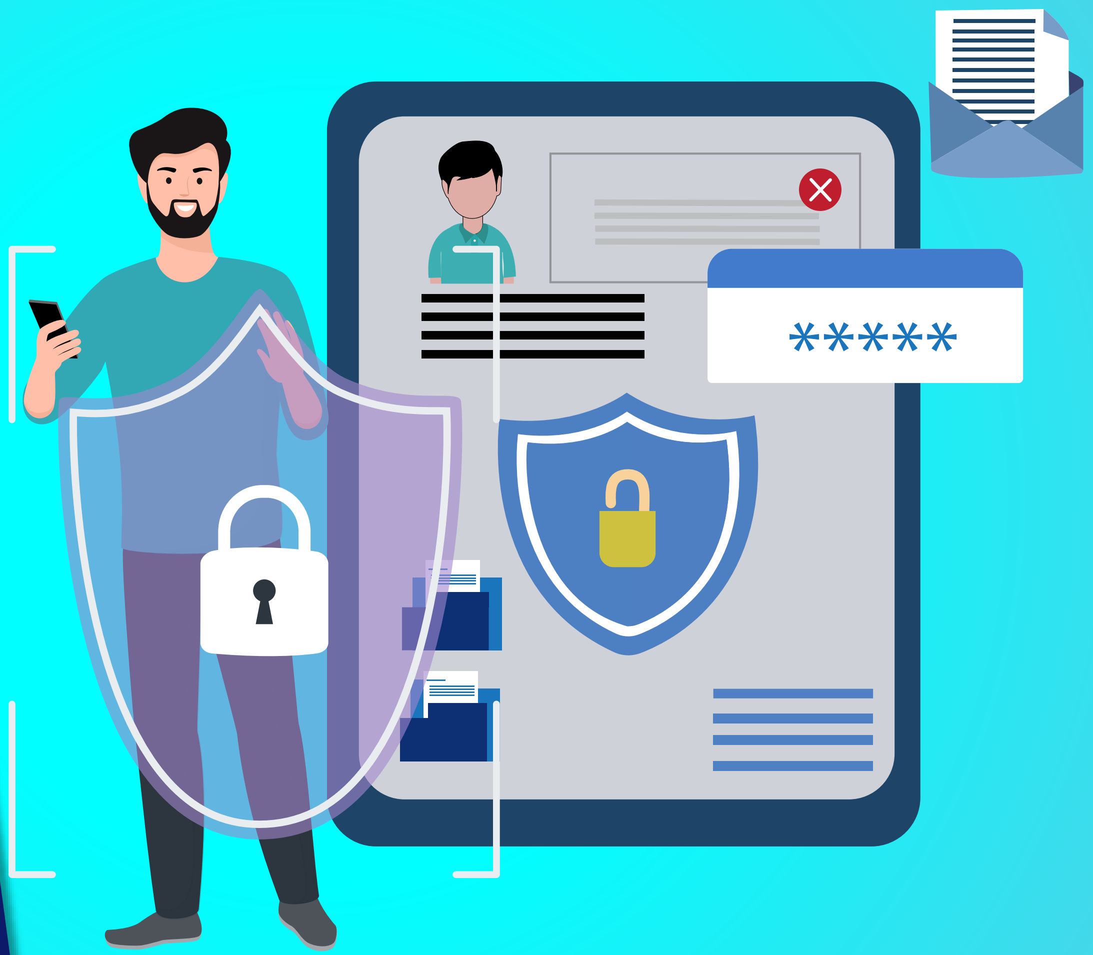
TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: FEBRUARY 11, 2025



TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today’s dynamic cyber environment, protecting critical systems is essential for individuals, businesses, and governments alike. Cyber threats pose significant risks, including financial losses, reputational damage, and operational disruptions.

Our weekly Cyber Threat Intelligence (CTI) report delivers actionable insights on emerging threats, empowering organisations to bolster security, reduce risks, and enhance cyber resilience. Backed by expert advisory services, this intelligence-driven approach identifies vulnerabilities and fortifies defence mechanisms. Stay proactive against cyber risks with cutting-edge knowledge and tools, safeguarding your digital assets and ensuring a secure future.

