Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

April 27, 2021

Try our April Working Remotely Quiz

This week's stories:

Saskatchewan Blue Cross turns off key systems after cybersecurity incident

Cybercriminals evolving their tactics to exploit collective human interest

Emotet Malware Destroys Itself From All Infected Computers

Despite arrests in Spain, FluBot operations explode across Europe and Japan

Hacking campaign targets FileZen file-sharing network appliances

What Can We Learn From the Garmin Ransomware Attack?

Qlocker ransomware gang is using 7zip utility to lock files on QNAP devices

Apple AirDrop users reportedly vulnerable to security flaw

Flubot Spyware Spreading Through Android Devices

Apple's iPhone privacy clampdown arrives after 7 month delay

Love in a time of quarantine can be costly

10,000+ unpatched home alarm systems can be deactivated remotely

Twitter alarms users with messages that resembled phishing emails

Passwordstate Hacked, Exposing Users' Passwords for 28 Hours

Canada's aging critical infrastructure strategy an increasing concern, say cybersecurity experts

Ransomware Gang Demands $50 Million For Apple Watch And MacBook Pro Blueprints

What Your Business Should Know About Email Spoofing

Cybersecurity isn't just for your company – it applies to your ecosystem too. Here are 3 ways to hardwire it in

Saskatchewan Blue Cross turns off key systems after cybersecurity incident

Saskatchewan Blue Cross has confirmed the company experienced a cybersecurity incident last week.

President and CEO Shelley Vandenberg said she won't know if private information was compromised until cybersecurity experts are able to learn more.

"We do not take security lightly," read a statement on the company's website.

"We immediately engaged cybersecurity experts to assist us with our investigation, assessment and remediation efforts and to help us restore services as quickly and safely as possible."

Key systems and services were turned off on April 20th once staff noticed unusual network activity.

Vandenburg said there's no timeline on when phone lines or the member portal will be back online.

https://www.cbc.ca/news/canada/saskatoon/saskatchewan-blue-cross-turns-off-key-systems-after-cybersecurity-incident-1.6002030

Click link above to read more

Cybercriminals evolving their tactics to exploit collective human interest

Phishing activity increased significantly in the first few months of 2020, taking advantage of pandemic-induced product shortages and increased usage of streaming services, OpenText reveals.

For the first time, eBay topped the list of brands most targeted for impersonations, with 31.1% of all phishing attacks in the month of February impersonating eBay. In March, phishing activity surged among streaming services YouTube (3064%), Netflix (525%) and Twitch (337%).

“Gathered from over 285 million real-world endpoints and sensors, and leveraging the extensive BrightCloud network of industry-leading partners, this year’s Threat Report clearly shows how cybercriminals are willing and able to evolve their tactics to exploit collective human interest and current events,” said Prentiss Donohue, EVP, SMB/C Sales, OpenText.

“The findings underscore the need for users and businesses of all sizes to enact a multi-layered approach to data security and protection given the persistent creativity of cybercriminals.”

https://www.helpnetsecurity.com/2021/04/26/cybercriminals-evolving-tactics/

Click link above to read more

Emotet Malware Destroys Itself From All Infected Computers

Emotet, the notorious email-based Windows malware behind several botnet-driven spam campaigns and ransomware attacks, was automatically wiped from infected computers en masse following a European law enforcement operation.

The development comes three months after a coordinated disruption of Emotet as part of "Operation Ladybird" to seize control of servers used to run and maintain the malware network. The orchestrated effort saw at least 700 servers associated with the botnet's infrastructure neutered from the inside, thus preventing further exploitation.

Law enforcement authorities from the Netherlands, Germany, the U.S., U.K., France, Lithuania, Canada, and Ukraine were involved in the international action.

https://thehackernews.com/2021/04/emotet-malware-destroys-itself-today.html

Click link above to read more

Despite arrests in Spain, FluBot operations explode across Europe and Japan

Cyber-security agencies in Germany and the UK warned the general public this month about a spike in SMS spam messages spreading the FluBot Android malware.

In security alerts published by Germany's Federal Office for Information Security (BSI) and the UK National Cyber Security Centre (NCSC), the two agencies said that malware gangs are sending malicious links to users via SMS posing as legitimate package delivery services.

