BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest
February 13, 2018

Tomorrow is Valentine’s Day!
Love yourself and your identity with some great tips:
'Love Your Online Life' Security Quiz

Mysterious Missed Calls on Cellphones Part of World-Wide Scam 🇨🇦

https://globalnews.ca/news/4012633/mysterious-missed-calls-on-cellphones-part-of-world-wide-scam/

A telephone scam sweeping Calgary and Alberta has prompted a warning to ignore missed overseas calls. Tony Tighe reports. The **one-ring scam** is back and is catching a new wave of unsuspecting cellphone owners. The calls show up on your phone as a missed call and come from overseas locations like Albania, Macedonia or the Seychelles.

Ebun Edewole got one while she was sleeping at 2 a.m. and thought it was a relative from overseas. She waited until morning to call back, but when she checked again, didn’t recognize the number. “Ever since then, I get at least one a day, maybe in the morning and then in the evening,” Adewole said. “I thought maybe my phone number was on a weird website or something or I thought it was a telemarketer. “It wasn’t until I started looking it up that I thought it might be a scam.”

According to the Calgary Better Business Bureau (BBB), it’s called the one-ring scam or the Japanese name “Wangiri” – where it started. The call disconnects right away and the people behind it are hoping you call back out of curiosity, according to Leah Brownridge with the BBB. “They may be connected to some kind of toll service. You may hear music playing, you may hear an automated recording of some sort,” she said. **“The longer you stay on the line, the chances are your phone bill is going to be racked up with long distance charges.”** Brownridge says past reports have recorded long distance rates anywhere from $20 per minute to hundreds of dollars.

Global contacted Rogers Communications and they are aware of the fraudulent activity and are monitoring it. They issued a warning on social media. “If you receive a call from an unknown international number that disconnects immediately it could be part of a world-wide scam … don’t call back.” It’s not clear if customers have to pay a bill if they call the number back, but Rogers says customers who have any questions about their account are asked to contact RCI. Adewole has been trying to block the numbers but each one is different. “Ever since then, **I’ve been warning my friends and my family not to answer any calls they don’t know**.”

The Driverless Revolution: Canadian Companies Bracing for Hackers with ‘Nefarious’ Intent 🇨🇦

https://globalnews.ca/news/4011089/the-driverless-revolution-canadian-companies-bracing-for-hackers-with-nefarious-intent/

When it comes to hacking driverless cars, the nightmare scenarios are almost too frightening to contemplate. Imagine a terrorist group plowing a handful of cars – unmanned – into a crowd. Or someone forcing a school bus travelling down a highway off the road. Or hackers halting an entire fleet of transport trucks and bringing the Trans-Canada Highway to a dead stop, costing the economy millions. Hollywood has already honed in on this potential, with movies like *The Fate of the Furious* depicting supervillains sowing chaos by steering hundreds of hacked cars through New York City. But as moviemakers let their imaginations run wild, manufacturers, governments and tech companies around the globe have stayed firmly rooted in reality. **And the reality is hacking a car remains difficult, and a Canadian city full of nothing but automated vehicles is probably decades away**.

Still, all these stakeholders acknowledge that complacency would be dangerous. The computer systems embedded in cars on the road right now have already proven vulnerable. And some of those vulnerabilities will persist when humans move out of the driver’s seat. Last month, Canada’s Senate released a long-awaited report into automated vehicles, and cybersecurity was a central theme. The report revealed that as industry speeds into the future, government regulation and coordination hasn’t kept pace. “Senators believe strong cybersecurity measures are essential to maintain public safety and public confidence in this new technology,” the senators wrote. **“These vehicles collect a vast amount of data and could be the target of hackers who want to use the vehicles for nefarious purposes.”** [lengthy interesting article has more discussion…]

Canada to Launch New Border Security App that Could Go Global

http://www.cbc.ca/news/technology/canada-to-launch-new-border-security-app-that-could-go-global-1.4529162

The federal government is embarking on a new pilot program that will allow people to cross borders faster if they create a digital profile filled with their personal information on their mobile devices. The **Known Traveller Digital Identity** is a joint venture between the governments of Canada and the Netherlands, and will be tested first on travellers going between those countries. The plan is to have it ready for a wider global rollout by 2020.

