K7 SECURITY

www.k7computing.com

RANSOMWARE CONTINUES TO LOOM

Ransomware has existed since the evolution of cyberspace. Though it has long been a fixture of the threat landscape, the sophistication of its behavior, attack vector, and impact has escalated exponentially. Despite widespread cybersecurity awareness campaigns, the threat still looms large.

Adversaries continue to favor ransomware because the impact is not only large but also immediate. The usual human tendency is to panic and want to return to normal operations quickly. As a result, organizations may feel pressured to meet the ransom demand to protect customer trust and avoid legal trouble.

However, ransom threats have become more deceptive of late. Despite paying the ransom, organizations either recover none of their data or only recover some of their critical data needed to resume their business as usual.

This shift means leadership can no longer view ransom payments as a form of disaster recovery. Organizations must prioritize cyber resilience through immutable backups, proactive threat hunting, and unified AI-powered protection, ensuring continuity regardless of adversary demands.

This report deconstructs the anatomy of such advanced campaigns, equipping decision-makers with the actionable intelligence required to outpace the adversary and secure their operational future.

Happy Reading!

Back To Contents

INFECTION RATE (IR)

Regardless of its type, a security breach is a concern 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.

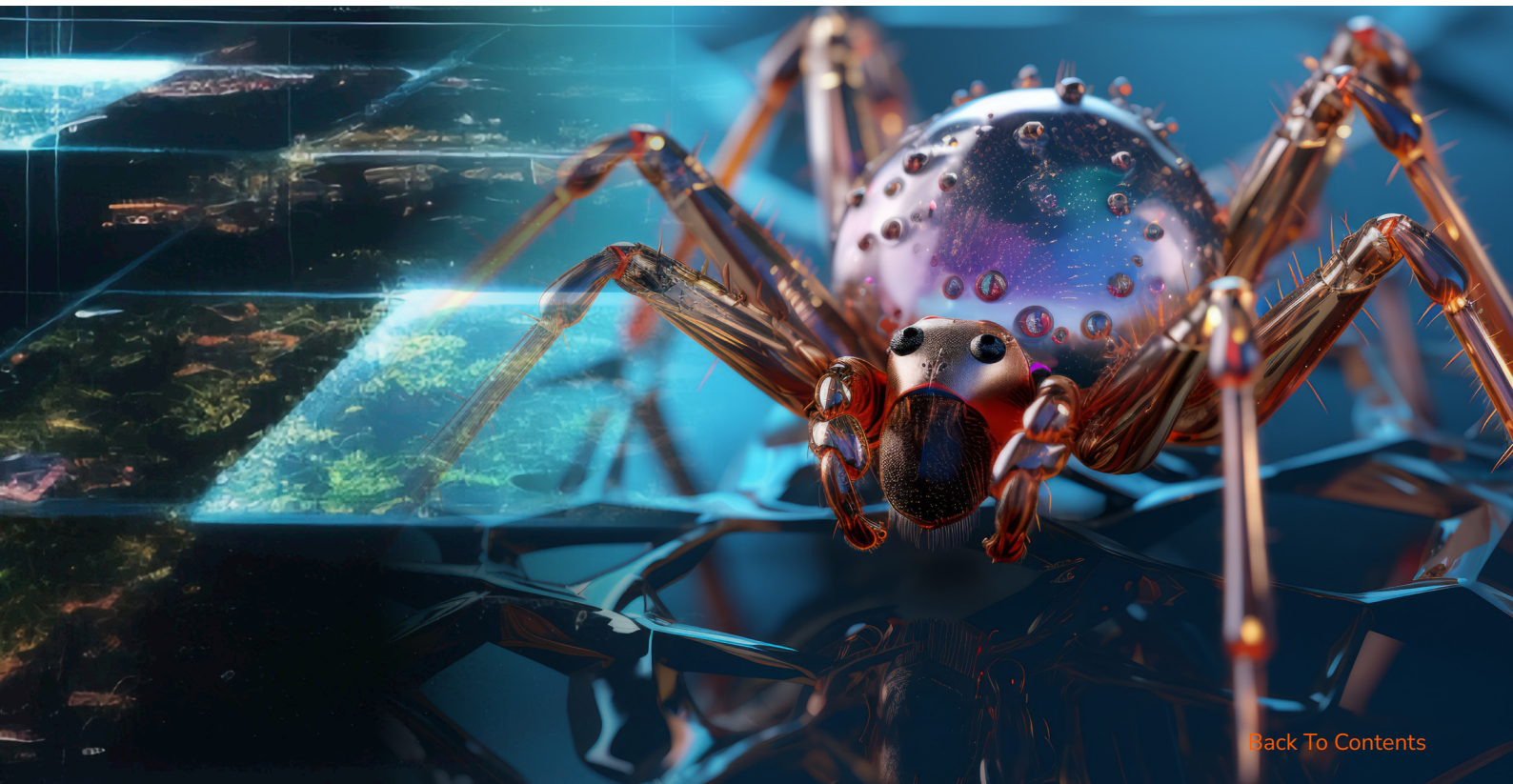
We use this IR factor to identify enterprises and netizens' exposure to cyber threats. IR is determined as the proportion of active K7 corporate or consumer users who encountered at least one cyber threat event that was blocked and reported to our K7 Ecosystem Threat Intelligence infrastructure (K7ETI).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

Infection Rate (IR) of an area

The Global IR for Q4_2025-26 was 52%

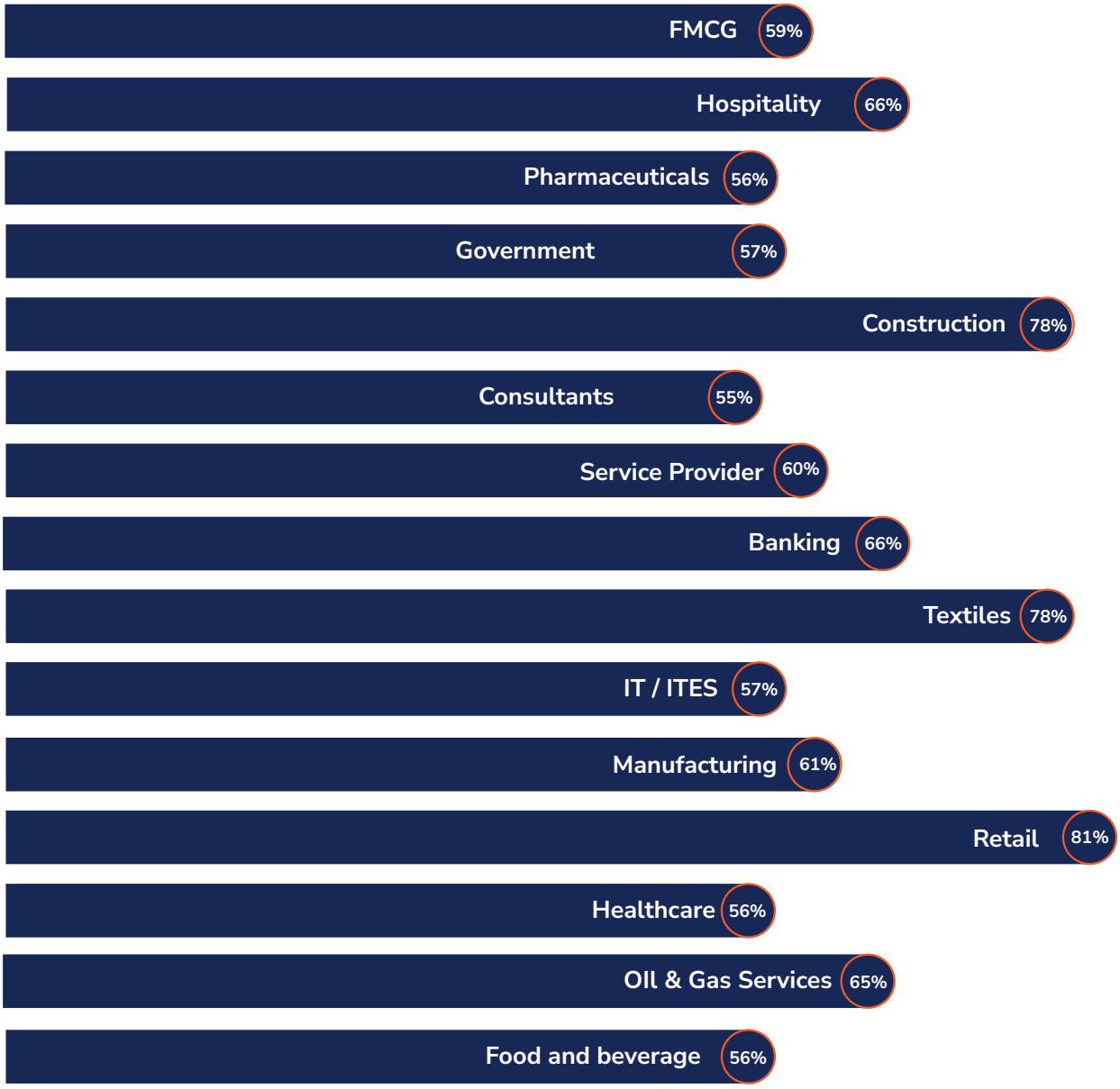


Back To Contents

A GRANULAR VIEW OF THE INDUSTRY THREAT LANDSCAPE

Incident response data highlight a shift in attacker focus, with sectors such as Retail (81%), Construction (78%), and Textiles (78%) facing concentrated assaults.

