K7 SECURITY

www.k7computing.com

ESCALATING CYBER WARFARE AMIDST GROWING POLITICAL CONFLICTS

The escalating political tensions across the globe aren't just a backdrop; they're a direct catalyst for a dangerous surge in cyber warfare. From the simmering conflict between Iran and Israel, marked by attacks on financial institutions, critical infrastructure, and the widespread use of disinformation, to the ongoing kinetic and cyber conflict between Russia and Ukraine, where wiper malware, DDoS attacks, and supply chain disruptions have become commonplace, and the persistent cyber skirmishes in the India-Pakistan dynamic, often characterized by website defacements, data breaches, and sophisticated phishing campaigns targeting government and defense entities, threat actors find this an unparalleled advantage. This will eventually lead to a breach of trust among nations, disturbing their entire ecosystem. Any peace talks among nations will eventually become void, as threat actors have taken advantage of geopolitical tensions.

The involvement of state-sponsored threat actors extends beyond these direct confrontations, creating a complex web of digital aggression. These interconnected operations mean enterprises are no longer insulated; they are increasingly finding themselves in the crosshairs, facing significant operational disruptions, data breaches, reputational damage, and the daunting challenge of attributing complex attacks amidst a fog of war.

Nations all over the world should stand together to fight against this ever-growing threat, showing no respite. Threat actors might not only do targeted attacks affecting enterprises and government industries, focusing on monetary benefits alone, but may also launch attacks on the entire nation to disrupt its economy.

All nations should focus on what is important rather than petty politics and should work together to address this ever-growing, alarming conflict. In such a tense scenario, threats could even span across supply chains, putting the entire world in mayhem.

Back To Contents

INFECTION RATE (IR)

Regardless of its type, a security breach is something to be concerned about in every aspect of our digital lives. And that's precisely what our infection rate indices indicate.

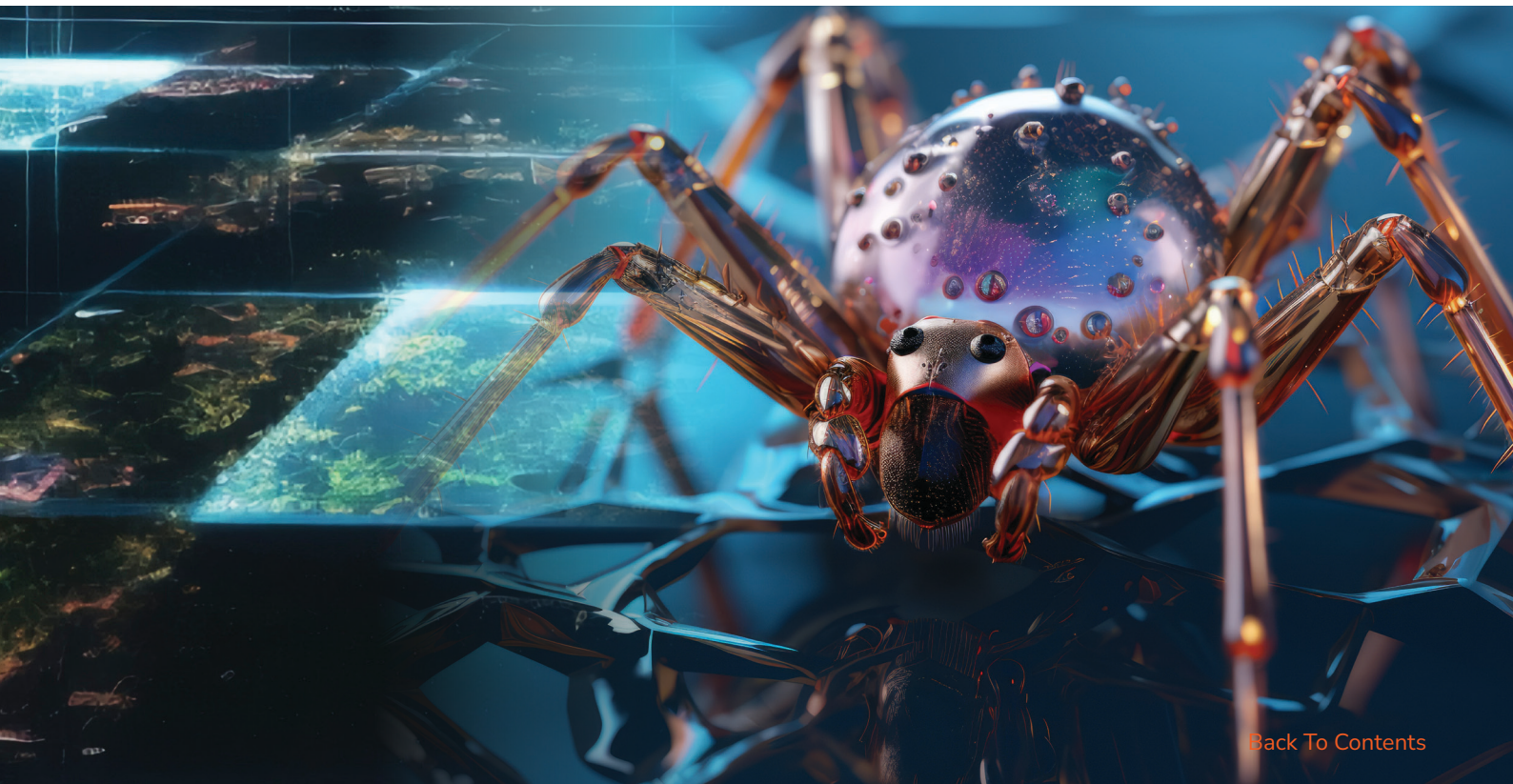
Those new to our quarterly report need to understand an important concept called "Infection Rate" (IR), which is used as the base for benchmarking cybersecurity risk for enterprises and netizens.

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

Infection Rate (IR) of an area



Back To Contents

GEOPOLITICAL FLASHPOINTS AND INDIA'S EVOLVING CYBER THREAT LANDSCAPE

The Pahalgam terror attack on April 22, 2025, and India's subsequent Operation Sindoor didn't just escalate ground conflict; it instantly ignited an unprecedented wave of cyber warfare. This period cemented cyberspace as a direct extension of geopolitical strife, with a dramatic surge in digital offensives targeting India's critical infrastructure.

Digital Attacks and Vulnerabilities

These attacks varied widely, from symbolic website defacements of defense portals to disruptive Distributed Denial of Service (DDoS) assaults on entities like Indian Railways. A major threat was malware infiltration, specifically Pakistan-based APT-36 deploying Crimson RAT against Indian government and defense personnel via phishing emails. Data exfiltration, ransomware, and destructive wiper malware also saw heightened prevalence, underscoring their severe potential impact during such flashpoints. Importantly, our indigenous K7 firewall rules have blocked such attacks, securing all our customers, including both enterprises and consumers.

Back To Contents

Post-Conflict Cyber Attack Typology (Operation Sindoor Context)

Attack Type	Primary Impact	Observed in Operation Sindoor	General Geopolitical Context Examples	Associated Actors
DDoS	Service Disruption	Yes (Telecom)	Russia-Ukraine, Iran-US/Israel	State-sponsored, Hacktivist
Defacement	Reputation Damage, Propaganda	Yes (Education Portals)	Estonia (2007), Iran-Israel	Hacktivist, State-sponsored
Credential Phishing/Theft	Data Theft, Initial Access	Yes (Healthcare)	DNC (2016), RSA Security (2011)	State-sponsored, Cybercriminal
Wiper Malware	Data Destruction, Disruption	Ares RAT deployed	Ukraine (HermeticWiper), Iran (Shamoon)	State-sponsored, Hacktivist

Initial vectors often exploited human vulnerabilities through deceptive phishing emails. The widespread presence of unpatched infrastructure in sectors like healthcare and manufacturing, along with compromised third-party vendors, created fertile ground for exploitation, introducing significant supply chain vulnerabilities.

Initial Attack Vectors and Strategic Goals (Operation Sindoor Context)

Initial Attack Vector	How it Works (Brief Description)	Strategic Goals Served	Common Actors	Relevance to Operation Sindoor
Spear Phishing	Targeted emails with malicious attachments/links	Espionage, Credential Theft, Initial Access, Disruption	State-sponsored, Cybercriminal	Primary vector, disguised as advisories
Exploiting Unpatched CVEs	Leveraging known software flaws for unauthorized access	Espionage, Initial Access, Disruption	State-sponsored, Hacktivist	Common in geopolitical conflicts, likely present
Watering Hole Attacks	Compromising trusted websites frequently visited by targets	Espionage, Data Theft, Initial Access	State-sponsored, Cybercriminal	Known state-sponsored technique

Back To Contents

State Actors, Hacktivists, and Blurred Lines

Both state-sponsored groups and nationalistic hacktivists capitalized on these events. State actors orchestrated sophisticated information operations using bot amplification to control public perception. Simultaneously, hacktivist groups, driven by patriotic fervor, launched retaliatory cyberattacks, employing digital operations as asymmetric tools for propaganda and disruption. This surge in nationalistic sentiment across offensive and defensive cyber maneuvers highlights the deep intertwining of digital conflict and national identity, blurring the lines between kinetic and cyber warfare.

Hybrid Warfare: Blurring Lines Between State and Non-State Actors

The Pahalgam incident vividly illustrates the deepening integration of cyber operations into hybrid warfare strategies. This approach seamlessly blends conventional military actions with unconventional tactics, including information manipulation, economic pressure, and cyberattacks. A significant challenge arising from this integration is the increasing difficulty in distinguishing between state-sponsored actors and non-state entities like hacktivist groups. As observed, hacktivists can amplify state-backed campaigns, claiming responsibility for attacks and leaking data, thereby providing plausible deniability for nation-states while maximizing the psychological impact. This strategic ambiguity complicates international response protocols and attribution efforts, making it harder to hold specific entities accountable under traditional international law.

