CYBER THREAT MONITOR REPORT

Q2_2024-25

K7 SECURITY

LEVERAGING THREAT INTELLIGENCE INDICATORS TO PROACTIVELY FIGHT CYBER THREATS

KEYWORDS

Ransomware; Security News

THE MAYHEM IN THE DIGITAL WORLD

The relentless emergence of countless malware families, particularly ransomware, continues to pose a significant cybersecurity threat. Ransomware's prevalence and impact have made it a focal point in the threat landscape. Among these ransomware families, Phobos has maintained its momentum, with new strains like the one affecting our clients demonstrating its adaptability and persistence. The discovery of the Purple Fox rootkit, which was also deployed alongside the Phobos ransomware, further underscores the sophisticated tactics employed by cybercriminals to ensure stealthy and long-term access to compromised systems.

In tandem with the grave concern of the onslaught, large and small software providers are putting immense effort into keeping their products unharmed by patching all the existing vulnerabilities. Microsoft is probably the most prominent among the lot. Patching a plethora of vulnerabilities, including zero-days, they are active in the race to keep their products safe. Ironically, many clients still ignore the dire importance of patching the old vulnerabilities despite the repeated requests, taking other factors into account, like time and resources required, among others.

Last quarter has also witnessed increased detection on Android platforms as well. This is mainly due to increased mobile penetration and the random misuse of app platforms, with least cyber awareness.

With enterprises having to bear the brunt of attacks and with different tailor-made Tactics, Techniques & Procedures (TTPs), and MITRE ATT&CK techniques being used, the cyber security industry must keep pace with the ever-growing threat industry to stay put.

We at K7 Labs offer significant protection from emerging and latest threats by closely examining and identifying such incidents and providing security at multiple layers.

Kindly read and share the report with your colleagues. Have a safe digital experience!

Enjoy reading!

INFECTION RATE (IR)

Irrespective of its type, a security breach is a thing to worry about in every aspect of our digital lives. And that's precisely what our infection rate indices indicate.

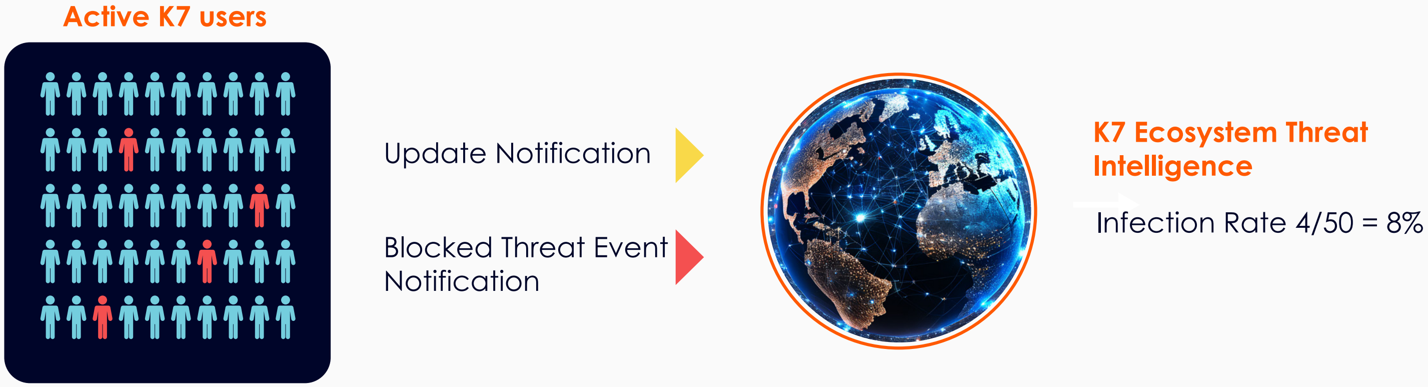
Those new to our quarterly report need to understand an important concept called "Infection Rate" (IR), which is used as the base for benchmarking cybersecurity risk for enterprises and netizens.

We use this IR factor to identify enterprises and netizens' exposure to cyber threats. IR is determined as the proportion of active K7 corporate or consumer users who encountered at least one cyber threat event which was blocked and reported to our K7 Ecosystem Threat Intelligence infrastructure (K7ETI). The higher the IR, the greater the risk.

Active users indicate users who have activated and updated their products.

The concept of Infection Rate is better explained by the below picturization.

Infection Rate (IR) of an area

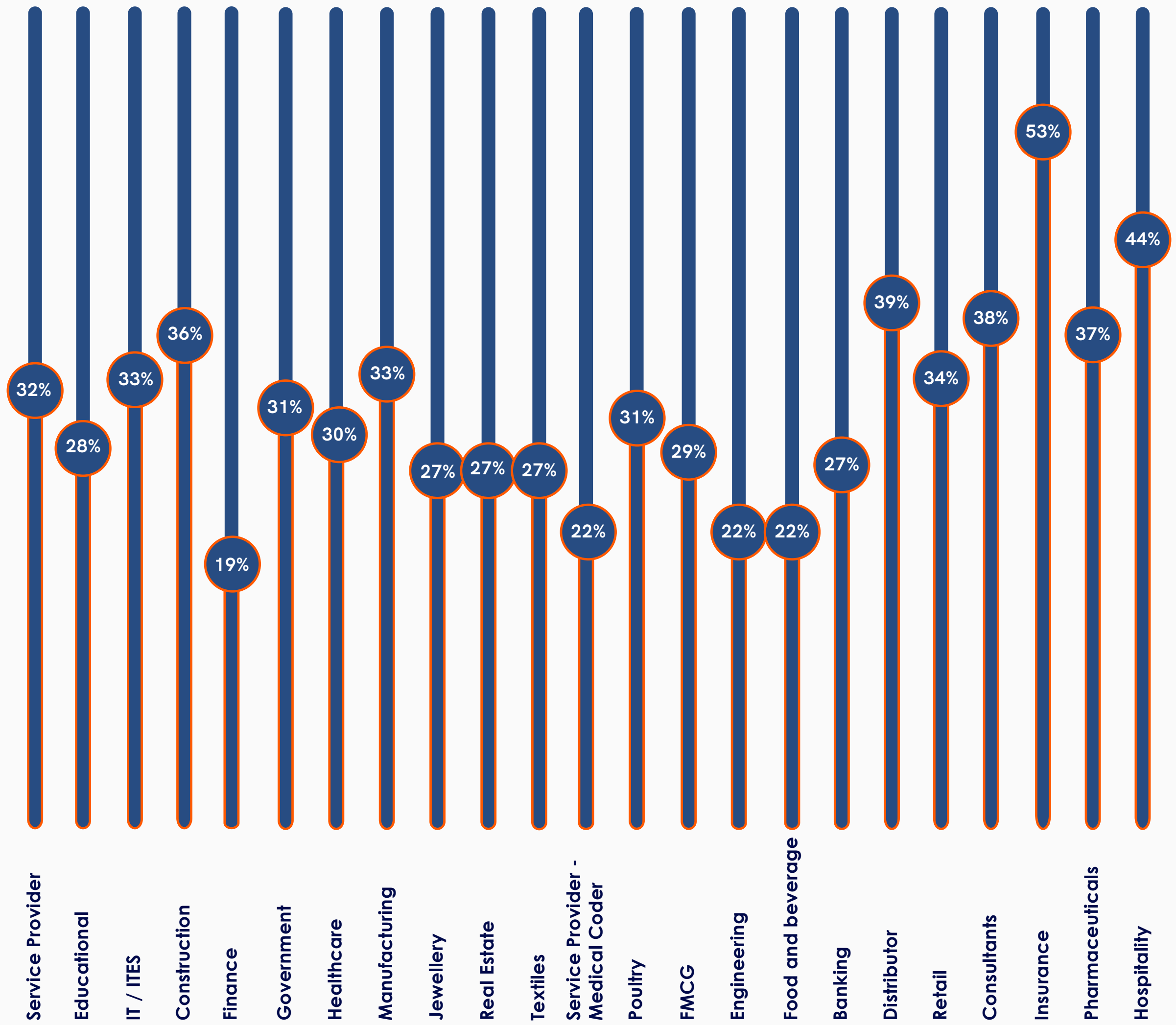

Active K7 users
Update Notification
Blocked Threat Event Notification
K7 Ecosystem Threat Intelligence
Infection Rate 4/50 = 8%

The Global IR for Q2_2024-25 was 44%

A GRANULAR VIEW OF THE INDUSTRY THREAT LANDSCAPE

The industry threat landscape chart offers a compelling comparison of how cyberattacks and their vulnerability levels target different sectors. By visually presenting the number of incidents faced by each industry, the chart provides crucial insights into risk exposure and preparedness. This data is vital for comprehending the wider economic impact of cyber threats on global markets, empowering organizations to anticipate trends and bolster their defenses.

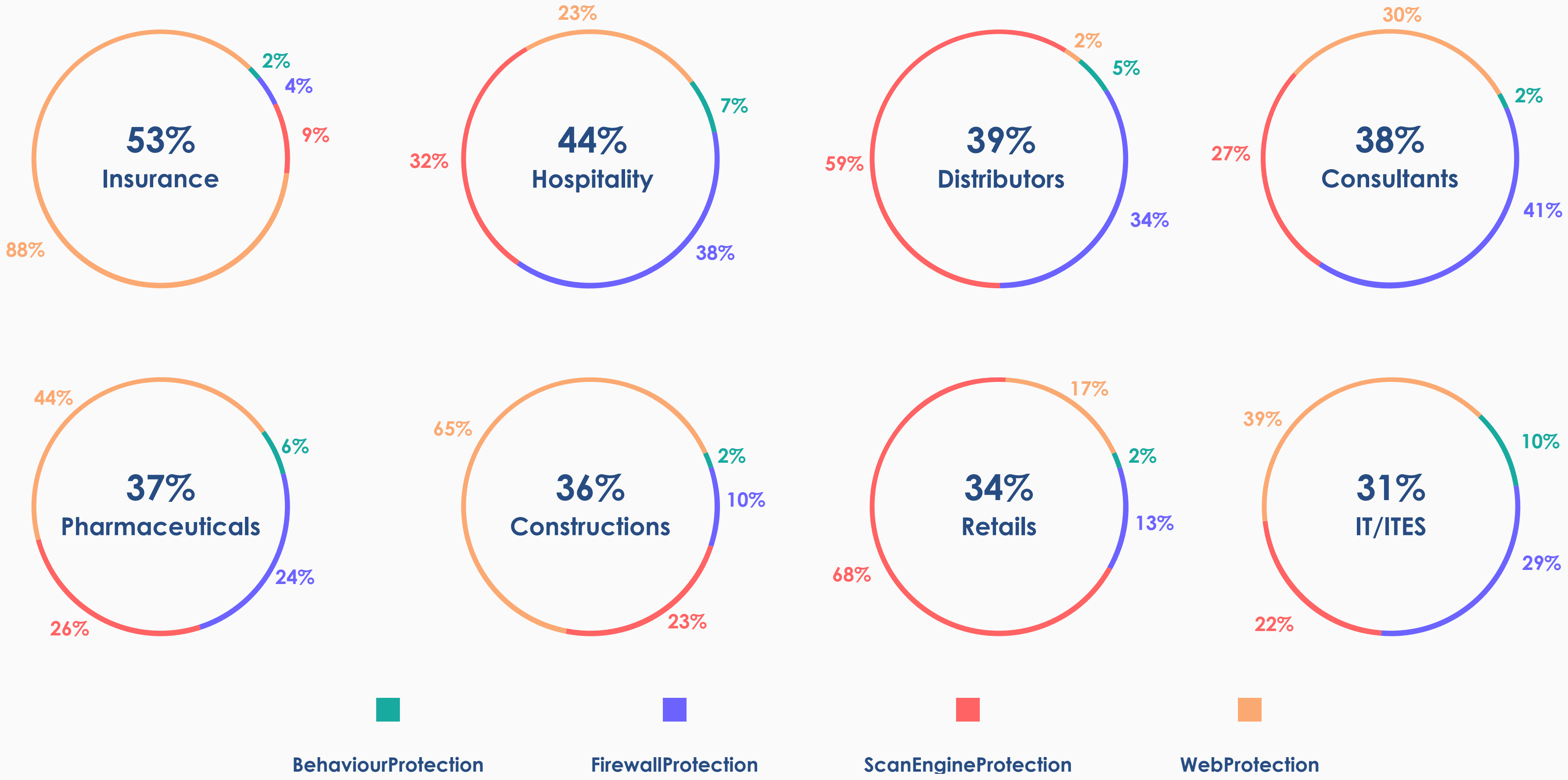
Top Industry Verticals Vulnerable to Cyber Threats



Back To Contents

THE LAYERED SPLIT

This comparison chart highlights the top eight industry verticals that faced the highest number of cyberattacks detected and prevented by K7's various cybersecurity solutions. It provides a clear view of which sectors are most frequently targeted, offering insights into threat patterns and protection effectiveness.



