BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest

March 20, 2018

March is Fraud Awareness Month

Take our quiz and test your knowledge

This week's stories:

CEO of Vancouver-based firm charged in U.S. for providing tech to drug cartels

http://www.cbc.ca/news/canada/british-columbia/ceo-of-vancouver-based-firm-charged-in-u-s-for-providing-tech-to-drug-cartels-1.4578873

The chief executive of a Vancouver-based company appeared in a Washington state court on Thursday in the **first U.S. case in which a company has been targeted for providing criminal drug cartels with the technology to evade law enforcement**, the U.S. Justice Department said.

Phantom Secure CEO Vincent Ramos was indicted, along with four of his associates, on charges related to providing criminal organizations with cellular phones and encrypted networks to coordinate the shipment of illegal drugs around the world.

"Phantom Secure allegedly provided a service designed to allow criminals the world over to evade law enforcement to traffic drugs and commit acts of violent crime without detection," said FBI Director Christopher Wray in a statement.

It is the first time the U.S. government has targeted a company and its principals for providing criminals with the technology to evade law enforcement while committing transnational drug trafficking, the Department of Justice said.

Phantom Secure, which has a public website promoting its encrypted email and chat service plans, advertised its products as "impervious to decryption, wiretapping or legal third-party records requests," according to court documents.

Ramos, a B.C. resident, was arrested in Seattle last week and will face charges in San Diego. The four other defendants remain at large.

Ramos or a representative of Phantom Secure could not be reached for comment.

Canada's Privacy Commissioner Wants to Limit Data Collection in National Security Bill

https://betakit.com/canadas-privacy-commissioner-wants-to-limit-data-collection-in-national-security-bill/

Canada's Privacy Commissioner Daniel Therrien has once again written recommendations to the House's Standing Committee on Public Safety and National Security challenging the types of information that should be made accessible to Canadian intelligence agencies.

The Office of the Privacy Commissioner of Canada (OPC) released on March 5th, 2018 a series of recommendations for Bill C-59 (The National Security Act 2017) that the agency hopes will help lessen some of the potential privacy infringements in the bill.

In particular, Therrien's **recommendations related to "publicly available information" sought to add limits on when Canadian intelligence agencies can use information available in online public spaces — such as Facebook, Twitter and other social networks.**

According to the OPC, all measures taken regarding public information should be done with reason and in proportion to the circumstances.

"In this way, a dual threshold would apply to national security information sharing," said Therrien. The bill itself currently states that "published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise, or is available to the public on request by subscription or purchase."

The privacy commissioner worried that information won't always be obtained in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA) — the federal law that governs how organizations handle private information — potentially allowing the Communications Security Establishment (CSE) to use forms of invasive surveillance to gather intelligence on Canadians.

This means that even though Canadians may have information about themselves available online, it would be a privacy invasion for a government agency to compile data and use it on Canadians without cause or consent.

[The story continues online]

Canadian hardware used for hacking in Turkey and Syria, watchdog reports

https://www.ctvnews.ca/sci-tech/canadian-hardware-used-for-hacking-in-turkey-and-syria-watchdog-reports-1.3835872

A Canadian company's hardware is being used to hack internet users along Turkey's border with Syria, researchers said Friday, adding that there were signs that Kurdish forces aligned with the United States might have been targeted.

The revelation comes as Turkey presses its offensive against the Kurds dug in along the country's frontier with northwestern Syria -- a conflict that threatens to disrupt the American-led effort to extinguish the Islamic State group. The apparent use of Canadian technology to target a U.S. ally was an irony underlined by Ron Deibert, the director of the University of Toronto internet watchdog group Citizen Lab, which published a report on the spying.

"These companies are not closely regulated -- and that can lead to a lot of unintended consequences, including consequences that harm our foreign policy interests and human rights interest as well," said Deibert. "It's a strong argument for government control over this kind of technology."

In a statement issued before the report's release, Sandvine said it investigates all allegations of abuse, but said it had been unable to complete its inquiry because Citizen Lab refused to provide the company with its findings in full.

"Once we have the necessary data, we will conduct a full investigation and take appropriate action," Sandvine said.

The statement also said Citizen Lab's allegations were "technically inaccurate and intentionally misleading," but a representative for the company has yet to supply an example of a misleading or inaccurate claim.

Citizen Lab said it discovered the hacking after a European cybersecurity company reported that network service providers in two unidentified countries were trying to compromise their users using a powerful hacking technique known as network injection. Citizen Lab scoured the internet for signs of the spying and eventually traced the activity to the Turkish provinces of Adana, Hatay, Gaziantep, Diyarbakir and to the Turkish capital, Ankara, as well as parts of northern Syria and Egypt.