Sophisticated phishing campaign exploits fake Amazon PDFs

A recent phishing campaign has been uncovered, leveraging malicious PDF files disguised as Amazon-related documents to deceive users and steal sensitive information. Cybersecurity researchers have identified this sophisticated attack, which involves emails containing seemingly legitimate PDF attachments. Once opened, these files prompt users to click on embedded links, redirecting them to fraudulent websites designed to harvest login credentials, financial data, and other personal information. The attackers exploit Amazon’s trusted brand to increase the likelihood of success, capitalising on the platform’s widespread use. This campaign highlights the evolving tactics of cybercriminals, who are increasingly using social engineering and file-based attacks to bypass traditional email security measures.

Experts urge vigilance, advising users to verify email sources, avoid clicking on suspicious links, and employ multi-factor authentication (MFA). Organisations are encouraged to enhance employee training and deploy advanced threat detection tools to mitigate such risks. This incident underscores the critical need for robust cybersecurity practices in an era of increasingly sophisticated phishing schemes.

ATTACK TYPE	Phishing	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.darkreading.com/cyberattacks-data-breaches/phishing-campaign-malicious-amazon-pdfs

INTRODUCTION
PHISHING CAMPAIGN TARGETS USERS WITH FAKE PDFS
STEALTHY TORNET BACKDOOR COMPROMISES USERS
MANIA CRYPTER ENCRYPTION ATTACKS WREAK HAVOC
WINDOWS LOCKER THREATENS DATA SECURITY
EBYTE LOCKER EMERGES AS A NEW RANSOMWARE THREAT
GLOBAL ORGANISATIONS ATTACKED BY THE LYNX RANSOMWARE
INTERLOCK RANSOMWARE CARRIES OUT CYBERATTACKS
SENSITIVE DATA OF MILLIONS OF GLOBAL USERS EXPOSED
SOUTH ASIAN ORGANISATIONS COME UNDER CYBERESPIONAGE THREAT
INNOK RANSOMWARE COMPROMISES DATA SECURITY AND THREATENS USERS

New Tornet backdoor campaign targets victims with stealthy malware

A newly discovered malware campaign, dubbed Tornet, has been uncovered by cybersecurity researchers, deploying a sophisticated backdoor to infiltrate and control victims' systems. The campaign, attributed to a yet-unidentified threat actor, leverages phishing emails and malicious documents to deliver the Tornet backdoor, which enables remote access, data exfiltration, and further malware deployment. Tornet stands out for its modular design, allowing attackers to customise its functionality based on their objectives. Once installed, it establishes communication with command-and-control (C2) servers, operating stealthily to avoid detection. The malware also employs anti-analysis techniques, making it harder for security tools to identify and mitigate.

This campaign highlights the growing sophistication of cybercriminals, who are increasingly using advanced tactics to bypass defences. Organisations are urged to enhance email security, conduct employee training, and deploy robust endpoint protection to guard against such threats. The discovery of Tornet underscores the critical need for vigilance in an ever-evolving threat landscape.

ATTACK TYPE	Malware	SECTOR	All
REGION	Germany, Poland	APPLICATION	Windows

Source - https://blog.talosintelligence.com/new-tornet-backdoor-campaign/

Mania Crypter ransomware strikes with encryption attacks

A new ransomware variant called Mania Crypter is wreaking havoc by encrypting victims' files and demanding ransom payments for decryption. Distributed through malicious email attachments, fake software updates, and exploit kits, this ransomware targets both individuals and businesses, locking critical data and leaving victims with limited options. Mania Crypter employs strong encryption algorithms, making file recovery without the attackers' decryption key nearly impossible. It also leaves a ransom note instructing victims to pay in cryptocurrency to regain access to their data. Cybersecurity experts warn against paying the ransom, as it fuels criminal activity and does not guarantee file recovery.

To combat this threat, users are advised to maintain regular backups, avoid suspicious email attachments, and keep software updated. Anti-malware tools can help detect and remove Mania Crypter, but prevention remains the best defence. As ransomware attacks grow more sophisticated, staying vigilant and proactive is crucial to safeguarding sensitive information.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.cyclonis.com/remove-mania-crypter-ransomware/

Windows Locker ransomware emerges to threaten data security

A new ransomware strain, Windows Locker, has been identified by cybersecurity researchers, targeting systems to encrypt files and demand ransom payments. Distributed through phishing emails, malicious downloads, and exploit kits, this ransomware locks users out of their data, displaying a ransom note with payment instructions in cryptocurrency. Windows Locker employs advanced encryption techniques, making data recovery without the attackers' key nearly impossible. It primarily targets individuals and small businesses, exploiting weak security measures. Researchers warn that paying the ransom does not guarantee file restoration and encourages further criminal activity.

To mitigate risks, experts recommend regular data backups, avoiding suspicious email attachments, and keeping systems updated with the latest security patches. Robust antivirus software can help detect and remove the ransomware, but proactive measures remain the best defence. The emergence of Windows Locker underscores the growing sophistication of ransomware attacks, highlighting the urgent need for enhanced cybersecurity practices to protect sensitive information.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyfirma.com/research/windows-locker-ransomware/

Ebyte Locker ransomware compromises users globally

A newly identified ransomware variant, Ebyte Locker, is causing widespread concern by encrypting victims’ files and demanding ransom payments for their release. Distributed through phishing emails, malicious attachments, and fake software updates, this ransomware targets both individuals and businesses, locking critical data and leaving victims with limited options. Ebyte Locker employs robust encryption algorithms, making file recovery without the attackers’ decryption key nearly impossible. It leaves a ransom note instructing victims to pay in cryptocurrency, often Bitcoin, to regain access to their files. Cybersecurity experts strongly advise against paying the ransom, as it fuels criminal activity and offers no guarantee of data recovery.

To protect against Ebyte Locker, users are urged to maintain regular backups, avoid suspicious email attachments, and keep software updated. Anti-malware tools can help detect and remove the ransomware, but prevention remains the best defence. As ransomware attacks grow more sophisticated, staying vigilant and proactive is essential to safeguarding sensitive information.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.cyclonis.com/remove-ebyte-locker-ransomware/

Lynx ransomware targets global enterprises

A sophisticated ransomware operation, dubbed Lynx, has been exposed by cybersecurity experts, revealing a highly organised campaign targeting global enterprises. Lynx ransomware infiltrates systems through phishing emails, malicious attachments, and exploit kits, encrypting critical data and demanding hefty ransom payments in cryptocurrency for decryption. What sets Lynx apart is its advanced evasion techniques, including anti-analysis measures and the use of legitimate software tools to avoid detection. The attackers also employ double extortion tactics, threatening to leak stolen data if the ransom is not paid. This approach has proven effective, with several high-profile victims reportedly paying to regain access to their systems.

Analysts warn that Lynx is part of a growing trend of ransomware-as-a-service (RaaS) operations, where cybercriminals collaborate to maximise impact. To mitigate risks, organisations are advised to enhance email security, conduct regular employee training, and maintain robust backup protocols. The emergence of Lynx underscores the escalating threat of ransomware and the urgent need for proactive cybersecurity measures.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	VMware ESXi, Windows, Linux

Source - https://www.group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/

Sophisticated cyberattacks carried out by Interlock ransomware

A recent analysis by cybersecurity experts has uncovered the inner workings of the Interlock ransomware, a highly advanced threat targeting organisations worldwide. Distributed through phishing campaigns and malicious attachments, Interlock encrypts victims' files and demands ransom payments in cryptocurrency for decryption. The ransomware employs a multi-layered approach, using robust encryption algorithms and anti-analysis techniques to evade detection. It also leverages double extortion tactics, threatening to leak sensitive data if the ransom is not paid. Researchers highlight Interlock's use of custom tools and its ability to disable security software, making it particularly dangerous.

Victims are urged not to pay the ransom, as it encourages further criminal activity and offers no guarantee of data recovery. Instead, organisations are advised to implement comprehensive email security, conduct regular employee training, and maintain up-to-date backups. The emergence of Interlock underscores the growing sophistication of ransomware attacks, emphasising the need for proactive cybersecurity measures to protect against evolving threats.

ATTACK TYPE	Ransomware	SECTOR	Healthcare
REGION	Global	APPLICATION	Windows

Source - https://any.run/cybersecurity-blog/interlock-ransomware-attack-analysis/

Major data breach exposes sensitive information of millions

In a shocking revelation, cybersecurity researchers have uncovered a massive data breach affecting millions of users worldwide. The breach involves the unauthorised access and exposure of sensitive personal information, including names, email addresses, phone numbers, and financial details. The compromised data is believed to have originated from a popular online platform, although the exact source remains under investigation. Early reports suggest that the breach may have been the result of a sophisticated cyberattack exploiting vulnerabilities in the platform’s security infrastructure.