Dissecting the detailed data of the detection slices in the top 8 affected industries in this quarter, we can figure out the following conclusion:

HIGH WEB PROTECTION DETECTION (88%) IN THE INSURANCE SECTOR:

This indicates that most infections in the insurance sector originated from web-based threats, such as malicious websites, phishing attacks, or compromised online portals.

Role of Vendors

The insurance sector relies on numerous third-party vendors for operations, including claims management, customer support, and payment processing. If any of these vendors have vulnerabilities or poorly secured systems, they can act as entry points for web-based threats, indirectly compromising the insurance companies.

Prevalent Threats:

- Phishing attacks: Targeting insurance companies via malicious links or fraudulent websites, often aimed at stealing sensitive customer information.
- Drive-by downloads: Infections that occur when users unknowingly download malware by visiting compromised vendor or partner websites.
- Ransomware: Distributed through malicious web links or ads, locking critical insurance data.
- Supply chain attacks: Threat actors exploit weak vendor networks to gain access to insurance systems, spreading malware from one compromised partner to another.

The high rate of web protection alerts suggests that the sector is particularly vulnerable to web-based infiltration, often through its extended network of vendors.

BALANCED DETECTION RATES IN HOSPITALITY SECTOR:

The detection rates across Firewall Protection (38%), ScanEngine Protection (32%), and Web Protection (23%) suggest that threats targeting the hospitality industry are diverse and widespread across multiple vectors, with no single protection layer being disproportionately activated.

- Firewall Protection (38%): Indicates that a significant portion of threats attempted to breach network perimeters, possibly through unauthorized access attempts or DDoS attacks aimed at disrupting operations.

- ScanEngine Protection (32%): Shows active detection of malware and vulnerabilities within internal systems, highlighting concerns like outdated software or malicious files within hotel networks.

- Web Protection (23%): Reflects web-based threats such as phishing and compromised websites, potentially targeting guest booking systems or hospitality-related online services.

MINUSCULE SECURITY BUDGETS:

These sectors—**distributors, consultants, construction,** and retail—often allocate smaller portions of their budgets to cybersecurity, making them more vulnerable to infections due to underinvestment in robust protection solutions.

Outdated Systems and not updated Software: Many companies in these industries may be operating with legacy systems and software that are not regularly updated or patched, exposing them to known vulnerabilities that threat actors can exploit.

Increased Vulnerability to Cyber Threats: The combination of minimal security spending and outdated infrastructure makes these sectors prime targets for attacks, as they lack the necessary resources to defend against evolving threats like malware, ransomware, and phishing campaigns.

Back To Contents

HIGH-VALUE DATA AND CRITICAL INFRASTRUCTURE:

The IT/ITES sector manages vast amounts of sensitive data, including financial, personal, and intellectual property, making it an attractive target for threat actors seeking high-value assets.

- Widespread Network and Cloud Usage: IT/ITES companies often operate complex, interconnected networks and rely heavily on cloud services, which increases the attack surface and provides multiple entry points for cybercriminals..

- Frequent System and Software Interactions: Due to their role in managing and supporting various technologies, IT/ITES platforms frequently interact with external systems, exposing them to a broader range of vulnerabilities and potential attacks.

- Ransomware and Business Disruption: Threat actors know that a successful attack on IT/ITES companies can severely disrupt operations, forcing them to pay ransoms or face costly downtime, incentivizing a higher frequency of attacks.

ENTERPRISES CAN REDUCE THEIR VULNERABILITY TO CYBERATTACKS BY FOCUSING ON THREE KEY AREAS:

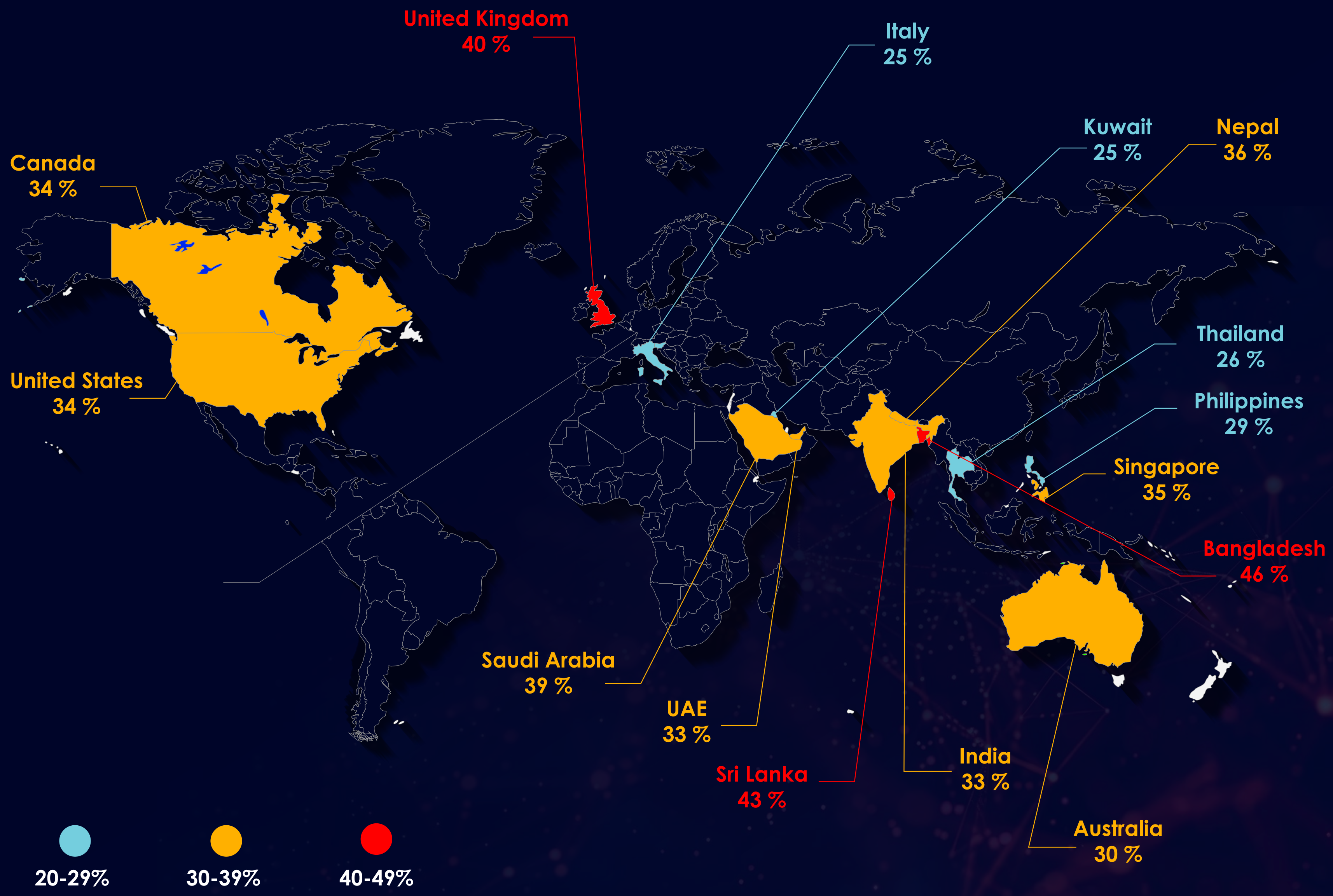
- Secure External Entry Points: Secure all external-facing systems to protect mobile networks, IoT devices, and cloud storage and prevent unauthorized access and potential data breaches.

- Enhance Email Security: Implement email scanning for malicious links and attachments, and train staff to recognize phishing attempts, as phishing remains a top method for attackers to infiltrate networks.

- Update and Secure Systems: Regularly update antivirus software, patch operating systems, and review firewall configurations to address vulnerabilities and prevent exploitation by threat actors.

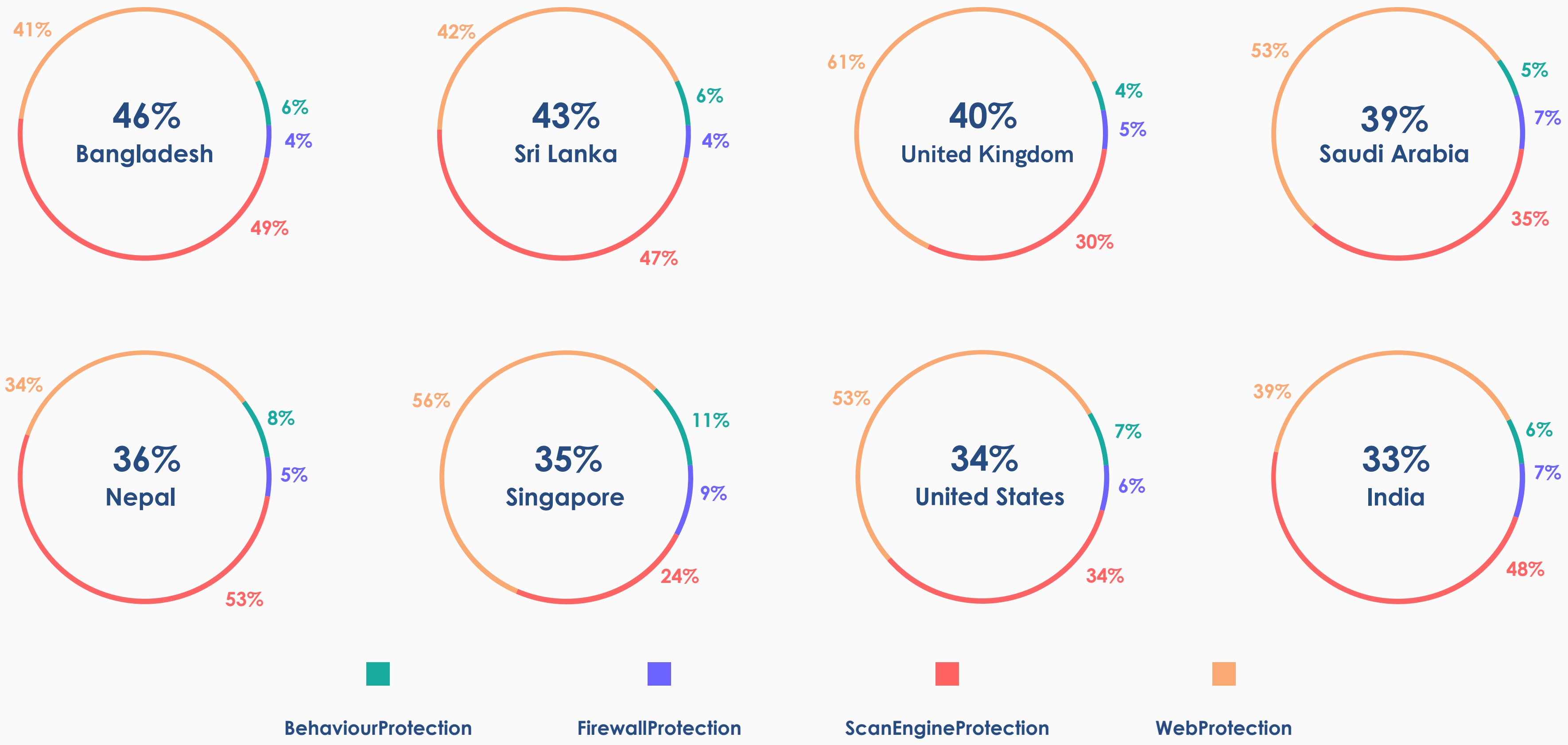
WORLDWIDE CYBER THREAT LANDSCAPE

Countries facing more cyberattacks are often those with advanced digital infrastructure, high-value economic assets, and strategic geopolitical influence, making them attractive targets for both financial gain and espionage. Threat actors also focus on nations with weaker cybersecurity defenses or political instability, exploiting vulnerabilities in critical sectors. A higher Incident Rate (IR) can signal escalating geopolitical tensions, as cyberattacks increasingly serve as tools for political leverage, economic disruption, and intelligence gathering.



