TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 9, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As we enter the second week of June 2026, the cyber threat landscape continues to evolve as adversaries demonstrate remarkable technical agility and operational breadth across interconnected digital ecosystems. State-sponsored espionage groups are expanding their geographic reach and rapidly maturing their evasion tradecraft, whilst financially motivated actors are leveraging sophisticated service-based models to scale criminal operations without commensurate increases in technical skill. The sustained abuse of trusted infrastructure underscores a structural shift in attacker methodology that fundamentally undermines conventional trust models and demands a recalibration of organisational defensive postures.

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.

INTRODUCTION

WANTTOCRY RANSOMWARE EXPLOITS SMB SERVICES FOR STEALTH REMOTE ENCRYPTION

IRANIAN APT SCREENING SERPENS EMPLOYS .NET HIJACKING AND DLL SIDELOADING IN NEW ATTACKS

FAKE MICROSOFT TEAMS DOWNLOAD SITES WEAPONISED TO DEPLOY VALLEYRAT MALWARE

ORACLE MAY 2026 CRITICAL PATCH UPDATE FIXES VULNERABILITIES WITH CVSS SCORES UP TO 10.0

CISA ADDS THREE SUPPLY CHAIN VULNERABILITIES TO KNOWN EXPLOITED VULNERABILITIES CATALOGUE

CISA FLAGS ACTIVE EXPLOITATION OF PAN-OS GLOBALPROTECT VPN AUTHENTICATION BYPASS

SHINYSPIDER DISTRIBUTES ILLUSION 2.6.5 INFOSTEALER AND RAT UNDER SILENT MAAS MODEL

TRUSTED AI PLATFORMS ABUSED AS MALWARE DELIVERY VECTORS THROUGH SOCIAL ENGINEERING

XWORM V7.4 CAMPAIGN DEPLOYS PYINSTALLER LOADER WITH AMSI BYPASS

MICROSOFT EXPOSES FOX TEMPEST MSAAS OPERATION DISTRIBUTING SIGNED RANSOMWARE AND INFOSTEALERS

TATA COMMUNICATIONS

WantToCry ransomware leverages exposed SMB services for agentless remote encryption

Sophos researchers have confirmed active WantToCry ransomware operations targeting organisations with internet-exposed SMB services on TCP ports 139 and 445. Operators scan for exposed devices using Shodan and Censys, then conduct automated brute-force attacks using weak or compromised credentials to establish authenticated sessions.

Uniquely, WantToCry performs encryption entirely on attacker-controlled infrastructure: files are exfiltrated via SMB, encrypted remotely, and rewritten back to their original locations, leaving no local malware footprint and substantially limiting detection opportunities. Organisations should disable SMBv1, block inbound SMB at internet-facing firewalls, enforce strong credential policies, and isolate backups from SMB-reachable paths.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Hospitality, BFSI, Manufacturing, IT, Government, Transportation, Energy, Defence, E-commerce, Aviation, Retail and Distribution, Telecommunications, Software Development
REGION	Global	**APPLICATION**	Windows

Source - https://securityonline.info/wanttocry-remote-ransomware-smb-brute-force-no-local-code/

TATA COMMUNICATIONS

Iranian APT Screening Serpens' espionage campaign uses .NET hijacking and DLL sideloading

Researchers identified sustained cyberespionage campaigns in 2026 attributed to the Iran-linked APT group Screening Serpens, targeting entities in the United States, Israel, the UAE, and the broader Middle East. The group deployed two evolving remote access Trojan families, MiniUpdate and MiniJunk V2, delivered through spear-phishing lures impersonating job portals and conferencing tools.

The campaign leverages DLL sideloading and advanced .NET AppDomainManager hijacking to bypass endpoint detection and response tools, disable runtime logging, and ensure stealthy execution throughout the intrusion chain. Targeted sectors include information technology, aerospace, defence, and telecommunications.

ATTACK TYPE	Malware, Cyber-espionage, APT	**SECTOR**	IT, Aerospace, Defence Industry, Telecommunications
REGION	Middle East, Europe, Israel, United States	**APPLICATION**	Microsoft .NET Framework, Windows

Source - https://unit42.paloaltonetworks.com/tracking-iran-apt-screening-serpens/

TATA COMMUNICATIONS

Fake Microsoft Teams sites deploy ValleyRAT through DLL sideloading and in-memory execution

Researchers identified a malware campaign using fake Microsoft Teams download websites, distributed through the X platform, to deliver a trojanised installer deploying ValleyRAT. The attack employs NSIS installers, DLL sideloading through Tencent's legitimate GameBox.exe, Windows Defender exclusions, hidden files, and AES and XOR-encrypted payloads, alongside reflective loading and in-memory shellcode execution.

The campaign also establishes persistence, captures clipboard data, and logs user activity, communicating with remote command-and-control infrastructure linked to suspected China-aligned threat activity. Targeted sectors span information technology, healthcare, financial services, manufacturing, government, and telecommunications, amongst others.

