TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: APRIL 8, 2025

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today’s fast-changing digital landscape, organisations must adopt proactive cybersecurity measures to combat rising threats. Our weekly Cyber Threat Intelligence (CTI) reports provide critical insights into emerging risks, vulnerabilities, and attack trends, empowering businesses to fortify defences and stay ahead of cyber adversaries.

Through expert analysis and actionable strategies, we help clients anticipate, detect, and neutralise threats before they escalate. This proactive approach not only protects critical assets but also ensures business continuity and strengthens stakeholder confidence. With our CTI insights, organisations can build long-term cyber resilience, navigating the digital world with greater security and assurance.

New Anonymous Xorist ransomware threatens Windows users

Security researchers have identified a dangerous new ransomware variant called Anonymous Xorist targeting Windows systems worldwide. The malware infiltrates through phishing emails, fake software cracks, and compromised websites, encrypting files and appending random extensions while leaving ransom notes in each folder. Using strong encryption algorithms, the ransomware demands cryptocurrency payments, though cybersecurity experts strongly advise against paying as recovery isn't guaranteed.

For infected systems, immediate action is crucial: disconnect from networks, boot into Safe Mode, and run updated antivirus scans. While some variants may be decrypted with specialised tools, prevention remains the best defence. Experts recommend maintaining regular offline backups (following the 3-2-1 rule), keeping all software updated, and training employees to recognise phishing attempts. As Anonymous Xorist continues to evolve, users are urged to implement robust security measures before falling victim to this growing threat.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyclonis.com/remove-anonymous-xorist-ransomware/

Pakistan’s Youth Laptop Scheme exploited in cyberattacks targeting India

Cybersecurity experts have uncovered a disturbing campaign where hackers are exploiting Pakistan’s Prime Minister’s Youth Laptop Scheme to deliver malware targeting Indian entities. Attackers are distributing trojanised application forms disguised as legitimate program documents, which install information-stealing malware when opened. The scheme, intended to provide free laptops to students, is being weaponised to compromise systems in government, defence, and education sectors across India.

The malware enables remote access, data theft, and surveillance capabilities, with evidence suggesting links to state-sponsored actors. Researchers warn this represents a dangerous trend of abusing welfare programs for cyber warfare. Indian organisations are urged to verify all document sources, use advanced email filtering, and conduct employee awareness training. Security teams recommend immediate scrutiny of any files related to the Pakistani laptop initiative.

ATTACK TYPE	Malware	SECTOR	Government, education, aerospace, defence
REGION	India	APPLICATION	Windows, Android

Source - https://www.cyfirma.com/research/turning-aid-into-attack-exploitation-of-pakistans-youth-laptop-scheme-to-target-india/

Snake Keylogger emerges as multistage threat in global cyberespionage campaign

Researchers have uncovered Snake Keylogger, a sophisticated multistage malware operation stealing sensitive data from victims worldwide. The infostealer employs advanced evasion techniques, distributing itself through phishing emails with malicious attachments and compromised software downloads. Once installed, it harvests keystrokes, screenshots, clipboard data, and browser credentials, while maintaining persistence through registry modifications and scheduled tasks.

The campaign primarily targets financial institutions, corporate enterprises, and government agencies, with evidence suggesting ties to state-sponsored hacking groups. Experts warn the malware's modular design allows for rapid adaptation to new targets. Organisations are urged to deploy behaviour-based threat detection, implement application whitelisting, conduct employee phishing simulations, and monitor for unusual data exfiltration. Security teams emphasise that traditional antivirus solutions may miss this evolving threat, requiring advanced endpoint protection.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.seqrite.com/blog/snakekeylogger-a-multistage-info-stealer-malware-campaign/

Operation ForumTroll target Western thinktanks in cyberespionage attacks

Researchers have exposed Operation ForumTroll, an ongoing cyberespionage campaign by Russian-linked threat actors targeting Western policy institutes, NGOs, and academic organisations. The hackers employ sophisticated spear-phishing tactics, posing as journalists and researchers to deliver malicious documents that install the Kapeka backdoor — a custom malware capable of file theft, screen capture, and remote system control. The operation, active since at least 2022, focuses on stealing sensitive geopolitical research and policy discussions.

