Security News Digest

April 17, 2018

April is 'Digital Spring Cleaning' Month

Take our quiz and test your knowledge

On this day in history (April 17th)

2009 — Canada Citizenship Act amendments restore or award citizenship to thousands of so-called "lost Canadians."

This week's stories:

Teen charged after personal information exposed in Nova Scotia government website breach

http://www.cbc.ca/news/canada/nova-scotia/freedom-information-personal-website-breach-1.4614424

A 19-year-old Halifax man has been arrested after a breach of the Nova Scotia government's freedom-of-information website that included access to personal information.

More than 7,000 documents were accessed. About four per cent were determined to have "highly sensitive personal information," according to government officials. They said the number of Nova Scotians affected is "in the thousands."

"This is not great news," Internal Services Minister Patricia Arab said Wednesday.

Sensitive information accessed includes birth dates, social insurance numbers, addresses and government-services client information. Credit card information was not accessed during the breach, according to the government.

Nova Scotians need better notification of privacy breaches, report says

Halifax Regional Police said they searched a Halifax address Wednesday morning and took a suspect into custody over the breach. Supt. Jim Perrin said **the man faces a charge of unauthorized use of a computer.**

"It's a seldom-laid charge," Perrin said at Halifax police headquarters Wednesday afternoon.

Perrin said they seized items in the search, but did not provide details. Police don't expect to charge anyone else, but the arrested man could face more charges. The man was released on a promise to later appear in court.

While the breach happened between March 3 and 5, government officials said they only became aware of it last Thursday when **a government employee, doing research on the site, inadvertently entered incorrect information and was granted access to documents that should not have been publicly available. The government shut the site down the same day.**

Even once the government learned of the breach, it waited until Wednesday to begin notifying affected people. Arab said they held off notifying people was because police suggested it would help them in their investigation.

But Perrin told reporters police did not make that request. He could not say if advising people would have compromised the investigation. The province's protocols for a privacy breach state it is supposed to inform people as soon as possible, unless otherwise instructed by law enforcement.

The web portal was set up 15 months ago to handle access-to-information requests made under the province's Freedom of Information and Protection of Privacy Act.

Government officials said someone got in by "exploiting a vulnerability in the system." The person wrote a script allowing them to alter the website's URL, which then granted access to the personal information.

Internal Services found more than 7,000 PDF documents had been downloaded by a "non-authorized user" in early March. They filed a complaint with police on Saturday.

Arab was tight-lipped earlier this week, refusing to answer questions from opposition politicians and reporters on Tuesday.

On Wednesday, she and Deputy Minister Jeff Conrad gave a fuller account to journalists. Arab said if the matter hadn't been raised by opposition members and reporters on Tuesday, Wednesday's information update still would have happened.

"We wanted the person responsible for this to not know that we knew that this had happened," Arab told reporters. "We needed to let Halifax Regional Police do their job and couldn't compromise the nature of their investigation."

The government said people's payment information was safe because it is managed by a different system. Officials are notifying affected people as of Wednesday.

[Read the rest of the article online to learn more]

Canadians' Trust In Social Media Dips Lower Than 'Traditionally Detested' Industries

https://www.huffingtonpost.ca/2018/04/10/canadians-trust-in-facebook_a_23407913/

We're still using it, but Canadians are losing faith in Facebook.

According to annual trust research done by Proof Inc. (formerly Environics), Canadians' trust in Facebook has taken a dive. **Just 34 per cent of Canadians now say they trust the platform, a 17-point drop from 51 per cent in 2017.**

Trust in social media overall has fallen to 22 per cent. By contrast, "traditionally detested" industries like telecoms and insurance companies sat at 30 per cent.

Proof Inc. executive vice-president Josh Cobden told HuffPost Canada that Facebook had one of the largest drops in trust of any company in their study, second only to Bombardier, which fell by 20 percentage points.

Despite the drop, the majority of Canadians— a whopping 84 per cent— still say they are actively using Facebook, a fact that Cobden called the social media network's "saving grace."

Cobden said Facebook continues to deliver a product that is reliable, which is the number-one source of trust.

"While we may have grave concerns about how Facebook behaves as an organization, we still use it, because it delivers the things we expect of it," Cobden said.

"But it's the stuff that we don't expect, and that's sort of the use of our data that is pulling them down in terms of reputation."

