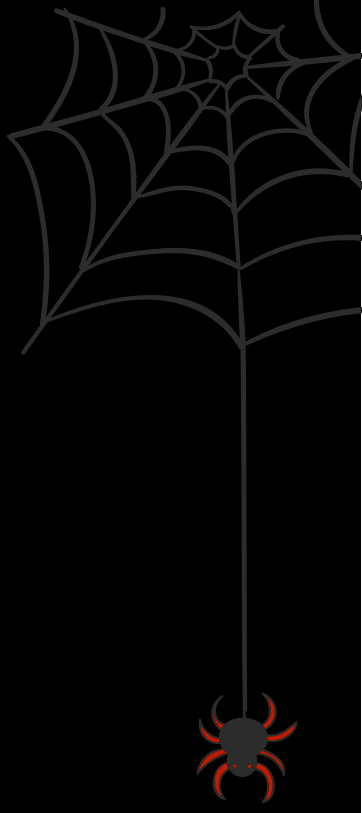
CYBER THREAT MONITOR REPORT

Q1_2026-27

K7 SECURITY

www.k7computing.com



BEC: THE WEAPONIZATION OF ORGANIZATIONAL TRUST

Companies pour billions into digital defenses, yet still hemorrhage cash to emails that look flawless and sound polite.

Business Email Compromise is not just another cyber threat; it marks a turning point. Sophisticated attackers now sidestep hardened systems and go straight for the human element, exploiting the psychology woven into every financial transaction.

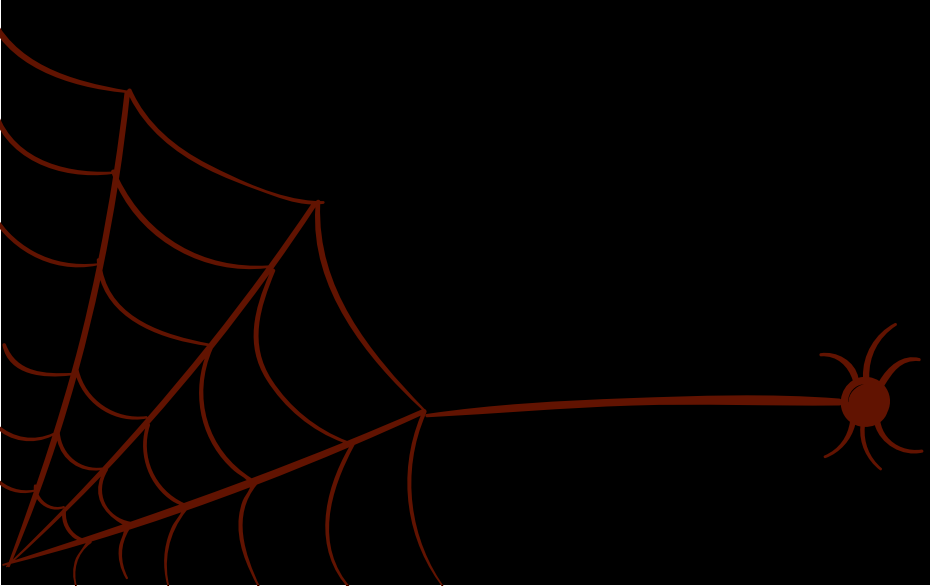
Inside sprawling, tightly linked global supply chains, attackers are scaling up their cons with AI. Generative text and real-time voice cloning have wiped out the old tells.

No more awkward phrasing or clumsy grammar. Now, cybercriminals can mimic executives and vendors with chilling precision. That $55.5 billion lost to BEC over the past decade? It's not about weak tech. It's about operational deception at scale. This is not a hypothetical risk. In one global case, a single finance employee greenlit $25.6 million in fraudulent transfers after a video call with what looked and sounded like company leadership, except it was all deepfake.

For enterprises, especially in high-volume sectors like BFSI, healthcare, manufacturing, and IT, this kind of psychological attack is a financial landmine. BEC doesn't just drain money. It shatters trust with vendors and grinds financial operations to a halt. If your finance team can't tell a real board directive from an AI-crafted fake, the entire foundation of corporate governance starts to crack.

Leaders need to stop seeing BEC as just an email problem. This is an identity crisis and a governance emergency. If a payment request looks legit just because it carries the CEO's name or a vendor's logo, you're already exposed. Verify every request independently. Firewalls guard your systems. Only independent checks guard your money and reputation.
Read on for our latest findings, and see what to do next.

And stay alert!



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.

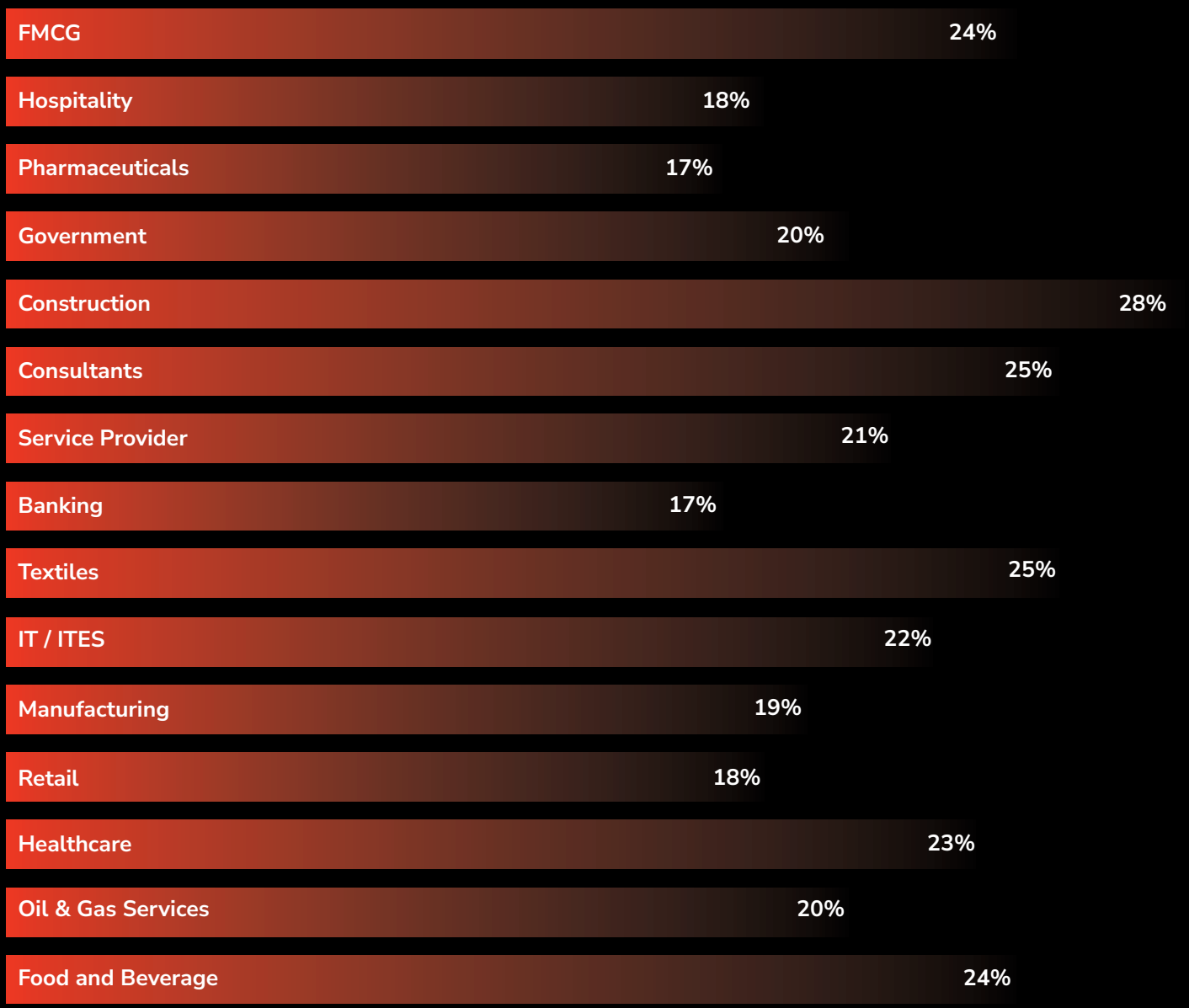
Infection Rate (IR) of an area

The Global IR for Q1_2026-27 was 37%

Back To Contents

A GRANULAR VIEW OF THE INDUSTRY THREAT LANDSCAPE

Recent telemetry points to a new target: sprawling, decentralized supply chains. Construction, textiles, and FMCG now report higher infection rates than banking or pharma. Attackers are zeroing in on vendor ecosystems riddled with weak spots and blind spots. Breaching these networks opens backdoors into enterprises, raising the stakes for disruption, theft, and data loss.

