TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 8, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

Cyberattacks are becoming more frequent and sophisticated, with threat actors constantly seeking out and exploiting vulnerabilities. The damage is being felt across individuals, businesses, and governments alike, with impacts ranging from data breaches and operational disruptions to financial and reputation losses.

The only way to stay ahead of these evolving threats is by leveraging timely, reliable insights. Our weekly Threat Intelligence Advisory keeps you updated on the latest developments in malware, ransomware, and other cyber risks. By subscribing, you gain actionable intelligence to help strengthen your digital defences and respond with confidence.

Trojanised ScreenConnect Installers: Malware hidden in trusted software

A new cyber campaign is exploiting trojanised, signed ConnectWise ScreenConnect installers to deliver malware using Authenticode stuffing. This method embeds malicious code without breaking the file's digital signature and allows the installers to evade most antivirus detection, making the campaign highly deceptive and effective. Victims are lured through phishing emails, malicious ads or fake update prompts. Once deployed, the malware establishes silent remote access that enables lateral movement and potential data theft; often under the guise of legitimate support activity.

The threat highlights the need for multi-layered endpoint protection, application allowlisting and routine integrity checks for remote access tools. Security teams must monitor remote access activity, restrict admin privileges for such tools and conduct regular audits of signed binaries to catch hidden threats early. Organisations should also train staff to recognise phishing attempts and verify the legitimacy of software updates.

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

Source - https://securityonline.info/connectwise-screenconnect-targeted-by-nation-state-actor/

INTRODUCTION | **TROJANISED SCREENCONNECT INSTALLERS EVADE ANTIVIRUS DETECTION** | SPYMAX RAT DISGUISED AS WEDDING INVITE HITS ANDROID USERS | WINOS AND HOLDINGHANDS MALWARE TARGET TAIWANESE GOVERNMENT | TAG-140 DEPLOYS DRAT V2 IN INDIAN CYBERESPIONAGE CAMPAIGN | DIRE WOLF RANSOMWARE STRIKES GLOBAL MANUFACTURING AND IT FIRMS | WOGRAT CAMPAIGN TARGETS SERVERS VIA MULTI-STAGE INTRUSION | ONECLIK MALWARE ABUSES CLICKONCE TO BREACH ENERGY SECTOR | ODYSSEY STEALER HITS MACOS USERS VIA FAKE CAPTCHA PROMPTS | AFRICAN BANKS HIT BY STEALTHY CL-CRI-1014 CAMPAIGN | SILVER FOX CAMPAIGN DROPS RAT AND ROOTKIT ON CHINESE SYSTEMS

TATA COMMUNICATIONS

SpyMax RAT via WhatsApp: Android users lured by fake wedding invites

A targeted spyware campaign is actively targeting Android users in India with WhatsApp messages containing a malicious APK disguised as a “Wedding Invitation”. The app deploys SpyMax RAT - a powerful remote access trojan - on installed devices that establishes a connection with a remote server and begins exfiltrating sensitive data in compressed form to reduce detection risk. The malware can intercept SMS messages, capture OTPs, steal banking credentials and monitor real-time activity. It then uses social engineering tactics, fake system prompts and anti-analysis techniques to avoid detection.

This campaign highlights the growing threat of mobile spyware delivered through trusted messaging platforms. Applying regular updates, using verified app sources and endpoint protection tools for Android can help mitigate the risk of RAT-based surveillance and data theft. Android users should avoid sideloading apps, especially those received through social messaging channels. Moreover, security-conscious organisations must enforce mobile device management (MDM) policies and promote awareness around mobile phishing threats.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	India	**APPLICATION**	Android

Source - https://labs.k7computing.com/index.php/spymax-a-fake-wedding-invitation-app-targeting-indian-mobile-users/

TATA COMMUNICATIONS

Taiwan targeted by advanced malware campaign using WinOS and HoldingHands RAT

A coordinated threat campaign is actively targeting Taiwanese government entities using a series of sophisticated malware strains. These include WinOS 4.0 and the HoldingHands remote access trojan linked to the Gh0stBins variant. The initial attacks began in early 2025 with phishing emails impersonating the National Taxation Bureau, delivering malicious ZIP attachments. Follow-up campaigns in March used similar tactics, leading to further infections and expanded payload delivery. These attacks employ advanced tactics such as DLL side-loading, anti-VM evasion, privilege escalation and complex C2 communications for dynamic data harvesting and modular malware deployment.

