Cyber Attack Security Bulletin

Stolen National Security Agency (NSA) Hacking Tools Made Freely Available on the Internet!

Thousands of Computers Attacked with "WannaCry" Ransomware - More Waves of Attacks Expected!

"WannaCry" Ransomware has affected **FedEx**, thousands of **Hospitals** and **Hospital Emergency Rooms** in the US, **Great Britain's NHS (National Health Service)**, as well as **Railroads**, **Police Stations**, 85% of the computers at the Spanish Telecom firm Telefonics, and many others including The United States, Russia, Germany, Turkey, Italy, Philippines and Vietnam, India and Scotland and over 150 other counties in less than 24 hours.

"**WannaCry**" Ransomware, turned loose on the Internet by a group called "**The Shadow Brokers",** unleashed a horde of Windows hacking tools and exploits allegedly purported to be stolen from the NSA (National Security Agency) that works on almost all versions of Windows.

The Hacking tools are purported to have belonged to "Equation Group", an elite cyber-attack unit linked to The National Security Agency (NSA). The Archive that contained the tools has been unencrypted and is widely available for download on many file sharing sites world wide.

The Microsoft Security Team discovered that most of the vulnerabilities that the hacking tools exploited had already been patched by a recent "Patch Tuesday Update".

"**WannaCry**" Ransomware is spread by taking advantage of Windows vulnerability that Microsoft released a security patch for in March. But computers and networks that haven't updated their systems are at risk.

Once infected with the "WannaCry" Ransomware, victims are asked to pay a ransom in order to remove the infection from their PC's or their PC's will remain unusable, and their files permanently locked.

Steps on how to avoid Ransomware

Derived and Modified by Flicker From https://www.us-cert.gov/security-publications/Ransomware

Patch you operating system with the latest Windows Updates using Windows Update!

Beware of emails – NCCIC has received multiple reports of WannaCry Ransomware infections worldwide. Ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, Ransomware is frequently delivered through phishing emails and exploits unpatched vulnerabilities in software.

Phishing emails are crafted to appear as though they have been sent from a legitimate organization or known individual. These emails often entice users to click on a link or open an attachment containing malicious code. After the code is run, your computer may become infected with malware.

- **Be careful when clicking directly on links in emails**, even if the sender appears to be known; attempt to verify web addresses independently (e.g., contact your organization's helpdesk or search the Internet for the main website of the organization or topic mentioned in the email).
- **Exercise caution when opening email attachments**. Be particularly wary of compressed or ZIP file attachments in Emails or portable media such as USB drives.
- **Update to the patch regarding Microsoft Security Bulletin MS17-010, by using Windows Update on your Computer** - Follow best practices for Server Message Block (SMB) and update to the latest version immediately. (See US-CERT's SMBv1 Current Activity - https://www.us-cert.gov/ncas/current-activity/2017/03/16/Microsoft-SMBv1-Vulnerability for more information.)

Cyber Attack Security Bulletin

For general best practices on patching and phishing, users should:

- **Ensure that your applications and operating system has been patched with the latest updates**. Vulnerable applications and operating systems are the target of most attacks. (See Understanding Patches - https://www.us-cert.gov/ncas/tips/ST04-006 .)
- **Be suspicious of unsolicited phone calls**, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- **Avoid providing personal information** or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- **Avoid revealing personal or financial information in email**, and do not respond to email solicitations for this information. This includes following links sent in email.
- **Be cautious about sending sensitive information over the Internet before checking a website's security**. (See Protecting Your Privacy - https://www.us-cert.gov/ncas/tips/ST04-013)
- **Pay attention to the URL of a website**. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- **If you are unsure whether an email request is legitimate, try to verify it** by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from anti-phishing groups such as the APWG - http://www.antiphishing.org/ .
- **Install and maintain anti-virus software, firewalls, and email filters** to reduce some of this traffic. (See Understanding Firewalls - https://www.us-cert.gov/ncas/tips/ST04-004 , Understanding Anti-Virus Software - https://www.us-cert.gov/ncas/tips/ST04-005 , and Reducing Spam - https://www.us-cert.gov/ncas/tips/ST04-007 for additional information.)

If you believe that you have been a victim of a phishing attack or Ransomware infection, immediately report the incident to your information technology (IT) helpdesk or security office.

For More Information, Resources and How to Report an Incident go to:
www.techsourcenews.com/cyber

Be careful of Emails, Web Search Links, and others offering remedies for these afflictions – Here are Our Credentials:

Flicker Thomas Master Telecom Agent
(800) 899-5350 flicker@flickertronics.com www.flickertronics.com
Flickertronics Business Internet and Phone Service Provider
55 S Dixie Hwy.
St Augustine, Florida 32084
Providing Business IT Support for Over 20 Years

Visit our News, Information and Free Virus Removal site www.techsourcenews.com

Flickertronics Partner, Solarwinds, is used by over 1 million IT professionals, and deployed by the following agencies:

http://www.solarwinds.com/federal-government/government-partners