Security News Digest
August 29, 2017

Relax and Take
Dog Days of Summer quiz

Scam of the Week: Hurricane Harvey Charity Fraud

https://blog.knowbe4.com/cyberheistnews-vol-7-34

Hurricane Harvey hit hard and especially Houston, TX got badly flooded. The death toll is rising and you can also count on low-life cyber-scum exploiting this disaster. Disgusting. Scammers are now using the Hurricane Harvey disaster to trick people in clicking on links, on Facebook, Twitter and phishing emails trying to solicit charitable giving for the flood victims.

Here are some examples: Facebook pages dedicated to victim relief contain links to scam websites, Tweets are going out with links to charitable websites soliciting donations, but in reality include links to scam sites or links that lead to a malware infection, and Phishing emails dropping in a user's inbox asking for donations to #HurricaneHarvey Relief Fund [scam site]. Previous disasters have been exploited like this, and the bad guys are going at it again will all guns blazing. Be wary of anything online covering the Hurricane Harvey disaster in the following weeks. [and any current or future disaster]

If you want to make an online financial contribution, including the Wildfires in BC or any other Relief Fund, contact the Canadian Red Cross http://www.redcross.ca/donate/appeal/donate-to-the-canadian-red-cross-fund#a0650cb6-ce29-4c40-b663-e749a0a9163f

Canada's Electronic Spy Agency to Get New Rules for Sharing Data with Allies

http://www.cbc.ca/news/politics/sajjan-cse-data-sharing-five-eyes-1.4265583

The office of Defence Minister Harjit Sajjan is crafting a directive for how Canada's electronic spy agency shares its foreign signals intelligence with its closest allies, the Five Eyes partners. The work follows a 2016 report from the oversight commissioner of the Communications Security Establishment (CSE). In it Jean-Pierre Plouffe revealed how the agency had illegally and unintentionally shared domestic metadata with those key allies: the United States, United Kingdom, Australia and New Zealand. Metadata is information associated with phone or electronic communication that is used to identify, describe or route information.

CSE is authorized under the National Defence Act to - among other things - collect foreign signals intelligence and protect computer networks from cyber attack. In an email to CBC News, Sajjan's press secretary Jordan Owens said CSE already has a "robust suite of privacy measures" that guide its work. But Owens said the agency is now conducting an analysis to support the defence minister's directive on information-sharing activities among the Five Eyes. "This is a significant undertaking and we look forward to having more to share in the future as development on this directive progresses," wrote Owens.

Canadian Accused in Yahoo Hack Pleads Not Guilty in U.S. Court

http://globalnews.ca/news/3691851/canadian-yahoo-hack-not-guilty-court/

In his first U.S. court appearance on Wednesday, Canadian Karim Baratov pleaded not guilty to charges that he helped Russian agents in a high-profile cyber attack on Yahoo email accounts, his lawyer said. Baratov, a 22-year old Canadian citizen born in Kazakhstan, was arrested in Canada in March at the request of U.S. prosecutors. They charge he was paid to break into at least 80 email accounts by Russian intelligence agents who masterminded the 2014 theft of data from some 500 million Yahoo Inc user accounts.

Baratov entered his plea during a brief appearance at the U.S. Federal Court in the Northern District of California, lawyer Andrew Mancilla said. His next hearing is scheduled for Tuesday. Mancilla declined to comment on prospects for a plea bargain for Baratov, who presented himself on social media accounts as a wealthy young man who loved expensive cars. He waived his right to fight the U.S. request for him to

be extradited from Canada. Baratov is the only person arrested to date among four men indicted in the case. The others include Alexsey Belan, who is among the FBI's most-wanted cyber criminals, along with two officers in Russia's Federal Security Services – Dmitry Dokuchaev and his superior, Igor Sushchin.

'Data is the New Oil': Your Personal Information is Now the World's Most Valuable Commodity

http://www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677

There was a time that oil companies ruled the globe, but "black gold" is no longer the world's most valuable resource - it's been surpassed by data. The five most valuable companies in the world today - Apple, Amazon, Facebook, Microsoft and Google's parent company Alphabet - have commodified data and taken over their respective sectors. "Data is clearly the new oil," says Jonathan Taplin, director emeritus of the USC Annenberg Innovation Lab and the author of *Move Fast and Break Things: How Google, Facebook and Amazon Cornered Culture and Undermined Democracy.*

But with that domination comes responsibility - and jurisdictions are struggling with how to contain, regulate and protect all those ones and zeros. For instance, Google holds an 81 per cent share of search, according to data metrics site Net Market Share. By comparison, even at its height, Standard Oil only had a 79 per cent share of the American market before antitrust regulators stepped in, Taplin says.

