TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: APRIL 2ND, 2024

THREAT INTELLIGENCE ADVISORY REPORT

In today's global landscape, cybersecurity is a top priority for organisations. With cyber threats constantly evolving, businesses aim to safeguard their assets and sustain operational stability. It's not solely about securing data anymore; it's about bolstering the fundamental frameworks on which modern organisations rely, guaranteeing resilience against a range of emerging threats.

Elevate your organisation's cybersecurity readiness with Tata Communications' weekly threat intelligence advisory. Gain valuable insights into the latest cyber risks and implement proactive measures to strengthen your defences, effectively addressing potential vulnerabilities.

INTRODUCTION | RANSOMWARE EXPLOITS TEAMCITY FLAW | WIPER MALWARE ATTACKS LINUX | CHINESE HACKERS TARGET 70 ORGS | ANDROXGH0ST EXPLOITS VULNERABILITIES | ATLASSIAN RELEASES SECURITY PATCHES | MUDDLED LIBRA INFILTRATES INDUSTRIES | CURIOUS SERPENS SPREADS BACKDOOR | FLUFFY WOLF USES META STEALER | KIMSUKY TARGETS ORGANISATIONS GLOBALLY | CHINESE HACKERS ATTACK F5 BIG-IP

TeamCity flaw targeted with ransomware, cryptomining, remote access attacks

Cybercriminals are exploiting JetBrains TeamCity's vulnerability (CVE-2024-27198) for ransomware attacks, cryptomining, and malware distribution, including Cobalt Strike beacons and Spark RAT. This activity leads to significant financial losses and operational disruptions, urging immediate system updates for mitigation. The evolving ransomware landscape, marked by increased collaboration among threat groups, complicates detection and response efforts.

JetBrains disclosed another critical vulnerability, CVE-2024-27199, enabling attackers to bypass authentication and seize administrative control. With existing proof-of-concept exploits and observed active exploitation, prompt software updates are crucial to safeguard data and systems. The US CISA has added CVE-2024-27198 to its Known Exploited Vulnerabilities (KEV) catalogue, emphasising the urgency of addressing these threats.

ATTACK TYPE	Ransomware, malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.trendmicro.com/en_us/research/24/c/teamcity-vulnerability-exploits-lead-to-jasmin-ransomware.html

New AcidPour wiper attacks Linux network devices

AcidPour, a new data-wiping malware, is threatening Linux x86 IoT and network devices, resembling AcidRain. It has originated in Ukraine and the similarity to past malware highlights evolving cyber threats, urging collaborative defence efforts in the cybersecurity community. AcidRain, previously used in a Viasat cyberattack, disrupted services in Ukraine and Europe.

Uploaded on March 16, 2024, AcidPour's operators are difficult to trace. Sharing wiping logic with VPNFilter's 'dstr' plugin and AcidRain, AcidPour targets embedded systems and devices using Logical Volume Management, expanding its range beyond AcidRain's focus on MIPS architecture. This necessitates heightened vigilance and analysis within the cybersecurity sector.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Linux

Source - https://www.bleepingcomputer.com/news/security/new-acidpour-data-wiper-targets-linux-x86-network-devices/

Chinese hacking group targets 70 organisations worldwide

The "Earth Krahang" cyberattack group, linked to China, has targeted 70 organisations and 116 entities across 45 countries, with a focus on government institutions. Using internet server vulnerabilities and spear-phishing, they installed backdoors and brute-forced passwords for intelligence gathering, showcasing advanced cyberespionage capabilities. While not a high-level military APT, they may be affiliated with iSoon, a private hack-for-hire operation linked to the Chinese Communist Party.

Employing standard tactics and open-source tools, they compromised organisations globally, spanning government, education, telecommunications, finance, and sports sectors. Their victims include various ministries and organisations across Asia, the Americas, Europe, and Africa.

ATTACK TYPE	Malware	SECTOR	Healthcare/hospitals, tourism/hospitality, manufacturing, IT, military, BFSI, real estate, broadcast, media production and distribution, and retail
REGION	Europe, Africa, Asia, US	APPLICATION	Windows, Linux

Source - https://www.darkreading.com/threat-intelligence/chinese-apt-earth-krahang-compromised-48-gov-orgs-5-continents

AndroxGh0st malware exfiltrates credentials and exploits vulnerabilities

AndroxGh0st, a sophisticated Python-based malware, has targeted Laravel web applications, aiming to pilfer sensitive data from .env files and exploit SMTP protocols. Its capabilities extend to AWS and Twilio credential theft, along with vulnerability exploitation and experimental brute force attacks, underscoring the need for robust cybersecurity measures. First detected in 2022, AndroxGh0st enables threat actors to access Laravel environment files and pilfer credentials for cloud-based platforms like AWS, SendGrid, and Twilio.

Exploiting known security flaws in Apache HTTP Server, Laravel Framework, and PHPUnit, it gains initial access, facilitates privilege escalation, and ensures persistence. Recently, U.S. cybersecurity agencies cautioned about AndroxGh0st's deployment in creating botnets for victim identification and network exploitation. Juniper Threat Labs reported increased activity linked to CVE-2017-9841 exploitation, emphasising the urgency of updating systems promptly.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://thehackernews.com/2024/03/androxgh0st-malware-targets-laravel.html

INTRODUCTION
RANSOMWARE EXPLOITS TEAMCITY FLAW
WIPER MALWARE ATTACKS LINUX
CHINESE HACKERS TARGET 70 ORGS
ANDROXGH0ST EXPLOITS VULNERABILITIES
ATLASSIAN RELEASES SECURITY PATCHES
MUDDLED LIBRA INFILTRATES INDUSTRIES
CURIOUS SERPENS SPREADS BACKDOOR
FLUFFY WOLF USES META STEALER
KIMSUKY TARGETS ORGANISATIONS GLOBALLY
CHINESE HACKERS ATTACK F5 BIG-IP

Atlassian releases security patches, highlighting critical Bamboo flaw

Atlassian has addressed 25 security issues, notably a critical SQL injection vulnerability (CVE-2024-1597) in Bamboo Data Center and Server, scoring 10.0 in severity. Despite its criticality, its exploitation requires specific driver versions of the PostgreSQL JDBC Driver. The company advises upgrading to the latest versions for protection.

Atlassian clarified that the vulnerability poses less risk to other Data Center products as they don’t use the PreferQueryMode=SIMPLE setting in SQL database connections.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Atlassian Bamboo, Atlassian Confluence, Atlassian JIRA, Atlassian Bitbucket

Source - https://thehackernews.com/2024/03/atlassian-releases-fixes-for-over-2.html

Muddled Libra adapts and breaches defences

Muddled Libra, a sophisticated cyber threat, employs a blend of social engineering and advanced technological tactics to breach various industries, including finance and software automation. Their adaptive strategies, such as using proxy services, custom malware, and social engineering, challenge even robust cybersecurity defences. Initially targeting software automation, outsourcing, and telecommunications, they have expanded to technology, hospitality, and financial sectors.

Notably, they exploit social engineering, like manipulating IT helpdesks, to gain network access. Investigations from mid-2022 to 2024 reveal their evolution from structured attacks on cryptocurrency firms to a ransomware affiliate model, prioritising extortion. Activities include using proxy services, email rules, custom virtual machines, and rootkits to gain administrative access. Proficiency in English aids their social engineering, while AI spoofing of victims' voices enhances their deception, primarily targeting US-based entities.

ATTACK TYPE	Social engineering, malware	SECTOR	Financial services, IT, hospitality
REGION	Global	APPLICATION	Generic

Source - https://unit42.paloaltonetworks.com/muddled-libra/

Curious Serpens spreads FalseFont backdoor by social engineering

In a recent investigation, cybersecurity experts have revealed the presence of FalseFont, a sophisticated backdoor employed by the Curious Serpens group, reportedly linked to Iran. The backdoor has been used since 2013 to conduct cyberespionage primarily targeting aerospace and energy sectors. Disguised as a HR software, FalseFont employs intricate social engineering techniques to infiltrate aerospace organisations, highlighting the pressing need for enhanced cybersecurity measures.

FalseFont, discovered in 2023, allows for unauthorised command execution and data extraction, posing a significant threat to targeted sectors. The Curious Serpens group, also known as Peach Sandstorm or APT33, has a history of espionage activities globally. Written in ASP .NET Core, FalseFont can execute commands, manipulating files, capturing screens, and stealing sensitive credentials. Public analysis has revealed its operational methods in January 2024.

ATTACK TYPE	Malware	SECTOR	Energy, aerospace, defence
REGION	Middle East, Europe, US	APPLICATION	Windows

Source - https://unit42.paloaltonetworks.com/curious-serpens-falsefont-backdoor/

Fluffy Wolf phishing campaign uses Meta Stealer to target businesses

The Fluffy Wolf cyber threat group has been conducting a sophisticated phishing campaign targeting Russian enterprises, utilising malware such as Meta Stealer and legitimate tools such as Remote Utilities. Despite being relatively inexperienced, they have executed over 140 successful attacks since 2022, exploiting the prevalence of phishing as the primary attack method in 68% of cyber incidents against Russian organisations. The group masquerades as a construction company, sending phishing emails with malicious attachments disguised as reconciliation reports.

