TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: DECEMBER 17, 2024

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today’s shapeshifting landscape of escalating cyber threats, protecting critical systems and data is essential for individuals, businesses, and governments. Cyber disruptions can cause financial losses, reputational damage, and jeopardise operational security.

Our weekly Cyber Threat Intelligence (CTI) report offers actionable insights into emerging global threats to fortify your defences. Backed by expert advisory services, we provide strategies to safeguard IT assets against evolving risks. Stay proactive with our intelligence-driven approach, empowering your organisation to enhance its security posture, mitigate persistent threats, and ensure a resilient, secure future in the face of dynamic cyber challenges.

APT35 exploits fake recruitment sites in new cyberespionage campaign

APT35, an Iranian state-sponsored threat group linked to the Islamic Revolutionary Guard Corps (IRGC), has escalated its cyberespionage operations. Active since 2014, the group targets aerospace and semiconductor industries across the US, Thailand, UAE, and Israel. Analysis revealed APT35 leveraging fake recruitment and corporate websites to lure experts into downloading malicious programmes. A recent campaign involved a counterfeit aerospace job portal offering unusually high salaries. The site embedded a legitimate OneDrive programme (SignedConnection.exe) alongside malicious files (secur32.dll, Qt5Core.dll) to bypass detection.

The malicious module, written in C#, executes stealthy tasks, including registry modifications and silent malware execution. APT35 also utilised trusted platforms like Google Cloud and GitHub for hosting malicious content, further complicating detection. The group's sophisticated tactics underscore the increasing need for vigilance against targeted phishing campaigns in critical industries. Security experts urge potential victims to verify site authenticity before engaging.

ATTACK TYPE	Malware	SECTOR	All
REGION	Thailand, UAE, US	APPLICATION	Windows

Source - https://threatbook.io/blog/id/1095

Howling Scorpius ransomware emerges as a threat behind Akira

Emerging in early 2023, Howling Scorpius, the group behind Akira ransomware-as-a-service (RaaS), has quickly become one of the top five most active ransomware actors. Leveraging a double extortion strategy, the group exfiltrates sensitive data before encryption, pressuring victims to pay by threatening public data leaks. Targeting small- and medium-sized businesses across North America, Europe, and Australia, Howling Scorpius impacts sectors like education, government, technology, and manufacturing. They utilise encryptors for Windows, Linux, and ESXi hosts, consistently enhancing their toolset to escalate threats.

Operating a retro-styled TOR-based leak site, the group publicly lists non-compliant victims and shares stolen data via .torrent files. Their negotiation site allows victims to access ransom details using unique passwords. Since March 2023, Howling Scorpius has increasingly targeted US-based organisations, affecting industries from legal services to retail. Their evolving tactics highlight the critical need for robust cybersecurity measures to counter these growing threats.

ATTACK TYPE	Ransomware	SECTOR	Financial services, manufacturing, education, retail distribution
REGION	Australia, Europe, Canada, UK	APPLICATION	VMware ESXi, Windows, Linux

Source - https://unit42.paloaltonetworks.com/threat-assessment-howling-scorpius-akira-ransomware/

Celestial Stealer: A new malware-as-a-service threat

In December 2024, cybersecurity researchers uncovered the Celestial Stealer, a sophisticated JavaScript-based infostealer offered as malware as a service (MaaS) on Telegram. Targeting Windows 10 and 11 systems, it masquerades as legitimate Electron or NodeJS applications to infiltrate devices. Once installed, it exfiltrates sensitive data from Chromium- and Gecko-based browsers, as well as applications like Steam, Telegram, and cryptocurrency wallets such as Atomic and Exodus. The malware employs advanced obfuscation and anti-analysis techniques, including evasion based on specific system usernames and computer names, to avoid detection.

Notably, the malware can inject malicious code into Exodus and Discord applications. Operators market Celestial Stealer as “fully undetectable” (FUD), offering subscriptions on weekly, monthly, or lifetime bases, and continually update it to maintain its stealth. This discovery highlights the growing threat of MaaS platforms, which lower the barrier for cybercriminals to deploy complex malware, emphasising the need for robust cybersecurity measures to protect sensitive user data.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.trellix.com/en-in/blogs/research/anatomy-of-celestial-stealer-malware-as-a-service-revealed/

INTRODUCTION | APT35 DRIVING CYBERESPIONAGE CAMPAIGN | HOWLING SCORPIUS FAST EMERGING AS GLOBAL THREAT | CELESTIAL STEALER COMPROMISES APPS AND SYSTEMS | ZEPHYR MALWARE MINES MONERO COVERTLY | BRAIN CIPHER RANSOMWARE TARGETS INDONESIA | SOCKS5SYSTEMZ BOTNET GOES ON A RAMPAGE | PAYROLL PIRATES COMPROMISES SMBS IN THE US | TURLA MALWARE TARGETS ANDROID USERS | SOPHISTICATED MALWARE ATTACKS MANUFACTURING INDUSTRY | CHINESE HACKERS INSTRUMENTAL IN EXPLOITING US FIRM