Most Impacted Industries Around The Globe

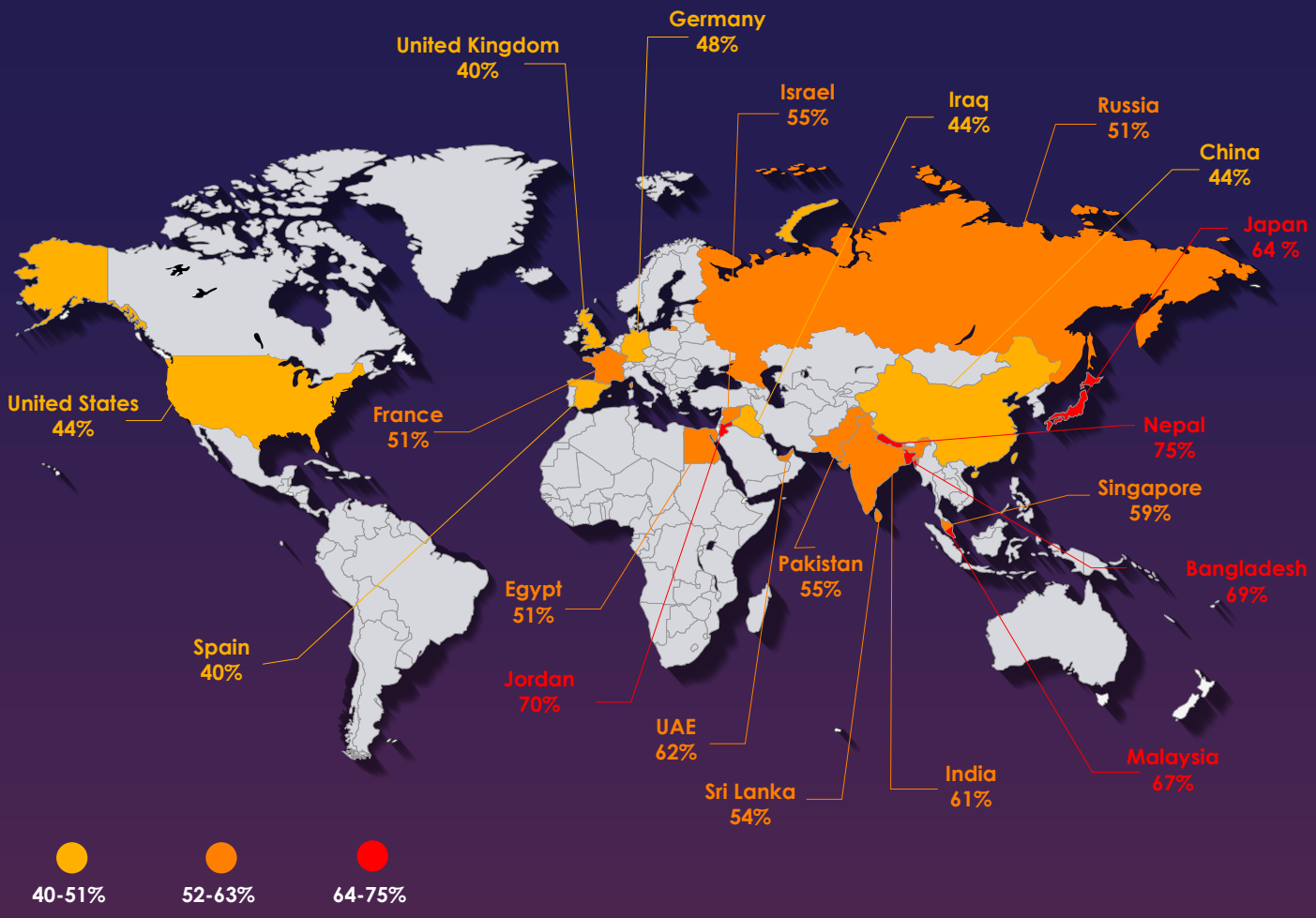


Threat actors now exploit the operational complexity and extensive supply chains in these industries, bypassing standard defenses to gain prolonged access. A single breach can rapidly form into widespread disruption, financial extortion, and loss of customer trust. This surge in targeted attacks demonstrates that high-transaction and supply-chain-heavy sectors are bearing the brunt of sophisticated cyber threats in the current landscape.

Back To Contents

WORLDWIDE CYBER THREAT LANDSCAPE

Recent global incident response data reveal a strategic pivot by adversaries, with emerging markets such as Nepal (75%), Jordan (70%), and Bangladesh (69%) experiencing significantly higher attack volumes than established regions like the UK and Spain (40%).



This stark contrast indicates that threat actors are intentionally targeting regions with rapidly growing digital infrastructures. By aggressively exploiting systemic vulnerabilities in these interconnected networks, attackers quietly establish unauthorized access. Such infiltrations pose severe strategic risks, primarily leading to devastating operational disruption and widespread data compromise.

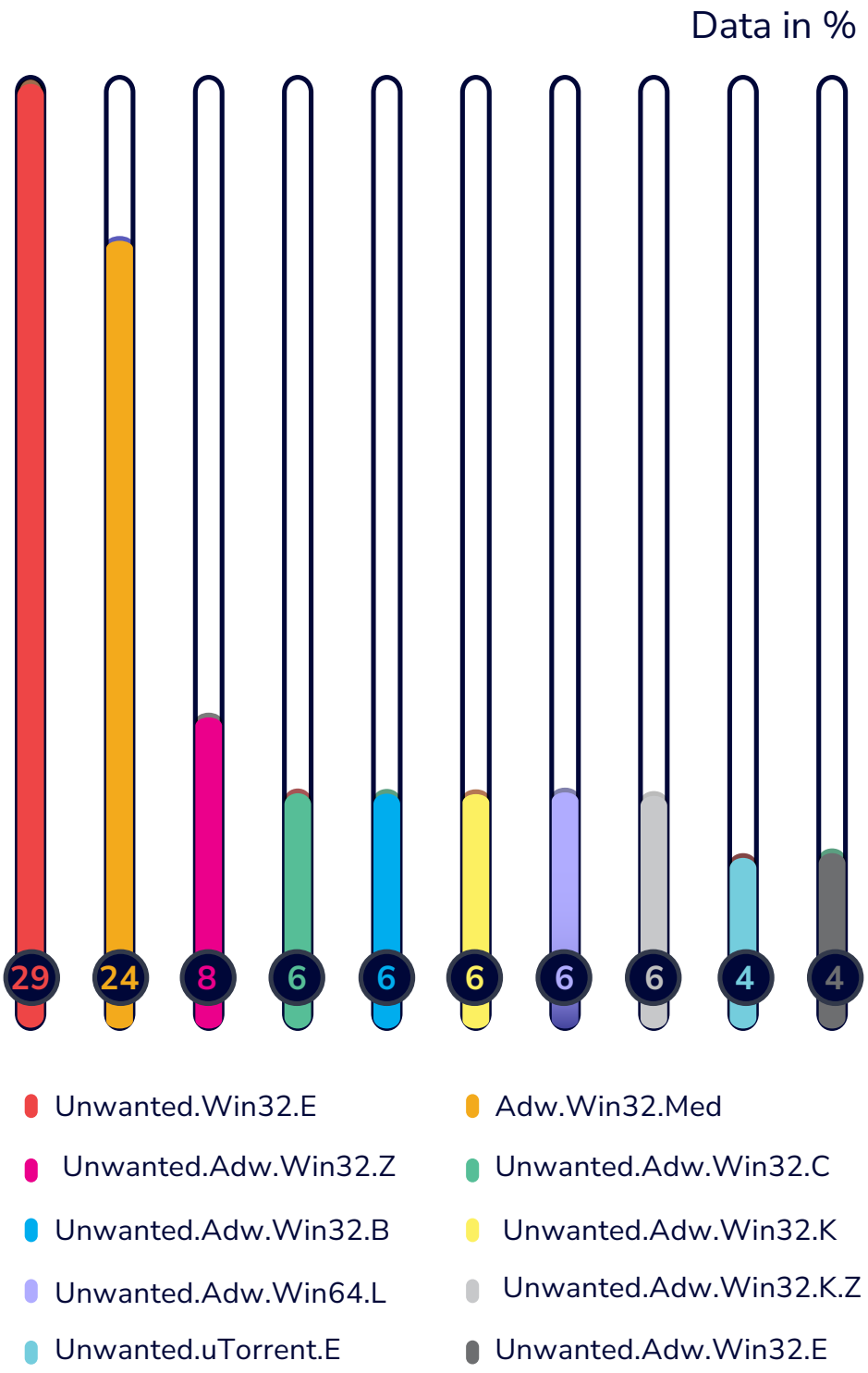
Back To Contents

WINDOWS THREAT LANDSCAPE

Being the primary engine driving global enterprise operations, Windows has always been a defining factor in the cyber threat landscape. Its massive market dominance creates an inherently sprawling attack surface, making it the top target for sophisticated adversaries. Because of its vast footprint across interconnected businesses, inherent vulnerabilities are rapidly weaponized by threat actors to execute severe ransomware and data theft campaigns, making it the absolute front line of corporate cyber risk, where business continuity faces its most direct operational tests.

TOP MALWARE TARGETING WINDOWS SYSTEMS

The high volume of Unwanted.Win32 (29%) and Adware (over 60% combined) detections signify a persistent grayware ecosystem targeting the human perimeter within global enterprises.

