Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

January 29th, 2019

January is Resolutions Month

Watch out for the 20th Annual Privacy and Security Conference from Feb.6th to 8th.

This week's stories:

- **U.S. formally requests extradition of Huawei executive Meng Wanzhou** 🇨🇦
- **UK to become world leader in cyber security**
- **Voicemail phishing scam goes after passwords**
- **Train staff to watch for vishing, smishing**
- **Facebook facing record-breaking fine over privacy violations**
- **Spam Campaign Follows the White Rabbit to NSFW Phishing Scams**
- **U.S. Government Systems Will Be 'At Risk for Years to Come'**
- **Facebook Details the "Defense-in-Depth" Approach Used to Secure its Platform**
- **Collusion Investigation: 37 Indictments and Counting**
- **Data Privacy Day advice for consumers and businesses**
- **Theoretical Ransomware Attack Could Lead to Global Damages Says Report**
- **xDedic servers, domains seized by European law enforcement agencies**

U.S. formally requests extradition of Huawei executive Meng Wanzhou🇨🇦

https://www.theglobeandmail.com/world/article-huawei-executive-meng-wanzhou-arrives-for-hearing-at-vancouver-court/

The Canadian government has received a formal request for the extradition of a senior executive of Chinese tech giant Huawei Technologies as a judge in Vancouver agreed to a minor change in Meng Wanzhou's bail conditions.

If a judge commits Meng for extradition, Justice Minister David Lametti would ultimately determine whether she would be extradited to the United States to face charges of bank fraud, wire fraud and two counts of conspiracy to commit both.

Click link above to read more

UK to become world leader in cyber security

https://www.openaccessgovernment.org/world-leader-cyber-security/57678/

The UK is set to become a world leader in the race to eradicate some of the most damaging cyber security threats facing businesses and better protect consumers.

Businesses and consumers will benefit from increased security and protections built into digital devices and online services we use every day. This is with the help of up to £70 million in government investment through the Industrial Strategy Challenge Fund and backed by further investment from industry.

Click link above to read more

Voicemail phishing scam goes after passwords

https://www.itworldcanada.com/article/voicemail-phishing-scam-goes-after-passwords/414543

As if warning staff about suspicious email document attachments and links isn't enough, now infosec pros have to tell them to watch out for suspicious voice mail attachments trying to steal passwords.

Security vendor EdgeWave said this week it has seen a "dramatic increase" in phishing email using .EML attachments, which is a file extension for an e-mail message that will have another file within it. In this campaign, the message purports to be a voicemail left on a user's phone.

Click link above to read more

Train staff to watch for vishing, smishing

https://www.itworldcanada.com/article/train-staff-to-watch-for-vishing-smishing-report/414503

Email phishing campaigns are one of the favoured tools of cyber attackers these days. But employees need to also be trained to watch for voice and SMS-based phishing attacks because they are increasing, according to a new report.

In security vendor Proofpoint's annual State of the Phish report, 49 per cent of infosec pros surveyed said their organizations had experienced vishing (voice phising) and or smishing (SMS/text) attacks last year. That was an increase from 45 per cent in 2017.

Click link above to read more

Facebook facing record-breaking fine over privacy violations

https://globalnews.ca/news/4864724/facebook-federal-trade-commission-fine/

Facebook may be facing the biggest fine ever imposed by the U.S. Federal Trade Commission for privacy violations involving the personal information of its 2.2 billion users.

The FTC is considering hitting Facebook with a penalty that would top its previous record fine of $22.5 million , which it dealt to Google in 2012 for bypassing the privacy controls in Apple's Safari browser, according to The Washington Post. The story published Friday cited three unidentified people familiar with the discussions.

