Security Digest
Information Security Branch
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer

July 17th, 2018

July is "Security while you travel" Month

This week's stories:

How to attempt to influence an election: Start with a spear-phishing campaign

https://www.itworldcanada.com/article/how-to-attempt-to-influence-an-election-start-with-a-spear-phishing-campaign/407102

Canadians worried about the possibility of a foreign government trying to secretly use the Internet to influence politics here could learn how it's apparently done by reading the indictment issued Friday against 12 Russian military intelligence officials accused of conspiring to interfere in the 2016 U.S. election.

The attack vector: The venerable spear-phishing attack with spoofed email addresses.

The treasure: Thousands of emails and documents from branches of the Democratic Party and the Hilary Clinton presidential campaign.

The deception: Deleted logs and computer files, including use of the commercial wiper software CCleaner.

The bitcoin angle: There's always a bitcoin angle. In this case it is alleged the conspiracy involved laundering the equivalent of $95,000 in the digital currency to pay for command and control servers and domains used for spoofing.

Click link above to read more

Thousands of patient records held for ransom in Ontario home care data breach, attackers claim

https://www.cbc.ca/news/technology/carepartners-data-breach-ransom-patients-medical-records-1.4749515

The detailed medical histories and contact information of possibly tens of thousands of home-care patients in Ontario are allegedly being held for ransom by thieves who recently raided the computer systems of a health-care provider.

CarePartners, which provides home medical care services on behalf of the Ontario government, announced last month that it had been breached. It said only that personal health and financial information of patients had been "inappropriately accessed," and did not elaborate further.

However, a group claiming responsibility for the breach recently contacted CBC News and provided a sample of the data it claims to have accessed, shedding new light on the extent of the breach.

Another document appears to contain more than 140 active patient credit card numbers and expiry dates, many with security codes.

The attackers claimed the sample was a subset of hundreds of thousands of patient records and related materials in their possession dating back to 2010.

Click link above to read more

UK info czar report highlights differences with Canada over political parties and privacy

https://www.itworldcanada.com/article/uk-info-czar-report-highlights-differences-with-canada-over-political-parties-and-privacy/407025

U.K. political parties should have to follow a statutory Code of Practice under the country's data privacy law if they use personal data in political campaigns, the country's information commissioner has urged in a report this week.

The tough recommendation stands in contrast with the Trudeau government's proposed Election Modernization Act (Bill C-76), which if passed in its current form would only oblige federal parties here to have an easily understandable policy explaining what personal information they collect, how it is used and how it is protected.

Bill C-76 is now being studied by the House of Commons committee on procedure.

Click link above to read more

South Korea's Bithumb loses $31.5m in cryptocurrency heist

https://www.theguardian.com/business/2018/jun/20/south-korea-bithumb-loses-315m-in-cryptocurrency-heist

The South Korean cryptocurrency exchange Bithumb said 35bn won ($31.5m) worth of virtual coins were stolen by hackers, the second local exchange targeted in just over a week as cyber thieves exposed the high risks of trading the digital asset.

Bithumb said in a notice on its website that it had stopped all trading after ascertaining "some cryptocurrencies worth about 35 billion won were seized between late yesterday and early morning today".

The exchange, the sixth busiest in the world according to Coinmarketcap.com, said it had stored all clients' assets in "safe cold wallets" – which operate on platforms not directly connected to the internet. It added that the company would fully compensate customers.

The Bithumb theft highlights the security risks and the weak regulation of global cryptocurrency markets. Global policymakers have warned investors to be cautious in trading the digital currency, given the lack of broad regulatory oversight.

Click link above to read more

'Data is a fingerprint': why you aren't as anonymous as you think online

https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy

In August 2016, the Australian government released an "anonymised" data set comprising the medical billing records, including every prescription and surgery, of 2.9 million people.

Names and other identifying features were removed from the records in an effort to protect individuals' privacy, but a research team from the University of Melbourne soon discovered that it was simple to re-identify people, and learn about their entire medical history without their consent, by comparing the dataset to other publicly available information, such as reports of celebrities having babies or athletes having surgeries.

The government pulled the data from its website, but not before it had been downloaded 1,500 times.

Click link above to read more

Microsoft calls for facial recognition technology rules given 'potential for abuse'

https://www.theguardian.com/technology/2018/jul/14/microsoft-facial-recognition-technology-rules-potential-for-abuse

Microsoft has called for facial recognition technology to be regulated by government, with for laws governing its acceptable uses.

In a blog post on the company's website on Friday, Microsoft president Brad Smith called for a congressional bipartisan "expert commission" to look into regulating the technology in the US.

