TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: May 28, 2024

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

In today's dynamic digital landscape, defending against cyber threats has emerged as a critical priority for organisations worldwide. With these threats evolving constantly, companies are not just focused on safeguarding their data but also on reinforcing the fundamental frameworks that drive modern business operations. The goal is to establish resilience against an ever-expanding array of emerging threats.

Elevate your organisation's cybersecurity readiness with Tata Communications' weekly threat intelligence advisory. Gain invaluable insights into the most recent cyber risks and implement proactive strategies to strengthen your defences, effectively mitigating potential vulnerabilities.

Chrome hit by sixth zero-day vulnerability of 2024

Google has issued urgent security updates for Chrome to address a high-severity zero-day vulnerability in the V8 JavaScript engine. Known as CVE-2024-4761, this flaw allows out-of-bounds writes, posing significant security risks such as unauthorised data access and arbitrary code execution. This update arrives just three days after a previous patch for CVE-2024-4671, a use-after-free vulnerability in the Visuals component.

Google urges Mac, Windows, and Linux users to update to the latest version 124.0.6367.207/.208 immediately to ensure protection. The vulnerability, reported by an anonymous researcher on 9 May 2024, is the sixth zero-day vulnerability in Chrome that Google has addressed this year. Full details are expected to remain restricted until most users have applied the fix to prevent further exploitation.

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

Source- https://www.bleepingcomputer.com/news/security/google-chrome-emergency-update-fixes-6th-zero-day-exploited-in-2024/

VMware patches bugs unveiled at Pwn2Own

VMware has patched four critical security vulnerabilities in its Workstation and Fusion hypervisors, including three zero-day exploits unveiled at the Pwn2Own Vancouver 2024 contest. The researchers earned significant rewards for their findings and prompted rapid responses from VMware, Google, and Mozilla.

The most severe flaw, CVE-2024-22267, is a use-after-free issue in the vBluetooth device, which potentially allows code execution on the host by a local admin on a virtual machine. VMware advises administrators to disable Bluetooth sharing if they cannot update immediately. Two additional high-severity vulnerabilities, CVE-2024-22269 and CVE-2024-22270, allow local admins to read privileged information from the hypervisor memory. The fourth flaw, CVE-2024-22268, involves a heap buffer overflow in the Shader functionality, which could lead to a denial of service if 3D graphics are enabled. These fixes highlight the importance of timely updates to maintain virtual environment security.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	VMware Fusion, VMWare Workstation

Source- https://www.bleepingcomputer.com/news/security/vmware-fixes-three-zero-day-bugs-exploited-at-pwn2own-2024/

Malicious emails deliver LockBit ransomware

Since April 24, 2024, researchers have been tracking malicious email campaigns that use Phorpiex's botnet to spread LockBit Black ransomware. This week-long series of high-volume campaigns marked the first large-scale use of the botnet, sending millions of emails daily, focusing on various global industries. The attack involved ZIP file attachments containing executables that downloaded the ransomware, likely created using a leaked 2023 builder.

The Cacti network monitoring framework maintainers have patched a dozen security flaws, including two critical vulnerabilities, CVE-2024-25641 and CVE-2024-29895, which could allow remote code execution. The remaining ten vulnerabilities impact all Cacti versions up to 1.2.26, posing significant challenges, especially with public proof-of-concept exploits available. Users are urged to update their instances to version 1.2.27 immediately to mitigate potential threats.

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

Source- https://thehackernews.com/2024/05/critical-flaws-in-cacti-framework-could.html

SideCopy and Transparent Tribe target India with similar tactics

The SideCopy advanced persistent threat (APT) group has been targeting South Asian nations, particularly India, with sophisticated malware campaigns targeting university students, via a malicious website, active since 2019. Evidence points to a potential overlap with Transparent Tribe, another APT group known for targeting universities, suggesting coordinated efforts.

The infection vector involves spam emails leading to a malicious archive file containing a shortcut (LNK) file. Once triggered, these files initiate a series of infection steps, deploying malware payloads like Reverse RAT and Action RAT, which then connect to command-and-control (C2) servers to commence malicious activities. As SideCopy constantly evolves its methods, understanding its operations is essential to avoid and swiftly respond to threats, safeguarding infrastructure and sensitive information.

ATTACK TYPE	Malware	**SECTOR**	Government, education, defence
REGION	India	**APPLICATION**	Windows

Source- https://cyble.com/blog/the-overlapping-cyber-strategies-of-transparent-tribe-and-sidecopy-against-india/

Threat actors exploit Microsoft's Quick Assist

Microsoft's threat intelligence team has identified a financially motivated cybercriminal group – Storm-1811 – exploiting Quick Assist through sophisticated social engineering campaigns. These attacks use impersonation and voice phishing to trick users into installing remote management tools, leading to the deployment of malware such as QakBot, Cobalt Strike, and Black Basta ransomware. The group's tactics include pretending to be tech support agents to gain initial access to devices and then running commands to download malicious payloads.

Active since April 2024, the campaign targets various industries, including manufacturing and transportation, to execute domain enumeration, lateral movement, and eventually deploy Black Basta ransomware across the network. Microsoft advises organisations to block or uninstall Quick Assist if not needed and to train employees to recognise tech support scams. The company is also working on incorporating warning messages in Quick Assist to alert users of potential scams.

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

Source- https://thehackernews.com/2024/05/cybercriminals-exploiting-microsofts.html

Russian hackers target diplomats with Lunar malware

The Russia-aligned Turla group, known for targeting high-profile entities, has launched a cyberespionage campaign against the European Ministry of Foreign Affairs (MFA) and its Middle Eastern missions, using two new backdoors, LunarWeb and LunarMail. The campaign employs advanced techniques, including exploiting software misconfigurations, http(s), email-based C2 channels, and spear-phishing to gain access.

LunarWeb mimics legitimate traffic for its communications, while LunarMail, persisting as an Outlook add-in, uses email messages. Both employ steganography to hide commands in images. The attack likely involved prior access to the MFA's domain controller for lateral movement. The investigation, which began with a payload decryption by a loader, revealed these backdoors to have been operational since at least 2020. Microsoft advises organisations to be vigilant and take proactive security measures against such threats.

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

Source- https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

Hackers exploit design flaw in Foxit PDF Reader

Cybercriminals have exploited a flaw in the Foxit PDF Reader, leading to significant security breaches and malicious command executions. Despite Adobe Acrobat Reader's market dominance, Foxit PDF Reader has a large user base, with 700 million+ active users in over 200 countries, including clients in the government and tech sectors.

The critical vulnerability causes users to be deceived into executing harmful commands by triggering security warnings and enabling sophisticated attacks involving espionage and cybercrime. The low detection rate of this exploit is due to the widespread use of Adobe Reader, which is not vulnerable to this flaw. With Foxit planning to resolve this issue in their 2024 update, users are advised to remain vigilant and follow standard cybersecurity practices in the meantime

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Foxit PDF Reader, Foxit PhantomPDF

Source- https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/?s=08

Kimsuky group unleashes new Linux malware

In early 2024, researchers identified Kimsuky, a North Korean hacker group, deploying a new Linux malware variant called Gomir. Derived from the GoBear backdoor, Gomir is spread via trojan software installers targeting South Korean entities. This malware shares several features with GoBear such as C2 communication and persistence mechanisms.

It operates with root privileges and ensures its persistence on infected systems. The malware supports 17 distinct operations triggered by commands from the C2 server via http POST requests. The campaign highlights North Korean espionage actors' preference for supply-chain attacks to maximise infection rates among South Korean targets. Researchers have also provided indicators of compromise for Gomir and related tools.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	South Korea	**APPLICATION**	Linux

Source- https://www.bleepingcomputer.com/news/security/kimsuky-hackers-deploy-new-linux-backdoor-in-attacks-on-south-korea/

Andariel group launches Dora RAT attacks

Recent reports confirm that the Andariel group has launched APT attacks on domestic companies and institutions, specifically targeting the manufacturing, construction, and educational sectors. Using backdoors, keyloggers, and infostealers, the group aims to control infected systems and steal sensitive data. Key malwares include the Nestdoor backdoor and the newly developed Dora RAT.

These attacks exploit vulnerabilities in outdated software, such as Apache Tomcat. Notably, tools from previous Lazarus group campaigns were also used. Andariel's attacks typically involve spear-phishing, watering-hole attacks, and software breaches. To mitigate risks, experts advise updating software patches and being cautious with email attachments from unknown sources.

ATTACK TYPE	Malware	**SECTOR**	Manufacturing, construction, education
REGION	South Korea	**APPLICATION**	Windows

Source- https://asec.ahnlab.com/ko/65495/

New malware SamsStealer steals sensitive data

Researchers have identified “SamsStealer,” a new 32-bit Windows malware written in .NET, targeting browsers and applications such as Discord, Chrome, and Microsoft Edge. This information stealer covertly extracts sensitive data, including passwords, cookies, and cryptocurrency wallet details. After collecting the data, it compresses it into a ZIP file, uploads it on an online file-sharing service, and sends the download link to the attacker via Telegram.

SamsStealer poses a significant threat to user privacy and security due to its stealthy operation, comprehensive data exfiltration capabilities, and use of concurrency for efficiency. As cyber threats evolve, mitigating the tactics employed by malware like SamsStealer is crucial for protecting sensitive information. Security professionals are advised to remain vigilant and adopt proactive defence strategies to stay safe against such threats.

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

Source- https://www.cyfirma.com/research/samsstealer-unveiling-the-information-stealer-targeting-windows-systems/

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