TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 14, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

Organisations have observed an unprecedented escalation in AI-powered social engineering offensives, meticulously coordinated supply chain compromises, and progressively sophisticated ransomware iterations throughout Q2 FY25. This constitutes definitive proof that traditional security protocols are fundamentally insufficient for contemporary threat environments. As we advance into the final months of FY25, cyber adversaries persist in amplifying their advanced campaigns with relentless determination. Therefore, sustaining cyber resilience requires that businesses strengthen their core security infrastructure whilst deploying comprehensive, intelligence-led defensive systems capable of anticipating and countering evolving threats.

Tata Communications' weekly threat intelligence updates are specifically designed to equip your security teams with this tactical superiority. Each report provides timely threat evaluations and actionable recommendations, enabling you to detect, prioritise, and neutralise vulnerabilities before they can disrupt your operational effectiveness.

INTRODUCTION

MULTI-STAGED GOVERNMENT CHAIN ATTACK LEVERAGES REMOTE ACCESS TROJANS

SOPHISTICATED CREDENTIAL THEFT MALWARE ACREED GAINS CYBERCRIME MOMENTUM

CROSS-PLATFORM LOCKBIT CAMPAIGN TARGETS WINDOWS, LINUX, AND ESXI SYSTEMS GLOBALLY

COUNTERFEIT MESSAGING APPLICATIONS EXPLOIT SIGNAL AND TOTOK USERS

MULTI-STAGE LUNAR SPIDER ATTACK CAMPAIGN TARGETS ENTERPRISE CREDENTIAL THEFT

UAT-8099 THREAT ACTORS DEPLOY APPS FOR LARGE-SCALE ADVERTISING FRAUD

NEW CERT-UA PHISHING CAMPAIGN EXPLOITS EXCEL ADD-IN VULNERABILITY

ZERO-DAY VULNERABILITY TARGETS ORACLE BUSINESS SUITE SYSTEMS IN DATA THEFT ATTACKS

PERSISTENT RAYINITIATOR BOOTKIT ENABLES STEALTHY NETWORK DEVICE COMPROMISE

CUSTOM NET-STAR MALWARE SUITE ENABLES LONG-TERM INTELLIGENCE OPERATIONS

State-sponsored Cavalry Werewolf campaigns deploy advanced RAT malware

From May to August 2025, in an active campaign, Cavalry Werewolf executed targeted phishing assaults masquerading as Kyrgyz government officials to infiltrate Russian state agencies and entities in energy, mining, and manufacturing sectors. Attack vectors included RAR attachments and compromised mailboxes delivering custom tools such as FoalShell reverse shells and StallionRAT, the latter controlled via Telegram C2 channels.

Detection efforts highlight telltale indicators of compromise: Outlook cache anomalies, suspicious cmd.exe launches, PowerShell executions with encoded command, and persistent binaries under C:\Users\Public\Libraries. The adversaries also installed persistence via Run-key registry entries, used SOCKS5 proxies, and launched tools like AsyncRAT, extending targeting beyond Russia into Tajikistan and Middle Eastern nations.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Manufacturing, Government, Energy, Mining
REGION	Middle East, Russia, Tajikistan	**APPLICATION**	Microsoft Outlook, Windows, PowerShell

Source - https://bi.zone/eng/expertise/blog/cavalry-werewolf-atakuet-rossiyu-cherez-doveritelnye-otnosheniya-mezhdu-gosudarstvami/?utm_source=x&utm_medium=social&utm_campaign=cavalry-werewolf-atakuet-rossiyu-cherez-doveritelnye-otnosheniya-mezhdu-gosudarstvami

TATA COMMUNICATIONS

Advanced Acreed infostealer exploits Blockchain for command control

First observed in early 2025, Acreed has rapidly gained traction across Russian language fora and dark web markets following Lumma's disruption. Distributed via loaders such as ShadowLoader, Acreed retrieves C2 information through unconventional dead drop channels, notably BNB Smart Chain Testnet records and abused Steam profile data, techniques that enhance persistence, frustrate takedown and improve operator OPSEC and covert communications.

Acreed primarily harvests browser data, cookies, autofill credentials, and cryptocurrency wallets, producing compact logs favoured for fraud and account takeover. Analysis reveals infrastructure overlap with Vidar and links to ProManaged LLC and bulletproof hosting providers, suggesting Acreed leverages established criminal services and resale channels. These ties have accelerated its market share growth and operational maturity among organised cybercrime actors globally.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Financial services, Manufacturing, IT, Education, E-Commerce, BFSI, Retailer, and Distributor
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, PowerShell

Source - https://www.intrinsec.com/wp-content/uploads/2025/09/TLP-CLEAR-Sept-2025-Acreed-infostealer-EN.pdf

TATA COMMUNICATIONS

Notorious LockBit 5.0 operation threatens enterprise virtualisation infrastructure

LockBit 5.0 embodies a significantly evolved cross-platform threat, combining new technical stealth with wide attack reach. The Windows variant leverages heavy obfuscation and DLL reflection while terminating security services and clearing event logs via ETW patching and EvtClearLog APIs. The Linux variant mirrors its functionality, offering command-line granularity for encryption targeting and exclusion logic.

