December 21, 2021

Challenge yourself with our NEW Gift Card Scam Awareness quiz!

Here are the top Security News Digest stories from 2021.

This is the last Security News Digest of 2021. Happy Holidays - see you in 2022!

This past year's stories:

The threats arising from the massive SolarWinds hack (January)

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

Russian hackers found to have accessed email of U.S. Homeland Security head, cybersecurity staff (March)

Stolen data of 533 million Facebook users leaked online (April)

Major U.S. pipeline crippled in ransomware attack (May)

Canada Post reports data breach to 44 large businesses, 950K customers affected (June)

U.S. government launches "StopRansomware" site (July)

Why phone scams are so difficult to tackle (August)

Why ransomware hackers love a holiday weekend (September)

Governments hacked REvil ransomware group & forced to go offline (October)

Phishing remains the most common cause of data breaches, survey says (November)

Apache Log4j vulnerability guidance (December)

The threats arising from the massive SolarWinds hack

Like the coronavirus, it came from overseas, arriving, initially, unnoticed. When it was finally, belatedly discovered, the outrage (for a few days at least) was epic. "This is nothing short of a virtual invasion by the Russians into critical accounts of our federal government," said Democratic Senator Dick Durbin. Republican Senator Mitt Romney called it "an extraordinary invasion of our cyberspace." The Russians, it's believed, hacked into the software of a company called SolarWinds, causing them to push out

malicious updates – call it a "cyber virus" – infecting the computer systems of more than 18,000 private and government customers. Almost a cyber pandemic.

https://www.cbsnews.com/news/the-threats-arising-from-the-massive-solarwinds-hack/

Click above link to read more.

Back to top

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

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 above link to read more.

Back to top

Russian hackers found to have accessed email of U.S. Homeland Security head, cybersecurity staff

Suspected Russian hackers gained access to email accounts belonging to the Trump administration's head of the U.S. Department of Homeland Security and members of the department's cybersecurity staff whose jobs included hunting threats from foreign countries, The Associated Press has learned.

The intelligence value of the hacking of then-acting secretary Chad Wolf and his staff is not publicly known, but the symbolism is stark. Their accounts were accessed as part of what's known as the SolarWinds intrusion, and it throws into question how the U.S. government can protect individuals, companies and institutions across the country if it can't protect itself. The short answer for many security experts and federal officials is that it can't — at least not without some significant changes.

"The SolarWinds hack was a victory for our foreign adversaries and a failure for DHS," said Sen. Rob Portman of Ohio, top Republican on the Senate's homeland security and governmental affairs committee. "We are talking about DHS's crown jewels."

https://www.cbc.ca/news/world/russian-hack-solarwinds-us-government-1.5968734

Click above link to read more.

Back to top

Stolen data of 533 million Facebook users leaked online

A user in a low-level hacking forum on Saturday published the phone numbers and personal data of hundreds of millions of Facebook users for free. The exposed data includes the personal information of over 533 million Facebook users from 106 countries, including over 32 million records on users in the US, 11 million on users in the UK, and 6 million on users in India. It includes their phone numbers, Facebook IDs, full names, locations, birthdates, bios, and, in some cases, email addresses. Insider reviewed a sample of the leaked data and verified several records by matching known Facebook users' phone numbers with the IDs listed in the data set. We also verified records by testing email addresses from the data set in Facebook's password-reset feature, which can be used to partially reveal a user's phone number.

https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

Click above link to read more.

Back to top

Major U.S. pipeline crippled in ransomware attack

A ransomware attack has halted pipeline activities for the Colonial Pipeline Co., which supplies the East Coast with roughly 45 percent of its liquid fuels. In a statement released on Saturday, Colonial Pipeline said it has temporarily halted pipeline operations in response to a cyberattack impacting the company starting Friday. “On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware,” the company wrote in the Saturday statement. As a precaution, the company took key systems offline to avoid further infections, it said. “In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems,” the company stated. “Upon learning of the issue, a leading, third-party cybersecurity firm was engaged, and they have launched an investigation into the nature and scope of this incident, which is ongoing.”

https://threatpost.com/pipeline-crippled-ransomware/165963/

Click above link to read more.

Back to top

Canada Post reports data breach to 44 large businesses, 950K customers affected

A malware attack on one of Canada Post’s suppliers has caused a data breach affecting 44 of the company’s large business clients and their 950,000 receiving customers, the postal agency confirmed Wednesday.

It said the information affected is from July 2016 to March 2019, and 97 per cent of it comprised the names and addresses of receiving customers. The remaining three per cent contained email addresses and/or phone numbers, the company said.

https://globalnews.ca/news/7894760/canada-post-data-breach/

Click above link to read more.

