TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: DECEMBER 2, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As the final quarter of 2025 advances, the cyber threat landscape is escalating, driven by the accelerating scale and sophistication of the emerging vulnerabilities. Traditional defence models are proving insufficient as adversaries exploit structural weaknesses across highly interconnected digital ecosystems. To preserve resilience and strategic advantage, organisations must reinforce foundational security frameworks, deploy multi-layered defences, and embed anticipatory intelligence across their architectures.

In this high-risk environment, Tata Communications' Cyber Threat Intelligence report becomes essential. Published weekly, it provides incisive analysis of emerging attack campaigns, shifting adversarial tactics, and sector-specific exposures. By converting intelligence into immediate defensive action, the bulletin enables security teams to anticipate, prepare for, and neutralise threats proactively — protecting critical operations before disruption takes hold.

INTRODUCTION
SHADOWPAD MALWARE SPREADS VIA MICROSOFT WSUS VULNERABILITY ABUSE
CREDENTIAL-BASED RDP BREACH LEADS TO LYNX RANSOMWARE DEPLOYMENT
ADVANCED RANSOMWARE SHINYSP1D3R FEATURES MULTI-PLATFORM CAPABILITIES
EMERGING GENTLEMEN RAAS OFFERS AFFILIATES ADVANCED ENCRYPTION ARSENAL
OAUTH TOKEN ABUSE TARGETS GAINSIGHT-SALESFORCE INTEGRATION PLATFORMS
ORACLE IDENTITY MANAGER RCE ADDED TO KEV (CVE-2025-61757) CATALOGUE
COVERT LOADER CHAINS DELIVER STEALTHY FDMTP BACKDOOR PAYLOAD
SPOOFED VPN INSTALLER DELIVERS SOPHISTICATED NKNSHELL BACKDOOR MALWARE
GH0ST RAT DEPLOYED VIA MULTI-STAGE RONINGLOADER ATTACK
ETERNIDADE SPREADS USES IMAP C2 INFRASTRUCTURE THROUGH MESSAGING

TATA COMMUNICATIONS

WSUS (CVE 2025 59287) vulnerability leveraged for deploying ShadowPad backdoor

As disclosed by security intelligence centres, the recently patched vulnerability CVE-2025-59287 in Microsoft Windows Server Update Services (WSUS) has already been weaponised in the wild. Attackers exploited unsafe deserialization to gain SYSTEM-level access on WSUS-enabled servers, then used PowerCat to obtain a remote shell. They followed up by downloading and installing the ShadowPad backdoor via standard Windows tools such as certutil and curl — a chain that allows full, unauthenticated remote code execution with minimal friction.

Once inside, the attackers deployed ShadowPad via DLL sideloading — using a legitimate binary (ETDCtrlHelper.exe) to load a malicious DLL (ETDApix.dll) — and established persistence via registry entries, scheduled tasks, services, and multiple execution paths. This staged, 'living-off-the-land' workflow illustrates how native OS tools and sideloading techniques are leveraged to maintain stealthy, system-level control — underlining the urgent need for organisations to patch WSUS immediately, restrict exposed access, and hunt for signs of PowerShell, certutil, curl or unusual network activity.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	Healthcare, Financial services, Manufacturing, IT, Government, Transportation, Education, Energy, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	Windows

Source - https://asec.ahnlab.com/ko/91101/

INTRODUCTION
SHADOWPAD MALWARE SPREADS VIA MICROSOFT WSUS VULNERABILITY ABUSE
CREDENTIAL-BASED RDP BREACH LEADS TO LYNX RANSOMWARE DEPLOYMENT
ADVANCED RANSOMWARE SHINYSP1D3R FEATURES MULTI-PLATFORM CAPABILITIES
EMERGING GENTLEMEN RAAS OFFERS AFFILIATES ADVANCED ENCRYPTION ARSENAL
OAUTH TOKEN ABUSE TARGETS GAINSIGHT-SALESFORCE INTEGRATION PLATFORMS
ORACLE IDENTITY MANAGER RCE ADDED TO KEV (CVE-2025-61757) CATALOGUE
COVERT LOADER CHAINS DELIVER STEALTHY FDMTP BACKDOOR PAYLOAD
SPOOFED VPN INSTALLER DELIVERS SOPHISTICATED NKNSHELL BACKDOOR MALWARE
GH0ST RAT DEPLOYED VIA MULTI-STAGE RONINGLOADER ATTACK
ETERNIDADE SPREADS USES IMAP C2 INFRASTRUCTURE THROUGH MESSAGING

