ESTABLISHED 1907
YOUR COMMUNITY · YOUR COMMITMENT
FIRST NORTHERN
BANK & TRUST
1stnorthernbank.com • Member FDIC

Cyber Security News

Volume 2, Issue 2
June, 2019

In this issue

Wormable Flaw in Windows

In a Blog post published on May 30th, members of the Microsoft Security Response Center cited findings published Tuesday by Errata Security CEO Rob Graham that almost 1 million Internet-connected computers remain vulnerable to the attacks.

“Microsoft is confident that an exploit exists for this vulnerability, and if recent reports are accurate, nearly one million computers connected directly to the internet are still vulnerable to CVE-2019-0708. Many more within corporate networks may also be vulnerable. It only takes one vulnerable computer connected to the internet to provide a potential gateway into these corporate networks, where advanced malware could spread, infecting computers across the enterprise. This scenario could be even worse for those who have not kept their internal systems updated with the latest fixes, as any future malware may also attempt further exploitation of vulnerabilities that have already been fixed.

If you haven’t already, please patch your systems to protect yourself and your company from this vulnerability.

Tech Support Scams: The variants are seemingly endless

“Hello, we are calling from Windows and your computer looks like it is infected. Our Microsoft Certified Technician can fix it for you.”

Tech support scams are a million-dollar industry and have been around since 2008. Every single day, innocent people are tricked into spending hundreds of dollars on non-existent computer problems. There is no sign of these scams slowing down, despite several actions taken by the Federal Trade Commission.

How tech support scams work

Cold calls from fake Microsoft (etc.) agents

The scam is straightforward: pretend to be calling from Microsoft, gain remote control of the machine, trick the victim with fake error reports and collect the money.

If you ever get a call from a Microsoft or Windows tech support agent out of the blue, the best thing to do is simply hang up. Scammers like to use VoIP (Voice over Internet Protocol) technology so their actual number and location are hidden. Their calls are almost free which is why they can do this 24/7.

As per Microsoft:

“You will never receive a legitimate call from Microsoft or our partners to charge you for computer fixes. “

Toll-Free Numbers (TFN) for fraudulent tech support companies

These companies heavily advertise on popular search engines as well as websites with high traffic. People call them for assistance and get fooled with similar techniques employed by cold callers.

Another source for these companies comes from some of their existing customers or customers of parent companies sent to them. The remote technician upsells the customer who only came to activate their software but ends up forking hundreds of dollars on “Windows support.”

Fake pop-ups claiming your computer is infected—reminiscent of FakeAV—are used by scammers to reel in innocent victims.

If you decide to call in for remote computer assistance, you need to be very careful about which company you are going to deal with. Simply picking the top ad on a search results page could end very badly.

Unfortunately, the company or technician being from the US is not a guarantee for honest service. Many businesses in the US are using dirty tricks to take advantage of people, with the unsavvy and elderly as their prime targets.

Remote access

The ‘technician’ requests to have remote access to your computer and may use remote login software to do so. Note that while these applications are perfectly legitimate, it is important to remember that if you run this type of software, you are effectively giving a complete stranger total control of your computer.

Continued on Page 2 →

New malware is bricking IoT devices

A new strain of malware, named Silex, is wiping the firmware of IoT (Internet of Things) devices. The malware had bricked (made them inoperable) around 350 devices when the investigation started, and the number quickly spiked to 2000, about an hour later. Silex works by trashing a devices storage, dropping firewall rules, removing the network configuration, and then halting the device.

It's as destructive as it can get without actually frying the IoT's devices circuits. To recover, victims must manually reinstall the device's firmware, a task too complicated for the majority of device owners.

It's expected that some owners will most likely throw devices away, thinking they've had a hardware failure without knowing that they've been hit by malware.

This malware was developed by a 14-year-old teenager who plans to develop the malware further and add even more destructive functions.

If you have any IoT devices, including smart lights, smart cameras, a smart coffee maker….etc., make sure to secure these devices. If you are unsure how to secure your particular device, reach out to the manufacturer and find out how to enable security settings.

