# Security News Digest
# June 27, 2017

**The Internet of Things? What things?**
**Take the Internet of Things Quiz and find out!**
[Lots of interesting reading in today's Digest, so get a beverage, relax and scroll on through…something for everyone!]

## June 30 is Social Media Day!

http://mashable.com/smday/

On June 30, 2010, Mashable launched Social Media Day as a way to recognize and celebrate social media's impact on global communication. Today, social media is the heart of global communication; and since its inception, Mashable's been using social media to connect between cultures, movements and super-fandom. *While every day is essentially Social Media Day, June 30th, 2017 marks the eighth-annual official global celebration*. No matter where you live, you can celebrate! Learn how to make Social Media Day official in your city, and follow @MashSMDay on Twitter for #SMDay updates.

## Shaw Go WiFi Helps Connect Canadians for Canada Day

http://globalnews.ca/news/3558013/shaw-go-wifi-helps-connect-canadians-for-canada-day/

A service usually only available to Shaw customers will be available for everyone in Canada to celebrate the nation's birthday. **Shaw announced Monday [June26] that it's providing complimentary access to its Shaw Go WiFi service between June 26 and July 3, meaning anyone can access the network regardless of if they are Shaw customers or not**. "This Canada Day long weekend, people want to share in the festivities with their family and friends," Chethan Lakshman, vice president of external affairs for Shaw Communications, said in a news release. "Whether you're posting pictures, looking up a place to go or getting directions, Shaw Go WiFi will help keep people connected while saving on cellular data usage." *The Shaw Go WiFi guest network has over 80,000 hotspots and can be accessed by selecting "ShawGuest" from the list of available networks on any WiFi-enabled device*.

## Snapchat's New Map Feature Could Be Tracking You All The Time

http://globalnews.ca/news/3554398/snapchats-new-map-feature-could-be-tracking-you-all-the-time/

Snap Inc., owner of the popular social media app Snapchat, recently released a new feature that has some privacy advocates concerned. Snap Maps was rolled out to several countries, including Canada, on Friday, and allows users to display their location on a map while using the app. If you choose to use this feature, Snapchat will track your location and share it with select friends, by placing your avatar in a specific location on the map. *However, on its lowest privacy settings, this feature is designed to broadcast your location to everyone on your friends list whenever you open the app*. *While there is the option to opt out of this feature, otherwise known as "Ghost Mode," critics have maintained in the days since it was released that Snap Map could be used to stalk or bully others*.

The child safety group Childnet International released a statement on how to safely use and enjoy Snap Maps: "It is important to be careful about who you share your location with, as it can allow people to build up a picture of where you live, go to school and spend your time." The group encourages people not to share their location, especially with strangers, because Snap Map shares where you are to "a precise pinpoint on a map."

*Snapchat isn't the only social media firm to be criticized for its location tracking practices*. As reported by the Guardian, Twitter allows people to add their location to tweets, while Facebook's check-ins and Messenger's "share location" function also allow people to track their contacts. Furthermore, the world's most popular mobile mapping app, *Google Maps, has also been called out for being less than forthcoming about how active its location tracking service really is*. According to a report by PC Mag, *Google Timeline, introduced by Google in 2015, allows Google Maps to keep track of every step you take, as long as your phone's location services are turned on*.

But for those individuals that just received Snapchat's new update, it is possible to modify the service or entirely turn it off. Here's how. (1) Navigate to your settings, which you can access from the new map. (2) Scroll down to "Who Can…" => See My Location. (If you navigated from the map, you'll automatically be taken here). (3) Choose who can see your location, or swipe "Ghost Mode" on to disable sharing your location to anyone. [Overall security/privacy message: Location Services? Do you need it? Do you need it all the time? Do you know who can see your location, what you have consented to? Do you know how to turn it off? Use it when you need it, the way you choose to use, and otherwise, turn it Off.]

## Average Data Breach Could Still Cost a Canadian Organization Millions: Report

http://www.itworldcanada.com/article/average-data-breach-could-still-cost-a-canadian-organization-millions-report/394171

*The average cost of a data breach suffered last year by 27 Canadian companies was $5.78 million, or $255 per lost or stolen record*, according to a study released Tuesday [June20]. It was the third annual report, paid for by IBM and conducted by the Ponemon Institute, *part of a survey of 419 breached organizations in 11 countries and two regions*. The good news is that the Canadian numbers represent a four per cent decrease in the total cost of a data breach among the group studied, and a nine per cent decrease in the cost per lost or stolen record, compared to the 2015/2016 study period.

The bad news is it's still a lot of money. Of all nations studied the Canadian group had the second highest costs. *One important take-away from the report is how being proactive can reduce the cost of a breach per record*, Raz Ghanaghounian of IBM's X-Force incident response and intelligence services team said in an interview Tuesday. *For example, for the group studied having an incident response team cut the average cost by $24, extensive use of encryption by almost $22 and employee training by almost $15* (see graph below). *CISOs also need to impress on the company the value not only of having the tactical team respond to a breach but also strategic (board and management) members as well*, he said. And many decisions - such as how to make breach notifications, who to notify, when to notify law enforcement.. - need to be made before an incident and not at the last minute.