TATA COMMUNICATIONS

Lynx ransomware strikes credential-driven intrusion across enterprise systems

As reported by threat analysts, the intrusion began in early March 2025 when a threat actor used pre-compromised credentials to access an exposed RDP server, bypassing brute-force or password-spray detection. Within minutes, they moved laterally to a domain controller using a second compromised domain administrator account, created multiple impersonation-style privileged accounts and added them to high-privilege groups. Over the ensuing days, they mapped out virtual infrastructure and network shares, extensively scanned the environment with SoftPerfect NetScan and NetExec tools, and identified hypervisors, file- and backup-servers for further exploitation.

After six days, the attackers compressed and exfiltrated sensitive files from multiple network shares to the temporary-sharing site temp.sh, then returned to delete backup jobs and deploy Lynx ransomware across multiple file and backup servers — with the full intrusion spanning nine days and a Time-to-Ransomware of approximately 178 hours. This attack is consistent with previously observed Lynx variants operating under a Ransomware-as-a-Service model, noted for double-extortion tactics, deletion of backups and shadow copies, and targeting corporate networks via exposed remote services.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Manufacturing, IT, Government, Education, Energy, E-Commerce, BFSI, Aviation, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Active Directory Services, Windows, Veeam , Veeam Backup Enterprise Manager

Source - https://thedfirreport.com/2025/11/17/cats-got-your-files-lynx-ransomware/

TATA COMMUNICATIONS

Emerging ShinySp1d3r RaaS threatens global Windows, Linux, and ESXi systems

ShinySp1d3r, a new ransomware-as-a-service under development by ShinyHunters and their allies in the Scattered LAPSUS$ Hunters collective, has recently surfaced — researchers obtained an early build via VirusTotal uploads. The encryptor, built from scratch rather than borrowed from established codebases, already demonstrates advanced capabilities: ETW-logging evasion, forced termination of file-locking processes, network propagation across shares and via WMI, free-space wiping, shadow-copy deletion, and ChaCha20/RSA-2048 per-file encryption.

Initial samples target Windows, but documentation shows that Linux, VMware ESXi and even a high-speed “lightning” ASM variant are planned — signalling broad ambitions for multi-platform impact. Once deployed, encrypted directories will carry a ransom note, and victims will face a warning wallpaper as part of the extortion routine. As such, ShinySp1d3r represents a serious emerging threat to enterprise networks and virtualised infrastructure, underscoring the urgent need for organisations to review and harden their security posture.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Manufacturing, IT, Government, E-Commerce, BFSI, Aviation, Broadcast Media Production, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - https://www.bleepingcomputer.com/news/security/meet-shinysp1d3r-new-ransomware-as-a-service-created-by-shinyhunters/

Multi-platform Gentlemen ransomware targets ESXi with dual extortion

As first reported by security researchers in July 2025, the newly emerged Gentlemen ransomware group has swiftly grown into a formidable Ransomware-as-a-Service (RaaS) operation. Within months, it has targeted organisations across multiple industries, combining dual-extortion tactics — encrypting critical files while exfiltrating sensitive business data — and threatening to publish stolen information if demands are not met.

What distinguishes The Gentlemen is its technical sophistication and versatility. Its toolkit delivers cross-platform lockers for Windows, Linux and ESXi environments, supports self-restart and run-on-boot persistence, and allows configurable encryption speeds. Propagation relies on legitimate administrative tools like WMI, PowerShell remoting and SCHTASKS, while built-in anti-forensics, EDR-kill routines and silent mode operations ensure deep stealth and persistence.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Manufacturing, IT, Government
REGION	Global	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - https://www.cybereason.com/blog/the-gentlemen-ransomware

Scattered Lapsus$ Hunters campaign pivot through Salesforce OAuth tokens

As recent investigations into the Salesforce–Gainsight incident deepen, it has emerged that attackers exploited stolen OAuth tokens — originally pilfered during the Scattered Lapsus$ Hunters' August 2025 breach of Salesloft — to gain unauthorised access to Salesforce-linked environments via Gainsight-published applications. In response, Salesforce promptly revoked all active access and refresh tokens tied to Gainsight apps and removed them from its AppExchange marketplace, underscoring that the breach stemmed from third-party integration abuse, not a flaw in Salesforce's core platform.

