TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 3, 2024

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As the digital landscape is constantly evolving, cyber threats are also evolving with equal vigour. Organisations worldwide are focusing on safeguarding their data and strengthening their core security frameworks. Staying updated on emerging cyberattack trends and promptly implementing security updates is vital for any organisation to protect its resources from potential threats.

Tata Communications' weekly threat intelligence advisory has been designed to help you stay ahead of the curve. By providing insights into the latest cyber risks, this report empowers you to implement proactive strategies to strengthen your defences and effectively mitigate potential vulnerabilities.

New malware exploits PHP flaw

Researchers have uncovered a new backdoor malware variant, Msupedge, targeting a Taiwanese university. This malware leverages DNS tunnelling to evade detection with its command-and-control server. Msupedge exploits a critical vulnerability in PHP (CVE-2024-4577, CVSS score: 9.8) and executes through dynamic-link libraries (DLLs). The backdoor's commands are linked to specific IP address segments, triggering a range of malicious actions. The malware is deployed via DLL files and responds to specific IP address octets to execute various commands.

Experts also linked the UTG-Q-010 threat group to a related phishing campaign distributing Pupy RAT, highlighting the evolving sophistication of cyberattacks. This incident underscores the importance of software updates and vigilance against phishing attempts for educational institutions.

ATTACK TYPE	Malware	SECTOR	Education
REGION	Taiwan	APPLICATION	PHP

Source - https://thehackernews.com/2024/08/hackers-exploit-php-vulnerability-to.html

WordPress plugin poses a critical risk

A critical vulnerability (CVE-2024-5932, CVSS score: 10.0) has been identified in the WordPress GiveWP plugin, putting over 100,000 websites at significant risk of remote code execution attacks. The vulnerability affects all versions of the plugin prior to 3.14.2, which was released on August 7, 2024. By exploiting this flaw, attackers can potentially gain full control over affected websites, leading to severe security breaches. WordPress site owners are strongly urged to update to the latest version immediately to mitigate this risk.

Researchers have uncovered severe vulnerabilities in other popular WordPress plugins, emphasising the importance of regular updates and the use of legitimate software. These findings underscore the critical need for ongoing vigilance in website maintenance, as outdated or unpatched plugins continue to be a major target for cybercriminals.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	WordPress

Source - https://thehackernews.com/2024/08/givewp-wordpress-plugin-vulnerability.html

CERT-UA alerts on new phishing campaign

CERT-UA has issued an urgent warning about a new phishing campaign orchestrated by the Vermin group. The attackers are distributing malware through emails that feature fake prisoner-of-war photos, a tactic designed to lure victims into opening a malicious ZIP file. Once opened, the file installs the spyware SPECTR and a newly identified malware, FIRMACHAGENT, on the victim's device. FIRMACHAGENT is particularly dangerous as it steals sensitive data and transmits it to a remote server controlled by the attackers.

The Vermin group, linked to the Luhansk People's Republic, has previously targeted Ukraine's defence forces, and this latest campaign continues to pose a significant threat. The alert serves as a critical reminder for all sectors in Ukraine to maintain heightened vigilance against such sophisticated phishing attacks.

ATTACK TYPE	Malware	SECTOR	All
REGION	Ukraine	APPLICATION	Windows

Source - https://thehackernews.com/2024/08/cert-ua-warns-of-new-vermin-linked.html

INTRODUCTION | MALWARE EXPLOITS PHP FLAW | WORDPRESS PLUGIN POSES A RISK | CERT-UA ALERTS ON PHISHING | RAT MOONPEAK UNVEILED | PHISHING COMPROMISES MOBILE BANKING | GHES FLAWS PATCHED | MALWARE EXPLOITS POSTGRESQL | CRYPTOMINING MALWARE TARGETS MACOS | CRITICAL FLAW IN SOLARWINDS WHD | APT TARGETS POLITICAL CAMPAIGNS

Advanced RAT MoonPeak unveiled

Researchers have identified a sophisticated new Remote Access Trojan (RAT) called “MoonPeak,” linked to the North Korean cyber threat cluster UAT-5394. This advanced malware, an evolution of XenoRAT, reflects the group’s evolving strategies and increasingly complex infrastructure. MoonPeak targets both Windows and Linux systems, enhancing its threat potential on a global scale. The development of this malware suggests possible ties to the notorious Kimsuky group, known for cyberespionage activities.

The discovery of MoonPeak underscores the growing capabilities of these threat actors and highlights the critical need for strong, multi-layered cybersecurity defences across all sectors. As cyber threats become more sophisticated, organisations worldwide must remain vigilant and proactive in fortifying their security measures to counter these evolving dangers.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows, Linux

Source - https://securityonline.info/north-korean-hackers-upgrade-arsenal-with-moonpeak-rat/

INTRODUCTION | MALWARE EXPLOITS PHP FLAW | WORDPRESS PLUGIN POSES A RISK | CERT-UA ALERTS ON PHISHING | RAT MOONPEAK UNVEILED | PHISHING COMPROMISES MOBILE BANKING | GHES FLAWS PATCHED | MALWARE EXPLOITS POSTGRESQL | CRYPTOMINING MALWARE TARGETS MACOS | CRITICAL FLAW IN SOLARWINDS WHD | APT TARGETS POLITICAL CAMPAIGNS

Phishing campaign targets banking credentials

A new phishing campaign is targeting mobile users through Progressive Web Applications (PWAs) to steal banking credentials. The attacks focus on users in the Czech Republic, Hungary, and Georgia, exploiting Chrome's WebAPK technology on Android and deceptive installation prompts on iOS. These tactics allow the malicious apps to bypass security warnings, making them appear legitimate to unsuspecting users. Researchers have traced the campaign back to two different threat actors, indicating a sophisticated and evolving cyber threat landscape.

The use of PWAs in this campaign marks a significant advancement in phishing techniques, particularly in how they exploit mobile technologies to bypass traditional security measures. This emerging threat underscores the need for mobile users to exercise caution when installing apps and to remain vigilant against suspicious prompts that could compromise their banking information.

ATTACK TYPE	Malware	SECTOR	BFSI
REGION	Czech Republic, Hungary, Georgia	APPLICATION	Android, iOS

Source - https://thehackernews.com/2024/08/czech-mobile-users-targeted-in-new.html

GitHub enterprise server flaws patched

GitHub has disclosed several critical vulnerabilities in the GitHub Enterprise Server (GHES), including a severe SAML authentication flaw (CVE-2024-6800) that could allow attackers to gain administrative access. Other vulnerabilities identified include unauthorised access to private repository data (CVE-2024-6337) and the ability to manipulate issue metadata (CVE-2024-7711). These flaws pose significant security risks, potentially compromising sensitive information and system integrity.

GitHub has released security updates addressing these vulnerabilities, and users are strongly advised to update their GHES installations immediately to mitigate potential threats. This incident serves as a reminder of the critical need for continuous vigilance in maintaining the security of enterprise software environments.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	GitHub Enterprise Server (GHES)

Source - https://securityonline.info/cve-2024-6800-cvss-9-5-critical-github-enterprise-server-flaw-patched-admin-access-at-risk/

INTRODUCTION | MALWARE EXPLOITS PHP FLAW | WORDPRESS PLUGIN POSES A RISK | CERT-UA ALERTS ON PHISHING | RAT MOONPEAK UNVEILED | PHISHING COMPROMISES MOBILE BANKING | GHES FLAWS PATCHED | MALWARE EXPLOITS POSTGRESQL | CRYPTOMINING MALWARE TARGETS MACOS | CRITICAL FLAW IN SOLARWINDS WHD | APT TARGETS POLITICAL CAMPAIGNS

Malware exploits PostgreSQL for crypto mining

Researchers have discovered a new malware strain named PG_MEM, which is targeting PostgreSQL databases by brute-forcing weak passwords. Once the attackers gain access, they exploit the COPY ... FROM PROGRAM SQL command to execute shell commands, download malicious payloads, and deploy a Monero cryptocurrency miner. This attack primarily affects internet-facing Postgres databases with weak Passwords.