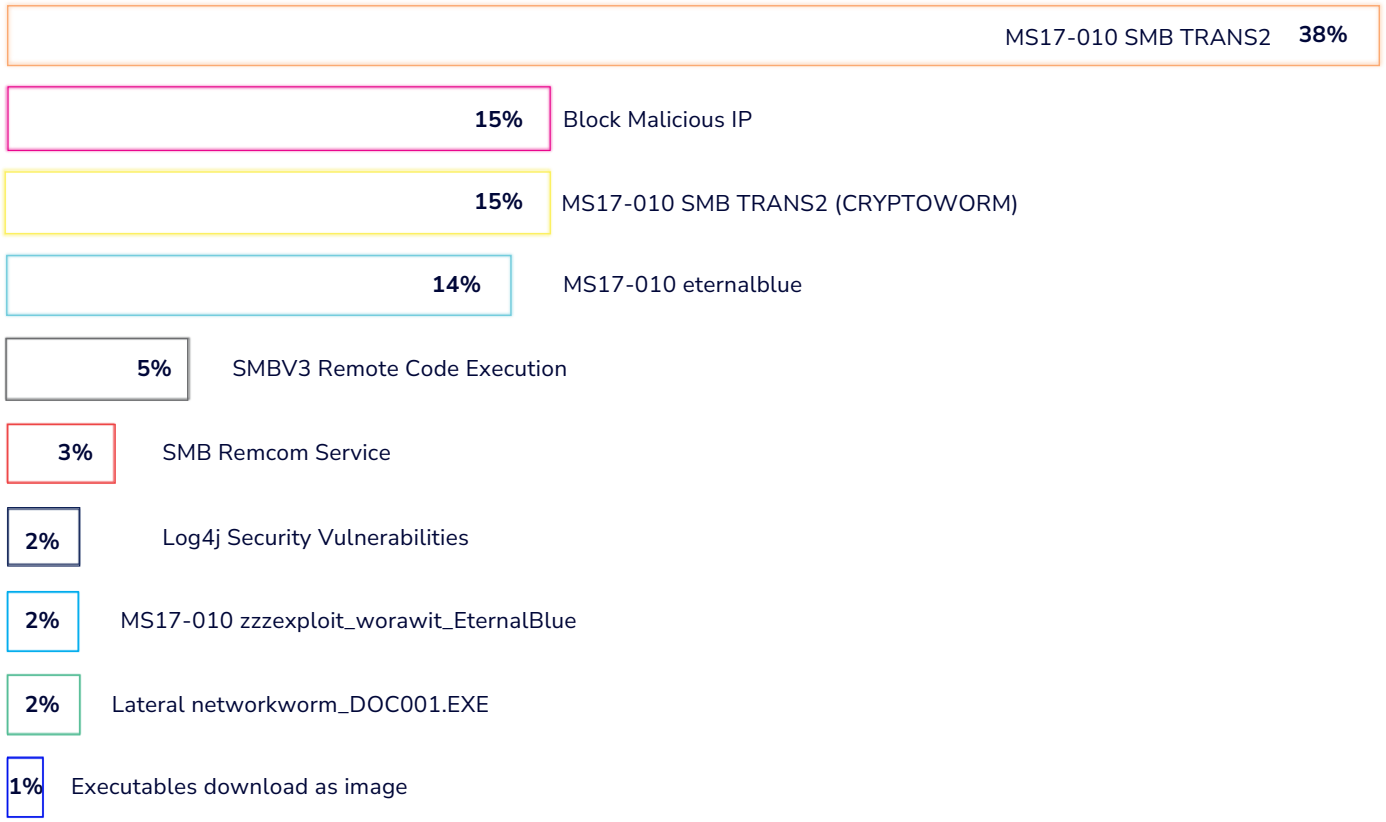


These threats typically operate by piggybacking on legitimate software or via deceptive downloads to gain a foothold, then modify system settings and monitor user activity. For businesses, this prevalence is particularly dangerous as these programs serve as precursors to more severe compromises, leading to significant operational disruption, sensitive data leakage, and the eventual degradation of hardware performance and organizational reputation.

Back To Contents

UNPATCHED VULNERABILITIES: THE ACHILLES' HEEL OF WINDOWS SYSTEMS

The overwhelming concentration of MS17-010 (EternalBlue) variants, accounting for nearly 70% of all detections, reveals a persistent reliance on legacy exploits for automated, worm-like lateral movement. By targeting the Server Message Block (SMB) protocol, actors can execute remote code to bypass traditional perimeters, a tactic reinforced by vulnerabilities in SMBv3 and Log4j.

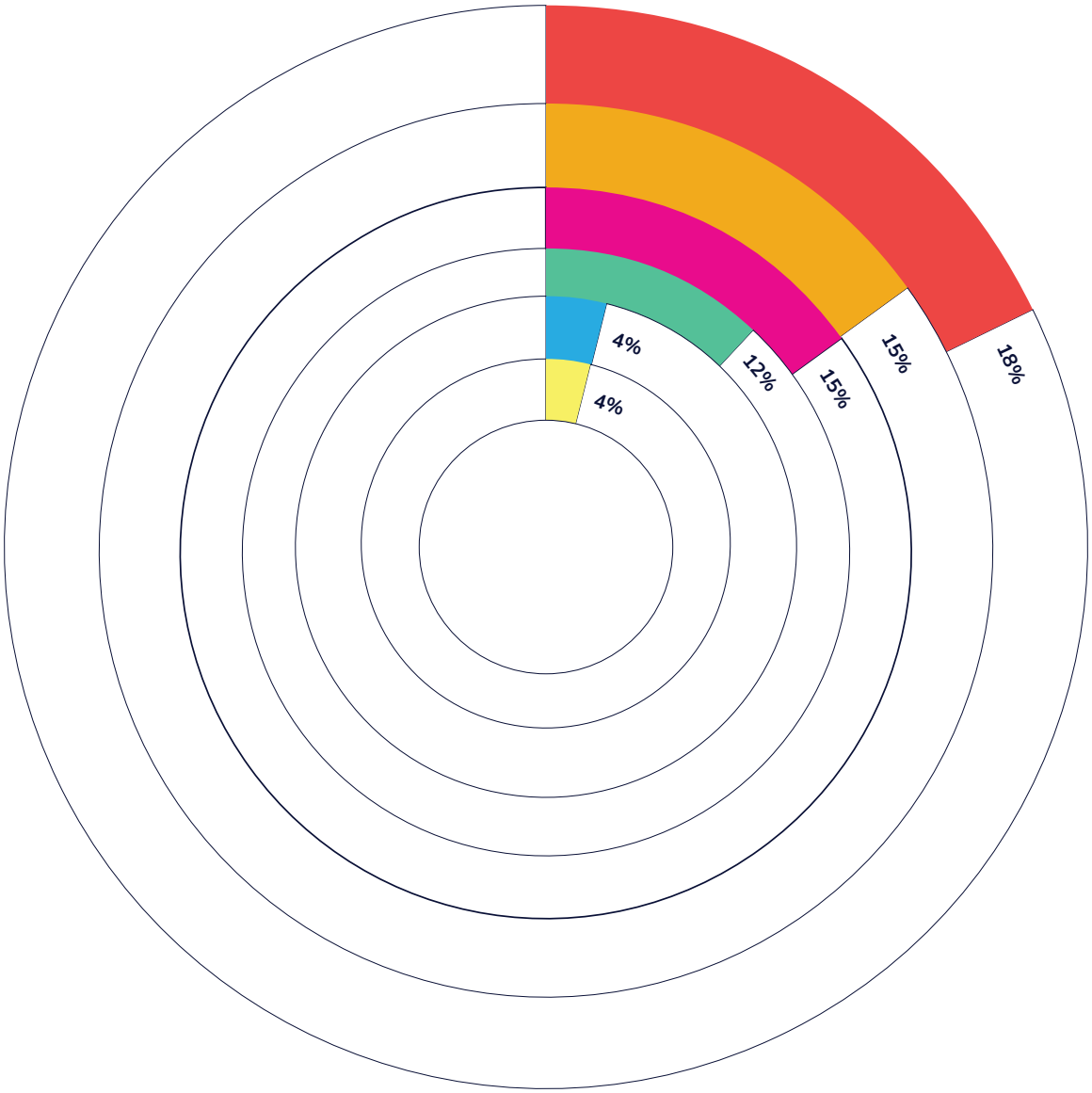


This pattern indicates that attackers are successfully weaponizing unpatched infrastructure to deploy ransomware or cryptoworms. For businesses, this translates into a heightened risk of total operational paralysis and rapid data compromise as infections propagate autonomously across interconnected corporate networks.

