Security News Digest
October 31, 2017
(sent out on November 1st)

The Information Security Branch "Security Day" is Wednesday, November 8th, with the theme "Defensible Security"

Go to the Security Day page to view the Agenda and to find the link for the Free Webcast!

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

State-Sponsored Cyberattacks on Canada Successful About Once a Week

http://www.cbc.ca/news/politics/cyber-attacks-canada-cse-1.4378711

The Canadian government's computer networks have been hit by state-sponsored cyberattacks about 50 times a week – and at least one of them usually succeeded. That acknowledgment from the Communications Security Establishment (CSE), the secretive agency charged with preventing such attacks, is a rare glimpse into the scale and frequency of attempts by foreign powers to penetrate federal government systems. "Between 2013 and 2015, the Government of Canada detected, on average a year, more than 2,500 state-sponsored cyber activities against its networks," says a new report. "Although more than six per cent of these attempts breached the Government of Canada's systems in 2013, this number had fallen to less than two per cent in 2015."

The report does not name the foreign states behind the attacks, though the government has previously identified China as responsible for a major cyberattack at the National Research Council in 2014 that forced a long shutdown of its systems and cost millions of dollars for recovery. Russia, Iran and North Korea are also well-known players in cyberwarfare, though have not been publicly identified as such by Canadian officials. The report did not say how CSE knows the attacks were state-sponsored.

Small-time hackers. The new report from the Public Safety Department says Canada successfully blocks some 600 million attempts each day to identify or exploit vulnerabilities in its government computer networks. But the vast majority are small-time hackers or other players not aligned with foreign states. Word of the frequency of state-sponsored hacking follows a deal struck between Canada and China on June 22, in which both sides agreed to refrain from conducting or supporting "cyber-enabled theft of intellectual property," such as private-sector trade secrets and confidential business information. That agreement, however, was silent about cyberattacks on government networks.

Last October, CSE reported to Parliament that it detected 4,571 "compromises" of federal systems because of cyberattacks in the first nine months of 2016. More than 2,000 were directed at federal systems related to natural resources, energy and the environment. The agency said only three of those attacks resulted in information being removed, none of it classified, but did not identify any players whether state-sponsored or not. CSE also warned in a separate report released earlier this year about threats to Canada's democratic process, saying that "almost certainly, multiple hackivist groups will deploy cyber capabilities in an attempt to influence the democratic process in 2019," the next scheduled federal election.

That June 16 report also warned that nation-states showed the "highest sophistication" in attempting to undermine democratic processes worldwide, again without naming any players. "Against Canada, nation-states are constantly deploying cyber capabilities to try to gain access to Government of Canada networks and the communications of federal government officials," the document said, without providing statistics on the level of threat. "They are the most capable adversaries." CSE said it had no evidence that any nation-state used cyberattacks in the 2015 federal election to influence the outcome of the vote. In the United States, the FBI has launched a high-level probe into alleged efforts

by Russia to influence the 2016 presidential election in favour of Donald Trump, an inquiry that resulted in charges against former Trump aides Monday.
Undetected for months. The latest CSE statistics on state-sponsored attacks on government networks were revealed in an evaluation of Canada's Cyber Security Strategy, a multi-department effort begun in 2010 to thwart hackers. CBC News first obtained the document through an Access to Information Act request. A cybersecurity expert says the new statistics on state-sponsored attacks are likely low-balled, because **it is often difficult to identify an attacker bent on anonymity. "Attribution is the hardest thing to do in cybersecurity,"** said Iain Paterson, managing director of Toronto-based Cycura, a technology security firm. "It's very possible, and not too hard, for an attacker to disguise their behaviour through changing their method of operation to mimic or imitate other attackers," he said in an interview. **Paterson also noted that in the private sector, systems and networks are typically compromised by intruders for 200 or more days before the owners become aware of the breach….**
Highly critical. The evaluation document was highly critical of Canada's cybersecurity strategy, citing poor information sharing, weak or non-existent record-keeping, and an approach that led to "confusion and frustration" among departments, agencies and private-sector stakeholders. The document also found that most federal efforts had been devoted to protecting federal government systems, and not enough to safeguarding private-sector networks. [see article for more discussion]

