TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: DECEMBER 24, 2024

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

In today's shifting landscape of increasing cyber threats, it is essential to protect critical systems and data for individuals, businesses, and governments. Cyber disruptions can lead to financial losses, reputational damage, and jeopardise operational security.

Our weekly Cyber Threat Intelligence (CTI) report offers actionable insights into emerging global threats to fortify defences. Backed by expert advisory services, we provide proactive strategies to safeguard IT assets against evolving risks. With our intelligence-driven approach, your organisation can take control of its security posture, mitigate persistent threats, and ensure a resilient, secure future in the face of dynamic cyber challenges.

Lynx ransomware group targets energy sector

The Lynx ransomware group has emerged as a significant threat to the global energy sector between 2022 and 2024. Targeting oil, gas, and utility organisations, the group employs double extortion tactics. This involves encrypting critical systems and threatening to release stolen sensitive data unless ransoms are paid. Exploiting outdated systems and the high operational cost of downtime, Lynx has driven a wave of attacks in an industry heavily reliant on seamless operations. These attacks pose financial, reputational, and security risks to organisations.

Experts recommend deploying comprehensive cybersecurity frameworks that include regular patching, advanced threat monitoring systems, and multi-layered defences. Employee training to recognise phishing and malicious emails, often the initial attack vectors, is equally crucial. Collaboration between public and private entities to share threat intelligence can help mitigate the evolving threat landscape.

ATTACK TYPE	Ransomware	**SECTOR**	Oil and gas, Energy
REGION	Global	**APPLICATION**	Generic

Source - https://www.cisecurity.org/insights/blog/lynx-ransomware-pouncing-utilities

ZLoader Malware Resurges with New Stealth Tactics

ZLoader, a notorious malware family, has resurfaced with advanced capabilities, posing a severe threat to global cybersecurity. Known for its role in distributing ransomware like Black Basta, the malware now incorporates DNS tunnelling, enabling encrypted and stealthy command-and-control (C2) communications. An interactive shell allows attackers to execute sophisticated commands, making ZLoader more effective in data exfiltration and ransomware facilitation. Enhanced evasion techniques, including advanced obfuscation and anti-analysis mechanisms, make detection and mitigation increasingly challenging. ZLoader primarily targets Windows systems and propagates through phishing emails, malicious websites, and drive-by downloads.

To mitigate this threat, organisations should deploy endpoint detection and response (EDR) tools, ensure regular patching, and train employees to recognise phishing tactics. Employing advanced email filtering and network monitoring solutions can also help in early detection and prevention.

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

Source - https://thehackernews.com/2024/12/zloader-malware-returns-with-dns.html

Surge in Remcos RAT attacks

Remcos RAT (remote access trojan) has seen a significant surge, leveraging advanced evasion techniques to bypass security measures. In Q3 2024, its widespread use in phishing campaigns showcased its adaptability. Attackers distribute Remcos via VBS files and Office Open XML documents attached to phishing emails. Once installed, it enables remote control, keylogging, data theft, and espionage by injecting itself into legitimate processes and maintaining persistence. Its obfuscation capabilities make it highly elusive, complicating detection and response. This malware is widely used in campaigns targeting businesses, governments, and individuals globally.

Security experts recommend robust email security systems, comprehensive endpoint protection, and proactive threat hunting to detect and eliminate this threat. Educating employees on phishing risks and maintaining up-to-date software are essential defensive measures.

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

Source - https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-stealthy-stalker-remcos-rat/

Nova Keylogger uses encrypted messaging for data exfiltration

Nova Keylogger, a sophisticated evolution of the Snake Keylogger, has advanced capabilities that make it a prominent threat to data security. Targeting sensitive information from web browsers, email clients, and operating systems, Nova uses multi-channel exfiltration methods, including FTP, SMTP, and Telegram. The malware employs advanced evasion techniques such as process hollowing and obfuscation to bypass detection. Additionally, its encrypted messaging ensures secure data exfiltration, complicating defensive efforts.

Nova's adaptability allows it to evolve with emerging cybersecurity measures, enabling it to maintain relevance across varied attack scenarios. Businesses are advised to use advanced anti-malware solutions, monitor network traffic, and secure configurations to reduce vulnerability. Continuous monitoring and endpoint security solutions are essential to defend against this malware.

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

Source - https://any.run/cybersecurity-blog/nova-keylogger-malware-analysis/

Hackers exploit retail and crypto wallets with sophisticated phishing

The Aggressive Inventory Zombies (AIZ) threat actor group has launched highly sophisticated phishing campaigns targeting retail giants like Amazon and crypto platforms such as Biance. By creating counterfeit websites with advanced chat integrations, AIZ deceives users into sharing credentials and financial details. Their operations are supported by an expansive infrastructure linked to India, making them resilient to takedown attempts.

