TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JULY 23RD, 2024

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In the fast-changing world, protecting against cyber threats is top of the agenda for companies. With cyber threats constantly evolving, businesses aim to safeguard their assets and sustain operational stability. It’s not solely about securing data anymore; it’s about bolstering the fundamental frameworks on which modern organisations rely, guaranteeing resilience against a range of emerging threats.

Get your organisation ready with Tata Communications’ weekly threat intelligence advisory. Get the latest threat information and take proactive steps to harden your defences and fix vulnerabilities.

Microsoft patches 142 security flaws, including four zero-days

On Microsoft’s July 2024 Patch Tuesday, the company fixed 142 vulnerabilities across its products including Windows, Office, .NET, Azure, and Xbox. Of these, 139 were new Common Vulnerability Exposures (CVEs) and three were from third-party sources. Five were critical, 133 were important, and three were moderate.

In addition, Microsoft fixed four zero-day vulnerabilities, two of which attackers were actively exploiting: a Windows Hyper-V Elevation of Privilege and a Windows MSHTML Platform Spoofing vulnerability. These vulnerabilities impact critical systems like SQL Server, Windows CoreMessaging, and Microsoft Office. Microsoft urges users to apply the necessary patches to ensure the safety of their systems.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2024-patch-tuesday-fixes-142-flaws-4-zero-days/

Malware spread through fake ebook torrents

ViperSoftX, a malware first spotted in 2020, has undergone several iterations. In the latest iteration, it has been found to spread through torrents posing as eBooks. This sophisticated malware leverages Common Language Runtime (CLR) to execute PowerShell commands within AutoIt. This allows it to skip traditional detection methods. The attackers selectively adapt necessary elements of the existing offensive security scripts to avoid writing new code. Using the existing script enables them to develop the malware quickly and employ strong evasion tactics.

Recent attacks have used ViperSoftX to spread Quasar Remote Access Trojan (RAT) and TesseractStealer, highlighting its evolving competencies. Experts advise that users must exercise caution when downloading ebooks using torrents.

ATTACK TYPE	Malware	SECTOR	Information technology, healthcare, construction, government, energy, BFSI, Aviation, telecommunications
REGION	Global	APPLICATION	Windows

Source - https://www.trellix.com/blogs/research/the-mechanics-of-vipersofts-exploiting-autoit-and-clr-for-stealthy-powershell-execution/

Critical vulnerability detected in WordPress calendar plugin

Cybersecurity experts have reported a critical security flaw (CVE-2024-5441) in the Modern Events Calendar WordPress plugin, used in over 150,000 websites globally. This vulnerability has received a high-severity score of CVSS v3.1: 8.8. Experts indicate that the flaw originates from the lack of file type validation in one of the functions of the plugin. Hackers are actively exploiting this vulnerability to potentially take remote control of vulnerable websites and upload malicious files.

Webnus, the developer of the plugin, has released version 7.12.0 to address this critical flaw. Users are urged to update immediately or disable the plugin to safeguard their sites. Wordfence, a prominent security firm, blocked over 100 exploitation attempts within 24 hours, highlighting the urgency of the situation.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	WordPress

Source - https://www.bleepingcomputer.com/news/security/hackers-target-wordpress-calendar-plugin-used-by-150-000-sites/

Android users targeted by new phishing scam

A new phishing scam impersonating India's Regional Transport Office is targeting Android users in India via WhatsApp. The scam tricks victims into downloading the malicious "VAHAN PARIVAHAN.apk" app, which stealthily collects sensitive data such as SMS messages and contacts. This data is then sent to attackers via Telegram bots. The malware does not feature a launcher icon and operates silently in the background, thus evading detection. This sophisticated approach makes it difficult for users to realise that their data has been compromised.

To protect against such attacks, users should always verify the authenticity of messages, download apps only from trusted sources, keep their devices updated, and use reputable security solutions. Vigilance and proactive security measures are crucial against such malicious phishing scams.

ATTACK TYPE	Phishing	SECTOR	All
REGION	India	APPLICATION	Android

Source - https://cyble.com/blog/regional-transport-office-phishing-scam-targets-android-users-in-india/

Malware targets Middle Eastern militaries

A Houthi-aligned threat actor has launched an ongoing surveillance campaign targeting military personnel in the Middle East. This operation uses an Android data-gathering tool named GuardZoo, which has compromised over 450 victims, mainly in Yemen. GuardZoo, an advanced version of the Dendroid RAT, is engineered to exfiltrate sensitive military data, including photos, documents, and mapping files. The malicious apps are distributed through WhatsApp and direct downloads, making it easier for the malware to infiltrate devices.

GuardZoo's sophisticated capabilities highlight the increasing cybersecurity threats targeting the military in these regions. The malware's design to collect and transmit critical information underscores the importance of robust security measures to protect sensitive military data from such espionage activities.