Gainsight has engaged Mandiant to conduct a full forensic investigation after evidence surfaced of unauthorised data-access attempts possibly impacting over 200 customer instances, according to analysts at Google Threat Intelligence Group (GTIG). As the cybersecurity community scrutinises this supply-chain style incident, organisations using third-party integrations with Salesforce are urged to re-examine all connected applications, revoke or rotate OAuth credentials, and audit logs for suspicious activity, to safeguard against further escalations.

ATTACK TYPE	Vulnerability, Breaches	**SECTOR**	Tourism, Manufacturing, Entertainment, IT, Government, Education, Business, BFSI, Aviation, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	Salesloft- Drift, Salesforce

Source - https://help.salesforce.com/s/articleView?id=005229029&type=1

Pre-authenticated Groovy compile-time RCE targets Oracle Identity Manager

As of 21 November 2025, the Cybersecurity & Infrastructure Security Agency (CISA) has formally added Oracle Identity Manager (OIM) vulnerability CVE-2025-61757 to its Known Exploited Vulnerabilities (KEV) catalogue following confirmed reports of active exploitation in the wild. This critical pre-authentication remote code execution flaw affects OIM versions 12.2.1.4.0 and 14.1.2.1.0 and stems from a weakness in its REST API layer.

Security researchers at Searchlight Cyber demonstrated that attackers can bypass authentication simply by appending "?WSDL" or ";.wadl" to a URL — tricking OIM's URI filter into treating protected endpoints as publicly accessible. Once access is gained, a Groovy compilation endpoint can be abused to execute arbitrary code without valid credentials, granting full takeover potential. Oracle issued a patch on 21 October 2025; under Binding Operational Directive 22-01, U.S. Federal Civilian Executive Branch agencies must remediate by 12 December 2025.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, Manufacturing, IT, Government, Business, BFSI, Airlines, Mining, Retailer and Distributor, Logistics
REGION	Global	**APPLICATION**	Oracle Identity Management

Source - https://www.bleepingcomputer.com/news/security/cisa-warns-oracle-identity-manager-rce-flaw-is-being-actively-exploited/

TATA COMMUNICATIONS

FDMTP backdoor campaign leverages compromised router infrastructure for C2

The FDMTP backdoor has been found actively deployed through a coordinated scheme utilising C++ loaders, patched Windows executables, and PowerShell-based shellcode. The threat actors are leveraging a SoftEther VPN network — likely hosted on compromised routers — to obscure command-and-control routing. Shared metadata and consistent development patterns across infections suggest a unified toolkit, raising serious concerns about targeted supply-chain or infrastructure-level intrusions.

Post-exploitation activities linked to FDMTP have been expanded via Cobalt Strike, enabling stealthy persistence, remote access, and evasive C2 operations. This combination of custom loaders, VPN-backed command channels and advanced post-exploitation tools reflects a highly organised campaign. Organisations are therefore urged to review their network ingress points, monitor for unusual SoftEther VPN usage, and apply rigorous endpoint defences — especially on patched executables and systems capable of executing PowerShell payloads.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Manufacturing, IT, Government, Defence Industry
REGION	Global	**APPLICATION**	Windows

Source - CERT-In

INTRODUCTION
SHADOWPAD MALWARE SPREADS VIA MICROSOFT WSUS VULNERABILITY ABUSE
CREDENTIAL-BASED RDP BREACH LEADS TO LYNX RANSOMWARE DEPLOYMENT
ADVANCED RANSOMWARE SHINYSP1D3R FEATURES MULTI-PLATFORM CAPABILITIES
EMERGING GENTLEMEN RAAS OFFERS AFFILIATES ADVANCED ENCRYPTION ARSENAL
OAUTH TOKEN ABUSE TARGETS GAINSIGHT-SALESFORCE INTEGRATION PLATFORMS
ORACLE IDENTITY MANAGER RCE ADDED TO KEV (CVE-2025-61757) CATALOGUE
COVERT LOADER CHAINS DELIVER STEALTHY FDMTP BACKDOOR PAYLOAD
SPOOFED VPN INSTALLER DELIVERS SOPHISTICATED NKNSHELL BACKDOOR MALWARE
GH0ST RAT DEPLOYED VIA MULTI-STAGE RONINGLOADER ATTACK
ETERNIDADE SPREADS USES IMAP C2 INFRASTRUCTURE THROUGH MESSAGING

