TATA COMMUNICATIONS

TATA

QUARTERLY EXECUTIVE THREAT REPORT Q3 2024

Executive summary

Q3 2024 saw a surge in sophisticated cyber threats. High-profile incidents included ransomware campaigns exploiting zero-day vulnerabilities in critical platforms. Nation-state actors drove cyberespionage, targeting sensitive industries such as aerospace, healthcare, and government. Additionally, the rise of AI-enhanced threats and advanced supply chain attacks further underscores the growing complexity of the cyber landscape. This quarter highlighted the need for enterprises to adopt proactive measures like AI-driven threat detection, robust patch management, and fortified incident response plans to counter evolving risks effectively.

A landscape of new threats – quarterly highlights

A staggering 22,254 common vulnerabilities and exposures (CVEs) were reported by mid-2024, reflecting a 30% jump compared to 2023 and a 56% increase from 2022[1].

As 2024 reaches its conclusion, the cybersecurity landscape remains ever more complex and dynamic. Threat actors continue to refine their methods, unleashing advanced malware and ransomware campaigns targeting critical industries such as energy, aerospace, healthcare, and government. Sophisticated exploits, including multi-stage attacks and zero-day vulnerabilities, demonstrate a shift toward espionage-driven and double extortion tactics, with devastating potential across sectors.

Q3 highlights the urgent need for proactive, AI-powered threat-hunting frameworks capable of countering increasingly stealthy and adaptive adversaries. From North Korea-linked espionage campaigns to widespread vulnerabilities in leading platforms, these incidents underscore the fragility of unpatched systems and the risks posed by supply chain weaknesses. In response, global regulatory bodies are ramping up advisories, advocating stricter data protection measures and greater collaboration between the public and private sectors. Enterprises are now prioritising zero-trust architectures and real-time threat detection to stay ahead of the evolving threat landscape.

According to a global research, in Q3 2024, an average of 1,876 cyberattacks per organisation was recorded, marking a 75% increase compared to the same period in 2023 and a 15% rise from the previous quarter[2].

Adapting to an evolving threat ecosystem – Top ten threats of Q3 2024

Based on the insights gained from our threat intelligence research, some of the key threats identified in Q3 are as below:

UNC2970 deploys new backdoor

A North Korean-linked hacking group, UNC2970, has launched a new cyberespionage campaign aimed at senior executives in critical sectors such as energy and aerospace[2]. The group is using phishing emails to deliver a trojanised version of SumatraPDF, which installs a backdoor named MISTPEN, granting attackers remote control over compromised systems. This stealthy attack is disguised as legitimate job opportunities to lure high-profile individuals into downloading the malicious software.

While the attack targets organisations worldwide, its primary focus is on high-value industries. Companies are urged to remain vigilant against phishing attempts and ensure that their employees are aware of the risks posed by unsolicited job offers. Strengthening cybersecurity protocols, especially in sectors handling sensitive data, is essential to prevent these advanced threats.

New SnipBot malware variant targets enterprise networks

A new variant of the RomCom malware family, named SnipBot, has been identified, posing a significant threat to enterprise networks worldwide[3]. First discovered in early 2024, SnipBot gains initial access via phishing emails and uses advanced anti-detection techniques to execute remote commands and exfiltrate sensitive data. Unlike its ransomware-focused predecessors, SnipBot is designed for intelligence gathering and espionage. It primarily targets industries such as IT services, legal sectors, and agriculture.

This sophisticated malware represents a growing shift toward espionage-driven cyberattacks, with attackers seeking to gather critical data from organisations globally. Enterprises across all sectors need to enhance their phishing defences and monitoring systems to detect and mitigate such threats effectively.

Fortinet shores up its defences against critical exploits to protect vulnerable endpoints

Fortinet's cybersecurity landscape in Q3 2024 has been severely impacted by multiple critical vulnerabilities exploited by advanced threat actors, potentially threatening nearly 150,000 devices and just as many critical servers by extension. BrazenBamboo, a sophisticated group, exploited a zero-day vulnerability in Fortinet's FortiClient for Windows using the DEEPDATA modular framework[4]. This multi-stage post-exploitation tool employs DLLs for credential theft, data exfiltration, and surveillance, particularly targeting communication platforms like WhatsApp, Signal, and Telegram. Alongside DEEPDATA, the group utilises DEEPPOST and LightSpy for cross-platform data theft and remote command execution, indicating a centralised Chinese origin. Despite early reporting of the FortiClient flaw in July, it remains unpatched, highlighting the necessity for enhanced cybersecurity measures to counter such advanced cyberespionage threats.

Additionally, a remote code execution (RCE) vulnerability, CVE-2024-23113, has been actively exploited, affecting FortiOS, FortiPAM, FortiProxy, and FortiWeb[5]. Compounding these challenges, a zero-day vulnerability in FortiManager, CVE-2024-47575, dubbed FortiJump, allows unauthorised access to sensitive data through a missing authentication function[6]. Rated 9.8 on the CVSS scale, it presents significant risks to system integrity. Fortinet has issued patches for affected products, urging prompt updates to mitigate potential breaches. Despite initial private notifications and mitigation guidance, details leaked publicly, leading to pre-emptive attacks. Fortinet advises immediate credential updates and continues to investigate the breach's full scope.

Interlock ransomware executes double extortion attacks

Researchers recently tracked a sophisticated attack using the new Interlock ransomware, which employed multiple stages of compromise[7]. The attacker used a remote access trojan (RAT) disguised as a browser updater, PowerShell scripts, credential stealers, and keyloggers before deploying the ransomware encryptor. Lateral movement within the network was primarily via Remote Desktop Protocol (RDP), with additional tools like AnyDesk and PuTTY. Data exfiltration occurred using Azure Storage Explorer, leveraging AzCopy to move data to an attacker-controlled Azure storage blob. The attack's timeline showed that the attacker remained in the victim's environment for about 17 days before executing the ransomware.

Interlock, identified in September 2024, is linked to big-game hunting and double extortion tactics. The ransomware targets various sectors, including healthcare, technology, and government, and operates a data leak site. Interlock's binary encrypts files with the *.interlock* extension and drops a ransom note. Both Windows and Linux variants of the ransomware are in use.

Emansrepo infostealer poses growing threat

Cybersecurity researchers have identified Emansrepo, a Python-based infostealer, as a growing threat. This virus, which is distributed by phishing emails disguised as purchase orders and invoices, uses three attack chains to avoid detection: AutoIt-compiled executables, HTA files, and obfuscated batch scripts. Emansrepo was first built to steal credentials, but it has now evolved to target PDFs, bitcoin wallets, and other files[8].

The malware's adaptability and multi-vector approach render it especially deadly. A separate effort also uses DBatLoader to transmit Remcos malware, which broadens the threat landscape. The expanding capabilities of Emansrepo emphasise the necessity for organisations to tighten email security and watch for suspicious activities to mitigate risks.

SafePay ransomware emerges with exfiltration and encryption tactics

Analysts have discovered SafePay, a sophisticated ransomware strain linked to advanced techniques and older ransomware families like LockBit[9]. Known for its stealth, SafePay appends a .safepay extension to encrypted files and issues ransom notes titled *readme_safepay.txt*. Researchers believe its creators may have utilised leaked LockBit source code, enhancing its capabilities. SafePay operates through a two-phase attack model: data exfiltration and encryption. Attackers archive files using WinRAR and exfiltrate them via FileZilla, removing traces post-operation. After that, using RDP and PowerShell scripts, they encrypt network shares, disable recovery systems, and demand negotiations via ominous ransom notes. Advanced features include UAC bypass, anti-analysis techniques, and a Cyrillic language-based kill switch to avoid Eastern European targets.

With a presence on TOR and TON networks, SafePay's leak site exposes stolen data and operational vulnerabilities, offering rare insights into this emerging cyber threat. The ramifications of SafePay's ransomware have already been felt in several high-profile attacks; one of the most notable of which was one on Muswellbrook Shire Council, a local government authority in New South Wales, Australia. SafePay claimed to have exfiltrated 175 GB of data from Muswellbrook Shire Council's systems, which put nearly 16,360 residents at high risk[10].

