TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 30, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As June 2026 has come to an end, the cyber threat landscape shows no sign of abating, with threat actors deploying increasingly sophisticated and coordinated tactics across highly interconnected digital environments. Conventional defence models continue to be tested as adversaries exploit systemic vulnerabilities at scale. Organisations must reinforce foundational security controls, adopt layered defence strategies, and embed forward-looking intelligence into operational frameworks to sustain resilience and competitive advantage.

Against this backdrop, the Tata Communications Cyber Threat Intelligence report remains an essential resource for security practitioners. Published weekly, it delivers incisive analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By translating intelligence into actionable defence guidance, it equips security teams to anticipate, respond to, and mitigate threats effectively, safeguarding the continuity of critical operations at scale.

TATA COMMUNICATIONS

Oracle’s June update fixes flaws across middleware, database, and enterprise applications

A remote attacker could exploit several of the vulnerabilities to trigger sensitive information disclosure, data manipulation, remote code execution, security restriction bypass, elevation of privilege, and denial-of-service conditions on affected systems. Impacted technologies span Oracle Communications, E-Business Suite, Fusion Middleware, JD Edwards, MySQL, PeopleSoft, Siebel CRM, Oracle Systems, and Oracle Virtualization, underscoring the update's broad enterprise reach.

Notably, CVE-2026-35273 is being actively exploited in the wild. An unauthenticated attacker with network access via HTTP may compromise PeopleSoft Enterprise PeopleTools, with successful attacks resulting in full takeover of the platform. The flaw has since been added to the CISA Known Exploited Vulnerabilities catalogue, and organisations are strongly urged to apply Oracle's fixes without delay.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Oracle Solaris, Oracle Application Server, Oracle Identity Management, Oracle PeopleSoft Enterprise, Oracle VM VirtualBox, Oracle WebCenter Sites, Oracle WebLogic Server

Source - https://www.hkcert.org/security-bulletin/oracle-products-multiple-vulnerabilities_20260617

TATA COMMUNICATIONS

Vidar infostealer bypasses Chrome ABE via memory scanning and APC injection

Documented by ThreatLabs, recent Vidar versions now ship weekly updates, combining process forking, memory pattern scanning, and APC injection to extract Chrome's master decryption key directly from live memory. Because ABE binds the v20_master_key to the browser process, attackers reading the key from memory cannot decrypt it outside the browser's process context, a barrier Vidar circumvents by operating within that context.

Vidar creates a silent, threadless browser fork using NtCreateProcessEx, producing a frozen memory snapshot that avoids triggering execution or alerting security tools. Parallel worker threads then scan thousands of memory regions for a specific byte pattern matching Chromium's internal KeyRing structure. To erase forensic traces, Vidar subsequently re-encrypts the key, restoring the browser's original state.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Chromium, Google Chrome

Source - https://cyberpress.org/vidar-malware-bypasses-chrome-encryption/

TATA COMMUNICATIONS

The Gentlemen weaponises EDR-killer ecosystem drivers to dismantle endpoint security

According to researchers, the most frequently used tool in the suite is a custom utility named GentleKiller, which has at least eight variants that impersonate legitimate products including Kaspersky, Valorant, Javelin, and WatchDog. Each variant leverages different vulnerable drivers to achieve kernel-level privileges, yet shares common strings, identical obfuscation techniques, and similar process-killing logic, enabling rapid driver swaps without major code changes.

GentleKiller targets more than 400 processes associated with approximately 48 security vendors, including Microsoft, CrowdStrike, SentinelOne, Palo Alto, Sophos, and Trend Micro. Its binaries are protected using the commercial Enigma and Themida packing tools, alongside stolen, though invalid, digital signatures. The collection further incorporates three external killers — HexKiller, ThrottleBlood, and HavocKiller — likely added for redundancy.

