

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 20, 2026



THREAT INTELLIGENCE ADVISORY REPORT

As October 2026 advances, the cyber threat landscape remains as formidable as ever, with threat actors mounting increasingly sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Traditional defence models are straining to keep pace as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now depends on organisations reinforcing foundational security controls, adopting layered defence strategies, and embedding forward-looking intelligence throughout their operational frameworks.

In this rapidly shifting environment, the Tata Communications Cyber Threat Intelligence report remains an indispensable resource for security practitioners. Published weekly, it delivers sharp, timely analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By turning intelligence into practical defence guidance, it equips security teams to anticipate, counter, and contain threats with confidence — preserving the continuity of critical operations at scale.

Warlock group disables defences and spreads across networks via SharePoint entry points

Researchers have reported that Warlock ransomware, operated by the China-nexus group it tracks as Longlegs (also known as Storm-2603), continues to exploit unpatched on-premises Microsoft SharePoint Server deployments for initial access. Over the past two months, the group has compromised at least four Portuguese- and Spanish-speaking organisations across Europe, Africa, and Latin America, including water, telecommunications, government, and education entities.

Once inside, the attackers deployed web shells, DLL sideloading, and Visual Studio Code tunnels to establish covert remote access. A signed but vulnerable driver disabled security software on at least 40 hosts within roughly two hours, before Warlock was staged in the domain SYSVOL share and replicated to at least 33 systems. Organisations must patch SharePoint and enforce driver blocklists.

ATTACK TYPE	Ransomware	SECTOR	Government, Education, Energy, Telecommunications
REGION	Europe, Africa, Latin America	APPLICATION	Microsoft Active Directory Services, Microsoft SharePoint Server, Windows, PowerShell

Source - <https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>

PAYLOAD weaponise Active Directory GPOs to disrupt entire network without encryption

A global emergency response team has detailed an April 2026 intrusion in which attackers compromised a Middle Eastern manufacturer through its FortiGate SSL VPN using stolen domain credentials. After obtaining domain-administrator privileges, they created a malicious Group Policy Object named PAYLOAD and linked it at the domain root, allowing it to reach every domain-joined Windows machine across the organisation.

Rather than encrypting files, the GPO distributed ransom notes, replaced desktop wallpapers, and lock screens, disabled local Administrator accounts and, via a second policy, switched off Windows Firewall. Data was exfiltrated and later published on the dark web, while a separate PAYLOAD sample targeting ESXi was found on Linux servers. Organisations should restrict GPO creation and enforce phishing-resistant MFA.

ATTACK TYPE	Ransomware, Breaches, Misconfiguration	SECTOR	Manufacturing
REGION	Middle East	APPLICATION	Microsoft Active Directory Services, VMware ESXi, Windows, Fortinet FortiGate SSL VPN

Source - <https://securelist.com/tr/payload-ransomware-via-group-policy/121335/>

UAT-11587 targets Asian governments with Antino backdoor hidden inside Microsoft 365

Cisco Talos has uncovered UAT-11587, a China-nexus activity cluster targeting government, defence, policy, academic, and civil-society organisations across Asia. Active since September 2025, the actor relies on highly targeted spear-phishing emails and tailored decoy documents to initiate a multi-stage infection chain. This culminates in a signed Microsoft binary sideloads Antino, a previously undocumented, Rust-compiled Windows backdoor.

Antino supports reconnaissance, command execution, persistence, file transfer, and in-memory shellcode loading. Its command-and-control channel operates entirely through Microsoft 365, using the Microsoft Graph API to treat Outlook and OneDrive as dead-drops, so malicious traffic blends with legitimate enterprise activity. Talos observed roughly 350 compromised endpoints across eight countries. Organisations should strengthen email filtering and monitor anomalous Microsoft 365 usage.

ATTACK TYPE	Phishing, Malware, Cyberespionage, APT	SECTOR	Government, Education, Military, Defence Industry
REGION	India, Cambodia, Myanmar (Burma), Pakistan, Philippines, Syria, Taiwan, Thailand	APPLICATION	Microsoft Outlook, Windows, Microsoft Office 365, Microsoft OneDrive, PowerShell, Microsoft Graph, Gmail

Source - <https://blog.talosintelligence.com/china-nexus-uat-11587-targets-government-and-policy-organizations-across-asia-with-antino-backdoor/>

BPFDoor and AVERAT target network-edge infrastructure via Covert SMTP communications

Researchers have identified a cluster of Linux malware targeting telecommunications and network-edge environments across South Korea and Taiwan, including mail-security appliances and embedded devices such as CCTV and DVR systems. The set comprises new BPFDoor variants, a BPF-enabled Rekoobe build, a ShareTech-focused dropper, and the previously unreported AVERAT implant, observed across six distinct builds.

To evade detection, the malware impersonates legitimate products such as SpamSniper, employing process masquerading, and fileless, unlinked execution to blend into normal appliance activity. BPFDoor and the Rekoobe build passively monitor traffic for attacker-controlled magic packets, while AVERAT beacons over TCP port 25 to disguise command-and-control as ordinary email. Defenders should hunt for unlinked processes and anomalous outbound mail traffic.

ATTACK TYPE	Malware	SECTOR	Telecommunications
REGION	South Korea, Taiwan	APPLICATION	Linux

Source - <https://securityonline.info/bpfdoor-averat/>

New CastleStealer evolves with browser credential protection bypass and RCE capabilities

First publicly identified in April 2026, CastleStealer is a C#-based information stealer targeting Windows systems. Analysis by Flashpoint shows its latest samples have matured considerably, most notably gaining the ability to bypass Chromium's App-Bound Encryption. By abusing Chrome's IElevator COM interface, the malware can now access browser login data, cookies, history, and extension information that were previously beyond reach.

Beyond data theft, newer variants let operators execute supplied shell commands, run a dropped file, and download and execute further payloads from a URL, broadening the malware into a wider post-compromise threat. Rather than one large archive, it exfiltrates data through small AES-encrypted raw TCP exchanges. Organisations should monitor for unusual processes abusing browser elevation services and reinforce endpoint defences.

ATTACK TYPE	Information Gathering, Malware	SECTOR	IT, Healthcare, Government, Transportation, Military, ONGC, Energy, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	APPLICATION	Microsoft Edge, Chromium, Mozilla Firefox, Opera Browser, Google Chrome, Telegram, Discord

Source - <https://gbhackers.com/castlestealer-malware/>

INTRODUCTION

WARLOCK RANSOMWARE
EXPLOITS SHAREPOINT
FLAWS TO TARGET
CRITICAL
INFRASTRUCTURES

PAYLOAD RANSOMWARE
ABUSES ACTIVE
DIRECTORY GPOS FOR
DOMAIN-WIDE
DISRUPTION

CHINA-LINKED ANTINO
BACKDOOR ABUSES
OUTLOOK AND ONEDRIVE
TO SPY ON GOVERNMENT

COVERT LINUX
BACKDOORS MIMIC
LEGITIMATE APPLIANCES
AND HIDE INSIDE MAIL
PORT TRAFFIC

CASTLESTEALER
UPGRADES BYPASS
BROWSER ENCRYPTION
AND RUN REMOTE
COMMANDS

TWO CRITICAL
NETSCALER ZERO-DAYS
EXPLOITED IN THE WILD
PROMPT URGENT CITRIX
PATCHING

ATTACKERS RELAY
CREDENTIALS AND MFA
IN REAL TIME TO STEAL
AUTHENTICATED
SESSIONS

NAILONG PHISHING
SERVICE USES FAKE
SOCIAL MEDIA LURES TO
STEAL CARDS AND
BYPASS MFA

FBI WARN FORTIBLEED
ATTACKERS ARE
HIJACKING AND LOCKING
FORTINET FIREWALLS

MEMORY OVERFLOW
FLAW IN CITRIX
NETSCALER ENABLES
REMOTE CODE
EXECUTION OR
OUTAGES

NetScaler ADC and gateway at risk from actively exploited unauthenticated RCE flaw

Citrix has released security updates addressing eight vulnerabilities in NetScaler ADC and NetScaler Gateway, disclosed on 27 September 2026. CISA has added two critical flaws, CVE-2026-88771 and CVE-2026-88772 (both CVSS 9.5), to its Known Exploited Vulnerabilities catalogue following confirmed active exploitation. CVE-2026-88771 is especially dangerous, enabling unauthenticated remote code execution against appliances running affected builds in their default configuration.

The remaining issues include memory overflow, HTTP request smuggling, feature-policy bypass, denial of service, and TCP initial sequence number prediction, several of which require non-default configurations such as DTLS. CISA reports that threat actors are exploiting the two critical flaws globally. Organisations are urged to upgrade every affected appliance immediately and review Citrix’s guidance for signs of prior compromise.

ATTACK TYPE	Vulnerability	SECTOR	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications, Software Development
REGION	Global	APPLICATION	Citrix NetScaler

Source - <https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>

UAT-11985 targets Taiwan researchers via AI-assisted phishing and Google AitM Attacks

Cisco Talos has disclosed UAT-11985, a spear-phishing campaign observed in mid-2026 targeting individuals affiliated with Taiwan-based research organisations. The operators impersonated legitimate institutions, including the Taiwan European Union Centre, using convincing event invitations whose near-identical structure suggests AI-assisted authorship. Alongside deceptive registration links disguised as Google Forms, the attackers copied genuine event posters and swapped in malicious QR codes.

Victims were directed to counterfeit Google sign-in pages backed by an operator-driven adversary-in-the-middle framework. Using HTTP requests and a persistent WebSocket connection, the kit relayed credentials and multi-factor authentication challenges to the genuine service in real time, enabling theft of authenticated sessions and full account takeover. Organisations should adopt phishing-resistant authentication, scrutinise QR codes and monitor accounts for anomalous activity.

