K7 SECURITY

www.k7computing.com

- **GEOPOLITICAL THREATS AFFECTING THE CYBER WORLD'S STABILITY**
- **INFECTION RATE (IR)**
- **A GRANULAR VIEW OF THE INDUSTRY THREAT LANDSCAPE**
  - MOST IMPACTED INDUSTRIES AROUND THE GLOBE
- **WORLDWIDE CYBER THREAT LANDSCAPE**
- **WINDOWS THREAT LANDSCAPE**
  - TOP MALWARE TARGETING WINDOWS SYSTEMS
  - UNPATCHED VULNERABILITIES: THE ACHILLES' HEEL OF WINDOWS SYSTEMS
  - HEURISTIC HOST INTRUSION PREVENTION SYSTEM (HIPS)
- **CYBER THREAT LANDSCAPE - INDIA**
  - THE QUARTERLY TRENDS AND STATISTICS
  - TOP INFECTION RATES IN TIER-2 CITIES
- **ENTERPRISE INSECURITY**
  - CASE STUDY: COINMINERS TARGET VULNERABLE SERVERS ON THE WEB
- **THE MOBILE DEVICE STORY**
  - TROJAN TAKEOVER LOOMS
  - THE ADWARE EVOLUTION: FROM NUISANCE TO PRECURSOR
- **THE MAC ATTACK**
  - THE UBIQUITOUS TROJANS
  - THE ADWARE BROUHAHA
  - THE SHARE OF PUPS
- **VULNERABILITIES GALORE**
  - SAMSUNG MOBILE DEVICES
  - RARLAB WINRAR
  - ANDROID FRAMEWORK
  - FORTINET FORTIWEB
  - MICROSOFT WINDOWS
  - ADOBE COMMERCE AND MAGENTO
  - GOOGLE CHROMIUM
  - REACT

- **LATEST SECURITY NEWS**
  - BRAZILIAN WHATSAPP CAMPAIGN SPREADING MALWARE
  - WINDOWS BINARY EXPLOITED VIA PYTHON CODE
  - THE PHANTOM STEALER
- **OUR VERDICT**
- **OUR OFFERINGS**
  - STREAMLINING CYBERSECURITY OPERATIONS
  - LEVERAGING AUTOMATION AND STRATEGIC OUTSOURCING
  - RISK PRIORITIZATION AND CLOUD-NATIVE SOLUTIONS

GEOPOLITICAL THREATS AFFECTING THE CYBER WORLD'S STABILITY

"In a world where digital warfare is now the first strike of kinetic conflict, cyberspace has become the ultimate amplifier for geopolitical chaos".

Threat actors are known to take advantage of situations that could trigger chaos in the cyber world market. The current geopolitical tensions swaying between war and peace are an obvious advantage for threat actors to exploit this scenario.

One of the primary reasons is that cyber world netizens are not only just educated and tech-savvy people, but there are also novice cyber users not aware of the cyber risks, and the uneducated people primarily depending on other people to guide them on how to use the cyber space, especially for e-commerce related work.

And when educated people themselves are falling victim to cyber threats, both sophisticated and otherwise, like phishing threats, which have been there ever since the cyber world has boomed, in spite of regularly updating them against such attacks, we would be able to gauge the impact of cyber risks on other users.

As the 'fog of war' shifts from the physical battlefield into our personal devices, a nation's security is no longer measured by its armory, but by the digital resilience of its most vulnerable citizens".

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!

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 serves as the basis for benchmarking cybersecurity risk for enterprises and netizens.

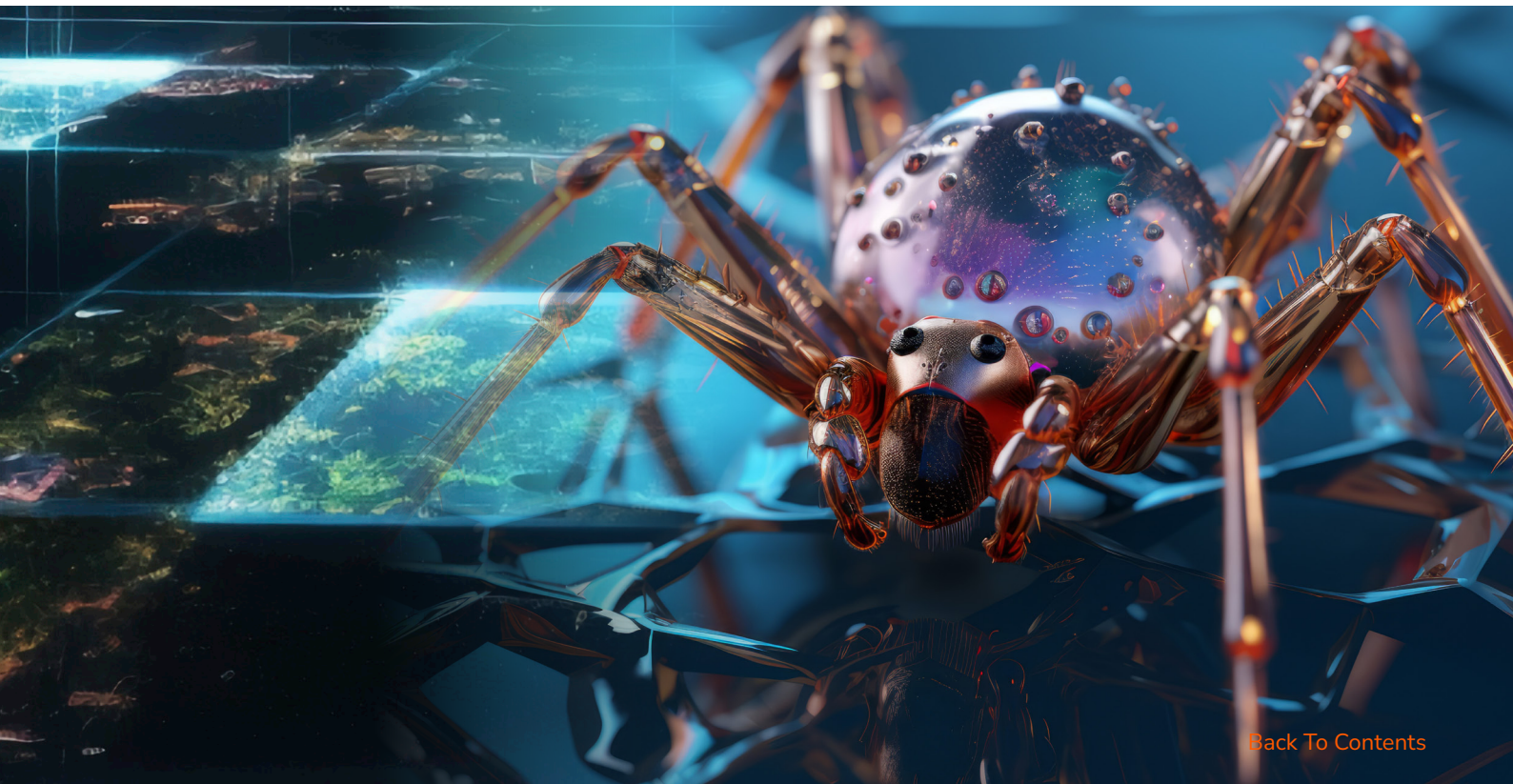
We use this IR factor to identify enterprises and netizens' exposure to cyber threats. IR is determined as the proportion of active K7 corporate or consumer users who encountered at least one cyber threat event that was blocked and reported to our K7 Ecosystem Threat Intelligence infrastructure (K7ETI).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

