Security News Digest
November 07, 2017
(sent Nov 8th)

Take the November Defensible Security Quiz to learn about this comprehensive cyber security model.

IBM Wants British Columbia to Track Legal Pot With Blockchain Tech

https://motherboard.vice.com/en_us/article/8x5vvp/ibm-british-columbia-canada-track-legal-cannabis-with-blockchain

Canada is gearing up for the legalization of weed next year, and the provinces are scrambling to figure out how they're going to manage and sell all that bud. Tech giant IBM recently pitched one possible high-tech solution to the British Columbia government: the blockchain. Blockchain technology, which is behind cryptocurrencies like Bitcoin and Ethereum, can help the BC government to stamp out the black market, the IBM document states.

IBM is heavily invested in the blockchain space, and offers a commercial platform to developers and companies that want to experiment with the technology. **Blockchains are public ledgers that record every action occurring within the network. This ledger is distributed across many computers, meaning that it's nigh-impossible to forge an entry without anybody else noticing**. For cryptocurrencies like Bitcoin, the blockchain keeps track of who owns what units of currency going all the way back to when the system was first switched on in early 2009.

Now, IBM Canada wants the BC government to use blockchain technology to keep track of weed as it goes from the manufacturer to some hoser's bong [really?? hoser's bong??]. Or, as the company put it in **a document hosted on the BC government's website** and marked November 1, "from seed to sale."

The document was submitted as part of the BC government's recent public consultation on how to manage legal pot in the province, which ran from late September to November 1. "Our submission was in response to a government request," an IBM spokesperson told Motherboard in an email. "IBM expertise is used to help guide federal and provincial government clients on best-practices, planning and execution upon request."

The idea of tracking pot with the blockchain isn't a new one. US company Medical Genomics already offers a service for growers to have their bespoke strains genetically sequenced and marked for posterity on the Bitcoin blockchain. [see article for more info on the IBM proposal]

Police Warn Parents About Anonymous Commenting App Sarahah

https://globalnews.ca/news/3842520/police-warn-parents-about-anonymous-commenting-app-sarahah/

While reading messages he received on the anonymous app Sarahah, YouTuber Lonnie Randall notes "it's kind of like an ego-destroying hate machine." The Canadian Centre for Child Protection and police departments across several U.S. states and in New Zealand are warning parents about Sarahah, an app that lets users send messages to each other anonymously.

Sue Scheff, a cyber-safety expert and author based in Florida, said the anonymity feature is what can enable online harassment among children and teenagers. "They're able to speak without looking at people face-to-face, which makes it easier for them to judge and criticize without having to see the reaction," Scheff told Global News. Sarahah, which means "frankness" or "honesty" in Arabic, was developed in Saudi Arabia. **It's been available for download in Canada since the spring. Since then, the app has soared in popularity, with hundreds of millions of users worldwide**.

Sarahah CEO Zain al-Abdin Tawfiq initially created the app for use in a workplace setting. On its website, Sarahaha is described as a tool for users to discover their strengths and weaknesses by "receiving honest feedback from employees and friends in a private manner." In practice, however, **Sarahah has been gaining traction among youth. Although the app store says users must be at least 17 years old, many are younger and therefore more vulnerable to bullying**. Scheff, who was cyberbullied as an adult, said vicious comments can emotionally devastate the victim. "Words hurt. It's just that simple," she said. **She counsels parents to have an ongoing conversation with their children about their**

cyber life. **"There's always going to be an app," Scheff said. "It's not the app — it's our social behaviour. It's our parenting."** Cracking down on cyberbullying in anonymous messaging apps is no easy feat, but leaving users to comment freely without constraints can end up backfiring.
……. Global News reached out to Sarahah for comment, but Tawfiq declined an interview. He told the BBC in August that Sarahah does have "features such as blocking and filtering and many other techniques" in place to prevent online harassment. Sarahah has already received several complaints about cyberbullying from users on Twitter and Facebook, but experts point out the issue of online harassment is not limited to any one channel or platform. Scheff said there will always be another new app where cyberbullying can emerge. Instead of targeting specific apps, she encourages parents to focus on changing their children's social-media behaviour. "Empathy and kindness starts offline, and we need to bring it online," Scheff said.

