TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: November 24, 2026



TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

With November 2026 well underway, the cyber threat landscape shows no sign of easing, as threat actors engineer increasingly sophisticated and well-coordinated campaigns across deeply interconnected digital environments. Traditional defence models are struggling to keep pace as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now depends on organisations reinforcing foundational security controls, adopting layered defence strategies, and embedding forward-looking intelligence throughout their operational frameworks.

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

INTRODUCTION

FAKE SERVICE ALERTS EXPLOIT REAL MICROSOFT 365 OUTAGE TO HARVEST LOGIN CREDENTIALS

BEAST RAAS DELETES SHADOW COPIES AND ENCRYPTS WINDOWS, NAS, AND VMWARE SYSTEMS

EMERGING CITRUS RANSOMWARE HIDES TRAFFIC AND USES AI-ASSISTED SCRIPTING TO ENCRYPT FILES

METAENCRYPTOR OPERATION TARGETS WINDOWS SYSTEMS USING DOUBLE-EXTORTION TACTICS

NEW AFFILIATE-DRIVEN DARK PROJECT RAAS STEALS AND ENCRYPTS DATA TO PRESSURE VICTIMS

MALICIOUS ADS IN STREAMING APPS DELIVER MIRAX TROJAN THAT DRAINS BANK ACCOUNTS REMOTELY

ESXI FRAMEWORK TURNS COMPROMISED HYPERVISORS INTO A SINGLE ATTACKER CONTROL PANEL

AI PENETRATION-TESTING ANTIFOX PLATFORM CHAINS WEB SHELLS TO STEAL AWS PRODUCTION SECRETS

STORM-2603 GROUP ABUSES SHAREPOINT FLAWS TO HIDE FILELESS BACKDOOR INSIDE IIS PROCESS

ARCTICRAT PAIRS HIDDEN REMOTE CONTROL WITH AI-DRIVEN FINANCIAL DATA THEFT

TATA COMMUNICATIONS

Attackers exploit Microsoft 365 outage with phishing emails citing real incident details

Microsoft Threat Intelligence has warned of an active phishing campaign exploiting the Microsoft 365 service disruption that began on 12 November 2026. The fraudulent messages impersonate Microsoft 365 service health notifications and cite the genuine Exchange Online incident, EX1550543, to appear credible. Subject lines follow an “Outage” pattern with a six-character code, while sender names mimic organisation-specific service alerts.

The emails falsely claim that messages held during the outage will be deleted within 24 hours unless recipients click a “Restore messages” link, which leads to a credential-harvesting page. Microsoft, which confirmed that the outage was a technical fault, has linked three domains to the campaign. Users should verify service notices only via the admin centre.

ATTACK TYPE	Phishing	**SECTOR**	IT, Healthcare, Government, Transportation, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Global	**APPLICATION**	Microsoft 365, Windows 11

Source - https://gbhackers.com/microsoft-warns-hackers-are-exploiting-microsoft-365-outage/

Beast affiliates customise attacks on Windows, NAS, and VMware systems

Beast is a ransomware-as-a-Service operation attributed to the threat actor Hyadina and regarded as the successor to the earlier Monster ransomware. Promoted on underground forums, it targets Windows systems, network-attached storage devices, and VMware ESXi hypervisors. A modular offline builder lets affiliates generate customised payloads for each platform, making Beast a flexible and persistent threat to enterprise environments.

On Windows, Beast encrypts files using ChaCha20 paired with Curve25519 key protection, while terminating dozens of critical services and processes to unlock files for encryption. It deletes Volume Shadow Copies and empties the Recycle Bin to frustrate recovery. With activity reported through 2026, Beast poses a serious availability risk. Organisations should maintain tested, offline backups and segment networks.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, Government, Transportation, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Global	**APPLICATION**	VMware ESXi, Windows

Source - https://gbhackers.com/beast-ransomware-attack/

TATA COMMUNICATIONS

New Citrus ransomware disguises command traffic as HTTPS to evade network defences

A threat research team has documented Citrus, a previously undescribed ransomware group targeting organisations in the financial, agricultural, and retail sectors, primarily in Russia. The group typically gains entry through compromised contractor credentials and infrastructure misconfigurations, then uses the Xray tool to establish reverse VLESS tunnels that disguise command-and-control traffic as ordinary HTTPS, helping its activity blend into legitimate network flows.