The costs are based on estimates provided by participating organizations. *The number of breached records per incident this year ranged from 4,300 to 69,844 and the average number of breached records was 21,750. Organizations with data breaches involving more than 100,000 compromised records weren't included because few Canadian breaches are that large*.

A breach is defined as an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk - either in electronic or paper format.

<u>The data also showed a number of interesting pieces of information that should resonate with CISOs, CIOs and boards of directors:</u>

- **Acting fast pays:** Canadian organizations that contained a breach in less than 30 days saved $1.79M compared to those that took longer ($4.88M vs $ 6.67M);
- **It still takes too long:** *On average, Canadian organizations in the group took 173 days to identify a breach, and 60 days to contain it*. Still, that was better than the global average. Of all 419 organizations studied, the days to identify the data breach dropped from an average of approximately 201 in 2016 to 191 days and the average days to contain the data breach from 70 to 66 days. *The report's authors attribute these improvements to investments in such enabling security technologies as security analytics, system information and event management (SIEM) software, enterprise-wide encryption and threat intelligence sharing platforms*;
- **The more records lost, the higher the cost of the breach:** In this year's study, the cost ranged from $3.81 million for data breaches involving 10,000 or fewer records to $7.25 million for the loss or theft of 25,001 to 50,000 records;
- **Investments in** incident response teams and plans, extensive use of encryption, employee training programs, board-level involvement or participation in threat sharing **were shown to reduce the per capita and total cost of data breach**;
- **In Canada, certain industries in the 27 organizations studied had higher data breach costs**. Services, financial services and technology companies had a per capita data breach cost above the mean of $255. Public sector, hospitality and transportation companies had a per capita cost well below the overall mean value. Note, however, that the small sample size means this can't be generalized for the sectors at large.

- Forty-eight per cent of incidents involved a malicious or criminal attack, 30 per cent involved negligent employees and 22 per cent involved system glitches, which includes both IT and business process failures.

## Canada and China Sign No-Hacking Agreement to Protect Trade Secrets

http://www.cbc.ca/news/politics/canada-china-no-hacking-agreement-1.4178177

Canada and China have agreed not to engage in state-sponsored hacking of each other's trade secrets and business information. The two countries reached the agreement during a meeting last week that was part of their new high-level national security dialogue. *"The two sides agreed that neither country's government would conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors,"* says a communique from the Prime Minister's Office. The two sides also had "candid" discussions about a possible extradition treaty, said the statement - something China wants, but that Canada has said is a long way off. Prime Minister Justin Trudeau and Chinese Premier Li Keqiang have deepened the political engagement between the two countries with regular "dialogues" such as the security one that took place last week in Ottawa. The two leaders also spoke by phone last Monday.

Daniel Jean, Trudeau's national security adviser, led the talks with Wang Yongqing, the secretary-general of China's Central Political and Legal Affairs Commission. *Cybersecurity was one the many topics on the agenda*, along with counter-terrorism, combating organized crime and regional security issues such as the crisis in Syria and North Korea's nuclear sabre-rattling. The government statement says the two sides also discussed "judicial and rule of law issues." John McCallum, the former immigration minister now serving as Canada's ambassador to China, has previously flagged judicial issues as an area of disagreement between the two as Canada tries to deepen its economic ties. "We disagree on the death penalty," McCallum told a House Commons committee in March. "We disagree on some aspects of the rule of law and privately and publicly on how the Chinese government treats human rights advocates."

## Experts Debate Value of China's Promise to Canada Not to Back Industrial Theft

http://www.itworldcanada.com/article/experts-debate-value-of-chinas-promise-to-canada-not-to-back-industrial-theft/394436

[Howard Solomon at IT World Canada gathered many perspectives and analyses for this discussion article on countries dealing with state-sponsored attacks. Here are a couple of comments – see article for the full discussion.]

China's promise not to conduct or knowingly support cyber theft of Canadian corporate intellectual property for its companies is worthless, says a Canadian expert. "I anticipate that the People's Republic will continue to conduct state driven cyber-espionage, that Canadian Intellectual property will continue to be stolen by state organs of the People's Republic, by Chinese universities, by Chinese businesses as well as individuals stealing for profit, and that the People's Republic of China will loudly denounce any finger pointing in their direction as unsubstantiated and that there is no evidence," said David Swan, the Alberta-based director of cyber intelligence at the Centre for Strategic Cyberspace and Security Science. China signed a similar document with the United States in 2015, he said, but it made no difference.

..Experts note the promise doesn't cover governments spying on each other, so, for example, it wouldn't have covered the alleged theft of U.S. federal employee data by China in 2015 at the Office of Personnel Management.