More Than 3,000 Canadian Names in the Paradise Papers

http://www.cbc.ca/news/business/paradise-papers-canada-connection-1.4386126

A supermarket giant, an NHL hockey team, several billionaires and a yacht captain. These are just a few of the roughly 3,300 Canadian companies, trusts, foundations and individuals whose names appear in the Paradise Papers, a leak of millions of records from offshore law firm Appleby and the corporate registries of 19 tax havens. The leak, revealed Sunday by CBC/Radio Canada and the Toronto Star, in partnership with the International Consortium of Investigative Journalists (ICIJ), is the largest ever involving Canadians who keep money in tax havens. It contains more than five times more Canadian companies and individuals than the 625 found in last year's Panama Papers leak. The records also show that Canada is one of Appleby's biggest markets for offshore financial services clients, behind the U.S., the U.K. and China.

Leaked data from the law firm shines a light on hundreds of well-known companies and wealthy Canadians who benefit from offshore trusts and corporations set up in countries where they pay little or no taxes, as a way to legally avoid - or potentially evade - paying taxes at home. The Paradise Papers name hundreds of Canadian contacts working as accountants, attorneys or consultants for clients of Appleby. Also named are companies, individuals and 306 organizers and beneficiaries of trust funds incorporated in Bermuda or the Cayman Islands. When news of the leak broke Sunday, John Power, a spokesperson for the minister of national revenue, said "the CRA [Canada Revenue Agency] is reviewing links to Canadian entities and will take appropriate action." [article lists some Canadian clients]

…. Dennis Howlett of Canadians For Tax Fairness says the leak reveals a bigger problem that goes beyond wealthy individuals. "It's big corporations taking advantage of subsidiaries in tax havens to shift their profits and pay a lot lower taxes," he said. Howlett said the Canadian government facilitates this practice by signing tax agreements with tax havens. "This is legal, and it should not be legal. That's the point."

Appleby repeatedly targeted Canada between 2011 and 2013 to look for new clients, especially in the mining industry. The firm's strategy included networking trips to Vancouver, Calgary and the annual convention of the Prospectors & Developers Association of Canada in Toronto. Records suggest all the wining and dining - at Toronto's Ritz-Carlton, the Fairmont Royal York and top-ranked restaurant Canoe - may have paid off, as the firm secured 127 new Canadian accounts in 2012 alone. The Paradise Papers reveal Appleby's clients in 2014 included at least 17 Canada-based resource companies. Appleby billed Canadian clients and law firms at least $12 million between 2009 and 2013, including $8.2 million through its Bermuda office. As last year's Panama Papers investigation revealed, Canada is fast becoming a tax haven because of the combination of its sterling reputation and registry rules that allow the true owners of companies to hide their identities.

'We're Designing Minds': Industry Insider Reveals Secrets of Addictive App Trade

http://www.cbc.ca/news/technology/marketplace-phones-1.4384876

The average Canadian teenager is on track to spend nearly a decade of their life staring at a smartphone, and that's no accident, according to an industry insider who shared some time-sucking secrets of the app design trade. CBC *Marketplace* travelled to **Dopamine Labs, a startup in Venice, Calif., that uses artificial intelligence and neuroscience to help companies hook people with their apps**. **Named after the brain molecule that gives us pleasure, Dopamine Labs uses computer coding to influence behaviour - most importantly, to compel people to spend more time with an app and to keep coming back for more**. Co-founder Ramsay Brown, who studied neuroscience at the

