UGANDA NATIONAL COMPUTER EMERGENCY RESPONSE TEAM (CERT.UG)

27/06/2017

INFORMATION SECURITY ALERT – IMPORTANT

Vulnerability Type: Ransomware

Variant: Petya

Severity: CERT.UG rates the severity of this vulnerability as **HIGH** due to ransomware's capability to cause data loss and negatively affect work environment productivity. This particular strain of ransomware encrypts the filesystem's Master File Table (MFT).

Risk Assessment: Ransomware refers to sophisticated software that utilizes advanced encryption algorithms to block system files and demand payment in return for the key that can decrypt the blocked content. A ransomware attack is potentially damaging to an organization's data with very high chances of complete data loss (on infected computers) as well as disruption in user productivity. Petya ransomware encrypts the master boot records of infected Windows computers, making affected machines unusable.

Vulnerability: The ransomware attack vector is through phishing e-mails and compromised websites. To a large extent, we have noticed that the main attack vector is through users who click on spam e-mail that contains malicious links or attachments. This attack is also made easier due to computers running unpatched Windows Operating Systems and lack of effective anti-malware protection.

Risk Mitigation: It's important to note that chances of recovery of encrypted data are very slim especially with the latest strains of ransomware. The best mitigation strategy is prevention which can be achieved through the following:-

a) Patch up all Windows Operating Systems using the Microsoft Security Bulleting MS17-010 via https://technet.microsoft.com/library/security/MS17-010
b) Keeping up to date back-ups of all critical data;
c) Ensuring that all systems are patched up (especially the browsers and all its plugins);

d) Ensuring that the principle of 'Least Privilege Access' is adhered to for all users;
e) Ensuring effective use of effective anti-virus solutions on all computers as well as rootkit scanners on critical servers (effective anti-virus should cover all the five distinct layers of protection: network, file, reputation, behavioral and repair). All e-mails and web downloads should be scanned to reduce exposure;
f) Ensuring only the necessary browser plugins are enabled;
g) All web traffic should be filtered to block potential threats; and
h) Awareness and education on safe web surfing skills as well as e-mail usage to all staff on avoid spam and phishing campaigns (especially e-mails with the .zip or .scr attachments in e-mails from unknown sources).
*****Awareness and education in addition to the technical setup is very effective in reducing exposure;

Workaround: In the event that any user on your network has been compromised, kindly undertake the following:

a) Immediate disconnection of the affected computer from the network. The more ransomware lingers on the network, the more it spreads;
b) Undertaking cleaning up any traces of ransomware. Some of the ransomware strains have available solutions for data recovery whereas the latest strains are more difficult when it comes to data recovery; and
c) Kindly inform us and we'll assist.

Note: Kindly contact us in case you would like us to:

a) Undertake an evaluation of your current network protection in order to identify improvement areas; and
b) Hold an awareness session for all your staff members.

Uganda National Computer Emergency Response Team
Plot 7A, Rotary Avenue (Former Lugogo Bypass)
Twitter: @CERT.UG | Facebook: Cert1.ug
info@cert.ug
www.cert.ug