InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. 'USB Anywhere' bugs open supermicro servers to remote attackers
2. Just an SMS could let remote attackers access all your mails
3. XKCD-Forum hacked
4. Firefox blocks third-party tracking cookies and crypto mining by default
5. ATM heist lesson for banks to shun complacence
6. Android Zero-day bug does not make it on Google's fix list

08/09/2019

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. 'USB Anywhere' Bugs open supermicro Servers to Remote Attackers

Description	
Researchers have uncovered a set of USB vulnerabilities in the baseboard management controller (BMC) on Supermicro's Server boards that could allow attackers to hijack thousands of servers. It can remotely be compromised by virtually plugging in malicious USB devices.	
Source	https://threatpost.com/usbanywhere-bugs-supermicro-remote-attack/147899/
Infected Technology	Supermicro server

2. Just an SMS Could let remote attackers access all your mails

Description	
Researchers have disclosed a new kind of advanced phishing attack targeting Android phones that can trick users into installing malicious settings on their devices that are disguised as innocuous network configuration updated.	
Source	https://thehackernews.com/2019/09/just-sms-could-let-remote-attackers.html
Infected Technology	Android
Recommendation	Do not open links that are delivered through SMS if it looks suspicious

3. XKCD-Forum Hacked

Description	
XKCD- the most popular webcomic has been hacked. Apparently, unknown Hackers were able to breach the XKCD forum and managed to steal personal data of over 562,000 users .The stolen data which has been leaked on the internet includes IP addresses , usernames, email address ,and their password encrypted in MD5 format which is an easy one to decrypt.	
Source	https://thehackernews.com/2019/09/xkcd-forum-hacked.html
Infected Company	XKCD

4. Firefox blocks third-party tracking cookies and crypto mining by default

Description	
Mozilla's Firefox web browser will protect your privacy by blocking third-party tracking software for all its users by default, theoretically keeping companies from keeping tabs on your online activity and potentially selling it to others. With Firefox version 69, Mozilla just flipped the switch to turn on its Enhanced Tracking Protection for all users, instead of just few users .	
Source	https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/

5. ATM heist lesson for banks to shun complacence

Description
Alleged hackers were caught while executing a targeted attack in Nepal's biggest financial banks. It is believed that they used a well-crafted malware to infect the transactional switch that resides in NEPS to generate a fake request that would allow them to cash-out even if the compromised accounts did not have enough balance.

Source	https://www.business-standard.com/article/news-ani/nepal-police-arrests-5-chinese-nationals-for-hacking-atms-119090100416_1.html
Infected Industry	Financial Institute(s) of Nepal
Recommendation	Harden your infrastructures; Monitor for malicious activities; Make and deliver a proper action plan

6. Android zero-day bug does not make it on Google's fix list

Description
Researchers are of high-severity zero-day vulnerability in Google's Android operating system, which if exploited could give a local attacker escalated privileges on target's device. Google yesterday present security patches for the Android mobile operating system but did not include the fix for at least one bug that enables increasing permissions to kernel level

Source	https://www.bleepingcomputer.com/news/security/android-zero-day-bug-does-not-make-it-on-google-s-fix-list/
Infected Technology	Android
Recommendation	Patch your android devices

For any queries/recommendations:

Contact us: whois@cryptogennepal.com