Cobden noted the Proof survey was carried out from Jan. 18 to Feb. 5 of this year, Facebook's drop in trust among Canadians is a result of research completed from Jan. 18 to Feb. 5, after news broke of Russian interference in the U.S. presidential election but before the Cambridge Analytica scandal.

"I think people have been worried about Facebook user privacy for as long as there's been a Facebook," he said.

"If we did the survey today, it might be even lower."

Canadians aren't big on artificial intelligence, either. **Just over a third of Canadians — 38 per cent — trust AI to contribute positively to the Canadian economy, and only 37 per cent trust it to improve their consumer experience.**

However, three in 10 Canadians are on the fence, saying they neither trust nor distrust AI.

Cobden said that as the neutral group comes to better understand AI, there will be more trust in it. Because AI is a relatively new industry, businesses have an opportunity to market themselves better and "to win the trust of Canadians," compared to traditional industries like telecommunications.

"We know more about them and familiarity tends to breed trust," Cobden said.

"For example, the reason that Google search works so well is because of AI. And that's just an everyday interaction that almost all of us have — in many cases — many times a day."

"But do people understand that it's AI in the algorithm that's making the search work so effectively— at least with Google— maybe not."

The Internet has serious health problems, Mozilla Foundation report finds

https://arstechnica.com/information-technology/2018/04/mozilla-foundation-report-details-decline-in-health-of-internet/

As Facebook CEO Mark Zuckerberg prepared to face nearly half of the Senate today to explain what went wrong with his company's handling of personal data for millions of Facebook users, the **Mozilla Foundation released a report that highlights the dangers posed to the entirety of the Internet ecosystem by the increasing concentration of control over how people experience the online world in the hands of companies like his.**

Zuckerberg opened his remarks today by saying, "Facebook is an idealistic and optimistic company" and that he and others believed that the tools Facebook created were a force for good. "It's clear now that we didn't do enough to prevent those tools from being used for harm as well," he admitted. The danger that Facebook executives overlooked, however, is described clearly by the Mozilla Foundation report.

Mozilla Foundation Executive Director Mark Surman explained the harm done by Facebook's platform clearly in a blog post today, describing the process of creating the 2018 Internet Health Report. As he and foundation fellows were discussing how to examine the topic of "fake news," he wrote, "I sketched out a list on a napkin to help order our thoughts:"

What the napkin said:

- Collecting all our data
- precision targeted ads
- bots and fake accounts
- FB dominates news distribution
- not enough Web literacy
- fuel for fraud and abuse,
- and very bad real world outcomes

The Internet Health Report, which evolved from a prototype launched in January of 2017, is not a medical chart for the Internet packed with metrics. Edited by Solana Larsen and written by Mozilla Foundation research fellows**, the report is an evaluation of "what's helping and what's hurting the Internet," and it focuses on five broad areas of concern—personal privacy and security, decentralization, openness, "digital inclusion," and general Web literacy.** And Facebook's part in the health of the Internet is writ large across the report.

Of particular concern were three issues:

- **Consolidation of power over the Internet**, particularly by Facebook, Google, Tencent, and Amazon.
- **The spread of "fake news,"** which the report attributes in part to the "broken online advertising economy" that provides financial incentive for fraud, misinformation, and abuse.
- **The threat to privacy posed by the poor security of the Internet of Things.**

The foundation's report isn't all bad news—it highlights progress in affordable access and the adoption of cryptography. But the cautionary notes outweigh the optimistic ones, especially on the topic of consolidation of control over Internet content and collection of personal data. **While the data collected and transformed into intelligence by the big social media and e-commerce vendors is vast, the Mozilla Foundation report warns, "The network control of major Internet services is only part of the grip they hold on our lives. Through sheer size and diverse holdings, a few companies including Google, Facebook, and Amazon—or if you live in China, Baidu, Tencent and Alibaba—have become intertwined not only with our daily lives, but with all aspects of the global economy, civic discourse, and democracy itself... they are too big. Through monopolistic business practices that are specific to the digital age, they undermine privacy, openness, and competition on the Web."**

That impact extends into the realm of "fake news," as the report points out, because "most people are getting at least some of their news from social media now." **This enabled the Russia-based Internet Research Agency's efforts to distort reality by creating dozens of 'fake' Facebook pages, including "BlackMattersUS" and "Heart of Texas," as the report cites—using the language of US political movements to attract followers and spread misinformation—as well as organizing actual protests, "and once even a protest and a counter protest at the same time," the report notes.**

At the same time, thousands of "fake news" stories were created entirely to generate revenue from advertising—many of them created by people in one town in Macedonia. Social media platforms allowed these fraudulent articles to generate hundreds of thousands of dollars in revenue for their creators.