The Global IR for Q3_2025-26 was 19%

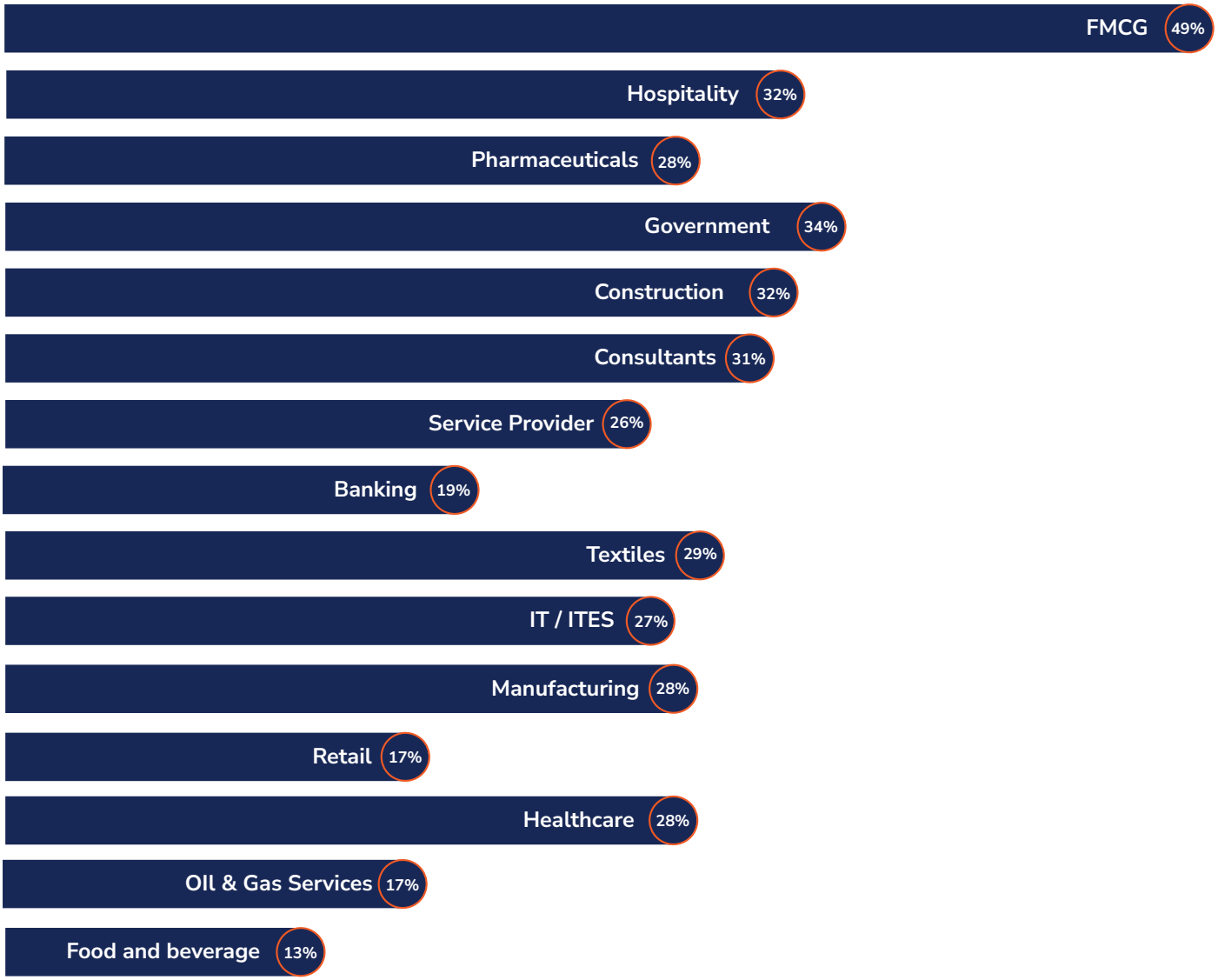


Back To Contents

A GRANULAR VIEW OF THE INDUSTRY THREAT LANDSCAPE

A granular view of the threat landscape is like a weather map; while the entire region may be under a storm, specific sectors are currently caught in a direct downpour.

Most Impacted Industries Around The Globe

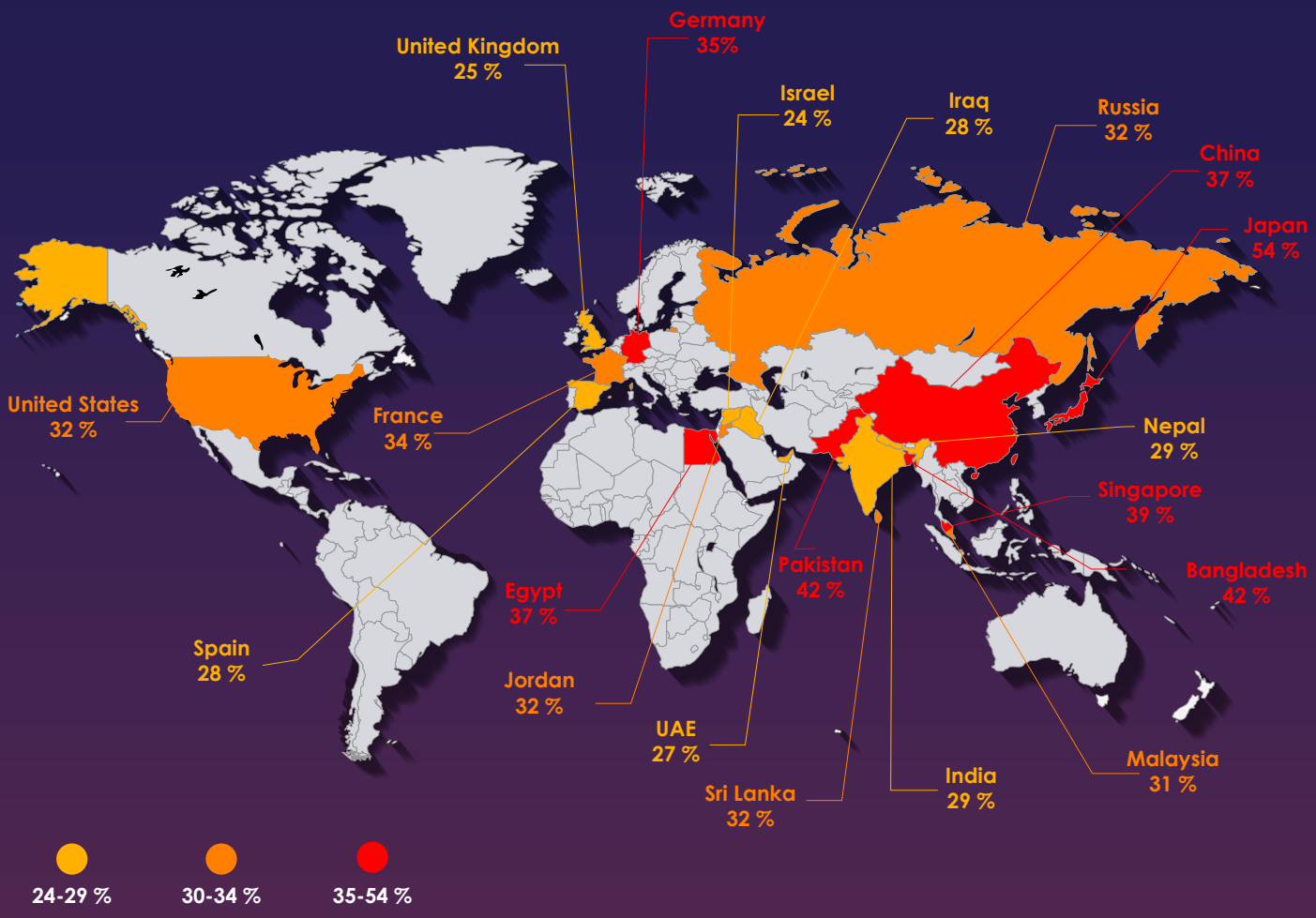


FMCG leads a besieged industrial landscape with a 49% infection rate, highlighting its status as a high-velocity target for disruption. Sectors like Government (34%), Hospitality (32%), and Construction (32%) are increasingly targeted because of their vast consumer records and critical public infrastructure. For leadership, these rates show that no industry is immune; even the 19% IR in Banking or 27% in IT/ITES reflects a persistent effort by adversaries to exploit vulnerability debt across the global economic engine.

Back To Contents

WORLDWIDE CYBER THREAT LANDSCAPE

Geopolitical tensions and economic interests are fueling a steady rise in malicious activity worldwide, as shown by the 33% Global IR. Japan's infection rate is exceptionally high at 54%, while Pakistan and Bangladesh both stand at 42%. These numbers show that regional tensions and digital growth lead to uneven risk levels. In this unpredictable environment, businesses need to adopt proactive and resilient security strategies to defend against attackers who exploit these regional weaknesses.