"It seems especially important to pursue thoughtful government regulation of facial recognition technology, given its broad societal ramifications and potential for abuse," he wrote. "Without a thoughtful approach, public authorities may rely on flawed or biased technological approaches to decide who to track, investigate or even arrest for a crime."

Microsoft is the first big tech company to raise serious alarms about an increasingly sought-after technology for recognising a person's face from a photo or through a camera.

Click link above to read more

US Charges 12 Russian Intelligence Officers for Hacking DNC, Running DCLeaks

https://www.bleepingcomputer.com/news/government/us-charges-12-russian-intelligence-officers-for-hacking-dnc-running-dcleaks/

The US Department of Justice (DOJ) indicted today 12 Russian intelligence agents on hacking charges related to the 2016 US Presidential Election.

According to a copy of the indictment obtained by Bleeping Computer, the 12 accused are part of Unit 26165 and Unit 74455 of the Russian government's Main Intelligence Directorate (GRU), the country's military intelligence service.

Click link above to read more

Passwords for Tens of Thousands of Dahua Devices Cached in IoT Search Engine

https://www.bleepingcomputer.com/news/security/passwords-for-tens-of-thousands-of-dahua-devices-cached-in-iot-search-engine/

Login passwords for tens of thousands of Dahua devices have been cached inside search results returned by ZoomEye, a search engine for discovering Internet-connected devices (also called an IoT search engine).

Discovered by Ankit Anubhav, Principal Researcher at NewSky Security, a cyber-security company specialized in IoT security, these passwords are for Dahua DVRs running very old firmware that is vulnerable to a five-year-old vulnerability.

Click link above to read more

Hackers have breached the network at LabCorp - one of the largest diagnostic blood testing laboratories in the US

http://www.dailymail.co.uk/news/article-5959021/LabCorp-blood-testing-labs-hacked-sparking-fears-exposing-MILLIONS-patients-records.html

Hackers breached the network of one of the largest clinical laboratories in America sparking fears of a major cyber security breach, DailyMail.com can reveal.

According to a company insider senior managers were informed that the entire computer network of LabCorp, a Fortune 500 company, was shut down across the US Sunday morning after hackers tried to access the private medical records of millions of people.

The firm's tech experts are now working to bring the system back online after what a LabCorp spokesperson told DailyMail.com was 'suspicious activity'.

But while the firm insists there is 'no evidence' of 'unauthorized transfer or misuse of data', a company insider claims it could be weeks before LabCorp's experts discover the extent of the breach and whether or not the hackers were 'pulling data'.

Click link above to read more

Vermont schools lag on cybersecurity while risks hit home with $50K fraud from Pownal

https://www.burlingtonfreepress.com/story/news/local/vermont/2018/07/16/vermont-schools-lag-cybersecurity-while-risk-hits-pownal-fraud/774632002/

A cyber thief infiltrated a Vermont supervisory union's computer network and made a $50,000 transfer out of a school bank account, but safe guards on the account alerted staff members to take action.

"A more sophisticated thief or hacker could have spent the time to turn off alerts, make all bank emails go directly to the junk folder, and give the crime time to be effective," Phil Susmann, cyber security expert and president of Norwich University's Applied Research Institutes wrote about the stealthy attack.

Click link above to read more

Global Business Email Compromise Losses Hit $12.5 Billion

https://www.databreachtoday.com/fbi-global-business-email-compromise-losses-hit-125-billion-a-11206

The latest FBI data draws on fraud reports submitted by victims around the world from October 2013 to May 2018. In that time frame, the FBI counts 41,058 total U.S. victims who collectively lost at least $2.9 billion.

IC3 is the contact point for U.S. consumers and businesses that want to report fraud to authorities.

Business email compromise - also called email account compromise or CEO fraud - "is a sophisticated scam targeting both businesses and individuals performing wire transfer payments," IC3 warns. "The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds."

Click link above to read more

Timehop Reveals Additional Data Compromised by Hacker

https://www.databreachtoday.com/timehop-reveals-additional-data-compromised-by-hacker-a-11210

Timehop, the social media app that resurfaces older social media posts for entertainment, says its ongoing data breach investigation has revealed that attackers may have compromised more personal information than it previously suspected.

The New York-based company released a detailed breakdown of the number of users affected by varying combinations of lost data. As part of what it says is an effort to be fully transparent, it also described the entire schema of the database that was compromised.

The new classes of data that Timehop says were exposed include genders, birthdates, country codes and IP addresses.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

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
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca