TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: February 13, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In the rapidly evolving digital landscape, individuals, businesses, and government entities are constantly confronted with complex cybersecurity challenges. These threats not only interrupt daily functions but also present substantial financial risks. So, it is vital to bolster your company's digital safeguards and protect against cyber threats jeopardising crucial enterprise data.

Remain vigilant against cyber threats and enhance security measures by using our weekly reports that provide advanced cyber threat intelligence. In the current landscape prioritising cyber resilience, our threat intelligence report furnishes invaluable insights to bolster your organisation's security readiness. Ensure the safety of your IT assets from malicious assaults with our thorough advisory services.

Major Linux distributions vulnerable to root privilege escalation attack

Attackers are gaining root access to various leading Linux distributions with default setups by exploiting a recently revealed local privilege escalation (LPE) flaw in the GNU C Library (glibc). Designated CVE-2023-6246, this critical security vulnerability resides in glibc's __vsyslog_internal() function. It is utilised by commonly used syslog and vsyslog functions to compose messages for the system message logger.

The flaw stems from a heap-based buffer overflow vulnerability. Exploiting the vulnerability necessitates specific conditions, such as an exceptionally lengthy argv[0] or openlog() ident argument. The extensive adoption of glibc renders this vulnerability a significant threat. The Debian, Ubuntu, and Fedora systems have been identified as vulnerable, with additional distributions likely impacted. This underscores the critical necessity for stringent security practices in software development, particularly concerning core libraries that are extensively utilised across numerous systems and applications.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Linux

Source- https://www.bleepingcomputer.com/news/security/new-linux-glibc-flaw-lets-attackers-get-root-on-major-distros/

Atlassian Confluence RCE vulnerability exploited in the wild

Atlassian has disclosed a remote code execution (RCE) vulnerability, CVE-2023-22527, affecting outdated Confluence datacentre and server versions. This flaw has been classified as critical, involving object-graph navigation language (OGNL) injection. The common vulnerability scoring system (CVSS) assigns this issue a high score of 10, indicative of its severity.

OGNL, a Java-based expression language, is utilised in applications such as Atlassian Confluence. Failure to properly validate and sanitise user input before integrating it into OGNL expressions in these applications can lead to a security flaw known as OGNL injection. Exploitation attempts were identified on January 26, with attackers targeting vulnerable instances globally. With a surge of approximately 30,000 new vulnerabilities reported in 2023 and the critical nature of the flaw, enterprises are advised to safeguard their IT assets.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Singapore, Russia, India, UK, China, Germany, Romania, United States, and Vietnam	**APPLICATION**	Atlassian Confluence

Source- https://cyble.com/blog/exploitation-of-atlassian-confluence-rce-vulnerability-cve-2023-22527/

Chinese hackers exploit VPNs, deploy KrustyLoader malware

Two zero-day vulnerabilities have been discovered in Ivanti Connect Secure (ICS) virtual private network (VPN) devices. Exploiting these vulnerabilities led to the deployment of KrustyLoader, a payload written in Rust. KrustyLoader then installed the open-source Sliver adversary simulation tool. These security flaws, tracked as CVE-2023-46805 with a CVSS score of 8.2 and CVE-2024-21887 with a CVSS score of 9.1, could be utilised together to achieve unauthenticated RCEs on susceptible appliances. Patches have not been released yet, but a temporary XML file mitigation has been provided by the company.

Exploiting these vulnerabilities has led to the distribution of XMRig miners and the Rust-based malware. This highlights the growing use of Sliver in offensive security tools, although Cobalt Strike remained dominant in 2023. Sliver, a cross-platform post-exploitation framework developed by BishopFox, is based on Golang. It has gained traction among threat actors (TAs) as a profitable alternative to established tools like Cobalt Strike.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source- https://thehackernews.com/2024/01/chinese-hackers-exploiting-critical-vpn.html

Phishing campaign targets Microsoft Teams users with DarkGate malware

Cybercriminals are leveraging Microsoft Teams group chat requests to distribute DarkGate malware through malicious attachments. The attackers leveraged what appears to be a compromised Teams user or domain to dispatch over 1,000 malicious Teams group chat invitations.

Upon acceptance of the chat request, the TAs coerce targets into downloading a file with a double extension, typically named “Navigating Future Changes October 2023.pdf.msi,” in line with DarkGate tactics. After installation, the malware establishes communication with its command-and-control (C2) server located at hgfdytrywq[.]com. This phishing exploit is facilitated by Microsoft’s default setting, which permits external Microsoft Teams users to message users in other tenants. The trend targets organisations with insecure configurations, spurred by a rise in DarkGate attacks following the Qakbot botnet disruption. It underscores the pressing demand for bolstered cybersecurity measures to counter evolving tactics. Unless essential for daily operations, experts recommend disabling external access in Microsoft Teams.

ATTACK TYPE	Phishing and malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Microsoft Teams

Source- https://www.bleepingcomputer.com/news/security/microsoft-teams-phishing-pushes-darkgate-malware-via-group-chats/

Russian hackers target Microsoft, steal sensitive emails

Microsoft has confirmed that the Russian Foreign Intelligence Service hacking group breached its executives' email accounts in November 2023. It stole emails from their leadership, cybersecurity, and legal teams. Some of these emails contained information about the hacking group itself, enabling the TAs to ascertain Microsoft's knowledge about them. Additionally, this group targeted other organisations as part of its malicious campaign.

Midnight Blizzard (also known as Nobelium or APT29) is a state-sponsored cyberespionage group affiliated with the Russian Foreign Intelligence Service (SVR). It primarily targets government organisations, non-governmental organisations (NGOs), software developers, and IT service providers in the United States and Europe. Exploiting a legacy test account without multi-factor authentication, the attackers gained heightened access by compromising an OAuth application. They employed residential proxies and "password spraying" brute-force tactics, focusing on a limited number of accounts. This included a "legacy, non-production test tenant account." The TA tailored their password spray attacks to a specific set of accounts, minimising the number of attempts to avoid detection and bypass account blocks caused by numerous failures.