Canada's Top Cop Said It Would Be 'Reckless' to Keep Using Federal Government's IT Service

http://www.cbc.ca/news/politics/ssc-rcmp-it-public-safety-1.4373232
Among his last moves as RCMP commissioner, Bob Paulson told the head of the federal government's vexed tech support agency it would be "reckless and arguably criminal" to renew its contract with Shared Services Canada. The correspondence, obtained by CBC News under Access to Information legislation, appears to be the culmination of **a long-standing complaint from the RCMP that SSC offers a one-size-fits-all government-wide service package that does not recognize the unique needs of a national police force**.
"Given that, I have concluded that the SSC model, our arrangement with you and how SSC manages risk represents a manifest threat to how the RCMP delivers on its mandate to Canadians - in other words, that our engagement with you puts Canadians and my employees at a greater risk than they already face - I cannot accept the terms of this agreement," stated Paulson, who retired from the force at the end of June. The letter is dated March 31, 2017 - the expiration date for the original business arrangement signed by all federal departments in 2012. **The previous government created the IT agency in 2011 to modernize federal information technology with the goal of saving money and improving security.** Referring to what was then the RCMP's pending trial over the provision of training and equipment to Mounties who responded to the June 2014 shooting rampage in Moncton, the commissioner explained why he felt he could not sign the business agreement that had been put before him. "Given that the force and I have recently been charged under the Canada Labour Code for allegedly allowing conditions of work to be unsafe, it would be reckless of me to rely on SSC to deliver on some of our IT services as it has. Reckless and arguably criminal," wrote Paulson.
A history of poor service. Earlier this year, for instance, an 11-hour network computer outage downed every single Mountie's BlackBerry, affected police dispatching and prevented 240 police forces from accessing the Canadian Police Information Centre (CPIC) database. Even on relatively low-tech yet crucial requests, SSC has failed to meet RCMP standards. In another case it took SSC several months to deliver on a high-priority request for new phones and telephone headsets for 911 dispatchers - and when the equipment arrived, it was used and faulty. Paulson wrote that if the two agencies couldn't agree on a new service arrangement that met the RCMP's distinct needs, he would have to take the force's IT services back in-house. [see article for more discussion]

Secret Government of Canada Data Stored on U.S. Servers? Memo Raises Possibility

http://www.cbc.ca/news/politics/storage-data-cloud-government-canadian-shared-services-microsoft-secret-1.4277836
[Sept.8] Two government agencies have been meeting with Microsoft Inc. to discuss ways to store secret Canadian data on American servers, a measure expressly forbidden by federal policy. Microsoft's talks this year with Shared Services Canada and the Communications Security Establishment reviewed

whether sensitive data about Canadians and other confidential matters could be securely encrypted on American "cloud" services. A May 2017 memo to the chief operating officer of Shared Services Canada (SSC) says the discussions examined in part how to protect Canada's sovereignty by insulating the data from legal demands under the USA Patriot Act, which forces firms to turn over confidential information to American law enforcement if demanded. "This memorandum is to provide you with an update on the feasibility of Microsoft - or any other cloud vendor - to hold Government of Canada encrypted data in such a manner that Shared Services Canada holds and owns the decryption keys and is able to access the data while the vendor is not able to access to the data," says the memo. A copy of the heavily censored document was obtained by CBC News under the Access to Information Act.

A spokesperson for Shared Services Canada, Monika Mazur, did not respond directly when asked whether the IT agency was still considering foreign cloud services for sensitive government data, but referred to a federal document that forbids it.

Ottawa's IT Strategic Plan 2016-2020 forbids storing secret data outside Canada's borders: "To ensure Canada's sovereign control over its data, departments and agencies will adopt the policy that all sensitive or protected data under government control will be stored on servers that reside in Canada."

