TATA COMMUNICATIONS

TATA

QUARTERLY EXECUTIVE THREAT REPORT Q2 2024

Executive Summary

The Jul-Sep quarter of 2024 has seen a surge in advanced persistent threats (APTs), ransomware attacks, and zero-day exploits, underscoring the evolving tactics of cybercriminals. Attackers are expanding their arsenal, leveraging complex malware, phishing campaigns, and ransomware to target enterprise weaknesses. This quarterly report delves into the most significant cybersecurity threats observed in Q2 2024, analysing their threat vectors, their extensive impact on global businesses, and Tata Communications' strategic recommendations for enhancing your organisation's cybersecurity posture. Through these insights, we aim to equip you with the knowledge to build a resilient, agile, and comprehensive cybersecurity framework that can withstand the rapidly evolving threat landscape.

A Landscape of New Threats – Quarterly Highlights

> ***'Recent threat reports have observed a 2% increase in incidences of ransomware in Q2 2024. This rise underscores the continued prominence of ransomware activity.[1]'***

As 2024 crosses the halfway mark, malware and ransomware attacks continue to evolve in new and terrifying ways. Both in terms of scope and complexity, these cyberthreats assert a renewed focus on critical infrastructure across industries, with healthcare, education, research, military, and government and military entities being targets of interest in Q2. Security initiatives need to be recalibrated beyond their current reactive parameters and into more proactive threat-hunting frameworks that are driven by AI if they are to stave off future catastrophes.

Advisories from global regulatory bodies are being released on regularly, with greater emphasis on stricter data protection and collaborative governance between public and private sector entities. This in turn strongly incentivises enterprises to shore up their cybersecurity infrastructure with zero-trust architecture and various other safeguards: an indicator of an even more serious approach to ensuring security.

> ***'In Q2 2024, the global cybersecurity landscape saw a significant surge in both the volume and impact of cyber threats. Research has shown a 30% increase in global cyberattacks in Q2 2024, highlighting the growing prevalence of these threats.[2]'***

Adapting to an Evolving Threat Ecosystem – Top Ten Threats of Q2 2024

Based on the insights from the Tata Communications threat intelligence, below are some of the key threats identified in Q2.

New PEAKLIGHT malware targets Windows

Businesses using Windows systems are on high alert following the discovery of PEAKLIGHT, a sophisticated in-memory malware dropper[3]. Disguised as pirated movie downloads, PEAKLIGHT launches PowerShell-based attacks that install malware like Lumma Stealer and CryptBot. PEAKLIGHT's memory-only execution minimises forensic traces, making detection and removal difficult.

The rise of PEAKLIGHT underscores the growing threat of supply chain attacks and the importance of robust cybersecurity defences. Organisations must prioritise user awareness training and utilise trusted software sources to mitigate these evolving threats.

Codes left vulnerable to exploitation with unpatched Gogs flaws

Gogs, a widely used open-source Git service, is at risk[4] due to critical unpatched vulnerabilities. The vulnerabilities, according to cybersecurity researchers, are CVE-2024-39930 (CVSS score: 9.9), CVE-2024-39931 (CVSS score: 9.9), CVE-2024-39932 (CVSS score: 9.9), and CVE-2024-39933 (CVSS score: 7.7).

Among these four vulnerabilities, three are considered highly severe that could allow attackers to infiltrate vulnerable systems. Exploiting these vulnerabilities, attackers could steal or delete source code and even install malicious backdoors. Experts state that Gogs instances running on Debian and Ubuntu are at high risk, while those running on Windows are safe. Users of Gogs are advised to exercise caution until a patch is released.

Critical risk identified in WordPress plugins

A critical vulnerability (CVE-2024-5932, CVSS score: 10.0) has been identified in the WordPress GiveWP plugin, putting over 100,000 websites at significant risk of remote code execution (RCE) attacks[5]. The vulnerability affects all versions of the plugin prior to 3.14.2, which was released on August 7, 2024. This vulnerability, with a CVSS score of 10.0, could allow attackers to gain complete control of affected websites, potentially leading to data breaches, financial losses, and reputational damage. WordPress site owners are strongly urged update to version 3.14.2 or later immediately to mitigate this risk.