University of Southern California, says it's all built into the design. "We're really living in this new era that we're not just designing software anymore, we're designing minds."
Brown is one of the few industry insiders who would talk. *Marketplace* contacted social media giants Facebook, Instagram and Snapchat. None would go on the record to discuss their design techniques.
Brown says he hopes by speaking to CBC, Canadians will be more informed about how they're being manipulated to spend so much time using apps
Habit-forming rewards. One of the most popular techniques, he says, is called **variable reinforcement or variable rewards. It involves three steps: a trigger, an action and a reward.** A push notification, such as a message that someone has commented on your Facebook photo, is a trigger; opening the app is the action; and the reward could be a "like" or a "share" of a message you posted. These rewards trigger the release of dopamine in the brain, making the user feel happy, possibly even euphoric, Brown says. "Just by controlling when and how you give people that little burst of dopamine, you can get them to go from using [the app] a couple times a week to using it dozens of times a week."
The rewards aren't predictable. We don't always get a like, a retweet or a share every time we check our phones. And that's what makes it compulsive, Brown says. **Plus, he says, app developers use artificial intelligence, which is essentially decision-making code, to predict the best time to make the payouts based on the user data they collect.**
Snapchat has several features that motivate users to keep checking in. For instance, **the Snapchat score - a tally based on the photo messages a user sends and receives - is essentially a reward for being active on Snapchat. Teenagers can have scores into the millions.** Emily, a 16-year-old from Guelph, Ont., who agreed to track her smartphone use for *Marketplace* this past summer using an app called Moment, has a Snapchat score of 1.2 million - several hundred thousand points ahead of her friends. She calls Snapchat "addictive."
Snapchat's streak feature is another reason why. It displays the number of days in a row a user snaps, or messages, a particular friend. The message could be as meaningless as a picture of a foot, yet the user feels they have an obligation to send it. "Especially if [the streak is] over a year, then it's really intense and you have to," says Emily, whose last name wasn't published for privacy reasons. **The streak feature is a technique known as a loss aversion, which often involves trying to keep users fixated on an app even when it's not useful or they don't enjoy it anymore.**
…. Lisa Pont, a social worker at the Centre for Addiction and Mental Health (CAMH) in Toronto, helps teens and parents to manage their technology use in healthier ways. While it's early days to know the full health impact, Pont says **research is starting to show heavy technology use affects our overall well-being, including memory, concentration, moods, sleep, anxiety and depression**. A recent study from CAMH shows Ontario teens' use of smartphones is on the rise, with 16 per cent spending five hours or more on social media per day. Many of the teens surveyed reported side-effects that include being less active, having a fear of missing out, anxiety, agitation, withdrawal and stress.
…. [Pont] suggests people take action to monitor and possibly reduce the amount of time they spend on their phones. Here are a few of her tips: (1) Keep phones out of the bedroom, (2) Enjoy tech-free family time, including dinner without devices, (3) Parents should lead by example, (4) Turn off notifications, and (5) Limit use of apps that have no creative or educational value.

Hackers Demand $30,000 Ransom from [BC] University of the Fraser Valley

http://www.metronews.ca/news/vancouver/2017/11/01/university-of-the-fraser-valley-investigating-breach-of-student-information.html
[Nov.1] The personal information of more than two dozen students attending the University of the Fraser Valley in British Columbia has potentially been breached online. Spokesman Dave Pinton said the Abbotsford-based university and police are investigating suspicious email related to the disclosure of "limited personal information" of 29 students. The information involves names, emails, phone numbers, addresses, grade point average and in one case, limited financial information.
Pinton said whoever sent an email to students on Monday a demanded $30,000 ransom. The university temporarily suspended access to some student and staff web systems and is working with the students and investigators, he said. The Office of the Information and Privacy Commissioner of B.C. has also been notified. "UFV takes the security of our email and information systems very seriously," he said, adding that the university is keeping students and staff updated on the availability of its online systems.
Abbotsford police say they were contacted by the university on Monday about demands for money involving the students' information.

Const. Ian MacDonald said the incident has been deemed an extortion attempt and computer forensic experts within the department's major crime unit are involved. The case appears similar to phone or email scams where fraudsters pretend to be police or government officials and demand the victim pay a fine or face detention, he said. Investigating scams can be a challenge, particularly online where perpetrators try to cover up their digital fingerprints or victims pay ransoms with Bitcoin or gift cards, MacDonald said. "From a policing standpoint we try to do as much as we can by way of prevention before people get separated from their money," he said.

'All of Us Can be Harmed': Investigation Reveals Hundreds of Canadians have Phoney Degrees

http://www.cbc.ca/news/business/diploma-mills-marketplace-fake-degrees-1.4279513

[Sept.14] A Marketplace investigation of the world's largest diploma mill has discovered many Canadians could be putting their health and well-being in the hands of nurses, engineers, counsellors and other professionals with phoney credentials. **Fake diplomas are a billion-dollar industry**, according to experts, and Marketplace obtained business records of its biggest player, a Pakistan-based IT firm called Axact. **The team spent months combing through thousands of degree transactions, cross referencing personal information with customers' social media profiles. The investigation revealed more than 800 Canadians could have purchased a fake degree**.

"Keep in mind this is just the one operation," said Allen Ezell, a former FBI agent who investigated diploma mills for decades. "This does not give you the totality of how many are being sold throughout Canada by all schools that are operating." Ezell, who co-wrote the book *Degree Mills: The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas*, **estimates half of new PhDs issued every year in the U.S. are fake**.

The impact of fake degrees is twofold, he said. They devalue legitimate degrees that people spend years and thousands of dollars earning. More importantly, professionals like engineers and health-care workers who lack the proper skills and expertise can put the public at risk. "All of us can be harmed by any professional that … does not have the full extent of training that his credentials purport that he has," Ezell said. "We can be harmed across the board, every day." [this is a lengthy, in-depth investigation by Marketplace on the topic of phoney degrees. It is introduced here because it is an important form of fraud to be aware of, but you will need to go to the link for the full report.]

'$300 Million in Cryptocurrency' Accidentally Lost Forever Due to Bug

https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether

More than $300m of cryptocurrency has been lost after a series of bugs in a popular digital wallet service led one curious developer to accidentally take control of and then lock up the funds, according to reports. Unlike most cryptocurrency hacks, however, the money wasn't deliberately taken: it was effectively destroyed by accident. The lost money was in the form of Ether, the tradable currency that fuels the Ethereum distributed app platform, and was kept in digital multi-signature wallets built by a developer called Parity. These wallets require more than one user to enter their key before funds can be transferred.

On Tuesday Parity revealed that, while fixing a bug that let hackers steal $32m out of a few multi-signature wallets, it had inadvertently left a second flaw in its systems that allowed one user to become the sole owner of every single multi-signature wallet. **The user, "devops199", triggered the flaw apparently by accident. When they realised what they had done, they attempted to undo the damage by deleting the code which had transferred ownership of the funds. Rather than returning the money, however, that simply locked all the funds in those multi-signature wallets permanently, with no way to access them. "This means that currently no funds can be moved out of the multi-sig wallets,"** Parity says in a security advisory. Effectively, a user accidentally stole hundreds of wallets simultaneously, and then set them on fire in a panic while trying to give them back. "We are analysing the situation and will release an update with further details shortly," Parity told users.

Hard fork. Some are pushing for a "hard fork" of Ethereum, which would undo the damage by effectively asking 51% of the currency's users to agree to pretend that it had never happened in the first place. That would require a change to the code that controls ethereum, and then that change to be adopted by the majority of the user base. The risk is that some of the community refuses to accept the change, resulting in a split into two parallel groups. …. The company also disputes that the currency is "lost", arguing that "frozen" is more accurate. But if it is frozen, it appears that no-one has the ability to unfreeze the funds.

“The Parity vulnerability was the result of an incorrectly coded smart contract used by the Parity wallet to store tokens on the Ethereum network,” said Dominic Williams, founder of blockchain firm DFINITY. “The vulnerability made it possible for anyone to ‘freeze’ the tokens held by that smart contract, making them immovable. At this time, the only method we are aware of to ‘unfreeze’ tokens held by the vulnerable smart contract would be to create a new ‘hard fork’ Ethereum client that deploys a fix. This would require every full node on the Ethereum network to upgrade by the date of the hard fork to stay in sync, including all miners, wallets, exchanges, etc.”
Ethereum has rapidly become the second most important cryptocurrency, after Bitcoin, with its price increasing more than 2,500% over the past year. One token of Ether is now worth a little over $285, up from $8 in January.

Apple Warned About Evil Wi-Fi Attack That Installs Malware On iPhones

https://www.forbes.com/sites/thomasbrewster/2017/11/01/apple-iphone-wi-fi-hack-pwn2own/

[Nov.01] Apple's security team is having a busy week thanks to Wi-Fi issues. First, it patched the scary KRACK vulnerability revealed in October to have exposed Wi-Fi encryption. **And now researchers from Tencent's Keen Lab have just shown off a hack that took advantage of four bugs to run malware on an iPhone 7 running the latest operating system, iOS 11.1, again via Wi-Fi**.
The hack was a winner on Tuesday at the Mobile Pwn2Own hacking contest run by Trend Micro's ZDI Initiative in Tokyo, where the researchers were handed $110,000 for their successful exploits.
There's not a wealth of information about the specific vulnerabilities exposed by Keen Lab, but a spokesperson from Trend Micro told *Forbes*: "The phone connects to a Wi-Fi network and a malicious app is installed. Sensitive information can be exfiltrated from the targeted device."
Apple, which has now been warned about the flaws, is aware of the issue and is working on a fix, which will be ready soon, the company told *Forbes*. Trend Micro said in a blog post that representatives from Apple, Google and Huawei were at the event. They have 90 days to fix the vulnerabilities or offer a valid reason for not addressing them, otherwise Trend will publish its own limited advisory.
The Keen hackers earned themselves another $45,000 by using two bugs to exploit Apple's Safari browser on an iPhone 7, on top of $100,000 for an attack on the Huawei baseband processor in the Chinese manufacturer's Mate9 Pro device. Another researcher, Richard Zhu (also known as 'fluorescence'), hacked the iPhone 7 with another set of Safari exploits and won himself $25,000. And another $70,000 was given to a security researcher known as mj0011, from Chinese firm Qihoo 360, for an attack of Samsung's Galaxy S8.
As the Pwn2Own contest continues, professional hackers will attempt to find other ways onto the Apple, Samsung and Huawei devices as well as the Google Pixel. As for users, they should update to the latest operating system, even if it won't protect them from the weaknesses exposed at Pwn2Own. Apple patched a slew of weaknesses with iOS 11.1, including 13 memory corruption bugs - most of which were uncovered by Google Project Zero staffer Ivan Fratric - that could've allowed hackers to run malicious code on an iPhone.

iPhone Apps with Camera Permissions Can Secretly Take Your Photo without You Noticing

https://thehackernews.com/2017/10/iphone-camera-spying.html

Are you a proud iPhone owner? If yes, this could freak you up. Trust me! Your iPhone has a serious privacy concern that allows iOS app developers to take your photographs and record your live video using both front and back camera - all without any notification or your consent. This alarming privacy concern in Apple's mobile operating system was highlighted by an Austrian developer and Google engineer, Felix Krause, who detailed the issue in his blog post published Wednesday.
The issue, Krause noted, is in the way Apple's software handles camera access. **Apparently, there is a legitimate reason for many apps, such as Facebook, WhatsApp, and Snapchat, to request access to your camera, in an effort to take a photo within the app. So, this permissions system is not a bug or a flaw instead it is a feature, and it works exactly in the way Apple has designed it, but Krause said any malicious app could take advantage of this feature to silently record users activities**.
Krause explained that granting camera permission could enable iOS app developers to access: both the front and the back camera of your device, photograph and record you at any time the app is in the

foreground, upload the recorded and captured content immediately, and run real-time face detection to read your facial expressions ...and all without warning or alerting you in any way.

