Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

December 24th, 2019

Try our December quiz – Shopping Safety

Save the date - February 5th to 7th is the Privacy and Security Conference

This week's stories:

- **LifeLabs cyberattack one of 'several wake-up calls' for e-health security and privacy** 🇨🇦
- **Two-Year Long Phishing Campaign Impersonates Canadian Banks** 🇨🇦
- **This password-stealing hacking campaign is targeting governments around the world**
- **Year in review: Cyber incidents in 2019, predictions for 2020**
- **Amazon used "security" to sell Ring doorbells, then blamed customers when hackers broke into them**
- **Facebook Ads Manager Exploited by Trojan That Steals Personal Data Using Legitimate-Looking Certificates**
- **Malware is going to get weirder in 2020, so it's time for enterprises to get weird too, says Trend Micro exec**
- **US Navy Bans TikTok, Citing 'Cybersecurity Threat'**
- **Contractor admits planting logic bombs in his software to ensure he'd get new work**

LifeLabs cyberattack one of 'several wake-up calls' for e-health security and privacy 🇨🇦

https://www.cbc.ca/news/lifelabs-data-breech-security-ehealth-1.5400817

The data breach of the Canadian laboratory testing company LifeLabs is one of "several wake-up calls" for security and privacy challenges that come with the push for a medical system in which eHealth plays a significant role.

"The medical field for us is one of the worst when it comes to cyber security practices," said David Kennedy, cyber security expert and founder and CEO of TrustedSec, an information security consulting firm.

"What's interesting about the large push for electronic patient health-care information that you put online is that a lot of these organizat

ions are not designed to withstand attacks."

Click link above to read more

Two-Year Long Phishing Campaign Impersonates Canadian Banks 🇨🇦

https://www.bleepingcomputer.com/news/security/two-year-long-phishing-campaign-impersonates-canadian-banks/

Canadian banks are being impersonated in a phishing campaign targeting both individuals and businesses via a large-scale infrastructure shared with previous attacks going back to 2017 and pointing to the same attackers.

The infrastructure behind these Canadian focused attacks includes hundreds of phishing websites designed to mimic major Canadian banks' websites as part of an effort to steal user credentials from the financial institutions' clients.

To get the targets on their phishing landing pages, the attackers use custom-crafted and legitimate-looking email messages with malicious PDF attachments.

Click link above to read more

This password-stealing hacking campaign is targeting governments around the world

https://www.zdnet.com/article/cybersecurity-this-password-stealing-hacking-campaign-is-targeting-governments-around-the-world/

A mysterious new phishing campaign is targeting government departments and related business services around the world in cyberattacks that aim to steal the login credentials from victims.

In total, the phishing attacks have targeted at least 22 different potential victim organisations in countries including the United States, Canada, China, Australia, Sweden and more. All of the attacks involve emails claiming to be related to the targeted government agencies and all of them attempt to trick victims into clicking an email link that asks for their username and password.

Anyone who enters their login credentials into the spoofed government agency websites will give cyber criminals access to their account.

Click link above to read more

Year in review: Cyber incidents in 2019, predictions for 2020

https://www.itworldcanada.com/article/year-in-review-cyber-incidents-in-2019-predictions-for-2020/425396

This year was a banner year globally in cybersecurity — for criminals.

Despite years of best practices available for organizations to follow, lessons still haven’t been learned by many firms in 2019.

Headlines about ransomware, business email compromise, e-commerce website scraped for credit card data and data theft popped up daily.

Click link above to read more

Amazon used "security" to sell Ring doorbells, then blamed customers when hackers broke into them

https://boingboing.net/2019/12/19/amazon-used-security-to-se.html

Just a week after hackers broke into a Ring camera in a childs’ bedroom taunting the child and sparking serious concerns about the company’s security practices, Buzzfeed News is reporting that over 3,600 Ring owners’ email addresses, passwords, camera locations, and camera names were dumped online. This Includes cameras recording private spaces inside homes.

This stunning new leak could potentially provide criminals and stalkers with access to view live video feeds from inside and around thousands of Ring customers' homes, see archived videos, and get the precise location of all Ring devices attached to the compromised account by studying the orientation of the footage and location information attached to each camera.

Click link above to read more

Facebook Ads Manager Exploited by Trojan That Steals Personal Data Using Legitimate-Looking Certificates

https://www.cpomagazine.com/cyber-security/facebook-ads-manager-exploited-by-trojan-that-steals-personal-data-using-legitimate-looking-certificates/

A trojan that steals user personal information has been running wild across the web in recent days. It originates from a fake PDF reader distributed by several different sites, and once installed attempts to access victim Facebook sessions to grab cookies and gain illicit access to Facebook Ads Manager. BleepingComputer is reporting that in addition to the attempt to steal Facebook data, the trojan also hijacks Amazon sessions in an attempt to breach user accounts.

The trojan-bearing software, called PDFReader, is especially insidious as it makes use of a legitimate-looking digital security certificate to signal to unwary downloaders that it is provided by a safe site.

Click link above to read more

Malware is going to get weirder in 2020, so it's time for enterprises to get weird too, says Trend Micro exec

https://www.itworldcanada.com/article/malware-is-going-to-get-weirder-in-2020-so-its-time-for-enterprises-to-get-weird-too-says-trend-micro-exec/425433

As we leave 2019 behind, a new year approaches. And with it comes the impending waves of new malware that businesses will have to defend themselves from.

Looking towards 2020, Myla Pilao, the director of technology marketing for cybersecurity firm Trend Micro, sees three major trends on the horizon: an increase in malware using unconventional behaviors, an emergence of Linux-based malware, and a continued increase in the volume and complexity of info-stealing malware.

Click link above to read more

US Navy Bans TikTok, Citing 'Cybersecurity Threat'

https://www.pcmag.com/news/372673/us-navy-bans-tiktok-citing-cybersecurity-threat

Lawmakers are urging the United States Armed Forces to drop TikTok as an approved app. Service members in the US can no longer use TikTok on government-issued smartphones, according to Reuters, due to the popular video-sharing app's emergence as a "cybersecurity threat."

Both the Navy and the Army are disabling smartphones with TikTok currently installed. Any members still using the app are now unable to access branch intranets. In a statement, Navy Lieutenant Colonel Uriah Orland confirmed TikTok has been banned to "address existing and emerging threats." Simply put: the US government doesn't trust developer ByteDance, and that's enough for the US Armed Forces to act.

Click link above to read more

Contractor admits planting logic bombs in his software to ensure he'd get new work

https://arstechnica.com/tech-policy/2019/12/contractor-admits-planting-logic-bombs-in-his-software-to-ensure-hed-get-new-work/

Many IT workers worry their positions will become obsolete as changes in hardware, software, and computing tasks outstrip their skills. A former contractor for Siemens concocted a remedy for that—plant logic bombs in projects he designed that caused them to periodically malfunction. Then wait for a call to come fix things.

On Monday, David A. Tinley, a 62-year-old from Harrison City, Pennsylvania, was sentenced to six months in prison and a fine of $7,500 in the scheme. The sentence came five months after he pleaded guilty to a charge of intentional damage to a protected computer. Tinley was a contract employee for Siemens Corporation at its Monroeville, Pennsylvania, location.

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