TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 15, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As September 2026 progresses, the cyber threat landscape continues to accelerate, with threat actors launching ever more sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Traditional defence models are buckling under pressure as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now depends on organisations strengthening foundational security controls, adopting layered defence strategies, and threading forward-looking intelligence through every layer of their operational frameworks.

In this rapidly shifting environment, the Tata Communications Cyber Threat Intelligence report remains an indispensable resource for security practitioners. Issued weekly, it provides sharp, timely analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By converting intelligence into practical defence guidance, it empowers security teams to anticipate, counter, and contain threats with confidence — preserving the continuity of critical operations at scale.

TATA COMMUNICATIONS

Google patches Chrome V8 zero-day of 2026 as CISA demands urgent remediation

Google has released an emergency security update for Chrome after confirming active exploitation of CVE-2026-85046, a high-severity type confusion flaw in the V8 JavaScript and WebAssembly engine. Rated 8.8 on the CVSS scale, the vulnerability allows a remote attacker to execute arbitrary code within the browser's sandbox simply by persuading a user to visit a specially crafted web page.

The patch, released on 3 September 2026 in Chrome 152.0.7977.82, addresses eleven further vulnerabilities alongside the zero-day. CISA added CVE-2026-85046 to its Known Exploited Vulnerabilities catalogue the following day, requiring federal agencies to remediate by 18 September. This marks the sixth actively exploited Chrome zero-day Google has patched in 2026. All users should update immediately.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, BFSI, IT, Government, Aerospace, Automobile, Broadcast Media Production, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Google Chrome OS, Google Chrome

Source - https://securityonline.info/chrome-zero-day-vulnerability/

INTRODUCTION

GOOGLE ISSUES EMERGENCY CHROME PATCH AFTER V8 ZERO-DAY FOUND IN ACTIVE USE

UNAUTHENTICATED ATTACKERS COULD GAIN ROOT ACCESS VIA CISCO NEXUS 9000 FLAW

CRITICAL VMWARE VULNERABILITY LETS A GUEST VM ATTACKER EXECUTE CODE ON THE HOST

.NET INFOSTEALER HIDES INSIDE IMAGE FILES TO HARVEST PASSWORDS AND CREDENTIALS

FAKE RECRUITER MESSAGES ON LINKEDIN DELIVER MIRAGE KITTEN ESPIONAGE MALWARE

STATE-LINKED QTFY HACKERS TARGET SECTORS USING IOT BOTNETS AND PROXY NETWORKS

COORDINATED TAKEDOWN CUTS A SALITY P2P BOTNET OFF FROM ITS CRIMINAL OPERATORS

TRINITITE WORM ABUSES CI WORKFLOW TO STEAL DEVELOPER AND CLOUD CREDENTIALS

FIRE ANT WEAPONISE TRUSTED ROUTERS AND AUTHENTICATION SERVERS TO GAIN COVERT ACCESS

FAKE CAPTCHA TRICKS USERS INTO RUNNING COMMANDS THAT OPEN NETWORK BACKDOORS

TATA COMMUNICATIONS

Cisco security updates address critical RCE and high-severity Nexus 9000 vulnerabilities

Cisco published its September 2026 security advisories on 2 September, addressing critical and high-severity flaws across multiple product families. The most severe is CVE-2026-20212, a CVSS 9.8 flaw in Silicon One-based Nexus 9000 switches. An unauthenticated remote attacker who can reach TCP ports 43210 or 43211 can execute arbitrary code with root privileges and force a device reload.

A separate IOS XR hardening release bundles seven umbrella CVEs, two rated 9.8, covering memory-safety, access-control and certificate-validation weaknesses that affect all IOS XR releases. Cisco additionally patched a high-severity denial-of-service flaw in SIP-based IP phones, including the Desk Phone 9800 and IP Phone 7800 and 8800 series. No active exploitation has been reported for any of the disclosed vulnerabilities.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Cisco NX-OS, Cisco IOS XR, Cisco Unified Communications Manager

Source - https://www.hkcert.org/security-bulletin/cisco-products-multiple-vulnerabilities_20260903

TATA COMMUNICATIONS

Critical integer overflow lets guest VM administrators run arbitrary code on the host

Broadcom has published advisory VMSA-2026-0007, disclosing two vulnerabilities in VMware Workstation and VMware Fusion affecting versions 25H2 and 26H1. The more severe, CVE-2026-59346, is a critical integer-overflow flaw in the VMXNET3 virtual network adapter rated CVSS 9.3. An attacker with administrative privileges inside a guest VM can exploit it to execute code on the host, effectively escaping the virtualised environment.

