

CYBER THREAT MONITOR REPORT

Q2 2026-27

- ▶ EXECUTIVE SUMMARY
- ▶ KEY HIGHLIGHTS
- ▶ A GRANULAR VIEW OF THE INDUSTRY THREAT LANDSCAPE

CYBER THREAT LANDSCAPE - INDIA

INDIAN TIER-1 CITY TRENDS

TOP INFECTION RATES IN TIER-2 CITIES

- ▶ ENTERPRISE INSECURITY
 - CASE STUDY: INSIDE THE WEAXOR RANSOMWARE CHAIN

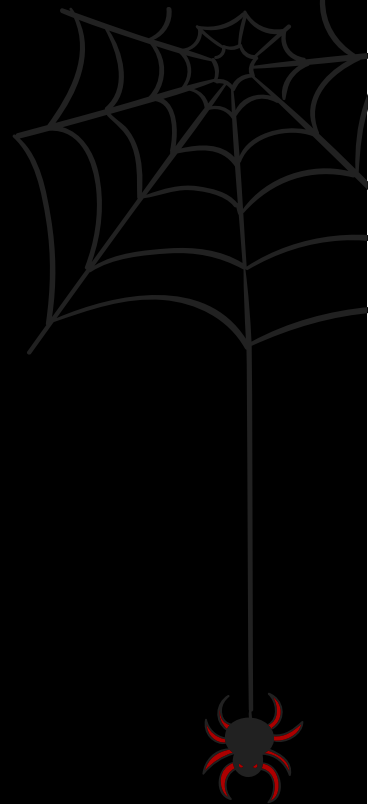
- ▶ WINDOWS THREAT LANDSCAPE
 - THE MALWARE PROLIFERATION
 - UNPATCHED VULNERABILITIES
 - CATCHING THE UNKNOWN (HIPS DETECTION)

- ▶ THE PERPETUAL SHIFT IN THE MOBILE SPACE
 - NOTABLE TARGETED ATTACKS
 - CASE STUDY: WHATSAPP BOSS SCAM
 - THE MYSTIFIED TROJANS
 - CASE STUDY: ANDROID OCTAGON RAT INFECTION CHAIN
 - THE LOOMING ADWARE

- ▶ THE EVOLUTION OF THE MACOS THREAT LANDSCAPE
 - THE DOMINANT PUA
 - THE SIGNIFICANCE OF TROJANS
 - ADVANCED ADWARE ACTS AS AN ENTERPRISE GATEWAY

- ▶ VULNERABILITIES GALORE
 - INDUSTRIES WITH THE HIGHEST VULNERABILITY CONCENTRATION
 - NETWORK & DEVICE VULNERABILITIES
 - MICROSOFT INTERNET KEY EXCHANGE (IKE) SERVICE EXTENSIONS
 - MICROSOFT SHAREPOINT SERVER
 - APPLE MACOS
 - APACHE TOMCAT
 - WORDPRESS CORE
 - NETWORK & DEVICE VULNERABILITIES
 - CISCO SECURE FIREWALL ADAPTIVE SECURITY APPLIANCE (ASA)
 - AND SECURE FIREWALL THREAT DEFENSE (FTD)
 - SONICWALL SMA1000 APPLIANCES
 - GOOGLE PIXEL

- ▶ CONCLUSION: THE SECURITY BOUNDARY HAS CHANGED
 - WHAT ORGANIZATIONS MUST DO DIFFERENTLY



EXECUTIVE SUMMARY

A single breach at a managed service provider, remote management platform, or any other supply-chain can quietly create a pathway into a multitude of businesses, turning trusted infrastructure into a launchpad for attacks. Attackers do not always need to break through an enterprise's hardened defenses when they can exploit the third-party providers those organizations already trust.

Three forces are accelerating this shift. Expanding digital ecosystems and increasingly complex webs of software and cloud integrations are pushing privileged access beyond traditional organizational boundaries. At the same time, cybercrime has become increasingly industrialized. Subscription-based attack platforms and crime-as-a-service models are lowering the barrier to entry, putting sophisticated tools and infrastructure within reach of less-skilled operators. Generative AI is adding another layer of acceleration, helping automate vulnerability discovery, personalize social engineering, and speed up attacks at a scale that enterprises may struggle to match.

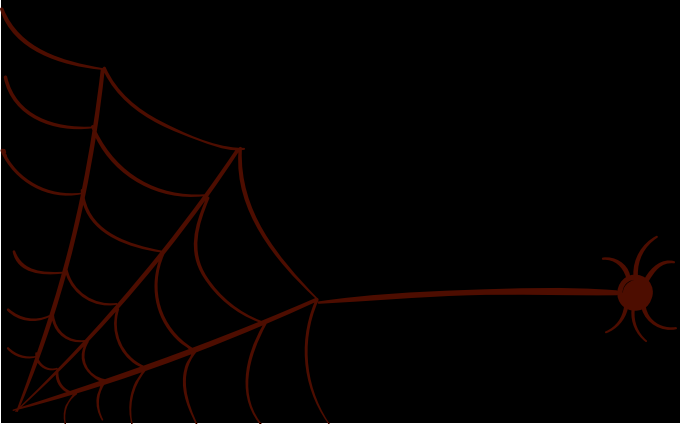
This quarter's telemetry reveals broad threat exposure across interconnected sectors. Textiles recorded the highest infection rate at 27%, followed by Consultants (25%) and FMCG, Hospitality, and Construction (23% each). Government and IT/ITES (21%), Pharmaceuticals (20%), and Service Providers (19%) also reported notable exposure, underscoring the need to assess risks across both operational environments and third-party relationships.

These sectors rely on extensive supplier networks, outsourced services, and shared digital infrastructure. A compromised vendor or trusted integration can open pathways into connected environments and extend the impact beyond the initial victim. In Textiles, FMCG, and Pharmaceuticals, disruptions can affect production and distribution. In hospitality and consultants, they can impact interconnected services and platforms.

As cybercrime platforms add automation and service capabilities, the conditions are increasingly favorable for complex, multi-stage attacks that exploit trusted relationships and interconnected infrastructure. Defending the modern enterprise therefore requires organizations to treat vendors, privileged access pathways, and critical software dependencies as part of their effective attack surface.

Read on for our latest findings and what organizations can do next.

And stay alert!



KEY HIGHLIGHTS

K7 CTM REPORT Q2 2026-27

1

IT/ITES, Manufacturing, Education, and Government were the most vulnerable sectors

2

Textiles, Consultants, Construction, FMCG, and Hospitality saw high infection rates

3

Legacy Windows network weaknesses drove 73% of observed threat activity

4

LOLBin executable, initial droppers, and registry tampering remained most favored by the adversaries

5

India's infection rate stood at 26%

Infection Rate (IR) of an area

Active K7 Users



Update
Notification



Blocked Threat
Event Notification



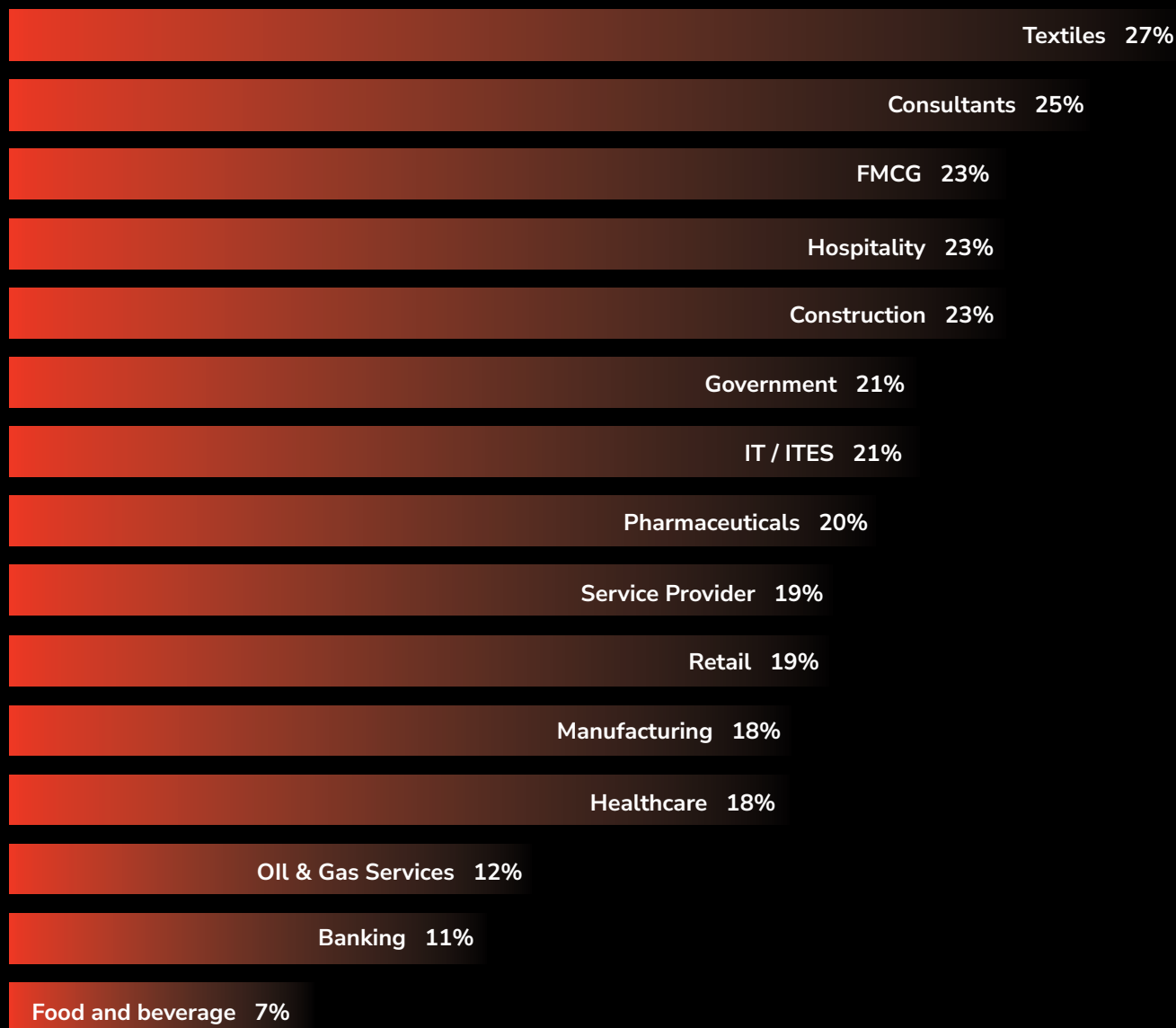
K7 Ecosystem
Threat Intelligence



Infection Rate at XYZ
 $4/50 = 8\%$

A GRANULAR VIEW OF THE INDUSTRY THREAT LANDSCAPE

Industry infection rate (IR) data offers a clear picture of the quarter and a fisheye view of how the threat landscape may evolve. Industries with the most infections are not necessarily easy targets; threat actors may focus on these sectors while ignoring others. Perpetrators usually have a clear agenda before targeting any industry, whether money or something more sinister.