Collaborative efforts between law enforcement and cybersecurity firms have exposed hundreds of phishing sites, revealing the group's widespread reach and meticulous planning. These campaigns exploit the booming e-commerce and crypto markets, often targeting busy holiday seasons. Businesses and individuals must remain vigilant, adopt multifactor authentication (MFA), and verify website authenticity to protect against these phishing schemes.

ATTACK TYPE	Phishing	**SECTOR**	Retailer and distributor
REGION	Global	**APPLICATION**	Generic

Source - https://www.silentpush.com/blog/aiz-retail-crypto-phishing/?utm_source=rss&utm_medium=rss&utm_campaign=aiz-retail-crypto-phishing

China-backed hackers leverage PHPsert for cyberespionage

China-backed cyberespionage groups have deployed PHPsert, a web shell leveraging PHP-based obfuscation techniques like XOR encoding and randomised variables to evade detection. This tool allows attackers to execute, modify, and retrieve malicious payloads in real-time. Targeting organisations globally, PHPsert supports operations including data theft, surveillance, and system manipulation.

To counter this threat, experts recommend implementing strong access controls, file integrity monitoring, input validation, and regular vulnerability assessments. Proactive incident response planning and adopting web application firewalls (WAF) can significantly mitigate risks.

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

Source - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2024-0040

New malware threatens critical infrastructure

IOCONTROL, a modular and sophisticated malware, poses a severe threat to critical infrastructure in the U.S. and Israel. Linked to the Iranian CyberAv3ngers group, this malware targets IoT and OT/SCADA systems used in industrial and critical sectors, including routers, programmable logic controllers (PLCs), and fuel management systems. IOCONTROL uses advanced evasion techniques, encrypted configurations, and versatile commands to exfiltrate data, disrupt operations, and grant attackers control over essential systems. These attacks threaten national security and can lead to severe operational downtime and data breaches.

To counter this threat, experts recommend robust cybersecurity frameworks tailored to critical infrastructure, including segmenting networks, enhancing system logging, and deploying specialised OT monitoring tools. Collaborative defence strategies between public and private sectors are also crucial to counteract this advanced threat.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Israel, US	**APPLICATION**	Windows/Linux

Source - https://www.bleepingcomputer.com/news/security/new-iocontrol-malware-used-in-critical-infrastructure-attacks/

Advanced Linux Rootkit, Pumakit found in the wild

Pumakit, a Linux rootkit targeting older kernels (pre-5.7), has emerged as a critical threat to enterprise and industrial systems. This modular malware comprises a dropper, kernel module rootkit, and userland component (Kitsune SO), enabling attackers to conceal malicious activities, intercept system calls, and execute commands stealthily. It grants attackers root access, allowing complete control over infected systems while communicating undetected with command-and-control (C2) servers.

Pumakit's primary targets are enterprises relying on outdated Linux systems, making kernel updates and vulnerability management essential. Effective mitigation includes implementing robust rootkit detection solutions, conducting regular system audits, and adhering to secure system configurations.

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

Source - https://www.elastic.co/security-labs/declawing-pumakit

Banking Trojan spreads through fake applications in India

Android/Banker, a sophisticated banking trojan, has emerged as a major mobile security threat in India. Masquerading as legitimate utility and banking apps, it propagates through phishing campaigns on platforms like WhatsApp. The malware exfiltrates sensitive user data, including credentials and financial details, using innovative methods like Supabase for data exfiltration. This trojan has compromised hundreds of devices, intercepted thousands of SMS messages, and caused significant financial losses. Its advanced evasion techniques make it resilient against traditional defences.

To protect against such threats, users must download apps exclusively from official stores, enable two-factor authentication, and use updated anti-malware software. Organisations should raise awareness about mobile phishing and enforce mobile device management (MDM) policies.

ATTACK TYPE	Malware	**SECTOR**	BFSI
REGION	India	**APPLICATION**	Android

Source - https://www.mcafee.com/blogs/other-blogs/mcafee-labs/a-new-android-banking-trojan-masquerades-as-utility-and-banking-apps-in-india/

DarkGate malware spreads through MS Teams

DarkGate malware exploits vulnerabilities in Microsoft Teams to facilitate unauthorised access, account takeovers, and privilege escalations. This malware employs phishing tactics, distributing malicious links or attachments through Teams messages to infiltrate organisations. Once inside, it establishes persistence and exfiltrates sensitive data. Its use of trusted communication platforms like Teams complicates detection and remediation.

Organisations are urged to adopt secure Teams configurations, deploy endpoint security solutions, and train employees to identify suspicious activity on collaboration platforms. Regular updates and patches to Microsoft Teams and associated software are essential to reduce vulnerabilities.

ATTACK TYPE	Phishing	**SECTOR**	All
REGION	Global	**APPLICATION**	Teams

Source - https://www.trendmicro.com/en_in/research/24/l/darkgate-malware.html

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