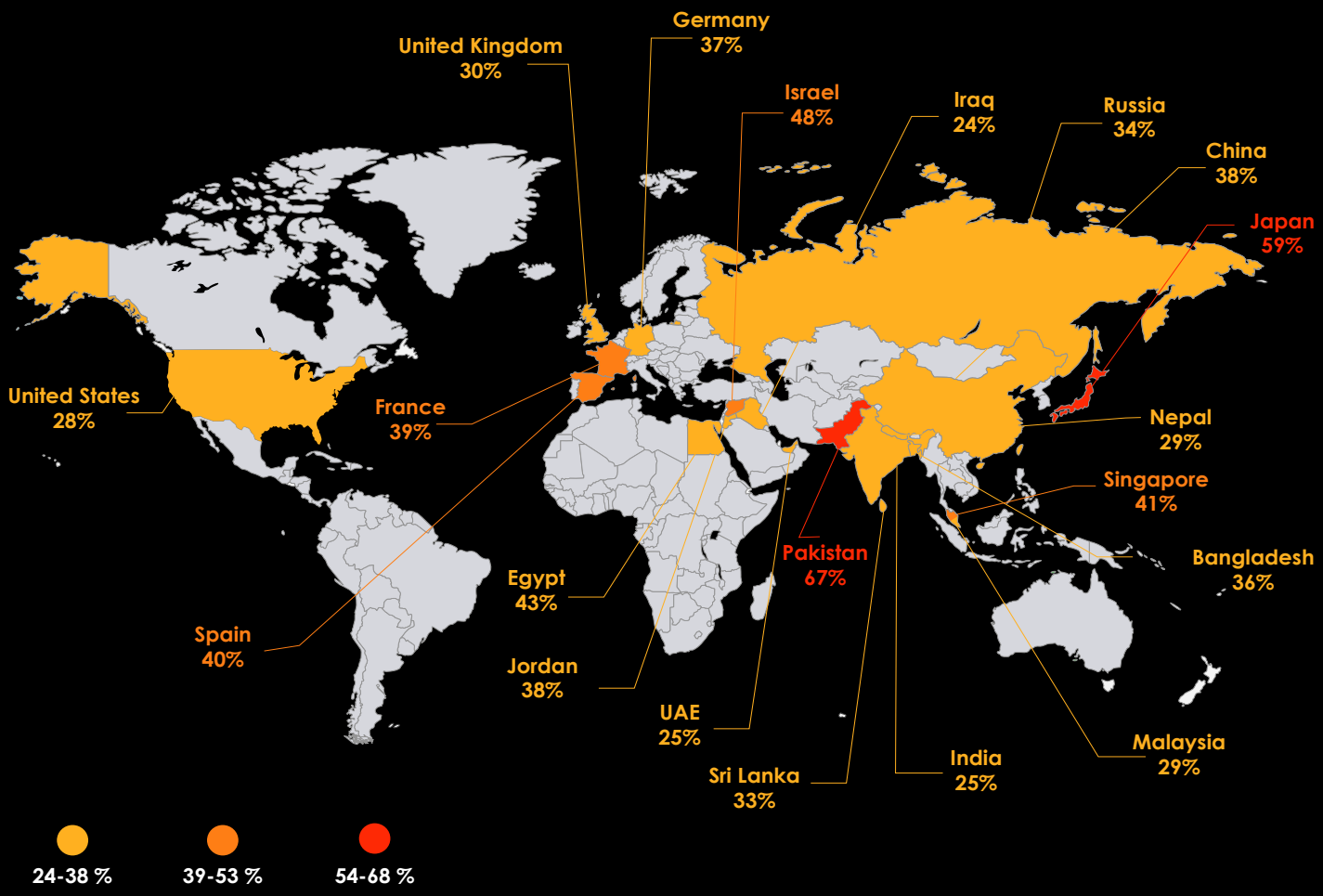


The surge in attacks signals a deeper shift in cybercrime itself. Ransomware-as-a-Service and AI-driven automation have slashed the skill and time needed for complex campaigns. Attacks are now scalable, repeatable, and ruthlessly efficient, letting threat actors hit more targets faster. Cybercrime has become an industry, turning once-specialized hacks into streamlined operations built for profit.

Back To Contents

GLOBAL CYBER THREAT LANDSCAPE

Incident response data paints a lopsided threat map. The global average is 37%, yet regions like Pakistan and Japan are heading north to 67% and 59%, respectively, exposing stark fault lines in digital defenses.



This fractured landscape marks a tactical pivot. Attackers are ditching broad, one-size-fits-all campaigns in favor of precision strikes, zeroing in on digital powerhouses like Israel (48%) and Singapore (41%), as well as fast-modernizing markets such as Egypt (43%). Meanwhile, the UK (30%) and US (28%) see fewer hits, but the attacks that do land are anything but basic. Adversaries exploit local weak spots and gaps in regional defenses, slipping in persistent footholds that quietly abuse cross-border trust.

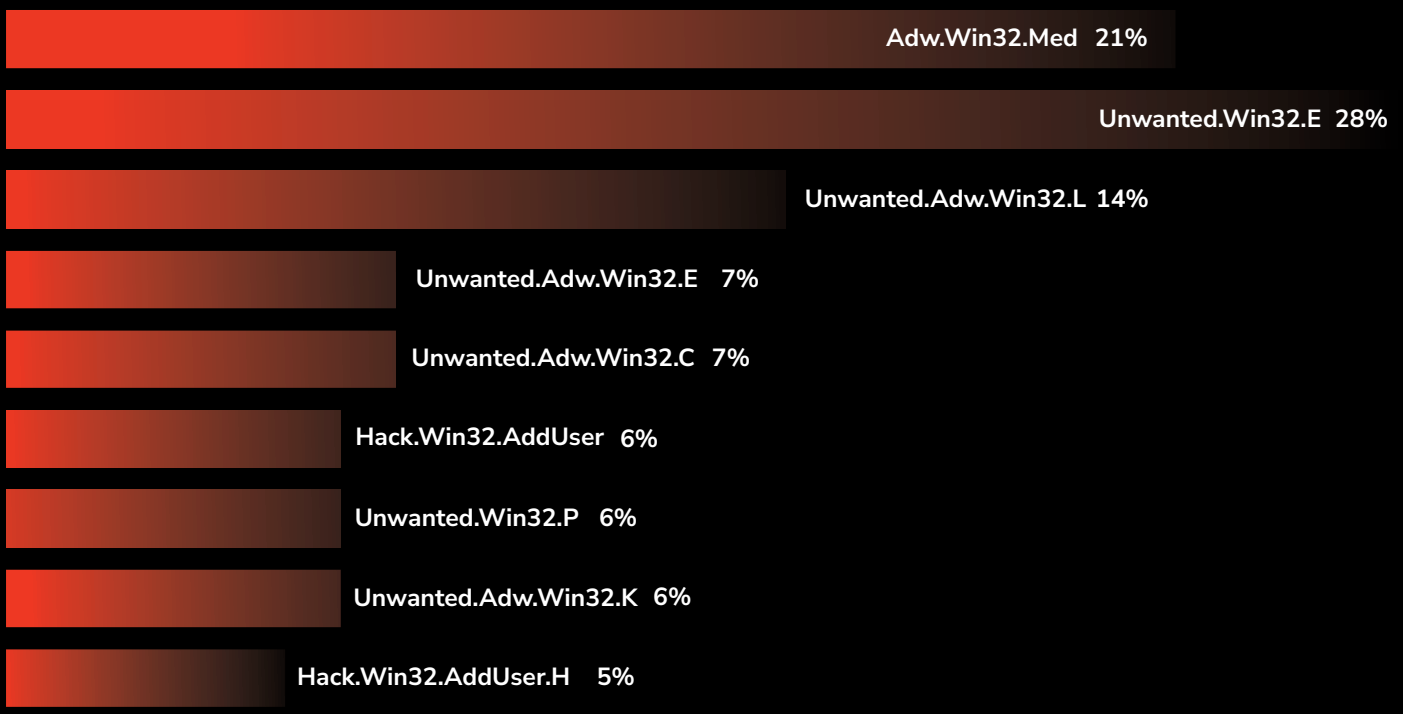
Back To Contents

WINDOWS THREAT LANDSCAPE

Windows environments are under siege like never before. Attackers are not just chasing profit. They are optimizing for scale and reach, aiming to dominate the enterprise landscape. Instead of relying on noisy malware, they twist built-in admin tools and Active Directory itself into silent weapons. By commandeering these trusted channels, they carve out deep, domain-wide access that slips past legacy defenses. For organizations, this flips their own infrastructure against them, triggering crippling outages, sweeping data theft, and ransom demands that can bring operations to a standstill.

THE MALWARE PROLIFERATION

Telemetry cuts through the noise: Med adware drives 21% of exposures, Unwanted.Win32.E variants hit 28%, and Unwanted.Adw.Win32.L clocks in at 14%. These grayware strains quietly reshape system settings and browser profiles, siphoning off tracking data under the radar.

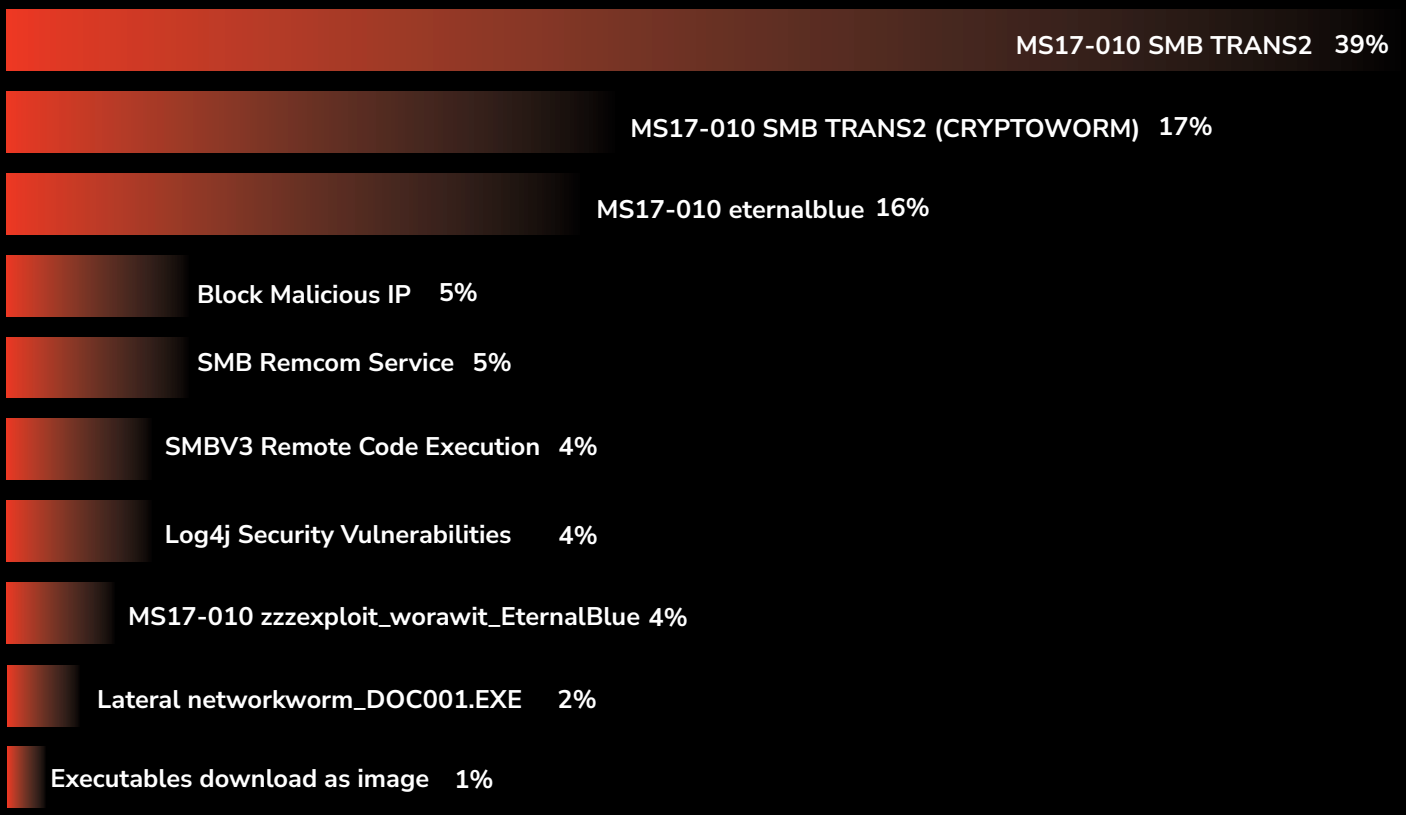


The 11% share held by Hack.Win32.AddUser variants signals a sharper escalation. These tools do not just watch. They seize control, manipulating local accounts and admin rights to lay the groundwork for silent lateral movement across the network.

