TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 29, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today's fast-evolving digital environment, organisations face complex challenges from an expanding range of cyber threats. These increasingly sophisticated threats can have a severe impact on individuals, enterprises, and public institutions, causing data leaks, financial losses, and significant operational downtime.

As cyber resilience becomes more critical than ever, we equip your organisation with the insights and resources needed to navigate this dynamic threat landscape with confidence. You can strengthen your cybersecurity posture with our weekly reports, offering up-to-date threat intelligence and expert analysis. Stay ahead of persistent risks and protect critical IT infrastructure with our in-depth advisory report.

BlackSuit ransomware delivers stealthy multi-stage attacks

BlackSuit ransomware is a sophisticated threat actor believed to be a rebranded operation by the Royal ransomware group, itself an offshoot of Conti. Active globally across healthcare, manufacturing, IT, government, education, and retail sectors, BlackSuit carries out multi-stage attacks characterised by speed, stealth, and advanced evasion tactics. Victims often face double extortion. First, data theft is followed by encryption, with the added destruction of backups to hinder recovery efforts. BlackSuit operators also employ selective encryption to quicken operations while maximising disruption. The ransomware's ability to mimic legitimate admin behaviour and evade traditional endpoint protections has made it especially challenging to detect and contain.

Organisations must harden their defences by auditing lateral movement tools, restricting remote access, isolating backup systems, and monitoring for signs of initial compromise. Proactive incident response planning and segmentation remain essential against threats like BlackSuit.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare/hospitals, Manufacturing, IT, Government, Education, Retailer and Distributor
REGION	Global	**APPLICATION**	Windows

Source - https://securityonline.info/blacksuit-new-royal-conti-rebrand-hits-with-speed-stealth-data-exfiltration/

Dark 101 ransomware blocks recovery to force ransom

Dark 101 is a new ransomware threat targeting global users with a weaponised and heavily obfuscated .NET binary. Once executed, the ransomware encrypts local files, deletes Volume Shadow Copies, disables recovery options, and blocks access to key system tools like Task Manager and Registry Editor. It simulates legitimate processes and operates under the radar to make infected machines unrecoverable till a ransom is paid in Bitcoin. Dark 101 employs standard ransomware tactics like demanding cryptocurrency for decryption, but its emphasis on disabling user recovery capabilities makes it especially damaging for unprepared victims. Security researchers have noted that its obfuscation techniques and system manipulation mirror previously known strains but with enhanced evasion and persistence capabilities.

Organisations must emphasise behavioural monitoring, backup integrity checks, and real-time file encryption alerts to defend against such threats. Additionally, educating users to identify suspicious emails and attachments remains a crucial layer in the defence strategy.

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

Source - https://cybersecuritynews.com/dark-101-ransomware-with-weaponized-net-binary/

Crux ransomware mimics system processes to avoid detection

Crux ransomware is a new strain exhibiting sophisticated behaviour and potential links to the BlackByte group, even though attribution remains unconfirmed. The ransomware starts access via valid RDP credentials and abuses native Windows processes to encrypt data and disable recovery tools. So far, Crux has been detected in three confirmed attacks, all following similar process patterns but using varying file hashes and executable names to evade signature-based detection. These obfuscation tactics and its use of legitimate system binaries make Crux hard to detect through traditional endpoint solutions. Security experts advise organisations to enforce stricter controls on RDP access, monitor system process anomalies, and deploy behaviour-based detection methods to identify such threats.

Crux highlights the evolving trend of ransomware leveraging “living off the land” techniques to remain undetected longer and inflict greater damage. Regular audits, patch management, and restricting admin privileges can significantly reduce the risk of infection.

