Security News Digest

June 12th, 2018

June is IoT (Internet of Things) Month

Take our monthly quiz and test your knowledge

This week's stories:

China watching: Scary arms race for surveillance tech in China

https://www.news.com.au/technology/gadgets/china-watching-scary-arms-race-for-surveillance-tech-in-china/news-story/79a0163a92f7840ce13e55846f7222da

IT CAN crack your smartphone password in seconds, rip personal data from call and messaging apps, and peruse your contact book.

The Chinese-made XDH-CF-5600 scanner — or "mobile phone sleuth", as sales staff described it when touting its claimed features — was one of hundreds of surveillance gadgets on display at a recent police equipment fair in Beijing.

The China International Exhibition on Police Equipment is something of a one-stop shop for China's police forces looking to arm up with the latest in "black tech" — a term widely used to refer to cutting-edge surveillance gadgets. The fair underscores the extent to which China's security forces are using technology to monitor and punish behaviour that runs counter to the ruling Communist Party.

Click link above to read more

How to Wrestle Your Data From Data Brokers, Silicon Valley — and Cambridge Analytica

https://www.propublica.org/article/how-to-wrestle-your-data-from-data-brokers-silicon-valley-and-cambridge-analytica#143274

Making statistically informed guesses about Americans' political beliefs and pet issues is a common business these days, with dozens of firms selling data to candidates and issue groups about the purported leanings of individual American voters.

Few of these firms have to give your data. But Cambridge Analytica is required to do so by an obscure European rule.

How You Can Request Your Data From Cambridge Analytica:

1. Visit Cambridge Analytica's website here and fill out this web form.
2. After you submit the form, the page will immediately request that you email to data.compliance@cambridgeanalytica.org a photo ID and two copies of your utility bills or bank statements, to prove your identity. This page will also include the company's bank account details.
3. Find a way to send them 10 GBP. You can try wiring this from your bank, though it may cost you an additional $25 or so — or ask a friend in the UK to go to their bank and get a cashier's check. Your American bank probably won't let you write a GBP-denominated check. Two services I tried, Xoom and TransferWise, weren't able to do it.
4. Eventually, Cambridge Analytica will email you a small Excel spreadsheet of information and a letter. You might have to wait a few weeks. Celeste LeCompte, ProPublica's vice president of business development, requested her data on March 27 and still hasn't received it.

Click link above to read more

Toronto Police to embark on six-month pilot project for using body-scanners

https://www.thestar.com/news/gta/2018/05/31/toronto-police-look-at-six-month-pilot-project-for-using-body-scanners.html

The use of the technology will not eliminate the use of strip-searches entirely, the police added.

"Similar technology is used at airports, as well as correctional facilities, here in Ontario, British Columbia and Alberta," said Toronto Police spokesperson Meaghan Gray. A body scan can find any items on, or inside, a person.

"The Toronto Police Service believes there is technology available that allows us to modernize our current search processes, increase public trust and accountability, and reduce the intrusiveness of such searches," Gray said. "These are reasons alone to consider such a project."

The data would be stored for 30 days following the scan provided nothing is found, police say. If an item is located on the scan and criminal charges result, the images would be kept for court.

Click link above to read more

Why you should keep your car keys in a metal coffee can

https://www.seattletimes.com/business/why-you-should-keep-your-car-keys-in-a-metal-coffee-can/

"Really, some cyber experts don't go to sleep without putting their key into a metal container," said Moshe Shlisel, a veteran of the Israeli Air Force and now CEO of GuardKnox Cyber Technologies. "It's called a Faraday Cage. You block the electromagnetic field."

Copying code from vehicle key fobs is easy. Tech thieves can do it from outside your home or a motel. Then they can steal a vehicle or just gain access without owners realizing they've been violated.

Cybersecurity companies, including the team at GuardKnox, are working with the Detroit Three and automakers globally to create protections that deter hackers who covet new cars and the data stored in them.