Researchers have uncovered severe vulnerabilities in other popular WordPress plugins, emphasising the importance of regular updates and the use of legitimate software. These vulnerabilities, if exploited, could have led to data breaches, website defacements, and financial losses. These findings underscore the critical need for ongoing vigilance in website maintenance, as outdated or unpatched plugins continue to be a major target for cybercriminals.

Vulnerabilities leave Microsoft scrambling for patches

Microsoft's August 2024 Patch Tuesday addresses a total of 89 flaws affecting Windows users[6]. 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, RCEs, 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.

Docker flaw puts systems at the risk of sinking

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[7]. 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, with experts recommending updating security patches and implementing security measures for enhanced protection.

Microsoft warns of critical flaw in VMware ESXi

Microsoft has issued a critical warning regarding a vulnerability (CVE-2024-37085) in VMware ESXi[8]. This flaw allows cybercriminals to bypass authentication and gain full control of ESXi hypervisors. These hypervisors manage virtual machines, which often house critical business systems. Exploiting this vulnerability, attackers can steal sensitive data, move freely across networks, and encrypt the entire hypervisor's file system, potentially crippling operations. Various threat actors, including Black Basta and Akira, have already exploited this flaw to carry out ransomware attacks.

Organisations are urged to upgrade to the patched version ESXi 8.0 U3 immediately and review their security measures to protect against this threat. This incident highlights the ongoing threat of ransomware and the importance of staying vigilant against emerging vulnerabilities.

Critical Apache HugeGraph vulnerability actively exploited

A critical security flaw (CVE-2024-27348) in Apache HugeGraph-Server is being actively exploited, risking RCE attacks[9]. It has a CVSS score of 9.8, indicating a severe risk. The flaw allows attackers to potentially take complete control of servers. This vulnerability is particularly concerning because attackers can bypass sandboxing and steal data, disrupt operations, or install malware.

Users have been directed to upgrade to version 1.3.0 with Java11 immediately and enable the Auth system, which fixes the issue. As the exploit codes are publicly available and the attacks are ongoing; hence, implementing additional security features such as authentication and access restrictions is crucial.

ALPHV ransomware leverages RDP and ScreenConnect to wreak havoc

A sophisticated ransomware attack – starting with a phishing email – has necessitated the urgent need for robust cybersecurity measures[10]. Hackers initially delivered the IcedID malware, followed by installing remote control software and lateral movement through Cobalt Strike and CSharp Streamer RAT. Over eight days, they extracted sensitive data before deploying the ALPHV ransomware.

The attackers used ScreenConnect for remote control, wmiexec for lateral movement, and rclone for data extraction. They persisted in their attack by using scheduled tasks and process injections, ultimately locking crucial data until a ransom was paid. The initial access vector was a malicious email tricking victims into downloading an obfuscated IcedID loader. This sophisticated method allowed the attackers to gain control, move laterally, and deploy ransomware, highlighting the need for businesses to implement stringent cybersecurity protocols.

APT41 uses a new loader for advanced attacks

In April 2024, researchers discovered a previously unknown loader named DodgeBox, which displayed remarkable similarities to StealthVector – a malicious program linked to the China-based APT41[11]. DodgeBox operates as a loader for the MoonWalk backdoor, which employs advanced evasion techniques and uses Google Drive for command-and-control (C2) communication. A detailed technical analysis has revealed DodgeBox's complex structure and methods, linking this threat to APT41. This sophisticated malware targets Windows systems and underscores the increasing capability of APT41 to conduct advanced cyberattacks.