Experts warn the campaign demonstrates state-sponsored tradecraft, with targets including NATO-aligned nations' foreign policy organisations. Security recommendations include enhanced email verification for unsolicited attachments, network segmentation for sensitive research data, behavioural detection for backdoor activity, and multi-factor authentication (MFA) for all privileged accounts. This revelation comes amid heightened tensions between Russia and Western institutions, highlighting the growing weaponisation of cybersecurity in geopolitical conflicts.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Microsoft Edge, Google Chrome

Source - https://securelist.com/operation-forumtroll/115989/

LockBit 4.0 ransomware variant emerges with advanced evasion tactics

Analysts have uncovered LockBit 4.0, a significantly upgraded version of the notorious ransomware that now incorporates next-generation evasion techniques. Compared to LockBit 3.0, the new variant features enhanced anti-analysis capabilities, including process hollowing to hide malicious activity, custom encryption algorithms, and improved persistence mechanisms. The ransomware-as-a-service (RaaS) operation continues targeting enterprise networks globally, with healthcare, finance, and critical infrastructure at highest risk.

Analysis reveals LockBit 4.0 demonstrates state-sponsored level sophistication, with evidence suggesting development resources have tripled since version 3.0. Organisations are urged to deploy behaviour-based detection, segment critical networks, maintain immutable backups, and patch within 24 hours of critical updates. With LockBit responsible for 28% of all ransomware attacks in 2023, security teams warn this upgrade represents a dangerous evolution in cyber threats.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.deepinstinct.com/blog/raas-evolved-lockbit-3-0-vs-lockbit-4-0

Frag ransomware emerges as new threat targeting global enterprises

Cybersecurity researchers have identified Frag, a sophisticated new ransomware strain targeting organisations worldwide. The malware employs advanced encryption methods to lock critical files while evading detection through fileless execution techniques. Frag spreads through phishing campaigns, RDP vulnerabilities, and drive-by downloads, with observed attacks hitting manufacturing, healthcare, and logistics sectors particularly hard. Security analysts note the ransomware's modular design allows for rapid adaptation to different network environments.

The attackers behind Frag utilise double extortion tactics, stealing sensitive data before encryption and threatening leaks if ransoms aren’t paid. Experts recommend immediate patching of internet-facing systems, network segmentation to limit lateral movement, behavioural monitoring for unusual file activity, and regular offline backups following the 3-2-1 rule. With ransomware attacks increasing 37% year-over-year, organisations are urged to strengthen defences against this evolving threat.

ATTACK TYPE	Ransomware	SECTOR	IT, healthcare, financial services, legal services, hospitality
REGION	Global	APPLICATION	Generic, Veeam, Veeam Backup Enterprise Manager

Source - https://cyberpress.org/frag-ransomware/

Arkana ransomware strikes WideOpenWest in latest critical infrastructure attack

Researchers have confirmed a disruptive Arkana ransomware attack against WideOpenWest (WOW), a major US telecommunications provider. The breach disrupted services for thousands of customers, with attackers reportedly stealing sensitive customer data before encrypting systems. Arkana operators utilised double extortion tactics, threatening to leak stolen information unless ransom demands were met. The attack vector appears to have exploited unpatched vulnerabilities in internet-facing systems, though investigators are still analysing the exact entry point.

This incident marks another escalation in attacks against critical communications infrastructure, following recent ransomware campaigns targeting ISPs globally. Security experts recommend immediate patching of VPN and RDP services, enhanced monitoring of data exfiltration attempts, network segmentation to contain breaches, and review of third-party vendor access. With telecom providers becoming frequent targets, experts warn the sector must prioritise cybersecurity investments to prevent cascading service disruptions.

ATTACK TYPE	Ransomware	**SECTOR**	Internet services, telecommunications
REGION	US	**APPLICATION**	Windows

Source - https://socradar.io/arkana-ransomware-attack-on-wideopenwest/

TATA COMMUNICATIONS

Trinity ransomware unleashes triple extortion threat via dark web RaaS operation

Dark web monitoring experts have uncovered Trinity, a sophisticated ransomware operation gaining traction among cybercriminals. This dangerous new variant employs triple extortion tactics: encrypting files, stealing sensitive data, and threatening DDoS attacks unless victims pay. The group operates a professionalised RaaS model on dark web forums, recruiting affiliates to expand its reach. Trinity specifically targets SMBs and healthcare providers, exploiting known vulnerabilities in VPNs and RDP services.

Analysis reveals Trinity’s attacks follow a three-phase approach: initial network access, lateral movement using PowerShell scripts, then simultaneous encryption and data exfiltration. Experts recommend immediate patching of internet-facing systems, network segmentation to limit spread, behavioural monitoring for unusual PowerShell activity, and 24/7 dark web surveillance for early leak detection. With Trinity's operator offering 85% profit sharing to affiliates, security teams warn this threat will likely escalate in coming months.

