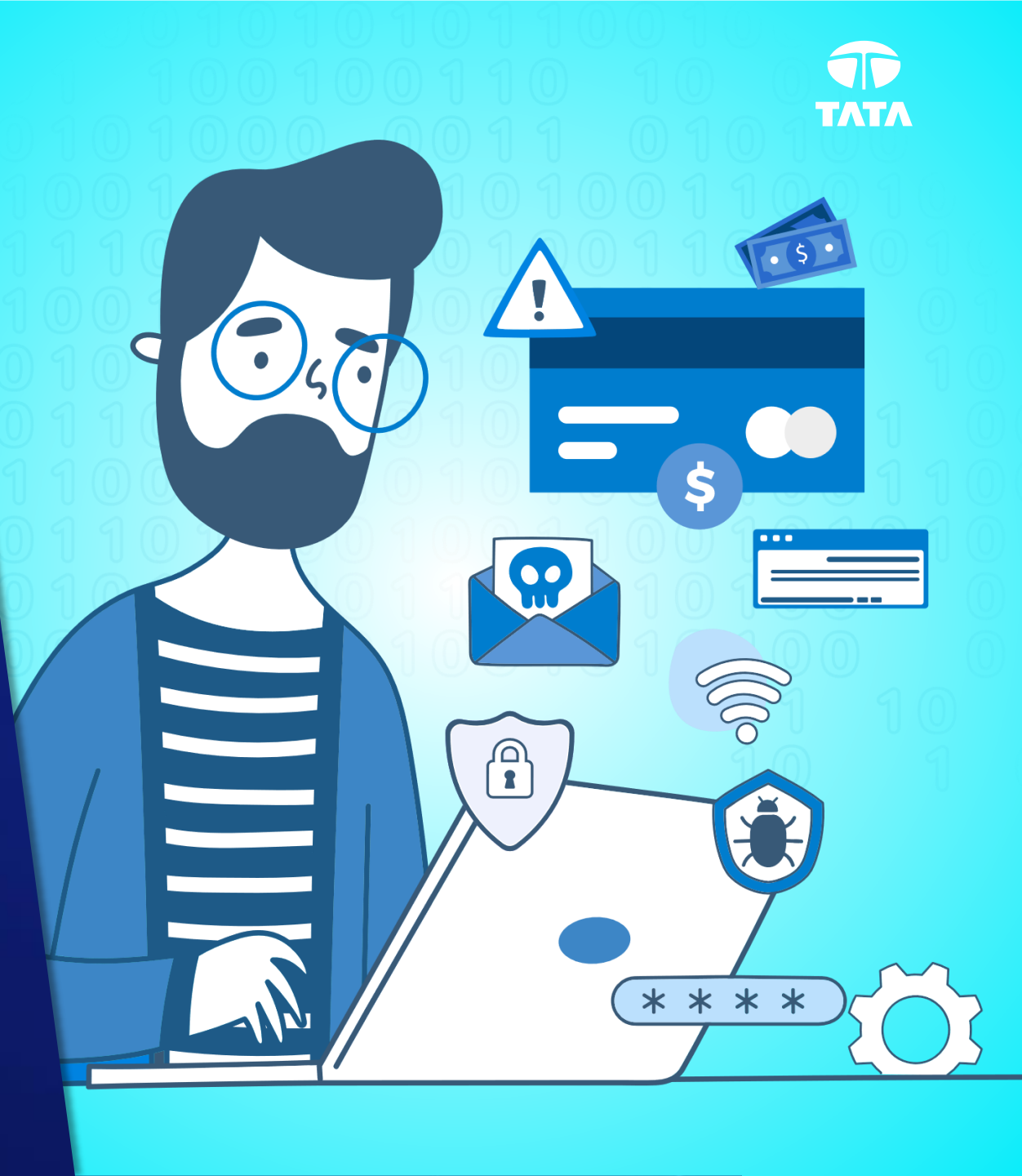
TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: APRIL 9TH, 2024



TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In the ever-changing global arena, safeguarding against cyber threats has become paramount for organisations. As these threats evolve ceaselessly, businesses strive not only to protect their data but also to fortify the essential structures that underpin modern operations. It's about ensuring resilience against a spectrum of emerging threats.

Enhance your organisation's cybersecurity preparedness with Tata Communications' weekly threat intelligence advisory. Acquire invaluable insights into the latest cyber risks and enact proactive strategies to fortify your defences, adeptly addressing potential vulnerabilities.

Chinese APT groups increase cyberespionage in ASEAN nations

Over the three months, researchers have detected two Chinese Advanced Persistent Threat (APT) groups engaged in cyberespionage against entities and member countries associated with the Association of Southeast Asian Nations (ASEAN). One group, identified as Stately Taurus, deployed tailored malware targeting organisations in Myanmar, the Philippines, Japan, and Singapore during the ASEAN-Australia Special Summit held on March 4-6, 2024. Meanwhile, another Chinese APT group compromised an ASEAN-affiliated entity, extending its cyberoperations to government entities in Cambodia, Laos, and Singapore.

