TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 1, 2024

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In the ever-changing global arena, safeguarding against cyber threats has become paramount for organisations. As these threats evolve ceaselessly, businesses strive not only to protect their data but also to fortify the essential structures that underpin modern operations. It’s about ensuring resilience against a spectrum of emerging threats.

Enhance your organisation’s cybersecurity preparedness with Tata Communications’ weekly threat intelligence advisory. Acquire invaluable insights into the latest cyber risks and enact proactive strategies to fortify your defences, adeptly addressing potential vulnerabilities.

Critical VMware vCenter flaw patched

Broadcom has issued a patch for a critical vulnerability (CVE-2024-38812) in VMware vCenter Server that could enable remote code execution through a crafted network packet. The flaw was uncovered during the 2024 Matrix Cup hacking competition in China. Though there are no signs of active exploitation, the vulnerability presents a serious threat to virtualised environments. Broadcom advises all users to apply the patch immediately. If patching is not feasible, organisations should enforce strict perimeter controls. Broadcom has also patched a related flaw (CVE-2024-38813) that could be used for privilege escalation.

This vulnerability highlights the importance of regular updates and proactive cybersecurity measures to mitigate emerging risks to essential infrastructure. Failure to patch such flaws can leave critical systems exposed to potential attacks.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	VMware vCenter Server

Source - https://www.bleepingcomputer.com/news/security/broadcom-fixes-critical-rce-bug-in-vmware-vcenter-server/

RustDoor malware campaign targets LinkedIn users

North Korean cybercriminals have launched a new malware campaign targeting LinkedIn users by masquerading as recruiters from legitimate cryptocurrency exchanges. The attackers are using social engineering tactics, persuading victims to download RustDoor malware by presenting it as part of coding challenges. This campaign focuses on infiltrating networks within the financial services and cryptocurrency sectors, with a particular emphasis on macOS users. The goal of these attacks is to raise funds for the Democratic People's Republic of Korea (DPRK) through illicit means.

Users are urged to exercise caution when receiving unsolicited messages from LinkedIn recruiters, especially in the cryptocurrency space. Ensuring up-to-date antivirus protections and practising vigilance with social media interactions can help mitigate the risks posed by this malware campaign.

ATTACK TYPE	Social engineering, malware	SECTOR	BFSI
REGION	South America, Europe, Africa, and Asia	APPLICATION	macOS

Source - https://thehackernews.com/2024/09/north-korean-hackers-target.html

UNC2970 deploys new backdoor

A North Korean-linked hacking group, UNC2970, has launched a new cyberespionage campaign aimed at senior executives in critical sectors such as energy and aerospace. The group is using phishing emails to deliver a trojanised version of SumatraPDF, which installs a backdoor named MISTPEN, granting attackers remote control over compromised systems. This stealthy attack is disguised as legitimate job opportunities to lure high-profile individuals into downloading the malicious software.

While the attack targets organisations worldwide, its primary focus is on high-value industries. Companies are urged to remain vigilant against phishing attempts and ensure that their employees are aware of the risks posed by unsolicited job offers. Strengthening cybersecurity protocols, especially in sectors handling sensitive data, is essential to prevent these advanced threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://securityonline.info/unc2970s-backdoor-deployed-via-trojanized-pdf-reader-targets-critical-infrastructure/

Fake CAPTCHA tests deliver Lumma Stealer

Cybersecurity experts have uncovered a new malware campaign that uses counterfeit CAPTCHA tests to compromise Windows systems. In these attacks, users are tricked into pressing “Windows + R” followed by “CTRL + V” and “Enter” sequence, which triggers the execution of a PowerShell script that installs the Lumma Stealer malware. Once installed, the malware can extract sensitive data, including passwords and cryptocurrency wallet credentials.

Users must exercise caution when encountering CAPTCHA challenges, especially on unfamiliar or suspicious websites, They must verify the legitimacy of websites and ensure their security software is up to date. The emergence of this attack highlights the increasing sophistication of malware distribution techniques.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://securityonline.info/cybercriminals-exploit-captcha-to-deliver-malware-experts-issue-warning/

Black Maskers intensify attacks

The hacktivist group Black Maskers has intensified its cyber offensive, moving beyond Distributed Denial of Service (DDoS) attacks to exploiting vulnerabilities in web applications. In a recent incident, they targeted a major Saudi platform, leading to significant disruptions. The group, driven by geopolitical motives, has threatened with future attacks on other platforms in the Middle East.

Experts warn that without enhanced cybersecurity protocols, organisations could face significant data breaches and operational failures. The group's advanced tactics demonstrate a growing capability to target essential services, making it crucial for affected sectors to implement immediate defensive measures. Cybersecurity professionals urge users to remain vigilant, patch vulnerabilities, and bolster defences to mitigate these evolving threats.

ATTACK TYPE	Hacktivism	SECTOR	All
REGION	Israel, Saudi Arabia, United Arab Emirates, United States	APPLICATION	IT, healthcare, manufacturing, construction, government, education, oil and gas, energy, defence, business, e-commerce, BFSI, aviation, mining, telecommunications

Source -

Earth Baxia targets APAC with new malware

Earth Baxia, a highly sophisticated cyberespionage group, has launched targeted attacks on government entities and critical sectors across the Asia-Pacific (APAC) region. Their campaign utilises spear-phishing emails and exploits a critical vulnerability (CVE-2024-36401) in GeoServer to deploy malware, including Cobalt Strike and a newly discovered backdoor called EAGLEDOOR. These tools allow Earth Baxia to steal sensitive data and maintain long-term access to compromised systems. Cybersecurity experts have also noted links between Earth Baxia's infrastructure and China, raising concerns about potential state-sponsored operations.

