TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MARCH 19TH, 2024

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today’s global landscape, cybersecurity is a matter of utmost concern for organisations. With the ever-evolving sophistication of cyber threats, businesses are in a constant pursuit to safeguard their assets and uphold operational continuity. It’s no longer solely about shielding data; it’s about fortifying the fundamental pillars on which modern organisations stand, ensuring resilience against a myriad of emerging threats.

Elevate your organisation’s cybersecurity readiness with Tata Communications’ weekly threat intelligence advisory report. Gain invaluable insights into the latest cyber risks and proactively establish measures to bolster your defences to mitigate potential vulnerabilities.

INTRODUCTION | EVASIVE PANDA TARGETS TIBETANS | MAGNET GOBLIN ATTACKS LINUX SYSTEMS | APPLE PATCHES IPHONE FLAWS | ONLINE MEETING WEBSITES SPREAD RATS | THREAT ACTORS UNLEASH GHOSTLOCKER 2.0 | RANSOMWARE SPREADS VIA POLICIES | BANKING TROJAN TARGETS BRAZILIANS | SOPHISTICATED MALWARE ATTACKS SERVERS | MALWARE CAMPAIGN TARGETS RUSSIANS | FINANCIAL FRAUDS ON THE RISE IN INDIA

Evasive Panda targets Tibetans with innovative threat tactics

Evasive Panda, a threat actor (TA) linked to China, has been orchestrating sophisticated attacks against Tibetan users since September 2023. Utilising watering hole and supply chain tactics, they disseminate malicious downloaders containing the backdoors MgBot and Nightdoor. These attacks, uncovered in January 2024, exploit compromised websites and the supply chain of a Tibetan software company. There are suspicions that they may exploit the Kagyu Monlam Festival in 2024 to target Tibetan communities across multiple countries.

Analysis of the IP address ranges targeted by the code reveals that the attack was aimed at users in India, Taiwan, Hong Kong, Australia, and the United States. Notably, the network of the Georgia Institute of Technology in the US is within the identified entities in the targeted IP address ranges. Previously, the university was cited in connection with the Chinese Communist Party's influence on educational institutions in the US.

ATTACK TYPE	Malware	SECTOR	All
REGION	Australia, India, Taiwan, United States, Hong Kong, Tibet	APPLICATION	macOS, Windows

Source - https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/

INTRODUCTION | EVASIVE PANDA TARGETS TIBETANS | MAGNET GOBLIN ATTACKS LINUX SYSTEMS | APPLE PATCHES IPHONE FLAWS | ONLINE MEETING WEBSITES SPREAD RATS | THREAT ACTORS UNLEASH GHOSTLOCKER 2.0 | RANSOMWARE SPREADS VIA POLICIES | BANKING TROJAN TARGETS BRAZILIANS | SOPHISTICATED MALWARE ATTACKS SERVERS | MALWARE CAMPAIGN TARGETS RUSSIANS | FINANCIAL FRAUDS ON THE RISE IN INDIA

Magnet Goblin group spreads custom malware on Linux systems

Magnet Goblin, a financially motivated hacking group, has capitalised on one-day vulnerabilities in public servers to deploy sophisticated malware like NerbianRAT and MiniNerbian, targeting various systems and services. Their rapid exploitation of disclosed vulnerabilities emphasises the urgency of patching and robust cybersecurity measures. Ivanti's security advisory has highlighted CVE-2023-46805 and CVE-2023-21887 vulnerabilities in Ivanti Connect Secure VPN that were swiftly exploited by multiple TAs for malicious activities.

Check Point Research has tracked these exploits, identifying clusters targeting vulnerable Connect Secure VPN appliances. Despite challenges in attribution, investigation into one prominent cluster linked to Magnet Goblin revealed a methodical approach in using one-day exploits to deploy custom Linux backdoors for financial gain. Notably, Magnet Goblin has targeted Magento, Qlik Sense, Apache ActiveMQ, and remote monitoring and management software like ConnectWise's ScreenConnect, though previous activities were publicly documented without specific attribution.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows, Linux

Source - https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/

Apple patches exploited iPhone zero-day flaws

Apple has swiftly responded to critical security concerns by releasing emergency updates for iOS, addressing two zero-day vulnerabilities exploited in attacks on iPhones. The flaws in the iOS Kernel and RTKit allowed unauthorised access to kernel memory protections, affecting devices from iPhone XS to various iPad models. Apple has not disclosed the origins of the vulnerabilities, urging prompt updates to mitigate risks. This marks the third instance in 2024 where Apple has addressed zero-day vulnerabilities.

The bugs, identified as CVE-2024-23225 and CVE-2024-23296, enabled attackers to bypass kernel memory protections with arbitrary read-and-write capabilities. The security patches apply to devices running iOS 17.4, iPadOS 17.4, iOS 16.76, and iPad 16.7.6, featuring enhanced input validation. While the list of impacted devices is extensive, Apple has not revealed the source of the zero-days or whether they were internally discovered. Despite no information on ongoing exploitation, iOS zero-day vulnerabilities are often exploited in state-sponsored spyware attacks against high-risk individuals like journalists and politicians.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	iOS

Source - https://www.bleepingcomputer.com/news/apple/apple-fixes-two-new-ios-zero-days-exploited-in-attacks-on-iphones/

Android and Windows RATs distributed through deceptive online meeting websites

Researchers uncovered a malicious campaign exploiting fake Skype, Zoom, and Google Meet platforms to disseminate SpyNote RAT for Android and NjRAT/DCRat for Windows. The TA employed deceptive URLs resembling legitimate platforms, hosted under Russian text-laden shared web hosting. Clicking on fake sites triggered downloads of malicious files, emphasising the necessity of robust security measures.

The attacker used a single IP address for hosting all fake meeting sites. Upon visiting, users unwittingly downloaded malicious APK or BAT files, leading to remote access trojan (RAT) payloads. This incident underscores the threat of malware impersonating online meeting apps, highlighting the need for vigilant security practices, regular updates, and patches to combat evolving cyber threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Android, Windows

Source - https://www.zscaler.com/blogs/security-research/android-and-windows-rats-distributed-online-meeting-lures

GhostSec and Stormous team up for widespread GhostLocker 2.0 attacks

The cybercrime collaboration between GhostSec and Stormous has unleashed the GhostLocker 2.0 ransomware, wreaking havoc in the Middle East, Africa, and Asia. Targeting diverse organisations, they demand ransom and threaten data exposure, offering advanced tools like STMX_GhostLocker and GhostPresser. Experts advise a multi-layered security approach and vigilance against emerging cyber threats.

GhostSec, financially motivated, conducts single and double extortion attacks globally, including denial-of-service (DoS) attacks and website takedowns. They claim to support hacktivist causes. Stormous and GhostSec rebuilt their Stmx_GhostLocker RAAS blog on the TOR network, inviting affiliates to join and disclose victims' data. The blog shows victim counts and disclosures, with a $500,000 USD ransom listed, though actual payments remain uncertain.

ATTACK TYPE	Ransomware	SECTOR	Information technology, manufacturing, government, transportation, education, energy, real estate, telecommunications
REGION	India, Argentina, Brazil, China, Cuba, Egypt, Indonesia, Israel, Lebanon, Morocco, Poland, Qatar, South Africa, Thailand, Turkey, Uzbekistan, Vietnam	APPLICATION	Windows

Source - https://blog.talosintelligence.com/ghostsec-ghostlocker2-ransomware/

INTRODUCTION | EVASIVE PANDA TARGETS TIBETANS | MAGNET GOBLIN ATTACKS LINUX SYSTEMS | APPLE PATCHES IPHONE FLAWS | ONLINE MEETING WEBSITES SPREAD RATS | THREAT ACTORS UNLEASH GHOSTLOCKER 2.0 | RANSOMWARE SPREADS VIA POLICIES | BANKING TROJAN TARGETS BRAZILIANS | SOPHISTICATED MALWARE ATTACKS SERVERS | MALWARE CAMPAIGN TARGETS RUSSIANS | FINANCIAL FRAUDS ON THE RISE IN INDIA

RA World ransomware evades antivirus and spreads via policies

The RA World ransomware syndicate, formerly known as the RA Group, has rapidly evolved into a significant cyber threat. Utilising advanced tactics such as manipulating group policies, they target diverse global sectors, notably Latin America's healthcare industry. Employing double-extortion tactics and leveraging the leaked Babuk ransomware source code, RA World poses a formidable challenge. Its attacks, widespread since April 2023, primarily target the US, with additional occurrences in Germany, India, and Taiwan, focusing on healthcare and financial sectors.