Stately Taurus, active since at least 2012, has a history of targeting governmental, non-profit, religious, and non-governmental organisations across North America, Europe, and Asia. These developments underscore the mounting cyber threats in geopolitical contexts and the critical necessity for bolstered cybersecurity measures. Organisations, especially in the ASEAN region, are advised to utilise this intelligence to strengthen defences against such espionage activities.

ATTACK TYPE	Malware, cyberespionage	**SECTOR**	All
REGION	Singapore, Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Thailand, Vietnam	**APPLICATION**	Windows

Source - https://unit42.paloaltonetworks.com/chinese-apts-target-asean-entities/

Updated version of the Agenda ransomware targets ESXi servers

Since its inception in 2022, the Agenda ransomware collective, also known as Qilin or Water Galura, has aggressively targeted global industries, particularly finance and legal sectors. Recent months have seen a surge in attacks, accompanied by the development of sophisticated tools like a Rust variant of the ransomware. Agenda employs advanced techniques such as exploiting vulnerable SYS drivers and utilising custom scripts for lateral movement, underscoring the necessity for robust cybersecurity measures.

Researchers have identified top targets including the US, Argentina, Australia, and Thailand. Detection of the Agenda ransomware escalated sharply since December 2023, indicating increased activity or broader targeting. Updated versions have been observed, with the group utilising Remote Monitoring and Management (RMM) tools and Cobalt Strike for deployment. The ransomware spreads via PsExec and SecureShell, exploiting various vulnerable SYS drivers for evasion.

ATTACK TYPE	Ransomware	**SECTOR**	IT, healthcare/hospitals, financial services, construction, law, real estate
REGION	Australia, Argentina, Thailand, US	**APPLICATION**	VMware ESXi, VMware vCenter Server

Source - https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html

Apple security bug exposes iPhones and iPads to RCE

CVE-2024-1580, a critical vulnerability allowing remote code execution (RCE) on Apple devices, has prompted updates for iOS, iPadOS, macOS, Safari, and visionOS. Originating from an out-of-bounds write in the dav1d AV1 library, it affects various iPhone and iPad models. Apple's updates target the Core Media framework and WebRTC implementations to mitigate risks. Security advisories stress the importance of immediate installation to prevent potential exploits.

The affected iOS and iPadOS devices include iPhone XS and later, iPad Pro 12.9-inch second generation and later, iPad Pro 11-inch first generation and later, iPad Air third generation and later, and iPad mini fifth generation and later. The vulnerability in dav1d AV1 affects the Core Media framework and WebRTC in iOS and iPadOS. Updates not only cover iOS and iPadOS but also extend to Safari, macOS Sonoma and Ventura, and visionOS for the Vision Pro headset. These updates follow the recent release of iOS 17.4 by Apple.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Apple macOS, iOS, Safari

Source - https://www.darkreading.com/endpoint-security/apple-security-bug-opens-iphone-ipad-rce

Hackers target sensitive data in India using malicious emails

On March 7, 2024, analysts detected a sophisticated cyberattack targeting various Indian government agencies and energy corporations. The attackers employed a modified version of the HackBrowserData malware, distributed through phishing emails posing as Indian Air Force invitation letters. Leveraging Slack for command and control (C2), the perpetrators exfiltrated a significant 8.81 GB of sensitive data, including confidential documents and personal information, in what analysts labelled, “Operation FlightNight.” This operation utilised open-source tools and legitimate platforms, emphasising the evolving cyber threat landscape.

Multiple government entities, responsible for electronic communications, IT governance, and national defence, were targeted, alongside private Indian energy firms. The stolen data encompassed financial documents, employee personal details, and information regarding oil and gas drilling activities. Researchers shared their findings with Indian authorities to aid victim identification and incident response, attributing the motive to likely cyberespionage. Behavioural similarities suggest a connection with a previous attack reported on January 17, 2024.

ATTACK TYPE	Phishing, malware, cyberespionage	**SECTOR**	Energy, defence
REGION	India	**APPLICATION**	Generic

Source - https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign

WarzoneRAT malware makes a comeback with new tactics

In February, the FBI dismantled the WarzoneRAT malware network, resulting in infrastructure seizure and the arrest of suspects. However, Cyble Research and Intelligence Labs (CRIL) discovered ongoing malware campaigns through tax-themed spam emails, spreading WarzoneRAT (Avemaria). These campaigns employ sophisticated techniques, including decompressed email attachments initiating chains of actions or DLL sideloading, enabling remote control operations through connection to C2 servers.

WarzoneRAT (Avemaria) is a Remote Administration Tool (RAT) malware, initially detected in a 2018 phishing campaign. Its persistence underscores the ongoing threat, despite law enforcement actions. Additionally, ThreatMon reported a new version, WarzoneRAT v3, in February, featuring enhancements. Infection starts with an archive file attached to spam emails, containing a disguised shortcut file. Execution initiates a series of actions leading to WarzoneRAT (Avemaria) deployment.