The project announcement was made at the Davos World Economic Forum last month but has mostly flown under the radar. According to the World Economic Forum document outlining the program, international traveller arrivals are expected to jump from 1.2 billion in 2016 to 1.8 billion by 2030. This will increase risk and security requirements for the aviation and travel and tourism sectors. Much like other trusted-traveller programs — such as Nexus, which allows people quicker movement between Canada and the U.S. — **the Known Traveller Digital Identity program will ask travellers for detailed personal information for pre-screening, including university education, bank statements and vaccination records**.

Border expert Bill Anderson said security officials are keen to get people screened well before they pack their bags for a trip. "The prevailing paradigm in border management is that we need to have risk assessment, and we need to identify those people who are very, very low risk so that you can focus your resources on the ones that you haven't identified as low risk," said the head of the Cross-Border Institute at the University of Windsor. **The pilot program will also make use of biometrics like retina and facial recognition for quicker traveller identification**.

Technology company Accenture is helping develop the program. It said user information will be safeguarded and users will be able to decide whom they want to share their information with, and when, on a case-by-case basis. **Accenture said keeping users in control of their data will be critical.** "No personal information is stored on the ledger itself, ensuring that personal information is not consolidated in one system, which would make it a high value target for subversion," the company said in a statement to CBC News. In addition to providing personal information before travelling, **user profiles would be automatically updated as they move around the world**. The more borders they cross, the more trusted they will become, said Anderson. In some ways, the program takes a page from private tech companies such as Google and Facebook that have become experts in creating profiles about their users. "It's a crazy world where, you know, Google is able to provide information to people in e-commerce that's more detailed about you than what these security agencies have," said Anderson.

Anderson says critics argue the advanced screening programs create a two-tiered travel system, with those not signed up ending up in longer lines and getting poorer service. Nina Brooks is the director of security for Airports Council International, which represents nearly 2,000 airports. Her organization supports the development of these new technologies, but also wants a system that creates a similar experience for all travellers. "In the long term, I think we're looking for the use of some of those concepts for the broader audience, for all travellers, and actually expediting travel for everybody, rather than a specific group of trusted travellers," she said.

Destructive Malware Wreaks Havoc at PyeongChang 2018 Winter Olympics

https://www.bleepingcomputer.com/news/security/destructive-malware-wreaks-havoc-at-pyeongchang-2018-winter-olympics/

Destructive malware intent on sabotaging PCs is to blame for the IT problems reported during the PyeongChang 2018 Winter Olympics opening ceremony. The issues, first reported on Friday by UK paper The Guardian, consisted of failing Internet and television systems for on-site journalists attending and reporting the opening ceremony. **While initially, Olympics organizers were quiet, officials finally admitted on Sunday that the IT failures were no accident and their network has been the victim of a malicious and coordinated cyber-attack.**

New details about these attacks came to light earlier today when security researchers from Cisco's Talos division published new research on the malware used by attackers. According to Cisco researchers,

attackers deployed a never-before-seen malware strain that was intent on data destruction and data destruction only. "There does not appear to be any exfiltration of data," Cisco Talos researchers Warren Mercer and Paul Rascagneres said about this malware, **which they named Olympic Destroyer. "The samples analysed appear to perform only destructive functionality."** "The destructive nature of this malware aims to render the machine unusable by deleting shadow copies, event logs and trying to use PsExec & WMI to further move through the environment. This is something we have witnessed previously with BadRabbit and Nyetya," Mercer and Rascagneres added.

