Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

April 16th, 2019

Try our April quiz - Spotting a Fake

This week's stories:

- **Ottawa should impose cyber obligations on banks, says national security expert** 🇨🇦
- **Canada, cyber and defence sectors 'lack mutual trust,' says industry report** 🇨🇦
- **How to control your privacy for Google services**
- **Huawei Poses 'No Threat' According to Belgium, Trump Not Convinced**
- **'Nasty List' Phishing Scam Targets Instagram Users**
- **Attackers Spoofing Known Tech, Security Brands**
- **England and Wales Police Get Dedicated Cybercrime Units**
- **WikiLeaks Editor Julian Assange Arrested & Removed from Ecuadorian Embassy**
- **US CERT Warns of N. Korean 'Hoplight' Trojan**
- **Mobile VPNs Promoted by 'You Are Infected' or 'Hacked' Ads**

Ottawa should impose cyber obligations on banks, says national security expert

https://www.itworldcanada.com/article/ottawa-should-impose-cyber-obligations-on-banks-says-national-security-expert/416944

Ottawa must give Canadian banks more pointed direction to improve their ability to withstand cyber-attacks, says the country's former national security advisor.

"Government legislatively has to impose obligations on financial institutions, much in the same way they have done with money laundering," Richard Fadden told parliament's Public Safety committee on Wednesday.

Click link above to read more

Canada, cyber and defence sectors 'lack mutual trust,' says industry report

https://www.itworldcanada.com/article/canada-cyber-and-defence-sectors-lack-mutual-trust-says-industry-report/417046

The federal government isn't working closely enough with the cyber security sector in purchasing products or sharing threat information, says a recent report from the country's defence sector.

The report by the Canadian Association of Defence and Security Industries (CADSI), says there's an urgent need for the Canadian Armed Forces (CAF) to operate, defend and project power in the cyber domain.

Click link above to read more

How to control your privacy for Google services

https://www.itworldcanada.com/article/how-to-control-your-privacy-for-google-services/416887

It should be no surprise that Google scrapes all sorts of information about you. The collected information is then used to produce targeted advertisements and improve services. Despite our vigilant efforts to safeguard our privacy on the web, it’s becoming harder and harder to avoid the grasp of such a wide-spread service.

Click link above to read more

Huawei Poses 'No Threat' According to Belgium, Trump Not Convinced

https://www.infosecurity-magazine.com/news/huawei-poses-no-threat-according/

The Belgian Centre for Cybersecurity (CCB) has reportedly decided not to issue "a negative opinion" on Huawei following several months of investigation with no concrete evidence found.

According to The Brussels Times, the CCB has been looking for evidence of spying by Huawei. This comes as the Chinese technology company has faced several accusations globally of spying.

In Belgium, Huawei works with Proximus, Orange and Telenet/Base. It also opened a cybersecurity lab in Brussels back in March.

Click link above to read more.

‘Nasty List’ Phishing Scam Targets Instagram Users

https://www.infosecurity-magazine.com/news/nasty-list-phishing-scam-targets-1/

Instagram users are being warned not to fall for a new phishing scam doing the rounds which aims to harvest log-ins and spread worm-like across the social network.

According to Twitter users who have posted screenshots of the scam, users typically first receive a direct message from an account they are following. This could include one of several variations on the same theme, which is that the recipient has been featured on a ‘nasty list.’

Click link above to read more

Attackers Spoofing Known Tech, Security Brands

https://www.infosecurity-magazine.com/news/attackers-spoofing-known-tech-1/

Researchers at GreatHorn have identified what they are calling a widespread attack in which attackers spoofed both the Microsoft brand in the display name and the Barracuda Networks brand in the return path and received headers, with the goal of stealing credentials.

The team identified an attack notable in that the return path spoofs a noreply.barracudanetworks.com return path. “The attackers crafted the received headers so that it appears to have gone through multiple “Barracuda” hops prior to sending the email via a server designed to look like a Barracuda server. Microsoft has then automatically appended legitimate received header details to the spoofed headers, making it appear that much more legitimate,” researchers wrote.

Click link above to read more

England and Wales Police Get Dedicated Cybercrime Units

https://www.infosecurity-magazine.com/news/england-wales-police-dedicated-1/

Every England and Wales police force now has a dedicated cybercrime unit, thanks to a multimillion-pound government investment, it was revealed yesterday.

The announcement was made by the National Police Chief's Council (NPCC) National Cybercrime Programme and claimed that forces were able to access £7m in funds to fill the units with specialist officers and equipment.

Click link above to read more

WikiLeaks Editor Julian Assange Arrested & Removed from Ecuadorian Embassy

https://www.infosecurity-magazine.com/news/wikileaks-assange-arrested-1-1-1-1/

Julian Assange, editor of whistleblowing website WikiLeaks, has been arrested by the Metropolitan Police for failing to surrender to a court.

According to a statement by the Metropolitan Police, Assange was arrested at the Embassy of Ecuador in Knightsbridge where he has been resident since June 19 2012. The warrant was issued on June 29 2012.

A statement from the Home Office confirmed that Assange was "arrested in relation to a provisional extradition request from the United States of America" where he is accused of computer related offences.

Click link above to read more

US CERT Warns of N. Korean 'Hoplight' Trojan

https://www.bankinfosecurity.com/us-cert-warns-n-korean-hoplight-trojan-a-12374

The U.S. Computer Emergency Readiness Team has issued a fresh warning about a newly discovered Trojan called Hoplight that is connected to a notorious advanced persistent threat group with links to North Korea.

The malware can disguise the network traffic it sends back to its originators, making it more difficult for security companies and law enforcement officials to track its movements, CERT reports. While Hoplight has been spotted in the wild, CERT did not name any victims or mention whether it has targeted a specific industry.

Click link above to read more

Mobile VPNs Promoted by 'You Are Infected' or 'Hacked' Ads

https://www.bleepingcomputer.com/news/security/mobile-vpns-promoted-by-you-are-infected-or-hacked-ads/

Mobile VPN affiliates are displaying scam ads that state your mobile device is infected, has been hacked, or is being tracked in order to scare visitors into purchasing a subscription.

VPN companies offer affiliate programs where web sites and online marketers can earn a commission by promoting their products. To do this, an affiliate will refer people to a VPN's site or product page using a specially crafted link. If the referred user purchases a VPN subscription, the affiliate earns a commission.

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer