Security News Digest
February 07, 2017

February is the month of Valentine's Day, with stores replete with cards, candy and flowers. Whether you love Valentines or find it all way too much, take the Love Security - Love Your Data Quiz.

This Week – February 8th to 10th, the **18th Annual Privacy and Security Conference** is being held in Victoria. Leading experts, thought-leaders, academics, and specialists in privacy and security will be engaging in stimulating intellectual presentations and discussions. In the spirit of this exciting event, is the following article on "filter bubbles". The article is presented in full – the rest of the SND follows.

We All Live in a Bubble. Here's Why You Step Out of It, According to Experts

http://globalnews.ca/news/3225274/we-all-live-in-a-bubble-heres-why-you-step-out-of-it-according-to-experts/

Picture this, you're online scrolling through your Facebook newsfeed and this is what you see: 'Keep them out! Finally nice to see there's accountability in this country #travelban.' Or you see this: 'How can this even be legal? Families are being torn apart #travelban.'

Depending on your ideologies and opinions, you might see one or the other. But usually not both. That's according to experts who say you're living in an online bubble. When the news of Donald Trump's executive order to ban the entry of people from seven Muslim-majority countries broke, the online talk became divisive and filtered, said Mary Charleson, a marketing and media strategist who teaches at Capilano University in Vancouver.

Social media platforms like Facebook or Instagram use algorithms to get you to spend time on your feeds. They immerse you with content that they believe you'll like, Charleson explains. "You live in a sea of sameness. You're getting constantly reinforced with views that are like your own and you're not being challenged by opinions different than your own, and that's a real danger," Charleson told Global News. If you're not being challenged in your thoughts, then you are not aware of what others who are different than you are thinking, she added. "And you are not being open to perhaps having your own views changed or altered."

In a term coined by Internet entrepreneur, Eli Pariser, *we live in "filter bubbles," an ideologically isolated and self-confirming online world*. And some psychologists have argued it can extend beyond to social gatherings, the books you read, the neighbourhood you live in and the people you surround yourself with. Your comfort zone, as Robert M. Yerkes and John D. Dodson suggested back in 1908 in a famous psychological experiment with mice, is a behavioural state that minimizes your stress and risk with a situation. By surrounding yourself with what you know - creating patterns and routines - you're in the ultimate safe haven. When it comes to the online world of cat memes, avocado toast and #motivationmonday, experts say we get sucked in and *there's a "dangerous unintended consequence."*

"Your filter bubble is kind of like your own personal and unique universe of information that you live in online. And what is in your filter bubble depends on who you are and what you do, *but the thing is you don't decide what gets in and more importantly, you don't actually see what gets edited out*," said Pariser, a left-wing political and internet activist who wrote *The Filter Bubble.* Pariser argues that we don't get exposed to information that could challenge or broaden our worldview. *Algorithmic filters on Google's search engine or social media newsfeeds are mainly looking at what you click or like. So the latest on Justin Bieber might trump information on Syria. "Instead of a balanced information diet, you could end up surrounded by information junk food," Pariser said, making the analogy that we all need our information vegetables just as much as our information desserts*.

But a sweet lemon meringue pie in the figurative sense, is not always more tempting than broccoli, one study suggests. Researchers at Oxford, Stanford and Microsoft Research analyzed how 50,000 Americans interacted online. What they found was that although social media was distancing people with different partisan positions, it was also increasing people's exposure to material "from his or her less-preferred side of the political spectrum." Regardless of opposing views, Charleson said we should be

using social media as tool and not a crutch. "There is a real beauty in browsing because you stumble upon things that perhaps you weren't looking for…or you stumble upon an opinion that challenges your own." She suggests poking your heads out of your social media bubble, or even news outlets you regularly read. *Proving yourself right is not as valuable as examining other views and theories as alternatives*, she said, which in the end is important for civil discourse and democracy. "Democracy is fragile. In the west we tend to assume that democracy will be here forever, and that freedom of speech, and the right to protest, and the right to having opposing views and acceptance of others who are unlike us is a given," Charleson said. But it's disarmingly easy for all of that to possibly go away, she added, unless we pop the bubble.

Canadians' Internet Data Affected As Trump Cancels Privacy Rules

http://www.huffingtonpost.ca/2017/01/31/internet-privacy-canada-trump-executive-order_n_14500862.html?utm_hp_ref=canada

[Jan31] *Activists and academics are calling on Canada's privacy commissioner to investigate after an executive order from President Donald Trump last week stripped Canadians and other foreigners of the limited digital privacy protections they had enjoyed previously in the U.S. The move could affect up to 90 per cent of Internet traffic in Canada, which is commonly routed through the U.S.* In an order signed last Wednesday, *Trump declared that federal agencies "shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."* The Department of Homeland Security in 2007 extended certain Privacy Act protections to include "non-U.S. persons including visitors and aliens." The original Privacy Act of 1974 did not cover non-U.S. citizens. *Trump's order "has enormous implications for the privacy of everyone living outside the United States," wrote Michael Geist, a professor of e-commerce law at the University of Ottawa*. "Given the close integration between U.S. and Canadian agencies - as well as the fact that Canadian Internet traffic frequently traverses into the U.S. - there are serious implications for Canadian privacy." *Ronald Diebert of the University of Toronto's Citizen Lab estimated that some 90 per cent of Canadian Internet traffic is routed through the United States*. When it comes to the Internet, "there is no border," he said in 2013.

..Trump's new executive order "has real life implications," consumer activist group OpenMedia said in a statement. "Everything from your financial status, to your medical history, your sexual orientation, and even your religious and political beliefs are exposed." The group said some Canadians "have had their lives ruined" due to inappropriate disclosure of data, even when they did no wrong. "Some have faced career limitations, while others have had to deal with travel restrictions. When health records are wrongfully shared with U.S. border agents, even an encounter with the mental health system 20 years ago can be grounds to deny entry," OpenMedia's statement said. Both OpenMedia and Geist are calling on the office of Canada's Privacy Commissioner to open an immediate investigation.

Feds Lobbying Against Trump's Push for Biometric Screening for U.S. Visitors

http://www.theglobeandmail.com/news/politics/feds-lobbying-against-trump-push-for-biometric-screening-for-us-visitors/article33876246/

Canada has launched a behind-the-scenes lobbying campaign against a push by Donald Trump to subject all visitors to the United States to biometric screening – such as finger-printing, retina scans or facial recognition tests – upon both entry and exit. The U.S. President's call for the stepped-up use of such technology, meant to monitor whether non-Americans are staying in the country longer than permitted, was issued in last Friday's executive order on immigration, but has mostly flown under the public radar amid controversy around a ban on travellers from seven predominantly Muslim-majority countries. *Among Canadian officials, however, it has sparked concerns of massive slow-downs in border traffic of both people and goods, particularly at land crossings* – prompting Public Safety Minister Ralph Goodale to raise the issue during a phone call this week with John Kelly, the new U.S. Homeland Security Secretary, Mr. Goodale's office confirmed.

That conversation appears to have been the start of an ongoing effort by Ottawa to head off the screening plan during a 100-day period in which Mr. Kelly has been tasked – per the executive order – with "expedit[ing] the completion and implementation of a biometric entry-exit tracking system for all travellers to the United States" and reporting back to the President on his progress. The lobbying effort will likely be

aimed not just at Mr. Kelly and other members of Mr. Trump's administration but also at members of Congress, who would need to approve large related expenditures in order for implementation to proceed.

How a Small Team at Google Montreal is Keeping the Internet Safe for More Than a Billion People 

http://business.financialpost.com/fp-tech-desk/personal-tech/how-a-small-team-at-google-montreal-is-keeping-the-internet-safe-for-more-than-a-billion-people

Many Internet users have become familiar with the necessary steps to stay safe from malware and viruses, but *hidden in plain sight beside legitimate online products are now businesses that make money by tricking users into downloading look-a-like offerings which slow down or damage computers*. Hard at work in Google's Montreal office is a small team that's quietly making the Internet a safer place for more than a billion people around the world. *Since 2008, the team - 10 developers and five analysts - has been fighting back against not just viruses and malware, but also the growing problem of unwanted software that sneaks into people's computers*.

"Malware often uses tricks or a vulnerability in a user's machine to get installed, whereas unwanted software often looks very legitimate because users are looking for something they want but it gets on user's machines in a deceptive way," said Nav Jagpal, a software developer on Google Montreal's Safe Browsing team. "Once installed, it does things to your machine that are very disruptive." For example, if someone is looking for a program like Adobe Flash, they might search Google and get a page full of results. Often the first result is correct, but others might look just as plausible and when clicked has a page with the software's name and a big download button. Instead of Adobe Flash, however, *it ends up being software that might permanently change the default search engine or continually cause pop-ups.*

..The Montreal group creates what is essentially a database of known sites or files that are problematic, plus a warning system - often a big, scary-looking screen - that's triggered when a user stumbles across them. The database is continually updated and offered for other companies to use for free, and it's already built into most popular web browsers including Google Chrome, Mozilla Firefox and Apple Safari - *meaning this team of Canadians are already protecting millions globally, regardless of someone using Google's other services or not*. .."The problem is this move toward social engineering, which is convincing people to click 'OK' under some kind of false pretense," said Fabrice Jaubert, the Google software developer who also heads up the Safe Browing team. "Maybe there's something you're led to believe you want, or it's something you truly want but it comes packaged with other stuff and you're not aware you're installing 10 other things, then those things on their own pull other things in like bloatware."

Former Victoria Nurse Pleads Guilty After Massive Child ~~Porn~~ [Abuse] Collection Seized 

http://vancouverisland.ctvnews.ca/former-victoria-nurse-pleads-guilty-after-massive-child-porn-collection-seized-1.3268366

An American man has pleaded guilty in connection with a child ~~pornography~~ [sexual exploitation] bust Victoria police say is one of the most prolific they've ever seen. David Stallcup, who worked as a nurse in Victoria, pleaded guilty to possession of child pornography in a Victoria courtroom on Jan. 18, according to police. A VicPD Internet Child Exploitation investigator began looking into Stallcup's activity in June 2014 after he shared 350 files, all believed to contain child pornography, within a 16-day period. Officers executed a search warrant in the 700-block of Fisgard Street, where he was staying, on March 10, 2015 and discovered over 20 pieces of evidence related to the investigation. *In the end, police seized 775 videos containing 139 hours of material, and 27,000 images*, all confirmed to be child pornography.

Police issued a warrant for Stallcup's arrest in April 2015 but learned he was using a false name, David Robert, and that he was in jail in Oregon.

Investigators also learned Stallcup had been dodging police in different states, from Colorado to Alaska to Montana, on outstanding charges, creating false identities to evade them. At some point, he obtained a Registered Nurse certificate in the Northwest Territories and *police said he had been working at a local Victoria facility. The B.C. College of Registered Nurses released a statement in May 2015 that a man named David Turner Robert was working as a RN for a B.C. employer despite not having practicing registration*. Police worked with Oregon officials to have Stallcup extradited to Canada on Nov. 16, 2016.

Last month an Oregon newspaper reported that Stallcup, using the name David Robert Rineheart, was running from authorities for more than a decade before he was caught. "I don't want to run anymore," he

told a judge, as reported by The Oregonian. He now remains in Victoria police custody and will soon face sentencing for the guilty plea.

Police in Delta, B.C., Using GPS Darts to Track Vehicles That Flee 

https://www.thestar.com/news/canada/2017/01/13/police-in-delta-bc-using-gps-darts-to-track-vehicles-that-flee.html

A police department in British Columbia's Lower Mainland is using technology that looks like it is taken from the latest Batman movie to track fleeing vehicles. Police in Delta have begun using GPS projectiles fired from the grilles of their vehicles to track those who won't stop. With an increasing number of vehicles fleeing officers, Delta police say they began researching options to deal with the problem early last year. The police department began working with StarChase Pursuit Management Technology, which has developed a GPS projectile that officers can fire at a vehicle to track its location until it stops. The Delta Police Foundation agreed to fund the project and over the past several months, the police department began working with the company to equip eight vehicles with the technology.

The department says the projectiles are fired from a compressed air launcher attached to the grill of a police vehicle. It has been tested, officers have been trained and the police department says the technology is in place to use. "We are now looking forward to seeing this technology in action," police Chief Neil Dubord said in a statement. "However, we do recognize there is no one tool that serves as a 'silver bullet' to solve any one issue. I do believe it is incumbent on us to employ advanced technology options that may assist us in our efforts to be effective at doing our job while mitigating risk to the public." He says the police department will assess the effectiveness of the projectiles over the next year in tracking fleeing vehicles.

US Border Agents Checking Facebook Profiles, Lawyer Says

https://www.cnet.com/au/news/border-patrol-agents-checking-facebook-profiles-trump-immigration-ban/

Should what's on your Facebook page be a factor in determining whether you're allowed to re-enter the United States? That's a question to ponder in the wake of President Donald Trump's ban on immigration that began on Friday [Jan13]. Border patrol agents are checking the Facebook accounts of people who are being held in limbo for approval to enter the US, according to a Saturday tweet by immigration lawyer Mana Yegani that was spotted by The Independent. *"US border patrol is deciding re-entry for green card holders on a case by case basis - questions about political views, checking Facebook, etc,"* Yegani's tweet writes. The ban currently applies to immigrants from seven countries, leading tech executives from almost every major company - including Apple, Google, Facebook and Netflix - to decry the move as "un-American." *Yegani, who is a member of the American Immigration Lawyers Association, told CNET that checking phones has been reported by other lawyers as part of the vetting process. "The CBP going through passengers phones from the seven banned countries happens when the individual is interrogated (put under extreme vetting)," Yegani said.*

Incidentally, that's in line with a warning from the Electronic Frontier Foundation that in general, anyone can have their phone checked while at the border. [This has been true when entering Canada for some time.] Yegani told The Independent that she and other lawyers have been fielding calls from people who are already cleared to live in America, but are getting stuck at the border regardless. "These are people that are coming in legally. They have jobs here and they have vehicles here," Yegani said in the report. The White House did not immediately respond to a request for additional comment.

Anonymous Hacker Took Down Over 10,000 Dark Web Sites; Leaked User Database

http://thehackernews.com/2017/02/dark-web-hosting-hacked.html

Dark Web is right now going through a very rough time. Just two days ago, a hacker group affiliated with Anonymous broke into the servers of Freedom Hosting II and took down more than 10,000 Tor-based .onion dark websites with an alarming announcement to its visitors, which said: "**Hello, Freedom Hosting II, you have been hacked.**" *Freedom Hosting II is the single largest host of underground websites accessible only through Tor anonymising browser that hosts somewhere between 15 and 20 percent of all sites on the Dark Web, anonymity and privacy researcher Sarah Jamie Lewis estimated*.

Besides defacing all Dark Web sites hosted on Freedom Hosting II with the same message and stealing its database, the hackers also demanded a ransom for 0.1 Bitcoin (just over $100) to return the compromised data to the hosting service.

Now, it has been reported that the stolen database from Freedom Hosting II has publicly been released online to a site hosted on the Tor network, which includes the email details of nearly 381,000 users, 'Have

I Been Pwned' tweeted. According to the Anonymous hackers, more than 50 percent of all files hosted on Freedom Hosting II servers were related to child pornography. Those illegal websites were using gigabytes of data when Freedom Hosting II officially allows no more than 256MB per site, the Anonymous hacker claimed. In addition to dark sites user details, the data dump also contains backups of website database, most of which are based on popular, free, open source content management systems and forums like WordPress and PHPBB. *In an interview with Motherboard, an Anonymous hacker who claimed responsibility for the hack said this was his first hack ever, and he never intended to take down the hosting provider. But when he allegedly discovered several large child pornography websites using more than Freedom Hosting II's stated allowance, he decided to take down the service. The hacker claimed to have downloaded 74GB of files and a users' database dump of 2.3GB*.
Lewis has been analyzing the leaked data and reported that the database contains Dark Web users' numerous plain text emails, usernames, and hashed passwords from forum websites hosted by Freedom Hosting II. While it's bad news for users who joined one of those forums providing their genuine personal details, law enforcement would be happy, as in a separate case, the FBI used location-tracking malware to infiltrate Dark Web porn sites and track individual users.

Dark Web Recruiters Target Insiders and Employees

https://www.infosecurity-magazine.com/news/dark-web-recruiters-target/

The cyber-risk from insiders - employees and contractors who have valid access to enterprise networks, a la Edward Snowden - is on the rise, in part due to cybercriminals recruiting them to help steal data, make illegal trades or otherwise profit. According to a report from RedOwl and IntSights, the recruitment of insiders within the Dark Web is active and growing, with forum discussions and insider outreach nearly doubling from 2015 to 2016. *Sophisticated threat actors use the Dark Web to find and engage insiders to help place malware behind an organization's perimeter security. Insiders then use these underground forums to "cash out" on their services through insider trading and payment for stolen credit card information.*
The puppet-masters are also able to arm insiders with the tools and knowledge necessary to help steal data and commit fraud, among other acts, and also to cover any tracks. In one instance, a hacker solicited bank insiders to plant malware directly onto the bank's network. This approach significantly reduces the cost of action as the hacker doesn't have to conduct phishing exercises and can raise success rates by bypassing many of the organization's technical defenses (e.g. anti-virus or sandboxing). The lures are significant. On one forum, the attacker explained the approach to a potential collaborator, indicating that he needs direct access to computers that access accounts and handle wire transfers, and that he offers to pay "7 figures on a weekly basis" for continued access. *What it means for businesses is that any insider with access to the internal network, regardless of technical capability or seniority, presents a risk*. The report recommends that risk management teams should join the growing number of organizations that are actively building insider threat programs. Ironically, 80% of security initiatives today focus on perimeter defenses, while fewer than half of organizations budget for insider threat programs.

Vizio Televisions Secretly Tracked Viewership in U.S. Without Consent

http://www.cbc.ca/news/business/vizio-tv-spying-ftc-1.3970339

Smart-television maker Vizio has agreed to pay $2.2 million US to authorities *to settle allegations that its televisions collected information on what 11 million viewers were watching, without their consent.*
According to the settlement of a lawsuit with the U.S. Federal Trade Commission and the Attorney General for New Jersey, *California-based Vizio has been collecting information on viewing habits from millions of unwitting customers who have bought one of the company's smart televisions since 2014*. "On a second-by-second basis," the FTC says, *"Vizio collected a selection of pixels on the screen that it matched to a database of TV, movie, and commercial content." In the industry, such information is known as "automatic content recognition" or ACR*, and in a statement to CBC News, Vizio Inc. confirms that the practice is not currently used on their TVs in Canada.
In the U.S. however, millions of devices are involved in a system whereby customers unwittingly signed up when they opted into the company's "Smart Interactivity" program, which gives them program suggestions based on their viewing habits. *But behind the scenes, the company was cross-referencing those hundreds of billions of daily data points against cable services, set-top boxes and even DVDs for a precise picture of what those 11 million TV sets were being used for. "All of this, the FTC and AG allege,*

was done without clearly telling consumers or getting their consent," FTC attorney Lesley Fair said in a blog post announcing the settlement. *The company also compiled detailed information on people who bought their TVs, including their sex, age, income, marital status, household size, education level, home ownership, and household value. Vizio then took that data and sold it to marketers eager for it*.

How to Turn Off Snooping Smart TV Features

http://www.consumerreports.org/cro/news/2015/03/how-to-turn-off-smart-tv-features-that-invade-privacy/index.htm
This article from 2015, which might or might not be useful for you, shows how to turn off the automatic content recognition (ACR) systems found on televisions from Samsung, LG, and Vizio.

'Can You Hear Me?': Don't Say 'Yes' in New Telephone Scam

http://globalnews.ca/news/3221328/can-you-hear-me-dont-say-yes-in-new-telephone-scam/
Telemarketing calls are annoying enough, but now *authorities are warning consumers about the risk of having their words on the phone used against them*. It's called the 'Can you hear me' scam and reports in the U.S. suggest it's growing in popularity as fraudsters use it to try to get your money. "He said, 'This is Tony Moore, can you hear me clearly?'" Gail Worth, a homeowner who got one of the calls, said. She immediately hung up, but *had she said, 'Yes,' her answer might have been edited and used to prove she had willingly subscribed to a service contract or to buy an unwanted product. Telemarketing organizations typically call back consumers for verification calls and rely on those to ensure the consumer pays.*
"Keep in mind, a scammer may already have gotten their hands on some of your personal information, such as credit card numbers, which they can use in tandem with your recorded affirmation to push through charges," warned the Better Business Bureau of Southfield, Mich. It recently issued a warning to businesses and consumers. *In some cases, the calls may be placed by a live person. But frequently, the calls are automated*. "We have seen these robocalls get more sophisticated and even mimic things like background noise to convince you, as the recipient of the phone call, that it is a real person," Ryan Kalember, senior vice president with the California cyber-security consulting company Proofpoint, said. *"If you answer, 'Yes,' there's a possibility that the scam artist behind the phone call has recorded you and will use your agreement to sign you up for a product or service and then demand payment. If you refuse, the caller may produce your recorded 'yes' response to confirm your purchase agreement," the BBB cautioned*. The U.S. Federal Trade Commission warns people to never provide personal information over the telephone and to hang up if they answer a pre-recorded sales call. So far, there are no reports any Canadians have been defrauded as a result of the scam.

2.5 Million Xbox and PlayStation Gamers' Details Hacked

https://www.cnet.com/au/news/2-5-million-xbox-and-playstation-gamers-details-hacked/
Uh-oh, Xbox and PSP gamers - a lot of you may have had your personal details hacked. *A data breach of two popular gaming forums has exposed the account details of 2.5 million users, potentially opening up their other online accounts to attack by hackers. The Xbox 360 and PSP ISOs, which host game download files, were hacked in September 2015*. That's according to security expert Troy Hunt's Have I Been Pwned? website, which tracks data breaches. Even if users didn't have financial details stored on the sites, the information could be used to break into other sites if users have the same password for different accounts. "Often people using seemingly low-security websites don't enforce good password security because it's not a financial target," said Mark James, IT security specialist at ESET, "But all data has a value and will be reused for other purposes. Every website should be treated as unique and require different passwords with a mix of usernames if possible." *"Breach after breach has shown that using the same username and password for multiple sites is a bad idea,"* said security expert Jonathan Sander of Lieberman Software. "If the Xbox and PSP crew haven't learned that they can't use the same email and password on every service by now, then likely it is game over for their personal data."

PCI Council Updates E-Commerce Guidance for Firms

https://www.infosecurity-magazine.com/news/pci-council-updates-e-commerce/
Industry body the Payment Card Industry Security Standards Council (PCI SSC) has updated its best practice guidelines for securing e-commerce transactions, *as more fraud migrates online. The Best Practices for Securing E-commerce guidance replaces the previous PCI DSS E-commerce Guidelines, published back in 2013. As such, there's new info in there for online merchants explaining SSL/TLS, how to select a certificate authority (CA), the different types of certificates out there and a list of questions*

merchants can ask service providers on digital certificates and encryption. The PCI SSC has mandated, for example, that all online merchants use TLS 1.1 encryption or higher by June 2018.
There's plenty of information on how to achieve PCI DSS validation and a chart showing the level of complexity for different types of implementation. "Securing the e-commerce environment continues to be critically important. According to several sources, e-commerce sales almost hit $2 trillion globally in 2016 with double-digit growth forecasted for several years to come," explained PCI CTO Troy Leach. *"We also know that fraud is moving to card-not-present (CNP) environments with the implementation and acceptance of EMV chip, making e-commerce merchants a prime target for criminal hackers. The Council is uniquely positioned to help merchants since we are aware of the changing threat landscape of e-commerce environments." Best practice tips from the PCI SSC include gaining visibility into the location of all data; eliminating any data that's not needed; and security training for all staff*. Many smaller businesses will outsource payment acceptance to a third party, Leach claimed. "Still, those merchants should be aware of how their e-commerce solution accepts payments, specific risks to their customer's cardholder data and best practices that they or their service providers should be following to mitigate those risks," he added. "That is what is intended by this guidance."

Two Arrested in UK for Hacking DC CCTV Cameras Before Trump Inauguration [follow-up from last week]

https://www.hackread.com/hackers-arrested-for-hacking-cctv-cameras/
On 12th January 70% of CCTV cameras in Washington DC were hacked with ransomware, that was just eight days before President Trump's inauguration on 20th January. Now, authorities in London, UK have arrested two hackers on suspicion of hacking those CCTV cameras. *The arrest took place on 20th January but the news about their detention has only been shared with media now*. According to The Sun, one of the arrested hackers is a Swedish woman and other a British man. The hacking feat took the city by shock since it posed a massive security threat considering the importance of the presidential inauguration and the possibility of terrorist attacks on the event. It must be noted that the hackers were able to hack 123 of the total 187 network video recorders installed inside the CCTV devices. The cameras could not record anything for more than 48 hours. The hackers also demanded ransom money which was rejected by the DC Police but it forced a major reinstallation spree across the city.

Hack Attack on Norway's Labour Party Revealed; Russia Allegedly Targeted Servers

https://hotforsecurity.bitdefender.com/blog/hack-attack-on-norways-labour-party-revealed-russia-allegedly-targeted-servers-17638.html
Russia allegedly hacked Norway's Labour Party parliamentary group in the fall of last year, according to the party's leader, Jonas Gahr Store, cited by International Business Times. Store said the party's electronic communications had also been previously compromised, according to the report. "It is primarily Russia that has the intentions and capacity to do intelligence activities with big damage potential for Norway and Norwegian interests," the annual report from the Police Security Service (PST) reads, as cited by The Barents Observer. "I can confirm that we are informed by PST that Labour's parliamentary group was subjected to an attempted digital attack by a group that PST ties to foreign intelligence," Store's spokesperson, Camilla Ryste, said in a statement to media outlet Nettavisen. The attack was believed to be in line with the hacking of the Democratic National Committee last year, which U.S. intelligence agencies have said was at the behest of Russian President Vladimir Putin, journalists say. This week, the Czech Republic also blamed a 'foreign state' for a 'very sophisticated' cyberattack against top government employees. As HotForSecurity [Bitdefender] noted, dozens of email account were targeted by a cyberattack allegedly carried out by a 'foreign state', according to the foreign ministry in the Czech Republic, cited by politico.eu. The minister's own email was also targeted by hackers. Authorities are also investigating whether the unexpected power outage in Ukraine's capital could be the latest in a series of hacking attacks that have struck the country's electric grid and financial infrastructure in the last year, as HotForSecurity also noted.

****

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

****