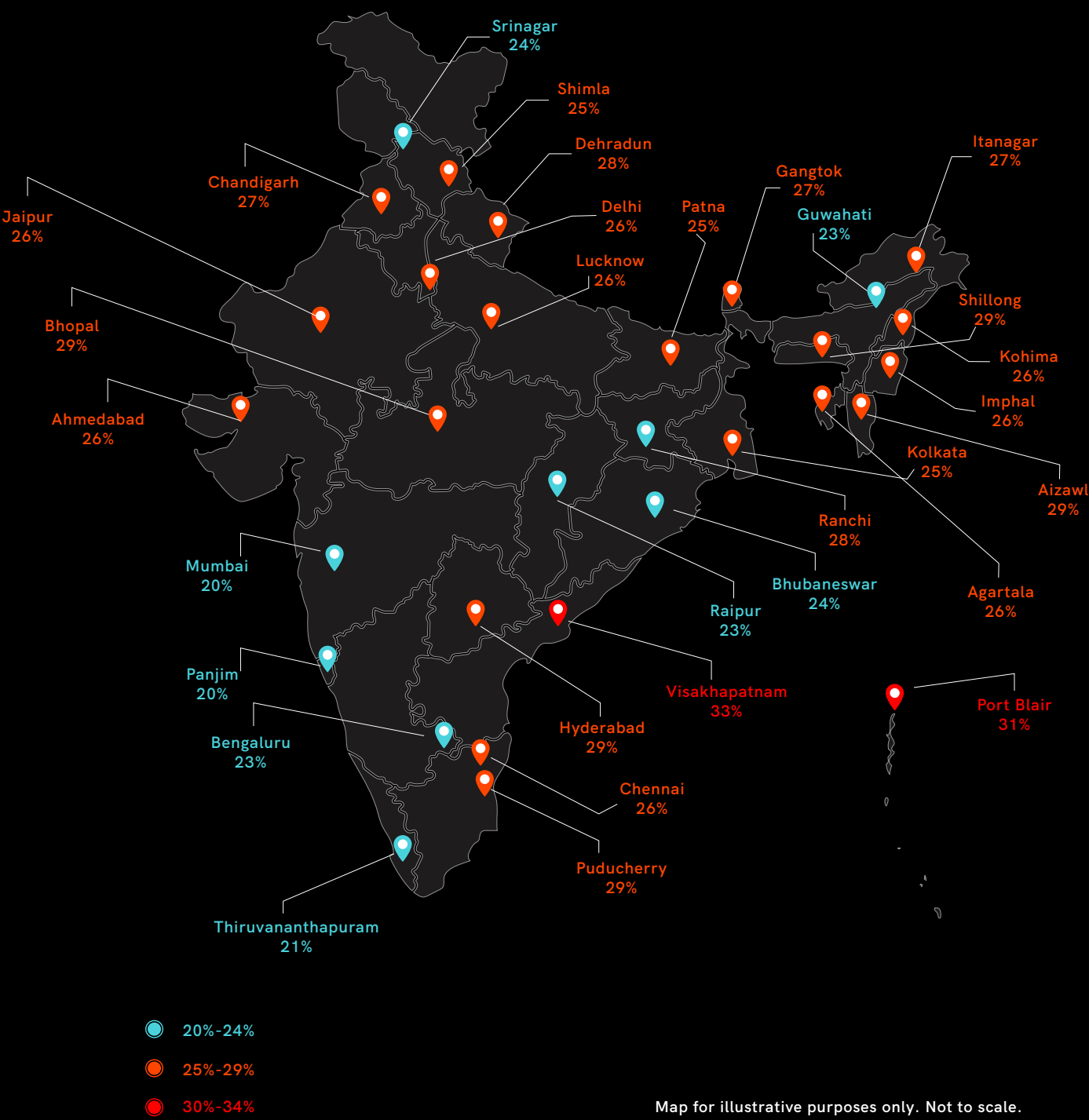


Textiles (27%) and Consultants (25%) recorded the highest infection rates, followed by FMCG, Hospitality, and Construction (23% each). These sectors' extensive vendor networks, outsourced infrastructure, and privileged client access can create pathways for compromise to spread. While infection rates alone do not prove supply-chain attacks, they highlight the exposure of highly connected businesses.

Industries reliant on third-party ecosystems face heightened threat exposure, highlighting supply-chain security risks.

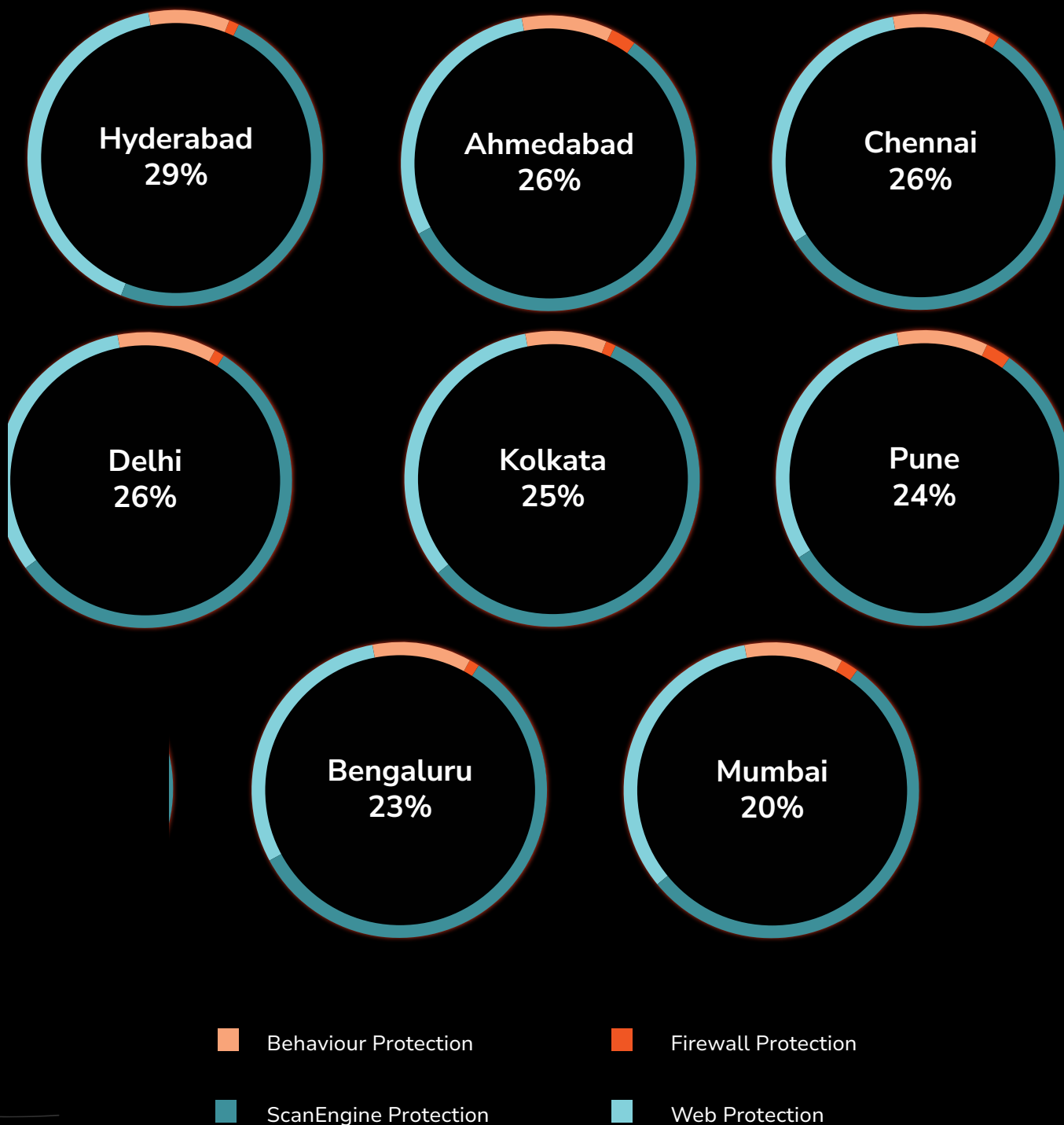


CYBER THREAT LANDSCAPE - INDIA



INDIAN TIER-1 CITY TRENDS

Tier-1 cities, home to large scale enterprises, are prime targets for sophisticated threat actors using novel initial access and long-term persistence tactics. The chart shows a significant presence of attacks, but most of this data represents automated opportunistic scanning. The most severe threats to these enterprise hubs come not from the high-volume noise but from stealthy, highly targeted campaigns.



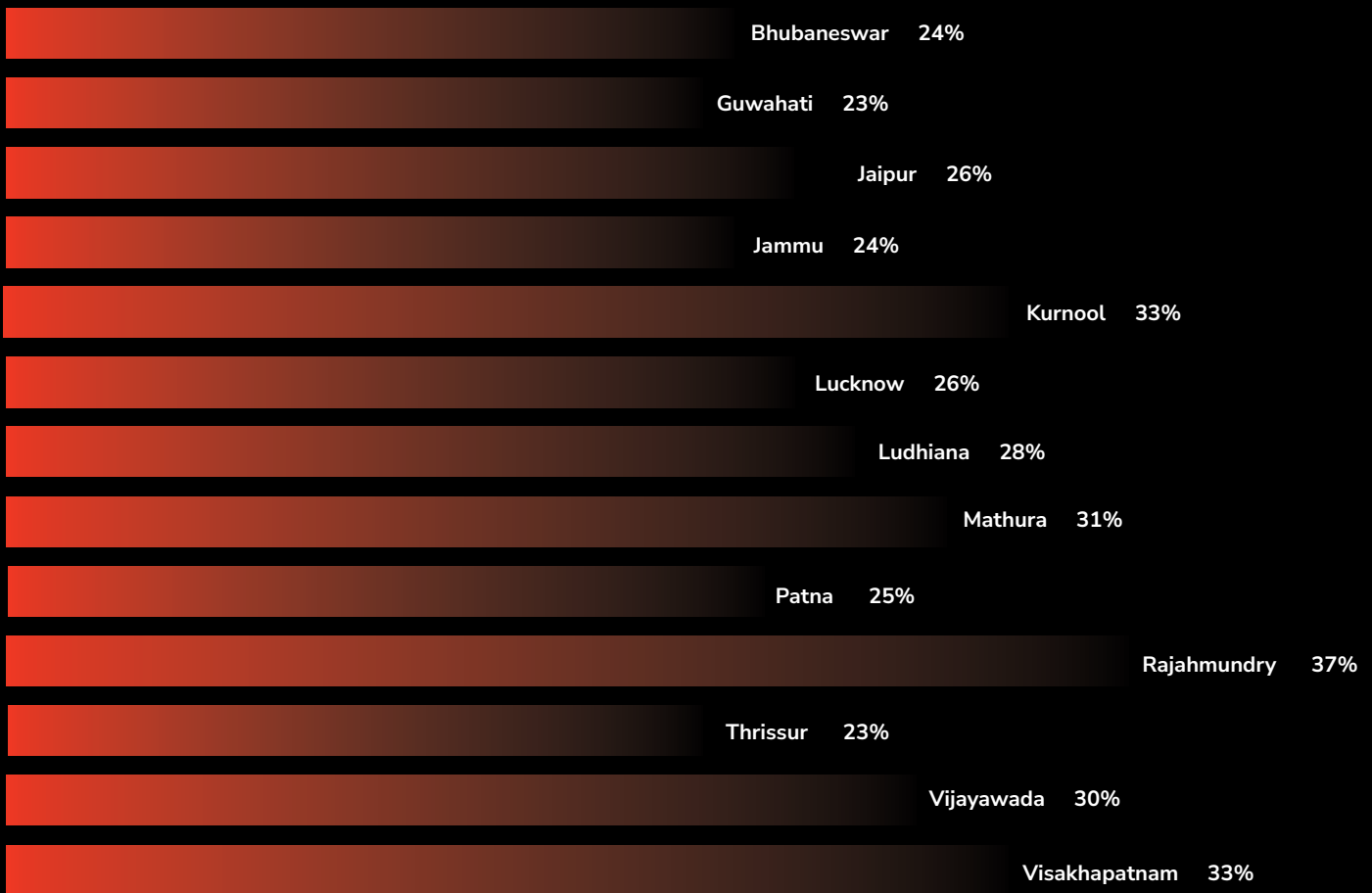
Tier-1 cities face high attack volumes, but stealthy, targeted campaigns pose the greater risk to enterprise security.