The dedicated ESXi build represents a strategic escalation: it enables mass encryption of virtual machines in a single strike. Its CLI parallels Windows and Linux variants, with parameters optimised for VM infrastructures. Despite the disruption of Operation Cronos, LockBit has reemerged with greater sophistication, posing acute dangers to enterprises and virtualisation environments alike.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Financial services, Manufacturing, Construction, IT, Government, Transportation, Internet Service Provider, Energy, Defence Industry, E-Commerce, BFSI, Aviation, Broadcast Media Production and Distribution, Retailer and Distributor
REGION	Global	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - https://www.trendmicro.com/en_us/research/25/i/lockbit-5-targets-windows-linux-esxi.html

TATA COMMUNICATIONS

Sophisticated Android spyware disguised as legitimate messaging applications

Threat analysts have identified two sophisticated Android spyware campaigns, ProSpy and ToSpy, targeting UAE users through fake Signal and ToTok apps. Both malware families are delivered via deceptive websites and third-party app stores, bypassing official channels. ProSpy presents itself as Signal plugins or ToTok Pro, while ToSpy impersonates ToTok via fake Galaxy Store pages. These spyware programs exfiltrate contacts, SMS, media files, and ToTok chat backups, using advanced persistence and social engineering tactics to remain undetected.

ProSpy, active since 2024, and ToSpy maintain ongoing command-and-control connections to continuously harvest data. ToSpy specifically targets .ttkmbackup files, enabling the extraction of ToTok chat history. Both campaigns exploit manual APK installations and mimic legitimate app onboarding processes, including redirections to official apps, to enhance perceived authenticity. Researchers have shared these findings with Google, and Android devices are protected through Google Play Protect against known variants of these spyware families.

ATTACK TYPE	Malware, Mobile	**SECTOR**	Business, Telecommunications
REGION	Netherlands, United Arab Emirates, United States	**APPLICATION**	Android

Source - https://www.welivesecurity.com/en/eset-research/new-spyware-campaigns-target-privacy-conscious-android-users-uae/

Prolonged Lunar Spider cyber intrusion uses layered attack techniques

In May 2024, a sophisticated cyber intrusion attributed to the Lunar Spider threat actor commenced when a user executed a malicious JavaScript file disguised as a W-9 tax form. This obfuscated script initiated the download of an MSI installer, which deployed the Brute Ratel loader. Subsequently, Brute Ratel injected the Latrodectus malware into the explorer.exe process, establishing command and control (C2) communications through multiple Cloudflare-proxied domains. Within an hour, the attackers initiated reconnaissance activities using native Windows commands such as ipconfig, systeminfo, nltest, and whoami.

Over the next several weeks, the threat actor escalated their access by deploying a custom .NET backdoor and a Cobalt Strike beacon, facilitating lateral movement and persistence within the network. Credential harvesting was conducted from various sources, including LSASS, backup software, browsers, and Windows Answer files. Approximately 20 days into the intrusion, data exfiltration commenced using Rclone and FTP. Despite the extensive access and prolonged dwell time, no ransomware deployment was observed during this nearly two-month-long intrusion.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Financial services, Manufacturing, IT, Energy, Defence Industry, Business, BFSI, IT Services and Consulting, Retailer and Distributor
REGION	Global	**APPLICATION**	Chromium, Windows, Veeam, Veeam Backup Enterprise Manager

Source - https://thedfirreport.com/2025/09/29/from-a-single-click-how-lunar-spider-enabled-a-near-two-month-intrusion/

TATA COMMUNICATIONS

Cybercrime UAT-8099 group exploits IIS servers for SEO fraud and credential theft

Researchers have uncovered a sophisticated global ad fraud operation, dubbed "SlopAds," orchestrated through 224 AI-themed applications. These apps amassed over 38 million downloads across 228 countries, including the U.S., India, and Brazil. Managed via command-and-control servers and promotional domains, they employed advanced techniques such as Firebase Remote Config, steganography, and encrypted configurations to conceal malicious activities. The malware, identified as FatModule, was delivered through hidden WebViews and exploited attribution mechanisms to generate fraudulent ad traffic.

At its peak, SlopAds was responsible for generating 2.3 billion daily bid requests, significantly impacting advertising ecosystems. The fraudulent activities led to degraded device performance, including sluggishness, battery drain, and weakened connections. In response to these findings, Google has removed the implicated applications from the Play Store, and Play Protect now actively blocks them to safeguard users. This disruption highlights the evolving challenges in combating AI-driven ad fraud and underscores the need for continuous vigilance in mobile security.

