TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: APRIL 16TH, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today's dynamic digital landscape, defending against cyber threats has emerged as a critical priority for organisations worldwide. With these threats evolving constantly, companies are not just focused on safeguarding their data but also on reinforcing the fundamental frameworks that drive modern business operations. The goal is to establish resilience against an ever-expanding array of emerging threats.

Elevate your organisation's cybersecurity readiness with Tata Communications' weekly threat intelligence advisory. Gain invaluable insights into the most recent cyber risks and implement proactive strategies to strengthen your defences, effectively mitigating potential vulnerabilities.

DinodasRAT evolves; unveils stealthy Linux backdoor

Researchers have been tracking a Chinese-linked cyberespionage group, focusing on Southeast Asia, Africa, and South America, using the Linodas Linux backdoor, a DinodasRAT variant. This malware, derived from an open-source project, shares traits with Gh0st RAT and targets Linux servers, featuring an evasion module. Analysis of Linodas underscores the attackers' Linux exploitation focus, emphasising heightened security needs. It has been reported that a Linux version of DinodasRAT is targeting China, Taiwan, Turkey, and Uzbekistan. DinodasRAT, aka XDealer, a C++ malware, harvests sensitive data.

Analysts uncovered Operation Jacana targeting Guyana with a Windows variant in October 2023. It has also been noted that Earth Krahang's shift to DinodasRAT since 2023 has influenced attacks on global government entities. Various China-nexus actors, including LuoYu, use DinodasRAT, mainly targeting Red Hat and Ubuntu Linux. It establishes persistence using SystemV or SystemD, communicates over TCP or UDP, performs file operations, alters command-and-control (C2) addresses, executes shell commands, and encrypts communications with TEA, evading detection.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	South America, Africa, Asia	**APPLICATION**	Linux

Source - https://thehackernews.com/2024/03/linux-version-of-dinodasrat-spotted-in.html

Over 16,000 VPN gateways impacted by new Ivanti RCE flaw

Ivanti has issued security updates targeting critical vulnerabilities in its Connect Secure and Policy Secure Gateways, addressing risks of unauthorised code execution and denial-of-service (DoS) attacks. The flaw, identified as CVE-2024-21894, has affected over 16,000 VPN gateways, potentially enabling DoS or remote code execution (RCE) attacks by unauthenticated users. Researched have identified 29,000 and 18,000 exposed instances, respectively, prompting Ivanti's urgent update recommendation.

While no active exploitation has been detected, over 16,500 instances remain vulnerable. Most of these instances are in the US, with significant exposures in Japan, the UK, and other countries. Earlier, state-sponsored actors exploited multiple Ivanti flaws, including zero-days, leading to widespread deployment of web shells. A recent report delves into these attacks, involving Chinese hackers and the "SPAWN" malware family. System administrators are urged to apply available fixes and mitigations promptly.

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

Source - https://www.bleepingcomputer.com/news/security/new-ivanti-rce-flaw-may-impact-16-000-exposed-vpn-gateways/

92,000+ internet-facing D-Link NAS devices vulnerable to hacking

A new vulnerability impacting various D-Link NAS models, including DNS-340L, DNS-320L, DNS-327L, and DNS-325, has been disclosed by threat researchers. This flaw, tracked as CVE-2024-3273, involves a backdoor with hardcoded credentials and a command injection vulnerability within the '/cgi-bin/nas_sharing.cgi' script. Exploitation could allow arbitrary command execution, affecting over 92,000 devices online.

Although D-Link confirmed end-of-life status for these devices and ceased support, they advised replacement with supported products. D-Link lacks automatic updates or customer outreach for these devices but issued a security bulletin, urging immediate retirement or replacement. They provide legacy device support through a dedicated page and recommend applying available updates.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	D-Link

Source - https://www.bleepingcomputer.com/news/security/over-92-000-exposed-d-link-nas-devices-have-a-backdoor-account/

“Mighty Stealer” malware steals cookies, passwords, and more

The emergence of the “Mighty Stealer” malware signals a significant cybersecurity threat, capable of sophisticated data theft via its user-friendly graphical user interface (GUI) and advanced evasion tactics. It targets various sensitive data, including cookies, credentials, digital wallets, and webcam images, emphasising the need for enhanced cybersecurity measures. To mitigate risks, users should prioritise updated antivirus software, cautious software installation, regular password updates, and the implementation of multi-factor authentication.

The malware’s sleek interface belies its malicious intent, posing severe privacy violations and potential financial loss. Vigilance against such threats is paramount, as proactive protection measures are crucial to safeguarding personal information and devices from exploitation.

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

Source - https://gbhackers.com/beware-of-new-mighty-stealer/

New ransomware variant “SEXi” targets VMware servers

IxMetro Powerhost, a Chilean datacentre, faced a severe cyberattack by the “SEXi” ransomware, a new variant linked to the Babuk family. This attack, demanding a record ransom of $140 million, targeted VMware ESXi servers, crippling services for customers. The incident highlights a concerning trend of specialised server attacks and sophisticated extortion tactics, particularly in Latin America. The ransomware, appending the .SEXi extension, encrypts servers and backups, posing significant challenges for data restoration.

Negotiation attempts resulted in a demand of two bitcoins per victim. While the ransomware operation mainly targets VMware ESXi servers, its infrastructure appears ordinary. The name SEXi is a wordplay on ESXi. The ransom notes instruct victims to use the Session messaging app for communication.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	VMware ESXi

Source - https://www.bleepingcomputer.com/news/security/hosting-firms-vmware-esxi-servers-hit-by-new-sexi-ransomware/

JSOutProx malware takes aim at financial institutions

Visa's Payment Fraud Disruption (PDF) division has alerted of a surge in JSOutProx malware attacks on financial sectors in South and Southeast Asia, the Middle East, and Africa. This sophisticated trojan, distributed through phishing, grants extensive control over infected devices, posing severe risks. Visa advises enhanced security measures to combat this evolving threat, urging awareness of phishing risks, secure acceptance technologies, and monitoring for suspicious transactions.