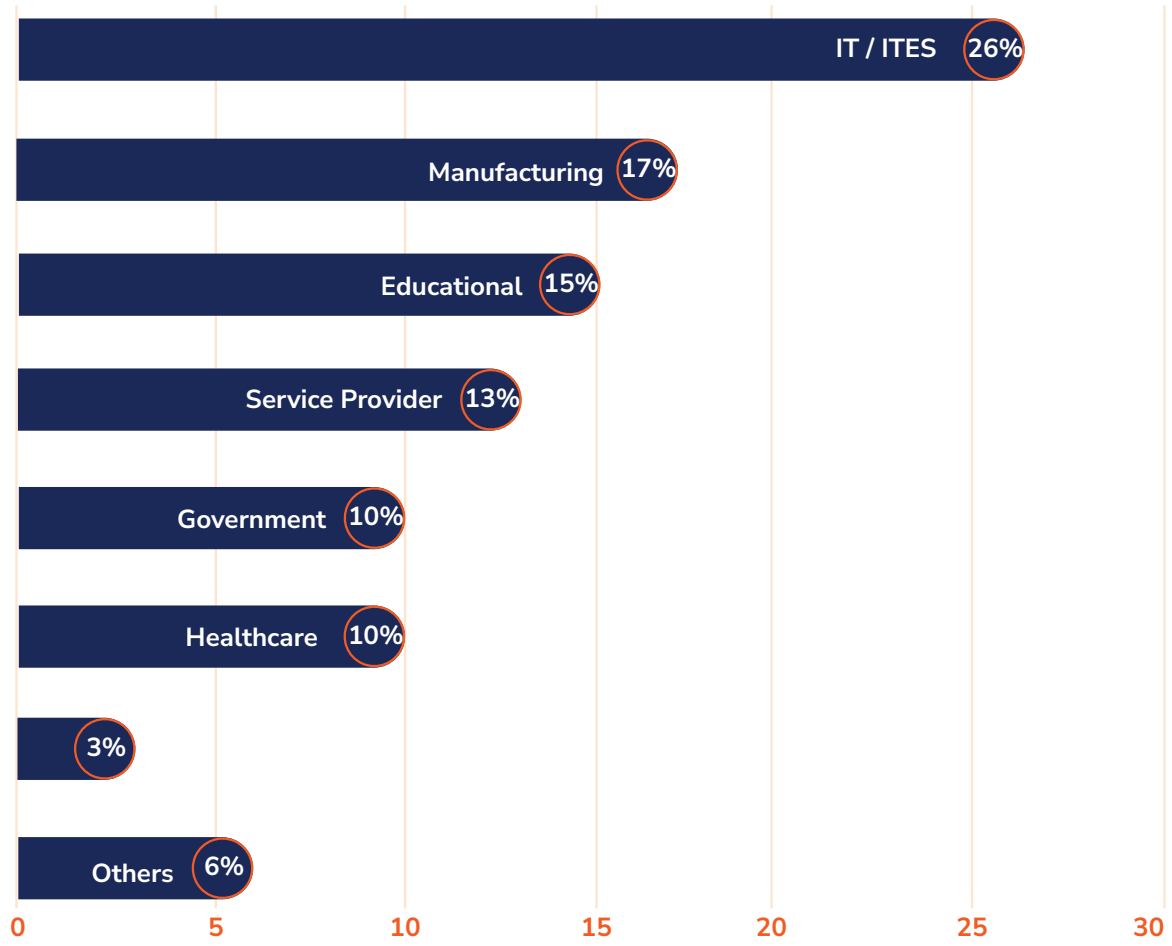
Back To Contents

VULNERABILITIES AND INDUSTRY IMPACT

Understanding prevalent vulnerabilities is crucial in today's dynamic threat landscape. Exploits reveal adversaries' tactics and preferred intrusion vectors. The internet's reach and the dark web's illicit trade in zero-day vulnerabilities empower threat actors to rapidly track and weaponize weaknesses. Some zero-day exploits targeting high-value assets can fetch up to $200,000 on the dark web.

Malware-as-a-Service (MaaS) has commoditized cybercrime, making sophisticated attacks accessible to those with limited technical expertise. This accessibility leaves administrators in a precarious race, as systems are often compromised before critical patches can be applied. The number of discovered software vulnerabilities surged by 61% in 2024, and the number of exploited vulnerabilities nearly doubled, rising by 96% year-over-year. Delving into these vulnerabilities provides vital intelligence on potential attacker targets, enabling proactive defense fortification.

Vulnerability Impact grouped by Industry



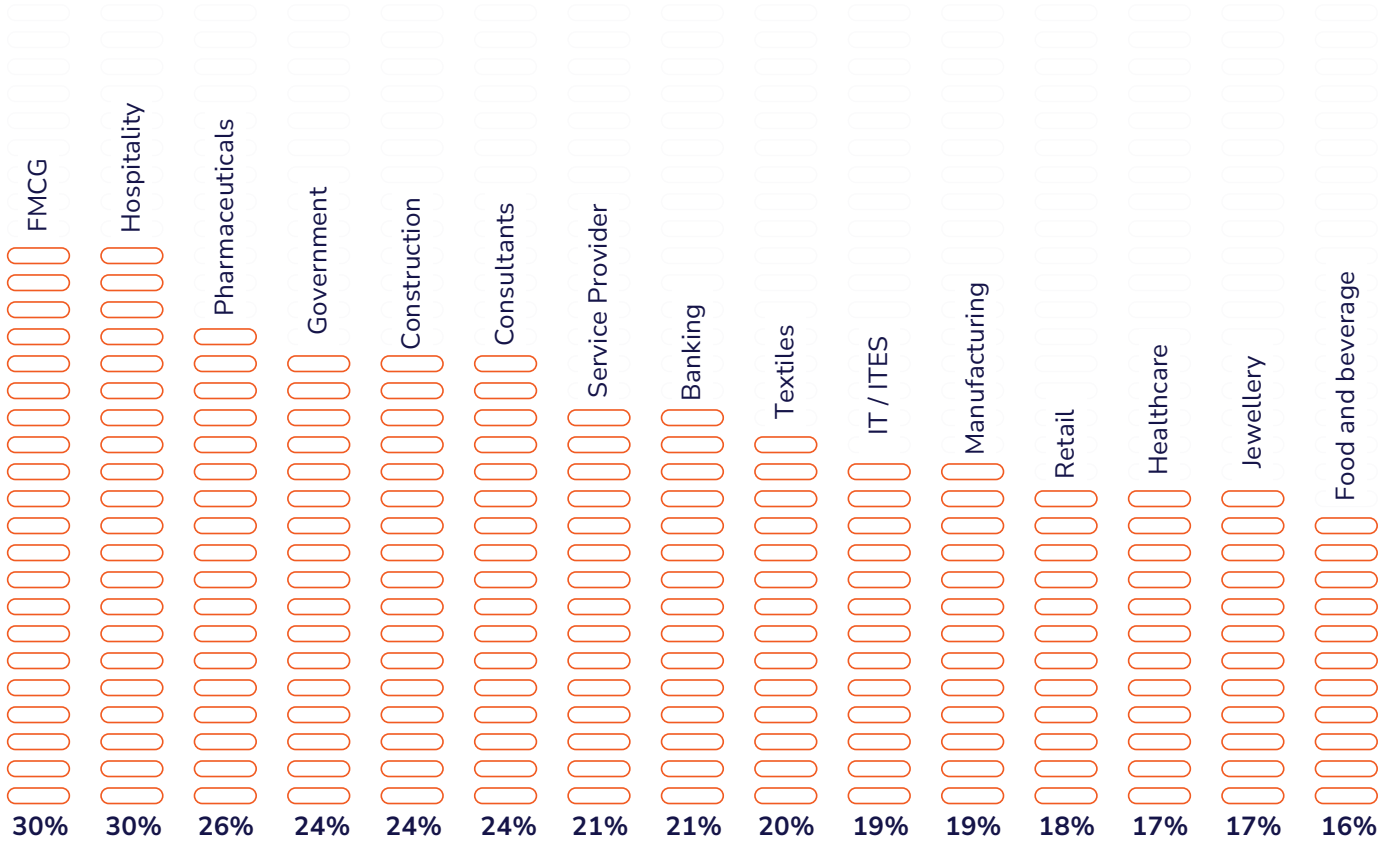
The accompanying chart data clearly indicates that IT/ITES, Manufacturing, Education, and Service Providers experience the highest volume of blocked detections, signifying their prominent position as preferred targets within the current threat landscape. This disproportionate impact implies these sectors are facing a significantly higher frequency of attempted intrusions, reflecting their attractiveness to adversaries due to valuable intellectual property, critical infrastructure, and extensive supply chains.

While numerous vulnerabilities emerged this quarter, our analysis focuses on a select few deemed most critical, demanding immediate attention from readers. These specific flaws represent the most significant intrusion vectors and potential points of compromise for enterprises.

Back To Contents

INDUSTRIES UNDER SIEGE: A SECTOR-BY-SECTOR THREAT PROFILE

Most Impacted Industries around the Globe



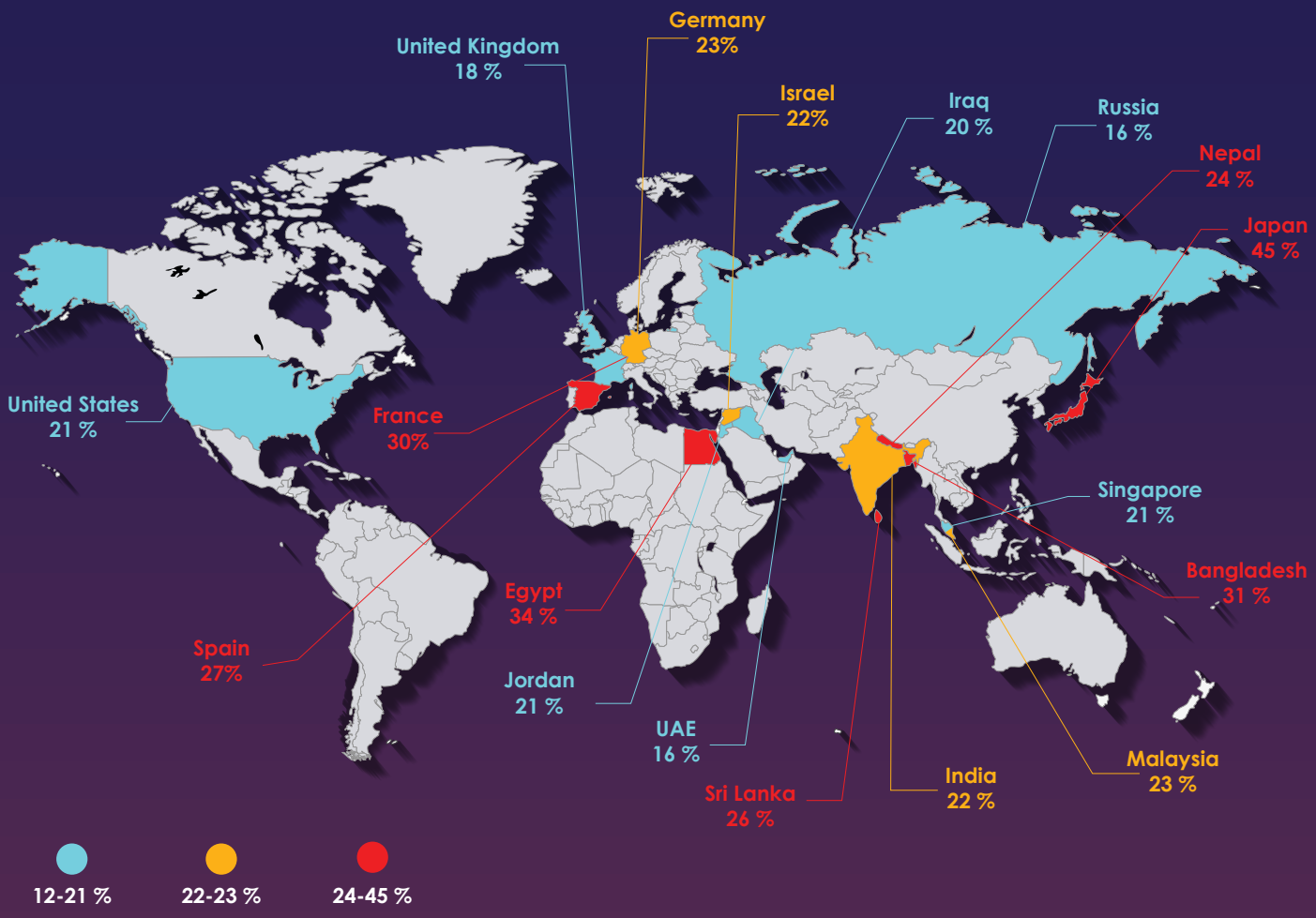
Here's how different industries are bearing the brunt of these sophisticated cyberattacks:

