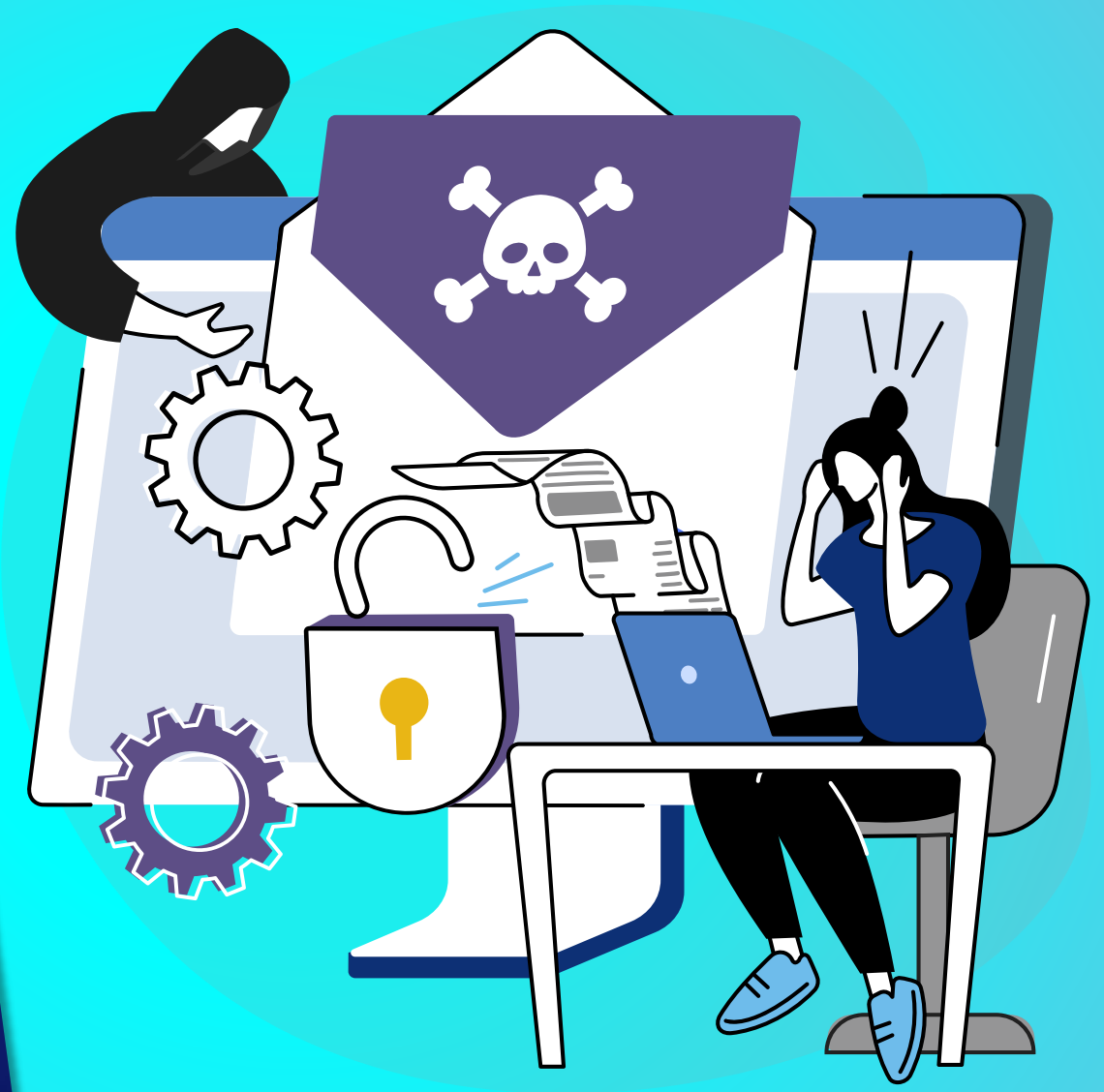
TATA COMMUNICATIONS

TATA

# YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: NOVEMBER 5, 2024



TATA COMMUNICATIONS

TATA

# THREAT INTELLIGENCE ADVISORY REPORT

In today's digital landscape, individuals, businesses, and government agencies face escalating cybersecurity threats with potentially severe financial and reputational impacts. Strengthening digital defences is essential to protect the integrity, confidentiality, and availability of enterprise data.