How a destructive attack takes place- Cisco has an in-depth analysis of this threat, but we summarized an Olympic Destroyer attack below, in easy to understand steps: [interested readers can access the link to the analysis, and read the set of technical steps, by going to the article]

Murky attribution, as always- As for attribution, things are murky, as they have always been when it comes to cyber-espionage operations. The two most obvious culprits are North Korea (South Korea and North Korea are still technically at war, North Korea has a long history of hacking its southern neighbor) and Russia (ICO has recently banned a large number of Russian athletes from participating in the Olympics).

Nonetheless, some observers will be quick to pile on the idea that this is most likely a Russian cyber operation. The reasons are plenty, starting with a Twitter account that many believe is operated by Russian intelligence and which has recently dumped large amounts of hacked information in an attempt to smear the International Olympic Committee following their ban of Russian athletes. Further, Olympic Destroyer and Bad Rabbit both use hardcoded credentials for lateral movement, an obvious clue that links - at least at the M.O. level - the two strains together. Last year, Ukrainian intelligence and a CIA report linked the NotPetya and Bad Rabbit ransomware outbreaks to Russian intelligence operations, and voices will be quick to point out that Olympic Destroyer is a more refined version of Bad Rabbit.

But things aren't as clear as they look. For example, Jay Rosenberg of Intezer Labs told *Bleeping Computer* earlier today that the malware's code has more links to cyber tools used by Chinese hackers in the past, rather than North Korea or Russia.

"Intezer has found, both in the malware targeting the Olympics from the report published by McAfee and in the report by Cisco Talos, that there are several minor code connections to known Chinese threat actors," Rosenberg told *Bleeping Computer*, also adding that his company will release a more in-depth report later on, as they have more time to analyze the samples unearthed by Cisco Talos researchers.

Two weeks ago, McAfee researchers published a report on a different strain of Powershell-based malware that was used to target Olympics organizers before the event's start.

Hackers Made $5,000 a Night Off Crypto Users by Impersonating Elon Musk and Bill Gates

https://hotforsecurity.bitdefender.com/blog/hackers-made-5000-a-night-off-crypto-users-by-impersonating-elon-musk-and-bill-gates-19568.html

While “Nigerian princes” abound on the internet in some of the oldest known scams, there has been only one Bill Gates and one Elon Musk. Until now. Hundreds of crypto users looking to make a quick buck were scammed by criminals impersonating the two billionaires and popular cryptocurrency traders like Vitalik Buterin, discovered BleepingComputer. How? People just don’t pay attention to minor changes such as extra or missing letters in the name. For the past two weeks at least, a dozen fake accounts such as @WarrenBuffert, @Billgavtes, @SatoshiLitev, @elonnmuusk, @VittaliBuuteri and @officialmcafee **tweeted they were giving away free cryptocurrency**. **If users wanted some, they had to also donate ethereum to the address in the tweet**. The fake profiles had similar messages; only the amounts varied. The most profitable accounts were those impersonating John McAfee, Elon Musk and Vitalik Buterin.

The scam made about $5,000 in a single night from gullible crypto users hoping to become rich quick through a crypto giveaway. Since cryptocurrency is anonymous by nature, the money is lost and the scammers can’t be detected. Because they are violating its user agreement, Twitter will most likely block the accounts, but that doesn’t mean hackers won’t create new ones. **It’s recommended users pay close attention to whom they engage with on social media. Before sending money, double check that the address, campaign or person involved are legitimate to reduce the risk of phishing. Avoid clicking on links that seem fake or if there are any doubts about the domain’s validity, especially when purchasing wallets. Most importantly, never give away personal information, passwords or private keys, and beware of deals that are too good to be true.**

U.S. Announces Takedown of Global Cyber Theft Ring

https://www.securityweek.com/us-announces-takedown-global-cyber-theft-ring

The US Justice Department announced indictments Wednesday for 36 people accused of running a transnational ring stealing and selling credit card and personal identity data, causing $530 million in losses. Thirteen members of the "Infraud Organization" were arrested in the United States, Australia, Britain, France, Italy, Kosovo and Serbia, it said. Created in Ukraine in 2010 by Svyatoslav Bondarenko, Infraud was a key hub for card fraud, touting itself with the motto "In Fraud We Trust." **It was "the premier one-stop shop for cybercriminals worldwide,"** said Deputy Assistant Attorney General David Rybicki.

