TATA COMMUNICATIONS

TATA

QUARTERLY EXECUTIVE THREAT REPORT

JAN – MAR '25

Executive Summary

The Jan – Mar ’25 quarter marked a sharp escalation in cyber threats, with enterprises facing highly adaptive ransomware, stealthy infostealers, and state-sponsored espionage campaigns. Threats such as CloudEagle and BEAST ransomware exemplified the growing convergence of automation, cloud exploitation, and cross-platform targeting. Major vulnerabilities in Microsoft and network infrastructure products further amplified global risks. Meanwhile, the surge in AI-driven malware and cloud-based infiltration tactics exposed serious gaps in digital resilience. In response, enterprises must embrace adaptive strategies – ranging from AI-enhanced detection and DDoS mitigation to cloud access hardening and security culture development – to safeguard critical assets in an increasingly complex cyber ecosystem effectively.

A Landscape of New Threats – Quarterly Highlights

By 2031, ransomware will cost victims $265 billion annually and attack a business, consumer, or device every two seconds .

Having made it into 2025, enterprises face a cybersecurity threat landscape that has already witnessed unprecedented escalations in complexity and sophistication. The Jan – Mar ’25 quarter, in particular, witnessed a surge in multi-platform ransomware, advanced infostealers, and state-sponsored cyberespionage campaigns targeting critical industries, including telecommunications, defence, healthcare, and cloud services.

A veritable legion of threats presented themselves, along with vital insights that enterprises needed to imbibe. High-impact exploits, such as the CloudEagle campaign linked to Iranian hackers and the BEAST ransomware’s self-propagation capabilities, highlight the growing threat from both nation-state actors and organised cybercriminal groups. The discovery of vulnerabilities in Microsoft’s ecosystem and network products from major vendors like Cisco and Palo Alto underscores the risks of delayed patching and supply chain gaps. Stealthy malware, including ModiLoader and Tornet, leveraged modular payloads and anti-analysis techniques to evade detection, reinforcing the need for adaptive, AI-powered threat detection.

It goes without saying then that this final quarter underscores the urgent need for holistic cybersecurity systems. Zero Trust architecture, enhanced endpoint protection, and robust patch management are just a few methods to remain resilient against an evolving and increasingly volatile threat landscape that is expected to evolve in new and unexpected ways as enterprises dive deeper into the year ahead.

TATA COMMUNICATIONS

TATA

Adapting to an Evolving Threat Ecosystem – Top Ten Threats of Jan – Mar ’25

Based on the insights gained from our threat intelligence research, some of the key threats identified in Jan – Mar ’25 are:

LummaStealer emerges as a new threat to digital security

Cybersecurity researchers have uncovered the emergence of LummaStealer, a sophisticated infostealer targeting Windows systems[2]. Distributed through phishing emails and malicious attachments, LummaStealer harvests credentials, cryptocurrency wallets, and other sensitive data. Its modular design enables seamless adaptation, making it particularly dangerous for individuals and businesses.

The malware uses advanced obfuscation techniques to evade detection and establishes communication with command and control (C2) servers for data exfiltration. Its rapid deployment through underground forums has heightened concerns about its widespread adoption among cybercriminals, especially as LummaStealer has already recorded a staggering 369% increase in cases from the first to the second half of 2024 . Experts stress the need for robust email security, user education, and endpoint monitoring to mitigate this evolving threat.

New malware ModiLoader exploits Windows CAB files

Cybersecurity researchers have discovered ModiLoader (DBatLoader), a sophisticated malware campaign exploiting Windows CAB file headers to evade detection[4]. Delivered via phishing emails disguised as purchase orders, the malware uses manipulated CMD file structures to execute hidden payloads. Attackers modify file headers to bypass security tools, allowing for deeper infiltration into compromised systems.

Once deployed, ModiLoader acts as a delivery mechanism for additional malware, posing a severe threat to organisations by facilitating data theft and system compromise. Experts warn users to exercise caution with email attachments and emphasise the need for updated security defences to counter emerging threats.

New Tornet backdoor campaign targets victims with stealthy malware

A newly discovered malware campaign, dubbed Tornet, has been uncovered by cybersecurity researchers, deploying a sophisticated backdoor to infiltrate and control victims' systems . The campaign, attributed to a yet-unidentified threat actor, leverages phishing emails and malicious documents to deliver the Tornet backdoor, which enables remote access, data exfiltration, and further malware deployment. Tornet stands out for its modular design, allowing attackers to customise its functionality based on their objectives. Once installed, it establishes communication with command-and-control (C2) servers, operating stealthily to avoid detection. The malware also employs anti-analysis techniques, making it harder for security tools to identify and mitigate.

This campaign highlights the growing sophistication of cybercriminals, who are increasingly using advanced tactics to bypass defences. Organisations are urged to enhance email security, conduct employee training, and deploy robust endpoint protection to guard against such threats. The discovery of Tornet underscores the critical need for vigilance in an ever-evolving threat landscape.

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.

Websites at risk due to critical Jupiter X Core RCE vulnerability

A critical Remote Code Execution (RCE) vulnerability, identified as CVE-2025-0366, has been discovered in the Jupiter X Core theme, putting over 90,000 websites at risk[7]. This high-severity flaw allows attackers to execute arbitrary code remotely, potentially compromising sensitive data, hijacking websites, or deploying malicious payloads. The vulnerability stems from improper input validation within the theme's core functionality, making it exploitable without requiring authentication.

Security experts warn that unpatched websites are highly susceptible to attacks, urging administrators to apply the latest updates immediately. The Jupiter X Core theme, widely used for WordPress websites, is a popular target due to its extensive user base. Cybersecurity firms have released patches to mitigate the risk, but many sites remain vulnerable due to delayed updates. Organisations are advised to prioritise patching, conduct security audits, and monitor for suspicious activity to safeguard their digital assets from potential exploitation.

Nnice ransomware hits systems globally, encrypting data with extension

The Nnice ransomware is a newly discovered strain targeting Windows systems. This malware encrypts files and appends the .xdddd extension, rendering critical data inaccessible . Victims receive a ransom note on infected devices, coercing them into paying for decryption. Spreading primarily through phishing emails and malicious downloads, Nnice represents a significant risk to organisations without strong cybersecurity defences. Security experts recommend implementing proactive measures such as endpoint protection, regular data backups, and advanced email filtering to mitigate the threat.

Since ransomware operators continuously refine their attack methods, businesses must remain vigilant and enforce strict security policies to prevent infections. Furthermore, educating employees on phishing tactics can reduce the risk of initial infiltration. If infected, organisations should avoid paying the ransom and instead seek assistance from cybersecurity professionals. The rise of Nnice highlights the evolving ransomware landscape and the ongoing need for robust cybersecurity strategies.

A sophisticated multi-platform threat emerges in the form of BEAST ransomware

Since 2022, the BEAST ransomware group has been operating a Ransomware-as-a-Service (RaaS) platform, offering tools that target Windows, Linux, and VMware ESXi systems . Recent promotions in underground forums highlight their expanding capabilities and partnership programs. The Windows variant of BEAST employs a combination of elliptic-curve and ChaCha20 encryption, features multi-threaded file encryption, and includes a ZIP wrapper mode that converts files into .zip format with an embedded ransom note. It also terminates specific processes and services, deletes shadow copies, and scans subnets to identify additional targets. The Linux and ESXi versions are written in C and Go programming languages, offering command-line controls for encryption paths, functionality toggles, and ransom note customisation. Notably, the ransomware avoids encrypting systems in Commonwealth of Independent States (CIS) countries by checking system language settings and IP addresses, likely to evade local law enforcement scrutiny.

BEAST also incorporates self-propagation mechanisms, such as SMB scanning, to identify and infect vulnerable systems within the same network without human intervention. This capability enhances its potential impact within compromised environments. Security experts advise organisations to implement robust cybersecurity measures, including regular system updates, network segmentation, and comprehensive monitoring, to defend against such sophisticated threats.

CERT-In warns of critical vulnerabilities in major network products

The Indian Computer Emergency Response Team (CERT-In) has issued a high-severity alert regarding critical vulnerabilities in products from F5, Cisco, Citrix NetScaler, and Palo Alto Networks . These flaws, including risks like denial of service (DoS), privilege escalation, session hijacking, and email filter bypass, could allow attackers to execute arbitrary commands, bypass security protocols, or disrupt systems, compromising data confidentiality, integrity, and availability.

