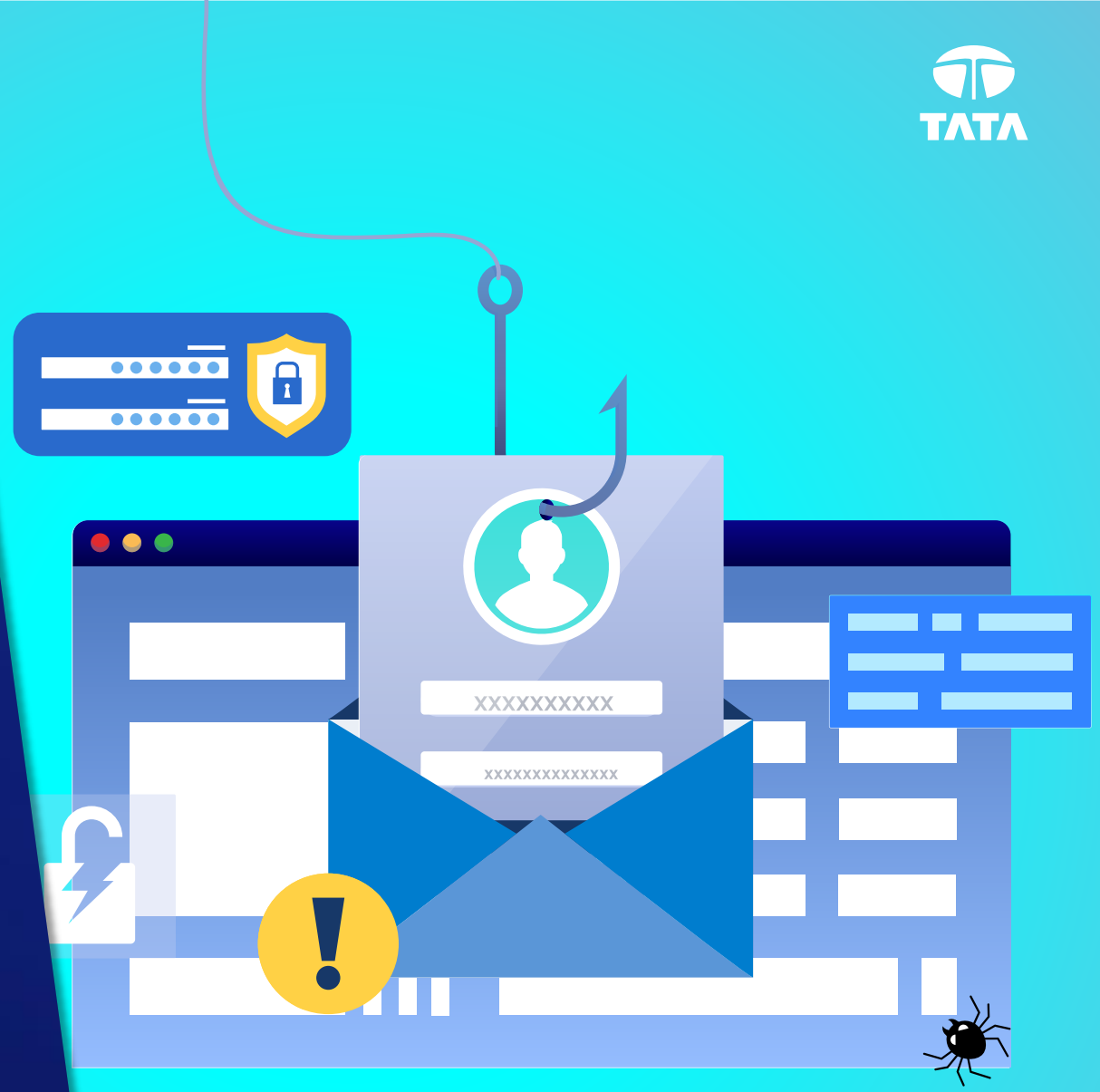
TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: DECEMBER 10, 2024



TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In an era of escalating cybersecurity threats, safeguarding critical systems and data is vital for individuals, businesses, and governments. Disruptions can lead to financial losses, reputational harm, and compromised operational security.

Our weekly Cyber Threat Intelligence (CTI) report delivers actionable insights on emerging global threats to bolster your defences. Supported by expert advisory services, we provide strategies to protect IT assets against persistent risks. Stay ahead of evolving cyber challenges with our intelligence-driven approach, empowering your organisation to strengthen its security posture and ensure a resilient, secure future.

TATA COMMUNICATIONS

Perfctl malware poses threat to Linux servers worldwide

Perfctl, a sophisticated malware campaign targeting Linux servers, poses a critical threat to organisations relying on these systems. Using advanced fileless techniques, Perfctl evades detection by masking itself within legitimate processes, enabling silent cryptocurrency mining and proxyjacking operations that drain server resources and degrade performance. This campaign primarily targets cryptocurrency platforms, NFT infrastructures, and software development sectors in regions such as the US, Germany, and South Korea – areas with high Linux server adoption. Perfctl's propagation is facilitated through developer forums and repositories, making open-source platforms particularly vulnerable.