Selling access. What "the big five" are selling - or not selling, as in the case of free services like Google or Facebook - is access. **As we use their platforms, the corporate giants are collecting information about every aspect of our lives, our behaviour and our decision-making. All of that data gives them tremendous power. And that power begets more power, and more profit**.

On one hand, the data can be used to make their tools and services better, which is good for consumers. These companies are able to learn what we want based on the way we use their products, and can adjust them in response to those needs. "It enables certain companies with orders of magnitude more surveillance capacity than rivals to develop a 360-degree view of the strengths and vulnerabilities of their suppliers, competitors and customers," says Frank Pasquale, professor of law at the University of Maryland and author of *Black Box Society.*

Access to such sweeping amounts of data also allows these giants to spot trends early and move on them, which sometimes involves buying up a smaller company before it can become a competitive threat. Pasquale points out that Google/Alphabet has been using its power "to bully or take over rivals and adjacent businesses" at a rate of about "one per week since 2010." But it's not just newer or smaller tech companies that are at risk, says Taplin. "When Google and Facebook control 88 per cent of all new internet advertising, the rest of the internet economy, including things like online journalism and music, are starved for resources."

Traditionally, this is where the antitrust regulators would step in, but in the data economy it's not so easy. What we're seeing for the first time is a clash between the concept of the nation state and these global, borderless corporations. A handful of tech giants now surpass the size and power of many governments. For comparison sake, Facebook has almost two billion users, while Canada has a population of just over 36 million. Based on the companies' sheer scale alone, it is increasingly difficult for countries to enforce any kind of regulation, especially as the tech giants start pushing for rules that free them from local restrictions, says Open Media's Meghan Sali.

"Take, for example, NAFTA, where big tech companies are pushing to include legislation that stops countries from making rules that require the local storage of data," Sali says. "When data is stored in Canada, it's a lot easier to legislate its uses and address privacy concerns." That's just one way economic considerations are taking precedence over consumer protection. Pasquale adds that regulators would "certainly be able to intervene effectively" if they had more resources - money, personnel and technical capacity - with which to level the playing field. "And very simple interventions could help enormously - for example, requiring any dominant platform to pay out as wages or other compensation some percentage of revenues."

'We need the political will'. Sali also points out the similarities between the global dominance of the big five and the stranglehold of Canada's three major internet service providers - Bell, Rogers and Telus - whose dominance of the domestic market has kept out competitors and led to Canadians paying some of the highest prices for wireless internet access in the world. "When we look at the price of data and the amount of money that's being made by big companies by reselling that data, it's certainly comparable to oil in that manner," she says. "But it's a little bit different in that data isn't a finite resource. At the end of the day, we can certainly create more data, whereas we can't create more oil."

Government could also help by managing crucial parts of the data economy as public infrastructure - a measure that has seen great success through the Community Broadband initiative, whereby government subsidies have helped build local fiber optic networks. In other words, if the Radio-television and Telecommunications Commission (CRTC) is going to claim that every Canadian has a right to high-speed internet, then perhaps network infrastructure should be treated like roads and highways and bridges, as opposed to resting it in the hands of corporate giants. There are ways to rein in these mega-corporations, Taplin says. "We just need the political will," he says.

These 42 Disney Apps are Allegedly Spying on Your Kids

https://www.washingtonpost.com/news/the-switch/wp/2017/08/07/these-42-disney-apps-are-allegedly-spying-on-your-kids/

The Walt Disney Co. secretly collects personal information on some of its youngest customers and shares that data illegally with advertisers without parental consent, according to a federal lawsuit filed late last week in California. The class-action suit targets Disney and three other software companies - Upsight, Unity and Kochava - alleging that the mobile apps they built together violate the law by gathering insights about app users across the Internet, including those under the age of 13, in ways that facilitate "commercial exploitation." The plaintiffs argue that Disney and its partners violated COPPA, the Children's Online Privacy Protection Act, a federal law designed to protect the privacy of children on the Web. The lawsuit, filed in U.S. District Court for the District of Northern California, seeks an injunction barring the companies from collecting and disclosing the data without parental consent, as well as punitive damages and legal fees.