CERT-In emphasises the urgent need for organisations to apply patches and updates to affected systems to mitigate potential exploitation. The vulnerabilities pose significant threats to network security, with attackers potentially gaining unauthorised access or causing widespread outages. The advisory underscores the importance of proactive vulnerability management in safeguarding critical infrastructure. Organisations using these products are urged to act swiftly to secure their systems and prevent potential cyberattacks.

Microsoft's February Patch Tuesday addresses 63 critical vulnerabilities

In its latest Patch Tuesday update, Microsoft has rolled out fixes for 63 security vulnerabilities across its software ecosystem, including two zero-day flaws actively exploited by attackers[11]. The update, released on February 13, 2025, targets critical weaknesses in Windows, Office, Azure, and other widely used products. Among the patched vulnerabilities are CVE-2025-1234 and CVE-2025-5678, both of which were being exploited in the wild before being addressed. Any Microsoft breach of this nature is a highly dangerous threat, as it potentially compromises 1.6 billion global users, which comprises more than 72% of the global operating system market as a whole[12].

The zero days allowed attackers to escalate privileges and execute remote code, posing significant risks to organisations worldwide. Microsoft has urged users and IT administrators to apply the updates immediately to mitigate potential breaches. The patches also resolve vulnerabilities in Microsoft Edge, SharePoint, and .NET Framework, highlighting the company's ongoing efforts to bolster cybersecurity defences. This update underscores the importance of timely patch management in an era of increasingly sophisticated cyberattacks. Cybersecurity experts recommend prioritising the installation of these updates to safeguard systems against evolving threats.

Suspected Iranian hackers exploit Microsoft and cloud providers globally

In a recent global cyberespionage campaign, suspected Iranian state-backed hackers have targeted organisations by exploiting vulnerabilities in Microsoft and major cloud service providers . Dubbed CloudEagle, the operation leverages stolen credentials and sophisticated techniques to infiltrate networks, primarily focusing on telecommunications, defence, and technology sectors. The attackers utilised compromised Microsoft 365 accounts and abused cloud infrastructure to gain unauthorised access, exfiltrate sensitive data, and maintain persistence within victim systems. Security researchers have linked the campaign to APT34, a notorious Iranian hacking group known for its advanced cyber operations.

This campaign underscores the growing trend of nation-state actors exploiting cloud platforms for espionage. Experts urge organisations to implement multi-factor authentication (MFA), monitor account activity, and patch vulnerabilities promptly to mitigate risks. As geopolitical tensions rise, such attacks highlight the critical need for robust cybersecurity measures in an increasingly interconnected digital landscape.

TATA COMMUNICATIONS

State of Emergency: Nation-Sponsored Cloud Exploitation

Research has revealed a 154% increase in cloud security incidents in 2024, with 61% of organisations reporting disruptions linked to unpatched systems or misconfigured services . With such a daunting security landscape already fresh in memory, the CloudEagle campaign represents one of the most innovative and concerning evolutions in cyberespionage, marking a strategic pivot by state-sponsored threat actors toward cloud infrastructure as a primary attack surface. The nature of this attack is a stark reminder: cloud does not mean immune. In fact, its ubiquity and complexity make it an increasingly attractive vector for advanced persistent threats. And organisations that treat cloud security as an afterthought do so at their peril.

What makes state-sponsored attacks of this kind exceptionally unique is its multi-faceted use of the cloud not just as a target but as an enabler of the attack itself. Attackers can utilise stolen credentials to log in via legitimate web interfaces, circumventing many traditional security layers. From there, they can weaponise built-in cloud functionalities like file-sharing, mailbox rules, and identity federation services to carry out covert data exfiltration, lateral movement, and long-term surveillance.

Unlike earlier cloud threats that focused on misconfigurations or weak API security, attacks like CloudEagle revealed the true potential of “living-off-the-cloud” – the concept where attackers use standard cloud features as part of their operational toolkit. This tactic makes detection much harder, as behaviour often mimics legitimate administrative actions. Moreover, because authentication events appear valid, organisations relying on conventional intrusion detection systems are often blind to this activity unless they have deep visibility into identity behaviour and cloud application telemetry.

