Security News Digest
February 28, 2017

Love Security - Love Your Data Quiz- the February Quiz

Starting tomorrow: March is Fraud Prevention Month

Happening Now: Here's Why The Internet Isn't Working Today (Amazon Web Services Outage)

http://money.cnn.com/2017/02/28/technology/amazon-web-services-outages/

The internet has been a little difficult for people to navigate on Tuesday. *Amazon Web Services, the popular storage and hosting platform used by a huge range of companies, reported that it is experiencing intermittent outages*. People are reporting outages and delays on services like Slack, Trello, Sprinklr, Venmo *and even Down Detector, which is the site that shows where real time outages are occurring*. Affected sites said the outage began around 12:40 p.m. ET. *The outage didn't just affect websites - AWS clients that use cloud storage could also be impacted. Nest customers reported widespread issues with their cameras, and the company tweeted that it was likely because of the AWS outage*.

Amazon acknowledged that it's having issues. In a note on its website, the company specified that it is the Simple Storage Service (S3) tied to its US-EAST-1 servers in Northern Virginia. "AWS services and customer applications depending on S3 will continue to experience high error rates as we are actively working to remediate the errors in Amazon S3." *An AWS spokesperson said the company believes it has identified the cause of the outage and is working to repair it*.

iCloud Experiencing Slow Performance as AWS Outage Affecting Multiple Internet Services

https://9to5mac.com/2017/02/28/icloud-outage-aws-slow-performance/

…Specifically, Apple says that iCloud Backup, iCloud Drive, iCloud Notes, iCloud Web Apps, iWork for iCloud, and Photos are experiencing performance issues. ..You can see how the new design [of the System Status Site] handles ongoing issues as well as recent issues on apple.com/support/systemstatus currently.

And Now, Today's Security News Digest Articles:

Navy's Mishandling of Classified Documents Spawns Series of Investigations

http://www.cbc.ca/news/politics/defence-leaks-inquiries-1.4001819

The Canadian military conducted almost a dozen formal internal investigations into the "loss or compromise" of classified information during a six year period, and over half of them involved the navy, internal defence department data shows. The handling - or mishandling - of secrets was a growing concern among the top brass and civilian leadership even before the recent suspension of the country's deputy military commander, Vice-Admiral Mark Norman. He was relieved of his responsibility, but not stripped of command, in early January after the RCMP opened what sources have said is a national security investigation. The Mounties, although they will not confirm or deny it, are looking for the source of leaks, possibly involving the federal government's multi-billion dollar shipbuilding program.

Last summer, the chief of defence staff, Gen. Jonathan Vance, and the deputy defence minister, John Forster, issued a directive that "re-emphasized" the proper handling of documents and data and took additional action to "prevent unauthorized disclosure of classified information," said Suzanne Parker, a spokeswoman for the department. Not only were military and civilian staff at the Department of National Defence subject to the formal notice, but civilian contractors embedded in the department were given a reminder and training. *Between 2010 and the end of 2016, the military conducted 11 boards of inquiry into the loss or jeopardizing of secret information, according to figures from the department's administrative investigation support centre. At least six of them involved the navy, and half of those*

investigations fell within the jurisdiction of the Pacific fleet headquarters in Esquimalt, B.C. Another spokeswoman, Ashley Lemire, said the bulk of the cases took place between 2010 and 2014 and the number of inquiries has started to taper off with no investigations recorded last year.

RCMP Commissioner Warns Continued IT Failures Will Have 'Catastrophic' Consequences

http://www.cbc.ca/news/politics/rcmp-it-commissioner-safety-1.3998221

Canada's top cop is warning that ongoing computer network failures and slipshod service from Shared Services Canada could have "catastrophic" consequences for police and the public. CBC News has obtained a blistering Jan. 20, 2017, memo to Public Safety Minister Ralph Goodale in which *Commissioner Bob Paulson details how critical IT failures have increased by 129 per cent since the beleaguered department took over tech support for the entire government five years ago*. Not only that, the memo says, *the duration of each outage has increased by 98 per cent*. "Its 'one size fits all' IT shared services model has negatively impacted police operations, public and officer safety and the integrity of the criminal justice system," reads the memo.