Cryptomining malware Zephyr growing in stature

Researchers have uncovered Zephyr, a stealthy cryptocurrency mining malware targeting Windows systems. Designed for clandestine operations, Zephyr consumes system resources to mine Monero, impacting device performance while evading detection through advanced techniques. The malware infiltrates via malicious email attachments, fake software updates, and pirated downloads, often disguised as legitimate files. Zephyr employs sophisticated evasion methods, including dynamic configuration downloads from command-and-control (C2) servers and system profiling to bypass virtual environments. Once activated, it silently mines Monero, degrading system performance and escalating electricity costs.

Recent campaigns indicate Zephyr's widespread deployment, affecting individuals and organisations alike. Researchers recommend updating antivirus solutions, avoiding unverified downloads, and monitoring system performance for unusual activity. As cryptomining malwares evolve, proactive measures are essential to safeguard against threats like Zephyr.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://blogs.quickheal.com/crypto-mining-malware-zephyr/

INTRODUCTION | APT35 DRIVING CYBERESPIONAGE CAMPAIGN | HOWLING SCORPIUS FAST EMERGING AS GLOBAL THREAT | CELESTIAL STEALER COMPROMISES APPS AND SYSTEMS | ZEPHYR MALWARE MINES MONERO COVERTLY | BRAIN CIPHER RANSOMWARE TARGETS INDONESIA | SOCKS5SYSTEMZ BOTNET GOES ON A RAMPAGE | PAYROLL PIRATES COMPROMISES SMBS IN THE US | TURLA MALWARE TARGETS ANDROID USERS | SOPHISTICATED MALWARE ATTACKS MANUFACTURING INDUSTRY | CHINESE HACKERS INSTRUMENTAL IN EXPLOITING US FIRM

Brain Cipher ransomware shakes up Indonesia’s National Data Centre

In June 2024, the newly emerged ransomware group Brain Cipher launched a major cyberattack on Indonesia’s temporary National Data Centre, crippling over 200 government agencies and vital public services, including immigration and passport systems. The group demanded an $8 million ransom in Monero cryptocurrency for decryption keys and to prevent sensitive data leaks. Brain Cipher’s malware is linked to the leaked LockBit 3.0 builder, enabling the group to craft sophisticated ransomware. Employing a double extortion tactic, they exfiltrate data before encryption, leveraging a TOR-based leak site to pressure victims by threatening public exposure.

Indonesia initiated recovery efforts post-attack, successfully restoring services across key ministries without confirming ransom payment. The incident highlights the growing menace of ransomware groups like Brain Cipher and underscores the urgent need for fortified cybersecurity measures to safeguard critical infrastructure against such evolving threats.

ATTACK TYPE	Ransomware	SECTOR	Healthcare, manufacturing, government, education
REGION	Indonesia	APPLICATION	Windows

Source - https://www.sentinelone.com/anthology/brain-cipher/

Socks5Systemz botnet powers global proxy network for cybercriminals

The Socks5Systemz botnet, active since 2013, has compromised up to 250,000 devices globally, serving as the backbone for the PROXY.AM service launched in 2016. This service offers anonymous proxy exit nodes for illicit activities, leveraging infected systems as SOCKS5 proxies. Disseminated through malware loaders like PrivateLoader and Amadey, the botnet’s infrastructure spans over 50 servers across Europe, with notable presence in France, the Netherlands, Sweden, and Bulgaria.

Despite a decline in activity, Socks5Systemz still maintains 85,000 to 100,000 active daily bots. Its operators profit by selling proxy access to compromised devices, with subscriptions ranging from $1 to $4,000, payable in cryptocurrency. This long-running operation underscores the evolving sophistication of proxy-based cybercriminal networks and highlights the urgent need for robust cybersecurity defences to counter such threats, safeguarding devices from covert infiltration and exploitation.

ATTACK TYPE	Malware	SECTOR	All
REGION	Russia, India, Algeria, Brazil, Indonesia, Turkey, Ukraine, Vietnam	APPLICATION	Generic

Source - https://www.bitsight.com/blog/proxyam-powered-socks5systemz-botnet

INTRODUCTION | APT35 DRIVING CYBERESPIONAGE CAMPAIGN | HOWLING SCORPIUS FAST EMERGING AS GLOBAL THREAT | CELESTIAL STEALER COMPROMISES APPS AND SYSTEMS | ZEPHYR MALWARE MINES MONERO COVERTLY | BRAIN CIPHER RANSOMWARE TARGETS INDONESIA | SOCKS5SYSTEMZ BOTNET GOES ON A RAMPAGE | PAYROLL PIRATES COMPROMISES SMBS IN THE US | TURLA MALWARE TARGETS ANDROID USERS | SOPHISTICATED MALWARE ATTACKS MANUFACTURING INDUSTRY | CHINESE HACKERS INSTRUMENTAL IN EXPLOITING US FIRM