Tech Support Scams - Continued

Screenlockers

A method that has been gaining popularity by tech support scammers is to spread malware with the sole purpose of locking the user out of his own computer. They may look like a BSOD (Blue Screen of Death) or a warning that you are using illegal software (asking for a registration key). The malware is offered as part of a bundle or posing as an installer for something else.

The ones that look like a BSOD usually have a telephone number on them that belongs to the scammers outfit. Once you call that number they will tell you a trick to get rid of the BSOD to gain your trust, but of course the trick was built into the program for that reason. The type asking for a registration number usually has a telephone number as well, but often they come with a few links that will open sites with popular remote assistance/ desktop software like TeamViewer, LogMeIn, Ammy Admin, Supremo, and others. In these cases, the scammers will ask you to install that software and give them your access code, so they can "repair" your computer. Selling you overpriced solutions and "service contracts" is the real goal.

Tricks you should look out for

Once logged into your computer, the remote technician will attempt to trick you by fabricating errors or even viruses on your computer. They like to use the default Windows tools and turn them against you, hoping you'll get scared and follow up their directions. Here are some examples of things a scammer might say:

The (value not set) registry trick

Scammer: *"Your network is not working properly as you can see it says: value not set and default."*

Facts: The network is working just fine. Scammers will use the registry editor to show empty keys and conclude your security is at risk.

The Process Explorer Error

Scammer: *"We need to manually remove the infected entries and delete all the error files from your computer."*

Facts: This [Error opening process] label happens because the user ran Process Explorer with limited privileges. It has nothing to do with errors on the computer.

The Digital Certificates

Scammer: *"Do you see the untrusted publishers? These are trying to compromise each and everything."*

Facts: These are normal and although the 'friendly name' is deceiving, those revoked certificates are used by your browser to protect you from untrusted sites.

The System Configuration Utility

Scammer: *"There are many programs that are stopped, indicating some serious damage to the backend of your computer and poor performance."*

Facts: It is perfectly normal to Have services that are stopped. In fact, you can actually speed up the boot time of your PC by disabling uneeded start up programs.

The Task Manager (CPU Spikes)

Scammer: *"These spikes are dangerous for your PC's health. Just like your heart rate, they should not go up. Your PC could suffer some irreparable damage."*

Facts: When your PC is active, you will see the CPU usage go up and down constantly. What would not be good is if the CPU was pegged at 100% utilization all of the time. This is not the case here.

Getting Help if you have been Scammed

Getting scammed one of the worst feelings to experience. In many ways, you feel like you have been violated and are angry to have let your guard down. Perhaps you are even shocked and scared, and don't really know what to do now. The following tips will hopefully provide you with some guidance.

1. Revoke remote access (if unsure, restart your computer)
2. Scan your computer for malware – the miscreants may have installed password stealers or other malware to capture your keystrokes
3. Change all your passwords – Windows password, email, online banking, etc.

For more tips to avoid and recover from these types of scams, as well as picture examples of the scams described, you can view this full article on Malwarebytes website. Please see the sources section for the link address.

Staying Cyber-safe on a Summer Vacation

An excerpt from the June, 2019 MSISAC newsletter

Typical travelers heading out on their summer vacation check that they have the right supplies and clothes for their trip before they hit the road. Expert travelers will be also checking to ensure they are educated and prepared to be cyber-safe with their devices and data. Thinking of your smartphones and devices as being just as important as your wallet is a proper step in the right direction. These devices contain everything from your banking and payment information to your treasured family photos, and ensuring they are secure and protected when away from home is paramount. In partnership with the National Cybersecurity Alliance (NCSA), here are some key tips, strategies, and resources to aid you in being secure during your travels.

Before your Trip:

Update your devices: One of the most simple and effective ways to stay cyber secure is to continuously update your devices to fix security flaws.

Password/Passcode protect your devices: Always establish a strong passcode with at least 6 numbers or a swipe pattern with at least 1 turn of direction when protecting the lock screen of your smartphone.

Set your device to lock after an amount of time: Once you have the passcode, password, or swipe pattern established, you should set an automatic device lock prompting for the access code after a specified time of inactivity. This will prevent a criminal from getting onto your device if you accidentally leave it unlocked.

Book your trip with trusted sites: When planning your trip and booking transportation, lodging, and experiences, it is important to complete those transactions with trusted, known businesses.