Zero-day vulnerabilities exploited in Ivanti CSA for persistent access and control

Threat research reports have highlighted the exploitation of three zero-day vulnerabilities in Ivanti Cloud Service Appliance (CSA) by a suspected nation-state adversary to carry out malicious actions[11]. These vulnerabilities include CVE-2024-8190 (command injection), CVE-2024-8963 (path traversal), and CVE-2024-9380 (authenticated command injection) and enabled unauthorised access, enumeration of users, and the theft of credentials. The attackers used the stolen admin credentials to drop a web shell maintaining persistent access and later patched the vulnerabilities to block other intruders.

The adversaries also exploited a critical flaw, CVE-2024-29824, in Ivanti Endpoint Manager (EPM) that unlocked remote code execution (RCE). This involved creating new users, performing reconnaissance, exfiltrating data using DNS tunnelling, and deploying a rootkit to ensure persistence. The severity of the threat was further underscored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) which added these vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue in October 2024.

Critical windows vulnerability requires urgent patching

Microsoft has revealed a critical zero-day vulnerability, identified as CVE-2024-43491, affecting the Servicing Stack in its Windows operating system[12]. With a severity score of 9.8, this flaw impacts Windows 10 version 1507 and certain components, causing the rollback of security patches and leaving systems exposed to previously mitigated threats. While no active exploitation has been detected, the vulnerability presents a serious risk by enabling remote code execution if left unpatched. The potential exploitation of this vulnerability could have wide-reaching consequences across various sectors, making it essential for organisations to act swiftly.

Microsoft urges all users to immediately apply the Servicing Stack update (KB5043936) and September 2024 Windows security updates (KB5043083) to secure their systems. Regular patching, alongside vigilant monitoring of system updates, is critical in preventing potential damage from this flaw.

Nitrogen malware targets organisations with innovative means

In November 2023, a BlackCat ransomware attack was traced back to Nitrogen malware hosted on a website impersonating the Advanced IP Scanner[13]. One year later, Nitrogen malware has taken on a new life, with renewed attacks on systems across the globe, estimating more than 1.8 terabytes of stolen privileged data from multiple industries[14]. A malicious ZIP file, downloaded from a fraudulent website, initiated the attack by executing Nitrogen, which deployed Sliver and Cobalt Strike beacons via Python scripts. Once inside the network, the attacker used tools like PowerSploit, SharpHound, and Impacket for lateral movement, harvesting domain credentials to expand control. They employed Restic, an open-source backup tool, to exfiltrate data from a file server to a remote server in Bulgaria.

Eight days after gaining initial access, the attacker modified a privileged user password and distributed the BlackCat ransomware across the network using PsExec and batch scripts. The ransomware was set to execute after rebooting systems into Safe Mode, leading to widespread file encryption. The entire intrusion spanned over eight days, with the ransomware deployment occurring approximately 156 hours after initial access. Six new rules were added to the Private Ruleset to address this attack.

New threat actors Earth Estries poised to wreak havoc globally

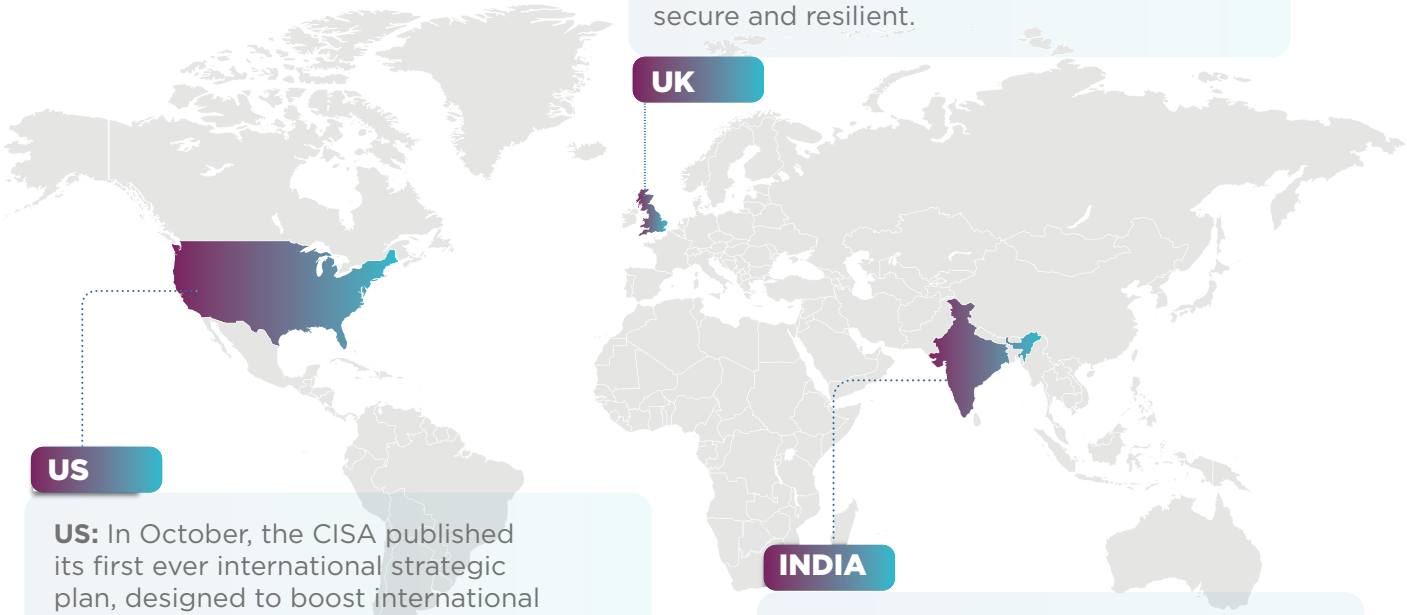
Earth Estries – an advanced threat group – has been a persistent problem since 2023 but has ramped up its operations in big ways in Q3 2024, having successfully compromised more than 20 major global organisations in industries that include telecommunications, technology, consulting, chemical, transportation, government agencies, and non-profit organisations (NGOs)[15]. The entity employs two distinct attack chains targeting governments and the tech industry, with both chains exploiting vulnerabilities in systems like Microsoft Exchange servers and adapter management tools, showcasing technical sophistication and adaptability. The first chain uses CAB-delivered tools like Cobalt Strike, Hemigate, and Crowdoor for lateral movement via PsExec, with Trillclient harvesting credentials from browser caches[16]. The second chain leverages malware like Zingdoor and SnappyBee, delivered through cURL, alongside web shells and DLL sideloading to maintain persistence and escalate privileges.

Earth Estries combines advanced tools, strategic exploitation, and a deep understanding of target environments to maintain prolonged access. Defenders should focus on securing external-facing systems, patching vulnerabilities, and implementing robust credential management to mitigate such sophisticated threats.

Important government cybersecurity advisories - Q3 2024

- Q2 2024

UK: In September, the UK Department of Science, Innovation and Technology announced that the Cyber Security and Resilience Bill will be introduced to Parliament in 2025[18]. Its aim is to strengthen the UK's cybersecurity and ensure that critical infrastructure and digital services are secure and resilient.



US: In October, the CISA published its first ever international strategic plan, designed to boost international cooperation in combatting cyber threats to critical infrastructure[19]. Set to be implemented for the year 2025-2026, the plan acknowledges the complex and geographically dispersed nature of cyber risks, and the need for threat information and risk reduction advice to be shared rapidly with international partners.

India: In September, the Computer Emergency Response Team (CERT-In) issued an advisory on multiple vulnerabilities have been identified in Microsoft products[17]. These vulnerabilities could potentially allow attackers to gain privileged access, bypass security restrictions to obtain sensitive information, and cause a variety of code executions and DDoS attacks.

More than meets the eye: cyberespionage dominates the landscape

Cyberespionage has taken a front seat with nation-state actors deploying sophisticated malware and backdoors in Q3 2024. Driven by a variety of factors, including emerging techniques, targeted sectors, and the rise of advanced persistent threats (APTs); these campaigns have become increasingly stealthier and more precise, highlighting the growing focus on gathering sensitive information rather than immediate financial gain.

Unique extraction techniques:

iOS devices have become a ripe target with the prevalence of mobile surveillance-ware developed by APT groups from China and Russia. These tools are designed to collect sensitive data, including location tracking and communication interception, directly from the victim's mobile devices. This dangerous shift is given further credence by research that highlights a 17% increase in enterprise-targeted threats of this nature compared to Q2, with an additional 32% increase in the number of malicious apps being found on iOS devices[20].

