TATA COMMUNICATIONS

# YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: AUGUST 05, 2025

TATA

# THREAT INTELLIGENCE ADVISORY REPORT

Today’s rapidly evolving digital landscape poses intricate challenges for organisations already grappling with an expanding array of cyber threats. Not only are these pervasive threats capable of inflicting substantial harm on business entities, but also on individuals and government bodies. Unsurprisingly, they can result in dire consequences such as data breaches, operational disruptions, and financial setbacks.

Through expert analysis and actionable strategies, we help clients anticipate, detect, and neutralise threats before they escalate with our weekly Cyber Threat Intelligence (CTI) reports. These provide critical insights into emerging risks, vulnerabilities, and attack trends, empowering businesses to fortify defences and stay ahead of cyber adversaries. In a time when cyber resilience is a significant concern, we equip you with the essential tools and knowledge to fortify yourself and your organisation in an ever-shifting digital terrain.

# DeadLock ransomware: Military-grade encryption with a Monero twist

DeadLock is a destructive ransomware strain that encrypts files with the .dlock extension and embeds a unique victim ID. It demands ransom in Bitcoin or Monero via Session messenger and changes the user’s desktop wallpaper to reinforce urgency. The malware is delivered through email attachments, pirated software, and infected USB drives. It employs advanced persistence techniques like bootloader tampering, process injection, and code obfuscation, making it extremely difficult to detect or remediate.

Enterprises must implement strong endpoint protection, regularly back up critical systems offline, and use application allowlisting. Employee education around safe file practices and phishing prevention is essential. EDR tools should monitor for file encryption behaviours and desktop wallpaper modifications, while threat hunting should focus on Session-based C2 indicators.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | All |
| REGION | Global | APPLICATION | Windows |

Source - https://www.pcrisk.com/removal-guides/33407-deadlock-ransomware , https://www.broadcom.com/support/security-center/protection-bulletin/deadlock-ransomware

INTRODUCTION
A DEADLOCK RANSOMWARE DEMANDS MONERO VIA SESSION MESSENGER
EPSILON RED CAMPAIGN GOES STEALTH WITH CLICKFIX LURE
GUNRA RANSOMWARE WEAPONISES CONTI CODE WHILE DELETING SHADOW COPIES
INTERLOCK RANSOMWARE SURGE THREATENS THE HEALTHCARE SECTOR
UNC3886 EXPLOITS ZERO-DAYS IN VMWARE, FORTINET AND JUNIPER DEVICES
UNC3944 BREACHES VSPHERE VIA HELP DESK SOCIAL ENGINEERING
CISCO CONFIRMS ACTIVE EXPLOITS OF CUIC AND ISE FLAWS
ANDROID BANKING MALWARE IMPERSONATES INDIAN BANK APPS
CHAOS RANSOMWARE LAUNCHES BIG-GAME DOUBLE EXTORTION ATTACKS
RANCOZ RANSOMWARE DESTROYS RECOVERY PATHS WHILE THREATENING DATA LEAKS

# Epsilon Red campaign evolves with Clickfix and fake bots

A new malware campaign is deploying Epsilon Red ransomware via a deceptive Clickfix-themed lure. Victims are tricked into visiting a malicious verification site that downloads and executes ransomware silently using ActiveX scripting. The campaign impersonates trusted services like Discord Captcha Bot, Twitch, and OnlyFans, exploiting brand trust to enhance phishing effectiveness. The approach signifies a shift toward automated, socially engineered drive-by ransomware delivery with minimal user interaction.

Security teams should block ActiveX controls in browsers and use secure DNS filtering to restrict access to phishing domains. Organisations should educate users about fake verification codes and platform impersonations. Browser-based behaviour analysis tools and web proxies can help detect and prevent automated payload delivery attempts.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | All |
| REGION | Global | APPLICATION | Windows |

Source - https://www.cloudsek.com/blog/threat-actors-lure-victims-into-downloading-hta-files-using-clickfix-to-spread-epsilon-red-ransomware