Members could buy and sell card and personal data for use to buy goods on the internet, defrauding the card owners, card issuers and vendors. Infraud operated automated vending sites to make it easy for someone to buy card and identity data from them. It had 10,901 approved "members" registered to buy and sell with them in early 2017, and maintained a rating and feedback system for members. The senior administrators continuously screened the products and services of vendors "to ensure quality products," said the indictment. The group operated moderated web forums to share advice among customers, and operated an "escrow" service for payments in digital currencies like Bitcoin, the Justice Department said. "As alleged in the indictment, Infraud operated like a business to facilitate cyber fraud on a global scale," said Acting Assistant Attorney General John Cronan. The **network of indicted Infraud leaders included** people from the United States, France, Britain, Egypt, Pakistan, Kosovo, Serbia, Bangladesh, **Canada** and Australia. Bondarenko remains at large, but the number two figure in the organization, Russian co-founder Sergey Medvedev has been arrested, according to US officials.

UK Unveils Extremism Blocking Tool

http://www.bbc.com/news/technology-43037899

The UK government has unveiled a tool it says can accurately detect jihadist content and block it from being viewed. Home Secretary Amber Rudd told the BBC she would not rule out forcing technology companies to use it by law. Ms Rudd is visiting the US to meet tech companies to discuss the idea, as well as other efforts to tackle extremism.

Thousands of hours of content posted by the Islamic State group was run past the tool, in order to "train" it to automatically spot extremist material. The government provided £600,000 of public funds towards the creation of the tool by an artificial intelligence company based in London. ASI Data Science said the software can be configured to detect 94% of IS video uploads. Anything the software identifies as potential IS material would be flagged up for a human decision to be taken.

The company said it typically flagged 0.005% of non-IS video uploads. On a site with five million daily uploads, it would flag 250 non-IS videos for review. It is intended to lighten the moderation burden faced by small companies that may not have the resources to effectively tackle extremist material being posted on their sites. Similar tools in the past have been heavily criticised by advocates of an "open" internet, saying such efforts can produce false positives - and that means content that is not particularly problematic ends up being taken down or blocked.

In London, reporters were given an off-the-record briefing detailing how ASI's software worked, but were asked not to share its precise methodology. However, in simple terms, it is an algorithm that draws on characteristics typical of IS and its online activity. In Silicon Valley, the home secretary told the BBC the tool was made as a way to demonstrate that the government's demand for a clampdown on extremist activity was not unreasonable. "It's a very convincing example of the fact that you can have the information you need to make sure this material doesn't go online in the first place," she said. "The technology is there. There are tools out there that can do exactly what we're asking for. For smaller companies, this could be ideal."

Silicon Valley giants such as Facebook and Google are pouring their own resources into solving this problem, but this tool is at first intended to be used by small companies, and they may one day be forced to use it. "We're not going to rule out taking legislative action if we need to do it," the home secretary said. "But I remain convinced that the best way to take real action, to have the best outcomes, is to have an industry-led forum like the one we've got."

The Global Internet Forum to Counter Terrorism, launched last year, brings together several governments including the US and UK, and major internet firms like Facebook, Google, Twitter and others. However, the bigger challenge is predicting which parts of the internet that jihadis will use next. The Home Office estimates that between July and the end of 2017, extremist material appeared in almost 150 web services that had not been used for such propaganda before.

