UGANDA NATIONAL COMPUTER EMERGENCY RESPONSE TEAM (CERT.UG)

30/6/2017

UPDATED INFORMATION SECURITY ALERT – IMPORTANT

Vulnerability Type: Lethal Wiper Malware

Severity: CERT.UG rates the severity of this vulnerability as **HIGH** due to the Malware's capability to cause complete data loss and negatively affect work environment productivity. This is critical for all unpatched Microsoft Operating systems especially the earlier versions such as Windows XP and Windows Server 2003.

Risk Assessment: Wiper Malware refers to sophisticated malicious software that destroys data on the compromised hard disk with extremely low chances of recovery. A successful attack is therefore disastrous due to the challenge in recovery of data and loss of productivity hours.

Vulnerability: This latest strain of this malware attack vector is highly lethal and evasive since its designed to spread through unsegmented networks infecting other hosts and encrypting the Master File Tree (MFT) tables for NTFS partitions followed by overwriting the Master Boot Record (MBR). This prevents a user from booting a compromised host. The entry exploit is the earlier communicated Windows SMB Vulnerability which was fixed by the Microsoft Security Bulleting - MS17-010.

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

IMMEDIATE ACTION

a) Urgently apply the latest Microsoft Security Update MS17-1010 – this reduces the affected SMB Server vulnerability used in this attack;
b) Avoid SMB (Port 445) and RDP on Servers;
c) Disable SMB1 or Block incoming traffic to port 445;
d) Kill Switch: create a file in %windir% called perfc.dat, this prevents creation of perfc.dat file by the malware. Also deny write permissions to perfc.dat
e) Block the following URLs in your environment:
    i. http://mischapuk6hyrn72.onion
    ii. http://petya3jxfp2f7g3i.onion

iii. http://mischa5xyix2mrhd.onion/MZ2MMJ
iv. http://mischapuk6hyrn72.onion/MZ2MMJ
v. http://french-cooking.com/
vi. http://benkow.cc/71b6a493388e7d0b40c83ce903bc6b04.bin
COFFEINOFFICE.XYZ
vii. http://petya3jxfp2f7g3i.onion/MZ2MMJ
viii. http://petya3sen7dyko2n.onion/MZ2MMJ
ix. Consider blocking access to all .onion domains

f) Block the following IP addresses:
   i. 95.141.115.108
   ii. 185.165.29.78
   iii. 84.200.16.242
   iv. 111.90.139.247
g) Update all Anti-Virus and Firewall Hashes;
h) Keep up to date back-ups of all critical data. Also test and make a separate copy of the backup. A Copy of backed up data MUST be stored offline;
i) Test and practice data recovery procedures for effectiveness;
j) Ensure that all systems are patched up (especially all Microsoft Windows Operating System, browsers and all its plugins);
k) Disable macro scripts in files transmitted via email;
l) Scan all incoming and outgoing emails to detect threats and filter executable files (extensions such as exe and scr) from reaching end users.

MUST DO:

m) Ensuring that the principle of 'Least Privilege Access' is adhered to for all users;
n) Ensuring effective use of effective anti-malware solutions on all computers as well as rootkit scanners on critical servers (effective anti-virus covers 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;
o) All web traffic should be filtered to block potential threats;
p) Review SMB Encryption as relates to your environment: https://technet.microsoft.com/en-us/library/dn551363(v=ws.11).aspx
q) 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)

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

a) Immediate disconnection 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;
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 area; 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