The operation's layered design and targeted impersonation suggest a persistent threat actor with access to well-developed toolsets. Government agencies and public-sector organisations in the region must strengthen email filtering, enforce endpoint monitoring and adopt network segmentation to limit lateral spread. Also, regular security assessments and employee awareness training remain essential to detect and contain such stealthy, multi-stage campaigns.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	Taiwan	**APPLICATION**	Windows

Source - https://www.fortinet.com/blog/threat-research/threat-group-targets-companies-in-taiwan

TATA COMMUNICATIONS

DRAT V2 deployed by TAG-140: Indian government in crosshairs of cyberespionage campaign

An evolving cyberespionage campaign, TAG-140, is actively targeting the Indian government, defence, and energy sectors. The campaign is linked to the SideCopy/Transparent Tribe APT group. DRAT V2, a Delphi-compiled remote access trojan engineered for post-exploitation control, remote command execution, and obfuscated C2 communication, lies at the core of its operations. The malware tricks victims into downloading compromised payloads and is distributed via spoofed Indian Ministry of Defence web portals and ClickFix-themed social engineering. DRAT V2's cross-platform compatibility across Windows, macOS and Linux and stealth mechanisms allow attackers to exfiltrate sensitive data while maintaining persistent access.

The campaign demonstrates increasing delivery and execution sophistication. Affected sectors must prioritise threat intelligence monitoring, adopt zero-trust access models and ensure endpoint detection tools can recognise Delphi-compiled binaries. Additionally, security teams should reinforce defences with phishing awareness training and regularly audit systems for unauthorised access or data movement.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Government, Oil and Gas, Defence Industry
REGION	India	**APPLICATION**	Apple macOS, Windows, Linux

Source - https://www.recordedfuture.com/research/drat-v2-updated-drat-emerges-tag-140s-arsenal

Dire Wolf ransomware: Global sectors hit with double extortion tactics

Since its emergence in May 2025, the Dire Wolf ransomware group has rapidly targeted manufacturing and IT sectors across India, Taiwan, and the U.S. The group uses double extortion to encrypt files and threatens to leak stolen data unless ransoms (up to $500 million) are paid. The ransomware is built on a Golang-based binary packed with UPX and the group leverages Curve25519 and ChaCha20 for strong encryption. It is capable of disabling logs, halting services, deleting backups and compromising recovery.

So far, researchers have identified 16 victims across 11 countries, with many listed on the group's public leak site. This highlights its focus on financial gain and tailored targeting. To combat this threat, organisations must implement offline backups, improve their incident response readiness and strengthen email and endpoint security to contain this and any future ransomware intrusions.

ATTACK TYPE	Ransomware	**SECTOR**	Manufacturing, IT
REGION	India, Taiwan, United States	**APPLICATION**	Windows

Source - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/dire-wolf-strikes-new-ransomware-group-targeting-global-sectors/

WogRAT campaign targets web servers using a multi-stage infection chain

A recent multi-platform attack campaign is targeting Windows IIS and Linux web servers. The attackers are using the WogRAT malware family, along with tools like MeshAgent, SuperShell and Ladon for privilege escalation and lateral movement. Web vulnerabilities are exploited to deploy persistent web shells, steal credentials and maintain stealth access. The persistent reuse of infrastructure and open-source tooling links it to previous WogRAT activity and suggests a sustained threat actor behind it.

