TATA COMMUNICATIONS

TATA

QUARTERLY EXECUTIVE THREAT REPORT

Q1 2024

Executive Summary

The year 2024 has already been marked by dramatic shifts in both offensive and defensive positions across the global cybersecurity landscape. In the last three months, several significant cyberattacks have highlighted how cyber criminals are widening the scope of malware and ransomware to exploit enterprise weaknesses. This quarterly report focuses on the some of the biggest incidents that have affected global businesses, along with insights on their threat vectors, major impacts of these events, and Tata Communications' recommendations for creating a holistic and agile cybersecurity framework for your organisation.

Today's Threat Landscape – Quarterly Highlights

In Q1 alone, the number of major cybersecurity breaches ***increased by 7%*** *when compared to the previous quarter*

There has been a surge in malware and ransomware attacks that have targeted critical infrastructure and financial institutions, highlighting an urgent need for stronger security measures. At the forefront of defence, AI-driven cybersecurity solutions have become more prevalent, offering advanced threat detection and response capabilities.

Meanwhile, regulatory bodies worldwide have enforced stricter data protection laws, compelling organisations to bolster their cybersecurity frameworks.Simultaneously, there has been a notable shift towards zero-trust architectures, reflecting a move to more secure network access models. Collaboration between public and private sectors has also intensified, with joint efforts aimed at combating sophisticated cyber threats and safeguarding sensitive information more effectively.

As of 2023, organisations spend ***approximately 11%*** *of their IT budgets on cybersecurity.*

Rabid Ransomware – Cybersecurity Threats Continue to Evolve

Modern malware delivery methodologies have evolved, leveraging advanced techniques to breach even robust cyber defences. Recent cybersecurity incidents reveal a surge in phishing campaigns, exploiting social engineering to trick users into downloading malicious attachments or clicking infected links.

- Ransomware attacks have escalated, targeting critical sectors like infrastructure, healthcare, and finance with alarming frequency. Despite this, in India specifically, only 20% of surveyed companies have a formal ransomware plan in place, with 10% resorting to paying the ransom demands.
- Instances of double extortion tactics are on the rise, where attackers encrypt data and threaten public release unless ransom demands are met
- RaaS has democratised cybercrime, making it more accessible for malicious actors to execute attacks
- Collaborative efforts between governments and cybersecurity agencies are crucial to disrupting ransomware networks and enhancing overall resilience against these pervasive threats through new technological advancements.

Over ***22% of surveyed enterprises*** *around the world are planning to integrate Generative AI into their security products and services within the year, while* ***33% are planning to experiment*** *with integrating the technology.*

An Evolving Cybercrime Ecosystem – Top Ten Threats of Q1 2024

Black Basta ransomware puts over 500 global organisations at risk

The FBI, CISA, HHS, and MS-ISAC reported that Black Basta ransomware affiliates breached over 500 organisations globally from April 2022 to May 2024. This ransomware-as-a-service (RaaS) variant has targeted 12 critical sectors, impacting entities across North America, Europe, and Australia.

The group is linked to the defunct Conti Group, laundering funds through the Russian crypto exchange, Garantex. US agencies recommend implementing security measures such as prompt updates, phishing-resistant multi-factor authentication, securing remote access, and regular backups to mitigate ransomware threats.

DinodasRAT Linux variant wreaks havoc across multiple countries

Researchers identified a Linux variant of the multi-platform backdoor DinodasRAT (also known as XDealer), used in cyberattacks targeting China, Taiwan, Turkey, and Uzbekistan. Written in C++, DinodasRAT supports extensive spying and data theft capabilities.

Initially discovered by ESET in October 2023, experts however believe it has been active since 2022. Having linked the malware to the China-linked APT group, Earth Krahang, this further highlights its use against government organisations.

Operation Diplomatic Spector sets its sights on government data

Operation Diplomatic Specter, a Chinese cyberespionage campaign, has targeted government entities in the Middle East, Africa, and Asia since late 2022. ESET researchers identified two novel backdoors, TunnelSpecter and SweetSpecter, used by the attackers. The campaign, attributed to a Chinese state-aligned APT group, focuses on political entities, including diplomatic missions, ministries, and high-ranking officials.

The threat actors infiltrate mail servers, exfiltrate sensitive information, and monitor geopolitical developments. They employ spear phishing and exploit vulnerabilities like ProxyLogon and ProxyShell. The persistence and adaptability of the attackers highlight the significant threat posed to international governmental operations.