[Back To Contents](#)

TOP INFECTION RATES IN TIER-2 CITIES

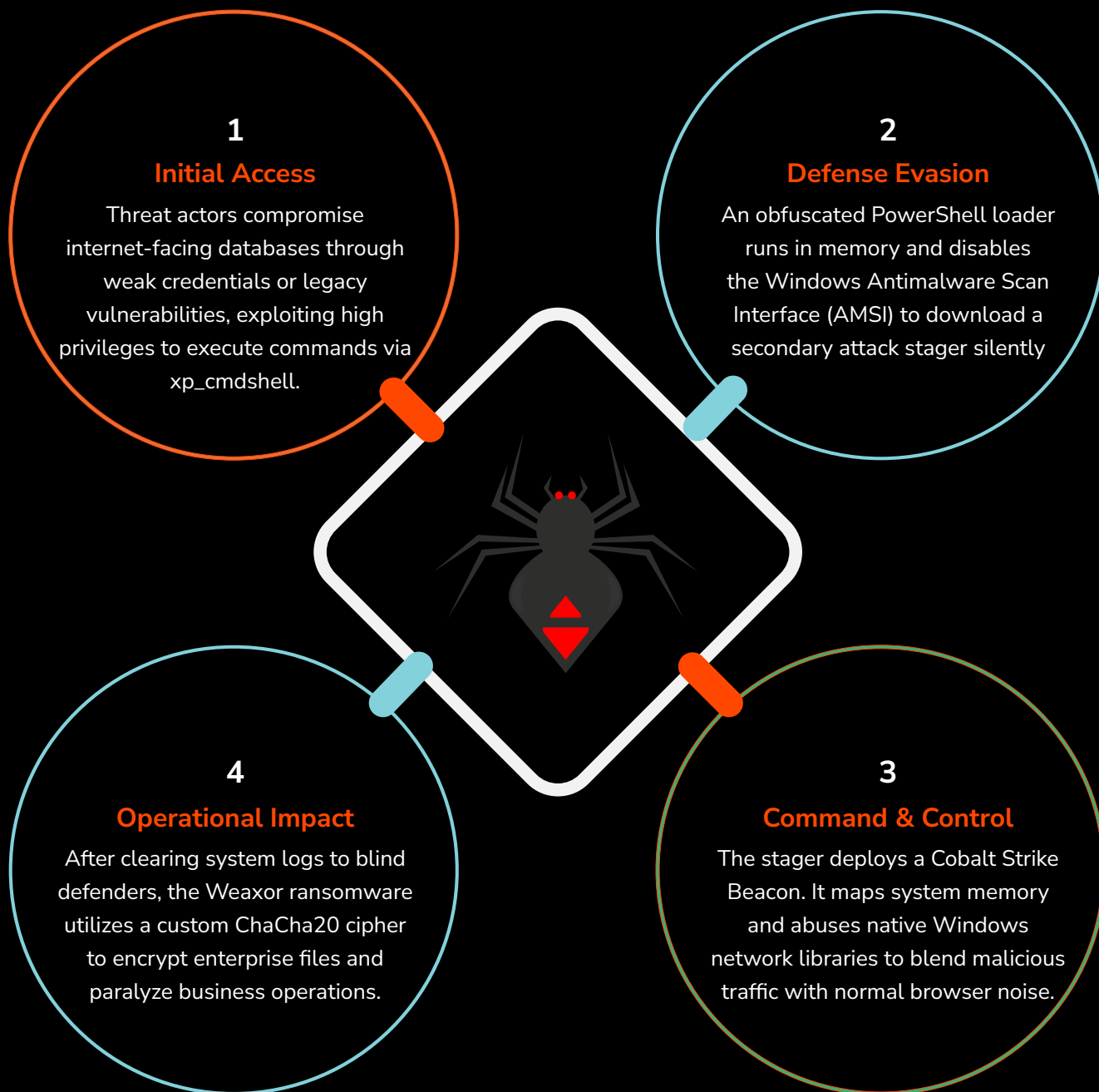
In India's Tier-2 cities, the rapid spread of digital technology has outpaced defensive measures, leaving security fragile. Unlike the highly targeted attacks in Tier-1 areas, activity here is mainly driven by opportunistic threats. These threat actors exploit outdated vulnerabilities, exposed remote assets, and poor security practices through automated campaigns. As a result, these growing economic centers suffer most from generic malware and random scanning because they quickly adopted new technologies without establishing security standards suitable for businesses.



ENTERPRISE INSECURITY

Adversaries often rebrand successful malware to bypass modern security controls. Weaxor, a highly evasive evolution of the infamous Mallox ransomware, does exactly that. By chaining together internet-facing SQL Server exploitation, layered PowerShell deobfuscation, and memory-resident Cobalt Strike Beacons, Weaxor represents a significant leap in attack sophistication. The infographic below breaks down the execution chain.

CASE STUDY: INSIDE THE WEAXOR RANSOMWARE CHAIN



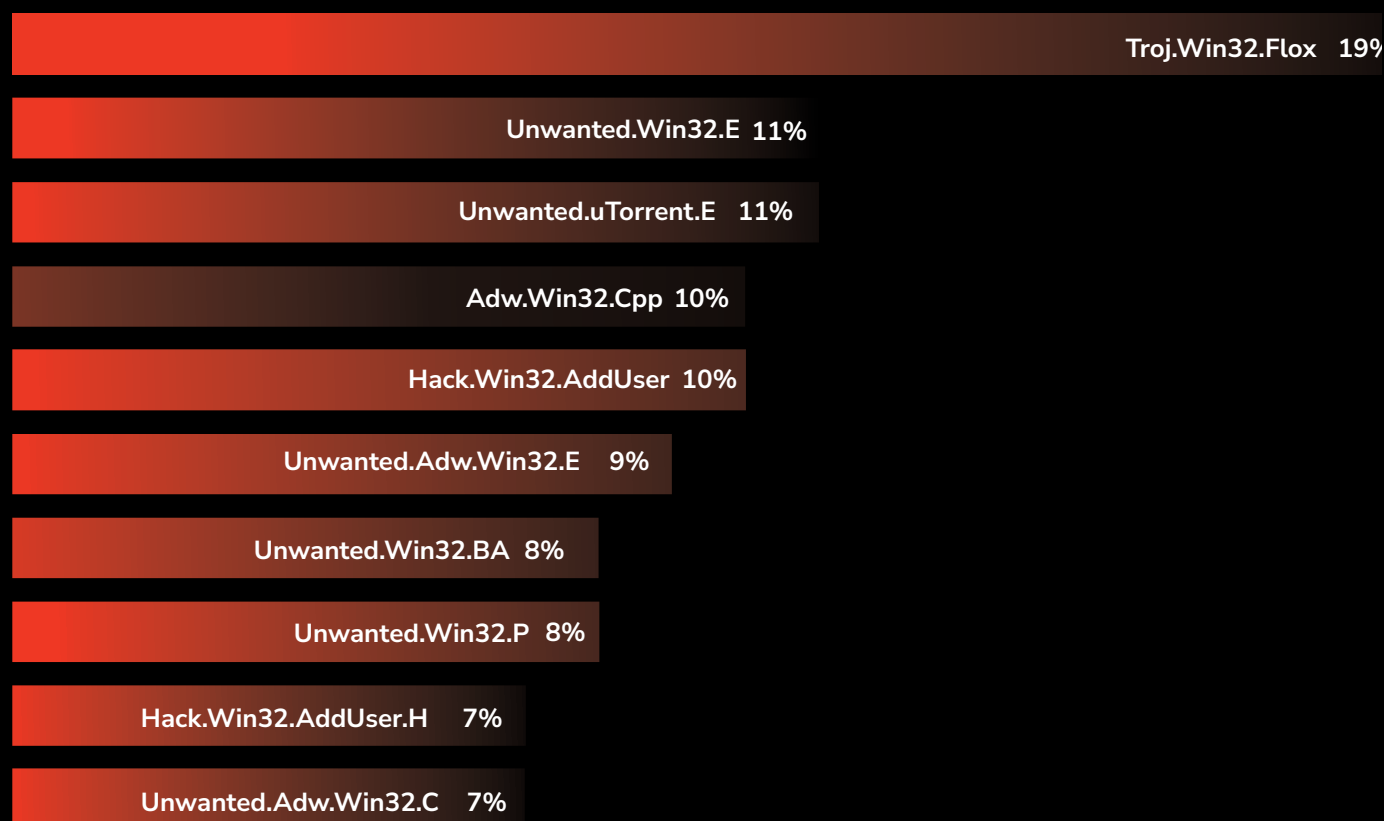
WINDOWS THREAT LANDSCAPE

Windows dominates the enterprise. Its near-universal deployment across corporate environments makes it the highest-value hunting ground for threat actors: more targets, credentials, and pathways into critical infrastructure. That concentration of exposure is why Windows-specific malware families continue to multiply and specialize.

THE MALWARE PROLIFERATION

The detection mix confirms this reality. Troj.Win32.Flox leads, occupying 19% of total visibility, and that prominence is not incidental. It is particularly precarious because of its capability to embed itself by modifying existing system files rather than dropping new ones, meaning standard removal can leave the infection structurally intact. Even when AV flags and quarantines it, the altered files remain. The device slows, freezes, and loses storage capacity while the compromise persists.

For enterprises running shared environments, domain-joined endpoints, or privileged workstations, that residual foothold is not an inconvenience. It is a standing entry point. A cleared alert does not equal a clean machine, and in a corporate network, that distinction carries serious consequences.