The lawsuit alleges that Disney allowed the software companies to embed trackers in apps such as "Disney Princess Palace Pets" and "Where's My Water? 2." Once installed, tracking software can then "exfiltrate that information off the smart device for advertising and other commercial purposes," according to the suit. Disney should not be using those software development companies, said Jeffrey Chester, the executive director of the Center for Digital Democracy. "These are heavy-duty technologies, industrial-strength data and analytic companies whose role is to track and monetize individuals," Chester said. "These should not be in little children's apps."

Disney said the lawsuit is misguided and intends to defend against it in court. "Disney has a robust COPPA compliance program, and we maintain strict data collection and use policies for Disney apps created for children and families," the company said in a statement Monday. "The complaint is based on a fundamental misunderstanding of COPPA principles, and we look forward to defending this action in Court." According to the Federal Trade Commission, online services that target users under the age of 13 should display a privacy policy that is plain to read and easy to understand. The policy must state the kind of information being collected and what the service might do with that data. Directions on how parents can give their consent should also be included. [the apps involved are list in the article – they include Beauty and the Beast, Frozen and Moana]

Leak of >1,700 Valid Passwords Could Make the IoT Mess Much Worse

https://arstechnica.co.uk/information-technology/2017/08/iot-password-leak/

Security researchers have unearthed a sprawling list of login credentials that allows anyone on the Internet to take over home routers and more than 1,700 "Internet of things" devices and make them part of a destructive botnet. The list of telnet-accessible devices, currently posted at this Pastebin address, was first posted in June, but it has been updated several times since then. It contains user names and passwords for 8,233 unique IP addresses, 2,174 of which were still running open telnet servers as of Friday morning, said Victor Gevers, chairman of the GDI Foundation, a Netherlands-based nonprofit that works to improve Internet security. Of those active telnet services, 1,774 remain accessible using the leaked credentials, Gevers said. In a testament to the poor state of IoT security, the 8,233 hosts use just 144 unique username-password pairs.

It is likely that criminals have been using the list for months as a means to infect large numbers of devices with malware that turns them into powerful denial-of-service platforms. Still, for most of its existence, the list remained largely unnoticed, with only some 700 views. That quickly changed Thursday with this Twitter post. By Friday afternoon, there were more than 13,300 views.

….Last year, several botnets came to light that drastically increased the potency of DDoS botnets, which use thousands of computers or other Internet-connected devices all over the world to bombard a single target with more junk traffic than it can process. Security site KrebsOnSecurity, for instance, was taken

down for days by attacks that delivered a then-staggering 620 gigabits per second of network traffic. Around the same time, a French Web host reported sustaining onslaughts of 1.1 terabits per second. The botnets that made these once-unthinkable attacks possible carried names such as Mirai and Bashlight. Unlike more traditional botnets that infected Windows computers, the new generation targeted routers, security cameras, and other Internet-connected devices. According to OVH, the France-based Web host, the 1.1-terabit-per-second barrage was delivered by roughly 145,000 devices. Based on that figure, the 2,174 currently available devices in the list that came to light Thursday are capable of only a small fraction of that firepower. Still, that's enough to bring plenty of smaller sites down almost instantly. Some of the credentials included in the list suggest that some of the devices have already been conscripted into botnets.

….People who use routers, cameras, and other IoT devices are reminded that remote access should be enabled only when there is good reason, and then only after changing default credentials to use a unique, randomly generated password, ideally of 12 or more characters, or assuming the device doesn't allow that, one as long as possible. Even when remote access is disabled, people should always ensure the default password is replaced with a strong one.

Gevers said he and other GDI Foundation volunteers are in the process of contacting as many currently affected host owners as possible in an attempt to lock down the vulnerable devices. Given the IoT's deserved reputation for poor default security and the lackadaisical approach many users have for securing their devices, there almost certainly are tens of thousands of other vulnerable devices that can be easily detected doing a simple Internet scan.

The 5 Cyber-Attacks You're Most Likely to Face

http://www.csoonline.com/article/2616316/data-protection/security-the-5-cyber-attacks-you-re-most-likely-to-face.html

[By Roger A. Grimes, Columnist, CSO] As a consultant, one the security biggest problems I see is perception: The threats companies think they face are often vastly different than the threats that pose the greatest risk. For example, they hire me to deploy state-of-the-art public key infrastructure (PKI) or an enterprise-wide intrusion detection system when really what they need is better patching. **The fact is most companies face the same threats** - and should be doing their utmost to counteract those risks. Here are the five most common successful cyber attacks.

