TATA COMMUNICATIONS

# YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: November 18, 2025

TATA COMMUNICATIONS

TATA

# THREAT INTELLIGENCE ADVISORY REPORT

As the final quarter of 2025 unfolds, the cyber threat landscape continues to intensify, marked by the rapid evolution of attacks in both scale and sophistication. Conventional defence mechanisms are increasingly inadequate as adversaries exploit systemic vulnerabilities across interconnected digital ecosystems. To maintain resilience and competitive advantage, organisations must strengthen core security frameworks, implement layered protection, and embed anticipatory intelligence throughout their architecture.

Here, businesses can stay ahead through Tata Communications' Cyber Threat Intelligence report. Published weekly, the report delivers incisive analysis of emerging campaigns, evolving adversarial tactics, and sector-specific risks. By transforming intelligence into actionable defence, security teams are empowered to anticipate, prepare for, and neutralise threats proactively — safeguarding critical operations before disruption can occur.

# Credential brute force leads to DragonForce-encrypted enterprise attack

Security researchers confirmed that a DragonForce-affiliated ransomware-as-a-service (RaaS) intrusion recently struck a manufacturing organisation. The attackers began with internal network scanning and credential brute-force, progressed to privileged administrator log-ins and SSH-based data exfiltration to ASN AS198953 (Proton66). They then deployed ransomware, encrypting files with a ".df_win" extension while dropping "readme.txt" ransom notes, exploiting the absence of an autonomous response.

According to the incident analysis from Darktrace, the root access was facilitated by the first-time use of highly privileged credentials and unusual Windows Registry modifications. The data exfiltration endpoint was identified on 2 September 2025, geolocated in Russia and tied to Proton66. The case underscores how RaaS operators are fragmenting tactics and enabling affiliates to launch tailored attacks that evade legacy defences.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | Manufacturing |
| REGION | Russia, UK | APPLICATION | Microsoft Internet Information Services (IIS), Windows |

Source - https://www.darktrace.com/blog/tracking-a-dragon-investigating-a-dragonforce-affiliated-ransomware-attack-with-darktrace

# OysterLoader spread through Rhysida malware operations via fake installers

Since May 2024, the organised threat actor formerly known as Vice Society and now operating as Rhysida has executed a sustained malvertising campaign. Targeting users with Bing-sponsored adverts that mimic installers for applications such as Microsoft Teams, PuTTY and Zoom (including results appearing in the Windows 11 Start menu), the actor's May–Sep 2024 phase and resumption in June 2025 have successfully posed as legitimate software installers.

At the core of the campaign lies the loader dubbed OysterLoader (also known as Broomstick and CleanUpLoader), which is code-signed using forty-seven distinct certificates in 2025 alone, making evasion of antivirus detection significantly easier. Expel's analysis reveals that Rhysida also deploys the Latrodectus malware as an alternate initial access tool, and the group is also abusing Microsoft's Trusted Signing system — a sophisticated approach that highlights a markedly higher operational tempo compared to the prior campaign.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | Healthcare, Financial services, Manufacturing, IT, Government, Transportation, Education, Energy, Retailer and Distributor, Telecommunications |
| REGION | Global | APPLICATION | PuTTY, Windows, Microsoft Teams, Zoom |

Source - https://expel.com/blog/certified-oysterloader-tracking-rhysida-ransomware-gang-activity-via-code-signing-certificates/

# Sage ransomware group weaponises domain admin for network-wide staging

Threat researchers detail a sophisticated intrusion chain consistent with Sage Ransomware Group activity. Attackers exploited a public-facing management application to gain remote code execution (RCE) and immediately created a local administrator account named “defaultaccount.” From there, they deployed the tunnelling tool Chisel to establish an outbound reverse SOCKS proxy, then proceeded with Active Directory enumeration and compiled a .NET binary in memory as part of their lateral-movement campaign.

Following persistence and reconnaissance, the actors escalated to domain-wide compromise by achieving Domain Admin privileges, executing WMIXEC on the domain controller and attempting AV/EDR disablement. They further modified the SYSVOL share and forced Group Policy replication, preparing a mass ransomware deployment across the domain via a malicious GPO. The rapid advancement from web application compromise to domain-wide staging underscores the danger inherent in exposed management interfaces and insufficient segmentation.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | IT |
| REGION | Global | APPLICATION | Microsoft ASP.NET, Microsoft Internet Information Services (IIS), Windows |

Source - https://blackpointcyber.com/blog/from-web-app-compromise-to-ransomware-attempt-tracing-the-sage-intrusion-chain/

# LANDFALL spyware exploits Samsung zero-day vulnerability for infiltration

Researchers have identified a previously unknown Android spyware family named LANDFALL, exploiting a zero-day vulnerability (CVE-2025-21042) within the image-processing library of Samsung devices. The campaign employed malicious DNG image files delivered via WhatsApp and specifically targeted Samsung Galaxy phones in the Middle East, enabling remote surveillance, comprehensive data exfiltration, and persistence.

