CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

23 March 2018 **Issue No. 2018-011**

Russia's internal internet can keep communication alive even if war breaks

The Russian government can cut off internet throughout the country and still keep communications active through a robust internal network in case of a crisis like war. This effort started off as a way to support an isolated government and military but now it has expanded into the civilian population as well. Russian president Vladimir Putin's top IT adviser Herman Klimenko said that they are ready for any action now and that a shift to their internal systems would be painless. To note, the Closed Data Transfer Segment (CDTS) is an intranet network originally built for the military and the government. **(IbTimes.com, 12 March 2018)**

Russia warns Britain against cyber attack response to spy poisoning

Russia's embassy in London said last 13 March that it was seriously concerned about reports that Britain could launch a cyber attack against Russia and urged the UK to carefully weigh the consequences of such action. The Russian embassy said that only Russia is groundlessly and provocatively accused of the Salisbury incident, but plans are being developed in the UK to strike Russia with Cyber Weapons. **(Reuters.com, 14 March 2018)**

GrayKey iPhone Unlocker poses serious security concerns

Opinions have been split on providing backdoor access to the iPhone for law enforcement. Some felt that Apple was aiding and abetting a felony by refusing to create a special version of iOS with a backdoor for accessing the phone's data. Cellebrite, an Israeli company, provides iPhone unlocking services to law enforcement agencies at $5,000 per device, and for the most part this involves sending the phones to a Cellebrite facility. But in late 2017, a new iPhone unlocker device called GrayKey, made by Grayshift company started to circulate. GrayKey is a gray box device with two lightning cables sticking out of the front. Two iPhones can be connected at one time, and are connected for about two minutes. After that, they are disconnected from the device. Sometime later, the phones will display a black screen with the passcode, among other information. Even disabled phones can be unlocked, according to Grayshift. **(Malwarebytes.com, 14 March 2018)**

Pre-installed Malware found on 5 million popular Android Phones

Security researchers discovered a massive continuously growing malware campaign that has already infected nearly five (5) million mobile devices nationwide. Dubbed as RottenSys, the malware that disguised as a 'System Wi-Fi service' app came pre-installed on millions of brand new smartphones manufactured by Honor, Huawei, Xiaomi, Vivo, Samsung and GIONEE and added somewhere along the supply chain. All these infected devices were shipped through Tian Pai, a Hangzhou-based mobile phone distributor, but researchers are not sure if the company has direct involvement in this campaign.

According Check Point Mobile Security team, who uncovered this campaign, RottenSys is an advanced piece of malware that does not provide any secure Wi-Fi related services but takes almost all sensitive Android permissions to enable its malicious activities. To evade detection, the fake System Wi-Fi service app comes initially with command-and-control servers to get the list of required components, which contain the actual malicious code. **(TheHackerNews.com, 15 March 2018)**

Palo Alto networks to acquire CIA-backed cloud security firm Evident.io for $300 million

Network security firm Palo Alto Networks on 14 March said that it has agreed to acquire cloud security and compliance firm Evident.io for $300 in cash. Palo Alto Networks currently has several security offerings that cater to cloud environments, including its VM-Series virtualized next-generation firewalls, API-based security for public cloud services infrastructure, and Traps for host based security.

Evident.io is backed by Bain Capital Ventures, True Ventures, Venrock, Google Ventures and In-Q-Tel, the not-for-profit venture capital arm of the Central Intelligence Agency. **(SecurityWeek.com, 15 March 2018)**

Intel redesigns its 8th Gen Core CPUs to fix Spectre and Meltdown

The Spectre and Meltdown debacle form earlier this year has forced Intel to make some major changes in its chips to mitigate critical vulnerabilities that exists at the processor level. Intel announced that they have redesigned parts of their processors to reduce new levels of protection through partitioning that that would introduce hurdles for bad actors by acting as "protective walls" between applications and user privilege levels. Meanwhile, the updated processor design will be released in the form of Intel Scalable chips (codenamed Cascade Lake) and 8th Gen Intel Core processors are expected to arrive in the market in the second half of 2018. **(Fossworldnews.com, 16 March 2018)**

Researchers discovers security issue on Chrome RDP

Security analysts at Check Point Research have flagged a bug to Google relating to its Chrome Remote Desktop extension (RDP). The flaw, which affects macOS users and machines, allows a "Guest User" to log-in as Guest and yet receive an active session of another user (such as an administrator) without entering a password. Chrome Remote Desktop is an extension to the Chrome browser that allows users to remotely access another computer through Chrome browser or a Chromebook. Google responded that from a CRD perspective, the login screen is not a security boundary. However, the researchers disagree and believe that users should be alert. **(InfoSecurity.com, 19 March 2018)**

Mozilla Master Password feature apparently not as secure as it seems

Mozilla Firefox web browser was always regarded as one of the popular browsers along with Google Chrome and the many iterations of Microsoft's web browser. Last year, Mozilla did a serious overhaul of their browser dubbed as Firefox Quantum. However it forgot to repair the safety holes that exist on their browser for nine (9) years. Moreover, the encryption scheme used for the Grasp Password function can be simply brute-forced, according to Wladimir Palant who is the creator of AdBlock Plus.

