TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MARCH 26TH, 2024

THREAT INTELLIGENCE ADVISORY REPORT

In the current global scenario, cybersecurity stands as a paramount concern for organisations. With cyber threats evolving continuously, businesses strive to protect their assets and maintain operational continuity. It is no longer just about securing data; it is about strengthening the foundational pillars on which modern organisations stand, ensuring resilience against a spectrum of emerging threats.

Enhance your organisation’s cybersecurity preparedness with Tata Communications’ weekly threat intelligence advisory. Acquire valuable insights into the latest cyber risks and take proactive steps to fortify your defences, mitigating potential vulnerabilities effectively.

INTRODUCTION
MS FIXES CRITICAL VULNERABILITIES
PHISHING CAMPAIGN DEPLOYS RATS
CRYPTOWIRE RANSOMWARE RESURFACES
XEHOOK TARGETS CRYPTO WALLETS
FORTINET DISCOVERS CRITICAL FLAWS
MALWARE TARGETS MANUFACTURERS
FAKEBAT BECOMES MORE DECEPTIVE
RANSOMWARE EVADES SECURITY
CISCO ADDRESSES VULNERABILITIES IN IOS XR
RUSSIAN THREAT GROUP EXPANDING OPERATIONS

Microsoft’s March Patch Tuesday fixes critical vulnerabilities

Microsoft recently released 59 patches addressing vulnerabilities across various products like Microsoft Windows, Office, Azure, and Skype. Among the critical vulnerabilities fixed are remote code execution (RCE) and elevation of privilege issues.

Other notable vulnerabilities include CVE-2024-21400, which could allow attackers to gain elevated privileges in Azure Kubernetes Service, and CVE-2024-26199, allowing authenticated users to gain SYSTEM privileges in Microsoft Office. Additionally, CVE-2024-20671, a security feature bypass vulnerability in Microsoft Defender, and CVE-2024-21411, a RCE vulnerability in Skype for Consumer, were resolved. These fixes demonstrate Microsoft’s commitment to enhancing cybersecurity.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2024-patch-tuesday-fixes-60-flaws-18-rce-bugs/

INTRODUCTION | MS FIXES CRITICAL VULNERABILITIES | PHISHING CAMPAIGN DEPLOYS RATS | CRYPTOWIRE RANSOMWARE RESURFACES | XEHOOK TARGETS CRYPTO WALLETS | FORTINET DISCOVERS CRITICAL FLAWS | MALWARE TARGETS MANUFACTURERS | FAKEBAT BECOMES MORE DECEPTIVE | RANSOMWARE EVADES SECURITY | CISCO ADDRESSES VULNERABILITIES IN IOS XR | RUSSIAN THREAT GROUP EXPANDING OPERATIONS

Phishing campaign uses malware to deploy VCURMS and STRRAT

A recent discovery by researchers reveals a highly sophisticated phishing campaign employing a malicious Java downloader to disseminate VCURMS and STRRAT remote access trojans (RATs). This campaign exploits public platforms such as AWS and GitHub to host malware, while ProtonMail ensures heightened privacy in email communications.

The operation utilises obfuscated code and various malicious components, including a keylogger and information stealer, demonstrating advanced evasion tactics. It orchestrates the simultaneous deployment of VCURMS and STRRAT, with VCURMS featuring a customised Rude Stealer and keylogger for extracting data. The attacker employs multiple obfuscation methods to evade detection, utilising email as the command and control (C2) interface. This multifaceted attack underscores the importance of robust cybersecurity measures against evolving threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.fortinet.com/blog/threat-research/vcurms-a-simple-and-functional-weapon

CryptoWire ransomware resurfaces with deceptive tactics

Recent studies highlight the resurgence of CryptoWire ransomware, recognised for its distribution through phishing emails and AutoIt script-based creation. The ransomware embeds persistently, spreading via network scans and employing a unique encryption method that complicates data recovery. Notably, it includes an embedded decryption key, emphasising cautious file execution and updated antivirus defences.

Initially discovered in 2018, CryptoWire's recent resurgence unveils a new delivery campaign, encrypting user files across various drives. Its ransom note appears as a pop-up window, with an uncommon feature of the decryption key located within the traffic sent back to the C2 servers or within the AutoIt script.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

Xehook targets crypto wallets and two-factor authentication

In January 2024, researchers unveiled Xehook Stealer, a .NET malware targeting Windows, exhibiting advanced data collection abilities from browsers, cryptocurrency support, and unique features such as custom traffic bots. Investigations revealed a potential evolutionary link between Xehook Stealer, Agniane Stealer, and the Cinoshi project, implying a pattern of rebranding and cyber threat development. This emphasises the urgency for robust defence mechanisms against such sophisticated malware.

Xehook Stealer, discovered by CRIL, dynamically collects data from Chromium and Gecko-based browsers, supporting over 110 cryptocurrencies and two-factor authentication (2FA) extensions. It features an API for traffic bot creation and Google cookie recovery. The connection between Xehook Stealer, Agniane, and the Cinoshi project was identified through shared code, configuration data, and web panel design similarities, suggesting continuous development and iteration.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://cyble.com/blog/xehook-stealer-evolution-of-cinoshis-project-targeting-over-100-cryptocurrencies-and-2fa-extensions/

Critical flaw found in Fortinet’s FortiClientEMS software

Fortinet issued a critical security alert (CVE-2023-48788) for a vulnerability in FortiClientEMS, posing a risk of unauthorised code execution. Users of affected versions (7.0.1 to 7.0.10, and 7.2.0 to 7.2.2) should upgrade to versions 7.0.11 or above and 7.2.3 or above. FortiOS and FortiProxy are also affected, requiring immediate upgrades despite no evidence of active exploitation.

The vulnerability was discovered by the UK’s National Cyber Security Centre (NCSC) and Fortinet developer, Thiago Santana. It allows unauthenticated attackers to gain RCE with SYSTEM privileges through SQL injection in the DB2 Administration Server (DAS) component. Fortinet advises prompt patching to mitigate potential risks associated with this critical vulnerability.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Fortinet

Source - https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-rce-bug-in-endpoint-management-software/

Blind Eagle targets North American manufacturers with Ande Loader malware

Blind Eagle, aka APT-C-36, has expanded its cyberattack methods, employing Ande Loader via phishing to distribute RATs like Remcos RAT and NjRAT, targeting Spanish-speaking individuals in North America's manufacturing sector. Tactics include password protected RAR and BZ2 archives delivered via Discord CDN links, with crypters from individuals Roda and Pjoao1578 enhancing malware efficacy. This financially motivated threat actor historically targets Colombian and Ecuadorian entities with RATs such as AsyncRAT, BitRAT, Lime RAT, and Quasar RAT.

These recent findings demonstrate an extended targeting range, utilising phishing emails. Password-protected RAR archives contain a malicious VBScript file, ensuring persistence in Windows Startup and initiating Ande Loader, which then deploys Remcos RAT. Alternatively, a BZ2 archive with a VBScript file is distributed via Discord CDN, deploying NjRAT through Ande Loader, as observed by Canadian cybersecurity experts.

ATTACK TYPE	Malware	SECTOR	Manufacturing
REGION	North America	APPLICATION	Windows

Source - https://thehackernews.com/2024/03/ande-loader-malware-targets.html

FakeBat malware spreads through deceptive adverts

In February, search-based malvertising surged, prominently featuring the FakeBat malware, which utilises MSIX installers with heavily obfuscated PowerShell scripts. Malvertisers shifted tactics from URL shorteners to compromising legitimate sites, broadening their targets beyond known brands. Despite Google’s efforts, these campaigns persist, underscoring the need for robust ad-blocking policies.

FakeBat stands out for its use of MSIX installers and evolving distribution tactics, including exploiting genuine websites. The diversity of recent campaigns is notable, moving beyond typical software brands like Parsec and Freecad. FakeBat remains a threat, bypassing Google’s security checks to redirect victims to deceptive websites. Defending against the malware and its infrastructure, especially through legitimate sites, poses challenges.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.malwarebytes.com/blog/threat-intelligence/2024/03/fakebat-delivered-via-several-active-malvertising-campaigns

StopCrypt ransomware uses evasion techniques to bypass security

The advanced StopCrypt ransomware variant employs a sophisticated, multi-staged execution process to evade detection, primarily targeting individual consumers with demands for small ransoms. Despite its widespread distribution and complex attack methods, StopCrypt often goes unnoticed compared to more infamous ransomware families. Its continuous evolution into a stealthier and more formidable threat reflects the escalating cybersecurity concerns, impacting a significant number of users with potentially severe consequences.

