CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

22 June 2018 **Issue No. 2018-023**

Trump-Kim Summit attracts wave of cyber attacks on Singapore

Reports from cyber security firm F5 Labs state that the number of cyber-attacks targeting Singapore skyrocketed from 11 to 12 June, during the meeting between U.S. President Donald Trump and North Korean President Kim Jong-un in a Singapore hotel. Most of these attacks originated from Russia. The number of attacks towards the U.S. from Russia was 88% of the total number of observed cyber attacks. Furthermore, 97% of all the attacks that originated from Russia during the timeframe targeted Singapore. Brazil was the second largest attacker, launching 8% of the assults. Germany rounded up top three attackers with 2%. The security researcher noted that there was no attempt made to conceal the attacks launched from Russia and that none of the attacks originating from said country carried malware. **(SecurityWeek.com, 15 June 2018)**

New campaign possibly linked to MuddyWater

Cybersecurity company Trend Micro reported that a newly discovered attack relying on malicious Word documents and PowerShell scripts appears related to the MuddyWater cyber-espionage campaign, which was first observed in 2017. The said campaign was targeting the Saudi government with PwerShell scripts deployed via Microsoft Office macros. A similar espionage campaign observed in March 2018 was targeting organizations in Turkey, Pakistan and Tajikistan. The attacks, which are difficult to clear up, were previously associated with the FIN7 hacking group, but artifacts observed in multiple assaults were also linked to a single framework last year. **(SecurityWeek.com, 15 June 2018)**

Upcoming iOS access restrictions could stymie law enforcement

Apple plans to equip iOS 12 with USB Restricted Mode, a feature that requires users to unlock their iPhone with their passcode before USB accessories can connect if the phone last was unlocked more than an hour earlier. The company included this feature in the developer versions of iOS 11.4.1 and iOS 12. Once the USB Restricted Mode is invoked, iOS stops sending data over the USB port. The second beta of iOS 11.4.1, released earlier last week, extends the SOS mode so that it blocks all USB communications, Touch ID and Face ID, until the user unlocks the iPhone with a passcode. There is a widespread belief that USB Restricted Mode targets law enforcement agencies, which use passcode cracking tools to get around iPhone security. **(TechNewsWorld.com, 16 June 2018)**

Gmail updates uses AI to identify, alert users of high priority emails

Google, through its Artificial Intelligence (AI) technology, is already offering the option to just get notified of emails that fall into the Primary category. However, that may still invite a lot of pings. Now, the app is rolling out a new way for iOS users to filter everything but “High-priority emails” therefore only getting alerted if emails are marked ‘important.’ In a blog from G Suites,

the company says that “these notifications leverage Gmail’s machine learning and AI capabilities to identify messages you may want to read first. **(Inquirer.net, 17 June 2018)**

Chinese cyber attacks on Taiwan government becoming harder to detect: source

Cyber attacks from China on Taiwan’s government computers are becoming more difficult to detect as hackers increasingly use online platforms such as search engines to break into systems. While the frequency of attacks by China’s cyber army has declined, the success rate of such incursions is rising. China has strongly denied accusations of engaging in cyber warfare or hacking, and has said it is itself one of the world’s biggest victims of such incidents. **(Reuters.com, 15 June 2018)**

5G network standard finalized, ready for commercialization

The 5G network has been finalized by the 3rd Generation Partnership Project (3GPP) Organizational Partners in the Philippines and will be ready for commercial adoption. The standalone specifications for next-generation 5G networks have been finalized on 14 July, signaling companies to start preparing for adopting 5G connectivity into their products. The new 5G system will include additional LTE frequency range to further enhance connectivity for mobile devices. It will also support data speeds of up to 20 gigabits per second. For comparison, the current 4G system has a theoretical peak data rate of only 100 megabits per second. **(Inquirer.net, 16 June 2018)**

MyloBot uses sophisticated evasion and attack techniques, deletes other malware

Security researchers found a new malware, dubbed MyloBot with sophisticated evasion, infection, and propagation techniques that imply that the authors have the experience and heavy infrastructure behind them. Discovered in the systems of an undisclosed Tier 1 data and telecommunications equipment company, the researchers observed MyloBot’s behaviors include process hollowing, reflective EXE, code injection, ransomware payload, and data theft. As it ropes in infected machines into a botnet, this new malware also removes all other malware from the system and inflicts extensive system damage.

While the researchers have yet to identify the source of infection and authorship, the malware has keyboard layout scan techniques that allow it to stop the attack routine if it finds a particular Asian character setup. Further, MyloBot’s evasion techniques include:

- Anti-VM capabilities
- Anti-sandbox capabilities
- Anti-debugging capabilities
- Reflective EXE, an uncommon technique that runs EXE files from memory and not on disk
- Process hollowing
- Code injection
- Delay of 14 days to command and control (C&C) communication for evasion, such as threat hunting, sandboxing and endpoint detection (**Trendmicro.com, 21 June 2018**)

Study finds nearly half of web applications put user data at risk

Despite the increased awareness of cybersecurity and high profile data breaches, a recent study by Positive Technologies revealed nearly half of web applications place users' personal data at risk of theft and all of them contained at least one vulnerability. The company conducted various tests on 23 web applications and found that attackers could obtain personal data from 44 percent of applications handling that information, such as those for bank websites, e-commerce stores, and telecoms companies. Researchers found that web application security remains poor and that every application tested had flaws of various security levels. **(SCMagazine.com, 20 June 2018)**

Vault 7: CIA engineer Joshua Schulte charged with data leak

Joshua Adam Schulte, a former Central Intelligence Agency (CIA) software engineer has been charged with leaking a stolen CIA archive in 2017. The alleged stolen classified information relating to national security will be transmitted to Wikileaks. Federal Bureau of Investigation (FBI) agents discovered alleged child porn in Mr. Schulte's apartment after his arrest. He faces 13 separate charges and could face up to 135 years in prison if found guilty.

