CYBER THREAT MONITOR REPORT

Q3_2024-25

www.k7computing.com

K7 SECURITY

LEVERAGING THREAT INTELLIGENCE INDICATORS TO PROACTIVELY FIGHT AGAINST CYBER THREATS

DECODING THE CYBER THREAT EVOLUTION: Q3 2024-25 INSIGHTS AND SOLUTIONS

The cybersecurity threat landscape is evolving at an unprecedented pace. Since 2011, attackers have consistently refined their tactics, tools, and goals, creating a dynamic environment that is increasingly difficult to navigate. Our latest findings underscore the complexity of this evolving threat matrix, where no "one size fits all" solution exists. Bad actors now tailor their methods to specific victims, targeting industries with motives ranging from financial gain to geopolitical disruptions. This diversity of intent and impact demands a nuanced approach to cybersecurity.

The Q3 2024-25 marks a pivotal moment in industrial cybersecurity awareness. Organizations worldwide took critical steps toward securing their operations, yet the threat landscape also became more dangerous. New actors, advanced breach techniques, and AI-powered malware emerged, underscoring the sophistication of adversaries. Attackers are leveraging AI to conduct reconnaissance, manipulate malware, and exploit social media for intelligence gathering, resulting in a surge in cyberattacks across all monitored regions. These trends align with patterns observed over the last five years, reflecting a steady rise in the scale and complexity of cyber threats.

This report provides an unparalleled, data-driven examination of the global threat landscape. By leveraging our comprehensive telemetry of historical data, we deliver actionable insights tailored to suit diverse industries. Our analysis empowers decision-makers to allocate resources more effectively, anticipate emerging threats, and implement proactive defenses.

Reasons to Read This Report

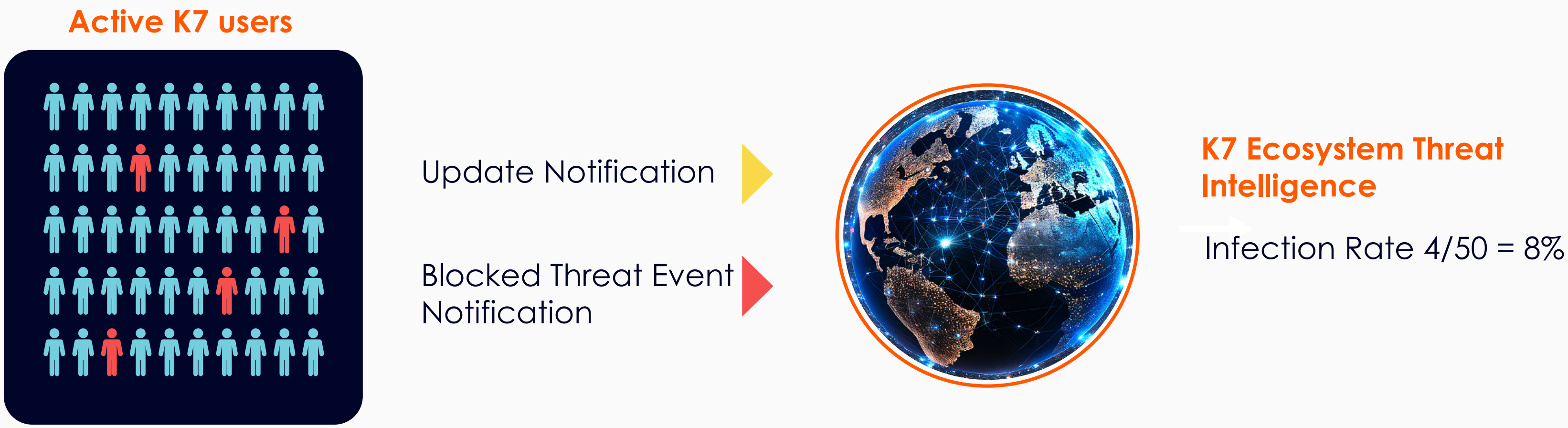
1. This is one of the industry's most downloaded reports, trusted by cybersecurity leaders across the world
2. Offers detailed, data-backed analysis to guide security priorities and in decision-making
3. Provides sector-specific insights, highlighting unique threats and its corresponding impacts
4. Delivers a deeper understanding of the latest evolving threats and their business implications
5. Goes beyond trends with validated data and context for institutional responses
6. Focuses on actionable insights, minimizing speculation to maximize strategic value

This report is one of your essential resources for staying ahead of the threat curve and for enterprises to secure themselves at the earliest.

INFECTION RATE (IR)

Those new to our quarterly report need to understand an important concept called “Infection Rate” (IR), which is used to benchmark 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 that 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 picture below better explains the concept of infection rate.