If users click the links, they are taken to a website posing as DHL or FedEx, where they are told to install an app to track a parcel meant to be delivered at their location.

https://therecord.media/despite-arrests-in-spain-flubot-operations-explode-across-europe-and-japan/

Click link above to read more

Hacking campaign targets FileZen file-sharing network appliances

Threat actors are using two vulnerabilities in a popular file-sharing server to breach corporate and government systems and steal sensitive data as part of a global hacking campaign that has already hit a major target in the Japanese Prime Minister's Cabinet Office.

The attacks target FileZen, a popular file-sharing network appliance from Japanese firm Soliton, and are eerily similar to the attacks that targeted Accellion's FTA file-sharing systems in late 2020, early 2021.

Both appliances work in the same manner. They are used to store large files that can't be sent via email. Users typically upload files on a FileZen server and then use a web-based panel to obtain links that they can share with fellow employees or persons outside of their organization.

https://therecord.media/hacking-campaign-targets-filezen-file-sharing-network-appliances/

Click link above to read more

What Can We Learn From the Garmin Ransomware Attack?

Famous ransomware attacks teach us certain lessons to follow while ensuring cybersecurity.

A few days ago, Quanta Computers Inc., a primary supplier of computers and Macbooks to Apple, acknowledged being dealing with a ransomware attack. A Bloomberg report revealed that a ransomware group REvil is behind the attack and they published a blog on its dark website on the same. This attack was reportedly an attempt to extract ransom from Apple and Quanta immediately upgraded its cybersecurity strategy.

This is just an example of recent ransomware attacks. Since data is considered the currency today, it becomes easier for the attackers to get hold of it and threaten companies. The higher vulnerability of data on certain platforms enables these kinds of cyberattacks. A similar infamous incident took the internet by storm in July last year, the Garmin ransomware attack. Garmin is a global tech company and is a key player in GPS navigation and wearables technology. The tech giant fell victim to a scandalous ransomware attack that was said to be initiated by EvilCorp, a Russian cybercrime gang. The attack was enabled through "WastedLocker" ransomware and it forced Garmin to shut down its website used by users to sync data, and other GPS-powered business operations. Various reports stated that the company paid a huge ransom to obtain an encryption key to restore the data. This huge cybersecurity breach enlightened many business systems and projected the importance of having better security in place. There are many lessons that the Garmin ransomware attack teaches us.

https://www.analyticsinsight.net/what-can-we-learn-from-the-garmin-ransomware-attack/

Click link above to read more

Qlocker ransomware gang is using 7zip utility to lock files on QNAP devices

A ransomware group has been targeting QNAP NAS users from all over the world in an ongoing attack that has enabled the group to generate about $260,000 within a week by remotely encrypting files on target devices using the 7zip archive utility.

According to Bleeping Computer, the Qlocker ransomware operation is exploiting some recently disclosed vulnerabilities to compromise QNAP devices and remotely execute the 7zip utility to password-protect all files on victims' NAS storage devices.

While the files on the target device are locked, QNAP's integrated Resource Monitor displays multiple 7z processes, the researchers found. Once the ransomware finishes its task, the files are stored in password-protected archives with a .7z extension.

https://www.computing.co.uk/news/4030356/qlocker-ransomware-gang-7zip-utility-lock-files-qnap-devices

Click link above to read more

Apple AirDrop users reportedly vulnerable to security flaw

Someone with the right know-how can obtain your phone number and email address when you try to share a file from your iPhone, say researchers at the University of Darmstadt.

iPhone users with AirDrop enabled may unknowingly expose certain personal information to a complete stranger. In a report released last week, researchers at the Department of Computer Science at the University of Darmstadt in Germany revealed their discovery of a security hole in Apple's AirDrop.

Utilized by many iPhone users, AirDrop allows you to share a file with someone else simply by sending it that person's device. As implemented by Apple, AirDrop appears to have a flaw in the way it checks whether or not you're in the other person's contact list.

https://www.techrepublic.com/article/apple-airdrop-users-reportedly-vulnerable-to-security-flaw/

Click link above to read more

Flubot Spyware Spreading Through Android Devices

The malware is spreading rapidly through ‘missed package delivery’ SMS texts, prompting urgent scam warnings from mobile carriers.