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

Source - https://securityonline.info/valleyrat-malware-campaign-teams/

TATA COMMUNICATIONS

Oracle May 2026 Critical Patch Update addresses high and critical enterprise vulnerabilities

Oracle's May 2026 Critical Patch Update addresses multiple high and critical vulnerabilities across Oracle Database Server, REST Data Services, Communications, E-Business Suite, and Hospitality applications. Issues include unauthenticated remote attacks, data compromise, denial of service, and full system takeover risks, with several flaws exploiting network services and third-party components, including Apache, Kafka, and Jetty.

Critical vulnerabilities with CVSS scores up to 10.0 allow attackers to access, modify, or destroy sensitive data across enterprise systems. Organisations running affected Oracle products are strongly advised to apply the update immediately to mitigate exposure across their environments.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, Manufacturing, Construction, IT, Government, Transportation, Education, Defence, Business, Aviation, Retail and Distribution, Telecommunications, Software Development, Logistics
REGION	Global	**APPLICATION**	Oracle Application Server, Oracle Collaboration Suite, Oracle Communications Unified, Oracle Database, Oracle E-Business Intelligence

Source - https://www.hkcert.org/security-bulletin/oracle-products-multiple-vulnerabilities_20260529

TATA COMMUNICATIONS

CISA flags critical Drupal SQL Injection flaw, putting PostgreSQL deployments at risk

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added three critical vulnerabilities — CVE-2026-8398, CVE-2026-45321, and CVE-2026-48027 — to its Known Exploited Vulnerabilities catalogue, emphasising ongoing supply chain compromises. The flaws involve maliciously signed installers, compromised npm packages, and a trojanised development extension, all enabling credential theft and system compromise.

Exploited in the wild, these vulnerabilities demonstrate how attackers abuse trusted distribution channels and developer identities to bypass defences and deliver malware. Organisations are urged to audit their software supply chain dependencies and apply all available remediations without delay.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, IT, Government, Education, Business, BFSI, Aviation, Automobile, Broadcast Media Production, Logistics
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, Daemon Tools Lite, TanStack npm, Nx Console

Source - https://www.cisa.gov/known-exploited-vulnerabilities-catalog

TATA COMMUNICATIONS

CISA KEV flags active exploitation of PAN-OS GlobalProtect VPN authentication bypass

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added CVE-2026-0257 to its Known Exploited Vulnerabilities catalogue, highlighting active exploitation of an authentication bypass vulnerability in Palo Alto Networks PAN-OS GlobalProtect. Despite carrying a medium CVSS rating, attackers have leveraged crafted cookies to bypass authentication and establish unauthorised VPN access.

Observed exploitation campaigns demonstrate repeated probing and limited internal access attempts against affected deployments. Organisations running PAN-OS GlobalProtect are advised to apply vendor mitigations immediately and monitor for anomalous VPN authentication activity indicative of exploitation attempts.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, Manufacturing, IT, Government, Transportation, Education, Defence, Business, E-commerce, Aviation, Retail and Distribution, Telecommunications, Software Development
REGION	Global	**APPLICATION**	Palo Alto Networks PAN-OS

Source - https://www.cisa.gov/news-events/alerts/2026/05/29/cisa-adds-one-known-exploited-vulnerability-catalog

TATA COMMUNICATIONS

ShinyHunters Silent MaaS delivers Illusion 2.6.5 infostealer and RAT via Telegram

Illusion-2.6.5-setup.exe is a malicious Electron-based installer delivering Silent Stealer v2.6.5 with integrated remote access Trojan functionality, distributed via Telegram by a threat actor known as ShinySpider. Operating under a Malware-as-a-Service model, the payload harvests credentials, cryptocurrency wallets, Discord tokens, and session data whilst establishing persistent remote access to compromised systems.

The malware employs multi-layer obfuscation, User Account Control bypasses, and defence evasion techniques to resist detection. Exfiltration occurs via cloud storage services and dedicated command-and-control infrastructure, and researchers identified an exposed operator panel within the campaign's infrastructure.

ATTACK TYPE	Malware	**SECTOR**	BFSI, Gaming, Business
REGION	Global	**APPLICATION**	Microsoft Edge, Google Chrome, Mozilla Firefox, Telegram, Discord

Source - https://ransom-isac.org/blog/shinyhunters-silent-maas/

TATA COMMUNICATIONS

Trusted AI platforms weaponised as malware delivery vectors through social engineering campaigns

Threat actors are increasingly abusing trusted AI platforms, search engines, and software distribution channels to deliver malware through sophisticated social engineering campaigns. Recent operations leveraged fake ChatGPT and Claude installation pages, malicious shared conversations hosted on legitimate AI platforms, SEO poisoning, and malvertising to distribute credential stealers, cryptocurrency-focused malware, and cryptojacking payloads.

The campaigns exploit the established trust users place in recognised AI brands to lower suspicion and drive the installation of malicious software. Targeted sectors include financial services, education, business, software development, and cryptocurrency, with the threat assessed as global in geographic scope.

