TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: APRIL 15, 2025

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.

CISA warns of active exploitation of critical Cisco Smart Licensing flaw

The Cybersecurity and Infrastructure Security Agency (CISA) has issued an urgent warning about active exploitation of a high-severity vulnerability (CVE-2024-20356) in Cisco’s Smart Licensing utility. The flaw, which allows attackers to execute arbitrary commands with elevated privileges, affects Cisco Smart Software Manager On-Prem and related products. Despite Cisco releasing patches in February 2024, unpatched systems remain vulnerable to attacks, potentially enabling unauthorised access, data theft, or system compromise.

CISA has added the bug to its Known Exploited Vulnerabilities (KEV) catalogue, mandating federal agencies to apply fixes by June 20. Cybersecurity experts urge all organisations using affected Cisco solutions to prioritise updates, as threat actors are actively targeting this vulnerability. The advisory highlights the growing risk of unpatched software in critical infrastructure, reinforcing the need for proactive vulnerability management.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic, Cisco Smart Licensing Utility

Source - https://securityonline.info/cisa-warns-of-active-exploitation-of-cisco-smart-licensing-utility-flaw/

Hunters International ransomware group expands attacks

A recent report has warned of the growing threat posed by Hunters International, a ransomware group actively targeting organisations worldwide. The group, which emerged after the disbandment of the notorious Hive ransomware operation, has adopted a double-extortion tactic – stealing sensitive data before encrypting systems and demanding hefty ransoms. Analysis reveals that Hunters International primarily exploits vulnerabilities in remote desktop protocols (RDP) and phishing campaigns to infiltrate networks, with healthcare, manufacturing, and financial sectors at highest risk.

The report highlights the group's increasing sophistication, including fast encryption speeds and customised ransom notes. Authorities urge businesses to strengthen endpoint security, enforce multi-factor authentication (MFA), and maintain offline backups to mitigate risks. With ransomware attacks surging globally, proactive defence measures are critical to thwarting Hunters International's escalating cybercrime spree.

ATTACK TYPE	Ransomware	SECTOR	Healthcare, financial services, manufacturing, education, automobile, food and beverage services, logistics and shipping
REGION	Canada, India, Japan, UK, Brazil, Chile, Dominican Republic, Germany, Latvia, Sri Lanka, US	APPLICATION	Windows, Fortinet

Source - https://www.linkedin.com/pulse/hunters-international-ransomware-report-foresiet-lfetc/

Apple rushes critical security patches to older devices amid active exploits

Apple has issued emergency security updates for older iPhones, iPads, and Macs to address three zero-day vulnerabilities (CVE-2024-23296, CVE-2024-23225, and CVE-2024-23222) actively exploited in attacks. These flaws, affecting WebKit and the kernel, could allow attackers to bypass security measures, execute malicious code, or gain elevated privileges. While Apple previously patched these issues in newer iOS and macOS versions, the newly backported fixes extend protection to legacy devices, including iPhone 6s, iPad Air 2, and 2017 MacBooks.

Cybersecurity experts warn that unpatched systems remain vulnerable to stealthy attacks, urging users to update immediately. The rapid backporting highlights Apple's response to persistent threats targeting outdated hardware still in widespread use. This marks Apple's second zero-day patch rollout in 2024, underscoring the growing risk of unpatched vulnerabilities in aging devices. Users are advised to install updates via Settings > General > Software Update to mitigate potential breaches.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	macOS, iOS

Source - https://securityonline.info/apple-backports-fixes-for-three-actively-exploited-zero-days-targeting-older-devices/

INTRODUCTION | CISA ALERTS ON ACTIVELY EXPLOITED CISCO ZERO-DAY FLAW | HUNTERS INTERNATIONAL RANSOMWARE TARGETS CRITICAL SECTORS | APPLE PATCHES ACTIVELY EXPLOITED ZERO-DAYS IN OLDER DEVICES | TSARBOT TROJAN HIJACKS BANKING DATA WITH FAKE LOGIN SCREENS | CRAZYHUNTER LAUNCHES TARGETED DOUBLE-EXTORTION ATTACKS | DARKCLOUD MALWARE THREATENS WITH ADVANCED EVASION TACTICS | QILIN RANSOMWARE EXPLOITS SCREENCONNECT IN GLOBAL ATTACKS | FMLN RANSOMWARE LAUNCHES DOUBLE ATTACK ON BUSINESSES | PELDOX RANSOMWARE LOCKS FILES IN 72-HOUR EXTORTION SCHEME | CHINESE HACKERS EXPLOIT IVANTI VPN FLAWS FOR CYBERESPIONAGE

