TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: April 23rd, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Cybersecurity threats are impacting businesses of all sizes and sectors and new threats are emerging every hour. Cybercrime and associated cyber-risks are a top concern for organisations and governments globally requiring staying vigilant and framing an effective cybersecurity strategy to shield their operations, business, and organisations.

Enhance your organisation's cybersecurity readiness with Tata Communications' weekly threat intelligence report. Subscribe to our weekly report to get actionable insights into the latest cyber threats and build effective mitigation strategies.

TATA COMMUNICATIONS

Microsoft's April 2024 patch update: 149 vulnerabilities patched, zero days resolved

Microsoft's April 2024 Patch Tuesday addressed a record-breaking 155 CVEs, including 147 new vulnerabilities across its products. Three of these vulnerabilities were Critical, 142 were Important, and two were Moderate, making it the most extensive release in Microsoft's history. However, no known active exploits or vulnerabilities were publicly disclosed.

An actively exploited bug added to the urgency for users to install the patches. While the number of vulnerabilities seemed overwhelming, Microsoft’s prompt response and the absence of known active attacks both provided reassurance and highlighted the importance of periodic software updates.

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

Source- https://thehackernews.com/2024/04/microsoft-fixes-149-flaws-in-huge-april.html/

TATA COMMUNICATIONS

"Starry Addax" campaign targets North African activists with fake apps and login pages

Cybersecurity experts have identified a cyberattack campaign called ‘’ Starry Addax’’ targeting human rights activists in North Africa, particularly those associated with the Sahrawi Arab Democratic Republic (SADR) cause. Phishing emails deploy a malicious Android application named "FlexStarling" to infiltrate devices in the guise of the Sahara Press Service (SPSRASD) app serving Spanish-language content from the SPSRASD website. The campaign, believed to be in its early stages, uses custom-built malware and infrastructure specifically designed for stealth, indicating a coordinated effort to avoid detection.

The malware requests permissions from Android devices to extract information and execute arbitrary code. It uses anti-emulation controls to bypass analysis and multiple commands from a C2 (Command and Control) server to execute the malicious code, downloading files and sending the data to the attacker’s Dropbox folders. Cisco Talos advises organisations to deploy security measures like Cisco Secure Endpoint and Umbrella to detect and mitigate such threats.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Morocco	**APPLICATION**	Android, Windows

Source- https://blog.talosintelligence.com/starry-addax/

TATA COMMUNICATIONS

Delivering multi-stage malware through invoice phishing using obfuscation techniques (BatCloak, ScrubCrypt)

Researchers have exposed a cyberattack that uses phishing emails with SVG file attachments to distribute malware, such as Venom RAT and NanoCore RAT. These attacks use advanced obfuscation techniques like BatCloak and ScrubCrypt to avoid standard security measures and target cryptocurrency wallets across platforms like Microsoft Windows.

Last year, FortiGuard Labs disclosed the 8220 Gang's use of an "antivirus evasion tool" ScrubCrypt, to target exploitable Oracle WebLogic Servers. ScrubCrypt's conversion of executables into undetectable batch files adds layers of complexity and prevents detection by antivirus. Recent findings reveal a surge in phishing emails containing malicious SVG files, facilitating the delivery of VenomRAT and other plugins like NanoCore and Remcos through BatCloak and ScrubCrypt.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source- https://www.fortinet.com/blog/threat-research/scrubcrypt-deploys-venomrat-with-arsenal-of-plugins

SharePoint vulnerabilities allow stealthy file exfiltration

In November 2023, Varonis identified two vulnerabilities in Microsoft SharePoint, a key platform to collaborate and manage documents. Attackers can bypass or disguise audit logs, enabling undetected data extraction. SharePoint's "Open in App" feature can be exploited by attackers to avoid triggering typical file download events, creating "Access" events that go unnoticed. Similarly, by spoofing user-agent strings to mimic routine data syncing operations, they can obscure their activities within the logs and evade scrutiny.

However, Microsoft is unlikely to implement immediate fixes for the moderate issue. Instead, SharePoint administrators are advised to remain vigilant, monitor access activity for anomalies, and scrutinize sync events for unusual patterns.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Microsoft Windows SharePoint Services

Source- https://www.bleepingcomputer.com/news/security/new-sharepoint-flaws-help-hackers-evade-detection-when-stealing-files/

Rust vulnerability ‘’BatBadBut’’ threatens Windows systems

CVE-2024-24576, an emerging vulnerability in the Rust Standard Library threatens Windows users with command injection attacks through improperly escaped arguments in batch files. Dubbed "BatBadBut" by security researcher RyotaK, this issue affects Rust and other programming languages, emphasizing the need for strict command execution and argument validation in Windows environments. With a maximum CVSS score of 10.0, the vulnerability targets batch files when invoked on Windows with untrusted arguments.

As the Rust Standard Library fails to escape arguments when invoking batch files on Windows, attackers can execute arbitrary shell commands. To prevent unexpected execution, RyotaK recommends users relocate batch files to directories not included in the PATH environment variable. Also, patch releases for Rust versions before 1.77.2 are issued, along with updates from Haskell, Node.js, PHP, and yt-dlp maintainers to address similar command injection vulnerabilities in their languages or tools.

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

Source- https://thehackernews.com/2024/04/critical-batbadbut-rust-vulnerability.html

RUBYCARP group behind decade-old cryptojacking operation

RUBYCARP, a Romanian botnet group, exploits existing vulnerabilities with brute force tactics to breach corporate networks. Managed via private IRC channels, the botnet controls over 600 compromised servers, promoting DDoS attacks and phishing attempts. RUBYCARP's low detection rate is proof of its dynamic infrastructure over a decade of operations.

Sysdig's report reveals 39 variants of RUBYCARP's Perl-based payload, with only eight detected on VirusTotal. The group's association with the Outlaw APT threat group suggests broader connections within the cyber threat landscape. Their recent probes target Laravel applications via CVE-2021-3129, exploit SSH servers through brute force, and compromise WordPress sites using credential dumps. RUBYCARP also engages in cryptocurrency mining and financial fraud through phishing campaigns. Although not ranked among the largest botnet operators, RUBYCARP's longevity and involvement in cyber weapon development highlight the need for increased vigilance and strong security measures.

ATTACK TYPE	Cyber Crime	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source- https://www.bleepingcomputer.com/news/security/rubycarp-hackers-linked-to-10-year-old-cryptomining-botnet/

TATA COMMUNICATIONS

LightSpy resurgence: Espionage operation threatens Southern Asia, potentially India

The LightSpy mobile espionage campaign has resurfaced targeting South Asia with an "F_Warehouse" spyware designed to extract sensitive data from iOS devices. Recent alerts from Apple and VirusTotal indicate active threats and potential victims within India. First discovered in 2020, LightSpy is a fully featured surveillance toolset specialising in extracting hyper-specific location data and audio recordings during voice-over IP calls. Its capabilities include stealing files from messaging apps like Telegram and WeChat, recording audio privately, and accessing browser history and WiFi connection lists.

Recommendations to counter the vulnerability include enabling Lockdown Mode on iOS devices, using secure communication solutions like SecuSUITE®, staying informed about the latest threats, and following security best practices for mobile devices. Businesses should also implement robust incident response plans, encourage employees to update their devices regularly, use strong passwords, and exercise caution with unkown links or attachments.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	India, South Asia	**APPLICATION**	Apple iOS

Source- https://blogs.blackberry.com/en/2024/04/lightspy-returns-renewed-espionage-campaign-targets-southern-asia-possibly-india

TATA COMMUNICATIONS

Malicious ads spread nitrogen malware disguised as PuTTY and FileZilla

Cybersecurity analysts have identified a campaign that targets system administrators by posing as popular utilities such as PuTTY and FileZilla. Strategically placed as a sponsored result on Google's search engine, these ads are primarily targeted toward North American users. Victims unknowingly download and execute the nitrogen malware disguised as a legitimate software installer to enable access on private networks and leading to data breaches and the deployment of ransomware including BlackCat/ALPHV. The malware utilises DLL sideloading to execute its payload, risking system security. Despite efforts to alert Google, action is yet to be taken.

The campaign has multiple stages including tricking victims with fraudulent ads, directing them to lookalike websites, and ultimately deploying malware through fake installers. Organisations are advised to enhance user education, deploy security measures, and consider Managed Detection and Response (MDR) services. Adopting endpoint protection strategies and DNS filtering can also reduce exposure to malicious advertisements.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	North America	**APPLICATION**	Windows

Source- https://www.malwarebytes.com/blog/threat-intelligence/2024/04/active-nitrogen-campaign-delivered-via-malicious-ads-for-putty-filezilla

TATA COMMUNICATIONS

Spyware campaign ‘’eXotic Visit’’ targets Android users in India and Pakistan

Active since November 2021, the ‘’eXotic Visit’’ malware campaign targets Android users in South Asia, particularly India and Pakistan. It disguises as legitimate communication platforms and service applications and distributes through fraudulent websites and the Google Play Store. The malware, Android XploitSPY Remote Access Trojan (RAT), promotes espionage activities including GPS tracking, microphone access, and data interception while evading detection and maximizing data extraction.

The fake apps have been downloaded by approximately 380 victims, with installations ranging from zero to 45. The malware gathers sensitive user data, accesses device functions, and execute commands. With time, the attackers behind the campaign have evolved their tactics using obfuscation techniques, emulator detection, and native libraries to avoid detection. While Google Play Protect offers some protection, defending against Android malware targeting users in specific regions remains challenging.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	India, Pakistan	**APPLICATION**	Android

Source- https://thehackernews.com/2024/04/exotic-visit-spyware-campaign-targets.html

Palo Alto firewalls under attack since March with backdoor malware

Since March 26, UTA0218 attackers have been exploiting the CVE-2024-3400 vulnerability in Palo Alto Networks' PAN-OS in the operation MidnightEclipse. This vulnerability allows root-level command execution on firewalls for data theft and network penetration and attackers leverage c2 infrastructure and cron jobs to automate attacks and compromise internal networks. CISA has triggered an urgent response to this, prompting security patches from Palo Alto Networks.

Volexity, the firm that discovered the zero-day vulnerability, found the campaign to be highly targeted with state actors potentially behind it. The attackers exploit Palo Alto Networks' GlobalProtect feature, deploying a custom backdoor named 'Upstyle' to execute commands. The breach extends beyond data theft, with instances of pivoting to internal networks to steal sensitive files and browser data. Similar targeted attacks on network devices, including those by China-linked and Russian state-sponsored groups, bring the increasing vulnerability of edge devices to the forefront.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Palo Alto Networks PAN-OS

Source- https://www.bleepingcomputer.com/news/security/palo-alto-networks-zero-day-exploited-since-march-to-backdoor-firewalls/

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