Staying Secure and Connected during your trip:

1. Keep track of your devices

2. Limit your activity on public Wi-Fi networks (Browsing and activity is not secure from prying eyes. To ensure information is not put at risk, avoid logging into your personal accounts

3. Don't overshare on Social Media: Consider posting updates about your trip after you return. Criminals may see you are away and attempt to steal from your home or scammers may attempt to contact your family and friends with a variety of scam tactics.

Did you know?

First Northern Bank & Trust prints out copies of the MS-ISAC Monthly Security Tips Newsletter each month and makes them available at all of our Branches. For a full copy of this publication, including additional tips on securing your devices, please stop by your local Branch, or email infosec@ 1stnorthernbank.com for a digital copy.

MS-ISAC
Multi-State Information Sharing & Analysis Center

Q&A Cyber Security Tip

Q: Does another company have access to all of my emails?

A: Maybe. If you use Office 365, and purchased your license through a resale partner instead of directly through Microsoft, Microsoft grants that partner administrative privileges in order to help the organization set up the tenant and establish the initial administrator account. Microsoft says customers can remove that administrative access if they do not want or need the partner to have access after the initial set up. Many companies partner with a third party just to obtain more favorable pricing, and not because they need someone to manage their email systems, and as such, are unaware full access has been given to this provider to access all of the emails stored in the cloud. This is what happened with a company whose email systems were rifled through by intruders who broke into PCM Inc., the world's sixth largest Cloud Service Provider. An employee of PCM was not using multifactor authentication, and upon having their email account hacked, so did many of PCMs customers. The breach at PCM is just the latest example of how cybercriminals increasingly are targeting employees who work at cloud data providers and technology consultancies that manage vast IT resources for many clients. (Krebs on Security)

Current Industry Trends

Verizon released their 2019 Data Breach Investigations Report (DBIR) which provides valuable insight on security trends.

Based on an analysis of more than 41,000 security incidents and more than 2,000 data breaches, Verizon's "2019 Data Breach Investigations Report" revealed that small businesses accounted for 43 percent of all attacks.

According to this year's data breach report, senior executives were 12 times more likely to be targeted by cybercriminals than in the previous year. Due to their higher level of access to sensitive information, C-level executives were also nine times more likely to receive social engineering campaigns such as phishing emails.

"Research points to users being significantly more susceptible to social attacks they receive on mobile devices. This is the case for email-based spear phishing, spoofing attacksthat attempt to mimic legitimate webpages, as well as attacks via social media."

The reason for this stems from how people interact with their smart phones. Having a smaller screen, a limited view in email apps, the tedious nature of toggling in between emails and other pages on a mobile phone, and the fact people are usually interacting with their mobile devices while walking, talking, driving, or other activities that interfere with the ability to pay careful attention to the emails they receive is coupled with mobile devices being desinged to give people the ability to make snap decsions. This all adds up to mobile devices being a useful tool to compromise email and other accounts.

Topic Requests

This newsletter was designed to provide you with the information you need to help secure your business. If there is a topic or question you would like to see covered in the next issue, please send an email to infosec@1stnorthernbank.com

Sources

Tech Support Scams: The variants are seemingly endless

https://blog.malwarebytes.com/tech-support-scams/

Wormable Flaw in Windows

https://arstechnica.com/information-technology/2019/05/microsoft-says-its-confident-an-exploit-exists-for-wormable-bluekeep-flaw/

New malware is bricking IoT devices

https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/

Q&A Cyber Security Tip

https://krebsonsecurity.com/2019/06/microsoft-to-require-multi-factor-authentication-for-cloud-solution-providers/

Current Industry Trends

https://securityintelligence.com/news/data-breach-report-small-businesses-and-c-level-executives-were-top-targets-in-2018/

https://enterprise.verizon.com/resources/reports/dbir/

Staying Cyber Safe on Summer Vacation – June 2019 MSISAC Newsletter

The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

FIRST NORTHERN
BANK & TRUST
1stnorthernbank.com • Member FDIC

Fourth Street & Lafayette Avenue
Palmerton, PA 18071
(610) 826-2239, (800) 344-2274

Member FDIC
EQUAL HOUSING LENDER