THE QUARTERLY TRENDS AND STATISTICS

Top Susceptible Countries to Cyberthreats



The Web Protection layer of an AntiVirus engine shields users from internet threats like malicious websites and phishing attacks. The top eight countries with the highest web protection detection rates highlight the increasing risk posed by cyber threats, emphasizing the need for advanced web protection measures. Industries reliant on digital services face challenges such as data breaches and loss of consumer trust. Increased cybersecurity investment and global cooperation are imperative to mitigate these risks. Advanced web protection measures, such as real-time threat intelligence and behavior-based detection, are crucial to stay ahead of these threats and protect our digital world.

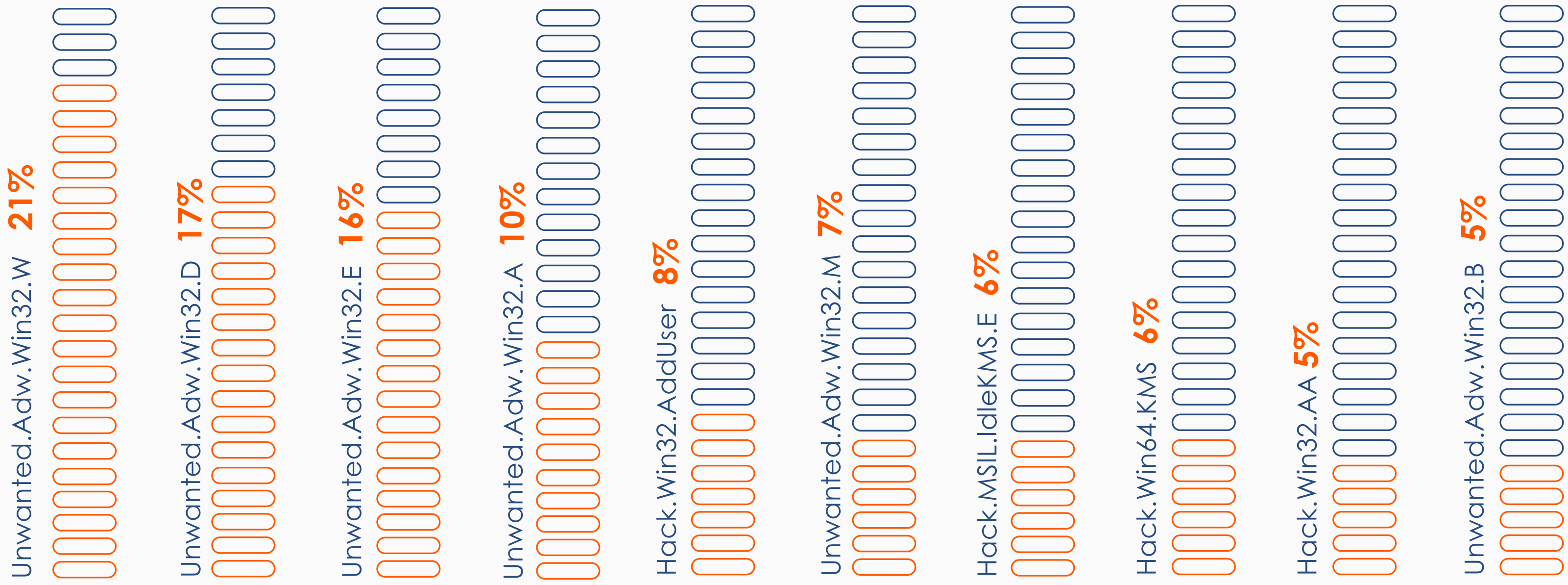
WINDOWS THREAT LANDSCAPE: EVOLVING RISKS

Windows, as the most widely used operating system across enterprises and individuals, presents a large and attractive target for cybercriminals. Its extensive user base and ubiquitous presence make it a prime platform for financially motivated attacks, with threat actors often exploiting unpatched vulnerabilities to infiltrate networks. The consequences of these attacks—ranging from data breaches to significant financial and reputational losses—pressure organizations to comply with demands, underscoring the critical need for proactive security measures to safeguard Windows environments.

Top Malware Targeting Windows Systems

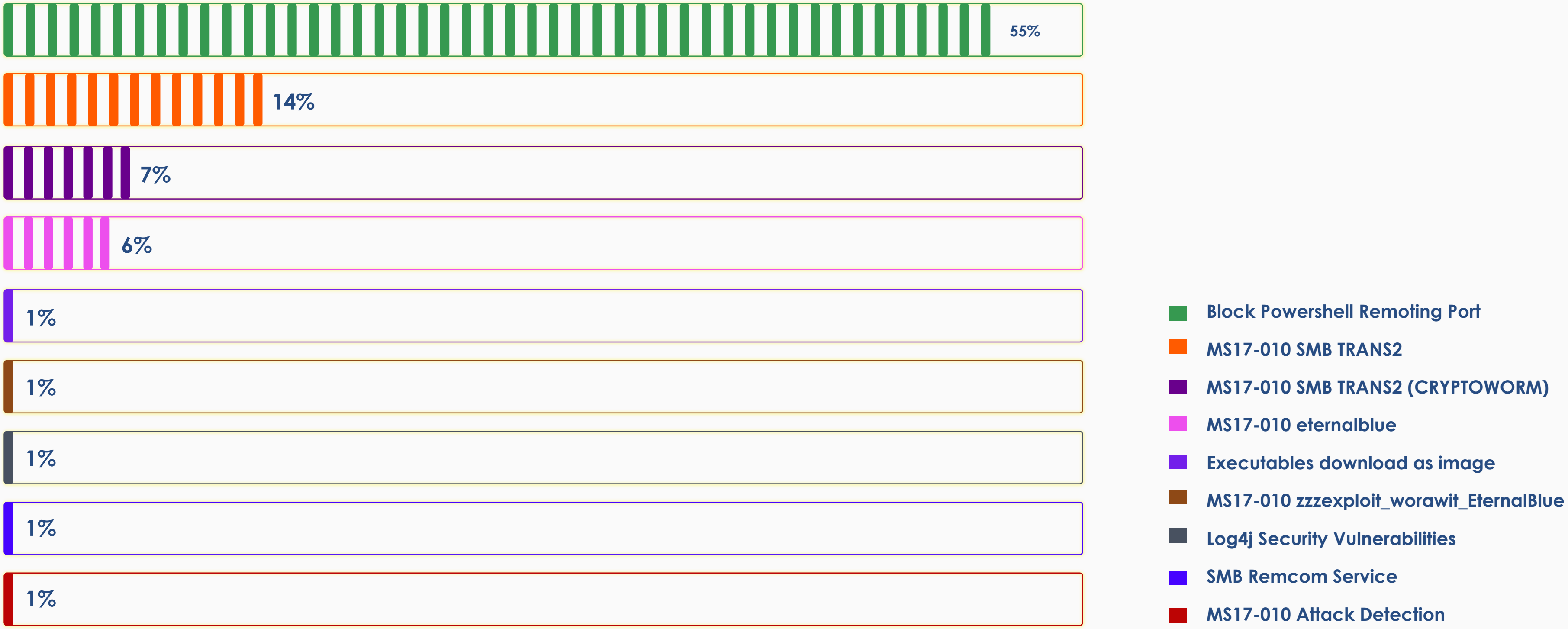
This chart presents crucial insights into the most prevalent malware affecting the Windows platform in the past quarter. It highlights emerging threats and patterns essential for informing strategic cybersecurity decisions and offers a clear view of evolving attack vectors and their potential impact on enterprise security and global digital infrastructure, making it invaluable for CXOs, IT professionals, enthusiasts, journalists, and readers contributing to the global digital landscape.

SPLIT OF WINDOWS TOP 10 DETECTIONS



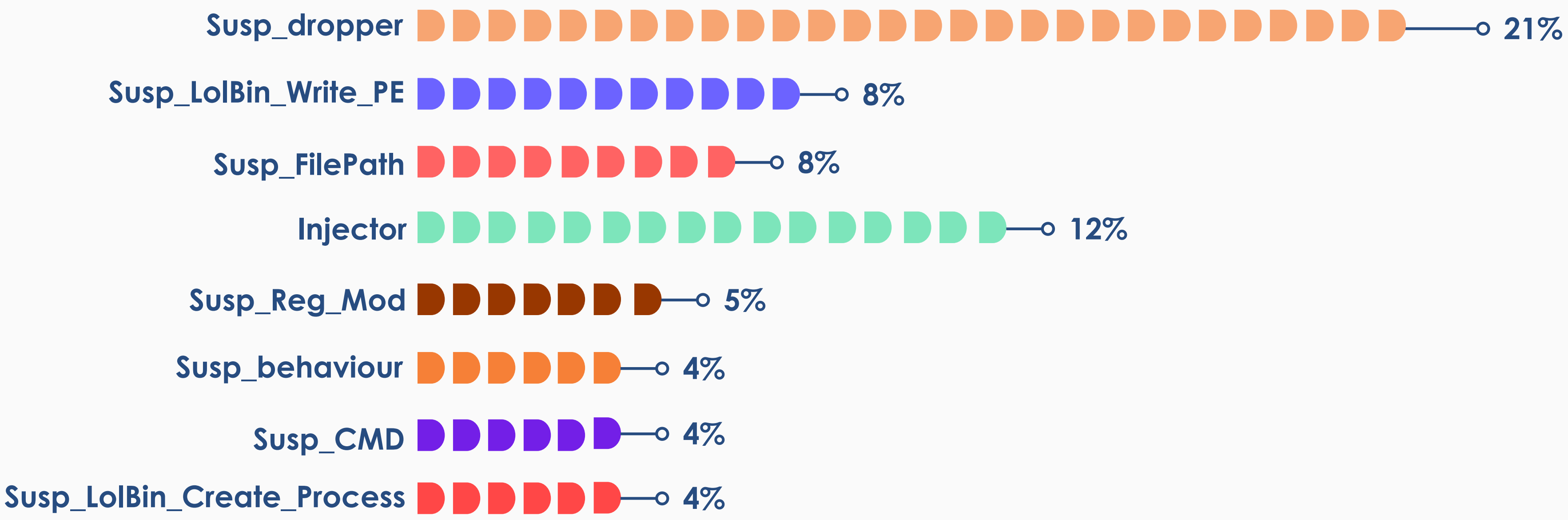
Unpatched Vulnerabilities: The Achilles' Heel of Windows Systems

Widespread neglect of system updates creates a fertile ground for threat actors to exploit unpatched vulnerabilities, allowing them to spread malware and launch attacks with greater ease. These overlooked security gaps serve as entry points, enabling cybercriminals to infiltrate networks, steal data, and disrupt operations, underscoring the critical need for regular updates and proactive vulnerability management.



