

# YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: DECEMBER 9, 2025



# THREAT INTELLIGENCE ADVISORY REPORT

The cyber threat landscape is intensifying, fuelled by the accelerating scale and sophistication of hostile activities. Traditional defence models are proving inadequate as threats exploit structural vulnerabilities across highly interconnected digital ecosystems. To maintain resilience and strategic advantage, organisations must strengthen foundational security frameworks, deploy multi-layered defences, and embed anticipatory intelligence throughout their architectures.

In this high-risk environment, Tata Communications' Cyber Threat Intelligence report becomes indispensable. Published weekly, it delivers incisive analysis of emerging attack campaigns, evolving adversarial tactics, and sector-specific exposures. By translating intelligence into immediate defensive action, the bulletin enables security teams to anticipate, prepare for, and neutralise threats proactively – safeguarding critical operations before disruption takes hold.

INTRODUCTION

APT36 DEPLOYS LINUX-BASED RAT TARGETING GOVERNMENT CRITICAL SYSTEMS

GOVERNMENT AND PRIVATE SECTORS UNDER SUSTAINED RANSOMWARE DDOS ASSAULT

SCATTERED LAPSUS DEPLOYS FAKE SSO PAGES TARGETING ZENDESK

ADVANCED KYBER RANSOMWARE DEPLOYS HYBRID ENCRYPTION TECHNIQUES

NEW CHICKENKILLER RANSOMWARE USES WMI FOR ENVIRONMENT VALIDATION

FSOCIETY AFFILIATE RAAS MODEL DRIVES SURGE IN GLOBAL ENTERPRISE ATTACKS

CLICKFIX STEALER DEPLOYS FAKE UPDATE SCREENS VIA CONCEALED PNG PAYLOADS

CLIPBOARD HIJACKING USED IN ELABORATE DPRK FAKE RECRUITMENT SITE ATTACK

WATER GAMAYUN DEPLOYS HIDDEN POWERSHELL CHAIN VIA MSC EXPLOIT

BLOODY WOLF APT USES FAKE MINISTRY EMAILS TO INSTALL SURVEILLANCE

# APT36 launches Linux-focused espionage chain targeting government entities

As of late November 2025, APT36 – also known as Transparent Tribe – has launched a sophisticated cyber-espionage campaign targeting Indian government entities. Cyber reports confirmed the attackers distribute spear-phishing emails containing weaponised Linux “.desktop” shortcut files that masquerade as benign documents. Once opened, these shortcuts silently fetch a 64-bit ELF executable and a shell script from attacker-controlled infrastructure, executing payloads in the background under the guise of opening a legitimate document.

The malware, compiled from Python using PyInstaller, enables cross-platform remote access and grants the attackers full control over compromised systems – from file-system enumeration and data exfiltration to real-time surveillance and continued persistence via systemd. This marks a strategic shift for APT36, historically focused on Windows-based attacks, underscoring a growing technical maturity and a deliberate move to compromise Linux-based environments widely used in government infrastructure.

<b>ATTACK TYPE</b>	Malware, Cyberespionage	<b>SECTOR</b>	Government
<b>REGION</b>	India	<b>APPLICATION</b>	Windows, Linux, LibreOffice, BOSS Linux OS

Source - <https://www.cyfirma.com/research/apt36-python-based-elf-malware-targeting-indian-government-entities/>

INTRODUCTION	APT36 DEPLOYS LINUX-BASED RAT TARGETING GOVERNMENT CRITICAL SYSTEMS	GOVERNMENT AND PRIVATE SECTORS UNDER SUSTAINED RANSOMWARE DDOS ASSAULT	SCATTERED LAPSUS DEPLOYS FAKE SSO PAGES TARGETING ZENDESK	ADVANCED KYBER RANSOMWARE DEPLOYS HYBRID ENCRYPTION TECHNIQUES	NEW CHICKENKILLER RANSOMWARE USES WMI FOR ENVIRONMENT VALIDATION	FSOCIETY AFFILIATE RAAS MODEL DRIVES SURGE IN GLOBAL ENTERPRISE ATTACKS	CLICKFIX STEALER DEPLOYS FAKE UPDATE SCREENS VIA CONCEALED PNG PAYLOADS	CLIPBOARD HIJACKING USED IN ELABORATE DPRK FAKE RECRUITMENT SITE ATTACK	WATER GAMAYUN DEPLOYS HIDDEN POWERSHELL CHAIN VIA MSC EXPLOIT	BLOODY WOLF APT USES FAKE MINISTRY EMAILS TO INSTALL SURVEILLANCE
--------------	---	--	---	--	--	---	---	---	---	---