Using information allegedly provided by Mr. Schulte, Wikileaks published thousands of documents in March 2017, detailing the CIA's cyber-warfare programme. Codenamed Vault 7, the 2017 breach told how the CIA can take over iPhones through malware and turn smart TCs into surveillance devices. It is believed to the agency's largest leak of classified documents. **(BBC.com, 19 June 2018)**

Researchers warn orgs should plan for partial IT failures in addition to system outages

Researchers are warning firms that they should make sure they are prepared for partial failures in IT infrastructure after a "very rate" data center glitch caused a payment meltdown on Visa systems. Earlier this month, a partial network switch failure in one of Visa's two data centers caused nearly 10 percent of 51.2 million attempted transaction in Europe to fail, resulting in millions of credit cards being declined over the course of 10 hours.

Visa has since launched several reviews and is in the process of migrating its European systems to a more resilient global processing system. And while Visa was able to resolve the issues relatively fast, researchers are warning other firms to better plan for partial network failures as well. **(SCMagazine.com, 21 June 2018)**

Thousands of mobile apps expose their unprotected firebase hosted databases

Mobile security researchers discovered unprotected Firebase databases of thousands of iOS and Android mobile applications that are exposing over 100 million data records, including plain text passwords, user IDs, locations, and in some cases, financial records such as banking and cryptocurrency transactions. Google's Firebase service is one of the most popular back-end development platforms for mobile and web applications that offers developers a cpuld-based database, which stores data in JSON format and synced it in the real-time with all connected clients

Researchers from mobile security firm Appthority discovered that many app developers' fail to properly secure their back-end Firebase endpoints with firewalls and authentication, leaving hundreds of gigabytes of sensitive data of their customers publicly accessible to anyone. Researchers had already contacted Google and provided a list of all vulnerable app databases, and also contacted a few app developers helping them to patch this issue. **(TheHackerNews.com, 21 June 2018)**

China-based hacking campaign is said to have breached satellite, defense companies

A sophisticated hacking campaign launched from computers in China burrowed deeply into satellite operators, defense contractors and telecommunications companies in the United States and Southeast Asia, security researchers at Symantec Corp said on Tuesday. Symantec said the effort appeared to be driven by national espionage goals, such as the interception of military and civilian communications. Such interception capabilities are rare but not unheard of, and the researchers could not say what communications, if any, were taken. More disturbingly in this case, the hackers infected computers that controlled the satellites, so that they could have changed the positions of the orbiting devices and disrupted data traffic, Symantec said.

Satellites are critical to phone and some internet links as well as mapping and positioning data. Symantec said it has already shared technical information about the hack with the U.S. Federal Bureau of Investigation (FBI) and Department of Homeland Security, along with public defense agencies in Asia and other security companies. (**CNBC.com, 19 June 2018**)

Google Solves Update Issue for Android Apps Installed from Unknown Sources

Late last year, Google announced its plan to set up an automated mechanism to verify the authenticity of an app by adding a small amount of security metadata on top of each Android application package (in the APK Signing Block) distributed by its Play Store. This metadata is like a digital signature that would help your Android device to verify if the origin of an app you have installed from a third-party source is a Play Store app and have not been tempered, for example, a virus is not attached to it.

It should be noted that this feature does not protect users from the threat of installing apps from third-party sources. Instead, it merely helps in receiving latest updates for apps if their origin is Google Play Store. Although Play Store itself is not completely immune to malware, users are still advised to download apps, especially published by reputable developers, from the official app store to minimize the risk of getting their devices compromised. (**Thehackernews.com, 20 June 2018**)

Zacinlo malware, another threat for all Windows 10 users

Researchers at Bitdefender have recently discovered a powerful malware that takes control over the PC and spams with advertisements. They have named it 'Zacinlo' after the last and final payload, looking at this as a transitory name for an intricate code. It has been around for almost six years extremely contaminating various Windows users. The researchers at the Cyber Threat Intelligence Lab, following a year of research have published a rather detailed paper about this malware. Despite the fact that the malware has been around since 2012, it became the most active in late the 2017. Zacinlo is said to be so powerful to the point that it

has the capability of deactivating the most anti-malware directly accessible. Well known targets of Zacinlo incorporate Bitdefender, Kingsoft, Symantec, Microsoft, Avast, and various different programs. The advancement of this malware makes its detection extremely hard. All the windows users are thus instructed to stay wary while downloading any applications from untrusted sources to shield themselves from any malware attacks. (**Ehackingnews.com, 20 June 2018**)

Critical flaws in AXIS camera models found

Cyber security experts claimed to have detected a slew of glaring security lapses across 400 sophisticated AXIS camera models deployed in security affairs. The vulnerabilities, even if not of dangerous magnitude, surfaced as the experts scrutinized the security aspects of a number of top camera models. The analysis of the camera models by the premier cyber security firm mainly concentrated on the IP cameras—known to be the best ever tool to ensure security.

In the recent technical findings, experts have already named as many as seven vulnerabilities in these camera models. They further claim that the hackers, if allowed to take the rein of these camera models, can only add it to a botnet and can only change the software. These hackers only can use the camera as an infiltration point for network. They would have the advantage to move the lens to a point where ever want. (**Ehackingnews.com, 20 June 2018**)