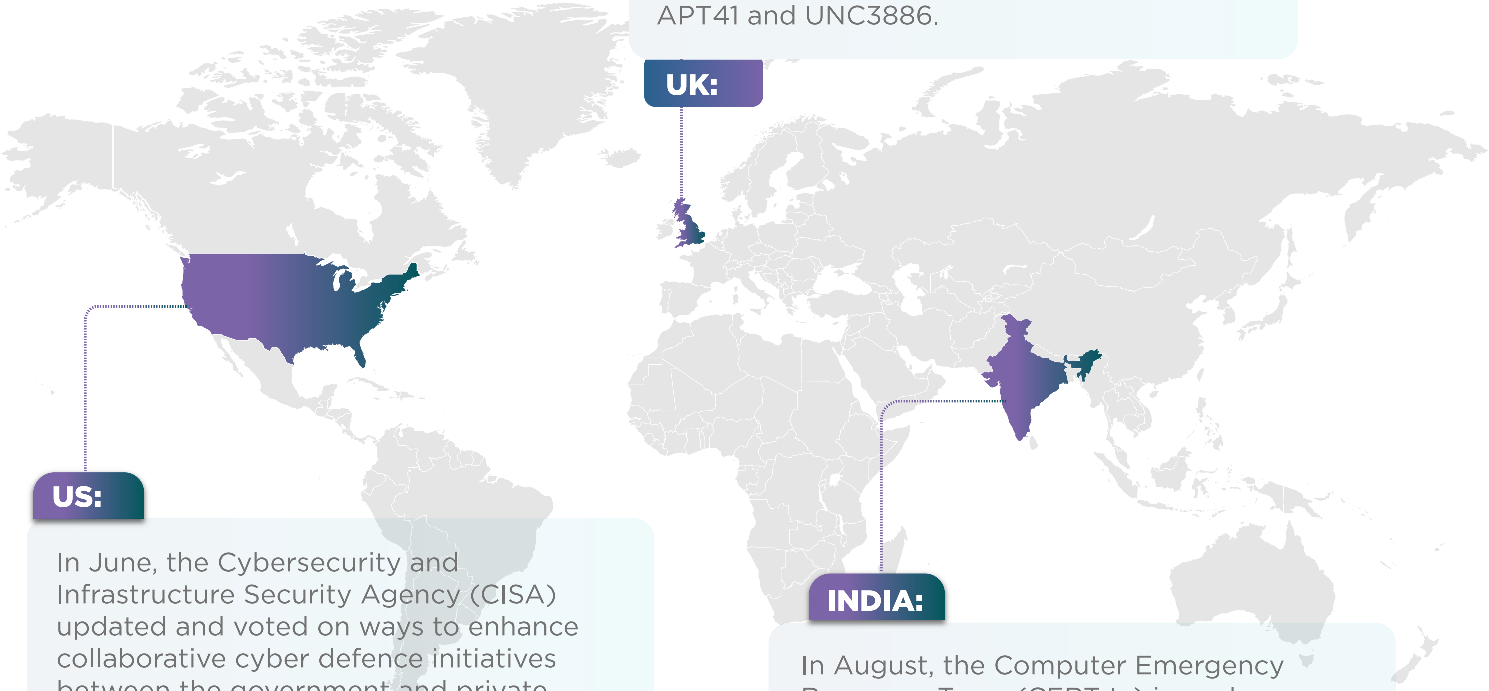
The discovery of DodgeBox highlights the evolving threat and the necessity for robust cybersecurity measures. Users are urged to remain vigilant and adopt adaptive security practices to counteract these advanced threats.

Cyberespionage group exploits zero-day vulnerabilities to attack enterprises

The Chinese cyberespionage group, UNC3886 has been exploiting zero-day vulnerabilities in Ivanti, Fortinet, Ivanti, and VMware devices and maintaining persistent access to compromised environments[12]. This evasive group employs rootkits, backdoors, and credential harvesting SSH clients to evade detection. These tools enable extended spying and data theft.

UNC3886 exploits zero-day flaws like CVE-2022-41328 (Fortinet FortiOS) and CVE-2022-22948 (VMware vCenter) to deploy malware, obtain credentials, and perform lateral movements within networks. The group's tactics include using rootkits like Reptile and Medusa on virtual machines. They also deploy backdoors such as MOPSLED and RIFLESPINE that exploit trusted services like GitHub and Google Drive for C2 operations. Organisations are advised to follow security recommendations from Fortinet and VMware to protect against these sophisticated threats.