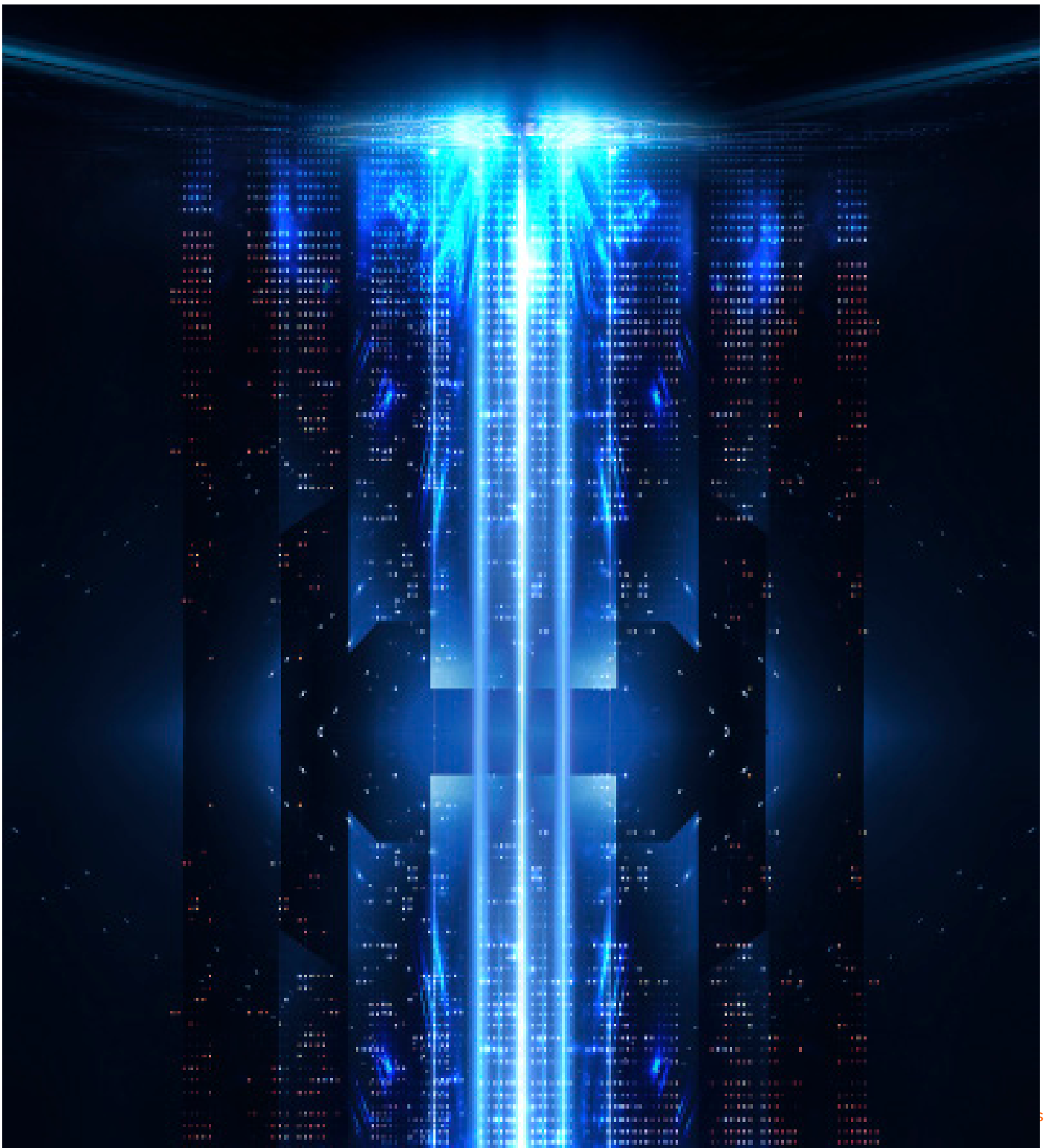


Back To Contents

WINDOWS THREAT LANDSCAPE

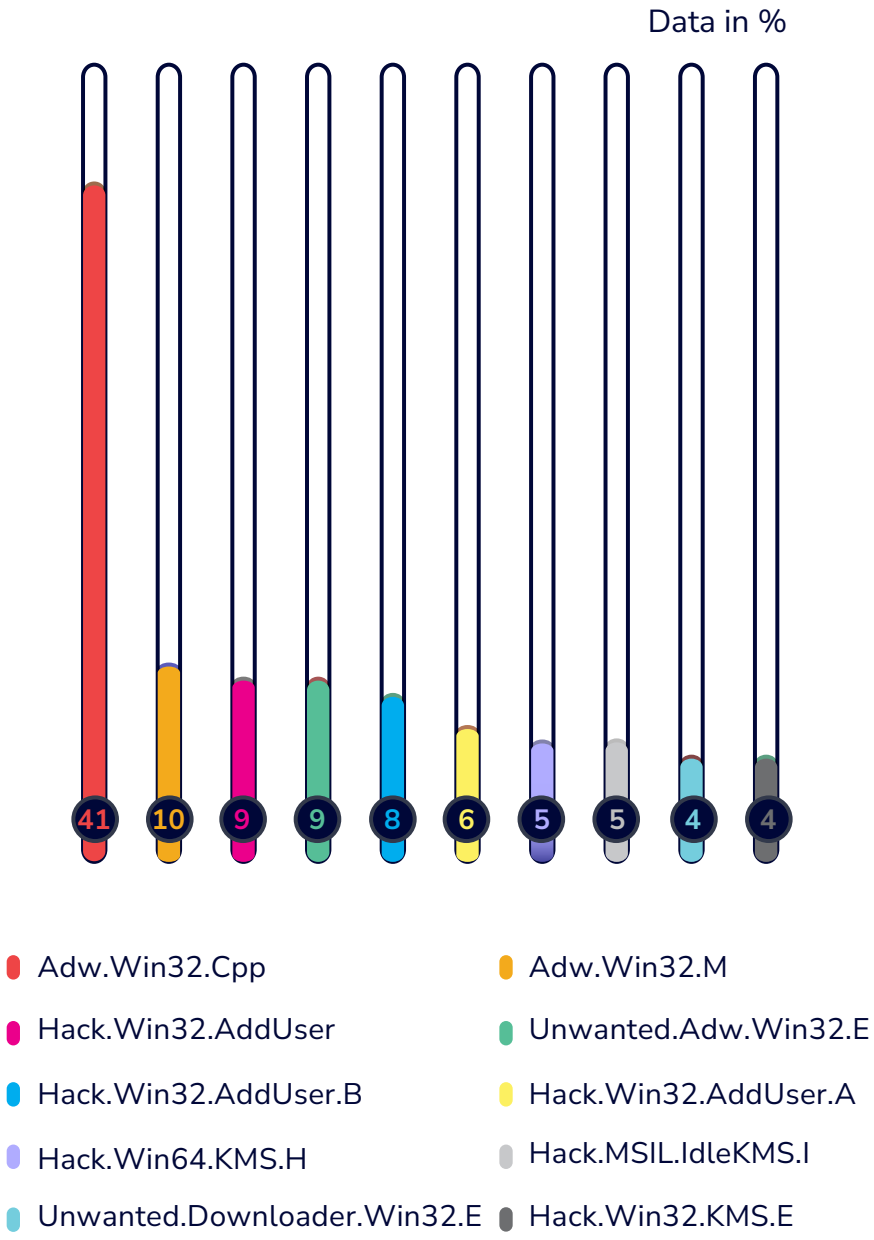
Windows remains the epicenter of cyber threats, driven by its large enterprise footprint and status as a high-reward platform for extortion and data theft. The landscape is intensifying through novel strategies and modified malware that bypass signature-based detection. This recycling lets adversaries maximize impact with minimal effort, making old threats appear new to standard security tools.

A primary driver of this volatility is vulnerability debt, the accumulation of unaddressed software flaws. Data shows that legacy exploits like MS17-010 (EternalBlue) still account for 76% of exploit detections, remaining the preferred weapon for network lateral movement years after a patch was released. Attackers are also shifting toward stealthy living-off-the-land tactics. Behavioral data confirms that PowerShell is weaponized in 18% of heuristic detections to bypass defenses. In this environment, every unpatched system is a ticking clock.



TOP MALWARE TARGETING WINDOWS SYSTEMS

Adware is the most common threat to Windows systems. The most widespread types are Adw.Win32.Cpp (20%) and Adw.Win32.Med (19%). The high number of these unwanted programs shows that attackers still use nuisance software to maintain a strong presence in business and home networks.

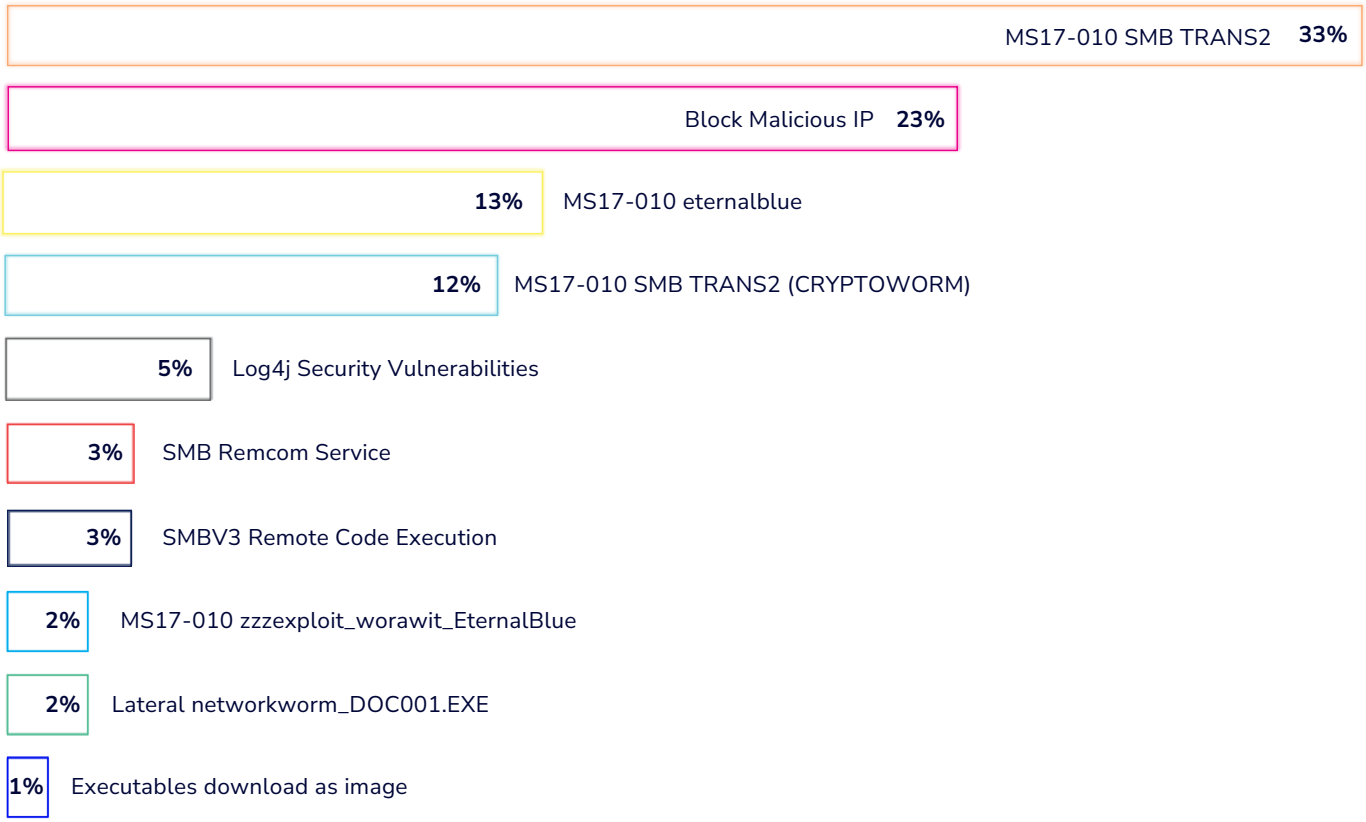


Although adware is the most common, Troj.Win32.Flox (10%) shows that attackers also focus on more serious, data-focused threats. Hack.Win32.AddUser variants (9%) are a concern because they create unauthorized accounts and increase user privileges, helping attackers move through networks. Unwanted.uTorrent.E (7%) highlights the risk of using unverified third-party software, which often leads to more dangerous threats like ransomware.

Back To Contents

UNPATCHED VULNERABILITIES: THE ACHILLES' HEEL OF WINDOWS SYSTEMS

An unpatched vulnerability is like leaving a master key under the doormat of a secure vault. No matter how strong the walls are, an intruder can just walk right in.



