TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 15, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Today’s fast-evolving digital landscape poses intricate challenges for organisations already grappling with an expanding array of cyber threats. Not only are these pervasive threats capable of inflicting substantial harm on business entities, but also on individuals and government bodies as well. Unsurprisingly, they can result in dire consequences such as data breaches, operational disruptions, and financial setbacks.

You can, however, secure your operations and elevate your defence mechanisms by following our weekly reports. These provide up-to-the-minute cyber threat intelligence, allowing you to stay ahead of emerging risks. In a time when cyber resilience is a significant concern, we equip you with the essential tools and knowledge to fortify yourself and your organisation in an ever-shifting digital terrain.

TATA COMMUNICATIONS

LapDogs ORB network: A stealthy China-nexus threat targeting SOHO devices

LapDogs, a recently uncovered Operational Relay Box (ORB) network linked to China-nexus APTs, is targeting Linux-based SOHO devices across the U.S., East Asia, and South Asia. The network focuses on espionage, using stealth techniques and unique TLS certificates to disguise malicious traffic as legitimate, enabling covert data collection and sustained access. Targets span IT, real estate, and broadcast media, with the campaign marked by deliberate, methodical growth and long-term operational goals.

To counter LapDogs, organisations must secure SOHO infrastructure, apply network segmentation, inspect outbound TLS traffic, and monitor devices for unauthorised certificates or suspicious lateral movement. Adopting zero-trust security, auditing remote access, and extending threat hunting beyond the core network are also critical to identifying and containing ORB-style threats like LapDogs.

ATTACK TYPE	Malware	**SECTOR**	IT, Real Estate, Broadcast Media Production and Distribution
REGION	Japan, South Korea, Taiwan, United States, South Asia, East Asia, Hong Kong	**APPLICATION**	Linux

Source - https://securityscorecard.com/wp-content/uploads/2025/06/LapDogs-STRIKE-Report-June-2025.pdf

Houken threat actor exploits Ivanti zero-days for targeted attacks

Houken, a China-linked threat actor first spotted in 2024, continues its global campaign by exploiting zero-day vulnerabilities in Ivanti devices. The threat blends sophistication and opportunism with custom Linux rootkits and public tools. It's like UNC5174, a threat actor suspected to be tied to China's Ministry of State Security (MSS), known for breaching critical networks undetected. The group's tactics highlight both technical precision and strategic persistence, focusing on long-term access and data collection across key sectors.

To defend against Houken, organisations should patch Ivanti systems immediately, monitor for signs of post-exploitation activity, and deploy EDR solutions capable of detecting rootkits. Regular configuration audits, privilege controls, and network segmentation are also essential to contain such stealthy, state-linked intrusions and keep business systems secure and functional.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Ivanti

Source - https://securityonline.info/anssi-exposes-houken-china-linked-threat-actor-exploiting-ivanti-csa-zero-days-deploying-linux-rootkits/

Qwizzserial Android malware drains Uzbek users via Telegram apps

A rising Android-based SMS stealer, Qwizzserial, is causing financial damage across Uzbekistan by intercepting 2FA codes and stealing banking credentials. The malware masquerades as legitimate apps on Telegram and uses Telegram bots for exfiltration. So far, the attack has rapidly exploited the heavy local reliance on SMS for authentication to cause 100,000+ infections and $62,000+ in fraud losses. Mirroring the tactics of Classiscam, Qwizzserial reflects the growing threat of mobile-first fraud in emerging markets.

To stay secure, Android users across Uzbekistan should avoid sideloading apps, even from trusted platforms like Telegram. Uzbek financial institutions must consider multi-factor authentication methods beyond SMS, and defenders should deploy mobile threat defence (MTD) and raise user awareness across affected regions.

ATTACK TYPE	Malware, Mobile	**SECTOR**	Financial Services
REGION	Uzbekistan	**APPLICATION**	Android

Source - https://www.group-ib.com/blog/rise-of-qwizzserial/

Gamaredon escalates spearphishing campaigns against Ukraine

In 2024, the Gamaredon APT group intensified its cyberespionage activities, focusing on Ukrainian government entities. The group deployed drive-based malware and wide-reaching spearphishing campaigns, refining its tools for stealth and persistence. Most notably, Gamaredon has begun tunnelling its command-and-control traffic via Cloudflare, successfully masking its operations from traditional detection methods. And despite operational limitations, the group continues to evolve its toolkit to exfiltrate sensitive government data and sustain network access across Ukraine.

To counter this persistent threat in a sensitive time, Ukrainian agencies must enforce phishing awareness training, enhance endpoint and network monitoring, and block suspicious tunnel traffic. Regular forensic reviews and infrastructure segmentation will help limit long-term espionage exposure, helping them stay secure and operational.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Ukraine	**APPLICATION**	Windows

Source - https://www.welivesecurity.com/en/eset-research/gamaredon-2024-cranking-out-spearphishing-campaigns-ukraine-evolved-toolset/

Leaked Shellter Elite tool powers evasive infostealer campaigns

A leaked version of the Shellter Elite v11.0, which was originally designed for red-team AV/EDR evasion, is now being misused by threat actors in active infostealer campaigns. Shellter's sophisticated features, such as polymorphic code, memory injection, and API hook evasion, are being leveraged to deploy malware such as LUMMA, ARECHCLIENT2, and RHADAMANTHYS. This makes the malware highly resistant to detection. Despite safeguards implemented by Shellter's developers to prevent abuse, the leak has allowed cybercriminals to weaponise its elite evasion capabilities at scale, targeting both enterprises and individuals across the world. The threat underscores the growing misuse of commercial red-teaming tools in live attacks.