Important Government Cybersecurity Advisories - Q2 2024



UK:

In July, The National Cyber Security Centre (NCSC) and its partners, in response to continued Chinese state-sponsored cyberespionage attacks from Q1, issued advisories to government, defence, and technology sectors[14]. These advisories included specific Indicators of Compromise (IoCs) related to the activities of groups such as APT41 and UNC3886.

US:

In June, the Cybersecurity and Infrastructure Security Agency (CISA) updated and voted on ways to enhance collaborative cyber defence initiatives between the government and private sectors[15]. This includes deploying advanced threat detection systems, regularly updating and patching software, and conducting continuous vulnerability assessments.

INDIA:

In August, the Computer Emergency Response Team (CERT-In) issued an advisory on multiple vulnerabilities that have been reported in Adobe products[13]. These gaps could be exploited by attackers to bypass security restrictions, carry out DDoS attacks on target systems, run arbitrary codes, and cause several other serious data breaches.

Malware Part Two: New Threats Emerge

The second quarter of 2024 saw several new insidious ways in which Malware proliferated across a variety of platforms. A global report highlighted the severity of this adaptability, with their research showing an average of 14.2% of all their users' computers (globally) having encountered at least one local malware threat in Q2 2024[16].

However, as the global cybersecurity landscape continues to shift and evolve, attackers continue to exploit vulnerabilities in software supply chains and leverage zero-day exploits to gain unauthorised access to systems.

Exploitation of zero-day vulnerabilities: APT groups like UNC3886 have been exploiting zero-day vulnerabilities in critical systems, such as VMware and Fortinet, allowing attackers to infiltrate and maintain long-term access to compromised networks. This underscores the critical need for continuous monitoring and rapid patch management.

Fileless malware and memory-resident threats: Fileless malware continues to challenge traditional detection methods by residing in memory rather than on disk. These threats, like those used by APT41, evade antivirus software, making them particularly dangerous.

Supply chain attacks and RCE exploits: Vulnerabilities in widely used software, such as Apache HugeGraph and Docker, have been exploited for RCEs, allowing attackers to infiltrate and control servers globally. These incidents highlight the growing risk posed by supply chain attacks and the importance of securing all layers of the technology stack.

Phishing and social engineering tactics: Malicious actors have intensified their use of phishing, as demonstrated by the ALPHV ransomware attack, where attackers leveraged sophisticated phishing techniques to gain initial access, followed by lateral movement and data extraction using remote control software.

Advanced spyware and covert surveillance: Spyware used by cyberespionage groups continues to evolve, enabling prolonged data exfiltration and covert surveillance. The deployment of backdoors and rootkits, as seen in the activity of UNC3886, poses severe threats to organisational security and confidentiality.

Rabid Ransomware – Variants Continue to Wreak Havoc

According to a research, Ransomware remains a dominant cyberthreat in 2024, with Q2 seeing increasingly sophisticated attacks targeting global organisations across various sectors. As stated previously, the education/research, military/government and healthcare sectors were the three most targeted industries in Q2 2024. The healthcare sector in particular witnessed a 53% increase in attacks compared to Q2 of the previous year[17]. Additionally, the proliferation of ransomware-as-a-service (RaaS) platforms enabled a broader range of threat actors to launch attacks. New ransomware variants continue to exploit vulnerabilities, with attackers adopting more aggressive tactics. Looking ahead, emerging threats such as cyber warfare and the potential misuse of generative AI will likely further shape the cybersecurity landscape in the coming quarters.

Surge in ransomware attacks: Ransomware attacks have escalated, particularly targeting critical infrastructure, healthcare, and government sectors. State-sponsored threat actors have leveraged ransomware for both financial gain and espionage, complicating attribution and response efforts.

