CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

Defense Situation Monitoring Center (DSMC) ■ Management Information System Service (MISS)

15 June 2018 **Issue No. 2018-022**

Chinese government hackers snag secret missile plans in Navy contractor breach

A report in the Washington Post said that hackers from the Chinese Ministry of State Security who broke into the systems of a contractor working for the U.S. Naval Undersea Warfare Center stole 614GB of sensitive information, including plans for a supersonic anti-ship missile to be launched from a submarine. The hacks, which occurred in January and February yielded details on the Sea Dragon missile program, which was created in 2012 to adapt existing military technology to new uses. The Pentagon and the FBI are investigating the breach. **(SCMagazine.com, 11 June 2018)**

Hackers could monitor, hijack, steal and even sink ships by exploiting flaws and poor security

Security researchers at Pen Test Partners discovered vulnerabilities in the communications and navigation networks used by the shipping industry which could potentially be exploited by hackers looking to track, hijack, redirect, steal and even sink shipping vessels. Researchers tested over 20 Electronic Chart Display and Information Systems (ECDIS), the system used by ship to navigate oceans, and found several vulnerabilities which could potentially give hackers the ability to control ship's engines, steering ballast pumps and more. Aside from these, the shipping industry is also plagued by lack of proper security hygiene, with many using default credentials on critical systems. **(Cyware.com, 12 June 2018)**

Israel: Social media monitoring nabs would-be attackers

Israel's Public Security Minister Gilad Erdan said Israeli authorities have foiled over 200 Palestinian attacks by monitoring social media and sifting through vast amounts of data to identify prospective assailants ahead of time. He said that Israel's use of algorithms and other technology has been an important factor in lowering the number of knife and shooting attacks in the country in recent years. He planned on sharing this knowledge with counterparts at an international security conference he is hosting that started on 12 June 2018. Participants include U.S. Homeland Secretary Kirstjen Nielsen and officials from Belgium, Germany, Kenya, Singapore, Spain and other countries. The agenda includes terrorism, radicalization and cyber attacks. On the top of the agenda will be government relationships with social media companies. Despite all the technology at his disposal, Erdan believes that social media giants should do far more to stop the spread of online hate. **(Inquirer.net, 13 June 2018)**

U.S. Department of Homeland Security (DHS) experts warn it's a "matter of time" before hackers hit commercial airliners

Cybersecurity experts at the Department of Homeland Security (DHS) issued a warning about the vulnerability of commercial airliners to hackers. Said experts hacked a Boeing 757 as part of the U.S. government's ongoing efforts to learn about the vulnerabilities. In a presentation, researchers from the Pacific Northwest National Laboratory warned that it is "a matter of time before cybersecurity breach on an airline occurs." The assessment came after a DHS decision

to launch “nose tail” tests of a Boeing 757 for hacking weak spots. The documents, which were first reported by the website Motherboard, showed DHS planned to begin developing mitigation efforts to protect against cyberattacks in 2017.

The tests came after a DHS team took just two days to hack remotely into a plane while it was parked at a Federal Aviation Administration (FAA) facility at the Atlantic City Airport in September 2016. The DHS team gained access through the plane’s radio frequency communications using “typical stuff” that could be brought through airport security.

In a statement, Boeing said that it is working with government agencies to ensure the cybersecurity of their aircrafts. The company also expressed confidence on the cybersecurity measures of its airplanes. **(CNBCNews.com, 12 June 2018)**

MIT researchers develop frequency-hopping transmitter that fends off attackers

Massachusetts Institute of Technology (MIT) researchers said that they have invented a transmitter that can secure billions of Internet of Things (IoT) products by individually scattering each bit of data that a device wirelessly sends out onto different radio frequency channels, thus preventing attackers from intercepting a full packet and manipulation of its data. In essence, the transmitter performs a new-and-improved version of a technique called “frequency hopping.”