The PG_MEM malware underscores the significant risks posed by misconfigured databases and weak security practices, particularly in environments where critical data is stored. The use of brute-force attacks to compromise PostgreSQL systems highlights the need for stronger password policies and regular security audits to protect against such threats. Organisations relying on PostgreSQL databases are advised to review and enhance their security configurations to prevent similar incidents.

ATTACK TYPE	Malware	SECTOR	All
REGION	Russia, China, Germany, Poland, United States	APPLICATION	PostgreSQL

Source - https://thehackernews.com/2024/08/new-malware-pgmem-targets-postgresql.html

Malware targets macOS systems

Researchers have uncovered a new macOS malware strain named "TodoSwift," linked to North Korean hacking groups, specifically the Lazarus Group's BlueNoroff subgroup. TodoSwift bears similarities to previous malware like RustBucket and KANDYKORN, and it primarily targets the cryptocurrency sector. The malware is designed to collect system information and execute additional malicious payloads, posing a significant threat to macOS users. Security experts from Apple have indicated that TodoSwift is distributed in the form of a signed file named TodoTasks, which includes a dropper component.

TodoSwift's sophisticated infection methods highlight the ongoing risks for users within the cryptocurrency industry and beyond. The discovery underscores the importance of maintaining robust cybersecurity practices on macOS systems, particularly in sectors that are frequently targeted by advanced threat actors. As macOS continues to be a target, users are advised to stay vigilant and ensure their security measures are up to date to mitigate these evolving threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	macOS

Source - https://thehackernews.com/2024/08/new-macos-malware-todoswift-linked-to.html

Critical flaw detected in SolarWinds software

SolarWinds has issued an urgent advisory for its Web Help Desk (WHD) software due to a critical vulnerability with a CVSS score of 9.1. This flaw allows unauthorised remote access, putting affected systems at high risk of data breaches and operational disruptions. As WHD is a widely used helpdesk software handling sensitive support tickets, customer data, and critical IT operations, the implication of this vulnerability can be severe.

SolarWinds has released SolarWinds Web Help Desk 12.8.3 Hotfix 2 to address this issue and strongly recommends that all users apply it immediately to mitigate the threat. The discovery of this vulnerability highlights the ongoing risks associated with software security and the importance of promptly addressing critical flaws.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	SolarWinds Web Help Desk

Source - https://securityonline.info/solarwinds-web-help-desk-hit-by-critical-vulnerability-cve-2024-28987/

INTRODUCTION | MALWARE EXPLOITS PHP FLAW | WORDPRESS PLUGIN POSES A RISK | CERT-UA ALERTS ON PHISHING | RAT MOONPEAK UNVEILED | PHISHING COMPROMISES MOBILE BANKING | GHES FLAWS PATCHED | MALWARE EXPLOITS POSTGRESQL | CRYPTOMINING MALWARE TARGETS MACOS | CRITICAL FLAW IN SOLARWINDS WHD | APT TARGETS POLITICAL CAMPAIGNS

APT group targets political campaigns

The GreenCharlie APT group, linked to Iran-backed Advanced Persistent Threat (APT) group, has been actively targeting US political campaigns since May 2024. This group has been reportedly building and spreading a sophisticated network of malicious infrastructure. It uses this infrastructure in various cyberespionage activities aimed at high-ranking government officials. It employs advanced phishing techniques and deploys malware such as GORBLE, POWERSTAR, and NokNok to exfiltrate sensitive information from its targets. These operations are part of a broader strategy aimed at intelligence-gathering and geopolitical interference.

GreenCharlie's use of a sophisticated malicious infrastructure highlights the ongoing threat to government sectors, particularly those involved in political processes. The group's activities underscore the need for robust cybersecurity measures to defend against state-sponsored threats. Organisations involved in political campaigns are urged to remain vigilant and implement advanced security protocols to counter these evolving threats.

ATTACK TYPE	Malware	SECTOR	Government
REGION	United States	APPLICATION	Generic

Source - https://securityonline.info/iranian-apt-greencharlie-escalates-threats-against-us-political-targets-using-gorble-and-powerstar-malware/

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.