Citrus relies on the Go-based Sn00py ransomware-as-a-service trojan, deployed across domains via malicious Group Policy Objects that also disable Microsoft Defender. Researchers observed LLM-assisted scripting and vulnerability exploitation throughout the intrusions. After exfiltrating sensitive data, Sn00py encrypts files with a .citrus extension and threatens to disclose them publicly. Organisations should enforce strict contractor access controls, segment networks, and maintain offline backups.

ATTACK TYPE	Ransomware, Emerging Threats	**SECTOR**	BFSI, Retail and Distribution
REGION	Russia	**APPLICATION**	Microsoft Active Directory Services, Telegram

Source - https://securelist.com/citrus-ransomware/121879/

TATA COMMUNICATIONS

Veteran MetaEncryptor ransomware continues data theft and extortion against Windows systems

MetaEncryptor is a double-extortion ransomware operation first observed in 2023, targeting organisations through data theft, public disclosure threats, and reported Windows-based file encryption. Researchers have linked it to the SFile ransomware family and the Mindware operation and consider the latter a rebrand of the LostTrust group. Its tradecraft includes credential theft, remote command execution, and system manipulation to enable encryption.

Recent victim claims span the healthcare, construction, and manufacturing sectors, including a medical technology firm named on its leak site in September 2026. While its leak site remained active with postings into late 2026, no new file-encryption activity has been confirmed during the year, suggesting a possible shift towards pure data-theft extortion. Organisations should harden remote access, enforce multi-factor authentication, and maintain offline backups.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, Manufacturing, Transportation, Energy, Broadcast Media Production and Distribution
REGION	Global	**APPLICATION**	Microsoft Active Directory Services, Microsoft Exchange Server, Microsoft SharePoint Server, Microsoft SQL Server, PostgreSQL, VMware ESXi, Windows, Apache Tomcat, PowerShell

Source - https://www.provendata.com/blog/metaencryptor-ransomware

TATA COMMUNICATIONS

Emerging Dark Project RaaS lures affiliates with an 80% cut of extortion payments

Dark Project is an emerging, financially motivated ransomware operation first observed in June 2026, running on a ransomware-as-a-service model. According to threat intelligence firms, it targets Windows environments through phishing, exposed RDP, compromised credentials, and VPN access. The group advertises an aggressive affiliate programme, passing partners 80% of proceeds while retaining 20% for infrastructure and negotiations.

Operating a double-extortion strategy, Dark Project exfiltrates sensitive data before encrypting systems, then threatens publication via its Tor-based leak portal. That site currently lists 38 alleged victims across eight countries, predominantly US manufacturing and healthcare organisations, though such claims remain unverified and serve partly as marketing. Organisations should enforce multi-factor authentication, secure remote access, and maintain tested offline backups.

ATTACK TYPE	Ransomware, Emerging Threats
REGION	Canada, UK, Brazil, Germany, Mexico, Philippines, Turkey, United States
SECTOR	Healthcare, BFSI, Manufacturing, Entertainment, Construction, Transportation, Retail and Distribution
APPLICATION	Windows, Cisco Secure Firewall, ScreenConnect, ConnectWise

Source- https://gbhackers.com/dark-project-ransomware/

TATA COMMUNICATIONS

Streaming app ads deliver Mirax Android trojan that intercepts OTPs and controls devices

Researchers have documented Mirax, an Android device-takeover trojan that infected thousands of retail banking customers across the META region between March and September 2026, with estimated losses in the millions. Distributed via malicious advertisements inside streaming applications, the malware impersonates Google Play Services and pressures victims into granting Accessibility Service permissions, the pivotal step enabling full device control.

Once active, Mirax steals credentials through overlay injection, intercepts OTPs from SMS and notifications, logs keystrokes, and captures the device PIN. Banking overlays are pushed from command-and-control servers after installation. Because fraudulent transfers originate from the victim's own device and genuine banking session, they can appear legitimate. Users should refuse Accessibility requests from entertainment apps and avoid advertised downloads.

ATTACK TYPE	Social Engineering, Cyber Crime, Phishing, Malware, Mobile	**SECTOR**	E-Commerce, BFSI, Cryptocurrency
REGION	Middle East, Africa, Turkey	**APPLICATION**	Android

Source - https://securityonline.info/mirax-android-rat/

TATA COMMUNICATIONS

GhostFrame post-exploitation malware gives attackers control over ESXi virtualisation layer

A research group has uncovered GhostFrame, a previously undocumented post-exploitation framework targeting VMware ESXi hypervisors and attributed to the threat activity group TAG-218. GhostFrame does not exploit a vulnerability. It requires pre-existing root-level access to an ESXi host. From there, it provides a single control panel to reach every virtual machine running on the compromised hypervisor.

