TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 6, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Cybersecurity has become a top priority for organisations around the world. The digital environment is continuously changing, producing new risks to sensitive data and the underlying infrastructure that underpins modern business. Building resilience in the face of an ever-expanding danger situation is critical.

Tata Communications provides a weekly threat intelligence advisory to help strengthen your organisation's cyber defences. This report gives insights into the most recent cyber hazards, enabling you to take preventive efforts to reduce and address potential vulnerabilities efficiently.

New infostealer mimics CrowdStrike repair manual

Cybercriminals are exploiting recent IT outages caused by a faulty CrowdStrike Falcon software update. CrowdStrike has issued a warning about this new information-stealing malware named Daolpu. It is being distributed through phishing emails. These emails masquerade as a recovery manual for Windows devices affected by the faulty update. The Daolpu malware is designed to steal login credentials and browser data from popular browsers like Chrome, Edge, Firefox, and Cốc Cốc. Daolpu has also been observed to collect system information, including hardware specifications and network configurations.

Cybercriminals are taking advantage of the confusion caused by the Falcon update's global IT outages to spread Daolpu and other malicious software. Users are advised to be vigilant and avoid downloading attachments from unsolicited emails to protect data from being compromised.

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

Source - https://www.bleepingcomputer.com/news/security/fake-crowdstrike-repair-manual-pushes-new-daolpu-infostealer-malware/

Chinese hackers upgrade macOS backdoor

Evasive Panda, a Chinese hacking group, have revamped their cyberespionage toolkit. Recent attacks in Taiwan and China saw them deploy updated versions of the Macma backdoor for macOS and Nightdoor malware for Windows. These attacks exploited server vulnerabilities and used sophisticated delivery methods. The group also utilised their advanced MgBot malware framework, highlighting their commitment to continuous tool development and staying ahead of detection.

The group's continued development of these tools highlights their persistent threat to organisations worldwide. Evidence indicates that Evasive Panda is actively exploring lateral movement capabilities within compromised networks. This suggests an increased interest in establishing persistent footholds and expanding their access to sensitive information. Cybersecurity experts recommend strong security measures to protect against such attacks.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	China, Taiwan	**APPLICATION**	Apple macOS, Windows

Source - https://www.bleepingcomputer.com/news/security/evasive-panda-hackers-deploy-new-macma-macos-backdoor-version/

TATA COMMUNICATIONS

Critical Docker flaw puts systems at risk

A critical flaw (CVE-2024-41110) has been discovered in Docker Engine versions 19.03.x and later. This vulnerability could allow attackers to bypass authorisation plugins and potentially gain complete control of the system. While the likelihood of an exploit is considered low, the potential impact is severe, especially for those running Docker in production environments. Given the widespread use of Docker in various industries, from cloud-native applications to software development, the consequences of a successful attack could be far-reaching.

To mitigate this risk, Docker recommends updating Docker Engine and Docker Desktop to the latest versions as soon as possible. If immediate updates are not feasible, temporary workarounds are available to reduce the attack surface. This vulnerability impacts all sectors globally using Docker applications. Experts recommend updating security patches and implementing security measures for enhanced protection.

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

Source - https://securityonline.info/docker-users-beware-cve-2024-41110-cvss-10-could-lead-to-system-takeover/

CISA warns to patch Microsoft and Twilio urgently

The UK's National Cyber Security Centre (NCSC) echoes a critical warning from the US Cybersecurity and Infrastructure Security Agency (CISA) regarding two actively exploited vulnerabilities. The reported flaws in Microsoft Internet Explorer (CVE-2012-4792) and Twilio Authy (CVE-2024-39891) pose significant risks, allowing attackers to remotely hijack systems and potentially access phone number data. These flaws are actively being exploited by malicious actors. These vulnerabilities can serve as entry points for broader attacks. Successful exploitation can lead to data breaches, ransomware deployments, and other malicious activities.

CISA urges immediate action, including applying patches, discontinuing the use of legacy browsers, and strengthening overall security measures. These threats impact all sectors globally, particularly Windows applications. Users and organisations are advised to prioritise these updates and enhance their security protocols.

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

Source - https://securityonline.info/cisa-warns-critical-exploits-targeting-microsoft-and-twilio-authy-discovered-in-the-wild/

Sophisticated malware targeting Indian politicians

A recently uncovered cyberattack campaign is targeting Indian politicians with a highly sophisticated malware payload. This malicious software, delivered through a deceptively simple .LNK file, leverages PowerShell to deploy a .NET loader. This loader then extracts a steganographically hidden payload from a seemingly innocuous PNG image. This payload, a Go-written Remote Access Trojan (RAT), grants attackers extensive control over the infected system, including the ability to deploy ransomware. The campaign displays a clear focus on Indian political figures, with the malware specifically designed to evade detection in Russian-speaking regions. This suggests that the threat actors are likely Russian-speaking and financially motivated.

The attack primarily affects Windows applications within the Indian government sector, highlighting the critical nature of this threat. To protect against this sophisticated attack, individuals, especially those involved in Indian political affairs, are strongly advised to exercise extreme caution when handling unknown files, particularly .LNK shortcuts.

ATTACK TYPE	Malware	**SECTOR**	Govt
REGION	India	**APPLICATION**	Windows

Source - https://cyble.com/blog/operation-shadowcat-targeting-indian-political-observers-via-a-stealthy-rat/

Vietnamese malware Braodo Stealer stealing logins

A new Vietnamese malware, Braodo Stealer, is targeting logins and banking information. Disguised as a zip file, this Python-based malware steals cookies, credentials, and system data upon extraction. It runs batch files to maintain persistence on the infected system. It then transmits the loot to the attackers via Telegram.

Braodo Stealer is regularly updated, with a strong emphasis on collecting network-related information for potential active reconnaissance. Braodo demonstrates a high level of sophistication. Its focus on network-related information suggests the potential for wider, more complex attacks in the future. Furthermore, the malware's preference for Python indicates a growing trend of malware developers increasingly using Python. Users are urged to use reliable antivirus software and exercise caution online.

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

Source - https://labs.k7computing.com/index.php/echoes-of-braodo-tales-from-the-cyber-underworld/

TATA COMMUNICATIONS

Global Microsoft 365 attack via Botnet

Cybercriminals are leveraging a botnet, known as Quad7 (7777), to launch brute-force attacks on Microsoft 365 accounts worldwide. This botnet, active since 2022, targets unsecured routers, particularly TP-Link models, to gain access and exploit vulnerabilities. It employs advanced techniques to avoid detection. The botnet's operations span several regions, including Russia, Bulgaria, Ukraine, and the United States, and affect all sectors.

The source of the attacks and specific weaknesses remain unclear, highlighting the need for international collaboration to combat this evolving threat. Businesses and individuals alike are advised to implement strong password policies and remain vigilant against suspicious activity in their Microsoft 365 accounts.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Russia, Bulgaria, Ukraine, United States	**APPLICATION**	Windows

Source - https://blog.sekoia.io/solving-the-7777-botnet-enigma-a-cybersecurity-quest/

GhostEmperor hacking group returns

An alarming development has been reported as the GhostEmperor hacking group resurfaces with an upgraded Demodex rootkit. This group is known for targeting governments and telecommunications companies. This malware shows improved evasion techniques and uses a reflective loader to execute its core implant. The upgraded malware utilises a multi-stage attack, including the installation of a kernel rootkit using sophisticated PowerShell scripts and DLL operations, to gain deep access to infected systems. The threat impacts all sectors and specifically targets Windows applications.

This incident highlights the evolving tactics of cybercriminals and underscores the crucial need for strong cybersecurity solutions and staying informed about the latest threats. Businesses and organisations in Southeast Asia are particularly advised to be vigilant.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	South Asia	**APPLICATION**	Windows

Source - https://www.sygnia.co/blog/ghost-emperor-demodex-rootkit/

Indian government departments targeted by phishing campaign

A recent cyberattack campaign has targeted Indian government departments with malicious phishing emails. The group behind the attack, TransparentTribe, is suspected to be based in Pakistan and has a history of targeting India. These attacks employ CrimsonRAT, a Trojan designed to steal sensitive information and system data, distributed via phishing emails. The emails, disguised as official documents related to the President's Award, contained malware capable of stealing sensitive data. This group demonstrates a high level of technical expertise and determination.

Indian government departments are advised to remain vigilant against phishing attempts and to implement strong cybersecurity measures. This includes implementing advanced threat detection and response solutions, employee training, and regular security audits.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	India	**APPLICATION**	Generic

Source - https://securityboulevard.com/2024/07/transparenttribes-spear-phishing-targeting-indian-government-departments/ https://labs.k7computing.com/index.php/threat-actors-target-recent-election-results/

Phishing scam targets Indian iPhone users

Indian iPhone users are being targeted by a sophisticated phishing campaign impersonating India Post. Smishing attacks deliver fake iMessages claiming undelivered packages awaiting collection at an India Post warehouse. Victims are tricked into clicking on malicious links that lead to fake India Post websites, where they are prompted to enter personal and financial information. The campaign's sophistication and scale highlight the increasing threat of smishing attacks in India. The fraud is attributed to the China-based Smishing Triad. This China-based operation has registered over 470 deceptive domains, primarily through Chinese registrars, and invested heavily in domain hosting.

The attacks aim to steal sensitive information like names, addresses, and even credit card details. Users are advised to be cautious of unsolicited messages, avoid clicking suspicious links, and verify any claims of package deliveries directly with India Post.

ATTACK TYPE	Phishing	**SECTOR**	All
REGION	India	**APPLICATION**	Apple iOS

Source - https://www.fortinet.com/blog/threat-research/phishing-campaign-targeting-mobile-users-in-india-using-india-post-lures

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