Infection Rate (IR) of an area



Active K7 users

Update Notification

Blocked Threat Event Notification

K7 Ecosystem Threat Intelligence

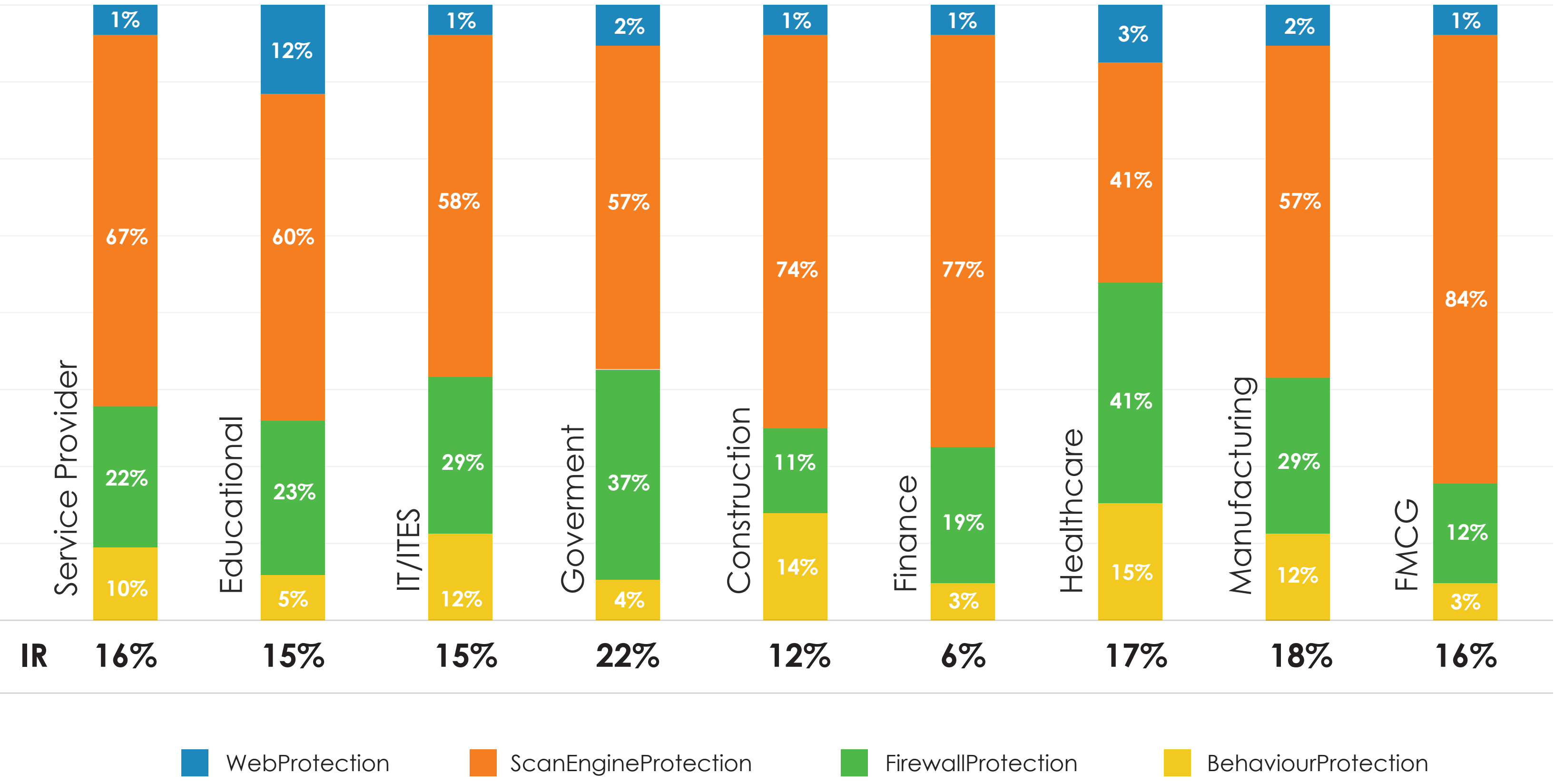
Infection Rate 4/50 = 8%

The Global Infection Rate (IR) for Q3_2024-25 was 22%

A Granular View of The Industry Threat Landscape

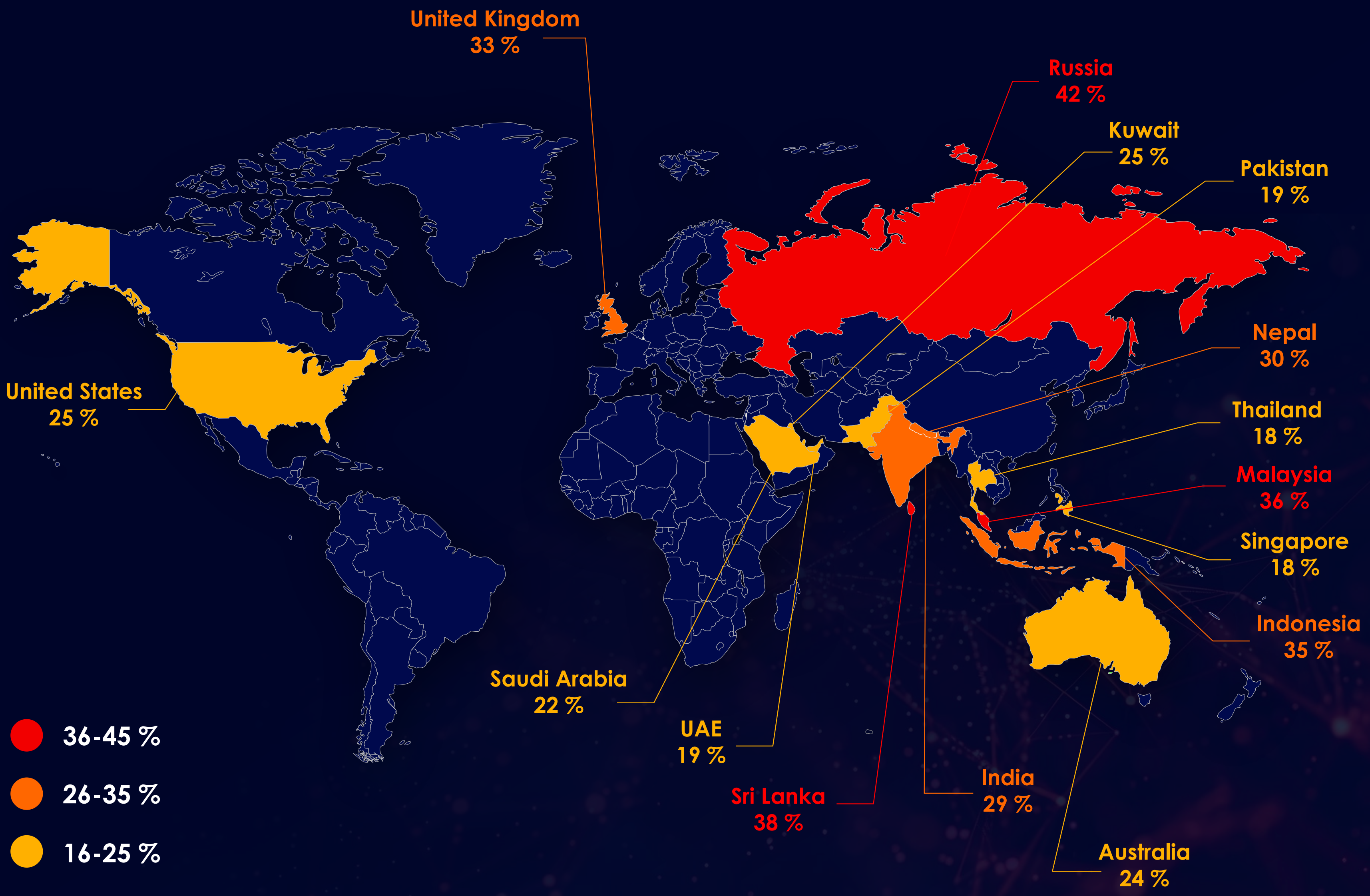
The constant surge of diverse malware families, driven by cybercriminal gangs and opportunistic individuals, continues to amplify the rising tide of malicious activity. These cybercriminal ecosystems operate like adaptive organisms, mutating and evolving to counter disruption and sustain the tempo of their attacks. While state-sponsored campaigns align with geopolitical agendas, targeting strategic assets and critical infrastructure, enterprises remain the primary victims—facing relentless disruptions, prolonged downtimes, and mounting remediation costs. In this high-stakes digital battleground, the convergence of sophisticated tactics, opportunistic exploits, and geopolitical tensions underscores an urgent need for resilient cybersecurity measures across all sectors.

Top Infection Rates Across Industry Verticals



Worldwide Cyber Threat Landscape

The global malware infection rate reflects a complex interplay of enterprise vulnerabilities and geopolitical tensions, with ransomware, social engineering attacks, and espionage activities driving significant fluctuations. Enterprises face escalating financial and operational risks, while nation-state actors exploit digital channels to pursue strategic objectives. This chart highlights various infection trends, offering insights into the evolving cyber threat landscape across borders.



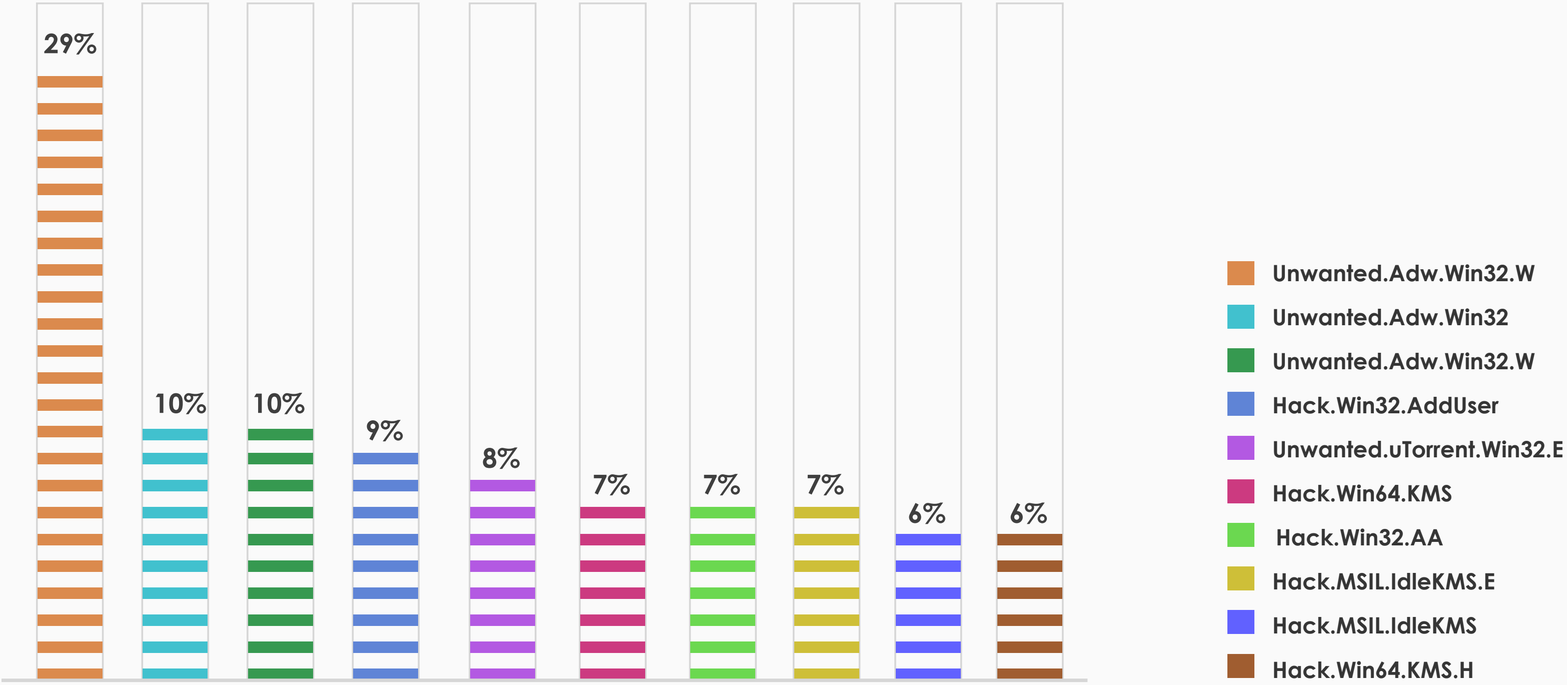
WINDOWS THREAT LANDSCAPE

Windows remains the primary target for cybercriminals due to its dominance across global enterprises, offering a vast attack surface ripe for exploitation. Despite increased targeting of Linux and macOS, Windows' widespread adoption, legacy systems, and frequent misconfigurations create persistent vulnerabilities. Cybercriminals leverage these weaknesses through ransomware, phishing campaigns, and zero-day exploits, compounding the rate of attacks. Yet, enterprises continue to rely heavily on Windows for critical operations, balancing its operational efficiency against ever-growing security risks.

Top Malware Targeting Windows Systems

A top-ten malware chart serves as a critical snapshot of the evolving digital threat landscape, offering CXOs, IT professionals, enthusiasts, and journalists clear insights into prevailing cyber risks. It highlights emerging attack trends, the most exploited vulnerabilities, and the strategies behind major cyber threats. Understanding this chart equips stakeholders to anticipate risks, fortify defenses, and make informed decisions in an increasingly volatile cyber ecosystem.

