CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

20 July 2018 **Issue No. 2018-027**

Smaller nation state attacks: a growing cyber menace

While there certainly remains a global hierarchy when it comes to cyber capabilities, smaller state and non-state actors are increasingly exploiting the asymmetric nature of cyberspace to achieve a broad range of objectives. The recent attacks against Qatar which is attributed to Saudi Arabia (previously to Russia), highlights new rising nation-state (and non-state affiliated) hacking groups and their adoption of tactics and techniques aimed to sow disruption. These capabilities are already playing out both between global powers as well as smaller regional rivals. Smaller nations are increasingly the attacker, and the range of victims is expanding well beyond the major powers and their traditional adversaries. **(ThreatPost.com, 18 July 2018)**

New and improved Magniber ransomware expands threats in Asia

Malwarebytes researchers detected the Magniber ransomware displaying notable improvements as its attack begin to expand within Asia after previously limiting its activity to South Korea. Said malware has been active since its inception in 2013 and has been distributed worldwide but eventually became a private operation that narrowed its focus on a select few Asian countries.

In 2017, researchers spotted the Magnitude exploit kit used to deliver Cerber ransomware via a filtering gate known as Magnigate and later that year the exploit kit operator began to distribute to its own breed of ransomware dubbed Magniber. Since this, the malware's author made significant changes to limit the malware's infection to South Korea. However, exploit attempts and infections were reported in Malaysia, Taiwan and Hong Kong. Moreover, the malware's code had been updated to whitelist more languages and has expanded to include other Asian languages such as Chine (Macau, China, Singapore) and Malay (Malaysia, Brunei). **(SCMagazine.com, 17 July 2018)**

Hackers used malicious MDM solution to spy on 'highly targeted' iPhone users

Security researchers uncovered a "highly targeted' mobile malware campaign that has been operating since August 2015 and found spying on 13 selected iPhones in India. The attackers, who are also believed to be operating from India, were found abusing mobile device management (MDM) protocol to deploy malicious applications remotely. MDM is a type of security software used by large enterprises to control and enforce policies on devices being used by their employees.

According to researchers, the attackers behind the campaign used the MDM service to remotely install modified versions of legitimate apps on target iPhones, which were designed to secretly spy on users, and steal their real-time location, contacts, photos, SMS and private messages from chat applications. **(TheHackerNews.com, 13 July 2018)**

Hacker compromises Air Force captain to steal sensitive drone info

Cyber security firm Recorded Future reported that a hacker has penetrated an Air Force captain’s computer to steal sensitive information about U.S. military drones and other state secrets. The firm’s Insikt Group, while monitoring underground criminal activity identified a newly registered member of a hacking forum, attempting to sell highly sensitive documents about the U.S. military MQ-9 Reaper drone. It looked into the offer and was able to contact the hacker and verify the veracity of the documents. The group was able to uncover the hacker’s tactic which was exploiting vulnerable Netgear routers with improperly setup FTP login credentials to gain access to an unidentified officer’s information. **(ThreatPost.com, 12 July 2018)**

Microsoft bounty program offers payouts for identity service bugs

Microsoft has lifted the curtain on a new bug-bounty program, offering payout as high as $100,000 for holes in identity services and implementations of the OpenID standard. The said program touches on Microsoft’s array of digital identity solutions, which tout strong authentication, secure sign-in session and API security. Those solutions include Microsoft Account and Azure Active Directory, which offer identity and access capabilities for both consumer and enterprise applications, as well as its OpenID authentication protocol.

According to Microsoft, an array of prizes between $500 to $100,000 are available for a significant authentication bypass, multi-factor authentication bypass, standards-based implementation vulnerabilities, cross-site scripting, cross-site request forgery or an authorization law. **(ThreatPost.com, 18 July 2018)**

Hackers steal dead people's medical records and sell them on the dark web

Cyber security researchers have discovered that medical records of deceased patients are appearing on illicit market places on the dark web. Cyber criminals are advertising huge caches of personal data of up to 140 million patients, with their value exceeding that of stolen credit card details. The morbid trend follows an increasing amount of incidents of medical data breaches, as reported by Oren Koriat, an analyst at the security firm Cynerio. The price of the data is listed as $2 per record in batches of 100, going down to $0.60 per record if bought in batches of 1,000. This gives all 140 million records a potential value of $280 million. (**Independent.co.uk, 13 July 2018**)

Report: Russia’s national vulnerability database is incomplete, and a cover for software snooping

A new research from cyber security firm Recorded Future revealed that the government organization running Russia’s national vulnerability database (NVD) is far less comprehensive that its American counterpart. The Russian database known as the BDU, is administered by the Federal Service for Technical and Export Control of Russia (FSTEC), a national military counterintelligence agency. Since 2014, FSTEC has published only about 10 percent of 107,901 total bugs announced by the American NVD, which is operated by the U.S. Commerce Department’s National Institute of Standards and Technology (NIST).