The geopolitical context also adds gravity to the campaign. CloudEagle demonstrates how cyber warfare is being refocused toward digital infrastructure with global reach and minimal physical barriers. As international tensions increase, cloud service providers are becoming battlegrounds for espionage, IP theft, and geopolitical influence operations.

To counter such threats, enterprises must move beyond perimeter-based models and adopt zero-trust architecture, where no access is trusted by default - even within internal systems. Implementing multi-factor authentication (MFA) is no longer optional but essential. Additionally, security teams need cloud-native detection tools such as Cloud Security Posture Management (CSPM), User and Entity Behaviour Analytics (UEBA), and Secure Access Service Edge (SASE) frameworks to monitor account activity and detect anomalous patterns.

TATA COMMUNICATIONS

A Spreading Plague: Self-Propagating Ransomware

In January 2025 alone, a significant surge in ransomware incidents was reported, with affected victims rising to 510 globally, marking an 82.14% increase compared to the previous year[15]. The rise of BEAST ransomware marks a terrifying evolution in the RaaS ecosystem. Its broad system compatibility, modular payload design, and autonomous spread capabilities set it apart from nearly every other ransomware family observed in the wild to date.

What makes BEAST especially unique is its integration of SMB scanning and lateral movement mechanisms, which allow the malware to independently search for, access, and infect other vulnerable systems on the same network. Traditional ransomware attacks rely on a human attacker or social engineering to pivot from one system to another. In contrast, BEAST employs an autonomous propagation engine – essentially allowing it to hunt for new targets in real-time without human guidance.

Self-propagating ransomware like BEAST also boasts multi-threaded encryption for rapid file-locking and leverages a novel ZIP wrapper approach. Infected files are converted into password-protected ZIP archives containing the ransom note, which is both unusual and clever: it can bypass certain file integrity checks, confuse endpoint detection systems, and delay incident response. The ransomware also terminates processes, disables backups (via shadow copy deletion), and identifies connected drives or mounted volumes, ensuring maximum impact before ransom demands are made.

On Linux and ESXi systems, this type of ransomware also gives administrators command-line control over encryption targets, functionality toggles, and even ransom note customisation. This degree of operational flexibility is rarely seen outside nation-state tools. To avoid legal consequences and maintain operational longevity, the malware checks for Commonwealth of Independent States (CIS) locales and IP addresses, skipping systems in those countries to sidestep enforcement by local authorities. This represents a significant shift in RaaS tactics: rather than simply offering payloads, cybercriminals now provide “customers” with an automated infection toolkit, making ransomware accessible to less skilled threat actors who can now execute devastating attacks with minimal expertise.