INTRODUCTION
A DEADLOCK RANSOMWARE DEMANDS MONERO VIA SESSION MESSENGER
EPSILON RED CAMPAIGN GOES STEALTH WITH CLICKFIX LURE
GUNRA RANSOMWARE WEAPONISES CONTI CODE WHILE DELETING SHADOW COPIES
INTERLOCK RANSOMWARE SURGE THREATENS THE HEALTHCARE SECTOR
UNC3886 EXPLOITS ZERO-DAYS IN VMWARE, FORTINET AND JUNIPER DEVICES
UNC3944 BREACHES VSPHERE VIA HELP DESK SOCIAL ENGINEERING
CISCO CONFIRMS ACTIVE EXPLOITS OF CUIC AND ISE FLAWS
ANDROID BANKING MALWARE IMPERSONATES INDIAN BANK APPS
CHAOS RANSOMWARE LAUNCHES BIG-GAME DOUBLE EXTORTION ATTACKS
RANCOZ RANSOMWARE DESTROYS RECOVERY PATHS WHILE THREATENING DATA LEAKS

# Gunra ransomware weaponises leaked Conti code

Gunra is a sophisticated ransomware strain built on the leaked Conti codebase. It uses hybrid RSA and ChaCha20 encryption to delete shadow copies and gives victims only five days to negotiate, increasing pressure to pay. Gunra is highly selective and focuses on fast encryption and operational disruption. It spreads through phishing, cracked software, and RDP exploitation, mimicking successful tactics from Conti and other top-tier ransomware operators.

Businesses must ensure offline backups, segment critical infrastructure, and apply strict patching policies. RDP and remote access solutions must be hardened or disabled. Threat hunting teams should scan for encryption activity, deleted logs, and known Gunra indicators. Recovery strategies should be tested in anticipation of short negotiation windows.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | All |
| REGION | Global | APPLICATION | Windows |

Source - https://asec.ahnlab.com/ko/89153/

INTRODUCTION | A DEADLOCK RANSOMWARE DEMANDS MONERO VIA SESSION MESSENGER | EPSILON RED CAMPAIGN GOES STEALTH WITH CLICKFIX LURE | GUNRA RANSOMWARE WEAPONISES CONTI CODE WHILE DELETING SHADOW COPIES | INTERLOCK RANSOMWARE SURGE THREATENS THE HEALTHCARE SECTOR | UNC3886 EXPLOITS ZERO-DAYS IN VMWARE, FORTINET AND JUNIPER DEVICES | UNC3944 BREACHES VSPHERE VIA HELP DESK SOCIAL ENGINEERING | CISCO CONFIRMS ACTIVE EXPLOITS OF CUIC AND ISE FLAWS | ANDROID BANKING MALWARE IMPERSONATES INDIAN BANK APPS | CHAOS RANSOMWARE LAUNCHES BIG-GAME DOUBLE EXTORTION ATTACKS | RANCOZ RANSOMWARE DESTROYS RECOVERY PATHS WHILE THREATENING DATA LEAKS

# Interlock ransomware surge targets healthcare

A joint advisory from CISA, FBI, HHS, and MS-ISAC warns of increasing Interlock ransomware activity. The group uses double extortion—encrypting data while also stealing it—and targets healthcare institutions in particular. Techniques include drive-by downloads and fake tools like FileFix, tricking users into activating ransomware. Interlock's ability to combine deception, data exfiltration, and encryption makes it a potent threat to operational continuity and patient privacy.

Healthcare organisations should enhance network segmentation, enable multi-factor authentication, and conduct frequent phishing simulations. Regular data backups, patching of internet-facing software, and monitoring for unusual outbound data transfers are critical. Endpoint solutions should block execution of unauthorised tools like FileFix.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | Healthcare/hospitals |
| REGION | Global | APPLICATION | Windows, Linux |

Source - https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a

# UNC3886 cyber-espionage campaign hits critical infrastructure

UNC3886, a China-linked cyber-espionage group, is exploiting zero-day vulnerabilities in Fortinet, VMware, and Juniper systems. Active since 2022, it uses malware like TINYSHELL, REPTILE, and MOPSLED, along with rootkits, credential harvesting, and log tampering. Their operations span sectors from healthcare to defence, affecting countries like Singapore, the U.S., and France. The group targets under-monitored systems such as hypervisors and routers, making detection extremely difficult.