LightSpy makes a comeback to strike fear in South Asia

Researchers uncovered a renewed cyberespionage campaign targeting South Asia with the sophisticated Apple iOS spyware, LightSpy. It has been revealed that the new version – dubbed as “F_Warehouse” – supports a modular framework with extensive spying capabilities. LightSpy can steal files from applications like Telegram, QQ, and WeChat, record audio, harvest browser history, compromise Wi-Fi

connections, and capture images. It grants attackers full control over infected devices, including access to Keychain data and the ability to execute shell commands.

New Ivanti RCE flaw exposes 16,500 VPN gateways to attack

Earlier in April, cybersecurity experts sounded the alarm over a critical remote code execution (RCE) flaw, CVE-2024-21894, affecting approximately 16,500 Ivanti Connect Secure and Poly Secure gateways. This heap overflow vulnerability in the IPSec component allows unauthenticated attackers to send specially crafted requests, potentially causing denial-of-service (DoS) attacks or executing arbitrary code. Ivanti has released security updates to address this critical flaw. Despite these patches, researchers have reported that a significant number of systems – particularly in the US, the UK, and Japan – remain unpatched and vulnerable. Fortunately, no active exploitation of this flaw has been reported yet.

The spyware spreads via compromised news websites, using a first-stage implant to deliver the core LightSpy implant and plugins. Further evidence suggests the creators are native Chinese speakers, raising concerns about state-sponsored activity.

New Lunar malware attacks leave diplomatic entities frustrated

ESET researchers discovered two new backdoors, LunarWeb and LunarMail, used by the Russia-aligned cyberespionage group Turla to compromise a European Ministry of Foreign Affairs (MFA) and its diplomatic missions. Active since at least 2020, LunarWeb and LunarMail facilitate extensive information collection and stealthy communication.

Turla, notorious for high-profile attacks since the late 1990s, leverages spear phishing and misconfigured software like Zabbix for initial access. LunarWeb gathers detailed system information and uses HTTP(S) with encrypted content for C2, impersonating legitimate traffic to evade detection. This attack underscores the persistent threat posed by sophisticated nation-state actors targeting critical diplomatic entities

Cybercriminals exploit Microsoft Graph API vulnerabilities

Cybersecurity analysts reported an increase in threat actors exploiting the Microsoft Graph API to communicate with command-and-control (C2) infrastructure hosted on Microsoft cloud services. This tactic – first observed in January 2022 – is employed by nation-state-aligned groups like APT28, APT29, and OilRig. By leveraging legitimate APIs, attackers evade detection, as seen with the deployment of previously undocumented malware like BirdyClient. In one instance, BirdyClient was used against a Ukrainian organisation, utilising the Graph API to interface with OneDrive for C2 operations.

Attackers used a malicious DLL posing as a legitimate component to maintain stealthy communications: a strategic shift that exploits the commonplace nature and cost-effectiveness of cloud services, highlighting the evolving complexity of modern cyberthreats.

Brokewell Trojan software compromises Android devices in Germany

A new trojan named Brokewell has been discovered targeting mobile banking apps on Android smartphones. Brokewell combines data-stealing and remote-control capabilities, enabling device takeover, data exfiltration, and extensive monitoring. Notably, it bypasses restrictions in Android versions 13, 14, and 15 and uses phishing tactics, such as fake browser updates, to trick users into installing the malware.

Once installed, the malware exploits the accessibility service to gain additional permissions and execute various malicious activities. These include displaying overlays to steal credentials, intercepting cookies, recording audio, and manipulating the device remotely. This can lead to financial fraud, data theft, and significant financial and reputational damage for victims.

Proof-of-concept Fortinet exploit is a wake-up call for enterprises

Security researchers unveiled a proof-of-concept (PoC) exploit for a critical vulnerability in Fortinet's SIEM solution, tracked as CVE-2024-23108. This command injection flaw allows remote unauthenticated attackers to execute commands as root via crafted API requests. Impacting FortiSIEM versions 6.4.0 and higher, this vulnerability was patched in February.