ATTACK TYPE	Malware	**SECTOR**	IT, Education, Telecommunications
REGION	Canada, India, Brazil, Thailand, Vietnam	**APPLICATION**	Android, Apple IOS, Microsoft Internet Information Services (IIS)

Source - https://blog.talosintelligence.com/uat-8099-chinese-speaking-cybercrime-group-seo-fraud/

TATA COMMUNICATIONS

CERT-UA Excel-based attack vector delivers a persistent backdoor threat

CERT-UA has reported a sophisticated cyber campaign distributing malicious Excel add-ins (XLLs) via Signal-shared ZIP files. Once executed, the XLL installs a randomly named runner executable in Startup, drops BasicExcelMath.xll into %APPDATA%\Microsoft\Excel\XLSTART, and configures both a Run registry entry and a scheduled task to launch Excel with the /e parameter, ensuring the add-in auto-loads. This attack enables persistent system compromise.

The loader subsequently extracts embedded shellcode from an Office.png file to deploy CABINETRAT, a TCP-based backdoor. This malware collects system information, executes arbitrary commands, captures screenshots, and facilitates file transfers. The campaign, tracked as UAC-0245, incorporates extensive anti-analysis and anti-virtualisation mechanisms, highlighting the attackers' intent to evade detection while maintaining a durable presence on compromised systems.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Financial services, Manufacturing, IT, Government, Energy, Defence Industry, Business, BFSI, Aviation, Software Development
REGION	Ukraine	**APPLICATION**	Microsoft Excel, Windows

Source - https://cert.gov.ua/article/6285549

TATA COMMUNICATIONS

Critical Oracle zero-day vulnerability enables remote code execution

Oracle has issued an urgent security alert for CVE-2025-61882, a critical zero-day vulnerability in Oracle E-Business Suite's Concurrent Processing module (BI Publisher Integration), rated CVSS 9.8. The flaw allows unauthenticated remote code execution and has been actively exploited by the Clop ransomware gang in August 2025. Oracle's emergency patch requires the installation of the October 2023 CPU beforehand, as public PoCs and IOCs confirm ongoing exploitation targeting enterprise systems.

Clop's attack leveraged Python-based scripts to gain remote shell access, resulting in extensive data theft from affected Oracle EBS servers. Oracle versions 12.2.3–12.2.14 are impacted. Threat intelligence from Mandiant and Google GTIG highlights that Clop combined this zero-day with previously patched vulnerabilities to steal sensitive corporate data. Administrators are strongly urged to apply Oracle's security updates immediately to mitigate risk and prevent further compromise.

ATTACK TYPE	Vulnerability, Ransomware	**SECTOR**	Financial services, Manufacturing, Government, Retailer, and Distributor
REGION	Global	**APPLICATION**	Oracle E-business Intelligence, Oracle

Source - https://www.bleepingcomputer.com/news/security/oracle-patches-ebs-zero-day-exploited-in-clop-data-theft-attacks/

TATA COMMUNICATIONS

RayInitiator bootkit and LINE VIPER loader emerge as critical Cisco ASA threats

RayInitiator is a persistent multistage GRUB bootkit targeting Cisco ASA 5500 X devices that lack secure boot. Flashed to GRUB, it survives reboots and firmware upgrades and patches the ASA loader and kernel to install a handler inside the lina process. The bootkit uses WebVPN authentication vectors and victim-specific tokens to load and execute the LINE VIPER shellcode in memory.

LINE VIPER is an x64 user-mode shellcode loader that can be tasked via WebVPN authentication over HTTPS or ICMP with TCP responses. It uses per-victim RSA keys for encrypted tasking and exfiltration. Modules enable CLI command execution, packet capture, AAA bypass, credential harvesting and syslog suppression. The NCSC describes this as a significant evolution from LINE DANCER and LINE RUNNER.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	Healthcare, Financial services, Manufacturing, Construction, IT, Government, Defence Industry, Business, BFSI, Aviation, Retailer, and Distributor
REGION	Global	**APPLICATION**	Cisco ASA

Source - https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/RayInitiator-LINE-VIPER/ncsc-mar-rayinitiator-line-viper.pdf

Phantom Taurus APT deploys NET-STAR malware in espionage operations

Phantom Taurus was elevated from cluster CL-STA-0043 to a distinct Chinese APT actor following sustained monitoring by Unit 42. The group has operated since 2022 against ministries, embassies, telecoms, and government bodies in Africa, the Middle East and Asia, reflecting alignment with PRC strategic goals.

Its newly identified NET-STAR malware suite provides advanced stealth via fileless IIS backdoors and modular .NET payload execution. Phantom Taurus has evolved its tactics to target databases using scripts like mssq.bat, leveraging WMI and in-memory execution to sustain long-term espionage while evading detection.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Government, Defence Industry, Telecommunications
REGION	Middle East, Africa, Asia, South Asia	**APPLICATION**	Microsoft Internet Information Services (IIS), Microsoft SQL Server

Source - https://unit42.paloaltonetworks.com/phantom-taurus/

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