TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: FEBRUARY 18, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In an increasingly volatile digital landscape, proactive cybersecurity has become critical across all sectors. Our comprehensive weekly Cyber Threat Intelligence (CTI) reports provide vital intelligence on emerging threats and vulnerabilities, enabling organisations to strengthen their security posture effectively.

By combining expert analysis with actionable insights, we help clients anticipate and mitigate potential cyber risks before they materialise. This strategic approach to cybersecurity not only protects valuable digital assets but also ensures operational continuity and maintains stakeholder trust through enhanced cyber resilience.

Human-AI collaboration uncovers secrets of ELF SSHInjector malware

A groundbreaking analysis of the ELF SSHInjector malware has been conducted, combining human expertise with artificial intelligence (AI) to reveal its sophisticated capabilities. The malware, targeting Linux systems, is designed to inject malicious code into Secure Shell (SSH) processes, enabling attackers to steal credentials and gain unauthorised access to compromised systems. Researchers at Fortinet dissected the malware, uncovering its ability to evade detection by leveraging dynamic code loading and encryption techniques.

The collaborative effort between human analysts and AI tools proved instrumental in decoding the malware's complex behaviour. AI accelerated the identification of patterns and anomalies, while human analysts provided contextual insights into its operational tactics. This hybrid approach highlights the growing importance of combining human intuition with machine efficiency in combating advanced cyber threats. As ELF SSHInjector continues to pose a risk to Linux environments, cybersecurity experts urge organisations to strengthen defences, monitor SSH activity, and adopt AI-driven solutions to stay ahead of evolving threats.

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

Source - https://www.fortinet.com/blog/threat-research/analyzing-elf-sshdinjector-with-a-human-and-artificial-analyst

Ukrainian organisations targeted in a cyberattack exploiting vulnerability

A recent cyberattack campaign has targeted Ukrainian organisations, exploiting a critical vulnerability – CVE-2025-0411 – to infiltrate systems and deploy malicious payloads. According to researchers, the attackers leveraged this zero-day flaw to gain unauthorised access, exfiltrate sensitive data, and disrupt critical operations. The campaign, believed to be state-sponsored, showcases advanced tactics, including custom malware and evasion techniques to bypass traditional security measures.

The vulnerability, which affects widely used software, allows attackers to execute arbitrary code remotely, posing significant risks to both public and private sectors. Ukrainian cybersecurity teams are working tirelessly to patch systems and mitigate the threat, but the incident underscores the growing sophistication of cyber warfare. Experts urge organisations globally to prioritise vulnerability management, implement robust detection tools, and share threat intelligence to combat such attacks. As geopolitical tensions escalate, this incident serves as a stark reminder of the critical need for proactive cybersecurity defences in an increasingly volatile digital landscape.

ATTACK TYPE	Vulnerability, malware	**SECTOR**	All
REGION	Ukraine	**APPLICATION**	7-Zip

Source - https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html

TAG-124 uses sophisticated traffic distribution systems to drive malware

A recent investigation has uncovered the inner workings of TAG-124, a cybercriminal group operating a highly sophisticated traffic distribution system (TDS) that fuels global malware campaigns. Security researchers revealed that TAG-124's TDS acts as a gateway, redirecting unsuspecting users to malicious websites hosting malware such as ransomware, stealers, and banking trojans. The system employs advanced filtering mechanisms to evade detection, targeting specific victims based on geolocation, device type, and browsing behaviour.

By analysing over 124,000 unique domains linked to the operation, experts found that TAG-124's infrastructure supports multiple threat actors, making it a critical enabler of cybercrime. The group's ability to dynamically adapt its tactics has allowed it to remain resilient against takedown efforts. This discovery highlights the growing complexity of cybercriminal ecosystems and underscores the urgent need for enhanced threat intelligence and collaborative cybersecurity measures to disrupt such operations and protect users worldwide.

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

Source - https://securityonline.info/tag-124-a-deep-dive-into-the-traffic-distribution-system-powering-malware-campaigns/

macOS stealer malware surges, targeting user data and cryptocurrency

A new report has revealed an alarming increase in macOS stealer malware, designed to steal sensitive data, credentials, and cryptocurrency from Apple users. These malicious programs, often disguised as legitimate software, exploit the growing popularity of macOS among consumers and professionals. Researchers identified several active campaigns distributing stealers like Atomic, Joker, and CherryPie, which target browser-stored passwords, cookies, and crypto wallets.

The malware is primarily spread through pirated software, fake updates, and phishing schemes, capitalising on user trust. Once installed, it operates stealthily, exfiltrating data to remote servers controlled by cybercriminals. The rise in macOS-targeted stealers highlights a shift in attacker focus, as traditionally Windows-centric threats expand to other platforms. Cybersecurity experts urge macOS users to avoid downloading software from untrusted sources, enable system updates, and use robust security solutions to mitigate risks. As these threats evolve, vigilance and proactive measures are essential to safeguarding personal and financial information.

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

Source - https://unit42.paloaltonetworks.com/macos-stealers-growing/

AsyncRAT campaign leverages Python payloads to target victims

A new wave of AsyncRAT malware campaigns has emerged, utilising Python-based payloads to infiltrate systems and steal sensitive data. According to cybersecurity reports, attackers are distributing the malware through phishing emails and malicious documents, exploiting Python's versatility to evade detection. Once executed, the payload establishes a connection to a command-and-control (C2) server, enabling remote access to compromised devices.

The campaign primarily targets Windows users, allowing attackers to harvest credentials, capture screenshots, and exfiltrate files. Researchers highlight the use of obfuscation techniques to bypass security tools, making detection challenging. This shift to Python-based payloads underscores the evolving tactics of cybercriminals, who are increasingly adopting unconventional methods to enhance malware effectiveness. Experts urge organisations to strengthen email security, educate employees on phishing risks, and deploy advanced threat detection solutions.

