TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: AUGUST 12, 2025

THREAT INTELLIGENCE ADVISORY REPORT

Today's rapidly evolving digital environment has made protecting against cybersecurity risks an essential concern for organisations across the globe. As these risks continue to transform, businesses are concentrating not only on securing their information but also on strengthening the core infrastructures that power contemporary commercial activities. The objective is to build durability against a continuously growing spectrum of new threats.

Strengthen your organisation's cybersecurity readiness with Tata Communications' weekly threat intelligence advisory. Gain invaluable insights into the most recent cyber risks and implement proactive strategies to strengthen your defences, effectively mitigating potential vulnerabilities.

OceanLotus APT targets trade intelligence

The OceanLotus APT group has launched a sophisticated cyber espionage campaign in early 2025, strategically targeting China-Africa cooperation units through supply chain attacks amid escalating US-China trade tensions. The operation involved spear-phishing emails containing malicious ZIP attachments with LNK files that deployed a Rust-based trojan loader, demonstrating the group's advanced technical capabilities.

The timing of this cyber operation coincides with renewed tariff wars initiated by the White House, which have significantly impacted global trade patterns and forced export-dependent economies to restructure their supply chains and explore alternative trading relationships with African markets. Organisations operating within China-Africa cooperation frameworks face heightened risks and must implement comprehensive threat detection systems. Security experts recommend deploying advanced threat defence engines capable of precisely blocking malicious attachments and detecting in-memory payload execution.

ATTACK TYPE	Malware	SECTOR	Government
REGION	Africa, China	APPLICATION	Windows

Source - https://ti.qianxin.com/blog/articles/apt-group-target-the-china-africa-community-with-a-shared-future-en/

Advanced info-stealer strike government and manufacturing sectors

The 0bj3ctivityStealer campaign begins with deceptive phishing emails bearing "Quotation offer" subjects, containing low-quality images masquerading as purchase orders. Victims are lured into clicking download links to access higher-quality versions hosted on MediaFire, which delivers heavily obfuscated JavaScript files containing over 3,000 lines of code with only 60 belonging to actual payload functionality. The malware employs steganography by embedding .NET DLL loaders within seemingly innocuous JPG images hosted on Archive.org, extracting payloads through RGB pixel value manipulation.

The malware utilises unidirectional data exfiltration through Telegram bots rather than dynamic command-and-control interaction, executing features indefinitely whilst harvesting system information, browser credentials, messaging applications, email clients, and cryptocurrency wallet data. Advanced evasion techniques include sandbox detection capabilities that terminate execution upon detecting virtualised environments or debuggers.

ATTACK TYPE	Malware	SECTOR	Manufacturing, Government
REGION	North America, Europe, Asia	APPLICATION	Windows

Source - https://securityonline.info/0bj3ctivitystealer-stealthy-info-stealer-uses-steganography-powershell-to-evade-detection/

Federal agencies warn of Scattered Spider campaign targeting critical sectors

The FBI, CISA, and international partners released updated guidance in July 2025 regarding Scattered Spider's enhanced operations, revealing sophisticated social engineering techniques targeting large companies and IT helpdesks. The group now deploys DragonForce ransomware alongside traditional tactics, employing multilayered spearphishing operations enriched by personal information from social media and commercial intelligence tools. Recent campaigns involve purchasing employee credentials from illicit marketplaces like Russia Market and compromising third-party services with network access.

Scattered Spider utilises legitimate remote access tools including AnyDesk, Fleetdeck.io, Level.io, and Teleport.sh for network infiltration, alongside malware variants such as AveMaria, Raccoon Stealer, and RattyRAT. The group exfiltrates data to MEGA[.]NZ and Amazon S3 whilst targeting Snowflake databases to extract large data volumes rapidly, often running thousands of queries simultaneously. Federal agencies emphasise implementing phishing-resistant MFA, offline backups, and application controls to counter these evolving threats effectively.