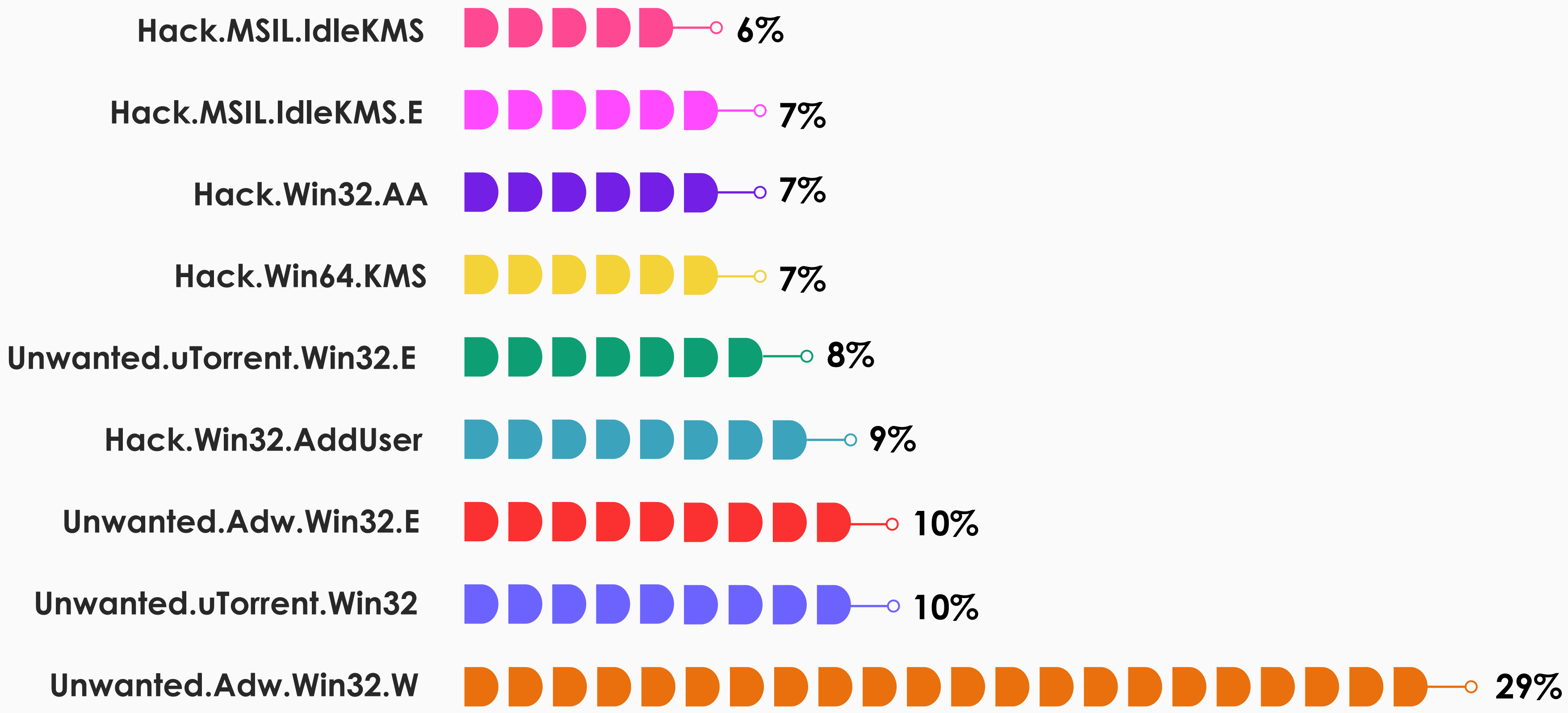
SPLIT OF WINDOWS TOP 10 DETECTIONS



Unpatched Vulnerabilities: The Achilles' Heel of Windows Systems

Vulnerabilities remain the entry point for most cyberattacks, with unpatched software, misconfigurations, and outdated systems serving as prime targets for exploitation. Ignoring or delaying vulnerability management exposes enterprises to ransomware, data breaches, and operational disruptions, often with catastrophic financial and reputational consequences. As threat actors continue to exploit these gaps with increasing precision, proactive vulnerability management is no longer optional—it's imperative for survival in the digital age.

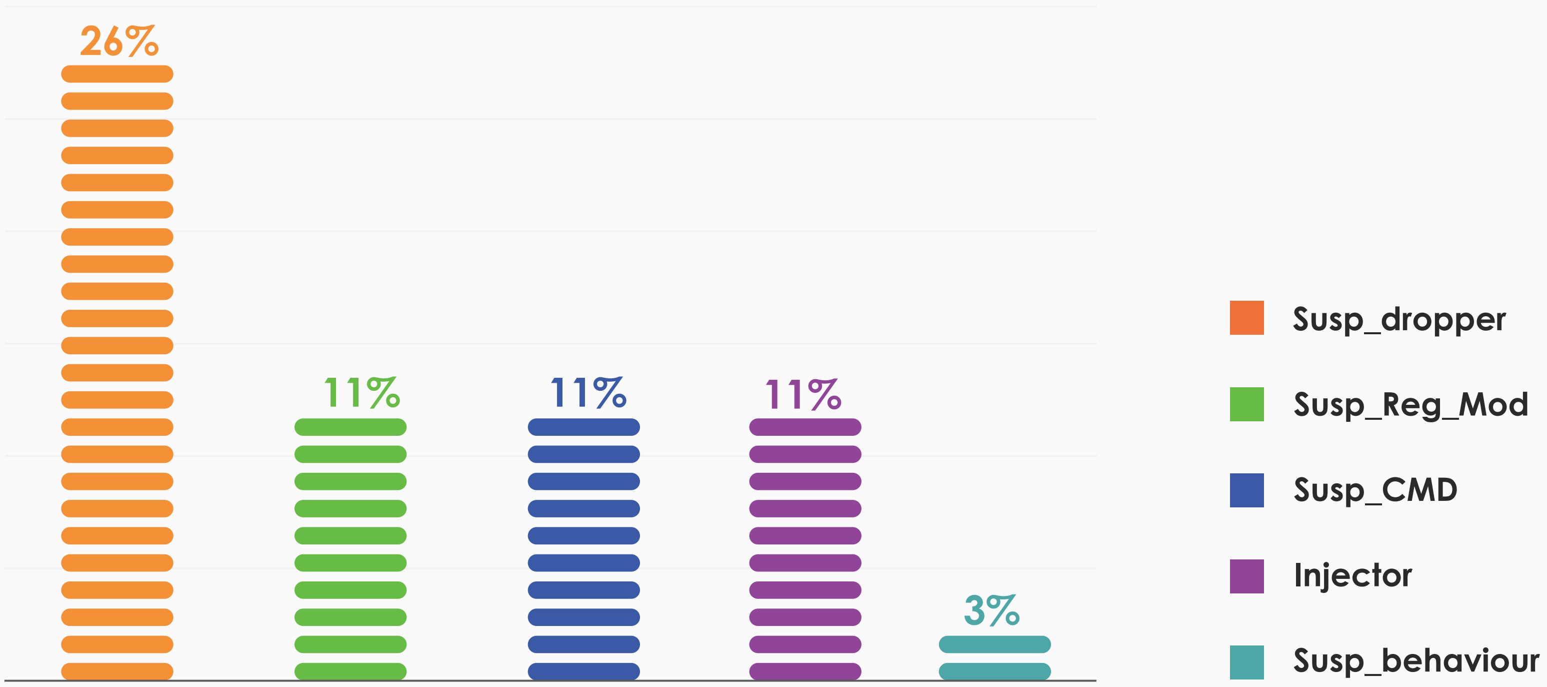
Most Prevalent Exploits



Heuristic Host Intrusion Prevention System (HIPS)

Heuristic behavioral detection identifies threats even without predefined signatures, making it a crucial defense against zero-day exploits and evolving malware variants. By analyzing patterns and behaviors rather than relying solely on known signatures, it offers a proactive shield against emerging threats.

Windows Heuristic Behavioural Detection



This chart highlights how droppers dominated with 26%, while registry modification, suspicious commands, and injectors each maintained a strong double-digit presence, underscoring the diverse tactics employed by modern cyber threats.