*On the other hand* Toronto lawyer Imran Ahmad, who is also a member of the advisory board of the Canadian Advanced Technologies Alliance's cyber security council, called the move "a step in the right direction. If we look at the similar U.S.-China agreement signed under President Obama, there's a general consensus that there has been a drop in cyber theft of corporate R&D (research and development) and intellectual property. If the same can be accomplished with the Canadian agreement, I think this is a good step forward. Also, I think the Canadian government was very good in leveraging the upcoming trade talks with China in order to get this agreement in place."

## Supreme Court Rules Facebook Can't Contract Out of B.C. Privacy Law

http://www.michaelgeist.ca/2017/06/supreme-court-rules-facebook-cant-contract-b-c-privacy-law/

[Note: the full article with legal arguments appears in Michael Geist's column at the link above. Here is the summary from the IAPP Daily Dashboard publication.]

The Supreme Court of Canada rejected Facebook's attempts to stop a privacy class-action lawsuit in British Columbia from moving forward, Michael Geist reports in his blog. *Within the forum selection clauses in Facebook's online contract, it specifies all legal actions against Facebook must be brought in California. The plaintiff in the case, involving the now-defunct Facebook "sponsored stories" program, argued online terms and conditions cannot override domestic privacy rights*. While the trial judge agreed with the plaintiff, the British Columbia Court of Appeal ruled Facebook's terms were "valid, clear, and enforceable" and halted the case. The Supreme Court, however, overturned the decision of the appeals court, focusing on the Facebook-consumer power dynamic and the ephemeral nature of "consent" in the online environment, and emphasizing privacy as a "quasi-constitutional right." "Canadian courts have a greater interest in adjudicating cases impinging on constitutional and quasi-constitutional rights because these rights play an essential role in a free and democratic society and embody key Canadian values," the ruling states.

Readers: **Please Note that the Petya (GoldenEye) massive global ransomware attack is an ongoing event** that has been evolving throughout the day. Here is a story that captures what has been happening. The media world-wide continues to provide updates. If you want the latest, do an internet search on "Petya".

## Global Petya Ransomware Attack: Update 2

https://www.scmagazine.com/global-petya-ransomware-attack-update-2/article/671372/

Petya ransomware continues to spread rapidly across the globe impacting multiple corporations and utilities and it has just been revealed that the attacker's email address needed to pay the ransom has been shut down eliminating that possibility for any victim.

The attack looks as if it may have started in Ukraine, where banks, energy companies, an airport and its metro network were affected, according to a Forbes report and additional sources. Outside the Ukraine, infections have also apparently hit Danish shipping and energy company Maersk, British advertiser WPP and Russian oil industry company Rosnoft, the report continues. ..The Chernobyl nuclear power plant in the Ukraine was also hit, according to the Mirror. The plant was destroyed in a meltdown in 1986, but is still being decommissioned.

The German email provider Posteo reported it has shut down the email address that the Petya attackers set up to receive ransom payments. [see the next article below] "This email address [wowsmith123456@posteo.net] is displayed in Petya's ransom note as the only way to contact the Petya author. Victims have to pay the ransom and send an email with their Bitcoin wallet ID and infection key to the author," Bleeping Computer reported, which means there is no longer any method in place for those with locked files to have them decrypted.

Nick Bilogorskiy, Cyphort's senior director of threat operations, has issued **an early breakdown of how the ransomware is operating and how it differs from WannaCry. "This is what Petya is, an older ransomware family that has been given a new life by embedding a way to self-replicate over SMB using Eternal Blue exploit,"** he said, adding so far nine people have forked over the $300 ransom.

…Reports from a number of security companies allege that the ransomware is locking up systems globally, including pieces of critical infrastructure and government bodies in Ukraine. The Kiev Metro system, "several chains" of Ukrainian petrol stations and the country's deputy prime minister all appear to have been hit. Kiev's Boryspil airline says that could cause flights to be delayed, the BBC reports.

Other companies include Russian oil company Rosneft and shipping operator Maersk, which confirmed on Twitter that its IT systems were down across "multiple sites" thanks to a cyber-attack. Cyber-security firm, Recorded Future claims that it is now starting to see US victims too.

…A spokesperson for the National Cyber Security Centre issued a statement saying, simply, "We are aware of a global ransomware incident and are monitoring the situation closely." NHS Digital said on Twitter that "There are no known significant cyber security threats affecting health." Last month the global WannaCry campaign took out 48 NHS trusts, leaving hospitals all over the UK paralyzed. *Much like WannaCry, GoldenEye appears to be quite cheap, charging a relatively meagre US$300 (£234) for decryption. The bitcoin wallet it is directing victims to has already received 13 transactions*.

It is not yet known what the propagating component is, but it is suspected to be wormable. [this has been confirmed] Javvad Malik, security advocate at AlienVault, told *SC Media UK* that **it appears to be "spreading via EternalBlue, the NSA vulnerability that was leaked by ShadowBrokers and spreads via the SMB1 protocol." EternalBlue was the same exploit that allowed WannaCry to spread to hundreds of thousands of endpoints in over 150 countries in a matter of hours**.