ATTACK TYPE	Ransomware, Malware, Cyberespionage	SECTOR	Financial services, IT, Government, E-Commerce, BFSI, Aviation, Hospitality, Retailer and Distributor, Telecommunications
REGION	Global	APPLICATION	AnyDesk, Windows, AWS S3, Team Viewer

Source - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

INTRODUCTION | ESPIONAGE CAMPAIGN EXPOSES SUPPLY CHAIN RISKS | STEALTHY INFO-STEALER HITS KEY SECTORS | SCATTERED SPIDER RAMPS UP ATTACK TACTICS | RANSOMWARE THREATS SURGE AFTER LOCKBIT LEAK | BEAST JOINS DARK WEB WITH LEAK SITE | CICADA3301 TARGETS PAYLOAD AND DATA THEFT SECTORS | SECP0 EXPLOITS LINUX VULNERABILITIES BYPASSING MFA | APT36 STARTS USING PDFS AND BACKDOOR | INTERLOCK'S CLICKFIX PROMPTS FOR TARGETED ATTACKS | DUAL-MALWARE ATTACKS WITH CUSTOM ANTIVIRUS TERMINATOR

LockBit 3.0 builder leak amplifies ransomware threats

LockBit ransomware operators leverage sophisticated DLL sideloading techniques by bundling malicious DLLs with legitimate, digitally signed applications including Jarsigner.exe with jli.dll, MpCmdRun.exe with mpclient.dll, and Clink_x86.exe with clink_dll_x86.dll. These attacks begin with remote access via MeshAgent and TeamViewer, followed by privilege escalation using NSSM and PsExec tools to run malicious payloads as system services. Threat actors employ masquerading tactics, renaming malicious executables to mimic legitimate system files like svchost.exe and explorer.exe whilst utilising legitimate application icons.

The LockBit 3.0 builder leak occurred following law enforcement disruptions in 2024, including the indictment of alleged ringleader Dimitry Khoroshev, making the ransomware accessible to any threat actor beyond its original developers. Recent attack chains involve credential theft via TokenUtils.exe, lateral movement through Group Policy deployment, and file encryption using obfuscated PowerShell scripts targeting over 40 file extensions including documents, media files, and databases.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.security.com/threat-intelligence/lockbit-ransomware-attack-techniques

Beast Ransomware launches Dark Web leak site with LockBit

Beast Ransomware employs sophisticated evasion tactics, including creating mutex objects with the unique "BEAST HERE?" string and avoiding encryption on devices located in Commonwealth of Independent States (CIS) countries like Russia, Belarus, and Moldova. This ransomware propagates through various attack vectors such as phishing emails, compromised Remote Desktop Protocol (RDP) endpoints, and SMB network scans, further leveraging "RstrtMgr.dll" (Restart Manager) to manipulate file access before encryption.

Intelligence suggests Beast has impacted over 12 victims across sectors including municipal government, healthcare, and engineering. The group’s Dark Web leak site reportedly launched on July 29, 2025, marking an operational milestone. Upon infiltration, Beast encrypts files, appends distinct extensions, and provides ransom notes. Its use of leaked LockBit builder components points to advanced code reuse and an evolving ransomware-as-a-service model.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - Threat Intel Sources

Cicada3301 Ransomware deploys Rust-based ransomware with data theft

Cicada3301 ransomware operates through a sophisticated admin panel where affiliates assemble payloads, select target platforms spanning Windows, Linux, and ESXi environments, and interact with victims through built-in chat functions. The group executed at least five confirmed attacks targeting life sciences, public services, construction, and gaming industries using opportunistic RDP credential abuse and phishing ZIP/ISO attachments delivering Rust loaders. The ransomware employs reflective injection techniques to avoid disk writes and executes service shutdown commands targeting endpoint detection systems like CrowdStrike.

The group utilises ChaCha20-Poly1305 encryption for per-file authentication, appending random seven-character extensions such as .jtu5s6r to encrypted files whilst maintaining persistence through scheduled tasks named "CicadaPersist". Advanced evasion techniques include UPX packing with custom headers to circumvent signature detection and data exfiltration capabilities reaching up to 2.5 terabytes prior to encryption deployment.

ATTACK TYPE	Ransomware	SECTOR	Construction, IT, Gaming Industry
REGION	Global	APPLICATION	VMWare ESXi, Windows, Linux

Source - https://redpiranha.net/news/threat-intelligence-report-july-15-july-21-2025

Secp0 Ransomware threatens critical Linux infrastructure

Secp0 ransomware operators leverage sophisticated initial access methods, including brute force attacks on SSH credentials and exploitation of CVE-2023-20269 vulnerabilities in Cisco ASA/FTD VPN appliances to bypass multi-factor authentication. Following successful infiltration, the group executes Bash one-liners to download ELF loaders and establishes persistence through hidden cron entries at /etc/cron.d/.scp0, running keepalive scripts every hour. The ransomware employs a variant of the Linux kernel Dirty Pipe exploit (CVE-2022-0847) for privilege escalation to root access on unpatched systems.

Advanced evasion techniques include disabling audit daemons via systemd commands and deleting VM snapshots on ESXi systems using vim-cmd tools whilst deploying mimit - a Linux port of Mimikatz, to extract credentials from /etc/shadow files. The group's structured approach includes network service scanning using nmap and custom Rust binaries for LDAP enumeration, indicating highly organised technical capabilities.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Linux

Source - https://redpiranha.net.au/news/threat-intelligence-report-july-22-july-28-2025

INTRODUCTION | ESPIONAGE CAMPAIGN EXPOSES SUPPLY CHAIN RISKS | STEALTHY INFO-STEALER HITS KEY SECTORS | SCATTERED SPIDER RAMPS UP ATTACK TACTICS | RANSOMWARE THREATS SURGE AFTER LOCKBIT LEAK | BEAST JOINS DARK WEB WITH LEAK SITE | CICADA3301 TARGETS PAYLOAD AND DATA THEFT SECTORS | SECP0 EXPLOITS LINUX VULNERABILITIES BYPASSING MFA | APT36 STARTS USING PDFS AND BACKDOOR | INTERLOCK'S CLICKFIX PROMPTS FOR TARGETED ATTACKS | DUAL-MALWARE ATTACKS WITH CUSTOM ANTIVIRUS TERMINATOR

APT36’s Phishing and Poseidon backdoor hit infrastructure targets

APT36 employs sophisticated .desktop files disguised as PDF documents, executing background scripts whilst users remain distracted by decoy content hosted on Google Drive. The group utilises two distinct attack variants: single command-and-control server configurations and redundant C2 infrastructure featuring servers at 165.232.114.63 and 165.22.251.224 for enhanced resilience. Payloads disguised as legitimate system files including p7zip-full, tcl-8.7, emacs-bin, and crond-98 are stored in directories like ~/.local/share/ and /dev/shm/ to evade detection.

The campaign leverages the Poseidon backdoor, developed using the open-source Mythic command-and-control framework and written in Go, enabling cross-platform functionality for persistent access and lateral movement. Researchers identified over 100 phishing domains impersonating organisations including DRDO, Ministry of External Affairs, and Ministry of Defence, utilising deceptive TLDs such as .report, .support, and .digital.

ATTACK TYPE	Malware, Cyberespionage	SECTOR	Government, Transportation, Oil and gas, Defence Industry
REGION	India	APPLICATION	Windows

Source - https://hunt.io/blog/apt36-india-infrastructure-attacks

Interlock Group deploys stealthy multi-stage attack chain

Since January 2025, the Interlock group has adopted ClickFix techniques, employing deceptive prompts to persuade victims into manually executing malicious PowerShell commands through fake CAPTCHA verifications and system update prompts. The attackers utilise disguised installers to deploy credential stealers and keyloggers, whilst maintaining persistent remote access through legitimate tools including AnyDesk and PuTTY.

Technical analysis reveals Interlock's ransomware binary as a 64-bit executable compiled on October 2, 2024, featuring custom unpacker code located in Thread Local Storage and multiple obfuscated stack strings. Despite continuous operations, Interlock has claimed 24 victims since September 2024, including only 6 in 2025, representing significantly fewer compromises compared to more prolific ransomware groups claiming over 100 victims in Q1 2025 alone.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	North America, Europe	APPLICATION	Windows

Source - https://www.esentire.com/blog/unmasking-interlock-groups-evolving-malware-arsenal

Storm 2603 launches dual malware ransomware attacks

Storm-2603 deploys a sophisticated dual-malware approach utilising both DNS tunneling backdoors and HTTP-based communications through the custom ak47c2 framework, with debugging symbols pointing to "C:\Users\Administrator\Desktop\work\tools\ak47c2". Multiple ransomware variants are deployed simultaneously against targets, with LockBit Black and Warlock/x2anylock strains using identical ransom note templates and contact information.

The group employs a custom "Antivirus Terminator" tool that abuses legitimate third-party signed drivers from Antiy System In-Depth Analysis Toolkit, originally named AToolsKrnl64.sys, to terminate security processes through IO control codes. Evidence suggests Storm-2603 operations in LATAM regions dating back to March 2025, with a RAR archive named "Evidencia.rar" containing artifacts from compromised machines uploaded to VirusTotal in April 2025.

ATTACK TYPE	Vulnerability, Ransomware, Malware	SECTOR	All
REGION	Global	APPLICATION	Microsoft SharePoint Server, Windows

Source - https://research.checkpoint.com/2025/before-toolshell-exploring-storm-2603s-previous-ransomware-operations/

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.