Back To Contents

UNPATCHED VULNERABILITIES: WEAPONIZING THE CORPORATE PATCH GAP

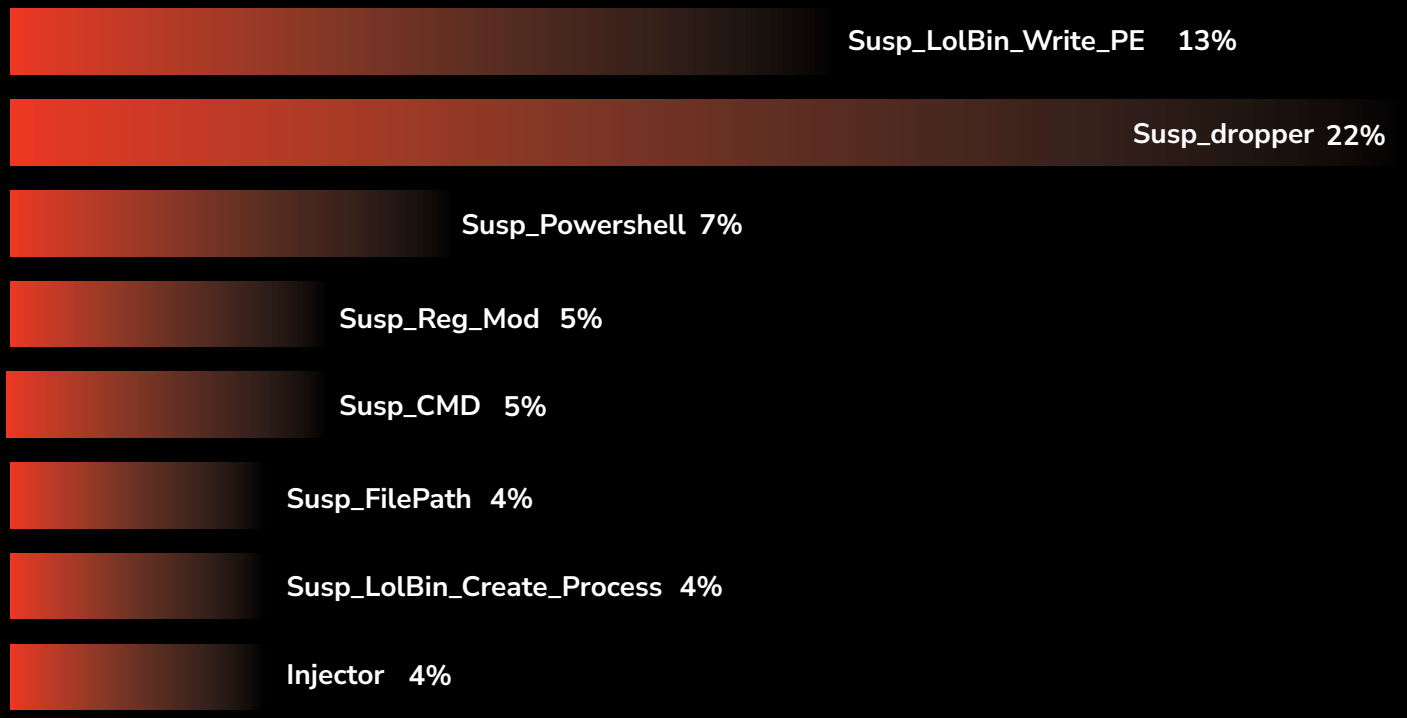
Telemetry exposes the mechanics: MS17-010 SMB TRANS2 exploits drive 39% of incidents, with Cryptoworm payloads at 17% and EternalBlue at 16%. Together, these vectors fuel fast, self-spreading outbreaks that can engulf entire networks.



SMB Remcom (5%) and Log4j remote execution (4%) add extra breach layers. With this stacked arsenal, attackers can flip one unpatched machine into a launchpad for chaos, paralyzing entire organizations in a matter of hours.

Back To Contents

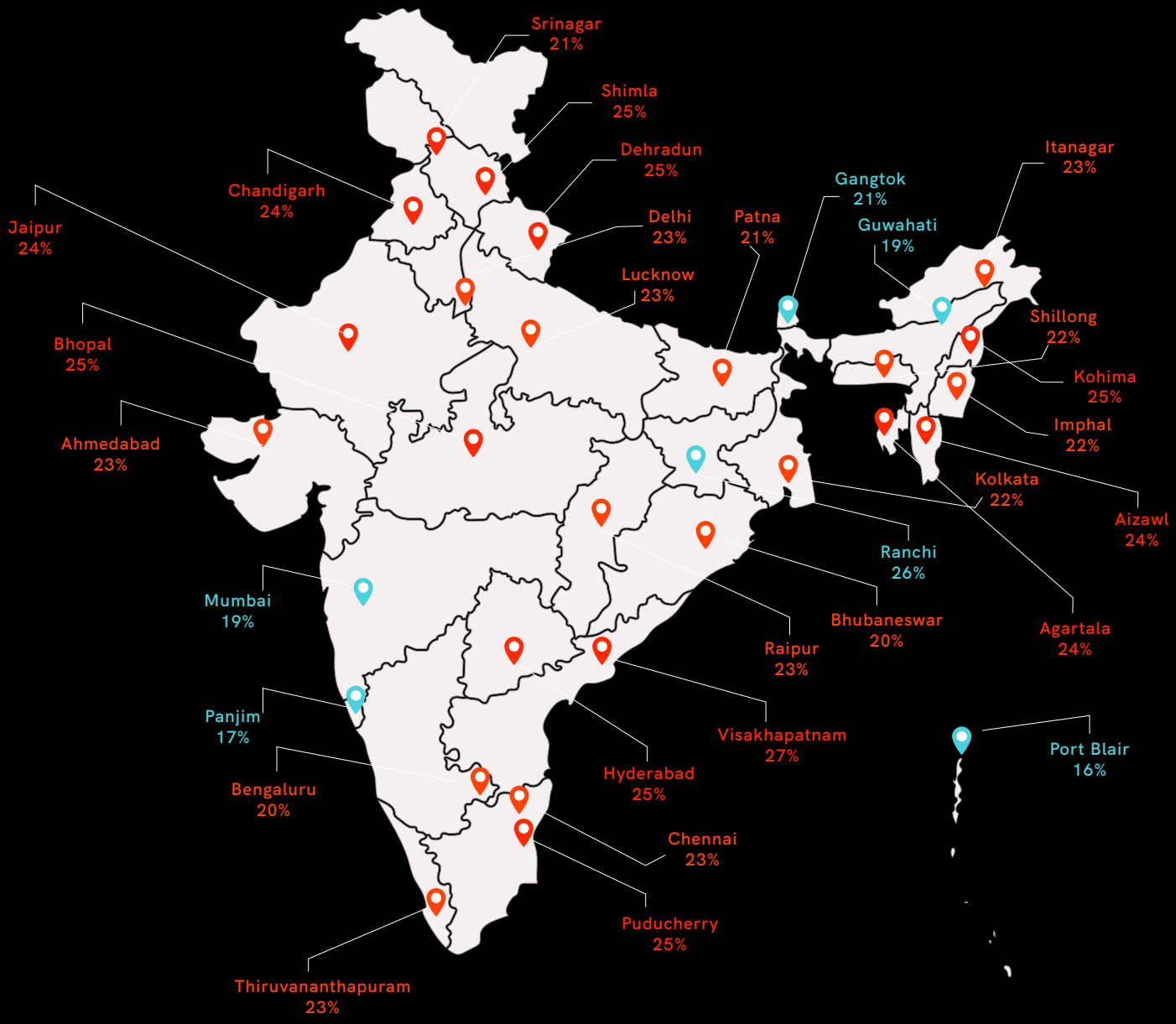
HEURISTIC INTRUSION PREVENTION SYSTEM (HIPS)



Endpoint telemetry tells a clear story: attackers lean hard on stealthy payload staging, with suspicious droppers leading at 22%. Once inside, they weaponize everyday admin tools: LoLBin_write (13%), PowerShell (7%), CMD commands (5%), to blend in with normal activity. Add registry tweaks (5%) and process injection (4%), and you have a playbook built for invisibility. These living-off-the-land moves sidestep legacy defenses, letting attackers dig in deep and siphon data for the long haul.

Back To Contents

CYBER THREAT LANDSCAPE - INDIA



16%-19%

20%-23%

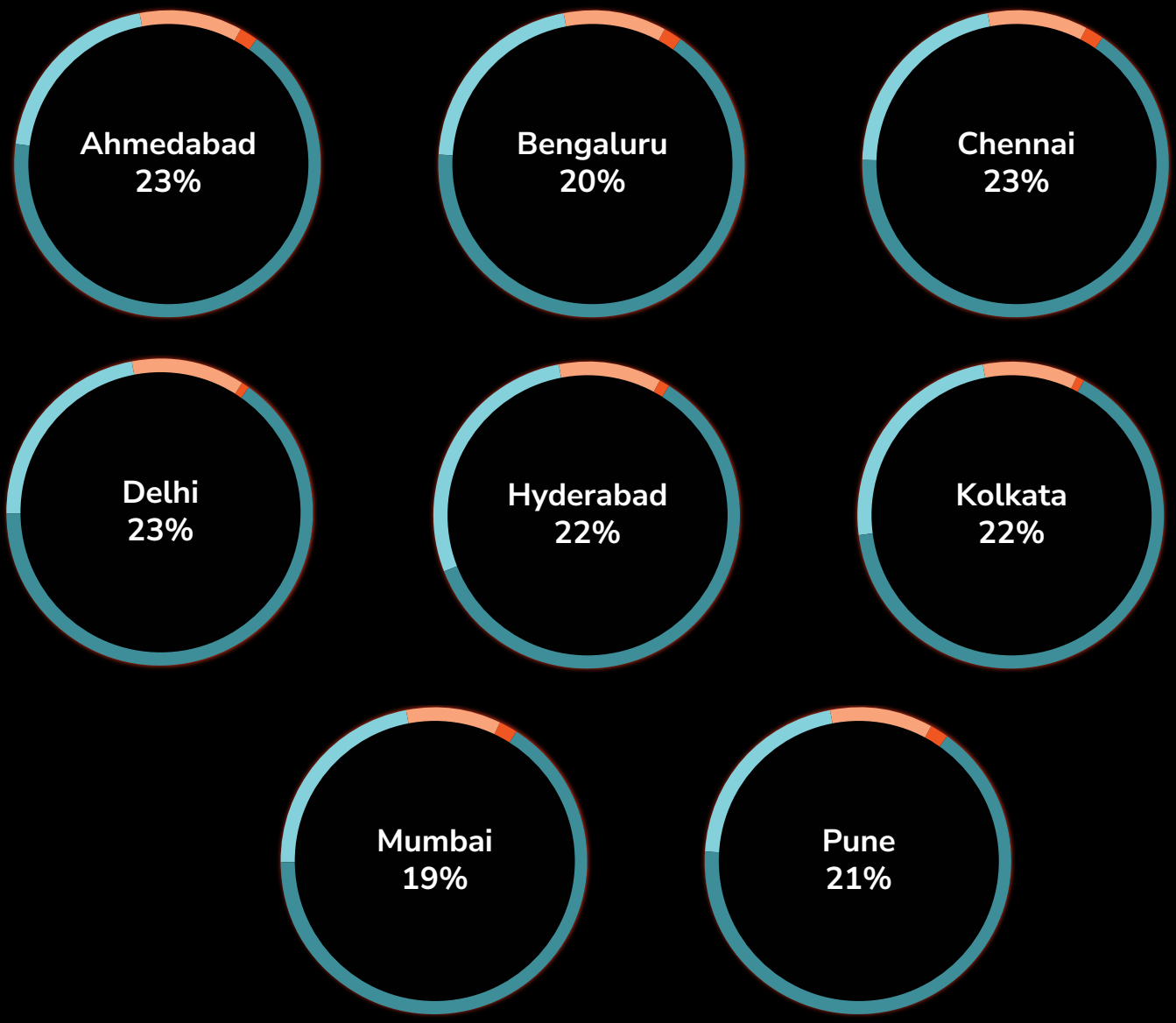
24%-27%

Map for illustrative purposes only. Not to scale.

Back To Contents

THE QUARTERLY TRENDS AND STATISTICS

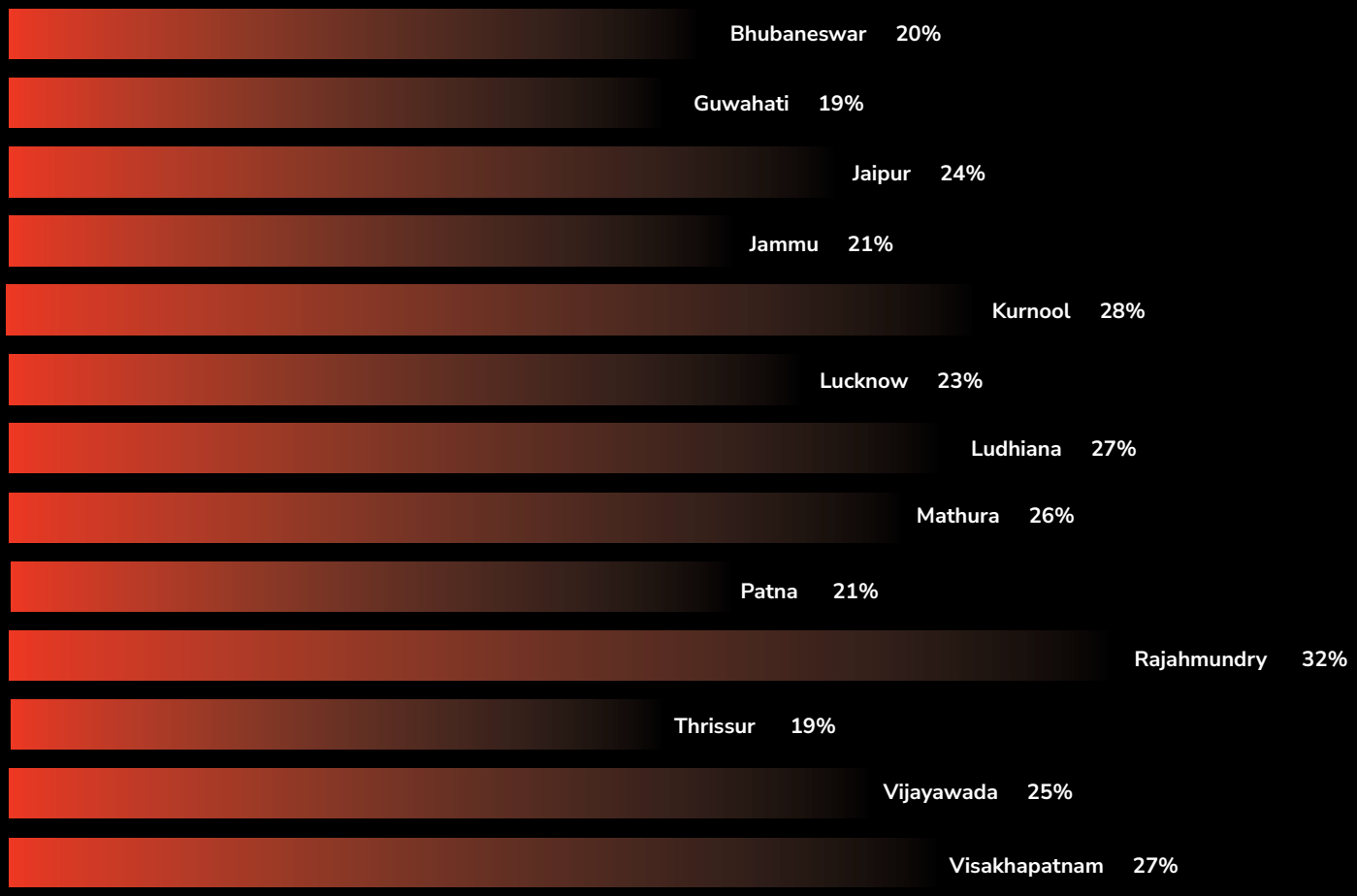
India's Tier-1 economic hubs have emerged as strategic platforms for advanced threat actors, who exploit the intricate interconnectivity of these hyper-digital metropolitan areas. By targeting localized structural vulnerabilities within these financial and technological centers, adversaries are subtly transitioning from regional compromises to global enterprise supply chains.



Back To Contents

TOP INFECTION RATES IN TIER-2 CITIES

India's rapidly digitizing Tier-2 and Tier-3 cities, especially Rajahmundry (32%) and Kurnool (28%), are emerging as active threat vectors. Regional hubs like Ludhiana (27%), Visakhapatnam (27%), and Mathura (26%) integrate into broader supply chains, making them vulnerable to adversaries exploiting their expanding, often under-secured digital footprints. These opportunistic campaigns establish unmonitored footholds, exposing interconnected national enterprises to cascading operational disruptions and severe data compromise.



Back To Contents

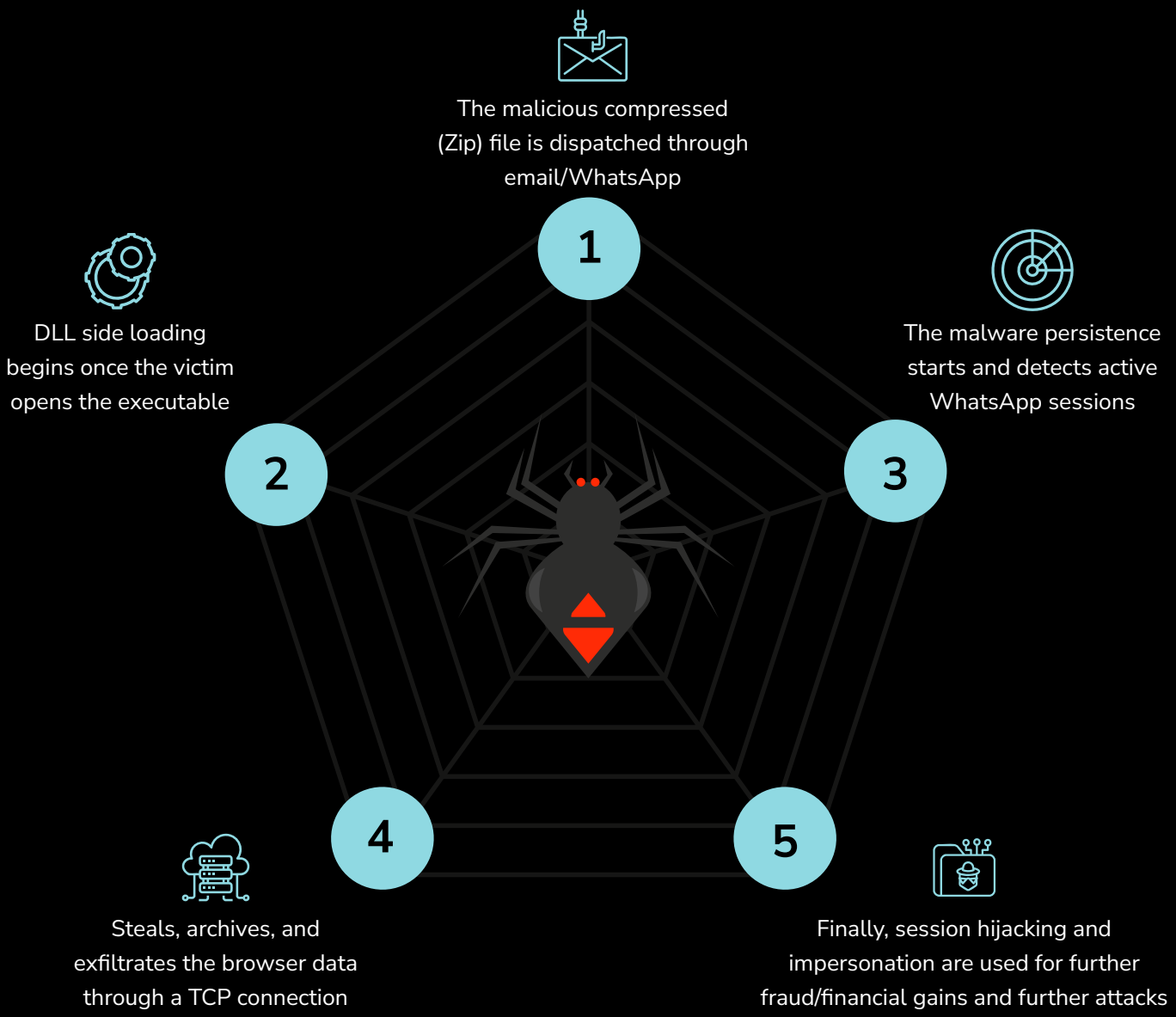
ENTERPRISE INSECURITY

Over the last few years, threat actors have shifted gears. Instead of launching a barrage of noisy attacks, they are staying lean and highly targeted, putting a bullseye on enterprises and public sector organizations for maximum impact. Among their arsenal of malicious weapons, Business Email Compromise has quietly become the most effective tool. More accurately, the weapon is compromised trust. By leveraging social engineering, criminals specifically target CXOs, making the Boss Scam its latest evolution.

