# Security News Digest
# February 21, 2017

**You might occasionally hate your computer,**
**so take the Love Security - Love Your Data Quiz.**

**Question: Do Hackers Hack Other Hackers? Answer: Of course they do! See the last article for details.**

## Digital Searches at the US Border: What You Need to Know

http://globalnews.ca/news/3258351/digital-searches-at-the-us-border-what-you-need-to-know/

Watchdog groups that keep tabs on digital privacy rights are concerned that U.S. Customs and Border Patrol agents are searching the phones and other digital devices of international travelers at border checkpoints in U.S. airports. The issue gained attention recently after at least three travelers, including a Canadian journalist, spoke out publicly about their experiences. ..Here are some things to know about the searches and your privacy rights.

**What has prompted the concern?**

The American Civil Liberties Union and the Electronic Frontier Foundation both say they have noticed an uptick in complaints about searches of digital devices by border agents. ..Customs officials say the perceived shift can be attributed to a jump in the number of electronic devices that people are carrying with them and shifting tactics as the agency adjusts to the amount and types of information that can be stored on today's devices.

**What search authority does the Border Patrol have?**

…Border agents have long had the right to search travelers' physical luggage without a warrant, and that interpretation has been expanded to include digital devices, ACLU staff attorney Nathan Freed Wessler said. In 2013, the 9th U.S. Circuit Court of Appeals ruled that if agents want to do a forensic search they need to have a reasonable suspicion of wrongdoing, he said. But the court stopped short of requiring agents to obtain a search warrant beforehand, he said. And an agent can flip through a phone in a cursory search for any reason.

**What does the Border Patrol say?**

…A senior CBP official briefed reporters on the issue Friday, but the agency insisted the official not be identified. "We see it as an article that is brought into the U.S., no different than a booklet of materials, no different than a suitcase with items in it," the official said. "We've uncovered very serious and significant information in these types of searches, everything from national security concerns to child pornography to evidence of crimes to determinations of people's admissibility status under the immigration laws."

**How can you protect your digital privacy while traveling?**

*Privacy advocates say travelers who are concerned should leave their phones and laptops at home and buy a cheap phone once they arrive at their destination*. The Council on American-Islamic Relations is also advising its members to do the same. Those who can't leave their devices behind should encrypt them and close out of all social media applications so they aren't accessible without a password, said Schwartz. But those steps won't matter much if a border agent asks a traveler to unlock the phone or provide a password, said Schwartz. *And travelers should also be aware of the rules in other countries*. Israel authorities can check mobile phones at the airport, for example.

**What happens if you refuse?**

The Border Patrol can't bar a U.S. citizen from entry [back into the US] if they refuse to comply, but agents can make things difficult. Travelers who don't unlock their phones could be questioned, detained temporarily and have their phones taken by agents for days. Travelers who are not U.S. citizens can be denied entry.

## How Saying Yes to Free Wi-Fi Could Mean 'You Are The Product' for Businesses

http://www.cbc.ca/news/canada/toronto/wifi-marketing-toronto-1.3988650

Twenty minutes after Zoe Elder stopped at a Gateway Newstands location in downtown Toronto to buy a pack of cigarettes, an email showed up in her personal Hotmail inbox. "Buy one Nestlé single bar + get one free," it began. The sender? Gateway Newstands. Though Elder, 30, didn't know it at the time, she was being *targeted by a Wi-Fi marketing campaign - anyone logged in to a store's free Wi-Fi is sent advertisements and promotions*. "I was completely floored. I didn't understand," said Elder. "I didn't know if it was a coincidence, or something I had signed up for … I was going through everything."

Turnstyle, the company that built the campaign that messaged Elder, said the emails are only sent if users first log in to Gateway's Wi-Fi, which then ends up giving over their email addresses. An email is sent that restates the users are giving their permission to get messages. Elder said she doesn't remember signing onto anything, and she never received the first email from Gateway or Turnstyle. "I actually feel like my phone got violated, to be honest," she said.

Bhupesh Shah, a professor of marketing and digital media at Seneca College, isn't surprised. "If you went to the average person on the street, they probably wouldn't be aware that [Wi-Fi marketing] is happening," he told CBC Toronto. That, said Shah, is going to change. "As technology improves, it becomes easier to employ these technologies into retail," he said. "This is something that more and more retail organizations will use."

Shah, Turnstyle and Gateway Newsstands couldn't explain what happened in Elder's case, arguing it's unlikely that the opt-in system could have such a serious glitch. *But Shah said it feeds into a bigger phenomenon: jumping on free Wi-Fi networks without realizing the possible implications*. *Signing in using your Facebook log-in, phone number or email is akin to opening a possible floodgate, said Shah. "You've in many cases allowed the organization to market to you, to collect your data,"* he said.

**So how can you avoid being targeted?**

Turnstyle vice-president Ryan Freeman told CBC Toronto that people receiving messages in a Turnstyle campaign are able to globally opt out of receiving any further advertising from any of his company's clients. *He said the first email is sent after log-in to ensure people know what they're signing up for. But Shah argues that for many, little attention is paid to a Wi-Fi sign-in. "I would say most people don't read the terms and conditions. If you want Wi-Fi, you want Wi-Fi - you really don't care," he said. Shah has a favourite saying about social media:' "If you're not paying for the product, you are the product."*

Gateway Newstands president Noah Aychental told CBC Toronto that *its three-month Wi-Fi marketing trial, undertaken with Nestlé as a partner, is specifically aimed at millennials. "We have to speak to them where most of their communications are happening.* They're not buying magazines, they're not reading newspapers," he said. Though Aychental can't say if his company will expand the trial beyond its current 25 Greater Toronto Area stores, *he is convinced it's a fair trade between business and consumer. "The deal is that if you are near our store, there's free internet access," he said*.

## PharmaNet Breach Compromises Personal Information of 7,500 B.C. Residents, Says Province

http://www.cbc.ca/news/canada/british-columbia/bc-pharmanet-breach-1.3985173

[Feb16] The personal information of approximately 7,500 British Columbians may have been compromised through the provincial government's PharmaNet system, according to the Ministry of Health. A letter from the ministry was sent last week to B.C residents affected by the breach. *The letter says an "unknown/unauthorized person obtained and used a physician's login to access PharmaNet." PharmaNet is the province-wide network that links all B.C. pharmacies to a central information system*.

According to the letter, obtained by CBC News, personal information such as individual names, addresses, dates of births, and Care Card numbers have been viewed.

The government confirmed the accuracy of the letter Wednesday evening, and said an investigation affecting 14 physicians is underway. They also said that of the approximately 7,500 individuals who had their profiles viewed, 80 also had their medication history over the past 14 months viewed. "The Ministry of Health has begun to send letters to all patients and doctors affected by the breach, notifying them of the incident and advising them of precautionary steps they can take to protect themselves from identify theft," wrote the ministry in a statement.

"Health Ministry staff are also working with the affected physicians and their offices and PharmaNet system vendors to identify security measures that should be put in place to provide increased protection, such as regularly changing passwords and using a secure internet provider." *There are four individual incidents, all of which have taken place since the fall of 2016, being investigated by the Ministry of Health*

*and the Corporate Information and Records Management Office of the Ministry of Finance. The ministry said it did not know how the breach occurred.*
…The ministry of health letter to patients, dated Feb. 6, 2017, states there is "no other private information, such as banking, attached to your record," but says "the information gathered could possibly be used as a starting point for identity theft." "We encourage you to take precautions to safeguard your other personal information," it says and suggests those affected may want to seek out the services of a credit monitoring company. The Ministry of Health says it has begun sending letters to all patients and doctors affected by the breach, and is working with affected physicians to identify security measures that should be put in place to provide more protection. In addition, various medical groups have been notified including Doctors of BC, the College of Physicians and Surgeons BC, the Canadian Medical Association and the Office of the Information and Privacy Commissioner.

## Websites Can Now Track You Online Across Multiple Web Browsers

http://thehackernews.com/2017/02/cross-browser-tracking.html
You might be aware of websites, banks, retailers, and advertisers tracking your online activities using different Web "fingerprinting" techniques even in incognito/private mode, but now sites can track you anywhere online - even if you switch browsers. *A team of researchers has recently developed a cross-browser fingerprinting technique - the first reliable technique to accurately track users across multiple browsers based on information like extensions, plugins, time zone and whether or not an ad blocker is installed*. Previous fingerprinting methods usually only work across a single browser, but the new method uses operating system and hardware level features and works across multiple browsers. This new fingerprinting technique ties digital fingerprint left behind by a Firefox browser to the fingerprint from a Chrome browser or Windows Edge running on the same device. *This makes the method particularly useful to advertisers, enabling them to continue serving targeted advertisements to online users, even if they avoid them by switching browsers*. The new technique can be found in a research paper titled *(Cross-)Browser Fingerprinting via OS and Hardware Level Features* by Lehigh University's Yinzhi Cao and Song Li, and Washington University in St. Louis' Erik Wijmans. The cross-browser fingerprinting technique relies on "many novel OS and hardware features, especially computer graphics ones" that are slightly different for each computer. [see article for tech details] The researchers plan to present their paper at the Network and Distributed System Security Symposium scheduled for February 26 through March 1 in San Diego, California.

## Charging Smartphone in Public Ports Leads to Data Hack - So Let's Stop

https://www.hackread.com/public-charging-ports-smartphone-data-hack/
A smartphone with a low battery is a real problem, especially when you are on the go. In such a scenario, finding a USB port installed somewhere or charging facility at public outlets seems to be a blessing. Public charging ports are installed almost everywhere for the users and visitors convenience such as at airports, conference centers, cafes, parks and planes, etc. All you need to do is plug in your cell phone and feel relaxed and relieved. However, Drew Paik from IT security firm Authentic8 told CNN that this is a very dangerous thing to do because *the outlet might be hacked and all the data present in your phone could easily be transferred to a hacker*.
Authentic8 is the developer of Silo web browser that facilitates anonymous web surfing. *The revelation from Paik is surprising and concerning as he states that simply through plugging your phone into a hacked charger or power strip would lead to getting your device infected at once and all your data will also be compromised. The reason is that the cord used to plug in your mobile phone is also used for sending data to and from the device*. For example, if you connect your iPhone to your Mac device using the same charging cord, you can easily transfer images and music from your mobile to your Mac. Hence, *through compromising this particular cord, a hacker can extract all sorts of data from your mobile* including pictures, emails, contact numbers, SMS messages, etc., without your knowledge obviously. This kind of hacking is called "Juice Jacking", which was a term created by security researchers in 2011 and this was followed by the creation of another term called "Video Jacking", which was introduced in 2016. This referred to a phone's ability to record everything that you typed or looked at due to being compromised by a hacked port.
*The findings of the research were demonstrated by Authentic8 at the RSA security conference held in San Francisco. The company installed a charging station at its stall and offered to charge cords to visitors so that they could charge their devices. Then the security firm ran a social experiment to analyze*

*the number of people who used this charging service, which turned out to be quite overwhelming with over 80% of the audience using the charging facility provided by Authentic8. Paik noted that none of these visitors seemed to care about the security aspect of charging mobiles from a public station despite the fact that they were attending a security conference*. [they trusted a 'security' company to be safe]

## Germany Bans Internet-Connected 'Spy' Doll Cayla

http://www.securityweek.com/germany-bans-internet-connected-spy-doll-cayla

German regulators have banned an internet-connected doll called "My Friend Cayla" that can chat with children, warning Friday that it was a de facto "spying device". *Parents were urged to disable the interactive toy by the Federal Network Agency which enforces bans on surveillance devices*. "Items that conceal cameras or microphones and that are capable of transmitting a signal, and therefore can transmit data without detection, compromise people's privacy," said the agency's head, Jochen Homann. "This applies in particular to children's toys. The Cayla doll has been banned in Germany. This is also to protect the most vulnerable in our society."

*The doll works by sending a child's audio question wirelessly to an app on a digital device, which translates it into text and searches the internet for an answer, then sends back a response that is voiced by the doll*. The German regulators in a statement warned that anything a child says, or other people's conversations, could be recorded and transmitted without parents' knowledge. "A company could also use the toy to advertise directly to the child or the parents," it said. *"Moreover, if the manufacturer has not adequately protected the wireless connection, the toy can be used by anyone in the vicinity to listen in on conversations undetected."*

Genesis Toys, which manufactures the doll, says on its website that it "is committed to protecting your and your family's personal information. "Our objective is to ensure that our products and services are safe and enjoyable for our customers". It also says Cayla "is programmed to not utter, display or say words or images that would be inappropriate for children to see or hear". The company regularly reviews "encryption and physical security measures" to guard against unauthorized access to customers' personal information. *But it warns on its website that "unfortunately no method of transmission over the Internet, or method of electronic storage, is 100 percent secure". The regulation agency added that it would "inspect other interactive toys and, if necessary, will take further action"*.

The European Consumer Organization said it welcomed the decision but criticized the fact consumers would struggle to get compensation. Its head Monique Goyens said that "if connected toys, such as this speaking doll, can be hacked to spy on or talk to children, they must be banned." She added that "EU product laws need to catch up with digital developments to deal with threats such as hacking, data fraud or spying".

## Yahoo Notifies Users of Sophisticated Breach Methods

http://www.securityweek.com/yahoo-notifies-users-sophisticated-breach-methods

Yahoo said Wednesday it was notifying some users that hackers may have been able to use a maneuver to break into their accounts without stealing passwords. The latest notifications were in response to the record breach disclosed late last year affecting an estimated one billion users - *which involved forging of "cookies" or files used to authenticate users when they log into their accounts*. The notification indicates the investigation into the attacks are in the final stage, according to a source familiar with the matter, noting that messages had been sent to "a reasonably final list" of Yahoo users. *A Yahoo spokesman said the company was notifying all potentially affected users and that it had "invalidated" the forged cookies*. "As we have previously disclosed, our outside forensic experts have been investigating the creation of forged cookies that could have enabled an intruder to access our users' accounts without a password," the company said in a statement. "The investigation has identified user accounts for which we believe forged cookies were taken or used."

## Donald Trump's Outdated Android Phone Prompts National Security Concerns

http://globalnews.ca/news/3257385/donald-trump-android-phone/

President Trump is still using his trusty old Android phone for early morning tweet storms - and California Congressman Ted Lieu [and many others] wants to put a stop to it. That's because consumer-grade Android phones, especially if they're dated like the one that Trump is reportedly using, can easily be hacked. "We are writing to request that the House Oversight and Government Reform Committee hold a

public hearing into troubling reports that the President is jeopardizing national security by egregiously failing to implement commonsense security measures," the letter reads.
Trump's continued use of his Android phone has been raising questions with security experts; the President is reportedly using a Samsung Galaxy S3, which isn't capable of running the latest version of Android. *The Galaxy S3 was also found to be vulnerable for "Stagefright," a software exploit that made it possible to hijack phones with a simple multimedia text message*. Samsung has pushed software updates to affected phones to deal with that specific issue, but it's unclear whether the President's phone was patched, and which other vulnerabilities it may be susceptible to.
The Secret Service successfully talked President Obama out of using an iPhone for security reasons. Instead, Obama used a locked-down Blackberry phone throughout his presidency. Trump on the other hand has reportedly resisted calls to trade in his Android phone [for the government-issued device], and tweets written by the President still originate from the device.

## Someone DDoSed A University Server By Hacking Its Vending Machines

https://www.hackread.com/university-servers-ddosed-through-vending-machines/

*It is a fact that Internet of Things (IoT) devices are extremely vulnerable to exploitation from malicious threat actors, thanks to the phenomena of default login credentials and widespread availability that makes them easy targets*. We have also come to know about the capabilities of even a smaller number of infected IoT devices as they turn into an army of botnets and create havoc at any targeted organization's internet network.
Verizon Enterprise's RISK (Research, Investigations, Solutions and Knowledge) department researchers were *tasked with the investigation of internet blockage at an unidentified US university and they discovered that a few thousand infected IoT devices are responsible for cutting off the internet*. The attackers reprogrammed the devices in such a way that they started attempting to connect with seafood-oriented websites sporadically. *The attackers hacked 5,000 devices so that these send out DNS queries continuously (DDoS attack) and to fulfill their malicious objectives they used a variety of devices from vending machines to street lamps*. The university's network, resultantly, started to slow down as the malware in the IoT devices started attacking its drink vending machines. When one device was infected, the malware started searching for more vulnerable devices and the chain reaction followed suite. *When a single device was infected, the malware modified its admin password making it difficult to remove the infection*. The report explained that *"The botnet spread from device to device by brute forcing default and weak passwords. The firewall analysis identified over 5,000 discrete systems making hundreds of DNS lookups every 15 minutes."*
When the IT staff of the university got a hint of the malware attack, they quickly responded by tracking down the new passwords and since these were transmitted in clear text format instead of being encrypted, their job became easier as they were able to intercept them using a packet-sniffing app. After receiving the list of new passwords, they launched a fix, which was an automated antidote that reset all the passwords and broke the chain of the botnets by freeing the devices. "Short of replacing every soda machine and lamp post, I was at a loss for how to remediate the situation. *We had known repeatable processes and procedures for replacing infrastructure and application servers, but nothing for an IoT outbreak," stated the IT admin*.
Hacking vending machines is not something new, in fact, there are several videos on YouTube showing how people are hacking these machines for free coffee and snacks but this incident proves that even a handful of infected IoT devices can do a lot of harm. This is why the IT department of the university has urged that companies *regularly inspect the network settings for their manufactured IoT devices and keep them separate from Internet access as well as from other devices*.

## Insecure Android Apps Expose Connected Cars

http://www.securityweek.com/insecure-android-apps-expose-connected-cars

Researchers at Kaspersky Lab have analyzed several Android applications for connected cars and determined that most of them lack important security features, making it easier for hackers to unlock the vehicles. Carmakers often provide mobile applications that allow owners to control various functions remotely, including locking and unlocking doors, starting the engine, locating the vehicle, obtaining service information, and controlling air conditioning. Kaspersky has analyzed seven of the most popular connected car Android applications, which have been installed by millions of users. *The applications have not been named, but the security firm has reported its findings to their developers*.

Researchers tested the apps to determine if they can be abused to steal a car or incapacitate its systems. They also looked for various security mechanisms, such as the use of obfuscation to prevent reverse engineering, checking if the device is rooted, checking the integrity of the code, and ensuring that the legitimate GUI is displayed to the user (i.e. overlay protection). All the tested applications can be used to unlock a vehicle's door and some of them also allow the user to start the engine. However, *the aforementioned security features are mostly missing from the apps* – only one encrypts the username and password, and none of them use obfuscation, overlay protection, root detection or code integrity checks. The lack of security mechanisms makes it easier for a piece of malware that has infected the Android device to take control of the smart car app. *And while hijacking the application does not allow an attacker to drive away with the car, it does allow them to unlock it and disable its alarm, which can make it easier to steal*. Researchers said *car apps should be as secure as online banking apps, but they believe these applications currently represent the weakest link*.

## Clinton Campaign Tested Staffers With Fake Phishing Emails

http://www.darkreading.com/attacks-breaches/clinton-campaign-tested-staffers-with-fake-phishing-emails/d/d-id/1328177

Email leaks notwithstanding, Hillary Clinton's campaign manager Robby Mook says the campaign conducted regular security training for staffers, which included sending fake phishing emails to campaign staffers to see how they'd be handled. "We sent out phishing emails of our own to test people and communicate back to the team to see how far they were clicking, to educate people, and show their vulnerability and how much their choices matter," Mook said in an interview at RSA Conference. He recalls at least three faux-phishing tests, adding there may have been more. Mook says the campaign also emailed staffers regularly about good IT hygiene. "We had signs up in the bathrooms about not sharing passwords and 'Don't click on that link, stop and think'," Mook says. Staff meetings also included regular security updates from the campaign's IT director, he adds. Mook made the rounds at the RSA Conference here this week, speaking about user vulnerability to inside attacks and speaking at the Global Insider Threat Summit sponsored by security vendor Dtex Systems. Mook also wants to make clear that it was the Democratic National Committee's servers that were hacked, not those of the Clinton campaign. The distinction is important; the campaign suffered from emails that were leaked from personal email accounts.

## Russian Black Hat Hacks 60 Universities, Government Agencies

http://www.securityweek.com/russian-black-hat-hacks-60-universities-government-agencies

A Russian-speaking black hat hacker has breached the systems of more than 60 universities and U.S. government agencies, according to threat intelligence firm Recorded Future. *The hacker, tracked by the company as "Rasputin," typically exploits SQL injection vulnerabilities to gain access to sensitive information that he can sell on cybercrime marketplaces*. Rasputin is the hacker who last year breached the systems of the U.S. Election Assistance Commission (EAC) and attempted to sell more than 100 access credentials, including ones providing administrator privileges. Researchers found evidence that he had been negotiating with a potential buyer representing a Middle Eastern government.

Recorded Future has been monitoring the hacker's activities and identified many of his victims, including over two dozen universities in the United States, ten universities in the United Kingdom, and many U.S. government agencies. The list of targeted government agencies includes local, state and federal organizations. The targeted federal agencies are the Postal Regulatory Commission, the Department of Housing and Urban Development, the Health Resources and Services Administration, and the National Oceanic and Atmospheric Administration.

There are plenty of free tools that can be used to find and exploit SQL injection vulnerabilities, ..however, Rasputin has been using a SQL injection tool that he developed himself. "Financial profits motivate actors like Rasputin, who have technical skills to create their own tools to outperform the competition in both identifying and exploiting vulnerable databases," said Levi Gundert, VP of intelligence and strategy at Recorded Future. *Experts believe Rasputin picks his targets based on their perceived investment in security controls and the potential value of the stolen data*. The personal information stored in the targeted organizations' databases can be highly valuable, particularly if the data is associated with users in North America and Western Europe.

## When Hackers Hack Hackers

http://www.darkreading.com/threat-intelligence/when-hackers-hack-hackers/d/d-id/1328095?piddl_msgorder=thrd&image_number=1

Notable cases of internecine [big word for 'happening between members of a group'] cyber squabbles:

**No Monopoly On Theft**

Thieves make the best targets for theft, because who are they going to take their complaints to? One enterprising hacker, w0rm, took this principle to heart by raiding the user database of a Dark Web forum called Monopoly, which facilitated in connecting the bad guys to talk shop about running botnets, pushing phishing campaigns, and committing credit card fraud. Just as with any other database breach, w0rm offered up the goods on Monopoly for about $500, in a similar tack. The difference here being that security pros were playing the world's tiniest violins for the victims of this breach.

**Peace Hacks w0rm**

Well known in Dark Web marketplaces, a cybercriminal by the handle of Peace_of_Mind got fed up with w0rm's antics. Apparently the Monopoly attack was far from an outlier. Peace claimed that w0rm had been stealing zero-days from certain forums and posting them as his own. What's more, he was irritated at w0rm for blowing the lid off vulnerabilities Peace was using to maintain access to compromised websites and for scamming people Peace knew. In retribution, Peace engaged in some good ol' fashioned cyber-vandalism, taking the digital spray paint to the website w0rm used to publish proof-of-concept codes and dump data breached from high profile attacks against targets like Wall Street Journal, Vice, and CNET.

**Dirty d33ds**

Cyber gang-on-cyber gang attacks are pretty common and date back far into hacking history. One example in the not-too-distant past - 2011 - saw a hacking group called d33ds bust into the online black market store of a rival called Srblche, who sold admin access to military education and government sites, along with website vulnerabilities. d33ds dumped data from the marketplace's server, including customer password hashes and administrative passwords.

**APT-on-APT Attacks**

In 2015, Kaspersky Lab explained a phenomenon it was calling advanced persistent threat (APT) wars, where two APT groups target one other with the same kind of techniques they use against their typical government and corporate victims. Their example anecdote told a Spy vs. Spy story of two groups called Hellsing and Naikon who duked it out with a back-and-forth battle of spearphishing emails and intelligence-gathering through customized backdoor payloads.

**Serving Up Rivals To Shadowserver**

The d33ds example smelled more of spite than of business, but security researchers are also running into competitive spats where attackers essentially bare their teeth over the same piece of meat. Last year a researcher with Shadowserver detailed how the organization is often able to carry out takedowns of command-and-control servers and domains based on tips from rival hackers. Attackers hoping to push competitors from the market dox one other, giving Shadowserver the information it needs to take them out.

**Hacking Team Doxed**

Perhaps one of the most well-known hacker-on-hacker attacks over the last two years, the Hacking Team breach of July 2015 was pure hacktivism. The Italian surveillance company was doxed by a hacker by the handle of Phineas Fisher to shed light on the company's ties with governments with poor human rights records. A purveyor of Remote Control System (RCS) software and zero-day exploit codes, Hacking Team had source code, internal documents, and client lists all exposed in the attack. Included in the exposure was evidence that the firm helped oppressive regimes to better spy on their citizens. Phineas Fisher later wrote a how-to guide that showed his methods, though even early on the exposed documents showed how bad the company's defenses were for a firm that specializes in hacking - in many cases key accounts used "Passw0rd" and "P4ssword" as shared secrets.

**Phineas Fisher Warms Up With Gamma International**

Phineas Fisher didn't come out of thin air. The hacker actually had a warm-up act the previous year when it leaked some 40GB of data about another surveillance company called Gamma International. Known for its FinFisher spyware technology, Gamma had previously been called an "Enemy of the Internet" by Reporters Without Borders for similar ties as Hacking Team to governments in Turkey, Egypt, and Oman.

**Cellebrite Breach Continues Backlash Against Surveillance Firms**

Other hackers are continuing the work of Phineas Fisher. Just last month, an Israeli firm that makes mobile phone hacking devices was hit with a 900 GB breach that included customer information and

technical data about the company's product. In this instance, the attacker didn't go public, but had been exchanging information in IRC chat rooms and with the media. Similar to the other hacking firms, Cellebrite's breached information suggested relationships with governments that have less than sterling human-rights records.

**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 Technology, Innovation and Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca



**********