Heuristic Host Intrusion Prevention System (HIPS)

Heuristic behavioural detections offers a way of detecting threats for which we might have not added a signature as yet. This detection layer is highly effective ideal for both defending against new threats (0-days) as well as being very effective against new variants of existing malware families.



Let’s delve into the insights to see what our heuristic behavioural technology has detected in the last quarter.

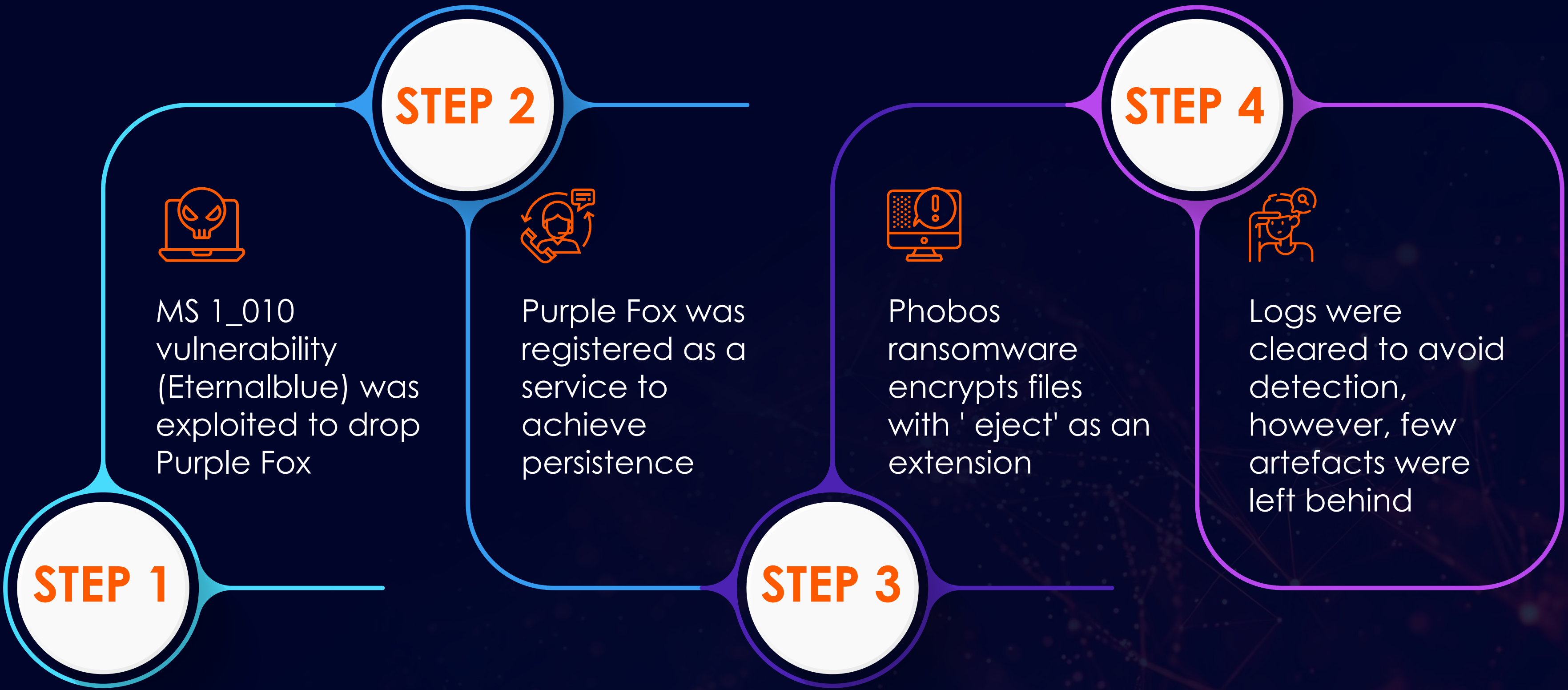
In the last quarter, Injectors and Droppers were the most prevalent. Injectors are a type of malware that use legitimate file names or locations to hide behind trusted names so as to evade detection. Injectors, as the name indicates, inject code into processes, typically legitimate and trusted services. This is also usually done to circumvent AV detections, or gain privilege elevation, or both. Droppers are used by threat actors in multi-stage attacks where additional malicious payloads are downloaded or dropped.

ENTERPRISE INSECURITY

Ransomware threats in the digital world have become common. With sensitive data and productivity at stake, enterprises are in a fix with the attackers' demands.

Phobos ransomware is one of its kind, wreaking havoc across the world. Let us now look at one of its kill-chains.

Case Study: Phobos, the Stealthy Infiltrator



STEP 1

MS 1_010 vulnerability (Eternalblue) was exploited to drop Purple Fox

STEP 2

Purple Fox was registered as a service to achieve persistence

STEP 3

Phobos ransomware encrypts files with ' eject' as an extension

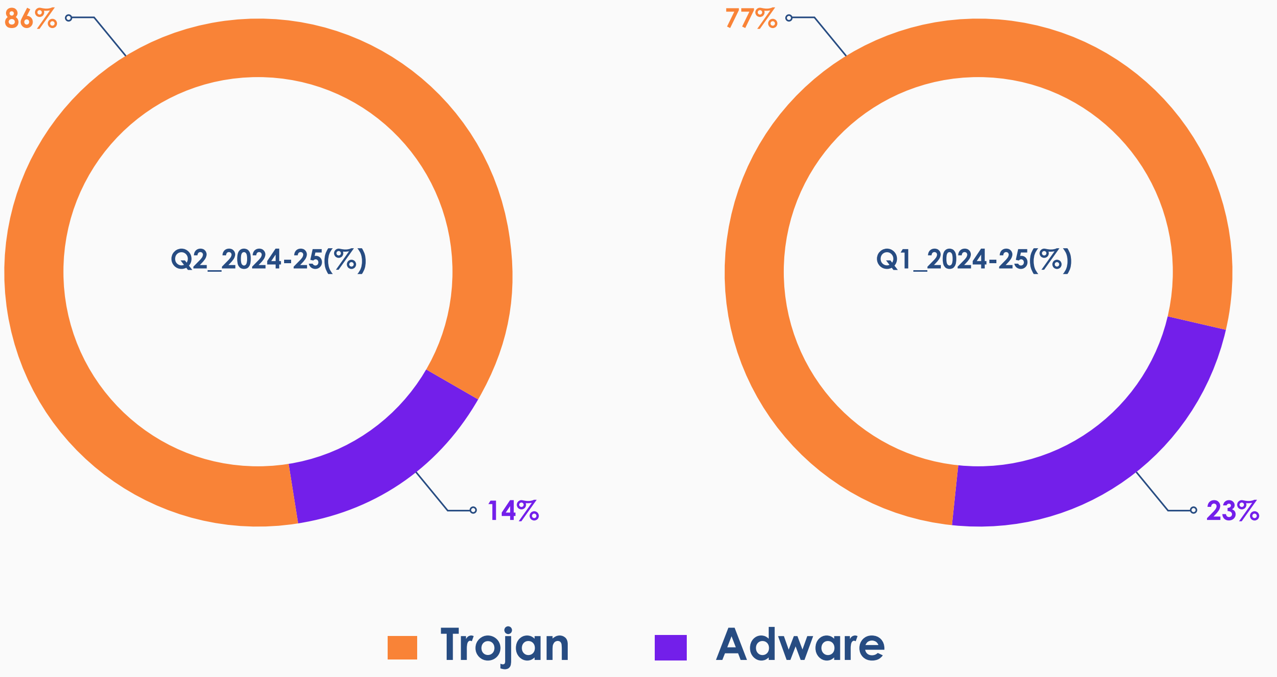
STEP 4

Logs were cleared to avoid detection, however, few artefacts were left behind

THE MOBILE DEVICE STORY

The resurgence of various Trojan families is heavily impacting the Android threat landscape, indicating significant risks for individual users and businesses since many employees rely primarily on smartphones for both professional and personal communication. The growing prevalence of Trojans also highlights the evolving tactics of attackers, who continue to exploit vulnerabilities despite increased security measures by Google and other device manufacturers.

Adware vs Trojan Proportional Split

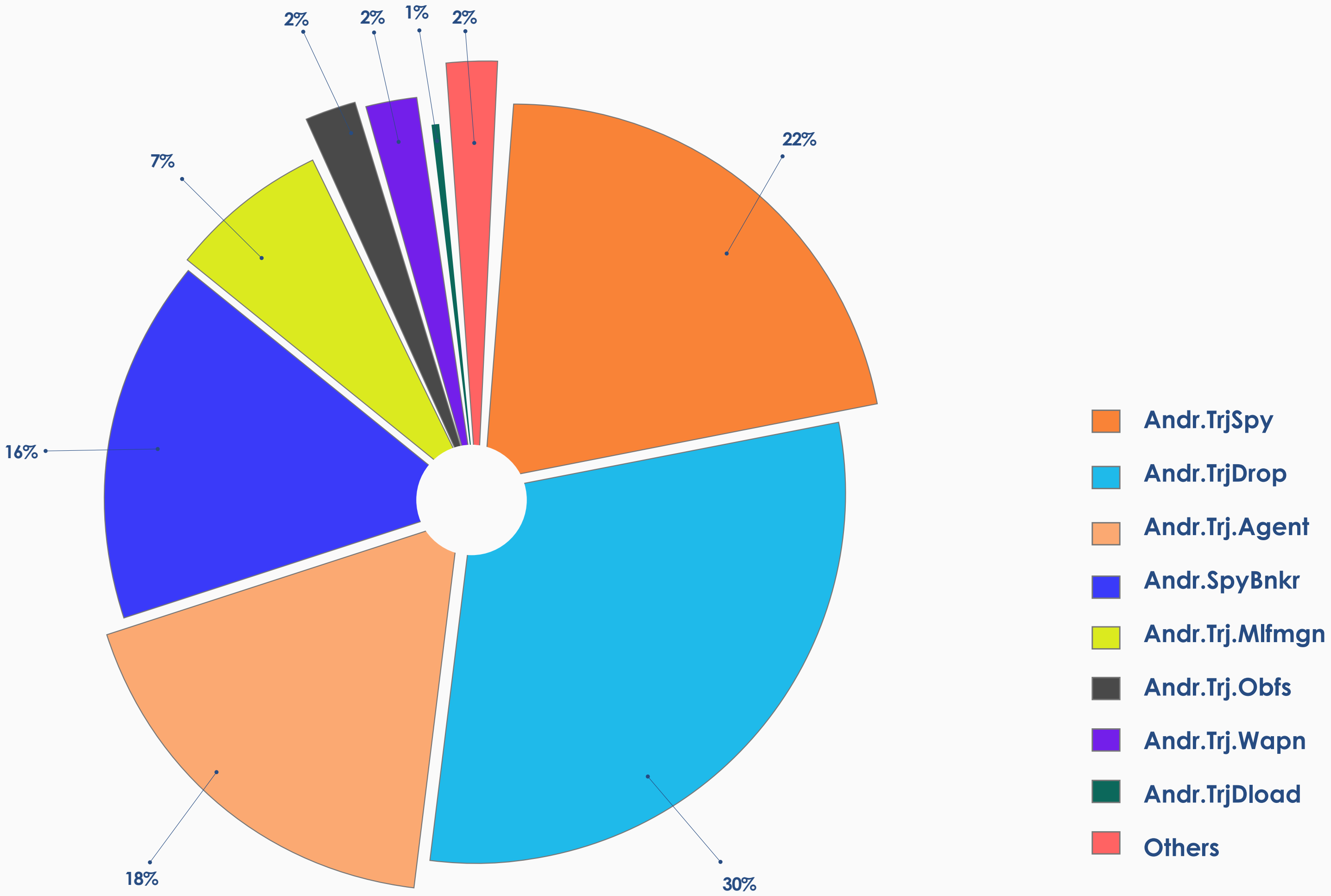


Trojans now account for 86% of threats—a 9% increase from the previous quarter.

