TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 21, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As July 2026 progresses, sustaining resilience and competitive advantage now demands that organisations reinforce foundational security controls, embrace layered defence strategies, and embed forward-looking intelligence across every layer of their operational frameworks.

In this regard, Tata Communications' cybersecurity capabilities are internationally recognised. It has been named an Overall Leader in MDR in the KuppingerCole Leadership Compass 2026, with leadership positions in both Product and Innovation. Some of its differentiators that set it apart have been carrier-scale network visibility for earlier detection, AI-assisted SOC operations with human validation, and strong integration across cloud, identity, OT, and network.

Besides, Tata Communications' Cyber Threat Intelligence weekly report continues to serve as an indispensable resource for security practitioners by translating intelligence into practical defence guidance. It equips security teams to anticipate, counter, and contain threats with confidence, ensuring the continuity of critical operations at scale.

INTRODUCTION

PALO ALTO NETWORKS FIXES MULTIPLE PAN-OS AND PRISMA FLAWS IN JULY UPDATE

ROGUEPLANET FIX INTRODUCES WINDOWS DEFENDER FLAW THAT CAN FILL ENTIRE SYSTEM DISK

MICROSOFT WARNS OF GIGAWIPER, A GOLANG BACKDOOR BUILT TO DESTROY WINDOWS COMPUTERS

THREAT GROUPS TURN MICROSOFT TEAMS INTO AN INITIAL ACCESS ROUTE FOR MALWARE DELIVERY

IRONWORM RUST MALWARE TARGETS DEVELOPER SECRETS VIA JSCRAMBLER NPM PACKAGE

NEW HELIX THREAT GROUP ABUSES MFA AND EXFILTRATES SHAREPOINT DATA FROM ENTERPRISES

NEW JAVA-BASED QUIMARAT MALWARE AS A SERVICE TARGETS WINDOWS, LINUX, AND MACOS

MALWARE CAMPAIGN USES FAKE INDIAN TAX WEBSITES TO DEPLOY DUAL REMOTE TROJANS

CRITICAL MINIORANGE SSO PLUGIN BUG PUTS MILLIONS OF WORDPRESS SITES AT TAKEOVER RISK

BEYONDTRUST PATCHES FLAWS IN REMOTE SUPPORT AND PRIVILEGED REMOTE ACCESS

TATA COMMUNICATIONS

Multiple security flaws patched across Palo Alto PAN-OS, Prisma, and Cortex products

Palo Alto Networks has disclosed a series of vulnerabilities affecting PAN-OS, Prisma Access, Prisma Access Agent, Cortex XDR Broker VM, GlobalProtect and Large-Scale VPN deployments. The flaws span buffer overflows, denial-of-service conditions, command injection, authentication bypass, server-side request forgery, information disclosure and cross-site scripting, exposing organisations to potential service disruption, unauthorised access and remote code execution.

The most serious issue, a buffer overflow in the User-ID Terminal Server Agent, could allow unauthenticated remote code execution and carries a high severity rating. Palo Alto Networks reported no evidence of active exploitation but urged prompt patching. Fixed releases are available across affected PAN-OS and Prisma versions, and administrators are advised to upgrade and restrict network exposure immediately.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Defence, Business, Aviation, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Global	**APPLICATION**	Palo Alto Networks GlobalProtect, Palo Alto Networks NetConnect, Palo Alto Networks PAN-OS, Palo Alto Firewall

Source - https://cyberpress.org/palo-alto-pan-os-buffer-overflow-flaws/

TATA COMMUNICATIONS

RoguePlanet PoC sparks discovery of new Windows Defender disk exhaustion vulnerability

Shortly after Microsoft patched the RoguePlanet privilege-escalation vulnerability (CVE-2026-50656) through a Malware Protection Engine update, researcher Nightmare Eclipse re-examined Windows Defender and uncovered fresh weaknesses in its file handling and memory management. The most serious is a proof-of-concept showing that Defender's caching of the Zone. Identifier Alternate Data Streams can be abused to exhaust a system's disk space entirely.

