TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MARCH 18, 2025

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today’s fast-paced digital landscape, proactive cybersecurity is a necessity for organisations in every sector. Our weekly Cyber Threat Intelligence (CTI) reports provide vital insights into emerging threats, vulnerabilities, and attack trends, equipping businesses to bolster their defences and stay ahead of evolving risks.

Combining expert analysis with actionable strategies, we empower clients to anticipate, detect, and mitigate potential threats before they escalate. This proactive approach not only protects critical digital assets but also ensures operational continuity and enhances stakeholder trust. With our CTI reports, organisations can cultivate lasting cyber resilience, fostering security and confidence in an increasingly unpredictable digital world.

Suspected Iranian hackers exploit Microsoft and cloud providers globally

In a recent global cyberespionage campaign, suspected Iranian state-backed hackers have targeted organisations by exploiting vulnerabilities in Microsoft and major cloud service providers. Dubbed CloudEagle, the operation leverages stolen credentials and sophisticated techniques to infiltrate networks, primarily focusing on telecommunications, defence, and technology sectors. The attackers utilised compromised Microsoft 365 accounts and abused cloud infrastructure to gain unauthorised access, exfiltrate sensitive data, and maintain persistence within victim systems. Security researchers have linked the campaign to APT34, a notorious Iranian hacking group known for its advanced cyber operations.

This campaign underscores the growing trend of nation-state actors exploiting cloud platforms for espionage. Experts urge organisations to implement multi-factor authentication (MFA), monitor account activity, and patch vulnerabilities promptly to mitigate risks. As geopolitical tensions rise, such attacks highlight the critical need for robust cybersecurity measures in an increasingly interconnected digital landscape.

ATTACK TYPE	Malware	SECTOR	Defence, telecommunication, IT
REGION	UAE	APPLICATION	Generic

Source - https://thehackernews.com/2025/03/suspected-iranian-hackers-used.html

Broadcom warns of critical vulnerability in enterprise software

Broadcom has issued a critical security advisory, warning customers of a high-severity vulnerability in its enterprise software that could allow attackers to execute arbitrary code or cause system crashes. The flaw affects multiple versions of the software and poses a significant risk to organisations using the platform. The vulnerability stems from improper input validation, enabling unauthenticated remote attackers to exploit the system. Successful exploitation could lead to unauthorised access, data breaches, or service disruptions. Broadcom has released patches to address the issue and is urging all users to update their systems immediately.

The advisory highlights the growing threat of vulnerabilities in enterprise software, emphasising the need for proactive security measures. Organisations are advised to monitor their systems, apply patches promptly, and implement additional safeguards to mitigate potential risks. Broadcom's swift response underscores the importance of vendor vigilance in combating cyber threats.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	VMware ESXi, VMware Fusion, VMware Workstation

Source - https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390

Typosquatted Go packages found delivering malware loaders to threaten developers

A recent investigation has uncovered a malicious campaign involving typosquatted Go packages designed to deliver malware loaders. Typosquatting, a technique where attackers mimic legitimate package names with slight misspellings, has been used to trick developers into downloading malicious codes. The campaign targets the Go programming language ecosystem, with packages like go-tools and go-utils being impersonated. Once installed, these packages deploy a malware loader capable of executing additional malicious payloads, potentially compromising systems and stealing sensitive data.

Research highlights the growing sophistication of supply chain attacks, emphasising the need for developers to verify package authenticity and use tools to detect typosquatting. The discovery underscores the importance of vigilance in open-source ecosystems, where such attacks can have far-reaching consequences. Developers are urged to review dependencies carefully and adopt security measures to mitigate risks. This incident serves as a stark reminder of the evolving threats in software supply chains.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	macOS, Linux

Source - https://socket.dev/blog/typosquatted-go-packages-deliver-malware-loader

INTRODUCTION | IRANIAN HACKERS TARGET MICROSOFT AND CLOUD PROVIDERS | BROADCOM IDENTIFIES VULNERABILITY IN ENTERPRISE SOFTWARE | TYPOSQUATTED GO PACKAGES DELIVERING MALWARE LOADERS | CHINESE CYBER ATTACKERS INITIATE OPERATION SEA ELEPHANT | AI-DRIVEN RANSOMWARE GROUP FUNKSEC EMERGES AS A THREAT | LUMMASTEALER DISGUISES AS FAKE RECAPTCHA TO TARGET USERS | BORAMAE RANSOMWARE EMERGES AS A THREAT, TARGETS VICTIMS | BADBOX MALWARE DISRUPTED IN 50K INFECTED ANDROID DEVICES | GOLANG-BASED EBYTE RANSOMWARE THREATENS SYSTEMS GLOBALLY | LITHIUMWARE EMERGES WITH DATA EXFILTRATION CAPABILITIES

Chinese threat actors driving cyberespionage campaign with Operation Sea Elephant

A recent report has revealed Operation Sea Elephant, a cyberespionage campaign targeting the Indian Ocean region. Linked to Chinese state-backed hackers, the operation employs advanced techniques to infiltrate government, military, and critical infrastructure entities. The attackers, dubbed The Dying Walrus, use custom malware, phishing emails, and compromised websites to gain access to sensitive systems. Their tools include a sophisticated backdoor capable of exfiltrating data and maintaining persistent access. The campaign focuses on geopolitical intelligence gathering, with victims spanning multiple countries in the region.

