocol (RDP) port or download of movies, software and applications from malicious sites such as torrents etc.

4. SYMPTOMS OF PHOBOS INFECTIONS

Display of a ransom note on desktop demanding payment of funds in bitcoins cryptocurrency to "phobos" actors, denied access to computing resources that were previously usable, change of files names and extensions i.e. infected files renamed to different file extension such as ".phobos", ".phoenix", ".barak", ".adage", ".blend", ".acute" bearing victim's unique identity (ID) and email address.

5. MITIGATION

Threats actors are constantly inventing new and sophisticated methods to infect victims with a malware, however, the impact of a successful infection can be significantly reduced if a robust data backup process is in place. Comprehensive data backups should be scheduled as often as possible and must be kept offline in a separate and secure location. The most effective method to prevent ransomware infections is to adhere to security best practices on appropriate and safe use of internet

and information and communication technology (ICT). Further regular cybersecurity training and awareness programs to ensure proficient in safe Internet-browsing techniques and the ability to identify phishing emails.

6. IMPORTANT

You are advised to report to TZ-CERT through incidents@tzcert.go.tz of any security incident encountered for immediate technical assistance. You are further advised to also refer ***ransomware security notices*** published on TZ-CERT website: https://www.tzcert.go.tz to obtain further information on how to manage and respond to ransomware attacks.

Issued by:
DIRECTOR GENERAL,
TANZANIA COMMUNICATIONS REGULATORY AUTHORITY
24th October 2019