Back To Contents

HEURISTIC INTRUSION PREVENTION SYSTEM (HIPS)

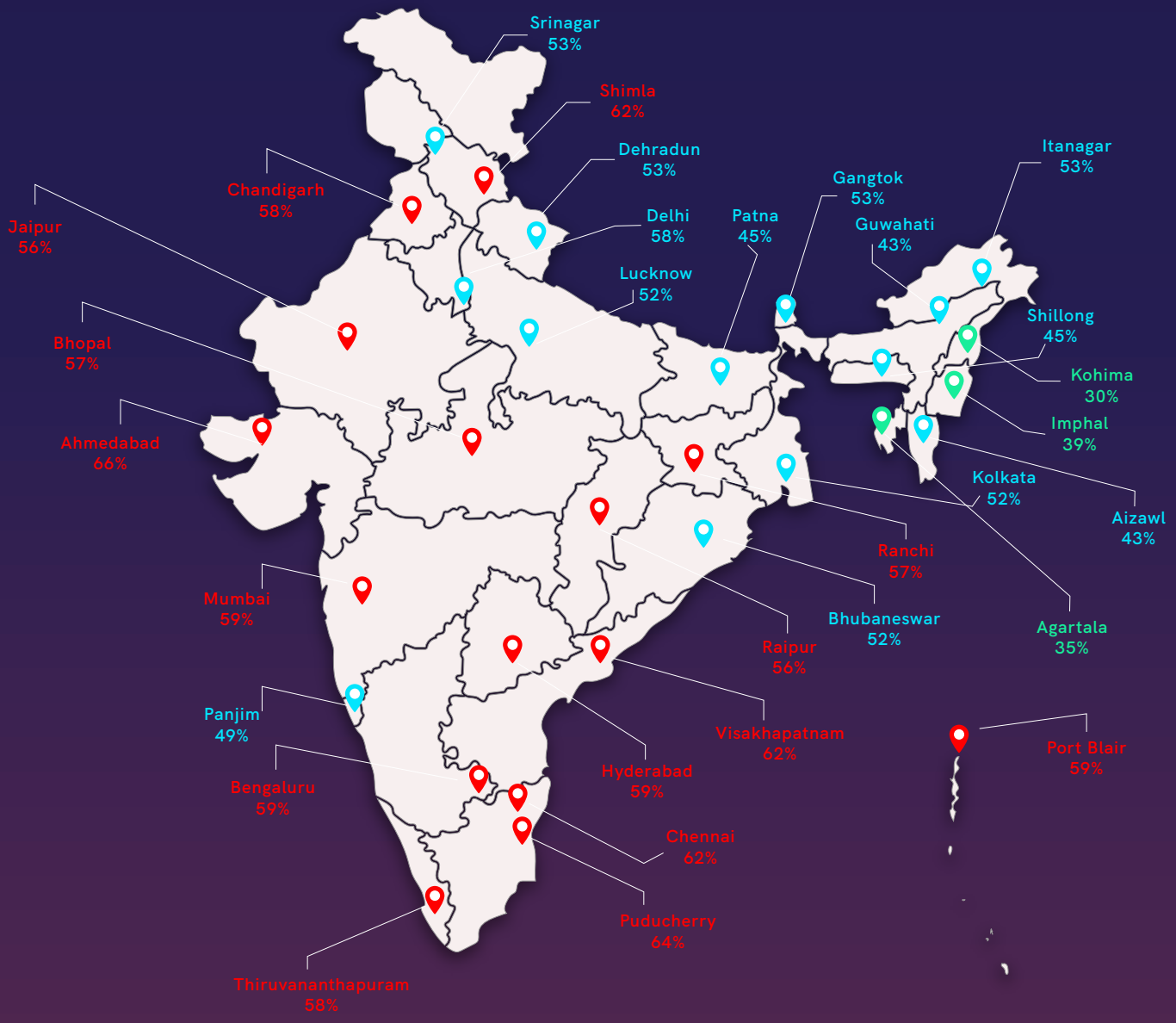
The high prevalence of Susp_dropper (18%) and Susp_Powershell (15%) highlights a strategic shift toward multi-stage, fileless execution within the global threat landscape. By leveraging Susp_LolBin_Write_PE (15%) and Create_Process (4%), actors are increasingly living off the land, repurposing trusted system binaries to bypass traditional perimeter defenses. The inclusion of Injector (12%) signals a sophisticated focus on memory-resident persistence, allowing malicious code to hide within legitimate processes.



For enterprises, these patterns indicate a shift from static payloads to dynamic, behavior-based intrusions that prioritize stealth and long-term operational access.

Back To Contents

CYBER THREAT LANDSCAPE - INDIA



30%-42%

43%-54%

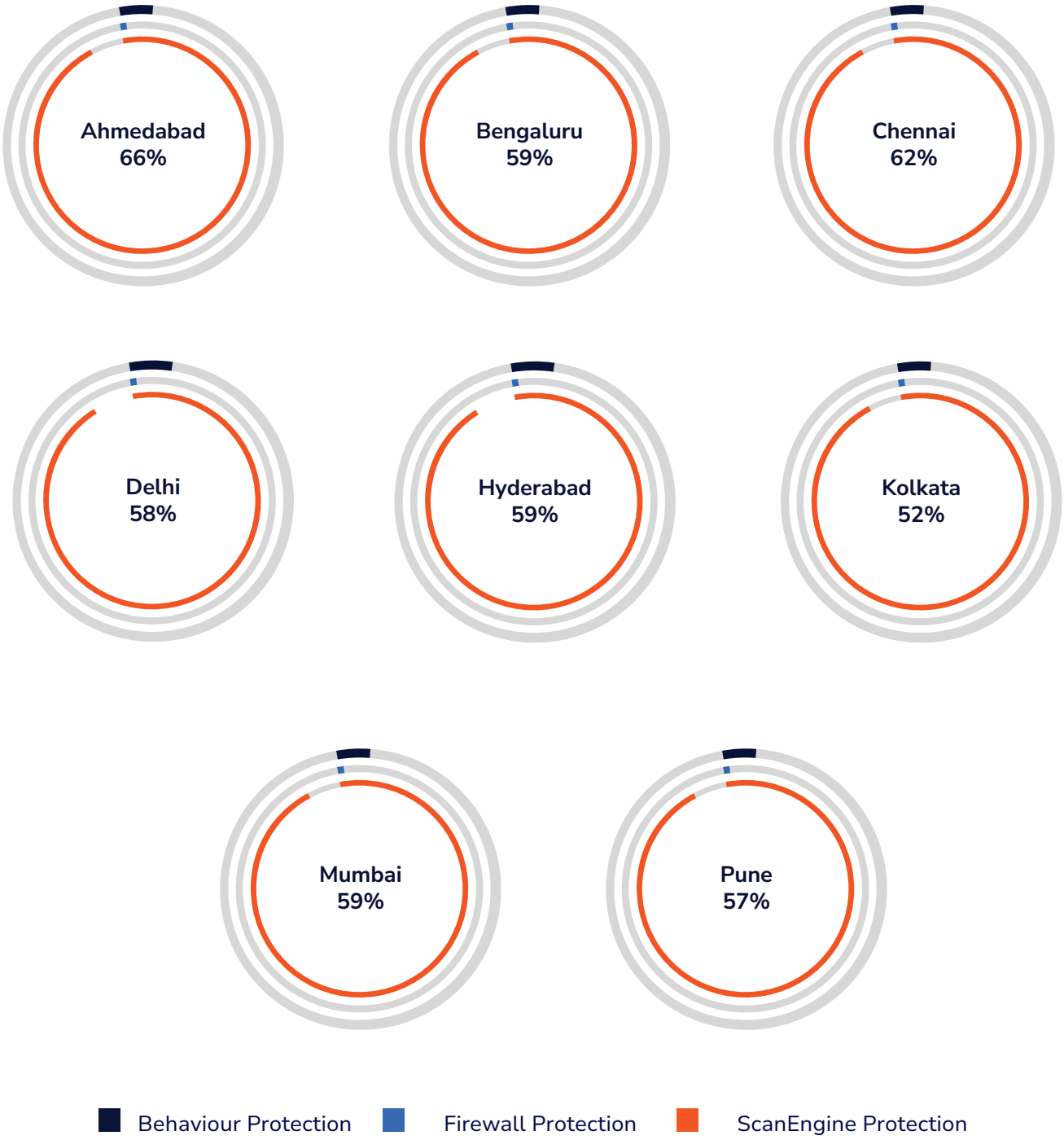
55%-66%

Map for illustrative purposes only. Not to scale.

