TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 7, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today's dynamic cybersecurity landscape, protecting critical systems and data is essential for individuals, businesses, and governments. Cyber threats can lead to financial losses, reputational damage, and operational disruptions.

Our weekly Cyber Threat Intelligence (CTI) report provides actionable insights into emerging threats worldwide, empowering organisations with proactive strategies to mitigate risks. Supported by expert advisory services, this intelligence-driven approach enhances security measures, addresses persistent vulnerabilities, and builds resilience against evolving challenges. Equip your organisation with the knowledge and tools needed to navigate the complexities of cybersecurity and ensure a robust, secure future.

New RedEyes malware campaign targets South Korea

Researchers have identified a new cyberattack campaign by RedEyes (APT37), a North Korea-linked group, targeting South Korean entities. The campaign employs a sophisticated malware called ROKRAT, delivered via malicious Hangul (HWP) documents exploiting CVE-2017-8291. This malware enables data theft and surveillance, compromising government and corporate systems.

The attackers leverage decoy documents and sophisticated evasion techniques to remain undetected. ASEC advises implementing robust endpoint protection, regular patch updates, and heightened vigilance against phishing attacks to mitigate these risks effectively.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	South Korea	**APPLICATION**	Windows

Source - https://asec.ahnlab.com/ko/85270/

Threat actors exploit brand collaborations to hack YouTube channels

Cybercriminals are leveraging fake brand collaborations to target popular YouTube channels. Posing as legitimate companies, attackers lure creators with enticing sponsorship deals, often using emails with malicious links or files. These payloads include password-stealing malware like Vidar or RedLine, granting hackers access to accounts. Once compromised, attackers rebrand the channel, promote scams such as fake cryptocurrency schemes, and exploit the creator's reputation to deceive subscribers. Researchers have highlighted that this tactic undermines trust between creators and their audience while leading to financial and reputational losses.

Creators are urged to verify collaboration offers, avoid clicking unsolicited links, and enable multi-factor authentication. These proactive measures are crucial to safeguarding digital assets and preserving audience trust in an increasingly targeted digital landscape.

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

Source - https://www.cloudsek.com/blog/how-threat-actors-exploit-brand-collaborations-to-target-popular-youtube-channels

WoolTea backdoor exploits Palo Alto devices

Cybersecurity researchers have uncovered active exploitation of CVE-2024-9474, a critical vulnerability affecting Palo Alto Networks devices. Threat actors are deploying the LittleLamb WoolTea backdoor to infiltrate networks, granting remote access and control over compromised systems. The backdoor exploits unpatched vulnerabilities, emphasising the need for immediate remediation. The WoolTea malware uses advanced evasion techniques, including encryption and obfuscation, to avoid detection. It allows attackers to execute arbitrary commands, exfiltrate sensitive data, and maintain persistence in victim environments.

Palo Alto Networks has issued advisories, urging users to apply the latest patches and implement additional security measures. Experts recommend enhanced monitoring, threat hunting, and strong access controls to mitigate potential impacts. This discovery highlights the growing sophistication of cyberattacks targeting enterprise hardware and the critical importance of timely vulnerability management.

ATTACK TYPE	Vulnerability, malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Palo Alto Networks

Source - https://securityonline.info/cve-2024-9474-exploited-littlelamb-wooltea-backdoor-discovered-in-palo-alto-devices/

PowerSCP Stealer malware threatens Windows systems

Cybersecurity experts have identified a sophisticated PowerShell-based malware dubbed PowerSCP Stealer, targeting Windows systems with a focus on credential theft and data exfiltration. Utilising the Secure Copy Protocol (SCP), the malware operates stealthily to validate user credentials and exfiltrate sensitive data to remote command-and-control (C2) servers. PowerSCP Stealer spreads primarily through spear-phishing campaigns, where victims are lured into interacting with malicious email attachments or links. Once activated, the malware employs deceptive password prompts to capture credentials, enabling attackers to execute further cyberattacks. Its advanced communication with C2 servers allows remote operators to maintain persistence and escalate their access within compromised systems.

This threat poses significant risks, including system compromise, data breaches, and potential operational disruption. To counteract its impact, cybersecurity experts recommend robust mitigation strategies, including enhanced user education, deployment of multi-factor authentication (MFA), advanced endpoint protection, and vigilant network monitoring to detect anomalous activities early.

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

Source - CERT-In

LockBit ransomware group makes a powerful comeback

The notorious LockBit ransomware group has resurfaced following Operation Cronos, which temporarily crippled its operations. Despite suffering significant setbacks, including the exposure of internal files, LockBit has rapidly regained momentum, relaunching its data leak site and targeting over 200 victims globally. The group now operates via advanced encryption techniques and decentralised file sharing using torrent technology, making it harder for law enforcement to track.

Recent victims include major companies such as Polycab and Crinetics, with ransom demands escalating. As the group adapts and evolves, experts warn of a renewed wave of cyberattacks targeting critical infrastructure and corporations worldwide.

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

Source - https://theravenfile.com/2024/06/26/the-return-of-lockbit/

Critical vulnerability in Apache NiFi exposing sensitive data

A newly discovered vulnerability (CVE-2024-56512) in Apache NiFi – a widely used data processing tool – exposes sensitive data to unauthorised access. This flaw affects NiFi versions 1.10.0 to 2.0.0 and arises from inadequate authorisation checks when creating Process Groups. Exploiting this issue, attackers can access non-sensitive parameters and bypass access controls, potentially leading to data breaches and compromising critical systems.

Apache NiFi is crucial for industries like finance, healthcare, and government. The issue has been addressed in NiFi version 2.1.0, and users are urged to upgrade immediately to mitigate risks. The vulnerability underscores the importance of robust authorisation systems to secure data processing workflows.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - https://securityonline.info/cve-2024-56512-apache-nifi-vulnerability-exposes-sensitive-data-to-unauthorized-users/

Botnets target D-Link devices via aging vulnerabilities

Botnets continue to exploit long-standing vulnerabilities in D-Link devices, despite the weaknesses being publicly known and patched years ago. Attackers are using these flaws, especially those related to the Home Network Administration Protocol (HNAP), to deploy Mirai and Kaiten botnets, known as FICORA and CAPSAICIN. These botnets spread through remote command execution vulnerabilities, giving cybercriminals control over affected devices, which can be repurposed for DDoS attacks or further exploitation.

FortiGuard Labs discovered these attacks were particularly active in October and November 2024. Despite the age of the vulnerabilities, their exploitation remains widespread, emphasising the need for enterprises to update devices regularly and monitor systems for malicious activity.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	D-Link

Source - https://www.fortinet.com/blog/threat-research/botnets-continue-to-target-aging-d-link-vulnerabilities

Exploitation of intricate flaw threatens industrial routers

A critical vulnerability (CVE-2024-12856) has been discovered in Four-Faith industrial routers, allowing attackers to execute remote commands and gain control of vulnerable devices. The flaw, linked to improper time modification functionality, affects Four-Faith F3x24 and F3x36 routers. Around 15,000 internet-facing devices are exposed to this risk.

This exploitation is ongoing, with attackers leveraging default credentials to initiate command injections. Researchers have released detection rules to counter the threat. Users are advised to update firmware and change default passwords immediately to prevent potential data breaches.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic, Four-Faith industrial routers

Source - https://securityonline.info/four-faith-industrial-routers-under-attack-cve-2024-12856-exploited-in-the-wild/

Critical SQL injection vulnerability discovered in Apache Traffic Control

A severe SQL injection vulnerability, CVE-2024-45387, has been identified in Apache Traffic Control, a widely used content delivery network (CDN) management tool. The flaw, found in versions 8.0.0 to 8.0.1, allows privileged users to execute arbitrary SQL commands by sending specially crafted PUT requests. Exploiting this vulnerability could compromise sensitive database content, leading to data breaches or system integrity issues.

With a CVSS score of 9.9, this flaw poses a significant risk to organisations. A proof-of-concept exploit has been published, increasing the urgency for affected users to upgrade to the patched version (8.0.2) to mitigate potential attacks.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Apache Traffic Control

Source - https://securityonline.info/cve-2024-45387-poc-published-for-critical-sql-injection-in-apache-traffic-control/

Cyber Anarchy Squad targets Russian organisations with rare trojans

A new threat actor group, Cyber Anarchy Squad (CAS), has been identified launching sophisticated attacks against Russian organisations using uncommon trojans. These trojans, which include versions of remote access tools (RATs), are being deployed via spear-phishing emails. The malware is designed to infiltrate critical networks, giving attackers the ability to execute arbitrary commands, steal sensitive data, and maintain long-term access. This group's tactics, which are less frequently seen in cybercriminal activity, focus on leveraging these rare trojans to bypass conventional cybersecurity defences.

Researchers warn that while the tools may be unfamiliar, their impact can be devastating, potentially leading to severe disruptions in targeted industries. The CAS' growing presence signals an escalation in cyberwarfare, highlighting the increasing sophistication of state-sponsored and hacktivist groups operating in the cyber domain.

ATTACK TYPE	Hacktivism	**SECTOR**	All
REGION	Russia, Belarus	**APPLICATION**	Windows

Source - https://securelist.com/cyber-anarchy-squad-attacks-with-uncommon-trojans/114990/

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