New Details Surface on Equifax Breach

https://www.securityweek.com/new-details-surface-equifax-breach

Documents provided recently by Equifax to senators revealed that the breach suffered by the company last year may have involved types of data not mentioned in the initial disclosure of the incident. In mid-May 2017, malicious actors exploited a known vulnerability in the Apache Struts development framework to gain unauthorized access to Equifax systems. The company said the breach affected roughly 145 million customers – mostly in the U.S., but **also in Canada** and the United Kingdom – including their social security numbers, dates of birth, addresses, and in some cases driver's license numbers, payment cards, and dispute documents.

Confidential documents sent by Equifax to the Senate Banking Committee, copies of which were seen by CNN and The Wall Street Journal, show that hackers may have also stolen tax identification numbers, email addresses, and driver's license information other than just license numbers. In response to news reports, **Equifax said its initial disclosure was never intended to include all the types of information that may have been compromised**.

U.S. Senator Elizabeth Warren has called on Equifax to provide clarifications on what she has described as "conflicting, confusing and incomplete information" provided by the company to the public and Congress. According to Sen. Warren, Equifax told the Banking Committee in early October that passport numbers had also been included in the database tables possibly accessed by the attackers, but now the credit reporting agency claims passports were not compromised. "As your company continues to issue incomplete, confusing and contradictory statements and hide information from Congress and the public, it is clear that five months after the breach was publicly announced, Equifax has yet to answer this simple question in full: what was the precise extent of the breach?" Sen. Warren wrote in a letter to Equifax.

The senator has given Equifax one week to provide a full and complete list of data elements confirmed or believed to have been compromised in the breach, along with a timeline of its efforts to determine the full extent of the intrusion. Sen. Warren last week published a 15-page report containing the findings of her own four-month investigation into Equifax's failures. The lawmaker's investigation found that the company had set up a flawed system to prevent data security incidents, it ignored numerous warning of risks to customer data, it failed to disclose the breach to stakeholders in a timely manner, and provided inadequate assistance and information to consumers. The report also said Equifax had taken advantage of federal contracting loopholes to force the IRS into signing a contract. Earlier this year, senators Warren and Mark Warner introduced a bill that would provide the Federal Trade Commission (FTC) with punitive powers over the credit reporting industry for poor cybersecurity practices. The bill came in response to the Equifax breach.

JavaScript Cryptomining Scripts Discovered in 19 Google Play Apps

https://www.bleepingcomputer.com/news/security/javascript-cryptomining-scripts-discovered-in-19-google-play-apps/

There doesn't appear to be an end in sight for the cryptojacking scourge affecting all facets of the web right now. If you're not bored already of reading yet another incident where miscreants deployed the Coinhive in-browser script to mine Monero behind users' backs, then this article might interest you.

Coinhive found inside Play Store apps- Our article is based on a 13-page report published last week by UK cyber-security firm Sophos. According to the company, **its engineers discovered 19 Android applications that were uploaded and made available through the official Google Play Store. Sophos says these apps were secretly loading an instance of the Coinhive script without user knowledge**. An analysis of the malicious apps revealed that app authors - believed to be the same person/group - hid the Coinhive JavaScript mining code inside HTML files in the apps' /assets folder. The malicious code executed when the user started the apps and the apps opened a WebView (Android stripped-down) browser instance.

In some cases, if the apps did not justify opening a browser window, the WebView component was hidden from view and the mining code ran in the background. In other instances, where the app was a news reader or tutorial viewer, the Coinhive in-browser JavaScript mining code ran along the app's legitimate content while the user was using the app.

One app had over 100,000 users- Sophos discovered this technique with 19 apps published via four developer accounts. Most apps barely made it to 100-500 installs, but one app (extreme/action/wwe/wrestin) was installed on between 100,000 and 500,000 devices. **The apps were uploaded on the Play Store around Christmas and Sophos researchers reported all apps to Google. All have been removed from the official Play Store at the time of writing**. A list of all the 19 Coinhive-laden apps is available on page 7 of the Sophos report, and users can review the list and see if they installed any of the apps on their devices. On page 10, there's another list of malicious apps, but these did not load the Coinhive JavaScript miner but instead embedded the native cpuminer library for mining Bitcoin and Litecoin. Sophos dubbed this malware CoinMiner and says it found it embedded in 10 apps made available through the coandroid.ru website, a third-party Android app store.