The second flaw, CVE-2026-59347, is a stack-based buffer overflow in the Host-Guest File System (HGFS), which handles shared folder access between guest and host, rated CVSS 8.1. It allows a local admin on a guest to execute code within the host's VMX process. No workarounds exist for either vulnerability; Broadcom has released version 26H1u1 as the sole remediation.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, IT, Government, Education, BFSI, Airline, Automobile, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	VMware Fusion, VMware Workstation

Source - https://securityonline.info/vmware-cve-2026-59346-code-execution-host/

TATA COMMUNICATIONS

Phantom .NET infostealer uses PNG files and PowerShell to loot compromised systems

Threat Research Team has detailed Phantom Stealer, a modular .NET-based infostealer observed in active campaigns since mid-2026. Delivered via phishing emails, cracked software and platforms such as Discord and Telegram, the malware uses PNG steganography to conceal its next-stage payload inside encrypted image resources embedded within .NET assemblies, frustrating static analysis and signature-based detection tools.

A secondary chain uses obfuscated PowerShell to compile C# code at runtime and inject shellcode into trusted Windows processes. Once active, Phantom Stealer harvests browser credentials, cookies, payment data, cryptocurrency wallets, clipboard contents, keystrokes and screenshots before exfiltrating to command-and-control infrastructure. The malware patches Windows telemetry functions to suppress in-memory scanning. Splunk has released 32 detection rules to assist defenders.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Edge, Microsoft Outlook, Opera Browser, Windows, Google Chrome

Source - https://www.splunk.com/en_us/blog/security/phantom-stealer-shellcode-steganography-credential-theft.html

TATA COMMUNICATIONS

Mirage Kitten uses fake job lures to plant NodeRabbit and PollCat cross-platform backdoors

Cyber researchers have attributed a new cyberespionage campaign to Mirage Kitten, also tracked as UNC1549, targeting software developers in aviation, aerospace and fintech sectors. Posing as legitimate recruiters on LinkedIn, the group delivers time-sensitive coding challenges hosted on Amazon S3. Running the trojanised archive silently launches NodeRabbit, a cross-platform Node.js remote access trojan, before any code is written.

A second malware family, PollCat, is an obfuscated JavaScript RAT delivered through a separate coding challenge requiring a recruiter-supplied one-time code and a one-hour window. Both implants support persistent access, command execution, file transfer and data theft across Windows, Linux and macOS. NodeRabbit additionally achieves persistence through a fake VS Code extension and malicious Git hooks targeting developer toolchains.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	Aerospace, Aviation, BFSI
REGION	Middle East, Africa, Afghanistan, Egypt, Ethiopia	**APPLICATION**	Apple macOS, Microsoft Outlook, Microsoft Visual Studio, Git Project, Git, Windows, Linux, VS Code, Node.js, npm

Source- https://thehackernews.com/2026/09/iranian-hackers-pose-as-recruiters-to.html

TATA COMMUNICATIONS

QTFY hacking group use hijacked IoT devices to disguise attacks on critical infrastructure

QTFY, a state-sponsored threat group linked to Nanjing Xinjiuwei Network Technology Company and active since 2018, has been exposed by researchers and government agencies as a persistent threat to critical infrastructure worldwide. Its QScan platform processes millions of scanning and exploitation tasks daily, drawing on a database of over 200 Python-based exploits to rapidly identify and compromise vulnerable internet-facing systems.

To conceal its origins, QTFY routes malicious traffic through QTRouter, an obfuscation network comprising compromised routers, hijacked IoT devices and commercial proxy services. On 26 August 2026, the FBI and US Department of Justice seized the QScan and QTRouter domains. Organisations are advised to review the published indicators of compromise and vet IP addresses before taking blocking action.

ATTACK TYPE	Vulnerability, Malware, Cyber-espionage	**SECTOR**	Healthcare, BFSI, Waste Disposal, IT, Government, Energy, Defence, Telecommunications
REGION	Middle East, Africa, Afghanistan, Egypt, Ethiopia	**APPLICATION**	Microsoft Exchange Server, Atlassian Confluence, Citrix Advanced Access Control, Fortinet FortiClient SSL VPN, F5 BIG-IP, Apache log4j, Ivanti, OpenWrt, Beyond Trust Privileged Remote Access, Beyond Trust Remote Support, CrushFTP

Source - https://www.safebreach.com/blog/qtfy-scan-factory-china-hacking-group/

TATA COMMUNICATIONS

Law enforcement cuts off a 23-year-old Sality P2P that silently hijacked crypto payments

An international law enforcement and industry operation on 31 August 2026 disrupted the Sality P2P botnet, active since 2003 — one of the longest-running criminal botnets in history. The polymorphic file-infecting malware maintained separate v3 and v4 peer-to-peer networks and had infected more than 15,000 machines worldwide. Partners included the US Department of Justice, FBI, CrowdStrike, Shadowserver Foundation and Europol.

Disruption exploited a fundamental weakness in Sality's peer-management protocol: bots accepted connections from any publicly reachable machine without authentication. CrowdStrike manipulated peer lists to insert sinkhole entries, cutting all 15,000 infected systems off from the operator. Payload-hosting URLs were simultaneously seized. The primary payload, EggJagger, had silently hijacked cryptocurrency clipboard addresses to steal at least $150,000 over eight years.