Back to top

U.S. government launches “StopRansomware” site

The U.S. government's first interagency initiative to address the growing threat of ransomware launched Wednesday.

StopRansomware.gov, a website managed by the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) along with the Department of Justice (DOJ) and the White House, offers cybersecurity resources, tools and other information. The site offers tips and guidance for ransomware attack preparation, prevention and response, with focuses on best practices such as restricting users' permissions, which may prevent malware from running or limit its capability to spread through a network. More importantly, incidents can be reported directly through the website.

https://searchsecurity.techtarget.com/news/252504063/US-government-launches-StopRansomware-site

Click above link to read more.

Back to top

Why phone scams are so difficult to tackle

Many of us now refuse to answer telephone calls from an unknown number, for fear that it could be a scam.

And we dread receiving a text message, purportedly from our bank or a delivery firm, again due to concerns that it might be from fraudsters.

A recent report suggests that we are right to be cautious. In the 12 months to March 2021, phone call and text message fraud across England, Wales and Northern Ireland was up 83% from the previous year, according to consumer group Which?.

https://www.bbc.com/news/business-58254354

Click above link to read more.

Back to top

Why ransomware hackers love a holiday weekend

On the Friday heading into Memorial Day weekend this year, it was meat-processing giant JBS. On the Friday before the Fourth of July, it was IT-management software company Kaseya and, by extension, over a thousand businesses of varying size. It remains to be seen whether Labor Day will see a high-profile ransomware meltdown as well, but one thing is clear: hackers love holidays.

Really, ransomware hackers love regular weekends, too. But a long one? When everyone’s off carousing with family and friends and studiously avoiding anything remotely office-related? That’s the good stuff. And while the trend isn’t new, a joint warning issued this week by the FBI and the Cybersecurity and Infrastructure Security Agency underscores how serious the threat has become.

https://arstechnica.com/information-technology/2021/09/why-ransomware-hackers-love-a-holiday-weekend/

Click above link to read more.

Back to top

Governments hacked REvil ransomware group & forced to go offline

On an active international operation that was executed recently by the US along with the multi-country law enforcement agencies, the Notorious ransomware group REvil themselves became the target of hacking and were forced to curtail their activities on the network.

The direct victims of the Russian-led criminal gang include top meatpacker JBS (JBSS3.SA), and the Colonial Pipeline. But, right now after this chasing incident the website of the REvil ransomware group known as “Happy Blog” is no longer available.

https://cybersecuritynews.com/governments-hacked-revil-ransomware-group/

Click above link to read more.

Back to top

Phishing remains the most common cause of data breaches, survey says

Phishing, malware, and denial-of-service attacks remained the most common causes for data breaches in 2021. Data from Dark Reading’s latest Strategic Security Survey shows that more companies experienced a data breach over the past year because of phishing than any other cause. The percentage of organizations reporting a phishing-related breach is slightly higher in the 2021 survey (53%) than in the 2020 survey (51%). The survey found that malware was the second biggest cause of data breaches over the past year, as 41% of the respondents said they experienced a data breach where malware was the primary vector.

Even though there have been a number of high-profile ransomware attacks over the past year, the number of organizations in the survey who experienced a breach as a result of ransomware is relatively low. Just 13% of organizations in the survey reported a ransomware-related breach in the past 12 months, compared to 17% in the 2020 survey.

https://www.darkreading.com/edge-threat-monitor/phishing-remains-the-most-common-cause-of-data-breaches-survey-says

Click above link to read more.

Back to top

Apache Log4j vulnerability guidance

CISA and its partners, through the Joint Cyber Defense Collaborative, are responding to active, widespread exploitation of a critical remote code execution (RCE) vulnerability (CVE-2021-44228) in Apache’s Log4j software library, versions 2.0-beta9 to 2.14.1, known as "Log4Shell" and "Logjam." Log4j

is very broadly used in a variety of consumer and enterprise services, websites, and applications—as well as in operational technology products—to log security and performance information. An unauthenticated remote actor could exploit this vulnerability to take control of an affected system.

Apache released Log4j version 2.15.0 in a security update to address this vulnerability. However, in order for the vulnerability to be remediated in products and services that use affected versions of Log4j, the maintainers of those products and services must implement this security update. Users of such products and services should refer to the vendors of these products/services for security updates. Given the severity of the vulnerability and the likelihood of an increase in exploitation by sophisticated cyber threat actors, CISA urges vendors and users to take the following actions.

https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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