The document appears to respond to a request for more information after a series of CBC News reports on the RCMP's long-standing dissatisfaction with Shared Services Canada (SSC). Despite the agency's creation of special teams and committees to address shoddy service and repeated computer outages, Paulson said minimal progress has been made. *The commissioner bolstered his arguments by enclosing an appendix of recent critical incidents to show just how little appreciation or understanding there is for operational law enforcement requirements*. Among the examples provided is more *information about an 11-hour network computer outage on Jan. 18 that downed every Mountie's BlackBerry, affected dispatching and prevented the RCMP and 240 other police forces from accessing the Canadian Police Information Centre (CPIC) database*. "A lack of CPIC access severely limits awareness of what threats officers may face when they respond to a call," wrote Paulson. "If a major crime or incident were to occur during an outage of these systems, then the results could be catastrophic."

Loblaw Resets PC Plus Passwords Following Breach

http://www.canadiansecuritymag.com/news/retail/loblaw-resets-pc-plus-passwords-following-breach

Toronto - Loblaw has reset passwords for all its PC Plus rewards collectors' online accounts *after points were stolen from some members' accounts*. The company posted a warning on its website saying it requires all members to create new passwords - regardless of whether or not they changed them following the recent security breach. Earlier this month, Loblaw urged members to create unique, secure passwords after some people noticed their points were missing. The company said at the time that *the breach stemmed from people using favourite or weak username and password combinations across multiple sites. Those were stolen from other sites and used to access PC Plus accounts*. [security awareness reminder: this is the reason for using different passwords for each account, so if one is breached, the hackers won't be able to access the user's other accounts – they will try because their efforts frequently pay off]

Victoria Tech Sector Aims High: $10 Billion in Revenues by 2030

http://www.timescolonist.com/business/victoria-tech-sector-aims-high-10-billion-in-revenues-by-2030-1.10337663#sthash.aJyctJ39.dpuf

Victoria's high-flying tech sector has set a bold new goal for itself - to have its constituent firms more than double their existing combined revenue to $10 billion by 2030. "I think it's ambitious, but entirely feasible," said Dan Gunn, chief executive of the Victoria Innovation, Advanced Technology and Entrepreneurship Council, which came up with the target at its last board meeting. "Our last revenue numbers showed revenues over $3 billion and that number is now three years old. It's probable the tech sector's revenue is approaching, if it hasn't already eclipsed, $4 billion," he said. "So we're talking about a little more than doubling in size in 13 years. The sector has shown it can do that." Gunn said what has held the city back in terms of tech growth is the same problem many tech hubs face: a lack of talent. "But as you get bigger, the gravity you create gets stronger and then you attract more of the resources you need," he said. *The tech sector in Victoria is on its way as it has grown to include more than 880 businesses and employs more than 15,000 directly. It also counts another 3,000 consultants and 5,000 others who work in tech jobs within larger firms and government*. VIATEC's own membership has doubled to 526 members over the last two years.

Ottawa Explores Potential of 'Blockchain,' Billed as Next-Generation Internet Tech

https://www.thestar.com/business/2017/02/28/ottawa-explores-potential-of-blockchain-billed-as-next-generation-internet-tech.html

Ottawa- An emerging technology has caught the eye of the innovation-obsessed federal government - a platform so packed with potential, many experts believe it could comprise the foundation for the next generation of the Internet. Blockchain, as it's known, holds a vast amount of promise for transforming business sectors and the lives of ordinary people around the world, although some say it's too early to say how broad the technology's reach could be. *Like a giant digital bulletin board, blockchain creates an online ledger or database where records - financial transactions, for instance - can be shared, moved and maintained on a transparent network, all without compromising security. With such activities available to be seen by a blockchain's many collaborators, the system is inherently secure, making it far less vulnerable to tampering, hacking and corruption than current systems, which depend on information being managed by intermediaries*. Experts say Canada has shown considerable potential in these early days of blockchain - and they believe it's key for the country to help create conditions to keep the momentum going. ..In December, senior government officials, including then-international trade minister Chrystia Freeland, met to discuss the concept with executives from companies, big banks, regulators and the tech sector. The attendees at the meeting explored the feasibility of Canada becoming a global hub for the blockchain "revolution," according to the agenda.