THE OMNIPRESENT TROJAN

The latest data reveals a significant presence of Trojans in the Android threat landscape, with Andr.TrjSpy accounts for 22%, Andr.TrjDrop for 30%, Andr.Trj.Agent for 18%, and Andr.SpyBnkr for 16%. These threats compromise user privacy, install additional malware, act as intermediaries for further attacks, and target sensitive financial data. Both individual users and corporate employees represent severe risks to personal information, business communication, and economic security, making them a critical concern in today's mobile-dependent environment.

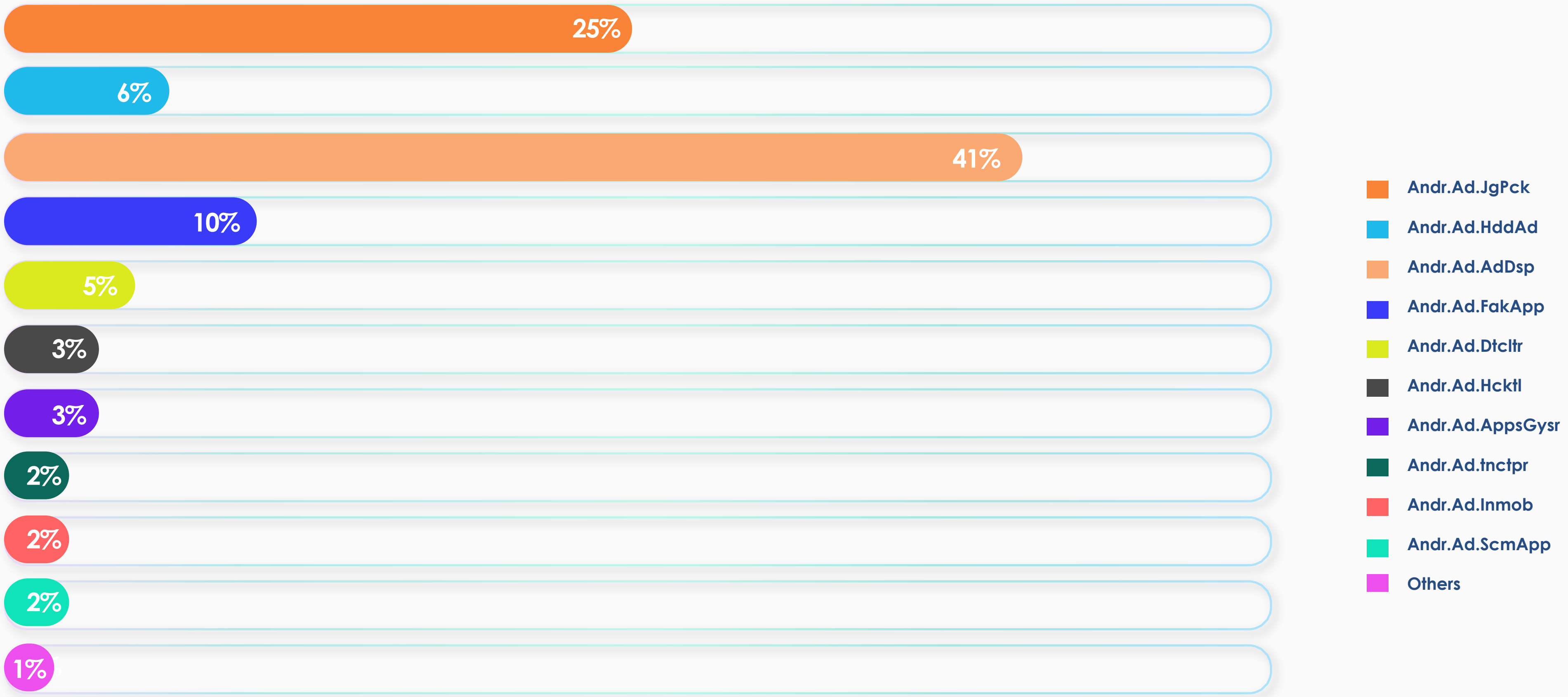
Most Prevalent Trojan Types



THE ADWARE SAGA

The latest data highlights a strong presence of adware in the Android threat landscape, with Andr.Ad.AdDsp, Andr.Ad.JgPck, and Andr.Ad.FakApp dominating with double-figure infection rates. These families lead to the adware surge, leaving other variants with a comparatively minor impact on users.

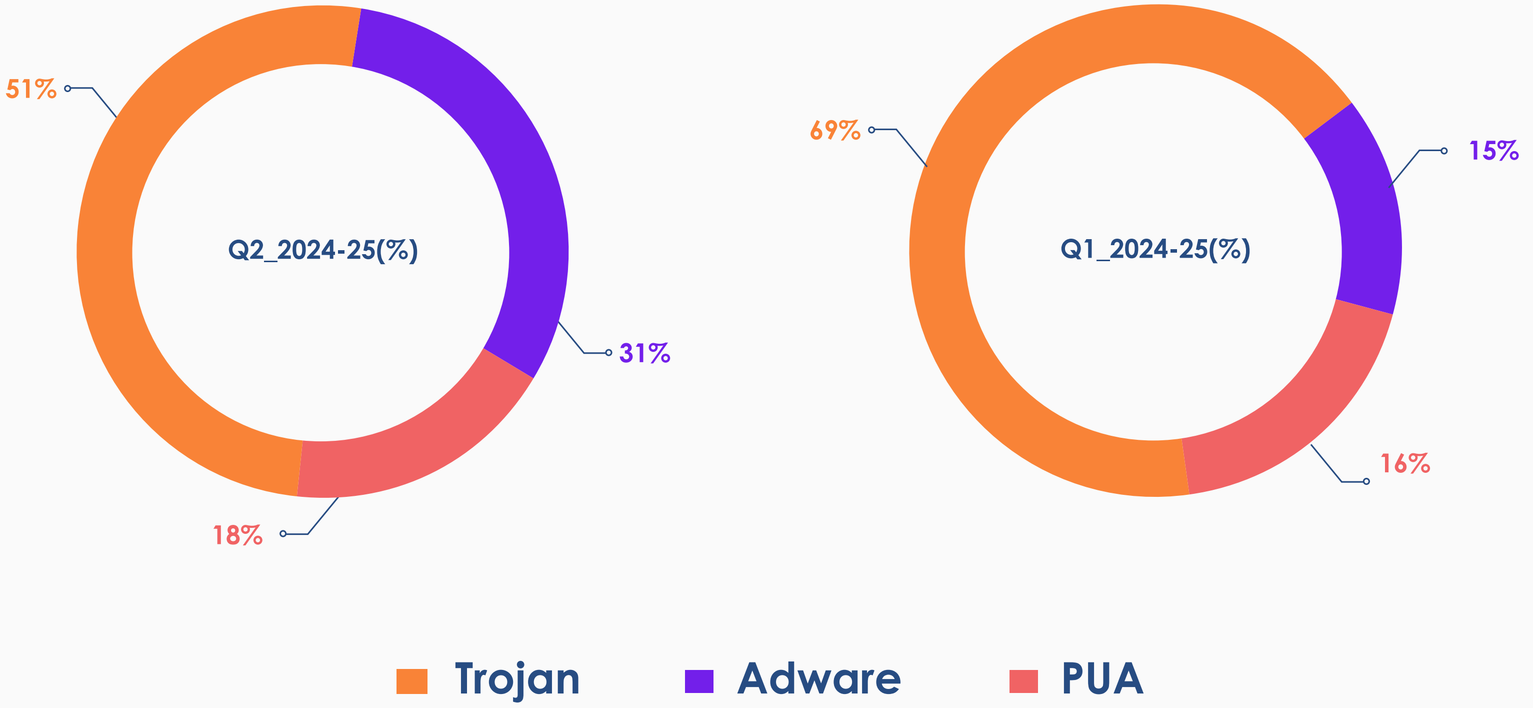
Trend Line Showing the Adware Plague



THE MAC ATTACK

The macOS threat landscape has experienced a similar shift, with adware surging as Trojans see a noticeable decline. This change highlights attackers' growing preference for adware, which is less detectable and more profitable. As Apple continues strengthening macOS security with each update, making traditional Trojans harder to execute, adware offers a stealthier method, often bypassing security checks unnoticed. Adware's ability to generate revenue through invasive ads makes it increasingly appealing to developers, while user reliance on third-party downloads and limited cyber hygiene awareness accelerate its spread. This shift underscores how attackers adapt, leveraging adware for monetization and as a potential gateway for more malicious software.

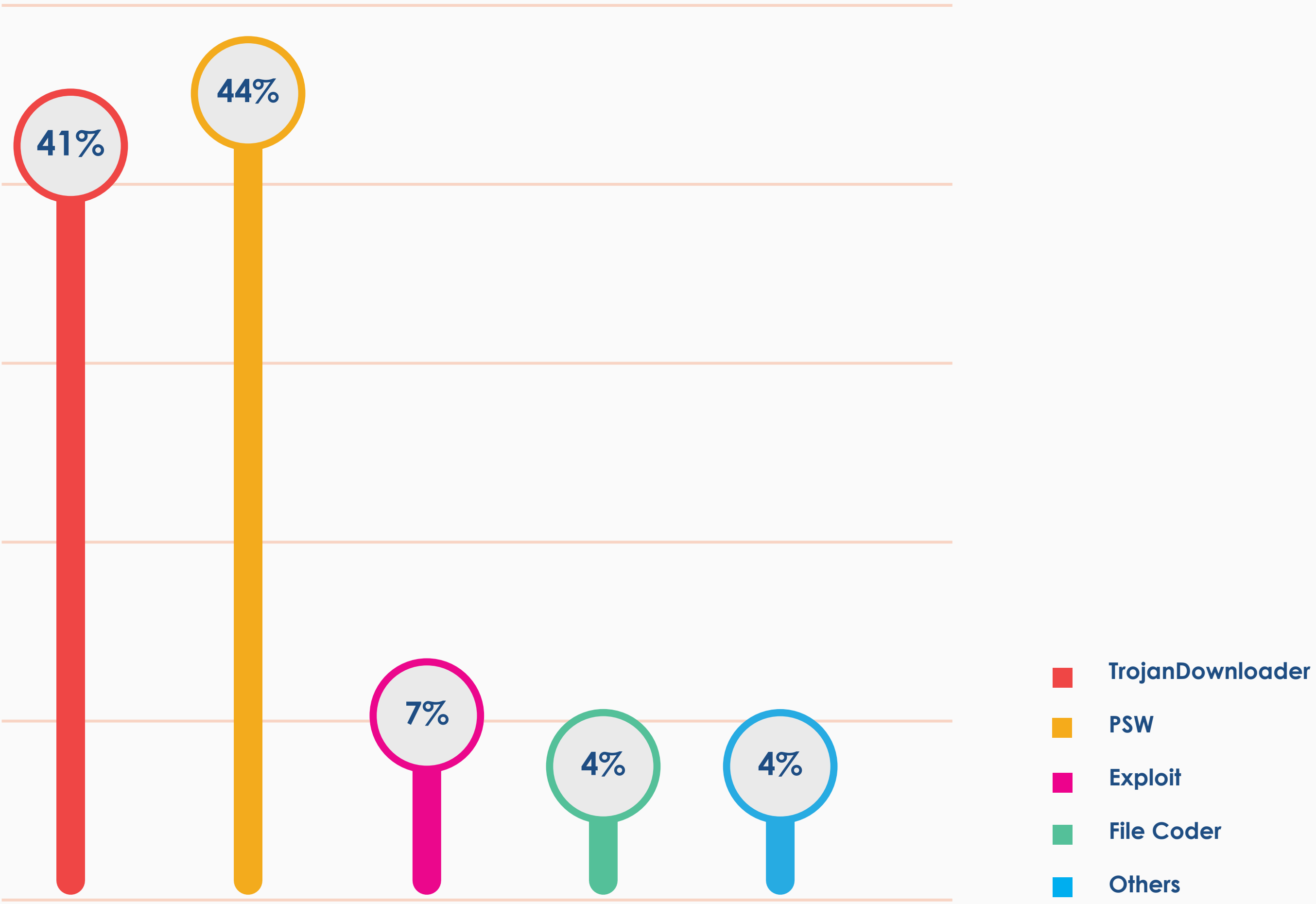
Trojan, Adware, and PUA Proportional Split



THE UBIQUITOUS TROJANS

The rapid growth of PSW and downloader Trojans in the space reflects a shift toward more targeted credential theft to execute more malice and distribute malware. These two families now account for 85% of visible Trojans. PSW focuses on stealing login credentials, while Downloader covertly installs additional malicious apps, exploiting encrypted URLs to evade detection.

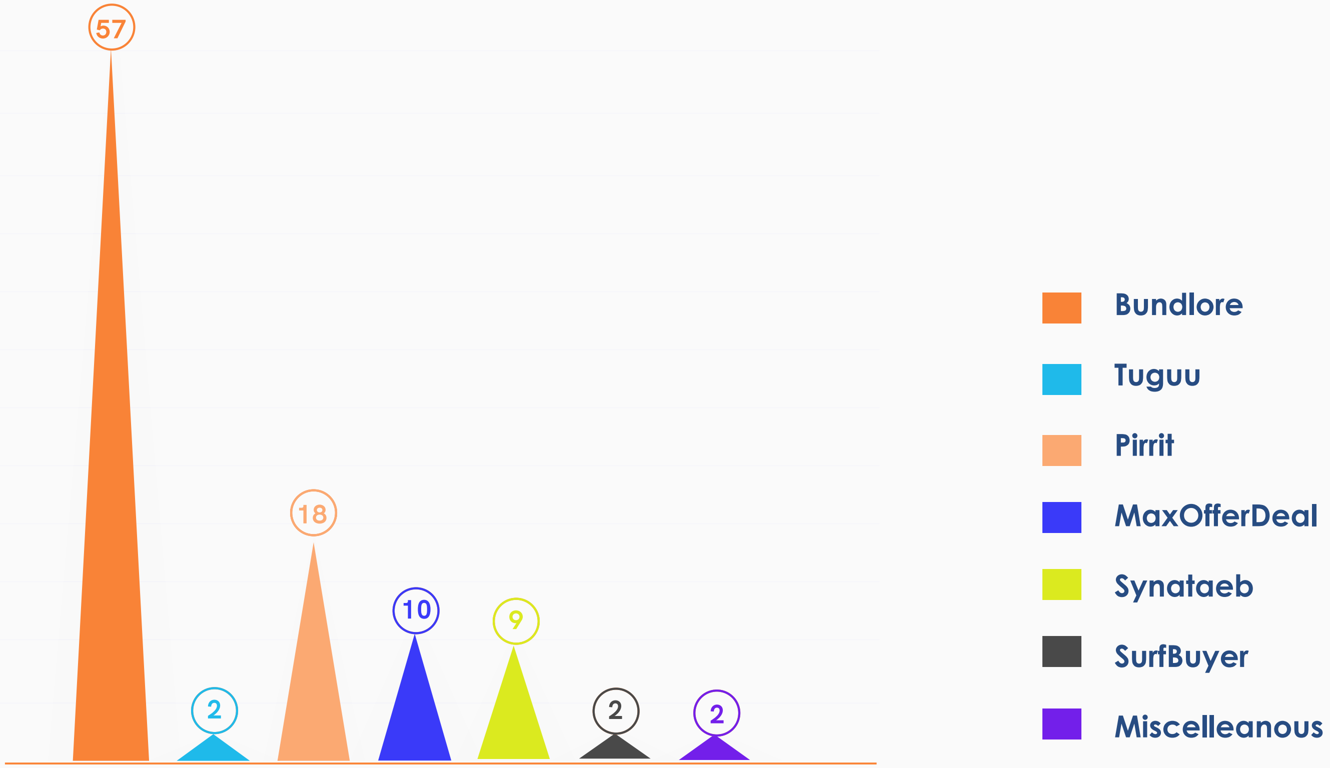
Trojan Detection Trend Line



THE ADWARE BROUHAHA

In the macOS adware landscape, Bundlore dominates with 57%, followed by Pirrit at 18% and MaxOfferDeal at 10%, reflecting a surge in intrusive advertising tactics. Bundlore bundles unwanted ads with legitimate apps, Pirrit uses stealth to evade detection while pushing ads, and MaxOfferDeal aggressively displays pop-up ads to drive fraudulent clicks. Together, these families fuel the growing threat of adware by exploiting user devices for profit through relentless advertising.

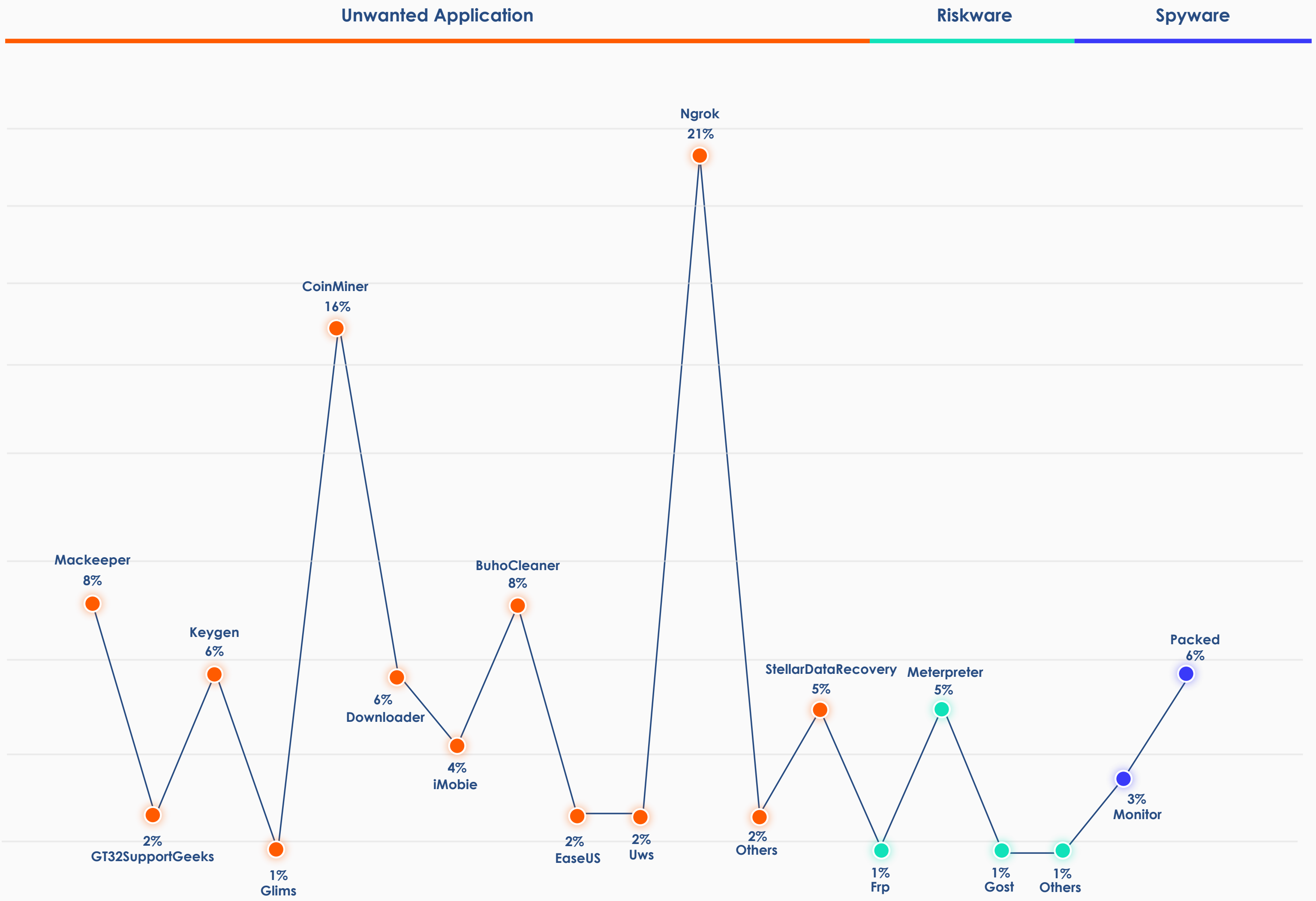
The Trend Line of Adware Variant Detections