- FMCG & Hospitality (30% Incident Rate):
  - Primary Threat: Disruptive Ransomware attacks.
  - Why Them? Extensive consumer data (including payment information and personal preferences) and deep operational reliance on interconnected systems make them prime targets for widespread disruption.
- Pharmaceuticals & Government Entities:
  - Primary Threats: RATs and persistent Data Exfiltration attempts.
  - Why Them? They hold highly sensitive intellectual property, critical research data, and classified information, making them targets for espionage and strategic, long-term data theft.
- Construction & Consulting (Mid-20s Incident Rate):
  - Primary Threats: Destructive Wiper Attacks and complex Supply Chain Compromises.
  - Why Them? Vulnerable to data eradication (project plans, client data) and ripple effects from compromised vendors within their interconnected supply chains.

Back To Contents

WORLDWIDE CYBER THREAT LANDSCAPE

The global cyber threat landscape is a complex tapestry where geopolitical ambitions clash with pure criminal greed, fueling a relentless surge in malicious activity worldwide. We're witnessing a constant barrage of attacks, from disruptive DDoS and humiliating website defacements to insidious data exfiltration, crippling ransomware, and destructive wiper malware. The initial attack vectors often exploit human frailties through sophisticated phishing emails or leverage unpatched infrastructure, particularly in nations like India, alongside supply chain compromises targeting third-party vendors.

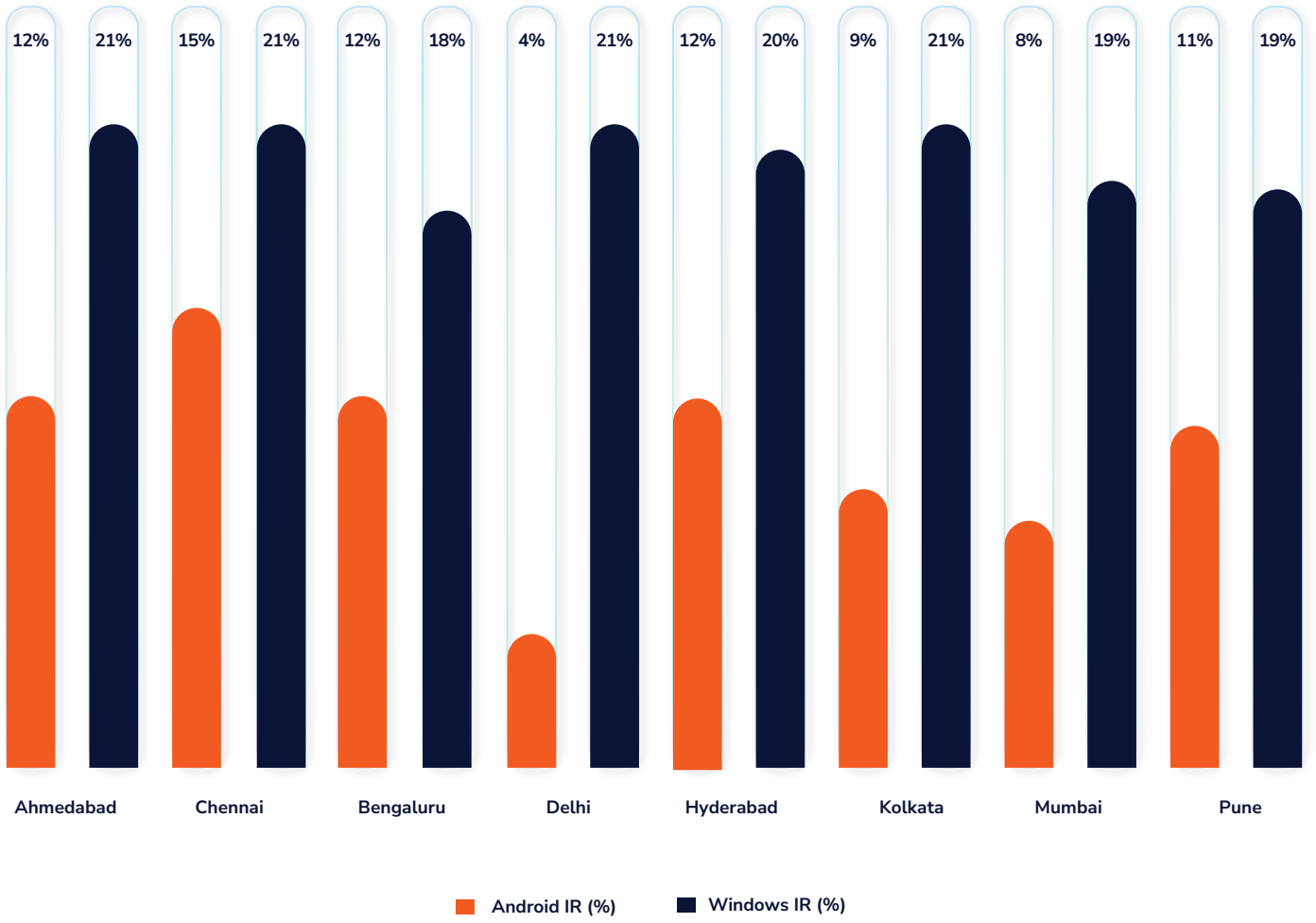


Both state-sponsored actors and ideologically driven hacktivist groups adeptly capitalize on these breaches. They wield cyber operations as potent, asymmetric tools for retaliation or propaganda. Their targets are broad, encompassing critical public sector entities, such as defense ministries, government portals, and essential utilities, as well as vital private enterprises, including banks, telecommunications providers, and critical manufacturing facilities. This escalating digital conflict has a profound impact on businesses globally, demanding an adaptive, resilient, and proactive defense posture against an ever-evolving and increasingly audacious adversary.

Back To Contents

WINDOWS THREAT LANDSCAPE

The Windows operating system remains an undeniable epicenter of cyber threats, consistently exhibiting higher visibility due primarily to its unparalleled global market share and historical entrenchment within both enterprise and consumer environments. Its pervasive adoption makes it the prime, preferred platform for threat actors seeking maximum impact and broader reach for their illicit operations. While other platforms, notably Android, are indeed experiencing a surge in malicious activity for various reasons, Windows continues to bear the undeniable brunt of sophisticated attacks.



Our incident response data across Indian cities vividly illustrates this stark disparity, with Windows consistently showing significantly higher threat visibility compared to Android. This enduring preference by adversaries underscores Windows' critical and pivotal role in the evolving global threat landscape, demanding continuous vigilance, the implementation of robust, proactive security measures, and the deployment of advanced defensive strategies to counteract persistent and ever-evolving threats.

Back To Contents

TOP MALWARE TARGETING WINDOWS SYSTEMS

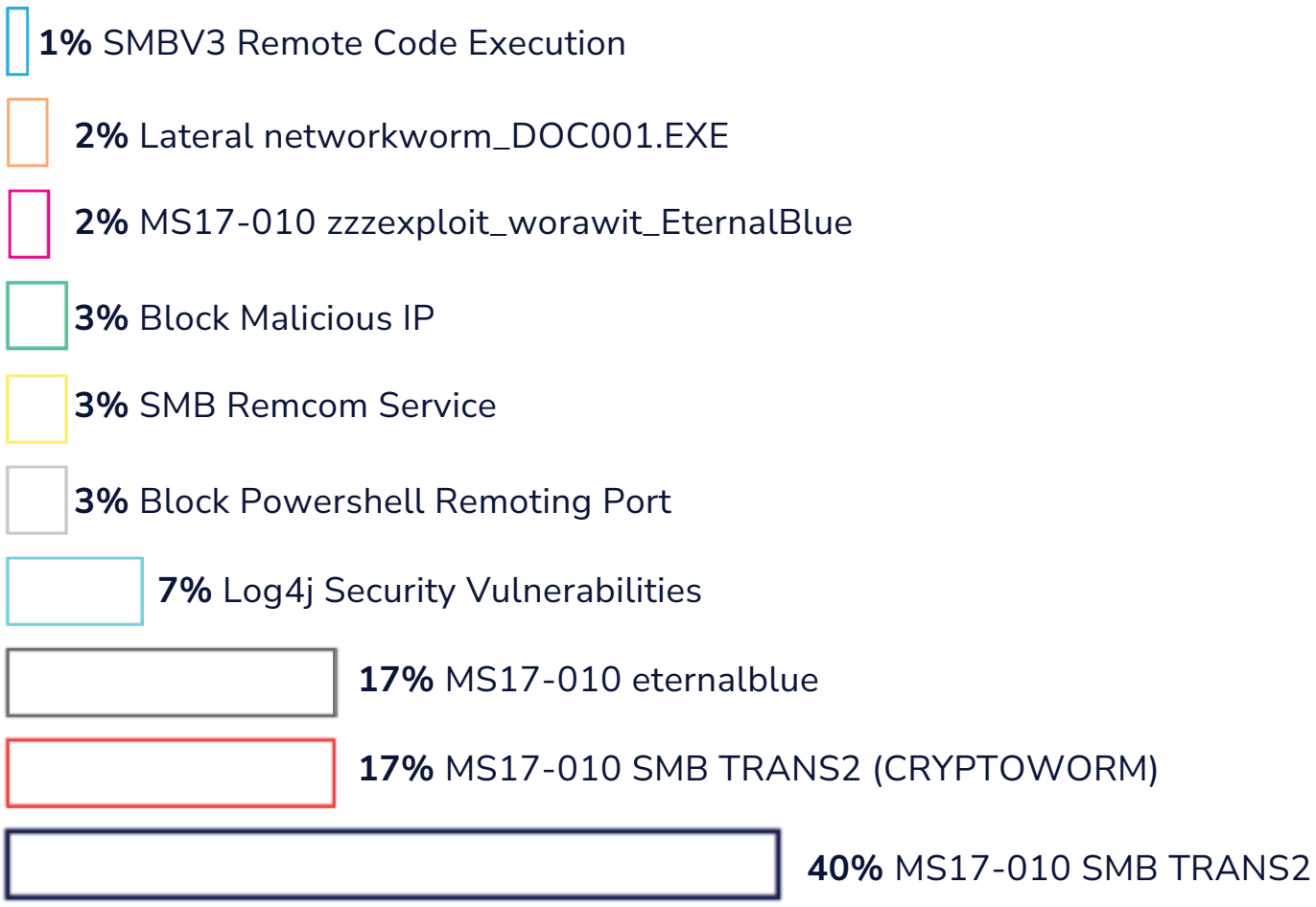
Our quarterly findings for Windows environments reveal a persistent and concerning landscape dominated by adware variants, indicating the enduring challenge of unwanted software.