To maintain persistence, the framework modifies boot scripts, masquerades its process as the legitimate vmhostd daemon, and tampers with host security controls. Its capabilities span credential harvesting, virtual machine manipulation, and network pivoting. TAG-218 activity overlaps with the Settra ransomware operation, posing a serious risk to virtualised enterprises. Organisations should monitor ESXi hosts closely and treat virtualisation infrastructure as a high-value target.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	IT, Healthcare, Government, Transportation, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Europe, United States	**APPLICATION**	Palo Alto Networks GlobalProtect, VMware ESXi, Fortinet, SonicWall

Source - https://www.recordedfuture.com/blog/ghostframe-esxi-implant-settra-ransomware

TATA COMMUNICATIONS

Open-source AI penetration-testing AntiFox under attack for AWS credentials and secrets theft

Arctic Wolf Labs has linked AntiFox, an open-source autonomous penetration-testing platform derived from ARTEX, to real-world attacks against internet-facing web applications and AWS environments. Self-hosted by threat actors on Alibaba Cloud, the agentic framework was observed compromising Microsoft IIS applications, where the w3wp.exe worker process deployed an ASPX web shell and executed commands to discover application credentials and configuration files.

Using valid AWS IAM identities, the attackers performed automated cloud-service enumeration, generating hundreds of API requests within 30 minutes to probe permissions. They successfully accessed production secrets and carried out S3 object operations, underscoring how agentic AI frameworks are accelerating multi-stage intrusions. Organisations should rotate exposed credentials, enforce least-privilege IAM policies, and correlate web-shell activity with unusual cloud API bursts.

ATTACK TYPE	**Cyber Crime, Breaches, Misconfiguration, Emerging Threats**
REGION	**Global**
SECTOR	**IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications**
APPLICATION	**Microsoft Internet Information Services (IIS), Amazon EC2, Amazon S3, AWS IAM, Windows**

Source - https://thehackernews.com/2026/11/antifox-ai-pentesting-platform-linked.html

TATA COMMUNICATIONS

Storm-2603 exploits SharePoint flaws to run fileless backdoor inside IIS server memory

Researchers have detailed an intrusion by Storm-2603, a China-based group linked to Warlock ransomware, which exploited Microsoft SharePoint's ToolShell vulnerabilities to achieve unauthenticated remote code execution. The attackers injected a memory-resident implant (writing no conventional web shell to disk) directly into the IIS worker process and ASP.NET runtime, leaving no reliable file-based artefacts for defenders to find.

The attackers then established remote access through legitimate administration and tunnelling tools, decoupling their foothold from the web shell and the IIS lifecycle. This meant that patching SharePoint and recycling the application pool alone would not evict them. The campaign culminated in an attempted ransomware deployment. Organisations should preserve memory and IIS telemetry, rotate machine keys, and hunt proactively.

ATTACK TYPE	Ransomware, Malware, APT	**SECTOR**	IT, Healthcare, Government, Transportation, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Global	**APPLICATION**	Microsoft SharePoint Server, Windows

Source - https://gbhackers.com/storm-2603-attack/

TATA COMMUNICATIONS

Crypto-stealer ArcticRAT evolves into AI-powered Android RAT with remote device control

Researchers have detailed ArcticRAT, an Android remote access trojan that has evolved from a narrow cryptocurrency stealer into a broad financial-theft platform. In samples from mid-July 2026, it integrates xAI's grok-4.20-0309-non-reasoning model to automate analysis of stolen SMS messages and installed applications, identifying banking and trading applications, and extracting one-time passcodes, balances, and transfer alerts.

Distributed through phishing websites and fake applications, ArcticRAT abuses Android Accessibility Services and Wireless ADB to gain remote control, operating the device behind black overlays while the victim believes it is locked. It deploys credential-stealing overlays, keylogging, and deceptive ransomware screens, though no actual encryption occurs. Organisations should warn users against sideloading apps and enforce mobile threat defence.

ATTACK TYPE	Phishing, Malware, Mobile	**SECTOR**	BFSI, Investment Management, Trading, Cryptocurrency
REGION	Global	**APPLICATION**	Android

Source - https://zimperium.com/blog/arcticrat-ai-powered-android-rat

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.