The ongoing espionage efforts highlight the need for immediate patching of vulnerabilities and increased awareness of phishing tactics to prevent further infiltration. Organisations in the APAC region are urged to bolster their cybersecurity measures to defend against these advanced threats.

ATTACK TYPE	Malware	SECTOR	IT, healthcare, BFSI, government, energy, manufacturing, oil and gas, energy, defence, aviation, e-commerce, chemical manufacturing, telecommunications
REGION	APAC	APPLICATION	Windows

Source - https://securityonline.info/sophisticated-cyber-espionage-earth-baxia-uses-cve-2024-36401-and-cobalt-strike-to-infiltrate-apac/

INTRODUCTION | CRITICAL VMWARE FLAW PATCHED | HACKERS TARGET LINKEDIN USERS | UNC2970 DEPLOYS NEW BACKDOOR | FAKE CAPTCHA DELIVER MALWARE | BLACK MASKERS ESCALATE ATTACKS | NEW APAC CYBER THREATS | KIMSUKY TARGETS ACADEMICS | GOMORRAH STEALER MALWARE | NEW RAT TARGETS USERS | EMS VULNERABILITY EXPLOITED

Kimsuky targets academic institutions

A new cyberattack campaign linked to the Kimsuky group is targeting academic institutions worldwide. The attackers disguise malicious files as lecture requests in Hangul document (HWP) and MSC formats, sent via spear-phishing emails. Once opened, the files download additional malware that can exfiltrate sensitive information, putting educational institutions at significant risk. The malware also leverages cloud platforms like Google Drive to manage command-and-control functions, increasing the attack's sophistication.

This campaign bears resemblance to earlier Kimsuky operations, which are often attributed to state-sponsored motives. As the education sector becomes a more frequent target of cyberespionage, experts urge academic institutions to implement stronger cybersecurity measures, including scrutinising unsolicited email attachments and maintaining updated antivirus software. The attack highlights the growing vulnerability of academia to sophisticated cyber threats, making vigilance crucial to safeguarding sensitive research and institutional data.

ATTACK TYPE	Malware	SECTOR	Education
REGION	Global	APPLICATION	Windows

Source - https://asec.ahnlab.com/ko/83239/

INTRODUCTION | CRITICAL VMWARE FLAW PATCHED | HACKERS TARGET LINKEDIN USERS | UNC2970 DEPLOYS NEW BACKDOOR | FAKE CAPTCHA DELIVER MALWARE | BLACK MASKERS ESCALATE ATTACKS | NEW APAC CYBER THREATS | KIMSUKY TARGETS ACADEMICS | GOMORRAH STEALER MALWARE | NEW RAT TARGETS USERS | EMS VULNERABILITY EXPLOITED

Gomorrah stealer threatens user data

Gomorrah Stealer, a sophisticated malware operating as Malware-as-a-Service (MaaS), is rapidly gaining traction as a significant threat to user data. This malware is designed to steal sensitive information such as passwords, credit card details, and browser cookies from infected systems. Its developers have employed advanced evasion techniques and persistence strategies, making detection and removal more difficult.

Distributed via Telegram, Gomorrah Stealer continuously evolves, with frequent updates enhancing its capabilities. The malware's ability to bypass traditional defences emphasises the need for strong cybersecurity measures, including regular software updates and stronger access controls, to protect against this growing menace. Security experts advise users to stay vigilant, particularly when interacting with Telegram channels, and to implement multi-layered defences to reduce exposure to such malware threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyfirma.com/research/gomorrah-stealer-v5-1-an-in-depth-analysis-of-a-net-based-malware/

SambaSpy malware targets users with phishing emails

A cyberattack campaign discovered in May 2024 has been targeting Italian users through phishing emails disguised as legitimate invoices. The attackers delivered a new Remote Access Trojan (RAT) named SambaSpy, designed specifically for Italian-speaking victims. To ensure that only Italian users were infected, the phishing campaign incorporated multiple checks during the attack process.

SambaSpy, a Java-based RAT, offers a range of malicious capabilities, including file management, credential theft, and remote desktop control. Security researchers believe Brazilian threat actors are behind the campaign, given the technical and linguistic aspects of the operation. The malware's focus on a single nation makes this attack highly targeted, requiring businesses and individuals in Italy to remain vigilant against phishing scams. To mitigate the threat, experts recommend users avoid clicking on suspicious email links and strengthen their cybersecurity measures.

ATTACK TYPE	Malware	SECTOR	All
REGION	Italy	APPLICATION	Windows

Source - https://securelist.com/sambaspy-rat-targets-italian-users/113851/

Cyberattacks exploit Fortinet FortiClient EMS vulnerability

Researchers have uncovered a series of cyberattacks exploiting a critical SQL injection vulnerability (CVE-2023-48788) in Fortinet's FortiClient Endpoint Management Server (EMS). This flaw allows attackers to gain unauthorised access and execute remote code within compromised systems. Once inside, cybercriminals employed legitimate Remote Monitoring and Management (RMM) tools to maintain persistence, conduct internal reconnaissance, and escalate privileges.

The attack also involved lateral movement across affected networks, demonstrating increasingly sophisticated post-exploitation tactics by cybercriminals. Fortinet has issued patches for the vulnerability, and organisations using FortiClient EMS are urged to update their systems immediately to avoid further exploitation.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Fortinet

Source - https://securityonline.info/cve-2023-48788-exploited-researcher-details-cyberattacks-on-fortinet-ems/

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.