February 9th, 2021

Try our February "LOVE SECURITY" Quiz

This week's stories:

- Ransomware attempt on British Columbia realtor raises question of supply chain attack
- Small businesses were forced online because of the pandemic — now a quarter say they've experienced a cyber attack
- B.C. privacy commissioner says privacy laws alone can't restrain big tech's 'predatory behaviour'
- Can The FBI Can Hack Into Private Signal Messages On A Locked iPhone? Evidence Indicates Yes
- How much is your info worth on the Dark Web? For Americans, it's just $8
- Hundred thousand Spotify accounts leaked in credential stuffing attack
- Hackers Are Using DDOS Attacks To Profit Off Businesses
- World Economic Forum calls cybersecurity one of the "key threats of the next decade"
- Instagram removes hundreds of accounts tied to username hacking
- Microsoft: Office 365 Was Not SolarWinds Initial Attack Vector
- Can your organization obtain reasonable cybersecurity? Yes, and here's how
- Phishing service provider 'SMS Bandit' arrested in the UK

Ransomware attempt on British Columbia realtor raises question of supply chain attack

A real estate agency in British Columbia is investigating a ransomware attack that the owner says was caught before serious damage was done. But the incident raises the question of whether the attack came through the infection of a third party's application.

Jerry Redman, owner and managing director of ReMax Kelowna, which has four offices in the city of 132,000, said in an interview Friday afternoon that fortunately, the attack happened at the same time as IT staff were overseeing a software update. The ransomware wasn't launched, although some files were copied.

"We were on it within minutes of knowing it started, and that's why [the attackers] don't have much," he said.

While a forensic investigation is still ongoing, so far Redman believes the only data attackers were able to copy was what he called "non-personal company data." This includes "graphic design stuff that the company does for people."

https://www.itworldcanada.com/article/ransomware-attempt-on-british-columbia-realtor-raises-question-of-supply-chain-attack/441914

Click link above to read more

🇨🇦 Small businesses were forced online because of the pandemic — now a quarter say they've experienced a cyber attack

With the pandemic-driven shift to e-commerce comes a new threat for small businesses: cyber fraud.

Last year thousands of businesses were victims, says the Canadian Federation of Independent Business (CFIB).

An October survey of 3,040 CFIB members across Canada found that nearly a quarter have experienced cyber attacks since March 2020, the time when many businesses had to increase their online presence — or start it from scratch.

Jasmin Guenette, CFIB's vice-president of national affairs, said the businesses that were able to adapt successfully to the e-commerce shift were, perhaps ironically, the most vulnerable to cyber attacks in the last year.

Almost five per cent of survey responders said the attack against them was successful. That's likely more than 60,000 small and medium businesses that fell victim to cyber fraud last year, if you extrapolate that five per cent to the approximate number of small and medium sized businesses out there by recent Statistics Canada data, according to the CFIB's report.

https://www.thestar.com/business/2021/02/04/small-businesses-pivoting-online-because-of-covid-19-are-vulnerable-to-cyber-attacks-cfib-report.html

Click link above to read more

🇨🇦 B.C. privacy commissioner says privacy laws alone can't restrain big tech's 'predatory behaviour'

Governments will have to use more than updated privacy laws if they want to stop technology companies from leveraging disinformation and lies for profit, says British Columbia's information and privacy commissioner.

"I do worry the current approaches we are pursuing have already gone beyond their best before date," Michael McEvoy said Friday in an online keynote speech during the Victoria Privacy and Security Conference. "It's evident to me that privacy laws alone cannot sufficiently restrain the predatory behaviour of technology companies, particularly the giants among them."

Countries will have to use many tools, including anti-competition, consumer protection and anti-trust laws, he added. One example he noted was the European Union fining Google 2.4 billion euros for manipulating its search engine to direct people to its own products. The U.S has also been aggressive: Last year, the federal government sued Google under its antitrust legislation, and the U.S. Federal Trade Commission fined Facebook $5 billion in 2019 for the collection of data relating to the Cambridge Analytica scandal.

https://www.itworldcanada.com/article/b-c-privacy-commissioner-says-privacy-laws-alone-cant-restrain-big-techs-predatory-behaviour/441954

Click link above to read more

Can The FBI Can Hack Into Private Signal Messages On A Locked iPhone? Evidence Indicates Yes

Signal has become the de facto king of secure messaging apps of late, stealing users from WhatsApp and gathering millions of others looking for private forms of communication. That means the police and governments will be wanting, more than ever, to ensure they have forensic techniques to access Signal messages. Court documents obtained by Forbes not only attest to that desire, but indicate the FBI has a way of accessing Signal texts even if they're behind the lockscreen of an iPhone.