ATTACK TYPE	Ransomware	**SECTOR**	BFSI, Manufacturing, Government, Education, Retail and Distribution, Telecommunications
REGION	South America, Europe, South Asia	**APPLICATION**	Microsoft Windows Defender, Windows

Source - https://www.bleepingcomputer.com/news/security/gentlemen-ransomware-uses-multiple-edr-killers-to-disable-defenses/

Rust-based rewrites and migrating affiliates drive INC ransomware's rapid expansion

The disruption of LockBit and the shutdown of BlackCat created opportunities for INC to expand as affiliates migrated to alternative ransomware operations. Both the Windows and Linux/ESXi encryptors have been rewritten in Rust, enabling cross-platform development while increasing analysis complexity. Following the 2024 sale of its source code, related families such as Lynx and Sinobi emerged with significant code overlap.

United States organisations account for more than 65% of listed victims, with legal services, manufacturing, construction, technology and health care among the most targeted sectors. Affiliates gain initial access through spear phishing, broker-supplied credentials and exploitation of public-facing applications, then deploy a modified Veeam credential dumper supporting the newer salted DPAPI encryption method used by modern deployments.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Legal services, Manufacturing, Construction, IT, Education
REGION	Australia, Canada, Global, Germany, Taiwan, United States	**APPLICATION**	Apple macOS, 7-Zip, AnyDesk, Citrix NetScaler, Windows, Linux, FortiGate EMS/SPP, TeamViewer, Veeam, FortiClient EMS, SimpleHelp RMM

Source - https://www.acronis.com/en/tru/posts/from-emerging-threat-to-top-tier-ransomware-as-a-service-the-evolution-of-inc-ransomware/

TATA COMMUNICATIONS

Mailbombing and fake support calls deliver Deno-based RAT that evades detection

The attack began with mailbombing, flooding a targeted employee's inbox with hundreds of emails to create panic. The attacker then called over Microsoft Teams from an external account mimicking internal IT support, using names and company context likely sourced from LinkedIn to build credibility. The victim was directed to a fake self-service portal and instructed to extract a file into AppData.

The implant was split across four heavily obfuscated JavaScript files, each handling orchestration, command and control, local execution, or network pivoting. By exploiting Deno's permission model, every module requested only what it needed, so no single process appeared suspicious. The C2 server sat behind a CloudFront domain, disguising outbound traffic as legitimate content delivery network activity.

ATTACK TYPE	Phishing, Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Windows Defender, Microsoft Teams

Source - https://cybersecuritynews.com/hackers-use-rokarolla-android-malware/

TATA COMMUNICATIONS

Open directory exposes inner workings of FortiBleed credential cracking operation

Despite its name, FortiBleed is not a software vulnerability or zero-day, but rather a verified dataset of working device credentials assembled through reuse, brute force, and offline hash cracking. The campaign came to light only because the operators left their own back-end server exposed with an open, browsable directory, holding validated credentials, tooling, automation scripts, and operator command histories.

Researchers' analyses found the widely reported figure of roughly 21,000 affected domains resolves to approximately 918 organisations with any captured internal traffic, and only around 148 confirmed compromises. The directory also contained a revenue-sorted catalogue of remote-access targets and a live SSL VPN configuration, confirming the operators held usable access primed for sale to other criminals.

ATTACK TYPE	Vulnerability, Breaches	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, E-Commerce, Aviation, Automobile, Broadcast Media Production, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Fortinet FortiClient SSL VPN, Fortinet FortiGate, Fortinet VPN, Fortinet, FortiClient, FortiOS

Source - https://www.cloudsek.com/blog/inside-the-fortibleed-open-directory-a-technical-analysis-of-what-the-attacker-left-behind

TATA COMMUNICATIONS

Remcos RAT delivered via GST-themed phishing using fileless execution techniques

The malicious executable masquerades as a legitimate brick-building game, running in the background after launch to reduce user suspicion. It conceals next-stage components within embedded resource sections, hiding payload data inside a serialised .NET Bitmap object using a steganographic delivery technique. Successive loaders, including Optimax.dll, are reconstructed and executed entirely in memory via reflection, leaving minimal forensic evidence on disk.