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

Source - https://www.huntress.com/blog/crux-ransomware

GLOBAL GROUP launches AI-powered ransomware attacks

GLOBAL GROUP is a newly discovered ransomware-as-a-service (RaaS) operation launched in June 2025. Believed to be a rebrand of BlackLock and Mamona ransomware, the group targets sectors across Australia, Brazil, the U.S., and parts of Europe. The group adopts a professionalised approach by leveraging initial access brokers, AI-powered negotiation panels, and customisable payload builders to orchestrate rapid and adaptable ransomware attacks. The group's infrastructure also includes support tools for affiliates, offering detailed dashboards and ransomware-as-a-service features. Researchers observed that GLOBAL GROUP exploits known vulnerabilities in platforms like Fortinet, Palo Alto, Microsoft Edge, and Windows.

The campaign’s emergence signals the continued evolution of ransomware as a business model, emphasising automation, scalability, and affiliate-driven monetisation. To defend against such operations, organisations must enforce vulnerability lifecycle management, threat surface reduction, and restrict privileged access across their digital environments.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Australia, Europe, UK, Brazil, United States	**APPLICATION**	Microsoft Edge, Windows, Fortinet, Palo Alto

Source - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/dire-wolf-strikes-new-ransomware-group-targeting-global-sectors/

TATA COMMUNICATIONS

Coordinated DDoS and defacement attacks surge from Allied Muslim hacktivist front

A newly declared hacktivist alliance known as the Allied Muslim Hacktivist Coalition has emerged as a growing cyber threat targeting Indian digital infrastructure. Comprised of groups such as Team BD Cyber Ninja, Team Insane PK, UNIT 1948, and Z-ALLIANCE, the coalition is conducting coordinated DDoS attacks and website defacements across the Indian defence, telecom, and education sectors. The coalition brands itself as a “cyber ummah,” invoking religious and political solidarity to justify its actions and recruit sympathisers. Their stated objective is to counter what they perceive as Indian cyber aggression, with a notable spike in activity anticipated around India’s Independence Day on August 15th. Some of their rhetoric and tactics also echo broader anti-India sentiment seen in past regional cyber conflicts.

While the group claims responsibility for multiple disruptions, Tata Communications’ CTI team has not independently verified all attack claims. Continued monitoring is advised, particularly for government-linked infrastructure that may be targeted in the lead-up to mid-August.

ATTACK TYPE	Hacktivism, DDOS, Cyberespionage	**SECTOR**	Government
REGION	India	**APPLICATION**	Generic

Source - https://www.cloudsek.com/threatintelligence/hacktivist-group-summons-allies-and-hackers-to-unite-against-govt-of-india , https://outpost24.com/blog/hacktivist-cyber-operations-iran-israel/ https://cyberpress.org/hacktivist-group-targets-over-20-critical-sectors/

KAWA4096 ransomware mimics Akira and Qilin tactics

KAWA4096 is a newly identified ransomware strain first observed in June 2025, targeting organisations across the U.S., Japan, India, and Germany. The ransomware is notable for borrowing features like site design and ransom note formatting from existing ransomware groups like Akira and Qilin. KAWA4096 employs multi-threaded encryption for speed, disables critical services, and deletes shadow copies to impede recovery. Since the attack chain is highly customisable via configuration files, it can tailor targeting and increase evasion capabilities. This flexibility, combined with borrowed but refined tactics, marks KAWA4096 as a sophisticated threat in its early development. Moreover, traditional signature-based solutions also find the ransomware harder to detect due to its ability to mimic proven elements while adapting its execution strategy.

Security professionals should prepare for this evolving strain by applying strict patching protocols, strengthening endpoint defences, and closely monitoring for encryption anomalies and service terminations, especially in high-risk geographies.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	India, Japan, Germany, United States	**APPLICATION**	Windows

Source - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/kawa4096s-ransomware-tide-rising-threat-with-borrowed-styles/

DiskStation ransomware targets misconfigured NAS devices

DiskStation ransomware targets Synology NAS devices running DiskStation Manager (DSM). It gains entry by exploiting exposed remote access or weak credentials, then uses strong algorithms to encrypt stored data and finally demands Bitcoin for decryption. Once infected, systems are locked out, and users face both operational downtime and potential data loss. Affected industries include media production, event management, and nonprofit organisations, or the sectors that rely heavily on NAS-based storage. As these environments often lack robust ransomware recovery solutions, the attack severely impacts operations. Authorities have launched investigations, with some disruption of the threat actor's infrastructure reported.

