January 3, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Critical Security Flaws with Apache HTTP Server led to Remote Code Execution
- New Android Malware Targeting Brazil's Itaú Unibanco Bank Customers
- Ongoing Autom Cryptomining Malware Attacks Using Upgraded Evasion Tactics
- New version of Log4J released with patch for RCE
- CISA, FBI and NSA Publish Joint Advisory and Scanner for Log4j Vulnerabilities

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.

Critical Security Flaws with Apache HTTP Server led to Remote Code Execution

Description	
Apache Software Foundation has released an urgent update to resolve critical vulnerabilities in its Apache HTTP Server (version 2.4.51 and earlier). The vulnerability is considered as critical and can be exploited by the threat actors to take control of a vulnerable system. The U.S. government's security agency (CISA) has also requested open-source community users around the world to immediately update their old vulnerable version with the latest one.	
Source	Security Flaws with Apache HTTP Server Let Hackers Execute Arbitrary Code (gbhackers.com)
Infected Technology	Apache HTTP Server 2.4.51 and earlier
Recommendation	Update to the newly released Apache HTTP Server 2.4.52 version.
CVE_ID	• CVE-2021-44790 • CVE-2021-44224

New Android Malware Targeting Brazil's Itaú Unibanco Bank Customers

Description	
Researchers have uncovered a new Android banking malware that uses spoof Google Play Store pages to carry out fraudulent financial transactions on victims' devices without their awareness. The malware has targeted Brazil's Itau Unibanco banking application. According to the researchers, the trojan's purpose is to leverage the accessibility API to make fraudulent financial transactions on the legal Ita Unibanco application by manipulating with the user's input fields, adding a long list of banking malware that uses the API. Google, for one, has begun to impose additional restrictions on the use of permissions that allow apps to collect sensitive data from Android devices.	
Source	New Android Malware Targeting Brazil's Itaú Unibanco Bank Customers (thehackernews.com)
Infected Technology	Brazil's Itau Unibanco Banking Application
Recommendation	Users should install applications only after verifying their authenticity and install them exclusively from the official Google Play Store and other trusted portals to avoid such attacks.

Ongoing Autom Cryptomining Malware Attacks Using Upgraded Evasion Tactics

Description	
According to new research, a continuing crypto mining campaign has updated its arsenal while expanding its defence evasion strategies, allowing threat actors to mask incursions and remain undetected. According to researchers from DevSecOps and cloud security firm Aqua Security, who have been tracking the malware operation for the past three years, 84 attacks against its honeypot servers have been reported to date, four of which occurred in 2021. However, 125 incidents were discovered in the wild in the third quarter of 2021 alone, indicating that the attacks are not abating. "The Autom campaign illustrates that attackers are becoming more sophisticated, continually improving their techniques and their ability to avoid detection by security solutions," the researchers said. To protect against these threats, it's recommended to monitor suspicious container activity, perform dynamic image analysis, and routinely scan the environments for misconfiguration issues.	
Source	Ongoing Autom Cryptomining Malware Attacks Using Upgraded Evasion Tactics (thehackernews.com)
Infected Technology	Misconfigured Docker Container Servers
Recommendation	It is recommended to monitor suspicious container activity, perform dynamic image analysis, and routinely scan the environments for misconfiguration issues.

New version of Log4J released with patch for RCE

Description	
Apache has released new version of Log4J, 2.17.1 which patches the newly discovered remote code execution vulnerability in 2.17.0. CVE-2021-44832 is the fifth CVE in Log4j in a month. The vulnerability has a CVSS score of 6.6. The researchers have disclosed the vulnerability with technical details, steps to reproduction and recommendations.	
Source	https://checkmarx.com/blog/cve-2021-44832-apache-log4j-2-17-0-arbitrary-code-execution-via-jdbcappender-datasource-element/
Infected Technology	Log4j 2.17.0
Recommendation	Update to version 2.17.1

CISA, FBI and NSA Publish Joint Advisory and Scanner for Log4j Vulnerabilities

Description	
In response to widespread exploitation of various vulnerabilities in Apache's Log4j software library by malevolent adversaries, cybersecurity authorities from Australia, Canada, New Zealand, the United Kingdom, and the United States announced a combined advisory on Wednesday. In response to widespread exploitation of various vulnerabilities in Apache's Log4j software library by malevolent adversaries, cybersecurity authorities from Australia, Canada, New Zealand, the United Kingdom, and the United States announced a combined advisory on Wednesday. The latest step taken by the governments arrives as the Apache Software Foundation (ASF) on Monday released updates for Apache HTTP Server to address two flaws — CVE-2021-44790 (CVSS score: 9.8) and CVE-2021-44224 (CVSS score: 8.2) — the former of which could be weaponized by a remote attacker to execute arbitrary code and take control of an affected system.	
Source	New Android Malware Targeting Brazil's Itaú Unibanco Bank Customers (thehackernews.com)
Infected Technology	Brazil’s Itau Unibanco Banking Application
Recommendation	Users should install applications only after verifying their authenticity and install them exclusively from the official Google Play Store and other trusted portals to avoid such attacks.

Microsoft Issues Fix for Exchange Y2K22 Bug That Crippled Email Delivery Service

Description	
Microsoft released a repair over the weekend to resolve an issue that caused email messages to become trapped on its Exchange Server platforms around the turn of the year, which it blamed on a date validation problem. As the year 2022 approached, the problem became more visible, leading the servers to stop delivering email messages and to display the following error message: "The 'Microsoft' Scan Engine in FIP-FS failed to load. 23092 PID, 0x80004005 Error Code Error Description: '2201010001' cannot be converted to long". To address the Y2K22 issue, Microsoft recommends that clients download "Reset-ScanEngineVersion.ps1," a PowerShell-based scan engine reset script that may be run on each Exchange mailbox server that downloads antimalware upgrades.	
Source	https://techcommunity.microsoft.com/t5/exchange-team-blog/email-stuck-in-exchange-on-premises-transport-queues/ba-p/3049447
Infected Technology	Microsoft Exchange Server
Recommendation	Customers are advised to download "Reset-ScanEngineVersion.ps1," a PowerShell-based scan engine reset script that may be run on each Exchange mailbox server used for obtaining antimalware upgrades. It's worth noting that the upgrade also brings the engine's version number up to 2112330001

New iLOBleed Rootkit Targeting HP Enterprise Servers with Data Wiping Attacks

Description

A previously undiscovered rootkit has been discovered targeting Hewlett-Packard Enterprise's Integrated Lights-Out (iLO) server management technology in order to conduct in-the-wild assaults that tamper with firmware modules and delete data from compromised computers. This week, Iranian cybersecurity firm Amnpardaz reported on the discovery, which is the first instance of real-world malware in iLO firmware. The rootkit, dubbed iLOBleed, has been used in attacks since 2020, with the purpose of modifying several original firmware modules to silently obstruct firmware updates. The changes to the firmware routine imitate the firmware upgrade process by ostensibly showing the correct firmware version and adding necessary logs when no upgrades are really executed

Source	https://threats.amnpardaz.com/en/2021/12/28/implant-arm-ilobleed-a/
Infected Technology	HP Enterprise Server
Recommendation	Another essential point to note is that there are techniques to access and infect iLO both through the network and the host operating system," the researchers said. "This means that even if the iLO network cable is disconnected fully, the malware can still infect the computer. Surprisingly, there is no option to entirely turn off or disable iLO if it is no longer required."

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/