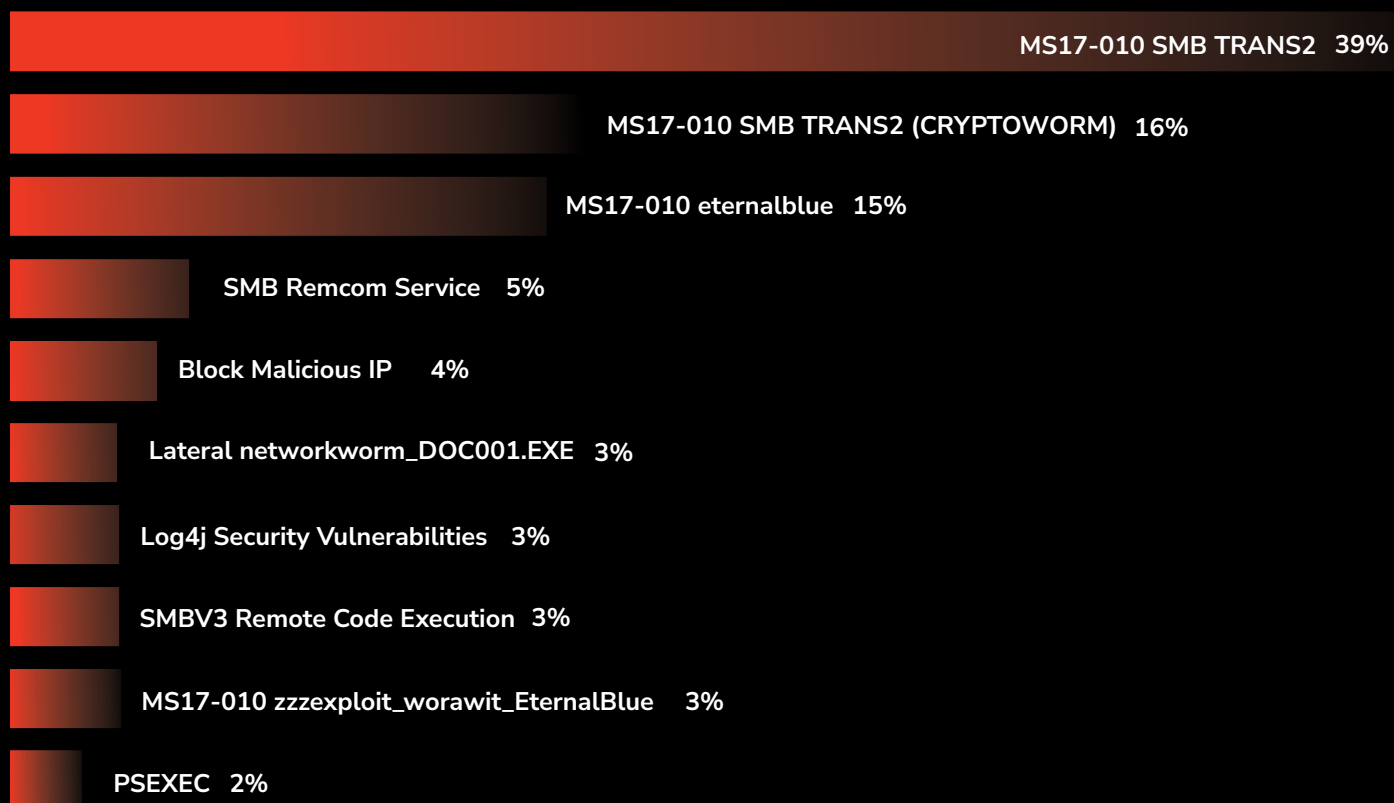


Below it, unwanted and adware variants fill most of the top slots, masking data harvesting as noise. Two Hack.Win32.AddUser variants (17%) create accounts and escalate privileges for lateral movement. Grayware lowers defenses, Trojans rewrite systems, and account manipulation secures control, leading to delayed breaches: stolen credentials, exposed data, and disruption.

From covert data harvesting to unauthorized access, Windows malware creates multiple pathways to data theft and enterprise compromise.

UNPATCHED VULNERABILITIES: WEAPONIZING THE CORPORATE PATCH GAP

Nearly a decade after Microsoft issued the patch, MS17-010 still sets the pace. Detections tied to these Server Message Block (SMB) weaknesses, including TRANS2, EternalBlue, and cryptoworm strains, account for 73% of observed activity. That figure is not a relic. It shows how much unpatched exposure remains inside enterprise networks.

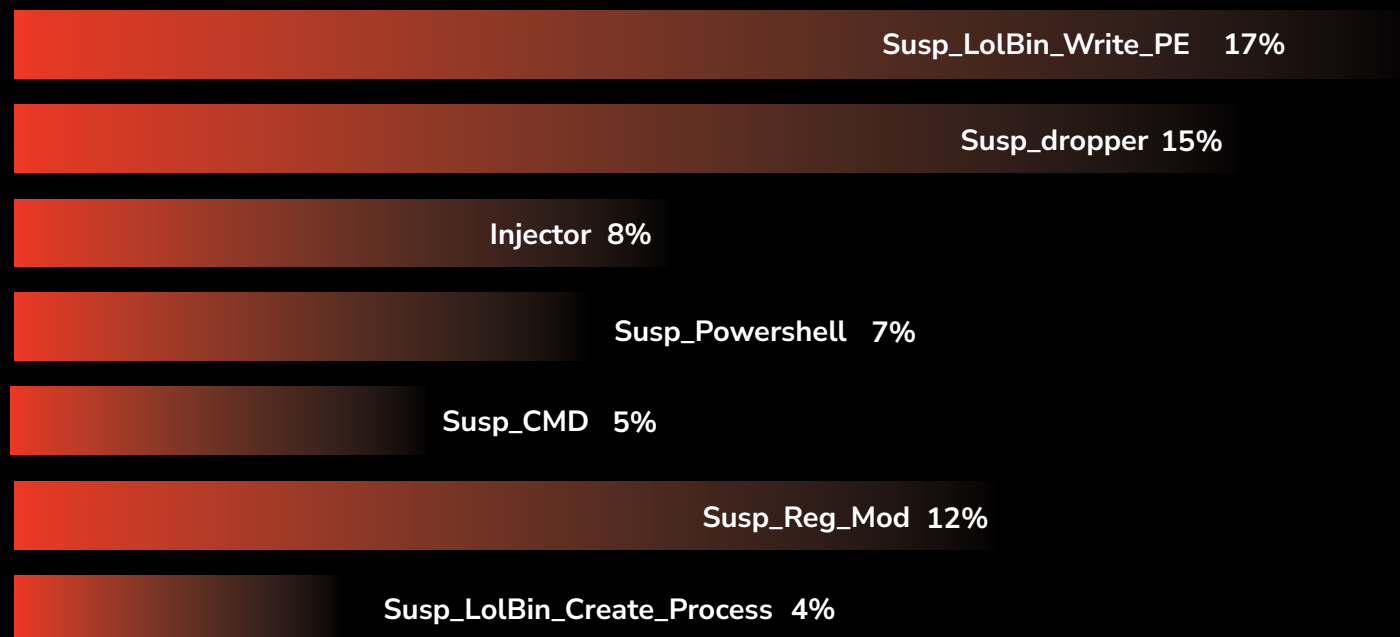


Attackers don't need zero-days when SMB, the protocol Windows uses for file sharing, still offers a backdoor that has never fully closed. Once inside, they combine self-propagating worms with administrative tools like PsExec and Remcom. They execute commands on remote machines disguised as routine IT activity. A single vulnerable endpoint becomes a launchpad. Compromise then cascades across connected systems at machine speed. For enterprises, the outcome is scale, not nuisance. Ransomware spreads domain-wide, operations halt, sensitive data is exposed, and financial losses multiply with every hour of downtime.

Legacy Windows vulnerabilities remain a persistent enterprise risk, enabling ransomware propagation and widespread network disruption.

CATCHING THE UNKNOWN (HIPS DETECTION)

These heuristic detections in Q2 signal a decisive shift. Attackers increasingly abuse native Windows utilities to blend malicious activity into legitimate system behavior, with suspicious LOLBin executable writes leading at 17%.



This data highlights how adversaries increasingly camouflage intrusions inside trusted operating system processes to circumvent conventional defenses within the current enterprise threat landscape.

Attackers combine initial droppers (15%) and process injection (8%) with registry tampering (12%), PowerShell, and command-line execution to establish evasive persistence. This use of legitimate system tools poses serious business risks by enabling prolonged, undetected access that causes widespread operational disruption, proprietary data compromise, and severe financial damage.

Attackers turn trusted Windows tools into covert entry points, putting enterprise data and operations at risk.



THE PERPETUAL SHIFT IN THE MOBILE SPACE

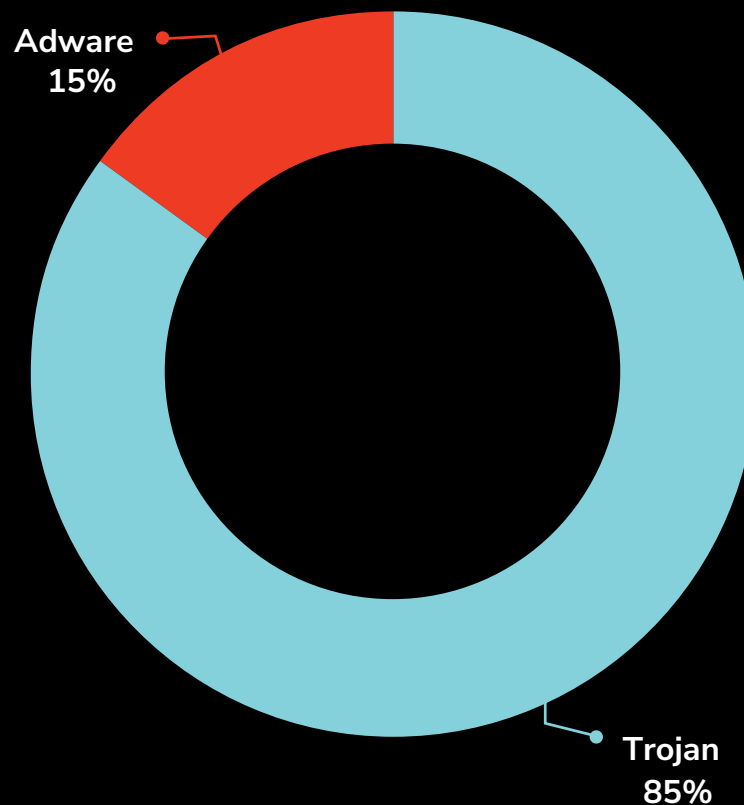
Mobile endpoints now sit at the crossroads of work and personal life, connecting everything in real time. Zero-days grab headlines, but they are not what keeps security teams on edge. The real grind comes from the endless tide of trojans and aggressive adware that quietly swamp enterprise environments.

Old risk models cannot keep up. Modern mobile trojans operate with precision, stealing credentials, intercepting multi-factor codes, and sidestepping identity checks almost effortlessly. Adware has evolved far beyond a minor nuisance. Hidden inside everyday apps, it now doubles as covert spyware: leeching data, breaking compliance, sneaking in third-party code, and pulling off a host of other malicious tricks right under IT's watch.

The impact on enterprises is broad and immediate. When a device succumbs to a trojan or gets choked by invasive adware, even the most tightly controlled workspaces and MAM containers begin to break down.

This is how trojans keep sweeping through the mobile landscape, leaving little untouched.

Trojan vs. Adware Proportional Split



Mobile Trojans steal credentials, while aggressive adware exposes enterprise data and weakens security.



NOTABLE TARGETED ATTACKS

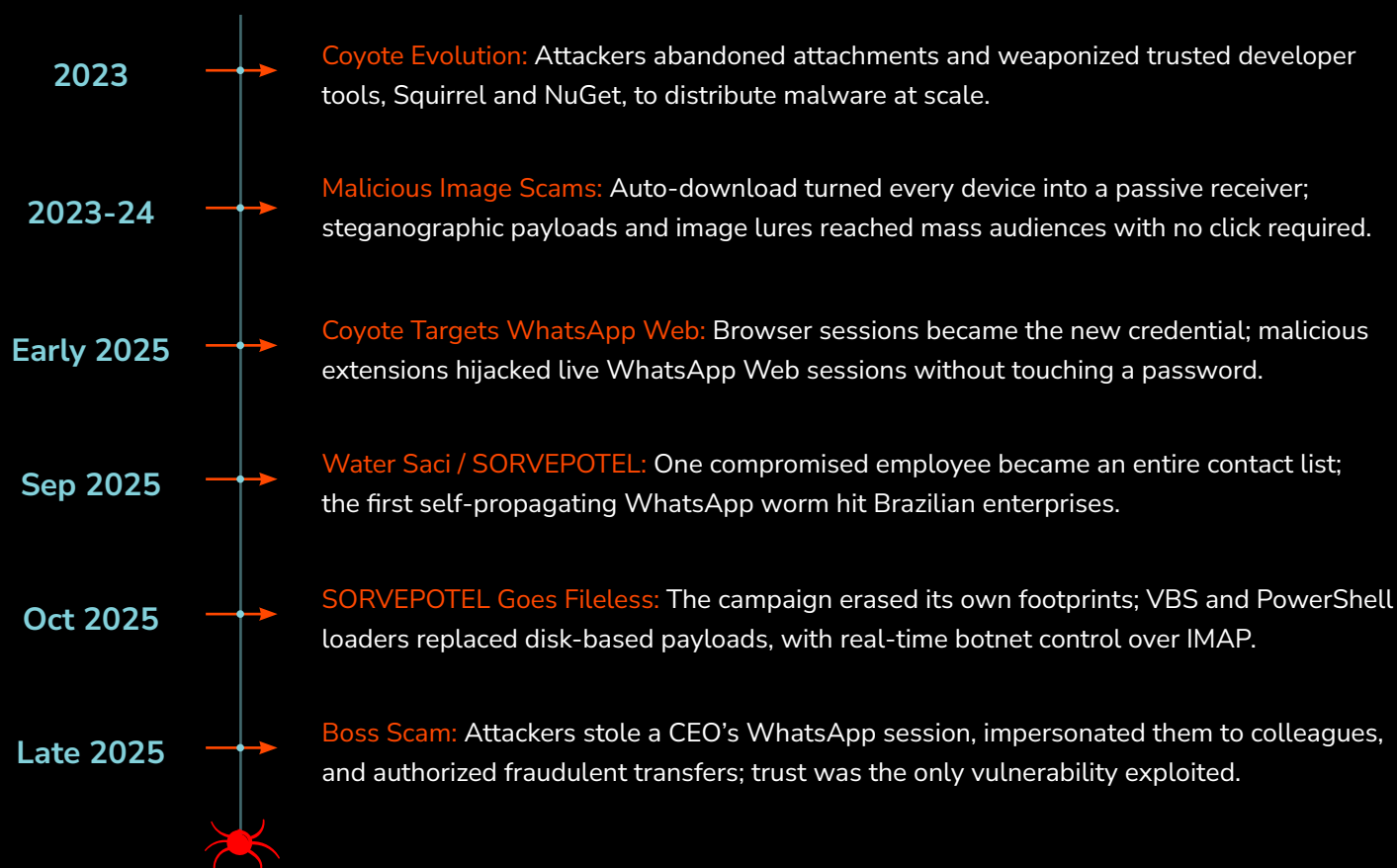
Smartphone vendors keep pushing platform-level defenses and security upgrades, but attackers aren't standing still. They keep finding critical holes, often in the most popular apps, especially in instant messaging. Smishing remains a favorite tactic for targeted attacks. The so-called boss scam on WhatsApp still dominates headlines in this space. Here is a closer technical look.

CASE STUDY: WHATSAPP BOSS SCAM

With over two billion active users globally, WhatsApp has become a primary business communication channel used by executives to approve decisions, finance teams to coordinate transfers, and employees to reach trusted colleagues. That ubiquity makes it lethal. A WhatsApp message carries implicit credibility that a cold email never could. It arrives on a personal device, from a saved contact, in a thread full of legitimate prior exchanges.

Attackers have studied this psychology carefully. They know that when your CEO sends an urgent message, you do not pause to question the sender. You act. Businesses of all sizes, from regional SMBs to global enterprises, share the same vulnerability: a platform they depend on for speed has become a vector adversaries exploit with surgical precision.

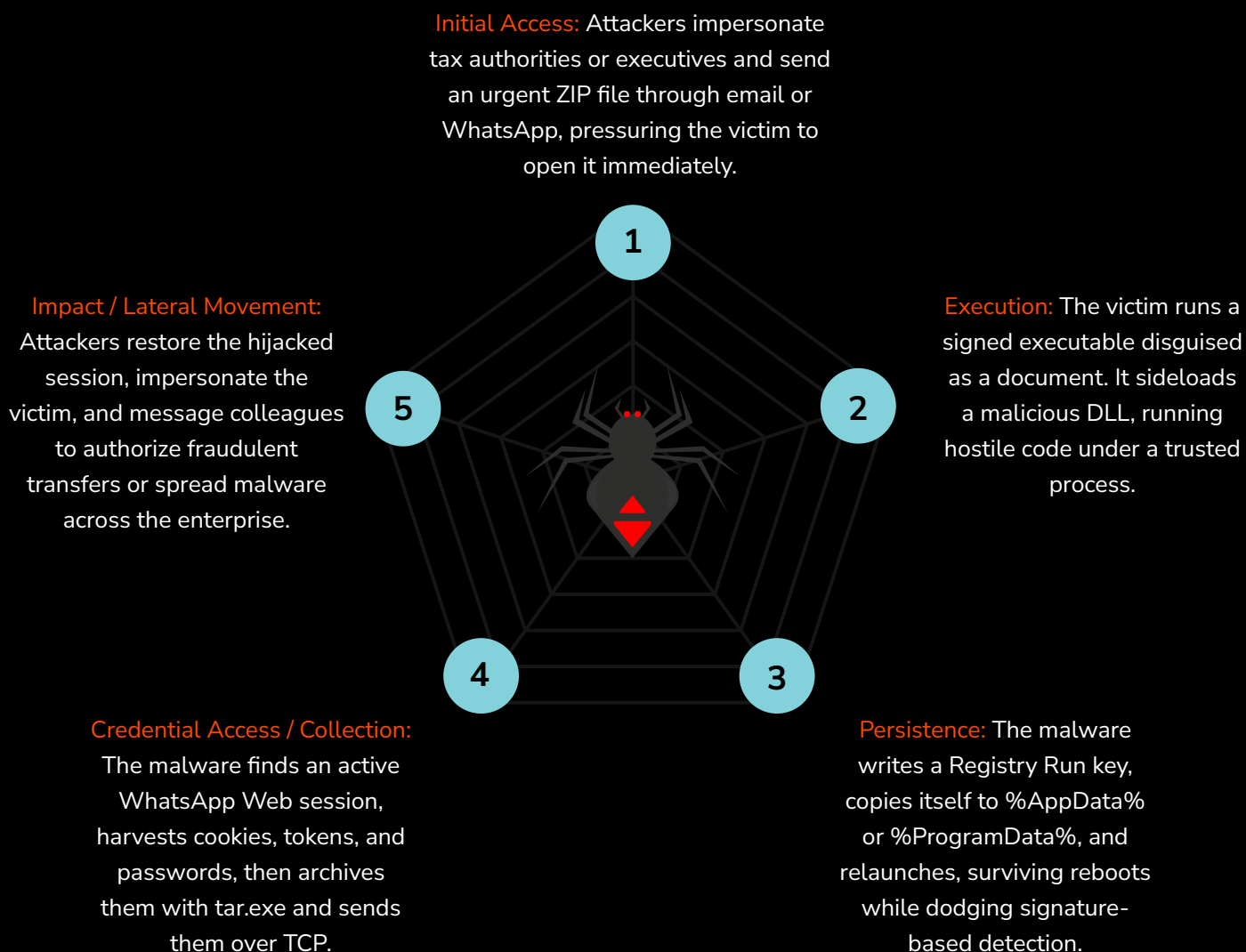
WhatsApp Scams Timeline



The Boss Scam is not an accident of opportunity. It deliberately exploits how businesses communicate. Adversaries have learned that WhatsApp's trusted-contact model is a structural vulnerability. When a message arrives from a known number, in an existing thread, with the right name attached, the brain classifies it as safe before reason engages. Attackers weaponize that reflex. They impersonate CEOs, finance officers, and compliance teams to inject urgency: a tax deadline, a regulatory notice, or an invoice needing immediate sign-off, delivered as a malicious ZIP or a link that pulls one down.

The following infographic outlines the kill chain.

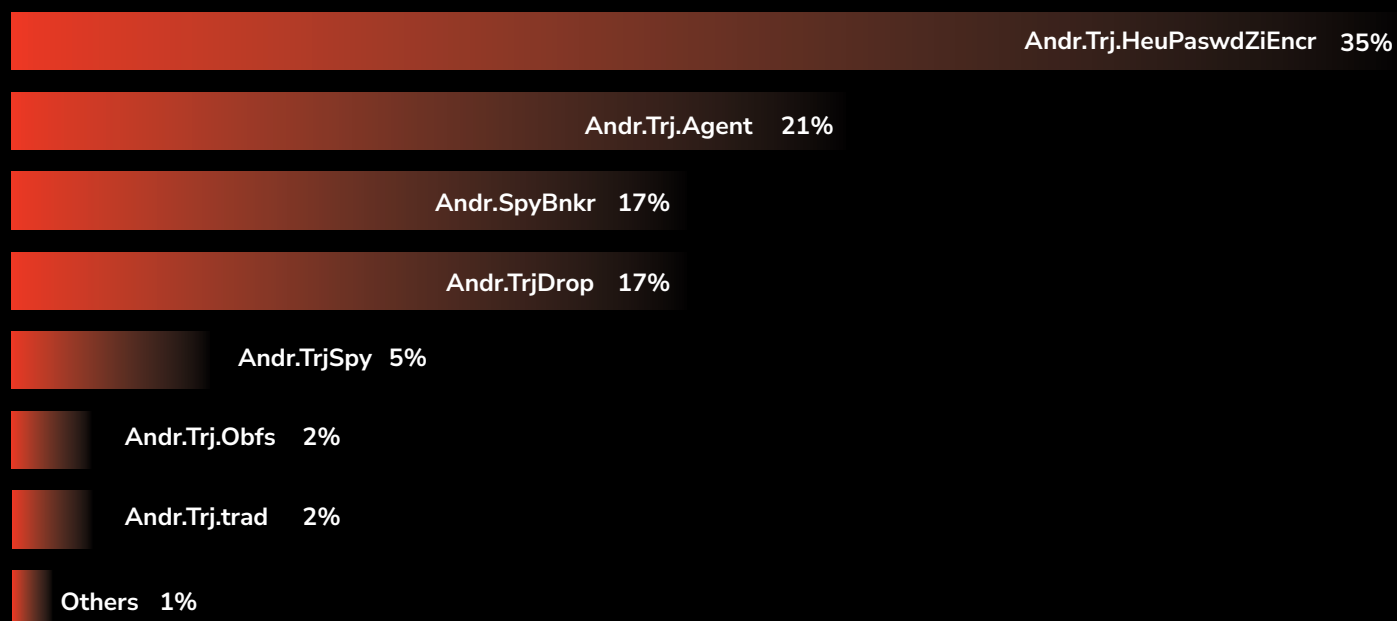
Boss WhatsApp Scam Blueprint



For more details, read the full analysis at <https://labs.k7computing.com/index.php/boss-scam-dont-trust-every-urgent-message-from-your-boss/>

Perpetrators increasingly exploit popular social platforms, refining their tactics to target users where they are most active.

THE MYSTIFIED TROJANS



Four main types of trojans dominated the scene: agents, droppers, banking-focused spyware, and those that bury their payloads in password-protected ZIP files. That last group hasn't faded into the background; it keeps showing up quarter after quarter, proving how effective the tactic remains.

Banking trojans surged into view, each flaunting its own tactics for breaking in, dodging defenses, and snatching credentials across borders. Among them, Octagon, a remote access trojan, cut through the noise with a distinct signature. Let's break down its attack chain, step by step.