Once deployed, Remcos RAT uses process hollowing to run under the victim's default browser process name and establishes persistence through Run registry keys. It checks for sandbox and virtual machine presence, bypasses UAC, and monitors user activity. The malware harvests Chrome and Firefox credentials, storing captured data in a file before exfiltrating it to its command-and-control server.

ATTACK TYPE	Cybercrime, Phishing, Malware	**SECTOR**	BFSI
REGION	India	**APPLICATION**	Windows, Google Chrome

Source - https://labs.k7computing.com/index.php/a-multi-stage-steganographic-loader-campaign-deploying-diverse-payloads-globally/

TATA COMMUNICATIONS

Stealthy DragonForce intrusion hides command traffic behind Microsoft Teams servers

Backdoor.Turn obtains an anonymous Teams visitor token from Microsoft's Skype-backed identity services, uses a legitimate Microsoft TURN relay to establish the connection, then runs a QUIC session to the attacker's real command-and-control server. To network defenders, the only visible traffic was outbound connections to legitimate Microsoft Teams servers, leaving them unaware that data was being quietly siphoned away.

The attackers gained initial access by exploiting a vulnerability in an SQL or MSSQL server, with activity beginning in December 2025. For defence evasion, they employed a sophisticated BYOVD strategy, including a novel Havoc Process Terminator technique abusing Huawei's HWAuidoOs2Ec.sys driver — a driver not officially known to be vulnerable at the time of the attack.

ATTACK TYPE	Ransomware	**SECTOR**	Business, IT Services and Consulting
REGION	Global	**APPLICATION**	Microsoft Skype, Oracle VM VirtualBox, Windows, Microsoft Teams

Source - https://www.security.com/threat-intelligence/dragonforce-msteams-backdoor

TATA COMMUNICATIONS

npm supply chain attack via easy-day-js delivers cross-platform crypto-stealing RAT

A single npm account mass-published more than 140 malicious packages across the Mastra scope within a short window on 17 June 2026. The compromised package versions themselves contained unmodified code; the attack was delivered through an injected dependency, a typosquatted package named easy-day-js added to each package's dependency list, evading source-level code review entirely.

Carrying an obfuscated payload in a post-install hook, the malware ran automatically during installation, before any application code was imported. The loader disabled TLS validation, fetched a cross-platform infostealer, and installed persistence across Windows, macOS, and Linux. With @mastra/core alone receiving over 918,000 weekly downloads, the campaign carried a substantial potential blast radius.

ATTACK TYPE	Supply chain	**SECTOR**	IT Services and Consulting, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, Node.js, Node Packager Manager (npm)

Source - https://socket.dev/blog/mastra-npm-packages-compromised

TATA COMMUNICATIONS

Rokarolla Trojan impersonates trusted apps to hijack banking and crypto credentials

Named after its command-and-control infrastructure, Rokarolla employs a sophisticated suite of 137 commands that grant extensive administrative control over an infected device. Its capabilities include harvesting lock screen credentials, exfiltrating contact lists and SMS data, and deploying keyloggers to record user input continuously, whilst concealing operations by blocking calls, suppressing audio, and deactivating Google Play Protect.

To steal financial credentials, the malware fetches a target list of banking and cryptocurrency applications, then downloads fake HTML-based phishing pages stored in a local database. When the victim launches a legitimate application, Rokarolla displays the stored content as a deceptive overlay, capturing entered credentials. It can also intercept SMS messages to harvest banking one-time passwords.

ATTACK TYPE	Malware, Mobile	**SECTOR**	BFSI, Retail and Distribution, Cryptocurrency
REGION	Global	**APPLICATION**	Android

Source - https://zimperium.com/blog/rokarolla-android-banker-with-complete-device-takeover-capabilities

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

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.

© 2026 Tata Communications. All rights reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Private Limited.