



Security News Digest

Information Security Branch







OCIO

Office of the
Chief Information Officer

June 30th, 2020

Try our June - [Connect with Care Quiz](#)

This week's stories:

- [Canadian privacy commissioners to investigate Tim Hortons data collection practices](#) 
- [Privacy commissioners in B.C., Ontario, order LifeLabs to improve security](#) 
- [Canadian political leaders need to get behind COVID-19 app, says expert](#) 
- [Canada's remote workers embrace change but lack clarity on what's next](#) 
- [Microsoft purchases CyberX: Four main takeaways](#)
- [Twitter 'incident' leaves billing info stored in browser cache](#)
- [Evil Corp's 'WastedLocker' Campaign Demands Big Ransoms](#)
- [Over Two-Thirds of Q1 Malware Hidden by HTTPS](#)
- [China's disinformation threat is real. We need better defences against state-based cyber campaigns](#)
- [Hackers Revealed More Than 300 Windows 10 Executables Are Vulnerable to DLL Hijacking Attack](#)

Canadian privacy commissioners to investigate Tim Hortons data collection practices

<https://www.itworldcanada.com/article/canadian-privacy-commissioners-to-investigate-tim-hortons-data-collection-practices/432594>

Canada's privacy commissioner and three provincial counterparts have launched an investigation into Tim Hortons' mobile app for how it's tracking its user's activities.

The Office of the Privacy Commissioner of Canada, along with the privacy commissioners of Quebec, British Columbia, and Alberta, will jointly examine if Tim Hortons' app adheres to the Personal Information Protection and Electronic Documents Act (PIPEDA).

[Click link above to read more](#)

Privacy commissioners in B.C., Ontario, order LifeLabs to improve security

<https://www.canadiansecuritymag.com/privacy-commissioners-in-b-c-ontario-order-lifelabs-to-improve-security/>

VICTORIA – A joint investigation by the privacy commissioners of Ontario and British Columbia says Lifelabs failed to put in place reasonable safeguards to protect the personal health information of millions of Canadians.

A statement released Thursday by the commissioners says the breach last year at LifeLabs, one of Canada's largest medical services companies, broke Ontario's health privacy law and B.C.'s personal information protection law.

[*Click link above to read more*](#)

Canadian political leaders need to get behind COVID-19 app, says expert

<https://www.itworldcanada.com/article/canadian-political-leaders-need-to-get-behind-covid-19-app-says-expert/432581>

Canada's officially-sanctioned national COVID-19 exposure notification mobile app will be released for beta testing in Ontario on July 2.

However, an expert warns the goal of widespread adoption when the final version is released will fail unless the country's leaders are regularly upfront about its capabilities.

[*Click link above to read more*](#)

Canada's remote workers embrace change but lack clarity on what's next: report

<https://www.canadiansecuritymag.com/canadas-new-remote-workers-have-embraced-change-but-lack-clarity-on-what-comes-next/>

Canada's new remote workers have embraced change, but their employers have not yet committed to a flexible future, according to a recent survey from VMware Canada.

While nearly nine in 10 (87 per cent) of those who began working remotely for the first time during the COVID-19 pandemic believe it will have a long-term impact on the way we work, just 22 per cent have received confirmation that working arrangements will permanently be more flexible, and only 17 per cent say plans to return to the office have been clearly communicated by their employer.

[*Click link above to read more*](#)

Microsoft purchases CyberX: Four main takeaways

<https://www.zdnet.com/article/microsoft-purchases-cyberx/>

Earlier this week, Microsoft announced that it has acquired Massachusetts-based internet-of-things (IoT) and industrial control system (ICS) security vendor CyberX. While the purchase price was not disclosed, media reports are speculating that the purchase price was somewhere between \$150 million to \$165 million. Founded in 2013, CyberX has raised \$48 million in venture capital, so this deal provides a good return to investors.

CyberX's core solution can monitor IoT and ICS environments (passively or actively) to obtain asset information, risk, and vulnerability information, and real-time alerts about threats and malfunctioning operational equipment. The strategic intent behind the merger appears to be to expand the existing Microsoft Azure Security stack into ICS/operational technology (OT) environments.

[*Click link above to read more*](#)

Twitter 'incident' leaves billing info stored in browser cache

<https://www.scmagazine.com/home/security-news/privacy-compliance/twitter-incident-leaves-billing-info-stored-in-browser-cache/>

A "data security incident" at Twitter caused billing information for companies using the social media company's advertising and analytics platform to be stored in the browser's cache.

While Twitter doesn't believe the information – including the last four digits off credit card numbers, email addresses and phone numbers – has been compromised it can't rule out others have had access to it, the BBC cited a Twitter email to customers as saying. "We're very sorry this happened. We recognise and appreciate the trust you place in us, and are committed to earning that trust every day," the company said.

[Click link above to read more](#)

Evil Corp's 'WastedLocker' Campaign Demands Big Ransoms

<https://www.bankinfosecurity.com/evil-corps-wastedlocker-campaign-demands-big-ransoms-a-14497>

The Evil Corp cybercrime group, originally known for its use of the Dridex banking Trojan, is now using new ransomware called WastedLocker, demanding ransom payments of \$500,000 to \$1 million, according to security researchers at NCC Group's Fox-IT.

So far, less than a dozen victims have been targeted by the campaign, Fox-IT says, but its new research report does not specify if any ransoms have been paid. Evil Corp has been operating since 2011 and is believed to be based in Russia. It recently shifted to the newly created WastedLocker malware with a campaign mainly targeting businesses through phishing attacks that use the SocGholish fake update framework, which is being distributed through a custom Cobalt Strike loader, Fox-IT reports.

[Click link above to read more](#)

Over Two-Thirds of Q1 Malware Hidden by HTTPS

<https://www.infosecurity-magazine.com/news/over-twothirds-of-q1-malware/>

Over two-thirds of malware detected in the first three months of the year was hidden in HTTPS encrypted tunnels in a bid to evade traditional AV, according to Watchguard.

The security vendor's latest Internet Security Report for Q1 2020 is distilled from analytics provided by its 44,000 global appliances.

During the period they blocked over 32 million malware variants and nearly 1.7 million network attacks.

Some 67% of that malware was delivered via HTTPS connections and 72% of these encrypted attacks apparently featured zero-day malware which would have been missed by legacy signature-based AV.

[Click link above to read more](#)

China's disinformation threat is real. We need better defences against state-based cyber campaigns

https://theconversation.com/chinas-disinformation-threat-is-real-we-need-better-defences-against-state-based-cyber-campaigns-141044?&web_view=true

The Australian government recently announced plans to establish the country's first taskforce devoted to fighting disinformation campaigns, under the Department of Foreign Affairs and Trade (DFAT).

Last week, Foreign Minister Marise Payne accused China and Russia of “using the pandemic to undermine liberal democracy” by spreading disinformation to manipulate social media debate.

[Click link above to read more](#)

Hackers Revealed More Than 300 Windows 10 Executables Are Vulnerable to DLL Hijacking Attack

<https://cybersecuritynews.com/300-windows-10-executables-are-vulnerable-to-dll-hijacking-attack/>

Personal privacy and security are some of the most crucial and essential subjects that most users neglect. As recently, a security expert has unveiled more than 300 Windows 10 executables, that are vulnerable to the DLL hijacking attacks.

So, we must take the security into account, as in the current time, most of the private data is stored and processed on our computers.

[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:

<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.

