InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Malware found in CamScanner
2. Checkpoint software patched
3. IOS Exploits
4. Hostinger Suffers Data Breach
5. xHelper, a Trojan Found in thousands of Androids Devices
6. IOT Botnet infecting Android Set-top boxes
7. Impreva Data Breach
8. Windows 7 End of Support Nears Closer
9. Foxit Software Disclose Data Breach Exposing User password
10. Critical Cisco Bug Exposes IOS XE Networking Devices

03/09/2019

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. Malware found in CamScanner

Description
CamScanner-a highly-popular Phone PDF creator app-has been found malicious as it contains a hidden Trojan Dropper module, that could allow remote attackers to secretly download and install malicious program on users' Android devices. The module also extracts and runs another malicious module from an encrypted file included in the app's resource.

Source	https://www.kaspersky.com/blog/camscanner-malicious-android-app/28156/
Infected Technology	Smart-phones
Recommendation	Uninstall CamScanner

2. Checkpoint Software Patched

Description
A Vulnerability in Checkpoint was discovered in Endpoint security Initial Client software for Windows allowing potential attackers to escalate privileges and execute code using System privileges. Attackers after exploitation can load and execute malicious payloads in a persistent way.

Source	https://www.bleepingcomputer.com/news/security/check-point-patches-privilege-escalation-flaw-in-endpoint-client/
Infected Technology	N/A
Recommendation	Patch available for this vulnerability so install updates
CVE ID	CVE-2019-8461

3. IOS exploits	
Description	
Vulnerabilities including iphone web browser, kernel and separate sandbox escapes were discovered in an Apple Ios. One of the privilege escalation chains was still 0-day and unpatched at the time of discovery.	
Source	https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html
Infected Technology	IOS
Recommendation	Be careful While Visiting Unknown Websites, they could be hacked websites.Wait for updates from manufacturer

4. Hostinger Suffer Data Breach	
Description	
Hostinger - a web hosting provider - suffers a massive data breach as an unauthorized third party gained access to “hashed passwords and other data” associated with millions of customers. The company was compromised as unknown hacker found an authorization token on one of the company’s servers. The attacker used authorization token to obtain further access and escalate privileges to their system Restful API Server.	
Source	https://thehackernews.com/2019/08/web-hosting-hostinger-breach.html
Infected Technology	N/A
Recommendation	Change credentials

5. XHelper , a Trojan found in thousands of Android devices

Description
Trojan dropper named xHelper has been spreading to more and more Android devices with 32,000 devices having been found infected in the last few months. These are the tools used by attackers to deliver other malware strains to devices that have already been compromised. xHelper spreads using Dalvik Executable files camouflaged as JAR archives, containing compiled Android application code. These encrypted DEX files are first decrypted and then compiled using the dex2oat compiler tool into an Executable and Linkable Format binary which gets executed natively by the device's processor.

Source	https://blog.malwarebytes.com/android/2019/08/mobile-menace-monday-android-trojan-raises-xhelper/
Recommendation	Do not install third party apps

6. IOT Botnet infecting Android Set-top boxes

Description	
Cyber security firm WootCloud Labs has found a new botnet named 'Ares' which is targeting android set-top boxes due to a port being left exposed. Android Debug Bridge (ADB) is a standard feature of the Android OS. It allows access to the Android OS via a command-line interface. ABD terminal can be accessed over a network or the internet via a device's port 5555. And if the vendors fail or forget to disable this service, it is being exposed to remote attacks. Once the Ares bot is installed on the android-based devices, it launch scanners to: fingerprint and detect more android devices via ADB interface Install attacker-specific payloads on the compromised devices to trigger additional set of attacks such as crypt-mining, etc.	
Source	https://www.wootcloud.com/blogs/ars_botnet.html
Infected Technology	Android

7. Impreva Data Breach

Description	
Impreva, a leading provider of Internet firewall services that help websites block malicious cyberattacks, alerted customers on 27 August that a recent breach exposed email address, scrambled passwords, API keys and SSL certificates for a subset of its firewall users.	
Source	https://www.securitymagazine.com/articles/90841-cybersecurity-software-company-imperva-suffers-data-breach
Infected Industry	Imperva

8. Windows 7 End Of Support Nears Closer

Description	
Microsoft is ending support for Windows after 14th January, 2020 which means no technical support, no software updates and most importantly no security updates. Still it is estimated that millions of PCs are still relying on windows 7 and thus leaving them exposed to new bugs that will probably never be patched. Microsoft has been recommending users to be upgraded to Windows 10 for years now and as the end of life for Windows 7 nears closer it is about time to be upgraded so as to stay protected from the inevitable new bugs.	
Source	https://www.microsoft.com/en-us/microsoft-365/windows/end-of-windows-7-support
Recommendation	Upgrade to the latest version of Windows

9. Foxit Software Disclose data Breach Exposing User Password

Description	
Foxit Software, the company behind the Foxit PDF reader app, said today that hackers breached its servers and have made off with some user information.	
Source	https://www.bleepingcomputer.com/news/security/foxit-software-discloses-data-breach-exposing-user-passwords/
Infected Technology	Foxit

10.	Critical Cisco Bug Expose IOS XE Networking Devices
Description	
Cisco has discovered a vulnerability that leaves devices running its IOS XE operating system open to malicious attacks. It allows attackers to bypass authentication checks and execute privileged commands on a device running Cisco IOS XE, the operating system installed on Cisco's enterprise network devices.	
Source	https://www.zdnet.com/article/patch-now-cisco-ios-xe-routers-exposed-to-rare-1010-severity-security-flaw/
Infected Technology	IOS XE Networking Devices
Recommendation	Install updates as Patch is available
CVE ID	CVE-2019-12643

For any queries/recommendations:

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