Some low-risk Government of Canada data already reside on American and other non-Canadian "cloud" servers, including data for web pages with the Canada.ca suffix, which provide only general information. Amazon Web Services in the United States, for example, hosts such Canadian pages. The previously undisclosed discussions with Microsoft are likely driven by a highly critical, $1.35-million report earlier this year on the repeated failures of Shared Services Canada since its creation in 2011 as Ottawa's IT department. The Jan. 12 report by international experts, assembled by consultants Gartner Inc., said the struggling agency needs to find more cloud-based solutions: "There is universal agreement from the Expert Panel that the progression of cloud and its continuing trajectory make this approach a vital component of a going-forward strategy for SSC." [see article for more details on the cloud discussion]

TD Customer Money Stuck 'in limbo' Due to e-Transfer Problems

http://www.cbc.ca/news/business/td-bank-e-transfer-interac-1.4380680

Shaun Rickard would like to know what happened to his $1,700. The home siding contractor received the payment yesterday morning via an Interac e-transfer from a customer. But when he tried to deposit the money into his TD Canada Trust account, it wouldn't work. "It's just kind of floating right now [in cyber space]" says Rickard who owns the business, Home Doctor, in Toronto. "It's very frustrating." Other TD customers are complaining online - including on Twitter and the website canadianoutages.com - that their e-transfers aren't going through, and that the bank isn't providing them with any explanation. "Been well over 24hrs and no answers??????" griped one customer on canadianoutages.com, which tracks problems at various companies and services.

Since Monday, about 30 TD customers have complained about the issue on the site. It is not clear when the problem began, or how many people are affected. Rickard said the problem is especially concerning for him because his customers often send him e-transfers. .. Lisa Darragh in Ottawa also wondered what was going on after she received an e-payment for $300 yesterday but couldn't deposit it into her TD account. "It's in limbo," she says. When Darragh went online looking for an explanation, she says she instead found numerous complaints by other unhappy TD customers in the same boat.

The bank told CBC News on Tuesday that the problem is only impacting a small number of customers. The trouble stems from "a recent update to provide enhanced features," said spokesperson Meghan Thomas in an email. She provided no further information on the update and did not answer our question about when the problem first started. "We apologize for the inconvenience this may have caused customers and we are working around the clock to fix it," she said. Thomas added that any pending e-transfers will be completed as soon as the problem is fixed. In July, customers at all of Canada's big banks experienced problems with e-transfers for about two days. It turned out Interac, which supplies the service, was having technical problems. Interac said the current TD problem has nothing to do with its operations.

Patients of Marijuana Dispensary Upset After Personal Information Shared in Email

http://ottawacitizen.com/news/local-news/patients-of-marijuana-dispensary-upset-after-personal-information-shared-in-email

The owner of a medical marijuana dispensary in Gloucester, Ontario, has apologized after emails were accidentally sent to 24 patients that revealed the names and addresses of all the store's customers. "Some people were obviously upset, for good reason," said Charlie Cloutier, owner of Greenworks Medicinal on Canotek Road. Staff phoned all the people who received the email to apologize and ask them to delete it, he said. **The email contained the names and addresses of about 250 people who are registered customers at Greenworks.** Unlike most of the dispensaries in town, **Greenworks only sells to customers with a doctor's prescription for marijuana. However, all the dispensaries are illegal. Medical marijuana can only be legally obtained by mail from producers licensed by Health Canada**, such as Tweed in Smiths Falls.

Cloutier said an employee was using a new computer program to send out a form email reminder to customers that their doctor's prescriptions were about to expire. Another window on the computer was open that contained the address list of members. Somehow the program grabbed the member list instead of the form letter, and the staffer only realized the problem after 31 emails had been sent, he said. Seven of the emails bounced back as return-to-sender, so 24 people received the email with the customer names and addresses. "It was definitely done in error and it won't be done again," said Cloutier. **The dispensary will no longer send emails to patients, instead contacting them in person**, he said. One Greenworks customer said she was astonished and upset when a neighbour told her she had seen her name and address on an email from Greenworks. It's a violation of privacy, she said, that could have devastating consequences. One of the people on the list, for example, could operate a daycare. "There are people who will lose their business if other people find out they are buying from a dispensary."

