Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

March 19th, 2019

March is Fraud Awareness Month

This week's stories:

- **'Dirty John'-style romance scams cost Canadians millions, police say**
- **Cyberattacks against Canadian businesses on the rise: report**
- **Facebook probed over data-sharing deals with world's biggest tech firms**
- **Mirai Botnet Code Gets Exploit Refresh**
- **Study: Hacking 10 percent of self-driving cars would cause gridlock in NYC**
- **The Christchurch shooting shows how a far-right web culture is driving radicalisation**
- **Tesla allegedly spied on and ran smear campaign on a whistleblower**
- **Fujitsu wireless keyboard model vulnerable to keystroke injection attacks**
- **Why Phone Numbers Stink As Identity Proof**

'Dirty John'-style romance scams cost Canadians millions, police say

https://globalnews.ca/news/5071990/dirty-john-romance-scam/

One expert calls it a "Dirty John" scenario: An alleged scam artist who woos victims with romance and charm. Simon Sherry, a clinical psychologist and professor in the Department of Psychology and Neuroscience at Dalhousie University, says such scams are often pulled off by people with "a very dark constellation of traits."

"These individuals tend to be narcissistic, psychopathic, Machiavellian, and sadistic," he says. "Someone possessed by these traits can be very exploitative and parasitic, and that's usually part of a lifelong pattern where others are used in a callus and unemotional way."

Click link above to read more

Cyberattacks against Canadian businesses on the rise: report

https://www.nsnews.com/cyberattacks-against-canadian-businesses-on-the-rise-report-1.23662807

Cybersecurity remains an ongoing and growing problem for Canadian businesses, with an estimated 83 per cent of companies having experienced a cybersecurity breach of some kind in the past year, a new survey indicates.

In its first Canada Threat Report, Massachusetts-based cybersecurity firm Carbon Black said a January survey shows 76 per cent of companies reported an increase in cyberattacks in the past year, 25 per cent saying the volume has grown by half in that period.

Click link above to read more

Facebook probed over data-sharing deals with world's biggest tech firms

https://globalnews.ca/news/5054489/facebook-investigation-data-sharing-deals/

Facebook is the subject of a federal criminal investigation that's looking into its data-sharing deals with some of the biggest tech firms on the planet, The New York Times reported Wednesday. The social media giant acknowledged the report in a tweet, saying that it is already facing federal investigations.

The Times reported that a New York grand jury has subpoenaed records from at least two companies that make smartphones and other equipment. Each of these companies had struck agreements with Facebook that allowed them to access users' personal information. Those companies were not named in the story, but the Times noted that Facebook has data-sharing partnerships with companies including Microsoft, Apple, Sony and Amazon.

Click link above to read more

Mirai Botnet Code Gets Exploit Refresh

https://www.bankinfosecurity.com/mirai-botnet-code-gets-exploit-refresh-a-12197

Mirai, the powerful malware that unleashed unprecedented distributed denial-of-service attacks in 2016, has never gone away. And now a new version has been equipped with fresh exploits that suggest its operators want to harness the bandwidth offered by big businesses.

Palo Alto Networks says it found 11 new exploits in a Mirai variant along with unusual new combinations of default credentials that can be used to log into devices. Some of the new exploits target internet of things equipment likely to only be used by enterprises.

"These new features afford the botnet a large attack surface," writes Ruchna Nigam, a senior threat researcher with Palo Alto's Unit 42 research group. "In particular, targeting enterprise links also grants it access to larger bandwidth, ultimately resulting in greater firepower for the botnet for DDoS attacks."

Click link above to read more

Study: Hacking 10 percent of self-driving cars would cause gridlock in NYC

https://arstechnica.com/science/2019/03/study-hacking-10-percent-of-self-driving-cars-would-cause-gridlock-in-nyc/

Vehicles on the road will only have greater interconnectivity from this point forward, with self-driving cars on the horizon. That poses a unique potential risk: if someone can hack one car, what happens if they manage to hack many at once in a major metropolitan city?

That question inspired scientists at the Georgia Institute of Technology to quantify the likely impact of such a large-scale hack on traffic flow in New York City. Worst-case scenario: a small-scale hack affecting just ten percent of cars on the road would be sufficient to cause city-wide gridlock, essentially cutting half of Manhattan off from the rest of the city. And unlike compromised data, compromised vehicles can lead to physical injury.

Click link above to read more.

The Christchurch shooting shows how a far-right web culture is driving radicalisation

https://www.newstatesman.com/science-tech/internet/2019/03/christchurch-new-zealand-shooter-pewdiepie-youtube-facebook-video-shows-we-need-take-online-radicalisation

It's no longer a luxury to understand the niche language of online radicalisation, but a necessity to prevent future attacks.

If you're reading this, you probably know that one of the suspected Christchurch shooters uploaded a video of himself carrying out the attack that has injured 20 and killed 49. Live streamed on Facebook, the

video that has been taken down but subsequently reposted online alarmed viewers not just because it literally shows people being murdered but because of how the video begins.

Ultimately, there's one simple takeaway that doesn't require unpacking at all. And that is that white supremacist radicalisation is happening – flying under the radar, in many cases, thanks to internet-specific irony and memes. And if it's not addressed now, more people will probably die.

Click link above to read more

Tesla allegedly spied on and ran smear campaign on a whistleblower

https://www.scmagazine.com/home/security-news/a-former-security-manager-told-bloomberg-businessweek-that-tesla-hacked-spied-on-and-engaged-in-a-smear-campaign-against-whistleblower-martin-tripp/

A former security manager told Bloomberg Businessweek that Tesla hacked, spied on, and engaged in a smear campaign against whistleblower Martin Tripp.

Sean Gouthro, a former security manager at Tesla's Nevada Gigafactory, claimed Elon Musk personally hired Tesla investigators to hack into an employee's phone, spy on his messages, and even mislead police about a potential mass shooting, all in response to whistleblowing.

He also claims a Tesla investigator installed a device at the factory that monitored everyone's private communications.

Click link above to read more

Fujitsu wireless keyboard model vulnerable to keystroke injection attacks

https://www.zdnet.com/article/fujitsu-wireless-keyboard-model-vulnerable-to-keystroke-injection-attacks/

Fujitsu LX wireless keyboards are susceptible to keystroke injections, SySS GmbH, a German pen-testing firm revealed today.

The attacks allow a threat actor to beam wireless radio signals to the keyboard's receiver (USB dongle) and inject rogue keyboard presses on a user's computer.

Fujitsu was notified of the vulnerability but has not released any firmware patches.

Click link above to read more

Why Phone Numbers Stink As Identity Proof

https://krebsonsecurity.com/2019/03/why-phone-numbers-stink-as-identity-proof/

Phone numbers stink for security and authentication. They stink because most of us have so much invested in these digits that they've become de facto identities.

At the same time, when you lose control over a phone number — maybe it's hijacked by fraudsters, you got separated or divorced, or you were way late on your phone bill payments — whoever inherits that number can then be you in a lot of places online.

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

https:www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca