TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 16, 2025

THREAT INTELLIGENCE ADVISORY REPORT

As we step into the second half of 2025, cyber adversaries are showing no signs of abatement. The first six months were marked by a sharp rise in AI-powered phishing campaigns, targeted supply chain breaches, and stealthier ransomware operations—clear signals that traditional defences may no longer be sufficient. Alongside technological advancement, malicious actors are increasingly refining their tactics, forcing organisations to rethink their safeguarding approach.

To stay resilient, businesses must be aware of the threat landscape. Awareness builds the prescience needed to strengthen core security foundations and adopt layered, intelligence-led strategies to anticipate and neutralise evolving threats. Tata Communications' weekly threat intelligence updates are designed to give your security teams this edge. Each report delivers timely assessments and actionable insights, helping you detect, prioritise, and respond to risks before they disrupt your operations.

Interlock ransomware expands double extortion operations globally

First observed in September 2024, the Interlock ransomware group has swiftly emerged as a potent cyber-threat, notably foregoing the common Ransomware-as-a-Service model in favour of a closed-door, opportunistic structure. It gains initial access via compromised legitimate websites and employs increasingly sophisticated social-engineering methods such as the “ClickFix” technique to deliver remote access trojans. The group then executes double-extortion campaigns, operating its private “Worldwide Secrets Blog” to pressure victims.

In mid-2025, Interlock expanded its toolkit by adopting the evolved “FileFix” delivery technique, which misleads users into pasting malicious commands into the File Explorer address bar, often resulting in the deployment of a PHP-based Remote Access Trojan (RAT). The RAT gathers system and Active Directory data, scans for backups, and ultimately deploys the Interlock ransomware payload. Recent campaigns in sectors such as healthcare and government underscore the growing regional risk across North America and Europe.

ATTACK TYPE	Ransomware	SECTOR	Government, IT, Healthcare, Manufacturing, Education, BFSI, Automobile
REGION	North America, Europe	APPLICATION	Windows, Linux

Source - https://arcticwolf.com/resources/blog/threat-actor-profile-interlock-ransomware/

Emerging World Leaks ransomware heightens enterprise security risks

World Leaks, formerly operating as Hunters International, formally ceased its ransomware-as-a-service (RaaS) operations after nearly two years of activity, redeploying as a pure data-extortion entity. In this new phase, the group abandons encryption in favour of stealing sensitive data and issuing threats to publicly leak it, intensifying pressure on victims to acquiesce.

World Leaks shifted its tactics to a streamlined extortion model, supplying affiliates with a bespoke exfiltration tool to automate data theft. Operating under a RaaS model since 2022, the group encrypts systems, steals sensitive data, and threatens public leaks to maximise payments. Its attack chain leverages phishing, vulnerable application exploits, PowerShell, malicious macros, and credential theft to achieve persistence, escalate privileges, and move laterally across networks, culminating in data exfiltration and encryption.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.linkedin.com/pulse/ransomware-spotlight-worldleaks-group-adam-tindall-l8gzc/

OAuth exploitation targets major enterprise SaaS systems

Google's corporate Salesforce environment and its Salesloft Drift integration were breached in a sophisticated campaign linked to ShinyHunters affiliates, tracked by Google as UNC6040 and UNC6395. Attackers combined vishing – impersonating IT support via phone with malicious OAuth apps and anonymised infrastructure such as Mullvad VPN and TOR to harvest business contact data, credentials, and tokens from hundreds of organisations.

These incidents underscore how identity-based intrusions and abused third-party SaaS integrations now represent primary attack vectors in modern cloud environments. The breach demonstrates an urgent need for tighter OAuth governance, continuous monitoring of authentication tokens, and strengthened call-centre defences. Organisations must also enforce least-privilege access, vet connected apps meticulously, and implement logging to detect anomalous activity within SaaS ecosystems.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Salesloft - Drift

Source - https://www.seqrite.com/blog/google-salesforce-breach-unc6040-threat-research/

NEZHA ransomware deploys lateral movement for propagation

Researchers have identified an emerging Windows-targeting ransomware strain named NEZHA, which encrypts files using the .NEZHA extension and deposits a README.TXT ransom note. Victims are promised one free decryption of a non-valuable file and warned that third-party decryption attempts, or file renaming, may result in permanent data loss. The note claims long-term network access, data exfiltration, and imminent public leakage if demands go unmet.