According to Recorded Future, the Russian database exists not so much to provide a public service, but rather to establish a minimum set of security guidelines for Russian officials tasked with securing government information systems. At the same time, having an official vulnerability database also gives Russia a seemingly legitimate cover for demanding that foreign software and security companies submit their products to FSTEC and related agencies for inspection of their source code. But in reality, this is just a thin veneer through which Russia disguises its efforts to gather intelligence on foreign software. **(SCMagazine.com, 16 July 2018)**

12 Russian spies charged for hacking

The U.S. Department of Justice has indicted 12 Russian intelligence agents for "conspiring to interfere with the 2016 presidential elections," Deputy Attorney General Rod J. Rosenstein announced on Friday. The defendants worked for two GRU (Russia's military intelligence service) units, one of which was tasked to steal information and another to disseminate it. They used "spearphishing" attacks to send misleading emails and trick targets into revealing their login credentials. GRU intelligence officers also used malicious software to infiltrate computer networks and spy on users, take screenshots, record keystrokes, and exfiltrate data. Rudy Giuliani, the private attorney for Donald Trump, tweeted that the indictments are "good news for all Americans" and called on the special counsel investigation to end. (**Fossbytes.com, 14 July 2018**)

Apple transfers Chinese users' iCloud data to state-controlled data centers

Apple's Chinese data center partner has transferred iCloud data, belonging to 130 million China-based users, to a cloud storage service managed by state-owned mobile telecom provider, raising concerns about privacy. In February this year, Apple moved the encryption keys and data of its Chinese iCloud users from its US servers to local servers on Chinese soils to comply with the new regulation of the Chinese government, despite concerns from human rights activists. For this Apple controversially signed a deal with Guizhou-Cloud Big data (GCBD), a Chinese company who gained operation control over Apple's iCloud business in China earlier this year.

Now, those sensitive data, including users' emails, text messages, pictures, and the encryption keys that protect it, has been passed on to Tianyi cloud storage service, a business venture managed by government-owned mobile operator China Telecom. **(TheHackerNews.com, 18 July 2018)**

Google fined a massive $5 billion for abusing its dominance in Android ecosystem

European regulators have slapped Google with a record-breaking fine of $5 billion for breaking antitrust laws regarding the Android operating system. The committee, led by Margrethe Vestager, accused Google of abusing its dominance in the smartphone OS market, who propels manufacturers into delivering pre-installed Google Search and Chrome Browser on new handsets.

This is not the first time Google has been slapped with an enormous fine raging in billions. Back in 2016, Google was fined 2.7 billion dollars for manipulating search results, offering the top position to its own shopping comparison website. Presently, the $5 billion fine would make Google top the list of "largest amount of fine received." The European regulators have scrutinized Google for paying hefty amounts to smartphone manufacturers and mobile operators for having Google search as their default search app. Officials even blamed Google for laying out harsh guidelines for OEM which restricts from developing Android forks based on Android Open Source Project. (**Fossbytes.com, 18 July 2018**)

‘Blackgear’ cyberspies resurface with new tools, techniques

The hackers behind a cyber espionage campaign known as Blackgear are back with an improved malware that abuses social media websites, including Facebook, for command and control (C&C) communications. The threat group, also known as Topgear and Comnie, has been around since at least 2008, mainly targeting entities in Taiwan, South Korea, and Japan. Their objectives include organizations in the telecommunications, defense, government, aerospace, and high-tech sectors. Some limited evidence suggests that the attacks may be conducted by Chinese state-sponsored actors. **(TheSecurityWeek.com, 17 July 2018)**

US company; evidence found of Chinese cyber attacks on Cambodia

U.S.-based cyber security company FireEye said it found evidence that a Chinese group attacked computers of people and organizations in Cambodia. One of them was Cambodia’s National Election Committee. Others include Cambodia’s ministries of interior, foreign affairs, and economics and finance. Moreover, FireEye said that the hackers targeted a jailed opposition leader and his daughter, human rights activists, media organizations, and two Cambodian diplomats overseas. Accordingly, the targets were given corrupted computer files from an unsecured server operated by a hacking group called TEMP.Periscope. **(VoaNews.com, 17 July 2018)**

U.S. lawmakers urge Google, Facebook to resist Vietnam cyber security law

Seventeen U.S. lawmakers urged the CEOs of Facebook and Google to resist changes stipulated by a new cyber security law in Vietnam, which critics say gives the communist-ruled state more power to crackdown on dissent. In a letter, the Congressional Vietnam Caucus said that if the Vietnam government is coercing the companies to aid and abet censorship, it is an issue of concern that needs to be raised diplomatically and at the highest levels. The letter also urged the companies to live up to their stated missions to promote openness and connectivity. **(Reuters.com, 17 July 2018)**

Juniper JunOS multiple vulnerabilities

A vulnerability was found in the Juniper JunOS which allows a remote attacker to exploit in order to trigger privilege escalation, denial of service, firewall rule bypass, security restriction bypass and sensitive information disclosure. On the 12th of July 2018, Juniper has released updates to address several vulnerabilities affecting JunOS products. Network administrators are advised to upgrade their affected systems. (**CertEU.com, 13 July 2018**)