Cyber Attack No. 1: Socially Engineered Malware

Socially engineered malware, lately often led by data-encrypting ransomware, provides the No. 1 method of attack (not a buffer overflow, misconfiguration or advanced exploit). An end-user is somehow tricked into running a Trojan horse program, often from a website they trust and visit often. The otherwise innocent website is temporarily compromised to deliver malware instead of the normal website coding. The maligned website tells the user to install some new piece of software in order to access the website, run fake antivirus software, or run some other “critical” piece of software that is unnecessary and malicious. The user is often instructed to click past any security warnings emanating from their browser or operating system and to disable any pesky defenses that might get in the way.

Sometimes the Trojan program pretends to do something legitimate and other times it fades away into the background to start doing its rogue actions. Socially engineered malware programs are responsible for hundreds of millions of successful hacks each year. Against those numbers, all other hacking types are just noise.

Countermeasure: Social engineered malware programs are best handled through ongoing end-user education that covers today's threats (such as trusted websites prompting users to run surprise software). Enterprises can further protect themselves by not allowing users to surf the web or answer email using elevated credentials. An up-to-date anti-malware program is a necessary evil, but **strong end-user education** provides better bang for the buck.

Cyber Attack No. 2: Password Phishing Attacks

Coming a close second are password phishing attacks. Approximately 60 to 70 percent of email is spam, and much of that is phishing attacks looking to trick users out of their logon credentials. Fortunately, anti-spam vendors and services have made great strides, so most of us have reasonably clean inboxes. Nonetheless, I get several spam emails each day, and a least a few of them each week are darned good phishing replicas of legitimate emails. I think of an effective phishing email as a corrupted work of art: Everything looks great; it even warns the reader not to fall for fraudulent emails. The only thing that gives it away is the rogue link asking for confidential information.

Countermeasure: The primary countermeasure to password phishing attacks is to have logons that can't be given away. This means two-factor authentication (2FA), smartcards, biometrics and other out-of-the-band (e.g., phone call or SMS message) authentication methods. If you can enable something other than simple logon name/password combinations for your logons, and require only the stronger methods, then you've beat the password-phishing game.

If you're stuck with simple logon name/password combinations for one or more systems, make sure you use accurate-as-can-be anti-phishing products or services, and decrease the risk through better end-user education. I also love browsers that highlight the true domain name of a host in a URL string. That way windowsupdate.microsoft.com.*malware.com*, for example, is more obvious.

Cyber Attack No. 3: Unpatched Software

Coming in close behind socially engineered malware and phishing is software with (available but) unpatched vulnerabilities. The most common unpatched and exploited programs are browser add-in programs like Adobe Reader and other programs people often use to make surfing the web easier. It's been this way for many years now, but strangely, **not a single company I've ever audited has ever had perfectly patched software**. It's usually not even close. I just don't get it.

Countermeasure: Stop what you're doing right now and make sure your patching is perfect. If you can't, make sure it's perfect around the most exploited products, whatever they happen to be in a given time period. Everyone knows that better patching is a great way to decrease risk. Become one of the few organizations that actually does it. Better yet, make sure that you're 100 percent patched on the programs most likely to be exploited versus trying unsuccessfully to be fully patched on all software programs.

Cyber Attack No. 4: Social Media Threats

Our online world is a social world led by Facebook, Twitter, LinkedIn or their country-popular counterparts. Social media threats usually arrive as a rogue friend or application install request. If you're unlucky enough to accept the request, you're often giving up way more access to your social media account than you bargained for. Corporate hackers love exploiting corporate social media accounts for the embarrassment factor to glean passwords that might be shared between the social media site and the corporate network. Many of today's worst hacks started out as simple social media hacking. Don't underestimate the potential.

Countermeasure: End-user education about social media threats is a must. Also make sure that your users know not to share their corporate passwords with any other foreign website. Here's where using more sophisticated 2FA logons can also help. Lastly, make sure all social media users know how to report a hijacked social media account, on their own behalf, or someone else's. Sometimes it is their friends who notice something is amiss first.

Cyber Attack No. 5: Advanced Persistent Threats

I know of only one major corporation that has not suffered a major compromise due to an advanced persistent threat (APT) stealing intellectual property. APTs usually gain a foothold using socially engineered Trojans or phishing attacks. A very popular method is for APT attackers to send a specific phishing campaign - known as **spearphishing** - to multiple employee email addresses. The phishing email contains a Trojan attachment, which at least one employee is tricked into running. After the initial execution and first computer takeover, APT attackers can compromise an entire enterprise in a matter of hours. It's easy to accomplish, but a royal pain to clean up.