Creepy Internet of Things [IoT] Teddy Bear Leaks Over 2 Million Parents' and Kids' Voice Messages

https://arstechnica.com/security/2017/02/creepy-iot-teddy-bear-leaks-2-million-parents-and-kids-voice-messages/

A maker of Internet-connected stuffed animal toys has exposed more than 2 million voice recordings of children and parents, as well as e-mail addresses and password data for more than 800,000 accounts. The account data was left in a publicly available database that wasn't protected by a password or placed behind a firewall, according to a blog post published Monday by Troy Hunt, maintainter of the Have I Been Pwned?, breach-notification website. He said searches using the Shodan computer search engine and other evidence indicated that, *since December 25 [Christmas Day!] and January 8, the customer data was accessed multiple times by multiple parties, including criminals who ultimately held the data for ransom*. *The recordings were available on an Amazon-hosted service that required no authorization to access*.

The data was exposed by Spiral Toys, maker of the CloudPets line of stuffed animals. The toys record and play voice messages that can be sent over the Internet by parents and children. The MongoDB database of 821,296 account records was stored by a Romanian company called mReady, which Spiral Toys appears to have contracted with. *Hunt said that, on at least four occasions, people attempted to notify the toy maker of the breach. In any event, evidence left behind by the ransom demanders made it almost certain company officials knew of the intrusions.*

…**Internet-connected toys? No thanks.** ..The lesson that emerged *long ago* is that the security of so-called Internet of things products is so poor that it often outweighs any benefit afforded by an Internet-connected appliance. As the CloudPets debacle underscores, the creep factor involved in Internet-connected toys makes the proposition even worse.

Hacker Shows How Easy it is to Hack People While Walking Around in Public

http://thehackernews.com/2017/02/hacking-in-public.html

Wi-Fi enabled devices - widely known as the Internet of Things (IoT) - are populating offices and homes in greater and greater numbers. From smartphones to connected printers and even coffee makers, most of these IoT devices have good intentions and can connect to your company's network without a problem. However, as the Internet of Things (IoT) devices are growing at a great pace, they continue to widen the attack surface at the same time, giving attackers a large number of entry points to affect you some or the other way. The attackers can use your smart devices to gain backdoor entry to your network, giving them the capability to steal sensitive data, such as your personal information, along with a multitude of other malicious acts.

An interesting attack scenario has recently been demonstrated by one of the renowned hackers, Jayson Street, who said all it is needed is to walk around with the right device to get into someone's device.

Before we jump into the technical details of the attack, [article has a video showing that how easy it is to hack smartphones and laptops in a crowded place by setting up an **EvilAP** (malicious access point).]
Here's How the Attack Works: Street used a simple penetration testing device and an internet connection to pwn [gain ownership of] people around him. *Technically, Street's hacking device automatically set up an 'Evil Twin Attack,' in which an attacker fools wireless users into connecting their smartphones and laptops to an evil (malicious) hotspot by posing as a legitimate WiFi provider. Once connected, all of the victim's information flows directly into the attacker's device, allowing cybercriminals to secretly eavesdrop on the network traffic and steal passwords, financial and other sensitive data and even redirect you to malware and phishing sites*.
How to Prevent Evil Twin Wi-Fi Attacks
Pwnie Express released its yearly industry report: Internet of Evil Things, providing insight on products that the IT professionals should be wary of. Using the report and additional information from security researchers at Pwnie, *we have listed five quick steps you can implement in order to prevent yourself or your workplace from being compromised*.
(1.) Turn your Wi-Fi Off: Turn off Wi-Fi devices when you are not using them, especially on the weekends - it saves energy and minimizes your exposure to hackers.
(2.) Use it or Lose it: Once the product is in your office, *turn off the functions you aren't using*. Enabled functionality usually comes with increased security risks. Also, make sure you review the products before you bring them into the workplace. If it is already there, do not be shy about calling customer service and walking through the steps required to shut down any unused functions.
(3.) Change Your Passwords: It is important *never to use the default credentials*. Set up strong, secure passwords to secure your devices.
(4.) Research Your Purchase: Before you even buy a product, always research what you're buying and make sure you know how to update any software associated with that device. Look for devices, systems, and services that make it easy to upgrade the device and inform the end user when updates are available.
(5.) Trust and Verify Every Device: Be aware of any device from brands known to have more security issues than others. The personalization of corporate hardware, including mobile hotspot vendors, is one of the top threats to network security.