Since Apple only requires users to enable camera access one time when they are asked to grant blanket permission to an app and gives free access to the camera without requiring any LED light or notification, Krause explained that a malicious app could leverage this loophole to go far beyond its intended level of access to spy on users. The researcher has even developed a proof-of-concept app only to demonstrate how a malicious app could abuse such permissions to silently take your pictures every second as you use the app, or even live stream video of your surrounding from your front and rear cameras without notifying you. Krause said his "*goal [to build the demo app] is to highlight a privacy loophole that can be abused by iOS apps.*"…..

How to Protect Your Privacy? There is a little user can do to protect them. Krause recommended Apple to introduce a way to grant temporary permissions to access the camera, allowing apps to take a picture during a limited period of time, and then revokes it after that. Another way is to introduce a warning light or notification to the iPhone that informs people when they are being recorded. **Most importantly, do not let any malicious app enter your smartphone. For this, always download apps from an official app store and read reviews left by other users about the app and its developer.** According to Krause, **for now, the only practical way to protect yourself is to cover your camera**, just like Facebook CEO Mark Zuckerberg and ex-FBI Director James Comey do.

Global CISOs Unprepared for Evolving Threats

https://www.infosecurity-magazine.com/news/global-cisos-unprepared-evolving/

Research by the Ponemon Institute focusing on chief information security officers (CISOs) worldwide has found worrying levels of business readiness for cybersecurity threats.

Drawing on insights from 184 global CISOs, the report noted that today's IT security strategies and tactics are shifting away from a focus on strong perimeters to smart data, networks, devices and applications. According to 60% of CISOs surveyed, material data breaches and cybersecurity exploits are driving change in organizations' attitudes to security programs, while another 60% of respondents believe security is considered a business priority. Yet, while awareness levels are clearly growing, the report's clear message is that there is plenty of room for improvement.

For instance, 80% of respondents said the internet of things (IoT) will cause "significant" or "some change" to their practices and requirements. However, most companies are not hiring or engaging IoT security experts (41%) or purchasing and deploying new security technologies to deal with potential new risks (32%).

"This new research provides a unique view into how CISOs are operating in today's challenging environment," said Mike Convertino, CISO at F5 Networks, which commissioned the report. "It's clear CISOs are making progress in how they drive the security function and the leadership role they are assuming within companies. Yet in many organizations, IT security is not yet playing the strategic, proactive role necessary to fully protect assets and defend against increasingly sophisticated and frequent attacks."

Finding the right talent is also a significant hurdle, with 56% struggling to identify and recruit qualified candidates. Almost half of surveyed CISOs branded their staffing as inadequate (42%). Interestingly, 50% consider computer learning and artificial intelligence important to address staffing shortages. In two years, 70% say these technologies will be important to their IT security functions.

Most CISOs agreed cybersecurity threats are here to stay. Organizations represented in the study experienced an average of two data breaches in the past 24 months. About 83% said the frequency of data breach will increase or stay the same. Another 87% believe the severity of data breach incidents will increase or stay the same. On average, respondents also experienced three cyber exploits or attacks in the past 24 months. Also, 89% of respondents said cyber exploits will increase or stay the same; while 91% predicted the severity of cyber exploits or attacks would increase or stay the same.

Advanced persistent threats (APTs) were ranked the top threat to the security system followed by DDoS, data exfiltration, insecure apps (including SQL injection), credential takeover, malicious insiders and social engineering.