Social media sites are a natural platform for this sort of deception and fraud, because it's where the eyeballs are. The reach of social media companies has continued to expand, as the report shows in this chart of monthly active users, in millions, for each social media platform. During 2017, Facebook managed to expand its monthly active user base from 1.87 billion to 2.17 billion, while expanding its reach into users' lives as millions more adopted Facebook's Messenger application and WhatsApp (each of which now has approximately 1.3 billion monthly active users).

The precision with which these platforms can be used to target particular types of users and to effectively distort their perception of the world around them makes the dominance of the Internet by Facebook and others even more dangerous, the researchers asserted.

The emerging Internet of Things poses its own sort of danger to the privacy and security of individuals. With 30 billion Internet-connected devices expected by 2020, the report's authors expressed concern about both the privacy impact of those devices and the threat posed by malware like the Mirai botnet that struck the Internet last year. The report warns that "the risk of all these insecure 'things' still exists, and the scale grows bigger with every new connected device."

82% of cyber pros worry employees don't follow cloud security policies

https://www.techrepublic.com/article/82-of-cyber-pros-worry-employees-dont-follow-cloud-security-policies/

90% of firms say at least half of their cloud data is sensitive information. — Oracle and KPMG, 2018

38% of cybersecurity and IT professionals report issues detecting and responding to cloud security incidents. — Oracle and KPMG, 2018

The shift to the cloud is becoming a business imperative for the majority of companies, as 87% of public and private organizations now have cloud-first initiatives in place, according to a Thursday report from Oracle and KPMG. While the cloud offers benefits such as cost savings and the ability to move faster on certain projects, it also creates an increasingly complex threat landscape for organizations to navigate, the report noted.

Of the 450 cybersecurity and IT professionals worldwide surveyed in the report, the vast majority—**90%—said that at least half of their cloud data is sensitive information. Keeping this information secure is tantamount, and 41% of organizations said they now have a dedicated cloud security architect on staff.**

The rise of the cloud has also created more security challenges due to shadow IT, the report found. While **97% of organizations surveyed said they require cloud services to be approved by the IT/security team, 82% expressed concern that employees and teams were violating those policies.**

When security incidents do arise, they have a major impact on businesses: 66% of companies said they had suffered a significant business operations interruption in the past two years, according to the report.

The rise in cyber threats and a lack of qualified security professionals has led 47% of organizations to use machine learning for cybersecurity purposes, the report found. Some 84% of companies said they are committed to increasing levels of security automation as well.

Outside of tools, a security approach that focuses on people and processes tends to deliver the best results, the report found**. When asked what actions had the most positive impact on improving an organization's security posture, the majority of respondents (31%) said increasing employee awareness and training programs. Other top actions were increasing security budgets (29%) and training security teams on new threat types and best practices (29%).**

Cryptocurrency-mining malware: Why it is such a menace and where it's going next

https://www.zdnet.com/article/cryptocurrency-mining-malware-why-it-is-such-a-menace-and-where-its-going-next/

Cyber-crooks are always looking for new means of making money and, for much of the last two years, **ransomware was the cyber-attack of choice for those looking to quickly make money.**

Recently, however, attackers have been leaving ransomware behind and are increasingly embracing a new form of making money from the internet: cryptocurrency mining.

Like many others, cybercriminals have recognised the potential riches that could await using the processing power of computers to mine for cryptocurrencies such as bitcoin and Monero, especially following the bitcoin boom of late last year.

However, rather than spending money on specialist systems to legitimately mine cryptocurrency, criminals are turning to cryptojacking malware to do the work for them.

The idea is simple: **unwitting victims have their computer or smartphone infected with malware, which uses the CPU power of the device to mine currency, with the profits being directed back into the wallet of the attacker.**

Aside from heavy use of the PC fan and driving up the energy cost of using the computer, cryptojacking doesn't make itself obvious, if it's not pushed too far, as the average victim isn't likely to worry too much their computer being a bit noisier than usual.