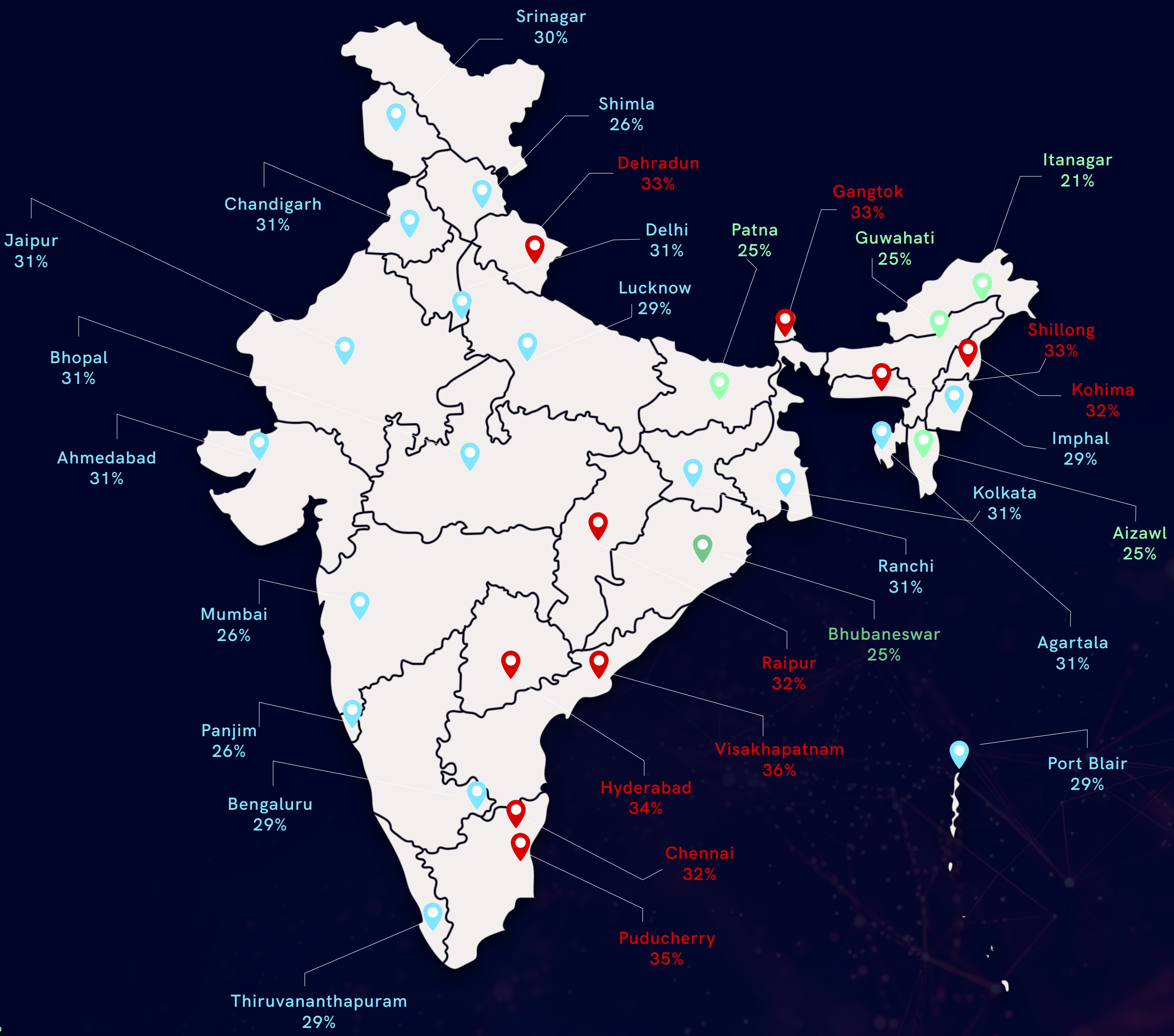
THE FARE SHARE OF PUPS

Ngrok and coinminer tools dominate the macOS PUA space, leveraging system vulnerabilities to establish unauthorized tunnels and mine cryptocurrency, respectively. Meanwhile, spyware accounts for 9% of attacks, reflecting a growing focus on covert data collection alongside these disruptive PUA threats.

Most Prevalent PUP Types



CYBER THREAT LANDSCAPE - INDIA

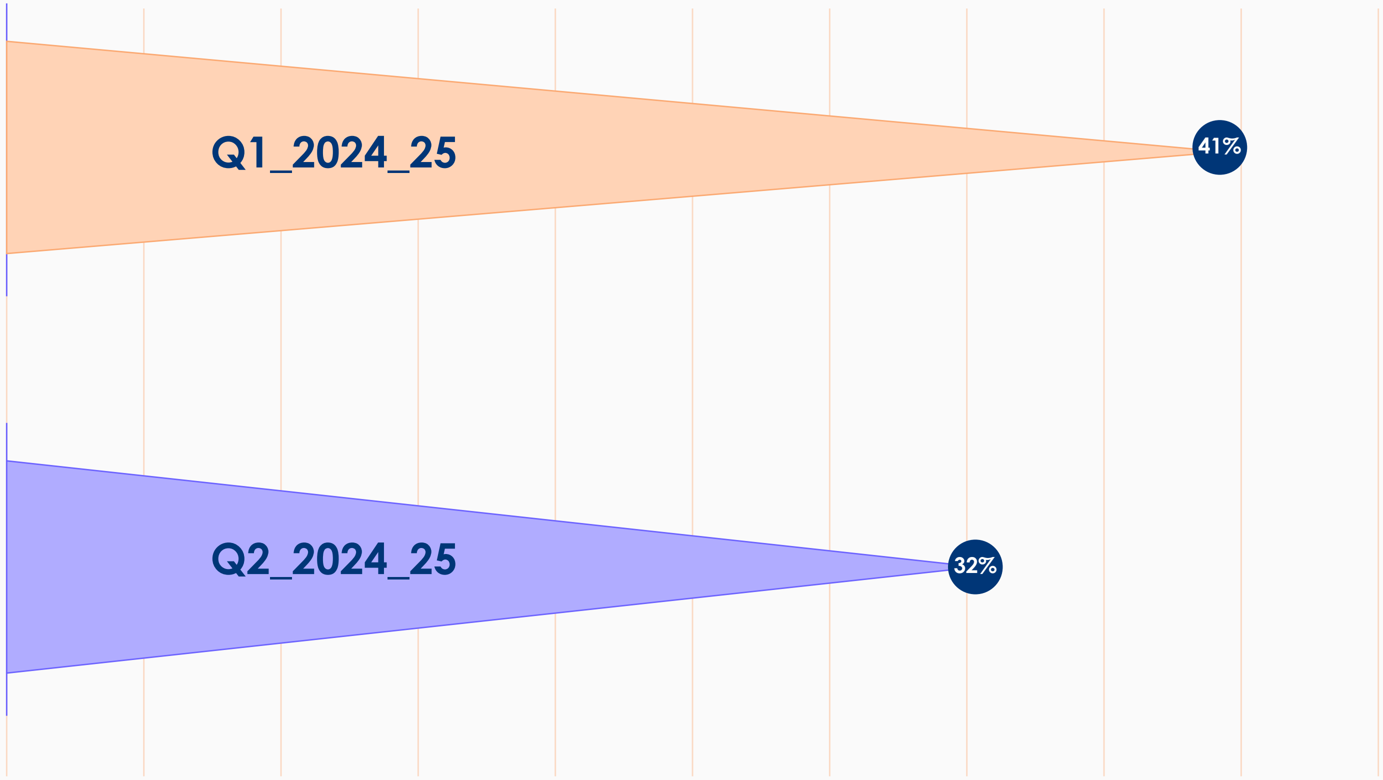


- ● 20%-25%
- ● 26%-31%
- ● 32%- 37%

Map for illustrative purposes only. Not to scale.

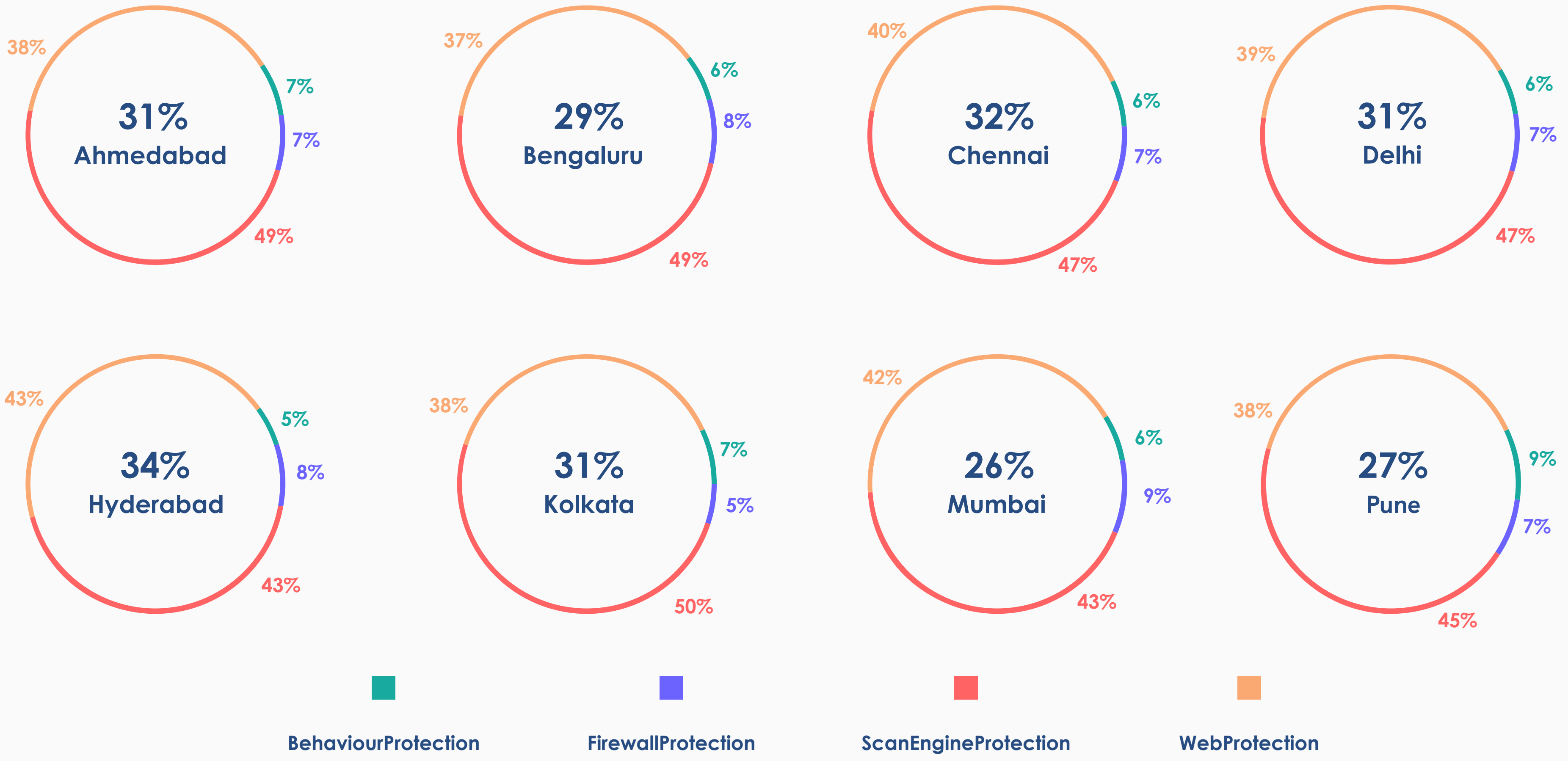
THE QUARTERLY TRENDS AND STATISTICS

The Overall Pan-India IR in comparison with the previous quarter is given below.

