CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

27 April 2018 **Issue No. 2018-016**

G7 tells tech firms to boost efforts to combat extremism

The Group of Seven leading industrialized nations told tech and social media companies on 24 April 2018 to ramp up efforts to combat the spread of extremism. Canada's Public Safety Minister Ralph Goodale said the G7 security ministers raised their concerns during a Toronto meeting with Facebook, Twitter Inc, Alphabet Inc's Google and Microsoft. The four companies are part of the Global Internet Forum to Counter Terrorism (GIFCT), set up last year under pressure from governments in Europe and the United States after a spate of deadly attacks. Security officials say the series of so-called lone wolf attacks around the world partly caused by people becoming radicalized by what they see online. **(Reuters.com, 24 April 2018)**

Surge in anonymous Asia Twitter accounts sparks Bot fears

A surge in new, anonymous Twitter accounts across some areas in Southeast and East Asia deepened fears of US-Style mass social media manipulation in the region. There was a notable surge of followers of prominent Twitter users in Cambodia, Thailand, Vietnam, Myanmar, Taiwan, Hong Kong and Sri Lanka. All of them noticed that these new followers were recently created accounts, adopting local sounding names but barely engaging on the platform, as if lying in wait for someone's command.

Most bots are used for commercial spam. But they have been deployed politically in Asia before. During the 2016 presidential elections in the Philippines, there was a surge of organized bots and trolls deployed to support a presidential candidate.

With elections due in Cambodia, Malaysia, Thailand and Indonesia in the next two years, many of those affected by the Twitter follow surge in Asia are asking whether Silicon Valley Tech giants are doing enough to stop fake accounts before they are given their marching orders. So far, Twitter has found nothing untoward. A spokesperson for Twitter said engineers were "looking into the accounts in question and will take action against any account found to be in violation of the Twitter rules. **(AFP.com, 22 April 2018)**

U.S. Democratic Party sues Russia, Trump, Wikileaks over 2016 hacks

The Democratic National Committee (DNC) filed a lawsuit against Russia, the Trump campaign, and Wikileaks alleging that the Russian government worked with Donald Trump's campaign and Wikileaks to help him win the election. The defendants listed include Guccifer 2.0, the hacker behind the dumped emails; Donal J. Trump, Jr., the president's son; and, Julian Assange, Wikileak's founder.

The lawsuit says Russian intelligence agents hacked DNC's computer, infiltrated its phone systems and stoles tens of thousands of documents and emails. It also alleges the Trump campaign willingly cooperated with the Russian effort, and knowingly used emails stolen in the hack. **(CNet.com, 20 April 2018)**

Microsoft announces new Windows platform security technology

Microsoft announced a new Windows platform security technology Windows Defender System Guard. It's a runtime attestation meant to mitigate attacks in software by taking advantage of the same hardware-rooted security technologies in virtualization-based security (VBS) as Credential Guard. This new security technology can provide supplementary signals for endpoint detection and response (EDR) and anti-virus vendors. It can also detect artifacts of kernel tampering, rootkits, and exploits. Moreover, it can be used for preventing cheating in games, protecting sensitive transactions (banking apps, trading platforms), and providing conditional access (enabling device security-based policies). **(SecurityWeek.com, 20 April 2018)**

Over 20 million users installed malicious ad blockers from Chrome store

A security researcher from AdGuard discovered five (5) malicious ad blockers extension in the Google Chrome Store already installed by at least 20 million users. Said malicious browser extensions are not new. They often have access to everything that users do online and could allow its creators to steal any information that the victims enter into any website they visit, including passwords, web browsing history and credit card details. The five malicious extensions are copycat versions of some legitimate, well-known Ad Blockers. Google immediately removed them from the Chrome Store after they were reported. **(TheHackerNews.com, 19 April 2018)**

Facebook plans to build its own chips for hardware devices

Facebook seems to be forming a team to build its own hardware chips. According to a post, Facebook is looking for experts in application-specific integrated circuit (ASIC) and field programmable gate array (FPGA) – two custom silicon designs to help it evaluate, develop and drive next generation technologies within Facebook – particularly in artificial intelligence and machine learning. Building its own processors would help the company reduce dependency on companies such as Qualcomm and Intel. It could also help power its artificial intelligence software, servers in its data center, as well as its future hardware devices, like Oculus virtual reality headsets and smart speakers. Moreover, using its custom chips would allow the company to gain more control over its own hardware roadmap better and eventual feature set to offer better performance to its users. **(TheHackerNews.com, 19 April 2018)**

Twitter bans ads from Kaspersky Lab

Twitter no longer allows Russia-based cybersecurity firm Kaspersky Lab to advertise on the platform. While Twitter's statement to the press did not provide any additional information, it cited a controversial Department of Homeland Security (DHS) Binding Operational Directive (BOD) that bans Kasperksky products in federal agencies due to concerns that the company may be aiding Russia's espionage efforts. **(SecurityWeek.com, 23 April 2018)**

Kaspersky calls out Twitter's Jack Dorsey over ad ban

In an open letter, Eugene Kaspersky criticized Twitter Chief Executive Officer Jack Dorsey and revealed that his firm has been banned from advertising on the social network. In the letter, Kaspersky revealed that Twitter banned the cybersecurity company saying that its business model 'conflicts with acceptable Twitter ads." It blames the same "geopolitical noise" for the

U.S. government's ban on Kaspersky products. Kaspersky said his company would not be advertising with Twitter for the rest of 2018, even if the ban were lifted. The funds will instead go to the Electric Frontier Foundation. **(CNet.com, 20 April 2018)**

‘Lazy hackers’ turn to automated attack tools

A study by security firm Cybereason revealed that cyber-attackers are turning to tools that automate the process of finding and hijacking vulnerable servers. The firm used a fake server known as a honeypot to log everything done to it by digital intruders. The server was quickly found and hijacked in seconds by a bot that broke through its digital defenses. While bots are widely used by cyber-criminals to seek out and subvert vulnerable servers, the process of going from initial compromise to full-blown breach is often carried out by a human. However, in this case, the bot did 80% of the work in just a couple of minutes. **(BBC.com, 17 April 2018)**

Britain “will” be the victim of serious cyber attack from Russia, says U.K.’s Government Communications Headquarters (GCHQ)

The head of U.K.’s Government Communications Headquarters (GCHQ) Claran Martin said they are focusing on building resilience in the systems believed to be Britain’s power and water supplies, internet and transport networks, and health services. He confirmed that GCHQ was on high alert for follow-up activity following the Salisbury attack last March 2018 wherein A retired Russian military intelligence colonel convicted for spying for the U.K. and her daughter were poisoned by a nerve agent.

Senior representatives from utility, transport and internet firms in additional to the National Health Service (NHS) are believed to have attended intelligence briefings at the National Cyber Security Centre (NCSC) on the specific methods being used by Russia to target Britain’s national infrastructure.

The NCSC believes that the U.K. is facing a serious cyber attacks. It wrote a letter to the government to set out urgent actions that departments and individual officials should take to protect Whitehall from cyber assaults. **(Express.co.uk, 20 April 2018)**