"Criminals act like a business. They'll have a business model for making as much money as they can with as little risk as possible -- and cryptocurrency mining represents a good return on investment and a low risk way of doing it," Mike McLellan, senior security researcher at the SecureWorks Counter Threat Unit, told ZDNet.

That cryptojacking doesn't require interaction with victims the way ransomware does offers a number of benefits to the crooks: it leaves the user unaware their machine is infected with malware, meaning rather than providing payment in one quick hit like ransomware, the operation can be sustained for a long period of time.

It also doesn't matter where in the world the victim is, allowing attackers to profit from virtually anyone -- opening additional markets of potential targets and fuelling the move towards cryptojacking.

"With a ransomware infection you might get a big pay off, but if you infect a computer in Africa, it's very unlikely you're actually going to get a payout from that. In areas of the world where people are less likely to pay ransoms, you might have just ignored those even though they're ripe for infection," Ryan Olson, intelligence director of Unit 42 at Palo Alto Networks, told ZDNet.

"But with cryptocurrency mining, it's completely egalitarian: different systems perform differently at how they mine cryptocurrency, but they can all do it, so they're all equal targets. That's an important element of why we're seeing this transition."

Cryptojacking is also increasingly attractive to attackers as, not only does it funnel funds directly into the wallets of attackers without the need to interact with the victims, but **the anonymous nature of cryptocurrency means that, unlike some other forms of cybercrime, there's no need for elaborate systems to hide or launder the profits.**

"Even when you think of the ease of stealing banking credentials, when you're dealing with regulated currencies, there are a lot of frameworks you have to work around to get it back into their pockets without it being easily traceable," Randi Eitzman, senior cyber security analyst at FireEye, told ZDNet.

"Cryptocurrencies offer that advantage to criminals. They don't have to have the system of money mules to launder the currencies. It's just running code of a remote machine and collecting profits," she added.

While the initial profits from cryptocurrency mining aren't as immediate as ransomware or selling stolen credentials, some of those who've focused heavily on this space have made millions of dollars in the last year alone.

The code behind cryptojacking malware is relatively simple and it can be delivered via phishing campaigns, malvertising, compromised websites, or even software downloads. Once on a system, the game is all about not getting caught.

While some attackers have been known to brazenly spin up CPUs to one hundred percent capacity, those campaigns don't last long because they can cause irreversible damage to the device -- and a broken system doesn't provide any benefit to malicious miners.

It's why those with serious networks of hijacked machines are tailoring instructions to systems: they spin up the CPU to such an extent that over time they can provide a decent profit, but do so while not running at such high capacity that the operation is uncovered.

"It's a numbers game: infect as many computers as you can, then keep them infected. You might think just make it 100 percent all of the time and that's what a lot of attackers do, because they think they'll earn the most money that way," said Olson.

"But if you use 100 percent of the CPU, the user is more likely to notice it's slow and make choices which lose you the mining device. There's choices attackers need to make the most money over time -- they've got to think about the most bang for their buck."

[Read the rest of the article online to learn more]

How Android Phones Hide Missed Security Updates From You

https://www.wired.com/story/android-phones-hide-missed-security-updates-from-you/

GOOGLE HAS LONG struggled with how best to get dozens of Android smartphone manufacturers—and hundreds of carriers—to regularly push out security-focused software updates**. But when one German security firm looked under the hood of hundreds of Android phones, it found a troubling new wrinkle: Not only do many Android phone vendors fail to make patches available to their users, or delay their release for months; they sometimes also tell users their phone's firmware is fully up to date, even while they've secretly skipped patches.**

On Friday at the Hack in the Box security conference in Amsterdam, researchers Karsten Nohl and Jakob Lell of the firm Security Research Labs plan to present the results of two years of reverse-engineering hundreds of Android phones' operating system code, painstakingly checking if each device actually contained the security patches indicated in its settings**. They found what they call a "patch gap": In many cases, certain vendors' phones would tell users that they had all of Android's security patches up to a certain date, while in reality missing as many as a dozen patches from that period—leaving phones vulnerable to a broad collection of known hacking techniques.**

"We find that there's a gap between patching claims and the actual patches installed on a device. It's small for some devices and pretty significant for others," says Nohl, a well-known security researcher and SRL's founder. In the worst cases, Nohl says, Android phone manufacturers intentionally

misrepresented when the device had last been patched. **"Sometimes these guys just change the date without installing any patches. Probably for marketing reasons, they just set the patch level to almost an arbitrary date, whatever looks best."**