Active from mid-2024 until early 2025, LANDFALL operated undetected until Samsung issued a patch in April 2025. Its modular architecture facilitated microphone recording, call-log harvesting, location tracking, and file exfiltration. The exploit chain shares trade-craft similarities with commercial-grade spyware operations linked to private-sector offensive actors in the region, underscoring the increasing sophistication of mobile-device threats.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware, Mobile | SECTOR | Government, Telecommunications |
| REGION | Middle East | APPLICATION | Android, WhatsApp |

Source - https://unit42.paloaltonetworks.com/landfall-is-new-commercial-grade-android-spyware/

# Cephalus targets weak RDP security controls for financial ransomware campaign

In mid-June 2025, a novel ransomware group known as Cephalus surfaced, declaring its operations purely financially motivated. According to detailed analysis, the group exploits Remote Desktop Protocol (RDP) accounts that lack multi-factor authentication for initial access. After gaining entry, Cephalus employs a customised Go-language ransomware that disables Windows Defender real-time protection, halts key backup services, and deletes volume snapshots to hinder recovery efforts.

The encryption routine deployed by Cephalus uses AES-CTR symmetric encryption with a single key for all files, the plaintext key being cryptographically protected by an embedded RSA public key to ensure only the attacker can decrypt the data. The group also applies psychological pressure by including ransom notes with leak-proof links to GoFile-style data dumps, signalling a tailored, persistent menace directed at targeted organisations.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | Financial services, BFSI |
| REGION | Global | APPLICATION | Windows |

Source - https://asec.ahnlab.com/ko/90859/

INTRODUCTION
DRAGONFORCE RANSOMWARE INFILTRATES MANUFACTURING ORGANISATION NETWORK
RHYSIDA SCHEME DELIVERS OYSTERLOADER THROUGH SEARCH AD SPOOFING
RCE EXPLOITATION ENABLES SAGE-LED DOMAIN-WIDE RANSOMWARE DEPLOYMENT
LANDFALL SPYWARE EXPLOITS SAMSUNG FLAW VIA WHATSAPP IMAGES
GO-BASED CEPHALUS RANSOMWARE DELETES BACKUPS BEFORE ENCRYPTION
DDOS AND DEFACEMENT ATTACKS ESCALATE AGAINST GOVERNMENT AND EDUCATION
COORDINATED HACKTIVIST OFFENSIVES INTENSIFY REGIONAL CYBER DISRUPTIONS
STATE-LINKED HTTPTROY BLINDINGCAN DEPLOY ENHANCED ENCRYPTION ARSENAL
SLEEPYDUCK RAT DISGUISED AS SOLIDITY EXTENSION INFECTS IDE USERS
DRAGONFORCE RANSOMWARE DEPLOYS BYOVD ATTACKS TARGETING ENTERPRISES

# Hacktivist groups accelerate DDoS and website defacement campaigns

Early November 2025 saw a marked surge in hacktivist-led disruptions against Indian entities, with government portals and educational institutions bearing the brunt. Campaigns favoured high-visibility tactics such as distributed-denial-of-service (DDoS) and website defacement to amplify political messages and cause service outages. Groups including THE GARUDA EYE and HellR00ters claimed several incidents, leveraging social channels to publish taunts and operational details.

Alongside protest-driven actions, financially motivated ransomware operators intensified pressure on private firms. Emerging families such as NightSpire and The Gentlemen adopted double-extortion playbooks — data exfiltration paired with encryption — and published victim lists on leak sites to force payment. Industry reporting shows higher per-incident costs in 2025, underscoring the blended threat of reputational harm and operational disruption. Organisations must prioritise backups and rapid incident response.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Hacktivism, DDOS, Cyberespionage | **SECTOR** | Healthcare, Financial services, Manufacturing, IT, Government, Education, Defence Industry, Broadcast Media Production and Distribution, Retailer and Distributor, Telecommunications |
| **REGION** | India | **APPLICATION** | Generic |

**Source** - Threat Intel Team Internal Research

# Coordinated cybergroups target government sectors with widespread DDoS attacks

Between 1–10 November 2025, Middle Eastern organisations were hit by coordinated offensives attributed to hacktivist collectives such as Hezi Rash, RipperSec, Server Killers and Keymous+. The campaign chiefly involved large-scale DDoS assaults that disrupted government, financial and education portals. Investigations also revealed data leaks and the sale of admin credentials, suggesting a mix of espionage and profit-driven motives, and internal team analysis.