Android mobile phone users across the U.K. are being targeted by text messages containing a particularly nasty piece of spyware called “Flubot,” according to the country’s National Cyber Security Centre.

The malware is delivered to targets through SMS texts and prompts them to install a “missed package delivery” app. Instead, it takes victims to a scam website where they download the “app” — which is really just the spyware. Once installed, it then sets about gaining permissions, stealing banking information and credentials, lifting passwords stored on the device and squirreling away various pieces of personal information. It also sends out additional text messages to the infected device’s contact list, which allows it to “go viral” — like the flu.

https://threatpost.com/flubot-spyware-android-devices/165607/

Click link above to read more

Apple's iPhone privacy clampdown arrives after 7 month delay

The new privacy feature rolled out Monday as part of an update to the operating system powering the iPhone and iPad

Apple is following through on its pledge to crack down Facebook and other snoopy apps that secretly shadow people on their iPhones to help sell more advertising.

The new privacy feature, dubbed “App Tracking Transparency,” rolled out Monday as part of an update to the operating system powering the iPhone and iPad. The anti-tracking shield included in iOS 14.5 arrives after a seven-month delay during which Apple and Facebook attacked each other’s business models and motives for decisions that affect billions of people around the world.

“What this feud demonstrates more than anything is that Facebook and Apple have tremendous gatekeeping powers over the market,” said Elizabeth Renieris, founding director of the Technology Ethics Lab at the University of Notre Dame.

https://www.canadiansecuritymag.com/apples-iphone-privacy-clampdown-arrives-after-7-month-delay/

Click link above to read more

Love in a time of quarantine can be costly

A new report says people were scammed out of a record-breaking $304 million in the past year after being "catfished."

Quarantining left many people bored and lonely and in search of love, but a lot were left with broken hearts: Romance scams have increased during the pandemic. A new report finds a record-breaking loss of $304 million in 20201 due to these scams compared to $202 million in 2019. There were 32,792 so-called catfishing cases reported, according to the report by Social Catfish.

"One way that people have tried to cure their loneliness is by creating online dating accounts, hoping to find their future significant other," the site said. "However, scammers flood these dating apps and pretend to be someone they aren't in order to lure their victims in."

https://www.techrepublic.com/article/love-in-a-time-of-quarantine-can-be-costly/

Click link above to read more

10,000+ unpatched home alarm systems can be deactivated remotely

Thousands of ABUS Secvest smart alarm systems are currently unpatched and vulnerable to a bug that would allow miscreants to remotely disable alarm systems and expose homes and corporate headquarters to intrusions and thefts.

ABUS patched the bug in January, but three months later, more than 90% of its customers have yet to apply the firmware patch.

Dutch security firm EYE, which discovered and reported the issue to ABUS last October, estimated the total number of Secvest alarm systems connected online to around 11,000, based on internet scan data collected by security firm Rapid7.

Most systems are located in Germany.

https://therecord.media/10000-unpatched-home-alarm-systems-can-be-deactivated-remotely/

Click link above to read more

Twitter alarms users with messages that resembled phishing emails

Twitter sparked a panic among some users that they were the subjects of a phishing attack in what was instead an accidental mass email.

The message sent to some Twitter users went out Thursday, asking them to confirm their email addresses by clicking on a button. To many of those users who commented about it on the social media platform, it smelled like a possible phishing attempt.

Twitter clarified what had happened later that same evening.

“Some of you may have recently received an email to ‘confirm your Twitter account’ that you weren’t expecting,” the company said. “These were sent by mistake and we’re sorry it happened. If you received one of these emails, you don’t need to confirm your account and you can disregard the message.”

https://www.cyberscoop.com/twitter-phishing-confirm-email-mistake/

Click link above to read more

Passwordstate Hacked, Exposing Users’ Passwords for 28 Hours

Passwordstate, the enterprise password manager offered by Australian software developer Click Studios, was hacked earlier this week, exposing the passwords of an undisclosed number of its clients for approximately 28 hours. The hack was carried out through an upgrade feature for the password manager and potentially harvested the passwords of those who carried out upgrades.

On Friday, Click Studios issued an incident management advisory about the hack. It explained that the initial vulnerability was related to its upgrade director—which points the in-place update to the appropriate version of the software on the company’s content distribution network—on its website. When customers performed in-place upgrades on Tuesday and Wednesday, they potentially downloaded a malicious file, titled “moserware.secretsplitter.dll,” from a download network not controlled by Click Studios.

