CYBER DEFENSE NEWS

In Cyber Defense and Security, You are the Center

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

29 June 2018 **Issue No. 2018-024**

Security pros expect rise in nation-state attacks

Nation-state attacks are a mounting concern for security professionals, who reportedly expect to see a rise in cyber attacks amid the backdrop of increasing geopolitical tensions. Cybersecurity company Tripwire conducted a survey at Infosecurity Europe 2018 and vast majority of respondents anticipate more nation-state attacks over the next 12 months.

Tripwire surveyed 416 conference attendees to gauge their expectations for the future, and almost all of them (93%) believe more trouble is on the way, with 83% saying they believe nation-states will expand their targets beyond government entities. The same amount of respondents believe that critical-infrastructure attacks from nation-states will rise and that attackers will intentionally cause direct harm. **(InfoSecurity-Magazine.com, 22 June 2018)**

‘Hidden tunnels’ help hackers launch financial services attacks

According to a report published by cyber security company Vectra, the security tools and strategies financial services organizations use to protect their data could be leveraged by cyber criminals who sneak in undetected via “hidden tunnels” to conceal their theft. Ironically, financial firms have the biggest non-government security budgets in the world.

Vectra looked into the case of consumer credit reporting agency Equifax, which experienced a breach that started when a Web server was exploited to access the corporate network. The attackers avoided using tools that would alert the company’s security team by instead building command-and-control (C&C) tunnels into Equifax. They installed more than 30 Web shells with different addresses to burrow into Equifax and, once inside the network, customized their hacking tools to Equifax software, evade firewalls, and exfiltrate information. **(DarReadinig.com, 20 June 2018)**

China TICK APT group targeting air-gapped systems in Asia

Palo Alto Networks experts uncovered a new operation conducted by the cyber espionage group known as Tick APT that has been targeting a secure USB drive built by a South Korean defense company with the intent of compromising air-gaped systems. The Tick APT group has been active for at least a decade, tracked also as Bronze Butler, it was first spotted in 2016 by Symantec and experts believe it is a China-linked threat actor. Experts highlighted the ability of the group in discovering a zero-day flaw in a software used in a certain region, such as Japan and South Korea.

The group has been observed using a variety of proprietary tools and custom malware. Recently, Palo Alto Networks Unit 42 discovered the Tick group targeted a specific type of secure USB drive created by a South Korean defense company. The weaponization of a secure USB drive is an uncommon attack technique and likely done in an effort to spread to air-gapped systems, which are systems that do not connect to the public internet. The malicious code used in the recent attacks conducted by the Tick APT were specifically developed to target systems running Windows XP or Windows Server 2003. (**Cyberdefensemagazine.com.com, 26 June 2018**)

Facebook app analytics mistakenly leaked to outsiders

Facebook confirmed in an email statement that roughly 3 percent of apps on Facebook Analytics has their weekly summary information leaked to outsiders. These reports contained three metrics about the app: the number of new users, weekly active users and page views, and were mistakenly sent to people identified as “testers.” This is just the latest incident to call into question Facebook’s attitude towards data. Unlike the previous incidents, in this one, little critical information about its users appeared to have leaked. Meantime, Facebook said that it started notifying the apps involved and have made technical changes to prevent such incident from happening again. **(CNet.com, 22 June 2018)**

Adobe says it can identify manipulated images using AI

The company behind the photo-editing program Photoshop said it has developed a tool that can detect if an image has been tampered with. Adobe researcher Vlad Morariu employed artificial intelligence (AI) to scan for signs of manipulation that are not usually visible to the naked eye. The AI could tell if an element had been added, moved or cut from a photo. But the company warned that no piece of technology could provide a foolproof verification system. **(BBC.com, 25 June 2018)**

EU States to Form 'Rapid Response' Cyber Force: Lithuania

Nine (9) European Union states are to create rapid response teams to counter cyber attacks within the framework of a new EU defense pact, project leader Lithuania announced last 21 June 2018. Lithuania Defense Minister Raimundas Karoblis said his counterparts from Croatia, Estonia, the Netherlands and Romania were set to join him last 28 June to sign the agreement in Luxembourg while Finland, France, Poland and Spain will join later this year. Teams formed by pooling experts on a rotational basis will be ready to help national authorities to tackled cyber attacks, with the schedule to be approved next year. **(SecurityWeek.com, 25 June 2018)**

Malware in South Korean Cyberattacks Linked to Bithumb Heist

Lazarus Group, a team of cyber criminals reportedly based in North Korea, is believed to be targeting South Korea with malicious documents. The files, recently reviewed by South Korean researcher and experts at AlienVault, pack Manuscrypt malware as the final payload. Researchers in South Korea first detected the documents. One is disguised as related to the G20 International Financial Architecture Working group Meeting and appears to target attendees, who met to discuss economic policies among the world’s financial superpowers. Another is seemingly related to the$31.5 million theft from the Bithumb cryptocurrency exchange. All documents were created in Hangul Word Processor (HWP), a South Korean document editor, and contain malicious code to download Manuscrypt malware.

