TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 28, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today’s evolving cyber landscape, safeguarding critical systems is vital for individuals, businesses, and governments. Cyber threats can cause financial loss, reputational harm, and operational disruptions.

Our weekly Cyber Threat Intelligence (CTI) report offers actionable insights on emerging threats, helping organisations enhance security, mitigate risks, and build cyber resilience. Supported by expert advisory services, this intelligence-driven approach identifies vulnerabilities and strengthens defence strategies. Stay ahead of cyber risks with the latest knowledge and tools to protect your digital assets and ensure a secure future.

New malware ModiLoader exploits Windows CAB files

Cybersecurity researchers have discovered ModiLoader (DBatLoader), a sophisticated malware campaign exploiting Windows CAB file headers to evade detection. Delivered via phishing emails disguised as purchase orders, the malware uses manipulated CMD file structures to execute hidden payloads. Attackers modify file headers to bypass security tools, allowing for deeper infiltration into compromised systems. Once deployed, ModiLoader acts as a delivery mechanism for additional malware, posing a severe threat to organizations by facilitating data theft and system compromise.

Experts warn users to exercise caution with email attachments and emphasize the need for updated security defences to counter emerging threats.

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

Source - https://asec.ahnlab.com/ko/85732/

Cybercriminals exploit software cracks to distribute malware

A recent report warns that cybercriminals are increasingly using fake software cracks and installers to distribute malware. These deceptive tools, often found on torrent sites and unauthorised download platforms, lure users into downloading malicious software disguised as legitimate applications. Once installed, these programmes can steal sensitive data, install backdoors, or deploy ransomware, severely compromising device security. The report highlights that malware within these fake installers can evade traditional detection methods, making it a persistent threat. Cybercriminals exploit users' desire for free software, leveraging social engineering tactics to bypass security defences. Researchers emphasise that avoiding pirated software, maintaining updated security tools, and using reputable sources for downloads are crucial for protection.

To mitigate risks, users are advised to verify software authenticity and enable multi-layered security solutions. Organisations should also educate employees about the dangers of downloading unauthorised software to prevent network breaches.

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

Source - https://www.trendmicro.com/en_us/research/25/a/how-cracks-and-installers-bring-malware-to-your-device.html

Russian-linked cyberespionage campaign targets Central Asian nations

A newly uncovered cyberespionage campaign, linked to Russian-backed group, UAC-0063, has targeted Kazakhstan and other Central Asian nations, exploiting weaponised documents to gather strategic intelligence. The campaign, believed to be connected to APT28, employed malicious Word files disguised as diplomatic correspondence, including recent communications between Kazakhstan and Germany.

The attack, identified through a series of macro-based infections, exploited government documents from Kazakhstan's Ministry of Foreign Affairs and other state institutions, posing significant risks to diplomatic and economic relations. Security experts emphasise the continued threat of cyberespionage in the region.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Central Asia	**APPLICATION**	Windows

Source - https://blog.sekoia.io/double-tap-campaign-russia-nexus-apt-possibly-related-to-apt28-conducts-cyber-espionage-on-central-asia-and-kazakhstan-diplomatic-relations/

New Linux rootkit sysinitd.ko discovered

A new Linux rootkit, named sysinitd.ko, has been uncovered by cybersecurity researchers. The malware exploits vulnerabilities to gain full remote control over compromised systems. Using a kernel module, the rootkit intercepts network traffic, installs persistent malware, and communicates with malicious user-space binaries. The rootkit is integrated into the system via malicious shell scripts and maintains persistence by modifying system files to load at startup.

As part of its operations, it registers network hooks and creates files that give attackers greater control. This rootkit, found on Ivanti appliance systems, is part of a larger malware campaign and poses a severe security threat to affected devices.

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

Source - https://www.fortinet.com/blog/threat-research/deep-dive-into-a-linux-rootkit-malware

Sophisticated threats emerge in the form of Formbook phishing campaigns

Cybersecurity researchers have uncovered a detailed Formbook phishing campaign that continues to evolve in sophistication. The campaign uses spear phishing emails with attachments, including a malicious PurchaseOrder.exe file. Upon execution, the file activates a multi-stage malware process, decrypting and loading additional malware stages from hidden resources.

Stage one involves the PurchaseOrder.exe hiding two malicious DLL files that are decrypted into memory and executed. Stage two, Arthur.dll continues the decryption process, using steganography to extract stage three, Montero.dll, from an image. This advanced technique makes detection difficult, as the malware evades conventional scanning methods by running entirely in memory. The final stage enables persistent malware installation, avoiding detection by creating mutexes and using hidden tasks for execution, making it challenging to remove. Researchers emphasize the need for vigilance against spear-phishing tactics, as this campaign highlights the persistent and evolving nature of modern cyber threats.

