April 13, 2021

Try our April Working Remotely Quiz

This week's stories:

LinkedIn denies 500 million user data breach

LinkedIn has formally denied a rumor that it suffered a devastating security breach that exposed the account details of more than 500 million of its registered users.

Rumors of a breach appeared last week after a threat actor claimed to have been in possession of a large trove of LinkedIn user data and proceeded to leak a sample of two million user records as proof.

But in a message published last week, LinkedIn said it investigated the breach and concluded that the hacker's data only included public information that was scraped off LinkedIn's website and which users consciously made public on their profiles.

"This was not a LinkedIn data breach, and no private member account data from LinkedIn was included in what we've been able to review," a LinkedIn spokesperson said.

https://therecord.media/linkedin-denies-500-million-user-data-breach/

Click link above to read more

Visa Describes New Skimming Attack Tactics

Visa's Payment Fraud Disruption team reports that cybercriminals are increasingly using web shells to establish command and control over retailers' servers during payment card skimming attacks.

"As a result, eSkimming, or digital skimming, is among the top threats to the payments ecosystem," according to the Visa report.

The web shells enable fraudsters conducting digital skimming attacks on e-commerce sites to establish and maintain access to compromised servers, deploy additional malicious files and payloads, facilitate lateral movement within a victim's network and remotely execute commands, Visa says.

The most common methods for deploying a web shell are malicious application plug-ins and PHP code, Visa reports.

https://www.bankinfosecurity.com/visa-describes-new-skimming-attack-tactics-a-16372

Click link above to read more

Wine scams spiked during COVID-19 lockdown

Absolute monsters.

Wine-themed domain registrations rose once COVID-19 lockdowns took hold, some of them malicious and used in phishing campaigns, Recorded Future and Area 1 Security said in a joint report out Wednesday.

“As the interest in virtual happy hours and get-togethers increased so did the increase in wine-themed domain registrations,” the report states.

Amid the COVID outbreak, alcohol has proven itself a target for hackers — but it hasn’t been clear before that scammers were trying to exploit people who were staying home and imbibing more. Alcohol delivery service Drizly, for instance, suffered a breach in July, while ransomware hit liquor and wine maker Brown-Forman around the same time.

Recorded Future observed a mild jump in wine domain registrations in March of 2020, from the usual 3,000 to 4,000 per month up to nearly 5,500. April saw a bigger leap, to almost 7,200, and the numbers took off in May to 12,400. They’ve stayed high ever since.

https://www.cyberscoop.com/wine-scams-phishing-bec-domain-registrations-recorded-future/

Click link above to read more

Covid-19 pandemic: How bug bounty programs helped secure some of the world’s leading track and trace apps

Crowdsourced security was a key tool in securing some countries’ efforts, while others missed the mark.

As the Covid-19 pandemic began spreading across the globe in 2020, governments worldwide raced to develop tracking apps to help contain the virus.

The list of countries with track and trace apps is exhaustive, with the UK, France, India, Australia, China, and Hong Kong just some of those included.

But as is often the case, the rush to push projects out in a short amount of time came at the expense of user security and privacy.

Notable issues, of those that have been publicly reported, include major privacy holes and the leaking of sensitive data in some cases.

As a result, last year saw the launch of a number of bug bounty programs and vulnerability disclosure programs (VDPs) specifically designed to secure track and trace applications.

https://portswigger.net/daily-swig/covid-19-pandemic-how-bug-bounty-programs-helped-secure-some-of-the-worlds-leading-track-and-trace-apps

Click link above to read more

Microsoft: Malware gang uses website contact forms for distribution

Microsoft said today it spotted a cybercrime operation abusing contact forms on legitimate websites to target companies and their workers in attempts to infect them with the IcedID malware.

One of Microsoft's security teams highlighted the creativity and effectiveness of this campaign, which is currently seeing a spike in activity.

The technique behind these attacks is simple and relies on threat actors using automated scripts to visit the websites of legitimate businesses and filling out contact forms with bogus legal threats.

https://therecord.media/microsoft-malware-gang-uses-website-contact-forms-for-distribution/

Click link above to read more

Alert — There's A New Malware Out There Snatching Users' Passwords

A previously undocumented malware downloader has been spotted in the wild in phishing attacks to deploy credential stealers and other malicious payloads.