ATTACK TYPE	Malware	SECTOR	Military
REGION	Egypt, Oman, Qatar, Saudi Arabia, Turkey, United Arab Emirates, Yemen	APPLICATION	Android

Source - https://www.lookout.com/threat-intelligence/article/guardzoo-houthi-android-surveillanceware

GitLab issues updates to critical vulnerabilities

GitLab has issued critical updates to address security vulnerabilities, including CVE-2024-6385. The vulnerability carries a CVSS score of 9.6 out of a maximum of 10.0. This severe flaw enables attackers to execute pipeline jobs as arbitrary users. The vulnerability affects both GitLab Community Edition (CE) and GitLab Enterprise Edition (EE), impacting users globally. The updates follow recent patches aimed at mitigating related issues, underscoring GitLab's commitment to maintaining strong security. This move is part of broader efforts to enhance cybersecurity, as other major companies like Citrix and Broadcom have also released patches to fix significant software flaws.

Meanwhile, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) continue to stress the importance of eliminating OS command injection vulnerabilities. These efforts are crucial in strengthening overall cybersecurity resilience.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	GitLab Community Edition (CE), GitLab Enterprise Edition (EE)

Source - https://thehackernews.com/2024/07/gitlab-patches-critical-flaw-allowing.html

Hackers exploit PHP flaw to spread malware

Hackers are actively exploiting CVE-2024-4577, a critical PHP vulnerability, to distribute remote access trojans, cryptocurrency miners, and DDoS botnets. This vulnerability, publicly disclosed in June 2024, allows remote execution of malicious commands on Windows systems with specific language locales. Threat actors are leveraging this flaw to infiltrate systems globally, affecting all sectors dependent on PHP. The surge in exploitation highlights the urgent need for users and organisations to update their PHP installations to protect against these threats.

Alongside this vulnerability, DDoS attacks have seen a significant year-over-year increase, worsening the cybersecurity landscape. The combination of malware spread through PHP and the rising tide of DDoS attacks underscores the importance of timely updates and tight security measures.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	PHP

Source - https://thehackernews.com/2024/07/php-vulnerability-exploited-to-spread.html

EstateRansomware targets unpatched Veeam backups

EstateRansomware, a new ransomware operation, has exploited a recently patched vulnerability (CVE-2023-27532) in Veeam Backup & Replication software. The initial breach occurred via a Fortinet FortiGate firewall, where attackers used a backdoor to gain further access. This allowed for network discovery and credential harvesting, ultimately leading to ransomware deployment. Researchers have found that EstateRansomware's tactics demonstrate increasing sophistication and diversification, highlighting the evolving threat prospect. This underscores the necessity for vigilant and adaptive cybersecurity measures to counteract such advanced attacks.

The widespread impact of this ransomware affects all sectors relying on Veeam software globally. Cybersecurity experts urge organisations to ensure their systems are updated to the latest patches to resolve these threats.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Veeam

Source - https://thehackernews.com/2024/07/new-ransomware-group-exploiting-veeam.html

APT41 uses new loader for advanced attacks

In April 2024, researchers discovered a previously unknown loader named DodgeBox, displaying remarkable similarities to StealthVector, a malicious program linked to the China-based APT41. DodgeBox operates as a loader for the MoonWalk backdoor, which employs advanced evasion techniques and uses Google Drive for command-and-control communication. A detailed technical analysis has revealed DodgeBox's complex structure and methods, linking this threat to APT41. This sophisticated malware targets Windows systems and underscores the increasing capability of APT41 to conduct advanced cyberattacks.

The discovery of DodgeBox highlights the evolving threat and the necessity for high cybersecurity measures. Users are urged to remain vigilant and adopt adaptive security practices to counteract these advanced threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Asia	APPLICATION	Windows

Source - https://www.zscaler.com/blogs/security-research/dodgebox-deep-dive-updated-arsenal-apt41-part-1

Linux variant of Mallox ransomware reported

The Mallox ransomware threat actors have introduced a new Linux variant. This variant employs custom Python scripts within a Flask-based web panel to manage and deploy ransomware payloads. This web panel can be used to quickly develop customisable ransomware to target Linux systems. Using AES-256 CBC encryption, the ransomware appends a ".locked" extension to the encrypted files and drops a ransom note. As a potential relief to the users, decryptors for several builds have been identified by researchers.

The global impact of this new variant highlights the increasing sophistication of ransomware threats and the importance of remaining vigilant. Organisations using Linux systems are urged to update their security protocols and stay informed about the latest protective measures.

ATTACK TYPE	Ransomware	SECTOR	Information technology, healthcare, manufacturing, construction, government, oil and gas, energy, defence, BFSI, telecommunications
REGION	Global	APPLICATION	Linux

Source - https://www.uptycs.com/blog/mallox-ransomware-linux-variant-decryptor-discovered

TATA COMMUNICATIONS

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.