February 23rd, 2021

Try our February "LOVE SECURITY" Quiz

This week's stories:

CRA suspends online accounts of over 100,000 Canadians after login credentials found for sale on dark web

OTTAWA – The Canada Revenue Agency had to suspend the accounts of more than 100,000 users of its online service because it detected troves of leaked login information on the dark web that could have led to data breaches.

If you received an unexpected and cryptic email on Feb. 16 from CRA warning you that your email had been deleted from the agency's web platform, MyCRA, do not worry: your account has not been breached.

In fact, the agency says it means that their new early cyber security issue detection system is working (though the communication strategy will be reviewed and it "regrets the inconvenience.")

But that also means your login data has probably been compromised through a third-party breach and you will need to contact CRA in order to regain access to your online account, particularly if you plan on filing your 2020 taxes online starting next week.

https://nationalpost.com/news/politics/cra-suspends-online-accounts-of-over-100000-canadians-after-their-login-credentials-found-for-sale-on-dark-web

Click link above to read more

Who's hacking your smart home?

The market for smart home devices is tipped to explode over the next few years, but many consumers remain woefully ignorant of the threats such tech can incur.

It might come as a shock to many synth-pop fans out there but this year marks the passing of 37 years since the release of ***Electric Dreams***. This 80s *in extremis* romcom introduced many to the concept of the connected or smart home, albeit one facilitated not by wireless IoT technology, but by an accidentally sentient pre-GUI computer.

While many cinema-goers at the time might have dismissed such possibilities as silly sci-fi fantasy at best, the fact remains that in the developed world at least smart homes are rapidly becoming a reality if not the norm. This is particularly so among members of the Millennial and Generation Z cohorts, with Finland's F-Secure reporting that extensive surveys conducted over several years show that the consumers most likely to purchase and deploy smart home technology "tend to be married Millennials in their 30s with college degrees, young children and a passion for filling their new homes with Internet-connected devices of all sorts."

Although such consumers are typically "better informed than their peers, explorative and in search of new technology offerings to try," they are certainly not alone in purchasing smart home gadgets and gizmos.

https://cybernews.com/security/whos-hacking-your-smart-home/

Click link above to read more

How to Fight Business Email Compromise (BEC) with Email Authentication?

An ever-evolving and rampant form of cybercrime that targets emails as the potential medium to conduct fraud is known as Business Email Compromise.

Targeting commercial, government as well as non-profit organizations, BEC can lead to huge amounts of data loss, security breach, and compromised financial assets.

It is a common misconception that cybercriminals usually lay their focus on MNCs and enterprise-level organizations. SMEs these days are just as much a target to email fraud as the larger industry players.

How Can BEC Affect Organizations?

Examples of BEC include sophisticated social engineering attacks like phishing, CEO fraud, fake invoices, and email spoofing, to name a few. It can also be termed an impersonation attack wherein an attacker aims to defraud a company by posing people in authoritarian positions. Impersonating people like the CFO or CEO, a business partner, or anyone you will blindly place your trust in is what drives these attacks' success.

https://thehackernews.com/2021/02/how-to-fight-business-email-compromise.html

Click link above to read more

Global Accellion data breaches linked to Clop ransomware gang

Threat actors associated with financially-motivated hacker groups combined multiple zero-day vulnerabilities and a new web shell to breach up to 100 companies using Accellion's legacy File Transfer Appliance and steal sensitive files.

The attacks occurred in mid-December 2020 and involved the Clop ransomware gang and the FIN11 threat group. Unlike previous attacks by these groups, the Clop file-encrypting malware was not deployed.

It appears that the actors opted for an extortion campaign. After stealing the data, they threatened victims over email with making stolen information publicly available on the Clop leak site unless a ransom was paid.

BleepingComputer has been tracking these Accellion-related breaches and discovered almost a dozen victims.

Among them are supermarket giant Kroger, Singtel, QIMR Berghofer Medical Research Institute, Reserve Bank of New Zealand, the Australian Securities and Investments Commission (ASIC), and the Office of the Washington State Auditor ("SAO").

https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/

Click link above to read more

Researcher Hacks 35 Major Companies In A Mock Supply Chain Attack

A cybersecurity researcher breached over 35 major companies, including Apple and PayPal in a novel software supply chain attack.

Ethical hacker Alex Birsan discovered a method to inject malicious dependency packages into commonly used open-source developer tools.

The exploit method affects several programming languages depending on the package manager to install dependencies into projects using public repositories.

Birsan’s hacking method, called dependency confusion, allowed him to exploit 35 companies, including Microsoft, Apple, PayPal, Shopify, Netflix, Yelp, Tesla, and Uber in a supply chain attack.

https://www.cpomagazine.com/cyber-security/researcher-hacks-35-major-companies-in-a-mock-supply-chain-attack/

Click link above to read more

Mysterious malware infects 30,000 Mac computers

Known as Silver Sparrow, the malware's intent is still unknown as it has yet to deliver an actual payload, says security firm Red Canary.

A piece of malware that has infected almost 30,000 Mac computers has triggered questions over its intent and ultimate payload.

Based on data from Malwarebytes, the malware dubbed Silver Sparrow by researchers at Red Canary, has so far landed on 29,139 macOS machines across 153 countries, including the US, UK, Canada, France and Germany. Questions have arisen because the malware hasn't actually done anything malicious yet, meaning there's been no observed payload delivery and no conclusions as to its purpose.