**Though a fix for the vulnerability has been released several times, it appears that many have not yet applied it, as evidenced by WannaCry recurrences in Honda factories last week**. F-Secure's CRO, Mikko Hypponen has taken to twitter to admonish those who have not yet patched and left themselves open to this kind of attack. New Petya uses the NSA Eternalblue exploit. So Wannacry was not enough of a wake-up call. You would think everybody would be patched by now.
The GoldenEye variant of Petya emerged in December last year, after a period of dormancy. Its first recorded attacks were aimed at German-speakers with **phishing emails** (!!!) loaded with malicious Microsoft Office documents.
*GoldenEye has two level of encryption. One encrypts files that are actually on the computer and the other goes after NTFS, which prevents the victim's computer from retrieving stored information*. After the targeted machine has been encrypted, GoldenEye reboots it so it cannot be used until the ransom is paid.
This particular variant apparently earned US$1 billion (£783 million) in 2016. - Please check back with SC Media (at link above) as we continue to follow this story.

## Hacker Behind Massive Ransomware Outbreak Can't Get Emails from Victims Who Paid

https://motherboard.vice.com/en_us/article/new8xw/hacker-behind-massive-ransomware-outbreak-cant-get-emails-from-victims-who-paid

**A German email provider has closed the account of a hacker behind the new ransomware outbreak, meaning victims can't get decryption keys.** On Tuesday, a new, worldwide ransomware outbreak [Petya] took off, infecting targets in Ukraine, France, Spain, and elsewhere. The hackers hit everything from international law firms to media companies. *The ransom note demands victims send bitcoin to a predefined address and contact the hacker via email to allegedly have their files decrypted. But the email company the hacker happened to use, Posteo, says it has decided to block the attacker's account, leaving victims with no obvious way to unlock their files*.
"If you see this text, then your files are no longer accessible, because they are encrypted," the ransom text reads. "Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service." From here, the hacker tells victims to send $300 worth of bitcoin. But to determine who exactly has paid, the hacker also instructs people to email their bitcoin wallet ID, and their "personal installation key." This is a 60 character code made up of letters and digits generated by the malware, which is presumably unique to each infection of the ransomware. That way, the hacker can release the specific key needed to unlock that individual victim's files. That process is not possible now, though.
*"Midway through today (CEST) we became aware that ransomware blackmailers are currently using a Posteo address as a means of contact," Posteo, the German email provider the hacker had an account with, wrote in a blog post. "Our anti-abuse team checked this immediately – and blocked the account straight away. We do not tolerate the misuse of our platform: The immediate blocking of misused email accounts is the necessary approach by providers in such cases."*
Just to be super-clear, Posteo clarified, "Since midday it is no longer possible for the blackmailers to access the email account or send emails," and "Sending emails to the account is no longer possible either." In other words, victims allegedly cannot contact the hacker by email, nor send the details necessary to unlock their files.
*In an email to Motherboard, Posteo said, "Please make no speculations about how high the chances are to decrypt files locked by ransomware if you pay a criminal."* The company did not respond to questions asking how victims can contact the hacker. At the time of writing, around 20 victims have sent just under $5,500 to the hacker's bitcoin address.

## Government Websites in 3 States Hacked with ISIS Messages

http://www.cnn.com/2017/06/26/politics/websites-hacked-isis/index.html

Government websites in Ohio, Maryland and New York have been hacked with what appears to be pro-ISIS propaganda. On Sunday, visitors to **governor.ohio.gov** were greeted with a black background and an Arabic symbol while an Islamic call to prayer played in the background. "You will be held accountable Trump," text on the landing page said, "you and all your people for every drop of blood flowing in Muslim countries." "I Love Islamic state," it said. *A group calling itself Team System DZ apparently hacked Gov. John Kasich's official site, along with the sites of first lady Karen Kasich and the Ohio Department of Rehabilitation and Corrections*. Those pages displayed the same message that Kasich's did. In addition to the pro-ISIS language, a line appeared on each page that said "Hacked by Team System DZ."

It was not immediately clear who the group is - or whether it is genuinely affiliated with ISIS. The Ohio sites were back to normal by Monday morning….

**Howard County, Maryland.** ISIS propaganda content also appeared on the Howard County, Maryland, government website Sunday. The county is in central Maryland, near Baltimore and Washington. It was restored to normal by Monday morning. "There was no breach of data and no personal information was compromised," according to a statement from Howard County Executive Allan H. Kittleman….

**Brookhaven, New York.** The official website for the town of Brookhaven, New York, also was hacked, according to Jack Krieger, Brookhaven communications director. Website visitors saw the same black background and logo found on the other hacked sites, with the same words about being held accountable and blood in Muslim countries. Town officials took the site down as soon as they learned of the problem and were working Monday morning to restore it to normal.