While ransomware like LockBit, BlackCat, and Clop dominate headlines, StopCrypt operates under the radar, mainly targeting consumers to elicit numerous small ransom payments. It is commonly distributed through malvertising and dubious sites offering adware bundles disguised as free software, game cheats, and software cracks. Despite minimal changes since its 2018 debut, new versions of StopCrypt warrant attention due to their substantial impact on affected users.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.bleepingcomputer.com/news/security/stopcrypt-most-widely-distributed-ransomware-now-evades-detection/

INTRODUCTION | MS FIXES CRITICAL VULNERABILITIES | PHISHING CAMPAIGN DEPLOYS RATS | CRYPTOWIRE RANSOMWARE RESURFACES | XEHOOK TARGETS CRYPTO WALLETS | FORTINET DISCOVERS CRITICAL FLAWS | MALWARE TARGETS MANUFACTURERS | FAKEBAT BECOMES MORE DECEPTIVE | RANSOMWARE EVADES SECURITY | CISCO ADDRESSES VULNERABILITIES IN IOS XR | RUSSIAN THREAT GROUP EXPANDING OPERATIONS

Cisco addresses high-severity vulnerabilities in IOS XR software

Cisco recently addressed high-severity vulnerabilities in IOS XR software, addressing privilege escalation and denial-of-service (DoS) risks. Notably, three vulnerabilities were patched: a SSH privilege escalation (CVE-2024-20320), a Layer 2 ethernet services flaw (CVE-2024-20318), and a PPPoE termination issue (CVE-2024-20327), capable of causing severe disruptions.

The SSH vulnerability affects Cisco IOS XR software for Cisco 8000 series routers and Cisco Network Convergence System (NCS) 540/5700 series routers, allowing authenticated attackers to elevate privileges. The Layer 2 ethernet flaw, impacting IOS XR software, permits unauthenticated attackers to cause a DoS condition. Similarly, the PPPoE vulnerability in ASR 9000 series routers enables adjacent, unauthenticated attackers to crash the ppp_ma process, resulting in a DoS scenario. While no exploits have been reported, users are advised to apply patches promptly to mitigate potential risks.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Cisco IOS XR

Source - https://securityaffairs.com/160489/security/cisco-ios-rx-flaws.html

APT28 phishing campaign targets Europe, Americas, and Asia

APT28, a Russian-linked cyber threat group, has broadened its phishing campaigns globally, targeting governmental and non-governmental entities with deceptive documents covering diverse topics. They exploit Microsoft Outlook vulnerabilities to spread malware like HeadLace and have recently utilised compromised WebDAV servers from routers for their operations, showcasing their adaptability and attack sophistication.

Ongoing ITG05 phishing campaigns mimic authentic documents from government and non-governmental organisations across Europe, the South Caucasus, Central Asia, and North and South America. These lures encompass various sectors like finance, critical infrastructure, cybersecurity, healthcare, and defence. ITG05 has adopted new techniques, such as the “search-ms” URI handler, leading to malware downloads from WebDAV servers. They have introduced new backdoors like MASEPIE and OCEANMAP, indicating evolving tactics. With connections to APT28 and other threat groups, ITG05 is likely to persist in its malicious activities to advance state interests.

ATTACK TYPE	Phishing, malware	SECTOR	All
REGION	Europe, Americas, Asia	APPLICATION	Android

Source - https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal/

INTRODUCTION | MS FIXES CRITICAL VULNERABILITIES | PHISHING CAMPAIGN DEPLOYS RATS | CRYPTOWIRE RANSOMWARE RESURFACES | XEHOOK TARGETS CRYPTO WALLETS | FORTINET DISCOVERS CRITICAL FLAWS | MALWARE TARGETS MANUFACTURERS | FAKEBAT BECOMES MORE DECEPTIVE | RANSOMWARE EVADES SECURITY | CISCO ADDRESSES VULNERABILITIES IN IOS XR | RUSSIAN THREAT GROUP EXPANDING OPERATIONS

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.