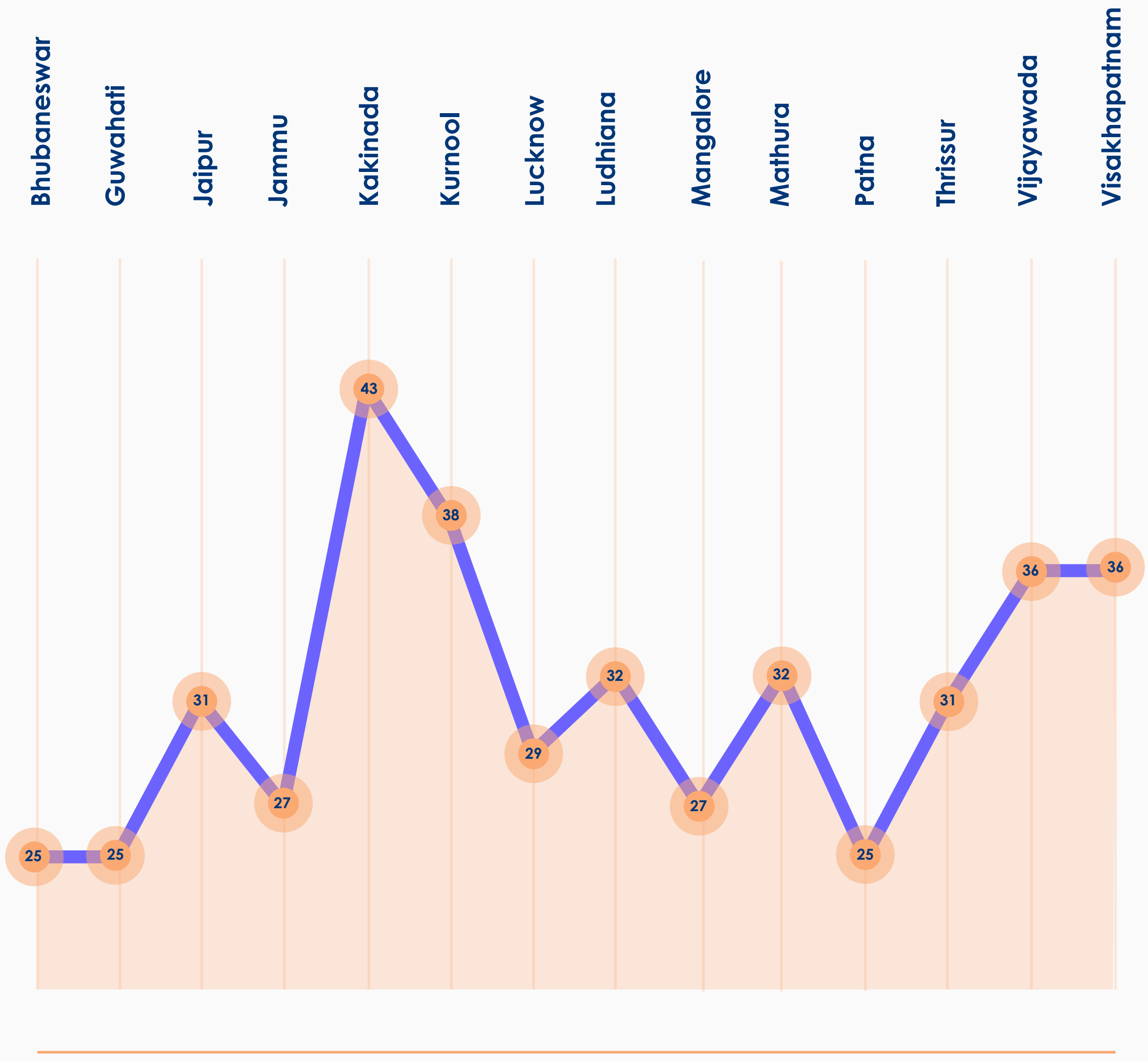


A declining infection rate may signal more targeted and sophisticated attacks as threat actors shift from random exploits to strategic infiltrations aimed at specific high-value targets. This trend concerns enterprises and governments alike, as it reflects a growing focus on precision, potentially leading to more profound breaches with more severe consequences.

THE METRO AND TIER-1 CITIES - INFECTION RATE



TOP INFECTION RATES IN TIER-2 CITIES



The surge of malware in Tier-2 cities is driven by rapid digital adoption, inadequate cybersecurity infrastructure, and lower awareness, making these regions easy targets for cybercriminals. This trend poses a growing concern for developing countries, as compromised systems can lead to economic disruption, data breaches, and the spread of malware across critical sectors.

SIGNIFICANT VULNERABILITIES FOR THE QUARTER

Apache's Traversal Vulnerability with a 9.8 CVSS score

A path traversal vulnerability "CVE-2024-32113" in Apache's OFBiz allows an attacker to construct malicious requests for the server which may lead to path traversal on a restricted directory due to improper limitation in the pathname having no filtering.

Apache OFBiz versions below 18.12.13 are vulnerable.

Windows Spoofing Vulnerability with a CVSS score of 7.5

CVE-2024-38112, vulnerability in Windows MSHTML Platform allows an attacker to access critical information by sending malicious files to the user and convincing them to open it.

Impacted versions exploited in the wild:

- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2

GeoServer's GeoTools Vulnerability

CVE-2024-36401, a path traversal vulnerability in GeoServer's GeoTools Library causes unsafe evaluation of property names as XPath expressions lead any unauthenticated attackers to send specially crafted input against GeoServer Installation and successfully execute remote code onto the server.

Versions Vulnerable:

Prior to versions 2.23.6, 2.24.4, and 2.25.2

Windows Scripting Engine Vulnerability - 7.5 CVSS score

The memory corruption vulnerability, CVE-2024-38178, in Windows Scripting Engine allows unauthenticated attackers to craft and send a malicious link to an authenticated client and convinces them to open the link in Edge executing in Internet Explorer mode leading to execute arbitrary code on the client system.

Vulnerable versions:

- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 for 32-bit Systems
- Windows 11 version 24H2 for ARM64-based Systems
- Windows 11 version 24H2 for x64-based Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2

EOP Vulnerability in Windows Installer

An elevation of privilege vulnerability, CVE-2024-38014, with a CVSS base score of 7.8 in Windows Installer creates improper privilege management while running repair functionality under low privileged users by maliciously interfering with the repair functions, an attacker may gain SYSTEM privileges.

Vulnerable versions:

- Windows 10 Version 1809 for 32-bit Systems,
- Windows 10 Version 1809 for x64-based Systems,
- Windows 10 Version 1809 for ARM64-based Systems,
- Windows Server 2019,
- Windows Server 2019 (Server Core installation),
- Windows Server 2022,
- Windows Server 2022 (Server Core installation),
- Windows 11 version 21H2 for x64-based Systems,
- Windows 11 version 21H2 for ARM64-based Systems,
- Windows 10 Version 21H2 for 32-bit Systems,
- Windows 10 Version 21H2 for ARM64-based Systems,
- Windows 10 Version 21H2 for x64-based Systems,
- Windows 11 Version 22H2 for ARM64-based Systems,
- Windows 11 Version 22H2 for x64-based Systems,
- Windows 10 Version 22H2 for x64-based Systems,
- Windows 10 Version 22H2 for ARM64-based Systems,
- Windows 10 Version 22H2 for 32-bit Systems,
- Windows 11 Version 23H2 for ARM64-based Systems,
- Windows 11 Version 23H2 for x64-based Systems,
- Windows Server 2022, 23H2 Edition (Server Core installation),
- Windows 11 Version 24H2 for ARM64-based Systems,
- Windows 11 Version 24H2 for x64-based Systems,
- Windows 10 for 32-bit Systems,
- Windows 10 for x64-based Systems,
- Windows 10 Version 1607 for 32-bit Systems,
- Windows 10 Version 1607 for x64-based Systems,
- Windows Server 2016,
- Windows Server 2016 (Server Core installation),
- Windows Server 2008 for 32-bit Systems Service Pack 2,
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation),
- Windows Server 2008 for x64-based Systems Service Pack 2,
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation),
- Windows Server 2008 R2 for x64-based Systems Service Pack 1,
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation),
- Windows Server 2012,
- Windows Server 2012 (Server Core installation),
- Windows Server 2012 R2,
- Windows Server 2012 R2 (Server Core installation)

Android Kernel's RCE Vulnerability

The linux kernel CVE-2024-36971 vulnerability may allow attackers to execute arbitrary code due to improper implementation of RCU rules in __dst_negative_advice() race when dst_cache() must be cleared, which leads to possible use-after-free.

Vulnerable versions:

- 4.6 < Linux Kernel < 4.19.316
- 4.20 < Linux Kernel < 5.4.278
- 5.5 < Linux Kernel < 5.10.219
- 5.11 < Linux Kernel < 5.15.161
- 5.16 < Linux Kernel < 6.1.94
- 6.2 < Linux Kernel < 6.6.34
- 6.7 < Linux Kernel < 6.9.4

SonicWall's Vulnerability

CVE-2024-40766, an improper access control vulnerability in SonicWall SonicOS exists in the SonicOS management access and SSLVPN functionality, which can potentially lead to unauthorized resource access and may cause firewalls to crash under specific conditions.

Vulnerable versions:

- Gen5 firewall - 5.9.2.14-12o and older versions.
- Gen6 firewall - 6.5.4.14-109n and older versions.
- Gen7 firewall - 7.0.1-5035 and older versions.

CSA Command Injection Vulnerability

An OS command injection vulnerability dubbed, CVE-2024-8190 with a CVSS score of 7.2, in Ivanti Cloud Services Appliance (CSA) could lead to unauthorized access by remote authenticated attackers with admin level privileges due to passing the commands to the underlying OS via the administrative console

Vulnerable versions:

- CSA 4.6 (All versions before Patch 519)

OUR VERDICT

The evolving threat landscape presents significant challenges to organizations of all sizes and across sectors. Without surprise, ransomware remains one of the most formidable threats, with incidents increasing in sophistication and scale. Notably, we witnessed a sharp rise in refurbished malware alongside a few novel strains. These can be attributed to several factors, primarily driven by the evolving strategies of threat actors seeking to maximize their impact while minimizing detection. Refurbishing existing malware allows cybercriminals to bypass traditional antivirus systems and security measures often designed to detect known threats. By slightly modifying the code or delivery mechanisms, they can evade signature-based detection, making these strains appear new or undetected.

Additionally, malware-as-a-service (MaaS) availability on dark web markets enables less-skilled actors to access refurbished malware, driving its widespread use. These platforms offer malware kits that can be easily customized, increasing the overall number of attacks.

Vulnerable perimeter devices are particularly attractive to both state-sponsored and cybercriminal actors, emphasizing the need for rigorous patch management. In addition, the rise of Adversary in The Middle phishing kits demonstrates the lengths to which attackers will go to bypass traditional multi-factor authentication (MFA), making the adoption of phishing-resistant MFA solutions an essential component of any security strategy.

Beyond ransomware, hacktivist activity continues to disrupt organizations, particularly those linked to conflict zones. These groups focus on denial of service and website defacement campaigns, causing reputational and operational damage. On the other hand, state-sponsored actors increasingly rely on stealth, leveraging obfuscation networks, living-off-the-land (LOTL) techniques, and commodity tools to remain undetected. These methods are also gaining popularity among ransomware groups, making detection and attribution even more challenging.

Organizations must urgently secure their networks, protect customer and vendor data, and prioritize cybersecurity. Arranging educational workshops for employees is another urgent requirement to create an environment for practicing cyber hygiene. They should also implement strong firewalls, impose robust password policies, and conduct regular risk assessments to identify and fix vulnerabilities. Ensuring these measures are in place is critical for organizations to defend against the rising tide of sophisticated and coordinated attacks, whether financially or politically motivated.

Back To Contents

ABOUT US

K7 Computing is one of the earliest and most accomplished cyber security companies protecting more than 25 million clients worldwide against threats to their IT environment. Backed by more than 30 years of cybersecurity expertise. K7 Security offers best-in-class solutions & products.

K7 Labs is a leader in threat research, threat intelligence and in enforcing and applying excellent standards in cyber security. With a wide range of expertise across the Lab, you can be rest assured that you are in safe hands if you have chosen our K7 Security Product.

COVERING ENTERPRISE NEEDS WITH K7 ENDPOINT SECURITY (K7 EPS)

K7 Endpoint Security (K7 EPS) provides cost effective anti-malware capabilities for enterprises without the high purchase price, complex deployment models, or expensive renewal and maintenance costs found in other vendor solutions. Highly scalable, K7 EPS offers quick deployment and granular and centralised control over applications, devices, and networks.

K7 EPS anticipates, detects, and blocks cyberthreats, ensuring uninterrupted operations and protecting confidential business information. Designed to satisfy the needs of the modern enterprise, K7 EPS scales to protect any size of business operations and does not need an extensive in-house IT team for deployment or management.

Our in-house K7 Cerebro Engine is an ultrafast and scalable scanning engine which is capable of detecting not only existing threats but also emerging threats by using artificial intelligence and machine learning. Its proactive approach can detect and prevent the most advanced attacks, ensuring protection from zero-day attacks.

Back To Contents

CYBER THREAT MONITOR REPORT

Q2_2024-25

K7 SECURITY

www.k7computing.com