Cybersecurity experts are urging affected users to change their passwords immediately and enable two-factor authentication (2FA) on all accounts. They also recommend monitoring financial statements for any suspicious activity and being cautious of phishing attempts, as cybercriminals often use stolen data for fraudulent purposes. This incident highlights the critical importance of robust cybersecurity measures and serves as a stark reminder of the ever-present threat of data breaches in our increasingly digital world. Authorities are currently investigating the breach, and further updates are expected as more information comes to light.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows, Linux

Source - https://x.com/500mk500/status/1884230787391971474

INTRODUCTION | PHISHING CAMPAIGN TARGETS USERS WITH FAKE PDFS | STEALTHY TORNET BACKDOOR COMPROMISES USERS | MANIA CRYPTER ENCRYPTION ATTACKS WREAK HAVOC | WINDOWS LOCKER THREATENS DATA SECURITY | EBYTE LOCKER EMERGES AS A NEW RANSOMWARE THREAT | GLOBAL ORGANISATIONS ATTACKED BY THE LYNX RANSOMWARE | INTERLOCK RANSOMWARE CARRIES OUT CYBERATTACKS | SENSITIVE DATA OF MILLIONS OF GLOBAL USERS EXPOSED | SOUTH ASIAN ORGANISATIONS COME UNDER CYBERESPIONAGE THREAT | INNOK RANSOMWARE COMPROMISES DATA SECURITY AND THREATENS USERS

Espionage campaign targets South Asian entities stealthily

A sophisticated espionage campaign is targeting government and private sector entities across South Asia. The operation, believed to be state-sponsored, employs advanced malware to infiltrate networks, steal sensitive data, and conduct surveillance. Attackers use phishing emails with malicious attachments and exploit vulnerabilities in widely used software to gain access. The campaign leverages custom tools, including remote access trojans (RATs) and credential stealers, to exfiltrate confidential information. Researchers highlight its stealthy nature, with attackers frequently updating tactics to evade detection.

This operation underscores the growing threat of cyberespionage in geopolitically sensitive regions. Organisations are urged to enhance email security, patch vulnerabilities, and deploy advanced threat detection systems. Regular employee training on recognising phishing attempts is also critical. As cyber threats evolve, this campaign serves as a stark reminder of the need for robust cybersecurity measures to protect sensitive data and maintain national security.

ATTACK TYPE	Malware, cyberespionage	SECTOR	Government, telecommunications
REGION	South Asia	APPLICATION	MySQL, Windows, Apache Tomcat

Source - https://unit42.paloaltonetworks.com/espionage-campaign-targets-south-asian-entities/

INTRODUCTION | PHISHING CAMPAIGN TARGETS USERS WITH FAKE PDFS | STEALTHY TORNET BACKDOOR COMPROMISES USERS | MANIA CRYPTER ENCRYPTION ATTACKS WREAK HAVOC | WINDOWS LOCKER THREATENS DATA SECURITY | EBYTE LOCKER EMERGES AS A NEW RANSOMWARE THREAT | GLOBAL ORGANISATIONS ATTACKED BY THE LYNX RANSOMWARE | INTERLOCK RANSOMWARE CARRIES OUT CYBERATTACKS | SENSITIVE DATA OF MILLIONS OF GLOBAL USERS EXPOSED | BUTCHER SHOP PHISHING CAMPAIGN TARGETS ENTITIES GLOBALLY | INNOK RANSOMWARE COMPROMISES DATA SECURITY AND THREATENS USERS

Innok ransomware strikes users and threatens data security

A newly identified ransomware variant, Innok, is causing alarm by encrypting victims' files and demanding ransom payments for their release. Distributed through phishing emails, malicious attachments, and fake software updates, this ransomware targets both individuals and businesses, locking critical data and leaving victims with limited options. Innok employs robust encryption algorithms, making file recovery without the attackers' decryption key nearly impossible. It leaves a ransom note instructing victims to pay in cryptocurrency, often Bitcoin, to regain access to their files. Cybersecurity experts strongly advise against paying the ransom, as it fuels criminal activity and offers no guarantee of data recovery.

To protect against Innok, users are urged to maintain regular backups, avoid suspicious email attachments, and keep software updated. Anti-malware tools can help detect and remove the ransomware, but prevention remains the best defence. As ransomware attacks grow more sophisticated, staying vigilant and proactive is essential to safeguarding sensitive information.

ATTACK TYPE	Rnasomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyclonis.com/remove-innok-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.