TATA COMMUNICATIONS

NKNShell backdoor emerges in VPN supply chain attack targeting domestic users

As reported by threat researchers, a South Korean VPN provider's website was compromised to distribute malware — a continuation of the long-running campaign by Larva-24010 active since 2023. The malicious installer, signed with a fraudulent NVIDIA certificate, executes a PowerShell-based payload that secretly installs multiple backdoors: a custom build of MeshAgent, a gs-netcat remote-shell tool, and a newly discovered implant called NKNShell.

NKNShell, written in Go, leverages the decentralised NKN protocol alongside MQTT — often used for IoT messaging — to communicate covertly with C2 servers, enabling remote control, system manipulation, data exfiltration, and maintenance of persistence. Alongside MeshAgent and gs-netcat, this toolset offers the attackers full system access, remote shell capability, and stealth C2 connectivity — underscoring a significant escalation in supply-chain malware sophistication and heightening risk for organisations relying on VPN-based distribution channels.

ATTACK TYPE	Malware	**SECTOR**	IT, Telecommunications
REGION	South Korea	**APPLICATION**	Windows, PowerShell

Source - https://asec.ahnlab.com/ko/91056/

TATA COMMUNICATIONS

Multi-stage RoningLoader delivers Gh0st RAT payload for stealthy espionage

As recently reported by Elastic Security Labs, the threat actor Dragon Breath (also tracked as APT-Q-27) is distributing a modified version of gh0st RAT via trojanised NSIS installers, principally targeting Chinese-speaking users. The initial installer masquerades as legitimate software (e.g., Chrome or Microsoft Teams). Once executed, a multi-stage loader — RONINGLOADER takes over, deploying a signed kernel-mode driver (ollama.sys), custom Windows Defender Application Control (WDAC) policies, and thread-pool / phantom DLL injection. This combination is designed specifically to disable major antivirus and EDR tools prevalent in the Chinese market, including Microsoft Defender and Qihoo 360.

Once defences are neutralised, the final payload — the updated gh0st RAT— executes stealthily. This campaign represents a significant escalation in sophistication compared to earlier activity by Dragon Breath, with extensive use of legitimate system mechanisms and signed drivers to bypass security protections. Given the threat's complexity and stealth, organisations — especially those with Chinese-language operations or user base — are strongly advised to update EDR/AV detection rules, monitor for signs of RoningLoader activity and enforce stricter application whitelisting and WDAC policies.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Healthcare, Hospitality, Manufacturing, IT, Government, BFSI, Retailer and Distributor
REGION	China	**APPLICATION**	Google Chrome OS, Windows, Google Chrome

Source - https://www.elastic.co/security-labs/roningloader

Delphi-based stealer Eternidade targets BFSI via WhatsApp Worm campaign

As reported by the researchers at Trustwave SpiderLabs, a novel banking malware dubbed Eternidade Stealer is spreading across Brazil via hijacked WhatsApp Web sessions. The campaign begins with an obfuscated VBScript that drops a Python-based worm, which automatically harvests victims' contact lists (filtering out groups and business accounts) and forwards malicious attachments. Once a contact interacts with the payload, an MSI installer deploys a Delphi-based stealer that only activates on systems with Brazilian Portuguese locale settings.

Once executed, Eternidade Stealer injects its payload into "svchost.exe" via process hollowing, then monitors user activity for banking or crypto-wallet applications (such as Bradesco, MercadoPago, Binance, MetaMask) before triggering overlay windows, keylogging, session tracking, and data exfiltration. The malware uses IMAP-based retrieval of dynamic command-and-control (C2) server details — with hard-coded fallback servers if needed — giving attackers resilience against takedown attempts. The campaign underscores a dangerous evolution in messaging-app-based cybercrime, demanding heightened vigilance from organisations and individuals alike.

ATTACK TYPE	Malware	**SECTOR**	Financial services, BFSI, Retailer and Distributor
REGION	Brazil	**APPLICATION**	Python, Windows, WhatsApp

Source - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/spiderlabs-ids-new-banking-trojan-distributed-through-whatsapp/

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