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

Source - https://www.seqrite.com/blog/formbook-phishing-campaign-analysis/

Cl0p ransomware campaign continues to target enterprises

Cl0p, a sophisticated ransomware strain linked to the TA505 cybercrime group, remains a significant threat to global organisations. Emerging in 2019, Cl0p has been used in high-profile attacks, particularly targeting large enterprises with encrypted file systems. Cybercriminals behind Cl0p deploy digitally signed payloads and multiple anti-analysis techniques to avoid detection. Interestingly, the ransomware is designed to avoid execution on Russian language systems. These measures make Cl0p notably more dangerous, allowing attackers to exfiltrate sensitive data and demand substantial ransom payments.

With the continued evolution of Cl0p's tactics, companies are urged to enhance their cybersecurity measures to defend against its ongoing campaigns.

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

Source - https://cyberint.com/blog/dark-web/cl0p-ransomware/, https://www.mimecast.com/content/clop-ransomware/, https://www.kaspersky.com/resource-center/definitions/cl0p-ransomware, https://www.sentinelone.com/anthology/clop/

ShadowSyndicate expands operations with RansomHub partnership

ShadowSyndicate, an advanced cybercriminal group active since 2022, has broadened its reach by aligning with RansomHub, a prominent ransomware-as-a-service (RaaS) platform. The group, known for executing multi-stage attacks and sophisticated data exfiltration via SSH, has successfully targeted over 500 victims by 2024. Their collaboration with RansomHub allows them to scale operations, leveraging its infrastructure for even more impactful ransomware campaigns.

This rise of RaaS underscores the escalating threat to organisations globally, highlighting the need for robust, proactive cybersecurity measures to mitigate such attacks.

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

Gootloader malware evolves with sophisticated SEO tactics

Researchers have detailed the inner workings of Gootloader, a malware strain that has successfully exploited search engine results to lure victims. The malware creators manipulate legitimate websites, redirecting users from search results to compromised pages that deliver the malicious payload. This multi-stage infection process is driven by server-side code that dynamically generates fake online conversations, tricking users into downloading the malware disguised as solutions to their search queries. Gootloader employs advanced obfuscation techniques to evade detection, including splitting code into smaller, functionally individual parts to hinder analysis. Additionally, it uses delays to slow down dynamic analysis and improve persistence.

The researchers also discovered the malware's ability to use poisoned SEO tactics, driving compromised sites to the top of search engine results in various languages. This evolving technique, relying on obfuscation and server-side manipulation, makes Gootloader a persistent and formidable cyber threat. To protect against Gootloader, users must exercise caution with search results, especially on unfamiliar sites, and maintain updated security systems to detect these kinds of obfuscations.

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

Source - https://news.sophos.com/en-us/2025/01/16/gootloader-inside-out/

Qilin ransomware poses growing threat with double extortion techniques

Cybersecurity experts have identified the Agenda (Qilin) ransomware as a rising threat in the cybercrime world. First observed in July 2022, this malware is written in Golang and supports multiple encryption modes, controlled by operators. Known for its double extortion strategy, Agenda demands payment both for decrypting files and preventing the release of stolen data. The ransomware's adaptability and evolving methods make it a formidable adversary for organisations, emphasising the need for robust cybersecurity measures.

Researchers recommend timely patches, data backups, and vigilance in monitoring abnormal network traffic to mitigate risks associated with this growing threat.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Others
REGION	Global	**APPLICATION**	Windows, Linux

Source - https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf, https://www.sentinelone.com/anthology/agenda-qilin/

Black Basta uses Microsoft Teams to phish victims and deploy malware

Cybersecurity experts have revealed a sophisticated phishing attack carried out by the Black Basta ransomware group, which targets victims via Microsoft Teams. The attack begins with spam emails and escalates through a Teams chat where the attacker impersonates IT support. Victims are convinced to grant remote access, enabling the criminals to deploy malware and steal sensitive data. Researchers highlight several detection strategies, including monitoring spikes in spam emails, scrutinising suspicious Teams activity, and identifying the use of remote access tools.

Preventative measures include blocking external Teams communications and strengthening anti-spam policies to protect organisations from this emerging threat.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	MS Teams

Source - https://blog.nviso.eu/2025/01/16/detecting-teams-chat-phishing-attacks-black-basta/

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