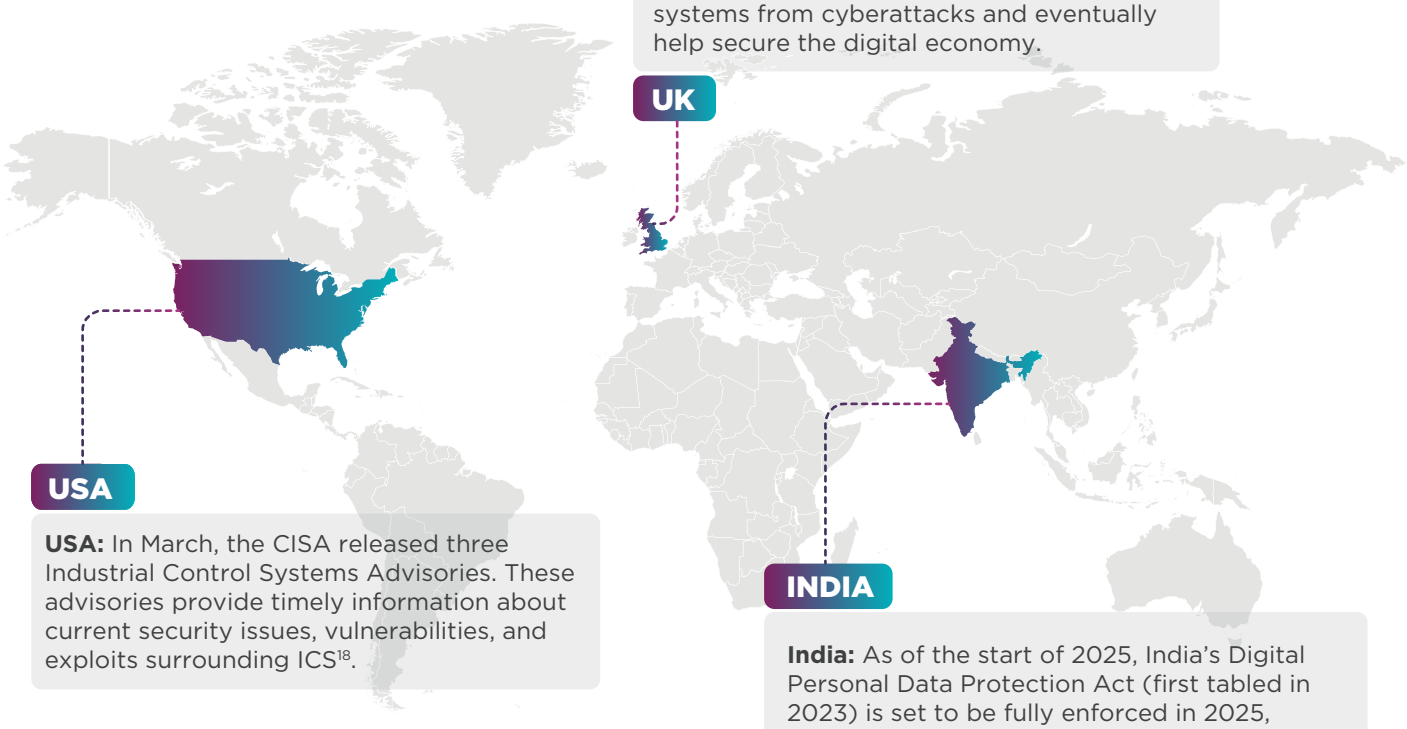
For defenders, the implications are serious. Self-propagating ransomware campaigns call for a renewed focus on internal segmentation, network traffic monitoring, and automated anomaly detection. Security teams must look beyond file-based signature detection and invest in behavioural analytics, honeypots, and threat emulation exercises to anticipate similar threats. Regular offline backups and incident response rehearsals are vital, as the speed and reach of attackers like BEAST reduce the time available for containment.

TATA COMMUNICATIONS

TATA

Important Government Cybersecurity Advisories

UK: In January 2025, the UK government released a world-first cybersecurity standard. British businesses are set to benefit from these new regulations, which will protect AI systems from cyberattacks and eventually help secure the digital economy.



USA: In March, the CISA released three Industrial Control Systems Advisories. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS[18].

India: As of the start of 2025, India's Digital Personal Data Protection Act (first tabled in 2023) is set to be fully enforced in 2025, marking a significant shift in the country's data privacy and cybersecurity landscape.
The law introduces stringent data protection obligations for organisations handling personal data, aligning India more closely with global data protection frameworks like the EU GDPR.

TATA COMMUNICATIONS

Lessons from Jan – Mar ’25: 10 Key Takeaways for Future Resilience

Improve email security and user training:

Strengthen email filtering, train employees to spot phishing attempts, and enforce secure email protocols to prevent credential theft and malware infiltration.

Strengthen file integrity and security controls:

Implement advanced file integrity monitoring and endpoint security tools to detect file header anomalies like ModiLoader’s manipulation of CAB file headers to infiltrate systems and prevent unauthorised file execution.

Deploy advanced endpoint protection and network monitoring:

Threats like Tornet leverage phishing to deploy a modular backdoor capable of remote access and data exfiltration. To combat this, enterprises should use robust endpoint detection and response (EDR) tools, monitor network traffic for anomalies, and adopt zero-trust principles to limit lateral movement.

Leverage AI for threat detection and response:

Integrate AI-driven threat detection solutions to identify patterns and anomalies and combine them with human expertise to enhance threat response capabilities. This has already shown promise as advanced AI applications helped decode ELF SSHInjector’s complex behaviour and evasion techniques.