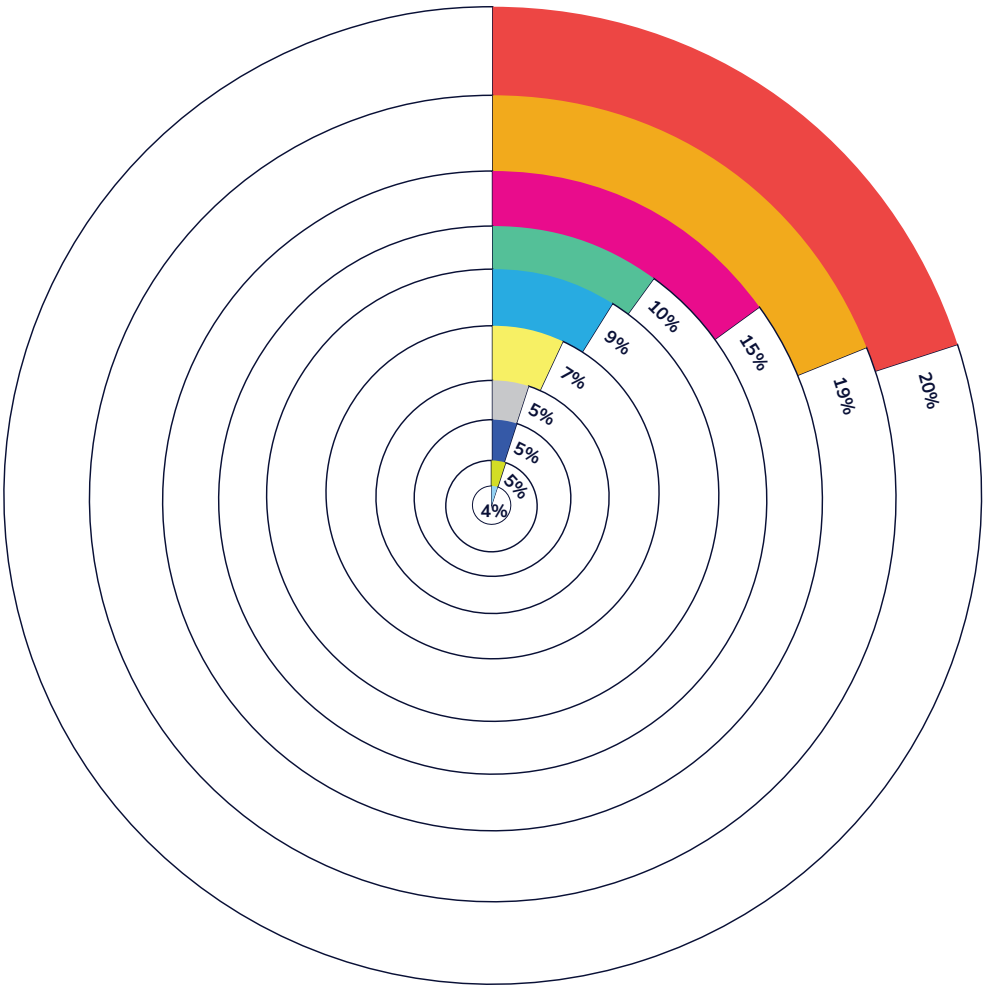
Any unpatched application or misconfigured setting gives cybercriminals an easy way into enterprise networks. Data shows that old exploits still dominate, with MS17-010 SMB TRANS2 (33%), eternalblue (13%), and CRYPTOWORM (12%) making up most of the exploit activity. Many organizations are not keeping up with patching, which lets attackers move through networks and spread ransomware even years after fixes are available. Besides SMB flaws, ongoing issues with Log4j (5%) and SMBV3 (3%) show that vulnerability debt is still a big problem in the supply chain. In the end, unpatched flaws are not just weaknesses; they are urgent problems, and a quick response is the key to defense.

Back To Contents

HEURISTIC HOST INTRUSION PREVENTION SYSTEM (HIPS)

Heuristic detection adds an essential layer of security by spotting threats based on behavior instead of fixed signatures. It is crucial for stopping zero-day exploits as they happen. Recent data shows that attackers are now using 'living-off-the-land' tactics, using normal system tools to get around standard defenses.

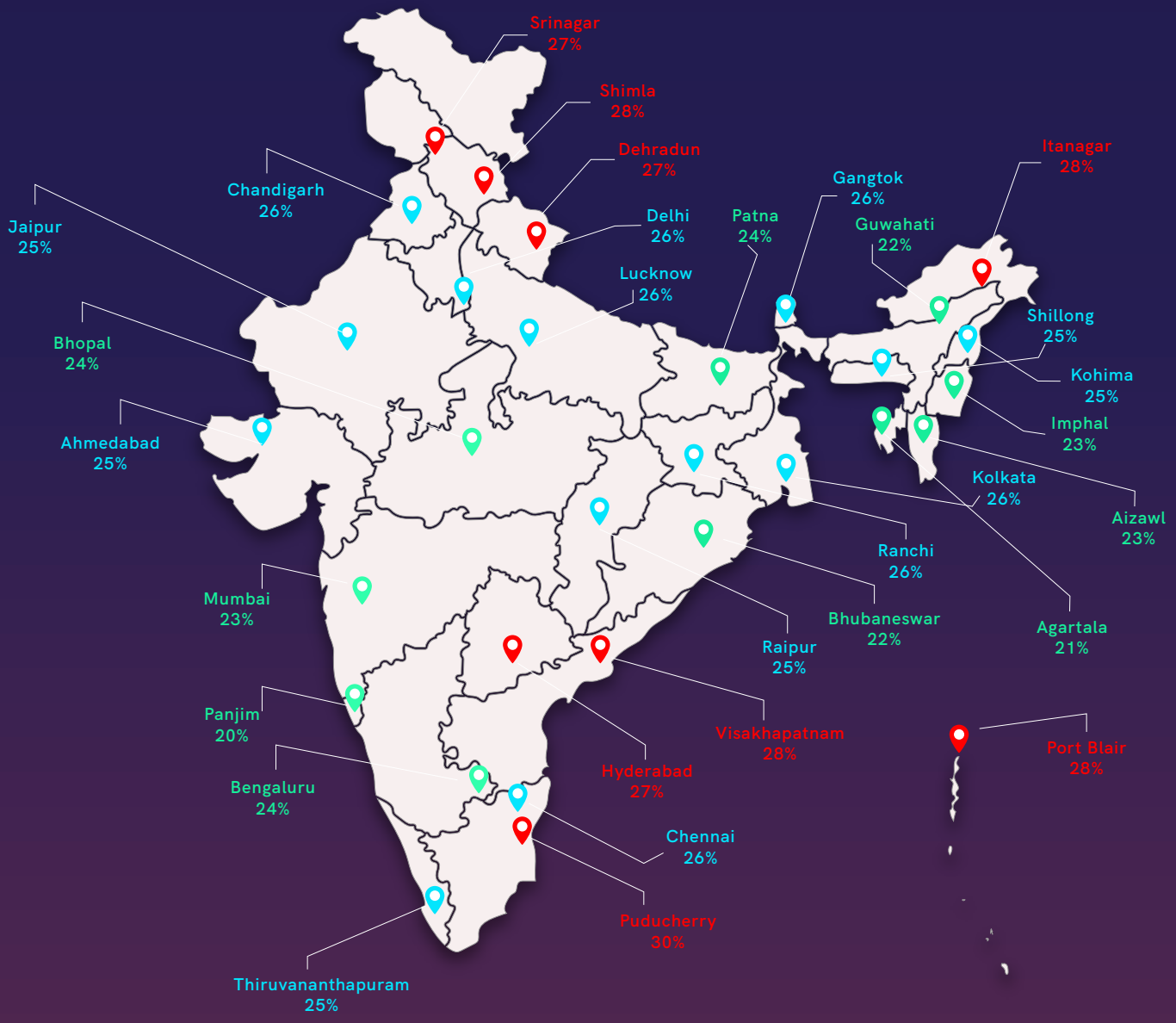
Windows Heuristic Behavioural Detection



Susp_Powershell (13%) is the top alert, showing that scripting is still the main way attackers run hidden commands and avoid detection. Susp_dropper (14%) and Susp_LolBin_Write_PE (32%) also show that attackers use complex, multi-step attacks to stay in systems and write harmful code with trusted programs. For today's businesses, watching for unusual behavior is a must, since signature-based tools often miss these attacks.

Back To Contents

CYBER THREAT LANDSCAPE - INDIA



20%- 24%

25%- 26%

27%- 30%

Map for illustrative purposes only. Not to scale.