Network injection -- so-called because malicious software is injected into everyday internet traffic by whoever controls the network -- has long been feared as a particularly powerful form of government spying.

"This can potentially be used to target anyone in the country with the click of the button," said Bill Marczak, the lead author of the report.

[The story continues online]

Women push back against 'blockchain bros'

https://www.theglobeandmail.com/report-on-business/women-push-back-against-blockchainbros/article38246963/

Women are traditionally underrepresented in the technology sector, where only 5 per cent of companies have a woman as sole chief executive officer, and it is affecting company culture, potential investors and the balance sheet, according to the 2017 Where's the Dial Now? report.

The study, co-authored by PwC Canada, MaRS Discovery District and non-profit MoveTheDial, goes on to say that **53 per cent of tech companies have no female executives at all, and that "companies with greater gender diversity, particularly those that have women on their executive teams, C-suites and boards, perform better financially because of the variety of skills and approaches their people offer."**

The authors note that "while #movethedial is primarily focused on advancing gender diversity, **every single form of diversity and inclusion in this industry matters: accessibility, gender, LGBTQ, racial equality, etc. … By moving the dial for women, we aspire to move the dial for all people who are currently a minority in tech."**

One of the most potentially disruptive technologies set to likely have an impact on almost every area, from government to business contracts, to currency, is blockchain – an online, distributed ledger and the tool behind cryptocurrencies such as Bitcoin.

But, like other parts of the tech sector, women have low representation in developing this potentially game-changing technology. **Nevertheless, there is a slow pushback against the "blockchain bros" and the industry's lopsided gender gap to ensure this technology represents a more diverse population of both its developers and its users.**

[Read the rest of the article to meet some of the top women working with bockchain]

Over 40% of online login attempts are attackers trying to invade accounts

https://www.welivesecurity.com/2018/02/26/login-attempts-attackers-invade-accounts/

As many as 43% of online login attempts globally are made by bots that are used for evil ends, as attackers are increasingly leveraging the automated tools for credential abuse, a report by Akamai has revealed.

Focusing on data for November, 2017, the content delivery network provider found that 3.6 billion out of 8.3 billion login requests during that month were malicious, specifically "attempts to log in to an account using password guessing or account details gathered from elsewhere on the Internet".

A breakdown of the figures shows that the websites of retailers handled the highest number of login requests in November – 2.8 billion. **"Only" 36% of them were intended to break into the accounts,** according to Akamai's Fourth Quarter 2017 State of the Internet / Security Report.

Meanwhile, the hospitality industry had to contend with the highest concentration of bad bots**. A staggering 82% of nearly 1 billion login attempts on the websites of airlines, hotels and online travel agencies were found to be malicious.**

Swarms of villain bots also swooped on the sites of high-tech businesses, with 57% out of 1.4 billion login attempts deemed malevolent.

The data was obtained by Akamai's identifying "IP addresses that make multiple attempts to log into accounts using leaked credentials with no other activity to the target site".

The data set covers mainly websites that use email addresses as login names. As a result, Akamai cautioned that the figures may understate the extent of the problem in industries in which email addresses are not used as user IDs, notably the financial industry.

Bots that traverse the internet on behalf of their human operators can fulfill both legitimate and malicious automated tasks. Statistics indicate that bot-driven internet traffic, by helper and harmful bots combined, surpasses human traffic.

"Increased automation and data mining have caused a massive flood of bot traffic to impact websites and Internet services. Although most of that traffic is useful for Internet businesses, cybercriminals are looking to manipulate the powerful volume of bots for nefarious gains," Akamai's senior security advocate Martin McKeay is quoted as saying.

"Enterprises need to watch who is accessing their sites to differentiate actual humans from both legitimate and malicious bots. **Not all web traffic and not all bots are created equal,**" he added.

In an automated technique known as 'credential stuffing', criminals leverage stolen or leaked access credentials that belong to one account in order to break into other – often higher-value – accounts. This tactic has been found to pay dividends in anywhere between 0.1% and 2% of attempts, owing its success primarily to the fact that many netizens recycle their credentials across multiple accounts. Databases with reams of stolen username and password pairs can be easily bought online.

[The story continues online]

Google Moves to Ban Ads for Bitcoin, Cryptocurrency

https://www.infosecurity-magazine.com/news/google-moves-to-ban-ads-for/

Following a similar no-quarter approach taken by Facebook, **Google plans to ban crypto-related advertising starting in June.**

The ban includes ads for initial coin offerings (ICOs), wallets and trading advice, across any Google platforms. The prohibition will be far ranging: Google's ad engines place ads on not just its own sites but also on third-party outlets.

