TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 17, 2024

THREAT INTELLIGENCE ADVISORY REPORT

In an era of more complex digital threats, organisations must emphasise not only data protection but also the reinforcement of their overall security architecture. The rapid evolution of cyber threats necessitates businesses be watchful and flexible, ensuring that their defences are resilient to a wide range of possible attacks. A comprehensive approach to cybersecurity, one that anticipates emerging risks, is essential for maintaining the integrity of business operations.

Stay ahead in the ever-shifting cybersecurity landscape with Tata Communications' weekly threat intelligence advisory. This resource provides you with timely insights into the latest cyber threats, enabling you to proactively enhance your preparedness. By staying informed and prepared, your organisation can better safeguard its critical assets and reduce the likelihood of falling victim to new and vicious cyber threats.

Godzilla WebShell malware hits financial institutions

Cybersecurity researchers recently uncovered a sophisticated cyberattack targeting financial institutions with vulnerable ASP.NET installations. Attackers used the ViewState function in ASP.NET to spread Godzilla WebShell malware, allowing remote command execution. This fileless assault is extremely difficult to detect since it bypasses traditional security procedures. The attack, which impacts the banking, financial services, and insurance (BFSI) sector globally, emphasises the importance of strong web application security.

To prevent future breaches, experts propose enabling ViewState MAC validation and using memory-based threat detection systems. Financial institutions are being urged to tighten their defences as the risks of similar assaults continue to increase. Regular security audits and updates are crucial for maintaining a secure environment. The attacks serve as a reminder for organisations to reevaluate their web application security protocols.

ATTACK TYPE	Malware	SECTOR	BFSI
REGION	Global	APPLICATION	Generic

Source - https://asec.ahnlab.com/ko/82668/

noMU backdoor attacks Exchange server users

An unknown attacker unleashed powerful reverse shells and backdoors targeting users in South Korea. To gain access to computers, the attacker used spear phishing techniques as well as vulnerabilities in Microsoft Exchange server and Internet Information Services (IIS). The malware used in the attack includes a reverse shell malware presumed to be self-created, a backdoor developed in Python called noMu, and a Chinese backdoor called Fxfdoor whose source code has been made public. Although the specific purpose is unknown, preliminary analysis indicates that the attacker intended to steal sensitive data such as web browser credentials.

This attack emphasises the necessity of safeguarding email and web services, especially for individuals and organisations that rely on Microsoft infrastructure. Experts advise rapid patching of known vulnerabilities in Exchange and IIS to avoid similar invasions. Regular security updates and comprehensive monitoring are essential to protect against evolving cyber threats and safeguard sensitive information.

ATTACK TYPE	Malware	SECTOR	All
REGION	South Korea	APPLICATION	Microsoft Exchange Server, Microsoft Internet Information Services (IIS)

Source - https://asec.ahnlab.com/ko/82628/

BMOF exploited to distribute XMRig miner

A new attack method has emerged, which uses Binary Managed Object Files (BMOF) to deploy the XMRig cryptocurrency miner. The attackers use BMOF files, which are part of Windows Management Instrumentation (WMI), to run malicious programs like JScript and VBScript. They acquire persistent access to the hacked systems by utilising Permanent Event Subscriptions. The assault executes the BMOF files using the "mofcomp.exe" Windows program, allowing for stealthy currency mining. This strategy targets a wide range of systems and has an impact across various industries, emphasising the importance of being vigilant when managing WMI configuration.

To avoid such assaults, experts advocate monitoring WMI operations frequently and removing unnecessary services. Implementing strict controls over script execution and performing routine security audits can also help identify and neutralise potential threats before they cause significant damage.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://asec.ahnlab.com/ko/82900/

PowerShell keylogger captures sensitive data

A new PowerShell-based keylogger is actively capturing personal information, including passwords and credit card numbers. To avoid detection, the malware uses advanced tactics such as system discovery and encoded command execution. Furthermore, it interacts anonymously using proxies and the Tor network, making it more difficult for security teams to track. Although the keylogger's persistence mechanism is currently imperfect, cybersecurity experts warn that future versions may offer a greater threat. The malware affects Windows computers worldwide and can attack any sector, prompting organisations to strengthen their defences against PowerShell-based assaults.

Experts advise eliminating superfluous PowerShell functions and installing comprehensive monitoring to detect such attacks early. Regular updates and patches, coupled with vigilant monitoring, can help organisations stay ahead of evolving threats and protect sensitive data from being compromised.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyfirma.com/research/cyfirma-research-powershell-keylogger/

Google releases Android security update

Google has released the September 2024 Android security update, which addresses 36 vulnerabilities, including the actively exploited CVE-2024-32896 zero-day. This critical Elevation of Privilege vulnerability allows attackers to get unauthorised access to sensitive data or take control of Android devices. The issue has been actively targeted in many assaults, requiring rapid attention from users. In addition, the patch addresses major vulnerabilities in Qualcomm components, which affect a wide range of devices.