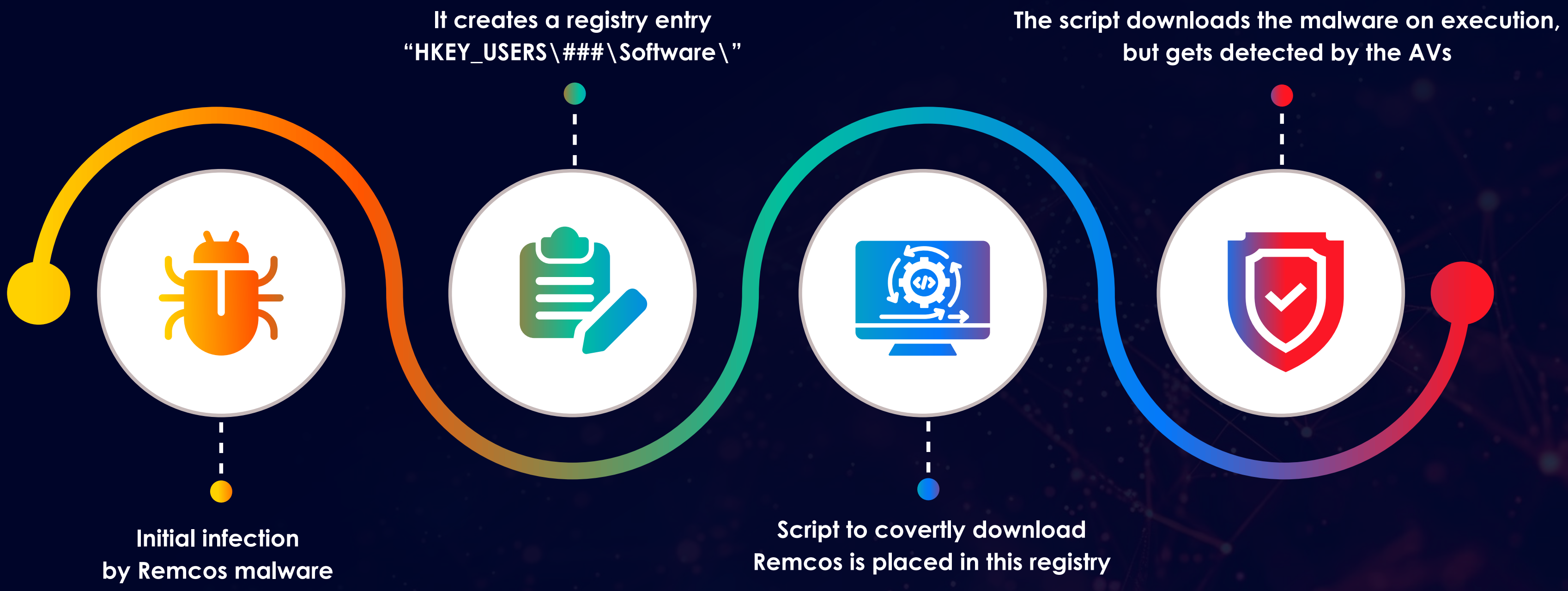
ENTERPRISE INSECURITY

Enterprises worldwide reported suspicious files downloaded to their temp folder without any apparent source. Further analysis revealed it to be the Remcos malware that was being covertly downloaded and promptly detected by the AV.

The kill-chain is as below:

- Initial infection by Remcos malware
- It creates a registry entry “HKEY_USERS\###\Software\”
- Script to covertly download Remcos is placed in this registry
- The script downloads the malware on execution, but gets detected by the AVs

Case Study: The Scripts Behind Remcos

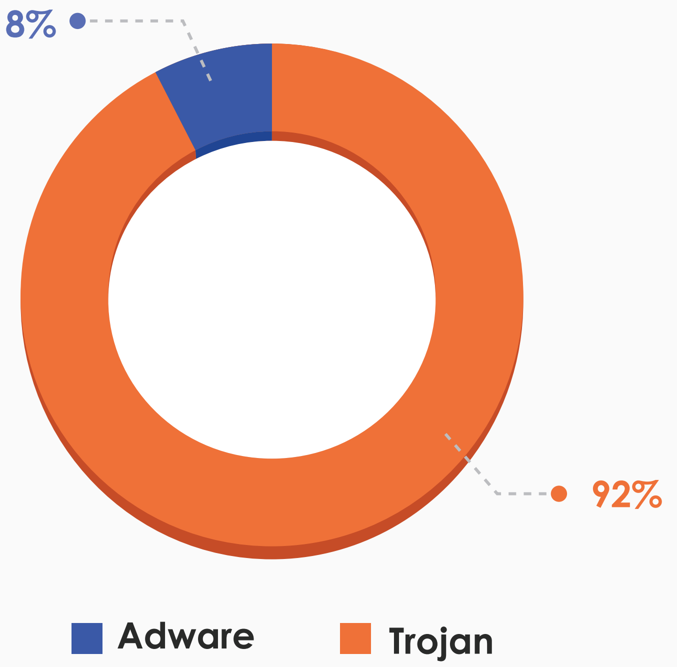

It creates a registry entry
“HKEY_USERS\###\Software\”
The script downloads the malware on execution,
but gets detected by the AVs
Initial infection
by Remcos malware
Script to covertly download
Remcos is placed in this registry

THE MOBILE DEVICE STORY

The skyrocketing acceptance of smartphones may be attributed to their versatility, functioning as digital Swiss Army knives capable of managing countless tasks through a single device. However, this growing reliance has not gone unnoticed by cybercriminals, who exploit these devices to orchestrate a wide array of scams. What once began as small-scale adware campaigns aimed at generating modest profits has escalated into sophisticated threats, including spyware, cryptominers, and Trojan-based malware schemes. These malicious tools not only steal sensitive user data but also serve as gateways for advanced attacks, such as smishing (SMS phishing) and SIM swapping, enabling threat actors to bypass security barriers and gain unauthorized access to personal and corporate accounts.

For enterprises, the implications are particularly grave. Smartphones often bridge the gap between personal and professional networks, making them prime targets for cybercriminals seeking entry points into organizational systems. A single compromised device can expose sensitive corporate data, disrupt workflows, and result in substantial financial and reputational damage.

Adware vs Trojan Proportional Split

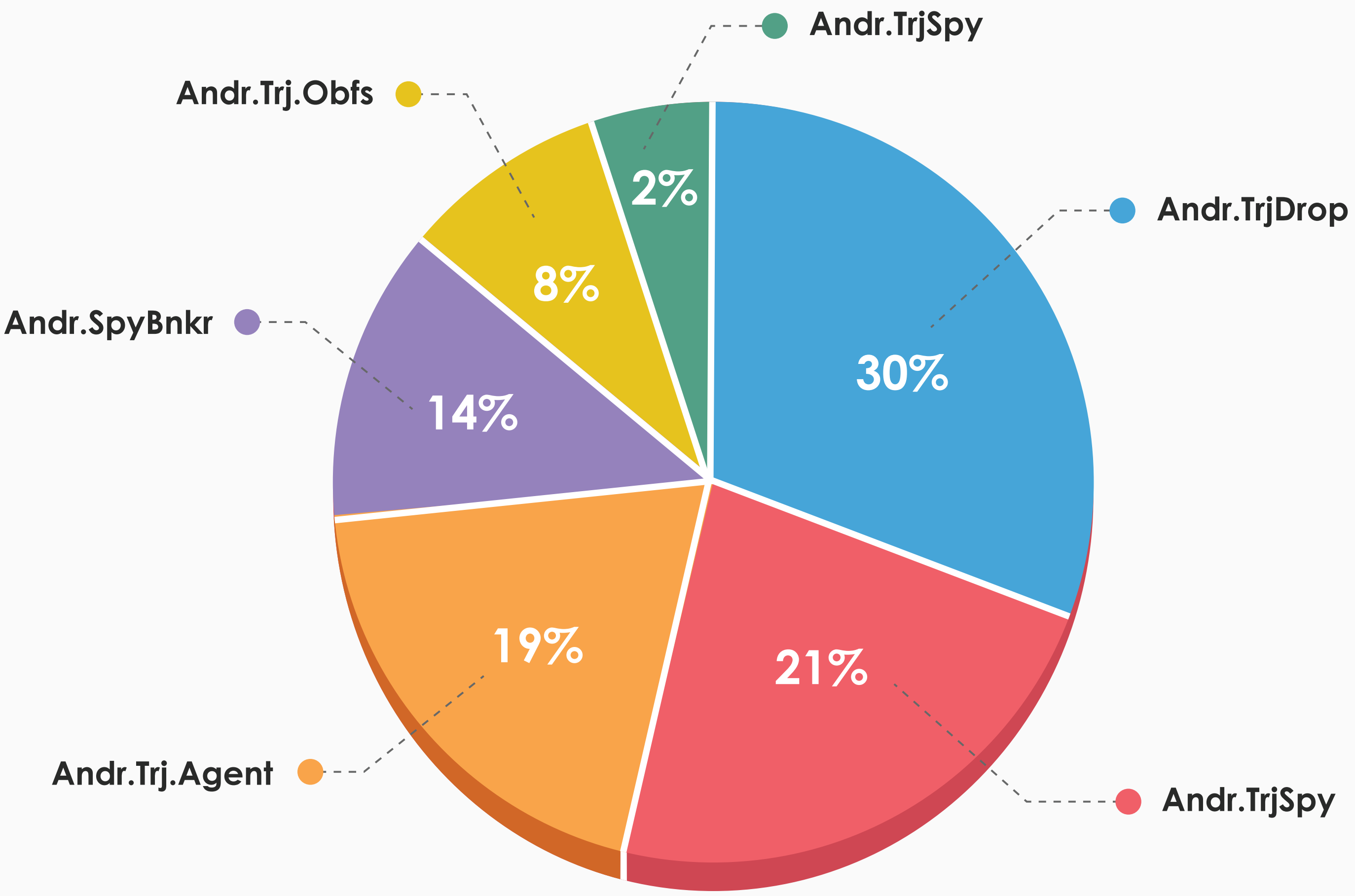


- Trojans Take the Lead: The sharp rise in Trojan detections to 92% reflects a shift towards stealthier, high-impact attacks. Unlike adware, which primarily annoys users with intrusive ads, Trojans enable cybercriminals to steal credentials, deploy ransomware, and maintain prolonged access to systems, posing a significant threat to enterprises.
- Evolving Cybercrime Tactics: The drop in adware to 8% signals a move away from quick-profit schemes towards sophisticated, long-term campaigns. Mobile devices are now prime targets for advanced persistent threats (APTs), where a single compromised phone can grant attackers entry into critical corporate systems.

Trojan Takeover Looms

The relentless rise of Trojan activity, dominated by Andr.TrjDrop, Andr.TrjSpy, Andr.Trj.Agent, and Andr.SpyBnkr variants at 30%, 21%, 19%, and 14% highlights a persistent shift towards highly targeted, profit-driven attacks. This steady dominance signals a growing reliance on sophisticated tactics to exploit vulnerabilities and maintain long-term access to compromised systems.