Our weekly cyber threat intelligence reports deliver the latest insights, helping you proactively shield IT assets from persistent cyber risks. Our advisory services also provide comprehensive support to bolster your organisation's security posture. In an era demanding cyber resilience, our reports empower your team with critical knowledge to enhance threat readiness and maintain robust operational security.


INTRODUCTION | VMWARE PATCHES CRITICAL VULNERABILITY | 6,000+ WORDPRESS SITES COMPROMISED | TRICKBOT TARGETS THE BFSI SECTOR | SOCGHOLISH ATTACKS THE PUBLIC SECTOR | REDLINE THREATENS DATA SECURITY | FORTIMANAGER IN ZERO-DAY ATTACK | GRANDOREIRO ATTACKS GO GLOBAL | SUPERSHELL EMPOWERS CYBERCRIMINALS | CRYPTOJACKERS AIDED BY MODERN PROTOCOLS | MALWARE FAMILY ATTACKS VARIOUS SECTORS

# VMware patches critical RCE vulnerability

VMware recently issued updated patches to address a critical vulnerability in its vCenter Server software. The flaw, identified as CVE-2024-38812 with a CVSS score of 9.8, is a heap-overflow vulnerability within the DCE/RPC protocol that could enable remote code execution (RCE). Exploitable through a specially crafted network packet, this issue poses a serious threat if not addressed.

VMware has clarified that the initial patches – released on September 17, 2024 – did not fully resolve the issue. The revised patches are now available for vCenter Server versions 8.0 U3d, 8.0 U2e, and 7.0 U3t, as well as for VMware Cloud Foundation versions 5.x, 5.1.x, and 4.x. Though no instances of exploitation in the wild have been observed, VMware strongly recommends users apply the latest patches.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Vulnerability | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | VMware vCenter Server |

Source - https://thehackernews.com/2024/10/vmware-releases-vcenter-server-update.html

# Over 6,000 WordPress sites compromised by malware

WordPress sites are increasingly targeted by threat actors (TAs) using malicious plugins to deliver fake update prompts, spreading information-stealing malware. This campaign, which has escalated in 2024 with a method called “ClickFix,” mimics software error messages and displays false error banners, such as browser updates and captcha warnings, to trick users into executing malware-laden PowerShell scripts.

Originally identified as “ClearFake” in 2023, the attack has evolved, with hackers compromising over 6,000 WordPress sites. These deceptive plugins resemble legitimate names and exploit previously stolen credentials from brute force or phishing attacks. Administrators experiencing suspicious alerts are advised to check installed plugins, remove unfamiliar ones, and reset admin passwords with unique, site-specific credentials to help safeguard site security and prevent data breaches.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | WordPress |

Source - https://www.bleepingcomputer.com/news/security/over-6-000-wordpress-sites-hacked-to-install-plugins-pushing-infostealers/

# Modular malware resurfaces and impacts the BFSI sector

The TrickBot malware has become a significant threat to the BFSI sector, evolving from a simple banking Trojan into a sophisticated modular malware ecosystem. Originally designed to steal banking credentials, TrickBot now includes advanced capabilities such as network reconnaissance, credential harvesting, and ransomware deployment, posing severe risks to financial institutions worldwide. Recent TrickBot campaigns have specifically targeted the BFSI sector with phishing emails, malicious attachments, and exploit kits to infiltrate networks.

TrickBot operators often use it as an entry point for subsequent ransomware attacks like Ryuk and Conti, causing costly data breaches and service disruptions. The malware's modular structure allows attackers to adapt quickly, evading traditional detection methods and compromising even well-defended networks. To counter TrickBot, BFSI organisations are advised to implement multi-factor authentication (MFA), bolster endpoint security, and conduct employee training to recognise phishing tactics. Proactive threat intelligence remains crucial to mitigating these escalating risks.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | BFSI |
| **REGION** | Global | **APPLICATION** | Generic |

**Source** - CERT-In

# Social engineering malware wreaks havoc in public sector

The SocGholish malware – a sophisticated JavaScript-based threat – has recently surged in cyberattacks, primarily targeting businesses and public sector organisations through drive-by-download campaigns. Disguised as legitimate software updates, SocGholish infects websites and prompts users to download malicious code, often posing as essential updates for common applications. Once installed, it opens the door for further infections, such as ransomware and information-stealing malware, impacting system integrity and compromising sensitive data.

In 2024, the SocGholish campaign has been responsible for numerous high-profile attacks, including breaches that disrupted operations and caused financial and reputational damage. Often distributed through compromised websites and trusted advertising platforms, SocGholish exploits user trust to increase infection rates across diverse sectors. Cybersecurity experts warn that SocGholish's rapid evolution, which leverages automation and highly targeted phishing techniques, poses severe risks. Organisations are advised to enhance web security measures, conduct user awareness training, and employ robust endpoint protection to prevent such infections from gaining entry.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | Windows |

Source - CERT-In

# Redline malware targets data security

The Redline malware, a highly active information-stealer, has gained prominence in recent attacks targeting individuals and organisations worldwide. Known for its accessibility on the dark web and ease of deployment, Redline enables cybercriminals to harvest sensitive data, including browser-stored credentials, credit card details, cryptocurrency wallets, and system information. Distributed primarily through phishing emails, malicious downloads, and compromised websites, Redline poses a significant risk, especially as attackers increasingly exploit remote work setups and home networks.

In 2024, Redline attacks have surged, impacting sectors from finance to healthcare and prompting considerable operational and financial fallout. Once Redline infiltrates a system, it exfiltrates data to command-and-control (C2) servers, leaving companies vulnerable to follow-up attacks, such as ransomware and account takeovers. Cybersecurity experts advise strengthening email security, employee awareness, and endpoint protection to reduce exposure to this malware. As Redline's tactics evolve, organisations must adopt a proactive defence strategy to counteract its pervasive data-theft threat.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | Windows |

Source - CERT-In

# FortiManager comes under zero-day attack

Fortinet has disclosed a critical zero-day vulnerability in FortiManager, identified as CVE-2024-47575, with a severity score of 9.8. This vulnerability, termed “FortiJump” by researchers, allows attackers to exploit a missing authentication function in the FortiManager fgfmd daemon. When exploited, it grants unauthorised access to steal sensitive configuration files, IP addresses, and credentials from managed devices. Fortinet initially notified customers privately, sharing mitigation steps until a security patch became available. However, details leaked on platforms like Reddit and Mastodon, revealing that some customers experienced attacks weeks before Fortinet’s official notifications.

Fortinet has publicly confirmed the flaw, urging device administrators to update credentials on all managed devices due to the data’s sensitive nature. While Fortinet hasn’t specified affected customers or linked the exploit to a particular threat actor, they are actively investigating the scope of the breach and recommending immediate credential updates.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Vulnerability | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | FortiManager |

Source - https://www.bleepingcomputer.com/news/security/fortinet-warns-of-new-critical-fortimanager-flaw-used-in-zero-day-attacks/

# New banking malware variants evade detection amid targeted attacks

Newly identified variants of the banking malware Grandoreiro demonstrate advanced tactics to evade anti-fraud defences, suggesting ongoing development despite partial law enforcement crackdowns. Recent analysis confirms that while some gang members were apprehended, others continue enhancing Grandoreiro and expanding infrastructure to target users globally. Key new features include a domain generation algorithm (DGA) for C2, ciphertext stealing (CTS) encryption, mouse tracking, and streamlined local versions specifically designed for Mexican banking customers. Since its 2016 launch, Grandoreiro has expanded its geographical reach to Latin America and Europe, enabling credential theft from over 1,700 financial institutions across 45 regions.