New banking trojan TsarBot targets financial sector with sophisticated overlay attacks

A dangerous new Android banking trojan named TsarBot has been discovered targeting the banking, financial services, and insurance (BFSI) sector through sophisticated overlay attacks. According to cybersecurity researchers, the malware disguises itself as legitimate applications while secretly creating fake login screens that mimic real banking apps to steal sensitive credentials. Once installed, TsarBot gains extensive permissions, enabling it to intercept SMS messages, bypass two-factor authentication (2FA), and even manipulate device settings to evade detection. The malware primarily spreads through phishing campaigns and malicious app downloads outside official stores.

Experts warn that TsarBot represents an evolving threat to mobile banking security, with its ability to dynamically adapt to different financial applications. Financial institutions and users are urged to verify app sources, avoid suspicious links, and implement robust mobile security measures. This discovery highlights the growing sophistication of mobile banking threats in 2024, requiring heightened vigilance from both organisations and consumers.

ATTACK TYPE	Malware	SECTOR	e-commerce, BFSI
REGION	Global	APPLICATION	Android

Source - https://cyble.com/blog/tsarbot-using-overlay-attacks-targeting-bfsi-sector/

CrazyHunter ransomware targets enterprises with sophisticated double extortion tactics

A dangerous new ransomware strain dubbed CrazyHunter has emerged, employing advanced double extortion techniques to pressure victims into paying ransoms. The malware not only encrypts critical files but also exfiltrates sensitive data, threatening public release if demands aren't met. CrazyHunter demonstrates concerning sophistication, using AES-256 encryption and selectively targeting enterprise systems while avoiding detection by security software. Analysis reveals the ransomware primarily infiltrates networks through compromised RDP connections and phishing campaigns, with recent attacks focusing on manufacturing, healthcare, and professional services sectors.

Security experts warn that CrazyHunter operators meticulously study victim organisations to maximise ransom pressure. Analysts have urged businesses to immediately implement MFA, maintain offline backups, and monitor for unusual network activity. The emergence of CrazyHunter highlights the evolving ransomware landscape, where cybercriminals increasingly combine technical prowess with psychological tactics to extort organisations. As attacks grow more targeted, proactive defence measures become critical for enterprise security.

ATTACK TYPE	Ransomware	SECTOR	Healthcare
REGION	Taiwan	APPLICATION	Windows

Source - https://labs.withsecure.com/publications/crazyhunter-ransomware

INTRODUCTION | CISA ALERTS ON ACTIVELY EXPLOITED CISCO ZERO-DAY FLAW | HUNTERS INTERNATIONAL RANSOMWARE TARGETS CRITICAL SECTORS | APPLE PATCHES ACTIVELY EXPLOITED ZERO-DAYS IN OLDER DEVICES | TSARBOT TROJAN HIJACKS BANKING DATA WITH FAKE LOGIN SCREENS | CRAZYHUNTER LAUNCHES TARGETED DOUBLE-EXTORTION ATTACKS | DARKCLOUD MALWARE THREATENS WITH ADVANCED EVASION TACTICS | QILIN RANSOMWARE EXPLOITS SCREENCONNECT IN GLOBAL ATTACKS | FMLN RANSOMWARE LAUNCHES DOUBLE ATTACK ON BUSINESSES | PELDOX RANSOMWARE LOCKS FILES IN 72-HOUR EXTORTION SCHEME | CHINESE HACKERS EXPLOIT IVANTI VPN FLAWS FOR CYBERESPIONAGE

DarkCloud malware threatens global cybersecurity with advanced evasion tactics

Security researchers have uncovered a sophisticated new malware strain dubbed DarkCloud that's actively targeting organisations worldwide. This advanced threat combines ransomware capabilities with data exfiltration tools, creating a dual-threat scenario for victims. DarkCloud employs polymorphic code that constantly changes its signature to evade detection by traditional antivirus solutions, while its modular architecture allows attackers to customise payloads for specific targets. The malware spreads through weaponised PDF attachments, compromised software updates, and exploits in unpatched VPN vulnerabilities. Early victims include healthcare providers, educational institutions, and mid-sized enterprises across North America and Europe.