Click link above to read more

Spam Campaign Follows the White Rabbit to NSFW Phishing Scams

https://www.bleepingcomputer.com/news/security/spam-campaign-follows-the-white-rabbit-to-nsfw-phishing-scams/

A peculiar spam campaign is underway that contains attachments with links that redirect you to fake NSFW (not-safe-for-work) adult dating sites or affiliate sites for sites like Ashleymadison.com. After analysis by a researcher, it was discovered that blocking 7 IP address could protect your network from over 4,600 adult spam and malware domains.

Click link above to read more

U.S. Government Systems Will Be 'At Risk for Years to Come'

https://www.bleepingcomputer.com/news/security/us-government-systems-will-be-at-risk-for-years-to-come/

The US government will apparently need to get a handle on the same cybersecurity issues it grappled with in 2018 as for some agencies, subpar performance is expected for years to come.

State sponsored espionage, insider threats, securing infrastructure and supply chains and increases in cybercrime and the cost of cybercrime are among the top issues the government has to come to terms with. Other challenges for the government include picking better passwords, staying on top of patch management and cybersecurity awareness training.

Click link above to read more

Facebook Details the "Defense-in-Depth” Approach Used to Secure its Platform

https://www.bleepingcomputer.com/news/security/facebook-details-the-defense-in-depth-approach-used-to-secure-its-platform/

Facebook revealed the "defense-in-depth" approach it uses to make sure that its platform and services are secure and to find, fix, and prevent security issues to reach live deployment and affect end users.

As described by Collin Greene, Facebook's Manager of Product Security, the social networks' development and security teams use a "layered" approach for bug prevention and patching.

Click link above to read more

Collusion Investigation: 37 Indictments and Counting

https://www.databreachtoday.com/blogs/collusion-investigation-37-indictments-counting-p-2715

As Special Counsel Robert Mueller's investigation into Russian interference in the 2016 U.S. presidential elections continues, you could be forgiven for needing a spreadsheet to keep track of what's known about the probe.

Quick math: After more than 18 months, Mueller's investigation has led to 199 criminal charges, 37 indictments or guilty pleas and four prison sentences.

Click link above to read more

Data Privacy Day advice for consumers and businesses

https://www.itworldcanada.com/article/cyber-security-today-jan-28-2019-data-privacy-day-advice-for-consumers-and-businesses/414552

Today is Data Privacy Day, dedicated to raising awareness and promoting data protection best practices. Organizations are obliged under federal and provincial law in Canada, and state laws in the U.S., to protect personal information. But you have a great deal to do with ensuring control over your personal information online, and I’m going to talk about that today.

Click link above to read more

Theoretical Ransomware Attack Could Lead to Global Damages Says Report

https://www.bleepingcomputer.com/news/security/theoretical-ransomware-attack-could-lead-to-global-damages-says-report/

According to a speculative cyber risk scenario prepared by Cambridge University for risk management purposes, a ransomware strain that would manage to impact more than 600,000 businesses worldwide within 24 hours would potentially lead to damages of billions not covered by insurers.

First of all, it is important to understand that although the numbers look very scary, this type of an attack is practically impossible to pull off at the moment when taking into consideration the current capabilities of malware, anti-malware, and current IT ecosystems.

Click link above to read more

---

xDedic servers, domains seized by European law enforcement agencies

https://arstechnica.com/tech-policy/2019/01/xdedic-servers-domain-seized-by-european-law-enforcement-agencies/

The notorious website xDedic, where online criminals offered access to compromised computers and more, has been shuttered by numerous law enforcement agencies.

According to federal prosecutors in Tampa, Florida, the site "facilitated more than $68 million in fraud."

Law enforcement agencies in Germany, Belgium, and Ukraine seized the site's domain names and servers in Europe. No arrests or indictments were announced.

Click link above to read more

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:

Information Security Awareness Team - Information Security Branch

Office of the Chief Information Officer,

Ministry of Citizens' Services

4000 Seymour Place, Victoria, BC   V8X 4S8

https:www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Information Security Branch
www.gov.bc.ca/informationsecurity

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer