TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 9, 2025

THREAT INTELLIGENCE ADVISORY REPORT

As cyber threats become increasingly advanced across the globe, malicious actors are deploying ever more intricate methods to penetrate corporate security systems. Traditional protective measures are proving inadequate against these sophisticated attacks, compelling organisations to bolster their essential digital foundations and adopt comprehensive, multi-tiered security frameworks to effectively counter emerging cyber adversaries.

Safeguard your organisation with Tata Communications' weekly threat intelligence updates. This weekly resource provides vital threat assessments and up-to-date security intelligence, enabling your security teams to identify and address potential cyber risks before they can compromise your operations.

HanKook operation uses hidden LNK payloads targeting systems

Operation HanKook Phantom is a covert espionage campaign orchestrated by North Korea–linked APT37 (aka ScarCruft, InkySquid, Ricochet Chollima), delivering malicious LNK shortcuts disguised as the “National Intelligence Research Society Newsletter – Issue 52”. Once executed, these LNK files initiate a multi-stage chain: decoy PDFs or Word documents, fileless PowerShell scripts, in-memory XOR decryption of payloads and finally evoke the RokRAT remote access Trojan.

APT37 targets South Korean academics, ex-officials and research institutions using sophisticated spear-phishing to steal sensitive data, establish persistence, monitor systems, and conduct long-term surveillance. The campaign abuses cloud services like Dropbox, pCloud, Yandex (and Google Cloud) as covert C2 channels, hiding communications. Observed techniques include anti-VM checks, living-off-the-land scripting, screenshot capture and remote command execution to evade detection.

ATTACK TYPE	Malware	SECTOR	Government
REGION	Middle East, Russia, India, Japan, China, South Korea, Kuwait, Nepal, Romania, Vietnam	APPLICATION	Windows

Source - https://www.seqrite.com/blog/operation-hankook-phantom-north-korean-apt37-targeting-south-korea/

INTRODUCTION | HANKOOK PHANTOM CAMPAIGN USES MALICIOUS LNK FILES | AI TECHNOLOGY POWERS NEXT-GENERATION RANSOMWARE | CEPHALUS MALWARE BYPASSES SECURITY THROUGH DLL LOADING | STORM-0501 SHIFTS TO CLOUD-BASED RANSOMWARE TACTICS | CSS OBFUSCATION POWERS ADVANCED RANSOMWARE CAMPAIGN | SINOBI ATTACKERS DISABLE SECURITY TOOLS BEFORE ENCRYPTION | STATE-SPONSORED HACKERS BREACH NETWORKS ACROSS MULTIPLE SECTORS | WHATSAPP ADDRESSES SEVERE “ZERO CLICK” SECURITY THREAT | PHISHING OPERATION USES UPCRYPTER FOR RAT DISTRIBUTION | DATA THEFT CAMPAIGN TARGETS SALESFORCE OAUTH TOKENS

Smart ransomware uses AI for automated global security attacks

PromptLock is believed to be the first known AI-powered ransomware which dynamically generates malicious scripts via an AI model. PromptLock runs a locally accessible generative language model via an API to dynamically generate malicious Lua scripts in real time. These cross-platform scripts, compatible across Windows, Linux and macOS, autonomously determine whether to exfiltrate or encrypt data based on predefined text prompts. This marks a potentially significant shift in cyber-attack modalities.

Although PromptLock remains a proof-of-concept, its discovery signals a concerning evolution. The malware is written in Golang, employs SPECK 128-bit encryption, and early variants have surfaced on VirusTotal. It even contains dormant, destructive functionality. By significantly lowering the barrier to sophisticated attacks through AI automation, PromptLock poses a real threat to detection efforts, illustrating how generative AI could complicate cyber-defensive operations.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows, Linux

Source - https://www.eset.com/us/about/newsroom/research/eset-discovers-promptlock-the-first-ai-powered-ransomware/

INTRODUCTION | HANKOOK PHANTOM CAMPAIGN USES MALICIOUS LNK FILES | AI TECHNOLOGY POWERS NEXT-GENERATION RANSOMWARE | CEPHALUS MALWARE BYPASSES SECURITY THROUGH DLL LOADING | STORM-0501 SHIFTS TO CLOUD-BASED RANSOMWARE TACTICS | CSS OBFUSCATION POWERS ADVANCED RANSOMWARE CAMPAIGN | SINOBI ATTACKERS DISABLE SECURITY TOOLS BEFORE ENCRYPTION | STATE-SPONSORED HACKERS BREACH NETWORKS ACROSS MULTIPLE SECTORS | WHATSAPP ADDRESSES SEVERE “ZERO CLICK” SECURITY THREAT | PHISHING OPERATION USES UPCRYPTER FOR RAT DISTRIBUTION | DATA THEFT CAMPAIGN TARGETS SALESFORCE OAUTH TOKENS