Cybersecurity experts note DarkCloud's concerning ability to remain dormant for weeks before activating, during which it maps network infrastructure and harvests credentials. The FBI's Cyber Division has issued a flash alert warning organisations to update endpoint protection systems and conduct security awareness training. With its rapid evolution and multi-stage attack chain, DarkCloud represents one of the most formidable cyber threats to emerge in 2025, demanding immediate attention from security teams globally.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://rexorvc0.com/2025/03/31/DarkCloud/

INTRODUCTION

CISA ALERTS ON ACTIVELY EXPLOITED CISCO ZERO-DAY FLAW

HUNTERS INTERNATIONAL RANSOMWARE TARGETS CRITICAL SECTORS

APPLE PATCHES ACTIVELY EXPLOITED ZERO-DAYS IN OLDER DEVICES

TSARBOT TROJAN HIJACKS BANKING DATA WITH FAKE LOGIN SCREENS

CRAZYHUNTER LAUNCHES TARGETED DOUBLE-EXTORTION ATTACKS

DARKCLOUD MALWARE THREATENS WITH ADVANCED EVASION TACTICS

QILIN RANSOMWARE EXPLOITS SCREENCONNECT IN GLOBAL ATTACKS

FMLN RANSOMWARE LAUNCHES DOUBLE ATTACK ON BUSINESSES

PELDOX RANSOMWARE LOCKS FILES IN 72-HOUR EXTORTION SCHEME

CHINESE HACKERS EXPLOIT IVANTI VPN FLAWS FOR CYBERESPIONAGE

Qilin ransomware's global attack spree exploits ScreenConnect flaws

Sophos Managed Detection and Response (MDR) has uncovered an aggressive campaign by Qilin ransomware affiliates targeting vulnerable ScreenConnect servers worldwide. The attackers are exploiting unpatched systems (CVE-2024-1709 and CVE-2024-1708) to deploy ransomware, with healthcare, manufacturing, and IT services as primary targets. Researchers observed the threat actors using living-off-the-land techniques, leveraging legitimate tools like AnyDesk and PowerShell for lateral movement before encryption. The attacks follow a disturbing pattern: initial access via ScreenConnect vulnerabilities, credential harvesting, network reconnaissance, and eventual ransomware deployment – often within 72 hours of infiltration. Qilin operators demand ransoms up to $5 million while threatening data leaks, a hallmark of their double-extortion strategy.

Researchers have warned that over 2,300 servers remain exposed, urging immediate patching and network segmentation. This campaign highlights how ransomware groups increasingly weaponise enterprise software flaws, with ConnectWise's ScreenConnect joining a growing list of managed service provider (MSP) tools abused in cyberattacks. Organisations using ScreenConnect must apply the February 2024 patches immediately to avoid compromise.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Generic, ScreenConnect

Source - https://news.sophos.com/en-us/2025/04/01/sophos-mdr-tracks-ongoing-campaign-by-qilin-affiliates-targeting-screenconnect/

New FMLN ransomware emerges as growing threat to businesses and consumers

Cybersecurity experts are warning about a dangerous new ransomware strain called FMLN that is rapidly infecting systems worldwide. Unlike typical ransomware, FMLN employs a dual attack strategy – encrypting files while also stealing sensitive data for potential extortion. The malware primarily spreads through malicious email attachments disguised as invoices or shipping notifications, exploiting human curiosity to gain entry. Once activated, FMLN uses AES-256 encryption to lock documents, databases, and multimedia files while establishing persistence through Windows Registry modifications. Victims receive ransom demands ranging from $500 to $50,000 in Bitcoin, with threats to leak stolen data on dark web forums if payments aren’t made. Recent attacks have targeted small-to-medium businesses, particularly in healthcare, legal services, and retail sectors.