## UK Parliament Shut Down External Access to Email Accounts after Cyberattack

http://securityaffairs.co/wordpress/60404/hacking/uk-parliament-cybercattack.html

The UK Parliament has suffered the biggest ever cyber attack against the email systems - it shut down external access to email accounts on Saturday to mitigate the threat. According to the authorities, the attack was "sustained and determined," - hackers launched a prolonged brute-force attack against the Parliament email system in the attempt to access accounts. ..*"The "brute force" assault lasted for more than 12 hours on Friday as unknown hackers repeatedly targeted "weak" passwords of politicians and aides."* ..It is not clear if the cyber attack was linked to the recent discovery of the availability of UK politicians' login credentials for sale on the dark web.

## Before You Hit 'Submit,' This Company Has Already Logged Your Personal Data

https://gizmodo.com/before-you-hit-submit-this-company-has-already-logge-1795906081

If you're daydreaming about buying a home or need to lower the payment on the one you already have, you might pay a visit to the Quicken Loans mortgage calculator. You'll be asked a quick succession of questions that reveal how much cash you have on hand or how much your home is worth and how close you are to paying it off. Then Quicken will tell you how much you'd owe per month if you got a loan from them and asks for your name, email address, and phone number.

You might fill in the contact form, but then have second thoughts. Do you really want to tell this company how much you're worth or how in debt you are? *You change your mind and close the page before clicking the Submit button and agreeing to Quicken's privacy policy. But it's too late. Your email address and phone number have already been sent to a server at "murdoog.com," which is owned by NaviStone, a company that advertises its ability to unmask anonymous website visitors and figure out their home addresses*. NaviStone's code on Quicken's site invisibly grabbed each piece of your information as you filled it out, before you could hit the "Submit" button.

During a recent investigation into how a drug-trial recruitment company called Acurian Health tracks down people who look online for information about their medical conditions, we discovered NaviStone's code on sites run by Acurian, Quicken Loans, a continuing education center, a clothing store for plus-sized women, and a host of other retailers. *Using Javascript, those sites were transmitting information from people as soon as they typed or auto-filled it into an online form. That way, the company would have it even if those people immediately changed their minds and closed the page. (It's yet another way auto-fill can compromise your privacy.)* NaviStone is an Ohio-based startup *in the business of identifying "ready to engage" customers and matching "previously anonymous website visitors to postal names and addresses." It says it can send postcards to the homes of anonymous website shoppers within a day or two of their visit, and that it's capable of matching "60-70% of your anonymous site traffic to Postal names and addresses."*

In yesterday's report on Acurian Health, University of Washington law professor Ryan Calo told Gizmodo that giving users a "send" or "submit" button, but then sending the entered information regardless of whether the button is pressed or not, clearly violates a user's expectation of what will happen. Calo said it could violate a federal law against unfair and deceptive practices, as well as laws against deceptive trade practices in California and Massachusetts. A complaint on those grounds, Calo said, "would not be laughed out of court."

There are at least 100 sites using NaviStone's code according to Builtwith.com, a service that tells you what technologies sites employ. We visited dozens of them to see the code in action. The majority of sites captured visitors' email addresses only, but some sites also captured their home addresses and

other entered information. *Only one site of the dozens we reviewed, Gardeners.com, explicitly revealed in its privacy policy what it was doing. It read, "Information you enter is collected even if you cancel or do not complete an order."* The rest of the sites had the usual legalese in their policies about using standard tracking tech such as cookies and Web beacons, which did not describe the way this particular information capture works. …*Businesses seem to be doing all they can to strip away consumers' ability to anonymously browse the Web, sacrificing privacy at the altar of commerce*. And it's illustrative of the way your sense of control online can be an illusion, the "submit" feature becoming just another placebo button. *As a result of our reporting, though, NaviStone says it will no longer collect email addresses from people this way*. "While we believe our technology has been appropriately used, we have decided to change the system operation such that email addresses are not captured until the visitor hits the 'submit' button," Abbott wrote.

## Google Hit With Record EU Fine Over Shopping Service

http://www.bbc.com/news/technology-40406542

**Google has been fined 2.42bn euros ($2.7bn; £2.1bn) by the European Commission after it ruled the company had abused its power by promoting its own shopping comparison service at the top of search results.** The amount is the regulator's largest penalty to date against a company **accused of distorting the market**. The ruling also orders Google to end its anti-competitive practices within 90 days or face a further penalty. The US firm said it may appeal. However, if it fails to change the way it operates the Shopping service within the three-month deadline, *it could be forced to make payments of 5% of its parent company Alphabet's average daily worldwide earnings. Based on the company's most recent financial report, that amounts to about $14m a day*.

The commission said it was leaving it to Google to determine what alterations should be made to its Shopping service rather than specifying a remedy. "What Google has done is illegal under EU antitrust rules," declared Margrethe Vestager, the European Union's Competition Commissioner. "It has denied other companies the chance to compete on their merits and to innovate, and most importantly it has denied European consumers the benefits of competition, genuine choice and innovation."

