TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 22, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Today’s rapidly-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.

Through expert analysis and actionable strategies, we help clients anticipate, detect, and neutralise threats before they escalate with our weekly Cyber Threat Intelligence (CTI) reports. These provide critical insights into emerging risks, vulnerabilities, and attack trends, empowering businesses to fortify defences and stay ahead of cyber adversaries. 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.

Amber Albatross: Malware hidden in fake PDF tool

Amber Albatross is a persistent malware campaign identified by Red Canary. Active since January 2024, it delivers Pyarmor-obfuscated PyInstaller executables with stealer-like features via potentially unwanted programs (PUPs) like PC App Store and Let's Compress. A key infection vector is PDFast—a fake PDF converter. Once installed, it can remain dormant for up to 21 days before executing payloads that conduct reconnaissance and exfiltrate browser credentials. Anti-analysis methods such as command-line obfuscation, scheduled tasks, and delayed execution make it difficult to detect.

MSPs and software developers should proactively hunt for artefacts like PDFast.exe, upd.exe, and suspicious scheduled tasks. Deploying advanced EDR solutions and using threat intelligence feeds can help detect obfuscated Python-based malware. It is also critical to implement strict application controls and user education to avoid PUP-based infections.

ATTACK TYPE	Malware	**SECTOR**	IT, Software Development
REGION	Global	**APPLICATION**	Windows

Source - https://redcanary.com/threat-detection-report/threats/amber-albatross/

Nitrogen ransomware now targets Linux systems

Nitrogen Ransomware has rapidly expanded its capabilities, targeting both Windows and Linux systems across the U.S., Canada, and Europe. Active since October 2024, it appends .nba to encrypted files and often demands €200,000 in ransom. The group threatens DDoS attacks if payment is not made and operates dedicated leak sites. It uses timestamp tampering, branding tactics, and obfuscation techniques similar to Cactus and AwfulRobber ransomware, and its recent pivot to Linux marks a strategic escalation.

Organisations should secure Linux environments with endpoint protections traditionally used for Windows. Backup systems must be segregated and tested. Network segmentation, timely patching, and strict privilege controls are key. Additionally, DDoS mitigation and ransom negotiation protocols should be prepared in advance.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Canada, France, Germany, Italy, Portugal, United States	**APPLICATION**	Windows, Linux

Source - https://github.com/TheRavenFile/Daily-Hunt/blob/main/Nitrogen%20Ransomware

NordDragonScan steals browser and system data

NordDragonScan is a stealthy infostealer that targets Windows systems through weaponised HTA scripts delivered in malicious RAR and LNK files. It disguises itself as legitimate documentation and drops adblocker.exe as the main payload while copying itself as install.exe. Once active, it collects system information, browser profiles, documents, and screenshots, and exfiltrates them to the C2 server kpuszkiev.com. Its use of LNK shortcuts and scripting enables easy bypass of traditional antivirus tools.

Enterprises should block execution of HTA scripts and inspect RAR archives and LNK files within emails. EDR solutions must monitor for file behaviours related to install.exe or adblocker.exe. DNS filtering and firewall rules should be enforced to prevent communications with suspicious domains such as kpuszkiev.com.

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

Source - https://www.fortinet.com/blog/threat-research/norddragonscan-quiet-data-harvester-on-windows

AiLock ransomware uses ChaCha20 and NTRUEncrypt

First spotted in March 2025, AiLock is a ransomware strain operating under the ransomware-as-a-service (RaaS) model. It encrypts files using ChaCha20 and NTRUEncrypt, appends the .AiLock extension, and drops ransom notes in affected directories. Its encryption engine is multithreaded and uses IOCP for efficiency. The group runs active leak sites and employs system modifications for persistence and stealth. Its structure and speed make it a growing concern among defenders.

Organisations must secure backups offline, isolate high-value assets, and use behaviour-based ransomware protection tools. Network monitoring and logging should focus on abnormal encryption activity and newly created ransom note files. Ransomware tabletop exercises should include AiLock-specific indicators to ensure preparedness.

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

Source - https://medium.com/s2wblog/detailed-analysis-of-ailock-ransomware-1d3263beff15

DoNot Team targets European diplomats with LoptikMod

DoNot Team, an APT group suspected to be India-linked, has shifted from South Asian targets to a European foreign affairs ministry. The group launched a spear-phishing campaign using spoofed defence ministry emails, ultimately deploying the custom malware LoptikMod. The malware enables surveillance and data exfiltration, and its deployment marks a geopolitical shift in DoNot Team's objectives. The campaign indicates improved tradecraft and adaptation to high-value targets in diplomatic circles.