The group gains entry through compromised domain controllers, deploying components to the SYSVOL share path for machine Group Policy Object (GPO). Malware placement within the Group Policy infrastructure indicates potential tampering with settings or scripts, facilitating execution across targeted machines during Group Policy processing, amplifying domain-wide impact. Comprehensive defence measures and employee awareness are essential to counter RA World's threats effectively.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, manufacturing, BFSI
REGION	India, Germany, South Korea, Taiwan, US	**APPLICATION**	Windows

Source - https://www.trendmicro.com/en_us/research/24/c/multistage-ra-world-ransomware.html

New banking trojan "CHAVECLOAK" uses malicious PDFs to attack Brazilian users

Researchers have uncovered CHAVECLOAK, a sophisticated banking trojan targeting Brazilian users through malicious PDFs. It employs DLL sideloading and deceptive pop-ups to steal sensitive financial information. This underscores evolving cyber threats in South America, emphasising the need for proactive cybersecurity. CHAVECLOAK has primarily targeted Brazil, utilising various tactics like phishing emails and browser manipulation.

Other notable banking Trojans in South America include Casbaneiro, Guildma, Mekotio, and Grandoreiro. These threats specialise in obtaining online banking credentials and personal data, posing significant risks to users in countries like Brazil and Mexico. CHAVECLOAK's command-and-control (C2) server telemetry has already been analysed thoroughly. The malware's capabilities include blocking screens, logging keystrokes, and displaying deceptive pop-ups, particularly targeting financial portals like banks and cryptocurrency platforms.

ATTACK TYPE	Malware	SECTOR	BFSI
REGION	Brazil and parts of South America	APPLICATION	Windows

Source - https://www.fortinet.com/blog/threat-research/banking-trojan-chavecloak-targets-brazil

Golang-based malware campaign targets Docker, Hadoop, Redis, and Confluence servers

Cybercriminals are targeting poorly configured servers running Apache Hadoop YARN, Docker, Confluence, or Redis with sophisticated Golang-based malware, exploiting vulnerabilities like CVE-2022-26134 in Atlassian Confluence for unauthorised code execution. Researchers discovered Golang payloads camouflaged as bash scripts, evading antivirus detection, indicating a stealthy threat. The campaign deploys unique payloads, including four Golang binaries, automating host discovery and infection.

Attackers exploit common misconfigurations and n-day vulnerabilities for Remote Code Execution (RCE), perpetuating infections. Subsequent shell scripts and Linux attack techniques deliver a cryptocurrency miner, spawn reverse shells, and ensure persistent access. Attribution remains challenging, but the campaign's shell script payloads resemble those of previous cloud attacks, including those linked to TeamTNT, WatchDog, and the Kiss a Dog campaign.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Atlassian Confluence, Docker, Redis

Source - https://www.cadosecurity.com/spinning-yarn-a-new-linux-malware-campaign-targets-docker-apache-hadoop-redis-and-confluence/

SapphireStealer malware campaign uses deceptive tactics to target Russians

A complex malware campaign is targeting Russian individuals by using deceptive PDFs and a counterfeit Russian government site to distribute the SapphireStealer malware. Disguised as PDFs, the executable steals sensitive data, leveraging social engineering tactics. Cyble Research and Intelligence Labs (CRIL) discovered the campaign through an executable obtained from a deceptive URL posing as a fake Russian government site, potentially distributed via spam emails.

Upon execution, SapphireStealer appears as a PDF document, deceiving users. It collects sensitive information while displaying decoy PDFs. The stolen data is sent to a C2 server in a compressed ZIP file. Although the campaign mirrors previous attacks documented by Talos researchers, the identity of the TAs remains elusive. CRIL observed the campaign targeting Russian individuals in late February, highlighting the continued evolution of cyber threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Russia	APPLICATION	Generic

Source - https://cyble.com/blog/sapphirestealer-sneaks-in-deceptive-legal-documents-prey-on-russians/

Pig-butchering scams targeting investors on the rise in India

India is witnessing a surge in financial scams, including the pig-butchering and Telegram Task scams. These target investors through fake trading apps, phishing sites, and deceptive job offers, often masquerading as legitimate platforms. The scams extend beyond India, with evidence linking them to cybercriminals in China. The scammers have also exploited compromised developer accounts, fabricated collaborations with reputable firms, and targeted countries like Taiwan and South Korea.

This underscores the importance of awareness and caution in navigating digital finance. The pig-butchering scam originated in China in 2020 and has spread across Asia, utilising dating and social media platforms to deceive victims into fraudulent cryptocurrency and trading schemes.

ATTACK TYPE	Cybercrime, spam	SECTOR	All
REGION	India, South Korea, Taiwan	APPLICATION	Android

Source - https://cyble.com/blog/the-spreading-wave-of-pig-butchering-scams-in-india/

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.