Cephalus ransomware campaign targets RDP through DLL loading

In mid-August, two distinct incidents saw the emergence of the Cephalus ransomware variant. Attackers gained initial access via compromised RDP accounts lacking multi-factor authentication and leveraged the MEGA cloud storage platform, presumably for data exfiltration. Execution relied on a stealthy technique: sideloading a malicious DLL through a legitimate SentinelOne executable (SentinelBrowserNativeHost.exe) in the Downloads folder, which subsequently loaded a data.bin file containing the ransomware payload

Once deployed, Cephalus systematically disabled recovery and security controls. It executed commands to delete shadow copies, create exclusions in Windows Defender, and disable real-time protection, behaviour monitoring, and related security services via PowerShell and registry changes. Ransom notes included links to news articles about prior Cephalus campaigns and even offered a GoFile.io link and password for victims to verify stolen data, underscoring the need to monitor pre-encryption activity closely.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

Storm-0501 leverages hybrid cloud security gaps for extortion

Recent analysis reveals that Storm-0501 has advanced from deploying traditional on-premises ransomware to exploiting hybrid cloud vulnerabilities, including misconfigured Entra ID identities and Entra Connect Sync accounts, to conduct cloud-centric extortion. Without deploying any malware, the group exfiltrates and deletes data and backups by escalating privileges in Active Directory and Entra ID.

Storm-0501's operations exploit visibility gaps in hybrid cloud environments, such as uneven Defender deployment and unchecked sync servers, to move laterally and gain global administrator rights. The group then exfiltrates data using Azure-native tools and destroys backups and storage resources without traditional ransomware executables. This rapid, stealthy shift demands enhanced monitoring of pre-encryption activity to detect and mitigate such cloud-based extortion tactics early.

ATTACK TYPE	Ransomware, Cyberespionage	SECTOR	Healthcare, Financial services, IT, Education, Business
REGION	Global	APPLICATION	Windows, Microsoft Azure, Microsoft Entra

Source - https://www.sentinelone.com/anthology/blacknevas/
https://www.cyfirma.com/news/weekly-intelligence-report-15-august-2025/

ClickFix Social Engineering conceals ransomware payloads

A novel ClickFix social engineering threat exploits AI summarisation tools by embedding malicious instructions within documents. The tool uses CSS obfuscation techniques such as zero-width characters, white-on-white text, tiny fonts, and off-screen positioning to render payloads invisible to humans yet readable to AI models. Combined with “prompt overdose,” whereby these hidden prompts are repeated to dominate the summariser’s context, the technique causes AI-generated summaries to include ransomware execution steps.

This attack vector dramatically amplifies enterprise risk by enabling summarisation tools in email clients, browsers, and productivity platforms to unwittingly deliver harmful commands. The result: amplified social-engineering lures and a lowered barrier to ransomware execution, even for non-technical users. Mitigation demands rigorous content sanitisation, including stripping obfuscated text before summarisation, implementing prompt filtering to detect overdosed payloads, and balancing AI contextual cues to prevent hidden instructions from commandeering outputs.

ATTACK TYPE	Ransomware, Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cloudsek.com/blog/trusted-my-summarizer-now-my-fridge-is-encrypted----how-threat-actors-could-weaponize-ai-summarizers-with-css-based-clickfix-attacks

Sinobi attackers disable security tools using compromised VPN access

A targeted deployment of Sinobi ransomware, which is believed to be a rebrand of Lynx, was deployed in a targeted attack. During this, the ransomware used stolen SonicWall VPN credentials tied to a domain admin account in August 2025. The initial access was gained using stolen SonicWall SSL VPN credentials tied to a domain-admin MSP account, enabling internal network access and direct RDP into a file server.

Once inside, attackers disabled Carbon Black EDR after discovering stored deregistration codes, and then exfiltrated sensitive data using RClone to remote hosting infrastructure. The deployed ransomware encrypted files across local and shared drives with robust Curve-25519 + AES-128-CTR cryptography, deleted shadow copies, killed backup-related processes, and left ransom notes (using the .SINOBI extension) to pressure victims into paying.

ATTACK TYPE	Ransomware	SECTOR	Allr
REGION	Global	APPLICATION	Windows, SonicWall

Source - https://www.esentire.com/blog/threat-actors-deploy-sinobi-ransomware-via-compromised-sonicwall-ssl-vpn-credentials

CISA exposes state-sponsored global espionage operation

Since 2021, PRC state-sponsored APT actors have been compromising global networks, particularly targeting telecommunications, government, transportation, lodging, and military infrastructure by exploiting known CVEs in backbone, provider edge, and customer edge routers. They gain access without zero-day exploits, leveraging obfuscation tactics and modifying router configurations for long-term persistence. This espionage illustrates the critical risk posed by under-monitored network edge devices.

Once embedded, these APT actors establish persistence through modified ACLs permitting attacker-controlled IPs, open or non-standard ports. They also deploy GRE or IPsec tunnels for covert lateral movement and data exfiltration. This activity aligns with known threat clusters such as Salt Typhoon, OPERATOR PANDA, RedMike, UNC5807, and GhostEmperor linked to Chinese network firms. The advisory urges defenders to enhance visibility across edge infrastructure to detect and evict these threats.

ATTACK TYPE	Vulnerability, Cyberespionage	SECTOR	All
REGION	Global	APPLICATION	Cisco IOS, Palo Alto Networks PAN-OS, Ivanti

Source - https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

Critical WhatsApp “Zero Click” vulnerability gets patched

WhatsApp has patched a serious zero-click vulnerability, CVE-2025-55177, affecting its iOS and macOS apps that involved incomplete authorisation of linked-device sync messages. Rated with a high CVSS score of 8.0, the flaw could allow an attacker to trigger the processing of content from an arbitrary URL without user interaction. The flaw was reportedly chained with an Apple OS flaw (CVE-2025-43300) in extremely sophisticated spyware campaigns.

Meta confirmed it has sent breach notifications to fewer than 200 users believed to have been targeted, urging recipients to apply updates and perform a full factory reset. Amnesty International’s Security Lab characterised the incident as a zero-click advanced spyware campaign affecting high-profile Apple users. This update underscores the enduring need for vigilance around messaging clients and swift patching of both app and OS vulnerabilities.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Generic, WhatsApp

Source - https://thehackernews.com/2025/08/whatsapp-issues-emergency-update-for.html

INTRODUCTION

HANKOOK PHANTOM CAMPAIGN USES MALICIOUS LNK FILES

AI TECHNOLOGY POWERS NEXT-GENERATION RANSOMWARE

CEPHALUS MALWARE BYPASSES SECURITY THROUGH DLL LOADING

STORM-0501 SHIFTS TO CLOUD-BASED RANSOMWARE TACTICS

CSS OBFUSCATION POWERS ADVANCED RANSOMWARE CAMPAIGN

SINOBI ATTACKERS DISABLE SECURITY TOOLS BEFORE ENCRYPTION

STATE-SPONSORED HACKERS BREACH NETWORKS ACROSS MULTIPLE SECTORS

WHATSAPP ADDRESSES SEVERE “ZERO CLICK” SECURITY THREAT

PHISHING OPERATION USES UPCRYPTER FOR RAT DISTRIBUTION

DATA THEFT CAMPAIGN TARGETS SALESFORCE OAUTH TOKENS

Sophisticated phishing campaign spreads UpCrypter malware loader

A sophisticated phishing campaign that uses personalised emails masquerading as voicemails or purchase orders to deliver malicious URLs directing recipients to realistic, domain-branded landing pages has been exposed recently. Users are enticed to download a ZIP containing an obfuscated JavaScript dropper known as UpCrypter, which then executes in-memory to deploy remote access tools without creating forensic artefacts.

UpCrypter acts as a versatile loader, employing anti-analysis checks such as connectivity tests, sandbox detection, and steganographic payload delivery in images and then launches RATs, including PureHVNC, DCRat, and Babylon RAT to grant full remote control. The campaign operates globally across sectors, including manufacturing, technology, healthcare, construction, and retail/hospitality, and its rapid detection doubling within weeks underscores its aggressive erosion of defences.

ATTACK TYPE	Malware	SECTOR	IT, Healthcare, Manufacturing, Construction, Hospitality, Retailer and Distributor
REGION	North America, South America, Europe, Africa, Asia	APPLICATION	Windows

Source - https://www.fortinet.com/blog/threat-research/phishing-campaign-targeting-companies-via-upcrypter

UNC6395 breaches Salesforce instances for mass exfiltration

Researchers have identified a data theft campaign by UNC6395, which exploited compromised OAuth tokens from the Salesloft Drift app to access Salesforce instances between 8 and 18 August 2025. The attackers exfiltrated sensitive data, including AWS keys, Snowflake tokens, and stored passwords. They conducted extensive searches for credentials and secrets, and deleted query jobs after use, although the underlying logs were still retained within affected environments.

Salesloft and Salesforce responded on 20 August by revoking exposed tokens and removing the malicious app from customer environments. Google researchers stress that the incident did not stem from a Salesforce flaw but rather from OAuth token misuse. Impacted organisations are advised to assume compromise, rotate credentials, review historical access logs, and tighten identity and access management controls to prevent follow-on intrusions or data misuse.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Generic, Amazon Web Services, Amazon Web Services AWS, Google OAuth

Source - https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift/

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.