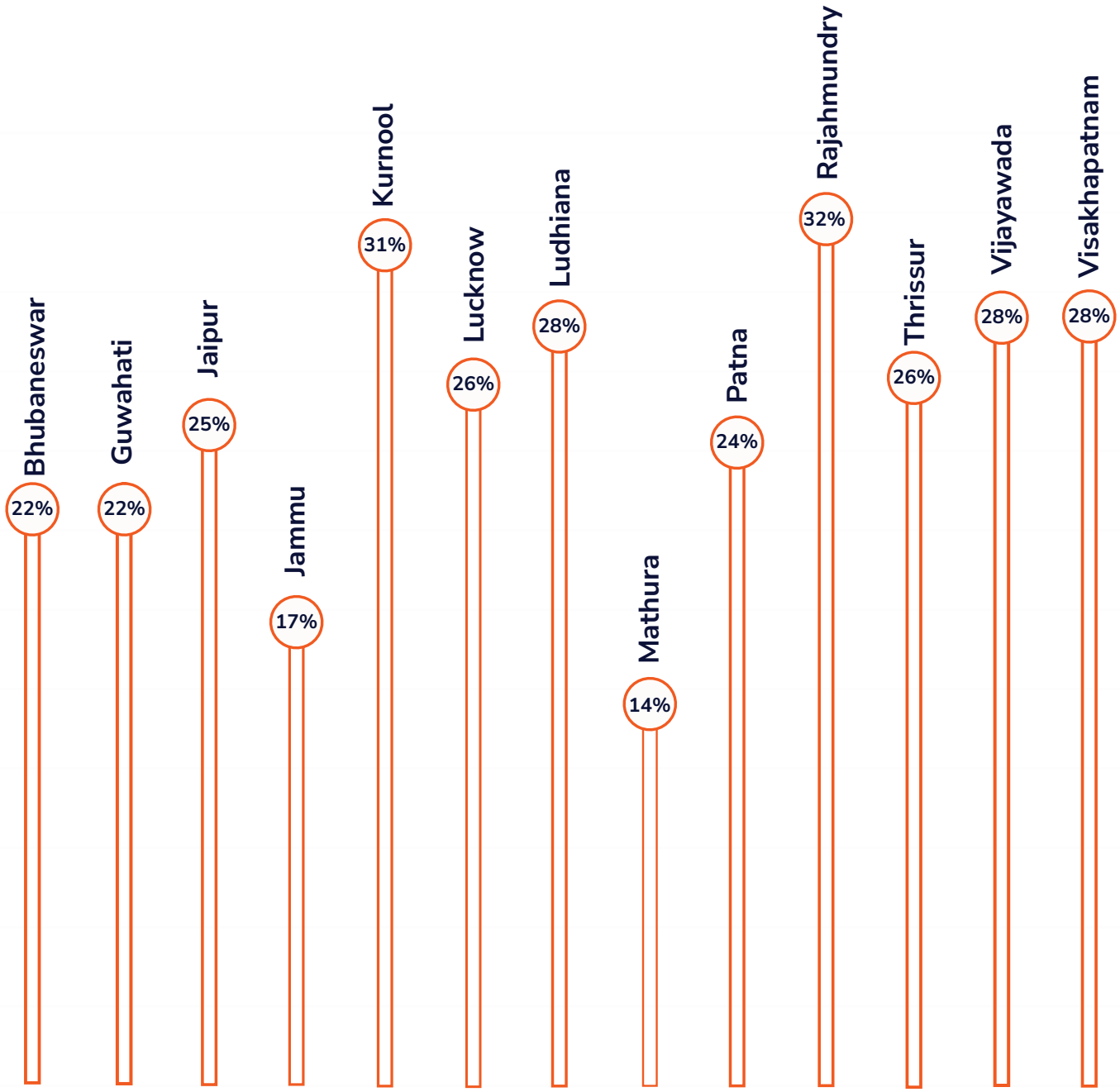
Back To Contents

THE QUARTERLY TRENDS AND STATISTICS

The PAN-India cyber infection rate has escalated to 26%, highlighting a critical necessity to embrace adequate safeguards in nationwide digital defenses.

Back To Contents

TOP INFECTION RATES IN TIER-2 CITIES



Cybercriminals are increasingly targeting India's Tier-2 cities because more people are using digital services, and many are not fully aware of online threats. Rajahmundry (32%) and Kurnool (31%) have the highest infection rates, showing that these cities face a serious risk from blocked malicious activity.

Back To Contents

ENTERPRISE INSECURITY

Case Study: Coinminers target vulnerable servers on the web

Threat actors have been deploying coinminers on victims' devices, using them for the devices' resources and to download additional malware onto the network. One such scenario was observed lately.

The kill-chain is as follows:

STEP: 1

Attackers scan for vulnerable PHP servers on the internet

STEP: 2

On finding an exploitable PHP server, malicious PHP packages containing PHP scripts are transferred to the server

STEP: 3

The malware installs and runs Ergo and Monero mining softwares in the server

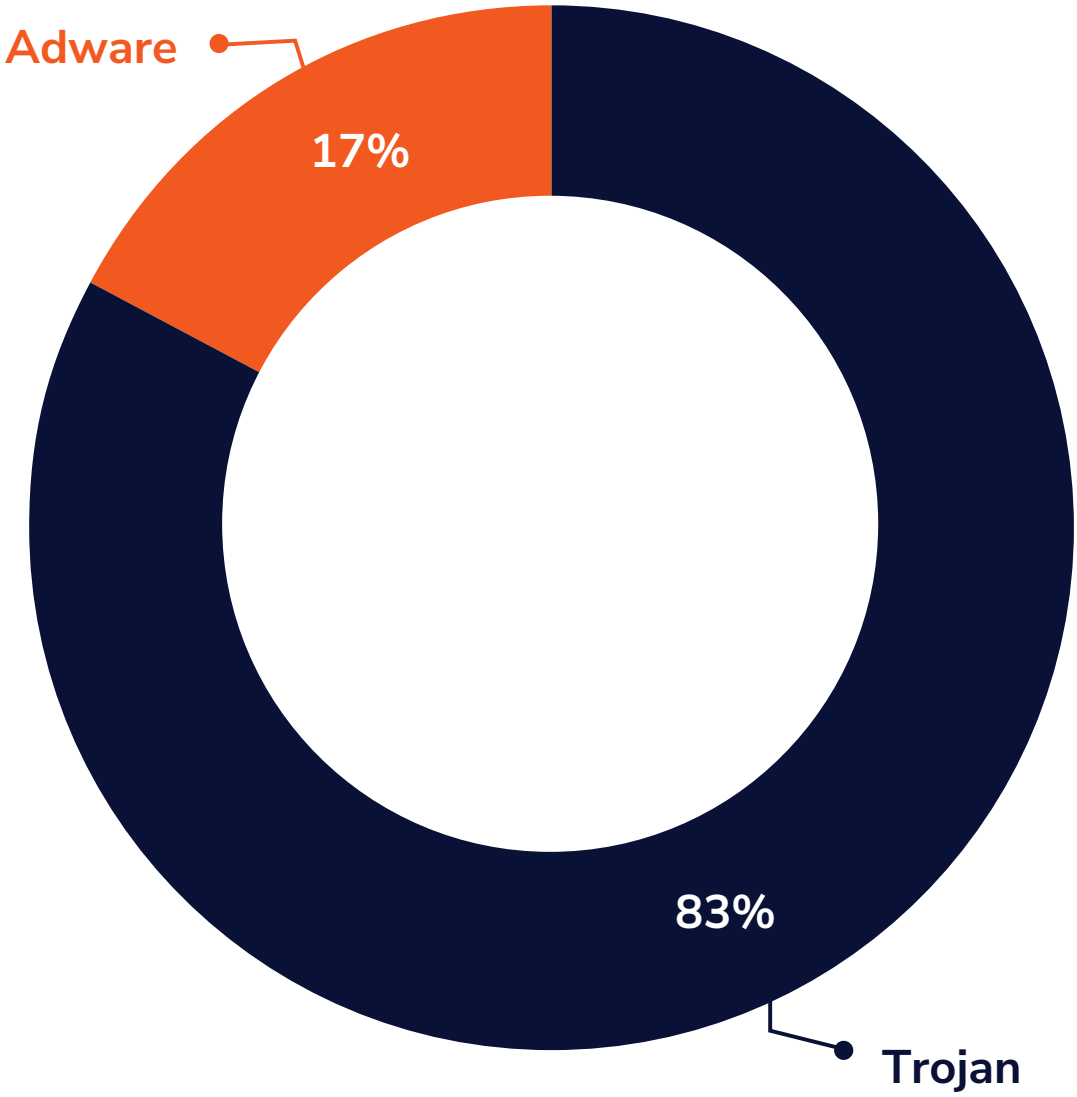
STEP: 4

SMB is used to find more vulnerable systems in the network

Back To Contents

THE MOBILE DEVICE STORY

Adware vs Trojan Proportional Split

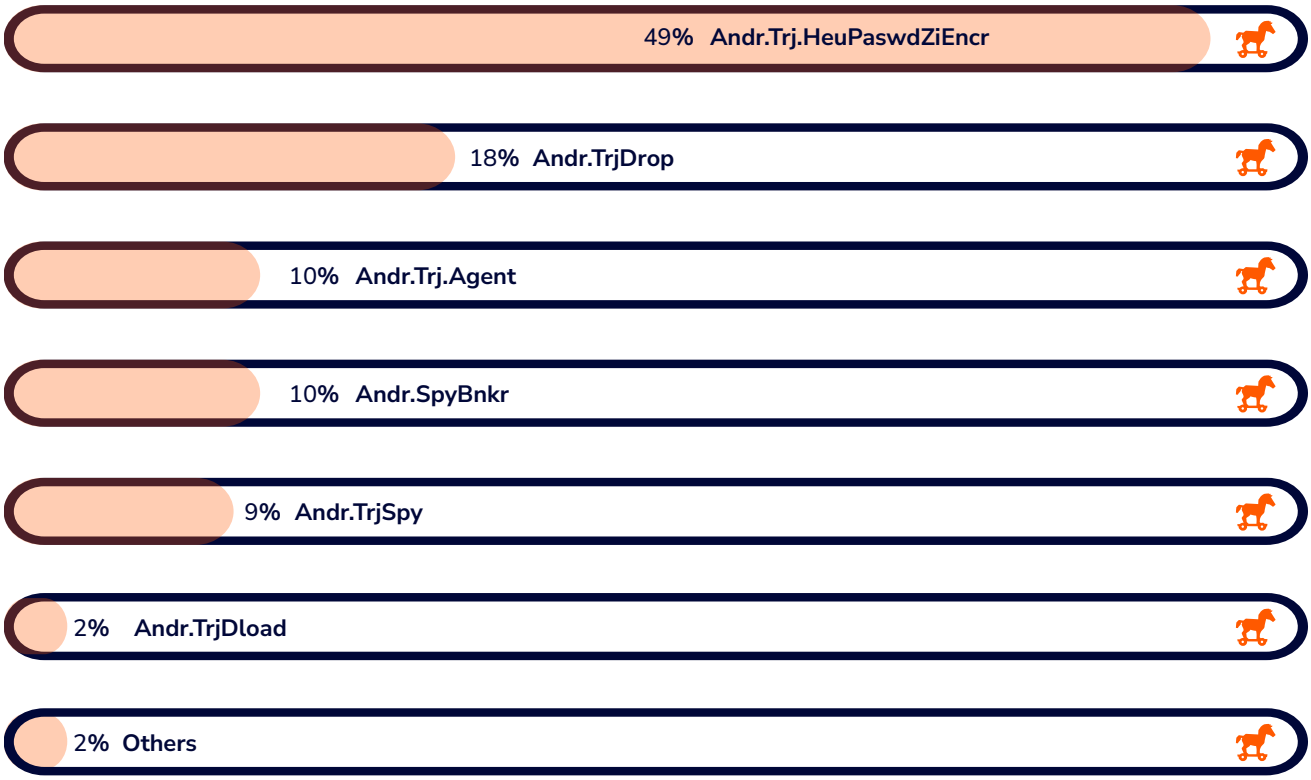


Trojan now accounts for a staggering 83% of mobile threats, leaving adware far behind at 17%. This isn't just a statistical blip; it's a clear signal that mobile attacks have evolved from mere annoyances to calculated, high-stake intrusions. For businesses, the smartphone in every pocket has become a prime entry point for data theft and network compromise. Attackers have shifted focus, chasing credentials instead of ad clicks, and they're exploiting the bring-your-own-device trend to sidestep legacy defenses. Security teams can't afford to treat mobile as an afterthought. The new playbook demands real-time threat intelligence and a mindset that sees every device as a potential breach point—because that's exactly what it is.