Cloudbleed: Big Web Brands Leaked Crypto Keys, Personal Secrets Thanks to Cloudflare Bug

http://www.theregister.co.uk/2017/02/24/cloudbleed_buffer_overflow_bug_spaffs_personal_data/
Big-name websites leaked people's private session keys and personal information into strangers' browsers, due to a Cloudflare bug uncovered by Google researchers. As we'll see, a single character – '>' rather than '=' – in Cloudflare's software source code sparked the security blunder. *Cloudflare helps companies spread their websites and online services across the internet*. Due to a programming blunder, for several months Cloudflare's systems slipped random chunks of server memory into webpages, under certain circumstances. That means if you visited a website powered by Cloudflare, you may have ended up getting chunks of someone else's web traffic hidden in your browser page. For example, *Cloudflare hosts Uber, OK Cupid, and Fitbit, among thousands of others. It was discovered that visiting any site hosted by Cloudflare would sometimes cough up sensitive information from strangers' Uber, OK Cupid, and Fitbit sessions. Think of it as sitting down at a restaurant, supposedly at a clean table, and in addition to being handed a menu, you're also handed the contents of the previous diner's wallet or purse.* This leak was triggered when webpages had a particular combination of unbalanced HTML tags, which confused Cloudflare's proxy servers and caused them to spit out data belonging to other people - even if that data was protected by HTTPS. Normally, this injected information would have gone unnoticed, hidden away in the webpage source, *but the leak was noticed by security researchers - and the escaped data made its way into the Google cache and the hands of other bots trawling the web*.
Timeline. The blunder was first spotted by Tavis Ormandy, the British bug hunter at Google's Project Zero security team, when he was working on a side project last week. He found large chunks of data including session and API keys, cookies and passwords in cached pages crawled by the Google search engine. These keys can be used to log into services as someone else. "The examples we're finding are so bad, I cancelled some weekend plans to go into the office on Sunday to help build some tools to clean up," he said today in an advisory explaining the issue. "I've informed Cloudflare what I'm working on. I'm finding private messages from major dating sites, full messages from a well-known chat service, online

password manager data, frames from adult video sites, hotel bookings. We're talking full https requests, client IP addresses, full responses, cookies, passwords, keys, data, everything." *Ormandy said that the Google team worked quickly to clear any private information and that Cloudflare assembled a team to deal with it. He provisionally identified the source of the leaks as Cloudflare's ScrapeShield application, which is designed to stop bots copying information from websites wholesale, but it turns out the problems ran deeper than that*.

World's Largest Spam Botnet [Necurs] Adds DDoS Feature

https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-adds-ddos-feature/

***Necurs**, the world's largest spam botnet with nearly 5 million infected bots, of which one million active each day, has added a new module that can be used for launching DDoS attacks*. Like most of today's top-tier malware families, Necurs' functionality is broken down across several modules that are loaded on infected computers in real-time, only when needed.

