UGANDA NATIONAL COMPUTER EMERGENCY RESPONSE TEAM AND COORDINATION CENTER (CERT.UG/CC)

25/10/2017

BAD RABBIT RANSOMWARE ADVISORY

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. Bad Rabbit ransomware encrypts victim's files and disk using the AES-128-CBC and RSA-2048 algorithms

Risk Assessment: Bad Rabbit ransomware 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.

How it spreads: The initial vector for this latest strain of ransomware is through 'drive-by attacks.' Essentially, attackers compromise unsecured websites to install malware droppers. In this case, the malware is disguised as Adobe Flash installer. The ransomware is activated (encrypts Windows files, video and audio) when a user visits a compromised website and clicks on the prompt to install the fictitious Adobe Flash installer. Security researchers note that if started, it will save the malicious DLL as C:\Windows\infpub.dat and launch it using rundll32. Also identified is that infpub.dat appears to be capable of brute-forcing NTLM login credentials to Windows machines that have pseudo-random IP addresses.

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) Create awareness amongst your users since the ransomware requires user action to spread
b) Urgently apply the latest patches for all your systems
c) Restrict rights to install software on your network to only those that need them
d) Restrict execution of files with the paths c:\windows\infpub.dat and C:\Windows\cscc.dat

e) Update all Anti-Virus and Firewall Hashes
f) 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
g) Test and practice data recovery procedures for effectiveness
h) Ensure that all systems are patched up (especially all Microsoft Windows Operating System, browsers and all its plugins)
i) Disable macro scripts in files transmitted via email
j) 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:

k) Ensuring that the principle of 'Least Privilege Access' is adhered to for all users
l) Ensuring effective use of effective anti-malware 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)
m) All web traffic should be filtered to block potential threats
n) Awareness and education on safe web surfing skills

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

a) Immediately disconnect the affected computer from the network. The more ransomware lingers on the network, the more it's chances of spreading;
b) Clean 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 and Coordination Center
Plot 7A, Rotary Avenue (Former Lugogo Bypass)
Twitter: @CERT.UG | Facebook: Cert1.ug
info@cert.ug
www.cert.ug