Adw.Win32.Cpp alone comprises over a quarter of all detections, highlighting its pervasive nature.

Equally significant is the consistent presence of hacking tools, particularly those linked to unauthorized user creation and system activation. This signals a clear intent by adversaries for persistent access and potential privilege escalation within compromised systems. This dual threat underscores how attackers effectively leverage both nuisance-ware and more direct compromise tools to maintain crucial footholds and achieve their objectives within Windows environments.

Back To Contents

UNPATCHED VULNERABILITIES: THE ACHILLES' HEEL OF WINDOWS SYSTEMS



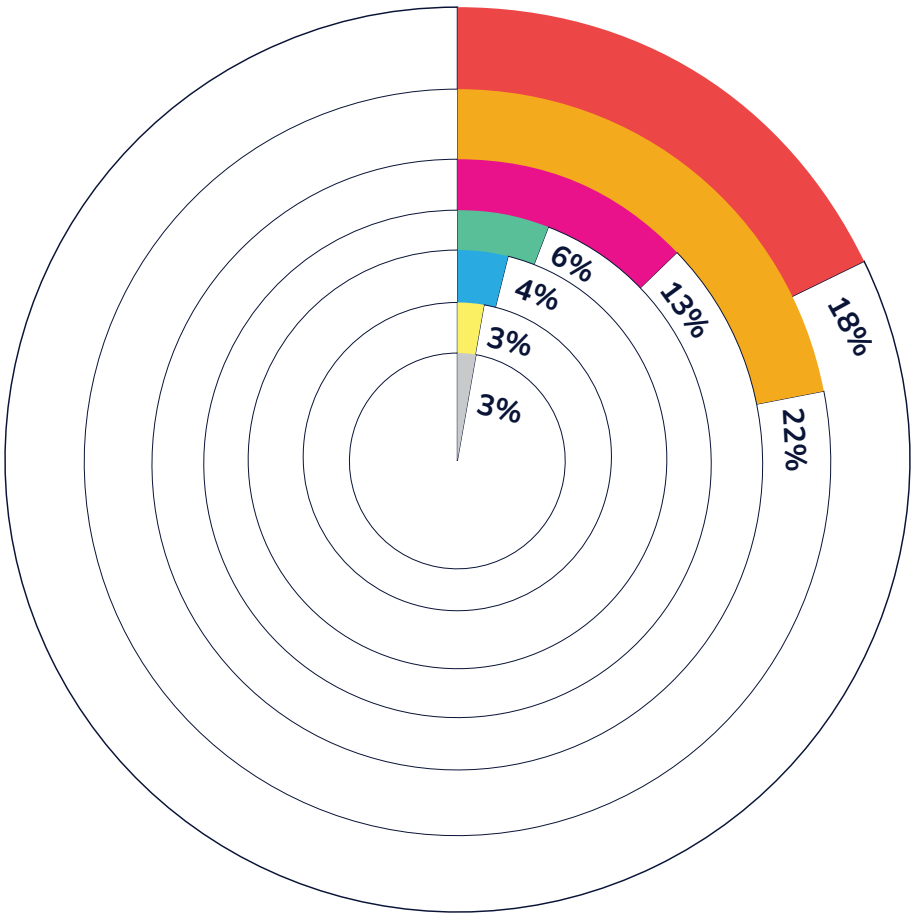
Our quarterly analysis reveals that legacy exploits, primarily MS17-010 SMB Trans2 variants, still dominate, accounting for a staggering 76% of all exploit detections. This persistent "EternalBlue" vulnerability highlights a critical failure in patching, leaving numerous systems exposed to severe remote code execution. Additionally, the emergence of Log4j Security Vulnerabilities at 7% underscores the enduring threat from supply chain weaknesses. These findings emphasize that fundamental patching hygiene remains paramount, as unaddressed vulnerabilities continue to enable widespread compromise.

Back To Contents

HEURISTIC HOST INTRUSION PREVENTION SYSTEM (HIPS)

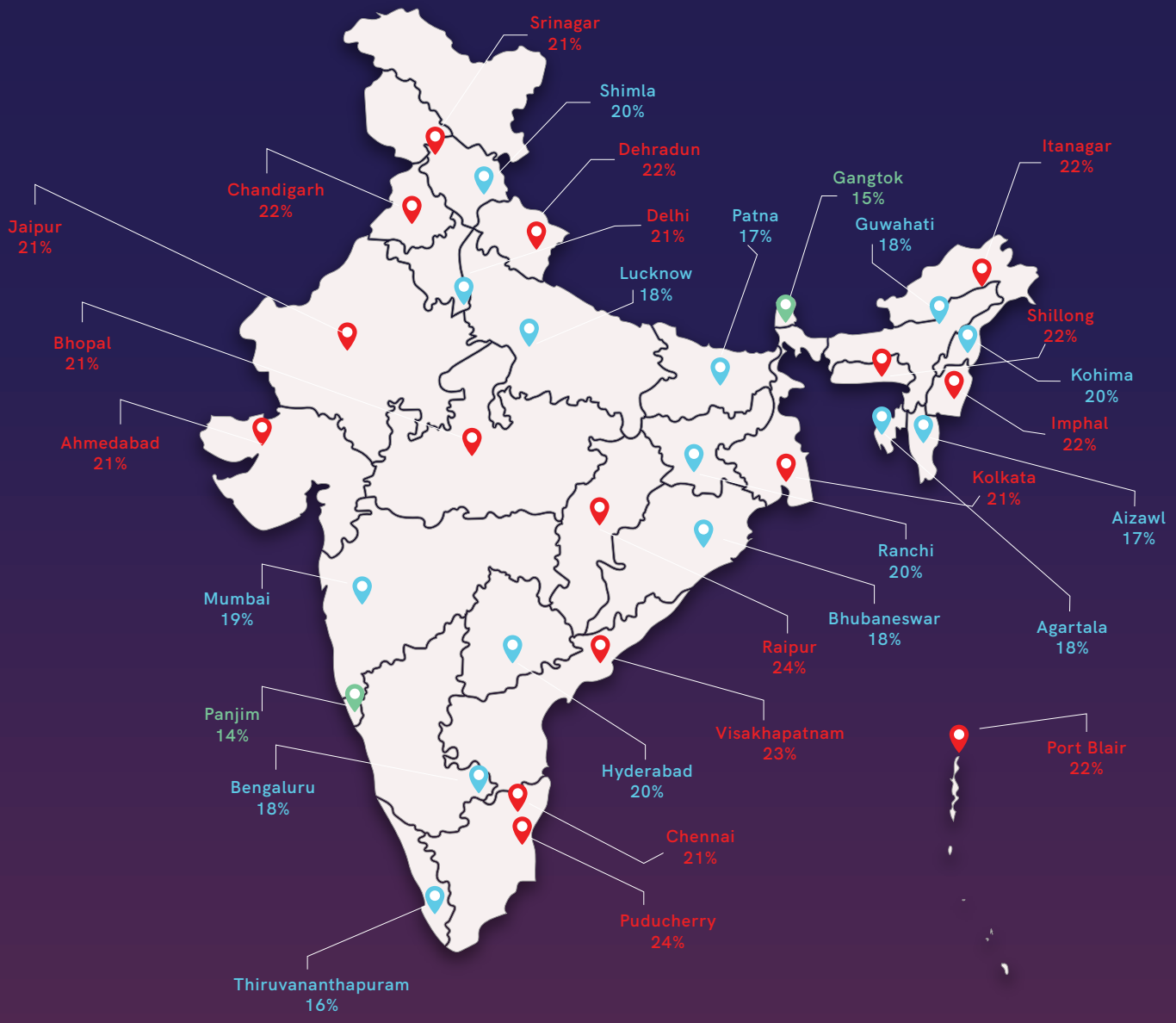
Our Heuristic HIPS detections offer crucial insights into adversary tactics, revealing a strong preference for “living-off-the-land” attacks. Susp_Reg_Mod (22%) and Susp_Powershell (18%) dominate, indicating attackers’ focus on registry modifications for persistence and PowerShell for execution. Susp_dropper (13%) further highlights attempts to deploy secondary payloads, often bypassing traditional defenses. These alerts collectively underscore active post-exploitation maneuvers, making behavioral monitoring indispensable for early threat detection.

Windows Heuristic Behavioural Detection



Back To Contents

CYBER THREAT LANDSCAPE - INDIA



- 11%- 15%
- 16%- 20%
- 21%- 25%

Map for illustrative purposes only. Not to scale.

Back To Contents

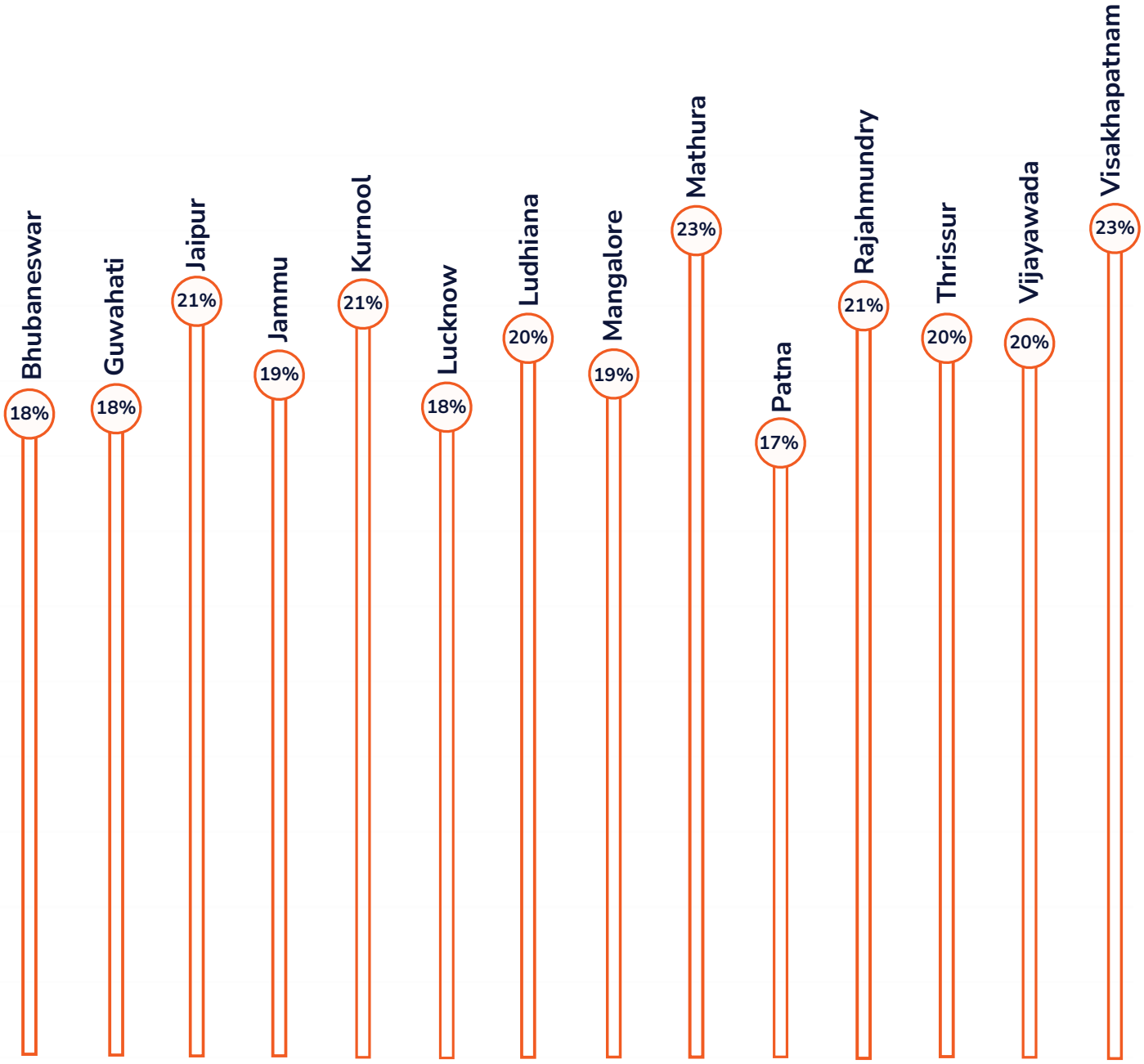
THE METRO AND TIER-1 CITIES - INFECTION RATE

Across major Indian cities, our detection data consistently reveals that signature-based defenses, particularly ScanEngineProtection, remain the undeniable frontline, identifying over 80% of threats. This overwhelming dominance primarily reflects the sheer volume of known malware circulating.

However, the comparatively lower figures for BehaviourProtection and FirewallProtection signal a critical vulnerability. It underscores an urgent need to significantly bolster proactive, anomaly-based detection and robust network-level threat mitigation. As the threat landscape becomes increasingly sophisticated, with novel and evasive attacks, relying solely on signature-based methods could prove insufficient, necessitating a more comprehensive and adaptive security posture.

Back To Contents

TOP INFECTION RATES IN TIER-2 CITIES



Back To Contents

ENTERPRISE INSECURITY

Malicious third-party software impacting Microsoft's integrity

Third-party software downloaded from dubious sources is one of the attack vectors used by ransomware operators. Improper cyber-hygiene practices at workplaces add to the success of these malicious operators. It is crucial that administrators be aware of such applications that are distributed on dubious sites and ensure those applications and sites are blacklisted.

One of our Enterprise customers became infected with ransomware after downloading KMSAuto from dubious sources. The following is the kill chain:

Step 1

Risky Download, Hidden Threat

Customers download KMSAuto from dubious sources and install it in multiple systems in the network

Step 2

Tracked, Probed, Exploited

KMSAuto is already a well-known vector for ransomware attacks. Attackers track the installation of KMSAuto in the customer system and probe it for vulnerabilities and exploitable services

Step 3

Foothold, Then Scan

Attackers gain a foothold in the customer network and scan the systems in the network

Step 4

Critical Systems Encrypted

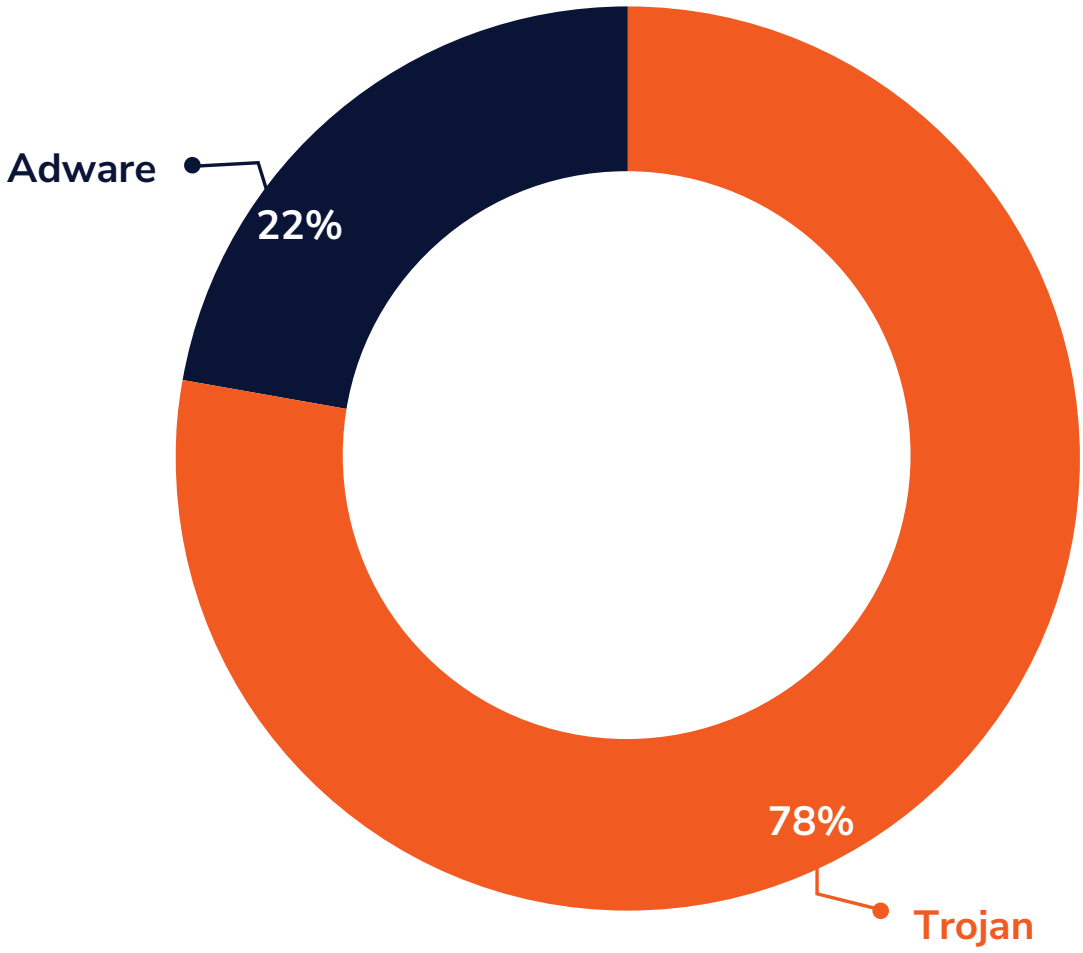
Attackers identify and enumerate critical systems and execute ransomware in those systems, thereby encrypting all the files

Back To Contents

THE MOBILE DEVICE STORY: A SHIFTING PARADIGM

The Android threat landscape is rapidly evolving, posing a more complex challenge for users and organizations alike. We're seeing a surge in new and refurbished attack vectors designed to circumvent traditional security measures. Attackers are now primarily targeting enterprise employees to infiltrate corporate networks and steal data. However, they still target individual users with poor cyber hygiene for direct financial gain or data harvesting.

Adware vs Trojan Proportional Split



Our recent detections reveal a significant surge in Trojan variants, which now account for a substantial 78% of all Android threats. Despite this dominance, adware remains prevalent, accounting for 22% of the threat landscape, underscoring its enduring nuisance.

Back To Contents

CASE STUDY 1: SPYWARE - A PERVASIVE THREAT DISTURBING MOBILE SECURITY

Spyware remains the most prevalent threat to the security of mobile devices. This is primarily due to the difficulty in identifying if someone is spying on you, irrespective of whether you are a top-notch security professional or a layperson.

K7 Labs dissects spyware disguised as a fake government app with a similar name, "PM KISAN YOJNA," designed to provide help for Indian citizens.
The kill chain is as follows:

01

Multi-stage malformed dropper technique was used as the payload, for bypassing static analysis

02

Permissions were requested to gain access to install apps without victims' knowledge

03

Steals sensitive information about the victims'

Back To Contents

CASE STUDY 2: FAKE WEDDING INVITATION APP CAUSING MAYHEM

Another spyware, disguised as a fake wedding invitation app, is being used to steal sensitive information from victims by targeting mobile users' contact lists. The malware is named SpyMax, a Remote Administration Tool (RAT).

01

Phishing campaign targeting Indian mobile users in the name of "Wedding Invitation" coming from one of their contacts in WhatsApp

02

On successful installation, it opens a fake Google Play Service to gain full control of the victims' device

03

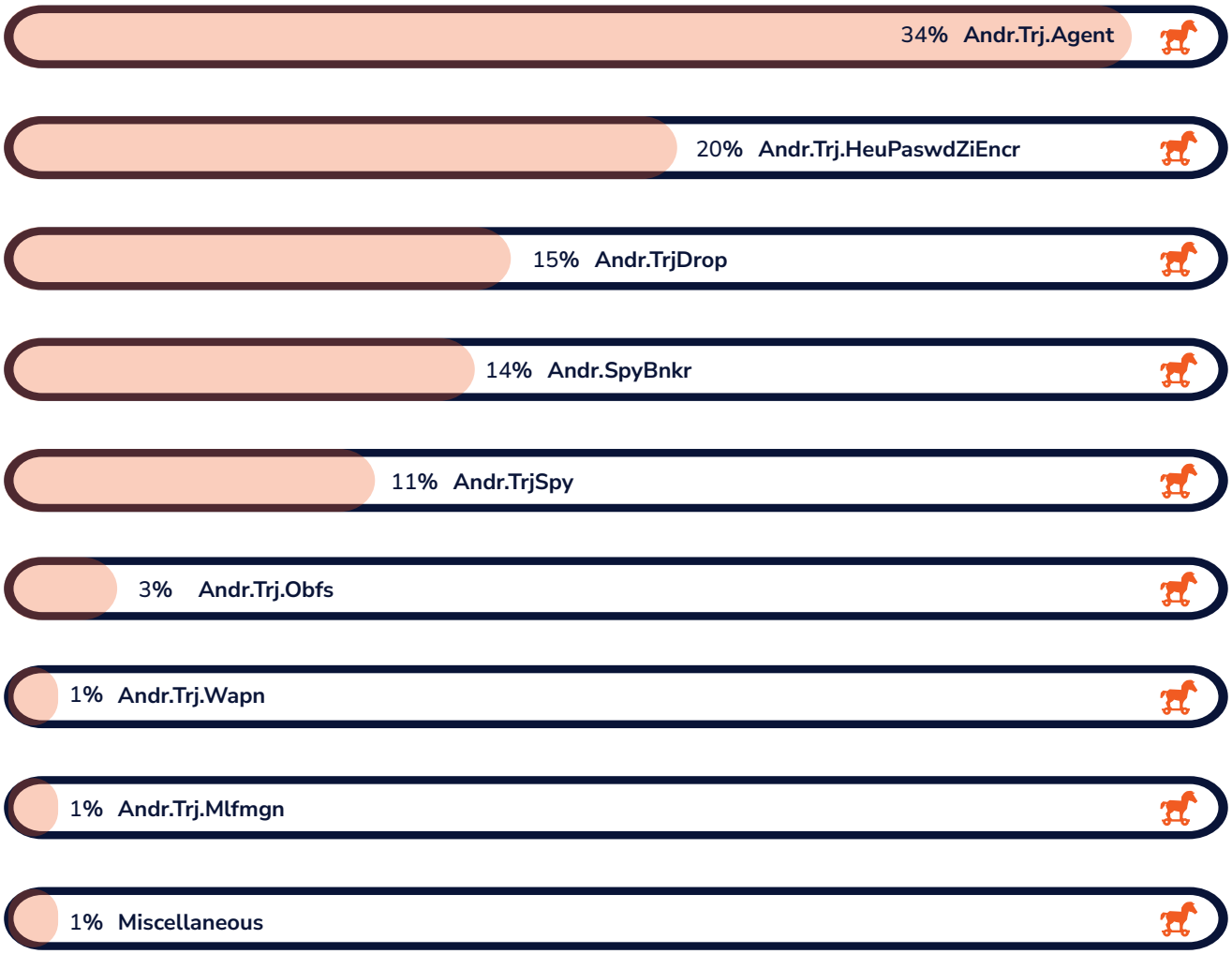
Steals sensitive information from victims' device