## Scammer Who Made 96 Million Robocalls Should Pay $120M Fine, FCC Says

https://arstechnica.com/information-technology/2017/06/scammer-who-made-96-million-robocalls-should-pay-120m-fine-fcc-says/

The Federal Communications Commission today said that a scammer named Adrian Abramovich *"apparently made 96 million spoofed robocalls during a three-month period" in order to trick people into buying vacation packages*. The FCC proposed a fine of $120 million, but it will give the alleged perpetrator a chance to respond to the allegations before issuing a final decision. *The robocalls appeared to come from local numbers [spoofed]*, and they told recipients to "press 1" to hear about exclusive vacation deals from well-known hotel chains and travel businesses such as Marriott, Expedia, Hilton, and TripAdvisor, the FCC said. "Consumers who did press the button were then transferred to foreign call centers where live operators attempted to sell vacation packages often involving timeshares," the FCC said. *"The call centers were not affiliated with the well-known travel and hospitality companies mentioned in the recorded message." In reality, the travel agencies that robocall recipients were directed to "were fronts for one or more Mexican-based call centers engaged in selling timeshares and vacation packages to various timeshare facilities," the FCC said*. These agencies contracted with Abramovich to receive calls generated by his robocall operation, paying him daily for various amounts of phone calls, the FCC said.

The FCC began investigating after TripAdvisor notified the commission of the scheme last year. A citation issued to Abramovich accuses him of violating the Telephone Consumer Protection Act's robocall limits. *The misrepresentations in the prerecorded messages also constitute criminal wire fraud*, the FCC said.

Abramovich, working through his marketing companies, "appears to have made 96,758,223 robocalls between October 1, 2016 and December 31, 2016," FCC Chairman Ajit Pai said at today's FCC meeting. *Commission investigators used software to analyze the details of all the calls, and they "hand-verified" more than 80,000 of them. The investigators found that each one was spoofed to appear to be a local number. Pai said the scheme preyed on the elderly, many of whom spent a few hundred or a few thousand dollars on "exclusive" vacation packages*.

"Robocalling is consistently the top-ranked category of complaints that consumers bring to the FCC. That's why I'm pleased that today the commission is taking major, unprecedented action against what appears to be the most egregious 'neighbor spoofing' robocalling scheme we have ever seen," Pai said. Abramovich's mass-robocalling campaigns during 2015 and 2016 *"bombarded American consumers and repeatedly disrupted a critical telecommunications service used by hospitals and emergency medical providers," the FCC also said. This critical telecommunications service was identified as Spōk, a medical paging system for hospitals, emergency rooms, and doctors*. "Because paging technology is not equipped to handle voice calls, a large-scale robocalling campaign will disrupt - and can potentially disable - the medical pager network," the FCC wrote. "According to Spōk, the large volume of illegal calls had the potential to render Spōk's network completely inoperable, and many of Spōk's customers reported intermittent outages."

…When the FCC proposes fines, the alleged perpetrator is given an opportunity to dispute the allegations. Sometimes the FCC will reach a settlement for a lower fine, but it could also issue an order requiring payment of the full amount. Abramovich was given 30 days to respond. ..Robocalls from spoofed numbers have been tricky to defeat with existing call-blocking tools. The FCC has proposed rules that would let carriers block spoofed robocalls when the Caller ID can't possibly be valid.

## Web Hosting Company Pays $1 Million to Ransomware Hackers to Get Files Back

http://thehackernews.com/2017/06/web-hosting-ransomware.html

A South Korean web hosting provider has agreed to pay $1 million in bitcoins to hackers after a Linux ransomware infected its 153 servers, encrypting 3,400 business websites and their data, hosted on them. According to a blog post published by NAYANA, the web hosting company, this unfortunate event happened on 10th June when ransomware malware hit its hosting servers and the attacker demanded 550 bitcoins (over $1.6 million) to unlock the encrypted files. However, the company later negotiated with the cyber criminals and agreed to pay 397.6 bitcoins (around $1.01 million) in three installments to get their files decrypted. The hosting company has already paid two installments at the time of writing and would pay the last installment of ransom after recovering data from two-third of its infected servers.

*According to the security firm Trend Micro, **the ransomware used in the attack was Erebus** that was first spotted in September last year and was seen in February this year with Windows' User Account Control bypass capabilities*. Since the hosting servers were running on Linux kernel 2.6.24.2, researchers believe that Erebus Linux ransomware might have used known vulnerabilities, like DIRTY COW; or a local Linux exploits to take over the root access of the system. [see article for technical information on this ransomware]

According to analysis conducted by the Trend Micro researchers, decryption of infected files is not possible without getting hold of the RSA keys. *So, the only safe way of dealing with ransomware attacks is prevention. As we have previously recommended, the best defense against Ransomware is to create awareness within the organizations, as well as to maintain back-ups that are rotated regularly*. Most viruses are introduced by opening infected attachments or clicking on links to malware usually in spam emails. So, DO NOT CLICK on links provided in emails and attachments from unknown sources. Moreover, ensure that your systems are running the latest version of installed applications.

