TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 27, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As digital transformation accelerates, the frequency and complexity of cyber threats continue to escalate. Organisations must now focus on defending their data and fortifying the infrastructure supporting their operations. This requires a proactive and forward-thinking approach to cybersecurity, where the goal is to not only react to threats but to anticipate them and build a robust line of defence that adapts to new and emerging risks.

Empower your organisation with Tata Communications' weekly threat intelligence advisory. Offering comprehensive insights into the most current cyber risks, this advisory equips you with the knowledge needed to enhance your security protocols. By staying informed about the latest threats, your business can implement preventive measures that reduce vulnerabilities, safeguarding your operations against an ever-evolving digital threat landscape.

The 7777 botnet exploits Asus routers

Cybersecurity experts have warned that 7777 botnet infections are on the rise, with nearly 13,000 active bots detected over a 30-day period ending 05 August 2024. Initially targeting Microsoft Azure cloud servers, this botnet has shifted its focus to exploiting Asus router vulnerabilities. The botnet uniquely opens the TCP port 7777 on compromised “zombie” routers. When scanned, the service on this port returns an xlogin: banner. Once compromised, the infected router opens a communication channel on port 7777, allowing the attacker remote control over the device.

Security experts recommend keeping the router firmware up to date, using strong and unique passwords, creating a separate guest Wi-Fi network, and maintaining vigilant network monitoring to defend against this threat.

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

Source - https://www.team-cymru.com/post/botnet-7777-are-you-betting-on-a-compromised-router

Cyberattackers target Ukraine with phishing

The Computer Emergency Response Team of Ukraine (CERT-UA) has identified a threat called UAC-0198, where attackers impersonate the Security Service of Ukraine (SSU) to distribute malware via phishing emails. These emails trick recipients into clicking malicious links or downloading infected attachments. The ANONVNC malware used allows remote access to steal credentials, disrupt operations, and launch further attacks. CERT-UA also reports phishing attempts mimicking UKR.NET login pages and using PicassoLoader malware to spread Cobalt Strike Beacon for deeper network infiltration.

CERT-UA urges all organisations in Ukraine to remain vigilant against suspicious emails and to verify the authenticity of messages claiming to be from official sources. Strengthening security measures, such as implementing multi-factor authentication and regularly monitoring systems, is crucial in mitigating the risks posed by these sophisticated phishing threats.

ATTACK TYPE	Phishing	**SECTOR**	All
REGION	Ukraine	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/08/ukraine-warns-of-new-phishing-campaign.html

APT36 malware attacks government systems

A recent investigation uncovered malicious software hosted on an open directory, linked to Pakistan-based APT36 (also known as Transparent Tribe) and its subgroup, SideCopy. These groups have targeted the Indian Air Force, shipyards, and port authorities, raising concerns about potential data breaches and disruptions. Experts found significant overlaps between APT36, SideCopy, and another hacking group, RusticWeb. These groups are known to share infrastructure, utilise enticing files to lure victims, and employ advanced techniques to bypass security measures to infiltrate Indian systems and steal sensitive data.

India's cybersecurity defences must stay vigilant against evolving attacks from Pakistani hacking groups. Experts urge government entities to strengthen security with regular system updates, employee training, and enhanced network monitoring to protect national security.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	India	**APPLICATION**	Windows, Linux

Source - https://www.seqrite.com/blog/umbrella-of-pakistani-threats-converging-tactics-of-cyber-operations-targeting-india/

Microsoft patches critical vulnerabilities

Microsoft's August 2024 Patch Tuesday addresses a total of 89 flaws affecting Windows users. Among these, six flaws are being actively exploited by attackers, and three additional zero-day vulnerabilities are publicly disclosed. Microsoft is still working on a fix for a tenth zero-day threat. Among the 89 vulnerabilities addressed, eight are categorised as critical, involving elevation of privileges, remote code execution, and information disclosure. The actively exploited vulnerabilities could allow attackers to gain unauthorised access, execute arbitrary code, or expose sensitive information.

Users and organisations are strongly urged to apply these updates immediately to protect against potential threats. Ensuring that systems are patched promptly is essential in mitigating the risks.

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

Source - https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2024-patch-tuesday-fixes-9-zero-days-6-exploited/

ValleyRAT campaign targets financial sector

Security experts have warned of a sophisticated malware campaign utilising ValleyRAT targeting Windows machines used in China. This malware tricks the users by displaying icons of legitimate applications, including Microsoft Office, with filenames related to financial documents. It injects malicious code directly into memory and uses advanced evasion tactics to avoid standard security measures. Once established, it communicates with a central server, allowing attackers to monitor victim activity, steal data, and potentially deploy additional malicious tools.

Financial services, e-commerce, and investment management sectors in China are particularly at risk. Experts recommend immediate action, including updating antivirus software and implementing robust monitoring tools, to mitigate the risks associated with this malware.