Cyber threat analysts state that an attacker configures a malicious SMB server that serves a file alongside an oversized Zone.Identifier stream, then stalls read requests to keep the session open. Defender bypasses its usual size limits and writes the cache indefinitely, filling the disk. Reproduced on Windows 11 25H2 and Windows Server 2025, the flaw triggers widespread application and service instability.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Defence, Business, Aviation, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Global	**APPLICATION**	Microsoft Windows Defender

Source - https://www.securityweek.com/microsoft-patches-defender-rogueplanet-vulnerability/

TATA COMMUNICATIONS

Microsoft uncovers GigaWiper, combining disk wiping, file encryption, and remote control

Microsoft Threat Intelligence has identified GigaWiper, a Golang-based backdoor first observed during destructive attacks in October 2025. Rather than a single tool, its operators combined code from at least three malware families, embedding multiple destructive functions within one implant. It maintains persistence through a scheduled task disguised as OneDrive Update, running at startup and every minute.

Operators can trigger disk wiping, overwrite drives, and force restarts, while a ransomware-style function encrypts files with a candy extension using keys that are never saved, leaving no recovery path. GigaWiper also enables event log clearing, screen recording and remote control. Microsoft strongly advises enabling tamper protection, cloud-delivered antivirus and endpoint detection in block mode.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Defence, Business, Aviation, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Global	**APPLICATION**	Microsoft Windows Defender, Windows, Redis, RabbitMQ

Source - https://hackread.com/microsoft-gigawiper-backdoor-destroy-windows-pcs/

INTRODUCTION | PALO ALTO NETWORKS FIXES MULTIPLE PAN-OS AND PRISMA FLAWS IN JULY UPDATE | ROGUEPLANET FIX INTRODUCES WINDOWS DEFENDER FLAW THAT CAN FILL ENTIRE SYSTEM DISK | MICROSOFT WARNS OF GIGAWIPER, A GOLANG BACKDOOR BUILT TO DESTROY WINDOWS COMPUTERS | THREAT GROUPS TURN MICROSOFT TEAMS INTO AN INITIAL ACCESS ROUTE FOR MALWARE DELIVERY | IRONWORM RUST MALWARE TARGETS DEVELOPER SECRETS VIA JSCRAMBLER NPM PACKAGE | NEW HELIX THREAT GROUP ABUSES MFA AND EXFILTRATES SHAREPOINT DATA FROM ENTERPRISES | NEW JAVA-BASED QUIMARAT MALWARE AS A SERVICE TARGETS WINDOWS, LINUX, AND MACOS | MALWARE CAMPAIGN USES FAKE INDIAN TAX WEBSITES TO DEPLOY DUAL REMOTE TROJANS | CRITICAL MINIORANGE SSO PLUGIN BUG PUTS MILLIONS OF WORDPRESS SITES AT TAKEOVER RISK | BEYONDTRUST PATCHES FLAWS IN REMOTE SUPPORT AND PRIVILEGED REMOTE ACCESS

TATA COMMUNICATIONS

Fake IT support on Microsoft Teams delivers EtherRAT and SNOW malware to enterprises

A wave of campaigns is exploiting Microsoft Teams as an initial access vector. The threat cluster UNC6692, tracked by Google Mandiant, pairs email bombing with helpdesk impersonation over Teams, luring victims into a fake mailbox patch. This deploys the modular SNOW suite — SNOWBELT, SNOWGLAZE and SNOWBASIN — enabling browser persistence, WebSocket tunnelling, credential theft and Active Directory compromise.

In a parallel campaign detailed by Palo Alto Networks, attackers place fake IT support voice calls over Teams, then guide employees into granting remote control and installing EtherRAT via a Node.js loader. Microsoft has since added external-caller warnings and bot controls, yet analysts urge firms to restrict external Teams access and verify helpdesk requests independently.