MIT’s press release explained that traditional frequency hopping breaks data down into large packets, but the process is just slow enough for adept hackers to still attack them. However, the new transmitter hops each individual “1” or “0” bit to a unique, random frequency every microsecond. Attackers simply cannot keep up with such a frenetic pace. **(SCMagazine.com, 11 June 2018)**

Google blocks Chrome extension installations from 3rd party sites

Google announced on 12 June 2018 in its Chromium blog that by end of this year, its Chrome browser will no longer support the installation of extensions from outside the Web Store in an effort to protect its users from shady browser extensions. Google’s browser extension crackdown will take place in three phases: 1) starting 12 June, the inline installation will no longer work for newly published extensions; 2) starting 12 September, the company will disable the inline installation feature for all existing extensions and automatically redirect users to the Chrome Web Store to complete the installation; and, 3) by December 2018, Google will also completely remove the inline install application programming interface (API) method from Chrome 71. **(TheHackerNews.com, 12 June 2018)**

Apple officially bans Crypto currency mining apps for MacOS and iOS

Apple has officially banned crypto currency mining apps from its App Store for iOS and MacOS platforms. In newly updated App Store Review Guidelines, Apple has explicitly mentioned that apps may not mine for crypto currencies unless the processing is performed off device. It is not the first time that Apple has disallowed crypto currency mining applications. In March this year, it removed “Calendar 2” app from Mac App Store after its premium version started mining crypto currency in exchange for additional features. In a bid to stop app developers from integrating any crypto-mining feature in apps submitted on the App Store, Apple has updated its review guidelines. The guidelines now has a dedicated section for crypto currencies which

states rules regarding crypto currency storage in wallets, crypto currency futures trading, and crypto currency mining.

Crypto jacking is a new form of cyber attack where an attacker uses the processing power of the target device to mine virtual currency without the knowledge of the user. This excessive use of resources slows down the device and also effects battery life negatively. **(Fossbytes.com, 12 June 2018)**

Microsoft patches 11 critical RCE flaws in Windows, browsers

Microsoft's Patch Tuesday updates for June 2018 address a total of 50 vulnerabilities, including nearly a dozen critical remote code execution (RCE) flaws affecting Windows and the company's Edge and Internet Explorer web browsers. None of the security holes patched this month appear to have been exploited for malicious purposes, but one of them has been publicly disclosed before the release of a fix. Said vulnerability is a use-after-free issue that allows an attacker to execute arbitrary code if they can convince the targeted user to open a malicious web page or file. It was reported to Microsoft through Trend Micro's Zero Day Initiative (ZDI). **(SecurityWeek.com, 12 June 2018)**

Yahoo fined £250,000 over 2014 cyber-attack

Yahoo's U.K. arm has been fined £250,000 ($335,000) by the U.K. Information Commissioner's Office (ICO) over a data breach affecting more than 500 million users. The incident was reported two years later. ICO said "state-sponsored" hackers had stolen personal information, which included names, emails, unencrypted security questions and answers. The firm said Yahoo failed to take appropriate measures to protect it. Yahoo said it did not comment on regulatory action. **(BBC.com, 12 June 2018)**

Vietnam lawmakers approve cyber law clamping down on tech firms, dissent

Vietnamese legislators approved a cybersecurity law on 12 June 2018 that tightens control of the internet and global tech companies operating in the country. The said cyber law, which takes effect on 01 January 2019, requires Facebook, Google and other global technology firms to store locally "important" personal data on users in Vietnam and open offices there. Also, under the said law, social media companies in Vietnam are required to remove offending content from their platforms within one day of receiving a request from authorities.

The vote in the National Assembly came a day after lawmakers delayed a decision on another controversial bill that had sparked violent protests in parts of the country during the weekend. Thousands of demonstrators in cities and provinces had denounced a plan to create new economic zones for foreign investment that has fueled anti-Chinese sentiment. Some protesters has also derided the cybersecurity bill, which experts and activists say could cause economic harm and stifle online dissent. **(Reuters.com, 12 June 2018)**

Facebook glitch changed millions of privacy settings to "public"

Around 14 million Facebook users had their posts shared with a broader audience than they intended. Facebook said that a software glitch for 10 days last month switched privacy settings to "public" for millions even if they had wanted only friends to see their posts. Facebook's chief privacy officer Erin Egan apologized for the said glitch and said that they have fixed the issue

and asked affected Facebook users to review any posts made during that time. **(CBSNews.com 07 June 2018)**

Operation Wire Wire: FBI busts massive global email fraud ring, 74 scammers arrested