'A Year and a Half of Hell': Customers, Businesses Pay Price for Online Reviews

http://www.cbc.ca/news/business/go-public-online-reviews-lawsuit-backlash-1.4369246

Online reviews can be bad for business and devastating to a company's reputation, but they can also cause serious problems for the people who write them. An Ontario couple learned that the hard way when a $3-million defamation lawsuit was filed against them - for posting negative online reviews - by Ontario-based contractor Design-Spec Building Group. The civil claim was eventually withdrawn by Design-Spec, which won a $100,000 settlement from the couple for breach of trust.

…. Go Public found Canada lags behind other countries in implementing protection for those who post online reviews and the businesses that are the focus of those posts. As a result, Canadians are being threatened with legal action while businesses are left with little recourse when targeted by unfair or inaccurate reviews. The Vareys posted their reviews on the popular website HomeStars. It publishes homeowner opinions about home improvement companies. The founder of the website, Nancy Peterson, says she was shocked when she heard about the lawsuit and surprised "somebody would go to that extreme, to sue a homeowner for a review of bad workmanship." [other examples are described in this article – go to the link to read more]

……. Late last year, the U.S. passed a federal law that aims to protect online review writers called The Consumer Review Fairness Act. "This piece of legislation prevents businesses from launching the types of suits where an honest and fair online review is given even if it's negative," U.S. lawyer Sarah Robertson, who specializes in online content, tells Go Public. There is no law like it in Canada. Ontario has the Protection of Public Participation Act that's designed to weed out lawsuits brought for the purpose of suppressing free speech. But according to lawyer Sue Gratton, that's just part of the problem. She says **provinces also need to update defamation laws to protect both businesses and people who write online reviews**. "There were complaints about it being out of date a century ago," said Gratton, who is heading up a project by the Law Commission of Ontario called Defamation Law in the Internet Age. "On the reputation side, negative online reviews can be devastating to reputation ... internet speech is instantaneous, it has global reach, it can be easily forwarded or hyperlinked, it can be anonymous and it is certainly very difficult to get rid of," she said. "On the other hand, there is a public interested in having online reviews in the marketplace. And the concern is for libel chill, where the threat of lawsuit may prevent a consumer from speaking their mind." The goal is to recommend provincial legislative changes that would address the issues. Gratton says she hopes other provinces move to address the issue soon.

Facebook, Twitter and Google Tell U.S. Lawmakers about 'Reprehensible' Russian Election Interference

http://www.cbc.ca/news/business/facebook-twitter-google-washington-1.4380153

Representatives from some of America's largest technology companies were in Washington on Tuesday, telling lawmakers about what they have learned about Russian attempts to influence last year's U.S. election over their networks. Facebook Inc., Twitter Inc. and Alphabet Inc.'s Google began testifying in front of a Senate judiciary subcommittee led by Republican Sen. Lindsay Graham that's probing the issue of Russian meddling in the election. The three companies - and others - have only recently come forward with hard numbers on how extensive those attempts to meddle were.

Russia's Internet Research Agency generated 80,000 posts from fake names on 120 different made-up pages between January 2015 and August 2017, Facebook revealed this week, which were eventually viewed by as many as 126 million Americans once they were shared. Twitter said it has identified and deactivated 2,752 accounts linked to the same group, which is known for promoting pro-Russian government positions. Those accounts put out 1.4 million election-related tweets between the start of September and election day. None of those tweets were considered advertising under those services' own rules.

"When it comes to the 2016 election I want to be clear, "Facebook's general counsel Colin Stretch said in his opening remarks. **"The foreign interference that we saw is reprehensible."** "Many are inflammatory," Stretch said of **the posts, which got around advertising rules by masquerading as genuine posts from real people**. "Some are downright offensive."