Click link above to read more

Cracking 2 factor authentication & how to protect against it

https://www.darkreading.com/endpoint/cracking-2fa-how-its-done-and-how-to-stay-safe/d/d-id/1331835

Two-factor authentication is common but hackable. If you haven't implemented 2FA, there's a good chance you're in the process. It's a growing best practice, especially in the workplace where growing stores of sensitive data demand employees strengthen their login security.

But 2FA isn't a guaranteed shield against cyberattacks. It can be bypassed, as most recently demonstrated by KnowBe4 chief hacking officer Kevin Mitnick in a hack last week. Mitnick used a phishing attack to prompt users for their LinkedIn credentials. When they were entered into the fake login page, the attacker could access their username, password, and session cookie. When Mitnick plugged the target's session cookie into his browser, he didn't need the second-factor code to log into the LinkedIn account.

Click link above to read more

BlackBerry launches latest phone with appeal to the security-conscious

http://vancouversun.com/technology/personal-tech/blackberry-launches-latest-phone-with-appeal-to-the-security-conscious

While the KEY2 release includes a new camera and a tweaked QWERTY keyboard, it is clear that TCL is seeking to encourage business users, who once fuelled BlackBerry smartphones' success, by delivering improved security and privacy in an Android phone.

"Security has never been so relevant and so important as today," Alain Lejeune, president of BlackBerry Mobile and senior vice-president, TCL communication, said in introducing the KEY2, the flagship smartphone replacing the KEYone. "People realize suddenly their smartphone has become a very public space, their data widely massively shared without any protection, without any control.

"This is bringing new challenges to the industry."

The strategy comes as software and hardware manufacturers are under increasing scrutiny from regulators, and consumers are learning their data is often shared without their knowledge. Companies were forced to amend policies to meet Europe's new privacy law and Facebook has faced questions over its sharing of user data.

Click link above to read more

Facebook made some private posts public for as many as 14M

http://vancouversun.com/pmn/business-pmn/facebook-made-some-private-posts-public-for-as-many-as-14m/wcm/7d218096-36fb-47fd-8311-93d2094b02db

Facebook said Thursday that a software bug made some private posts public for as many as 14 million users over several days in May.

The problem, which Facebook said it has fixed, is the latest privacy scandal for the world's largest social media company.

It said the bug automatically suggested that users make new posts public, even if they had previously restricted posts to "friends only" or another private setting. If users did not notice the new default suggestion, they unwittingly sent their post to a broader audience than they had intended.

Erin Egan, Facebook's chief privacy officer, said the bug did not affect past posts. Facebook is notifying users who were affected and posted publicly during the time the bug was active, advising them to review their posts.

The news follows recent furor over Facebook's sharing of user data with device makers, including China's Huawei. The company is also still recovering from the Cambridge Analytica scandal, in which a Trump-affiliated data-mining firm got access to the personal data of as many as 87 million Facebook users.

Click link above to read more

---

74 Arrests in Business Email Compromise Takedown

https://www.databreachtoday.com/74-arrests-in-business-email-compromise-takedown-a-11070

A six-month coordinated global law enforcement effort to crack down on business email compromise schemes has resulted in 74 arrests, the U.S. Department of Justice announced Monday.

The effort, known as "Operation Wire Wire," led to the arrests of 42 suspects in the U.S., 29 in Nigeria and others in Canada, Mauritius and Poland, as well as the seizure of nearly $2.4 million. It also led to the "disruption and recovery" of about $14 million in fraudulent wire transfers, the Justice Department says in a statement.

Click link above to read more

Era of the eBay-Like Underground Markets Is Ending

https://www.databreachtoday.com/era-ebay-like-underground-markets-ending-a-11065

It probably wasn't a good idea anyway: Creating an underground online market with all the features of eBay, but offering a smorgasbord of fake IDs, drugs, malware and stolen credit card numbers.

The most famous market, Silk Road, was shuttered in 2013 after an off-duty IRS agent discovered an email address that led to its lead developer, Ross Ulbricht. Last year, AlphaBay was seized after a similar mistake by one of its developers, and Hansa fell after law enforcement manage to infiltrate the site.

Other underground markets, such as Dream Market and Olympus, are still around. But neither match the popularity of AlphaBay, says Digital Shadows, a threat intelligence company that studies cybercrime.