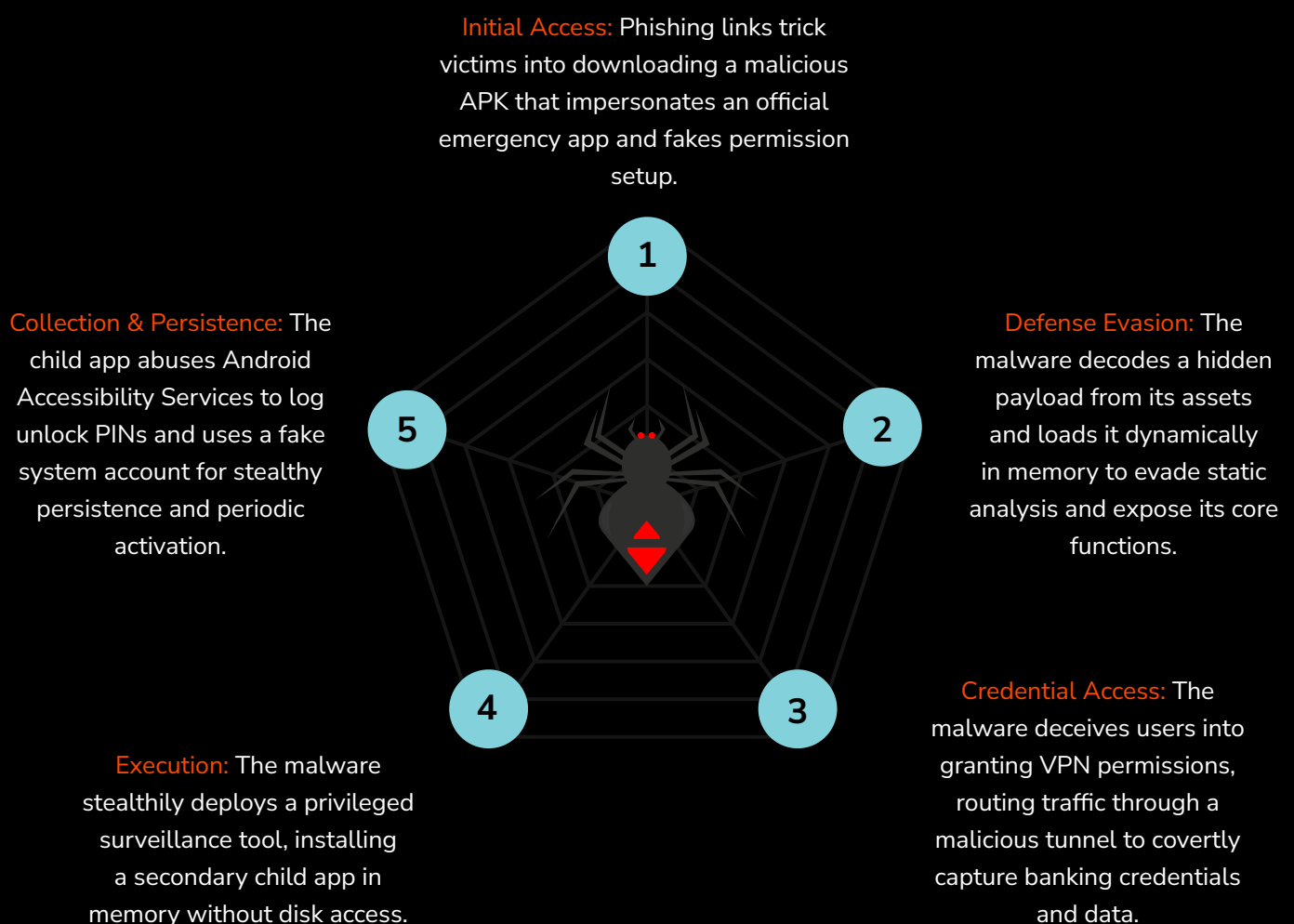
Android Trojans use stealthy delivery and remote access to steal credentials, compromise financial data, and threaten enterprise security.



Case Study: Android Octagon RAT Infection Chain

Octagon is a multi-stage Remote Access Trojan (RAT) that infects Android mobile devices through fake phishing apps. It first pretends to be an official emergency services app, like “BH Alert.” To avoid detection, it decrypts and loads its main payloads (DEX and JAR files) directly into memory. After activation, Octagon uses Android’s VPN framework to steal banking credentials and secretly installs a secondary “child APK” in memory. This child app uses Android’s Accessibility Services to log screen-unlock PINs and passwords. It uses the AccountManager sync framework to maintain a hidden, ongoing connection to its command-and-control (C2) servers.

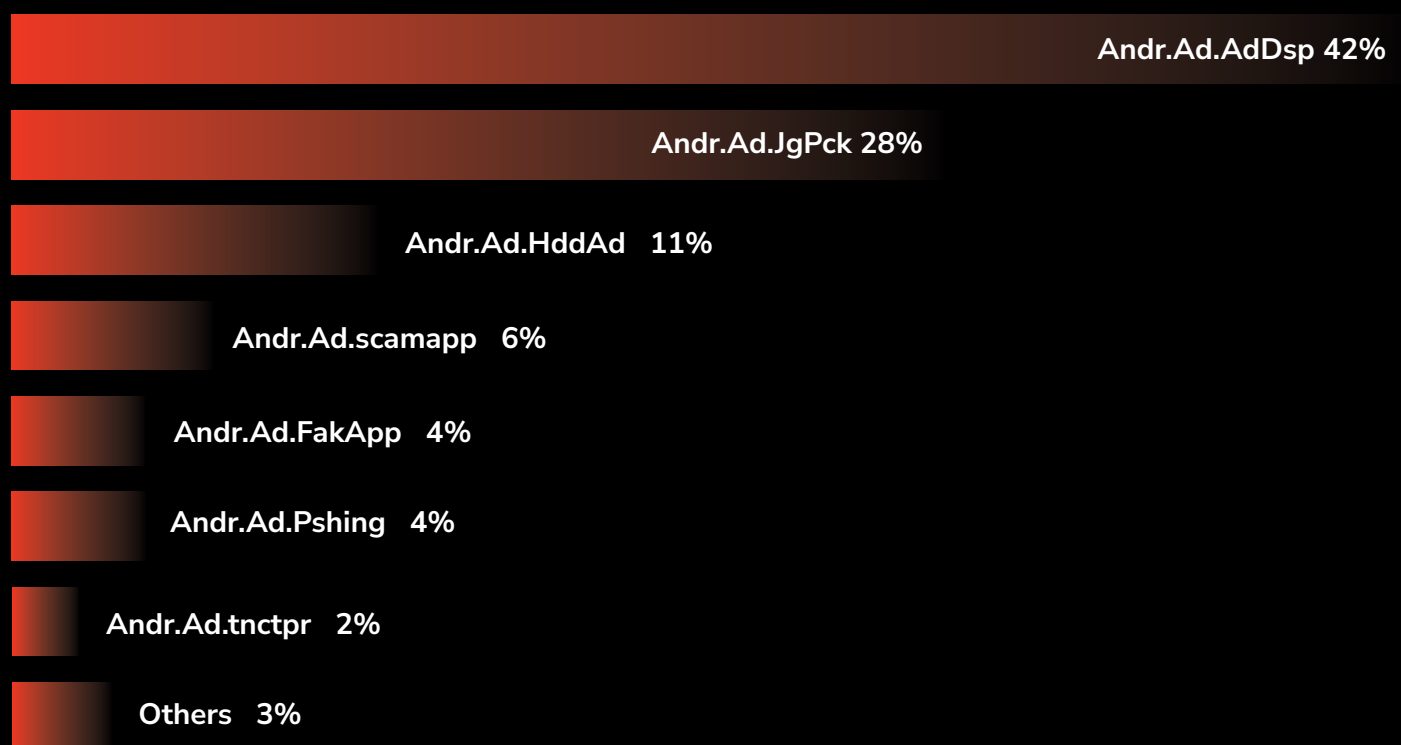
The following infographic explains the complex, multi-stage infection process.



For more details read

<https://labs.k7computing.com/index.php/octagon-technical-analysis-of-a-fake-bahrain-civil-defense-application/>

THE LOOMING ADWARE



One adware strain, Andr.Ad.AdDsp, accounts for nearly half the adware segment. It sneaks onto devices through disguised third-party downloads, then unleashes a barrage of relentless, out-of-app ads. By hiding its icon and posing as a system process, it dodges deletion and quietly drains battery, data, and performance.

Mobile adware threatens enterprise data by turning everyday apps into channels for covert data collection and unauthorized access.

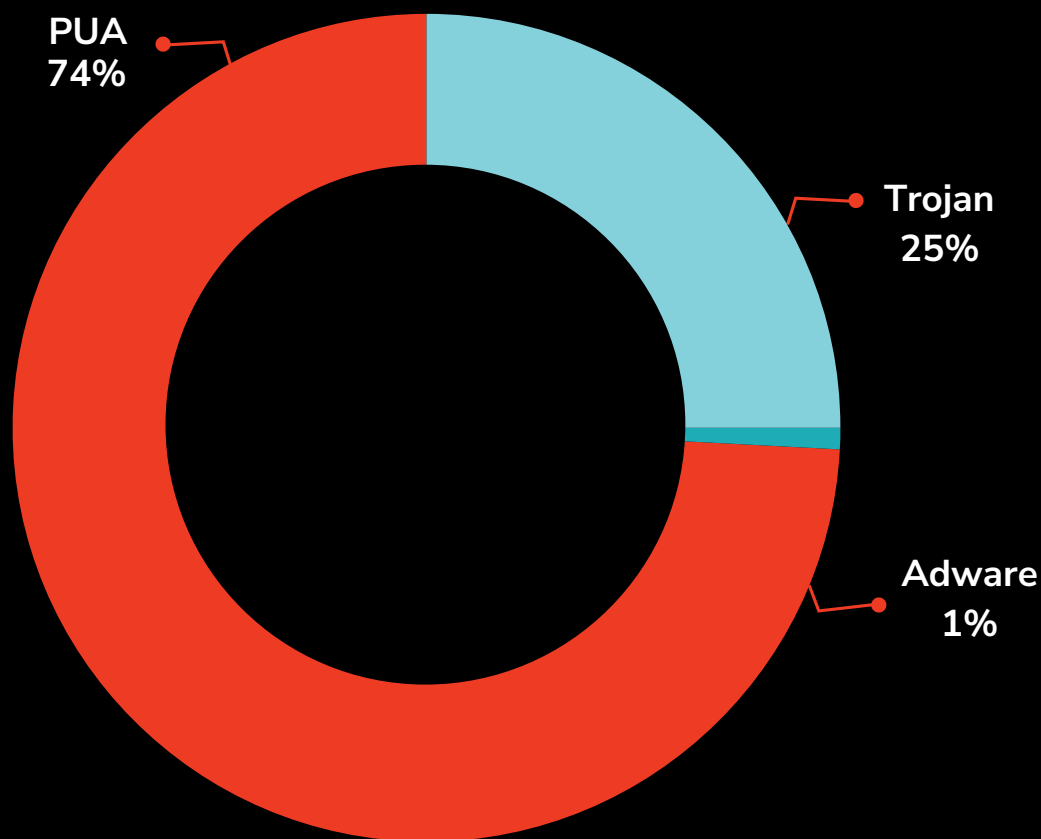
THE EVOLUTION OF THE MACOS THREAT LANDSCAPE

macOS has shifted from an afterthought to a prime enterprise target. Attackers now see Macs as open doors to the heart of a company: credentials, cloud accounts, developer keys, and sensitive data all converge here.

A single Mac can be a treasure trove: browser sessions, saved logins, developer tokens, and direct access to cloud platforms. Breach one endpoint and the fallout can ripple outward: lateral movement, cloud intrusions, even fractures in the software supply-chain.

When so much identity and access converge on one device, a breach goes far beyond lost files. Attackers monetize credentials at scale, twisting legitimate macOS features and user-approved workflows to sidestep Apple's defenses. Malware is just one piece of the puzzle.

