CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

25 May 2018 **Issue No. 2018-019**

Skills shortage a major cyber security risk

A survey by the Institute of Information Security Professionals (IISP) shows that skills shortage remain a major risk to long-term information security capability and business is still struggling to defend against cyber breaches – but it is getting better at dealing with them. The proportion of information security professionals who feel organizations are getting worse at defending against major cyber security breaches has leapt from 9% to 18 % in the past three years. However, in contrast, the number of businesses that feel prepared to respond to and deal with incidents rose from 47% to 66% over the same period.

Security industry leaders are increasingly putting emphasis on cyber resilience based on good detection and response capabilities, rather than relying mainly on defense technologies and controls. **(ComputerWeekly.com, 23 May 2018)**

Embattled Kaspersky to open Swiss data center 'for transparency'

Cyber-security firm Kaspersky Lab said it will relocate some of its operations from Moscow to Switzerland, after the U.S. government and others accused it of spying on customers at the Russian state's demand. The company had chosen Switzerland for its "policy of neutrality" and data protection laws. It believed shifting servers to Zurich will help ease concerns over laws that let Russian security services monitor data transmissions inside the country. In a statement, the tech firm insisted that it "has never helped, nor will help, any government in the world with its cyber espionage or offensive cyber efforts." **(BBC.com, 15 May 2018)**

Vault 7 inquiry: CIA data leak suspect named by media

U.S. media revealed that a former Central Intelligence Agency (CIA) software engineer is the prime suspect in the leaking of a stolen archive of the CIA last year. However after searching his home, prosecutors charged Joshua Schulte, 29, with having 10,000 child abuse images. He denies the charges and remains as suspect in leaking extensive CIA data to anti-secrecy website Wikileaks. Mr. Schulte designed malware used to break into terrorism suspects' and other targets' computers for the CIA for six years. He quit the CIA in 2016 to work in the private sector.

The 2017 breach, codenamed Vault 7, details how the CIA can take over iPhones through malware and turn smart TVs into surveillance devices and is believed to be the agency's largest leak of classified documents. **(BBC.com, 16 May 2018)**

Amazon asked to stop selling facial recognition technology to police

More than two dozen civil rights organizations are calling on Amazon CEO Jeff Bezos to stop selling its facial recognition technology to the government, according to a letter made public

by the American Civil Liberties Union (ACLU) on 22 May 2018. The technology, called Rekognition, uses artificial intelligence to identify the objects, people, scenes, and more from images or videos. An Amazon executive touted public safety as a “common use case” for the technology in one presentation

While Amazon may be marketing the technology as a way for law enforcement to more easily catch criminals, civil rights organizations worry it could infringe on privacy rights and be used to target vulnerable populations. An Amazon spokesperson said that the company requires customers comply with the law and be responsible when they use Amazon Web Services (AWS). When they find that AWS are being abused by a customer, they suspend the customer’s right to use their services. **(CNN.com, 23 May 2018)**

Cisco warns 500,000 routers have been hacked in suspected Russian plan to attack Ukraine

Cisco warned on 23 May 2018 that hackers have infected at least 500,000 routers and storage devices in dozens of countries with highly sophisticated malicious software, possibly in preparation for another massive cyber attack on Ukraine. Cisco’s Talos cyber intelligence unit said it has high confidence that the Russian government is behind the campaign, dubbed VPNFilter, because the hacking software shares code with malware used in previous cyber attacks that the U.S. government has attributed to Moscow.

Cisco said the malware could be used for espionage, to interfere with internet communications or launch destructive attacks on Ukraine, which has previously blamed Russia for massive hacks that took out parts of its energy grid and shuttered factories. **(CNBC.com, 24 May 2018)**

U.S. disrupts Russian botnet of 500,000 hacked routers

The U.S. Justice Department said on 23 May 2018 that it had seized an internet domain that directed a dangerous botnet of half-million infected home and office network routers, controlled by hackers tied to Russian intelligence, The move was aimed at breaking up an operation deeply embedded in small and medium-sized computer networks that could allow the hackers to take control of computers as well as easily steal data. The Justice Department said the “VPNFilter” botnet was set up by a hacking group variously called APT28, Pawn Storm, Sandworm, Fancy Bear and Sofacy Group. **(SecurityWeek.com, 24 May 2018)**

Roaming Mantis malware expands its reach, now targeting iOS devices.

A malware called 'Roaming Mantis' that infects smartphones through Wi-Fi routers is rapidly spreading across the world. The malware uses compromised routers to infect Android smartphones and tablets, redirect iOS devices to a phishing site, and run CoinHive, a crypto mining script, on desktops and computers. According to Kaspersky Lab, Roaming Mantis has added two dozen more languages including Arabic, Russian, and a host of European languages. Although the malware only affected Android devices when it first emerged, its creators have now taught it to attack iOS devices. Android users are prompted to update their browser, before downloading a malicious app disguised as Chrome or Facebook, which requests a series of permissions and uses these to crack two-factor authentication and hijack Google accounts. Users of iOS, meanwhile, are redirected to a mockup of the Apple website,

named security.apple.com, and are prompted to enter their login details, as well as their bank card number. **(ITNews.com.au, 22 May 2018)**

Misconfigured reverse proxy servers spill credentials

Researchers have created a proof-of-concept attack (PoC) that allows unauthenticated adversaries to extract user credentials from misconfigured reverse proxy servers in order to delete, manipulate or extract data from websites and applications. The PoC attack targets major cloud customers of services such as Amazon Web Services, Microsoft Azure and Google Cloud, according to researchers at RedLock that published a report on their findings Tuesday.

Gaurav Kumar, RedLock CTO, shared one PoC example wherein WordPress servers use credentials to do things like connect to other cloud services. A website might use Identity and Access Management (IAM) credentials to automatically connect to an Amazon Web Services (AWS) storage bucket to backup daily transaction data. Kumar said IAM credentials rely on web server Application Programming Interface (APIs) to link cloud services. By using a simple Client URL (cURL) command, IAM role credentials are freely available for programs to obtain. And that's where RedLock said API and IAM credential abuse can occur. **(ThreatPost.com, 18 May 2018)**

Fiber routers vulnerable to authentication bug, command injection via URL change

Security researchers discovered a remote code execution (RCE) vulnerability in more than a million gigabit passive optical network (GPON) home routers. The vulnerability easily lets an attacker bypass the login authentication page by modifying the URL in the browser's address bar, allowing almost complete access to the router. Accordingly, the search engine used to find connected devices around the world, half of the vulnerable routers are located in Mexico, while the remaining half is in Kazakhstan and Vietnam.

Routers manufactured by Dasan Networks allows anyone to skip the authentication pages by adding "?images/" to the end of any of the router's configuration pages' web address. The flaw also allowed the researchers to exploit a command injection vulnerability, remotely executing other commands on the device and the network through the modified DNS settings.

To protect routers and devices from these threats, the following must be done: 1) familiarize self with the features of router; 2) update and download patches for software regularly; 3) check router's DNS settings to see if they've been tampered with; 4) enable router's built-in firewall; 5) encrypt wireless connections; and, 6) change default credentials and use more complicated passwords. **(TrendMicro.com, 04 May 2018)**