The clues came via Seamus Hughes at the Program on Extremism at the George Washington University in court documents containing screenshots of Signal messages between men accused, in 2020, of running a gun trafficking operation in New York. (The suspects have not yet entered a plea and remain innocent until proven guilty). In the Signal chats obtained from one of their phones, they discuss not just weapons trades but attempted murder too, according to documents filed by the Justice Department. There's also some metadata in the screenshots, which indicates not only that Signal had been decrypted on the phone, but that the extraction was done in "partial AFU." That latter acronym stands for "after first unlock" and describes an iPhone in a certain state: an iPhone that is locked but that has been unlocked once and not turned off. An iPhone in this state is more susceptible to having data inside extracted because encryption keys are stored in memory. Any hackers or hacking devices with the right iPhone vulnerabilities could then piece together keys and start unlocking private data inside the device.

https://www.forbes.com/sites/thomasbrewster/2021/02/08/can-the-fbi-can-hack-into-private-signal-messages-on-a-locked-iphone-evidence-indicates-yes/?ss=cybersecurity&sh=4e912e656624

Click link above to read more

How much is your info worth on the Dark Web? For Americans, it's just $8

A Comparitech report found that Japan and the UAE have the most expensive identities available on illicit marketplaces at an average price of $25.

Personal information from US citizens found on the Dark Web—ranging from Social Security numbers, stolen credit card numbers, hacked PayPal accounts, and more—is worth just $8 on average, according to a new report from tech research firm Comparitech.

Researchers pored through the prices of personal data and information—called "fullz" by those searching for "full credentials"—that are available for sale on nearly 50 different Dark Web marketplaces, finding that Japan, the UAE, and EU countries have the most expensive identities available at an average price of $25.

The report also said the prices for stolen credit card numbers range from just 11 cents to nearly $1,000. There were similarly huge price swings for stolen PayPal account data, which cost anywhere between $5 and $1,767, Comparitech researchers found, adding that the prices for accounts based in the US or UK were cheapest because they represented most of what was available.

https://www.techrepublic.com/article/how-much-is-your-info-worth-on-the-dark-web-for-americans-its-just-8/?ftag=TREa988f1c&bhid=19662319145962710268575546540229&mid=13261416&cid=712327807

Click link above to read more

Hundred thousand Spotify accounts leaked in credential stuffing attack

It was recently revealed that Spotify has suffered its second credential stuffing attack in three months. It is estimated that almost a hundred thousand accounts can face a takeover.

What is Credential Stuffing?

A script is written by cybercriminals that is capable of checking stolen IDs and passwords one by one. These credentials can be taken from another website's database or there are some databases available online for purchase.

The attackers try these credentials until one works and benefit from the people who have the same password on several websites.

https://www.hackread.com/spotify-accounts-leaked-credential-stuffing-attack/

Click link above to read more

Hackers Are Using DDOS Attacks To Profit Off Businesses

Distributed Denial of Service Attacks (DDOS) have been used by hackers since the earliest days of the web.

Get enough internet-connected devices to ping a server at the same time, and you can knock the server offline.

Keep the pressure on and you can keep it offline, pretty much indefinitely.

These days, given the web's importance, that can easily bring financial ruin to all but the most deep-pocketed companies. Hackers know this of course, which is why such attacks are still in use to this very day.

https://www.comtech-networking.com/blog/item/hackers-are-using-ddos-attacks-to-profit-off-businesses/

Click link above to read more

World Economic Forum calls cybersecurity one of the "key threats of the next decade"

The Global Risks Report highlights the onslaught of cyberattacks and a failure of governments to stop them.

Cybersecurity took center stage in the 16th edition of the World Economic Forum's Global Risks Report alongside the COVID-19 pandemic, climate change, and debt crises. Since 2004 the report has detailed the most critical risks facing the world and has highlighted cyberattacks and data breaches as far back as 2012.