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

Source - https://www.bleepingcomputer.com/news/security/fake-it-support-calls-on-microsoft-teams-push-etherrat-malware/

TATA COMMUNICATIONS

IronWorm Rust infostealer delivered via hijacked jscrambler npm package on all platforms

Security researchers have uncovered a sophisticated software supply chain attack that compromised the widely used Jscrambler npm package. Attackers abused legitimate publishing credentials to distribute five malicious releases containing an evolved IronWorm Rust-based infostealer. Uploaded to npm on 11 July 2026, the tainted versions execute during package installation or import, deploying platform-specific payloads across Linux, Windows and macOS.

Once active, the malware harvests developer credentials, cloud secrets, cryptocurrency wallets, VPN configurations and browser data, while scanning for password managers and offensive-security tools. It establishes persistent, encrypted command-and-control communications routed through the Tor network, tailoring payloads to each operating system. Cyber researchers urge affected organisations to rotate all credentials, revoke npm tokens and remove the compromised versions.

ATTACK TYPE	Malware	**SECTOR**	IT Services and Consulting, Business, Cryptocurrency
REGION	Global	**APPLICATION**	Apple macOS, Chromium, Docker, Kubernetes, Windows, Linux, Microsoft Azure, Node Packager Manager (NPM), Telegram, Slack, GitHub

Source - https://research.jfrog.com/post/ironworm-returns-rustier-than-ever/

TATA COMMUNICATIONS

Helix extortion campaign targets enterprises through vishing and SharePoint data theft

Security researchers have uncovered a previously unreported data extortion operation named Helix, which compromises enterprises through identity-based intrusion rather than malware. Analysed by ReliaQuest, the group combines voice phishing and device-code phishing to capture session tokens, rapid MFA registration for persistence, and automated SharePoint enumeration. Its tradecraft, infrastructure, and timing overlap closely with the BlackFile and ShinyHunters ecosystem.

Attacks begin with convincing pretext calls, sometimes spoofing a manager's name to trigger a device-code authentication flow. Operators capture the session token, register a fresh authenticator, then pivot to a hosted server for scripted bulk downloads. ReliaQuest advises disabling device-code authentication as the highest-impact mitigation, alongside restricting sensitive access to managed endpoints and blocking newly registered domains.

ATTACK TYPE	Ransomware	**SECTOR**	IT and BFSI
REGION	Global	**APPLICATION**	Microsoft Exchange Server, Microsoft SharePoint Server, OneDrive, Microsoft Teams, Microsoft Authenticator

Source - https://gbhackers.com/new-helix-extortion-group/

INTRODUCTION | PALO ALTO NETWORKS FIXES MULTIPLE PAN-OS AND PRISMA FLAWS IN JULY UPDATE | ROGUEPLANET FIX INTRODUCES WINDOWS DEFENDER FLAW THAT CAN FILL ENTIRE SYSTEM DISK | MICROSOFT WARNS OF GIGAWIPER, A GOLANG BACKDOOR BUILT TO DESTROY WINDOWS COMPUTERS | THREAT GROUPS TURN MICROSOFT TEAMS INTO AN INITIAL ACCESS ROUTE FOR MALWARE DELIVERY | IRONWORM RUST MALWARE TARGETS DEVELOPER SECRETS VIA JSCRAMBLER NPM PACKAGE | NEW HELIX THREAT GROUP ABUSES MFA AND EXFILTRATES SHAREPOINT DATA FROM ENTERPRISES | NEW JAVA-BASED QUIMARAT MALWARE AS A SERVICE TARGETS WINDOWS, LINUX, AND MACOS | MALWARE CAMPAIGN USES FAKE INDIAN TAX WEBSITES TO DEPLOY DUAL REMOTE TROJANS | CRITICAL MINIORANGE SSO PLUGIN BUG PUTS MILLIONS OF WORDPRESS SITES AT TAKEOVER RISK | BEYONDTRUST PATCHES FLAWS IN REMOTE SUPPORT AND PRIVILEGED REMOTE ACCESS

TATA COMMUNICATIONS

Cross-platform QuimaRAT uses encrypted plugins to control Windows, Linux, and macOS

Threat researchers have uncovered QuimaRAT, a novel Java-based remote access trojan capable of compromising Windows, Linux and macOS systems. Sold under a malware-as-a-service model, it costs between $150 for a month and $1,200 for lifetime access. Its modular design supports encrypted plugins that operators can load, unload and update directly from command-and-control infrastructure.