Payroll Pirates campaign targets small businesses in the US

A new cybercrime campaign, dubbed Payroll Pirates, has been targeting small- and medium-sized businesses (SMBs) across the US, exploiting vulnerable payroll systems to steal funds. Silent Push researchers uncovered the campaign, which leverages phishing emails designed to lure employees into clicking malicious links or downloading harmful attachments. The attackers disguise their messages as official communications, often impersonating legitimate companies to gain trust. Once victims interact with the malicious content, their credentials are harvested, granting attackers access to payroll accounts. The stolen credentials are then used to divert salaries and other funds to fraudulent accounts.

Researchers have traced this campaign to advanced phishing kits, frequently updated to evade detection. The impact of these attacks highlights the need for SMBs to implement robust security measures, such as multi-factor authentication and employee training on phishing awareness, to safeguard sensitive payroll data and protect against financial losses.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.silentpush.com/blog/payroll-pirates/

Russia-linked Turla uses Pakistani malware to target Android devices

Cybersecurity researchers have uncovered a sophisticated campaign by the Russia-linked Turla APT group, repurposing an Android-based malware strain initially developed by Pakistan’s SideCopy group. This malware, originally designed for local espionage, now serves Turla’s broader objectives of targeting Android devices globally. The campaign uses fake Android apps masquerading as legitimate tools, such as the Wasta WhatsApp app, to deceive users into downloading malware. Once installed, the spyware collects sensitive data, including call logs, SMS messages, contact lists, and precise geolocation data. This information is exfiltrated to Turla-controlled servers, highlighting the group’s strategic shift towards leveraging third-party tools to expand their capabilities.

Turla’s exploitation of existing malware demonstrates an innovative approach to cyberespionage, allowing the group to adapt quickly while minimising development costs. The campaign underscores the growing threat posed by advanced threat actors repurposing regional cyber tools for global surveillance and espionage operations.

ATTACK TYPE	Malware	SECTOR	Government
REGION	Afghanistan	APPLICATION	Windows

Source - https://thehackernews.com/2024/12/russia-linked-turla-exploits-pakistani.html

Targeted malware attack strikes the manufacturing sector

A cybercriminal group has launched a series of attacks targeting the manufacturing industry with sophisticated malware designed to disrupt operations and steal data. These attacks primarily impact SMBs. The malware is delivered through phishing emails, often disguised as legitimate communications, enabling the hackers to harvest sensitive credentials.

Once compromised, the attackers use these credentials to gain access to payroll systems and other critical infrastructure, leading to financial theft. Experts emphasise the importance of enhanced cybersecurity defences, particularly for smaller businesses that are more vulnerable to these types of attacks.

ATTACK TYPE	Malware	SECTOR	Manufacturing
REGION	Global	APPLICATION	Windows

Source - https://cyble.com/blog/threat-actor-targets-manufacturing-industry-with-malware/

INTRODUCTION | APT35 DRIVING CYBERESPIONAGE CAMPAIGN | HOWLING SCORPIUS FAST EMERGING AS GLOBAL THREAT | CELESTIAL STEALER COMPROMISES APPS AND SYSTEMS | ZEPHYR MALWARE MINES MONERO COVERTLY | BRAIN CIPHER RANSOMWARE TARGETS INDONESIA | SOCKS5SYSTEMZ BOTNET GOES ON A RAMPAGE | PAYROLL PIRATES COMPROMISES SMBS IN THE US | TURLA MALWARE TARGETS ANDROID USERS | SOPHISTICATED MALWARE ATTACKS MANUFACTURING INDUSTRY | CHINESE HACKERS INSTRUMENTAL IN EXPLOITING US FIRM

Chinese hackers behind 4-month cyberattack on US firm

A four-month-long cyberattack on a US firm has been linked to Chinese hackers, according to researchers. The intrusion, discovered between April and August 2024, involved lateral movement across the network, compromising several computers, including Exchange servers. The attackers deployed data exfiltration tools and exploited DLL side-loading techniques, common in Chinese cyberespionage tactics. The goal appeared to be harvesting sensitive email data and compromising systems for future breaches.

Researchers identified tools like FileZilla, Impacket, and PowerShell, further pointing to state-sponsored groups like Crimson Palace and Daggerfly. While the breach's entry point remains unclear, its long duration and sophisticated techniques highlight the evolving threat from state-backed cyber actors.

ATTACK TYPE	Malware	SECTOR	All
REGION	US	APPLICATION	macOS, Windows, Linux, FileZilla Client

Source - https://thehackernews.com/2024/12/researchers-uncover-4-month-cyberattack.html

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.