In most instances, the offending posts that Facebook uncovered were designed to favour certain candidates over others. But in others, they didn't favour any one party and instead seemed targeted at certain issues in certain places - including posts about racial strife in places like Ferguson, Miss., and Baltimore, Md. "They were intended to attract people who were following certain causes to subscribe to those pages," Stretch said. The Russian government has denied it intended to influence the election, in which President Donald Trump, a Republican, defeated Democrat Hillary Clinton.

U.S. lawmakers have responded angrily to the idea of foreign meddling, introducing legislation to require online platforms to say who is running election ads and what audiences are targeted. "The companies need to get ahead of the curve here," said James Lewis, senior vice-president of the Washington-based Center for Strategic and International Studies. If they can, he added, they might avoid regulation. Lewis, speaking during the Reuters Cyber Summit in Washington, said he expects European officials to watch the U.S. hearings closely.

Facebook and Twitter have taken steps toward self-regulation, saying they would create their own public archives of election-related ads and also apply more specific labels to such ads. Google followed on Monday, saying it would create a database of election ads including ones on YouTube. The companies have meanwhile disclosed new details about the extent of Russia-based material, raising alarms about a sector that once inspired idealism. **"The internet was seen as a great engine for promoting democracy and transparency. Now we are all discovering that it can also be a tool for hijacking democracy,"** said Karen Kornbluh, a senior fellow for digital policy at the Council on Foreign Relations.

Facebook, Twitter, Google Executives Face 2nd Day of Testimony on Russian Election Interference

http://www.cbc.ca/news/business/technology-washington-russia-1.4381768

[Nov.1] Executives from Facebook, Google and Twitter faced a second day of grilling from lawmakers on Wednesday, from a Senate committee demanding answers about Russian attempts to meddle in the recent U.S. election. The three companies are in Washington this week to tell various Senate committees what they know about what Russia did during the recent election campaign to try to influence results.

Facebook revealed Tuesday that Russian-linked accounts managed to get viewed by up to 136 million Americans through fake posts that were shared widely. **On Wednesday, Facebook also revealed additional details about activities on its network, specifically that Instagram, the photo sharing network, was also targeted**. Facebook's chief counsel Colin Stretch revealed that starting in October 2016, an additional 16 million people were reached by bogus Instagram accounts that were later suspended for being in violation of the site's terms of service. "It pains me personally to see that our platform was abused in this way," Stretch said.

But Facebook wasn't alone in facing tough questions. Twitter's acting general counsel Sean Edgett was grilled by Virginia Republican Senator Mark Warner about why the site was so slow to act on accounts that were set up to disseminate misinformation. Twitter revealed this week that it had closed fewer than 3,000 accounts linked to Russian propaganda network, but those accounts generated more than one

million election-related tweets in the run-up to last November's vote. Warner grilled Edgett about why the service doesn't do a better job about getting rid of fake accounts, especially once they go viral.
He pointed out that one such, **the now-deactivated @TEN_GOP, purported to be the official account of the Republican party in Tennessee. At its peak, the account had more than 156,000 followers, but was in fact a fake account run by Russian operatives**. **The Twitter account of the real Tennessee Republican party, by contrast, only had roughly 13,000 followers and complained to the company to shut down the imposter - but it took months for that to happen.** "That was an absolute mess," Edgett told an irate Warner "[but] we've gotten better since."
The testimony, which continues Wednesday and Thursday, can be viewed live in the player [on the CBC site available at the article link], and on many news outlets.

Alleged Hacker 'Used Army of 9,000 'Zombie' Computers to Attack Websites Such As Skype, Google and Pokemon'