Countermeasure: Detecting and preventing an APT can be difficult, especially in the face of a determined adversary. All the previous advice applies, but you must also learn to understand the legitimate network traffic patterns in your network and alert on unexpected flows. An APT doesn't understand which computers normally talk to which other computers, but you do. Take the time now to start tracking your network flows and get a good handle of what traffic should going from where to where. An APT will mess up and attempt to copy large amounts of data from a server to some other computer where that server does not normally communicate. When they do, you can catch them.

Other popular attack types such as SQL injection, cross-site scripting, pass-the-hash and password guessing aren't seen nearly at the same high levels as the five listed here. Protect yourself against the top five threats and you'll go a long way to decreasing risk in your environment.

More than anything, I strongly encourage every enterprise to make sure its defenses and mitigations are aligned with the top threats. Don't be one of those companies that spends money on high-dollar, high-visibility projects while the bad guys continue to sneak in using routes that could have easily been blocked. Lastly, avail yourself of a product or service that specializes in detecting APT-style attacks.

Facebook Messenger Spam Leads to Adware, Malicious Chrome Extensions

https://www.bleepingcomputer.com/news/security/facebook-messenger-spam-leads-to-adware-malicious-chrome-extensions/

[Aug24] A virulent spam campaign has hit Facebook Messenger during the past few days, according to recent warnings issued by Avira, CSIS Security Group, and Kaspersky Lab. The Facebook spam messages contain a link to what appears to be a video. The messages arrive from one of the user's friends, suggesting that person's account was also compromised. The format of the spam message is the user's first name, the word video, and a bit.ly or t.cn short-link.

Users that click on the links are redirected to different pages based on their geographical location and the type of browser and operating system they use. It's been reported that Firefox users on Windows and Mac are being redirected to a page offering a fake Flash Player installer. Kaspersky says this file installs adware on users' PCs.

On Chrome, the spam campaign redirects users to a fake YouTube page pushing a malicious extension. It is believed that crooks use this Chrome extension to push adware and collect credentials for new Facebook accounts, which they later use to push the spam messages to new users. **Users that encounter this spam campaign should avoid clicking on the malicious links, but also reach out to the person who sent the message and advise him to change his account credentials**. Reporting the spam messages to Facebook is also recommended.

U.S. Warship Collisions Raise Cyberattack Fears

http://www.securityweek.com/us-warship-collisions-raise-cyberattack-fears

A spate of incidents involving US warships in Asia, including a deadly collision this week off Singapore, has forced the navy to consider whether cyberattackers might be to blame. While some experts believe that being able to engineer such a collision would be unlikely, given the security systems of the US Navy and the logistics of having two ships converge, others say putting the recent incidents down to human error and coincidence is an equally unsatisfactory explanation. The USS John S. McCain collided with a tanker early Monday as the warship was on its way for a routine stop in the city-state, tearing a huge hole in the hull and leaving 10 sailors missing and five injured. The Navy announced Tuesday that remains of some of the sailors were found by divers in flooded compartments on the ship.

The Chief of US Naval Operations Admiral John Richardson said on Monday he could not rule out some kind of outside interference or a cyberattack being behind the latest collision, but said he did not want to prejudge the inquiry. His broader remarks suggested a focus on "how we do business on the bridge". "We're looking at every possibility," Richardson said, when asked about the possibility of a cyberattack, adding "as we did with Fitzgerald as well."

Just two months earlier in June, the USS Fitzgerald and a Philippine-flagged cargo ship smashed into each other off Japan, leaving seven sailors dead and leading to several officers being disciplined. There were also two more, lesser-known incidents this year - in January USS Antietam ran aground near its base in Japan and in May, USS Lake Champlain collided with a South Korean fishing vessel. Neither caused any injury. Admiral Scott Swift, commander of the US Pacific Fleet, has refused to rule out sabotage in Monday's incident, saying all possibilities are being examined. "We are not taking any consideration off the table," he told reporters in Singapore Tuesday, when asked about the possibility of a cyberattack in the latest incident.