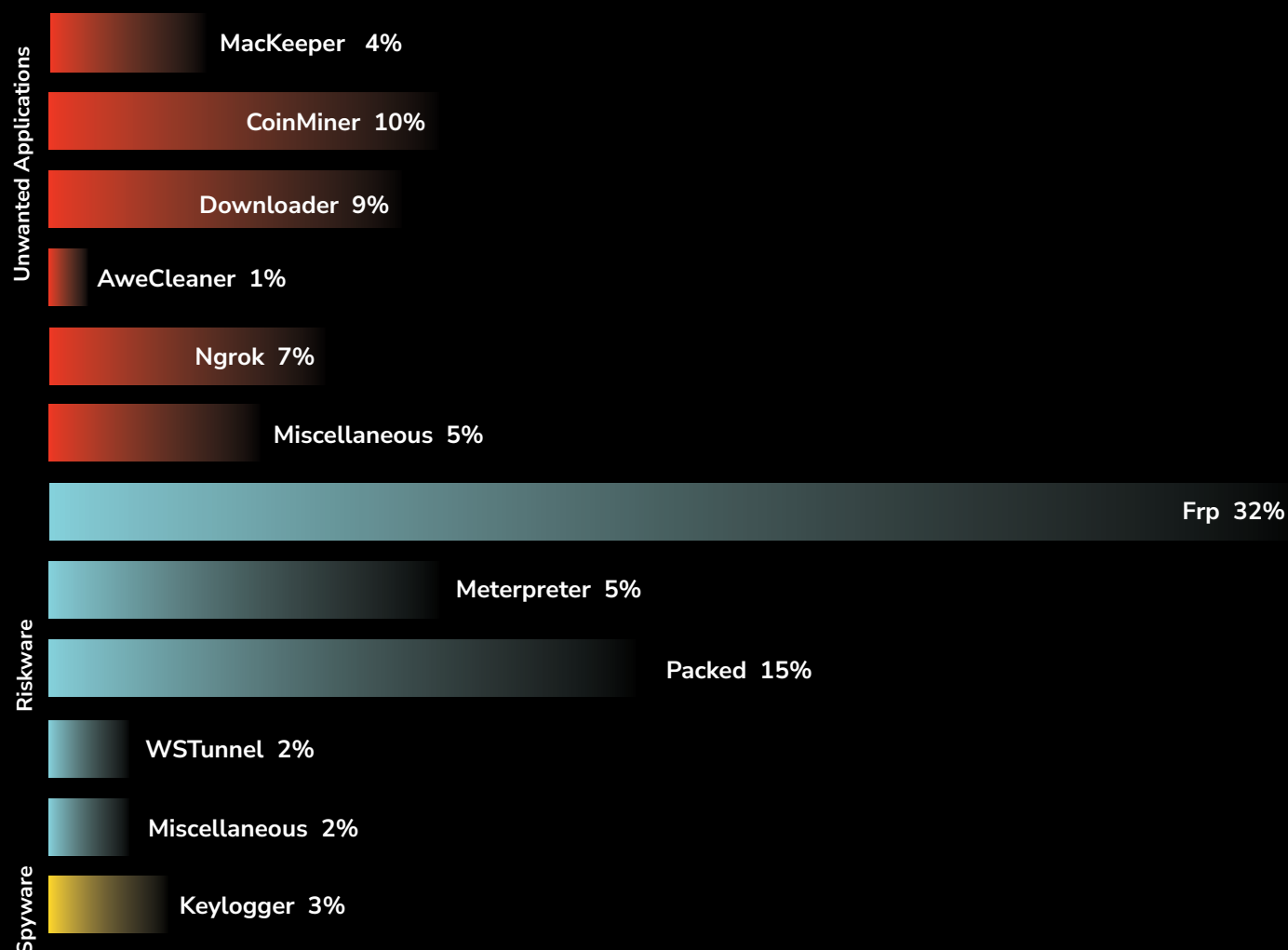
Trojan, Adware, and PUA Proportional Split



The chart above shows that Potentially Unwanted Applications (PUAs) make up most of the threats, covering almost three-quarters of the landscape. However, just because there are many of them doesn't mean they are advanced. Their high numbers show how easily simple, user-driven threats can get into the Mac ecosystem. The bigger concern is what's hidden underneath. Infostealers and trojans are now targeting credentials, sessions, developer secrets, and other valuable information.

PUAs dominate macOS detections, but infostealers and Trojans pose a greater enterprise risk by targeting credentials, cloud access, and developer secrets.

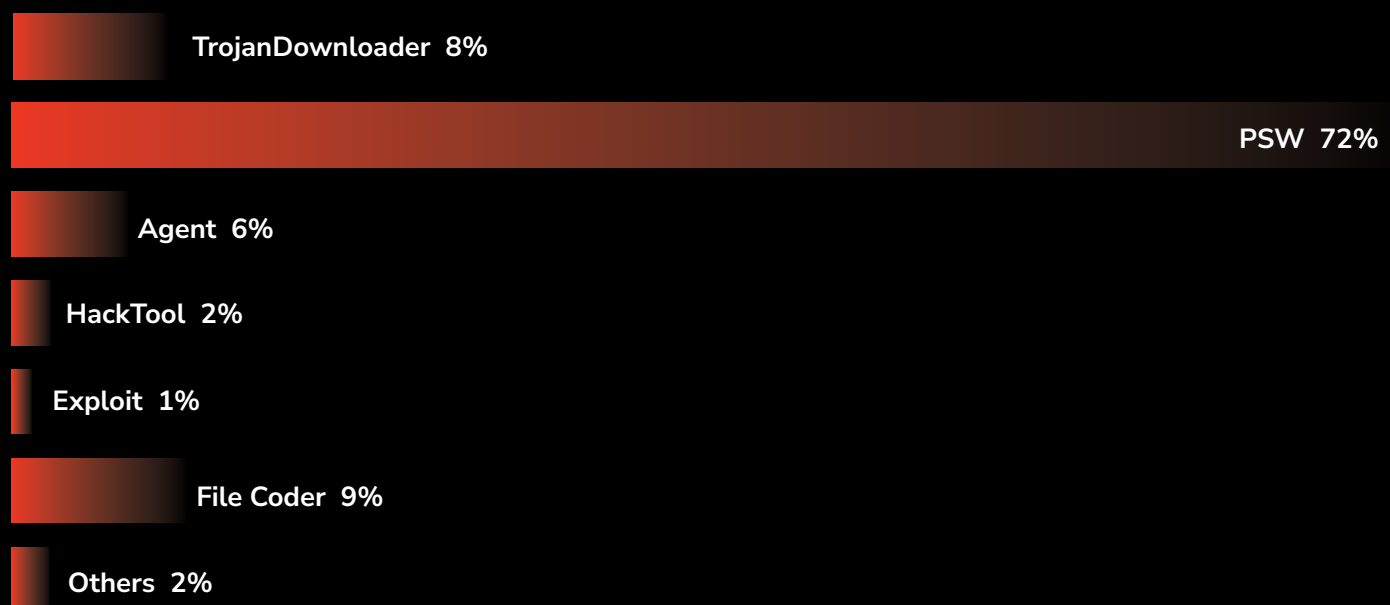
THE DOMINANT PUA



Among unwanted apps, riskware, and spyware, FRP stands out in Q2, and for a notable reason. Fast Reverse Proxy can punch through firewall restrictions and set up reverse connections, giving attackers a backdoor for Command and Control. It may not be classic malware, but if it lands on your system without your say-so, your organization's security posture suffers.

Unwanted remote-access tools can bypass network restrictions, creating covert entry points into enterprise systems and exposing sensitive data.

THE SIGNIFICANCE OF TROJANS



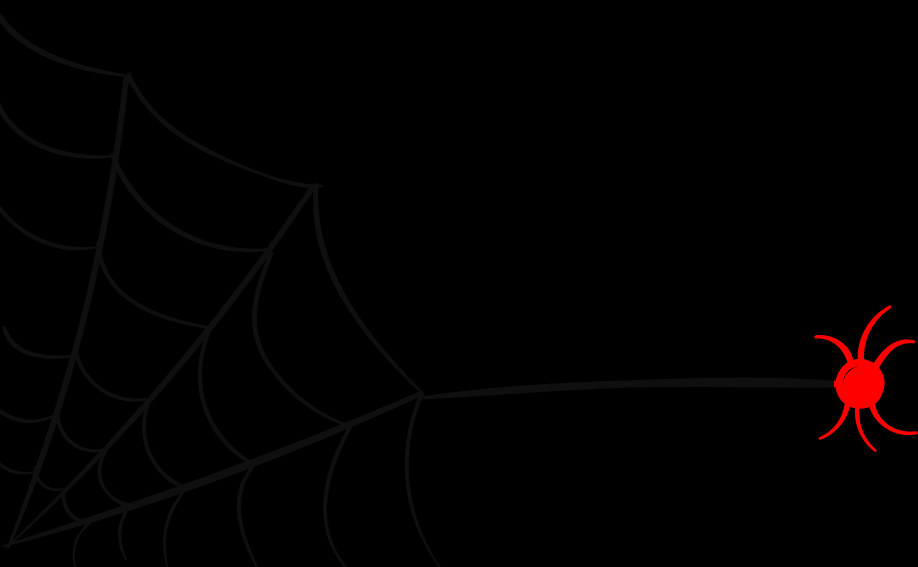
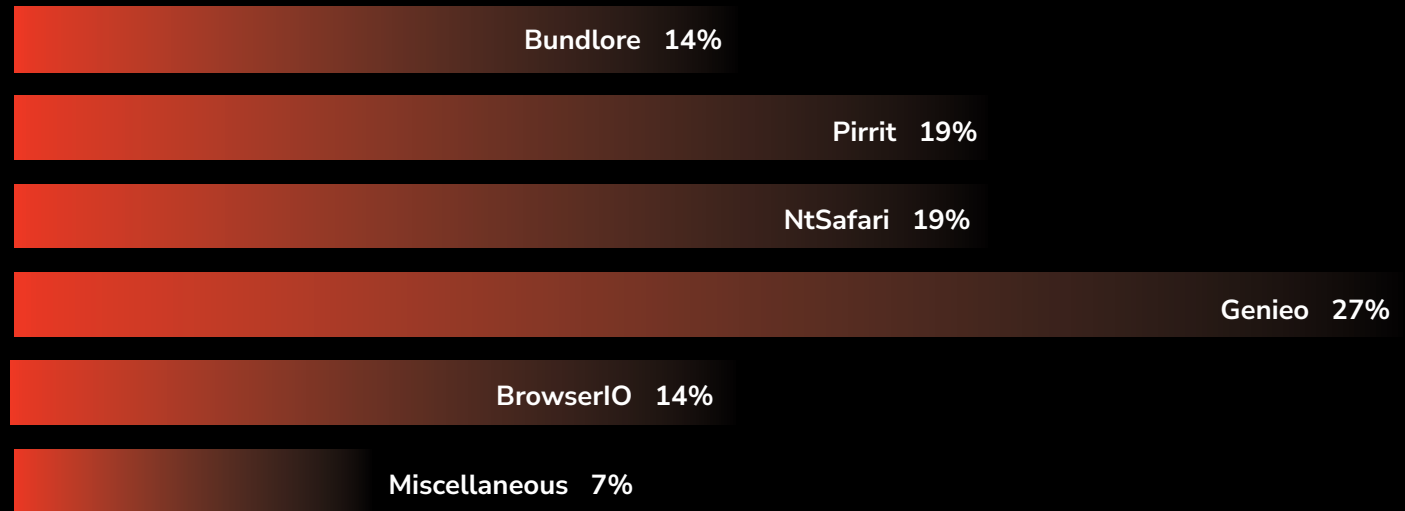
PSW (password-stealing ware) has carved out a niche in the macOS threat landscape. These tools are crafted to swipe everything from account logins and saved passwords to browser cookies and crypto wallets. Some even push fake password prompts to dig deeper into the system. It's no surprise they top the charts.