Security experts stress the importance of updating Android devices to protect against possible threats, warning that delayed upgrades may leave users open to exploitation. With Android devices in use globally, organisations and individuals alike should stay up to speed with security patches to prevent exposure to such serious threats.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Android

Source - https://securityonline.info/google-patches-actively-exploited-zero-day-in-september-android-update/

INTRODUCTION | GODZILLA WEBSHELL HITS BFSI | BACKDOOR ATTACKS EXCHANGE SERVER | BMOF EXPLOITED TO SPREAD CRYPTOMINER | POWERSHELL KEYLOGGER THREAT | CRITICAL ANDROID FIX | URGENT CISA WARNING | GROWING INFOSTEALER THREAT | STATE-SPONSORED RANSOMWARE ATTACKS | JOB SEEKERS TARGETED | CRIMINALS MISUSE MACROPACK

CISA urges patching of exploited vulnerabilities

The Cybersecurity and Infrastructure Security Agency (CISA) has added three major vulnerabilities to its Known Exploited Vulnerabilities database, advising organisations to patch immediately. Two of the vulnerabilities affect Draytek routers, allowing attackers to obtain unauthorised access to networks. The third, which affects Kingsoft WPS Office, has been exploited by a South Korean cyberespionage group. These flaws offer serious threats, including potential data leaks and system intrusions. With active exploitation currently underway, CISA emphasises the importance of immediate action to safeguard impacted infrastructure and reduce potential damage.

Patching these vulnerabilities is advocated as a top priority for organisations worldwide to preserve sensitive data and ensure operational security. Regular security assessments, timely updates, and proactive threat monitoring are essential to mitigate the risks associated with these and other vulnerabilities.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	WPS office

Source - https://securityonline.info/cisa-issues-alert-three-actively-exploited-vulnerabilities-demand-immediate-attention/

INTRODUCTION
GODZILLA WEBSHELL HITS BFSI
BACKDOOR ATTACKS EXCHANGE SERVER
BMOF EXPLOITED TO SPREAD CRYPTOMINER
POWERSHELL KEYLOGGER THREAT
CRITICAL ANDROID FIX
URGENT CISA WARNING
GROWING INFOSTEALER THREAT
STATE-SPONSORED RANSOMWARE ATTACKS
JOB SEEKERS TARGETED
CRIMINALS MISUSE MACROPACK

Emansrepo infostealer poses growing threat

Cybersecurity researchers have identified Emansrepo, a Python-based infostealer, as a growing threat. This virus, which is distributed by phishing emails disguised as purchase orders and invoices, uses three attack chains to avoid detection: AutoIt-compiled executables, HTA files, and obfuscated batch scripts. Emansrepo was first built to steal credentials, but it has now evolved to target PDFs, bitcoin wallets, and other files. The malware's adaptability and multi-vector approach render it especially deadly. A separate effort also uses DBatLoader to transmit Remcos malware, which broadens the threat landscape.

The expanding capabilities of Emansrepo emphasise the necessity for organisations to tighten email security and watch for suspicious activities to mitigate risks.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.fortinet.com/blog/threat-research/emansrepo-stealer-multi-vector-attack-chains

State-sponsored hackers linked to ransomware operations

Iranian state-sponsored hackers, dubbed "Pioneer Kitten" and "Lemon Sandstorm," are increasingly assisting ransomware operations. These cyber threat actors are now working as access brokers for ransomware gangs like ALPHV (BlackCat), selling network access to important infrastructure sectors like healthcare, finance, and defence. In addition to providing access, they engage in state-sponsored espionage and hack-and-leak operations. Their combined role in cybercrime and state-sponsored activities highlights the increasing complexities of modern cyber threats.

Organisations are urged to tighten defences and be watchful against such sophisticated assaults, as the risk to global vital infrastructure grows.

ATTACK TYPE	Ransomware	SECTOR	Financial services, education, defence industry, healthcare
REGION	Global	APPLICATION	Windows

Source - https://cyble.com/blog/iranian-state-sponsored-hackers-have-become-access-brokers-for-ransomware-gangsca/

Hackers target job seekers with malware

Threat actors associated with the North Korean Lazarus Group are running a financially motivated effort named "Contagious Interview," which targets job seekers with bogus interviews. They spread malware disguised as video conferencing software, such as FreeConference.com, which infects both Windows and macOS systems. The malware, which includes BeaverTail and InvisibleFerret, allows for data theft, keylogging, and remote control.

These assaults are largely aimed at stealing cryptocurrencies and browser data, with an increasing interest in targeting decentralised finance businesses. The employment of powerful social engineering tactics makes this campaign very risky. Job searchers are encouraged to exercise caution when attending online interviews or downloading unfamiliar software.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Apple, macOS, Windows, Linux

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

INTRODUCTION | GODZILLA WEBSHELL HITS BFSI | BACKDOOR ATTACKS EXCHANGE SERVER | BMOF EXPLOITED TO SPREAD CRYPTOMINER | POWERSHELL KEYLOGGER THREAT | CRITICAL ANDROID FIX | URGENT CISA WARNING | GROWING INFOSTEALER THREAT | STATE-SPONSORED RANSOMWARE ATTACKS | JOB SEEKERS TARGETED | CRIMINALS MISUSE MACROPACK

MacroPack misused to deploy Brute Ratel

Cybercriminals are found to be misusing the MacroPack framework, which was originally built for Red Team activities, to spread harmful payloads such as Havoc, Brute Ratel, and PhantomCore. This platform is being misused to develop evasive, document-based assaults worldwide. The attackers use complex MacroPack features such as code obfuscation and anti-malware bypass techniques, making it harder for security systems to detect and eliminate threats.

This trend has raised serious concerns among cybersecurity specialists, as cyber threat actors are increasingly abusing the tool's capabilities. Organisations are encouraged to improve document security practices and stay watchful against such sophisticated malware campaigns.

ATTACK TYPE	Malware	SECTOR	All
REGION	Russia, China, Pakistan, United States	APPLICATION	Generic

Source - https://www.bleepingcomputer.com/news/security/red-team-tool-macropack-abused-in-attacks-to-deploy-brute-ratel/

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.