Back To Contents

THE QUARTERLY TRENDS AND STATISTICS

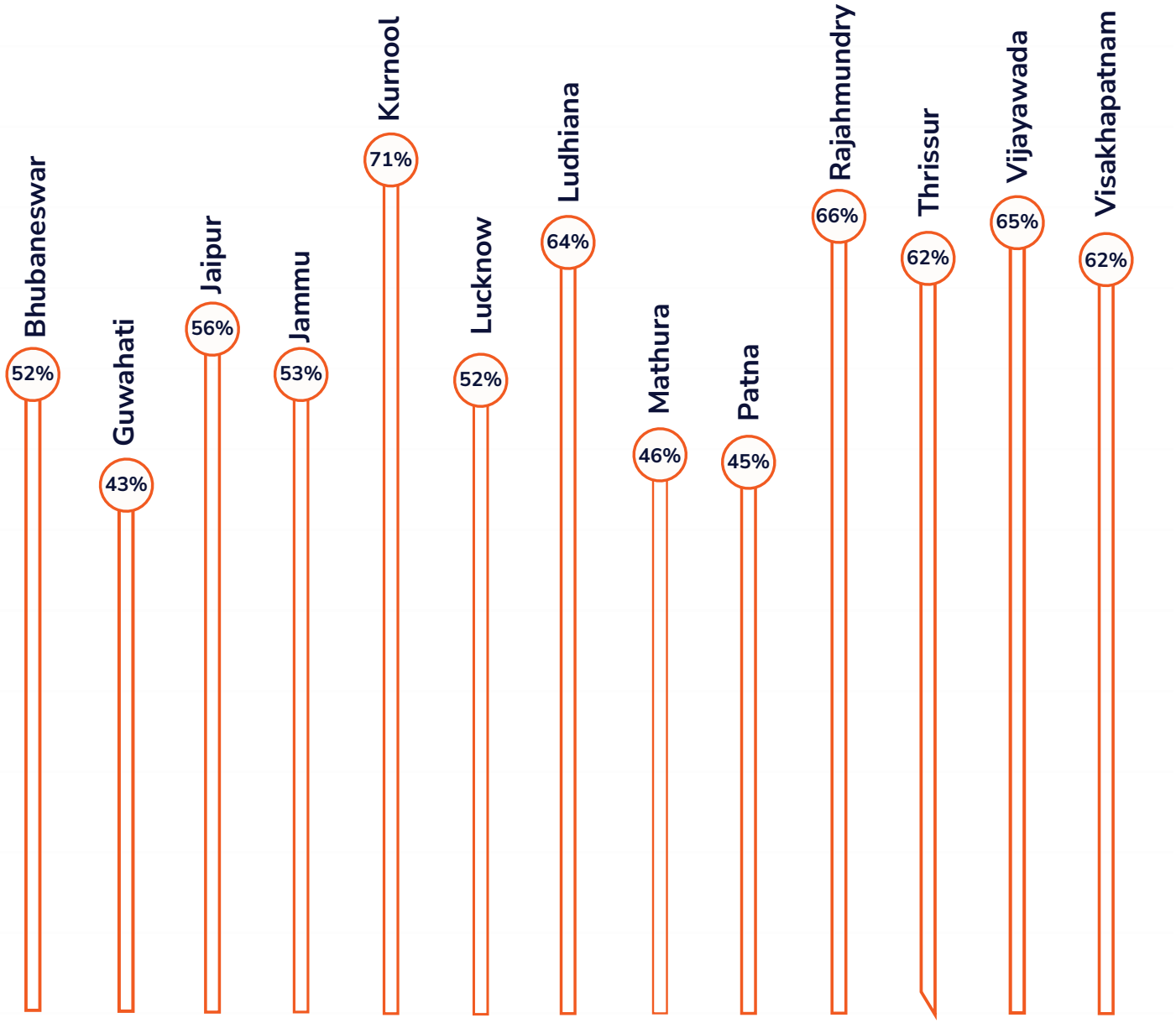
With a national infection rate (IR) peaking at 60%, the data underscores a critical saturation of cyber threats across India, where more than half of monitored digital environments have been successfully compromised or targeted by malicious activity.



Back To Contents

TOP INFECTION RATES IN TIER-2 CITIES

The current infection data reveals a significant shift in India's threat landscape, with Tier-2 and Tier-3 cities emerging as primary hotspots. Kurnool (71%), Rajahmundry (66%), and Vijayawada (65%) lead this surge, signaling that attackers are pivoting toward regions with rapidly expanding digital footprints.



This trend targets localized infrastructure, often bypassing urban-centric defenses.

Back To Contents

ENTERPRISE INSECURITY

Ransomware threats are not new to the cyberworld. It has been around since the time cyberspace evolved. Just that the attack techniques have evolved over the years. Recently, multiple client machines were infected with ransomware. The sequence of attack is as follows:

Case Study: Ransomware bruteforcing its way into the clients' network

STEP: 1

Extensive brute-force attack through internet-facing ports and compromised LAN systems

STEP: 2

Successful access was achieved via a LAN system on the user account named "admin"

STEP: 3

TightVNC (TVNServer.exe) was deployed for persistent remote control. Registry entries were set to auto start TightVNC on reboot

STEP: 4

Tools like Process Hacker, Advanced IP Scanner, IPScan25exe, IOBitUnlocker, PowerShell Remote Execution were downloaded and utilized

STEP: 5

Finally, ransoware was executed, encrypting all their files

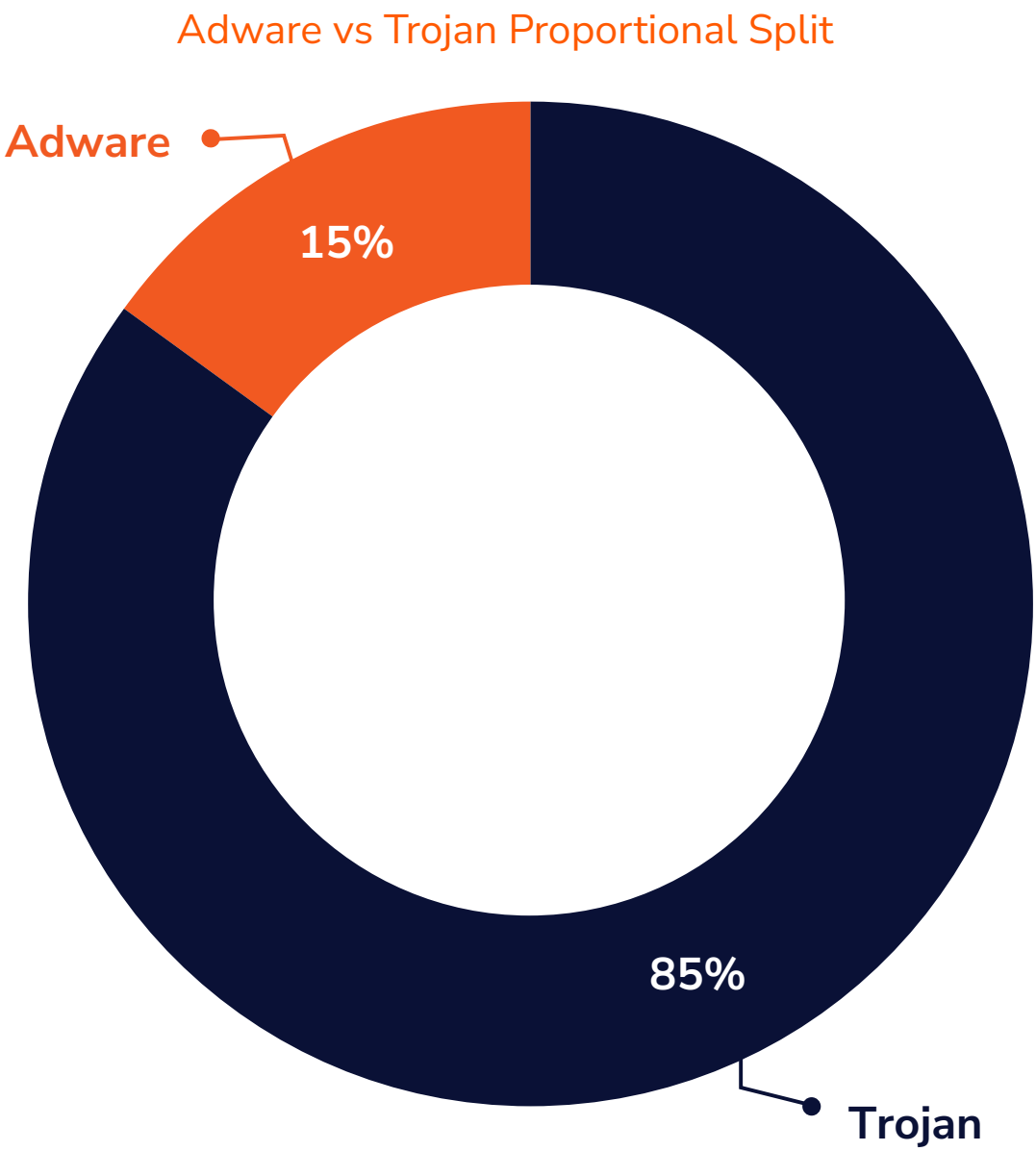
STEP: 6

Security event logs were cleared shortly after encryption

Back To Contents

THE MOBILE DEVICE STORY

Mobile threats are exploding. Trojans now account for a staggering 85% of detections, leaving adware far behind at just 15%. Attackers have moved on from quick cash grabs, zeroing in on corporate networks with precision and intent to cause real damage.