Ransomware's role:

Ransomware, the perennial threat, has also been linked as the most frequently documented method tied to cyberespionage cases, being a favourite for criminal groups who seek to exploit vulnerabilities in different industries. Often, legacy systems and a lack of robust cybersecurity measures open more avenues for criminals to leverage ransomware. This is becoming more prevalent with industries that still maintain a more archaic approach to cybersecurity, with sectors like the construction industry marking a 7.8% increase in cybersecurity breaches from the previous quarter[21].

Priority targets:

The healthcare sector has been particularly targeted due to its critical nature and the sensitive data it holds. In Q3 2024, healthcare organisations witnessed a 12.8% increase in cyberattacks, with 53 victims reported compared to 47 in the previous quarter[22]. This trend underscores how cybercriminals are homing in on organisations with valuable data, particularly during times when such entities are focused on service delivery amidst challenges posed by inadequately secured legacy technologies.

Avant-garde intelligence: the rise of AI-generated malware

AI-generated malware represents a significant threat due to its sophisticated characteristics, which enhance its evasion capabilities and attack effectiveness. Simply put, this is malicious software that leverages artificial intelligence techniques, allowing it to autonomously adapt and improve its methods, making detection and prevention more difficult than traditional malware.

The quantum of impact due to AI-generated malware varies across industries. The total cost of cybercrime is projected to exceed $10.5 trillion globally by 2025, reflecting the growing economic burden of these threats. In the healthcare sector alone, the cumulative cost of data breaches has reached an average of $4.88 million per incident as of 2024, exacerbated by incidents involving AI-generated attacks23.

Closer home, the India Cyber Threat Report 2025 by DSCI has revealed a rapidly evolving cyber threat landscape in India24. With 369 million malware detections across 8.44 million endpoints, the nation faced average of 702 potential threats per minute, highlighting the growing sophistication and volume of cyberattacks, with AI-generated malware being a significant threat both currently and going forward.

To this end, understanding the key characteristics that make AI-generated malware such a prominent threat is critical for developing robust cybersecurity measures that are robust enough to face this terrifying new generation of cyber threats:

Autonomous adaptation:

AI-generated malware can learn from its environment and adjust its behaviour in real-time based on the defences it encounters. This dynamic adaptability allows it to modify its attack vectors, increasing its resilience against standard protective measures.

Advanced impersonation:

A concerning feature of AI malware is its ability to mimic existing threat actors and recognised malware families with high accuracy. By training on open-source intelligence and past malware campaigns, it can generate malicious code that closely resembles known threats, which can complicate attribution and mislead security teams.

Polymorphic behaviour:

AI malware often exhibits polymorphic traits, enabling it to continuously alter its code structure. Each infection or replication may result in a different variant that can evade traditional signature-based detection systems. This feature overwhelms security tools with numerous variants that perform similar malicious actions.

Obfuscation techniques:

To evade detection, AI-generated malware employs sophisticated obfuscation methods, including payload encryption, dead code insertion, and instruction substitution. These techniques conceal the true functionality of the malware, complicating the analysis and response from cybersecurity experts.

Real-time decision-making:

AI-generated malware can execute decisions in real time, adjusting its attack vectors as necessary. Its ability to analyse the environment enables it to adjust its tactics on-the-fly, thereby maintaining the effectiveness of its malicious activities throughout the attack.

Dynamic malware payloads:

Such malware can modify its actions or load additional malware during an attack. This adaptability ensures that the attack remains undetected and effective against security measures in place, creating complex chains of attacks that evolve based on the response from security systems.

Enhanced social engineering:

AI-generated malware can produce highly personalised phishing emails, utilising data collected from various sources to craft messages that appear tailored to individuals. This increases the success rate of phishing attempts, as the emails often reference specific details relevant to the targets, making them more convincing.

Zero-day exploit capabilities:

AI accelerates the discovery of vulnerabilities and the creation of exploits. This capability allows attackers to launch attacks quickly, often targeting previously unknown bugs within systems and software before they can be patched.

Lessons from Q3 – 10 key takeaways for future resilience

Train for advanced phishing detection:

Train employees to recognise sophisticated phishing tactics, particularly those mimicking legitimate job offers. This can prevent initial access and safeguard high-value sectors like aerospace and energy.