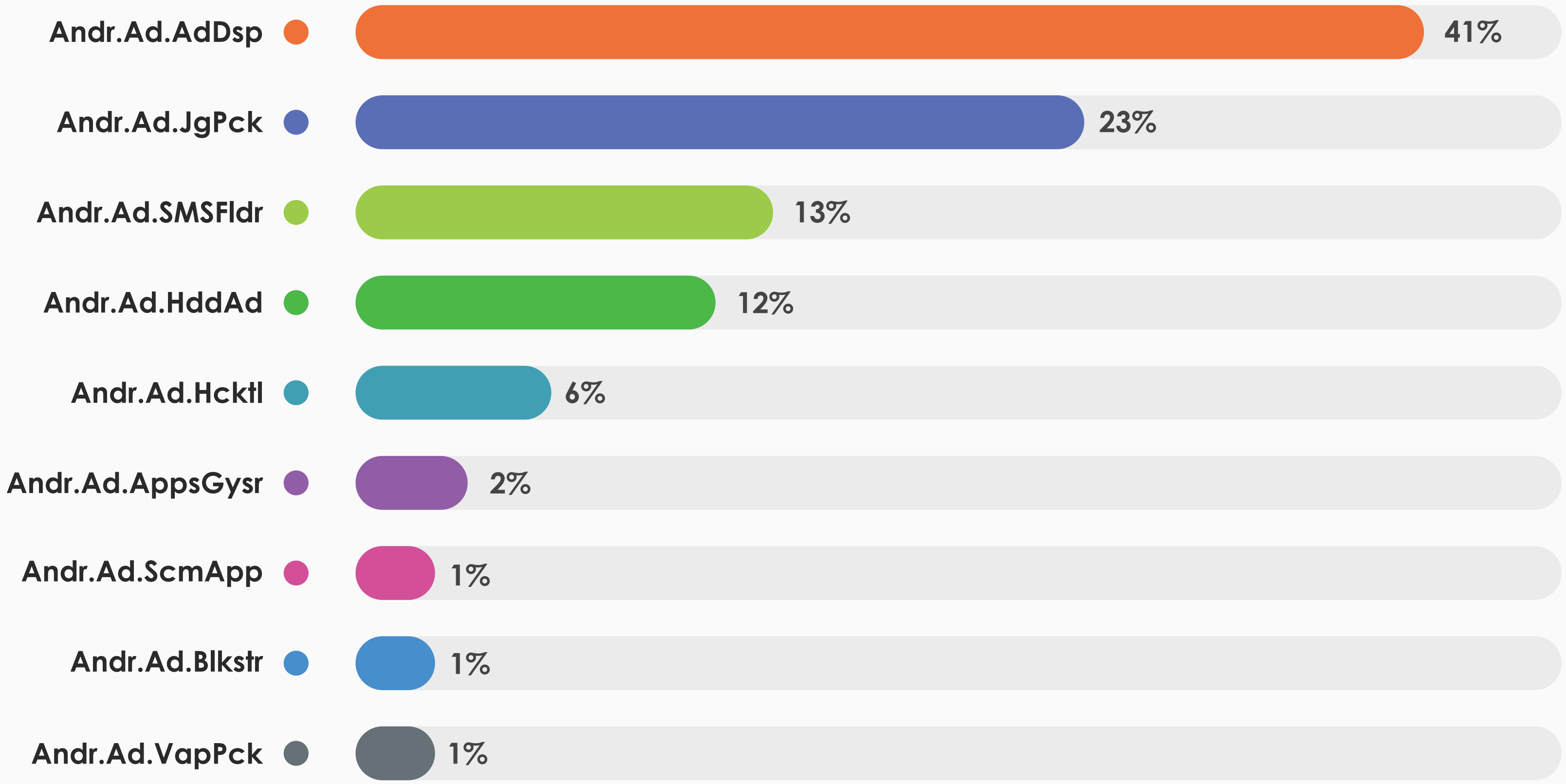
The Wicked Treadline of Trojan



The Diminishing Adware

In the adware space, the prevalence of Andr.Ad.AdDsp and Andr.Ad.JgPck prevails, while a few other families, like Andr.Ad.SMSSldr and Andr.Ad.HddAd, manages to occupy a fair share of visibility in the period.

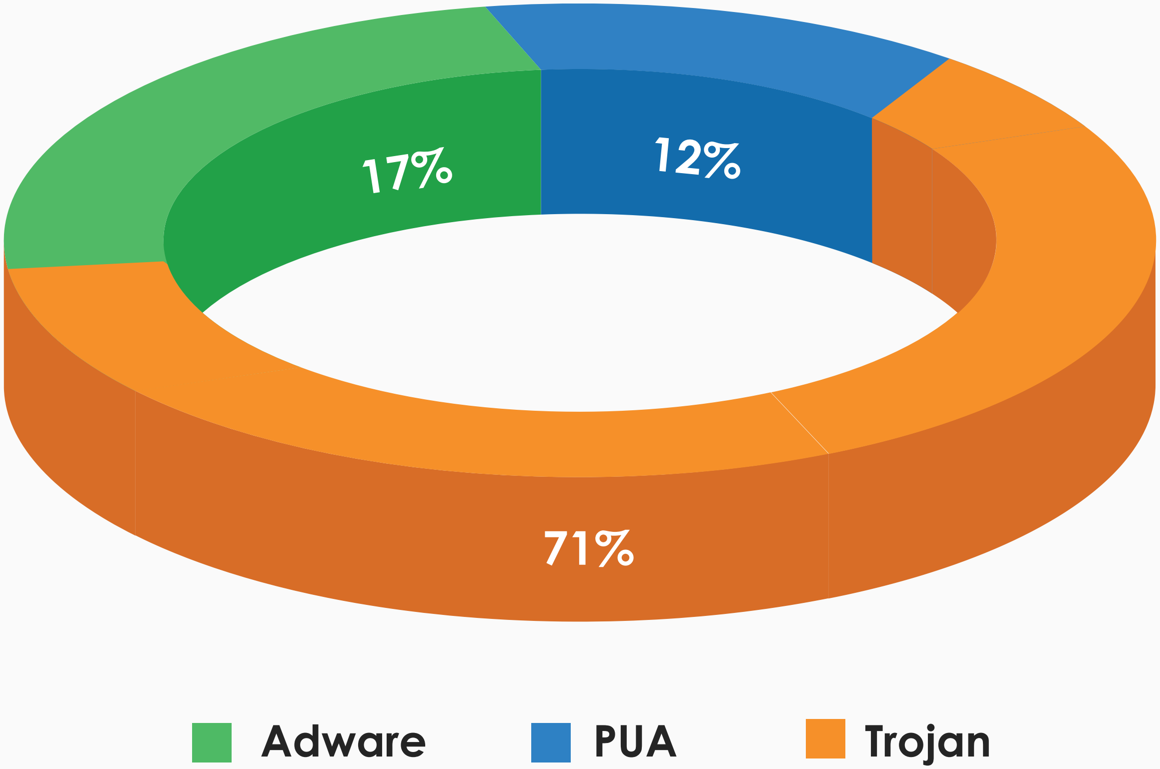
Most Prevalent Adware Types



THE MAC ATTACK

Even though the majority of threat actors focus primarily on targeting the Windows user base, macOS, too, has its fair share of threats, combining various categories similar to budding operating system platforms. Quarter after quarter, we witnessed a significant surge in both the variety and accessibility of macOS malware. Discussions on the darknet have surged enormously, featuring tips on bypassing macOS security measures, utilizing AI tools for malware creation, and exploiting social engineering tactics to offer macOS malware-as-a-service (MaaS).

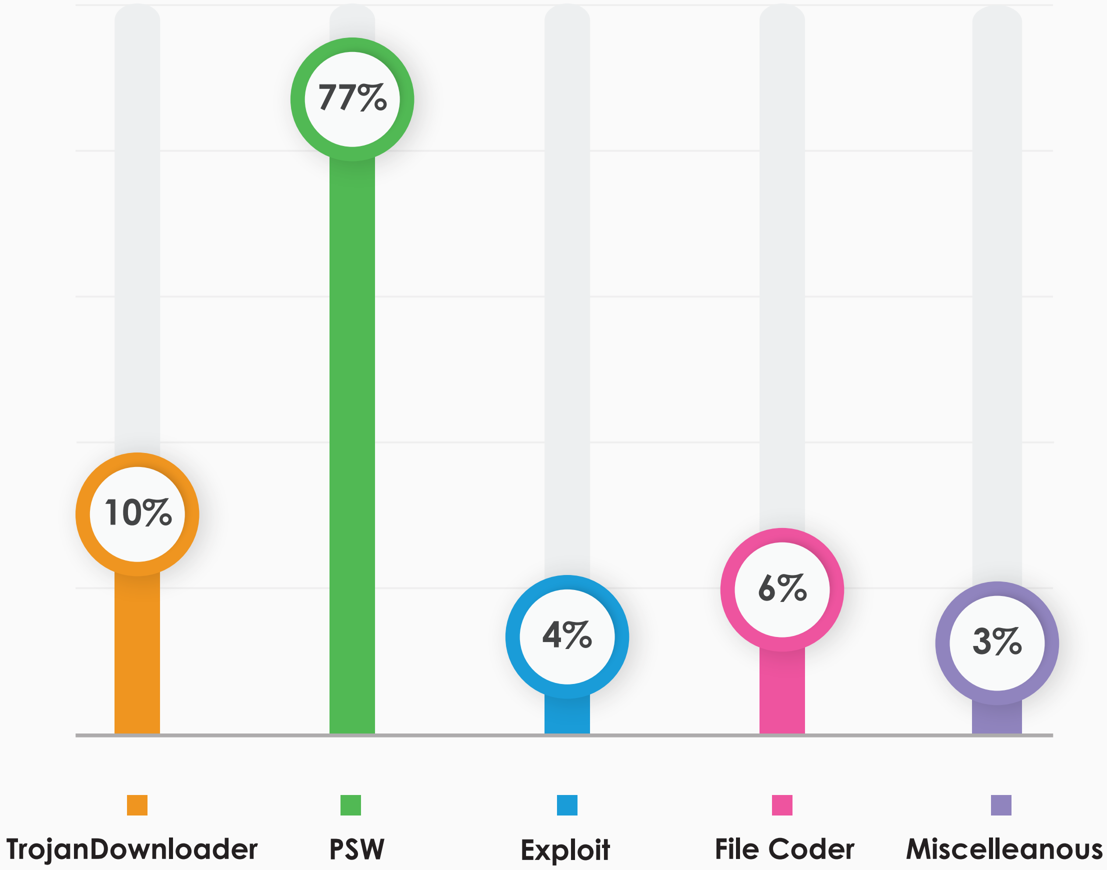
Trojan, Adware, and PUA Proportional Split