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

Source - https://cyble.com/blog/warzonerat-returns-with-multi-stage-attack-post-fbi-seizure/

DinodasRAT Linux variant used in multi-country cyberattacks

Recent cybersecurity investigations have uncovered the DinodasRAT, or XDealer, malware, targeting regions like China, Turkey, and sensitive systems, including government entities in Guyana. Associated with Chinese threat groups, it's part of broader cyber espionage efforts like Operation Jacana. Noteworthy for its advanced capabilities, including a newly discovered Linux variant, DinodasRAT is significant in global data theft and espionage. This multi-platform backdoor tracks and harvests sensitive data, initially observed in attacks against Guyana's government entities.

Researchers have documented the Windows version as part of Operation Jacana. The new Linux variant, discovered in October 2023, primarily targets Red Hat-based distributions and Ubuntu Linux, ensuring single instance execution and generating unique identifiers for each infected machine. Operators behind Operation Jacana successfully infected Linux infrastructure, emphasising access maintenance, granting full control over infected machines, aiding data exfiltration, and espionage.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	China, Taiwan, Turkey, Uzbekistan	**APPLICATION**	Linux

Source - https://securelist.com/dinodasrat-linux-implant/112284/

Leaked code unleashes a new wave of crypto drainers

Cybersecurity experts have cautioned against the rising threat posed by malicious actors exploiting platforms like Google Ads and social media platforms to disseminate crypto drainers. Source codes leaked on cybercrime forums are facilitating the creation of dangerous variants. For instance, the Solana Drainer incident, linked to a $59 million theft, underscores these risks. Attackers employ sophisticated social engineering tactics to compromise wallets and drain cryptocurrency assets, necessitating enhanced digital security measures.

CRIL uncovered multiple drainer source codes leaked on cybercrime forums, including the Solana drainer. These codes enable the creation of new variants, with detailed instructions for deployment. Crypto drainers swiftly drain cryptocurrency wallets by assessing asset values and executing transactions. They spread through fake websites, emails, and phishing schemes, tricking users into authorising transactions. These malicious campaigns often begin with fake airdrops or phishing schemes advertised on social media or via email.

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

Source - https://cyble.com/blog/solana-drainers-source-code-saga-tracing-its-lineage-to-the-developers-of-ms-drainer/

Rhadamanthys malware targets users, spreads through fake installer

Researchers recently uncovered a sophisticated cyberattack campaign distributing the Rhadamanthys malware. The attackers employed a fake website resembling an authentic one, using search engine ads to lure victims into downloading the malware disguised as a legitimate groupware installation program. Rhadamanthys employs an evasion technique called indirect syscall to evade detection by manipulating system calls, allowing it to infiltrate Windows system processes undetected.

Unlike traditional API interactions, Rhadamanthys directly stores stub code and system call numbers in registers, bypassing user mode hooking used by antivirus and analysis programs. This technique involves directly reading the ntdll.dll file and mapping it to memory, enabling the malware to evade detection and inject malicious code into the system. Analysts confirmed the distribution of Rhadamanthys malware, emphasising the need for robust cybersecurity measures against such sophisticated threats.

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

Source - https://asec.ahnlab.com/ko/63412/

TheMoon botnet preys on vulnerable devices for criminal activities

TheMoon botnet, previously neutralised but now revived, has hijacked over 40,000 obsolete routers and IoT devices in 88 countries to establish a proxy network called Faceless, allowing cybercriminals to conceal their activities for less than a dollar per day. This resurgence, particularly targeting the financial sector through password attacks and data theft, exploits vulnerabilities in end-of-life devices, with a substantial number located in the US, indicating a strategic and persistent expansion of its malicious operations.

Faceless, unveiled by security journalist Brian Krebs in April 2023, serves as a nefarious residential proxy service, enabling threat actors to mask their true identities by routing traffic through compromised systems. Operators of malware like SolarMarker and IcedID utilise Faceless infrastructure to connect to their C2 servers, concealing their IP addresses. Researchers first detected this malicious activity in late 2023, aiming to compromise end-of-life routers and IoT devices and integrate them into Faceless.

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

Source - https://thehackernews.com/2024/03/themoon-botnet-resurfaces-exploiting.html

Sync-Scheduler stealer targets Office documents and user files

Researchers have conducted an in-depth analysis of the Sync-Scheduler stealer malware, emphasising its document theft capabilities and advanced evasion techniques. Distributed via Office documents, it conceals itself using file-nesting and obfuscation. The malware targets various file types and communicates with C2 servers for data exfiltration. Equipped with anti-analysis features, it terminates in detection scenarios.

To mitigate risks, users must exercise caution with file sources, use reputable antivirus software, update systems regularly, and be wary of social engineering. Education is crucial in empowering users to recognise and avoid such threats, fostering a more secure online environment.

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

Source - https://www.cyfirma.com/research/sync-scheduler-a-dedicated-document-stealer/

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