# Hacktivists groups escalate ransomware and DDoS campaigns nationwide

Cyber intelligence teams observed a significant surge in hacktivist operations, with government portals and educational institutions targeted by sustained DDoS and website-defacement campaigns. Groups such as THE GARUDA EYE and HellR00ters claimed multiple incidents, using social channels to publicise taunts and operational details, amplifying political messages and causing service outages across highly connected public-facing systems. Organisations must prioritise rapid mitigation and continuity planning.

Concurrent ransomware activity increasingly targets private-sector firms, notably IT services and manufacturers, with families such as NightSpire, Sinobi, CLOP, BlackShrantac and The Gentlemen deploying double-extortion tactics and publishing victim lists. The advisory also highlights data breaches, illicit trade in unauthorised access and politically motivated alerts; organisations are urged to harden backups and accelerate incident response. Note: Our team has not independently validated all claims.

**Note: The CTI team has not independently validated all claims.**

<b>ATTACK TYPE</b>	Hacktivism, DDOS, Cyberespionage	<b>SECTOR</b>	Healthcare, Pharmaceuticals, Manufacturing, Government, Education, BFSI, Media, IT Services and Consulting, Telecommunications
<b>REGION</b>	India	<b>APPLICATION</b>	Generic

Source - CTI Team Internal Research

INTRODUCTION	APT36 DEPLOYS LINUX-BASED RAT TARGETING GOVERNMENT CRITICAL SYSTEMS	<b>GOVERNMENT AND PRIVATE SECTORS UNDER SUSTAINED RANSOMWARE DDOS ASSAULT</b>	SCATTERED LAPSUS DEPLOYS FAKE SSO PAGES TARGETING ZENDESK	ADVANCED KYBER RANSOMWARE DEPLOYS HYBRID ENCRYPTION TECHNIQUES	NEW CHICKENKILLER RANSOMWARE USES WMI FOR ENVIRONMENT VALIDATION	FSOCIETY AFFILIATE RAAS MODEL DRIVES SURGE IN GLOBAL ENTERPRISE ATTACKS	CLICKFIX STEALER DEPLOYS FAKE UPDATE SCREENS VIA CONCEALED PNG PAYLOADS	CLIPBOARD HIJACKING USED IN ELABORATE DPRK FAKE RECRUITMENT SITE ATTACK	WATER GAMAYUN DEPLOYS HIDDEN POWERSHELL CHAIN VIA MSC EXPLOIT	BLOODY WOLF APT USES FAKE MINISTRY EMAILS TO INSTALL SURVEILLANCE
--------------	---	---	---	--	--	---	---	---	---	---

# Scattered Lapsus\$ Hunters steal credentials via fake Zendesk help desks

Security researchers have disclosed that the threat group Scattered Lapsus\$ Hunters is launching a sophisticated phishing campaign targeting users of the Zendesk customer support platform. Over the past six months, more than 40 typosquatted and impersonating domains – such as “znedesk[.]com” and “vpn-zendesk[.]com” – have been created to mirror legitimate Zendesk login portals. Many of these domains host fake single sign-on (SSO) pages to harvest credentials.

In addition to external phishing sites, attackers have reportedly submitted fraudulent support tickets to genuine Zendesk portals used by organisations, posing as urgent IT or password-reset requests. These fake tickets may deliver remote-access Trojans (RATs) or other malware to help-desk staff – thereby enabling unauthorised access, potential lateral movement and exfiltration of sensitive internal or customer data.

<b>ATTACK TYPE</b>	Social engineering, Cyberespionage	<b>SECTOR</b>	Healthcare, Hospitality, Manufacturing, IT, Government, Business, BFSI, Airlines, Retailer and Distributor
<b>REGION</b>	Global	<b>APPLICATION</b>	Generic, Zendesk

Source - CERT-IN

# Emerging KYBER ransomware combines advanced encryption with data theft

A new global cyber-risk vector has emerged with alarming speed in the final months of 2025. According to a recent cyber report, KYBER ransomware – a strain targeting Windows systems, network shares, removable media and cloud environments – is rapidly evolving. KYBER encrypts files using AES-256-CTR with hybrid key generation via X25519 and Kyber1024, renames them using random extensions, and leaves a “ReadMeForDecrypt.txt” note.

Beyond simple file locking, KYBER operators claim large-scale data exfiltration and threaten leak-site exposure unless communications are initiated via Tor within a week. The malware exhibits advanced tactics such as persistence, WMI misuse, anti-analysis techniques and long-sleep evasion – evidence that ransomware groups are shifting toward structured, data-driven extortion models rather than mere encryption-based attacks.

<b>ATTACK TYPE</b>	Ransomware	<b>SECTOR</b>	Healthcare, Tourism, Manufacturing, IT, Government, Education, Energy, Defence Industry, Business, BFSI, Airlines
<b>REGION</b>	Global	<b>APPLICATION</b>	Windows

Source - <https://www.cyfirma.com/news/weekly-intelligence-report-31-october-2025/>

INTRODUCTION	APT36 DEPLOYS LINUX-BASED RAT TARGETING GOVERNMENT CRITICAL SYSTEMS	GOVERNMENT AND PRIVATE SECTORS UNDER SUSTAINED RANSOMWARE DDOS ASSAULT	SCATTERED LAPSUS DEPLOYS FAKE SSO PAGES TARGETING ZENDESK	<b>ADVANCED KYBER RANSOMWARE DEPLOYS HYBRID ENCRYPTION TECHNIQUES</b>	NEW CHICKENKILLER RANSOMWARE USES WMI FOR ENVIRONMENT VALIDATION	FSOCIETY AFFILIATE RAAS MODEL DRIVES SURGE IN GLOBAL ENTERPRISE ATTACKS	CLICKFIX STEALER DEPLOYS FAKE UPDATE SCREENS VIA CONCEALED PNG PAYLOADS	CLIPBOARD HIJACKING USED IN ELABORATE DPRK FAKE RECRUITMENT SITE ATTACK	WATER GAMAYUN DEPLOYS HIDDEN POWERSHELL CHAIN VIA MSC EXPLOIT	BLOODY WOLF APT USES FAKE MINISTRY EMAILS TO INSTALL SURVEILLANCE
--------------	---	--	---	---	--	---	---	---	---	---

# Coercive ChickenKiller variant emerges with automated encryption and evasion

As reported by threat analysts on 28 November 2025, a newly discovered Windows-focused ransomware strain named ChickenKiller has emerged from underground monitoring. Once executed, ChickenKiller encrypts user files and appends the “.locked” extension, drops a ransom note titled “RECOVERY\_INSTRUCTIONS.txt,” and deletes Windows Volume Shadow Copies – thereby disabling native file recovery mechanisms.

In addition, ChickenKiller employs stealth and evasion techniques such as WMI-based commands and anti-analysis checks – allowing it to examine whether it’s running in a sandbox or debug environment before triggering the payload. According to reports, the operators rely on coerced negotiation via live-chat or payment portals, underscoring the broader shift in financially motivated ransomware toward automation, rapid encryption, evasion and modular, adaptive toolsets.

<b>ATTACK TYPE</b>	Ransomware	<b>SECTOR</b>	Healthcare, Hospitality, Manufacturing, IT, Government, Education, Energy, Defence Industry, Business, BFSI, Aviation
<b>REGION</b>	Global	<b>APPLICATION</b>	Windows

Source - <https://www.cyfirma.com/news/weekly-intelligence-report-28-november-2025/>

# Modular FSociety ransomware operation expands through affiliate partnerships

FSociety – also operating as Flocker – is a 2024-born Ransomware-as-a-Service (RaaS) syndicate that arms affiliates with ready-built malware tools, including C2 infrastructure, RATs, stealers and DDoS modules. The group employs a double-extortion strategy: encrypting victim data while threatening disclosure of stolen information via Dark-Web leak sites.