ATTACK TYPE	Malware, DDoS	**SECTOR**	Trading, Cryptocurrency
REGION	Russia, Ukraine	**APPLICATION**	Windows

Source - https://securityonline.info/sality-botnet-disruption/

INTRODUCTION | GOOGLE ISSUES EMERGENCY CHROME PATCH AFTER V8 ZERO-DAY FOUND IN ACTIVE USE | UNAUTHENTICATED ATTACKERS COULD GAIN ROOT ACCESS VIA CISCO NEXUS 9000 FLAW | CRITICAL VMWARE VULNERABILITY LETS A GUEST VM ATTACKER EXECUTE CODE ON THE HOST | .NET INFOSTEALER HIDES INSIDE IMAGE FILES TO HARVEST PASSWORDS AND CREDENTIALS | FAKE RECRUITER MESSAGES ON LINKEDIN DELIVER MIRAGE KITTEN ESPIONAGE MALWARE | STATE-LINKED QTFY HACKERS TARGET SECTORS USING IOT BOTNETS AND PROXY NETWORKS | COORDINATED TAKEDOWN CUTS A SALITY P2P BOTNET OFF FROM ITS CRIMINAL OPERATORS | TRINITITE WORM ABUSES CI WORKFLOW TO STEAL DEVELOPER AND CLOUD CREDENTIALS | FIRE ANT WEAPONISE TRUSTED ROUTERS AND AUTHENTICATION SERVERS TO GAIN COVERT ACCESS | FAKE CAPTCHA TRICKS USERS INTO RUNNING COMMANDS THAT OPEN NETWORK BACKDOORS

TATA COMMUNICATIONS

Attackers weaponise GitHub Actions workflow to deploy Mini Shai-Hulud “Trinitite” worm

Attackers compromised a widely used npm package generating TanStack Query code with over 150,000 weekly downloads by abusing a misconfigured GitHub Actions release workflow that allowed any user to trigger a publish via pull request comments. Ten malicious versions were released in approximately twenty minutes on 28 August 2026, each carrying valid npm provenance to evade standard supply chain checks.

The payload, identified as a new Trinitite wave of the Mini Shai-Hulud worm family, fired through preinstall hooks and an obfuscated binding.gyp file. Once running, it downloaded Bun and harvested credentials across GitHub, cloud platforms, Kubernetes and CI pipelines before using stolen tokens to republish poisoned packages across npm, RubyGems and, for the first time, PyPI.

ATTACK TYPE	Supply Chain	**SECTOR**	IT
REGION	Global	**APPLICATION**	Microsoft Windows Defender, Kubernetes, VS Code, SentinelOne, Microsoft Azure, CrowdStrike, AWS, npm, PyPI, GitHub

Source - https://www.endorlabs.com/learn/trojanized-7nohe-openapi-react-query-codegen-adds-pypi-to-a-self-replicating-npm-worm

TATA COMMUNICATIONS

Fire Ant pivots from hypervisors to network infrastructure to harvest enterprise credentials

Sygnia has documented a 2026 expansion of Fire Ant, a China-nexus espionage actor that moved beyond VMware hypervisors to compromise Cisco IOS XR routers, TACACS authentication servers and Linux management hosts. The group deployed two new tools: BridgeAgent, a Linux backdoor disguised as a monitoring agent, and TacTap, a toolkit purpose-built to intercept and harvest TACACS credentials.

Compromised routers were turned into collection platforms, capturing network traffic, suppressing syslog output and filtering CLI command results to obscure malicious activity from administrators. Fire Ant also established covert tunnels and manipulated logs to frustrate forensic investigation. By controlling infrastructure that routes and authenticates enterprise environments, the actor explored access paths toward connected high-value and critical infrastructure networks.

ATTACK TYPE	Cyber-espionage, APT	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Cisco iOS, Linux, Zabbix, SentinelOne

Source - https://www.bitdefender.com/en-us/blog/businessinsights/silkparasite-tracking-china-nexus-apt-across-central-asia

TATA COMMUNICATIONS

TerminalFix uses PowerShell and steganography for multistage reverse tunnel implant

Microsoft Threat Intelligence has detailed TerminalFix, a sophisticated variant of the ClickFix social engineering technique targeting organisations across multiple sectors. The campaign operates through compromised websites displaying fake Cloudflare CAPTCHA overlays, directing users to paste malicious PowerShell commands into Windows Terminal rather than the Run dialogue, significantly increasing the likelihood of complex multi-line scripts executing successfully.

Once executed, the chain progresses through DLL sideloading of a legitimate signed binary, steganographic payload extraction from PNG images, dual persistence via scheduled tasks and Registry Run keys, and Active Directory reconnaissance. A custom Python reverse tunnel then connects outbound over an encrypted WebSocket, granting persistent SOCKS-style proxy access and turning the endpoint into a full internal network pivot.

ATTACK TYPE	Social engineering, Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Python, Windows, PowerShell

Source - https://www.microsoft.com/en-us/security/blog/2026/08/28/terminalfix-campaign-deploys-reverse-tunnel-through-multistage-intrusion/

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