CYBER DEFENSE NEWS

In Cyber Defense and Security, You are at the Center

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

06 July 2018 **Issue No. 2018-025**

Recently discovered RANCOR cyber espionage group behind attacks in South East Asia

Security researchers at Palo Alto Networks have uncovered a new cyber espionage group tracked as RANCOR that has been targeting entities in South East Asia. Accordingly, the RANCOR APT group has been targeting political entities in Singapore, Cambodia, and Thailand, and likely in other countries, using two previously unknown strain of malware. The two malware families were tracked as DDKONG and PLAINTEE.

The hackers leverage spear phishing messages using weaponized documents containing details taken from public news articles on political news and events. These decoy documents are hosted on legitimate websites, such as the website of the Cambodian government, and Facebook. The recent campaign appears related to the KHRAT Trojan, a backdoor that was associated with the China-linked APT group tracked as DragonOK (also known as *NetTraveler (TravNet), PlugX, Saker, Netbot, DarkStrat, and ZerTi).* **(CyberDefenseMagazine.com, 28 June 2018)**

Facebook admits sharing users' data with 61 tech companies

Facebook has admitted that the company gave dozens of tech companies and app developers' special access to its users' data after publicly saying it had restricted outside companies to access such data back in 2015. However, in a 747-page long document delivered to Congress on 29 June 2018, Facebook admitted that it continued sharing data with 61 hardware and software makers, as well as app developers after 2015 as well. The disclosure comes in response posed to Facebook CEO Mark Zuckerberg by members of Congress in April about its company's practices with data of its billions of users.

Among other things, the documents revealed that Facebook granted a "one-time" six-month extension to 61 companies including AOL, Nike, United Parcel Service and dating app Hinge to come into compliance with Facebook's new privacy policy on user data. Moreover, the documents also acknowledged that Facebook partnered with 52 domestic and international companies, including U.S. tech giants Apple, Microsoft, Spotify, Amazon, Sony, Acer, China-based Huawei and Alibaba, and device-makers Samsung and Blackberry.

The company shared information about its users with these companies to help them create their own versions of Facebook or Facebook features for their devices, "under the terms and policies they provide to their users." **(TheHackerNews.com, 01 July 2018)**

Researchers uncover new attacks against LTE network protocol

A team of researchers has discovered some critical weaknesses in the ubiquitous LTE mobile device standard that could allow sophisticated hackers to spy on users' cellular networks, modify the contents of their communications, and can even re-route them to malicious or phishing websites. LTE or Long Term Evolution, is the latest mobile telephony standard used by billions of people designed to bring many security improvements over the predecessor standard known as Global System for Mobile (GSM) communications.

However, multiple security flaws have been discovered over the past few years, allowing attackers to intercept user's communications, spy on user phone calls and text messages, send fake emergency alerts, spoof location of the device and knock devices entirely offline. **(TheHackerNews.com, 29 June 2018)**

Facebook makes additional application programming interface (API) changes to secure user data

Facebook announced that it will be introducing new restrictions and changes regarding the Graph API Explorer App, Profile expressions Kit, Media Solutions APIs, Pages API, Marketing API, Lead Ads Retrieval and Live Video APIs, all with the goal of better protecting user information. Starting 02 July 2018, Facebook is deprecating its Graph API Explorer App and developers will need to use their own app's access tokens to do test queries on the Graph API Explorer. It will also be deprecating its Profile Expression Kit tool on 01 October due to low adoption. **(SCMagazine.com, 02 July 2018)**

Bug bounty programs turn attention to data abuse

Experts say that more companies, particularly social media firms, may follow Facebook's footsteps in turning to bug bounty programs to scout out any data privacy abuse on their platforms. After its Cambridge-Analytica scandal in March, Facebook launched a "Data Abuse Bounty Program" in an attempt to crackdown on data misuse by third-party app developers. The program was put to good use after a bounty hunter working through the program spotted a popular Facebook app that was exposing the personal data, including private information, friends, posts and photos, of millions of users. **(ThreatPost.com, 01 July 2018)**