## Hackers Leak Eight Episodes of Unaired ABC Show 'Steve Harvey's Funderdome'

http://variety.com/2017/digital/news/steve-harveys-fundeerdome-leak-1202453754/

[June4] The Dark Overlord is back: The hacker who previously leaked almost the entire fifth season of Netflix's "Orange Is the New Black" targeted ABC with a new leak Sunday night, apparently releasing eight episodes of the network's still-unaired show "Steve Harvey's Funderdome" on The Pirate Bay. *"Time to play another round," the hacker wrote in a note accompanying the release. "We're following through on our threats as we always do." The Dark Overlord first threatened to target Disney-owned ABC this past Friday*. "If you prefer your meat bloody, we're serving it bloody as can be," the note continued. "We're bringing another piece from the world of unaired mainstream media content."

"Steve Harvey's Funderdome" is scheduled to premiere on ABC on June 11. The show, which is an MGM Television production that counts Mark Burnett as one of its executive producers, has two entrepreneurs pitching their ideas to a studio audience. Said audience gets to vote on the winner, who then receives seed funding for their business. Variety wasn't immediately able to verify the authenticity of the leak. However, details on The Pirate Bay show that the upload consisted of a total of eight video files,

with names suggesting that the files are the first eight episodes of the show. Disney representatives didn't immediately respond to a request for comment.
*It's still unclear who The Dark Overlord actually is, or whether it is even a single person or a group of hackers. We do know that The Dark Overlord has been hacking and then blackmailing companies for a couple of months now*. However, until recently, Hollywood wasn't actually a target of the hacker. Instead, he primarily targeted clinics and medical businesses. All of that changed when The Dark Overlord was able to break into the network of Larson Studios, a Hollywood-based audio post-production company, late last year. The hacker stole a number of shows and movies from multiple studios during that incident, and *initially threatened the post-production vendor directly, demanding ransom payments to not release any of the bounty. When that failed, The Dark Overlord began to target studios directly, which led to the release of ten "Orange Is the New Black" episodes in late April*. A list of shows and movies allegedly stolen by The Dark Overlord included around three dozen titles from multiple studios, including CBS, Fox and NBC. The list also named "Steve Harvey's Funderdome" as one of the affected ABC shows.

## How Hollywood Got Hacked: Studio at Center of Netflix Leak Breaks Silence

http://variety.com/2017/digital/features/netflix-orange-is-the-new-black-leak-dark-overlord-larson-studios-1202471400/
This story first appeared in the June 20, 2017 issue of Variety. It is abbreviated here but the full saga is available at the above link.]
Larson Studios president Rick Larson and his wife and business partner, Jill Larson, didn't recognize the number that sent them these two short text messages via their personal cell phones two days before Christmas last year, so they simply ignored them. "We didn't really think much of them," said Jill Larson. *Little did they know that the messages were part of Hollywood's biggest security breach since the Sony Pictures hack of 2014*. But in an exclusive interview with Variety, the Larson Studios principals are breaking their silence on an incident that threatened the existence of their family-owned audio post-production business. *An incident that led them to quietly wire more than $50,000 in extortion money to a group of hackers, only to see some of the most valuable works of their clients, including 10 unreleased episodes of Netflix drama series "Orange Is the New Black," leak online*. …A hacking group calling itself the Dark Overlord told them it had broken into Larson's server, and was threatening to leak all of the company's data.
Larson Studios chief engineer David Dondorf and director of digital systems Chris Unthank left their families on Christmas morning and rushed to the studio to examine the hackers' claims. "Once I was able to look at our server, my hands started shaking, and I almost threw up," Unthank remembered. The hackers had stolen and deleted all of the data, just as they had threatened in their letter. They demanded ransom payments via the crypto-currency Bitcoin to return what they had stolen.
*…….They eventually pieced together how the attack had unfolded. The Dark Overlord had been scanning the internet for PCs running older versions of Windows that it could easily break into, and happened to stumble across an old computer at Larson Studios that was still running Windows 7. "They were basically just trolling around to see if they could find a computer that they could open," Dondorf explained. "It wasn't aimed at us."*
*News of the hack broke in April, when the Dark Overlord publicly tried to pressure Netflix. The hackers first leaked one unreleased episode of "Orange Is the New Black," and when Netflix didn't pay, followed up with nine more episodes a month and a half before the show was scheduled to premiere on the service. Netflix declined comment for this story*.
"A lot of what went on was ignorance. We are a small company." Larson said. That's not to say that the company didn't care about security before. Larson's employees just didn't know all that much about it. Having a computer running an ancient version of Windows on the network was clearly a terrible lack of oversight, as was not properly separating internal servers from the internet.
…In many ways, the hack was a wake-up call for all of Hollywood. Studios had already significantly beefed up security after hackers broke into Sony Pictures in 2014 and subsequently leaked tens of thousands of emails. **But security experts had long warned of the lack of security at third-party vendors, of which there are many**. *Studios regularly rely on outside companies for sound processing, color correction, 3D upscaling and much more*. Some of these outside vendors are big players themselves, but many are family businesses like Larson Studios. In the wake of the Dark Overlord's hack, there is talk about standardizing security for these businesses. Work on security continues at Larson Studios, which is still undergoing audits commissioned by some of its major clients…

