TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 20, 2024

THREAT INTELLIGENCE ADVISORY REPORT

In today's dynamic digital environment, defending against cyber threats is a strategic priority for organisations across the globe. Companies are not only focused on protecting their data but also on strengthening the core frameworks that support modern business operations, as these threats constantly evolve. The goal is to build resilience against an expanding range of threats.

Tata Communications provides this weekly threat intelligence advisory to help strengthen your organisation's cyber defences. By giving insights into the most recent cyber hazards, we enable you to take preventive efforts to reduce vulnerabilities efficiently.

Chameleon banking Trojan poses as CRM app

In July 2024, mobile threat intelligence experts have uncovered new campaigns from the Chameleon trojan. The Chameleon banking trojan, posing as a customer relationship management (CRM) app, was found targeting a Canadian restaurant chain with global operations. The trojan uses a dropper that bypasses Android 13+ restrictions and misleads the users into feeding their employee ID into what looks like a CRM login page. It then successfully installs the Chameleon payload. By targeting employees with access to corporate banking and CRM systems, attackers can potentially steal financial information and cause significant financial loss.

This campaign underscores the importance of strong security measures and employee awareness about mobile banking malware for both businesses and financial institutions. Financial organisations must fortify their defences and educate customers about the risks posed by such threats.

ATTACK TYPE	Malware	SECTOR	Hospitality
REGION	Europe, Canada	APPLICATION	Android

Source - https://www.threatfabric.com/blogs/chameleon-is-now-targeting-employees-masquerading-as-crm-app

INTRODUCTION | CHAMELEON TROJAN DISGUISES AS CRM APP | CHROME PATCHES CRITICAL FLAW | RHADAMANTHYS INFOSTEALER TARGETS ISRAEL | HACKERS HIJACK SOFTWARE UPDATES | GOGRA TARGETS MEDIA HOUSE | USB WORM THREATENS RUSSIAN TARGETS | PROTON'S EVOLUTION ZOLA DISCOVERED | HAMSTER KOMBAT PLAYERS TARGETED | ANDROID USERS UNDER SIEGE | THREAT CLUSTER ATTACKS INDIAN BUSINESSES

Chrome rushes to patch a critical flaw

Google has released a critical security update to address five vulnerabilities in Chrome. These vulnerabilities, including a critical one, CVE-2024-7532, in the ANGLE graphics engine, could potentially allow attackers to execute malicious code on a device. The remaining four vulnerabilities are rated as high severity and affect various components of the browser. They are CVE-2024-7533, CVE-2024-7550, CVE-2024-7534, CVE-2024-7535, and CVE-2024-7536.

The update, versions 127.0.6533.99/.100 for Windows and Mac, and 127.0.6533.99 for Linux, is being rolled out gradually. This update addresses vulnerabilities found in the ANGLE graphics engine, sharing feature, V8 JavaScript engine, layout component, and WebAudio API. Experts urge users to update the Chrome browser as soon as possible to ensure safety.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Google Chrome

Source - https://securityonline.info/google-chrome-update-fixes-critical-code-execution-vulnerability-cve-2024-7532/

Rhadamanthys infostealer targets Israeli users

Rhadamanthys infostealer malware is targeting Israeli users. This malware, emerged in 2023, is targeting users through sophisticated phishing emails disguised as urgent copyright infringement notices from reputed Israeli media outlets Calcalist and Mako. These emails trick recipients into downloading infected RAR attachment. Once deployed, Rhadamanthys uses advanced techniques to evade detection and steal sensitive data, including passwords, cryptocurrency information, and system details. This malware employs a multi-stage infection process to steal sensitive data.

Experts suggest users implement strict cybersecurity measures to protect themselves from such attacks. This includes implementing strong security measures like email filtering, analysing attachments using sandboxes, deploying endpoint protection software, regular data backup, and employee training to identify and avoid phishing attempts.

ATTACK TYPE	Malware	SECTOR	All
REGION	Israel	APPLICATION	Windows

Source - https://securityonline.info/new-cyber-threat-rhadamanthys-infostealer-targets-israel/

INTRODUCTION | CHAMELEON TROJAN DISGUISES AS CRM APP | CHROME PATCHES CRITICAL FLAW | RHADAMANTHYS INFOSTEALER TARGETS ISRAEL | HACKERS HIJACK SOFTWARE UPDATES | GOGRA TARGETS MEDIA HOUSE | USB WORM THREATENS RUSSIAN TARGETS | PROTON'S EVOLUTION ZOLA DISCOVERED | HAMSTER KOMBAT PLAYERS TARGETED | ANDROID USERS UNDER SIEGE | THREAT CLUSTER ATTACKS INDIAN BUSINESSES

Hackers hijack software updates to spread malware

A Chinese hacking group, StormBamboo (also known as Evasive Panda), has developed an aggressive method to infect devices. The group used DNS poisoning to redirect update requests to their servers. This allows them to distribute malware, like MACMA and POCOSTICK, disguised as legitimate updates for Windows and macOS devices. Following exploitation, the malicious browser extension RELOADEXT was used to exfiltrate the victim's email data.

StormBamboo’s use of a wide range of malware in numerous campaigns demonstrates a large investment of effort, with actively maintained payloads for macOS, Windows, and even network equipment. Recent attacks targeted international NGOs and organisations in China and Taiwan. Experts suggest vigilance and using only trusted sources for software updates.

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

Source - https://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/

GoGra backdoor targets South Asian media organisation

Cybersecurity experts have discovered a new Go-based backdoor, dubbed GoGra, targeting a South Asian media organisation in November 2023. GoGra, believed to be state-sponsored, reads messages from an Outlook username "FNU LNU" whose subject line starts with the word "Input." This clever tactic allows GoGra to blend in with normal traffic, making it harder to detect. GoGra decrypts and executes commands received via emails and transmits results back in a similar encrypted manner.

This incident highlights a growing trend of cyberespionage actors exploiting legitimate cloud services for malicious purposes. Understanding the strategies used by sophisticated attackers like GoGra allows firms to reduce risks and secure their precious data.

ATTACK TYPE	Malware	SECTOR	Broadcast media production and distribution
REGION	South Asia	APPLICATION	Generic

Source - https://thehackernews.com/2024/08/new-go-based-backdoor-gogra-targets.html

USB worm threatens Russian high-value targets

Cybersecurity experts have discovered a malicious self-spreading worm named "CMoon" aimed at high-value targets in Russia. CMoon payload is downloaded when users click on the links to regulatory documents on the compromised website of a gas supply company. Once a device is infected, the worm can steal login credentials and other sensitive data. It also can download additional malware, capture screenshots, and even launch denial-of-service attacks, further disrupting operations. Even though the compromised gas company website has been taken down, CMoon's self-replication capabilities pose an ongoing risk.

This attack appears to be focused on Russia, with Windows machines being the primary target. Experts advise caution when downloading files, especially from unfamiliar websites. Users are urged to regularly update security software and remain vigilant for suspicious activity.

ATTACK TYPE	Malware	SECTOR	All
REGION	Russia	APPLICATION	Windows

Source - https://www.bleepingcomputer.com/news/security/new-cmoon-usb-worm-targets-russians-in-data-theft-attacks/

Zola ransomware: Proton's deadly evolution

In March 2024, experts uncovered a new ransomware Zola, which, on further investigation, turned out to be a new variant of the Proton family. This new strain boasts unique features like a "Persian kill switch" that shuts down if a specific keyboard layout is detected. It employs advanced anti-forensic techniques to hamper data recovery efforts after an attack. Zola also uses advanced encryption techniques, including the ChaCha20 scheme. While these features are new, Zola retains the core functionalities that made the Proton family so successful.