The mechanics are simple but devastating. Attackers impersonate senior executives to trick victims into opening attachments or authorizing bank transfers.

The following kill chain breaks down this threat in sequence.

CASE STUDY: THE BOSS TRUST EXPLOITATION



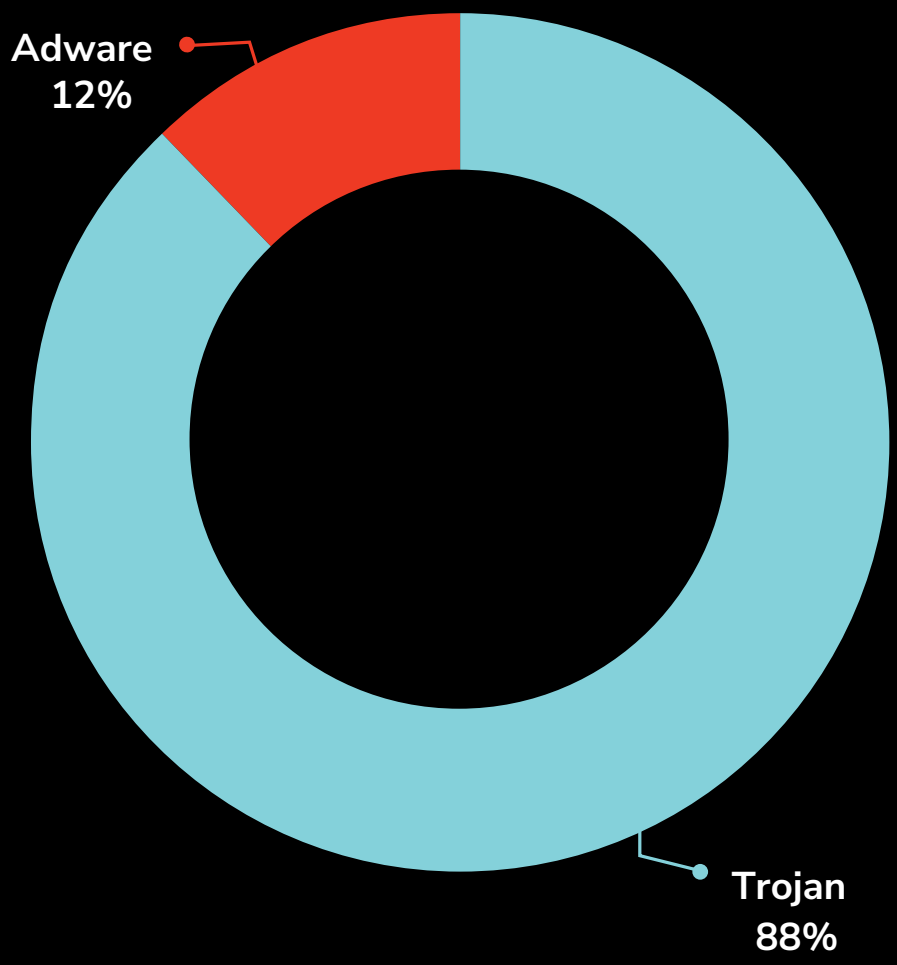
For further reading, see our detailed kill chain analysis.

Back To Contents

THE SHIFT IN GLOBAL MOBILE THREAT VECTORS

Global mobile threat data shows a massive consolidation toward high-impact attacks. Trojans now account for 88% of all mobile malware volume, while adware accounts for the remaining 12%.

Trojan vs. Adware Proportional Split



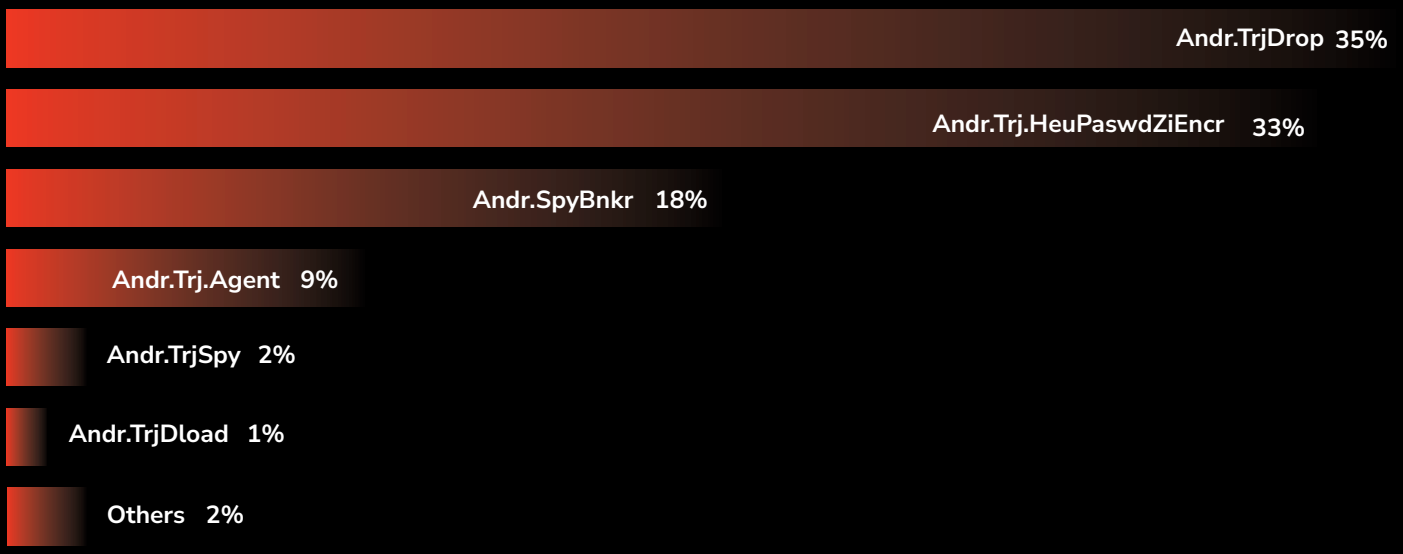
This division indicates a clear shift away from simple advertising nuisances toward aggressive, access-driven corporate espionage. While adware quietly siphons basic user data, modern Trojan campaigns establish stealthy beachheads designed to bypass security perimeters, harvest enterprise credentials, and disrupt business operations.

Back To Contents

HOW TROJAN DROPPERS PIERCE CORPORATE DEFENSES

Recent threat telemetry highlights a strategic move toward multi-tiered, low-visibility operations. Trojan droppers lead the category at 35%, closely followed by heuristic password-encrypting threats at 33%. Together, these two categories account for over two-thirds of all malicious mobile activity. Advanced threat actors have largely abandoned simple, single-stage exploits. Instead, they deploy modular campaigns engineered for prolonged, undetected network access.

The Rising Tide of Mobile Trojans



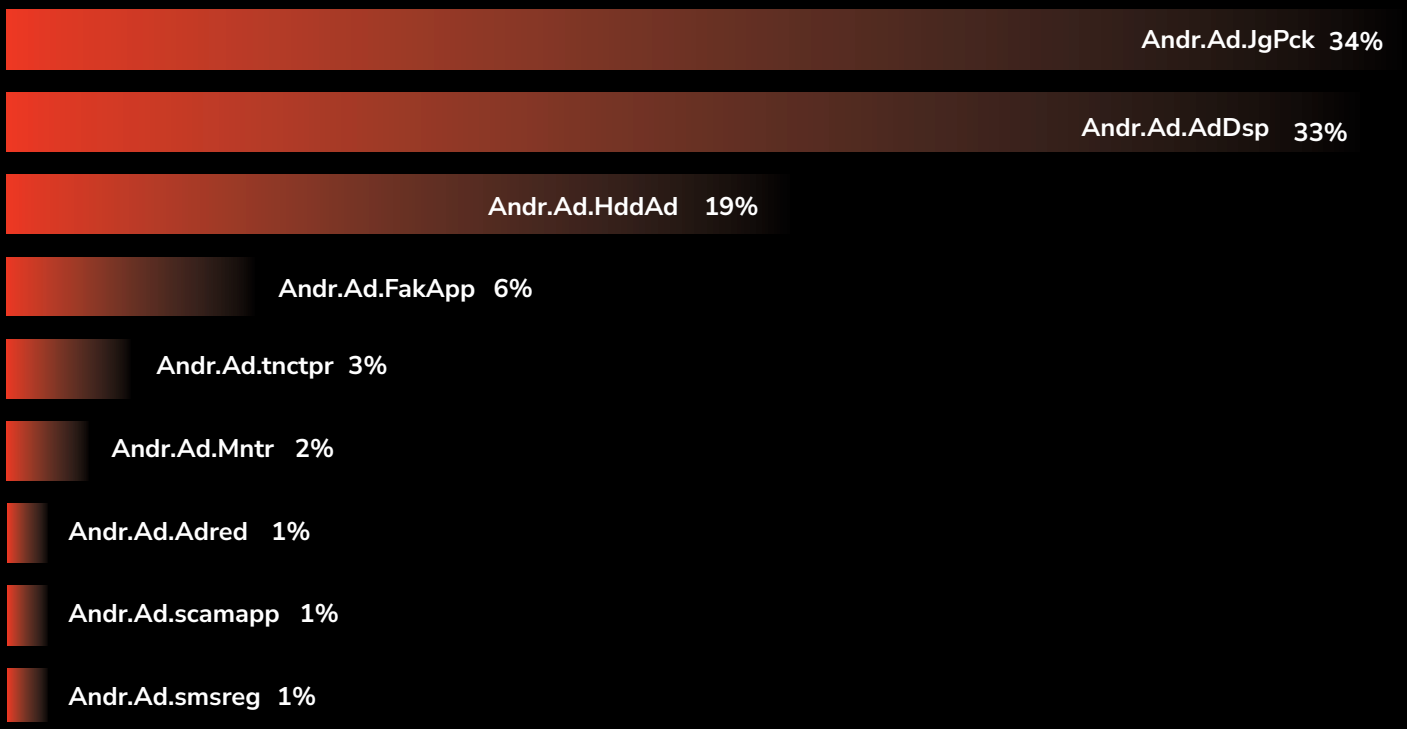
Attackers routinely disguise these sophisticated droppers and credential-harvesting implants as ordinary business software. This tactic takes advantage of the loose security boundaries common in hybrid work models. These low-signature threats easily evade automated app-store filters and perimeter defenses. Once inside, they allow threat groups to map internal network topologies, bypass multi-factor authentication (MFA) systems, and deploy targeted secondary payloads. For example, banking spyware accounts for 18% of these secondary threats, often customized for financial theft or espionage.

