CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

23 February 2018 **Issue No. 2018-007**

Hackers target major US Defense contractors to steal military secrets

According to an Associated Press investigation, 40% of 87 U.S. defense contractors who were targeted by hackers clicked on malicious phishing links which were sent to them via email, possibly compromising their personal accounts and classified information. Fancy Bear hackers targeted employees at both major and small defense companies, including Lockheed Martin, Boeing, Airbus and General Atomics among others. The hackers mostly targeted victims' personal Gmail accounts along with a few corporate accounts. In January, Trend Micro said the group has been targeting the U.S. Senate to swipe official credentials for espionage purposes as well. (**IBTimes.co.uk, 08 February 2018**)

WordPress warning

Israeli security researcher Barak Tawily warns that almost all WordPress websites could be taken down due to unpatched Common Vulnerability and Exposure (CVE) DoS flaw. The expert explained that the CVE-2018-6389 flaw is an application-level DoS issue that affects the WordPress CMS and that could be exploited by an attacker even without a massive amount of malicious traffic. Tawily revealed that the flaw exists in almost all versions of WordPress released in the last nine years, including the latest one (Version 4.9.2). The flaw affects the "load-scripts.php" WordPress script it receives a parameter called load[] with value 'jquery-ui-core'. In the response, the CMS provides the JS module 'jQuery UI Core' that was requested. The load-scripts.php file was designed for WordPress admins and allows to load multiple JavaScript files into a single request, but the researcher noticed that it is possible to call the function before login allowing anyone to invoke it. (**Cyber Defense Magazine, 08 February 2018**)

Russia steps-up cyberattacks on U.K.

Britain is being hit by 60 significant cyberattacks a month including attempts by Russian state-sponsored hackers to steal defense and foreign policy secrets, Ciaran Martin, head of U.K.'s National Cyber Security Centre (NCSC) warned. There had been a "step change" in Russia's online aggression against the West as well as more attacks on "soft targets" such as local councils and charities to steal personal data, and universities to steal research secrets. (**Thetimes.co.uk, 12 February 2018**)

Hackers stole more than $17 million from Russian banks

A security tool used to test the strength of an organization's cyber defense has been used by hackers to attack banks in Russia and Europe. Central bank Deputy Governor Dmitry Skobelkin told an information security conference in the Russian city of Magnitogorsk on Tuesday that Hackers stole more than 1 billion roubles ($17 million) from Russian banks using

a security tool. Russia is under intense scrutiny over cybercrime allegations that hackers backed by Moscow have attacked targets in the United States and Europe. An accusation which Kremlin has repeatedly denied. Russian authorities are now keen to show that Russia too is a frequent victim of cybercrime and that they are working hard to combat it. (**News18.com, 13 February 2018**)

U.K. blames Russia for crippling cyberattack

The British government says that Russia was behind a massive global cyberattack that hit major companies in June 2017. British Foreign Office minister Tariq Ahmad said in a statement on 15 February that the Russian military was responsible for a cyberattack, which initially targeted computers in Ukraine but quickly spread beyond its borders. The attack, called NotPetya, hit companies including British advertising group WPP, Oreo maker Mondelez, U.S. drug maker Merck, and global shipping company FedEx.

The attack which masqueraded as ransomware infected computers and locked down their hard drives. It would then demand a $300 ransom to be paid in bitcoin. But even if the victims paid, they did not recover access to their files. Britain's National Cyber Security Centre, which investigated the attack, said it demonstrated a "high level of planning, research and technical capability." It said that the ransomware was inserted into a legitimate piece of software used by most of Ukraine's financial and government institutions. Meantime, the Russian government said it "categorically denies the accusations." (**CNN.com, 15 February 2018**)

U.S. will impose costs on Russia for cyber 'acts of aggression,' White House cybersecurity czar

Special assistant to the president and White House cybersecurity coordinator Rob Joyce said that Russia will be made to pay for its acts of aggression on the international stage. The act in question was the malware attack NotPetya that wiped out billions of dollars as it spread across 64 countries in July 2017. For the first time the White House directly blamed Russia's military for the attack. Joyce said that the U.S. is going to work on the international stage to impose consequences. He also stressed the need for companies to invest heavily in cybersecurity, noting that much of the NotPetya damage would have been avoidable if better security measures had been in place. (**CNBC.com, 16 February 2018**)

Cyberattacks are costly, and things could get worse: US report

A report by the White House Council of Economic Advisers said on 12 February that Cyberattacks cost the United States between $57 billion and $109 billion in 2016. It also warned of a "spillover" effect for the broader economy if the situation worsens. The report sought to quantify what it called "malicious cyber activity directed at private and public entities" including denial of service attacks, data breaches and theft of intellectual property, and sensitive financial and strategic information. It warned of malicious activity by "nation-states" and specifically cited Russia, China, Iran, and North Korea. (**Inquirer.net, 17 February 2018**)

U.S. charges Russians with 2016 election tampering

The U.S. Justice Department has charged 13 Russians and three companies in an indictment that unveiled a sophisticated network designed to subvert the 2016 election and to support the campaign of Mr. Donald Trump. The operation stretched from an office in St Petersburg, Russia, into the social feeds of Americans and ultimately reached the streets of election battleground states. The Russians stole the identities of American citizens, posed as political activists and used the flash points of immigration, religion and race to manipulate the campaign.

The 37-page document describes a sophisticated and well-funded multi-year operation, dubbed "Project Lakhta" by Russian entities, to influence the election, beginning as early as May 2014. The operation employed hundreds of people, from creators of fictitious identities to technical experts, and by September 2016 its monthly budget exceeded US$1.2 million (S$1.6 million), the court document said. (**Straitstimes.com, 18 February 2018**)

U.N. chief urges global rules for cyber warfare

During his speech during a ceremony at Lisbon University in Portugal on 19 February, U.N. Secretary General Antonio Guterres called for global rules to minimize the impact of electronic warfare on civilians as massive cyberattacks look likely to become the first salvoes in future wars. He offered the United Nations as a platform where various players from scientists to governments could meet and work out such rules “to guarantee a more humane character” of any conflict involving information technology and, more broadly, to keep the internet as “an instrument in the service of good.” Significantly, a group of North Atlantic Treaty Organization (NATO) allied said last year that they were drawing up cyber warfare principles to guide thoer militaries on what justifies deploying cyberattack weapons more broadly, aiming for agreement by early 2019. Some NATO allies believe shutting down an enemy power plant through a cyberattack could be more effective than air strikes. (**Reuters.com, 19 February 2018**)

New Saturn ransomware spotted in the wild

Currently, the malware requests victims of US$300 payment that doubles after 7 days. Once infected a system, the Saturn Ransomware checks if it is running in a virtual environment and eventually it halts the execution to avoid being analyzed by researchers. Then it performs a series of actions to make it impossible for the victims to restore the encrypted files, it deletes shadow volume copies, disables Windows startup repair, and to clear the Windows backup catalog. Researchers are still analyzing the Saturn ransomware, even if it is being actively distributed, it is still unclear what distribution vector threat actors are using to spread it. (**Cyber Defense Magazine, 19 February 2018**)