The malware, first seen in December 2019, allows remote control, file execution, and keyboard/mouse manipulation. While the campaign's goal remains unconfirmed, Visa suspects fraudulent activities targeting financial institutions. Researchers have noted fabricated financial notifications sent via phishing emails containing JSOutProx payloads. Attribution to the Solar Spider group is uncertain, but analysts suggest Chinese or China-affiliated threat actors due to the attacks' sophistication and targeted geography. Visa's alert includes indicators of compromise and mitigation recommendations.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Middle East, Africa, APAC	**APPLICATION**	Windows

Source - https://www.bleepingcomputer.com/news/security/visa-warns-of-new-jsoutprox-malware-variant-targeting-financial-orgs/

Fake e-commerce campaign targets banks in Southeast Asia

Researchers have uncovered an advanced fake e-commerce campaign targeting Malaysian banks, now expanding to Vietnam and Myanmar. Utilising sophisticated malware, the threat includes screen-sharing and complex communications, evolving since 2021. Originating from deceptive ads, it now employs phishing websites, focusing mainly on Southeast Asia. The campaign masquerades as cleaning services on social media, tricking victims into contacting via WhatsApp.

The campaign has so far targeted banks in Southeast Asia, demonstrating social engineering tactics combined with phishing. It aims to replace SMS apps and gain screen capture permissions, suggesting sophisticated attacks. The fake e-shop scheme lures users to fake products, stealing credentials and banking information. Recent enhancements include screen-sharing and exploiting accessibility services, signalling an intent to broaden targets and data theft. This escalation underscores the imperative for heightened cybersecurity awareness and measures.

ATTACK TYPE	Malware	**SECTOR**	BFSI
REGION	Malaysia, Myanmar, Vietnam	**APPLICATION**	Android

Source - https://cybersecuritynews.com/fake-e-shopping-attack/

Stealth malware “UNAPIMON” used by China-linked hackers

The cyberespionage group, Earth Freybug, linked to APT41, has deployed the new UNAPIMON malware, showcasing their sophisticated attack tactics like DLL hijacking. UNAPIMON, written in C++, evades security measures using innovative techniques, reflecting the group’s adaptability. Researchers have identified UNAPIMON’s deployment via batch files, exploiting a service for DLL sideloading, enhancing stealth. It employs Detours, an opensource Microsoft library, to prevent monitoring of its child processes, emphasising its sophistication.

Analysts have underscored the challenge of detecting UNAPIMON due to its skilled coding and use of off-the-shelf libraries. They have recommended robust cybersecurity measures including blocking Indicators of Compromise (IoCs), periodic hardening of systems, and awareness of social engineering and phishing attacks. Implementing the Principle of Least Privilege, keeping software updated, and having behavioural detection solutions are advised for organisations to mitigate such threats effectively.

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

Source - https://varutra.com/ctp/threatpost/postDetails/China-Linked-Hackers-Unleash-Stealthy-UNAPIMON-Malware-for-Covert-Operations/SlY5NVFSUnZkUmRHRFBwbzBjU3g5QT09/

Vietnamese hackers found stealing financial information across Asia

Security analysts have uncovered CoralRaider, a suspected Vietnamese threat group conducting cyberespionage in Asia since May 2023. Their focus is on extracting valuable data using sophisticated malware like RotBot and XClient stealer, particularly targeting business and advertising accounts. CoralRaider innovatively employs Telegram for data exfiltration and dark web trading, showcasing the evolving cyber threat landscape, demanding heightened cybersecurity defences. The group's activities span various Asian countries, with targets including India, China, South Korea, Bangladesh, Pakistan, Indonesia, and Vietnam.

They utilise a range of malware, including AsyncRAT, NetSupport RAT, and Rhadamanthys, to steal credentials and financial and social media data. Telegram is used for data exfiltration, with stolen information traded on underground markets for profit. CoralRaider's operators, evidenced by their Telegram communication and language preferences, primarily operate from Vietnam. Researchers have also disclosed a malvertising campaign exploiting generative AI tools on Facebook.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	India, Bangladesh, China, Indonesia, South Korea, Pakistan, Vietnam	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/04/vietnam-based-hackers-steal-financial.html

Google issues patches for Chrome, Android, and Pixel phones

Google Chrome recently tackled numerous security flaws, including a critical zero-day vulnerability (CVE-2024-3159) found during the Pwn2Own contest. These vulnerabilities – from the V8 JavaScript engine to Bookmarking and WebCodecs – could lead to DoS attacks, unauthorised data disclosure, or RCE. The updates aim to mitigate these risks, also addressing other zero-day vulnerabilities in Android and Google Pixel smartphones, emphasising the importance of regular security updates.

Google has also patched 28 vulnerabilities in Android and 25 bugs in Pixel devices, including two exploited in the wild (CVE-2024-29745 and CVE-2024-29748). The flaws affected Pixel's bootloader and firmware, with indications of limited, targeted exploitation. Google often connects these vulnerabilities to commercial spyware vendors. The Pixel update resolves 24 vulnerabilities leading to elevation of privilege (EoP) and information disclosure, alongside other bugs in Qualcomm components.

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

Source - https://www.securityweek.com/google-patches-exploited-pixel-vulnerabilities/

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