TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: NOVEMBER 19, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As cybersecurity threats grow more complex, they pose serious risks to individuals, businesses, and government entities, potentially causing disruptions, financial losses, and reputational harm. Strengthening digital defences is essential to protect data integrity, confidentiality, and availability.

Our weekly Cyber Threat Intelligence (CTI) report provides timely insights on global threats, empowering you to stay ahead of emerging risks. Combined with our advisory services, this resource supports a robust security strategy, helping you safeguard IT assets and enhance your overall security posture.

Indian entities attacked by Pakistan-based APT36

Pakistan-based APT36 has conducted a decade-long cyberespionage campaign against Indian government, military, and diplomatic entities, now leveraging an enhanced version of its “ElizaRAT” malware. The latest ElizaRAT includes advanced evasion tactics, improved command-and-control (C2) capabilities, and a new dropper, making detection more challenging. APT36 also introduced “ApoloStealer” to gather specific file types, transferring them to C2 servers for analysis.

APT36, also known as Transparent Tribe, employs legitimate software, living-off-the-land binaries (LoLBins), and popular communication platforms like Telegram and Google Drive to mask its activities. The group has targeted not only Indian assets, but also organisations in Europe, Australia, and the US, focusing on intelligence gathering. Recent campaigns include attacks on Maya OS with ELF binaries and Android-based attacks using romantic lures to spread “CopraRAT” malware, further underscoring the sophistication and adaptability of APT36’s tactics.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	India	**APPLICATION**	Android, Windows, Linux

Source - https://www.darkreading.com/cyberattacks-data-breaches/apt36-refines-tools-attacks-indian-targets

Google releases urgent updates to fix critical vulnerabilities

Google has issued a Chrome update to address two high-severity vulnerabilities – CVE-2024-10826 and CVE-2024-10827 – impacting Windows, Mac, and Linux users. Both vulnerabilities involve “use-after-free” flaws that could allow attackers to execute arbitrary code or crash the browser. CVE-2024-10826 affects the “Family Experiences” component, while CVE-2024-10827 impacts “Serial.” Users are advised to upgrade to version 130.0.6723.116/.117 to mitigate these risks.

The Stable channel has been updated to version 130.0.6723.116/.117 for Windows, Mac, and Linux, and the Extended Stable channel to 130.0.6723.117 for Windows and Mac, rolling out over a few days. Google restricts access to bug details until most users are protected, and it may maintain restrictions if the vulnerability is in a third-party library and is still unpatched.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Google Chrome

Source - https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop.html

Apple iOS' symlink vulnerability exploited

CVE-2024-44258 is a symlink vulnerability in Apple's ManagedConfiguration framework and profiled daemon, allowing attackers to manipulate backup restoration by bypassing destination folder checks for symlinks. This flaw enables unauthorised file migration to protected directories, potentially leading to privilege escalation and unauthorised data access.

Actively exploited for months, Apple addressed the vulnerability by improving symlink handling in iOS 18.1 beta 5. The issue is now fixed in iOS 18.1, iPadOS 18.1, iOS 17.7.1, iPadOS 17.7.1, visionOS 2.1, and tvOS 18.1, preventing malicious backup files from modifying protected system files.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	iOS

Source - https://www.tenable.com/cve/CVE-2024-44258

Stealc malware compromises user information

Researchers have unearthed Stealc, a sophisticated infostealer targeting credentials from browsers, cryptocurrency wallets, and fileshare servers. It tracks user activity, including keystrokes and mouse clicks, disables security applications, and alters network settings to enable proxy connections. Stealc thoroughly scans system hardware and Windows settings, gathering details down to monitor resolution.

The malware file appears as a standard executable, though its code is partially obfuscated and packed within the ".text" section. Upon execution, Stealc employs evasion techniques such as debugger detection, locale checks, and extended sleep, alongside VirtualProtect guard pages for runtime protection. It queries the system for hardware, software, user accounts, network settings, and registry keys. Specifically targeted items include browsers (Chrome, Firefox), wallets (Monero), SaaS accounts (Azure, AWS), and various applications (Word, FileZilla, Telegram). During execution, it writes and later deletes test registry keys to validate its operation.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - https://blog.sonicwall.com/en-us/2024/11/stealc-malware-checks-everything-even-the-screen-resolution/

Phishing campaign manipulates search engine

Researchers have uncovered a new phishing campaign targeting Keybank customers via Microsoft's Bing search engine. A search for "Keybank login" returns malicious links, with one fraudulent site appearing as the top result. Despite Bing's small market share, this campaign shows how criminals exploit its algorithms to bypass security measures. The phishing site, registered just weeks ago, misleads users with a redirect to a fake Keybank login page after showing a legitimate-looking site designed to evade detection by crawlers.

This attack highlights the importance of using advanced security practices, as the attackers bypassed two-factor authentication (2FA) and exploited Bing's indexing system. We recommend adopting phishing-resistant login methods like passkeys, which eliminate passwords altogether, and upgrading to more secure authentication methods like an authenticator app instead of SMS verification. It's crucial to remain vigilant, as cybercriminals may also attempt to trick users into providing one-time codes.