Once the malicious file was loaded, it set off a process that extracted information about the computer system as well as data stored in Passwordstate, including URLs, usernames and passwords. The information was then posted to the hackers’ content distribution network.

https://gizmodo.com/enterprise-password-manager-passwordstate-hacked-expos-1846756832

Click link above to read more

Canada's aging critical infrastructure strategy an increasing concern, say cybersecurity experts

The $144.9 million earmarked in the 2019 budget for cybersecurity of Canada’s critical infrastructure still hasn’t been put to use after two years, despite warnings that systems such as energy grids and telecom networks could be targeted by hostile actors.

The 2019 budget outlined the money would be spent over five years “to protect Canada’s critical cyber systems including in the finance, telecommunications, energy and transport sectors.” The funding was dependent on new legislation to “introduce a new critical cyber systems framework,” which still hasn’t materialized.

https://nationalpost.com/news/politics/canadas-aging-critical-infrastructure-an-increasing-concern-say-cybersecurity-experts

Click link above to read more

Ransomware Gang Demands $50 Million For Apple Watch And MacBook Pro Blueprints

A notorious cybercrime gang behind the REvil ransomware operation claims to have stolen the schematics for new Apple Watch and MacBook Pro products, amongst other confidential documents related to major brands.

Bleeping Computer reports that Apple supplier Quanta Computer was the target of the ransomware attack. The ransom demand, it says, was initially made of Quanta, but when the company didn't communicate with the attackers, they switched to Apple to demand payment of a $50 million ransom.

REvil has already published several documents on the dark web 'Happy Blog' it uses. Although many of the schematics leaked so far appear to be component-specific and not necessarily related to new products, that doesn't appear to be the case for all of them. Online publication 9to5Mac has determined that documents relating to the 2021 MacBook Pro reveal a lack of Touch Bar and changes to ports, for example.

https://www.forbes.com/sites/daveywinder/2021/04/23/ransomware-gang-demands-50-million-for-apple-watch-and-macbook-pro-blueprints/?sh=70d380565839

Click link above to read more

What Your Business Should Know About Email Spoofing

In a recent email fraud incident, employees in the finance department of a clinical trial software firm based in New York City were conned into wiring $4.8 million to an offshore bank account to facilitate a supposed company acquisition. The fraudulent emails purportedly came from the company president (they even included the executive's picture) and an outside attorney. In reality, cybercriminals had simply made it appear that the emails "from" fields were legitimate.

Could something like this happen to your company?

Business email compromise (BEC) attacks are widely known as "spoofing" attacks because the attacker falsifies ("spoofs") a sender's email address and/or display name. To the unsuspecting recipient, the email appears legitimate. The email's purpose is often brazen theft, with the sender trying to dupe the recipient into paying money, usually via a wire transfer, or for a falsified vendor invoice.

To spoof an email, cyber thieves use two methods:

- Email address spoofing. In this attack, the sender's email address and name are falsified so the incoming email appears legitimate.
- Display name spoofing. In this attack, only the sender's displayed name is falsified. The email address itself, if examined closely, reveals the email isn't legitimate.

https://www.forbes.com/sites/tmobile/2021/04/26/what-your-business-should-know-about-email-spoofing/?sh=788112a944ed

Click link above to read more

Cybersecurity isn't just for your company – it applies to your ecosystem too. Here are 3 ways to hardwire it in

• Business ecosystems are reaching global scale, exposing companies to massive losses for cybersecurity breaches.

• Thinking about cybersecurity early is mandatory for any innovation-focused company.

• Cybersecurity training can dramatically increased resilience among employees.

In the digital age, ecosystems take the evolution of business to a whole new level. The ecosystem surrounding a company can include a network of partners, suppliers, manufacturers, as well as various processes, all working together as a single organism.

Some ecosystems have already reached global scales. Insufficient security of their components could result in enormous losses. A supply chain attack can cause a domino effect, unless each member of the ecosystem takes responsibility for their own security.

https://www.weforum.org/agenda/2021/04/cybersecurity-business-ecosystems/

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Security News Digest
Information Security Branch
British Columbia OCIO | Office of the Chief Information Officer