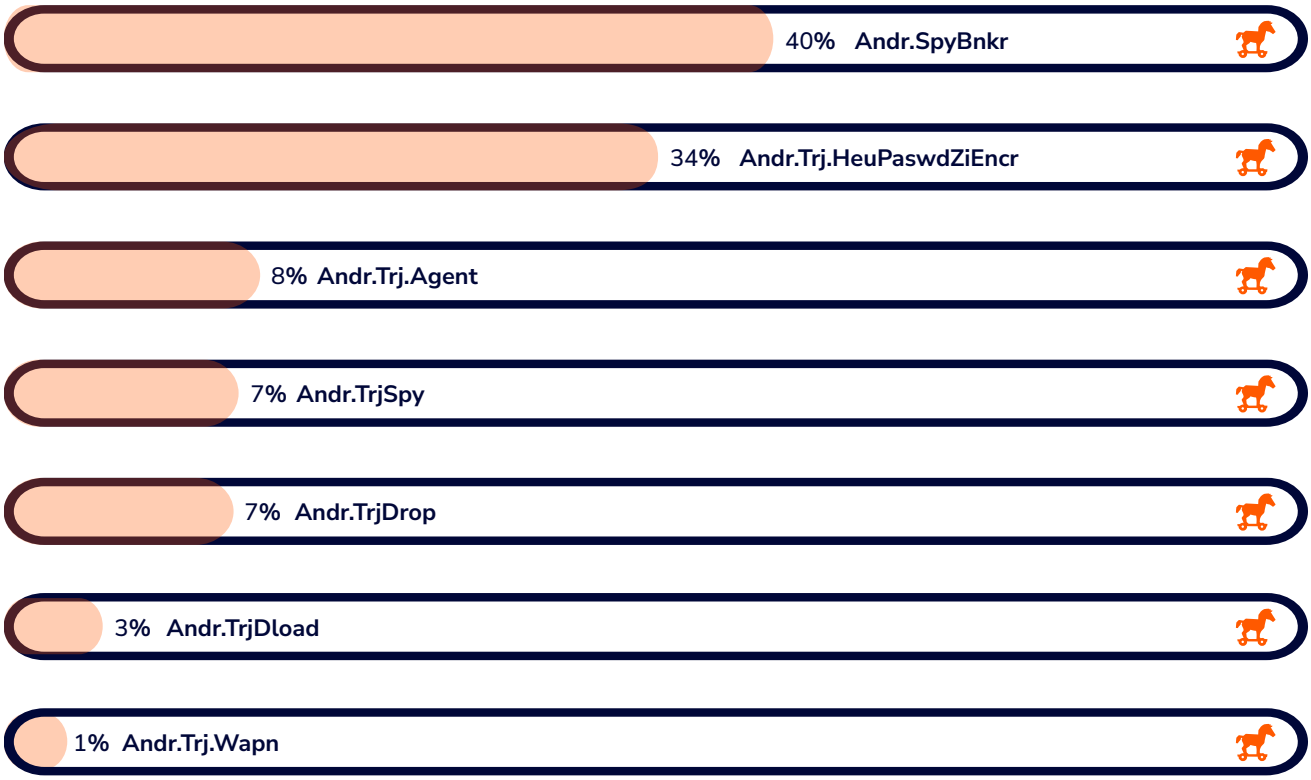


Trojans now masquerade as everyday apps, sneaking past defenses and quietly opening backdoors for ransomware and lateral movement. The risk is immediate: one undetected breach can trigger data theft, business shutdowns, and costly extortion. The old playbook, waiting and reacting, no longer works.

Back To Contents

TROJAN TAKEOVER LOOMS

The Wicked Trendline of Trojans

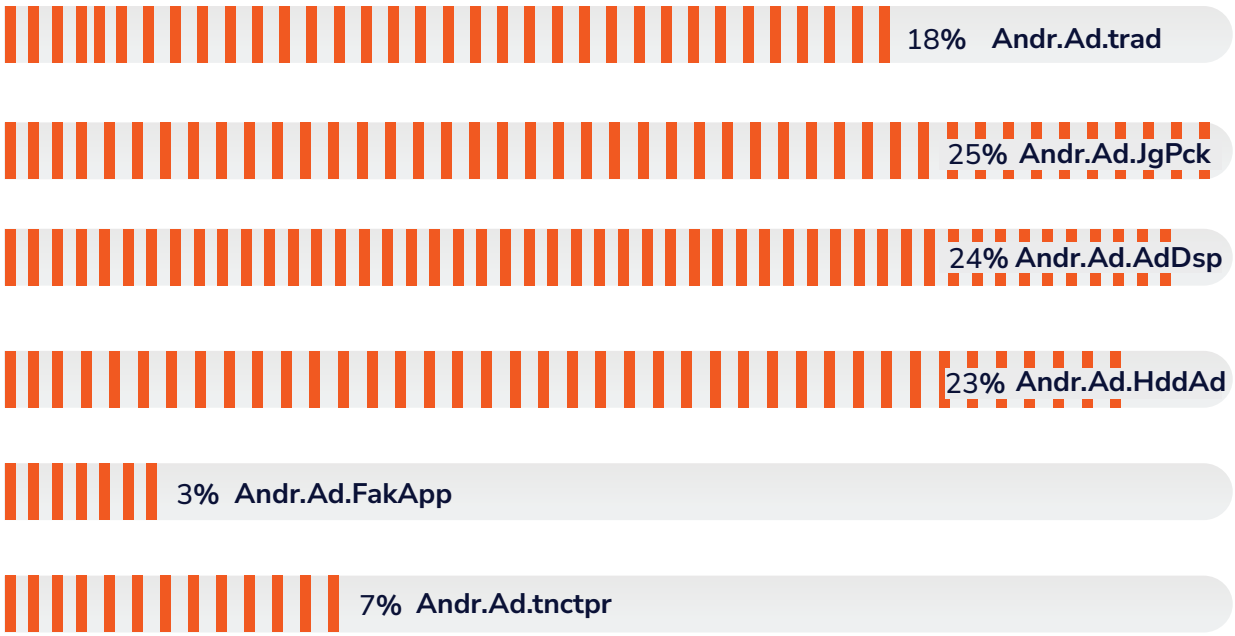


Banking Trojans and password stealers now make up nearly three-quarters of all mobile threats, 40% and 34% respectively. As employees rely on smartphones beyond the safety of office walls, attackers pounce, using fake overlays to snatch credentials and MFA codes. Unmanaged devices are the soft underbelly. Just one compromised phone can open the door to network breaches, financial hits, and data leaks that erode trust and put compliance at risk.

Back To Contents

THE ADWARE EVOLUTION: FROM NUISANCE TO PRECURSOR

Most Prevalent Adware Types



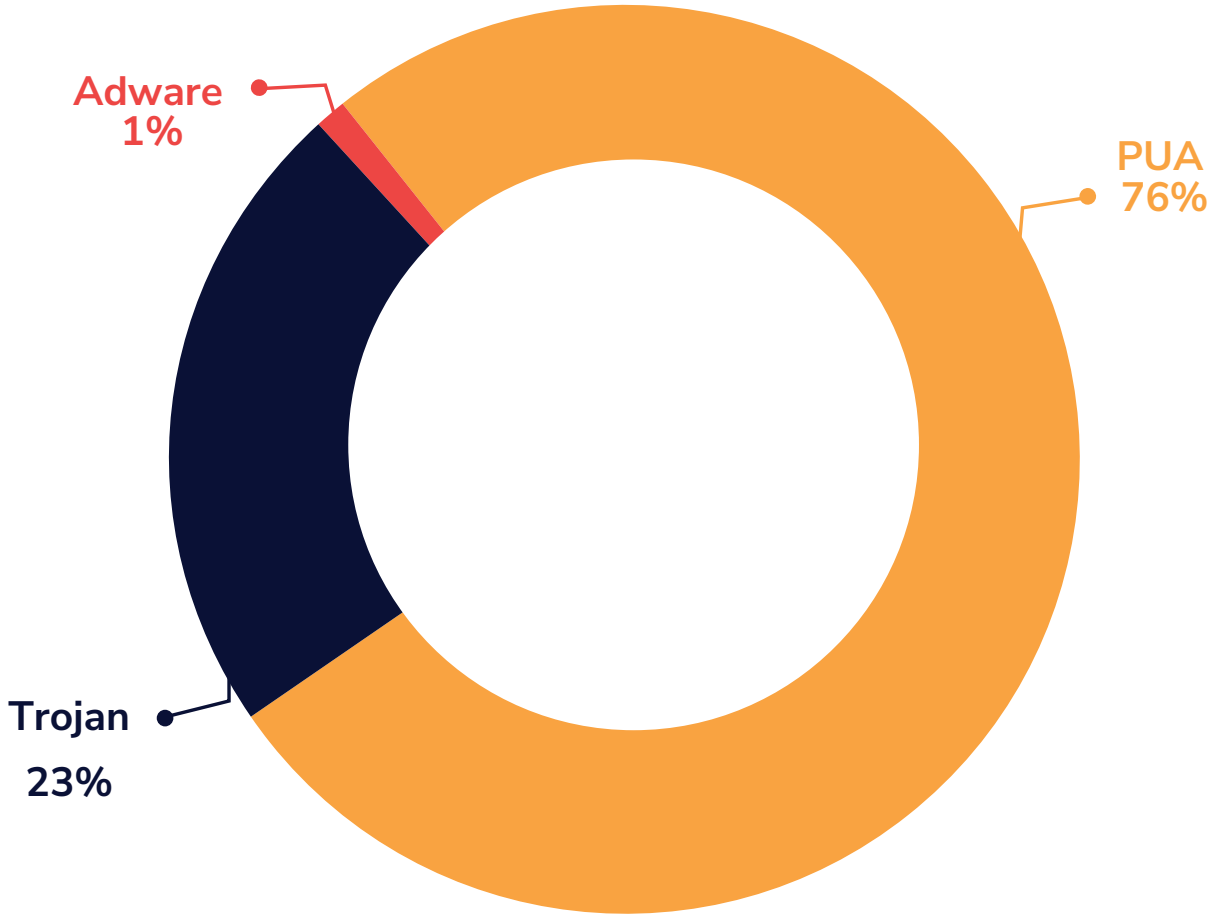
Adware is no longer just a nuisance. Hidden variants and aggressive pop-ups now hijack nearly half of BYOD devices, siphoning off telemetry and tracking users in the background. The fallout? Lost productivity, quiet data theft, and a wider attack surface that hands adversaries a shortcut into corporate systems.

Back To Contents

THE MAC ATTACK

As enterprises increasingly adopt macOS for its perceived security, adversaries are aggressively pivoting to exploit this growing attack surface. The long-standing myth of Mac invulnerability is now a strategic liability, placing high-value users directly in the crosshairs. Relying on legacy reputation is no longer viable; protecting intellectual property requires dedicated, enterprise-grade security.