Dubbed "Saint Bot," the malware is said to have first appeared on the scene in January 2021, with indications that it's under active development.

"Saint Bot is a downloader that appeared quite recently, and slowly is getting momentum. It was seen dropping stealers (i.e. Taurus Stealer) or further loaders (example), yet its design allows [it] to utilize it for distributing any kind of malware," said Aleksandra "Hasherezade" Doniec, a threat intelligence analyst at Malwarebytes.

https://thehackernews.com/2021/04/alert-theres-new-malware-out-there.html

Click link above to read more

Official client for the APKPure Android app store compromised with malware

The official client for APKPure, the second-largest Android app store after the Google Play Store, was compromised with malware this week, three security firms said on Friday.

Version 3.17.18 of the APKPure application contained a copy of the Triada trojan, a type of Android malware that can perform banking fraud, steal user data, or download and install additional payloads.

Android users who installed or updated to this version of the APKPure client are advised to update to version 3.17.19, released earlier today, which removes the malware from their devices.

APKPure released the updated version today after receiving notifications that malware slipped into its official client yesterday from Russian security firms Dr.Web and Kaspersky.

https://therecord.media/official-client-for-the-apkpure-android-app-store-compromised-with-malware/

Click link above to read more

Facebook 'knew about phone number data leak vulnerability two years before issue was fixed', claims security researcher

Social media giant says 'scraping' was cause of issue that affected 500 million users.

As Facebook defends its actions over a massive data leak, one researcher says he notified the company of the issue a full two years before the problem was fixed.

Last week, Business Insider revealed that the personal data of more than 500 million Facebook users had been posted in a low-level hacking forum where phone numbers were being offered for sale.

Facebook has defended itself in a lengthy blog post, pointing out that the data was obtained by scraping, rather than hacking.

“We believe the data in question was scraped from people’s Facebook profiles by malicious actors using our contact importer prior to September 2019.

https://portswigger.net/daily-swig/facebook-knew-about-phone-number-data-leak-vulnerability-two-years-before-issue-was-fixed-claims-security-researcher

Click link above to read more

Maze/Egregor ransomware cartel estimated to have made $75 million

The group behind the Maze and Egregor ransomware operations are believed to have earned at least $75 million worth of Bitcoin from ransom payments following intrusions at companies all over the world.

“We believe this figure to be much more significant, but we can only assess the publicly acknowledged ransom payments. Many victims never publicly report when they pay a ransom,” security firm Analyst1 said in a 58-page report [PDF] published this week.

Analyst1’s findings are in line with a similar report from blockchain analysis firm Chainalysis, which listed the Maze gang as the third most profitable ransomware operation —behind Ryuk and Doppelpaymer.

A previous report estimated Ryuk’s earnings at around $150 million. Doppelpaymer figures are not available.

https://therecord.media/maze-egregor-ransomware-cartel-estimated-to-have-made-75-million/

Click link above to read more

PHP maintainers release post-mortem report after backdoor planted in Git repo

More details released about the incident, though the attacker remains unidentified.

The maintainers of PHP have released a post-mortem report after an unknown actor pushed backdoored code onto the scripting language’s official PHP Git repository.

As previously reported by The Daily Swig, an attacker pushed two commits to the php-src repo that contained a backdoor allowing for remote code execution (RCE).

They are thought to have gained access to the main server, which allowed them to plant the backdoor under the guise of a minor edit made in a maintainer’s name.

Last night (April 6), maintainer Nikita Popov released more details related to the attack and said the team no longer believes the git.php.net server was compromised, but that the master.php.net user database was leaked.

https://portswigger.net/daily-swig/php-maintainers-release-post-mortem-report-after-backdoor-planted-in-git-repo

Click link above to read more

Researchers uncover a new Iranian malware used in recent cyberattacks

An Iranian threat actor has unleashed a new cyberespionage campaign against a possible Lebanese target with a backdoor capable of exfiltrating sensitive information from compromised systems.

Cybersecurity firm Check Point attributed the operation to APT34, citing similarities with previous techniques used by the threat actor as well as based on its pattern of victimology.

