April 06, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Marriott International Data Breach
- Malware on Docker Containers
- Thousands of Android apps contain hidden behaviors
- Firefox patches two zero-days exploit
- Safari patches several zero-day vulnerabilities
- More than 15,000 Elasticsearch server wiped and defaced by attacker

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE's that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, ebay, eset, bugcrowd, under armour, coinbase, CCM, etc have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team's professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

1. Marriott International Data Breach

Description	
Hotel empire Marriott International has suffered a second major data breach, the first one was in 2018. Information such as the guests' contact details like name, mailing address, phone number is believed to have been disclosed. According to an online notice posted by Marriott, the attack was carried out via third-party software that Marriott's hotel properties use to provide guest services.	
Source	https://mysupport.marriott.com/
Infected Company	Marriott International

2. Malware on Docker Containers

Description	
A crypto-mining malware named 'Kinsing' is being installed by hackers on Docker servers running API ports exposed to the internet without a password. According to the security researcher at Aqua, hackers use the access provided by the exposed port to spin up an Ubuntu container where they download and install the malware. It is a cryptocurrency mining malware which is able to run scripts, gather local SSH credentials to infect other cloud systems with the same malware.	
Source	https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability
Infected Technology	Docker containers
Recommendation	Disable open API ports on docker container

3. Thousands of Android apps contain hidden behaviors

Description	
An academic study published by students and researchers from The Ohio State University, New York University, CISPA Helmholtz Center for Information Security discovered hidden behaviors like backdoors. The academics developed a tool named 'InputScope' which analyzed input form fields inside more than 150,000 Android applications. They identified more than 10,000 apps containing a variety of back doors such as secret access keys, master passwords and secret commands. These backdoor mechanisms could allow attackers to gain unauthorized access of users' account and even allow the attackers to run code on devices with elevated privileges if they have physical access to the device. These apps included screen locker app, live streaming app, translation app with millions of installs.	
Source	https://panda.moyix.net/~moyix/papers/inputscope_oakland20.pdf
Infected Technology	Android Devices
Recommendation	Do not install application without researching on them

4. Firefox patches two zero-days exploit

Description	
Firefox updated their browsers which patched two vulnerabilities, CVE-2020-6819 and CVE-2020-6820. The bugs are user-after-free vulnerabilities. These bugs reference memory even after it has been freed and cause a program to crash, use unexpected values, or execute code. Firefox advises its users to update their browsers to the latest 74.01 build.	
Source	https://www.zdnet.com/article/firefox-gets-fixes-for-two-zero-days-exploited-in-the-wild/
Infected Technology	Firefox browsers
Recommendation	Update to the latest Firefox browsers

5. Safari patches several zero-day vulnerabilities

Description	
The attackers behind WP-VCD, a family of Wordpress infection, have started distributing pirated version of Corona virus plugin which creates a backdoor in a website. Safari patched several vulnerabilities spanning different versions which allowed attackers to secretly access the device's camera, microphone, locations and in some cases save passwords, which was discovered by security researcher Ryan Pickren. This was possible because Safari browser grants access to certain permissions such as camera, microphone, location and more on a per-website basis. Safari can access these features without any permissions to certain trusted sites. Safari failed to check if the websites adhered to the same-origin policy, thereby granting access to a different site that shouldn't have obtained permissions in the first place.	
Source	https://www.ryanpickren.com/webcam-hacking
Infected Technology	iOS devices
Recommendation	Update to the latest Safari browsers

6. More than 15,000 Elasticsearch server wiped and defaced by attacker

Description	
An attacker is attempting to break into Elasticsearch server and wipe its content. The automated attack started around March 24 and is leaving name of a cyber-security firm, Night Lion Security, in the servers to divert the blame. According to BinaryEdge search, the firm's name is left in more than 15,000 servers that are exposed online.	
Source	https://www.zdnet.com/article/a-hacker-has-wiped-defaced-more-than-15000-elasticsearch-servers/
Infected Technology	Elasticsearch servers
Recommendation	Use authentication and authorization methods

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**