The U.S. Department of Justice (DoJ) announced on 11 June 2018 that the FBI arrested 74 scammers in a massive global email scam crackdown. The scammers were arrested for their involvement in business email compromise (BEC) schemes, which involved attempts to steal both data and money from individuals and businesses. The arrests were made after a six-month long operation called Operation Wire Wire, which was a collaborative effort of the DoJ, FBI, U.S. Treasury Department, Department of Homeland Security (DHS), as well as the U.S. Postal Inspection Service. **(Cyware.com, 12 June 2018)**

InvisiMole Spyware turns computer into a video camera and steals secrets

The security researchers at anti-virus provider company ESET have uncovered InvisiMole, a spyware that has been active at least since 2013. The company's security products recently detected it in Russia and Ukraine. As its name suggests, InvisiMole remains hidden and performs highly targeted actions with low infection ratio. The malicious components of the malware turn the computer into a spying video camera to closely monitor the victim's activities. Apart from hijacking, the malware also employs other loading and persistence methods, including the installation of a registry key and scheduling a task. No matter what persistence method this spyware adopts, the actual attack payload remains the same. Finally, after connecting to its command and control server, additional data is downloaded to perform the backdoor actions. InvisiMole encrypts its internal files, strings, network communication, and configuration data to remain hidden. **(Fossbytes.com, June 11, 2018)**

ADB exploit leaves thousands of Android devices exposed to attackers

A network worm has surfaced on Android devices that exploits Android Debug Bridge (ADB) feature of the mobile OS, a feature that is enabled by default by phone manufacturers. One security researcher revealed this issue in a blog post stating that ADB is completely unauthenticated and thousands of Android devices connected to the internet are currently being exploited through this vulnerability.

Hardware manufacturers ship their products with Android Debug Bridge left enabled, and the service listens to TCP port 5555 through which anyone can connect to a device over the internet. To enable it, a person has to physically connect to a device using USB and first enable the Debug Bridge. A worm called ADB.Miner worm spread to several devices in February. Accordingly, there are thousands of Android-based devices still exposed online. Anybody connected to a device running ADB can execute commands remotely. Android device owners are advised to disable the ADB interface immediately. **(Fossbytes.com, 11 June 2018)**

Microsoft Hyper-V lets users on a guest system cause denial of service on the host system

Microsoft confirmed the report that Hyper-V guest system can cause denial of service conditions on the host system. A local privileged user on the guest system can run a specially crafted application to trigger a flaw in the Hyper-V Network Switch and cause the host system to crash. The vendor has issued a fix. All system administrators are advised to apply updates to Microsoft Hyper-V. **(SecurityTracker.com, 12 June 2018)**

Microsoft removes tech support for Windows 7, 8.1, IE10, other old product forums

Microsoft seems to be reminding users to upgrade to their latest offering Windows 10. For the users of older versions like Windows 7, Microsoft Answers is an official place where they can find solutions to their problems. In its latest move, Microsoft announced last weekend that its staff who are actively contributing to Microsoft Answers will not provide support and assistance for the following products across different forums, starting next month:

- Windows 7, 8.1, 8.1 RT
- Microsoft Security Essentials
- Internet Explorer 10
- Office 2010, 2013
- Surface Pro, Surface Pro 2, Surface RT, Surface 2
- Microsoft Band – this topic will be locked. Users can participate in Band 2 topic.
- Mobile devices forum – Microsoft support will continue in "Other Windows mobile devices" topic
- Zune – this topic will be locked, but will remain available for browsing
-

Both Windows 7 and 8.1 are already out of mainstream support and not getting feature updates, like Windows 10. Meantime, Windows 7 users have almost a year and a half long extended support for security patches that will end on 14 January 2020. For Windows 8.1, the extended support will terminate on 10 January 2023. **(Fossbytes.com, 12 June 2018)**

Windows NTFS access control flaw lets local users gain elevated privileges

A vulnerability was reported in Windows NTFS that a local user can run a specially crafted application to exploit an access check error and execute a process on the target system with elevated privileges. This allows an ordinary user to obtain elevated privileges on the target system. Affected versions are the following:

- Windows 7 SP1
- Windows 2008 R2 SP1
- Windows 2008 SP2
- Windows 2012
- Windows 2012 R2
- Windows 8.1
- Windows RT 8.1
- Windows 10
- Windows 2016
- Windows 10 Version 1607
- Windows 10 Version 1703
- Windows 10 Version 1709
- Windows 10 Version 1803

The vendor has issued a fix. All System Administrators are advised to apply update all their client OS. **(SecurityTracker.com, 12 June 2018)**