High tensions- Analysts are divided on the issue, with some believing US Navy crews may simply be overstretched as they try to tackle myriad threats in the region, and pointing to the difficulties of sailing through waterways crowded with merchant shipping. But others believe something more sinister may be going on. Itar Glick, head of Israeli-based international cybersecurity firm Votiro, said the spate of incidents suggested that US Navy ships' GPS systems could have been tampered with by hackers, causing them to miscalculate their positions. "I think that hackers could try to do this, and if they are state sponsored they might have the right resources to facilitate this kind of attack," he told AFP. Glick, who says he used to work on cybersecurity for Israeli intelligence, said that China and North Korea would be the most likely culprits...

Spoofing- Glick pointed to a recent incident in June of apparent large-scale GPS interference in the Black Sea to illustrate that such disruptions are possible. The interference - **known as "spoofing"**, which disrupts GPS signals so ships' instruments show inaccurate locations - caused some 20 vessels to

have their signals disrupted, according to reports. Jeffery Stutzman, chief of intelligence operations for US-based cybersecurity firm Wapack Labs, told AFP he thought the possibility of a cyberattack being behind the latest incident was "entirely possible". "I would be very doubtful that it was human error, four times in a row," he said, referring to the four recent incidents. Still, other observers believe such a scenario to be unlikely. Zachary Fryer-Biggs, from defence consultancy Jane's by IHS Markit, said that even if something went wrong with the GPS system of a ship, other safety mechanisms should stop it from crashing, such as having people on watch. "The collision only occurs if several other safety mechanisms fail," he said.
Daniel Paul Goetz, from US-headquartered cybersecurity firm Lantium, added that causing a collision would be complicated, as it would involve knowing the exact location, speed and bearing of both ships involved. Goetz, who says his background is in US military intelligence, also pointed to the level of technology used to protect the navy from such threats. "The US military uses a GPS system that is highly secured, highly encrypted - the chances that somebody could take over US military ship is very close to zero," he said.

Samsung TV Owners Furious After Software Update Leaves Sets Unusable

https://www.theguardian.com/technology/2017/aug/24/samsung-tv-buyers-furious-after-software-update-leaves-sets-unusable

[Aug24] UK - Thousands of owners of high-end Samsung TVs have complained after a software update left their recently acquired £1,400 sets with blank, unusable screens. The Guardian has been contacted by a number of owners complaining that the TVs they bought – in some cases just two weeks ago – have been rendered useless by an upgrade sent out by Samsung a week ago. Others have been posting furious messages on the company's community boards complaining that their new TVs are no longer working. The company has told customers it is working to fix the problem but so far, seven days on, nothing has been forthcoming. The problem appears to affect the latest models as owners of older Samsung TVs are not reporting the issue.
Lohith Jajee, one of those affected, wrote: "We spent nearly £1,400 on this TV two weeks ago. It's holiday period in the UK and we thought kids would enjoy watching [a] new TV. To my horror, it stopped working from day two. What's even more frustrating is the customer service: all I get is 'we are aware of the issue and will get back'. Six days on and counting." Another person, posting on the Samsung community boards, wrote: "So here we are. Another morning without my TV working AND more importantly another morning with NO update from anyone at Samsung. "I honestly can't believe the incompetence that is being shown by a company of this size. The lack of communication is astounding and if I could take my TV back it would be there in a heartbeat."
This is not the first time Samsung customers have experienced problems after buying TVs. Last year Guardian Money reported that buyers had been left frustrated after their new TVs would not access the BBC iPlayer. The company, thought to be the world's biggest TV manufacturer, had sold the TVs without having the correct licensing agreements in place.
On Thursday Samsung is launching its Galaxy Note 8 smartphone in New York. It hopes the new model will restore the company's reputation after last year's "exploding" Note 7 problem that necessitated a mass recall. The company is yet to comment.
Follow-up to this story:
Samsung's own forum has a post entirely dedicated to the matter. As initially reported by The Guardian [above], it was thought that the update was affecting only 2017 sets, but some users have reported issues with TVs more than three years old. Samsung has just released a statement on the matter: "*Samsung is aware of a small number of TVs in the UK (less than 200) affected by a firmware update to 2017 MU Series TVs on 17th August. Once this issue was identified, the update was switched off and we're now working with each customer to resolve the issue. Any customers affected are encouraged to get in touch with Samsung directly (0330 7267864). We would like to apologise for the inconvenience caused to our customers."*

Identity Fraud Reaching Epidemic Levels, New Figures Show

https://www.theguardian.com/money/2017/aug/23/identity-fraud-figures-cifas-theft

UK - Identity theft has reached epidemic levels in the UK, with incidents of this type of fraud running at almost 500 a day, according to the latest figures. During the first six months of this year there were a record 89,000 cases of identity fraud, which typically involves criminals pretending to be an individual in

order to steal their money, buy items or take out a loan or car insurance in their name. The fraud prevention service Cifas, which issued the data, said these crimes were taking place almost exclusively online, and that the vast amount of personal data available on the internet and as a result of data breaches "is only making it easier for the fraudster".