Back To Contents

MODERN ADWARE SERVES AS A NETWORK ENTRY POINT

The adware landscape reveals a similar transition toward hidden, systemic exploitation. This segment is heavily dominated by specific packaging utilities and display frameworks:

Most Prevalent Adware Types



Packaging engines like JgPck account for 34% of detections, while display frameworks like AdDsp account for 33%. When paired with hidden modules like HddAd at 19%, these prominent vectors quietly take control of devices under the guise of everyday utility apps.

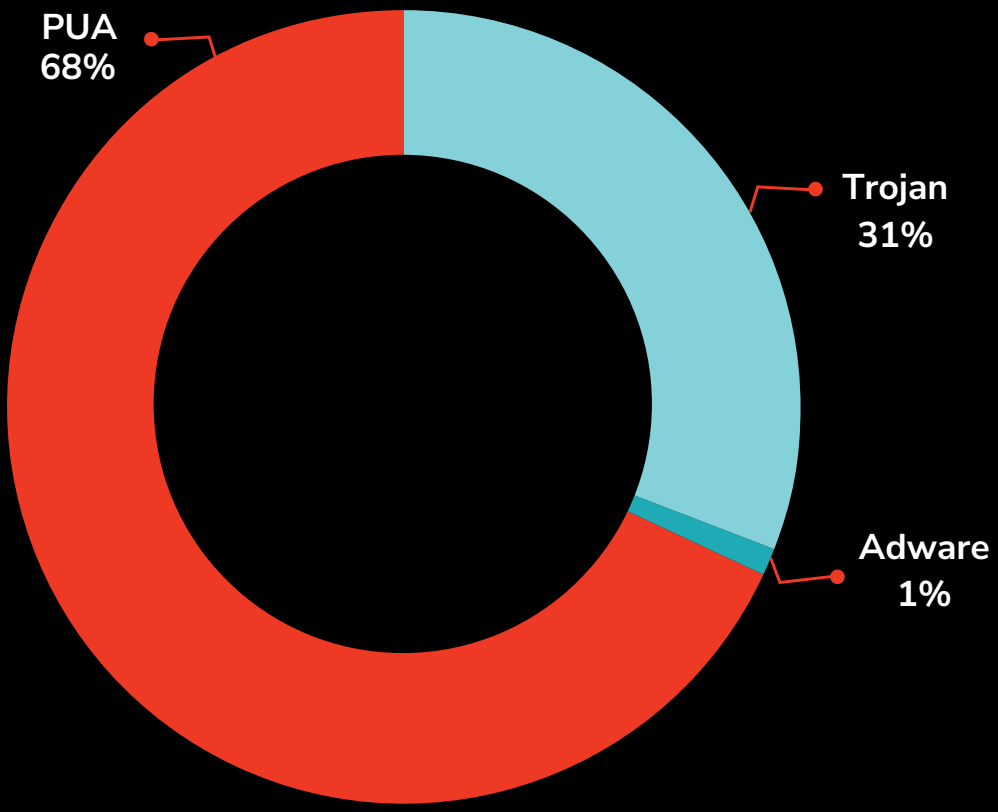
Today's adware goes far beyond delivering annoying pop-ups. It actively runs background tracking and gathers telemetry to map out user environments. This activity drains device productivity and hands sophisticated attackers a direct, unmonitored shortcut into enterprise networks.

Back To Contents

THE EVOLUTION OF THE MACOS THREAT LANDSCAPE

The long-standing belief in Apple invulnerability no longer matches corporate reality. Attackers have shifted their focus away from complex, brute-force exploits to deploy low-signature initial access operations. Modern threats target macOS by quietly infiltrating endpoints to build persistence and extract high-value user credentials.

Trojan, Adware, and PUA Proportional Split



Recent telemetry confirms that Potentially Unwanted Applications (PUAs) dominate the landscape at 68% of all detections. High-impact Trojans account for 31% of volume, while traditional adware accounts for a mere 1%.

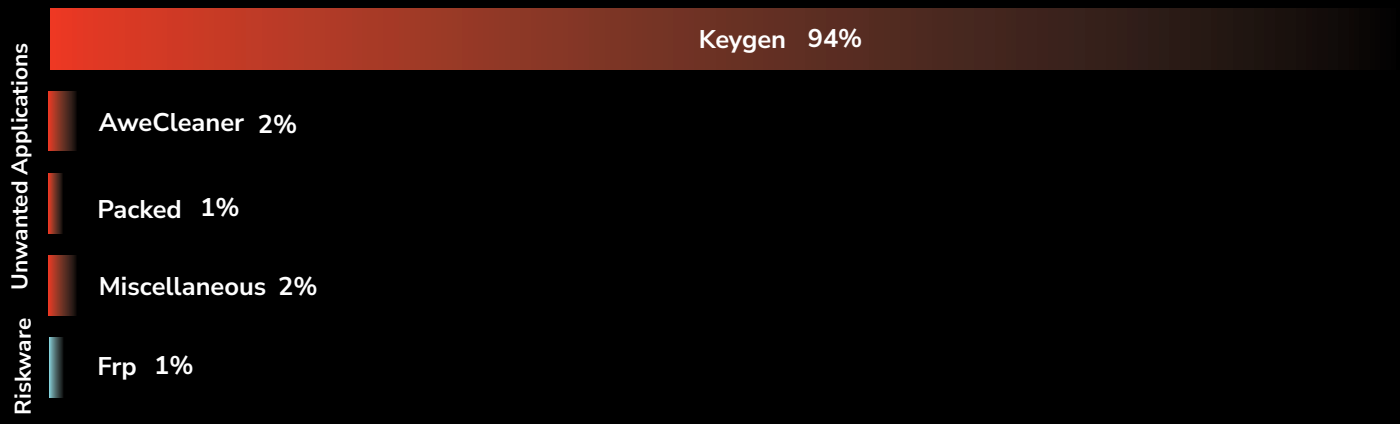
This footprint reveals that threat actors heavily rely on grayware to slip past perimeter defenses. Disguised as legitimate utility software, these applications establish quiet footholds on corporate endpoints. Once active, they serve as staging infrastructure to deliver damaging Trojan payloads, triggering data leaks and severe business disruption.

Back To Contents

SHADOW IT AND POTENTIALLY UNWANTED PROGRAMS (PUPS)

The widespread use of unapproved applications and pirated software introduces severe vulnerabilities into the corporate defense matrix. Telemetry reveals a massive concentration within the grayware ecosystem, where Keygen utilities command 94% of all Potentially Unwanted Application (PUA) volume. Secondary risks like AweCleaner at 2% and Frp riskware at 1% remain marginal by comparison.

The Trendline of PUP



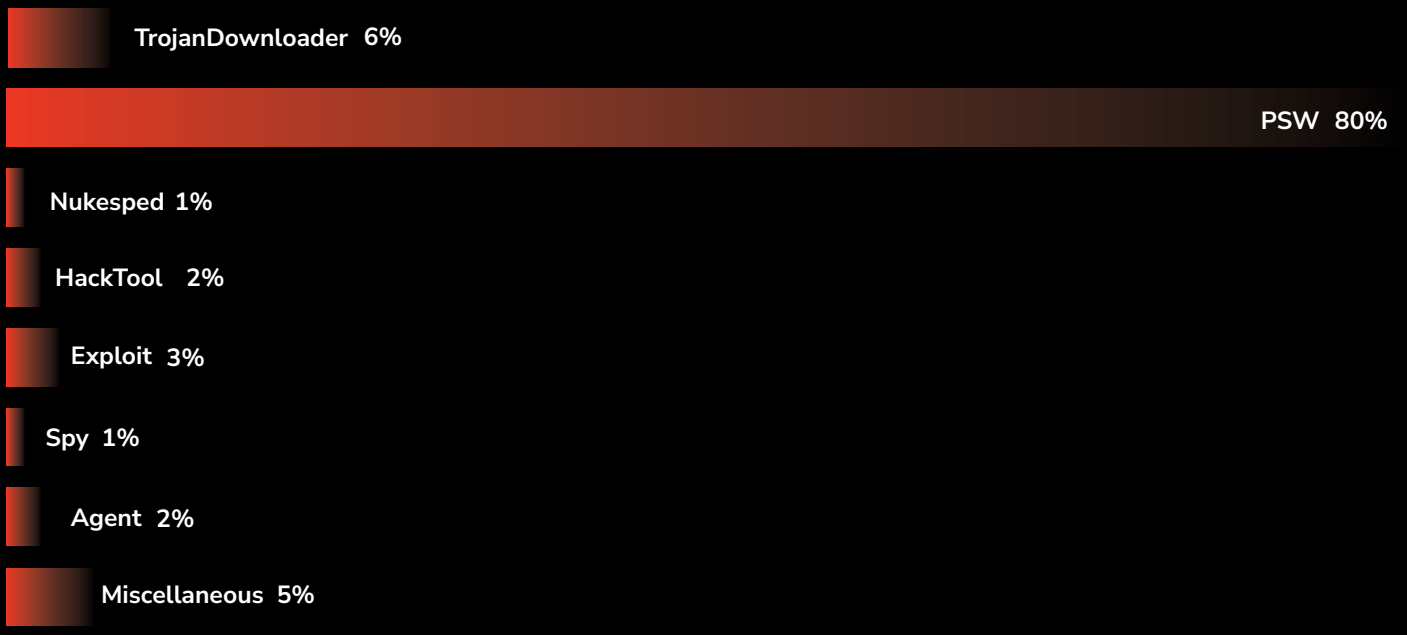
This lopsided distribution underscores how software-cracking tools serve as a primary gateway for enterprise intrusion. When users download these utilities to bypass licensing costs, they typically grant the software administrative privileges. Attackers exploit this access to alter core system files and deploy hidden payloads, including reverse shells and command infrastructure.

Back To Contents

IDENTITY THEFT TRIGGERS A SURGE IN MACOS TROJANS

Enterprise threat data highlights a sharp pivot toward identity and credential theft on macOS systems. Password Stealers (PSW) now command an overwhelming 80% of all Trojan threat volume. This concentration easily eclipses other specialized vectors, including exploits at 3% and Trojan downloaders at 6%.