ATTACK TYPE	Cybercrime	**SECTOR**	IT, government, IT services, and consulting
REGION	Europe and the United States	**APPLICATION**	Windows

Source- https://www.bleepingcomputer.com/news/security/microsoft-reveals-how-hackers-breached-its-exchange-online-accounts/

TATA COMMUNICATIONS

Zero-day flaws allow new malware to exploit Ivanti VPN users

A new malware used by China-linked espionage group UNC5221 has been discovered. It exploits the vulnerabilities CVE-2023-46805 and CVE-2024-21887 in ICS VPN. These flaws have been exploited actively as zero-day flaws since December 2023.

UNC5221, known for targeting strategic industries in China, employs open-source utilities and Linux-based tools. These flaws have been used to distribute backdoors, cryptocurrency miners, and a Rust-based loader named KrustyLoader. The threat involves custom web shells, including CHAINLINE, embedded in Ivanti packages. In a new advisory, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) revealed that adversaries are using these two weaknesses to seize credentials and deploy web shells, allowing for further infiltration of enterprise networks. The recent update follows the exploitation of CVE-2023-46805 and CVE-2024-21887 by various TAs. Ivanti has released updates to address the vulnerabilities, including CVE-2024-21893, which is currently being actively exploited.

ATTACK TYPE	Vulnerability and malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source- https://thehackernews.com/2024/01/alert-ivanti-discloses-2-new-zero-day.html

Hackers leverage online platforms to host USB malware payloads

A financially driven cybercriminal group, UNC4990, is using USB drives to infect victims. It then misuses trusted platforms like GitHub, Vimeo, and Ars Technica to hide a malicious code. This code downloads a malware that steals data and mines cryptocurrency. Although it appears to be innocuous on these platforms, the text becomes active when incorporated into the attack sequence.

UNC4990 utilises EMPTYSPACE, also recognised as VETTA Loader and BrokerLoader, a downloader capable of executing any payload provided by its C2 server. Additionally, QUIETBOARD, a backdoor, is distributed through EMPTYSPACE. The attackers adapt their methods, making it difficult to detect and stop them. Users are cautioned to exercise vigilance with USB drives and to remain alert for suspicious activity on trusted websites.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source- https://www.mandiant.com/resources/blog/unc4990-evolution-usb-malware

Ukrainian CERT warns of the widespread PurpleFox malware campaign

The Computer Emergency Response Team in Ukraine (CERT-UA) has issued a warning about the PurpleFox malware. The malware has infected over 2,000 computers in the country. It disguises itself as the Telegram app. Functioning as a downloader, it introduces more powerful second-stage payloads onto compromised systems, provides its operators with backdoor capabilities, and can also operate as a distributed denial of service (DDoS) bot.

PurpleFox, also known as “DirtyMoe,” operates as a Windows botnet with rootkit capabilities. It commonly infects systems when victims execute tainted Microsoft Software Installers (MSIs). The malware showcases its self-replicating abilities by exploiting known vulnerabilities and employing password brute-forcing techniques. CERT-UA has provided detailed information on identifying infections and recommended steps for removal, emphasising the importance of network monitoring and implementing security measures to prevent re-infection.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Ukraine	**APPLICATION**	Windows

Source- https://www.bleepingcomputer.com/news/security/purplefox-malware-infects-thousands-of-computers-in-ukraine/

TATA COMMUNICATIONS

Nation-state threat actor under suspicion for attack on Cloudflare's Atlassian server

A suspected nation-state attacker has breached Cloudflare's internal Atlassian server. Initially infiltrating the self-hosted Atlassian server on November 14, the attacker later breached Confluence and Jira after reconnaissance. The TA gained access to the company's Confluence wiki, Jira bug database, and Bitbucket source code management system.

Returning on November 22, they established persistent access by leveraging ScriptRunner for Jira. Furthermore, they infiltrated the source code management system through Atlassian Bitbucket. Moreover, they made unsuccessful attempts to breach a console server to access the company's not-yet-operational São Paulo datacentre. Despite the breach on November 14, customer data has not been compromised. Cloudflare has taken extensive measures to address the incident, attributing it to the nation-state actor's persistent attempts to gather information about their global network.

ATTACK TYPE	Breaches	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source- https://www.bleepingcomputer.com/news/security/cloudflare-hacked-using-auth-tokens-stolen-in-okta-attack/

Mispadu malware targets Windows users with a banking trojan

The Mispadu banking trojan is exploiting a Windows SmartScreen flaw to target users in Mexico. The malware employs a sophisticated phishing approach. Recent data indicates the harvesting of over 90,000 bank credentials since August 2022.

Mispadu, a Delphi-based data thief, targets victims primarily in the Latin American (LATAM) region. It is affiliated with Grandoreiro, the broader category of LATAM banking malware. The latest attack method involves deceptive internet shortcut files within fake ZIP archives exploiting CVE-2023-36025 (CVSS score: 8.8). This tactic revolves around crafting specific internet shortcut files (.URL) or hyperlinks directing to malicious content capable of bypassing SmartScreen warnings. Additionally, insights into DICELOADER reveal its use by the Russian FIN7 group, showcasing their advanced obfuscation techniques for covert operations.

ATTACK TYPE	Malware
SECTOR	Financial services
REGION	Europe and Mexico
APPLICATION	Windows

Source- https://thehackernews.com/2024/02/new-mispadu-banking-trojan-exploiting.html

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.

© 2023 Tata Communications. All rights reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Private Limited.