DDoS feature hidden in the Necurs Proxy module –[see article for technical details]

A Necurs DDoS attack would easily break every DDoS record. It is worth mentioning that *at the time of this article no DDoS attack has ever been attributed to the Necurs botnet. If Necurs would ever decide to use its bots for a DDoS attack, the scale of such an attack would be beyond any other DDoS attack we've seen in the past*. The sheer size of the Necurs botnet, even in its worst days, dwarfs all of today's IoT botnets. The largest IoT botnet ever observed was Mirai Botnet #14 that managed to rack up around 400,000 bots towards the end of 2016. On the other hand, Necurs reached these massive numbers by infecting classic desktop computers. The botnet grew so big because it was never used for disruptive DDoS attacks that usually tend to get the attention of law enforcement agencies, who then coordinate takedown attempts. *For most of its lifespan, the authors of the Necurs botnet have used it to send spam from infected hosts, usually carrying the Dridex banking trojan, and more recently the Locky ransomware*.

DDoS feature unlikely to be ever deployed. It is currently a mystery why Necurs operators decided to add a DDoS feature to their botnet, but according to different people, this decision doesn't make any sense. ..Outside a higher revenue stream the Necurs gang stands to earn from spam, we must also take into consideration other reasons why it's highly unlikely that we're going to see DDoS attacks from Necurs. [see article for discussion]

30,000 Taxpayers Affected by W-2 Phishing Scams, IRS [Internal Revenue Service] Warns

https://hotforsecurity.bitdefender.com/blog/30000-taxpayers-affected-by-w-2-phishing-scams-irs-warns-17736.html

Now that tax season has begun, IRS-related phishing scams are back. This year, hackers are expanding their victim range to include school districts, NGOs [non-government organizations] and tribal organizations, according to an IRS alert released in February. *"It can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns.* We need everyone's help to turn the tide against this scheme," IRS Commissioner John Koskinen said.

Phishing scams are on the dirty dozen list put together by the IRS, and this time *the focus is on W-2 forms, "the most dangerous email scams the agency has seen in a long time." Also known as Business Email Compromise (BEC) attacks*, compromised W-2 form scams affected over 30,000 taxpayers and 145 organizations in 2016. Confirmed victims include school systems, a restaurant, a software company and others in healthcare, finance, manufacturing and utilities.

Other dangers on the dirty dozen list for 2017 are phone scams, identity theft, return preparer fraud, fake charities, inflated refund claims, excessive claims for business credits, falsely padding deductions on returns, falsifying income to claim credits, abusive tax shelters, frivolous tax arguments and offshore tax avoidance. "We continue to work hard to protect taxpayers from identity theft and other scams," said Koskinen. "*Taxpayers can and should stay alert to new schemes which seem to constantly evolve*. We urge them to do all they can to avoid these pitfalls – whether old or new."

Teens Charged with Sharing Child Porn on Social Media

http://www.canada.com/technology/teens+charged+with+sharing+child+porn+social+media/12788234/story.html

Six teenagers in New Jersey who may have been inspired by a movie about crime being legalized for one night a year have been charged with sharing nude photos of other teens online. The Passaic County prosecutor's office says a 14-year-old boy and two 15-year-old girls created social media accounts seeking nude photos. Three boys, ages 14 and 15, provided images of a 13-year-old and two 15-year-old girls without their consent. The accounts had the name "Purge" in some form as the title. Deputy

First Assistant Prosecutor Michael DeMarco says that appears to be a reference to "The Purge" horror film series. Law enforcement elsewhere have reported similar incidents since the first of the three movies were released in 2013. The six teens face child pornography and invasion-of-privacy charges.

Removing User Admin Rights Mitigates 94% of All Critical Microsoft Vulnerabilities

https://www.bleepingcomputer.com/news/microsoft/removing-user-admin-rights-mitigates-94-percent-of-all-critical-microsoft-vulnerabilities/

Just by preventing access to admin accounts, a system administrator could safeguard all the computers under his watch and prevent attackers from exploiting 94% of all the critical vulnerabilities Microsoft patched during the past year. This is the conclusion of a study carried out by cyber-security firm Avecto for the second year in a row, after, at the same time last year, it discovered that a sysadmin could mitigate 86% of all critical vulnerabilities Microsoft patched in 2015, just by taking the same action and disabling admin rights. *What this growth from 86% to 94% means is that the security of Microsoft products is getting better, if users would only start following industry best practices and stop using admin accounts for daily work*.