This operation highlights the growing threat of state-sponsored cyberespionage in strategically significant areas. Experts urge organisations to enhance cybersecurity measures, including network monitoring, employee training, and threat intelligence sharing. As geopolitical tensions rise, such campaigns underscore the critical need for robust defences against increasingly sophisticated cyber threats.

ATTACK TYPE	Cyberespionage	SECTOR	All
REGION	South Asia	APPLICATION	Windows

Source - https://ti.qianxin.com/blog/articles/operation-sea-elephant-the-dying-walrus-wandering-the-indian-ocean-en/

FunkSec emerges as an AI-driven ransomware group with affiliate network

A new ransomware group, FunkSec, has been found leveraging AI and an affiliate-powered model to amplify its attacks. The group uses AI to automate and optimise its operations, including phishing campaigns, vulnerability scanning, and payload deployment, making it a formidable threat to businesses worldwide. FunkSec operates on a Ransomware-as-a-Service (RaaS) model, recruiting affiliates to distribute its ransomware in exchange for a share of the profits. This approach allows the group to scale rapidly and target a wide range of industries. Victims are extorted through double extortion tactics, where data is encrypted and stolen, threatening public release unless a ransom is paid.

The emergence of FunkSec highlights the evolving sophistication of ransomware groups, combining AI and affiliate networks to maximise impact. Businesses are urged to strengthen defences, implement robust backup strategies, and educate employees to mitigate the growing threat of AI-driven cyberattacks.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.bitdefender.com/en-us/blog/businessinsights/funksec-an-ai-centric-and-affiliate-powered-ransomware-group

INTRODUCTION | IRANIAN HACKERS TARGET MICROSOFT AND CLOUD PROVIDERS | BROADCOM IDENTIFIES VULNERABILITY IN ENTERPRISE SOFTWARE | TYPOSQUATTED GO PACKAGES DELIVERING MALWARE LOADERS | CHINESE CYBER ATTACKERS INITIATE OPERATION SEA ELEPHANT | AI-DRIVEN RANSOMWARE GROUP FUNKSEC EMERGES AS A THREAT | LUMMASTEALER DISGUISES AS FAKE RECAPTCHA TO TARGET USERS | BORAMAE RANSOMWARE EMERGES AS A THREAT, TARGETS VICTIMS | BADBOX MALWARE DISRUPTED IN 50K INFECTED ANDROID DEVICES | GOLANG-BASED EBYTE RANSOMWARE THREATENS SYSTEMS GLOBALLY | LITHIUMWARE EMERGES WITH DATA EXFILTRATION CAPABILITIES

LummaStealer malware disguised as fake reCAPTCHA targets online users

A new phishing campaign has been uncovered, deploying the notorious LummaStealer malware through fake reCAPTCHA pages. Cybercriminals are luring victims with seemingly legitimate reCAPTCHA verification prompts on compromised websites, tricking users into downloading malicious payloads. LummaStealer, known for stealing sensitive data such as credentials, cryptocurrency wallets, and browser cookies, is being distributed via these deceptive pages. Once installed, the malware exfiltrates critical information, putting individuals and businesses at risk of financial loss and identity theft.

Security experts warn that the campaign exploits user trust in reCAPTCHA systems, highlighting the need for heightened vigilance. Users are advised to verify website authenticity, avoid clicking on suspicious prompts, and keep security software updated. This incident underscores the evolving tactics of cybercriminals, who continue to innovate in their efforts to bypass defences and exploit unsuspecting victims.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.gdatasoftware.com/blog/2025/03/38154-lummastealer-fake-recaptcha

INTRODUCTION
IRANIAN HACKERS TARGET MICROSOFT AND CLOUD PROVIDERS
BROADCOM IDENTIFIES VULNERABILITY IN ENTERPRISE SOFTWARE
TYPOSQUATTED GO PACKAGES DELIVERING MALWARE LOADERS
CHINESE CYBER ATTACKERS INITIATE OPERATION SEA ELEPHANT
AI-DRIVEN RANSOMWARE GROUP FUNKSEC EMERGES AS A THREAT
LUMMASTEALER DISGUISES AS FAKE RECAPTCHA TO TARGET USERS
BORAMAE RANSOMWARE EMERGES AS A THREAT, TARGETS VICTIMS
BADBOX MALWARE DISRUPTED IN 50K INFECTED ANDROID DEVICES
GOLANG-BASED EBYTE RANSOMWARE THREATENS SYSTEMS GLOBALLY
LITHIUMWARE EMERGES WITH DATA EXFILTRATION CAPABILITIES

Boramae ransomware emerges as a growing Threat, targets victims globally

A new ransomware strain, Boramae, has been identified, targeting individuals and organisations worldwide. Known for its aggressive encryption tactics, Boramae locks victims' files and demands ransom payments in cryptocurrency for decryption. The ransomware is distributed through phishing emails, malicious attachments, and exploit kits, making it a significant threat to unprepared users. Cybersecurity experts have analysed Boramae's behaviour, revealing its use of advanced encryption algorithms to render files inaccessible. The ransomware also leaves a ransom note, instructing victims on payment procedures and threatening permanent data loss if demands are not met.

