TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 21, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In an increasingly complex cybersecurity landscape, protecting critical systems and data is essential for individuals, businesses, and governments. Cyber threats can lead to financial losses, reputational damage, and operational disruptions.

Our weekly Cyber Threat Intelligence (CTI) report delivers actionable insights into emerging threats worldwide, empowering organisations with proactive defence strategies. Supported by expert advisory services, this intelligence-driven approach helps identify vulnerabilities, strengthen security frameworks, and enhance resilience against evolving cyber risks. Stay ahead of cyber threats with the knowledge and tools needed to secure a robust digital future.

TATA COMMUNICATIONS

A sophisticated multi-platform threat emerges in the form of BEAST ransomware

Since 2022, the BEAST ransomware group has been operating a Ransomware-as-a-Service (RaaS) platform, offering tools that target Windows, Linux, and VMware ESXi systems. Recent promotions in underground forums highlight their expanding capabilities and partnership programs. The Windows variant of BEAST employs a combination of elliptic-curve and ChaCha20 encryption, features multithreaded file encryption, and includes a ZIP wrapper mode that converts files into .zip format with an embedded ransom note. It also terminates specific processes and services, deletes shadow copies, and scans subnets to identify additional targets. The Linux and ESXi versions are written in C and Go programming languages, offering command-line controls for encryption paths, functionality toggles, and ransom note customisation. Notably, the ransomware avoids encrypting systems in Commonwealth of Independent States (CIS) countries by checking system language settings and IP addresses, likely to evade local law enforcement scrutiny.

BEAST also incorporates self-propagation mechanisms, such as SMB scanning, to identify and infect vulnerable systems within the same network without human intervention. This capability enhances its potential impact within compromised environments. Security experts advise organisations to implement robust cybersecurity measures, including regular system updates, network segmentation, and comprehensive monitoring, to defend against such sophisticated threats.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	macOS, Windows, Linux

Source - CERT-In

Gayfemboy botnet exploits zero-day vulnerability in industrial routers

In early 2024, cybersecurity researchers identified the emergence of the Gayfemboy botnet, a sophisticated variant of the Mirai malware. Initially unremarkable, this botnet rapidly evolved, incorporating advanced obfuscation techniques and exploiting both known and previously undisclosed vulnerabilities. Notably, in November 2024, Gayfemboy began leveraging a zero-day vulnerability in Four-Faith industrial routers (CVE-2024-12856), significantly expanding its reach. By late 2024, the botnet had compromised over 15,000 devices daily, predominantly in China, the US, Iran, Russia, and Turkey. Its targets included industrial routers, network-attached storage devices, and smart home systems. Demonstrating aggressive behaviour, the botnet launched DDoS attacks against researchers who registered its command-and-control (C2) domains, with attack traffic estimated in the hundreds of gigabits per second.

Gayfemboy's rapid development and effective exploitation of zero-day vulnerabilities underscore the escalating threat posed by modern botnets. Security experts advise organisations to implement robust cybersecurity measures, including regular system updates, network segmentation, and comprehensive monitoring, to defend against such sophisticated threats.

ATTACK TYPE	Vulnerability, malware	**SECTOR**	All
REGION	US, UK, China, Germany	**APPLICATION**	Generic, Four-Faith industrial routers, ASUS routers

Source - https://blog.xlab.qianxin.com/gayfemboy/

Nitrogen ransomware campaign exploits fake software installers

Cybersecurity researchers have identified a growing threat from the Nitrogen ransomware campaign, which leverages fake software installers to infect Windows systems. This sophisticated malware campaign, first observed in mid-2023, primarily spreads through deceptive Google search ads and phishing emails that masquerade as legitimate software downloads, such as WinSCP and PuTTY. Once executed, the fake installer deploys a PowerShell script that downloads and installs additional malicious payloads, including the Nitrogen ransomware itself. The ransomware encrypts critical files on the victim's system, appends a unique extension to affected files, and drops a ransom note demanding payment in cryptocurrency.

Notably, the campaign employs stealthy evasion techniques, such as process hollowing and DLL sideloading, to bypass security measures. Researchers have also linked the attack infrastructure to previous ransomware operations, indicating a well-coordinated cybercriminal effort. Organisations are advised to avoid unofficial software downloads, maintain updated security software, and implement endpoint detection solutions to mitigate this growing threat.

ATTACK TYPE	Ransomware	**SECTOR**	BFSI, manufacturing, construction
REGION	Canada, US, UK	**APPLICATION**	Generic

Source - https://hoploninfosec.com/nitrogen-ransomware/

Banshee Stealer malware targets macOS users

Cybersecurity researchers have uncovered Banshee Stealer, a newly emerging malware designed to infiltrate macOS systems and exfiltrate sensitive data. Distributed through malicious downloads and deceptive social engineering tactics, the stealer targets login credentials, browser-stored passwords, and cryptocurrency wallets. Unlike traditional malware that primarily affect Windows, Banshee Stealer is specifically crafted to exploit macOS environments, leveraging advanced obfuscation techniques to evade detection. Once executed, Banshee establishes persistence, allowing it to harvest data over an extended period. The malware communicates with C2 servers to transmit stolen information, enabling cybercriminals to exploit compromised accounts for further attacks. Security experts highlight its ability to bypass standard macOS defences, posing a severe risk to both individual users and enterprises relying on Apple systems.