Double and triple extortion tactics: Ransomware operators are increasingly using double extortion tactics, where they not only encrypt data but also threaten to leak sensitive information unless their demands are met. In some cases, such as those involving ALPHV ransomware, triple extortion is employed, adding the threat of DDoS attacks to pressure victims.

Ransomware-as-a-Service (RaaS): The democratisation of cybercrime through RaaS platforms has enabled a wider range of threat actors to carry out attacks. This has led to a significant increase in the volume and variety of ransomware incidents, with new groups like Black Basta exploiting vulnerabilities in VMware ESXi to deploy ransomware.

Collaboration for resilience: Governments and cybersecurity agencies worldwide are intensifying efforts to disrupt ransomware networks. Collaborative efforts and public-private partnerships are crucial to enhancing overall resilience against these pervasive threats. The emphasis is on adopting advanced cybersecurity frameworks and improving incident response capabilities.

Critical vulnerability exploits: The exploitation of critical vulnerabilities, such as those in Docker and WordPress plugins, has facilitated ransomware attacks, allowing adversaries to gain control over systems and deploy malicious payloads. This trend highlights the urgent need for continuous patch management and vulnerability remediation across all industries.

Lessons from Q2 – 10 Key Takeaways for Future Resilience

Increased risk of credential theft and privacy breaches: The MalAgent.AutoITBot malware captures keystrokes and reads clipboard data, making it easier for attackers to steal login credentials and sensitive information.

Prolonged operational downtime and financial loss: The sophisticated tactics of the ALPHV ransomware attack, including lateral movement and data extraction before encryption, highlight the potential for prolonged operational disruptions and substantial ransom demands.

Threats to cloud-native and containerised environments: The Docker vulnerability highlights risks for industries using containerisation for application deployment.

National security risks and public service disruption: Ransomware attacks on government entities can lead to the exposure of sensitive national information and disrupt critical public services.

Uncontrolled server compromise and data breach potential: The active exploitation of a critical flaw in Apache HugeGraph poses a significant threat of server takeover, data breaches, and operational disruptions.

Exposure to source code theft and manipulation: Unpatched vulnerabilities in Gogs expose organisations to the risk of attackers stealing or modifying source code, potentially leading to intellectual property loss or the introduction of malicious code into software projects.

Widespread exploitation and urgent need for patch management: The exploitation of multiple critical vulnerabilities in Microsoft products underlines the necessity for rapid patch deployment.