Trojan, Adware and PUA Proportional Split



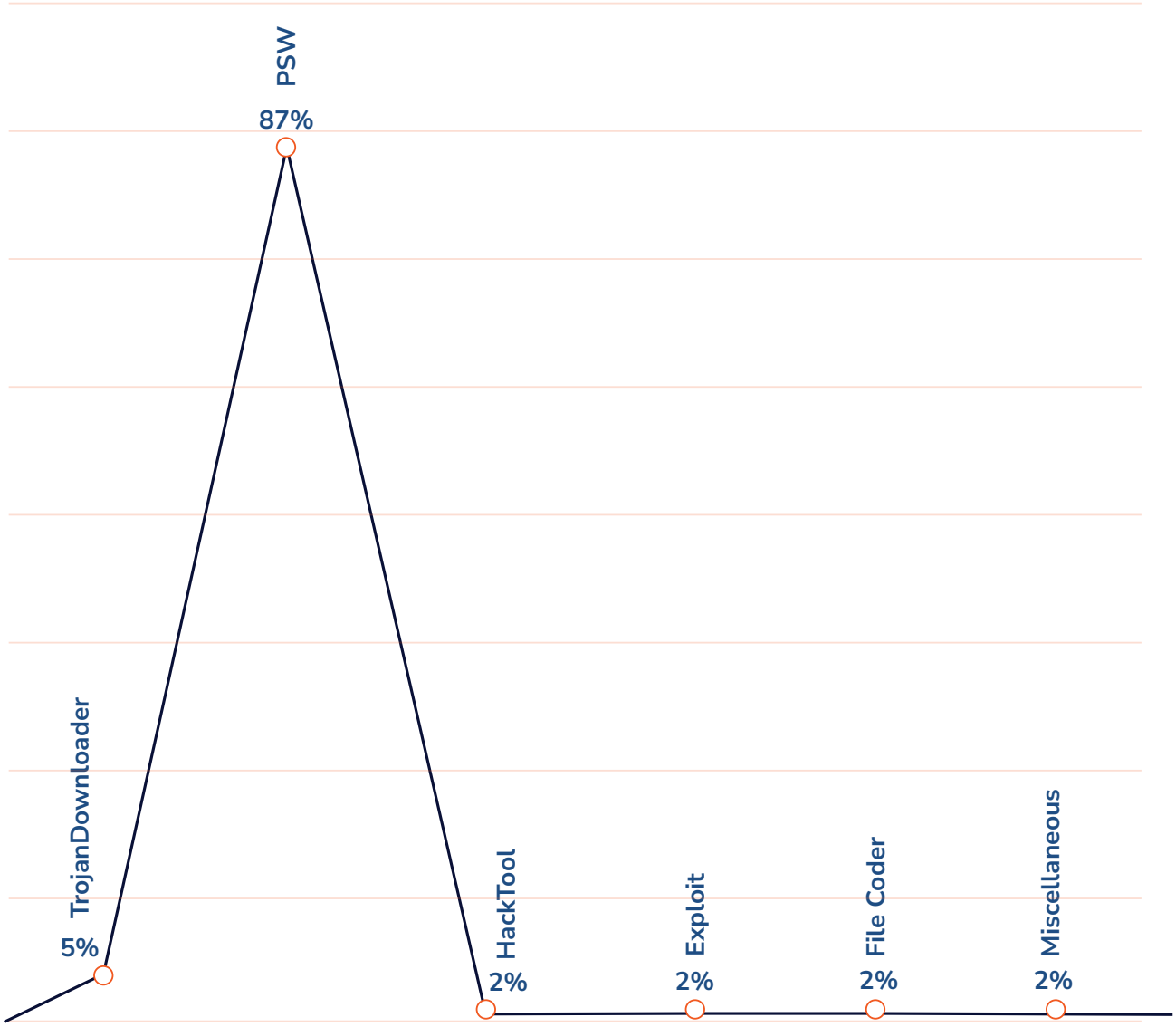
Modern macOS threats do not rely on brute force. Instead, they quietly infiltrate systems to establish persistence and target user credentials. Recent telemetry reveals that Potentially Unwanted Applications (PUAs) now account for 76% of initial access points, driving nearly a quarter of all Trojan payloads. Attackers are effectively weaponizing grayware to bypass traditional security perimeters, making proactive endpoint defense a critical business requirement.

Back To Contents

THE RISE OF TROJANS

The cybersecurity battleground has shifted from compromising infrastructure to stealing identities. Adversaries prioritize credential harvesting, using stolen logins to bypass multi-factor authentication and embed themselves within critical networks. These tools operate silently in the background, extracting browser data and session tokens to establish a persistent foothold.

Trojan Detection Trend Lines



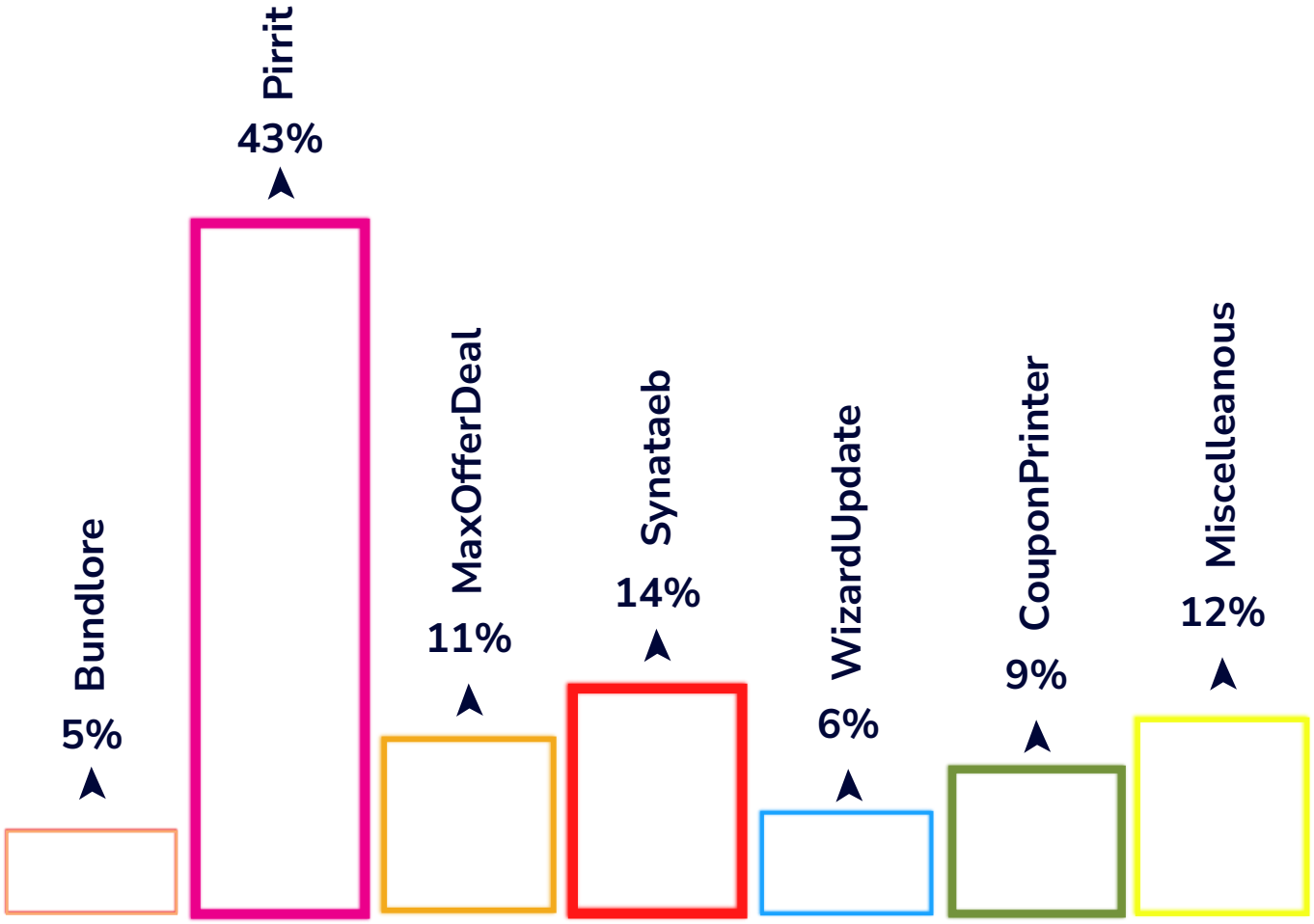
The business fallout from compromised identities is severe, ranging from deep network infiltration to sweeping data leaks that expose sensitive operational intelligence. With digital sovereignty becoming a board-level priority, this surge in identity-driven attacks dictates a clear strategic response: robust credential management and a strict Zero Trust architecture are imperative for organizational resilience.

Back To Contents

THE HIDDEN RISKS OF ADWARE

Adware remains a significant operational hurdle, currently dominated by variants like Pirrit and Synataeb. As hybrid work environments blur the boundaries between personal and business applications, attackers use grayware to penetrate corporate networks. These threats embed themselves deeply into system settings and browser extensions to hijack traffic and siphon off telemetry data, often evading signature-based defenses entirely.