The Trojan establishes persistence through operating-system-specific methods, including registry run keys on Windows, crontab tasks on Linux and a LaunchAgent on macOS. It supports credential theft, webcam surveillance, fileless execution and file transfer, granting attackers comprehensive control. LevelBlue warns QuimaRAT should be treated as a modular platform designed to rotate its fingerprints while preserving core malicious behaviour.

ATTACK TYPE	Malware	**SECTOR**	BFSI, IT, Government, Education
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, Java

Source - https://thehackernews.com/2026/07/new-java-based-quimarat-maas-built-to.html

TATA COMMUNICATIONS

Fake Indian income tax websites deliver dual remote access trojans through malware

Threat analysts have uncovered an active campaign that lures Indian taxpayers to counterfeit Income Tax Department websites bearing official Government branding. Victims are shown urgent compliance notices, routed through a fake Microsoft verification page, and prompted to download a ZIP archive posing as an offline tax utility. The archive conceals a signed executable alongside a malicious DLL.

Running the executable triggers DLL sideloading, launching a six-stage infection chain that escalates privileges, installs a disguised Windows service, and retrieves a polyglot JPEG hiding multiple encrypted payloads. Later stages execute entirely in memory through reflective loading and injection into svchost.exe. The campaign ultimately deploys two remote access trojans across separate command-and-control channels, ensuring resilient attacker access.

ATTACK TYPE	Malware	**SECTOR**	BFSI, Government
REGION	India	**APPLICATION**	Microsoft Edge, Windows

Source - https://www.cyderes.com/howler-cell/fake-indian-itr-notice-dual-rat-deployment

TATA COMMUNICATIONS

Unpatched miniOrange OAuth SSO flaw exposes WordPress sites to administrator takeover

Security firm has disclosed a critical authentication bypass in the miniOrange OAuth Single Sign-On plugin for WordPress, tracked as CVE-2026-57807 and rated 9.8 on the CVSS scale. The flaw, rooted in CWE-288, lets unauthenticated attackers abuse the plugin's password recovery mechanism to bypass login controls and gain full administrator access to affected WordPress sites.

All plugin versions up to and including 38.5.8 are affected, and no official fix is yet available from the vendor. Patchstack has issued a virtual patch for its own customers, though this may disrupt legitimate single sign-on traffic. Administrators are urged to deactivate the plugin immediately, restrict login endpoints, and audit their sites for unauthorised administrator accounts.

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

Source - https://cyberpress.org/wordpress-oauth-sso-plugin-flaw/

TATA COMMUNICATIONS

BeyondTrust warns of critical flaws affecting Remote Support and Privileged Remote Access

BeyondTrust has disclosed four vulnerabilities in its Remote Support and Privileged Remote Access appliances through advisory BT26-03. Two critical pre-authentication bugs, CVE-2026-40138 and CVE-2026-40139, each carry a CVSS v4 score of 9.2 and could let network-positioned attackers bypass access controls, reaching accounts with elevated privileges. All versions at or below 25.3.2 are considered vulnerable to exploitation.

Two further high-severity flaws, CVE-2026-40140 and CVE-2026-40141, allow denial-of-service conditions and unauthorised resource access respectively. BeyondTrust patched all cloud-hosted instances on 21 April 2026, while self-hosted customers should apply the April 2026 security rollup or upgrade to version 25.3.3. No active exploitation has been reported, though the firm's appliances have drawn repeated attacker interest previously.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Defence, Business, Aviation, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, Beyond Trust Privileged Remote Access, Beyond Trust Remote Support

Source - https://securityonline.info/cve-2026-40138-beyondtrust-pre-authentication-vulnerability/

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