Back To Contents

TROJAN TAKEOVER LOOMS

The Wicked Trendline of Trojans

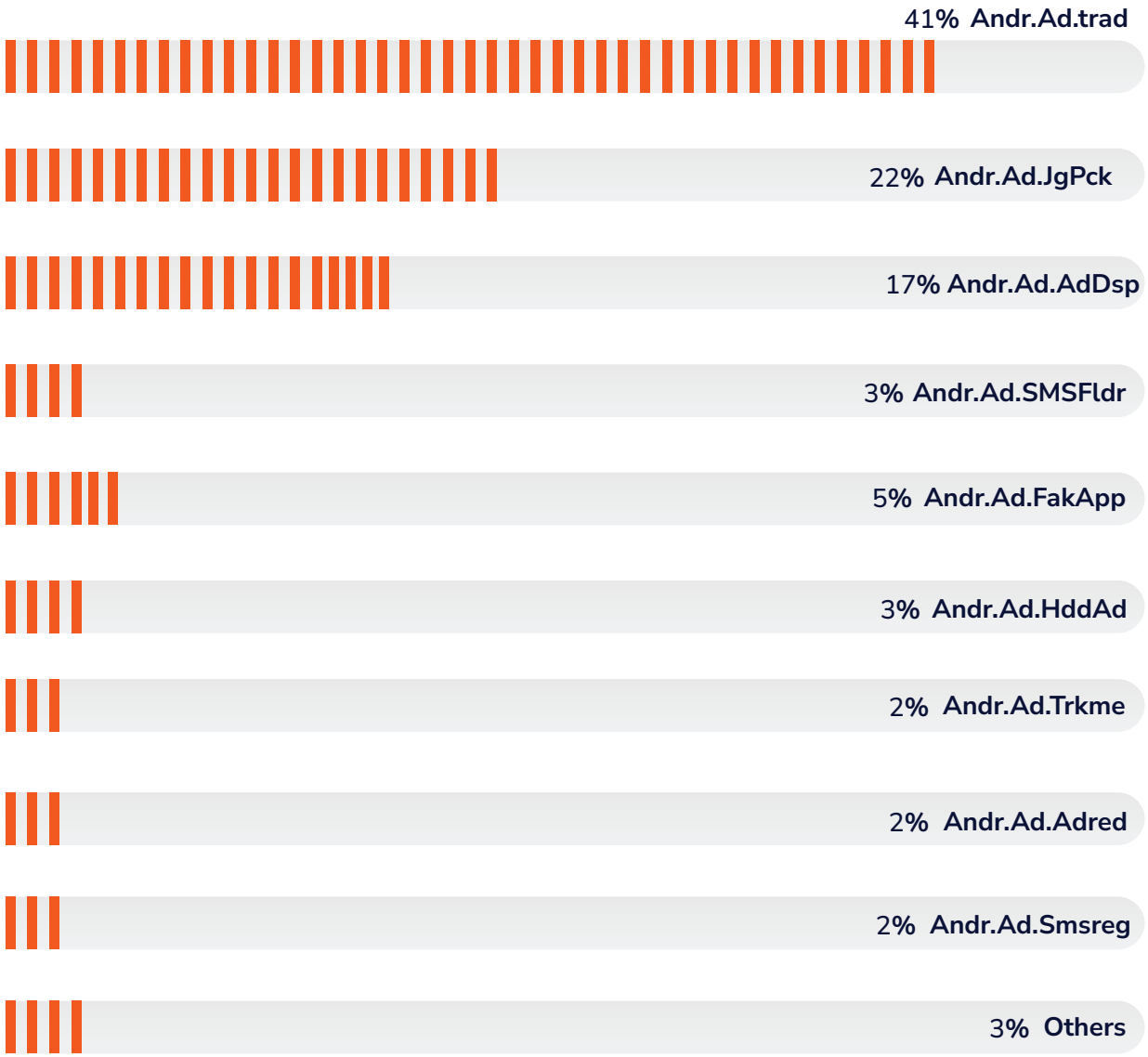


The granular data reveals a calculated offensive: nearly half (49%) of Trojan activity is driven by Andr.Trj. HeuPaswdZiEncr, a variant engineered for credential theft and obfuscation. For enterprises, this confirms that the main objective of current mobile malware is access acquisition to infiltrate corporate networks. The combined prevalence of Andr.TrjDrop (18%) and Andr.Trj.Agent (10%) highlights a strategic reliance on droppers, initial infection vectors designed to deploy secondary, often more destructive payloads like rootkits or ransomware. This ecosystem suggests a future where mobile devices serve as persistent, multi-stage staging grounds for corporate espionage and financial fraud.

Back To Contents

THE ADWARE EVOLUTION: FROM NUISANCE TO PRECURSOR

Most Prevalent Adware Types

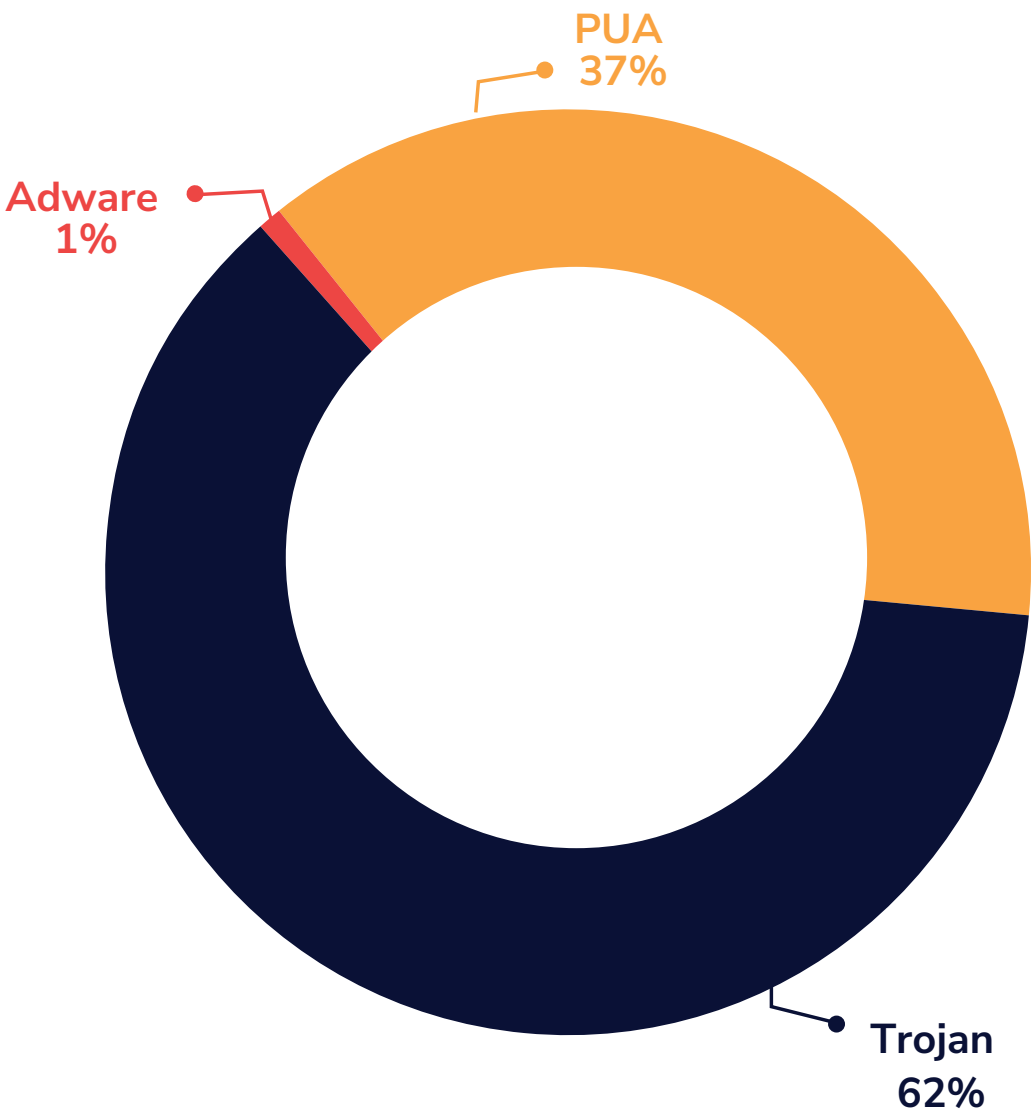


Traditional adware (Andr.Ad.trad) still leads at 41%, but the combined presence of Andr.Ad.JgPck (22%) and Andr.Ad.AdDsp (17%) shows a worrying trend. These types often enter through channels that look legitimate or act as the first step in more complex attacks. For businesses, this means adware is no longer just a small problem; it can be the start of serious security breaches. With strains like Andr.Ad.FakApp (5%) is also appearing; mobile devices are becoming hidden entry points for attackers. Organizations should treat these minor infections as important security threats.