ATTACK TYPE	Social Engineering, Phishing, APT	SECTOR	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications, Software Development
REGION	Taiwan	APPLICATION	Google, Google Forms

Source - <https://blog.talosintelligence.com/uat-11985/>

Milk Dragon phishing kit uses social media discounts to steal payment card and MFA data

Researchers have detailed Milk Dragon, also tracked as NaiLong, a Phishing-as-a-Service kit active since October 2025 and sold through Telegram communities. Rather than relying on fear or urgency, it lures victims with heavily discounted products advertised on Facebook and TikTok. Impersonating trusted brands, the operation has spawned 258 phishing pages affecting shoppers across 66 countries worldwide.

Built on WordPress and WooCommerce, the kit uses a malicious plugin called BytePress to inject fake payment options and capture card details, personal data and MFA codes in real time. Through Adversary-in-the-Middle techniques, operators relay one-time passwords to defeat authentication, then display counterfeit order confirmations to delay detection. Shoppers should verify retailers independently and avoid discount links from social media.

ATTACK TYPE	Cybercrime, Phishing	SECTOR	BFSI, E-Commerce, FnB Service, Retail and Distribution
REGION	Global	APPLICATION	WordPress, Telegram, Facebook

Source - <https://cybersecuritynews.com/milk-dragon-aitm-kit/>

Ongoing FortiBleed campaign locks out firewall admins and fuels ransomware intrusions

The FBI and U.S. Secret Service have issued a joint advisory warning that FortiBleed, a global credential-compromise campaign targeting internet-facing Fortinet FortiGate firewalls and SSL VPN gateways, remains active. Attackers are using stolen credentials to gain administrative access, then deleting or changing legitimate accounts to lock organisations out of their own devices while retaining control and pivoting into internal networks.

Rather than exploiting a new flaw, the operators rely on credential stuffing and password spraying, drawing on earlier Fortinet leaks and infostealer logs, with weak legacy password hashing easing offline cracking. Compromised devices are then sold on as entry points for ransomware affiliates. Organisations should reset all credentials, strengthen access controls, hunt for rogue accounts and monitor for unauthorised activity.

ATTACK TYPE	Vulnerability, Breaches	SECTOR	Healthcare, Hospitality, Construction, IT, Government, E-Commerce, BFSI, Airlines, Automobile, Broadcast Media Production, Mining, Retail and Distribution, Telecommunication, Logistics
REGION	Global	APPLICATION	Fortinet FortiClient SSL VPN, Fortinet FortiGate, Fortinet VPN, Fortinet, FortiClient, FortiOS

Source - FortiBleed Operations Continue Targeting Exposed Systems Leading to Reports of Lockouts

INTRODUCTION

WARLOCK RANSOMWARE
EXPLOITS SHAREPOINT
FLAWS TO TARGET
CRITICAL
INFRASTRUCTURES

PAYLOAD RANSOMWARE
ABUSES ACTIVE
DIRECTORY GPOS FOR
DOMAIN-WIDE
DISRUPTION

CHINA-LINKED ANTINO
BACKDOOR ABUSES
OUTLOOK AND ONEDRIVE
TO SPY ON GOVERNMENT

COVERT LINUX
BACKDOORS MIMIC
LEGITIMATE APPLIANCES
AND HIDE INSIDE MAIL
PORT TRAFFIC

CASTLESTEALER
UPGRADES BYPASS
BROWSER ENCRYPTION
AND RUN REMOTE
COMMANDS

TWO CRITICAL
NETSCALER ZERO-DAYS
EXPLOITED IN THE WILD
PROMPT URGENT CITRIX
PATCHING

ATTACKERS RELAY
CREDENTIALS AND MFA
IN REAL TIME TO STEAL
AUTHENTICATED
SESSIONS

NAILONG PHISHING
SERVICE USES FAKE
SOCIAL MEDIA LURES TO
STEAL CARDS AND
BYPASS MFA

FBI WARN FORTIBLEED
ATTACKERS ARE
HIJACKING AND LOCKING
FORTINET FIREWALLS

MEMORY OVERFLOW
FLAW IN CITRIX
NETSCALER ENABLES
REMOTE CODE
EXECUTION OR
OUTAGES

Citrix urges urgent patching of critical NetScaler flaw affecting SAML-configured appliances

Citrix has disclosed a critical memory overflow vulnerability, CVE-2026-107406 (CVSS v4.0: 9.5), affecting NetScaler ADC and NetScaler Gateway appliances. Addressed in security bulletin CTX697191 on 8 October 2026, the flaw stems from improper restriction of operations within a memory buffer (CWE-119). An unauthenticated remote attacker could exploit it to achieve remote code execution or trigger denial-of-service conditions.

Exploitation is possible only when the appliance is configured as a SAML Service Provider or Identity Provider, with exposure varying by software version. While the attack requires no privileges or user interaction, it carries high complexity, and Citrix reports no known exploitation in the wild. Administrators should verify their SAML configuration and upgrade to a fixed release immediately.

ATTACK TYPE	Vulnerability	SECTOR	IT, Healthcare, Construction, IT, Government, Transportation, Military, ONGC, BFSI, Real Estate, Aviation, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	APPLICATION	Citrix NetScaler

Source - [FortiBleed Operations Continue Targeting Exposed Systems Leading to Reports of Lockouts](#)

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.