Unlike traditional malware, Perfctl avoids conventional antivirus tools by mimicking regular system files and leveraging Linux's inherent openness. Its impact highlights the urgent need for robust, behaviour-based detection and enhanced cybersecurity measures. Security teams must prioritise proactive defences, including monitoring unusual resource usage, isolating compromised systems, and implementing threat-hunting strategies to combat this evolving menace to Linux-based infrastructures.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Germany, South Korea, US	**APPLICATION**	Linux

Source - https://socradar.io/perfctl-campaign-exploits-millions-of-linux-servers-for-crypto-mining-and-proxyjacking/

Matrix's DDoS campaign targets IoT and enterprise systems

Researchers have uncovered a global distributed denial-of-service (DDoS) campaign orchestrated by a threat actor named Matrix. Exploiting IoT and enterprise systems, Matrix leverages misconfigurations, weak credentials, and public scripts to create a botnet capable of widespread disruption. The operation has targeted nearly 35 million internet-connected devices globally, with attackers employing compromised servers and tools like Shodan to expand their reach.

Matrix’s campaign demonstrates how accessible hacking tools and minimal expertise can enable large-scale attacks. While the threat actor shows signs of Russian affiliation, the absence of Ukrainian targets suggests financial, not political, motives. Unique to this operation is its shift from cryptomining to targeting both development and production servers, signalling a broader focus on corporate vulnerabilities. As Matrix’s botnet disrupts online businesses and backend operations, organisations must strengthen their defences to mitigate the escalating risks posed by such accessible yet potent threats.

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

Source - https://www.aquasec.com/blog/matrix-unleashes-a-new-widespread-ddos-campaign/

Persistent access tactics employed by hackers to target RD-Web

Researchers recently analysed a unique cyber intrusion where attackers established persistent remote access within a victim's network. This case highlights the increasing sophistication of modern threat actors, who combined deceptive social engineering with advanced post-exploitation tactics. The attackers gained initial access by exploiting a vulnerable Microsoft Exchange server, deploying an open-source reverse proxy tool for covert communication. Uniquely, they used scheduled tasks and legitimate system utilities for persistence, avoiding detection by antivirus solutions. Analysts noted their operational patience, with attackers lying dormant for weeks before launching data exfiltration and lateral movement activities.

The campaign also showcased a shift in targeting strategies, with small- and medium-sized businesses increasingly at risk. Researchers have emphasised the importance of proactive threat hunting, endpoint monitoring, and robust patch management to mitigate such risks. This case serves as a stark reminder of evolving cyber threats and the critical need for vigilance across all organisational layers.

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

Source - https://www.huntress.com/blog/know-thy-enemy-a-novel-november-case-on-persistent-remote-access

Vidar build IDs tied to Lumma Stealer payload surge

Researchers have identified a significant correlation between Vidar stealer's build IDs and the distribution of Lumma Stealer payloads. Vidar, a notorious information-stealing malware, assigns a unique 32-byte hexadecimal build_id to each variant, linking it to specific threat actors. This identifier facilitates tracking and management within the malware's command and control (C2) infrastructure. In early October 2024, a surge in activity involving multiple Vidar build IDs was observed. Analysis revealed that 28 out of 31 build IDs were associated with the dissemination of two primary tasks, each leading to numerous unique payloads identified as Lumma Stealer.

These tasks resulted in a combined total of 131 unique Lumma Stealer payloads. The high volume of payloads suggests that the threat actors employed automation to frequently update the payloads, likely aiming to evade detection mechanisms. Notably, the same tasks were also distributed by StealC with botnet identifiers default and us_test, indicating potential overlaps or collaborations among different threat actors.

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

Source - https://insights.loaderinsight.agency/posts/vidar-build-id-correlation/

Earth Kasha resurfaces with spear-phishing campaign targeting Japan

Researchers have brought to light a spear-phishing campaign attributed to Earth Kasha, ongoing since June 2024. The campaign revives the ANEL backdoor, previously used by APT10, alongside the NOOPDOOR backdoor. Targeting individuals linked to political organisations, research institutions, and international relations in Japan, attackers use phishing emails with ZIP file attachments hosted on OneDrive. The campaign demonstrates Earth Kasha's shift from targeting enterprises to individuals, particularly those with ties to Japan's national security.

The ANEL backdoor is used for persistent access, deploying advanced payloads that steal sensitive data. Meanwhile, NOOPDOOR, a modular backdoor, was deployed on high-value targets. This attack highlights the sophistication of Earth Kasha's evolving tactics and the continued risk to individuals with varying security postures. Experts emphasise the importance of caution with email attachments and proactive threat intelligence to defend against this growing threat.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Japan	**APPLICATION**	Windows

Source - https://www.trendmicro.com/en_us/research/24/k/return-of-anel-in-the-recent-earth-kasha-spearphishing-campaign.html

TATA COMMUNICATIONS

Elpaco ransomware variant exploits Windows search library

Cybersecurity experts have identified Elpaco, a variant of the Mimic ransomware, which uniquely leverages the legitimate Windows search library, Everything, to locate files for encryption. This approach enhances its stealth and efficiency. Elpaco employs a 7-Zip installer mechanism, often misclassified as benign, to evade detection. Upon execution, it drops a session key file, session.tmp, to resume encryption if interrupted.