But the latest report comes at a time when multiple cyberattacks every day are commonplace. Hospitals and schools now have to be prepared to respond to crippling ransomware attacks. The US government is struggling to root out Russian government hackers who managed to break their way into the State Department, the Justice Department, the Treasury, the Centers for Disease Control and Prevention, the Department of Homeland Security, and even nuclear labs associated with the Department of Energy.

https://www.techrepublic.com/article/world-economic-forum-calls-cybersecurity-one-of-the-key-threats-of-the-next-decade/

Click link above to read more

Instagram removes hundreds of accounts tied to username hacking

(Reuters) - Facebook Inc on Thursday took down hundreds of Instagram accounts that were hacked and sold for their high-value usernames, including the accounts of people behind this activity.

A Facebook spokeswoman said the people engaged in this rule-breaking practice were well-known figures in a community known as the OGUsers, who trade desirable usernames for popular websites from Twitter Inc to Netflix for money and clout.

The usernames, which can sell for tens of thousands of dollars, are often short words prized for their scarcity, like @food or letters like @B. Social media companies including Facebook-owned Instagram have rules against the sale of accounts.

https://www.reuters.com/article/us-facebook-instagram-cyber/instagram-removes-hundreds-of-accounts-tied-to-username-hacking-idUSKBN2A42HY

Click link above to read more

Microsoft: Office 365 Was Not SolarWinds Initial Attack Vector

Microsoft's security team says the company's Office 365 suite of products did not serve as an initial entry point for the hackers who waged the SolarWinds supply chain attack.

And SolarWinds' CEO, in a new blog, says the company "has not identified a specific vulnerability in Office 365 that would have allowed the threat actor to enter our environment." The incident, he says, involved the compromise of an email account through the theft of credentials.

Microsoft also points to credential theft. "In our investigations to date, data hosted in Microsoft services - including email - was sometimes a target in the [SolarWinds-related] incidents, but the attacker had gained privileged credentials in some other way," according to Microsoft's security team, which published a blog Thursday.

https://www.bankinfosecurity.com/microsoft-office-365-was-solarwinds-initial-attack-vector-a-15939#:~:text=Microsoft%27s%20security%20team%20says%20the,the%20SolarWinds%20supply%20chain%20attack.&text=Microsoft%20also%20points%20to%20credential%20theft.

Click link above to read more

Can your organization obtain reasonable cybersecurity? Yes, and here's how

Cybersecurity expectations are vague, and that has to change if there is any chance of approaching a reasonable amount of cybersecurity.

An IT axiom, "Do you know where your data is?" has been eclipsed by something more accountable: "Is your data reasonably secure?" That's what companies have to determine to protect themselves in the event of a cybersecurity attack.

"With data breaches making daily headlines and hackers developing innovative methods to penetrate cyber defenses, businesses must contemplate what 'reasonable-security' posture to implement for when—not if—a threat occurs," said Rick Lazio, former member of the US House of Representatives and senior vice president of Alliantgroup, and Mike Davis, CISO of Alliantgroup, in their article *Cybersecurity Risk: What does a 'reasonable' posture entail and who says so?* in CIO Dive.

https://www.techrepublic.com/article/can-your-organization-obtain-reasonable-cybersecurity-yes-and-heres-how/

Click link above to read more

Phishing service provider ‘SMS Bandit’ arrested in the UK

The UK’s Metropolitan Police force has arrested a 20-year-old man from Birmingham for allegedly operating an online service that provided SMS phishing (or smishing) campaigns. Known in the cyber underworld as “SMS Bandit”, the phishing service would involve cybercriminals distributing fake SMS messages in high volumes to unsuspecting victims, pretending to be from reputable brand names including PayPal, telecommunication providers, COVID-19 pandemic services.

Once the scammers gained access to account credentials, these would then be sold across the dark web marketplaces they operated. Having been first reported by Krebs on Security, there are several users associated with this particular phishing service, posting promotional messages on various cybercrime forums under the following alias’: “SMSBandits,” “Gmuni,” “Bamit9,” and “Uncle Minus.”

https://www.itsecurityguru.org/2021/02/05/phishing-service-provider-sms-bandit-arrested-in-the-uk/?utm_source=rss

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