In recent months, FSociety has expanded its reach by publicly allying with another emerging cybercrime cartel, enabling coordinated campaigns that increase both scale and impact. With more than forty victims spanning major U.S. sectors – including finance, retail, and technology – the group’s latest operations underscore a rising threat for corporate networks globally.

**ATTACK TYPE**

Ransomware

**SECTOR**

Financial services, IT, Government, Education, BFSI

**REGION**

Canada, India, Germany, United States

**APPLICATION**

Windows

Source - <https://socradar.io/dark-web-profile-fsociety-flocker-ransomware/>

INTRODUCTION

APT36 DEPLOYS LINUX-BASED RAT TARGETING GOVERNMENT CRITICAL SYSTEMS

GOVERNMENT AND PRIVATE SECTORS UNDER SUSTAINED RANSOMWARE DDoS ASSAULT

SCATTERED LAPSUS DEPLOYS FAKE SSO PAGES TARGETING ZENDESK

ADVANCED KYBER RANSOMWARE DEPLOYS HYBRID ENCRYPTION TECHNIQUES

NEW CHICKENKILLER RANSOMWARE USES WMI FOR ENVIRONMENT VALIDATION

FSOCIETY AFFILIATE RAAS MODEL DRIVES SURGE IN GLOBAL ENTERPRISE ATTACKS

CLICKFIX STEALER DEPLOYS FAKE UPDATE SCREENS VIA CONCEALED PNG PAYLOADS

CLIPBOARD HIJACKING USED IN ELABORATE DPRK FAKE RECRUITMENT SITE ATTACK

WATER GAMAYUN DEPLOYS HIDDEN POWERSHELL CHAIN VIA MSC EXPLOIT

BLOODY WOLF APT USES FAKE MINISTRY EMAILS TO INSTALL SURVEILLANCE

# Steganography enabled ClickFix malware in fake verification prompts campaign

Threat researchers have unveiled a sophisticated multi-stage campaign called ClickFix, which abuses social-engineering lures such as “Human Verification” or convincing fake Windows Update screens to trick users into running malicious commands. Once the user hits Win+R and pastes the command, the chain leverages legitimate Windows tools like mshta.exe and PowerShell to fetch a steganographic loader, which decodes malware concealed inside PNG pixel data directly into memory.

This campaign ultimately delivers potent info-stealing malware, including LummaC2 and Rhadamanthys, stealthily exfiltrating credentials and sensitive data. Its use of image-based steganography and in-memory execution helps bypass traditional signature-based defences – heightening risk to organisations reliant on standard antivirus or endpoint defences alone.

<b>ATTACK TYPE</b>	Malware	<b>SECTOR</b>	Healthcare, Financial services, Manufacturing, IT, Government, Transportation, Education, Energy, Retailer and Distributor, Telecommunications
<b>REGION</b>	Global	<b>APPLICATION</b>	Windows

Source - <https://www.huntress.com/blog/clickfix-malware-buried-in-images>

# DPRK job listing scam deploys malware through clipboard manipulation technique

As detailed by cyber researchers, a newly uncovered variant of the Contagious Interview operation has deployed a sophisticated fake job platform – hosted at lenvny[.]com – to target AI, crypto and software professionals. Built with React/Next.js, the site offers convincing UX: dynamically generated job listings, corporate branding and an “Integrated AI-Powered Interview Tool.” The platform uses social engineering via staged “video-introductions” to lure candidates into recording responses.

When applicants attempt to “fix” webcam issues, the site triggers a stealthy “ClickFix” clipboard-hijack that substitutes copied commands with a multi-stage infection chain: a ZIP file is downloaded, unpacked via PowerShell, and executed through a VBS loader. The result: deployment of malware capable of stealing credentials, crypto wallets and sensitive intellectual property, especially from high-value U.S.-based AI or crypto targets.