NEZHA uses sophisticated tactics, including WMI, credential theft, keylogging, system and network discovery, obfuscation, masquerading, access-token manipulation, and lateral movement via shared content. While still in its nascent stage, the ransomware's evolving TTPs and confirmed indicators suggest increasing sophistication and potential adoption of more scalable extortion models — such as double or even triple extortion or RaaS frameworks.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	SAP NetWeaver ABAP, SAP HANA Cloud

Source - https://www.cyfirma.com/news/weekly-intelligence-report-05-september-2025/

SAP S/4HANA flaw enables arbitrary code execution worldwide

A critical ABAP code-injection flaw, CVE-2025-42957, affecting SAP S/4HANA (both private-cloud and on-premises), is now being actively exploited in the wild. This vulnerability allows even low-privileged users to inject arbitrary ABAP code via exposed RFC modules, bypassing authorisation checks and effectively functioning as a backdoor. Discovered in late June 2025, the flaw was patched on 11 August 2025. Presently, unpatched systems remain dangerously exposed.

SecurityBridge and Pathlock have confirmed real-world misuse of the flaw, warning that exploitation requires minimal effort and may result in full system compromise. Attackers with basic SAP access can steal data, elevate privileges, create admin-level accounts, alter business processes, and even deploy ransomware or malware on the host OS. As the ABAP code is transparent, reverse-engineering the patch to develop exploits is relatively trivial.

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

Source - https://www.csoonline.com/article/4051870/alert-exploit-available-to-threat-actors-for-sap-s-4hana-critical-vulnerability.html
https://www.bleepingcomputer.com/news/security/critical-sap-s-4hana-vulnerability-now-exploited-in-attacks/

CISA confirms active exploitation of three KEV catalogue vulnerabilities

CISA has added three newly verified, actively exploited vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue, with remediation mandated by 25 September 2025 under BOD 22-01 for federal agencies. These include CVE-2025-38352, a Linux kernel TOCTOU race condition in POSIX CPU timers; CVE-2025-48543, an Android Runtime privilege escalation vulnerability; and CVE-2025-53690, a deserialisation flaw in Sitecore allowing remote code execution.

These flaws enable a range of attacks, including privilege escalation, sandbox escape, denial of service and arbitrary code execution, and are associated with malware such as WeepSteel, Dwagent, and Earthworm. Although the 25 September remediation deadline applies to FCEB agencies, CISA strongly advises all organisations to apply vendor-recommended mitigations immediately to curtail escalating risks across Linux, Android, and Sitecore environments.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Android, Sitecore CMS, Linux

Source - https://securityonline.info/cisa-adds-three-new-vulnerabilities-to-catalog-urges-immediate-patching/

APT28 NotDoor leverages Outlook VBA macros for covert data theft

Researchers have uncovered NotDoor, a novel Outlook VBA macro backdoor attributed to the Russia-linked APT28, targeting NATO-associated organisations. The malware is deployed via DLL side-loading through Microsoft’s OneDrive.exe, bypassing macro defences. Once loaded, it leverages Outlook’s event hooks to monitor incoming emails for a specific trigger word and, upon activation, allows attackers to execute commands, exfiltrate data, and upload files with stealth and precision.

NotDoor employs multiple stealth techniques, including obfuscation, Base64-encoded PowerShell commands, registry modifications for persistence, and suppression of Outlook dialogues. It creates a staging folder in %TEMP%\Temp to hold exfiltrated data and sends it to a Proton Mail address. The backdoor supports functionality to parse email triggers such as “Daily Report” to execute commands, transfer files, and erase traces, posing a significant covert threat to targeted organisations.

ATTACK TYPE	Malware	SECTOR	All
REGION	Europe, Canada, UK, Greece, Turkey, Ukraine, United States	APPLICATION	Microsoft Outlook, Microsoft OneDrive

Source - https://thehackernews.com/2025/09/russian-apt28-deploys-notdoor-outlook.html

PowerShell multi-stage attack compromises energy networks

A previously unknown APT group, dubbed Noisy Bear, has emerged. Active since April 2025, the group is known to specifically target Kazakhstan’s oil and gas sector, most notably KazMunaiGas. The operation, codenamed Operation BarrelFire, initiates via spear-phishing emails containing a ZIP attachment with a malicious .LNK shortcut disguised as a salary schedule. These emails mimic internal HR or policy communications to deceive recipients.

