InfoSec Weekly

Compilation of InfoSec News

Topics for Infosec Quickly:

1. Cookie-Stealing Malware found in Android
2. Coronavirus Maps-a malware infecting PCs
3. WordPress Plugin Bug Threatens 100K Websites
4. Google Cloud Shell Root Compromise
5. Flaws Riddle Zyxel's Network Management Software
6. BlackWater Malware Abuses Cloudflare Workers for C2 Communication
7. COVID-19 Testing Center Hit by Cyberattack

16/03/2020

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. **Cookie-Stealing Malware found in Android**

Description	
A dangerous Android Malware dubbed as "Cookie Thief '' has been found stealing users authenticated cookies from web browsing and other apps, including Chrome and Facebook. The malware works by acquiring superuser root rights on the target devices, and subsequently, transfer stolen cookies to a remote command-and-control server operated by attackers. Malware creates a proxy server on the infected device to impersonate the account owner's geographic location to make the access requests legitimate. So, a cyber-criminal can gain complete control over the victim's account and not raise suspicion from Facebook.	
Source	https://thehackernews.com/2020/03/android-cookies-malware-hacking.html
Infected Technology	Android
Recommendation	Block third party cookies and u\se private browsing mode

2. **Coronavirus Maps-a malware infecting PCs**

Description	
COVID-19, Corona Virus disease is becoming an opportunity for attackers to spread malware or launch cyber-attacks. Coronavirus maps is a new attack that takes advantage of internet users increased craving for information about the novel coronavirus that is wreaking havoc worldwide. The malware attack specifically aims to target those who are looking for cartographic presentations of the spread of COVID-19 on the Internet, and tricks them to download and run a malicious application that, on its front-end, shows a map loaded from a legit online source but in the background compromises the computer.	
Source	https://thehackernews.com/2020/03/coronavirus-maps-covid-19.html

3. WordPress Plugin Bug Threatens 100K Websites

Description	
A high severity flaw has been found in a popular WordPress plugin called Popup builder which could enable an unauthenticated attacker to infect malicious JavaScript into a popup, opening more than 100k websites to take over. A specific plugin, AJAX hook was available to unprivileged users, and it lacked nonce checks or capability checks for the functions called. "This meant that an unauthenticated attacker could send a POST request to wp-admin/admin-ajax.php with an array parameter, 'allPopupData', containing a number of key-value pairs, including a popup's ID (visible in the page source) and a malicious JavaScript payload, which would then be saved in that popup's settings and executed whenever a visitor navigated to a page where the popup was displayed.	
Source	https://threatpost.com/wordpress-plugin-bug-popup-builder/153715/
Infected Technology	WordPress
CVE Details	CVE-2020-10196 CVE-2020-10195

4. Google Cloud Shell Root Compromise

Description	
A new vulnerability was found in google cloud shell where that is a container escape that leads to host root access and the ability to use privileged containers. The Google Cloud Shell is a Linux- and browser-based front-end for administrators that provides access to various resources in the Google Cloud Platform. When the Cloud Shell instance is done starting a terminal window is presented to the user. If an attacker can compromise your Cloud Shell, it can access all your GCP resources. After that, with root access, an attacker was also able to reconfigure Kubernetes to flip all of the containers from unprivileged to privileged by writing a new "cs-6000.yaml" configuration file and setting the old config file to "/dev/null."	
Source	https://threatpost.com/100k-google-cloud-shell-root-compromise/153665/
Infected Technology	Google cloud shell

5. Flaws Riddle Zyxel's Network Management Software

Description

A networking hardware vendor Zyxel and its Cloud CNM SecuManager software is chock-full of unpatched vulnerabilities that kick open the doors for hackers to exploit. 16 new vulnerabilities have been identified ranging from multiple backdoors and default credentials to insecure memory storage. The attack surface is very large, and many different stacks are being used, some daemons are running as root and are reachable from the WAN. Also, there is no firewall by default.	
Source	https://threatpost.com/flaws-zyxels-network-management-software/153554/
Infected Technology	Zyxel
CVE Details	CVE-2020-9054
Recommendation	Update and apply all available patches

6. BlackWater Malware Abuses Cloudflare Workers for C2 Communication

Description	
A new backdoor malware called BlackWater was found abusing Cloudflare Workers as an interface to the malware's command and control server. A BlackWater malware was found distributing a malicious file "Important - COVID-19.rar" which is pretending to be information about the Coronavirus (COVID-19). This file uses word icon, when opened the malware will extract a word document, while extracting that file this malware also extracts the sqltuner.exe file which launches malware using a command line that causes the BlackWater to connect to a Cloudflare Worker that acts as a command and control server or at least a passthrough to one.	
Source	https://www.bleepingcomputer.com/news/security/blackwater-malware-abuses-cloudflare-workers-for-c2-communication/
Infected Technology	Cloudflare
Recommendation	Do not fall for phishing mails. Review mail address before opening any links or downloading files

7. COVID-19 Testing Center Hit by Cyberattack

Description	
A University Hospital Brno faced a Cyber-attack affecting a dozen of results for COVID-19 tests that have been delayed in the past couple of days due to the cyber-attack. Due to this attack computer systems started "falling gradually" and had to be shut down. Also, the medical data collected by lab systems is stuck there and cannot be recorded in the databases. Due to this attack, Recipes are written by hand or typed, leading to longer examination times.	
Source	https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/
Infected Area	Hospital
Recommendation	Periodically perform Vulnerability Assessment and update security measures

For any queries/recommendations:

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