Ransomware incidents were fewer but notable: Qilin exhibited opportunistic lateral movement and continued high victim counts, exploiting remote management tools and publishing extortion listings, while NightSpire emerged as an opportunistic double-extortion actor in 2025. These operators favoured lateral exploitation following initial access, underscoring the importance of credential hygiene, RMM monitoring and rapid detection to curb post-compromise spread and timely patching of exposed systems.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Hacktivism, DDOS, Cyberespionage | SECTOR | Healthcare, Financial services, Manufacturing, IT, Government, Education, Defence Industry, Broadcast Media Production and Distribution, Retailer and Distributor, Telecommunications |
| REGION | Middle East | APPLICATION | Generic |

**Source** - Threat Intel Team Internal Research

# Layered HttpTroy and BLINDINGCAN malware evade global detection systems

Recent investigations reveal that DPRK-linked actors have introduced two sophisticated toolsets. The group Kimsuky deployed a back-door chain beginning with a ZIP archive lure, followed by the loader MemLoad _V3 and culminating in the drop of HttpTroy. Meanwhile, Lazarus utilised Comebacker and Compcat_v1.dll to install a refined version of the BLINDINGCAN RAT, each with layered obfuscation, COM-based persistence, and multi-stage loaders.

The renewed BLINDINGCAN variant features enhanced encryption, modular command capabilities, and remote execution mechanisms, while HttpTroy supports full control functions, including file upload/download, screenshot capture, and reverse shell execution. Both campaigns underscore a strategic shift in threat-actor tactics, emphasising stealth, dynamic API resolution, and memory-only execution to evade detection. Security teams must prioritise monitoring for these behaviours and update defences accordingly.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | Government, Education, Energy, Defence Industry, Telecommunications |
| REGION | Canada, South Korea | APPLICATION | Windows |

Source - https://www.gendigital.com/blog/insights/research/dprk-kimsuky-lazarus-analysis

INTRODUCTION | DRAGONFORCE RANSOMWARE INFILTRATES MANUFACTURING ORGANISATION NETWORK | RHYSIDA SCHEME DELIVERS OYSTERLOADER THROUGH SEARCH AD SPOOFING | RCE EXPLOITATION ENABLES SAGE-LED DOMAIN-WIDE RANSOMWARE DEPLOYMENT | LANDFALL SPYWARE EXPLOITS SAMSUNG FLAW VIA WHATSAPP IMAGES | GO-BASED CEPHALUS RANSOMWARE DELETES BACKUPS BEFORE ENCRYPTION | DDOS AND DEFACEMENT ATTACKS ESCALATE AGAINST GOVERNMENT AND EDUCATION | COORDINATED HACKTIVIST OFFENSIVES INTENSIFY REGIONAL CYBER DISRUPTIONS | STATE-LINKED HTTPTROY BLINDINGCAN DEPLOY ENHANCED ENCRYPTION ARSENAL | SLEEPYDUCK RAT DISGUISED AS SOLIDITY EXTENSION INFECTS IDE USERS | DRAGONFORCE RANSOMWARE DEPLOYS BYOVD ATTACKS TARGETING ENTERPRISES

# SleepyDuck Trojan infiltrates Open VSX marketplace, leveraging Blockchain

A newly identified remote access trojan, known as SleepyDuck, has infiltrated the Open VSX Registry's IDE-extension marketplace by masquerading as a popular Solidity tool. While initially benign, it later received a malicious payload after accumulating over 14,000 downloads. Once active on Windows systems, the malware evades sandbox environments, retrieves commands from the domain "sleepyduck[.]xyz," and establishes persistent control over infected endpoints.

SleepyDuck's distinctiveness lies in its blockchain-based fallback mechanism: via an embedded Ethereum smart contract, the malware dynamically updates its command-and-control server if its primary infrastructure is disrupted. This clever technique enables adversaries to maintain control and complicates takedown efforts significantly. Analysts warn that this incident underscores the growing threat of supply-chain attacks on developer tools and emphasises the need for heightened extension-source verification and strong endpoint defences.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | Software Development |
| REGION | Global | APPLICATION | VS Code |

Source - https://secureannex.com/blog/sleepyduck-malware/

# Conti's successor DragonForce weaponises BYOVD for widespread attacks

Since emerging in 2023, the entity known as the DragonForce cartel has evolved from a traditional ransomware-as-a-service operation into a sophisticated affiliate ecosystem. Rebranded in early 2025 as a "cartel", it offers affiliates customisable encryptors and infrastructure while leveraging leaked code from Conti. It now employs BYOVD (bring-your-own-vulnerable-driver) attacks using the drivers truesight.sys and rentdrv2.sys to terminate security processes.

In partnership with initial-access brokers such as Scattered Spider — and affiliated networks linked to LAPSUS$ and ShinyHunters — the DragonForce cartel has exposed more than two hundred victims worldwide across retail, insurance, airlines, MSPs and other sectors. It has also addressed encryption flaws previously observed in Akira ransomware variants, demonstrating a heightened technical maturity and persistence of the threat.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Ransomware | **SECTOR** | Retail, Aviation, IT |
| **REGION** | Global | **APPLICATION** | Windows, Linux, and VMware ESXi systems |

Source - https://secureannex.com/blog/sleepyduck-malware/

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*