Once executed, the shortcut downloads batch scripts that deploy obfuscated PowerShell loaders known as DOWNSHELL, which disable AMSI, inject reverse-shell payloads, and load DLL implants. Infrastructure analysis reveals the use of open-source red-team tools and hosting via Aeza Group LLC, a service provider linked to sanctioned Russian infrastructure, thereby suggesting Russian origins. The multi-stage infection chain underscores Noisy Bear’s operational sophistication.

ATTACK TYPE	Malware	SECTOR	All
REGION	Kazakhstan	APPLICATION	Microsoft Outlook, Windows, PowerShell

Source - https://www.seqrite.com/blog/operation-barrelfire-noisybear-kazakhstan-oil-gas-sector/\

INTRODUCTION | SOCIAL ENGINEERING POWERS INTERLOCK RANSOMWARE CAMPAIGN | WORLD LEAKS RANSOMWARE ESCALATES DOUBLE EXTORTION ATTACKS | ENTERPRISE PLATFORMS BREACHED THROUGH OAUTH MANIPULATION | SOPHISTICATED NEZHA VARIANT ADOPTS WMI FOR MULTI-EXTORTION TACTICS | SAP S/4HANA CODE INJECTION FLAW EXPLOITED GLOBALLY | CRITICAL KEV FLAWS IN LINUX, ANDROID, AND SITECORE EXPLOITED | NOTDOOR INFILTRATES THROUGH EMAIL PLATFORM BYPASSING SECURITY PROTECTIONS | SPEAR-PHISHING CAMPAIGN DELIVERS ADVANCED POWERSHELL MALWARE | NEW NIGHTSHADEC2 INFOSTEALER TARGETS WINDOWS UAC VULNERABILITIES | HACKERS EXPLOIT THREAT INTEL PLATFORMS FOR EVASION

NightshadeC2 exploits UAC prompt bombing to evade detection

NightshadeC2, a new botnet and infostealer delivered via ClickFix-style phishing lures and trojanised legitimate utilities, has been discovered recently. The malware employs a novel evasion technique dubbed “UAC Prompt Bombing”, coercing users to approve repeated Windows UAC prompts to exclude payloads from sandbox and Defender detection. Both C and Python variants have been identified.

The NightshadeC2 offers extensive capabilities: reverse shells, credential harvesting, keystroke and clipboard capture, DLL/EXE payload execution, screen capture, and remote control, including mouse and keyboard simulation. It persists through registry keys, communicates via encrypted channels, and fingerprints environments by collecting external IP and system identifiers. In response, TRU isolated affected hosts, conducted global threat hunts, and developed bespoke detection and prevention rules.

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

Source - https://www.esentire.com/blog/new-botnet-emerges-from-the-shadows-nightshadec2

Threat actors weaponise security intel platforms against defenders

North Korean threat actors behind the "Contagious Interview" campaign exploit platforms like Validin, VirusTotal, and Maltrail to monitor their infrastructure and find new assets. These actors exploit cyber threat intelligence platforms while coordinating via Slack. Rather than enhance stealth, they rapidly deploy replacement infrastructure when one asset is disrupted, prioritising operational continuity over long-term concealment.

Between January and March 2025, over 230 individuals – predominantly crypto-sector job seekers were targeted via ClickFix-style social engineering lures involving fake interviews delivered over Slack and other channels. Despite awareness of their own indicators of compromise, the threat actors only made minimal modifications to exposed infrastructure, demonstrating poor OPSEC. Their emphasis remains on rapid asset turnover and campaign volume rather than infrastructure hardening.

ATTACK TYPE	Malware, Cyberespionage	SECTOR	Financial services, IT
REGION	Global	APPLICATION	Apple Mac OS, Windows, Linux, Node.js, Node JS, Node Packager Manager (NPM)

Source - https://www.sentinelone.com/labs/contagious-interview-threat-actors-scout-cyber-intel-platforms-reveal-plans-and-ops/

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.