Experts advise against paying ransoms, as it fuels further criminal activity. Instead, they recommend regular data backups, robust antivirus software, and employee training to mitigate risks. The emergence of Boramae underscores the escalating ransomware threat, highlighting the need for proactive cybersecurity measures to protect sensitive data and systems.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyclonis.com/remove-boramae-ransomware/, https://www.cyfirma.com/research/boramae-ransomware/

INTRODUCTION

IRANIAN HACKERS TARGET MICROSOFT AND CLOUD PROVIDERS

BROADCOM IDENTIFIES VULNERABILITY IN ENTERPRISE SOFTWARE

TYPOSQUATTED GO PACKAGES DELIVERING MALWARE LOADERS

CHINESE CYBER ATTACKERS INITIATE OPERATION SEA ELEPHANT

AI-DRIVEN RANSOMWARE GROUP FUNKSEC EMERGES AS A THREAT

LUMMASTEALER DISGUISES AS FAKE RECAPTCHA TO TARGET USERS

BORAMAE RANSOMWARE EMERGES AS A THREAT, TARGETS VICTIMS

BADBOX MALWARE DISRUPTED IN 50K INFECTED ANDROID DEVICES

GOLANG-BASED EBYTE RANSOMWARE THREATENS SYSTEMS GLOBALLY

LITHIUMWARE EMERGES WITH DATA EXFILTRATION CAPABILITIES

BadBox malware disrupted on infected Android devices in global takedown

In a significant cybersecurity operation, the notorious BadBox malware has been successfully disrupted on over 500,000 infected Android devices worldwide. The malware, which infiltrated devices through pre-installed software on low-cost smartphones, enabled backdoor access, ad fraud, and unauthorised data exfiltration. The takedown was orchestrated by a coalition of cybersecurity firms, law enforcement agencies, and tech companies. BadBox's infrastructure was dismantled, preventing further exploitation of compromised devices. The malware primarily targeted users in the US, Europe, and Asia, highlighting the global scale of the threat.

Authorities urge affected users to update their devices, remove suspicious apps, and install reputable antivirus software. This operation underscores the risks of pre-installed malware and the importance of securing supply chains. While the disruption marks a major victory, experts warn that similar threats remain, emphasising the need for continued vigilance in the mobile security landscape.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Android

Source - https://www.bleepingcomputer.com/news/security/badbox-malware-disrupted-on-500k-infected-android-devices/

EByte ransomware emerges as a new Golang-based threat targeting systems

A new ransomware variant, EByte, has been identified, written in the Go programming language, making it a versatile and cross-platform threat. According to research, EByte targets both Windows and Linux systems, encrypting files and demanding ransom payments in cryptocurrency for decryption. The ransomware employs advanced encryption algorithms, ensuring files remain inaccessible without the attacker's decryption key. EByte also deletes shadow copies to prevent recovery, leaving victims with limited options. Its Go-based architecture allows for easy adaptation to different operating systems, increasing its potential reach.

EByte is distributed through phishing campaigns, malicious attachments, and exploit kits, targeting organisations globally. Cybersecurity experts recommend regular data backups, robust endpoint protection, and employee training to mitigate risks. The emergence of EByte highlights the growing trend of ransomware leveraging modern programming languages for cross-platform attacks, underscoring the need for heightened vigilance and proactive defence strategies in an evolving threat landscape.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows, Linux

Source - https://www.cyfirma.com/research/go-language-based-ebyte-ransomware-a-brief-analysis/

LithiumWare ransomware emerges as a new threat with data exfiltration capabilities

A new ransomware strain, LithiumWare, has been identified, combining file encryption with data exfiltration to intensify its impact. According to research, LithiumWare not only encrypts victims' files but also steals sensitive data, threatening to leak it unless a ransom is paid. The ransomware targets organisations across various sectors, exploiting vulnerabilities in network security to gain access. Once inside, it encrypts critical files and exfiltrates data, using double extortion tactics to pressure victims into paying. LithiumWare's operators demand payment in cryptocurrency, making transactions difficult to trace.

Cybersecurity experts warn that LithiumWare's dual-threat approach increases the stakes for victims, as non-compliance could lead to reputational damage and regulatory penalties. Organisations are advised to strengthen network defences, implement robust backup solutions, and conduct regular security audits. The emergence of LithiumWare highlights the evolving sophistication of ransomware, emphasising the need for proactive measures to combat these escalating threats.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyfirma.com/research/lithiumware-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.