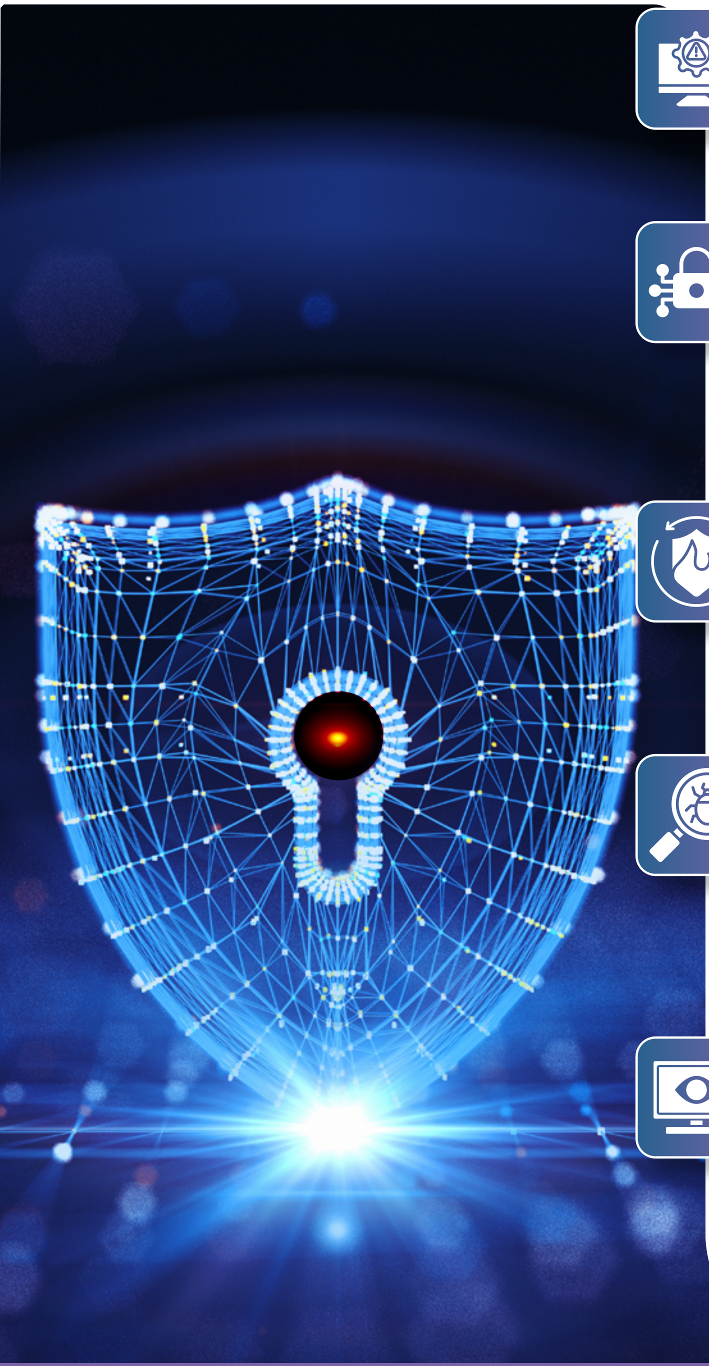
Enhanced threat to network integrity and data security: The advanced malware loader used by APT41, DodgeBox, illustrates a heightened ability to evade detection and maintain persistence within networks.

Large-scale website defacements: The critical flaw in the WordPress GiveWP plugin exposes over 100,000 websites to potential full control takeover, risking significant data breaches and operational downtime.

Compromise of virtualised environments and data loss: The VMware ESXi vulnerability, allowing full control over hypervisors, poses a severe threat to virtualised environments hosting critical business applications.

Our Top 5 Recommendations

As threats continue to evolve and exploit digital security vulnerabilities in new and innovative ways, the need for a truly holistic threat mitigation framework remains essential. Tata Communications is committed to safeguarding enterprises from the latest threats as they are discovered, while also building resilience against future risks. With all this in mind, and with the insights gained from some of Q2's biggest cybersecurity incidents, here are five key recommendations for enterprises:



Proactive protection to mitigate risks: Enterprises should establish a proactive patch management policy, prioritise critical vulnerabilities, and ensure all systems are regularly updated to close security gaps.

Prioritise endpoint and network defences to shield against the unknown: Enhance endpoint security with advanced detection and response solutions to protect against sophisticated malware and ransomware attacks, such as ALPHV ransomware and APT41's advanced malware.

Build resilience with a comprehensive backup and disaster recovery plan: Develop and regularly test a comprehensive backup and disaster recovery plan to ensure business continuity in the event of a ransomware attack or data breach.

Future-Proof Security through transformation and awareness: Regularly conduct security awareness training and systematically revamp the organisation's security framework with advanced technologies, processes, and policies to strengthen resilience against evolving threats.

Anticipate threats by leveraging threat intelligence and continuous monitoring: Enterprises should adopt a risk-hunting approach that leverages threat intelligence services to track, identify and mitigate threats before they can cause significant damage.

Sources: Tata Communications Threat Intelligence and Research

1 Kroll | 2 Check Point | 3 The Hacker News | 4 The Hacker News | 5 The Hacker News | 6 Bleeping Computer | 7 Security Online | 8 The Hacker News | 9 The Hacker News | 10 GB Hackers on Security | 11 Zscaler | 12 The Hacker News | 13 CERT-In | 14 National Cyber Security Centre | 15 Cybersecurity and Infrastructure Security Agency | 16 SecureList by Kaspersky | 17 Check Point

For more information, click here

CONTACT US