This campaign underscores the expanding scope of ransomware threats beyond traditional endpoints into critical storage infrastructure. Organisations using NAS devices should ensure systems are regularly updated, remote access is secured or disabled, and strong, unique credentials are enforced. Creating offline backups and segmenting storage access further reduces risk.

ATTACK TYPE	Vulnerability, Ransomware	**SECTOR**	Business, Broadcast Media Production and Distribution
REGION	Israel, United States, European Union	**APPLICATION**	Generic, Synology

Source - https://www.bleepingcomputer.com/news/security/police-disrupt-diskstation-ransomware-gang-attacking-nas-devices/

H2Miner botnet deploys AI-generated scareware

The H2Miner botnet, known for Monero crypto-mining, has added an AI-generated ransomware component, Lcrypt0rx. This campaign combines recycled code, public hacking tools, and VPS infrastructure to infect Windows, Linux, and containerised systems globally. While Lcrypt0rx encrypts files and issues ransom demands, its weak encryption suggests scareware-like intent rather than effective extortion. The AI-generated payload reduces the barrier for entry by allowing even low-skill actors to deploy malware, pointing to growing automation in cybercrime. Analysts describe the campaign as more of an opportunistic mashup than a high-impact threat, but it exemplifies how accessible automation tools can produce rudimentary, yet functional ransomware.

To defend against this trend, organisations must enforce least privilege, use anomaly-based detection, and educate users on suspicious behaviours. Although Lcrypt0rx lacks technical sophistication, its use alongside a mining botnet signals how traditional cyber threats are evolving into hybrid monetisation campaigns.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows, Linux

Source - https://www.fortinet.com/blog/threat-research/old-miner-new-tricks

CrazyHunter ransomware exploits drivers and USBs in Taiwan

CrazyHunter is a rising ransomware threat primarily affecting Taiwan's healthcare, tech, and industrial sectors. It uses BYOVD (Bring Your Own Vulnerable Driver) to bypass security solutions and disables endpoint defences to avoid detection. Spread via infected USB drives and open-source tools, CrazyHunter attacks combine ransomware encryption with data exfiltration, leveraging a leak site for extortion pressure. The group's tactics highlight an evolving trend toward multi-layered ransomware campaigns with tailored infection vectors and strong psychological pressure on victims. Though currently focused on Taiwan, some operations have also been detected in the U.S.

Organisations must adopt USB device restrictions, endpoint hardening, and file access monitoring to mitigate such threats. CrazyHunter blends stealth, persistence, and aggressive extortion to represent a serious challenge to sectors reliant on high data integrity and uptime.

ATTACK TYPE	Ransomware	**SECTOR**	Information technology, Healthcare/hospitals, Manufacturing, Education
REGION	Taiwan , United States	**APPLICATION**	Windows

Source - https://socradar.io/dark-web-profile-crazyhunter-ransomware/

NailaoLocker ransomware blends Chinese SM2 with AES-256

NailaoLocker is a Windows-based ransomware strain that combines standard AES-256-CBC encryption with China's SM2 cryptographic algorithm, a rarely used method in ransomware campaigns. It employs DLL side-loading for stealthy execution and includes both encryption and decryption routines within the payload. However, the embedded private key appears non-functional, suggesting the malware may be a test build or internal tool rather than a full-scale deployment. NailaoLocker's integration of SM2 indicates a shift toward region-specific encryption methods, potentially aimed at sidestepping international detection or aligning with local cryptographic standards. The strain reflects a broader trend in ransomware evolution, where attackers experiment with unique cryptographic implementations to test resilience or confuse analysis.

While NailaoLocker's impact remains limited, its technical design warrants attention. Organisations should monitor for DLL side-loading activity, verify encryption routines, and stay informed on emerging regional cryptographic techniques used in malware.

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

Source - https://www.fortinet.com/blog/threat-research/nailaolocker-ransomware-cheese

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