Back To Contents

TROJAN TAKEOVER LOOMS

Three Trojan variants are currently dominating the Android threat landscape. Andr.Trj.Agent (34% of detections) primarily functions as a “dropper,” capable of installing additional, more dangerous malware, such as rootkits, and initiating complex, multi-stage attacks.

The Wicked Trendline of Trojans

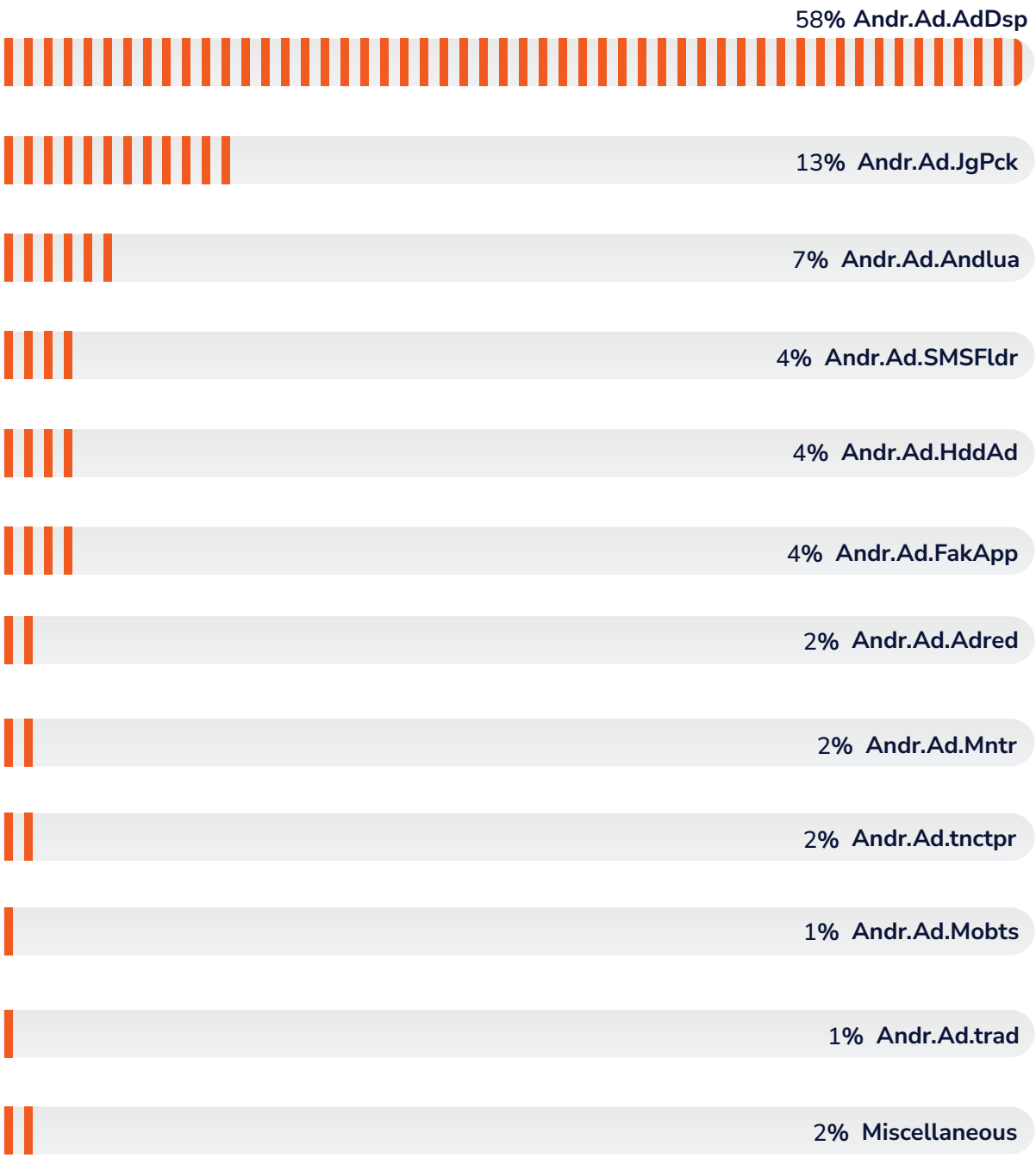


Andr.Trj.HeuPaswdZiEncr (20% of detections) is a sophisticated threat designed to steal sensitive user credentials, often employing obfuscation to evade detection during data exfiltration. Lastly, Andr.TrjDrop (15% of detections), another notable dropper, plays a crucial role in delivering diverse malware families, ensuring a constant and varied influx of threats to compromised devices.

Back To Contents

THE COLOSSAL ROLE OF ADWARE

Most Prevalent Adware Types



While Trojans currently dominate, adware presents a distinct and evolving challenge:

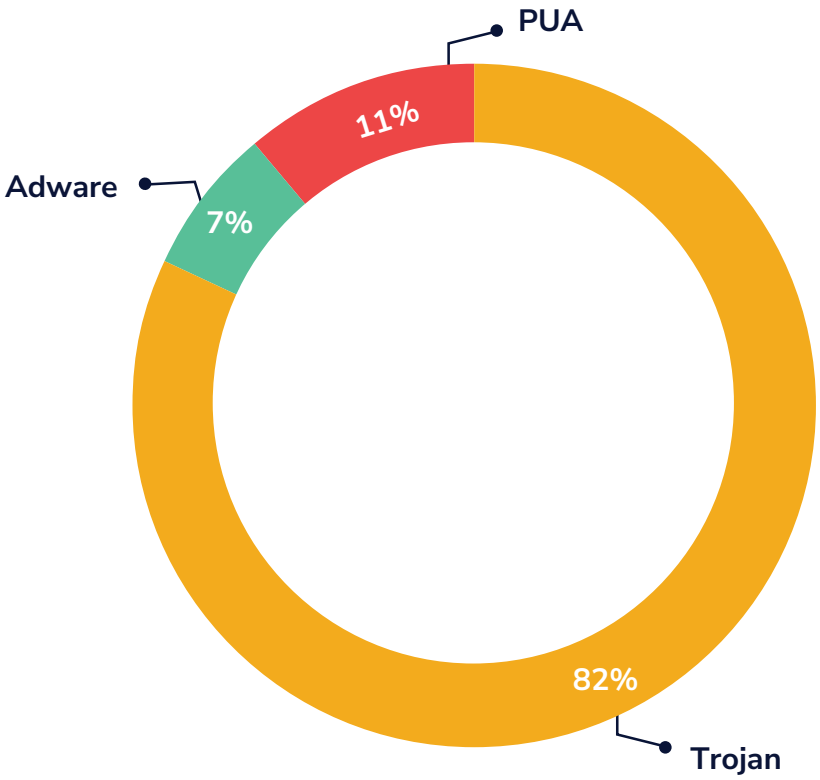
- Adware as a Precursor: The prominence of Andr.Ad.AdDsp suggests adware is increasingly a foundational layer, potentially enabling more complex, multi-stage attacks beyond simple monetization.
- Blurred Distribution Lines: Andr.Ad.JgPck indicates adware's infiltration through seemingly legitimate channels, making detection and differentiation significantly harder for users.
- Evolving Capabilities: The emergence of Andr.Ad.Andlua highlights adware's progression to include advanced functionalities like data collection, signaling a shift towards more versatile and insidious threats.

Back To Contents

THE MAC ATTACK

The macOS threat landscape, once considered a sanctuary, is rapidly transforming into a complex and concerning battleground. Cyber adversaries are relentlessly sharpening their techniques, unleashing sophisticated malware engineered to bypass even Apple's robust security measures. This significant shift is largely fueled by the increasing adoption of macOS within enterprise environments, making these systems lucrative targets for attackers aiming to seize high-value data and gain network access. While familiar threats persist, the current climate demands a heightened vigilance against novel and highly targeted campaigns.

Trojan, Adware and PUP proportional Split

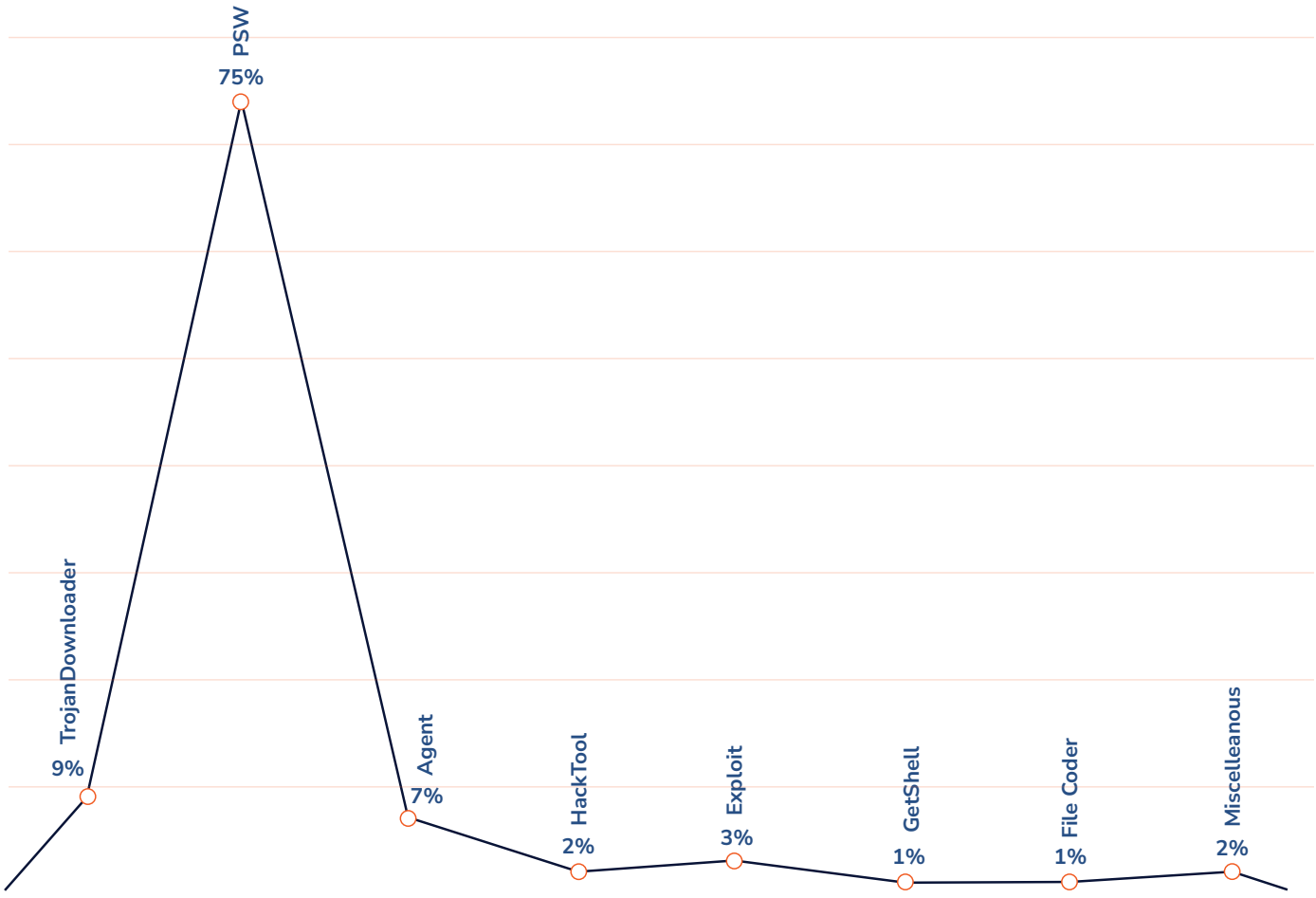


Our recent analysis of detections vividly illustrates this evolving threat profile, revealing a pronounced dominance of Trojan activity. As shown in the accompanying pie chart, Trojans now account for a staggering 82% of all identified macOS threats, cementing their role as the primary weapon in malicious campaigns. Despite this overwhelming surge, Potentially Unwanted Applications (PUA) maintain a notable presence at 11%, often acting as vectors for unwanted software or privacy intrusions. Even traditional adware, though a smaller piece of the pie at 7%, serves as a reminder that seemingly minor annoyances can still signal underlying vulnerabilities.

Back To Contents

THE UBIQUITOUS TROJANS

Trojan Detection Trend Lines



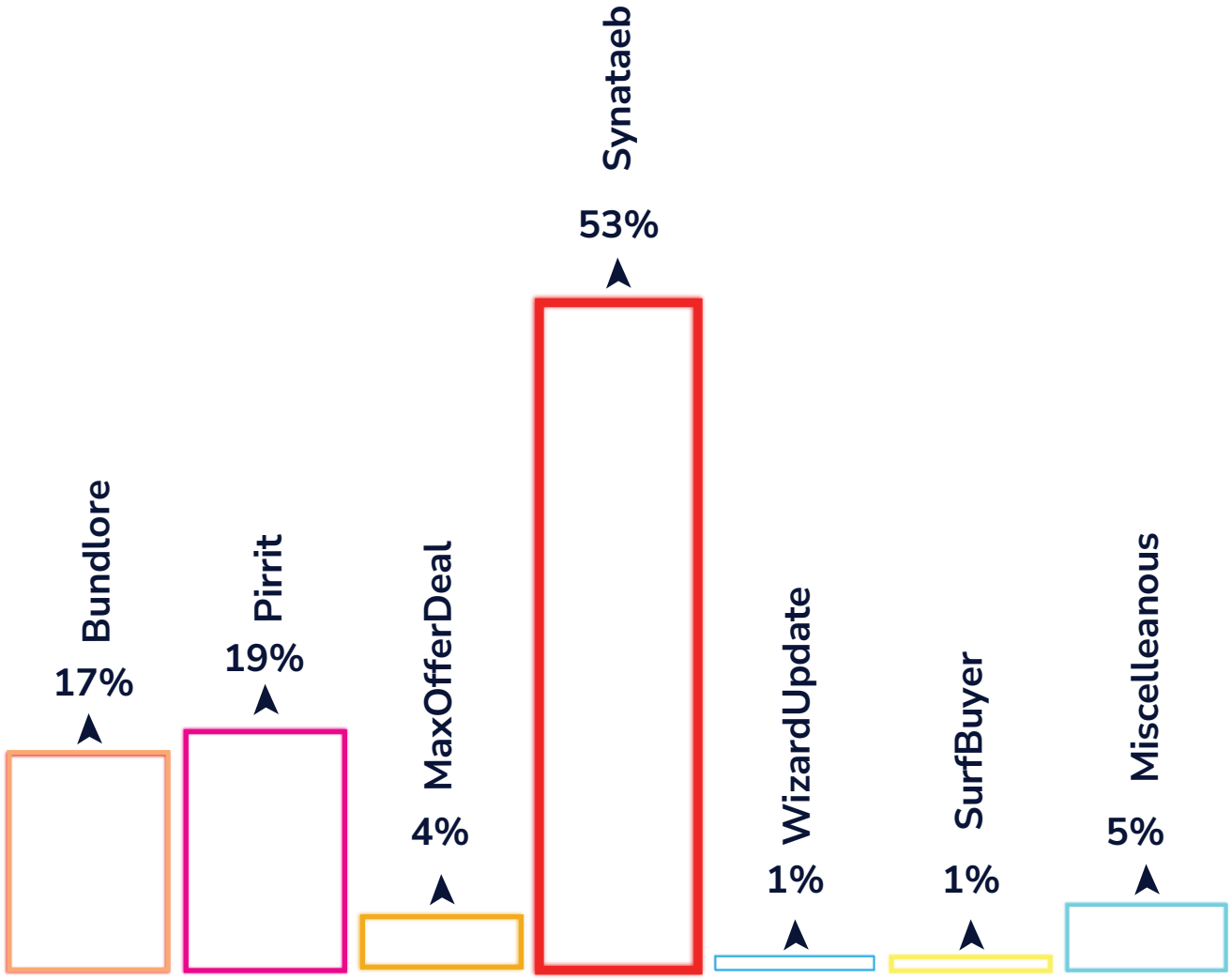
The current macOS Trojan detections offer critical insights into the evolving threat landscape, highlighting three key transformations:

- Dominance of Credential Theft: The overwhelming 75% prevalence of PSW (Password Stealer) Trojans signals a critical shift. Attackers are clearly prioritizing direct credential harvesting to gain unauthorized access to user accounts and sensitive corporate resources, making robust identity and access management paramount for future security.
- Persistent Infiltration and Staging: The significant presence of TrojanDownloader (9%) and Agent (7%) variants underscores a strategic focus on establishing persistent footholds. This indicates that initial compromises are increasingly aimed at building a resilient infrastructure for long-term espionage, data exfiltration, or subsequent malware deployment, rather than immediate, overt impact.
- Multi-faceted Attack Vectors: The combined detections of Exploit (3%) and HackTool (2%) reveal that Trojans are now frequently paired with software vulnerabilities and legitimate system utilities. This points to a future where macOS threats will leverage a more diverse array of techniques, demanding a comprehensive and highly adaptive security posture to defend against these blended attacks.

Back To Contents

THE ADWARE BROUHAHA

The Trend Line of Adware Variant Detections



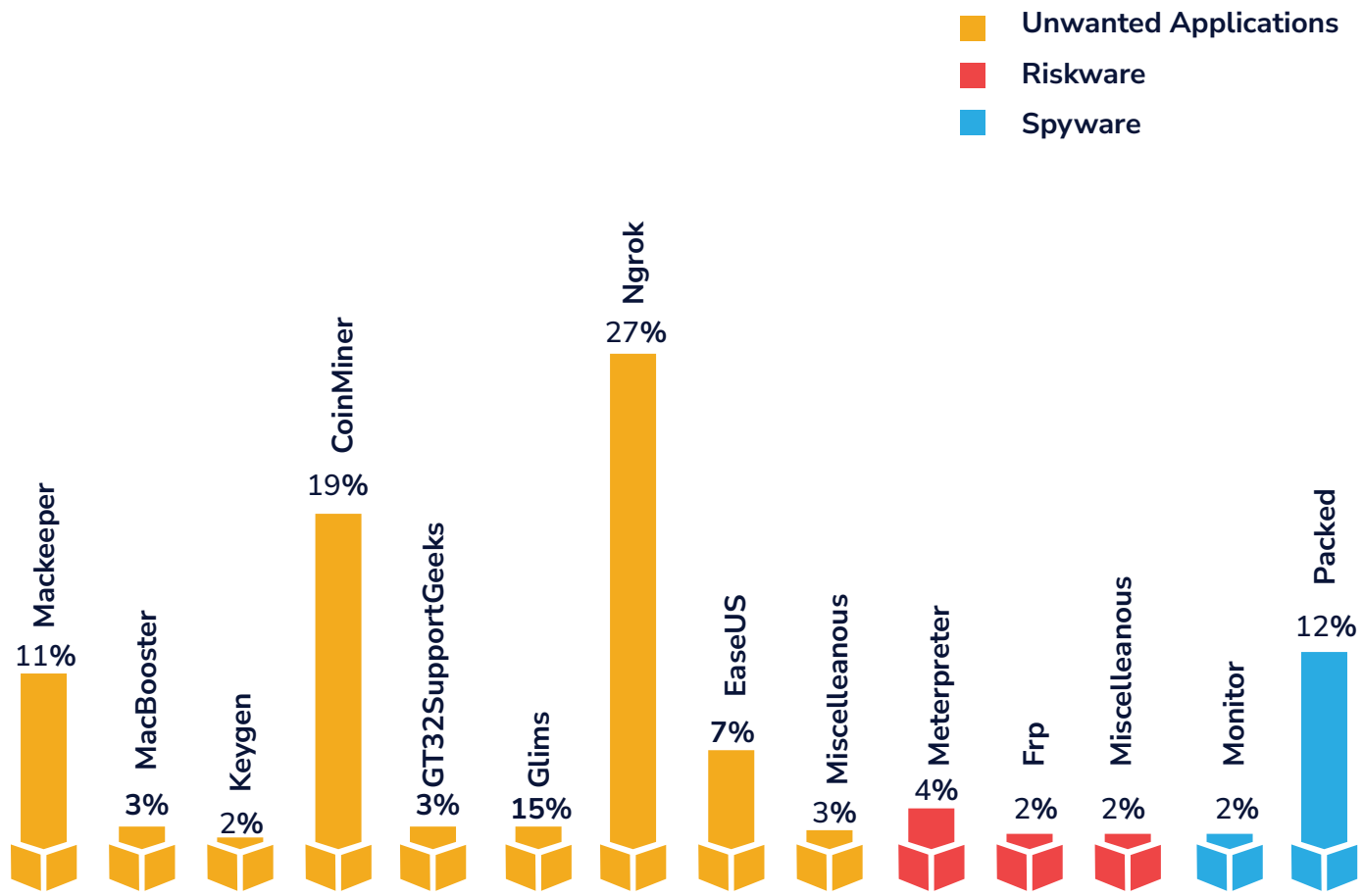
While Trojans currently dominate, macOS adware presents a distinct and evolving challenge, hinting at future transformations:

