E-GOVERNMENT AGENCY

ICT SECURITY ADVISORY

ADVICE NO: eGASEC03167 – Unpatched Windows Operating Systems under attack worldwide

eGA

13-May-17

APPLICABLE TO: ALL PUBLIC INSTITUTIONS

e-Government Agency shall promote a secure computing environment for public servants and all stakeholders. This document will help ensure that all vulnerable computing platforms on government networks/systems/websites are guarded against vulnerabilities and protected at all times.

UNPATCHED WINDOWS OPERATING SYSTEMS UNDER ATTACK

1. INTRODUCTION

On Friday 12th May, 2017 in United Kingdom, NHS Hospitals were hit by a large-scale cyber-attack by a malware/ransomware named "WannaCry / WannaDeCrypt0r", the ransomware encrypted data on the computers, it demands payment in three days or the price is doubled, and if none is received in seven days the files will be deleted, the screen message claims. A lot more other countries and firms like Russia interior Ministry, Spanish telecom giant Telefonica and FEDEX have experienced similar attacks and acknowledged that some of their Windows OS based computers have been rendered useless.

Cyber extortionists tricked victims into opening malicious malware attachments to spam emails that appeared to contain invoices, job offers, security warnings and other legitimate files. Also, the malware was said to scan and affect devices with security flaws on the same network.

Researchers with security software maker Avast said they had observed 57,000 infections in 99 countries, with Russia, Ukraine and Taiwan being the top targets.

These attacks are related to NSA claimed flaw that was released in April 2017. An online hacker group "Shadow brokers" tried to auction cyber weapons stolen from NSA, after turning up with no buyers they decided to dump/leak the tools and other hacking secrets online. Those tools have been utilized by cybercriminals/hackers worldwide for various purposes. Mostly they target Windows Operating Systems that exists with vulnerabilities from Windows 2000 up to Server 2012 and Windows 7 and 8.

Microsoft released patches for the some of the vulnerabilities even before the leak and other vulnerabilities have been patched via windows update since then, however not all systems are updated/patched out there.

2. IMPLICATIONS

With the massive attacks happening around the world, the following are the implications;

i) Unpatched Windows Operating Systems from workstations to servers are at risk of being infected by the "Wanna DeCrypt0r" and related malwares targeting unpatched windows systems.

ii) Public Institutions data that rely on Windows Operating Systems like Outlook, SharePoint, File Servers and Active directories are at risk of falling under extortion.

iii) All poorly protected windows based workstations/servers will get infected once one computer gets infected on your Institution's network.

iv) Ultimately your business operations will be disrupted or halted.

3. ADVISORY TO ADDRESS THIS INCIDENT (eGASEC03167)

The following are the advised course of actions to remediate the issue;

i. All Public Institutions are advised to inspect windows based computers for signs of ransomware infection and disconnect from the network of the suspected infected computers and report it to Government ICT Security Team via ***gicts@ega.go.tz*** (*This guide or the steps in your incident response plan is recommended to be followed*).

ii. For uninfected Windows OS enabled devices disable/remove SMB1 as a temporary measure and make sure you are blocking port 445 in your firewalls.

iii. Update/patch all unpatched windows operating systems at your Institution (*Follow patch management procedures if available*). This should be done periodically.

iv. Let all users at your Institutions know that they should not download and open unknown mail attachments as well as they should not download and install cracked/pirated applications or unknown applications from the internet.

v. Also, let your Institution users know that they should be extremely wary of any Microsoft Office email attachment that advises them to enable macros to view its content. Unless they are absolutely sure that it is a genuine email from a trusted source, they should not enable macros and instead immediately delete the email and report it to your security mail.

vi. In case opening suspicious attachment or installation of suspicious application has happened, let users know that they should report to your institution designated ICT security email that is like ictsecurity@yourInstitution F.Q.D.N e.g. ictsecurity@utumishi.go.tz). For escalation if the issue is unresolved the ICT Security Single Point of Contact (SPOC) for your Institution should report the incident to Government ICT Security Team via ***gicts@ega.go.tz.***

vii. All Public Institutions should be on alert to activate the Disaster Recovery Plan in case of this attack or related security incident.