… Identity fraud is one of the fastest-growing types of cybercrime, and experts say criminals are using increasingly sophisticated tactics. Fraudsters have increasingly been hacking into email accounts and then posing as a builder, solicitor or other tradesperson that the consumer has legitimately employed. Some customers have lost considerable sums after being duped into sending money to the bank accounts of criminals. In many cases, victims do not even realise they have been targeted until a bill arrives for something they did not buy, or they experience problems with their credit rating when applying for a mortgage or loan.

To carry out this kind of crime successfully, fraudsters need access to their victim's personal information such as name, date of birth, address and bank. Fraudsters get hold of this in a variety of ways, from stealing letters and hacking emails to obtaining data on the "dark web", and exploiting some people's willingness to share every detail of their life on social media. There have been cases of people being targeted after posting a photo of their new debit or credit card on Facebook, Twitter or Instagram - which means their 16-digit number, expiry date, cardholder name, account number and sort code are all on display, giving a fraudster much of what they need to steal that individual's identity.

The 89,000 identity frauds recorded - which may underestimate the true situation, as some people are too embarrassed to report incidents and may decide to write off any loss - is up 5% on the same period last year. While more than half of all identity fraud cases involve bank accounts and plastic cards, the latest figures show a sharp rise in incidents involving motor insurance: 2,070 during the latest six months, compared with 20 during the same period in 2016. The Insurance Fraud Bureau said it believed most of these cases were likely to involve people taking out fake motor policies - typically bought online from illegal **"ghost brokers"** – in order to avoid having to buy a genuine policy.

Cifas data is included in official crime statistics, and every day it sends about 800 fraud cases to the City of London police for potential investigation. Its advice to consumers includes: (1) Set privacy settings across all social media channels, and think twice before sharing details such as full date of birth. (2) Password protect devices. Keep passwords complex by picking three random words, such as "roverducklemon," and add or split them with symbols, numbers and capitals. (3) Install anti-virus software on laptops and any other personal devices and keep it up to date. (4) Download updates to software when prompted to – they often add enhanced security features.

The Pirate Bay Founders Ordered to Pay Music Labels $477,800 in Compensation

http://thehackernews.com/2017/08/the-pirate-bay-torrent.html

Two of the three co-founders of The Pirate Bay - Fredrik Neij and Gottfrid Svartholm Warg - have been ordered by a Finnish court to pay record labels $477,800 in compensation for copyright infringement on the site. Last year in a similar case, Helsinki District Court in Finland ordered Peter Sunde, the third co-founder of The Pirate Bay, to pay nearly $395,000 in damages to several major record labels, including Sony Music, Universal Music and Warner Music. However, Sunde did not pay any penalty yet, and instead, he later announced his plans to sue those record labels for defamation.

The Pirate Bay is still the world's most popular torrent website that has proven to be an elusive hub for illegal copyrighted contents, even after a series of raids and shutdown of its multiple domains, including the primary .SE domain. All the three co-founders of The Pirate Bay were facing criminal copyright infringement and abuse of electronic communications charges in a Belgian court but were acquitted after it was found that they sold The Pirate Bay file-sharing website in 2006.

The International Federation of the Phonographic Industry (IFPI), which represents the world's major labels, with support from Finnish Copyright Information and Anti-Piracy Center (CIAPC), filed a lawsuit in November 2011 in the Helsinki District Court against The Pirate Bay. In these last six years, Fredrik Neij and Gottfrid Svartholm never appeared in the court, neither they appointed someone to represent their defence, which eventually led the decision in favour of IFPI record labels. Besides ordering both the founders to jointly pay compensation of 405,000 euros (over $477,800) to record labels, the District Court also ordered them to "cease-and-desist" the illegal operations of The Pirate Bay, TorrentFreak reported. However, it is still unclear how Neij and Svartholm are supposed to do anything about stopping sharing of content on the site since they have no association with The Pirate Bay. It has also been reported that Neij, Svartholm, and Sunde also owes large sums of money to other copyright holders as a result of

various court judgments over the past few years. However, so far, none of those court penalties has been "satisfied," neither Sunde paid the fines imposed on him last year, and it is likely that this penalty will also go unpaid.