Stay agile with AI-driven threat systems:

Implement advanced threat detection systems with AI-driven behavioural analysis to identify and mitigate espionage-focused attacks like SnipBot before they exfiltrate sensitive data.

Stay secure with constant updates:

Regularly update and patch all software and devices, focusing on known vulnerabilities to minimise exposure to zero-day exploits and prevent credential theft.

Boost endpoint detection:

Employ robust endpoint detection and response (EDR) solutions to monitor lateral movements within networks. This ensures early detection of ransomware campaigns like Interlock before significant damage occurs.

Strengthen email security with smarter filtering:

Strengthen email security and enforce strict filtering of attachments and links to reduce risks from phishing-delivered malware like Emansrepo.

Master patch management for critical protection:

Develop a comprehensive patch management process that prioritises critical vulnerabilities (e.g., CVE-2024-23113). Ensure timely updates to protect against severe risks like remote code execution.

Monitor for hidden threats in real time:

Monitor for indicators of compromise (IOCs) tied to persistent access techniques, such as unauthorised user enumeration and DNS tunnelling, to quickly address exploitation of vulnerabilities.

Ensure security with regular system audits:

Conduct regular system audits to identify unpatched systems and enforce compliance with security updates, especially for high-severity vulnerabilities like CVE-2024-43491.

Fortify supply chains against cyberattacks:

Bolster supply chain security by scrutinising third-party software and downloads, as malware like Nitrogen leverages impersonated tools to gain initial access.

Expedite incident response for quick action:

Enhance incident response protocols to address zero-day vulnerabilities quickly and mitigate unauthorised access to sensitive configuration data, even before public disclosures.

Our top 5 recommendations

The dynamic nature of cybersecurity threats and their exploitation of innovative vulnerabilities underscore the importance of a holistic approach to threat mitigation. By implementing these frameworks, enterprises can establish a robust, adaptive, and comprehensive cybersecurity framework to address current and emerging threats effectively. Tata Communications is committed to this all-encompassing approach to cybersecurity, and with the insights gained Q3's major cybersecurity incidents, they recommend five key recommendations that enterprises can imbibe:

Shore up against phishing attempts:

Phishing remains a primary vector for many threats, including UNC2970's backdoor and Emansrepo. Enterprises should invest in continuous employee training to recognise phishing attempts and deploy advanced email filtering solutions to detect and block malicious content.

Proper patching prevents poor performance:

Critical vulnerabilities, such as those in Fortinet products, Ivanti CSA, and Windows products, highlight the importance of timely patching. Enterprises should adopt automated patch management systems, conduct regular vulnerability assessments, and ensure rapid deployment of updates to minimise exposure to zero-day threats.

Advanced threat detection that weeds out new risks:

Threats like SnipBot, Interlock ransomware, and Nitrogen malware leverage stealthy and advanced techniques to infiltrate systems. Implementing AI-driven detection systems, endpoint detection and response (EDR) solutions, and network monitoring tools can help identify unusual activities and mitigate threats in real time.

Master recovery with rock-solid incident response systems:

Sophisticated attacks like BlackCat ransomware and BrazenBamboo's Fortinet exploit demonstrate the necessity of having a well-defined incident response plan. Regularly updating, testing, and simulating responses ensures teams are prepared to contain breaches and minimise damage effectively.

Reinforce supply chain security and third-party access:

Many threats exploit vulnerabilities in third-party tools or external-facing systems, as seen in the Nitrogen malware incident and tactics used by Earth Estries. Enterprises should enforce stringent access controls, conduct regular security audits of third-party vendors, and require compliance with security best practices to safeguard against supply chain attacks.

Sources: Tata Communications Threat Intelligence and Research

1 SC Media UK | 2 Checkpoint | 3 Security Online | 4 Unit 42 by Palo Alto Networks | 5 Hacker News Cybersecurity News | 6 Bleeping Computer | 7 Talos Intelligence | 8 Fortinet | 9 Security Online | 10 Halcyon | 11 Fortinet | 12 Security Online I 13 The DFIR Report | 14 Halcyon | 15 Trend Micro | 16 Trend Micro | 17 CERT-IN | 18 Skadden | 19 Infosecurity Magazine | 20 Lookout | 21 Corvus Insurance | 22 CERT-IN | 23 Cobalt | 24 Seqrite

For more information, click here

CONTACT US