Trojans threaten enterprise security by stealing credentials and exploiting compromised devices to gain access to corporate systems and data.



ADVANCED ADWARE ACTS AS AN ENTERPRISE GATEWAY

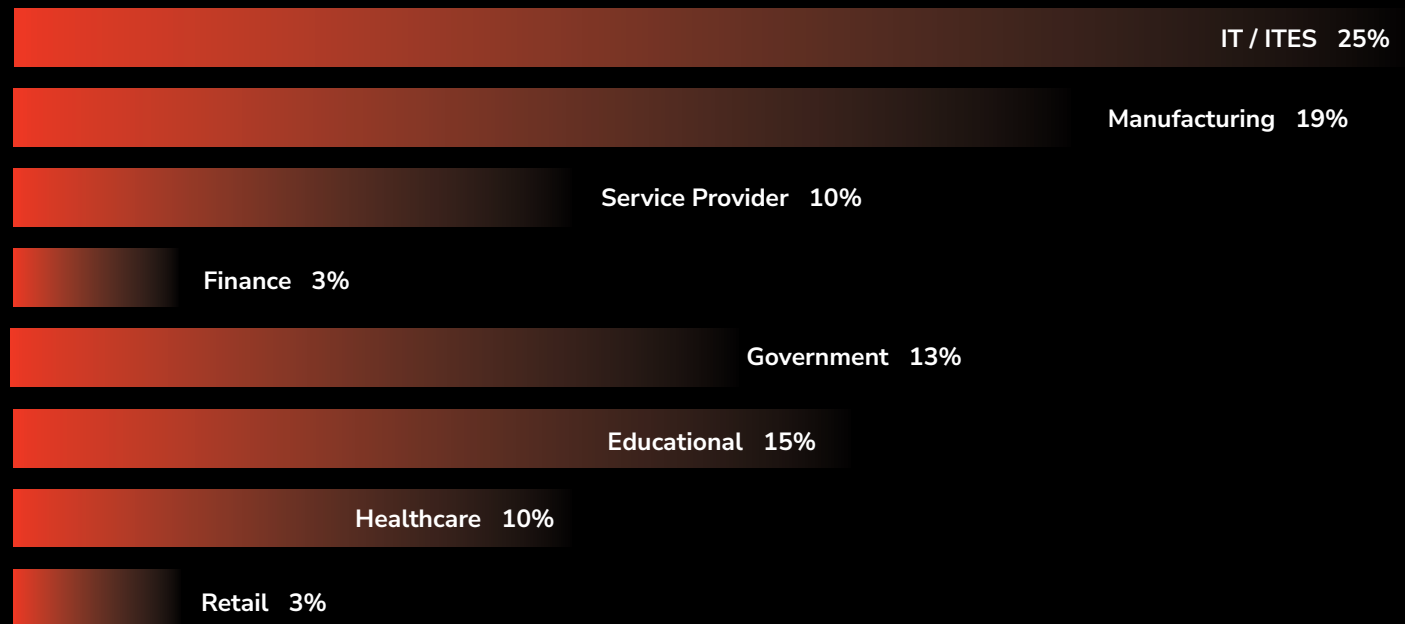
Don't assume adware's mere numbers in macOS mean it is worth ignoring. The modern adware presence shows how easily simple, user-facing malware can get into the Mac ecosystem without letting the system wave a red flag.



VULNERABILITIES GALORE

INDUSTRIES WITH THE HIGHEST VULNERABILITY CONCENTRATION

IT/ITES leads at 25%, a position it has held for multiple quarters because it operates across client environments, privileged systems, and remote connections that turn a single breach into many. Manufacturing follows at 19%. Newly connected production lines convert intrusion directly into halted output and lost revenue. This interconnected risk structure lets localized compromise cascade across partners and customers, causing operational disruption, sensitive data exposure, and financial impact.



Supply-chains are adding vendors, integrations, and dependencies faster than visibility can keep up. Complexity has become the exposure.

Unpatched vulnerabilities across interconnected enterprise systems can turn a single weakness into widespread disruption, data exposure, and supply-chain compromise.



THE MOST PREVALENT VULNERABILITIES IN Q2 2026–27, ALONG WITH THE RELEVANT MITRE CODES AND SAFEGUARDS.

ORACLE HTTP SERVER & WEBLOGIC SERVER

CVE-2026-21962 | CVSS 10.0 | Improper Access Control → Unauthorized Data Manipulation

IMPACT: An improper access control vulnerability allows unauthorized users to create, modify, delete, or access critical data.

MITRE Codes:

- T1190 Exploit Public-Facing Application
- T1565.001 Stored Data Manipulation

ACTION: Apply the latest security patches/updates provided by Oracle for the affected versions, and review access-control configurations to ensure only authorized users can access or modify critical resources.

MICROSOFT INTERNET KEY EXCHANGE (IKE) SERVICE EXTENSIONS

CVE-2026-33824 | CVSS 9.8 | Double Free → Remote Code Execution

IMPACT: Allows an unauthenticated remote attacker to execute arbitrary code by sending specially crafted packets to a system with Internet Key Exchange IKEv2 enabled.

MITRE Codes:

- T1190 Exploit Public-Facing Application

ACTION: Apply the latest Microsoft security updates addressing CVE-2026-33824 and, where feasible, disable IKEv2 if it is not required.

MICROSOFT SHAREPOINT SERVER

CVE-2026-55040 | CVSS 9.1 | Weak Authentication → Security Feature Bypass

IMPACT: A critical authentication bypass vulnerability could allow an unauthenticated remote attacker to impersonate a user and make an anonymous connection, enabling unauthorized disclosure of files and modification of data.

MITRE Codes:

- T1190 Exploit Public-Facing Application
- T1565.001 Stored Data Manipulation

ACTION: Apply the latest Microsoft security updates for SharePoint Server and ensure that affected SharePoint instances are not unnecessarily exposed to untrusted networks.

Every top vulnerability mapped to MITRE ATT&CK, helping CISOs connect exposure to attacker techniques and prioritize defenses.



APPLE MACOS

CVE-2026-65400 | CVSS 9.8 | Improper Authentication → Full Account Takeover

IMPACT: Allows a network-based attacker to authenticate to Screen Sharing without valid credentials, gaining unauthorized access to the system.

MITRE Codes:

- T1190 Exploit Public-Facing Application
- T1210 Exploitation of Remote Services
- T1021.005 Remote Services: VNC

ACTION: Install the latest Apple security updates for CVE-2026-65400 and limit Screen Sharing access to authorized users and trusted networks whenever possible.

APACHE TOMCAT

CVE-2026-34486 | CVSS 7.5 | Missing Encryption → Sensitive Data Exposure

IMPACT: Allows an attacker to bypass the EncryptInterceptor function due to missing encryption, exposing sensitive data.

MITRE Codes:

- T1190 Exploit Public-Facing Application
- Secondary: T1040 Network Sniffing

ACTION: Upgrade Apache Tomcat to a version that addresses CVE-2026-34486 and apply all relevant security updates.

WORDPRESS CORE

CVE-2026-60137 | CVSS 9.1 | Accepting Untrusted Input → SQL injection

IMPACT: Allows the attacker to exploit a SQL injection vulnerability in WordPress Core through untrusted input supplied by a plugin or theme.

MITRE Codes:

- T1190 Exploit Public-Facing Application

ACTION: Upgrade WordPress Core to the latest security-patched version and ensure all installed plugins and themes are updated. Restrict untrusted input handling to mitigate potential SQL injection.

NETWORK & DEVICE VULNERABILITIES

CISCO SECURE FIREWALL ADAPTIVE SECURITY APPLIANCE (ASA) AND SECURE FIREWALL THREAT DEFENSE (FTD)

CVE-2026-20349 | CVSS 8.6 | Insufficient Error Checking in HTTP requests → Denial of Service

IMPACT: Allows an unauthenticated remote attacker to exploit insufficient HTTP request error handling in the Remote Access SSL VPN service of Cisco Secure Firewall ASA/FTD Software, causing the affected device to reload and resulting in a denial-of-service condition.

MITRE Codes:

- T1499.004 Endpoint Denial of Service: Application or System Exploitation

ACTION: Apply the latest patch by the vendor and restrict exposure of the Remote Access SSL VPN service to trusted networks and monitor for anomalous or crafted HTTP requests.

SONICWALL SMA1000 APPLIANCES

CVE-2026-15409 | CVSS 10.0 | Accepting Untrusted Input → Server-Side Request Forgery

IMPACT: Allows a remote unauthenticated attacker to exploit an SSRF vulnerability in the SonicWall SMA1000 Appliance Work Place interface, causing the appliance to send requests to unintended locations.

MITRE Codes:

- T1190 Exploit Public-Facing Application

ACTION: Apply the latest SonicWall security updates addressing the vulnerability and restrict access to the Work Place interface to trusted networks where possible; monitor outbound requests from the appliance for suspicious or unexpected destinations.

GOOGLE PIXEL

CVE-2026-58704 | CVSS 8.8 | Improper Authorization → Privilege Escalation

IMPACT: Allows bypassing cellular-modem permission checks and escalate privileges due to a logic error in the code, without authentication or user interaction.

MITRE Codes:

- T1404 Exploitation for Privilege Escalation

ACTION: Update the Google Pixel device to the latest security patch to mitigate the vulnerability and prevent unauthorized privilege escalation.

CONCLUSION: THE SECURITY BOUNDARY HAS CHANGED

The next breach may never originate inside your environment. It can arrive through a software update you authorized, a service provider you depend on, or a vendor account with legitimate access. The security boundary is no longer defined solely by what sits inside your walls. It increasingly extends to who and what you trust. Supply-chain compromise is becoming a structural security risk, not just an isolated third-party incident.

Numbers alone can understate the real threat. Supply-chain attacks exploit access and trust organizations have already authorized. A signed software update, legitimate vendor credential, or trusted integration can become the vehicle for compromise. Legitimate credentials open legitimate doors, while malicious activity blends into expected traffic. When one supplier serves many customers, a single compromise can create disproportionate downstream exposure. Why pick the lock when the key is already trusted?

The real risk isn't a single breach, but what organizations inherit. Every software dependency, cloud provider, MSP, and third-party identity introduces risks that can extend into the connected enterprise. Weak access controls, delayed patching, misconfigurations, and visibility gaps in those dependencies can become part of an organization's risk surface. When many organizations depend on the same providers, one compromise can create concentration risk across the entire ecosystem.

WHAT ORGANIZATIONS MUST DO DIFFERENTLY

Defenses must increasingly follow where trust and dependency extend. Four priorities stand out:

- **Map critical dependencies:** Identify the suppliers, platforms, services, and identities the business cannot function without.
- **Prioritize by blast radius:** Rank suppliers according to the potential business impact of their compromise.
- **Continuously monitor third-party access:** Treat vendor identities, privileged accounts, and integrations as potential attack paths.
- **Rehearse supplier compromise:** Conduct incident-response exercises that begin with a trusted provider as the initial point of compromise.

Annual questionnaires can show intent. Only continuous visibility reveals real exposure.

Supply chain attacks are likely to become more consequential as organizations connect more suppliers, platforms, services, and identities to their core operations. Resilient organizations will be those that understand their critical dependencies, continuously assess the access they grant, and can contain the impact when trusted relationships are compromised.

The security perimeter is no longer a wall. It is the ecosystem of relationships, technologies, and dependencies an organization chooses to trust.

CYBER THREAT MONITOR REPORT

Q2 2026–27



Copyright 2026 K7 Enterprise Security Pvt Ltd. All Rights Reserved. This material has been compiled by K7 Labs. This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorized personnel of K7 Enterprise Security Pvt Ltd. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7cybersecurity.com