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

Source - https://thehackernews.com/2025/02/asyncrat-campaign-uses-python-payloads.html

Daixin Team ransomware grows as a cyber threat, targets critical sectors

The Daixin Team ransomware has rapidly gained notoriety as a significant cyber threat, targeting critical sectors such as healthcare, transportation, and manufacturing. Known for its double-extortion tactics, the group not only encrypts victims' data but also exfiltrates sensitive information, threatening to leak it unless ransom demands are met. Recent attacks have exploited vulnerabilities in VPNs and remote desktop protocols (RDP) to infiltrate networks, showcasing the group's technical sophistication.

Cybersecurity experts warn that Daixin Team's operations are highly organised, with a focus on maximising financial gain and disruption. The ransomware's ability to evade detection and spread laterally within networks makes it particularly dangerous. Organisations are urged to strengthen their defences by patching vulnerabilities, implementing multi-factor authentication (MFA), and conducting regular security audits. As ransomware threats continue to evolve, proactive measures and threat intelligence sharing are critical to mitigating risks and safeguarding sensitive data from this escalating menace.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, government
REGION	Global	**APPLICATION**	VMware ESXi, Windows, Linux

Source - https://hivepro.com/threat-advisory/daixin-team-ransomware-a-growing-cyber-threat/

TATA COMMUNICATIONS

SparkCat Stealer malware threatens user data on App Store and Google Play

A new malware threat, SparkCat Stealer, has infiltrated both the Apple App Store and Google Play, masquerading as legitimate apps to steal sensitive user data. The malicious apps target credentials, banking information, and cryptocurrency wallets, posing a significant risk to millions of users. SparkCat Stealer employs sophisticated obfuscation techniques to evade detection, highlighting the growing challenge of securing app marketplaces. Once installed, the malware silently harvests data and sends it to remote servers controlled by cybercriminals. Researchers warn that the apps often appear harmless, such as productivity tools or games, making them difficult to identify.

This breach underscores the need for heightened vigilance among users and stricter vetting processes by app stores. Cybersecurity experts recommend downloading apps only from trusted developers, reviewing permissions, and using robust security software. As malware continues to exploit app platforms, proactive measures are essential to protect personal and financial information from evolving threats.

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

Source - https://securelist.com/sparkcat-stealer-in-app-store-and-google-play/115385/

Hunter Prince ransomware encrypting files and demanding ransom

A new ransomware strain, Hunter Prince, has been discovered, targeting users worldwide by encrypting files and demanding payment for their release. The ransomware appends the ".hunter_prince" extension to encrypted files and drops a ransom note titled "HOW TO RECOVER ENCRYPTED FILES.TXT," instructing victims to contact attackers via email or Telegram for decryption. Hunter Prince employs strong encryption algorithms, making file recovery without the attackers' key nearly impossible. It infiltrates systems through phishing emails, malicious downloads, or exploited vulnerabilities.

Cybersecurity experts warn that paying the ransom does not guarantee file recovery and may further fund criminal activities. To protect against Hunter Prince, users are advised to avoid suspicious emails, keep software updated, and maintain regular backups. As ransomware threats continue to evolve, proactive cybersecurity measures and awareness are critical to mitigating risks and safeguarding sensitive data from such malicious attacks.

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

Source - https://www.pcrisk.com/removal-guides/32074-hunter-prince-ransomware

TATA COMMUNICATIONS

ALPHV ransomware targeting enterprises with advanced double-extortion

ALPHV (BlackCat) ransomware has emerged as a formidable threat to enterprises worldwide, leveraging advanced double-extortion tactics to maximise impact. The ransomware not only encrypts victims' data but also exfiltrates sensitive information, threatening to leak it unless ransom demands are met. Known for its sophistication, ALPHV employs Rust programming language, enabling cross-platform attacks and enhanced evasion capabilities. The group targets industries such as healthcare, finance, and manufacturing, exploiting vulnerabilities in remote desktop protocols (RDP) and phishing campaigns to infiltrate networks. Its affiliate-based model allows for rapid scalability, making it one of the most active ransomware groups today.

Cybersecurity experts urge organisations to strengthen defences by patching vulnerabilities, implementing MFA, and conducting regular backups. As ALPHV continues to evolve, proactive threat detection and response strategies are essential to mitigate risks and protect critical data from this escalating ransomware menace.

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

Source - https://www.picussecurity.com/resource/blog/alphv-ransomware

TATA COMMUNICATIONS

Abyss Locker ransomware strikes with precision, targets critical infrastructure

A recent analysis has revealed the alarming tactics of Abyss Locker ransomware, which has been targeting critical infrastructure with surgical precision. The ransomware employs a multi-stage attack strategy, exploiting vulnerabilities in internet-facing systems and leveraging legitimate tools like PowerShell and PsExec to evade detection. Once inside, it encrypts files and demands ransom, leaving victims with limited recovery options. Abyss Locker distinguishes itself by using custom encryption algorithms and targeting specific high-value assets, maximising disruption and financial gain. The attackers also exfiltrate sensitive data, threatening to leak it if ransom demands are not met.

Reports underscore the importance of proactive defence measures, including regular patching, network segmentation, and robust endpoint detection. As ransomware groups like Abyss Locker continue to refine their methods, organisations must prioritise cybersecurity resilience to protect critical systems and data from these increasingly sophisticated threats.

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

Source - https://www.sygnia.co/blog/abyss-locker-ransomware-attack-analysis/

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