Facebook apologizes for bug that temporarily unblocked people

Facebook announced on 02 July that it will notify 800,000 people about a bug that unblocked accounts those users had previously blocked. The said bug was active between 29 May and 05 June. In a blog post, Facebook's chief privacy officer, Erin Egan, said that some blocked users could not view posts that the person who blocked them shared with friends, but they could have seen things that person shared. The company said that 83% of users impacted by the bug had one person temporarily unblocked. A user who was unblocked during that time may have been able to talk to the person who blocked them on Messenger. Facebook said the issue has been resolved, and all previous settings have been reinstated. **(CNN.Com, 02 July 2018)**

The Pirate Bay again caught mining crypto-currency using CPU power

It was last year when The Pirate Bay was first caught mining crypto-currency without notifying the users. This year, the Monero crypto-currency miner has been found to make an appearance once again, according to TorrentFreak. According to a user who was trying to upload torrents to The Pirate Bay, his CPU got "really hot" during the process. Upon inspecting the source code, he found the crypta.js mining script. In order to block in-browser mining, users must install "NoScripts" browser extension. (**Fossbytes.com, 04 July 2018**)

California lawmakers approve data-privacy bill opposed by Silicon Valley

California Governor Jerry Brown signed last 28 June 2018 a data privacy legislation aimed at giving consumers more control over how companies collect and manage their personal information. Under the proposal, large companies, such as those with data on more than 50,000 people, would be required starting on 2020 to let consumers view the data they have collected on them, request deletion of data, and opt out of having the data sold to third parties. Companies must provide equal service to consumers who exercise such rights under the law. Each violation would carry a $7,500 fine. The law applies to users in California. **(Reuters.com, 29 June 2018)**

Fortinet, Interpol ink threat sharing info deal to combat cybercrime

Interpol, the organization that facilitates global police cooperation, signed an agreement with cyber security company Fortinet, which would ensure that law enforcement has access to the most comprehensive threat intelligence necessary to take effective action against cybercrime. Under the said partnership, both organizations will collaborate to combat cybercrime and threats to privacy globally by sharing threat information.

A threat intelligence expert from Fortinet will be assigned to collaborate with experts at the Interpol Global Complex for Innovation (IGCI) to provide a clearer understanding of the current threat landscape. Before the announcement Fortinet has been an active member of an expert working group within the Interpol. **(Inquirer.net, 27 June 2018)**

Iranian hackers impersonate Israeli security firm

A group of Iranian hackers focused on cyber espionage recently built up a website to impersonate ClearSky Ceyber Security, the Israeli firm that exposed their activities last year. The hackers, tracked as APT35 and also known as NewsBeef, Newscaster, and Charming Kitten, have been active since at least 2011, with their activities detailed for the first time several years ago.

The security firm announced on its Twitter account that Charming Kitten built a phishing website impersonating their company as clearskysecurity\.et (the real website is http://clearskysec.com). The APT copied entire pages from the legitimate website, but also changed one of them to include a sign in option with multiple services. Anyone entering credentials there would have had then sent to the hackers instead. **(SecurityWeek.com, 03 July 2018)**

Google slammed for giving Gmail access to third party developers

According to a report from the Wall Street Journal, third-party apps have access to users' Gmail accounts and permission to read people's emails but only after the consent of the users which nowadays is not important anymore. The publication has named two apps among the list of many. Return Path and Edison Software that are known to have allowed employees to read thousands of emails to train their smart reply feature. Typically, a popup box is thrown in front of the users asking them for permissions to access different kinds of data and device components. Google says it thoroughly checks third-party developers before giving them access to user data. This includes verifying that an app correctly identifies its developers and its privacy policies are clear and easily accessible. (**Fossbytes.com, 03 July 2018**)

Open-Xchange App Suite multiple bugs discovered

According to security tracker, there are several vulnerabilities reported in Open-Xchange App Suite. A remote authenticated user can obtain potentially sensitive information on the target system. Said user can conduct cross-site scripting attacks and obtain potentially sensitive information. The impact of this multiple bugs in open Xchange app is the disclosure of authentication information, system information, user information, and the execution of arbitrary code via network, as well as the modification of user information (**SecurityTracker.com, 05 July 2018**)