Defending against such attacks requires an elevated approach towards enterprise security. Organisations must patch known vulnerabilities, monitor server logs for anomalies and limit administrative access to critical infrastructure to ensure the safety and continuity of

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

Source - https://asec.ahnlab.com/en/88627/

OneClik malware campaign targets the energy sector via Microsoft ClickOnce

A new APT campaign using the OneClik malware is targeting the energy and oil & gas sectors in the Middle East. The malware is delivered through phishing and Microsoft ClickOnce abuse, and once installed, it deploys .NET-based loaders and a Golang backdoor (RunnerBeacon) via AppDomainManager hijacking. It also communicates with AWS-based C2 infrastructure to blend in with legitimate traffic and features sandbox evasion, anti-analysis and modular architecture.

Cybersecurity experts researching OneClik suggest potential links to Chinese state-sponsored actors. Organisations are advised to enhance cloud traffic inspection, restrict ClickOnce usage and conduct regular behavioural analysis of endpoint activity.

ATTACK TYPE	Malware	**SECTOR**	Oil and Gas, Energy
REGION	Middle East	**APPLICATION**	Windows

Source - https://www.trellix.com/blogs/research/oneclik-a-clickonce-based-apt-campaign-targeting-energy-oil-and-gas-infrastructure/

Odyssey Stealer: macOS malware hijacks credentials and crypto assets

A sophisticated new macOS threat named the Odyssey Stealer is exploiting typosquatted domains and fake CAPTCHA prompts (ClickFix tactic) to trick users into executing malicious AppleScripts. The Odyssey Stealer is linked to a rebranded version of Poseidon Stealer and features a full-featured command-and-control panel and is reported to steal browser logins, crypto wallets, Keychain data and personal files.

The malware is also known to avoid CIS regions, signifying its links to Russian-speaking threat actors. Its focus on Western users and financial data indicates a blend of espionage and cybercrime. All users of macOS should avoid sideloaded apps, use threat-aware antivirus tools and monitor unusual access to Keychain and browser stores to protect their system and confidentiality.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	BFSI
REGION	United States, European Union	**APPLICATION**	Apple macOS

Source - https://www.cyfirma.com/research/odyssey-stealer-the-rebrand-of-poseidon-stealer/

CL-CRI-1014: Financial institutions in Africa targeted with stealth tools

The CL-CRI-1014 campaign is actively targeting African financial institutions using tools such as PoshC2, Chisel and Classroom Spy to gain persistent access, conduct credential theft and sell network footholds on dark web markets. The attackers disguise the tools as legitimate software and use network tunnelling to avoid detection. Their tactics indicate a well-resourced operation, possibly even serving as initial access brokers in larger cybercrime ecosystems.

Financial institutions in Africa should apply real-time monitoring, restrict outbound tunnelling protocols and leverage threat intelligence to detect lateral movement and beaconing and safeguard themselves against the CL-CRI-1014 campaign.

ATTACK TYPE	Malware	**SECTOR**	BFSI
REGION	Africa	**APPLICATION**	Apple macOS, Android, Windows, Linux

Source - https://unit42.paloaltonetworks.com/cybercriminals-attack-financial-sector-across-africa/

Silver Fox campaign delivers Sainbox RAT and stealth rootkit to Chinese users

A targeted campaign dubbed Silver Fox is delivering malware to Chinese-speaking users via phishing sites offering fake installers for popular apps like WPS Office and Sogou. Victims are infected with Sainbox RAT, a Gh0stRAT variant and a stealthy Hidden rootkit. The Malware leverages DLL side-loading via Shine.exe and persistence through the Windows Run key and is dropped using MSI and PE files. The rootkit conceals files and processes and ensures a stealthy presence.

To defend against stealthy malware campaigns like Silver Fox, organisations should validate software sources, monitor for suspicious behaviours - such as DLL side-loading and unauthorised Run key modifications - and deploy rootkit detection tools. Strengthening endpoint defences, enforcing least privilege, training users against phishing, and leveraging behavioural EDR/XDR tools are also critical for detecting and mitigating similarly designed persistent threats.

ATTACK TYPE	Malware	**SECTOR**	IT, Software Development
REGION	China	**APPLICATION**	Windows

Source - https://www.netskope.com/blog/deepseek-deception-sainbox-rat-hidden-rootkit-delivery

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