The Ubiquitous Trojans

As you can see in the chart, the Trojan landscape in the past quarter was majorly occupied by PSW, hinting at the swelling number of activities like credential theft saved in browsers and macOS keychains, system info collection, recording keystrokes, capturing screenshots, extracting stored credentials from email clients (e.g., Apple Mail) and messaging apps, modifying system settings or installing persistent launch agents to ensure the Trojan starts automatically with the OS, thereby transmitting the stolen information to remote servers controlled by attackers.

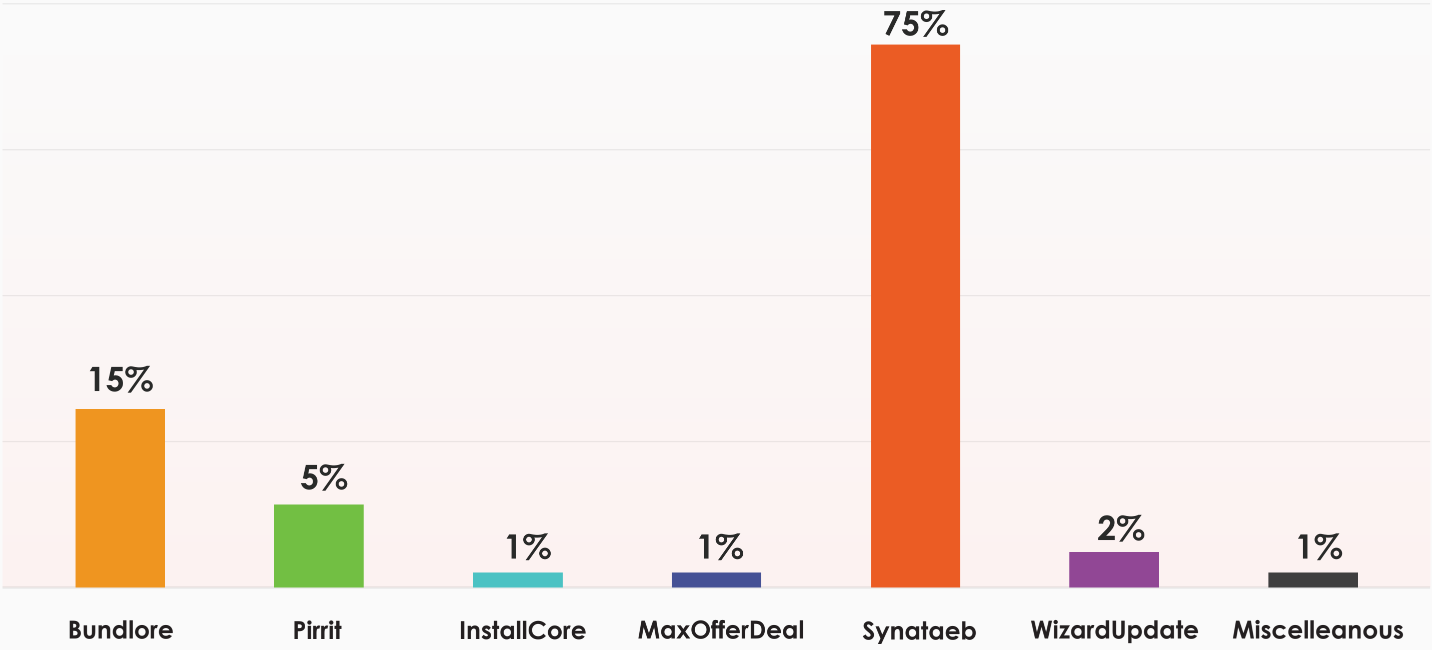
Trojan Detection Trend Line



The Adware Brouhaha

Unlike other OS platforms, adware continues to be a dominant factor in terms of volumes, even though the numbers have shrunk a bit. However, the adware campaigns are more focused on delivering widespread infections.

The Trend Line of Adware Variant Detections



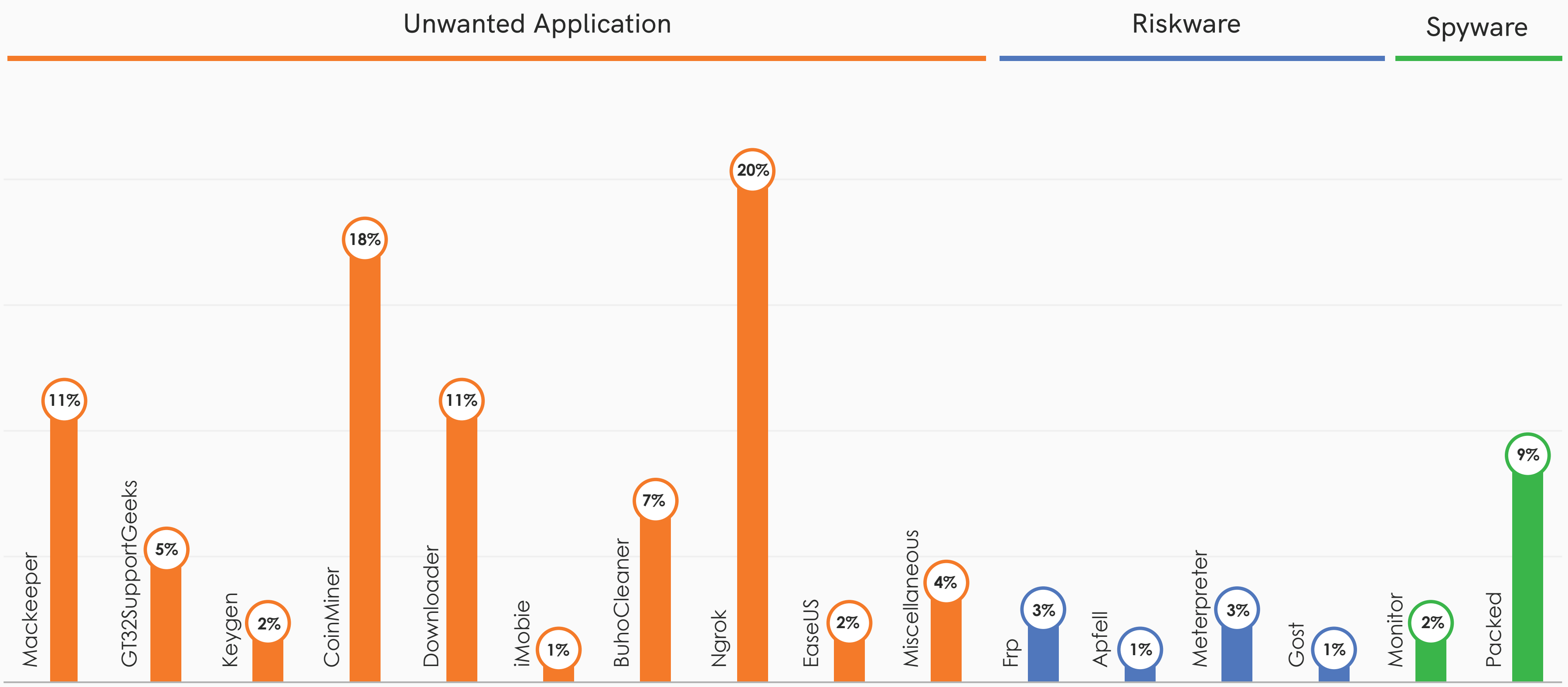
Synataeb adware has emerged as a dominant force in the macOS threat landscape, accounting for nearly three-fourths of all adware detections. This overwhelming presence highlights its widespread distribution and effectiveness in infiltrating systems compared to other adware families.

Once installed, Synataeb bombards users with intrusive ads, hijacks browsers, tracks user data, and degrades system performance, often acting as a gateway to more severe malware. Its role in the macOS threat ecosystem is significant, serving as a tool for revenue generation through ad frauds and as a catalyst for broader security risks, ultimately undermining user privacy and system integrity.