Critical infrastructure operators must patch vulnerable virtualisation and network equipment immediately. Implementing segmentation between management and production environments is essential. Organisations should also adopt host-based intrusion detection systems (HIDS) and centralised logging to catch stealthy malware activity, even in non-user-facing infrastructure.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Vulnerability, Malware, Cyberespionage | SECTOR | Healthcare/hospitals, Manufacturing, IT, Government, Transportation, Energy, Aerospace, Defence Industry, Hospitality, Retailer and Distributor, Telecommunications |
| REGION | Australia, Singapore, India, Armenia, Chile, France, Ireland, Liechtenstein, Philippines, South Africa, Spain, Switzerland, Taiwan, United States, Vietnam | APPLICATION | Fortinet FortiGate, Juniper Router, VMware vCenter Server, VMware Tools |

Source - https://www.cyclonis.com/unc3886-cyber-espionage-group/

# UNC3944 targets vSphere with social engineering and ransomware

UNC3944, tied to the groups "0ktapus" and "Scattered Spider," has launched a high-impact campaign targeting VMware vSphere environments. The group gains access through fake help desk calls, escalates privileges via Active Directory, and pivots to ESXi servers for data exfiltration and ransomware deployment. Its use of “living-off-the-land” techniques allows it to operate within legitimate processes, evading most detection tools.

Retail, airline, and insurance sectors must implement phishing-resistant MFA and disable insecure help desk workflows. Organisations should enforce logging across Active Directory, vSphere, and Veeam environments. Regular access reviews and privilege minimisation are also essential to prevent lateral movement.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware, Social engineering | SECTOR | Transportation, Airlines and Aviation, Retailer and Distributor |
| REGION | North America | APPLICATION | VMWare ESXi  VMware vCenter Server, VMware vSphere Server, Windows, Veeam Backup Enterprise Manager |

Source - https://cybersecuritynews.com/unc3944-attacking-vmware-vsphere/

INTRODUCTION | A DEADLOCK RANSOMWARE DEMANDS MONERO VIA SESSION MESSENGER | EPSILON RED CAMPAIGN GOES STEALTH WITH CLICKFIX LURE | GUNRA RANSOMWARE WEAPONISES CONTI CODE WHILE DELETING SHADOW COPIES | INTERLOCK RANSOMWARE SURGE THREATENS THE HEALTHCARE SECTOR | UNC3886 EXPLOITS ZERO-DAYS IN VMWARE, FORTINET AND JUNIPER DEVICES | UNC3944 BREACHES VSPHERE VIA HELP DESK SOCIAL ENGINEERING | CISCO CONFIRMS ACTIVE EXPLOITS OF CUIC AND ISE FLAWS | ANDROID BANKING MALWARE IMPERSONATES INDIAN BANK APPS | CHAOS RANSOMWARE LAUNCHES BIG-GAME DOUBLE EXTORTION ATTACKS | RANCOZ RANSOMWARE DESTROYS RECOVERY PATHS WHILE THREATENING DATA LEAKS

# Critical Cisco vulnerabilities under active exploitation

Cisco has confirmed active exploitation of critical vulnerabilities in its Unified Intelligence Center (CUIC) and Identity Services Engine (ISE). These flaws, including unauthenticated remote file upload and code execution as root, can result in full system compromise. Attackers can manipulate data, disable security features, and establish long-term persistence. The vulnerabilities are rated as high as CVSS 10.0, with PoCs already in circulation.

Organisations must urgently patch affected Cisco systems and internet exposure should be restricted or disabled entirely until patched. Admins should monitor for file upload anomalies and unusual process behaviour. Segmentation and strict firewall rules should also be enforced to isolate sensitive identity infrastructure.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Vulnerability | SECTOR | All |
| REGION | Global | APPLICATION | Cisco Identity Services Engine (ISE), Cisco Unified Intelligence Center, CISCO ISE |