The malware uses the SetSearchW function from the Everything DLL to search for files, encrypting them with the ChaCha20 stream cipher. Notably, Elpaco mimics the legitimate svchost.exe process by using the name svhostss.exe, further obfuscating its presence.

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

Source - https://securelist.com/elpaco-ransomware-a-mimic-variant/114635/

TATA COMMUNICATIONS

APT-C-60 targets Japanese organisation with SpyGlace backdoor

APT-C-60, a South Korea-aligned cyberespionage group, launched a sophisticated attack on a Japanese organisation in August 2024. Utilising a job application-themed phishing email, the group delivered the SpyGlace backdoor via legitimate services like Google Drive, Bitbucket, and StatCounter. The attack exploited a remote code execution (RCE) vulnerability (CVE-2024-7262) in WPS Office, triggering a chain of infections. The phishing email contained a link to a VHDX file hosted on Google Drive, which, once opened, initiated the malware download through a Windows shortcut.

The malware employed unique methods, including COM hijacking and using Bitbucket to fetch subsequent payloads. The SpyGlace backdoor established contact with a remote C2 server, enabling file theft and further cyberespionage actions. This attack demonstrates a growing trend of advanced, non-standard malware delivery techniques by Asian threat groups, highlighting the evolving tactics in the region's cyber threats.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Japan	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/11/apt-c-60-exploits-wps-office.html

GodLoader malware campaign exploits Godot Engine

A new malware campaign, dubbed GodLoader, has exploited the popular open-source Godot Engine, infecting over 17,000 systems since June 2024. Cybercriminals leverage Godot's GDScript code to execute malicious commands, evading detection by most antivirus engines. The attack uses the Stargazers Ghost Network – comprising fake GitHub repositories and accounts – to distribute GodLoader, which then downloads payloads like RedLine Stealer and XMRig miner. These attacks primarily target Windows systems but can be adapted for macOS and Linux.

The malware is spread via custom Godot executables, relying on .PCK files to load the malware. Security experts highlight that the campaign's cross-platform nature and stealth techniques have made it particularly effective. The Godot security team has urged users to download software from trusted sources and avoid cracked versions to mitigate such risks. This incident underscores the growing threat of cybercriminals exploiting legitimate platforms for large-scale malware campaigns.

ATTACK TYPE	Malware	**SECTOR**	Automobile, manufacturing
REGION	Global	**APPLICATION**	macOS, iOS, Android, Windows, Linux

Source - https://thehackernews.com/2024/11/cybercriminals-exploit-popular-game.html

TATA COMMUNICATIONS

Bootkitty marks shift in the UEFI threat landscape

A newly discovered UEFI bootkit, named Bootkitty, represents the first proof-of-concept bootkit designed for Linux systems. Created by cybersecurity students in South Korea's Best of the Best (BoB) training program, Bootkitty aims to raise awareness about the risks of UEFI bootkits. Unlike previous bootkits that targeted only Windows systems, Bootkitty focuses on Linux, aiming to disable kernel signature verification and preload unknown ELF binaries. The bootkit is still in its early development phase and has not been observed in the wild.

The bootkit's creation marks a significant shift, as UEFI bootkits are now moving beyond Windows. It contains artifacts suggesting it was a proof of concept, including unused functions and traces that link it to the developers. Despite its limited scope, Bootkitty underscores the importance of maintaining updated security measures, such as enabling UEFI Secure Boot and keeping systems up to date, to defend against emerging threats.

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

Source - https://www.welivesecurity.com/en/eset-research/bootkitty-analyzing-first-uefi-bootkit-linux/

New PixPirate malware campaign targets users globally

A new wave of the PixPirate malware has been detected, primarily affecting users in Brazil, India, Italy, and Mexico. Initially targeting Brazilian banks and Pix payment services, this malware has expanded globally. PixPirate consists of two components: a downloader and a droppee application, both controlled by cybercriminals. The downloader, masquerading as a legitimate app, prompts users to install the malware via a YouTube tutorial. Once installed, the malware operates incognito, without an icon, making it harder to detect. The malware can steal user data, execute financial fraud, and spread through WhatsApp messages.

The latest PixPirate campaign also features new evasion techniques, including anti-virtual machine capabilities and hidden app icons. While the malware was first observed in Brazil in late 2021, its recent expansion and sophistication signal a growing threat, with India potentially becoming the next major target due to its widespread use of the UPI payment system.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	India, Brazil, Italy, Mexico	**APPLICATION**	Android

Source - https://securityintelligence.com/posts/pixpirate-back-spreading-via-whatsapp/

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