<b>ATTACK TYPE</b>	Cyberespionage	<b>SECTOR</b>	IT, Software Development
<b>REGION</b>	South Korea	<b>APPLICATION</b>	OneDrive, Windows, PowerShell, Next.js, React

Source - [https://www.validin.com/blog/inside\\_dprk\\_fake\\_job\\_platform/](https://www.validin.com/blog/inside_dprk_fake_job_platform/)

# Water Gamayun chains PowerShell stages through compromised MSC file

As detailed by recent research from threat hunting teams, the threat group Water Gamayun has executed a highly sophisticated campaign using a compromised legitimate site and a look-alike domain to distribute a double-extension RAR archive masquerading as a PDF. That archive exploits the critical Windows zero-day vulnerability CVE-2025-26633 – known as “MSC EvilTwin” – to inject malicious code into mmc.exe and launch hidden TaskPad-snap-in commands which trigger layered PowerShell stages.

The multi-stage chain proceeds with downloading UnRAR.exe, extracting strong password-protected archives, compiling a .NET window-hider, and executing ItunesC.exe loaders. Ultimately, this leads to contact with a dual-path command-and-control infrastructure and deployment of backdoors or stealers – potentially including known Water Gamayun payloads such as SilentPrism or DarkWisp – enabling persistent access, credential theft and possible data exfiltration.

<b>ATTACK TYPE</b>	Vulnerability, Malware, Cyberespionage	<b>SECTOR</b>	Government
<b>REGION</b>	Global	<b>APPLICATION</b>	Windows, PowerShell

Source - <https://www.zscaler.com/blogs/security-research/water-gamayun-apt-attack>

# Bloody Wolf leverages official impersonation for targeted RAT deployment

Since late 2023, the advanced persistent threat group Bloody Wolf has carried out a series of regionally targeted spear-phishing assaults across Central Asia, primarily in Kyrgyzstan and now Uzbekistan. The group impersonates Ministries of Justice using forged PDF attachments and spoofed domains to trick recipients into installing Java Runtime so they can execute small Java Archive (JAR) loaders. Once run, these JAR files – built with Java 8 via a custom generator – quietly fetch and deploy a legacy version of NetSupport RAT, creating persistence through Startup .bat scripts, HKCU Run-key entries, scheduled tasks, and fake error dialogues to disguise the infection.

Recent findings show that the campaign, active since mid-2025 in Kyrgyzstan, had expanded to Uzbekistan by October 2025, with the same infection approach and infrastructure. This pattern underscores Bloody Wolf’s shift towards streamlined, low-cost yet sophisticated attacks – blending social engineering, legitimate remote-access tools and custom loaders – emphasising how even simple, widely available tools can yield high-impact, persistent threats.

<b>ATTACK TYPE</b>	Malware, Cyberespionage	<b>SECTOR</b>	Healthcare, Government, Education
<b>REGION</b>	Kazakhstan, Kyrgyzstan, Uzbekistan	<b>APPLICATION</b>	Windows

Source - <https://www.group-ib.com/blog/bloody-wolf/>

INTRODUCTION	APT36 DEPLOYS LINUX-BASED RAT TARGETING GOVERNMENT CRITICAL SYSTEMS	GOVERNMENT AND PRIVATE SECTORS UNDER SUSTAINED RANSOMWARE DDOS ASSAULT	SCATTERED LAPSUS DEPLOYS FAKE SSO PAGES TARGETING ZENDESK	ADVANCED KYBER RANSOMWARE DEPLOYS HYBRID ENCRYPTION TECHNIQUES	NEW CHICKENKILLER RANSOMWARE USES WMI FOR ENVIRONMENT VALIDATION	FSOCIETY AFFILIATE RAAS MODEL DRIVES SURGE IN GLOBAL ENTERPRISE ATTACKS	CLICKFIX STEALER DEPLOYS FAKE UPDATE SCREENS VIA CONCEALED PNG PAYLOADS	CLIPBOARD HIJACKING USED IN ELABORATE DPRK FAKE RECRUITMENT SITE ATTACK	WATER GAMAYUN DEPLOYS HIDDEN POWERSHELL CHAIN VIA MSC EXPLOIT	BLOODY WOLF APT USES FAKE MINISTRY EMAILS TO INSTALL SURVEILLANCE
--------------	---	--	---	--	--	---	---	---	---	---

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.