The Grasp Password function is used to secure the login credentials saved by the customers. Wladimir discovered out that the SHA1 iteration for the Grasp Password is 1 iteration. This is in contrast with standard industry practices, which use at least 10,000 as a minimum iterations. The very low iteration makes the password supervisor susceptible to attackers. With the help of trendy GPUs, the Grasp Password may be cracked in much less a minute's time with the assistance of brute-force assaults. **(Trendmicro.com, 19 March 2018)**

Cambridge Analytica: Warrant sought to inspect the company

United Kingdom Information Commissioner Elizabeth Denham said that she will seek a warrant to look at the databases and servers used by British firm Cambridge Analytica. The company is accused of using the personal data of 50 million Facebook members to influence the U.S. presidential election in 2016. Its executives have also been filmed by a news channel suggesting it could use honey traps and potentially bribery to discredit politicians. The company denies any wrongdoing. Meanwhile, Christopher Wylie, who worked with the company, claimed it amassed the data of millions of people through a personality quiz on Facebook that was created by an academic. **(BBC.com, 20 March 2018)**

Facebook under fire in escalating data row

Politicians in the U.S., Europe and the U.K. are calling on Facebook to explain how data on millions of its users was harvested. U.S. senators have called on Mark Zuckerberg to testify before the Congress about how it will protect users. Meantime, the head of the European Parliament said it would investigate to see if the data was misused. A spokesman for British Prime Minister Theresa May said she was "very concerned" about the revelations. **(BBC.com, 20 March 2018)**

Responding to Cybersecurity incidents still a major challenge for businesses

According to a research conducted by Ponemon Institute and sponsored by IBM Resilient, over 75% of respondents across the globe admitted that they do not have a formal cybersecurity incident response plan in place across their organization. Moreover, half of the respondents reported that their incident response plan is either informal, ad-hoc or completely non-existent. Ted Julian, Vice President of product management and co-founder of IBM Resilient said that having the right staff is critical but arming them with the most modern tools to augment their work is equally important.

With the European Union's (EU) General Data Protection Regulation (GDPR) coming into effect in May 2018, the lack of a consistent cybersecurity incident response plan could prove costly for businesses. However, most countries surveyed did not report confidence in their ability to comply with GDPR. Furthermore, IBM found that the cost of data breach was nearly $1 million lower on average when organizations were able to contain the breach in less than 30 days, showing the financial benefits of having a good response plan in place. **(Infosecurity-Magazine.com, 20 March 2018)**

Windows Remote Assistance tool can be used for targeted attacks

The Windows Remote Assistance tool that ships with all Windows distributions can abused for clever hacks in targeted attacks. Belgian security researcher Nabeel Ahmed discovered a vulnerability in this tool in February last year and reported it to Microsoft in October. The

vulnerability allows an attacker to extract any file from a victim's computer without the target's knowledge and upload it to a remote server. Because of this, the vulnerability is perfect for data exfiltration and can be used to sneakily steal any file from a victim's computer. The good news is that this cannot be mass-exploited and needs social engineering to trick a victim into opening a remote assistance session. **(BleepingComputer.com, 20 March 2018)**

Ex-Israeli spy chief enlists top hackers for new cybersecurity firm

Former chief of National Intelligence Agency of Israel “Mossad” Tamir Pardo said he has assembled a team of Israeli hackers for his new cybersecurity company, XM Cyber, which takes an innovative approach to securing networks from malicious attacks by imitating real hackers. Pardo told the Reuters news agency on Tuesday that he had recruited a team of 30 hackers from the country’s most elite security and intelligence services to work at his firm. Unlike other cybersecurity firms that offer a one-time hacker-simulated attack on a network to expose its vulnerabilities,

“You can destroy a country and win a war without ever firing a single shot. In the next war, our enemies won’t need fighter jets and rockets. They can hit us hard with cyber-attacks and disable all of the systems here,” said Pardo. **(TimesofIsrael.com, 21 March 2018)**