Back To Contents

THE MAC ATTACK

Trojan, Adware and PUA Proportional Split



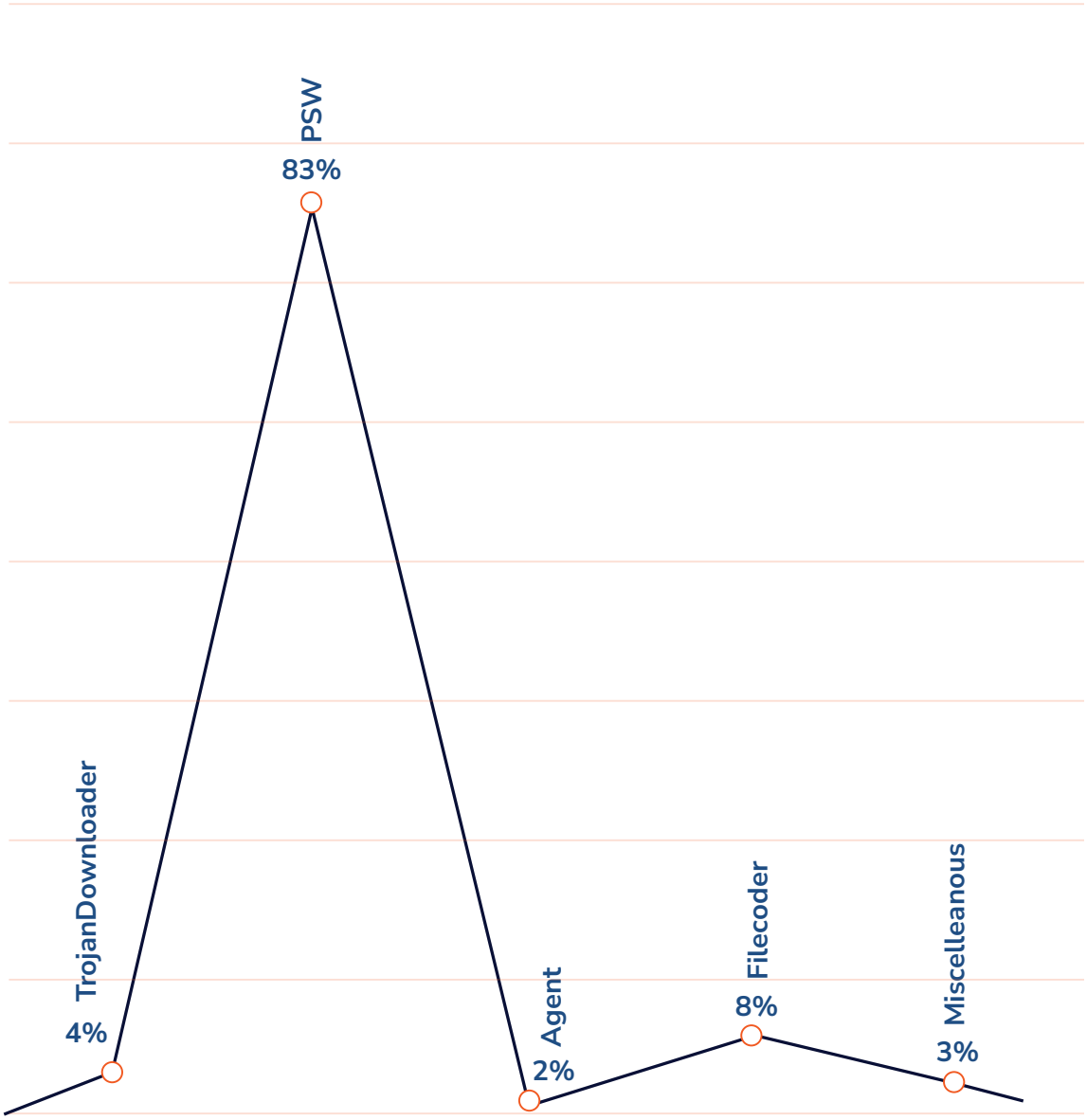
With Trojan at 62% and PUA at 37%, compared to a negligible 1% for Adware, the macOS threat landscape has shifted from nuisance to targeted compromise. For enterprises, this surge in Trojans shows that Mac endpoints are now primary vectors for credential theft and network infiltration, not just ad-revenue targets. The strong PUA presence warns of a future where grayware and weaponized legitimate tools bypass traditional defenses to establish persistent backdoors. Security strategies must quickly evolve to detect these stealthy, high-impact incursions.

Back To Contents

THE UBIQUITOUS TROJANS

The quoted data reveals a decisive strategic pivot by adversaries: with 83% of Trojan activity attributed to Password Stealing Ware (PSW), the primary objective is no longer mere disruption, but identity theft.

Trojan Detection Trend Lines

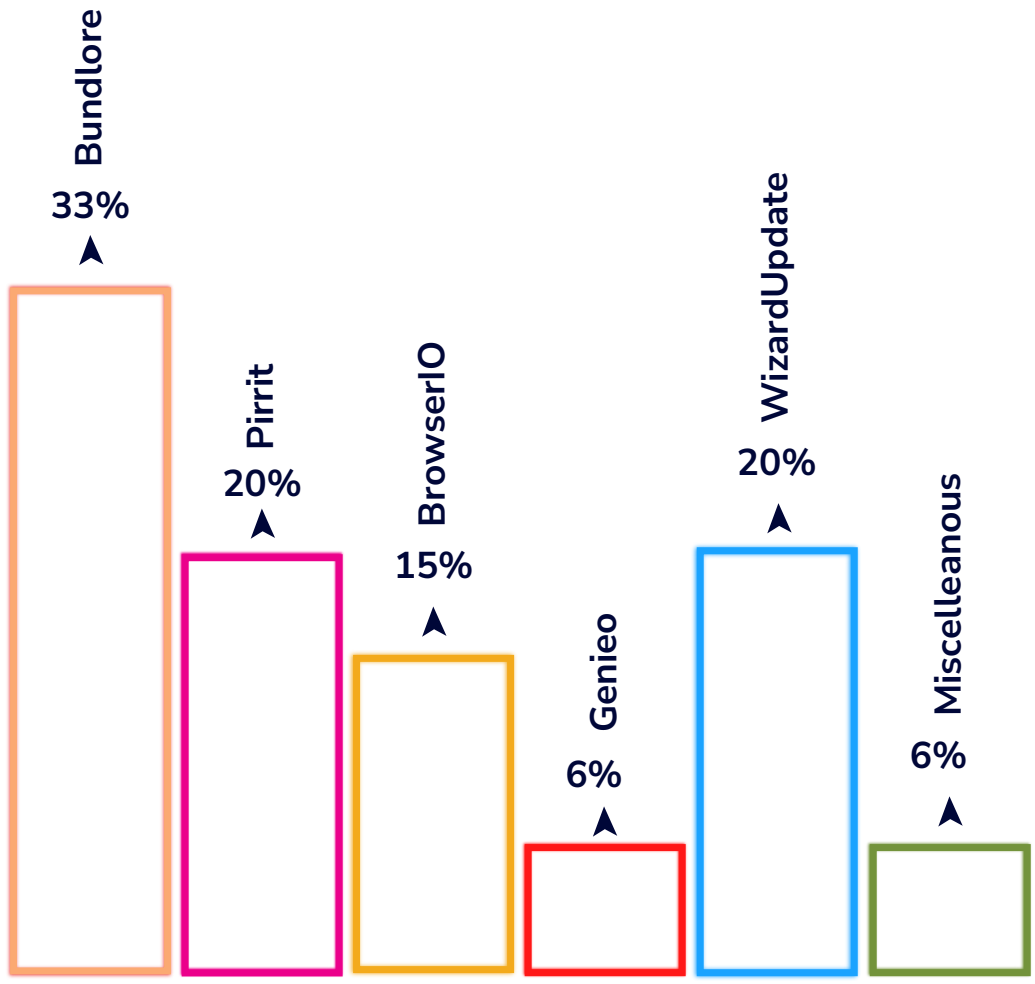


For enterprises, this focus on credential harvesting means attackers bypass traditional perimeter defenses by simply “logging in” as legitimate users instead of breaking in. While Filecoders (8%) remain a threat for ransomware-style extortion and operational paralysis, they are secondary to the strategic acquisition of access. The presence of TrojanDownloaders (4%) and Agents (2%) highlights a reliance on droppers to establish stealthy, persistent footholds for long-term espionage and payload delivery.