This is not the first time researchers have linked Manuscrypt to Lazarus Group, which allegedly also used the malware in advanced persistent threat (APT) attacks targeting financial institutions and the SWIFT banking network. **(DarkReading.com, 25 June 2018)**

539 percent uptick in attacks targeting consumer-grade routers since, study

The first quarter of 2018 saw a dramatic increase in the number of cyber attacks targeting consumer-grade routers many of which were in the education, construction, and biotechnology sectors due to their high concentration of the routers. The eSentire Quarterly Threat Report noted a 539 percent uptick in attacks targeting the router since the fourth quarter of 2017 with the high threat volume of attacks likely indicating an over exposed threat surface in the sectors.

Researchers noticed attackers were using legitimate Microsoft binaries such as PowerShell and MSHTA which in the wrong hands, are powerful tools for downloading and executing malicious code in the initial stages of a malware infection. **(SCMagazine.com, 27 June 2018)**

Phishing emails sidestep Microsoft Office 365 filters using ZeroFont

An old tactic is being used by cybercriminals to bypass Microsoft Office 365 (O365) filters for phishing emails. The technique, called ZeroFont, involves the manipulation of text font sizes to trick O365's natural language processing, a tool that identifies malicious emails by checking for text elements commonly used by fraudsters. According to Avanan, the cloud security company that spotted the use of ZeroFont in phishing attacks, cybercriminals send emails that contain text seen differently by the recipient and by the O365 filters. Random text characters or words were added throughout the email, thus preventing the filters from flagging suspicious words or phrases. The ZeroFont technique allows cybercriminals to present different versions of the email. Email recipients would see a normal-looking email while O365 filters will disregard the font size and read the entire plain text as a random string of characters. (**Trendmicro.com, 25 June 2018**)

Voice data of 5.1 million people collected and stored by UK tax authority

The U.K. privacy advocate group Big Brother Watch published a report about the biometric data, specifically voice data, collection practices of HM Revenue and Customs (HMRC). The report shows that the HMRC, U.K.'s tax authority which offers a number of services to citizens, has collected 5.1 million taxpayers' voiceprints as part of its new voice identification (voice ID) policy. According to the report, the HMRC apparently needs to meet lawful processing requirements outlined by the current U.K. Data Protection Act (DPA) and the EU's General Data Protection Regulation (GDPR). HMRC adopts the new technology reliant on biometric data. (**Trendmicro.com, 26 June 2018**)

A new variant of Ursnif banking Trojan served by the Necurs botnet hits Italy

Starting from 6th June, a new version of the infamous banking Trojan, Ursnif hit Italian companies. This malware is well known to the cyber security community. The Ursnif banking Trojan was the most active malware code in the financial sector in 2016 and the trend continued through 2017 to date. Said malware is able to steal users' credentials, credentials for local webmail, cloud storage, cryptocurrency exchange platforms and e-commerce sites.

In order to trick the victim into opening the malicious email, the message is presented as the reply to an existing conversation conducted by the victim in the past.

While investigating the domains involved in the last phishing campaign against the Italian companies, the researchers discovered that many of them were registered by the same email address, “whois-protect[@]hotmail[.]com.” This email address is directly connected to infamous Necurs Botnet, the malicious architecture that was used in the past months to push many other malware. (**CyberdefenseMagazine.com, 27 June 2018**)

Scammers abuse multilingual domain names

Cyber criminals are abusing multilingual character sets to trick people into visiting phishing websites. The non-English characters allow scammers to create “lookalike” sites with domain names almost indistinguishable from legitimate ones. Farsight Security found scam sites posing as banks, loan advisers and children’s brands Lego and Haribo. Smartphone users are at greater risk as small screens make lookalikes even harder to spot. **(BBC.com, 26 June 2018)**