The company issued a new report earlier this week that notes that cybercriminal activity certainly isn't declining, but the era of the underground market may be passing. Instead, cybercriminals are doing deals using encrypted chat platforms.

Click link above to read more

Coinrail Cryptocurrency Exchange in South Korea Hacked

https://www.databreachtoday.com/coinrail-cryptocurrency-exchange-in-south-korea-hacked-a-11068

On Sunday, South Korean exchange Coinrail reported that it had suffered a hack attack early in the day, leading to the loss of 30 percent of all of the cryptocurrency tokens - or coins - that it was storing.

In a statement on the homepage of the Coinrail website, the company said that it has successfully recalled or frozen two-thirds of the stolen coins, thus holding out hope that many of the missing funds might be recovered.

The exchange says it's also moved all of the cryptocurrency that wasn't stolen to cold storage, which refers to cold wallets, or offline storage devices that get be plugged into a PC or server only when required, which makes them safer from hack attacks. Otherwise, cryptocurrency typically gets stored in hot wallets, referring to internet-connected repositories that enable exchanges and service providers to facilitate instant payments.

Coinrail is currently unavailable to users, with the website as of Monday continuing to resolve to a "system maintenance" page and statement about the hack attack and losses.

"The exact damage from the leaked coins/tokens is currently being confirmed, which may require some time," the exchange says in its statement, noting that police are investigating the incident and that the exchange is working closely with coin issuers to try and quickly recover stolen coins.

Click link above to read more

Congress Considers Ways to Beef Up Healthcare Cybersecurity

https://www.databreachtoday.com/congress-considers-ways-to-beef-up-healthcare-cybersecurity-a-11060

As part of efforts to bolster the nation's readiness to deal with health disasters and emergencies - natural and man-made - Congress is considering beefing up the focus on healthcare sector cybersecurity issues in legislation to reauthorize the Pandemic and All-Hazards Preparedness Act, which was enacted in 2006.

A Wednesday hearing of the House Energy and Commerce Committee's Subcommittee on Health focused on bipartisan draft legislation, the Pandemic and All-Hazards Preparedness Reauthorization Act of 2018 introduced by Rep. Susan Brooks R-Ind., and Rep. Anna Eshoo, D-Calif.

The legislation seeks to beef up the nation's ability to prepare for and respond to health threats from infectious diseases, bioterrorism, chemical attacks, radiological emergencies and cybersecurity incidents.

Click link above to read more

Canadian hacker sentenced to five years for major Yahoo security breach

https://www.canadiansecuritymag.com/news/data-security/canadian-hacker-sentenced-to-five-years-for-major-yahoo-security-breach

A Canadian young computer hacker who American investigators say unwittingly worked for Russian spies was sentenced to five years in prison Tuesday for his role in a massive security breach at Yahoo that U.S. federal agents say was directed by a Russian intelligence agency.

U.S. Judge Vince Chhabria also fined Karim Baratov $250,000 during a sentencing hearing in San Francisco.

Baratov, 23, pleaded guilty in November to nine felony hacking charges. He acknowledged in his plea agreement that he began hacking as a teen seven years ago and charged customers $100 per hack to access web-based emails. U.S. prosecutors allege he was "an international hacker for hire" who indiscriminately hacked for clients he did not know or vet, including dozens of jobs paid for by Russia's Federal Security Service.

Click link above to read more

Can airplanes be hacked? U.S. officials say it's 'only a matter of time'

https://globalnews.ca/news/4267715/airplane-hack-only-matter-of-time/

Virtually everything that's connected to the internet can be hacked

With that in mind, questions have been raised over the past few years regarding whether the increasing digitization of airline operations and flight controls puts in-flight aircrafts at risk of becoming the victims of cyber threats.

The U.S. Department of Homeland Security (DHS) reported in government documents, obtained by Motherboard, that it's "only a matter of time" before cyber criminals are able to hack and remotely control an airplane.

"Potential of catastrophic disaster is inherently greater in an airborne vehicle," a section of a recent presentation from the Pacific Northwest National Laboratory (PNNL), a Department of Energy government lab, reads.

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

****