http://www.dailymail.co.uk/news/article-5026697/Liverpool-man-21-charged-hacking-Skype-Google.html
[Oct28] A man has been charged with using an army of 9,000 'zombie' computers to attack websites such as Skype, Google and Pokemon. Alex Bessell, 21, is accused of using them to orchestrate Distributed Denial of Service (DDoS) attacks on several major online firms in a bid to crash their operations. The attacks took over their systems and caused them to crash, leaving users unable to access them.
It is alleged the 21-year-old from Liverpool also set up the web business 'Aiobuy' and has made more than $700,000 (£533,193) in sales of harmful IT viruses since 2011. He has also been charged with designing a 'crypter' software package that hides bugs from computer users and makes them invisible to anti-virus systems.
A police spokesman said: 'Bessell will face a total of 11 charges, including unauthorised access to computers, impairing the operation of computers, making and supplying malware, money laundering and making false statements to Companies House. 'The charges follow an investigation by cybercrime detectives at the West Midlands Regional Organised Crime Unit (ROCU) based in Birmingham.' He is due to appear before Birmingham magistrates on Monday.
Oct30 update: Alex Bessell faces 11 charges including infecting and controlling more than 9,000 "zombie" computers to attack Skype, Google and other firms. The 21-year-old, from Liverpool, appeared at Birmingham Magistrates' Court on Monday after an investigation by West Midlands Police. He is due to appear in Crown court in November. [the Security News Digest will follow up on this story]

Researchers Hack Vacuum Cleaner; Turn It Into Perfect Spying Device

https://www.hackread.com/researchers-hack-vacuum-cleaner-turn-it-into-perfect-spying-device/
According to the findings of Check Point researchers, **there is a vulnerability in the LG smart home infrastructure through which hackers can take full control of an authentic user account and later remotely hijack LG SmartThinq home appliances including refrigerators, dryers, dishwashers, microwaves and robotic vacuum cleaners. When a user leaves any of these devices switched on or off, cybercriminals get the perfect opportunity to convert them into real-time spying devices.**
To prove their point, Check Point researchers demonstrated how a hacker could turn LG Hom-Bot vacuum cleaner into an espionage gadget. This was made possible through taking control of the integrated video camera installed inside the device. They disassembled the Hom-Bot to locate the Universal Asynchronous Receiver/Transmitter (UART) connection, and when it was discovered, that they could manipulate it to acquire access to the file system. Once the main process was debugged, they started looking for the code that initiated communication between the Hom-Bot and the SmartThinq mobile app.
"This is when we had the idea to investigate the SmartThinq application – leading to the discovery of the HomeHack vulnerability," revealed Check Point researchers. Investigation of the app and backend platform was made possible after installation of the app on a rooted phone and utilizing debugging tools. When the anti-root and SSL pining mechanisms were bypassed, it became possible to intercept the app's traffic, and this helped in the creation of an LG account. Now it was not a big deal to log in to the app.
Afterwards, researchers analyzed the login process and identified that there wasn't any direct link between the authentication request through which user credentials were identified and the creation of username based signature, which generated the access token for the user account. Therefore, it was

identified that attacker could use his username to bypass the authentication process and then switch to the victim's username to get the access token and this is how the login process can successfully be completed. This is termed as the HomeHack vulnerability by Check Point researchers in their blog post. "By exploiting the HomeHack vulnerability, the attacker could take over the victim's account and control his smart LG devices," researchers noted. **Check Point identified the vulnerability on July 31st, 2017 and LG immediately fixed the issue in its SmartThinq app by the end of September and the company has urged users of LG smart appliances to update to the app v1.9.23 version, which can be downloaded from Google Play Store or Apple's App Store. On the other hand, to update smart home physical devices, click on the smart home product option available on SmartThinq app Dashboard.**

According to Check Point's products vulnerability research head Oded Vanunu, with the advancements in hacking capabilities, **cybercriminals are shifting their focus more on hacking individual devices through exploiting software flaws. This would eventually affect user's homes and result in leaking of sensitive user data**. This is why it is important that users beware of the "security and privacy risks" associated with using IoT devices and robust security mechanisms must be employed to ensure that software and devices both remain protected from unauthorized access and manipulation, stated Vanunu.

The Nasty Future of Ransomware: Four Ways the Nightmare is About to Get Even Worse

http://www.zdnet.com/article/the-nasty-future-of-ransomware-four-ways-the-nightmare-is-about-to-get-even-worse/

2017 has been the year of ransomware. While the file-encrypting malware has existed in one form or another for almost three decades, **over the last few months it's developed from a cybersecurity concern to a public menace**. The term even made it into the [Merriam Webster] dictionary in September. In particular, 2017 had its own summer of ransomware: while incidents throughout 2016 showed the potential damage - both operational and financial - ransomware can cause to organisations, it was in the space of six weeks during May and June this year that the impact of ransomware really became apparent.

