TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 24, 2024

THREAT INTELLIGENCE ADVISORY REPORT

As the digital world constantly changes, cyber threats evolve at an unparalleled rate. Organisations worldwide are strengthening their efforts to protect their data and fortify the security frameworks underpinning their operations. To guard against potential dangers, it is critical to stay vigilant of emerging cyber threats and implement appropriate security measures proactively.

Tata Communications' weekly threat intelligence advisory keeps you ahead of the curve by providing insights into the latest cyber threats. These insights allow you to execute proactive methods that increase your organisation's defences and successfully reduce vulnerabilities before they are exploited.

GeoServer exploit enables remote code execution

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a critical vulnerability in GeoServer to its Known Exploited Vulnerabilities (KEV) catalogue. Threat actors have been actively exploiting this critical vulnerability identified as CVE-2024-36401 (CVSS score: 9.8) in GeoServer versions prior to 2.23.6, 2.24.4, and 2.25.2. This flaw allows attackers to remotely execute code by sending specially crafted payloads. The vulnerability has been actively abused by various malware, including GOREVERSE, SideWalk, and cryptocurrency mining programs, with attacks impacting industries across the globe. CISA has also identified a critical flaw in OSGeo GeoServer GeoTools, which has been exploited by botnets, miner groups, and GOREVERSE, leading to malware spread and malicious actions.

GeoServer's users are advised to update to the latest version to protect their systems from potential damage caused by this exploit. Organisations are advised to implement strong security measures to prevent further exploitation. Regular patching and diligent monitoring of network traffic are essential to mitigate the threat.

ATTACK TYPE	Vulnerability, Malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.fortinet.com/blog/threat-research/threat-actors-exploit-geoserver-vulnerability-cve-2024-36401

NoName group intensifies global attacks

The NoName ransomware group, also known as CosmicBeetle, has intensified its cyberattacks against small and medium-sized businesses across South America, Europe, Africa, and Asia. This group utilises custom malware known as the Spacecolon malware family, including ScRansom, and exploits vulnerabilities such as EternalBlue (CVE-2017-0144) and ZeroLogon (CVE-2020-1472) to infiltrate Windows-based systems. Recently, the group has begun using RansomHub, a platform designed to enhance their ransomware operations. Although they have faced some technical setbacks, NoName's growing capabilities and evolving tactics pose an ongoing and serious threat to businesses globally. The group's ability to adapt by partnering with RansomHub signals a more sophisticated approach, making it critical for organisations to strengthen their defences.

Applying the latest security patches, especially for Windows systems, and maintaining strong cyber hygiene practices are vital to mitigating this threat. Businesses are urged to remain vigilant, as NoName continues to develop its operations and expand its global reach.

ATTACK TYPE	Ransomware, Malware	SECTOR	All
REGION	South America, Europe, Africa, Asia	APPLICATION	Windows

Source - https://www.bleepingcomputer.com/news/security/noname-ransomware-gang-deploying-ransomhub-malware-in-recent-attacks/

Cyberespionage campaign targets government organisations

The Crimson Palace cyberespionage campaign, attributed to Chinese-linked threat actors, has been actively targeting government organisations across Southeast Asia. This campaign operates through three coordinated clusters, named Alpha (STAC1248), Bravo (STAC1870), and Charlie (STAC1305), each playing a role in infiltrating systems, maintaining access, and exfiltrating sensitive intelligence data. These threat clusters employ advanced malware, compromised networks, and sophisticated command-and-control (C2) frameworks to conduct their operations. The attackers continuously refine their methods to evade detection, adapting their techniques to maintain a persistent presence within targeted networks. This ongoing campaign poses a significant risk to government entities, as the threat actors focus on gathering intelligence and causing potential disruptions.

Organisations in Southeast Asia, particularly those using Windows-based systems, are urged to enhance their cybersecurity defences and monitor for any signs of compromise, as this campaign continues to evolve and grow in complexity.

ATTACK TYPE	Malware	SECTOR	Government
REGION	Asia	APPLICATION	Windows

Source - https://thehackernews.com/2024/09/experts-identify-3-chinese-linked.html

New ransomware group poses global threat

Repellent Scorpius, a ransomware-as-a-service (RaaS) group, has emerged as a rising cyber threat since May 2024. This group uses the Cicada3301 ransomware in a double extortion model, where they not only encrypt stolen data but also threaten to release it unless a ransom is paid. By partnering with affiliates and initial access brokers, Repellent Scorpius infiltrates networks, steals sensitive information, and demands payment for both decryption and the prevention of data publication. Their operations have rapidly evolved, with continuous updates to their ransomware techniques, making them increasingly dangerous to organisations across various sectors worldwide. Windows-based systems are their primary target, and their growing influence signals a more aggressive approach to cyberattacks.

Organisations must implement comprehensive security measures, including regular patching, to mitigate the risk posed by this group. The rise of Repellent Scorpius highlights the critical need for stronger defences in the face of advancing ransomware threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://unit42.paloaltonetworks.com/repellent-scorpius-cicada3301-ransomware/

Lazarus expands global malware operations

The Lazarus Group, a North Korean cyber threat organisation operating under the Reconnaissance General Bureau (RGB), has intensified its global operations. Divided into at least six sub-groups, they employ malware targeting Windows, macOS, and Linux systems. These groups engage in espionage, financial theft, and destructive attacks, threatening industries across the globe. The Lazarus Group's tactics continually evolve, making their attacks increasingly sophisticated and difficult to detect. As their toolkit grows, they are becoming a more prominent and dangerous actor in the cyber threat landscape.

Organisations worldwide are advised to adopt multi-layered security strategies to mitigate the risks posed by these advanced threats. Ensuring regular software updates, conducting thorough network monitoring, and implementing strong defences across all operating systems are essential.

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

Source - https://unit42.paloaltonetworks.com/threat-assessment-north-korean-threat-groups-2024/

Quad7 botnet expands to new devices

The Quad7 botnet has significantly evolved, now targeting a wider range of small office and home office (SOHO) devices, including Zyxel VPN appliances, Ruckus wireless routers, and Axentra media servers, alongside TP-Link and ASUS routers. The botnet has adopted advanced evasion tactics, shifting to the KCP protocol for stealthier communication, which makes it harder to detect. Additionally, it has integrated a new backdoor named 'UPDTAE' that establishes HTTP reverse shells for remote control on the infected devices. Though still in its early stages, this expansion highlights the botnet’s potential to exploit further vulnerabilities and increase its global impact. The increasing sophistication of the Quad7 botnet poses a serious threat to various sectors, emphasising the need for strong cybersecurity measures.

Organisations using the targeted devices should implement regular patches, monitor network activity, and strengthen defences to mitigate the risks posed by this growing botnet.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Zyxel VPN

Source - https://www.bleepingcomputer.com/news/security/quad7-botnet-targets-more-soho-and-vpn-routers-media-servers/

INTRODUCTION
GEOSERVER SECURITY CRISIS
NONAME RANSOMWARE THREAT
CRIMSON PALACE RISK
REPELLENT SCORPIUS PERIL
LAZARUS THREAT INTENSIFIES
QUAD7 BOTNET EVOLVES
CRITICAL WINDOWS FLAW
SCATTERED SPIDER TARGETS CLOUD
DRAGONRANK MANIPULATES SEO
FORTINET DATA BREACH

Critical Windows vulnerability requires urgent patching

Microsoft has revealed a critical zero-day vulnerability, identified as CVE-2024-43491, affecting the Servicing Stack in its Windows operating system. With a severity score of 9.8, this flaw impacts Windows 10 version 1507 and certain components, causing the rollback of security patches and leaving systems exposed to previously mitigated threats. While no active exploitation has been detected, the vulnerability presents a serious risk by enabling remote code execution if left unpatched. The potential exploitation of this vulnerability could have wide-reaching consequences across various sectors, making it essential for organisations to act swiftly.

Microsoft urges all users to immediately apply the Servicing Stack update (KB5043936) and September 2024 Windows security updates (KB5043083) to secure their systems. Regular patching, alongside vigilant monitoring of system updates, is critical in preventing potential damage from this flaw.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://securityonline.info/cve-2024-43491-cvss-9-8-critical-windows-0-day-flaw-uncovered-urgent-patching-required/

Scattered Spider targets cloud infrastructures

The Scattered Spider group has launched a new wave of ransomware attacks, specifically targeting cloud infrastructures in the insurance and financial sectors. Employing sophisticated social engineering tactics such as vishing, smishing, and SIM swapping, they have successfully bypassed multi-factor authentication (MFA) protections, gaining unauthorised access to cloud platforms. The group's use of cloud-native tools to further exploit these environments, combined with a possible collaboration with the BlackCat/ALPHV ransomware group, signals a growing and more dangerous threat.

Organisations in the insurance and financial sectors are urged to strengthen their defences, particularly around MFA and cloud security protocols.

ATTACK TYPE	Malware	SECTOR	BFSI
REGION	Global	APPLICATION	Windows

Source - https://securityonline.info/scattered-spider-targets-the-cloud-a-growing-threat-to-the-insurance-and-financial-sectors/

DragonRank campaign targets IIS servers for SEO manipulation

The DragonRank campaign, operated by a China-based threat actor, is actively targeting web application services across Asia and Europe, focusing on manipulating search engine optimisation (SEO) rankings. By deploying malware such as PlugX and BadIIS, the group compromises Internet Information Services (IIS) servers, converting them into relay points for proxy fraud and SEO manipulation. These compromised servers are used to drive traffic to malicious websites, manipulating search engine algorithms to push fraudulent content. DragonRank offers customised SEO services to clients, exploiting compromised servers to enhance the visibility of harmful content.

Organisations using IIS servers are urged to strengthen their security measures to prevent being compromised by this growing threat, which can lead to financial losses and reputational damage.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, manufacturing, IT, transportation, broadcast media
REGION	Asia, Europe	**APPLICATION**	Generic

Source - https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

INTRODUCTION | GEOSERVER SECURITY CRISIS | NONAME RANSOMWARE THREAT | CRIMSON PALACE RISK | REPELLENT SCORPIUS PERIL | LAZARUS THREAT INTENSIFIES | QUAD7 BOTNET EVOLVES | CRITICAL WINDOWS FLAW | SCATTERED SPIDER TARGETS CLOUD | DRAGONRANK MANIPULATES SEO | FORTINET DATA BREACH

Fortinet data breach exposes customer information

Fortinet, a leading cybersecurity firm, has confirmed a data breach impacting a small number of its customers in the Asia-Pacific region. An unauthorised individual gained access to files stored on a third-party cloud-based drive, raising concerns about cloud security. Although Fortinet has assured customers that no malicious activity has been detected as a result of the breach, the incident has highlighted vulnerabilities in cloud storage systems. Fortinet is conducting a thorough investigation and collaborating with affected customers to mitigate any potential risks.

The breach underscores the importance of strong cloud security measures, even for leading cybersecurity providers. Fortinet’s quick response and transparency offer some reassurance, but the attack has triggered a broader conversation on the security of sensitive data in cloud environments.

ATTACK TYPE	Breach	SECTOR	All
REGION	Global	APPLICATION	Fortinet

Source - https://www.bleepingcomputer.com/news/security/fortinet-confirms-data-breach-after-hacker-claims-to-steal-440gb-of-files/

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.