What is known is that Silver Sparrow is a strain of malware designed for Macs powered by the new Apple M1 chip, which the company introduced late last year as a move away from Intel architecture. This makes it only the second known piece of macOS malware to target the new chips, according to Ars Technica. With the missing payload piece and other questions, the malware has led to concerns among Red Canary researchers.

https://www.techrepublic.com/article/mysterious-malware-infects-30000-mac-computers/?ftag=TREe01923b&bhid=19662319145962710268575546540229&mid=13276320&cid=712327807

Click link above to read more

Experian challenged over massive data leak in Brazil

XAfter receiving feedback from Experian over a massive data leak in Brazil, São Paulo state consumer rights foundation Procon described the company's explanations as "insufficient" and said it is likely that the incident was initiated in a corporate environment.

Procon notified the credit information multinational following the emergence of a leak that exposed the personal data of more than 220 million citizens as well as companies, currently offered for sale in the dark web. Security firm PSafe discovered the incident, which exposed all manner of personal details, including information from Mosaic, a consumer segmentation model used by Serasa, Experian's Brazilian subsidiary.

Following the emergence of the leak in January, Procon notified the credit bureau, and asked the company for a confirmation of the incident, and an explanation of the reasons that caused the leak, the steps taken to contain it, how it will repair the damage to consumers impacted and the measures taken to prevent it from happening again.

https://www.zdnet.com/article/experian-challenged-over-massive-data-leak-in-brazil/?mkt_tok=MTM4LUVaTS0wNDIAAAF7agWNKaBvOar0oGWZBGcUtTmpxCyb5sqE4tiMFojPYW5OQrHYCj-VEPh2_C9j8Zrwl4WnAMOaZyioHsObd66wur8V7lxhIX6rWhDs-9gA6VxT

Click link above to read more

Malvertiser abused WebKit zero-day to redirect iOS & macOS users to shady sites

A cybercrime group specialized in showing malicious ads has abused an unpatched zero-day vulnerability in WebKit-based browsers to break security restrictions and redirect users from legitimate portals to shady sites hosting online gift card scams.

The attacks were first spotted in June 2020 and are still active today; however, patches for the WebKit zero-day have been released at the start of the month.

According to a report from cyber-security firm Confiant, shared with *ZDNet* last week, the culprits behind the attacks are a group previously known as ScamClub.

Active since 2018, this group operates by buying large quantities of ad slots on multiple platforms in the hope that some of its bad ads make it through security checks.

Since it was first discovered almost three years ago, ScamClub has typically targeted iOS users with malicious ads that often redirected users to sites hosting online scams that tried to collect users' financial information.

https://www.zdnet.com/article/malvertiser-abused-webkit-zero-day-to-redirect-ios-macos-users-to-shady-sites/

Click link above to read more

'Spy pixels in emails have become endemic'

The use of "invisible" tracking tech in emails is now "endemic", according to a messaging service that analysed its traffic at the BBC's request.

Hey's review indicated that two-thirds of emails sent to its users' personal accounts contained a "spy pixel", even after excluding for spam.

Its makers said that many of the largest brands used email pixels, with the exception of the "big tech" firms.

Defenders of the trackers say they are a commonplace marketing tactic.

And several of the companies involved noted their use of such tech was mentioned within their wider privacy policies.

Emails pixels can be used to log:

- if and when an email is opened
- how many times it is opened

- what device or devices are involved
- the user's rough physical location, deduced from their internet protocol (IP) address - in some cases making it possible to see the street the recipient is on

https://www.bbc.com/news/technology-56071437

Click link above to read more

Microsoft's Power BI gets new tools to prevent leakage of confidential data

Whatever business intelligence tool you're using, it connects to Excel. "If you want to build a new BI product, the first feature you build is export to Excel," jokes Arun Ulag, CVP of Microsoft Power BI. "People want to be able to work with data in the tools that they use." he adds.

But when you export a report to Excel to dig into the numbers, what happens to any rights management that's been applied to sensitive company data? Role-based access permissions, row-level security and object-level security may not be enough to protect data – particularly with so many people working at home.

"Data travels, and if the security is left behind as the data travels from your data warehouse to your BI system to Excel to PowerPoint to PDF, then how good is it?" Ulag points out. "If I can export my data out to Excel and then email it to somebody and that's where the security stops, it really breaks down, especially in the world of remote work. This is a paradox: you're taking your most sensitive corporate data, you're giving it to everybody – and everybody's working from home."

Blocking export to PDF to protect confidential data is frustrating for employees who need to work with the data. So Power BI will now use sensitivity labels from Microsoft Information Protection (MIP) to protect information in Power BI Desktop, in the Power BI service and when reports are exported to Excel, PowerPoint or PDF. This will allow you to use the same data security policy, compliance and auditing tools for Power BI as for Office (and third-party applications that build in MIP). You can label and classify the PBIX files that Power BI Desktop works with, and you can label datasets and reports in the Power BI service.

https://www.techrepublic.com/article/microsofts-power-bi-gets-new-tools-to-prevent-leakage-of-confidential-data/?ftag=TREa988f1c&bhid=42420269&mid=13271420&cid=2176068089

Click link above to read more

Millions of patients affected by healthcare breaches last year

Millions of staff and patients had personal information exposed in healthcare data breaches across the US last year, new research has revealed.

According to security firm Bitglass, a total of 599 healthcare breaches affected more than 26 million people in 2020, with 91.2% of the records exposed as a result of hacking and IT incidents.

The average cost per breach also increased for healthcare organizations, from $429 in 2019 to $499 last year, and data loss incidents accounted for losses of $13.2 billion in total.

https://www.techradar.com/news/millions-of-patients-affected-by-healthcare-breaches-last-year?utm_source=SmartBrief&utm_medium=email&utm_campaign=79B375AA-AA0B-4881-99A1-64F0F9BDBE17&utm_content=85199BFA-187E-432A-9930-28289C41D80E

Click link above to read more

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