TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 9, 2024

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As the digital landscape continues to evolve, cyber threats are intensifying with equal vigour. Companies worldwide are focusing on safeguarding their data and reinforcing their core security frameworks. Staying informed about emerging cyberattack trends and proactively implementing security updates are imperative for any organisation to protect its resources from potential threats.

Tata Communications' weekly threat intelligence advisory is designed to help you stay ahead of the curve. By offering insights into the latest cyber risks, this report empowers you to implement proactive strategies to strengthen your defences against potential cyber vulnerabilities.

Kimsuky's HappyDoor malware poses persistent threat

Kimsuky's HappyDoor malware has been a persistent cyber threat since 2021. HappyDoor features hard-coded version details and unique execution arguments. It spreads primarily via spear-phishing emails containing obfuscated scripts. Upon execution, the malware operates in three stages—install*, init*, and run*—to conduct various malicious activities, including information theft and backdoor operations.

Analysts named the malware “HappyDoor” after finding the “happy” string in its code. Recent investigations show HappyDoor is frequently patched, making it a significant threat. Security experts advise constant vigilance and updated defences to counteract its sophisticated operations. The malware's stealthy nature and persistent updates highlight the ongoing cyber risk posed by Kimsuky's tactics.

ATTACK TYPE	Malware	SECTOR	Healthcare, financial services, manufacturing, construction, IT, government, oil and gas, energy, defence, e-commerce, BFSI, aviation, automobile, telecommunications
REGION	Global	APPLICATION	Windows

Source - https://asec.ahnlab.com/ko/67128/

Critical security flaw discovered in MOVEit software

A critical vulnerability, CVE-2024-5806, has been discovered in MOVEit Transfer software, scoring 9.1 on the CVSS scale. This flaw allows attackers to bypass SFTP authentication and access sensitive data. Progress Software has urgently issued patches for affected versions due to immediate exploitation attempts. Another critical vulnerability, CVE-2024-5805, with the same CVSS score, also affects MOVEit Gateway.

This vulnerability also poses significant risks of unauthorised access and potential data breaches. MOVEit Gateway version 2024.0.0 is specifically impacted, and Progress Software has released a patch (MOVEit Gateway 2024.0.1). The developer stresses the importance of promptly applying the patch despite any temporary system outage it may cause, citing substantial security benefits. These vulnerabilities highlight the ongoing risks to enterprises managing large volumes of sensitive data.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://securityonline.info/cve-2024-5805-critical-sftp-authentication-bypass-vulnerability-in-moveit-gateway/

New Medusa Android banking trojan attacks

Cybersecurity researchers have discovered an updated version of the Medusa Android banking trojan, now targeting users in Canada, France, Italy, Spain, Turkey, the UK, and the US. Active since July 2023, the new variant operates through five botnets. It includes features like full-screen overlays and remote app uninstallation.

Researchers noted the trojan's ability to read SMS messages, log keystrokes, capture screenshots, and perform unauthorised fund transfers. The malware uses dropper apps disguised as updates and utilises legitimate apps such as Telegram to retrieve command-and-control (C2) servers. Researchers highlight the strategic reduction of permissions to enhance the trojan’s stealth and effectiveness. This evolution reflects the deliberate efforts by threat actors to diversify their targets and broaden their attack surface.

ATTACK TYPE	Malware	SECTOR	BFSI
REGION	Canada, UK, France, Italy, Spain, Turkey, United States	APPLICATION	Android

Source - https://thehackernews.com/2024/06/new-medusa-android-trojan-targets.html

INTRODUCTION | HAPPYDOOR MALWARE POSES THREAT | CRITICAL SECURITY FLAW IN MOVEIT | TROJAN MEDUSA LAUNCHES ATTACKS | UAC-0184 CAMPAIGN SPREADS RAT | RANSOMWARE TARGETS GOVERNMENT ENTITIES | BACKDOOR TARGETS AEROSPACE AND DEFENCE | ATTACKERS EXPLOIT MS WORD FLAW | CISA ADDS NEW FLAWS TO KEV | SPYWARE DEPLOYED VIA MS OFFICE FLAW | LULZSEC THREATENS INDIAN BANKS

UAC-0184 malware campaign distributes RAT

The threat actor group UAC-0184 has recently targeted Ukraine with a malware campaign employing a malicious .lnk file to deploy the XWorm Remote Access Trojan (RAT). This attack involves a PowerShell script that downloads a ZIP file containing malicious Python components, using DLL sideloading and Shadowloader techniques.

Previously, this group targeted Ukrainian entities in Finland using the Remcos RAT. The current campaign involves deceptive documents to distribute XWorm RAT, reflecting persistent efforts to infiltrate Ukrainian systems. The use of Python-related files and advanced evasion techniques highlights the ongoing threat posed by UAC-0184.

ATTACK TYPE	Malware	SECTOR	IT, healthcare, financial services, pharmaceuticals, manufacturing, construction, government, oil and gas, energy, defence, BFSI, aviation, automobile, mining, telecommunications
REGION	Ukraine	APPLICATION	Windows

Source - https://cyble.com/blog/uac-0184-abuses-python-in-dll-sideloading-for-xworm-distribution/

INTRODUCTION | HAPPYDOOR MALWARE POSES THREAT | CRITICAL SECURITY FLAW IN MOVEIT | TROJAN MEDUSA LAUNCHES ATTACKS | UAC-0184 CAMPAIGN SPREADS RAT | RANSOMWARE TARGETS GOVERNMENT ENTITIES | BACKDOOR TARGETS AEROSPACE AND DEFENCE | ATTACKERS EXPLOIT MS WORD FLAW | CISA ADDS NEW FLAWS TO KEV | SPYWARE DEPLOYED VIA MS OFFICE FLAW | LULZSEC THREATENS INDIAN BANKS

Ransomware targets global government entities

Between 2021 and 2023, cyber espionage campaigns linked to China and North Korea targeted global government entities and critical infrastructure with ransomware attacks. Researchers identified two main clusters of activity: one attributed to the ChamelGang and the other to Chinese and North Korean state-sponsored threat actors. ChamelGang, believed to be a China-linked group, operates with varied motivations, including intelligence gathering and financial gain.

The ChamelGang attack involved CatB ransomware and Cobalt Strike against high-profile organisations like the All India Institute of Medical Sciences and the Presidency of Brazil. These sophisticated attacks blur the lines between cybercrime and espionage, complicating attribution and response efforts. The attacks also involve tools like Jetico BestCrypt and Microsoft BitLocker, targeting industries across North America, South America, and Europe. The tactics observed align with those used by APT41 and Andariel, state-sponsored groups from China and North Korea.

ATTACK TYPE	Malware	SECTOR	Healthcare, manufacturing, aviation
REGION	North America, South America, Europe, India, East Asia	APPLICATION	Generic

Source - https://thehackernews.com/2024/06/chinese-and-n-korean-hackers-target.html

Novel backdoor attacks aerospace and defence sectors

Experts have uncovered a series of sophisticated cyberattacks by North Korean state-sponsored hackers targeting the aerospace and defence sectors. The key feature of these attacks is the newly identified “Niki” backdoor, which allows attackers to exfiltrate data, execute commands, and manipulate files. The campaign, linked to the Kimsuky group (APT43), began in late May 2024. It employs advanced obfuscation techniques and multiple stages to evade detection and delivers the Niki backdoor. Niki is written in various programming languages, including Go.

This development highlights the increasing sophistication of North Korean cyber operations. The analysis underscores the significant risk posed by these attackers to global cybersecurity. Organisations are urged to remain vigilant, use advanced detection tools, and educate their workforce to mitigate these evolving threats.

ATTACK TYPE	Malware	SECTOR	Aerospace, defence
REGION	Global	APPLICATION	Windows

Source - https://securityonline.info/new-north-korean-backdoor-niki-targets-aerospace-and-defense-sectors/

Cyberattack campaign exploits Microsoft Word vulnerability

Cybersecurity researchers have identified a sophisticated cyberattack campaign using a weaponised Microsoft Word document, named FAKTURA.docx, to deploy the Remcos RAT. This malware grants attackers full control over infected systems, leading to potential data breaches, surveillance, and corporate espionage.

The attack exploits a known vulnerability (CVE-2017-11882) in Microsoft Word's Equation Editor. It uses URL shorteners and steganography to evade detection, hiding malicious scripts within seemingly harmless images. These scripts, once activated, download and execute the Remcos RAT. The attackers gain the ability to execute commands, steal data, and monitor user activity. Organisations are advised to implement robust security measures, keep software updated, and educate users on recognising suspicious documents to mitigate these threats effectively.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Microsoft Word

Source - https://securityonline.info/beware-of-word-remcos-rat-lurks-in-malicious-documents/

INTRODUCTION | HAPPYDOOR MALWARE POSES THREAT | CRITICAL SECURITY FLAW IN MOVEIT | TROJAN MEDUSA LAUNCHES ATTACKS | UAC-0184 CAMPAIGN SPREADS RAT | RANSOMWARE TARGETS GOVERNMENT ENTITIES | BACKDOOR TARGETS AEROSPACE AND DEFENCE | ATTACKERS EXPLOIT MS WORD FLAW | CISA ADDS NEW FLAWS TO KEV | SPYWARE DEPLOYED VIA MS OFFICE FLAW | LULZSEC THREATENS INDIAN BANKS

CISA adds three vulnerabilities to its KEV catalogue

The US Cybersecurity and Infrastructure Security Agency (CISA) has added three critical vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue. These include a remote code execution flaw in GeoServer (CVE-2022-24816), a privilege escalation issue in the Linux Kernel (CVE-2022-2586), and a cross-site scripting vulnerability in Roundcube Webmail (CVE-2020-13965). Organisations are urged to apply patches by 17 July 2024 to mitigate these threats.

The GeoServer flaw, with a CVSS score of 9.8, could be exploited to achieve remote code execution. The Linux Kernel issue, scored 7.8, could lead to privilege escalation. The Roundcube Webmail vulnerability, scored 6.1, is a cross-site scripting (XSS) flaw that allows arbitrary JavaScript execution via XML attachments. Despite the availability of proof-of-concept exploits, there have been no reports of active exploitation before CISA's alert.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Linux, Roundcube webmail servers

Source - https://www.securityweek.com/cisa-warns-of-exploited-geoserver-linux-kernel-and-roundcube-vulnerabilities/

Attackers leverage Microsoft Office flaw to deploy spyware

Analysts have identified an attack leveraging the CVE-2021-40444 vulnerability in Microsoft Office, leading to the deployment of the spyware MerkSpy. This spyware monitors user activities and captures sensitive data without consent. The attack starts with a deceptive Microsoft Word document that, when opened, exploits the MSHTML component vulnerability.

The document downloads a malicious HTML file, "olerender.html," containing shellcode to fetch a secondary payload, "GoogleUpdate," which is MerkSpy. The spyware then injects itself into system processes and ensures persistence by disguising itself as a legitimate Google update. This sophisticated spyware captures keystrokes, screenshots, and Chrome login data, transmitting this information to remote servers controlled by attackers.

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

Source - https://www.fortinet.com/blog/threat-research/merkspy-exploiting-cve-2021-40444-to-infiltrate-systems

Attack group LulzSec threatens banks

The notorious cyber threat group LulzSec has threatened to target Indian banks. This warning follows a series of DDoS attacks, data breaches, and web page defacements impacting financial institutions in the UK, Europe, the US, and Israel. Hacktivist groups are reportedly targeting Indian banks due to the country's political stance on the Israel-Palestine conflict. Indian digital wallets and banking applications are at a high risk of exploitation.

In June, various cyber threat actors claimed responsibility for DDoS attacks using freely available tools and scripts from GitHub. Some hackers have also taken control of the social media accounts of major banks to promote cryptocurrency scams. Financial institutions are urged to enhance security measures, including multi-factor authentication, strong passwords, regular audits, and cloud-based DDoS protection services.

ATTACK TYPE	Hacktivism	SECTOR	BFSI
REGION	India	APPLICATION	Generic

Source - https://identityweek.net/lulzsec-cyber-threat-group-claims-attacks-on-indian-banks/

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.