To mitigate the threat, researchers urge macOS users to download software exclusively from trusted sources, enable Gatekeeper and XProtect, and implement robust endpoint security measures to detect suspicious activity.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	macOS

Source - https://blog.checkpoint.com/research/cracking-the-code-how-banshee-stealer-targets-macos-users/

Black Basta ransomware adopts advanced social engineering techniques

Black Basta, a notorious ransomware group, has intensified its cyberattacks by integrating sophisticated social engineering tactics and deploying advanced malware payloads, including Zbot, DarkGate, and custom-developed tools. This evolution in their attack strategy underscores the critical need for robust cybersecurity measures across various sectors. The attack sequence begins with email bombing, where victims' inboxes are overwhelmed by subscribing them to multiple mailing lists. Subsequently, attackers impersonate IT support staff on platforms like Microsoft Teams, convincing users to install remote access tools such as AnyDesk or TeamViewer. Once installed, these tools grant attackers control over the compromised systems. Upon gaining access, the attackers deploy credential harvesters to collect sensitive information. This is followed by the execution of malware like Zbot, which facilitates lateral movement within networks, and DarkGate, which exfiltrates data and deploys ransomware payloads. These sophisticated techniques enable attackers to evade detection and maintain persistence within compromised environments.

The resurgence of Black Basta highlights the evolving nature of cyber threats, emphasising the necessity for organisations to implement comprehensive security measures, including robust email filtering, endpoint detection tools, and regular security awareness training. Proactive defence strategies are essential to mitigate the risks posed by such advanced cybercriminal activities.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, BFSI, manufacturing, energy
REGION	Global	**APPLICATION**	MS Teams

Source - https://socradar.io/black-basta-deploying-zbot-darkgate-bespoke-malware/

Hunters ransomware group increases attacks with advanced tactics

Hunters ransomware, known for its sophisticated tactics, has escalated its activities by deploying advanced malware and using evasive techniques. This group primarily targets large enterprises, often exploiting phishing schemes and social engineering to infiltrate networks. Once inside, they deploy Remote Access Trojans (RATs), enabling further movement within systems and exfiltration of sensitive data. Following this, the attackers issue ransom demands, leveraging stolen data to strengthen their extortion tactics.

Experts urge organisations to bolster their cybersecurity infrastructure, including enhanced detection and response capabilities, to mitigate the growing threat from these highly organised cybercriminals.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, BFSI, manufacturing, education, logistics and shipping
REGION	Global	**APPLICATION**	Windows

Source - https://www.vectra.ai/threat-actors/hunters , https://cyberint.com/blog/research/hunters-ransomware/

Play ransomware escalates cyberattacks using sophisticated techniques

Play ransomware, also known as Balloonfly or PlayCrypt, has affected over 300 organisations globally since June 2022. The attackers exploit vulnerabilities like ProxyNotShell in MS Exchange Server and FortiOS to gain initial access. Once inside, they deploy tools such as Mimikatz for credential theft, and use AnyDesk and Cobalt Strike for lateral movement and command control. The group uses advanced evasion tactics, including disabling security tools and leveraging legitimate software like Process Hacker.

The ongoing threat highlights the importance of robust cybersecurity defences to mitigate these sophisticated ransomware attacks.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://asec.ahnlab.com/en/85580/

FunkSec ransomware targets organisations with evasive techniques

FunkSec ransomware has emerged as a significant cyber threat, using sophisticated techniques to target enterprises. This malware is designed to evade detection by exploiting unpatched vulnerabilities and leveraging complex encryption methods. After infiltrating networks, FunkSec demands hefty ransoms, often threatening to release stolen data.

Organisations are advised to patch vulnerabilities promptly, implement strong network defences, and adopt best practices in cybersecurity hygiene to mitigate the risks posed by this growing threat.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - https://www.broadcom.com/support/security-center/protection-bulletin/funksec-ransomware

TATA COMMUNICATIONS

Hexalocker v2 propagated by Skuld Stealer, causing a growing cybersecurity threat

The Hexalocker v2 ransomware variant has been actively distributed by the Skuld Stealer malware, significantly increasing the impact of cyberattacks. This sophisticated malware uses various techniques to infect systems, enabling attackers to encrypt critical data and demand ransom. Organisations are urged to strengthen their defences, patch vulnerabilities, and maintain robust security measures to mitigate these escalating threats.

The combination of Skuld Stealer's data-stealing capabilities and Hexalocker v2's encryption has resulted in severe consequences for multiple industries.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://cyble.com/blog/hexalocker-v2-being-proliferated-by-skuld-stealer/

SocGholish malware targets users with deceptive update tricks

SocGholish, a malicious social engineering tool, has been wreaking havoc by tricking users into executing a harmful JavaScript payload disguised as a system or browser update. This malware primarily spreads through compromised websites, utilising techniques like drive-by downloads and fake updates or malicious ads. Once activated, it can deploy additional malware such as ransomware and RATs, compromising users' systems further.

To protect against SocGholish, cybersecurity experts recommend employing web filtering, disabling auto-downloads, and ensuring web browsers are regularly updated. These measures are essential for minimising exposure to this growing threat and ensuring the security of users' online activities. Organisations and individuals alike are urged to stay vigilant against these increasingly sophisticated attack methods.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - Cert-In

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