APT34 (aka OilRig) is known for its reconnaissance campaigns aligned with the strategic interests of Iran, primarily hitting financial, government, energy, chemical, and telecommunications industries in the Middle East.

https://thehackernews.com/2021/04/researchers-uncover-new-iranian-malware.html

Click link above to read more

Indian Brokerage Firm Upstox Suffers Data Breach Leaking 2.5 Millions Users' Data

Online trading and discount brokerage platform Upstox has become the latest Indian company to suffer a security breach of its systems, resulting in the exposure of sensitive information of approximately 2.5 million users on the dark web.

The leaked information includes names, email addresses, dates of birth, bank account information, and about 56 million know your customer (KYC) documents pulled from the company's server.

The breach was first disclosed by independent researcher Rajshekhar Rajaharia on April 11. It's not immediately clear when the incident occurred.

https://thehackernews.com/2021/04/indian-brokerage-firm-upstox-suffers.html

Click link above to read more

New ransomware changes all your passwords

The internet brought about a lot of great changes, online shopping anybody? But it also brought about many risks. Hackers have become a constant concern in our daily lives. Every time we enter our credit card online to buy something, we put our finances at risk.

Viruses, malware and sneaky internet criminals are constantly evolving. The risks of losing your personal information and having your computer taken over by strangers continue to rise every day. Tap or click here to see five scams online that can cost you thousands.

REvil ransomware is well known and it's just become even more dangerous. This terrifying security threat has introduced a new attack mode and it's fully automated.

https://nationalcybersecuritynews.today/new-ransomware-changes-all-your-passwords-malware-ransomware-hacking/

Click link above to read more

Windows, Ubuntu, Zoom, Safari, MS Exchange Hacked at Pwn2Own 2021

The 2021 spring edition of Pwn2Own hacking contest concluded last week on April 8 with a three-way tie between Team Devcore, OV, and Computest researchers Daan Keuper and Thijs Alkemade.

A total of $1.2 million was awarded for 16 high-profile exploits over the course of the three-day virtual event organized by the Zero Day Initiative (ZDI).

Targets with successful attempts included Zoom, Apple Safari, Microsoft Exchange, Microsoft Teams, Parallels Desktop, Windows 10, and Ubuntu Desktop operating systems.

https://thehackernews.com/2021/04/windows-ubuntu-zoom-safari-ms-exchange.html

Click link above to read more

Vyveva: Lazarus hacking group's latest weapon strikes South African freight

Researchers have discovered a new backdoor employed by the Lazarus hacking group in targeted attacks against the freight industry.

On Thursday, ESET said the new backdoor malware, dubbed Vyveva, was traced in an attack against a South African freight and logistics firm.

While the initial attack vector for deploying the malware is not yet known, examining machines infected with the malware revealed strong links to the Lazarus group.

Lazarus is an advanced persistent threat (APT) group of North Korean origin. The state-sponsored cyberattackers are prolific and are deemed responsible for the global WannaCry ransomware outbreak; $80 million Bangladeshi bank heist; attacks against South Korean supply chains, cryptocurrency theft, the 2014 Sony hack, and various other assaults against US organizations.

https://www.zdnet.com/article/vyveva-lazarus-latest-weapon-strikes-south-african-freight/

Click link above to read more

Microsoft doubles down on cloud healthcare business with $16 billion Nuance buy

Microsoft Corp said on Monday it would buy artificial intelligence and speech technology firm Nuance Communications Inc for about $16 billion, as it expands cloud solutions for healthcare customers.

The deal comes after the companies partnered in 2019 to automate clinical administrative work such as documentation. It shows Microsoft's ambition to extend its leadership into an industry where digital transformation has picked up speed during the pandemic. Healthcare providers have invested more in technology to improve productivity and digital health services.

"This acquisition brings our technology directly into the physician and patient loop, which is central to all healthcare delivery. The acquisition will also expand our leadership in cross-industry enterprise AI and biometric security," Microsoft CEO Satya Nadella said on an investor call.

https://www.reuters.com/article/us-nuance-commns-m-a-microsoft/microsoft-doubles-down-on-cloud-healthcare-business-with-16-billion-nuance-buy-idUSKBN2BZ1FS

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.