EternalBlue is Back, with New Tricks

https://www.infosecurity-magazine.com/news/eternalblue-is-back-with-new-tricks/

An email-server message block (SMB) blended threat has been uncovered, which uses the compromised machine as a stepping stone to propagate laterally via the EternalBlue exploit.
Netskope Threat Research Labs said that the inclusion of the EternalBlue exploit is insidious because it will be launched internally from the newly infected machine, permitting direct access to shared SMB machines such as file shares and backup systems. This puts core data stores at risk in a fashion that may be impossible to anticipate. Also, SMB, a file sharing protocol that provides shared access to files in a network, is a widely adapted program, meaning the vulnerability has a considerable impact.
"We have observed that the presence of embedded document files in a cloud storage and collaboration services possesses a more significant threat to an enterprise environment since it arrives from a trusted source," said Netskope researcher Ashwin Vamshi. **"Once an endpoint is compromised with the second-stage payload like EternalBlue, it creates a wormed infection, leading all neighboring internal computers to be attacked via SMB from the newly compromised internal stepping-stone system."**
Earlier this year, The Shadow Brokers group disclosed a series of exploits, backdoors and several attack tools affiliated with nation-state activity. One of the exploits, EternalBlue, targets open SMB ports to leverage remote code execution, and has been widely used in attacks such as WannaCry, NotPetya and more recently Bad Rabbit. In this case, the initial attack begins with a Swiss regional email which contains a Word Document with an embedded .lnk object, which is actually a backdoor that downloads the EternalBlue payload. From there, the threat moves from a cross-perimeter attack to an internal attack, with EternalBlue spreading itself across an organization's network, without any user intervention, leading to internal attacks that organizations may not be prepared for.
"The use of cloud services by enterprises, along with the implicit trust, has led to an increase in malware attacks and thus posing a new challenge for organizations," said Vamshi, adding that organizations should enforce policy on usage of unsanctioned services as well as unsanctioned instances of sanctioned cloud services.

US Identifies Six Russian Government Officials Involved in DNC Hack

https://thehackernews.com/2017/11/dnc-email-russian-hackers.html

The United States Department of Justice has reportedly gathered enough evidence to charge at least six Russian government officials for allegedly playing a role in hacking DNC systems and leaking information during the 2016 presidential race. Earlier this year, US intelligence agencies concluded that the Russian government was behind the hack and expose of the Democratic National Committee (DNC) emails in order to influence the 2016 presidential election in Donald Trump's favour.
Now, citing people familiar with the investigation, the Wall Street Journal reported on Thursday that United States federal prosecutors could bring charges against the alleged unnamed Russian officials early next year. The US federal intelligence investigators also believe that "dozens" of other Russian officials may have also participated in the DNC hack, which was allegedly ordered by Russian President Vladimir Putin himself. However, both Putin and Russian government officials have denied allegations.
The DNC computer system hack last year led to thousands of stolen DNC emails, including personal and sensitive emails from Hillary Clinton campaign manager John Podesta, appeared on whistleblowing website WikiLeaks.
In a separate forensic investigation conducted by FireEye incident response firm Mandiant identified hacking tools and techniques used in the DNC hack associated with Fancy Bear - also known as APT28, Sofacy, Sednit, and Pawn Storm - a state-sponsored hacking group believed to be a unit of Russian Military Intelligence (the GRU).
U.S. federal agents and prosecutors in Washington, Pittsburgh, Philadelphia and San Francisco have been cooperating with the DNC investigation. However, none of them has revealed the actual identity of the six suspects. **However, even after getting charged, the Russian officials or hackers will hardly be prosecuted in the United States until they enter the US soil because the country has no extradition agreement with Russia**. This is the second time in this year when the United States has charged Russian officials with cybercrimes.
In March 2017, the DoJ charged two Russian intelligence officers - Dmitry Aleksandrovich Dokuchaev and Igor Anatolyevich Sushchin - and two criminal hackers - Alexsey Alexseyevich Belan and Karim Baratov - in connection with the 2014 Yahoo hack that exposed about 500 million Yahoo user accounts. However, no one has ever seen the insides of a United States courtroom.

Critical Tor Flaw Leaks Users' Real IP Address - Update Now

https://arstechnica.com/information-technology/2017/11/critical-tor-flaw-leaks-users-real-ip-address-update-now/

Mac and Linux versions of the Tor anonymity browser just received a temporary fix for a critical vulnerability that leaks users' IP addresses when they visit certain types of addresses. TorMoil, as the flaw has been dubbed by its discoverer, is triggered when users click on links that begin with file:// rather than the more common https:// and http:// address prefixes. When the Tor browser for macOS and Linux is in the process of opening such an address, "the operating system may directly connect to the remote host, bypassing Tor Browser," according to a brief blog post published Tuesday by We Are Segment, the security firm that privately reported the bug to Tor developers.

