April 12, 2022

Challenge yourself with our Spring Cleaning quiz!

This past week's stories:

- University of Calgary launches new cybersecurity hub
- Researchers uncover how Colibri malware stays persistent on hacked systems
- Phishing hook: Are you on the line? Cybersecurity experts explain how the criminals lure you in
- Report: Increase in socially engineered, sophisticated cybersecurity attacks plagues organizations
- Researchers warn of FFDroider and Lightning info-stealers targeting users in the wild
- No plain sailing: modern pirates hack superyachts' cybersecurity
- Experts reflect: what are the biggest threats to cybersecurity in 2022?
- 67% of app developers have shipped code with known vulnerabilities
- Nordic countries discuss joint cyber defence
- Cybersecurity: Travel sector in the crosshairs of hackers
- European Commission officials targeted by spyware
- Wider access to training can ease business leaders' cybersecurity woes
- Major French hospital group stops ransomware attack with Darktrace AI

University of Calgary launches new cybersecurity hub

A new cybersecurity hub at the University of Calgary aims to arm students and industry with the tools to mitigate cyberattacks.

The Canadian Cyber Assessment, Training and Experimentation Centre opened Thursday. Its labs are designed to simulate situations that cybersecurity experts face in the field.

https://calgaryherald.com/news/local-news/university-of-calgary-launches-new-cybersecurity-hub

Click above link to read more.

Back to top

Researchers uncover how Colibri malware stays persistent on hacked systems

Cybersecurity researchers have detailed a "simple but efficient" persistence mechanism adopted by a relatively nascent malware loader called Colibri, which has been observed deploying a Windows information stealer known as Vidar as part of a new campaign.

"The attack starts with a malicious Word document deploying a Colibri bot that then delivers the Vidar Stealer," Malwarebytes Labs said in an analysis. "The document contacts a remote server at (securetunnel[.]co) to load a remote template named 'trkal0.dot' that contacts a malicious macro," the researchers added.

https://thehackernews.com/2022/04/researchers-uncover-how-colibri-malware.html

Click above link to read more.

Back to top

Phishing hook: Are you on the line? Cybersecurity experts explain how the criminals lure you in

You get hacked and suddenly everyone in your contact list gets spam. It's something we've all dealt with at one point or another. It happened to a WINK News anchor recently, and as he was warning everyone and changing his passwords, Investigative Reporter Céline McArthur went on the hunt to see what we can learn from this scam.

Identifying and tracking down cybercriminals can be nearly impossible. They're good at hiding in cyberspace and there are just so many of them. This is a screenshot of a cybersecurity threat intelligence map created by a company called FireEye. The company says it tracks cybercrimes across the globe in real-time.

https://www.winknews.com/2022/04/07/phishing-hook-are-you-on-the-line-cybersecurity-experts-explain-how-the-criminals-lure-you-in/

Click above link to read more.

Back to top

Report: Increase in socially engineered, sophisticated cybersecurity attacks plagues organizations

A new cybersecurity report from San Francisco-based Abnormal Security found that medical industries and insurance companies had a 45-60% chance of being the target of a phone fraud attack via email: a sophisticated scam where the scammer sends an email to the target, asking the target to call them. In the second half of 2021, those attacks increased by 10 percent.

Additionally, healthcare systems are seeing a rise in more legitimate-looking yet problematic business email compromise (BEC) attacks. This occurs when the scammer accesses the target's business email

and impersonates the target, and then uses that identity to create rapport with victims and get them to pay money.

https://medcitynews.com/2022/04/report-increase-in-socially-engineered-sophisticated-cybersecurity-attacks-plagues-organizations/

Click above link to read more.

Back to top

Researchers warn of FFDroider and Lightning info-stealers targeting users in the wild

Cybersecurity researchers are warning of two different information-stealing malware, named FFDroider and Lightning Stealer, that are capable of siphoning data and launching further attacks.

"Designed to send stolen credentials and cookies to a Command & Control server, FFDroider disguises itself on victim's machines to look like the instant messaging application 'Telegram,'" Zscaler ThreatLabz researchers Avinash Kumar and Niraj Shivtarkar said in a report published last week.

https://thehackernews.com/2022/04/researchers-warn-of-ffdroider-and.html

Click above link to read more.

Back to top

No plain sailing: modern pirates hack superyachts' cybersecurity

Superyachts are battling anonymous cyberattacks from a new kind of pirate whilst hydrogen-powered boats are on track to replace fossil fuels. These themes and more dominated this year's 28th edition of the Dubai International Boat Show.

