June 1, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- New Android Flaw Affecting over 1 billion Phones
- Valak malware steals credentials from MS-Exchange Servers
- Cisco hacked by exploiting vulnerable SaltStack Servers
- NSA claims an Exim flaw is being exploited by Russian govt hackers since 2019
- Hacker leak database of dark web hosting providers
- Octopus Scanner Malware
- ComRAT Malware uses Gmail for CnC Communication
- German govt urges iOS users to patch critical Mail app flaw

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, Trip Advisor, 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. New Android Flaw Affecting over 1 billion Phones

Description	
A security vulnerability affecting Android that malicious apps can exploit to disguise as any other app installed on a targeted device to display fake interfaces to the users, tricking them into giving away sensitive information. Researchers also confirmed that some attackers were already exploiting the flaw in the wild to steal users' banking and other login credentials, as well as to spy on their activities.	
Source	https://thehackernews.com/2020/05/stranhogg-android-vulnerability.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2238.qx0a00e50w.1ek8
Infected Technology	Android Phones
Recommendation	Update the latest patch available

2. ComRAT Malware uses Gmail for CnC Communication

Description	
Security researchers disclose a new version of ComRAT malware used by Turla APT, a threat actor that is known for its watering hole and spear-phishing campaigns against governments and diplomatic entities in Europe, Central Asia and the Middle East. The main use of ComRAT is stealing confidential documents. In one case, its operators even deployed a .NET executable to interact with the victim's central MS SQL Server database containing the organization's documents. The ComRAT v4 malware uses two different channels to communicate with its C&C server: one mechanism involves the HTTP protocol and the other uses the Gmail web interface.	
Source	https://thehackernews.com/2020/05/gmail-malware-hacker.html
Infected Technology	Gmail

3. Octopus Scanner Malware

Description

A new malware dubbed Octopus Scanner by security researchers at GitHub Security Lab finds and backdoors open source NetBeans projects hosted on the GitHub web-based code hosting platform to spread to different systems and deploy a Remote Administration Tool (RAT). The malware infects NetBeans repositories after planting malicious payloads within JAR binaries, project files and dependencies, later spreading to downstream development systems. The information-stealing malware will backdoor all the NetBeans projects builds it can find by injecting a dropper in any built JAR files. This dropper will subsequently allow the malware to gain local system persistence and would subsequently spawn a Remote Administration Tool (RAT). The attackers targeted developers' highly sensitive information such as additional projects, production environments, database passwords and other critical data. They can gain access to the developers' organization's critical systems after they commit backdoored code into the organization's repositories.

Source	https://www.bleepingcomputer.com/news/security/new-octopus-scanner-malware-spreads-via-github-supply-chain-attack/
Infected Technology	NetBeans projects on GitHub
Recommendation	Do not clone NetBeans projects from GitHub especially to devices having access to organizations’ critical systems.

4. Valak malware steals credentials from MS-Exchange Servers

Description

A previously known malware that helped to deliver other trojans has been also identified to steal email login credentials and certificates from enterprise. Valak hides it payloads, C2 details in the registry and later reaches for the tools it needs for various task. The initial phase of this malware is known to be delivered with email attachment of a Microsoft Word document that have malicious macro code inside.

Source	https://www.bleepingcomputer.com/news/security/valak-malware-steals-credentials-from-microsoft-exchange-servers/
Infected Technology	Microsoft Exchange Servers
Recommendation	Verify email source and attachment before opening

5. Cisco hacker by exploiting vulnerable SaltStack servers

Description	
According to Cisco, its VIRL-PE a network modeling and simulation environment's backend servers were hacked by exploiting SaltStack vulnerability. Attacker are found leveraging the StalkStack Vulnerabilities to execute unauthenticated attacks with full read and write access to the salt-master server as root.	
Source	https://www.bleepingcomputer.com/news/security/cisco-hacked-by-exploiting-vulnerable-saltstack-servers/
Infected Technology	CISCO VIRL-PE
Recommendation	Update your SaltStack servers to the latest version

6. NSA claims an Exim flaw is being exploited by Russian govt hackers since 2019

Description	
NSA, the National Security Agency of U.S. claims that a critical flaw in the Exim mail transfer agent is being exploited by Sandword Team (Russia Sponsored Hacking group) since 2019. The exploit dubbed "The Return of the WIZard" is known to perform unauthenticated remote attack as root on vulnerable mail server by sending specially crafted email.	
Source	https://www.bleepingcomputer.com/news/security/nsa-russian-govt-hackers-exploiting-critical-exim-flaw-since-2019/
Infected Technology	Unpatched Exim mail transfer agent
CVE	CVE-2019-10149
Recommendation	Patch your Exim mail agent to latest

7. German govt urges iOS users to patch critical Mail app flaw

Description	
Germany's federal cybersecurity agency today urged iOS users to immediately install the iOS and iPadOS security updates released by Apple on May 20 to patch two actively exploited zero-click security vulnerabilities impacting the default email app. The two no-click vulnerabilities are a memory consumption issue that may lead to heap corruption and an out-of-bounds write issue which may lead to unexpected memory modification or application termination, both of them triggered after the Mail app processes a maliciously crafted mail message.	
Source	https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Warnung_iOS-Mail_230420.html
Infected Technology	IOS mail app
Recommendation	Update your iOS devices to 13.5

8. Hacker leak database of dark web hosting providers

Description	
A hacker, KingNull, has recently leaked database of Daniel's Hosting (DH), one of the largest free web hosting providers for dark web services. The leaked data was obtained on March 10, 2020 when the hacker breached the portal, gained sensitive information and wiped the server. The wiped server was removed from the service and migrated to new server since then. The leaked data contains 3671 email addresses, 7,205 hashed passwords, and 8,580 private keys for .onion (dark web) domains that can be tied up to dark web service providers.	
Source	https://www.zdnet.com/article/hacker-leaks-database-of-dark-web-hosting-provider/
Infected Technology	Daniel Hosting
Recommendation	Change the credentials if found on the dump

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