On Friday, members of the Tor Project issued a temporary work-around that plugs that IP leak. Until the final fix is in place, updated versions of the browser may not behave properly when navigating to file:// addresses. They said both the Windows versions of Tor, Tails, and the sandboxed Tor browser that's in alpha testing aren't vulnerable. "The fix we deployed is just a workaround stopping the leak," Tor officials wrote in a post announcing Friday's release. "As a result of that navigating file:// URLs in the browser might not work as expected anymore. In particular entering file:// URLs in the URL bar and clicking on resulting links is broken. Opening those in a new tab or new window does not work either. A workaround for those issues is dragging the link into the URL bar or on a tab instead. We track this follow-up regression in bug 24136."

Friday's post went on to say that We Are Segment CEO Filippo Cavallarin privately reported the vulnerability on October 26. Tor developers worked with Mozilla developers to create a work-around the following day, but it only partially worked. They finished work on a more complete work-around on Tuesday. The post didn't explain why the fix, delivered in Tor browser version 7.0.9 for Mac and Linux users, wasn't issued until Friday, three days later. The Tor browser is based on Mozilla's open-source Firefox browser. The IP leak stems from a Firefox bug.

Tor officials also warned that alpha versions of the Tor browser for Mac and Linux haven't yet received the fix. They said they have tentatively scheduled a patch to go live on Monday for those versions. In the meantime, the officials said, Mac and Linux alpha users should use updated versions of the stable version. Tor's statement Friday said there's no evidence the flaw has been actively exploited on the Internet or darkweb to obtain the IP addresses or Tor users. Of course, the lack of evidence doesn't mean the flaw wasn't exploited by law enforcement officers, private investigators, or stalkers. And now that a fix is available, it will be easy for adversaries who didn't know about the vulnerability before to create working exploits. Anyone who relies on a Mac or Linux version of the Tor browser to shield their IP address should update as soon as possible and be ready for the possibility, however remote, their IP addresses have already been leaked.

No Prison for Student who Developed Spam Botnet to Pay College Fee

https://www.hackread.com/no-prison-for-student-who-developed-spam-botnet-to-pay-college-fee/

Sean Tiernan, 29 from Santa Clara, California was given 24 months' probation on October 30th for his involvement in developing a massive spam botnet that infected more than 77,000 devices to send spam and make money for his college fee. The good news for Tiernan is that he is not facing any prison time for his crime since the bot was used to infect computers to serve as proxies to send spam messages and not to infect users with malware for other serious malicious purposes.

He was arrested in 2012 with CAN-SPAM violation by the Federal Bureau of Investigation (FBI) for developing, using and sending spams to users through the botnet where most of the infected devices were located in the Western District of Pennsylvania. He pleaded guilty in 2013. According to US Department of Justice Press Release: "Once a computer was infected with the malware, the malware was programmed by Tiernan to automatically communicate and receive direction from servers over the Internet which were controlled by Tiernan, without knowledge of the infected computers' owners." According to a report by Bleeping Computer, Tiernan confessed to his crime immediately and cooperated with the Bureau.

After his arrest, Tiernan decided to pursue a career in the field of cybersecurity. It was due to his skills that a reputed cybersecurity firm hired him and he is now planning to go to the Stanford CyberSecurity Graduate Program for further education. One has to acknowledge that **Tiernan was lucky to skip jail time. Based on previous cases, the United States has been pretty strict on cybercriminals**. The case of British hacker Lauri Love is a prime example of - if deported to the United States, could face 99 years in prison for hacking US government computers in the States. The FBI also

arrested WannaCry ransomware hero and British citizen Marcus Hutchins who was in the United States to attend a cybersecurity conference for creating a banking Trojan targeting US citizens. Hutchins is currently out on bail.

Feel free to forward the Digest to others that might be interested.
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

****