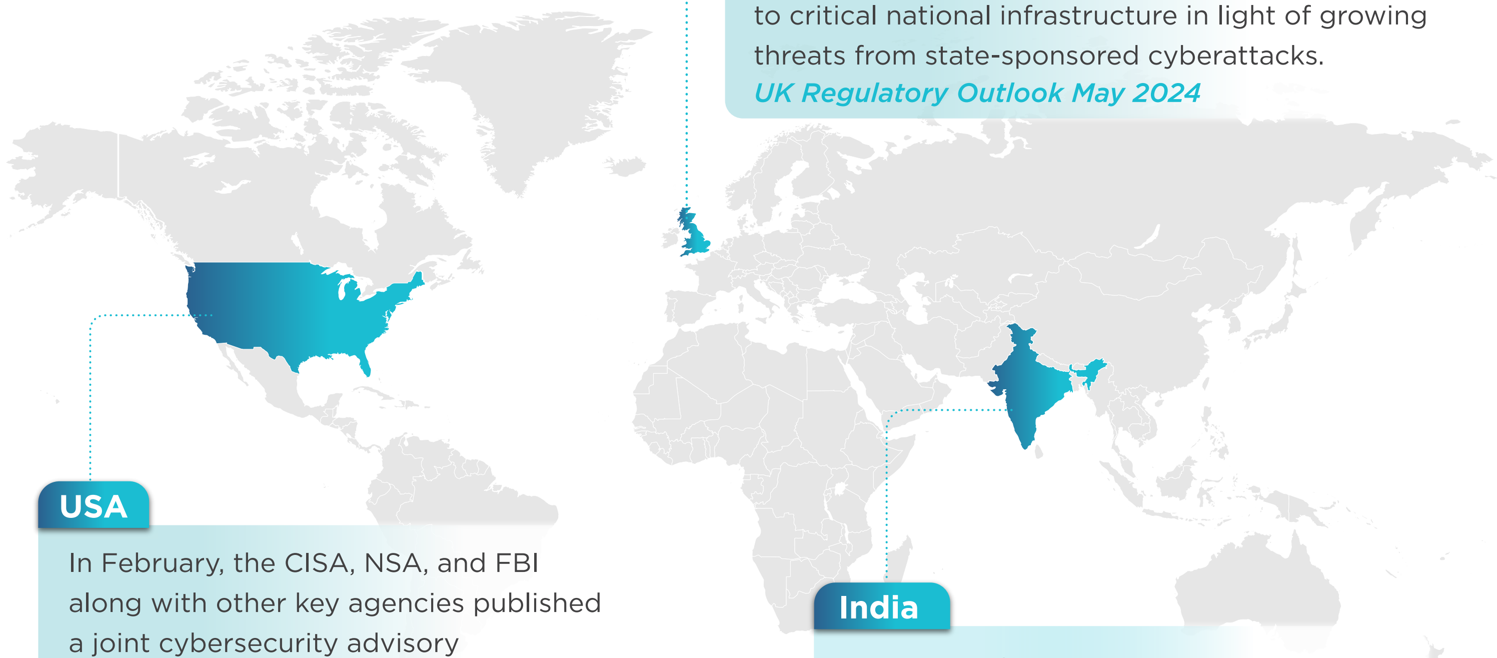
Despite initial denials from Fortinet, the company later confirmed the severity of CVE-2024-23108, highlighting its similarity to an earlier flaw, CVE-2023-34992. The exploitation underscores the ongoing risk of Fortinet vulnerabilities being leveraged in ransomware and cyberespionage attacks.

Latest ValleyRAT variant diversifies to skitter past cybersecurity blockades

Researchers have uncovered a sophisticated campaign involving the latest variant of ValleyRAT, a notorious remote access trojan (RAT) first identified in early 2023. This iteration introduces enhanced capabilities, including screenshot capture, process filtering, forced shutdowns, and the ability to clear Windows event logs.

Deployed through phishing emails and malicious downloads, the campaign employs multi-stage deception tactics. Initial stages utilise an HTTP File Server (HFS) for downloading subsequent attack components. The malware employs advanced evasion techniques like anti-virus checks, DLL sideloading, and process injection. Modifications in this ValleyRAT version enhance its device fingerprinting, bot ID generation, and command functionalities, underscoring ongoing threats from China-based threat actors.

Important Government Cybersecurity Advisories - Q1 2024



UK

In May, the NCSC updated its Cyber Assessment Framework to reflect the heightened cyberthreats to critical national infrastructure in light of growing threats from state-sponsored cyberattacks.

UK Regulatory Outlook May 2024

USA

In February, the CISA, NSA, and FBI along with other key agencies published a joint cybersecurity advisory highlighting malicious activities by Chinese state-sponsored cybercriminal known as Volt Typhoon, which could potentially lead to the compromising of critical state infrastructure.