The danger of cryptojacking to mobile devices- While many news sites are oversaturated with articles about illegal cryptocurrency mining, **users should be aware that mining cryptocurrency on their smartphone may permanently damage the device**, as Kaspersky researchers proved last month when they discovered the Loapi Android malware.

But users don't have to install malware-laced apps on their devices to be affected. Yesterday, security researchers from Malwarebytes announced they discovered a malvertising campaign that targets Internet users utilizing Android mobile browsers. The campaign used malicious code hidden in ads to redirect users to sites where crooks were mining Monero (via Coinhive) while the user was trying to solve a CAPTCHA field. The user didn't have to install an app to be affected, and just surfing the web was enough to be affected.

While desktop computers may stand the hardware stress that comes with cryptocurrency mining, mobile devices such as smartphones and tablets are more fragile and may risk permanent damage, especially to their batteries, which could overheat and deform.

Browsealoud Plugin Hacked to Mine Monero on 4,000 Govt Websites

https://www.hackread.com/browsealoud-plugin-hacked-to-mine-monero/

On February 11th, an IT security researcher Scott Helme discovered that there are over 4,000 government websites that have been hacked to mine Monero cryptocurrency including the official website of American court system (uscourts.gov), the website of U.K.'s Information Commissioner's Office (ico.org.uk), U.K.'s General Medical Council (GMC), National Health Service (NHS) and United States Social Security Administration.

According to Helme's blog post, the targeted websites were infected with a malware that has been using the computing power of sites visitors to mine Monero. **Remember, the technique in which websites are compromised to mine cryptocurrency is also known as in-browser cryptojacking in which CPU power of unsuspected website visitors is secretly used by hackers to generate cryptocurrency while users end up with expensive electricity bills.**

Upon further digging, Helme found that hackers compromised a popular Browsealoud plugin to make their way into the government websites and infected them with cryptocurrency mining malware. **The Browsealoud plugin helps visitors access content on websites including dyslexia patients, users not familiar with the English language and mild visual impairments. There are over 3 million Browsealoud users around the world while 6,000 websites are currently using the plugin.**

However, this time the plugin was used for malicious purposes allowing hackers to manipulate its original code with a Javascript code provided by Coinhive, a company that provides cryptocurrency miner and sends any coins mined to the browser of the websites' owners.

At the time of publishing this article, HackRead noticed that the Browsealoud plugin was closed on 11th February and its official page on WordPress now shows the message "This plugin was closed on February 11, 2018, and is no longer available for download."

Authorities are examining the situation- The British National Cyber Security Centre (NCSC) said that they are familiar with the situation. According to their official statement: "NCSC technical experts are examining data involving incidents of malware being used to illegally mine cryptocurrency. The affected service has been taken offline, largely mitigating the issue. Government websites continue to operate securely. At this stage, there is nothing to suggest that members of the public are at risk." Now that the authorities are aware of the situation Helme fears hackers can pull a similar stunt in the future which could be devastating. The news came as a shock since the general perception about government owned websites is that they are secured and scanned for malware and malicious codes by their administrators on regular bases.

Brandon Dixon, VP at digital threat management firm RiskIQ told HackRead "We are seeing threat actors around the world exploiting what is already a hostile currency in a lawless digital world.