First WannaCry hit hundreds of thousands of systems around the globe, thanks to worm-like capabilities of a leaked NSA exploit being attached to the ransomware. The UK's National Health Service was particularly badly hit and thousands of appointments were cancelled. Weeks later came another global ransomware epidemic in the form of Petya, equipped with similar worm-like features, plus the ability to irrecoverably wipe data from infected machines. If making money from ransom was the end goal, neither campaign was successful. Those behind WannaCry - intelligence agencies suspect North Korea - eventually cashed out $140,000 from the Bitcoin wallets associated with the attack, something of a paltry sum considering the scale and impact of the campaign.

But what both WannaCry and Petya outbreaks managed to do was make it clear just how much of a problem ransomware has become. **And it hasn't gone away again either with the recent Bad Rabbit ransomware attacks in Russia and Ukraine showing that malware writers are still working on new versions.**

Ransomware as a diversion. We've already seen how **ransomware can come with other malicious items in tow. For example, Petya included a wiper designed to irrecoverably destroy data on infected machines**. It's a cunning tactic - while the ransomware presents itself as the immediate problem, **the attack may also be doing something else in the background**.

"Ransomware will be the public face of what's going on, scary and visible, but behind the scenes a whole range of other things can be happening: machine infiltration, scraping of data, transfer of funds, all while you have a really big diversion happening," says Perry Carpenter, strategy officer at security company KnowBe4. This could mean **the ransomware infection could being the least of your problems**. **Trojan malware or stolen credentials could give attackers outright access to the network,** even after the 'ransomware' infection has been dealt with, so organisations could potentially give in and pay a ransom to criminals who then remain able to exploit vulnerabilities in the network. Another potential development of ransomware is the emergence strains that not only encrypt your data but also steal it.

Ransomware that blackmails you too. "How else might someone use access to a computer to make money? **I think we might see more cases of ransomware which aren't just about data encryption and 'pay me and get it back' but more about doxxing - gathering sensitive information and threatening to release it if you don't pay up,"** says Mark Dufresne, director of threat research and adversary prevention at security company Endgame.

This tactic has already been adopted by some families of ransomware. For instance, a form of Android ransomware has already used the threat of exposing private information to the victim's contacts as 'encouragement' for paying up. Meanwhile some forms of malware claim to be able to see the websites victims have been visiting, although it's unlikely the ransomware actually has this capability - yet. "You can't solve that with good backups. If you've got compromising emails in your inbox, or anything which might be secretive or problematic, you're going to be incentivised to pay in order to stop that getting out," says Dufresne.

Enterprise ransomware. Another potential tactic could see criminals go after enterprise infrastructure. Locking users out of PCs is bad, but **getting ransomware onto critical systems could be highly disruptive to businesses and highly lucrative for crooks**. "We're going to see an increased focus on **the concept of enterprise ransomware, where they're moving away from targeting one specific machine to trying to spread virally throughout the organisation and trying to get as many machines as possible**," says Dmitri Alperovitch, co-founder and CTO of security company Crowdstrike. This would certainly take more effort than randomly distributing ransomware via email campaigns, but would lead to a bigger payoff.

"For a few hundred thousand dollars, nobody would think twice. I've no doubts that if the ransom asked was $10m, it'd still be paid," says Alperovitch. "All considerations go out the window when your business is down and you're facing hundreds of millions of dollars in damages, if you can, you'll pay at that point and the boards and CEO will make that decision without any hesitation."

New network attacks. But not every cybercriminal operation is going to spend time and resources in order to go after specific targets - **ransomware will continue to be randomly distributed in spam emails because that still works**. And as demonstrated throughout 2017, the use of SMB exploits like EternalBlue or EternalRomance can aid that by helping ransomware easily spread itself across a network with minimal effort.

