Security News Digest
Information Security Branch

OCIO Office of the Chief Information Officer

July 30th, 2019

Try our July quiz – Summer Phishing

This week's stories:

- **Next in the Facebook-Cambridge Analytica scandal: Canadian privacy commissioners' report on AggregateIQ**
- **More than 90% of security decision-makers fail to keep tabs on workloads in the cloud**
- **Six million Canadians impacted by Capital One data breach**
- **Notorious MyDoom Worm Still on AutoPilot After 15 Years**
- **No More Ransom Success Story: Saves $108+ Million in Ransomware Payments**
- **Ransomware Attacks Prompt Louisiana to Declare State of Emergency**
- **Streaming Service Suffers 13-Day DDoS Siege by IoT Botnet**
- **US issues hacking security alert for small planes**
- **Judge Rules No Jail Time for WannaCry 'Killer' Marcus Hutchins, a.k.a. MalwareTech**

Next in the Facebook-Cambridge Analytica scandal: Canadian privacy commissioners' report on AggregateIQ

https://www.itworldcanada.com/article/next-in-the-facebook-cambridge-analytica-scandal-canadian-privacy-commissioners-report-on-aggregateiq/420288

Now that Facebook has agreed to pay a US$5 billion fine for its part in the Cambridge Analytica data collection and political advertising scandal, there is one more question to be answered: What role if any was played by a Canadian company called AggregateIQ Data Services?

The Victoria, B.C. public opinion polling and audience analysis firm is under investigation by the federal and B.C. privacy commissioners for possible violation of Canadian privacy law after news broke in 2018 that there was a local angle to the story.

Click link above to read more

More than 90% of security decision-makers fail to keep tabs on workloads in the cloud

https://www.itworldcanada.com/article/more-than-90-of-security-decision-makers-fail-to-keep-tabs-on-workloads-in-the-cloud/420387

Executives' desire to not miss out on a competitive advantage is leading to security professionals losing track of workloads on the cloud, according to a new study from Symantec Corp.

The report, which surveyed 1,250 security decision-makers across the globe, indicates that more than 53 per cent of computing workloads from enterprises have been moved to the cloud. That number is 48 per cent in Canada. The report's findings also said that an overwhelming 93 per cent of those surveyed reported that they had issues keeping tabs on all of their cloud workloads and only 27 per cent believed they were capable of addressing all cloud security threats.

Click link above to read more

Six million Canadians impacted by Capital One data breach

https://www.itworldcanada.com/article/six-million-canadians-impacted-by-capital-one-data-breach/420465

An alleged hacker who accessed the personal information of as many as 6 million Canadian Capital One credit applications has been arrested by the FBI, the bank said Monday.

Paige A. Thompson was charged with a single count of computer fraud and abuse in a U.S. District Court in Seattle. Thompson, who also goes by the handle "erratic", made an initial appearance in court and was ordered to remain in custody pending a detention hearing Thursday, according to media reports.

Click link above to read more

Notorious MyDoom Worm Still on AutoPilot After 15 Years

https://www.bleepingcomputer.com/news/security/notorious-mydoom-worm-still-on-autopilot-after-15-years/

The notorious Mydoom email worm, considered to be one of the most damaging malware strains ever developed, is still doing rounds on the Internet, working on autopilot and actively targeting email users all over the world.

Click link above to read more

No More Ransom Success Story: Saves $108+ Million in Ransomware Payments

https://www.bleepingcomputer.com/news/security/no-more-ransom-success-story-saves-108-million-in-ransomware-payments/

Today marks the third anniversary of No More Ransom and through its partners from the public and private sectors, law enforcement, academia, and researchers, the project has been able to help hundreds of thousands, if not millions, of victims get their encrypted files back for free.

Click link above to read more

Ransomware Attacks Prompt Louisiana to Declare State of Emergency

https://www.bleepingcomputer.com/news/security/ransomware-attacks-prompt-louisiana-to-declare-state-of-emergency/

Louisiana Governor John Edwards has declared a state of emergency after a wave of ransomware attacks targeted school districts this month. This Emergency Declaration will allow Louisiana state resources and cybersecurity experts to assist local governments in securing their networks.

Click link above to read more

Streaming Service Suffers 13-Day DDoS Siege by IoT Botnet

https://www.bleepingcomputer.com/news/security/streaming-service-suffers-13-day-ddos-siege-by-iot-botnet/

A botnet of over 400,000 IoT devices held a 13-day distributed denial-of-service (DDoS) siege against the streaming app of a company in the entertainment business.

Directed at the authentication component, the attack started around April 24 and hit with as many as 292,000 requests per second (RPS) at its peak, making it one of the largest Layer 7 DDoS strikes.

Click link above to read more

US issues hacking security alert for small planes

https://www.wagmtv.com/content/news/US-issues-hacking-security-alert-for-small-planes-513385231.html

The Department of Homeland Security issued a security alert Tuesday for small planes, warning that modern flight systems are vulnerable to hacking if someone manages to gain physical access to the aircraft.

An alert from the DHS critical infrastructure computer emergency response team recommends that plane owners ensure they restrict unauthorized physical access to their aircraft until the industry develops safeguards to address the issue, which was discovered by a Boston-based cybersecurity company and reported to the federal government.

Most airports have security in place to restrict unauthorized access and there is no evidence that anyone has exploited the vulnerability. But a DHS official told The Associated Press that the agency independently confirmed the security flaw with outside partners and a national research laboratory, and decided it was necessary to issue the warning.

Click link above to read more

Judge Rules No Jail Time for WannaCry 'Killer' Marcus Hutchins, a.k.a. MalwareTech

https://thehackernews.com/2019/07/marcus-hutchins-sentenced.html

Marcus Hutchins, better known as MalwareTech, has been sentenced to "time served" and one year of supervised release for developing and selling the Kronos banking malware.

Yes, Hutchins will not go to prison, United States District Judge J.P. Stadtmueller ruled today in Milwaukee County Court, after describing his good work as "too many positives on the other side of the ledger."

Click link above to read more

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