The concern is that virtual currency speculation has created a boom in the sector, yet the space largely lacks regulation and consumer protections. Cryptocurrencies like Bitcoin, Monero and others have also been the impetus for various fraud efforts and are at the heart of coin-mining, which has proven to be a lucrative new revenue stream for cybercriminals.

"We don't have a crystal ball to know where the future is going to go with cryptocurrencies, but we've seen enough consumer harm or potential for consumer harm," Scott Spencer, Google's director of sustainable ads, told CNBC.

The change is part of Google's update to its financial services-related ad policies. **The search engine, which makes 84% of its revenue from advertising, is no stranger to censoring ads: In a report, it said it took down more than 3.2 billion ads in 2017 for violating its policies. That's nearly double the 1.7 billion it removed in 2016.**

The ban follows Facebook's decision to prohibit ads that "promote financial products and services that are frequently associated with misleading or deceptive promotional practices, such as binary options, initial coin offerings and cryptocurrency."

Enforcement is ramping up across Facebook's platforms, including the main social media site, Audience Metrics and Instagram.

Google Moves to Ban Ads for Bitcoin, Cryptocurrency

https://www.infosecurity-magazine.com/news/google-moves-to-ban-ads-for/

Following a similar no-quarter approach taken by Facebook, **Google plans to ban crypto-related advertising starting in June.**

The ban includes ads for initial coin offerings (ICOs), wallets and trading advice, across any Google platforms. The prohibition will be far ranging: Google's ad engines place ads on not just its own sites but also on third-party outlets.

The concern is that virtual currency speculation has created a boom in the sector, yet the space largely lacks regulation and consumer protections. Cryptocurrencies like Bitcoin, Monero and others have also been the impetus for various fraud efforts and are at the heart of coin-mining, which has proven to be a lucrative new revenue stream for cybercriminals.

"We don't have a crystal ball to know where the future is going to go with cryptocurrencies, but we've seen enough consumer harm or potential for consumer harm," Scott Spencer, Google's director of sustainable ads, told CNBC.

The change is part of Google's update to its financial services-related ad policies. **The search engine, which makes 84% of its revenue from advertising, is no stranger to censoring ads: In a report, it said it took down more than 3.2 billion ads in 2017 for violating its policies. That's nearly double the 1.7 billion it removed in 2016.**

The ban follows Facebook's decision to prohibit ads that "promote financial products and services that are frequently associated with misleading or deceptive promotional practices, such as binary options, initial coin offerings and cryptocurrency."

Enforcement is ramping up across Facebook's platforms, including the main social media site, Audience Metrics and Instagram.

And Now this:

AI's dirty little secret: It's powered by people

https://www.ctvnews.ca/sci-tech/ai-s-dirty-little-secret-it-s-powered-by-people-1.3829235

There's a dirty little secret about artificial intelligence: It's powered by an army of real people.

From makeup artists in Venezuela to women in conservative parts of India**, people around the world are doing the digital equivalent of needlework --drawing boxes around cars in street photos, tagging images, and transcribing snatches of speech that computers can't quite make out.**

Such data feeds directly into "machine learning" algorithms that help self-driving cars wind through traffic and let Alexa figure out that you want the lights on. **Many such technologies wouldn't work without massive quantities of this human-labeled data.**

These repetitive tasks pay pennies apiece. But in bulk, this work can offer a decent wage in many parts of the world -- even in the U.S. This burgeoning but largely unseen cottage industry represents the foundation of a technology that could change humanity forever: AI that will drive us around, execute verbal commands without flaw, and, possibly, one day think on its own.

This human input industry has long been nurtured by search engines Google and Bing, who for more than a decade have used people to rate the accuracy of their results. Since 2005, Amazon's Mechanical Turk service, which matches freelance workers with temporary online jobs, has also made crowd-sourced data entry available to researchers worldwide.

More recently, investors have poured tens of millions of dollars into startups like Mighty AI and CrowdFlower, which are developing software that makes it easier to label photos and other data, even on smartphones.

Venture capitalist S. "Soma" Somasegar says he sees "billions of dollars of opportunity" in servicing the needs of machine learning algorithms. His firm, Madrona Venture Group, invested in Mighty AI. **Humans will be in the loop "for a long, long, long time to come," he says.**

Accurate labeling could make the difference between a self-driving car distinguishing between the sky and the side of a truck -- a distinction Tesla's Model S failed in the first known fatality involving self-driving systems in 2016.

"We're not building a system to play a game, we're building a system to save lives," says Mighty AI CEO Daryn Nakhuda.