Cybercriminals aren't going to just forget about these exploits. **Bad Rabbit has once again demonstrated how so many organisation simply haven't applied critical patches issued over half a year ago , so attackers will capitalise on newly discovered exploits - and look to take advantage of lax patching by businesses and consumers.** "The next thing I would say is the big risk from malicious software is the addition of more network propagation. They'll be doing what they've traditionally done - be it ransomware or malware - but adding more network propagation," says Holly Williams, penetration test team leader at Sec-1 Ltd. Leaked NSA exploits have played a large role in aiding the spread of self-propagating malware: WannaCry took advantage of the EternalBlue SMB vulnerability, while BadRabbit exploited EternalRomance. But it won't take another NSA leak for ransomware writers to find a new means of attacking networks.

"There are many more methods which malware can use to propagate across a network and NotPetya chose a handful of those - a published vulnerability and other features we've known about in pen testing for a long time. The ability to extract plain text credentials from a machine - like NotPetya had - has been around since 2012. The priority order of vulnerabilities changes," says Williams. While 2017 might be viewed by many as the year ransomware was recognised as a real menace, it could be that there is still worse to come. "Increasingly you'll see the criminals realise that's where the big money is. That's not a few thousand dollars but a few million dollars and that's a game changer," says Alperovitch.

Malaysia Data Breach Comprises 46.2M Mobile Numbers

http://www.zdnet.com/article/malaysia-data-breach-comprises-46-2m-mobile-numbers/

A massive cybersecurity breach is reported to have compromised personal data of 46.2 million mobile numbers in Malaysia, exposing details such as home addresses and SIM card information. The breach affected both postpaid and prepaid numbers as well as subscribers from all major mobile carriers in the country, including Maxis, Altel, Digi, and Celcom, according to Lowyat.net. The local website earlier this month said it received information that personal data linked to millions of Malaysians were being peddled online.

Apart from customer data from local telcos, it added that the information included those that belonged to various websites such as Jobstreet.com, Malaysian Medical Association, and Malaysian Housing Loan Applications. Leaked data from Jobstreet.com, for instance, contained the candidate's login name, nationality, and hashed passwords. Timestamps in the compromised data suggested that the breach occurred between 2014 and 2015, said Lowyat. It said it had handed the information to industry regulator, Malaysian Communications And Multimedia Commission (MCMC), which later released a

statement confirming it was investigating the incident. According to local reports, Communications and Multimedia Minister Datuk Seri Salleh Said Keruak said the police also was involved in the investigation. Malaysia has a population of some 31.2 million, so some subscribers likely will hold more than one compromised mobile number. The report added that the list may contain inactive numbers as well as temporary ones issued to visitors to the country.

Apple Fires iPhone X Engineer After Daughter's Hands-On Video Goes Viral

https://www.theverge.com/2017/10/28/16565110/apple-engineer-iphone-x-youtube-video

Apple has reportedly dismissed an engineer after his daughter's iPhone X hands-on video went viral on YouTube. Brooke Amelia Peterson published a vlog earlier this week, which included a trip to the Apple campus to visit her father and see an unreleased iPhone X. Peterson's video was quickly picked up by sites like *9to5Mac*, and it spread even further on YouTube.

Peterson now claims her father has been fired as a result of her video. In a tearful video, Peterson explains **her father violated an Apple company rule by allowing her to film the unreleased handset at Apple's campus**. Apple reportedly requested that Peterson remove the video, but it was clearly too late as the content spread further and further. The video itself may have seemed like an innocent hands-on, but **it did include footage of an iPhone X with special employee-only QR codes. A notes app was also shown on the iPhone X in the video, which appeared to include codenames of unreleased Apple products**. Filming on Apple's campus is strictly prohibited, so filming an unreleased iPhone X is a definite rule violation.

We've seen similar dismissals in the past. A Microsoft employee was dismissed after his son posted pictures of the Xbox 360 before its release. The Apple engineer in question had worked at the company for around four years, building the iPhone RF and wireless circuit design. *The Verge* reached out to Apple to confirm the dismissal, but the company has not yet responded to a request for comment.