Source - https://thehackernews.com/2025/07/cisco-confirms-active-exploits.html

INTRODUCTION
A DEADLOCK RANSOMWARE DEMANDS MONERO VIA SESSION MESSENGER
EPSILON RED CAMPAIGN GOES STEALTH WITH CLICKFIX LURE
GUNRA RANSOMWARE WEAPONISES CONTI CODE WHILE DELETING SHADOW COPIES
INTERLOCK RANSOMWARE SURGE THREATENS THE HEALTHCARE SECTOR
UNC3886 EXPLOITS ZERO-DAYS IN VMWARE, FORTINET AND JUNIPER DEVICES
UNC3944 BREACHES VSPHERE VIA HELP DESK SOCIAL ENGINEERING
CISCO CONFIRMS ACTIVE EXPLOITS OF CUIC AND ISE FLAWS
ANDROID BANKING MALWARE IMPERSONATES INDIAN BANK APPS
CHAOS RANSOMWARE LAUNCHES BIG-GAME DOUBLE EXTORTION ATTACKS
RANCOZ RANSOMWARE DESTROYS RECOVERY PATHS WHILE THREATENING DATA LEAKS

# Android banking malware targets Indian users via fake apps

A new Android malware campaign is impersonating Indian banking apps to steal credentials, intercept SMS OTPs, and conduct unauthorised transactions. The malware abuses permissions, installs silently, and uses Firebase for C2 communication. It spreads through phishing, fake websites, and Trojanised APKs, representing a growing threat to financial security on mobile platforms.

Banks should warn customers against sideloading apps and enforce Play Store-only distribution. Mobile device management (MDM) tools, mobile threat defence (MTD), and behavioural analysis are vital. Users should verify app sources and deny excessive permissions. Financial institutions must detect unauthorised API access or account changes.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | BFSI |
| REGION | India | APPLICATION | Android |

Source - https://www.cyfirma.com/research/android-malware-posing-as-indian-bank-apps/

# Chaos ransomware group launches big-game hunting attacks

Chaos is a rapidly emerging RaaS group using hybrid encryption, selective file targeting, and double extortion tactics. They leverage remote monitoring and management (RMM) tools and anti-analysis techniques for stealth. Believed to be linked to Royal or BlackSuit, Chaos is conducting big-game hunts across manufacturing, IT, and education sectors globally. Their targeting includes both local and virtual environments, like ESXi.

Organisations must harden RMM tools, enforce app allowlisting, and deploy deception-based defences. Offline backups, network segmentation, and EDRs configured for lateral movement detection are essential. Threat intel should monitor for overlap in TTPs with Royal and BlackSuit campaigns.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | Manufacturing, IT, Education, IT Services and Consulting |
| REGION | India, UK, New Zealand, United States | APPLICATION | VMWare ESXi, Windows, Linux |

Source - https://blog.talosintelligence.com/new-chaos-ransomware

# Rancoz ransomware deletes logs, backups and threatens data leaks

Rancoz is a ransomware strain that encrypts files with the .rec_rans extension and immediately deletes system backups, volume shadow copies, and event logs. Victims are confronted with ransom notes and desktop wallpaper changes. The group threatens data exposure if ransom demands are not met. Its destructive behaviour eliminates recovery paths and increases pressure on victims.

Backup strategies must include isolated, immutable storage and frequent integrity checks. Endpoint defences should monitor for shadow copy deletion and unauthorised access to event logs. Incident response teams must prepare to handle data leaks and enforce encryption-at-rest to reduce breach impact.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | All |
| REGION | Global | APPLICATION | Windows |

Source - https://www.sentinelone.com/anthology/rancoz/

INTRODUCTION
A DEADLOCK RANSOMWARE DEMANDS MONERO VIA SESSION MESSENGER
EPSILON RED CAMPAIGN GOES STEALTH WITH CLICKFIX LURE
GUNRA RANSOMWARE WEAPONISES CONTI CODE WHILE DELETING SHADOW COPIES
INTERLOCK RANSOMWARE SURGE THREATENS THE HEALTHCARE SECTOR
UNC3886 EXPLOITS ZERO-DAYS IN VMWARE, FORTINET AND JUNIPER DEVICES
UNC3944 BREACHES VSPHERE VIA HELP DESK SOCIAL ENGINEERING
CISCO CONFIRMS ACTIVE EXPLOITS OF CUIC AND ISE FLAWS
ANDROID BANKING MALWARE IMPERSONATES INDIAN BANK APPS
CHAOS RANSOMWARE LAUNCHES BIG-GAME DOUBLE EXTORTION ATTACKS
RANCOZ RANSOMWARE DESTROYS RECOVERY PATHS WHILE THREATENING DATA LEAKS

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.