Governments and diplomatic institutions should enforce email authentication protocols (DMARC, SPF, DKIM) and deploy robust anti-phishing tools. Threat detection should focus on identifying LoptikMod behaviours, while red-teaming exercises should simulate APT-style spear-phishing. Cross-border threat intelligence sharing is essential to anticipate further attacks.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	Europe, South Asia	**APPLICATION**	Windows

Source - https://www.trellix.com/blogs/research/from-click-to-compromise-unveiling-the-sophisticated-attack-of-donot-apt-group-on-southern-european-government-entities/

SafePay ransomware mimics LockBit 3.0, hits 200+ targets

SafePay is a centralised ransomware operation—not a typical affiliate-based model—which has already targeted over 200 MSPs and SMBs globally. It closely mimics LockBit 3.0 in its evasion and encryption tactics but maintains tighter internal controls over the entire attack lifecycle. Its malware is highly stealthy and incorporates exfiltration prior to encryption. SafePay is believed to be behind high-profile breaches such as Ingram Micro, signalling a rise in vertically integrated cybercrime operations.

MSPs and SMBs must apply zero-trust principles, implement endpoint detection with exfiltration alerting, and secure third-party access points. Regular threat simulations and incident response reviews are critical. Logging must be centralised to detect early signs of data theft or malware staging.

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

Source - https://securityonline.info/safepay-ransomware-unleashed-new-lockbit-3-0-variant-hits-200-msps-smbs-worldwide/
https://www.acronis.com/en-us/tru/posts/safepay-ransomware-the-fast-rising-threat-targeting-msps/

Pay2Key.I2P: Iranian ransomware campaign resurfaces

Pay2Key.I2P is an advanced ransomware operation aligned with Iranian interests, believed to be linked to the Fox Kitten APT. It combines financial motivations with ideological targeting, focusing on Western organisations in sectors like IT, healthcare, and BFSI. Affiliates are incentivised with high revenue shares, and over $4 million has been extorted in four months. Technical similarities to Mimic ransomware and use of the I2P network for anonymity add to its sophistication.

Businesses in targeted sectors must enhance email security, restrict admin privileges, and segment sensitive infrastructure. Linux defences must match Windows parity. Threat intel should include I2P indicators and known Mimic artifacts. Collaboration with national CERTs is also strongly advised.

ATTACK TYPE	Ransomware	**SECTOR**	Information technology, Healthcare/hospitals, Manufacturing, IT, Education, BFSI
REGION	Israel, United States, European Union	**APPLICATION**	Windows, Linux

Source - https://www.morphisec.com/blog/pay2key-resurgence-iranian-cyber-warfare/

SLOW#TEMPEST uses sophisticated obfuscation tactics

The SLOW#TEMPEST campaign features advanced malware that uses dynamic code jumps, indirect function calls, and DLL side-loading to defeat static and dynamic analysis. Payloads are separated from the main loader to hinder reverse engineering. Security researchers developed custom emulation scripts to reveal hidden behaviours. This underscores the growing complexity of threat actor tradecraft, especially in campaigns targeting Fortinet's FortiWeb WAF products.

Security teams should enhance dynamic sandbox analysis and script-based emulation to detect such obfuscated malware. Organisations using FortiWeb must ensure all firmware is up to date and monitor for abnormal DLL load behaviours. Threat detection rules should be updated to reflect SLOW#TEMPEST techniques.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Fortinet FortiWeb WAF

Source - https://unit42.paloaltonetworks.com/slow-tempest-malware-obfuscation/

Fortinet FortiWeb SQLi vulnerability under attack

A critical SQL injection vulnerability in Fortinet FortiWeb (CVE-2025-25257) allows unauthenticated remote code execution. The flaw lies in the Fabric Connector API and was publicly disclosed with proof-of-concept (PoC) exploits released. Affected FortiWeb versions are highly susceptible unless patched, and the vulnerability has wide-reaching impact across IT, hospitality, and BFSI sectors.

Organisations must immediately upgrade FortiWeb devices to patched versions. Until then, isolating vulnerable appliances from the internet is critical. Web application firewall rules should be tightened, and all access logs should be reviewed for potential exploitation attempts dating back to early July 2025.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare/hospitals, Tourism/Hospitality, IT, Aviation, BFSI
REGION	Global	**APPLICATION**	Fortinet

Source - https://www.bleepingcomputer.com/news/security/exploits-for-pre-auth-fortinet-fortiweb-rce-flaw-released-patch-now / https://thehackernews.com/2025/07/fortinet-releases-patch-for-critical.html

Solar Spider hits Indian and Middle Eastern banks with JSOutProx

Solar Spider, a financially motivated Chinese APT, is using JSOutProx—a modular remote access trojan—to target cooperative banks in India and financial entities in the Middle East. Delivered via spear-phishing, JSOutProx enables credential theft, transaction tampering (especially NEFT/RTGS), and remote access. The malware is hosted on trusted platforms like GitHub, making detection difficult. The attackers' focus on H2H and SFMS infrastructures suggests in-depth understanding of banking operations.

To combat this threat, banks must enforce multi-layered email security and isolate SFMS/H2H systems from broader networks. Threat intelligence should track GitHub and GitLab payload activity. EDR solutions must be fine-tuned for remote access and credential theft behaviour. Collaboration with central banks and financial CERTs is essential for coordinated defence.

ATTACK TYPE	Malware	**SECTOR**	Government, BFSI
REGION	Middle East, India	**APPLICATION**	Windows

Source - https://www.cert-in.org.in/

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