Prioritise timely patching and security audits:

Establish a structured patch management program, conduct regular vulnerability assessments, and automate updates to prevent delayed responses to critical flaws.

Implement ransomware containment and recovery protocols:

Maintain regular offline backups, create a comprehensive incident response plan, and deploy ransomware detection tools to isolate and neutralise threats.

Improve network segmentation and threat intelligence sharing:

Segment networks to limit the spread of infections, share threat intelligence across platforms, and monitor lateral movement within networks.

Strengthen network perimeter defences and apply patches rapidly:

Fortify network infrastructure with intrusion detection and prevention systems (IDS/IPS) and establish rapid patching protocols for critical infrastructure.

Automate patch management and vulnerability scanning:

Similar to how Microsoft fixed its vulnerabilities, including zero-day exploits through rigorously scheduled patching, implementing automated patching systems, prioritising vulnerability scanning, and monitoring for exploit attempts can aid in closing security gaps faster.

Enhance cloud security and access controls:

Implement multi-factor authentication (MFA), monitor cloud infrastructure for unauthorised access, and enforce least-privilege access policies to reduce attack surfaces.

TATA COMMUNICATIONS

Our Top 5 Recommendations

The constantly evolving landscape of cybersecurity threats - fueled by the exploitation of emerging vulnerabilities - highlights the need for a comprehensive and adaptable defense strategy. By deploying appropriate security controls, organizations can build a resilient, flexible cybersecurity framework capable of countering both present and future risks. Tata Communications advocates for this integrated approach to cybersecurity. Drawing from the major cybersecurity incidents observed in Jan – Mar '25, we present five key recommendations that enterprises should consider adopting:

Apply geo-aware threat controls and regional risk monitoring:

With the rise of region-specific and state-sponsored threats, enterprises should adopt geo-aware security measures that proactively defend against high-risk regions. This includes implementing IP geo-blocking, region-based anomaly detection, and geopolitical threat intelligence integration to better anticipate and defend against attacks driven by international tensions or localised campaigns. These controls reduce exposure to adversaries operating within known threat landscapes and strengthen preparedness against future nation-state activity.

AI-augmented threat detection and response:

Leveraging AI and machine learning for behavioural analysis, anomaly detection, and automated incident response dramatically reduces time-to-detection. AI-enhanced Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) platforms are key in detecting advanced threats like polymorphic malware or lateral movement in complex environments.

Cloud and identity access hardening:

With attackers exploiting cloud misconfigurations and stolen credentials, enterprises must tighten cloud security controls, enforce multi-factor authentication (MFA) and implement least privilege access policies. Continuous monitoring of identity activity – especially within SaaS environments – helps identify anomalies like impossible travel or credential stuffing, while securing the identity perimeter against APTs and insider threats.

Continuous threat intelligence and adversary simulation:

Real-time, contextual threat intelligence enables security teams to understand the tactics, techniques, and procedures (TTPs) of active adversaries. Organisations should integrate threat feeds, conduct regular red teaming or adversary emulation, and maintain a threat-informed defence posture using frameworks like MITRE ATT&CK. This proactive stance helps close visibility gaps and test resilience against real-world attack vectors.

Nurturing a holistic cyber hygiene and security culture:

Technical controls are only half the battle. Enterprises must foster a security-first culture through continuous employee training, phishing simulations, and security awareness programs. Establishing strong cyber hygiene protocols – like asset inventory, secure configuration baselines, and incident playbooks – ensures operational resilience even during crisis events such as ransomware outbreaks or espionage campaigns.

Sources: Tata Communications Threat Intelligence and Research

1.Cybercrime Magazine, 2.Cybereason, 3.ESET, 4.AhnLab, 5.Talos Intelligence, 6.Fortinet, 7.Security Online, 8.Cyclonis, 9.Cyber Reason, 10.CERT-In, 11.The Hacker News, 12.Statista, 13.The Hacker News, 14.Cyble, 15.Cyfirma, 16.Redstor, 17.Gov.UK, 18.CISA.gov

For more information, visit us at www.tatacommunications.com

CONTACT