January 11, 2022

Challenge yourself with our NEW Cyber Security Resolutions quiz!

This past week's stories:

'There is no Omicron Emergency Benefit': What to do if you receive this text

Barrie police issued a fraud alert for residents regarding a COVID-19 scam sent as a text message.

"A new year and yet another new scam," the force noted on social media.

The police service said the message was sent to a Barrie Police Services issued phone regarding a so-called Omicron Emergency Benefit.

https://barrie.ctvnews.ca/there-is-no-omicron-emergency-benefit-what-to-do-if-you-receive-this-text-1.5730012

Click above link to read more.

Back to top

Man charged after 'phishing' scheme to get unpublished works from Margaret Atwood, Ethan Hawke uncovered

Authorities say they've solved a publishing industry whodunit with the arrest Wednesday of a man accused of numerous literary heists in recent years, allegedly impersonating others in the industry to amass a veritable library of unpublished works.

Filippo Bernardini, an Italian citizen working in publishing in London, was arrested Wednesday after arriving at John F. Kennedy International Airport in New York, said Damian Williams, U.S. attorney for the Southern District of New York in a statement.

https://www.cbc.ca/news/entertainment/phishing-unpublished-arrest-1.6306584

Click above link to read more.

Back to top

Google Docs comments weaponized in new phishing campaign

The operators behind a recent phishing campaign are exploiting the commenting feature in Google Docs to send seemingly legitimate emails that convince targets to click malicious links.

This isn't the first time threat actors have found ways to exploit user trust in Google's popular productivity suite, report the Avanan researchers who discovered this campaign. Earlier this year, they observed attackers sending links to Google Docs files that contained a malicious download. Victims who downloaded the file were tricked into entering their login credentials.

https://www.darkreading.com/attacks-breaches/google-docs-comments-weaponized-in-new-phishing-campaign

Click above link to read more.

Back to top

Google fixes nightmare Android bug that stopped user from calling 911

Android's January security patch is out, and it's addressing one of the nastiest Android bugs to come up in some time: certain apps can stop you from contacting 911 or other worldwide emergency services numbers.

In early December, a harrowing tale popped up in the GooglePixel subreddit from a user whose Pixel 3 crashed when they needed it most: while dialing 911 for their grandmother who "appeared to be having a stroke." The whole phone subsystem seemed to immediately crash upon calling emergency services, with user "KitchenPicture5849" saying they couldn't get the call to connect or hang up to try the call again. Luckily, a nearby landline was available after their Android phone let them down, and emergency services was able to be contacted.

https://arstechnica.com/gadgets/2022/01/google-fixes-nightmare-android-bug-that-stopped-user-from-calling-911/

Click above link to read more.

Back to top

Chinese police rap Walmart for cybersecurity loopholes - local media

Chinese authorities rapped Walmart for allegedly violating cybersecurity laws, local media reported, the latest trouble for the U.S. retailer that is already a target of accusations in the country for supposedly stopping sales of products from Xinjiang.

Police in the southern Chinese city of Shenzhen discovered 19 "vulnerabilities" in Walmart's network system in late November and accused it of being slow to fix the loopholes, the China Quality News, backed by the country's market regulator, reported on Wednesday.

https://ca.finance.yahoo.com/news/chinese-police-rap-walmart-cybersecurity-055858256.html

Click above link to read more.

Back to top

3.7M FlexBooker records dumped on hacker forum

Attackers are trading millions of records from a trio of pre-holiday breaches on an online forum.

A threat group that identifies itself as Uawrongteam is dumping data stolen from FlexBooker – a popular online appointment scheduling tool for booking services ranging from counseling to haircuts – on a cybercriminal forum.Click above link to read more.

https://threatpost.com/flexbooker-records-dumped-hacker-forum/177460/

Click above link to read more.

Back to top

UK NHS: Threat actor targets VMware Horizon servers using Log4Shell exploits

The security team of the UK National Health Service (NHS) said that it detected an unknown threat actor using the Log4Shell vulnerability to hack VMWare Horizon servers and plant web shells for future attacks.

“The web shell can then be used by an attacker to carry out a number of malicious activities such as deploying additional malicious software, data exfiltration, or deployment of ransomware,” the NHS team said in a security alert published on Wednesday.

https://therecord.media/uk-nhs-threat-actor-targets-vmware-horizon-servers-using-log4shell-exploits/

Click above link to read more.

Back to top

Log4j updates: flaw challenges global security leaders

The security world continues its fight against potential widespread exploitation of the critical remote code execution vulnerability - tracked as CVE-2021-44229 - in Apache's Log4j software library, versions 2.0-beta9 to 2.14.1, known as "Log4Shell" and "Logjam."