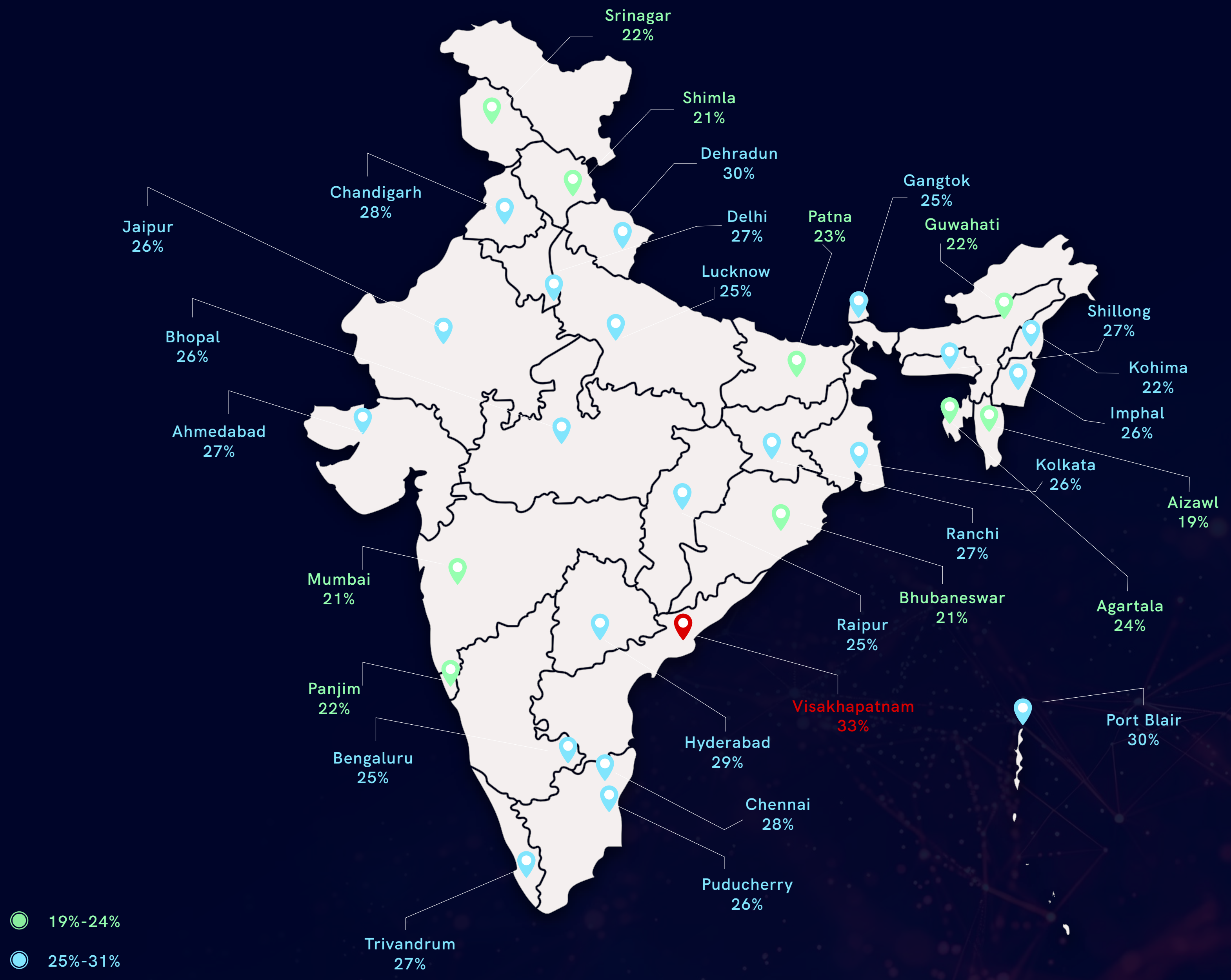
The Share of PUPs

Diverse detections in the potentially unknown programs (PUP) showcases that groups of threat actors focus on malicious activities, including establishing persistent remote access, executing arbitrary commands remotely, coin mining, spying among others.

Most Prevalent PUP Types



CYBER THREAT LANDSCAPE - INDIA



Map for illustrative purposes only. Not to scale.

Back To Contents

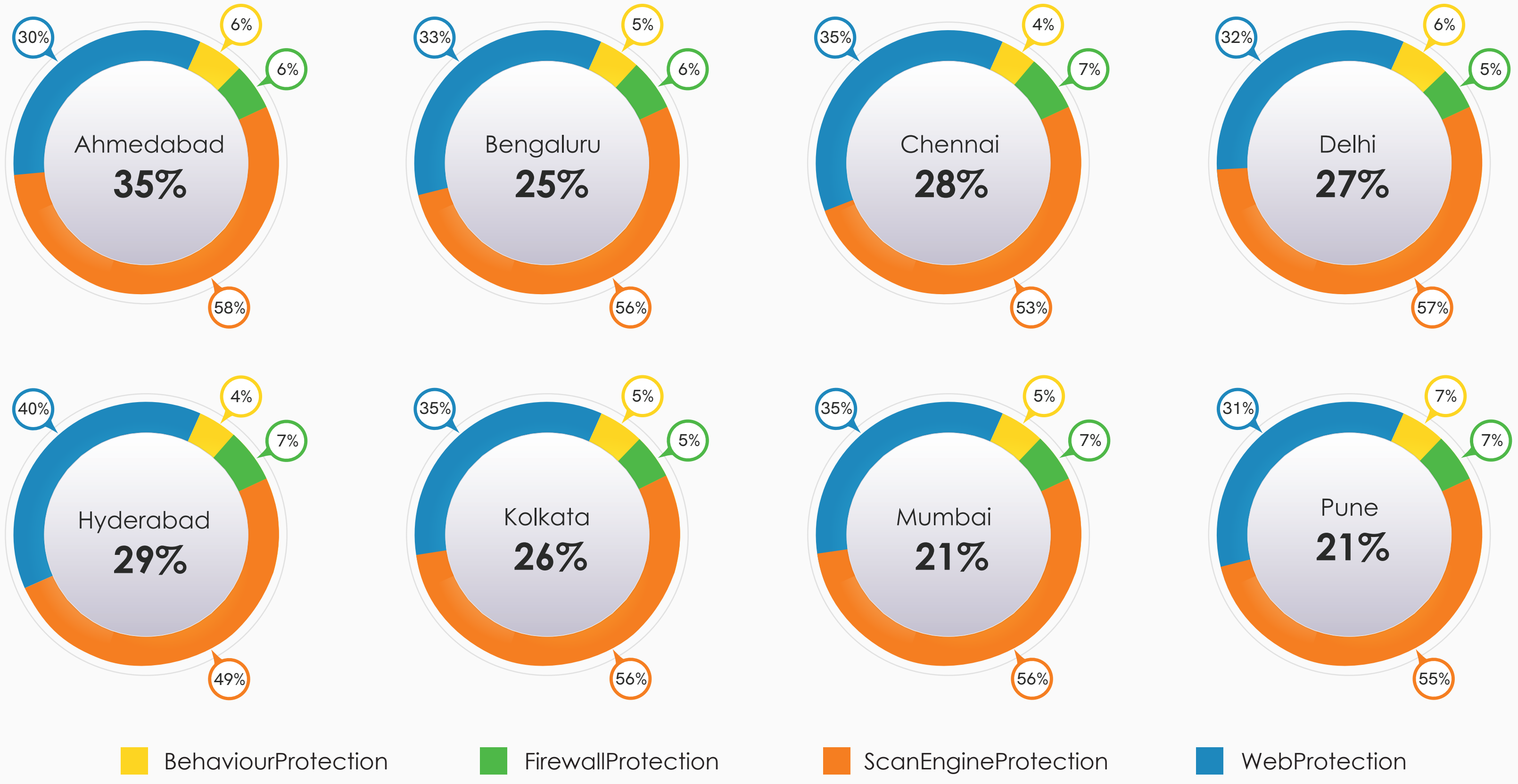
The Quarterly Trends And Statistics

The PAN-India cyber infection rate has surged to 26%, underscoring a critical vulnerability in nationwide digital defenses.