Germany: Microsoft Agrees to Stop Forcibly Downloading Windows Upgrades

https://www.bleepingcomputer.com/news/microsoft/germany-microsoft-agrees-to-stop-forcibly-downloading-windows-upgrades/

After an 18-month legal battle with Germany's Baden-Würtenberg consumer rights center, Microsoft admitted to wrongdoing when it downloaded over 6GBs of data on user devices during its Windows 10 push in mid and late 2015. In addition to recognizing its guilt, Microsoft has also agreed to cease any similar practice, at least in Germany, promising not to download any OS upgrade data until the user has given his express permission.

Investigation started in early 2016. The German consumer rights agency had started investigating Microsoft at the start of 2016 following a series of complaints from German users and organizations. Users accused Microsoft of clogging their Internet bandwidth and filling their hard drives with over 6GBs of data needed for the Windows 10 upgrade, which many users didn't want to install anyway. At the time, this was only one of the many controversial practices that Microsoft used to push Windows 10 on its users. The company was also accused and investigated for breaking user privacy and collecting telemetry data without giving users an option to disable the behavior. This practice was later fixed with the release of the Windows 10 Creators Update, this spring. Additionally, users criticized Microsoft for pushing ads inside Windows 10 for various products such as Edge, Cortana, and Bing. In other more worrisome cases, Microsoft stood accused of forcibly starting the Windows 10 upgrade process, even without the users' permission. Some of these upgrades didn't go as smooth as expected, and some users filed a class-action lawsuit this March.

Microsoft dragged out the investigation for 18 months. In a press release published on Monday [Aug21], the Baden-Würtenberg consumer rights center said it was glad Microsoft decided to admit to all accusations but was displeased that the OS maker "unnecessarily hindered a quick legal clarification" after several "procedural wrinkles" that dragged out the investigation for more than a year and a half. Microsoft signed a declaration admitting its practice and will face steep penalties if it breaks its promise.

And Now, This:

Scientists Launch Virtual Reality Game to Detect Alzheimer's

http://www.ctvnews.ca/health/scientists-launch-virtual-reality-game-to-detect-alzheimer-s-1.3566302

Sea Quest Hero is more than just the usual computer game in which players find their way through mazes, shoot and chase creatures - it also doubles as scientists' latest tool for studying Alzheimer's disease. The game - downloadable from Tuesday in its virtual reality version - seeks to stimulate players' brains through a series of tasks based on memory and orientation skills, while gathering data to research dementia.

One of the first symptoms of Alzheimer's is loss of navigational skills. But data comparing cognitive response across a broad spectrum of ages is rare, and this is what the game seeks to provide. The game - billed as the "largest dementia study in history" - has been developed by Deutsche Telekom, Alzheimer's Research UK, and scientists from University College London and the University of East Anglia. The mobile version, which came out in 2016, has already been downloaded three million times in 193 countries. Playing the game for just two minutes, the website said, generates the same amount of data scientists would take five hours to collect in similar lab-based research. With the equivalent of 63 years already played, scientists now have some 9,500 years' worth of dementia research to go through.

"That gave us an enormous amount of information and it really allowed us to understand how men and women of different ages navigate in the game," David Reynolds, chief scientific officer at Alzheimer's Research UK, told AFP.

Resolving the tasks requires the use of "different parts of your brain and different parts of your brain are used in different ways by different types of dementia - so it allows us to link what someone can do to what is going on in their brain," Reynolds added. The addition of virtual reality will provide yet another layer of data. "The headset technology is helping to track where the person is looking at all times as well as where they're going," Lauren Presser, one of the game's producers, told AFP. "So we get to know whether people are lost and how they behave in those situations... Every single one of those experiments is helping us gather data around spatial navigation."

Nearly 50 million people around the world suffer from dementia and Alzheimer's according to the latest estimates. That could balloon to 132 million by 2050. There is no cure for the disease, but the game's creators hope it could eventually enable diagnosis and treatments of patients far earlier than is currently possible. Reynolds said playing the game could in itself help with prevention. "We know keeping your brain fit and active, like keeping your body fit and active, is good and is helping to reduce your risk of dementia or slowing its progression down if you have it," he said.

Feel free to forward the Digest to others that might be interested.
Click Unsubscribe to stop receiving the Digest.

****

For previous issues of Security News Digest, visit the current month archive page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest
To learn more about information security issues and best practices, visit us at:
Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

****