As the U.S. Cybersecurity and Infrastructure Security Agency warns, Log4j is "very broadly used in variety of consumer and enterprise services, websites, and applications - as well as in OT products - to log security and performance information." An unauthenticated remote actor, CISA warns, could exploit this vulnerability to take control of an affected system.

https://www.bankinfosecurity.com/log4j-updates-flaw-challenges-global-security-leaders-a-18142

Click above link to read more.

Back to top

Researchers find bugs in over a dozen widely used URL parser libraries

A study of 16 different Uniform Resource Locator (URL) parsing libraries has unearthed inconsistencies and confusions that could be exploited to bypass validations and open the door to a wide range of attack vectors.

In a deep-dive analysis jointly conducted by cybersecurity firms Claroty and Synk, eight security vulnerabilities were identified in as many third-party libraries written in C, JavaScript, PHP, Python, and Ruby languages and used by several web applications.

https://thehackernews.com/2022/01/researchers-find-bugs-in-over-dozen.html

Click above link to read more.

Back to top

---

7 predictions for global energy cybersecurity in 2022

We now live in a world where cyberattacks can shut down critical infrastructure. Those who follow the mega-trends driving the global economy — like the convergence of the digital revolution and the energy transition — understand that with more and more critical infrastructure remotely operated or digitally managed, it was only a matter of time before a cyberattack caused disruptions that crossed over into the physical world. Last year, I wrote that 2021 would "shine a light on the need for industrial cybersecurity."

Sure enough, a ransomware attack on the Colonial Pipeline operators prompted a weeklong shutdown, cutting nearly half of liquid fuel supplies for the eastern United States. Gas prices spiked, more than 10,000 gas stations ran out of fuel, and the targeted company paid $4.4 million in ransom. Federal and state governments stepped in to soften the economic impact, offering a $10 million reward to identify the individuals who perpetrated the attack.

https://www.darkreading.com/vulnerabilities-threats/7-predictions-for-global-energy-cybersecurity-in-2022

Click above link to read more.

Back to top

Exploit chains explained: How and why attackers target multiple vulnerabilities

Exploit chains (also known as vulnerability chains) are cyberattacks that group together multiple exploits to compromise a target. Cybercriminals use them to breach a device or system to greater success or impact compared to focusing on a single point of entry.

“The goal with exploit chain attacks is to gain kernel/root/system level access to compromise a system in order to execute an attack,” Forrester analyst Steve Turner tells CSO. “Exploit chains allow attackers to blend in within an organization’s environment by using vulnerabilities in normal system processes bypassing numerous defenses to quickly elevate themselves,” he adds. While exploit chain attacks typically require more time, effort, and expertise for cybercriminals, chaining exploits together allows malicious actors to carry out attacks that can be increasingly difficult to remediate depending on the length and sophistication of the vulnerability sequence.

https://www.csoonline.com/article/3645449/exploit-chains-explained-how-and-why-attackers-target-multiple-vulnerabilities.html

Click above link to read more.

Back to top

Cyber-spike: Orgs suffer 925 attacks per week, an all-time high

2021 dragged itself to a close under a Log4Shell-induced blitzkrieg. With millions of Log4j-targeted attacks clocking in per hour since the flaw’s discovery last month, there’s been a record-breaking peak of 925 cyberattacks a week per organization, globally.

The number comes out of a Monday report from Check Point Research (CPR), which found Log4Shell attacks to be a major contributor to a 50-percent increase year-over-year in overall attacks per week on corporate networks for 2021.

https://threatpost.com/cyber-spike-attacks-high-log4j/177481/

Click above link to read more.

Back to top

Google Drive accounted for the most malware downloads from cloud storage sites in 2021

The more that cybercriminals can take advantage of a legitimate service, the better their chances of tricking people into falling for their scams. That's why popular services from the likes of Google and Microsoft are exploited in malicious attacks. In fact, Google Drive ended 2021 as the most abused cloud storage service for malware downloads, according to security provider Netskope.

In its "January 2022 Cloud and Threat Report" released Tuesday, Netskope noted that cloud storage apps gained even greater adoption in 2021. For the year, 79% of the customers analyzed used at least one cloud storage app, up from 71% in 2020. The number of cloud storage apps in use also rose. Organizations with 500 to 2,000 employees used 39 different cloud storage apps last year, up from 35 the prior year.

https://www.techrepublic.com/article/google-drive-accounted-for-the-most-malware-downloads-from-cloud-storage-sites-in-2021/?ftag=TREe01923b&bhid=19662319145962710268575546540229&mid=13653872&cid=712327807

Click above link to read more.

Back to top

****

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