Countrywide Infection Rate Comparison

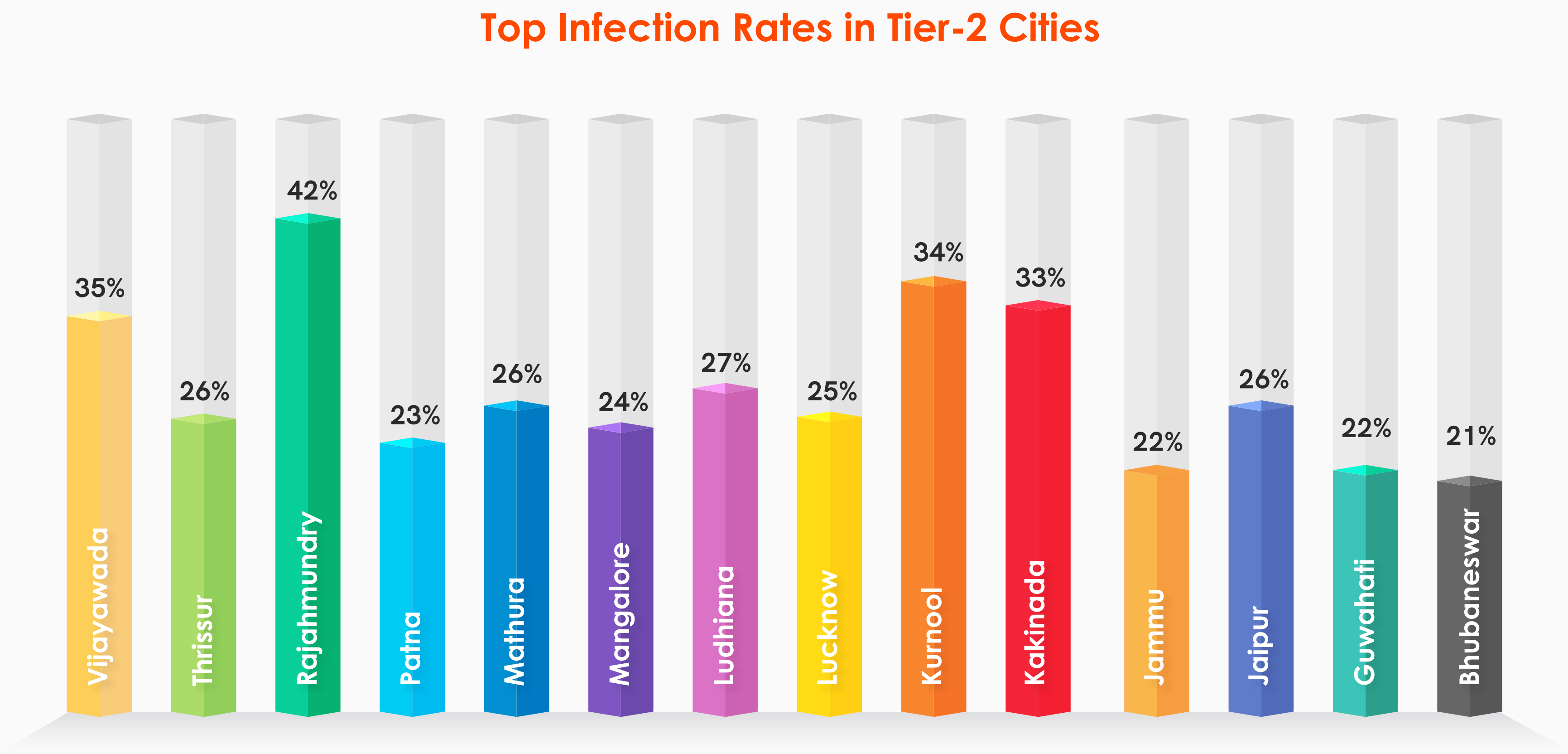
26% **Q3_2024-25**

The Metro And Tier-1 Cities- Infection Rate

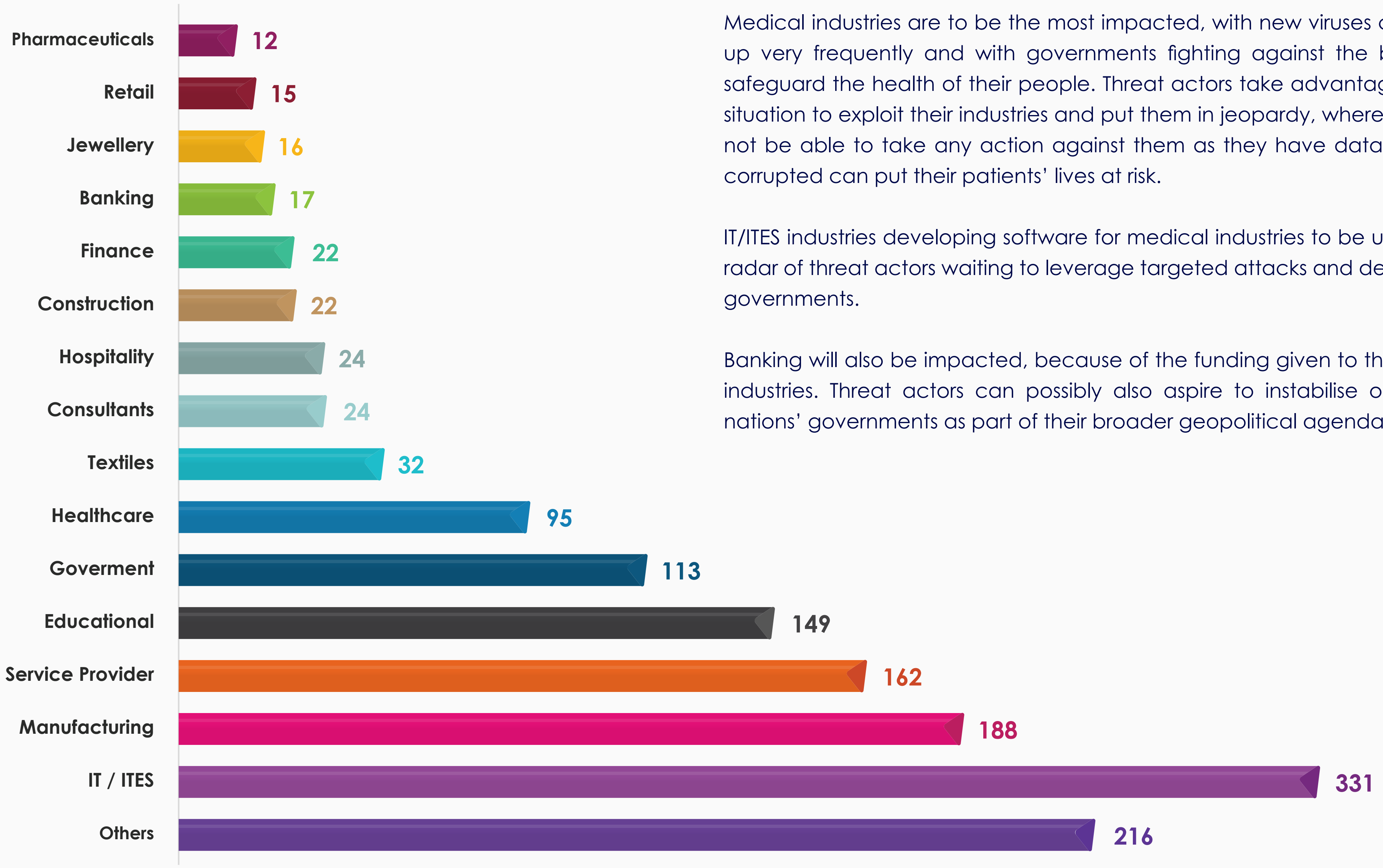


Top Infection Rates in Tier-2 Cities

The surge in cyberattacks on Tier-2 cities over recent quarters highlights a growing concern fueled by rapid economic growth, comparatively lower digital literacy, and weaker cybersecurity infrastructure. MSMEs in these regions remain prime targets, facing ransomware, phishing scams, and malicious campaigns that exploit systemic vulnerabilities. This trend signals a red alert, underscoring the urgent need for robust cybersecurity measures to protect emerging digital hubs from escalating threats.



VULNERABILITIES - WORLD AND DOMESTIC



Medical industries are to be the most impacted, with new viruses cropping up very frequently and with governments fighting against the battle to safeguard the health of their people. Threat actors take advantage of this situation to exploit their industries and put them in jeopardy, where they will not be able to take any action against them as they have data which if corrupted can put their patients' lives at risk.

IT/ITES industries developing software for medical industries to be under the radar of threat actors waiting to leverage targeted attacks and demoralize governments.

Banking will also be impacted, because of the funding given to the above industries. Threat actors can possibly also aspire to instabilise opponent nations' governments as part of their broader geopolitical agenda.

OUR VERDICT

The evolving threat landscape underscores the urgent need for organisations to bolster their cybersecurity defences against increasingly sophisticated adversaries. Ransomware, once a sporadic inconvenience, has transformed into a pervasive menace orchestrated by well-funded and highly organised criminal syndicates. These groups operate with startling efficiency, employing tactics that mimic legitimate business strategies, including targeted victim profiles, recruitment strategies, and even customer support for victims.

The shift in focus to critical sectors, such as healthcare, highlights the alarming erosion of ethical boundaries among cybercriminals. Simultaneously, the surge in phishing as a primary attack vector underscores its effectiveness in exploiting human vulnerabilities, making it a consistent entry point for adversaries. Small and medium-sized businesses, with their limited resources and expertise, remain particularly susceptible to these threats, often serving as gateways to larger networks. Meanwhile, enterprises face more complex challenges, from sophisticated attacks targeting high-value individuals to vulnerabilities stemming from their expansive attack surfaces.

Looking ahead, the threat landscape is likely to further diversify, with adversaries leveraging advancements in artificial intelligence, automation, and deepfake technologies to amplify their attacks. Organisations must adopt a proactive, industry-specific approach to cybersecurity, tailoring defences to their unique risk profiles. This includes investing in threat intelligence, fostering a culture of security awareness, and collaborating across sectors to share insights and bolster collective resilience.

Ultimately, the responsibility to combat these threats lies with all stakeholders—businesses, governments, and individuals. By understanding the evolving tactics of cybercriminals and adopting a unified defense strategy, we can mitigate risks and build a safer digital future.

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 modern enterprises, 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

Q3_2024-25

K7 SECURITY

www.k7computing.com