Trojan Detection Trend Lines



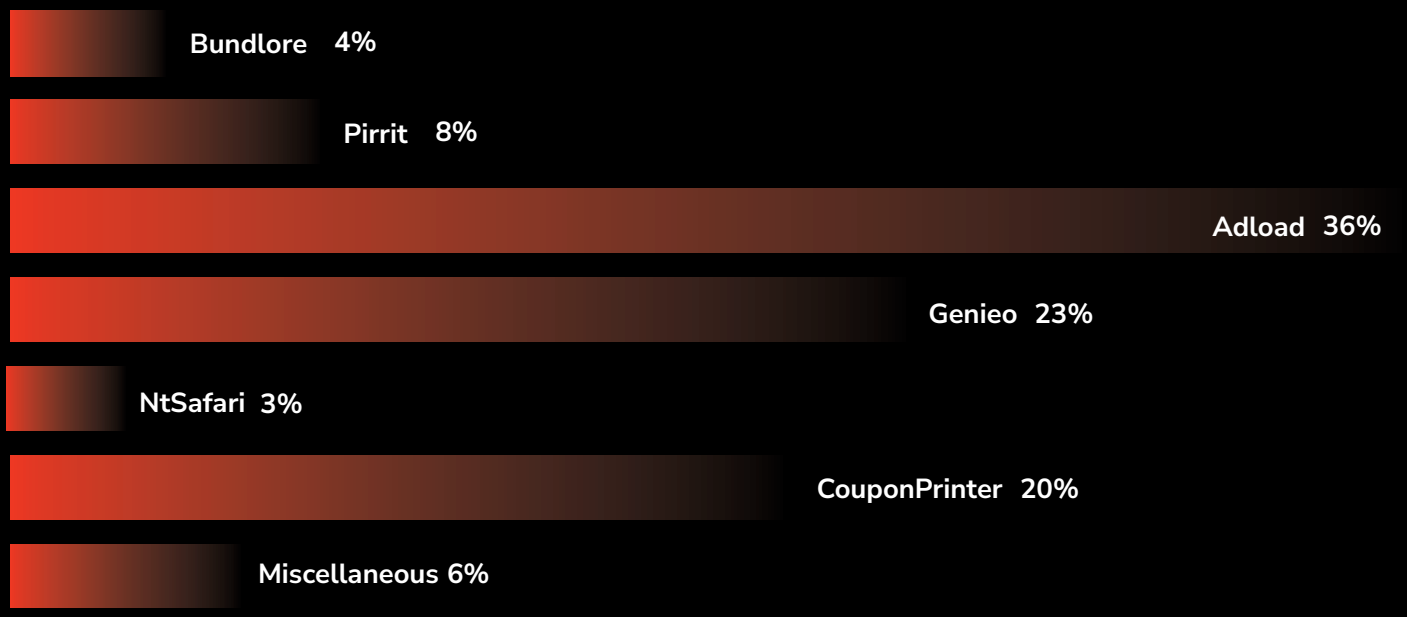
This distribution proves that adversaries prioritize stealing user identities over damaging underlying infrastructure. These silent tools focus on harvesting session tokens and browser data to bypass multi-factor authentication (MFA) workflows. For businesses, a compromised identity poses an acute risk, enabling threat actors to move laterally within internal networks and access sensitive cloud repositories.

Back To Contents

ADVANCED ADWARE ACTS AS AN ENTERPRISE THREAT GATEWAY

Adware on macOS has evolved far beyond an operational nuisance. Current endpoint telemetry shows a highly concentrated market dominated by three distinct variants:

The Trendline of Adware Variant Detections



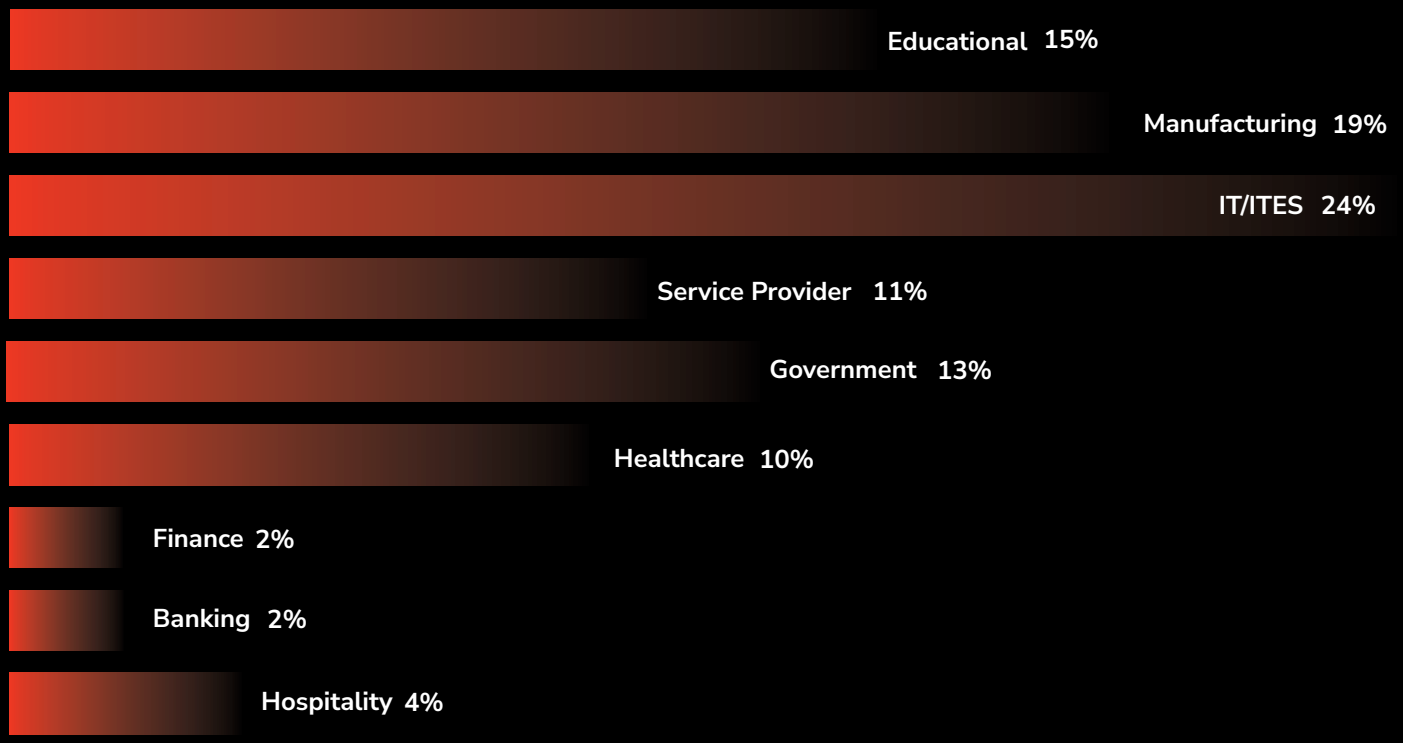
The persistent Adload variant leads the category at 36%, followed by Genieo at 23% and CouponPrinter at 20%. Together, these three strains account for nearly 80% of all adware activity. Instead of merely serving pop-up ads, these programs modify core system configurations and install unauthorized browser extensions to siphon off valuable user telemetry. This behavior transforms basic grayware into a severe corporate hazard, opening unmonitored backdoors that expose the enterprise to deeper downstream compromise.

Back To Contents

VULNERABILITIES GALORE

WIDESPREAD VULNERABILITIES

Attackers are no longer fixated on well-defended financial systems. Instead, they are zeroing in on the softer underbelly of global supply chains, especially in IT/ITES and manufacturing, where third-party networks often slip under the radar.



By slipping through these overlooked connections, a single vendor compromise can ripple outward, triggering large-scale disruptions and exposing critical infrastructure to both downtime and data theft. Security teams need to keep a constant, watchful eye on every digital dependency, not just the obvious ones.

Here is the list of the most prevalent vulnerabilities during the period Apr-Jun 2026 along with the relevant MITRE codes and necessary safeguards.

Back To Contents

SPLUNK ENTERPRISE

CVE-2026-20253 | CVSS 9.8 | Missing Authentication for Critical Function→Arbitrary File Creation/Truncation
IMPACT: Allows an unauthenticated, network-reachable attacker to create or truncate arbitrary files through a vulnerable PostgreSQL sidecar service endpoint. Successful exploitation can be leveraged to achieve remote code execution by overwriting executable files or scripts on the Splunk server.
MITRE T1190: Exploit Public-Facing Application
MITRE T1105: Ingress Tool Transfer
ACTION: Upgrade Splunk Enterprise to 10.0.7 or 10.2.4 (or later). If an immediate upgrade is not possible, disable the PostgreSQL sidecar service where feasible, restrict network access to the service, and ensure the affected endpoints are not exposed to untrusted networks.

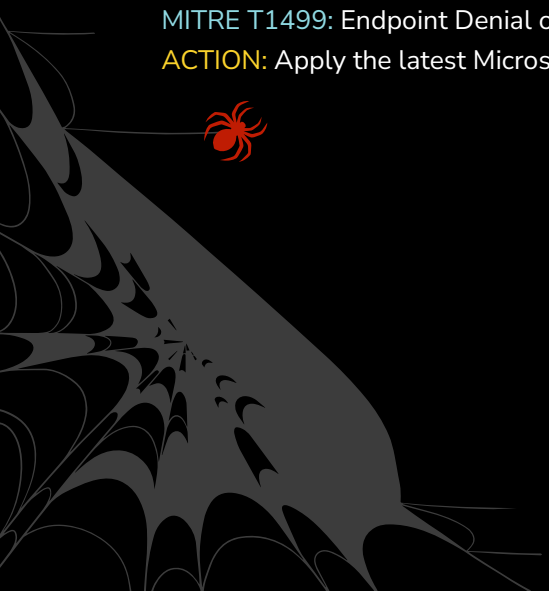
Trend Micro Apex One Server (On-Premise)
CVE-2026-34926 | CVSS 6.7 | Relative Path Traversal→Directory access
IMPACT: Allows an authenticated local attacker with administrative server access to modify a critical database table and inject malicious code for deployment to managed agents.
MITRE T1190: Exploit Public-Facing Application
MITRE T1059: Command and Scripting Interpreter
ACTION: Upgrade to the latest fixed version of Trend Micro Apex One as provided by Trend Micro and restrict administrative access to the Apex One server using least-privilege principles and strong authentication.

MICROSOFT DEFENDER VULNERABILITIES

CVE-2026-41091 | CVSS 7.8 | Link following→Privilege escalation
IMPACT: Allows an attacker to exploit an improper link resolution flaw to perform unauthorized file operations and elevate privileges to SYSTEM level on the affected system.
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Ensure Microsoft Defender and the operating system are kept fully patched and up to date.