Threat actors hack vulnerable sites or spin up fake, illegitimate websites to siphon money off of major brands, often with typosquatting domains and fraudulent branding. By leveraging domains or subdomains that appear to belong to major brands, these actors trick people into visiting their sites running cryptocurrency mining scripts to monetize their content. When we looked at domains running the cryptocurrency mining script Coinhive, we found many examples of typosquatting and domain infringement,"

Cryptocurrency mining is increasing- The IT security community is rightly worried about the sudden surge in cryptocurrency mining attacks. Some are even considering it as a replacement for ransomware. Lately, some high-profile websites and institutions have been found infected with cryptocurrency mining malware including YouTube, Oracle, BlackBerry, Starbucks and even the Russia based world's largest oil pipeline company Transneft.

In December last year, Sucuri security firm identified 5,000 WordPress websites were infected with CoinHive cryptocurrency miner scripts and generating Monero through visitors computing power. In some cases, researchers have also identified that hackers are using leaked NSA exploits EternalBlue, EsteemAudit and EternalSynergy in their cryptocurrency mining malware which means the worse is still to come.

And Now, This:

'Panty Buster' Toy Left Private Sex Lives Of 50,000 Exposed

https://www.forbes.com/sites/thomasbrewster/2018/02/01/vibratissimo-panty-buster-sex-toy-multiple-vulnerabilities/#6f7194155a94

[The Internet of Insecure Things…] Valentine's Day is just around the corner. Some might be considering the purchase of a special kind of pleasure-giving device for their partner as a gift. But they might want to rethink those plans: the quality of cybersecurity in newfangled, connected sex toys has been unsurprisingly shocking in recent years. And it doesn't look to be getting much better, if research released by Austrian company SEC Consult on Thursday is anything to go by.

Probing Vibratissimo's 'Panty Buster' sex toy for women, **the researchers found the device and associated websites had multiple vulnerabilities**. By far the most severe issue (and one that was thankfully immediately addressed by Vibratissimo's owner, Amor Gummiwaren) **allowed anyone to obtain a database of all customer information by simply grabbing a username and password from an open file on the vibratissimo.com website. And it was possible to grab passwords for the sex toy owner accounts, as they were left open in plain text**. From there, a hacker could look at sensitive data, including explicit images, sexual orientation and home addresses, according an SEC blog post.

There was more. **Remote control of the toy without consent was possible thanks to a flawed feature**, SEC explained. When Vibratissimo users want to allow someone far away to control the Panty Buster, they have the app create a link, which is then sent to the partner. But those links are easy to guess and **the toy owner isn't asked to confirm they want another person to take over**. "The attacker could simply guess this predictable ID in order to control the victim directly," SEC noted. To prove how simple it was to take control of the device via this method, SEC produced a video [if interested, go to the article] Whilst the problem hasn't yet been fully addressed by Vibratissimo's owners, SEC believes updates are coming.

Given the popularity of Vibratissimo's apps, **users would be wise to avail themselves of updates when they can. According to Google Play figures, between 50,000 and 100,000 have downloaded the relevant Android app. It's unclear how many iPhone owners enjoy the Panty Buster too, though SEC estimated the total number of affected users was in the six-figure ballpark**.

The Panty Buster used insecure Bluetooth too, failing to authenticate incoming connections, allowing an attacker to take control of the device just as long as they were in range. After SEC disclosed the issue to CERT-Bund, a German body that helps with disclosing security vulnerabilities to vendors, it emerged this was a feature, not a bug, according to the blog. Vibratissimo claimed its customers wanted fully open access, in particular those attending swinger parties, according to SEC's narrative. The issue has been addressed, though, as the researchers said the manufacturer had introduced a more secure pairing method. But as the update is in the firmware, customers have to send the device to Amor Gummiwaren to get the fix.

A further, still unresolved issue allowed anyone to view images uploaded by Vibratissimo users. **The flaw was a result of images being openly searchable by simply knowing the correct URL to**

type in. As the identifier for each photo is just a number, incremented by one every time an image is added, it wouldn't be too much of a stretch for outsiders to guess what to search.
Amor Gummiwaren hadn't responded to requests for comment at the time of publication.

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

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

****