ATTACK TYPE	Phishing	**SECTOR**	BFSI
REGION	Global	**APPLICATION**	Generic

Source - https://www.malwarebytes.com/blog/scams/2024/11/crooks-bank-on-microsofts-search-engine-to-phish-customers

Various vulnerabilities found in Apache ZooKeeper

The Apache Software Foundation (ASF) has addressed several security vulnerabilities in its Apache ZooKeeper project, highlighting concerns over both authentication and information disclosure risks. The CVE-2024-51504 vulnerability is a flaw in the ZooKeeper Admin Server's IP-based authentication, allowing attackers to bypass authentication by spoofing client IP addresses. This could lead to unauthorised execution of admin commands, impacting security. A fix is available in ZooKeeper versions 3.9.3 and later.

CVE-2024-23944 is a critical information disclosure vulnerability in persistent watcher handling. It exposes znode paths without an ACL check, potentially leaking sensitive information. This affects ZooKeeper versions 3.9.1 through 3.7.2, with fixes in versions 3.9.2 and 3.8.4. CVE-2023-44981 is a SASL Quorum Peer authentication bypass vulnerability that could allow unauthorised endpoints to join clusters and propagate counterfeit changes. Users are urged to upgrade to 3.9.1 or later to mitigate the issue. ASF urges users to report undisclosed vulnerabilities and to follow best security practices by upgrading to the latest patched versions.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Apache ZooKeeper

Source - https://zookeeper.apache.org/security.html

Interlock ransomware executes double extortion attacks

Researchers recently tracked a sophisticated attack using the new Interlock ransomware, which employed multiple stages of compromise. The attacker used a remote access trojan (RAT) disguised as a browser updater, PowerShell scripts, credential stealers, and keyloggers before deploying the ransomware encryptor. Lateral movement within the network was primarily via Remote Desktop Protocol (RDP), with additional tools like AnyDesk and PuTTY. Data exfiltration occurred using Azure Storage Explorer, leveraging AzCopy to move data to an attacker-controlled Azure storage blob. The attack's timeline showed that the attacker remained in the victim's environment for about 17 days before executing the ransomware.

Interlock, identified in September 2024, is linked to big-game hunting and double extortion tactics. The ransomware targets various sectors, including healthcare, technology, and government, and operates a data leak site. Interlock's binary encrypts files with the ".Interlock" extension and drops a ransom note. Both Windows and Linux variants of the ransomware are in use.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows, Linux

Source - https://blog.talosintelligence.com/emerging-interlock-ransomware/

Phishing campaign employs copyright infringement tactics

Researchers have been tracking a large-scale, sophisticated phishing campaign, dubbed CopyRh(ight)adamantys, which has been ongoing since July 2024. The campaign targets regions such as the US, Europe, East Asia, and South America, using a copyright infringement theme. Impersonating various companies, mostly from the entertainment, media, and tech sectors, the campaign sends tailored phishing emails from different Gmail accounts, adapting the company and language for each target. It appears automated, with a potential use of AI tools to distribute lures.

The emails prompt recipients to download an archive containing a DLL side-loading exploit, which installs the latest version of the Rhadamanthys stealer (v0.7). This new version includes an optical character recognition (OCR) component, which, contrary to claims, uses older machine learning techniques. The campaign's widespread targeting and automated tactics suggest it is led by a financially motivated cybercriminal group rather than state-sponsored actors.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - https://research.checkpoint.com/2024/massive-phishing-campaign-deploys-latest-rhadamanthys-version/

PAN-OS vulnerable to RCE risks

Palo Alto Networks has issued an advisory about a potential remote code execution (RCE) vulnerability in the PAN-OS management interface, though the specifics remain unclear. While no active exploitation has been detected, the company urges customers to restrict access to the management interface, allowing only trusted internal IPs.

The vulnerability appears limited to on-premises PAN-OS deployments, with no impact on Prisma Access or cloud NGFW. Palo Alto emphasises following best practices by ensuring the management interface is not exposed to the internet.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	PAN-OS

Source - https://security.paloaltonetworks.com/PAN-SA-2024-0015

Critical vulnerability exposed in WordPress LMS theme

A critical vulnerability – CVE-2024-10470 (CVSS 9.8) – has been discovered in the WPLMS WordPress theme, used for online course management. This flaw allows unauthenticated attackers to read and delete sensitive files, including wp-config.php, due to insufficient sanitisation of the “zip_file” parameter. Exploiting this vulnerability could lead to full site takeovers, forcing sites into setup mode. The issue affects all versions up to 4.962, regardless of whether the theme is actively enabled.

Although there is no evidence of active exploitation, attackers could use this vulnerability to compromise servers, delete critical files, and gain remote control. Wordfence recommends updating to version 4.963 to mitigate the risk and protect sites from potential disruptions or breaches.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	WordPress

Source - https://cyble.com/blog/path-traversal-vulnerability-in-wplms-wordpress-theme-exposes-websites-to-rce/

TATA COMMUNICATIONS

TATA

Visit one of our **Cyber Security Response Centres** to learn how we can help your enterprise navigate the complexities of today's cyber threat landscape.

Book your visit