InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Electron Based apps can easily be backdoor
2. Guest-to-Host escape In Microsoft Hyper V
3. Facebook Sues two app developers for click fraud
4. KDE Linux Desktops Could Get Hacked Without Even Opening Malicious Files
5. Clever attack uses SQLite database to hack other apps, malware Software

11/08/2019

www.cryptogennepal.com

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. Electron Based apps can easily be backdoored

Description	
Electron is a development platform which is used apps such as skype, WhatsApp, slack. It has been discovered that electron-based applications can be easily based application can be easily modified without triggering warnings. A security researcher demonstrated a tool he created called BEEMKA, which allowed others to unpack Electron ASAR archive files and inject new code into Electron's JavaScript and built-in Chrome Browser Extensions.	
Source	https://arstechnica.com/informationtechnology/2019/08/skype-slack-other-electron-based-appscan-be-easily-backdoored/
Infected Technology	Electron Platform

2. Guest-to-Host escape In Microsoft Hyper V

Description	
Hyper -V Manager Inherits all the security Vulnerabilities Occupied by Windows RDP which lets the host machine to connect with guest virtual machine and share synchronized resources, including clipboard hijacking and path-traversal vulnerabilities, that could lead to guest-to-host VM escape attack. An attacker who successfully exploited this vulnerability could execute arbitrary code on victim's system and then install, view, change, or delete program/data or create new accounts with full user rights.	
Source	https://thehackernews.com/2019/08/reverse-rdp-windowshyper-v.html?m=1
Infected Technology	Windows

3. Facebook Sues two app developers for click fraud

Description

Both Hong Kong-based JediMobi and the Singapore-based LionMobi developers created android apps infected with malware that faked user click on social media platform adds. The Program lets Facebook's advertisers host their ads on participating mobile apps, whose developers receive a payout if a user clicks through. Those apps include apps to clear up phone storage, save battery life, scan for viruses etc. The malware will show ads on your desktop even leaving the app, and the app has unauthorized access to the phone's lock screen or contacts.

Source	https://www.engadget.com/2019/08/06/facebook-suestwo-app-developers-for-click-fraud/
Infected Technology	Android

4. KDE Linux Desktops Could Get Hacked Without Even Opening Malicious Files

Description

An unpatched Zero-day vulnerability disclosed by security researcher in the KDE software framework that could allow maliciously crafted desktop and directory files to silently run arbitrary code on a user's computer-without even requiring the victim to actually open it

Source	https://thehackernews.com/2019/08/kde-desktoplinux-vulnerability.html
Infected Technology	KDE Linux Desktop

5. Clever attack uses SQLite databases to hack other apps, malware servers

Description

Checkpoint Security Researcher showed demos of tainted SQLite database hijacking the command and server of a malware operation, and malware using SQLite to achieve persistence on iOS devices.

Source	https://www.zdnet.com/article/clever-attack-uses-sqlitedatabases-to-hack-other-apps-malware-servers/
Infected Technology	iOS Device

For any queries/recommendations:

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