Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

August 25th, 2020
Try our August - 'Summer social media' Quiz

This week's stories:

- **Business email compromise attacks are rising in Canada: Canadian Anti-Fraud Centre**
- **CJEU invalidates the Privacy Shield: Why should Canada care?**
- **Canada's privacy laws have 'no teeth': What I learned during an eight-month investigation into Tim Hortons' data tracking**
- **A ransomware attack hit TFI International's four Canadian courier divisions last week, Canpar Express, ICS Courier, Loomis Express and TForce Integrated Solutions.**
- **Microsoft says the pandemic has changed the future of cybersecurity in these five ways**
- **CISA Releases 5G Security Guidelines**
- **Why Cybersecurity Is Crucial in Smart Cities**
- **CISA, FBI Alert Warns of Vishing Campaign**
- **New Cybersecurity Code of Practice for Installers Unveiled by BSIA**
- **NSA and CISA Alert Highlights Urgency for OT Security**
- **DarkSide: New targeted ransomware demands million dollar ransoms**

Business email compromise attacks are rising in Canada: Canadian Anti-Fraud Centre

https://www.itworldcanada.com/article/business-email-compromise-attacks-are-rising-in-canada-canadian-anti-fraud-centre/434796

Last December, an employee working out of the office for a Canadian firm received an email supposedly from the IT department asking them to reset their login credentials. That was the beginning of a complex scam that several months later cost the company $400,000 in part due to disarray caused by the COVID-19 pandemic.

Click link above to read more

CJEU invalidates the Privacy Shield: Why should Canada care?

https://www.itworldcanada.com/blog/cjeu-invalidates-the-privacy-shield-why-should-canada-care/434874

After months of eager anticipation, the Court of Justice of the European Union (CJEU) delivered its decision in Schrems II, the latest chapter in the ongoing tug-of-war between US laws that demand surveillance and EU data protection laws that require privacy.

The case assessed the tolerability of Facebook transferring personal information from the EU to the US, particularly in view of the vast scope and reach of America's pervasive surveillance apparatus.

Click link above to read more

Canada's privacy laws have 'no teeth': What I learned during an eight-month investigation into Tim Hortons' data tracking

https://www.thechronicleherald.ca/news/canada/canadas-privacy-laws-have-no-teeth-what-i-learned-during-an-eight-month-investigation-into-tim-hortons-data-tracking-488019/

I had been impatiently waiting for a particular email to arrive for two months before it finally hit my inbox last week. I was hoping to learn something new about Tim Hortons' location surveillance efforts by asking one of its technology partners what it had about me.

Back in June, I'd reported that the coffee chain had been tracking me and countless other customers through its mobile ordering app.

But Tim Hortons itself wasn't doing the data analytics work to process GPS signals and figure out where I lived and worked, as well as whenever I visited one of its competitors. Instead, Tim Hortons' parent company, Restaurant Brands International Inc., contracted that work out to New York-based Radar Labs Inc.

Click link above to read more

A ransomware attack hit TFI International's four Canadian courier divisions last week, Canpar Express, ICS Courier, Loomis Express and TForce Integrated Solutions.

https://securityaffairs.co/wordpress/107476/cyber-crime/canpar-express-ransomware.html

A couple of days after the transportation and logistics TFI International company raised millions of dollars in a share offering, the news of a ransomware attack against its four Canadian courier divisions (Canpar Express, ICS Courier, Loomis Express and TForce Integrated Solutions) made the headlines.

The news of the ransomware attack was published by the company on its website.

.

Click link above to read more

Microsoft says the pandemic has changed the future of cybersecurity in these five ways

https://www.techrepublic.com/article/microsoft-says-the-pandemic-has-changed-the-future-of-cybersecurity-in-these-five-ways/

A new report from Microsoft suggests that cloud-based technologies and Zero Trust architecture will become mainstays of businesses' cybersecurity investments going forward.

Cybersecurity has shot to the top of business agendas in recent months, as the sudden shift of workforces from the office to the home highlighted a host of new threats within remote-working setups. Add to that the explosion in opportunistic cybercriminals hoping to cash in on the situation, and businesses are faced with a security minefield as the prospect of remote work looms indefinitely.

Click link above to read more

CISA Releases 5G Security Guidelines

https://www.darkreading.com/mobile/cisa-releases-5g-security-guidelines/d/d-id/1338740

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has released the National Strategy to Secure 5G as directed by the United States National Cyber Strategy.

Within the strategy there are four defined lines of effort and five strategic initiatives to implement that strategy. The lines of effort are Facilitate Domestic 5G Rollout; Assess Risks to & Identify Core Security Principles of 5G Infrastructure; Address Risks to United States Economic and National Security During Development and Deployment of 5G Infrastructure Worldwide; and Promote Responsible Global Development and Deployment of 5G.

Click link above to read more

Why Cybersecurity Is Crucial in Smart Cities

https://iotbusinessnews.com/2020/08/24/49898-why-cybersecurity-is-crucial-in-smart-cities/

Smart cities are the future. Today more than ever, nations around the globe are starting to adopt new developments to enhance their cities' smart capabilities.

One such nation is Macau, which joined hands with the Chinese technology giant Alibaba group in 2017. The goal was to develop a public-private partnership project that aims to turn the special administrative region into a leading smart city in the Asia Pacific region.

Click link above to read more

CISA, FBI Alert Warns of Vishing Campaign

https://www.securityweek.com/cisa-fbi-alert-warns-vishing-campaign

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have issued an alert to warn of a voice phishing (vishing) campaign targeting the employees of multiple organizations.

As part of the attacks, which started in mid-July, adversaries were attempting to gain access to employee tools via phishing phone calls. Once they were in the possession of credentials, the attackers would access the databases of victim companies to harvest information on their customers and conduct further attacks.

Click link above to read more

New Cybersecurity Code of Practice for Installers Unveiled by BSIA

https://www.darkreading.com/physical-security/new-cybersecurity-code-of-practice-for-installers-unveiled-by-bsia/d/d-id/1338734

Installation of safety and security systems – cybersecurity code of practice, developed by the BSIA's Cybersecurity Product Assurance Group (CySPAG), will assist in providing confidence throughout the supply chain promoting secure connection of products and services and delivering client assurance regarding connected solutions. The code of practice will assist the supply chain in its duty of care to other network users, particularly with respect to protecting the integrity of existing cyber security countermeasures already in place, or the implementation of such countermeasures in new solutions.

Click link above to read more

NSA and CISA Alert Highlights Urgency for OT Security

https://www.securityweek.com/nsa-and-cisa-alert-highlights-urgency-ot-security

In the last few years, we've seen ample evidence of how cyberattacks on critical infrastructure can be leveraged by nation-states and other powerful adversaries as weapons in geopolitical conflicts. The attacks on the Ukraine power grid and several other incidents demonstrated a show of power and how a country's infrastructure can be disrupted. The indiscriminate use of destructive exploits in NotPetya (which caused widespread, collateral damage to operational technology (OT) networks and halted operations) revealed to security professionals just how poor the cyber risk posture of their OT networks is and prompted swift actions in many of the largest companies.

Click link above to read more

DarkSide: New targeted ransomware demands million dollar ransoms

https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/

A new ransomware operation named DarkSide began attacking organizations earlier this month with customized attacks that have already earned them million-dollar payouts.

Starting around August 10th, 2020, the new ransomware operation began performing targeted attacks against numerous companies.

In a "press release" issued by the threat actors, they claim to be former affiliates who had made millions of dollars working with other ransomware operations.

Click link above to read more