To counter this, defenders must strengthen memory analysis, implement behaviour-based EDRs, and watch for stealthy injection techniques. The release of a dynamic unpacker by researchers can also offer a valuable resource to reverse-engineer payloads and map evolving threat chains for faster response and more secure operations.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://www.elastic.co/security-labs/taking-shellter

Janela RAT and browser extension steal data in a LATAM campaign

A variant of BX RAT, the Janela RAT is now part of a coordinated campaign in Latin America, targeting financial sector users. Delivered through GitLab-hosted MSI installers, it drops both a stealthy RAT and a malicious Chromium browser extension to steal cookies, history, and system information. The attack chain includes obfuscated Go binaries, .NET scripts, and encrypted WebSocket C2 communication channels. The malware uses Eziriz.NET Reactor and base64-encoded URLs to evade detection and obscure infrastructure and payload paths. Once a system is infected, the bundled extension runs in the background, silently harvesting sensitive browser data while reporting to attacker-controlled servers.

Users across Latin America should avoid unverified extensions and executable downloads. Financial institutions must harden browser configurations, implement outbound traffic inspection, and monitor for signs of modular malware and web-based credential theft.

ATTACK TYPE	Malware	**SECTOR**	Financial Services
REGION	Latin America	**APPLICATION**	Windows, Chromium

Source - https://medium.com/walmartglobaltech/janela-rat-and-a-stealer-extension-delivered-together-e274469a7df8

RondoDox botnet evades detection with stealth Linux campaign

A newly identified Linux-based botnet, the RondoDox, is leveraging stealth and persistence to infect enterprise systems worldwide. Unlike traditional botnets, RondoDox employs custom backdoors, encrypted config files, and low-noise C2 tunnels to stay hidden. Its modular design helps it bypass standard detection tools and pose significant risks to Linux-based infrastructure. Researchers also found that the botnet uses uncommon ports, minimal system calls, and encrypted outbound communication to mask its presence. It can adapt rapidly, deploy new modules dynamically, and survive reboots through obfuscated persistence mechanisms.

For security, organisations must adopt anomaly-based detection, conduct deep packet inspection, and scan Linux environments for unauthorised daemons or traffic anomalies. Limiting outbound connections and isolating critical infrastructure can further disrupt botnet activity.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Linux

Source - https://www.fortinet.com/blog/threat-research/rondobox-unveiled-breaking-down-a-botnet-threat

APT36 leverages BOSS Linux to spy on Indian defence personnel

APT36, a Pakistan-linked threat group, has launched a cyberespionage campaign against Indian defence personnel using the BOSS Linux OS, an open-source platform promoted in government environments. The campaign begins with phishing emails delivering ZIP archives containing a .desktop shortcut. Once launched, the file runs a decoy PowerPoint while silently executing a malicious ELF binary (BOSS.elf). What follows is a multi-stage infection chain that grants stealth access to systems, enabling long-term espionage and sensitive data exfiltration. The attackers demonstrate growing sophistication in targeting niche operating systems with legitimate government use.

Defence organisations must enforce hardened BOSS Linux configurations, enable shell execution monitoring, and run regular checks on shortcut behaviours. Security teams should also enhance sandboxing and phishing defences for users, especially those in sensitive roles.

ATTACK TYPE	Malware	**SECTOR**	Government, Military, Defence Industry
REGION	India	**APPLICATION**	Windows, Linux

Source - https://www.cyfirma.com/research/phishing-attack-deploying-malware-on-indian-defense-boss-linux/

Datacarry ransomware abuses Fortinet flaw in global extortion spree

Between June 2024 and June 2025, the Datacarry ransomware group exploited a known Fortinet EMS vulnerability to breach 11 global organisations across multiple sectors, including finance, healthcare, tourism, and IT. The attacks employed WebSocket C2 channels and Chisel tunnelling for stealthy data exfiltration and encryption. Its focus on unpatched enterprise security tools reinforces the critical need for vulnerability lifecycle management. The group's activity spiked in spring 2025, with operations halting by late June, suggesting either a tactical shift or a need to regroup.

To stay secure against similar attacks in future, enterprises must prioritise patching, restrict admin-level remote access, and monitor for unusual tunnelling behaviour. Regular threat hunting and segmented recovery plans are also key to limiting ransomware impact and downtime.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Tourism, IT, Aviation, BFSI
REGION	Global	**APPLICATION**	Fortinet

Source - https://unit42.paloaltonetworks.com/cybercriminals-attack-financial-sector-across-africa/

DEVMAN ransomware emerges with offline encryption and a hybrid codebase

DEVMAN, an emerging ransomware strain, is deployed across Europe, Africa, Asia, and Latin America. DEVMAN performs offline encryption, features a dedicated leak site, and exhibits quirks like encrypting its ransom notes. And even though the ransomware is built partly on the DragonForce codebase, it displays unique attributes that make it difficult to attribute with certainty. Researchers suspect this may be a test build by a new affiliate or a forked strain being trialled in real-world environments. Its distinct behavioural patterns further complicate static detection and signature-based defences.

Security teams must adopt fileless threat detection, maintain immutable backups, and analyse ransomware TTP overlaps across campaigns. Proactive reverse engineering and code comparison can be critical to spotting hybrid evolution in emerging ransomware families.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Europe, Africa, Asia, Latin America	**APPLICATION**	Windows

Source - https://any.run/cybersecurity-blog/devman-ransomware-analysis/

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