ATTACK TYPE	Malware	**SECTOR**	Financial services, e-commerce, investment management
REGION	China	**APPLICATION**	Windows

Source - https://www.fortinet.com/blog/threat-research/valleyrat-campaign-targeting-chinese-speakers

Hacktivist groups unleash DDoS attacks

Hacktivist groups such as RipperSec, CyberEcho BD, Bangladesh Dark Net, and Anonymous KSA have launched attacks targeting Indian websites from a wide range of sectors. These attacks, which include Distributed Denial of Service (DDoS) attacks and website defacement, have disrupted online services and caused inconvenience to users. While the authenticity of some of these claims remains unverified, the trend is clear. Organisations in India must be prepared to face an increased threat of cyberattacks from hacktivist groups.

Considering these developments, organisations are advised to upgrade their cybersecurity measures. Enhancing defences against DDoS attacks, implementing robust firewalls, and conducting regular security audits are crucial steps to reduce the risk of such hacktivist activities.

ATTACK TYPE	DDoS	**SECTOR**	All
REGION	India	**APPLICATION**	Generic

Source - TATA Comm research

Black Basta's SystemBC malware threat

The Black Basta ransomware gang is deploying a new attack strategy involving the SystemBC malware. This campaign leverages social engineering tactics to infiltrate user systems. Black Basta sends email barrages ("email bombs") to overwhelm inboxes. These emails might appear urgent or contain fake notifications. Following the emails, users may receive calls claiming to be from IT support, urging them to install legitimate remote access software, AnyDesk, to "fix" the email issue. Once AnyDesk is installed, attackers exploit it to steal login credentials and deploy the SystemBC malware. SystemBC acts as a gateway for further malicious activity, potentially leading to data theft or ransomware deployment.

To counter these evolving threats, organisations and individuals must remain vigilant and implement robust security measures. Enhancing email filtering, conducting regular security training, and ensuring up-to-date antivirus protection are essential steps to mitigate the risks posed by such social engineering attacks.

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

Source - https://www.rapid7.com/blog/post/2024/08/12/ongoing-social-engineering-campaign-refreshes-payloads/

Spear-phishing attack on NGOs

Eastern European non-governmental organisations (NGOs) and independent media outlets are facing a barrage of cyberattacks believed to be orchestrated by Russian hackers. Two separate spear-phishing campaigns, dubbed "River of Phish" and "COLDWASTREL," have been identified targeting these groups. The "River of Phish" campaign, attributed to the COLDRIVER group with links to Russia's Federal Security Service (FSB), employs advanced social engineering tactics. These tactics involve sending highly convincing phishing emails designed to trick recipients into revealing sensitive login credentials. A newly identified group, COLDWASTREL, has also emerged, using similar methods with subtle variations. Both campaigns aim to infiltrate target systems and potentially steal valuable data.

The attacks highlight the growing threat to organisations in Europe, particularly those involved in broadcast media production and distribution. Regular training, rigorous email filtering, and maintaining up-to-date security protocols are essential to lower the risks posed by these campaigns.

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

Source - https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/

Gafgyt variant exploits weak SSH passwords

Researchers have discovered a new variant of the Gafgyt botnet targeting machines with weak SSH passwords, focusing on mining cryptocurrency using GPU power, particularly in cloud-native environments. Previously known for DDoS attacks, Gafgyt has shifted its strategy to infiltrate systems and exploit their GPU power for cryptomining. Once gaining access through brute forcing an SSH connected to the internet, the malware downloads two payloads via the newly established SSH connection. It also employs advanced techniques to maintain control over compromised systems, highlighting the urgent need for organisations to secure their SSH servers against evolving threats.

Organisations across all sectors are urged to implement strong SSH password policies, regularly update software, and monitor network activity for unusual behaviour to protect against this growing threat.

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

Source - https://www.aquasec.com/blog/gafgyt-malware-variant-exploits-gpu-power-and-cloud-native-environments/

Hackers spread malware via fake brand sites

Cybersecurity researchers have uncovered a sophisticated information stealer campaign called "Tusk," targeting Windows and macOS users. Orchestrated by Russian cybercriminals, Tusk uses fake websites and social media accounts that mimic legitimate brands to deceive users into downloading malware like DanaBot and StealC. These malicious programs can steal login credentials, financial information, and other sensitive data. The campaign is widespread, operating through multiple sub-campaigns and primarily delivered via phishing emails. This approach leaves users vulnerable to financial fraud and other serious security risks.

Organisations and individuals must exercise caution and enhance their security measures to protect against such threats. Regularly updating software, verifying the authenticity of websites, and staying informed about the latest phishing tactics are crucial steps in mitigating the risks posed by this campaign.

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

Source - https://thehackernews.com/2024/08/russian-hackers-using-fake-brand-sites.html

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