CVE-2026-33825 | CVSS 7.8 | Insufficient Granularity of Access→Privilege escalation
IMPACT: Allows a low-privileged attacker to bypass intended authorization boundaries and execute operations with elevated privileges.
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Ensure Microsoft Defender and the operating system are kept fully patched and up to date.

CVE-2026-45498 | CVSS 4.0 | Uncontrolled Resource consumption→Denial of service
IMPACT: Allows an unauthenticated attacker with local access to exploit an uncontrolled resource consumption vulnerability by triggering excessive consumption of system resources, resulting in a denial-of-service condition.
MITRE T1499: Endpoint Denial of Service
ACTION: Apply the latest Microsoft security updates that address CVE-2026-45498



Back To Contents

MICROSOFT EXCHANGE SERVER

CVE-2026-42897 | CVSS 8.1 | Cross-site scripting→Server spoofing
IMPACT: Allows an attacker to deliver a specially crafted email which, when opened in Outlook Web Access (OWA) and user interaction requirements are met, executes arbitrary JavaScript in the victim's browser session, potentially enabling server spoofing.
MITRE T1059.007: Command and Scripting Interpreter- JavaScript
ACTION: Apply the latest Microsoft Exchange Server security updates, restrict access to Outlook Web Access where feasible.

PALO ALTO NETWORKS PAN-OS

CVE-2026-0300 | CVSS 9.3 | Buffer overflow→Execute arbitrary code with root access
IMPACT: Allows an unauthenticated remote attacker to send specially crafted packets that trigger arbitrary code execution with root privileges.
MITRE T1190: Exploit Public-Facing Application
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Apply the vendor security updates immediately and restrict access to the User-ID Authentication Portal to trusted internal IP addresses only, in accordance with Palo Alto Networks security best practices.

FORTINET FORTICLIENT EMS

CVE-2026-21643 | CVSS 9.1 | SQL Injection→Execute unauthorized code
CVE-2026-35616 | CVSS 9.1 | Improper access control→Execute unauthorized code
IMPACT: Allows an unauthenticated remote attacker to send specially crafted HTTP requests that manipulate backend SQL queries, potentially resulting in unauthorized command execution on the affected server.
MITRE T1059: Command and Scripting Interpreter
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Immediately apply the vendor-provided security updates for FortiClient EMS, restrict access to the management interface, and monitor for suspicious HTTP requests.

ADOBE ACROBAT AND READER

CVE-2026-34621 | CVSS 8.6 | Prototype pollution→Execute code execution
IMPACT: Allows an attacker to achieve arbitrary code execution in the context of the current user when a victim opens a specially crafted malicious PDF file.
MITRE T1204.002: User Execution: Malicious File
MITRE T1059: Command and Scripting Interpreter
ACTION: Upgrade Adobe Acrobat Reader to a patched version immediately and educate users to avoid opening PDF files from untrusted or unsolicited sources.

Apache ActiveMQ

CVE-2026-34197 | CVSS 8.8 | Improper Input Validation→Remote Code Execution
IMPACT: Allows an authenticated attacker to achieve remote code execution on the Apache ActiveMQ broker by abusing the exposed Jolokia JMX-HTTP bridge to invoke vulnerable MBean operations with a crafted discovery URI, causing a malicious remote Spring XML application context to be loaded and executed on the broker JVM.
MITRE T1190: Exploit Public-Facing Application
MITRE T1059: Command and Scripting Interpreter

Back To Contents

MITRE T1505.003: Server Software Component
ACTION: Upgrade Apache ActiveMQ Classic to 5.19.4 or 6.2.3 (or later). If immediate patching is not possible, restrict or disable access to the Jolokia JMX-HTTP endpoint (/api/jolokia/), limit JMX access to trusted administrators only, and enforce strong authentication and network segmentation to prevent unauthorized access.

MICROSOFT HTTP.SYS MODULE

CVE-2026-49160 | CVSS 7.5 | HTTP/2 Bomb Attack→Denial Of Service
IMPACT: Allows an unauthenticated local attacker to exploit uncontrolled resource consumption in HTTP/2 by leveraging the HTTP/2 Bomb attack, sending specially crafted requests with highly compressed headers that force a vulnerable server to allocate large amounts of memory and processing resources, resulting in a denial-of-service condition over the network.
MITRE T1499: Endpoint Denial of Service
MITRE T1499.001: OS Exhaustion Flood
ACTION: Apply the latest Microsoft security updates that address CVE-2026-49160.

MICROSOFT BITLOCKER

CVE-2026-50507 | CVSS 6.8 | Protection mechanism failure→Security Feature Bypass
IMPACT: Allows an unauthenticated attacker with physical access to a vulnerable Windows system to exploit this failure in the BitLocker protection mechanism to bypass Device Encryption and gain unauthorized access to data stored on the encrypted drive.
MITRE T1562.001: Disable or Modify Security Tools
ACTION: Apply the latest Microsoft security updates and ensure BitLocker is configured according to Microsoft's security best practices, including using TPM with a PIN or startup authentication where appropriate.

IOT VULNERABILITIES

Cisco Catalyst SD-WAN Controller
CVE-2026-20182 | CVSS 10.0 | Bypass authentication→Administrative privileges
CVE-2026-20128 | CVSS 7.5 | Stored passwords→Information Disclosure
IMPACT: Allows an unauthenticated remote attacker to exploit this vulnerability by sending crafted HTTP requests to bypass authentication and obtain administrative privileges on a system.
MITRE T1190: Exploit Public-Facing Application
ACTION: Immediately upgrade affected systems to the vendor-fixed version, restrict management interface access to trusted networks, and monitor for unauthorized administrative logins and configuration changes.

Ubiquiti Unifi
CVE-2026-34910 | CVSS 10.0 | Improper Input Validation→Command Injection
IMPACT: Allows an unauthenticated attacker to exploit an Improper Input Validation vulnerability found in UniFi OS devices to execute a Command Injection.
MITRE T1190: Exploit Public-Facing Application
MITRE T1059.004: Unix Shell
ACTION: Apply the latest UniFi OS security updates provided by Ubiquiti to remediate CVE-2026-34910.

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.

Fake Microsoft Teams Campaign

- A campaign leveraging convincing Microsoft Teams themed luring potential victims to deliver a multistage malware framework culminating in ValleyRAT deployment.
- Has evasion and stealthy capabilities and sending the victims' sensitive data to the threat actor's C2 server.
- Refer to our ValleyRAT blog for details

RVTools Masquerades to deploy Python RAT

- Threat actors are abusing RVTools, a go-to utility for VMware administrators, by distributing a trojanized installer carrying a valid Sectigo digital signature to stealthily deploy a modular Python RAT.
- Capability of exfiltrating sensitive host data and establishing persistent attacker access.
- Refer to our PythonRAT blog for details

Phishing Campaign deploying REMCOS RAT

- This blog discusses how threat actors leverage a bank and GST-based phishing campaign to deploy a REMCOS RAT payload via multi-stage loaders using Steganography and in-memory execution techniques (fileless malware).
- Refer REMCOS for deets.

Back To Contents

OUR VERDICT

Key Takeaways

The threat landscape no longer deals in one-off breaches. Instead, we see a calculated offensive targeting the very dependencies that keep operations running. Attackers twist outdated infrastructure, rogue software, and silent droppers into tools that leave classic defenses groping in the dark. For any business wired into the global grid, these cracks in the foundation can turn routine digital hiccups into full-blown operational meltdowns.

Key Observations:

- Our telemetry paints a picture of a threat perimeter splintering into ever more tangled and unpredictable shapes.
- Construction, textiles, and FMCG top the global hit list, with banking and pharma trailing close behind.
- The surge in droppers signals a shift: attackers now lean hard on 'living-off-the-land' tricks to slip past old-school defenses.
- Legacy systems remain buzzing hives for threat actors, teeming with opportunity.
- Unapproved apps and pirated software punch gaping holes in the corporate shield, inviting trouble.

K7 Mitigations:

- Enforce a rule that explicitly highlights how low-sophistication vectors (such as shadow IT, unauthorized software, or legacy endpoints) are exploited by advanced threat actors to achieve high-impact outcomes.
- If a section is designated as an Incident Pattern Analysis or Threat Landscape Snapshot, explicitly forbid the inclusion of defensive advice, remediation steps, or generic best practices.

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 such as malware analysis and threat hunting, fostering multifunctional expertise and reducing operational silos.

Leveraging Automation and Strategic Outsourcing

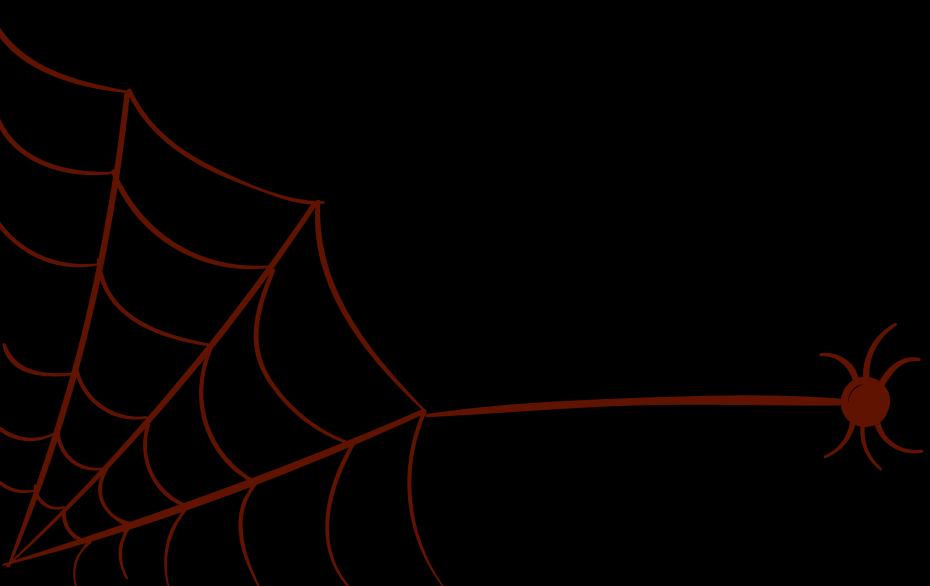
Automation is key to K7's approach. InfiniShield utilizes AI-driven threat detection, behavioral analysis, and deception technology to reduce false positives and accelerate response times. Its SOAR integration automates tasks such as patch deployment and malware containment, significantly reducing remediation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

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 that resources are allocated to threats that pose the greatest financial or operational risk.

Finally, K7's cloud-native solutions drastically reduce infrastructure costs. Their Cloud Endpoint Security uses lightweight, AI-driven agents to protect endpoints, 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_2026-27

K7 SECURITY

www.k7computing.com