Removing admin rights thwarts all IE, Edge, Office 2016 security threats

Even more interesting is that the Avecto 2016 report highlights that if sysadmins had forced users to utilize a low-privileged account instead of an admin-level profile, they would have mitigated 100% of all critical Internet Explorer and Microsoft Edge browser vulnerabilities patched during the past year. The same 100% threshold also stands for Office 2016, showing the large number of security threats a system admin could mitigate just by a proper user management policy. "Times have changed; removing admin rights and controlling applications is no longer difficult to achieve," noted Mark Austin, co-founder, and co-CEO at Avecto, an opinion he also shared with Sami Laiho, a famous Windows security expert. The above statistics do not include medium and low-level security flaws because their impact was already deemed insufficient to receive a "critical" classification, regardless of the user level access they needed to execute from. [The chart in the article] shows the bigger picture. The simple conclusion of the Avecto report is that most companies and users would be able to avoid malware infections and network compromises if they'd only follow the example of Linux users and avoid using admin accounts as their primary profiles.

And Now, This:

Study Reveals Bot-on-Bot Editing Wars Raging on Wikipedia's Pages

https://www.theguardian.com/technology/2017/feb/23/wikipedia-bot-editing-war-study

For many it is no more than the first port of call when a niggling question raises its head. Found on its pages are answers to mysteries from the fate of male anglerfish, the joys of dorodango, and the improbable death of Aeschylus. But beneath the surface of Wikipedia lies a murky world of enduring conflict. A new study from computer scientists has found that the online encyclopedia is a battleground where silent wars have raged for years.

Since Wikipedia launched in 2001, its millions of articles have been ranged over by software robots, or simply "bots", that are built to mend errors, add links to other pages, and perform other basic housekeeping tasks. In the early days, the bots were so rare they worked in isolation. But over time, the number deployed on the encyclopedia exploded with unexpected consequences. *The more the bots came into contact with one another, the more they became locked in combat, undoing each other's edits and changing the links they had added to other pages. Some conflicts only ended when one or other bot was taken out of action*. "The fights between bots can be far more persistent than the ones we see between people," said Taha Yasseri, who worked on the study at the Oxford Internet Institute. "Humans usually cool down after a few days, but the bots might continue for years."

The findings emerged from a study that looked at bot-on-bot conflict in the first ten years of Wikipedia's existence. The researchers at Oxford and the Alan Turing Institute in London examined the editing histories of pages in 13 different language editions and recorded when bots undid other bots' changes. They did not expect to find much. *The bots are simple computer programs that are written to make the encyclopedia better. They are not intended to work against each other*. "We had very low expectations to see anything interesting. When you think about them they are very boring," said Yasseri. "The very fact that we saw a lot of conflict among bots was a big surprise to us. They are good bots, they are based on good intentions, and they are based on same open source technology." While some conflicts mirrored those found in society, such as the best names to use for contested territories, others were more

intriguing. Describing their research in a paper entitled Even Good Bots Fight in the journal Plos One, the scientists reveal that among the most contested articles were pages on former president of Pakistan Pervez Musharraf, the Arabic language, Niels Bohr and Arnold Schwarzenegger.

…..**Artificial Intelligence:** Earlier this month, researchers at Google's DeepMind set AIs against one another to see if they would cooperate or fight. When the AIs were released on an apple-collecting game, the scientists found that the AIs cooperated while apples were plentiful, but as soon as supplies got short, they turned nasty. It is not the first time that AIs have run into trouble. In 2011, scientists in the US recorded a conversation between two chatbots. They bickered from the start and ended up arguing about God. Hod Lipson, director of the Creative Machines Lab at Columbia University in New York, said the work was a "fascinating example of the complex and unpredictable behaviours that emerge when AI systems interact with each other."

"Often people are concerned about what AI systems will ultimately do to people," he said. "But what this and similar work suggests is that what AI systems might do to each other might be far more interesting. And this isn't just limited to software systems – it's true also for physically embodied AI. Imagine ACLU drones watching over police drones, and vice versa. It's going to be interesting."

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

****