May 4, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- LineageOS attacked due to use of unpatched Salt framework
- Data breach in Tokopedia, Indonesia's largest online store
- Critical SaltStack RCE Bug Affects Thousands of Data
- New Android Malware Steals Banking Passwords, Private Data and Keystrokes
- Microsoft Teams Impersonation Attacks Flood Inboxes
- TrickBot Attack Exploits COVID-19 Fears with DocuSign-Themed Ploy
- Targeted Phishing Attacks Successfully Hacked Top Executive at 150+ Companies
- Xiaomi tracks private browser and phone usage, defends behavior
- RDP brute-force attacks are skyrocketing due to remote working

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. LineageOS attacked through Unpatched Salt framework

Description	
LineageOS, a mobile operating system was targeted by hackers. An intrusion was detected on their infrastructure, which is said to have been discovered before the attackers could do any harm. LineageOS developers have stated that the attack occurred because of an unpatched vulnerability in recently disclosed Salt framework vulnerabilities. The responsible vulnerabilities: CVE-2020-1161(an authentication bypass) and CVE-2020-11652(a directory traversal) could allow attackers to login procedures and run code on Salt master servers left exposed on the internet. Salt is an open-source software for event-driven IT automation, remote task execution and configuration management. LineageOS is a mobile operating system based on Android, used for smartphones, tablets and set-top boxes.	
Source	https://www.zdnet.com/article/hackers-breach-lineageos-servers-via-unpatched-vulnerability/
Infected Technology	LineageOS

2. Data breach in Tokopedia, Indonesia's largest online store

Description	
Details of about 15 million registered Tokopedia users have been released by the attacker. The hacker claims the data was obtained in an attack that took place earlier this year. The leaked file was a PostgreSQL database dump, containing user information such as full names, emails, phone numbers, hashed passwords, and Tokopedia profile related details. The hashed passwords are secure for the time being, but the users have been advised to reset their account passwords. Tokopedia is Indonesia's largest online store with over 90 million monthly active users and more than 7 million registered merchants.	
Source	https://www.zdnet.com/article/hacker-leaks-15-million-records-from-tokopedia-indonesias-largest-online-store/
Infected Technology	Tokopedia
Recommendation	Change the credentials

3. Critical SaltStack RCE Bug Affects Thousands of Dat

Description

Two severe security flaws have been discovered in the open-source SaltStack Sat configuration framework that could allow an adversary to execute arbitrary code on remote servers deployed in data centers and cloud environments.

Source	https://thehackernews.com/2020/05/saltstack-rce-vulnerability.html
Infected Technology	SaltStack Configuration Framework
CVE-ID	CVE-2020-11651, CVE-2020-11652
Recommendation	Follow best practices to secure the salt environment

4. New Android Malware Steals Banking Passwords, Private Data and Keystrokes

Description

A new type of mobile banking malware has been discovered abusing Android's accessibility features to exfiltrate sensitive data from financial applications, read user SMS messages, and hijack SMS-based two-factor authentication codes. The malware is dubbed "EventBot" and can target over 200 different financial apps, including banking, money transfer services and crypto-currency wallets also.

Source	https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born
Infected Technology	Banking application
Recommendation	Always use official apps from the store

5. Microsoft Teams Impersonation Attack Flood Inboxes

Description

The attacker crafted convincing emails that impersonate notifications from Microsoft Teams to steal O365 credentials. Two separated attack has been targeted as many as 50,000 team users where attack utilizes numerous URL redirection in order to conceal real URL to host attack I.e where users are taken to malicious page which impersonate Microsoft office login page. Second One, the email link points to a YouTube page, from which users are redirected twice to finally land on another Microsoft login phishing site. Since Microsoft Teams is linked to Microsoft Office 365, the attacker may have access to other information available with the user's Microsoft credentials via single sign on

Source	https://threatpost.com/microsoft-teams-impersonation-attacks/155404/
Recommendation	Always be cautious when giving off sensitive personal or account information

6. TrickBot Attack Exploits COVID-19 Fears with DocuSign-Themed Ploy

Description

TrickBot is a well-known and sophisticated banking Trojan first developed in 2016 as a banking malware that has a history of transforming itself and adding new features to evade detection. It is developed over the years into a full-fledged, module-based crimeware solution typically aimed at attacking corporations, though the latest campaign seems to deviate from that target audience. The malware seems to be distributed by the same parties who were involved with the previous TrickBot such as "Marco on Close" function for DocuSign Theme.

Source	https://threatpost.com/news-wrap-microsoft-sway-phish-malicious-gif-and-spyware-attacks/155401/
Infected Technology	DocuSign
Recommendation	Take precautionary steps for any phishing emails. Do not open attachments that you are not expecting.

7. RDP brute-force attacks are skyrocketing due to remote working

Description

Attackers are increasingly targeting corporate resources used by employees who have now moved to work from home due to lockdown and shelter in place orders issued during the ongoing pandemic. A highly popular solution to access enterprise devices remotely is the Remote Desktop Protocol (RDP) which enables remote workers to access their work from the comfort of their home. There has been a growth in the number of brute-force attacks launched by threat actors against RDP services. Attacks of this type are attempts to brute-force a username and password for RDP by systematically trying all possible options until the correct one is found. The search can be based on combinations of random characters or a dictionary of popular or compromised passwords.

Source	https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/
Infected Technology	Exposed RDP
Recommendation	Monitor

8. Xiaomi tracks private browser and phone usage, defends behavior

Description

Xiaomi found tracking sensitive information like internet searches including incognito mode sessions and sending them to its servers in Singapore and Russia. The data forwarded is not anonymous and can be associated with users which is more concerning as any targeted user's activity can be easily traced. The session is only forwarded from the Mi Browsers which comes bundled in any Xiaomi devices. Additionally, the manufacturer also tracks the music player activities, folders accessed, screen viewed by user along with configured settings. These data are also recorded by other browsers by Mi, i.e. Mi Browser Pro and Mint Browser.

Source	https://www.bleepingcomputer.com/news/technology/xiaomi-tracks-private-browser-and-phone-usage-defends-behavior/
Infected Medium	Xiaomi Phones
Recommendation	Use alternate application for browsing and file access.

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