ATTACK TYPE	Phishing, Malware	**SECTOR**	BFSI, Education, Business, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Apple macOS, Microsoft .NET Framework, Chromium, Windows, Linux, Google Chrome, ChatGPT, ScreenConnect, Anthropic Claude Code

Source - https://www.malwarebytes.com/blog/threat-intel/2026/05/fake-chatgpt-download-site-infects-windows-and-mac-users-with-malware

INTRODUCTION
WANTTOCRY RANSOMWARE EXPLOITS SMB SERVICES FOR STEALTH REMOTE ENCRYPTION
IRANIAN APT SCREENING SERPENS EMPLOYS .NET HIJACKING AND DLL SIDELOADING IN NEW ATTACKS
FAKE MICROSOFT TEAMS DOWNLOAD SITES WEAPONISED TO DEPLOY VALLEYRAT MALWARE
ORACLE MAY 2026 CRITICAL PATCH UPDATE FIXES VULNERABILITIES WITH CVSS SCORES UP TO 10.0
CISA ADDS THREE SUPPLY CHAIN VULNERABILITIES TO KNOWN EXPLOITED VULNERABILITIES CATALOGUE
CISA FLAGS ACTIVE EXPLOITATION OF PAN-OS GLOBALPROTECT VPN AUTHENTICATION BYPASS
SHINYSPIDER DISTRIBUTES ILLUSION 2.6.5 INFOSTEALER AND RAT UNDER SILENT MAAS MODEL
TRUSTED AI PLATFORMS ABUSED AS MALWARE DELIVERY VECTORS THROUGH SOCIAL ENGINEERING
XWORM V7.4 CAMPAIGN DEPLOYS PYINSTALLER LOADER WITH AMSI BYPASS
MICROSOFT EXPOSES FOX TEMPEST MSAAS OPERATION DISTRIBUTING SIGNED RANSOMWARE AND INFOSTEALERS

TATA COMMUNICATIONS

XWorm V7.4 campaign uses PyInstaller loader and AMSI bypass for stealth malware deployment

Researchers analysed a PyInstaller-packed Python malware sample linked to the XWorm V7.4 campaign, revealing a multi-stage loader utilising advanced obfuscation, Antimalware Scan Interface bypass, and staged payload deployment. The malware reconstructs an encrypted payload in memory, deploys it stealthily, and executes it silently to evade endpoint detection.

The final payload provides full remote access, data exfiltration, and command execution via TCP-based command-and-control communication. The campaign demonstrates modern attack techniques, including in-memory execution, anti-analysis decoys, and modular RAT capabilities designed for sustained persistence and control over compromised systems.

ATTACK TYPE	Malware	**SECTOR**	IT
REGION	Global	**APPLICATION**	Microsoft .NET Framework, Python, Windows

Source - https://securityonline.info/xworm-pyinstaller-loader-amsi-patching-defense-evasion/

TATA COMMUNICATIONS

Fox Tempest malware-signing-as-a-service operation enables global distribution of signed malware

Microsoft exposed Fox Tempest, a financially motivated threat actor operating a malware-signing-as-a-service platform that enables cybercriminals to distribute trusted, signed malware at scale. By abusing Microsoft Artifact Signing, the group generated short-lived certificates to bypass security controls and deliver ransomware and infostealers, including Rhysida, Lumma, and Vidar.

Fox Tempest operated via platforms including signspace[.]cloud and virtual machine-based infrastructure, streamlining malicious code signing at scale. The group targets the healthcare, financial services, IT, government, and education sectors globally, and Microsoft's disruption of the operation represents a significant action against the wider cybercriminal ecosystem that the service enabled.

ATTACK TYPE	Malware, APT	**SECTOR**	Healthcare, BFSI, IT, Government, Education
REGION	Global	**APPLICATION**	Windows

Source - https://securityonline.info/microsoft-disrupts-fox-tempest-malware-signing-as-a-service/

INTRODUCTION
WANTTOCRY RANSOMWARE EXPLOITS SMB SERVICES FOR STEALTH REMOTE ENCRYPTION
IRANIAN APT SCREENING SERPENS EMPLOYS .NET HIJACKING AND DLL SIDELOADING IN NEW ATTACKS
FAKE MICROSOFT TEAMS DOWNLOAD SITES WEAPONISED TO DEPLOY VALLEYRAT MALWARE
ORACLE MAY 2026 CRITICAL PATCH UPDATE FIXES VULNERABILITIES WITH CVSS SCORES UP TO 10.0
CISA ADDS THREE SUPPLY CHAIN VULNERABILITIES TO KNOWN EXPLOITED VULNERABILITIES CATALOGUE
CISA FLAGS ACTIVE EXPLOITATION OF PAN-OS GLOBALPROTECT VPN AUTHENTICATION BYPASS
SHINYSPIDER DISTRIBUTES ILLUSION 2.6.5 INFOSTEALER AND RAT UNDER SILENT MAAS MODEL
TRUSTED AI PLATFORMS ABUSED AS MALWARE DELIVERY VECTORS THROUGH SOCIAL ENGINEERING
XWORM V7.4 CAMPAIGN DEPLOYS PYINSTALLER LOADER WITH AMSI BYPASS
MICROSOFT EXPOSES FOX TEMPEST MSAAS OPERATION DISTRIBUTING SIGNED RANSOMWARE AND INFOSTEALERS

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