Back To Contents

THE ADWARE BROUHAHA

The Trendline of Adware Variant Detections



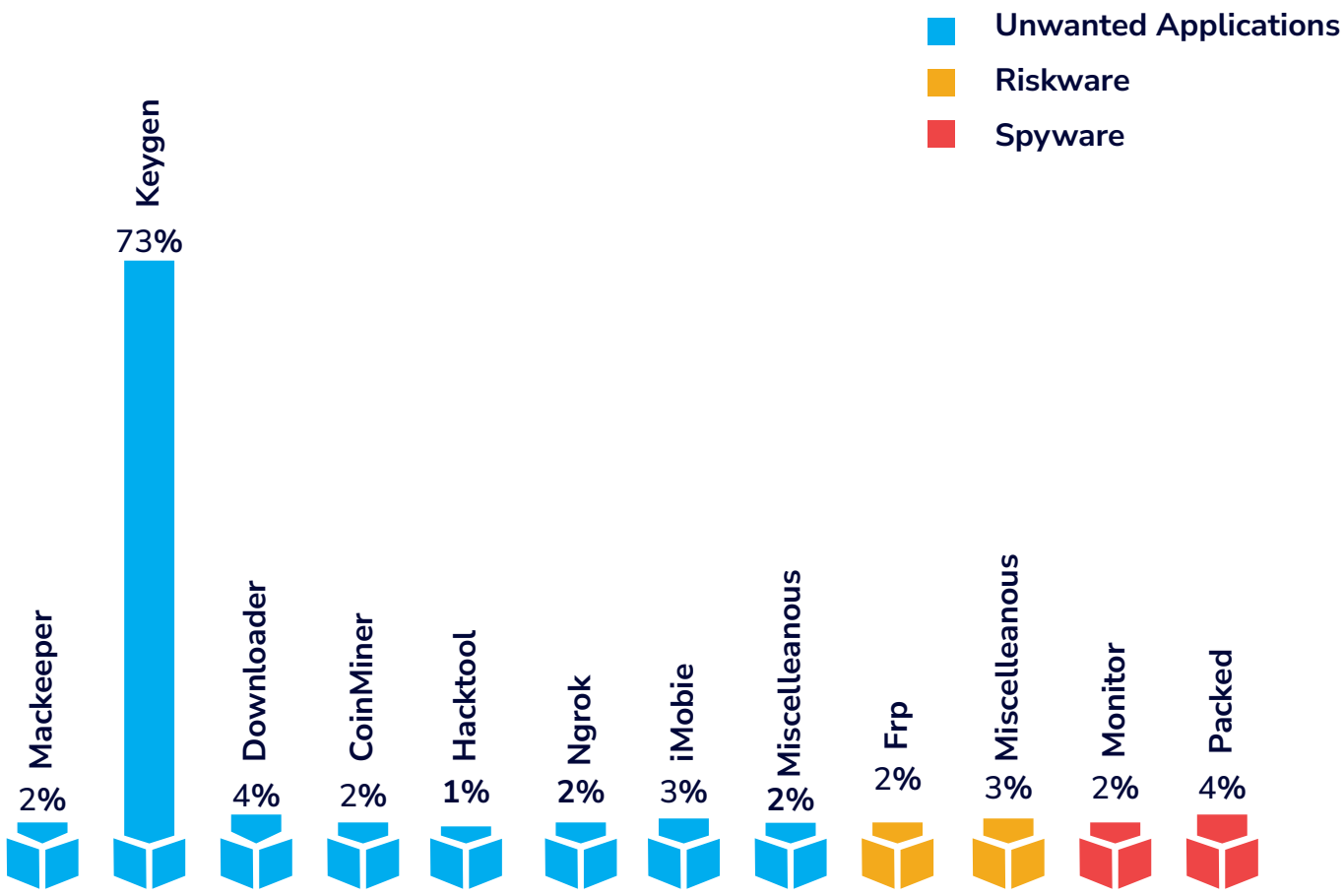
The data shows a fragmented but aggressive macOS adware landscape, dominated by Bundlore (33%). This prevalence confirms that bundling hijacking browser settings and installing unwanted extensions through seemingly legitimate downloads remains the primary infiltration vector. The equal prominence of Pirrit (20%) and WizardUpdate (20%) signals a dual threat: Pirrit uses stealth to inject intrusive ads, while WizardUpdate exploits user trust by posing as essential system updates. With BrowserIO (15%) and Genieo (6%) also compromising browsing environments, these variants collectively degrade endpoint integrity and serve as gateways for more severe network incursions.

Back To Contents

THE SHARE OF PUPS

The PUA telemetry uncovers a disturbing trend driven by user complicity: Keygens dominate at 73%, dwarfing all other categories. This figure shows that the primary vector for grayware is not accidental exposure, but active software piracy by users. For enterprises, this signals a critical internal risk where employees, trying to bypass licensing, inadvertently invite malware into the network.

Most Prevalent PUP Types



The presence of Packed executables (4%) and Downloaders (4%) warns that these piracy tools often serve as deceptive vessels for deeper system compromise. Furthermore, the detection of tunneling tools like Ngrok and Frp suggests that seemingly benign unwanted programs are evolving into gateways for stealthy data exfiltration and persistent backdoor access, effectively weaponizing legitimate utilities against the enterprise.

Back To Contents

VULNERABILITIES GALORE

In the current threat landscape, security vulnerabilities have evolved from static flaws into “live, ticking clocks” that adversaries exploit quickly using tools like Shodan and exploit kits. The rise of Malware-as-a-Service (MaaS) and the dark web trade in zero-day exploits have made every unpatched system a potential entry point for intrusion. This chapter goes beyond a catalog of weaknesses to serve as a strategic decision matrix, highlighting critical flaws where the key metric for enterprise defense is reaction speed.

SAMSUNG MOBILE DEVICES

CVE-2025-21043 | | CVSS 8.8 | Out-of-Bounds Write → Arbitrary Code Execution
IMPACT: Full compromise of the Samsung mobile devices running Android 13, 14, 15, and 16
MITRE T1203: Arbitrary code execution
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Apply Android security patch for proper input validation

RARLAB WINRAR

CVE-2025-6218 | CVSS 7.8 | Directory Traversal → RCE
IMPACT: Allows arbitrary code execution as the current user in versions before 7.12
MITRE T1566: Phishing (Malicious Archives)
MITRE T1203: Exploitation for Client Execution
ACTION: Upgrade required to version 7.12+

ANDROID FRAMEWORK

CVE-2025-48572 | CVSS 7.8 | Bypass permissions → Privilege escalation
CVE-2025-48633 | CVSS 5.5 | Code logic error → Add device owner → Information disclosure
IMPACT: Allows total compromise of the Android devices running 13, 14, 15, and 16
MITRE T1404: Exploitation for Privilege Escalation
MITRE T1412: Capture Device Configuration Information
MITRE T1406: Access Sensitive Device Data
ACTION: Apply the latest Android security patch

FORTINET FORTIWEB

CVE-2025-64446 | CVSS 9.4 | Path traversal → Execute administrative commands
CVE-2025-58034 | CVSS 6.7 | Input validation → OS command injection
IMPACT: Allows an authenticated attacker to execute unauthorized code on the system via crafted HTTP requests or CLI commands
MITRE T1190: Exploit Public-Facing Application
MITRE T1059: Command and Scripting Interpreter
ACTION: Immediately apply critical vendor patches to prevent unauthorized command execution

MICROSOFT WINDOWS

CVE-2025-33073 | SMB Client | CVSS 8.8 | Bypass NTLM relay mitigation → SMB client privilege escalation
CVE-2025-59230 | Remote Access Connection Manager | CVSS 7.8 | Improper Access Control → Privilege Escalation
CVE-2025-24990 | Agere Modem Driver | CVSS 7.8 | Untrusted Pointer Deference → Privilege Escalation
CVE-2025-59287 | Windows Server Update Service (WSUS) | CVSS 9.8 | Deserialization of Untrusted Data → Remote Code Execution
CVE-2025-62215 | Windows Kernel | CVSS 7.0 | Race Condition → Privilege Escalation

Back To Contents

IMPACT: Allows low-privilege accounts to gain system-level privileges
MITRE T1190: Exploit Public-Facing Application
MITRE T1557: Adversary-in-the-Middle
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Patch the system with the latest security update to prevent the bypass mechanism

ADOBE COMMERCE AND MAGENTO

CVE-2025-54236 | CVSS 9.1 | Improper Input Validation → Session Hijacking
IMPACT: Achieves session takeover and arbitrary code execution
MITRE T1190: Exploit Public-Facing Application
MITRE T1059: Command and Scripting Interpreter
MITRE T1539: Steal Web Session Cookie
ACTION: Apply vendor security patches

GOOGLE CHROMIUM

CVE-2025-13223 | CVSS 8.8 | Type Confusion → Heap Corruption
IMPACT: Potentially allows for exploitation heap corruption before version 142.0.7444.175
MITRE T1203: Exploitation for Client Execution
ACTION: Apply vendor security patches

REACT

CVE-2025-55182 | CVSS 10.0 | Insecure Deserialization → Remote Code Execution
IMPACT: Gains arbitrary code execution on React.js version 19.0.0, 19.1.0, 19.1.1, 19.2.0
MITRE T1190: Exploit Public-Facing Application
MITRE T1059: Command and Scripting Interpreter
ACTION: Apply vendor security patches

Back To Contents

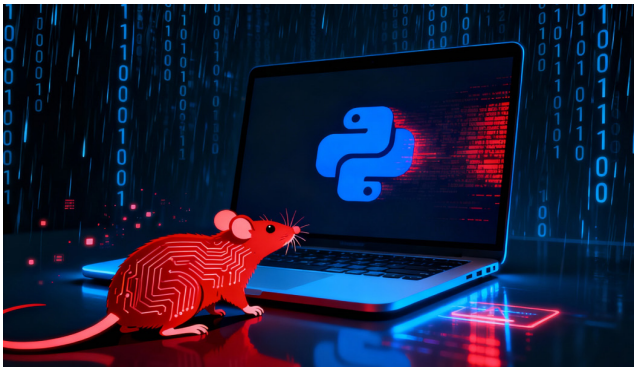
LATEST SECURITY NEWS

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

Brazilian WhatsApp Campaign spreading malware

- A massive phishing campaign against Brazil is being used to spread malware via WhatsApp web from the victim's machine to their contacts and also loads a banking Trojan into memory.
- This exploits the WhatsApp automation script from Github, an open source to achieve the same.

Refer Brazilian Campaign for details



Windows binary exploited via Python code

A hidden python code injects malware into legitimate Windows binary and performs multilevel de-obfuscation to finally deliver Remote Access Trojan (RAT).

For more details refer Python Code Malware

The Phantom Stealer

Phantom, a stealer malware sends sensitive data like passwords, browser cookies, credit card information, crypto wallet credentials, victim's IP addresses, etc to the attacker, thereby using it for identity theft, account takeovers or even worse, the infected machine can be used as a tool to facilitate bigger malware attacks.

For more details refer The Phantom Stealer

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

Back To Contents

OUR VERDICT

The digital world is in a state of persistent conflict where cyber operations are integral to statecraft, eroding global trust and stability. The biggest threat to resilience is mounting vulnerability debt, shown by legacy exploits like MS17-010 still making up 76% of detections years after patches became available. Adversaries are no longer just hacking code; they are hacking human emotions, using social contracts of respect and authority to bypass even the most advanced technical perimeters.

For the modern enterprise, reactive security is a failed strategy. Survival in this volatile landscape requires a proactive, risk-centric approach that treats patch management as an urgent business priority and values behavioral intelligence over static signatures. At K7 Labs, we are dedicated to fortifying digital sovereignty by blending AI-driven automation with human expertise, ensuring that as threats grow bolder, our defenses stay ahead.

In a world where unpatched flaws are “live, ticking clocks,” the only metric that matters is the speed of response.

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

K7 SECURITY

www.k7computing.com