## Russia Targeted At Least 21 States in Wide-Spread Election Hack: Officials

http://globalnews.ca/news/3545954/russia-hack-election/

[June21] A sinister portrait of Russia's cyberattacks on the U.S. emerged Wednesday *as current and former U.S. officials told Congress that Moscow stockpiled stolen information and selectively disseminated it during the 2016 presidential campaign to undermine the American political process*. The Russians "used fake news and propaganda and they also used online amplifiers to spread the information to as many people as possible," Bill Priestap, the FBI's top counterintelligence official, told the Senate Intelligence committee.

While he said the Russians had conducted covert operations targeting past American elections, *the internet "has allowed Russia to do so much more" than before*. *But, he added, the "scale and aggressiveness" was different this time, with the primary goal being to sow discord and aid the candidacy of Republican Donald Trump, the eventual winner*. Russia's actions did not change the final election count, they said, but warned that Moscow's efforts will likely continue. "I believe the Russians will absolutely try to continue to conduct influence operations in the U.S.," which will include cyberattacks, Priestap said.

Jeanette Manfra, Homeland Security undersecretary for cybersecurity, said *there is evidence that 21 state election systems were targeted, but she told the Senate intelligence committee she couldn't disclose the identities of the states because that was up to the states*. Last September, DHS told The Associated Press that hackers believed to be Russian agents had targeted voter registration systems in more than 20 states. *Former Homeland Security Secretary Jeh Johnson from the Obama administration told the House Intelligence committee that Moscow's high-tech intrusion did not change ballots, the final count or the reporting of election results*. Johnson described the steps he took once he learned of the hacking of the Democratic National Committee, his fears about an attack on the election itself and his rationale for designating U.S. election systems, including polling places and voter registration databases, as critical infrastructure in early January, two weeks before Donald Trump's inauguration.

"In 2016 the Russian government, at the direction of (President) Vladimir Putin himself, orchestrated cyberattacks on our nation for the purpose of influencing our election – plain and simple," Johnson said. Johnson described his discussions with state election officials about ensuring the integrity of the voting process. He said 33 states and 36 cities and counties used his department's tools to scan for potential vulnerabilities. He also said he contacted The Associated Press, which counts votes, and its CEO, Gary Pruitt. "Prior to Election Day, I also personally reviewed with the CEO of The Associated Press its long-standing election-day reporting process, including the redundancies and safeguards in its systems," Johnson said. ....American elections are highly decentralized. Voters cast ballots in roughly 185,000 precincts spread over 9,000 jurisdictions during the 2016 presidential election. Elections are also subject to rigorous and elaborate rules that govern how and what equipment is used.

## *And Now, This:*

## How You Move a Computer Mouse May Reveal If You're Lying

http://money.cnn.com/2017/06/21/technology/future/computer-mouse-honesty-study/index.html#sthash.xaJcoYYI.dpuf

The smallest things we do can give away our biggest secrets. According to researchers at the University of Padova in Italy, how a person moves a mouse when answering questions on a computer may reveal whether or not they're lying. *The finding has the potential to identify everything from fake online reviews and fraudulent insurance claims to pedophiles and terrorists, the team suggests. The researchers used an artificial intelligence algorithm trained to make decisions based on data*. The computer system was presented labeled examples from individuals answering questions honestly and those providing false answers. *With experience, the algorithm began to identify the differences in mouse movements between an honest and dishonest answer*. During the study, which involved 60 students at the University of Padova, participants answered a series of questions - some of which were unexpected. Half were told to assume a false identity and given time to practice it. *The truthful individuals slid their mouse directly to an answer. The dishonest individual took a longer, indirect path to their answer. "Our brain is built to respond truthfully. When we lie, we usually suppress the first response and substitute it with a faked response,"* said Giuseppe Sartori, lead researcher and a University of Padova professor. The study was published recently in the online journal Plos One. Sartori envisions the technology helping authorities identify terrorists who are entering European countries under false identities. *Sartori's technique does not require a person to know certain information, such as an accurate birthday or address, to determine if*

*they are lying. Instead, authorities could detect lies by the manner in which specific questions were answered*.
Related: Data of almost 200 million voters leaked by GOP analytics firm Sartori said the technology could also be used to identify a pedophile who signed up for an online service with a false age. A well-coached individual could learn to lie convincingly with quick responses to questions. But they might stumble on tangential questions, such as stating their zodiac sign or a cross street near their home address.
*However, there are limitations to the approach - artificial intelligence is only as good as the data it's trained on*. Sartori said more subjects need to be studied to ensure the results accurately reflect all human behavior. The team's next step is to examine the differences between how honest and dishonest individuals type on a keyboard when answering questions.

**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



**********