- Aggressive Browser Manipulation: The overwhelming prevalence of Synataeb (53%) indicates a future where adware isn't just a nuisance; it's a primary tool for aggressively manipulating user browsing sessions, potentially setting the stage for data harvesting or redirection to more malicious content.
- Persistent Bundling Tactics: The significant presence of Pirrit (19%) underscores the enduring effectiveness of aggressive software bundling and intrusive ad injection. This suggests a continued challenge in user awareness and a need for stronger system-level defenses against the proliferation of unwanted programs.
- Entrenched Browser Hijacking: The consistent detection of Bundlore (17%) points to a persistent threat where adware deeply embeds itself by hijacking browser settings and installing unwanted extensions. This implies a future where adware maintains a foothold by altering core browsing experiences, leading to prolonged exposure to compromised content or privacy vulnerabilities.

Back To Contents

THE SHARE OF PUPS

Most Prevalent PUP Types



The PUA category reveals a concerning trend of legitimate tools being weaponized and a growing sophistication in evasion. Ngrok (27%) stands out, signaling a future where seemingly benign tools are increasingly abused to bypass security, essentially opening backdoors for more insidious malicious activity. This is further compounded by the substantial presence of CoinMiner (19%), which points to a rising focus on unauthorized resource hijacking for illicit cryptocurrency mining, silently draining system performance. Finally, the consistent detection of deceptive system optimizers like MacKeeper (11%) and the Packed (12%) nature of some PUAs illustrate a future where these applications are more adept at evading detection and exerting system impact, blurring the lines between merely unwanted and actively harmful software.

Back To Contents

A PEEK INTO A FEW SIGNIFICANT VULNERABILITIES

Here are the critical vulnerabilities demanding immediate notice:

Apache Tomcat Critical Path Equivalence (CVE-2025-24813)

Rated 9.8 CVSS, this flaw in Tomcat's partial PUT requests is actively exploited. It enables remote attackers to execute arbitrary code, disclose sensitive information, or inject malicious content into uploaded files. Immediate patching for versions 11.0.0-M1 through 11.0.2, 10.1.0-M1 through 10.1.34, and 9.0.0-M1 through 9.0.98 is crucial.

- Ref - https://nvd.nist.gov/vuln/detail/CVE-2025-24813

Ivanti Connect Secure/Policy Secure/ZTA Gateways Critical Buffer Overflow (CVE-2025-22457)

This critical stack-based buffer overflow, also rated 9.8 CVSS, is under active exploitation. It allows remote, unauthenticated attackers to execute arbitrary code. Urgent patching is vital for Connect Secure before version 22.7R2.6, Policy Secure before version 22.7R1.4, and ZTA Gateways before version 22.8R2.2.

- Ref - https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

Windows Common Log File System Driver Privilege Escalation(CVE-2025-29824 & CVE-2025-32706)

Two high-severity privilege escalation vulnerabilities, both rated 7.8 on the CVSS scale, are reportedly being exploited in the wild. These flaws (use-after-free and heap-based buffer overflow, respectively) enable a local authorized attacker to gain full system access. Immediate patching across affected Windows 10, 11, and Server versions is critical.

- Ref - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-32706

Windows Desktop Window Manager (DWM) Elevation of Privilege (CVE-2025-30400)

This high-severity use-after-free flaw (CVSS 7.8) in dwmcore.dll is reportedly exploited as a zero-day. It allows an authenticated local attacker to execute arbitrary code with SYSTEM privileges. Immediate patching for affected Windows 10, 11, and Server versions is crucial.

- Ref - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30400

Back To Contents

IOT VULNERABILITIES

Fortinet Product Line Critical Buffer Overflow (CVE-2025-32756)

A CVSS 9.8 critical stack-based buffer overflow was actively exploited across FortiCamera, FortiVoice, FortiRecorder, FortiMail, and FortiNDR. Remote, unauthenticated attackers can execute arbitrary code via malicious hash cookies in HTTP requests. Immediate patching of all affected versions is imperative.

- Ref - https://nvd.nist.gov/vuln/detail/CVE-2025-24813

Samsung MagicINFO Server Critical Path Traversal (CVE-2025-4632)

This 9.8 CVSS critical path traversal flaw is actively exploited in the wild, allowing attackers to write arbitrary files with system-level privileges, potentially leading to complete system compromise. Organizations using MagicINFO 9 Server versions before 21.1052 must apply security updates immediately.

- Ref - https://security.samsungtv.com/securityUpdates#SVP-MAY-2025

Qualcomm Adreno GPU Drivers Use-After-Free (CVE-2025-27038)

A high-severity (CVSS 7.5) use-after-free vulnerability affecting Qualcomm chipsets, specifically Adreno GPU drivers in Chrome. This flaw allows memory corruption and potential arbitrary code execution. Reportedly exploited as a zero-day vulnerability, users are advised to apply the latest updates.

- Ref - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html

Back To Contents

LATEST SECURITY NEWS

This section lists the latest happenings in the cyber world. For more details, please read our blogs on the same.

‘Wedding Invite’s’ Could Be Stealing Your Data

Threat actors are using WhatsApp to spread malware disguised as a digital wedding invite app coming from known contacts to steal sensitive data and further install malicious apps compromising digital safety.

Refer SpyMax for details

Fake government app targeting Android users in India!

This talks about how government schemes meant to help indigenous farmers such as “PM KISAN YOJNA” are being used by cybercriminals to their advantage.

For more details refer Android Spyware Alert

New macOS Stealer Threatens Your Data!

Here, we investigate whether this stealer is a repackaged version of the notorious Atomic macOS Stealer (AMOS) or an entirely new threat.

Refer macOS Stealer for more info

Subscribe to our K7 Labs Technical Blogs to know more about the latest happenings in cybersecurity.

Back To Contents

THE UNSEEN BATTLEFIELD: FORTIFYING OUR DIGITAL SOVEREIGNTY

The digital realm has starkly become a key battleground. Intensifying geopolitical tensions are directly fueling a dangerous surge in cyber warfare, deeply affecting international relations and enterprise security. From financial disruptions to destructive wiper attacks and relentless data breaches, cyber operations are now integral to statecraft, eroding trust and global stability.

Enterprises face unprecedented disruptions. Malware-as-a-Service (MaaS) and a dramatic 61% rise in software vulnerabilities in 2024—with 96% of those exploited—highlight a volatile threat landscape. Our Infection Rate (IR) metric clearly benchmarks this escalating risk.

IT/ITES, Manufacturing, Education, and Service Providers are the most targeted. Windows remains a dominant platform for adversaries, exhibiting significantly higher threat visibility compared to Android. Persistent adware and hacking tools for system access are prevalent, compounded by critical patching failures. Legacy exploits, such as MS17-010 (76% of detections), continue to enable severe remote code execution. Adversaries often leverage living off the land (LOTL) using legitimate tools for stealth.

In India, an over-reliance on signature-based defenses (80% of threat identifications) underscores the urgent need for proactive, anomaly-based detection. Compromises via malicious third-party software also reveal poor cyber hygiene.

The Android threat landscape is rapidly evolving, dominated by Trojans (78%) acting as droppers or credential stealers. macOS faces similar challenges, with Trojans (82%) primarily targeting credential theft and persistent infiltration. Weaponized legitimate tools and cryptocurrency miners further complicate the picture.

Critical, actively exploited vulnerabilities, such as Apache Tomcat (CVE-2025-24813) and Ivanti Connect Secure (CVE-2025-22457), demand immediate patching. This escalating digital conflict requires nations to unite, prioritize advanced threat intelligence, and adopt an agile, proactive defense posture to safeguard our interconnected world.

Back To Contents

OUR OFFERINGS

K7 Computing offers a compelling suite of cybersecurity solutions perfectly aligned with modern, cost-effective team strategies. Their offerings emphasize integrated platforms, managed services, and risk-driven frameworks to optimize resource allocation while maintaining robust protection.

Streamlining Cybersecurity Operations

K7's InfiniShield platform is a cornerstone for role consolidation, integrating endpoint security, SIEM, threat intelligence, and compliance into a single, unified console. This eliminates the need for disparate tools and specialized teams, providing cross-functional visibility and centralized incident response via Managed Detection and Response (MDR) services. The K7 Academy further supports this by cross-training teams in areas like malware analysis and threat hunting, fostering multi-functional expertise and reducing operational silos.

Leveraging Automation and Strategic Outsourcing

Automation is key to K7's approach. InfiniShield utilizes AI-driven threat detection with behavioral analysis and deception technology to reduce false positives and accelerate response times. Its SOAR integration automates tasks like patch deployment and malware containment, significantly cutting remediation efforts.

For organizations lacking internal 24/7 capabilities, K7 offers SOC-as-a-Service and MDR, providing continuous monitoring, threat hunting, and incident validation. They also offer Red Team outsourcing for periodic penetration testing and Purple Team exercises, allowing organizations to scale security operations without expanding full-time staff.

Risk Prioritization and Cloud-Native Solutions

K7's approach is inherently risk-centric. They offer Vulnerability Assessment and Penetration Testing (VAPT) and Attack Surface Management (ASM) to identify high-impact vulnerabilities and prioritize patching based on the potential for exploitation. This ensures resources are allocated to threats posing the greatest financial or operational risk.

Finally, K7's cloud-native solutions drastically reduce infrastructure costs. Their Cloud Endpoint Security utilizes lightweight, AI-driven agents for protection, eliminating the need for on-premises servers. The InfiniShield SaaS model centralizes management in the cloud, simplifying updates and reducing hardware expenses. This comprehensive approach ensures robust security that is both efficient and scalable.

Back To Contents

CYBER THREAT MONITOR REPORT

Q1_2025-26

K7 SECURITY

www.k7computing.com