These attachments contain password-protected files housing various malware payloads, including Meta Stealer. Fluffy Wolf also distributes other malware like WarZone RAT and XMRig miner. While primarily targeting Russian organisations, their tactics could extend to other regions, highlighting the risk posed by unsophisticated threat actors leveraging malware-as-a-service models for cyberattacks.

ATTACK TYPE	Malware	SECTOR	All
REGION	Russia	APPLICATION	Windows

Source - https://www.darkreading.com/threat-intelligence/fluffy-wolf-spreads-meta-stealer-in-corporate-phishing-campaign

INTRODUCTION | RANSOMWARE EXPLOITS TEAMCITY FLAW | WIPER MALWARE ATTACKS LINUX | CHINESE HACKERS TARGET 70 ORGS | ANDROXGH0ST EXPLOITS VULNERABILITIES | ATLASSIAN RELEASES SECURITY PATCHES | MUDDLED LIBRA INFILTRATES INDUSTRIES | CURIOUS SERPENS SPREADS BACKDOOR | FLUFFY WOLF USES META STEALER | KIMSUKY TARGETS ORGANISATIONS GLOBALLY | CHINESE HACKERS ATTACK F5 BIG-IP

Kimsuky targeting organisations with malicious CHM files

The North Korea-linked threat group Kimsuky, known for evolving attack methods, has begun employing Compiled HTML Help (CHM) files to distribute malware and steal sensitive data, enhancing its cyberespionage capabilities since 2012. Targeting primarily South Korea and other regions globally, Kimsuky's recent use of CHM files, capable of executing JavaScript, signifies a sophisticated adaptation aimed at intelligence gathering and supporting North Korea's illicit financial activities.

Kimsuky, also known as Black Banshee or Emerald Sleet, targets entities in South Korea, North America, Asia, and Europe. Kimsuky's use of CHM files in distributing malware alongside other file types like Microsoft Office documents and Windows shortcut files. The attacks are ongoing and evolving, with Kimsuky employing various infection sequences, including using CHM files to initiate data harvesting and establish connections with command-and-control (C2) servers for data exfiltration.

ATTACK TYPE	Malware	SECTOR	All
REGION	South Korea, North America, Europe, Asia	APPLICATION	Windows

Source - https://thehackernews.com/2024/03/n-korea-linked-kimsuky-shifts-to.html

INTRODUCTION | RANSOMWARE EXPLOITS TEAMCITY FLAW | WIPER MALWARE ATTACKS LINUX | CHINESE HACKERS TARGET 70 ORGS | ANDROXGH0ST EXPLOITS VULNERABILITIES | ATLASSIAN RELEASES SECURITY PATCHES | MUDDLED LIBRA INFILTRATES INDUSTRIES | CURIOUS SERPENS SPREADS BACKDOOR | FLUFFY WOLF USES META STEALER | KIMSUKY TARGETS ORGANISATIONS GLOBALLY | CHINESE HACKERS ATTACK F5 BIG-IP

China-linked hackers exploit software flaws to breach networks

The Chinese-affiliated cyber threat group, UNC5174 exploited vulnerabilities in ConnectWise ScreenConnect and F5 BIG-IP to deploy malware targeting Linux systems across the US, UK, and Southeast Asia. Using sophisticated tools like SNOWLIGHT and SUPERSHELL, they focus on intelligence gathering, possibly acting as an initial access broker for the Chinese Ministry of State Security. UNC5174, also known as “Uteus,” has attempted to sell access to various institutions and government entities. Their aggressive targeting includes research and education institutions, businesses, charities, and government organisations.

Despite extensive reconnaissance and scanning, successful exploitation of some strategic targets remains unconfirmed. Notably, it was observed that UNC5174’s infrastructure history, revealing reconnaissance activities and vulnerability scanning on internet-facing systems, particularly prominent universities and think tanks in the US, Oceania, and Hong Kong.

ATTACK TYPE	Malware	SECTOR	Business
REGION	UK, US, Hong Kong, Asia, Oceania	APPLICATION	Apple macOS, Windows, Linux, F5 BIG-IP

Source - https://www.mandiant.com/resources/blog/initial-access-brokers-exploit-f5-screenconnect

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.