Returning for the first time since the arrival of COVID, the Dubai International Boat Show is a highlight on the annual calendar for luxury boat manufacturers. Over 800 companies from more than 50 countries use the event as a platform to showcase and unveil their latest products.

https://www.euronews.com/next/2022/04/11/no-plain-sailing-modern-pirates-hack-superyacht-cybersecurity

Click above link to read more.

Back to top

Experts reflect: what are the biggest threats to cybersecurity in 2022?

The global threats faced by the UK are increasingly digital. Amid reports of cyberwarfare in Ukraine, CSW hears from key voices on the biggest threats and what the public sector can do to minimise them.

https://www.civilserviceworld.com/in-depth/article/experts-reflect-what-are-the-biggest-threats-to-cybersecurity-in-2022

Click above link to read more.

Back to top

67% of app developers have shipped code with known vulnerabilities

While software developers acknowledge the importance of a security-minded approach in the development lifecycle, 86% do not view application security as a top priority when writing code.

According to the State of Developer-Driven Security 2022 survey from Secure Code Warrior, developers' actions and attitudes toward software security are in conflict, opening up organizations to cyber threats.

https://www.securitymagazine.com/articles/97399-67-of-app-developers-have-shipped-code-with-known-vulnerabilities

Click above link to read more.

Back to top

Nordic countries discuss joint cyber defence capability

Nordic governments are holding urgent cross-border talks about IT network security collaboration with the aim of developing a common strategy to strengthen their national defences against the heightened threat of cyber attacks following Russia's invasion of Ukraine.

The need for a joint approach and collective action in cyber security is driven by the rapid deterioration in trade and political relations with a more openly menacing Russia.

https://newsazi.com/nordic-countries-discuss-joint-cyber-defence-capability/

Click above link to read more.

Back to top

Cybersecurity: Travel sector in the crosshairs of hackers

While the travel and tourism industry was one of the worst-hit sectors in the Covid-19 years, it has begun to pick up at a faster-than-expected pace because of several factors. Even at the peak of the pandemic in 2020, though, the travel and tourism industry's contribution to the GDP was $121.9 billion. The figure is expected to reach $512 billion by 2028.

With such growth, the sector is increasingly attracting the attention of cybercriminals. In the past 1-2 years, there have been an increasing number of cyberattacks on travel and tourism companies. In the last 12 months, we have also witnessed a rise in more sophisticated cyberattacks on IoT and crypto jacking attacks. With this, cybersecurity has become a top priority for the sector. Companies across the globe are setting aside budgets to keep themselves and their customers cybersafe.

https://www.financialexpress.com/lifestyle/travel-tourism/cybersecurity-travel-sector-in-the-crosshairs-of-hackers/2487349/

Click above link to read more.

Back to top

European Commission officials targeted by spyware

At least five officials at the European Commission were targeted by spyware last year, according to a report by news agency Reuters. The alleged breach reveals the failings of conventional cybersecurity defences, experts told Tech Monitor, and bolsters the argument for spyware to be regulated like military technology.

Former European Justice Commissioner Didier Reynders and at least four other Brussels-based officials were targeted using spyware, news agency Reuters reported today.

https://techmonitor.ai/technology/cybersecurity/european-commission-targeted-spyware

Click above link to read more.

Back to top

Wider access to training can ease business leaders' cybersecurity woes

The COVID-19 pandemic has only exacerbated this issue, creating new challenges now that remote working is more commonplace and society reliance on technology has generally increased.

Some data from last year offers useful context as to how prevalent the problem is. The Cyber Security Breaches Survey 2021 found that among those identifying any breaches or attacks, half of businesses (49%) and over two fifths of charities (44%) say this happens once a month or more often.

https://www.bcs.org/articles-opinion-and-research/wider-access-to-training-can-ease-business-leaders-cybersecurity-woes/

Click above link to read more.

Back to top

Major French hospital group stops ransomware attack with Darktrace AI

Darktrace, a global leader in cyber security AI, today announced that Antigena, its autonomous response technology, stopped a sophisticated ransomware attack at Dordogne Groupements Hospitaliers de Territoire (Dordogne GHT).

In 2021, still in the midst of the Covid-19 pandemic, Dordogne GHT selected Darktrace's detect, respond and investigate capabilities to defend against threats across all eleven of its hospitals including across corporate and medical devices in its accident and emergency departments. Just two months after deploying Darktrace, the Group, which employs close to 5,000 staff, was targeted by Ryuk ransomware - a notorious ransomware strain known to target critical organizations across the public sector globally.

https://finance.yahoo.com/news/major-french-hospital-group-stops-113200572.html

Click above link to read more.

Back to top

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