ATTACK TYPE	Ransomware	SECTOR	Healthcare, financial services, legal services, manufacturing, construction, IT
REGION	Canada, Spain, US	APPLICATION	Windows

Source - https://socradar.io/dark-web-profile-trinity-ransomware/

INTRODUCTION
ANONYMOUS XORIST RANSOMWARE THREATENS WINDOWS USERS
PAKISTAN’S YOUTH LAPTOP SCHEME EXPLOITED IN CYBERATTACKS
SNAKE KEYLOGGER EMERGES AS A CYBERESPIONAGE CAMPAIGN
OPERATION FORUMTROLL PROPAGATES CYBERESPIONAGE ATTACKS
LOCKBIT 4.0 VARIANT EMERGES WITH ADVANCED EVASION TACTICS
FRAG RANSOMWARE TARGETS ENTERPRISES IN A GLOBAL CAMPAIGN
ARKANA RANSOMWARE ATTACKS WIDEOPENWEST’S CRITICAL INFRA
TRINITY RANSOMWARE DEPLOYS TRIPLE EXTORTION TACTICS IN DARK WEB
NEW WORRY RANSOMWARE SPREADS PANIC WITH PSYCHOLOGICAL TACTICS
MATTVENOM RANSOMWARE EMERGES AS A THREAT TO WINDOWS SYSTEMS

New Worry ransomware spreads panic with psychological tactics

Cybersecurity analysts warn of Worry (Whatswrongscared), a disturbing new ransomware strain that combines file encryption with psychological warfare tactics. The malware displays threatening messages like "What's wrong? Scared?" during attacks, amplifying victim distress. It spreads through malicious email attachments, fake software updates, and compromised websites, encrypting files with a complex algorithm while leaving ransom notes demanding cryptocurrency payments.

The ransomware primarily targets individual users and small businesses, exploiting weak security practices. Removal requires disconnecting infected devices, booting in safe mode, using anti-malware tools, and restoring from clean backups. Researchers emphasise never paying ransoms, as this funds criminal operations without guaranteeing file recovery. With ransomware attacks growing more sophisticated, experts urge regular backups, software updates, and security awareness training as critical defences against emerging threats.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyclonis.com/remove-worry-whatswrongscared-ransomware/

INTRODUCTION

ANONYMOUS XORIST RANSOMWARE THREATENS WINDOWS USERS

PAKISTAN'S YOUTH LAPTOP SCHEME EXPLOITED IN CYBERATTACKS

SNAKE KEYLOGGER EMERGES AS A CYBERESPIONAGE CAMPAIGN

OPERATION FORUMTROLL PROPAGATES CYBERESPIONAGE ATTACKS

LOCKBIT 4.0 VARIANT EMERGES WITH ADVANCED EVASION TACTICS

FRAG RANSOMWARE TARGETS ENTERPRISES IN A GLOBAL CAMPAIGN

ARKANA RANSOMWARE ATTACKS WIDEOPENWEST'S CRITICAL INFRA

TRINITY RANSOMWARE DEPLOYS TRIPLE EXTORTION TACTICS IN DARK WEB

NEW WORRY RANSOMWARE SPREADS PANIC WITH PSYCHOLOGICAL TACTICS

MATTVENOM RANSOMWARE EMERGES AS A THREAT TO WINDOWS SYSTEMS

MattVenom ransomware targets Windows users with aggressive encryption tactics

Cybersecurity researchers have identified MattVenom, a dangerous new ransomware variant actively targeting Windows systems. The malware infiltrates through phishing emails, malicious downloads, and exploit kits, encrypting files with a strong AES-256 algorithm while appending the .mattvenom extension. Victims receive ransom notes demanding payment in cryptocurrency, with threats of permanent data deletion if demands aren’t met within a strict deadline.

The ransomware demonstrates rapid encryption capabilities, particularly targeting documents, images, and databases. Removal requires immediate disconnection from networks, safe mode booting to prevent spread, antivirus scanning with updated definitions, and system restoration from clean backups. Security experts strongly advise against paying ransoms, emphasising regular offline backups and employee phishing awareness training as critical defences. With MattVenom’s operators actively refining their tactics, users are urged to update security software immediately.

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

Source - https://www.cyclonis.com/remove-mattvenom-ransomware/

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

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.