Cybersecurity and Infrastructure Security Agency

India

In March of this year, the government's CERT-In warned citizens of a new security vulnerability in Google Chrome that could put hundreds of users at risk of remote attacks.

Google Chrome Users Alert

The Malware Mafia – An Arsenal of Weaponised Delivery Methods

Modern malware delivery methodologies have evolved, leveraging advanced techniques to breach even robust cyber defences. Recent cybersecurity incidents reveal a surge in phishing campaigns, exploiting social engineering to trick users into downloading malicious attachments or clicking infected links.

Drive-by downloads, often embedded in compromised websites, silently install malware. Supply chain attacks have increased, with adversaries infiltrating trusted vendors to distribute malware.

File-less malware, residing in memory, evades traditional detection methods, while malicious macros in seemingly legitimate documents continue to be a prevalent threat

Sophisticated ransomware variants employ double extortion, encrypting data and threatening to leak sensitive information, amplifying the impact on victims

Spear phishing for targeted attacks, exploiting zero-day vulnerabilities, and using malware to infiltrate systems is on the rise

APTs deploy sophisticated spyware, enabling prolonged data exfiltration and covert surveillance, significantly impacting organisations' security and confidentiality

Learning from the Past – 10 Key Takeaways from Q1 for Future Resilience

Impact on critical infrastructural security:

DinodasRAT's advanced spying and data theft capabilities, targeting government organisations, highlight heightened risks to critical infrastructural security worldwide

Threat to privacy and governance:

The LightSpy iOS spyware's ability to infiltrate South Asian regions via compromised websites raises concerns about privacy breaches and state-sponsored espionage impacting governance

Cloud security challenge:

Exploitation of Microsoft Graph API by APT groups highlights the challenge in securing cloud environments, posing risks to data integrity and confidentiality globally

Disruptions to diplomatic relations:

Turla's use of LunarWeb and LunarMail to target European diplomatic entities disrupts international relations, showcasing the geopolitical impact of cyberespionage

Enterprise security vulnerabilities:

Fortinet's SIEM vulnerability (CVE-2024-23108) underscores ongoing risks in enterprise security, potentially facilitating unauthorised access and data breaches

Vulnerability in global networking:

The Ivanti Connect Secure and Poly Secure gateway vulnerability poses a significant risk to global networking, potentially allowing attackers to execute arbitrary code and disrupt operations in unpatched systems

Financial sector vulnerabilities:

Brokewell's targeting of mobile banking apps underscores vulnerabilities in the financial sector, exposing users to financial fraud and data theft

Impact on healthcare infrastructure:

Black Basta ransomware's widespread attacks on healthcare infrastructure globally, including critical sectors, pose severe risks to patient data security and operational continuity

Governmental security breach:

Operation Diplomatic Specter's targeting of government entities in Asia, Africa, and the Middle East threatens national security through information theft and geopolitical monitoring

Sophisticated cyberthreats:

ValleyRAT's advanced functionalities and multi-stage delivery tactics highlight evolving cyberthreats, particularly from China-based threat actors, impacting global cybersecurity readiness

Our Top 5 Recommendations

In an ever-changing and dynamic digital security ecosystem, Tata Communications understands the importance of a holistic threat mitigation strategy that allows enterprises to safeguard their businesses from the latest and greatest threats that cybercriminals can deploy. Based on the insights gained from some of today's top cybersecurity threats, here are 5 key recommendations for enterprises to consider:

Ensure Security Hygiene:

Regularly update patches, configurations, and maintain baseline security settings.

Assess Attack Surface and Paths:

Analyze potential attack vectors and paths to stay prepared and prioritize risk mitigation strategies.

Secure Identities and Privileges:

Effectively manage identities, privileges, and entitlements based on principle of least privilege (POLP).

Protect Industrial Control Systems:

Enhance security for industrial control systems to support Industry 4.0 initiatives.

Simulate Attack Scenarios:

Test and evaluate the effectiveness of people, processes, and security technologies through attack simulations.

Sources and Credits -

Tata Communications Threat Intelligence and research, OEM Partner sources, BleepingComputer, IANS Research, CISA, SEST Research, Osborne Clark UK Regulatory Outlook May 2024, 2024 Thales Data Threat Report.

For more information, visit us at www.tatacommunications.com

CONTACT US

© 2024 Tata Communications Ltd. All rights reserved. TATA COMMUNICATIONS and TATA are trademarks or registered trademarks of Tata Sons Private Limited in India and certain countries.