SRL tested the firmware of 1,200 phones, from more than a dozen phone manufacturers, for every Android patch released in 2017. The devices were made by Google itself as well as major Android phone makers like Samsung, Motorola, and HTC, and lesser-known Chinese-owned companies like ZTE and TCL. **Their testing found that other than Google's own flagship phones like the Pixel and Pixel 2, even top-tier phone vendors sometimes claimed to have patches installed that they actually lacked. And the lower-tier collection of manufacturers had a far messier record.**

The problem, Nohl points out, is worse than vendors merely neglecting to patch older devices, a common phenomenon. Instead, it's that they tell users they install patches that they in fact don't, creating a false sense of security**. "We found several vendors that didn't install a single patch but changed the patch date forward by several months," Nohl says. "That's deliberate deception, and it's not very common."**

More often, Nohl believes, companies like Sony or Samsung would miss a patch or two by accident. But in other cases, the results were harder to explain: **SRL found that one Samsung phone, the 2016 J5, was perfectly honest about telling the user which patches it had installed and which it still lacked, while Samsung's 2016 J3 claimed to have every Android patch issued in 2017 but lacked 12 of them—two considered as "critical" for the phone's security.**

[Read the rest of the article online to learn more]

Majority of divisive Facebook ads bought by "suspicious groups" – study

https://www.reuters.com/article/us-facebook-ads/majority-of-divisive-facebook-ads-bought-by-suspicious-groups-study-idUSKBN1HN2KV

Most of the political ads about divisive issues that ran on Facebook Inc before the 2016 U.S. presidential election were sponsored by "suspicious groups" with no publicly available information about them, according to a study released on Monday and based on a database of five million ads on Facebook.

One in six of those groups was linked to Russia, according to a University of Wisconsin-Madison study here, and the identities of the rest of the 122 groups that are labeled "suspicious" are still unknown, an indication of the influence of "astroturf" or shell companies in U.S. politics.

Over a quarter of the suspicious ads mentioned Donald Trump or Hillary Clinton, two of the presidential candidates in the election, and 9 percent expressly advocated for or against individual candidates.

Most other ads deliberately avoided mentioning candidate names while still getting the message out by doing things like supporting policies pushed by candidates, Young Mie Kim, the lead researcher said.

The researchers labeled suspicious ad-buyers as groups with pages that have been inactive, inaccessible, removed or banned by Facebook since the election and there was no information available publicly about them.

Project DATA, the research team, also found that voters were also disproportionately targeted in swing states like Wisconsin and Pennsylvania with ads that focused on issues like guns, immigration and race relations.

Facebook Chief Executive Officer Mark Zuckerberg has announced a crackdown on who buys ads about divisive issues, saying this month that **the company would require every such advertiser to confirm their identity and location.**

And Now this:

This Quantum Random Number Generator Can Never Be Hacked

https://www.livescience.com/62271-random-numbers-quantum-mechanics.html

Lotteries, accidents and rolls of dice — the world around us is full of unpredictable events. Yet generating a truly random series of numbers for encryption has remained a surprisingly difficult task.

Now, researchers have used a mind-bending experiment relying on both Albert Einstein's theory of relativity and quantum mechanics, which describes the probabilistic nature of subatomic particles, to produce strings of numbers that are guaranteed to be random.

"If you sent in some team of people to examine our experimental components as closely as they wanted and then have them try to come up with a prediction for what these random numbers would be afterwards, there's just no way they could predict them," study co-author and mathematician Peter Bierhorst of the National Institute of Standards and Technology (NIST) in Boulder, Colorado, told Live Science.

Computers everywhere use random numbers as keys to lock or unlock encrypted information. Many processes for producing these keys — such as the random number generator that's probably on your computer right now — use an algorithm that spits out a seemingly arbitrary string of numbers. Other approaches try to make use of real-world randomness, for instance measuring the length of time between keystrokes or the fluctuating temperature of a computer server, to produce random numbers.

But such methods are still susceptible to attack. Savvy hackers can either tamper with a random number generator or learn its underlying principles to figure out what numbers it's going to produce. In 2012, security researchers found that tens of thousands of internet servers were vulnerable to hacking because of their reliance on poor-quality random number generators.

[Read the rest of the article online to learn more]