This threat highlights the constant evolution of ransomware tactics, a worrying trend for businesses worldwide. Businesses should be vigilant, update security software regularly, and implement robust backup procedures to mitigate the risks posed by Zola and other evolving ransomware threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.acronis.com/en-us/cyber-protection-center/posts/zola-ransomware-the-many-faces-of-the-proton-family/

INTRODUCTION | CHAMELEON TROJAN DISGUISES AS CRM APP | CHROME PATCHES CRITICAL FLAW | RHADAMANTHYS INFOSTEALER TARGETS ISRAEL | HACKERS HIJACK SOFTWARE UPDATES | GOGRA TARGETS MEDIA HOUSE | USB WORM THREATENS RUSSIAN TARGETS | PROTON'S EVOLUTION ZOLA DISCOVERED | HAMSTER KOMBAT PLAYERS TARGETED | ANDROID USERS UNDER SIEGE | THREAT CLUSTER ATTACKS INDIAN BUSINESSES

Hamster Kombat players under malware attack

Security researchers warn of a widespread malware campaign featuring fake games malware imitating the popular clicker game “Hamster Kombat” targeting both Android and Windows users. Fake apps and infected tools that flood users with unwanted ads are circulating through unofficial channels. These malicious programs can subscribe gamers to unwanted premium services, draining their wallets.

In particular, Windows users are at risk from GitHub repositories hosting farm bots and auto-clickers embedded with Lumma Stealer malware, which is designed to steal valuable data. Cybersecurity experts are advising players to be cautious and download the game only from the official app and be cautious about "play-to-earn" scams.

ATTACK TYPE	Malware	SECTOR	Gaming industry
REGION	Global	APPLICATION	Windows, Android

Source - https://gbhackers.com/hamster-kombat-malware-attack/

Gigabud phishing attack on Android users

Since July 2024, researchers have observed a surge in activity by Gigabud malware. This malware employs sophisticated phishing tactics, mimicking legitimate airline and financial applications to trick victims into downloading and installing it. Analysis reveals a significant overlap in the code with another malicious program Golddigger. Both malware strains utilise similar techniques, such as the use of a native file named "libstrategy.so," which aids in mimicking user interfaces of banking apps. This suggests both are likely the handiwork of the same cybercriminal group.

The latest version of Gigabud features more than 30 API endpoints, enabling it to support a wide range of new features. This development indicates a deliberate effort by the threat actors to persistently evolve the malware's functionality. These malware programs can steal sensitive data from Android devices.

ATTACK TYPE	Malware	SECTOR	All
REGION	Bangladesh, Ethiopia, Indonesia, Mexico, South Africa	APPLICATION	Android

Source - https://cyble.com/blog/unmasking-the-overlap-between-golddigger-and-gigabud-android-malware/

Cyber threat cluster targets Indian businesses

Cybersecurity researchers have uncovered a new sophisticated threat activity cluster STAC6451 targeting Indian organisations. It exploits vulnerabilities in Microsoft SQL Servers to gain unauthorised access and activates the “xp_cmdshell” feature to enable remote code execution. Once in, it executes malicious programs, including ransomware like Mimic. The ultimate aim is to deploy ransomware, potentially causing significant disruption and financial losses. The cluster stages its attacks by uploading payloads via the Bulk Copy Program (BCP) and creating backdoor accounts to maintain persistence within the compromised network. It also uses tools like Cobalt Strike for lateral movement and privilege escalation.

Experts urge organisations to review security configurations and update all software with the latest patches, monitor for suspicious activity and unauthorised access attempts, and regularly assess security posture to identify and address any vulnerabilities.

ATTACK TYPE	Ransomware, Malware	SECTOR	All
REGION	India	APPLICATION	Microsoft SQL Server

Source - https://news.sophos.com/en-us/2024/08/07/sophos-mdr-hunt-tracks-mimic-ransomware-campaign-against-organizations-in-india/

TATA COMMUNICATIONS

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.