Operating under a selective malware-as-a-service (MaaS) model, Grandoreiro detects installed software like web browsers, VPNs, and cloud storage, and it acts as a clipper to redirect cryptocurrency transactions. Updates to its attack methods now include a CAPTCHA bypass, keystroke logging, Outlook spam capabilities, and tracking for banking security solutions, underscoring its adaptability and threat scope.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | Aviation, BFSI, energy, government, healthcare, IT, manufacturing, mining, oil and gas, telecommunications |
| **REGION** | Global | **APPLICATION** | Windows |

Source - https://thehackernews.com/2024/10/new-grandoreiro-banking-malware.html

# Supershell malware targets entities globally

The Supershell C2 platform has emerged as a notable tool in the cybersecurity landscape, gaining traction among cybercriminals for its robust capabilities. Designed to facilitate remote access and management of compromised systems, Supershell provides a centralised interface for attackers to deploy various payloads, execute commands, and maintain persistence on victim networks. Recent reports indicate that Supershell is being utilised in widespread ransomware and information-stealing campaigns, significantly impacting organisations across multiple sectors. Supershell's ability to blend in with legitimate traffic poses challenges for detection and mitigation efforts.

As law enforcement and cybersecurity professionals intensify their focus on disrupting these C2 infrastructures, the proliferation of Supershell highlights the ongoing evolution of cyber threats. Organisations are advised to strengthen their defences, emphasising proactive monitoring, employee training, and incident response planning to combat the risks posed by such sophisticated tools.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | Aviation, BFSI, energy, government, healthcare, IT, manufacturing, mining, oil and gas, telecommunications |
| **REGION** | Global | **APPLICATION** | Generic |

Source - CERT-In

# Hackers leverage modern protocols for cryptojacking

Researchers have identified a novel method employed by cybercriminals to deploy the SRBMiner cryptominer on Docker remote API servers. This attack exploits the gRPC protocol over h2c (clear text HTTP/2) to bypass security measures while mining XRP cryptocurrency. The attack initiates with the threat actor scanning for vulnerable Docker API servers. Upon locating a target, the attacker assesses the Docker API's version and availability, then sends a request to upgrade to gRPC/h2c. This crucial step enables remote manipulation of Docker functionalities without detection.

After upgrading the connection, the attacker uses gRPC methods for operations like file synchronisation, authentication, and SSH forwarding, effectively allowing command execution as if they were managing the server directly. Following this, the SRBMiner is deployed by building a Docker image from a legitimate base image and placing the miner in the directory. This approach raises significant security concerns, as it obscures malicious activities, making detection challenging. The findings underscore the need for stringent protection of containerised environments like Docker, as attackers continue to evolve their strategies.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | Docker |

Source - https://securityonline.info/cryptojacking-alert-hackers-exploit-grpc-and-http-2-to-deploy-miners/

# Critical malware family identified targeting various sectors

WarmCookie, also known as BadSpace, is a malware family that emerged in April 2024, distributed through ongoing malspam and malvertising campaigns. It is designed for initial access and persistence, allowing attackers to maintain long-term control of compromised environments. WarmCookie facilitates the delivery of additional malware, including CSharp-Streamer-RAT and Cobalt Strike. The malware's post-compromise activities show significant overlap with those attributed to the threat actor group TA866, suggesting that WarmCookie may have been developed by the same group responsible for the Resident backdoor.

Throughout 2024, WarmCookie distribution campaigns have utilised various lure themes, particularly invoice-related and job agency motifs, to entice victims into clicking malicious links in emails or attached documents. This malware provides a range of functionalities for attackers, such as payload deployment, file manipulation, command execution, screenshot collection, and persistence, making it a valuable tool for maintaining access within compromised networks.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | Aviation, BFSI, energy, government, healthcare, IT, manufacturing, mining, oil and gas, telecommunications |
| **REGION** | Global | **APPLICATION** | Windows |

Source - https://blog.talosintelligence.com/warmcookie-analysis/

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*