November 1, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- 'AbstractEmu' Malware can gain root access on Android devices
- Tel Aviv City's +3,500 Wi-Fi Networks cracked
- Wslink malware detected acting as a server and executing modules in memory
- Increased password spray attacks targeting privileged cloud accounts

CryptoGen Nepal

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.

'AbstractEmu' Malware can gain root access on Android devices

Description	
A new android malware has been found infecting smartphones with methods to evade detections. Various android apps were found posing as utility apps and system tools like password managers, money managers, app launchers, and data saving apps, seven of which contained the rooting functionality. These apps have also been seen on third party app stores such as Amazon Appstore and Samsung Galaxy Store along with Apotide and APKPure.	
Source	https://blog.lookout.com/lookout-discovers-global-rooting-malware-campaign
Infected Technology	Android Smartphones
Recommendation	Do not download apps from stores before validating

Tel Aviv City's +3,500 Wi-Fi Networks cracked

Description	
A Isreli Researcher was able to crack hashes for over 5,000 Wi-Fi Networks to highlighting how unsecure Wi-Fi passwords can become a gateway for serious threats to individuals, small businesses, and enterprises. The attack method used to demonstrate this issue is based on Jens "atom" Steubes earlier finding in 2018. The attack was performed by capturing PMKIDs associated with clients and used brute-force attack by using cracking tool named hashcat. A successful compromise of the Wi-Fi network could enable a threat actor to mount man-in-the-middle (MiTM) attacks to gain access to sensitive information.	
Source	https://www.cyberark.com/resources/threat-research-blog/cracking-wifi-at-scale-with-one-simple-trick
Infected Technology	Wi-Fi networks with weak credentials
Recommendation	Enforce stronger password (at least 12 characters with one lower case character, one upper case character, one symbol, one digit)

Wslink malware detected acting as a server and executing modules in memory

Description	
A highly targeted malware attack detected by Slovak cybersecurity firm which runs as a service and infects the victim host by executing PE file when loaded into memory. The malware is found to be delivered to the victim PC by cryptographic key exchange method.	
Source	https://www.welivesecurity.com/2021/10/27/wslink-unique-undocumented-malicious-loader-runs-server/
Infected Technology	Windows
Recommendation	Update End Point Protection/AV signatures and monitor for malicious activities

Increased password spray attacks targeting privileged cloud accounts

Description	
Microsoft's DART team has detected a rise in password brute force attack targeting privileged cloud accounts and high-profile identities such as C-level executives. The list of most popular targeted accounts includes profiles from security, Exchange service, global, and Conditional Access administrators to SharePoint, helpdesk, billing, user, authentication, and company admins.	
Source	https://techcommunity.microsoft.com/t5/azure-active-directory-identity/advancing-password-spray-attack-detection/ba-p/1276936
Infected Technology	Cloud Based Services
Recommendation	Use strong password credential with minimum 12 characters

Hive ransomware now encrypts Linux and FreeBSD system

Description

Internet security firm, ESET has discovered a new variant of the Hive ransomware that is targeting Linux and FreeBSD systems. The new variant of the ransomware is still in development, looks buggy and lacks functionality. The Linux variant of the ransomware currently fails to execute without root permission and comes only in one execution option.

Source	https://twitter.com/ESETresearch/status/1454100591261667329
Infected Technology	Linux and FreeBSD system
Recommendation	Do not download application from untrusted sources Use EDR solutions to monitor and protect endpoint devices
CVE-ID	N/A

WordPress bug impacts 1M sites

Description

WordPress's OptinMonster plugin has been found to be affected by a high severity bug that allows an unauthenticated attacker to access the API and export sensitive information. The plugin has been installed on over 1,000,000 sites. The plugin was meant to be designed to create sales campaigns on WordPress sites using dialogs. The REST-API endpoints had been insecurely implemented making the unauthenticated attacks to various endpoints on site running the vulnerable version possible.

Source	https://www.bleepingcomputer.com/news/security/wordpress-plugin-bug-impacts-1m-sites-allows-malicious-redirects/
Infected Technology	OptinMonster
Recommendation	Update patch to 2.6.5
CVE-ID	CVE-2021-39341

Microsoft makes web content filtering generally available

Description

Microsoft has made web content filtering generally available for all windows enterprise customers. The web content filtering reports can be accessed and viewed via the new Microsoft 365 Defender portal through security.microsoft.com where admins can customize the web filtering categories to address any false positives may occur. The policies can be deployed to block any following parent or child categories. Policies can be deployed to block any of the following parent or child categories: Adult content, High bandwidth, Legal liability, Leisure, Uncategorized.

Source	https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide#configure-web-content-filtering-policies

Mozilla Blocks malicious add-ons installed by 455k Firefox users

Description

The Mozilla Firefox team has blocked add-ons that were misusing the proxy API, preventing around 455,000 users from upgrading their browsers. The add-ons were using the proxy API, which is used by APIs to control how Firefox connects to the internet. The add-ons named Bypass and Bypass XM were intercepting and redirecting web requests in order to prevent users from downloading updates, updating remotely specified content, and accessing updated blocklists.

Source	https://blog.mozilla.org/security/2021/10/25/securing-the-proxy-api-for-firefox-add-ons/
Infected Technology	Mozilla Firefox
Recommendation	Update the latest version of Firefox

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**

OUR SERVICES

Our services as information security company includes:

- INFORMATION SECURITY AUDIT
- VULNERABILITY ASSESSMENT
- PENETRATION TESTING
- MANAGED/CO.MANAGED SOC
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER HARDENING
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/