Security analysts note FMLN’s concerning ability to disable backup systems and evade detection by common antivirus programs. Experts recommend immediate patching of systems, employee phishing awareness training, and maintaining offline backups as critical defences against this evolving threat. The emergence of FMLN underscores the continuing sophistication of ransomware attacks in 2024.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

INTRODUCTION | CISA ALERTS ON ACTIVELY EXPLOITED CISCO ZERO-DAY FLAW | HUNTERS INTERNATIONAL RANSOMWARE TARGETS CRITICAL SECTORS | APPLE PATCHES ACTIVELY EXPLOITED ZERO-DAYS IN OLDER DEVICES | TSARBOT TROJAN HIJACKS BANKING DATA WITH FAKE LOGIN SCREENS | CRAZYHUNTER LAUNCHES TARGETED DOUBLE-EXTORTION ATTACKS | DARKCLOUD MALWARE THREATENS WITH ADVANCED EVASION TACTICS | QILIN RANSOMWARE EXPLOITS SCREENCONNECT IN GLOBAL ATTACKS | FMLN RANSOMWARE LAUNCHES DOUBLE ATTACK ON BUSINESSES | PELDOX RANSOMWARE LOCKS FILES IN 72-HOUR EXTORTION SCHEME | CHINESE HACKERS EXPLOIT IVANTI VPN FLAWS FOR CYBERESPIONAGE

Peldox ransomware strikes with sophisticated encryption and stealth tactics

A dangerous new ransomware variant called Peldox has emerged, targeting both individual users and businesses with advanced file-locking capabilities. Cybersecurity analysts report that Peldox employs a combination of RSA and AES-256 encryption algorithms to securely lock victims' files while evading detection through sophisticated obfuscation techniques. The malware primarily spreads through malicious email attachments and compromised software downloads, often disguised as legitimate productivity tools or document files. Once executed, Peldox scans the system for valuable data files – including documents, databases, images, and backups – before encrypting them with a unique key for each victim. The ransomware then drops a ransom note demanding payment in cryptocurrency, typically ranging from $1,000 to $50,000, with threats to permanently delete decryption keys if payment isn't made within 72 hours.

Security experts warn that Peldox demonstrates skill in disabling security software and deleting shadow copies, making recovery without backups nearly impossible. The emergence of Peldox highlights the continuing evolution of ransomware threats in 2024, with attackers developing more sophisticated methods to maximise their payouts while minimising detection.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

INTRODUCTION | CISA ALERTS ON ACTIVELY EXPLOITED CISCO ZERO-DAY FLAW | HUNTERS INTERNATIONAL RANSOMWARE TARGETS CRITICAL SECTORS | APPLE PATCHES ACTIVELY EXPLOITED ZERO-DAYS IN OLDER DEVICES | TSARBOT TROJAN HIJACKS BANKING DATA WITH FAKE LOGIN SCREENS | CRAZYHUNTER LAUNCHES TARGETED DOUBLE-EXTORTION ATTACKS | DARKCLOUD MALWARE THREATENS WITH ADVANCED EVASION TACTICS | QILIN RANSOMWARE EXPLOITS SCREENCONNECT IN GLOBAL ATTACKS | FMLN RANSOMWARE LAUNCHES DOUBLE ATTACK ON BUSINESSES | PELDOX RANSOMWARE LOCKS FILES IN 72-HOUR EXTORTION SCHEME | CHINESE HACKERS EXPLOIT IVANTI VPN FLAWS FOR CYBERESPIONAGE

Hackers exploit critical Ivanti vulnerabilities in global espionage campaign

Google Cloud’s Mandiant has uncovered a widespread cyberespionage campaign by Chinese state-linked actors exploiting two critical Ivanti vulnerabilities (CVE-2023-46805 and CVE-2024-21887) to infiltrate global organisations. The attacks, attributed to a China-nexus threat group tracked as UNC5221, target government, technology, and defence sectors across North America, Europe, and Asia. Hackers are weaponising these Ivanti Connect Secure VPN flaws to bypass authentication, deploy web shells, and establish persistent access to victim networks. Mandiant observed the group using novel malware like LITTLELAMB.WOOLTEA to evade detection while exfiltrating sensitive data. Despite patches being available since January 2024, thousands of unpatched systems remain vulnerable. The campaign highlights China’s continued focus on exploiting edge devices like VPNs for intelligence gathering.

Cybersecurity agencies urge immediate patching of Ivanti systems, network segmentation, and credential rotation. This operation marks one of the most aggressive exploitation campaigns of 2024, demonstrating nation-state actors’ increasing sophistication in leveraging enterprise vulnerabilities for strategic advantage.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Generic, Ivanti

Source - https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability

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.