The Trendline of Adware Variant Detections



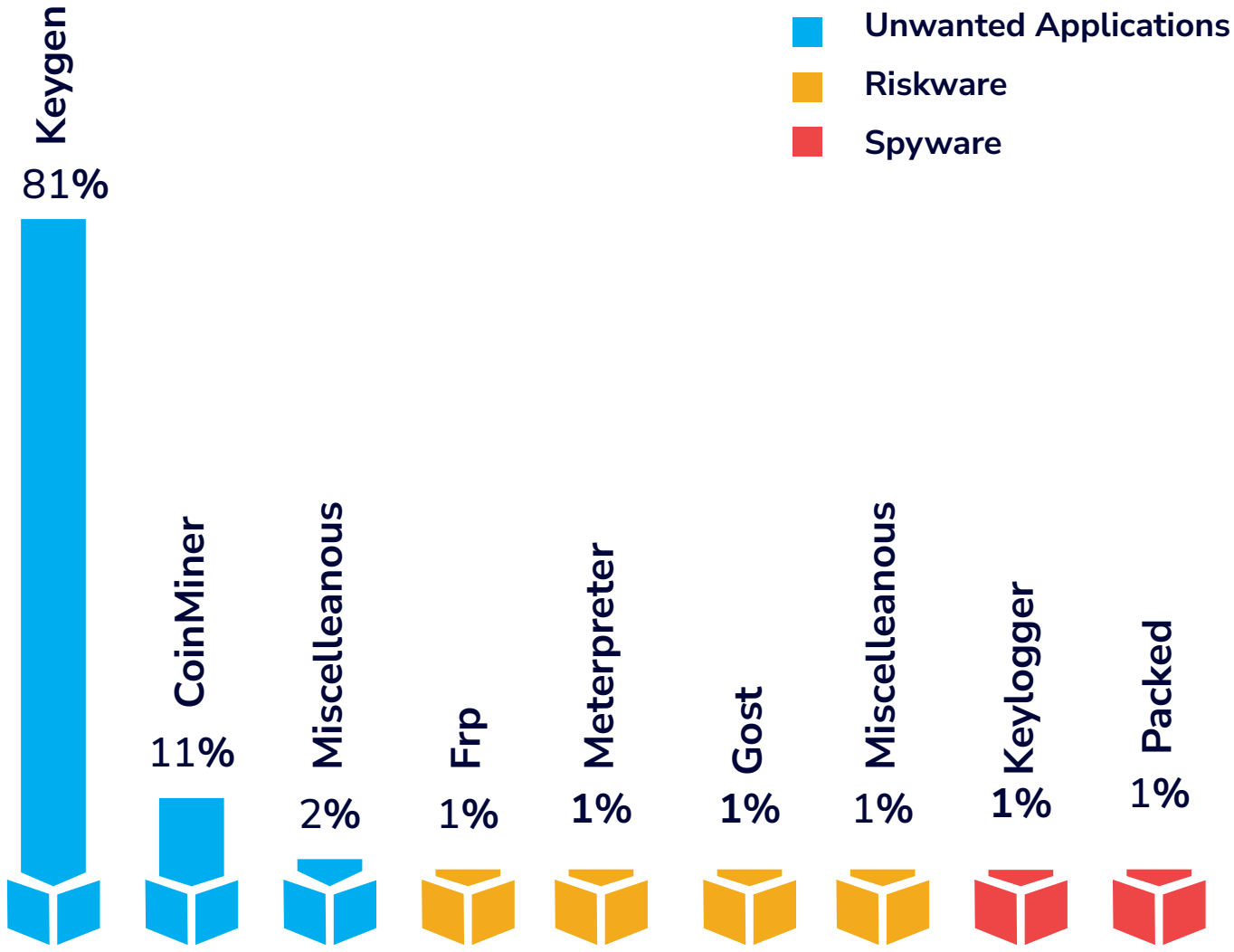
Treating adware as a mere nuisance is a dangerous oversight. These persistent installers act as gateways for more destructive threats, including spyware and targeted credential theft. Overlooking these seemingly minor intrusions allows sophisticated adversaries to establish access, ultimately leading to system degradation, major data breaches, and a loss of customer trust.

Back To Contents

SHADOW IT AND POTENTIALLY UNWANTED PROGRAMS (PUPS)

The proliferation of Potentially Unwanted Programs, particularly Keygen tools, represents a glaring vulnerability in the corporate defense matrix. When employees utilize shadow IT or pirated software to bypass licensing costs, they unknowingly introduce advanced malware into the network.

Most Prevalent PUP Types

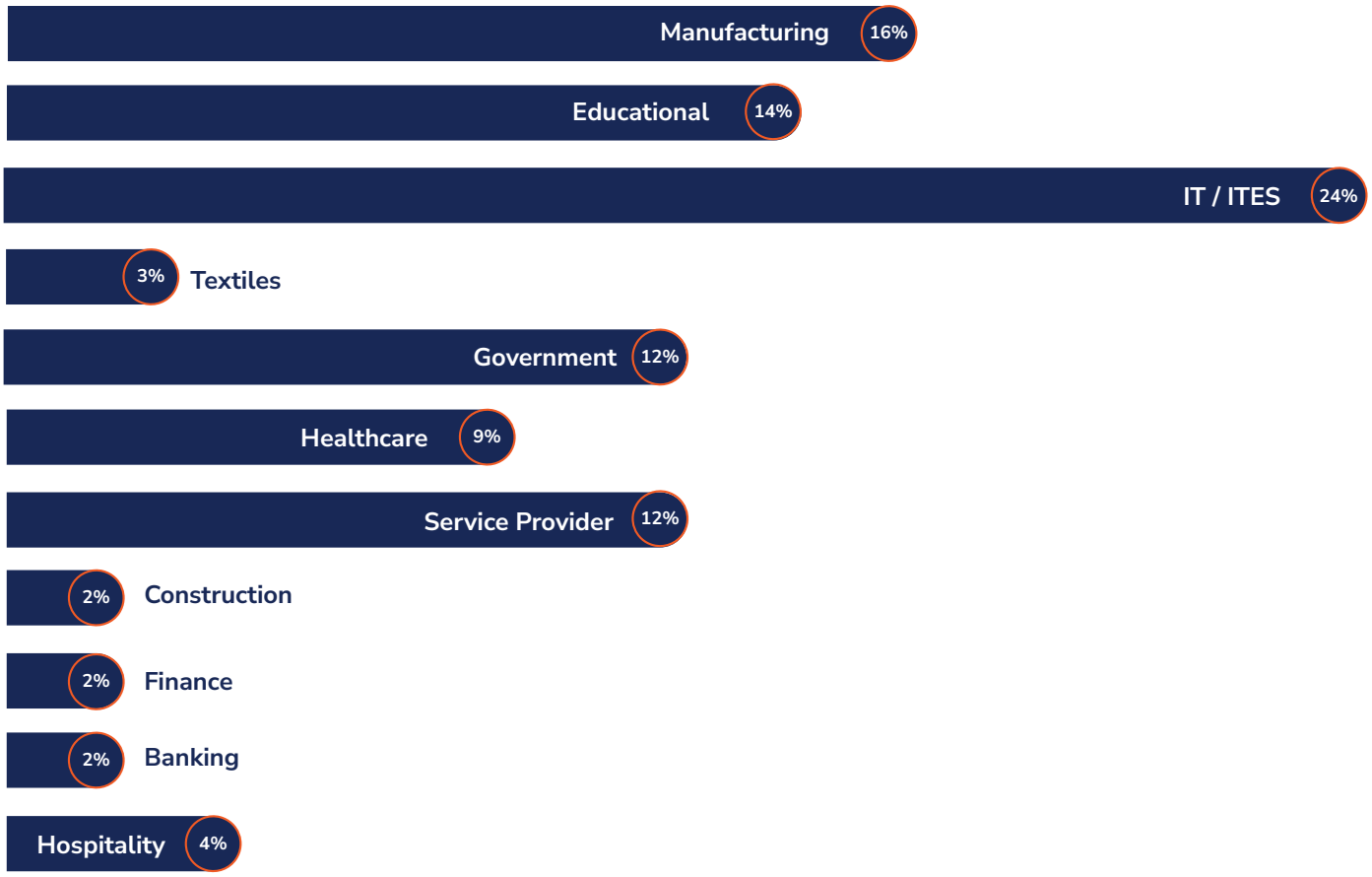


Armed with administrative privileges, these malicious tools can rewrite core system files. Telemetry actively tracks the deployment of CoinMiners and Meterpreter shells through these vectors, enabling attackers to hijack hardware for crypto-mining or establish remote command infrastructure. The resulting business impacts extend far beyond degraded machine performance; they introduce critical compliance failures, enable stealthy data theft, and provide threat actors with a direct foothold into your digital infrastructure.

Back To Contents

VULNERABILITIES GALORE

Unpatched vulnerabilities enable large-scale breaches, as attackers use legacy exploits to bypass current security measures. These weaknesses let state-sponsored actors target critical infrastructure, especially in the current geopolitical environment.



Global telemetry shows that MS17-010 variants account for over 60% of detections, demonstrating that older exploits remain prevalent. The continued presence of SMBV3 and Log4j vulnerabilities points to a trend of automated, worm-like attacks that can disrupt global supply chains. For businesses, this highlights the importance of addressing known vulnerabilities to prevent data breaches and operational disruptions.

Below are the most significant vulnerabilities identified during this period. For reference, we've added MITRE ATT&CK and CVE codes, along with vulnerability data that turn a static technical flaw into strategic intelligence.

Back To Contents

CISCO UNIFIED COMMUNICATIONS PRODUCTS

CVE-2026-20045 | CVSS 8.2 | Improper validation of user input in HTTP requests → Remote Code Execution

IMPACT: An attacker can gain user-level access, then ride a privilege-escalation path straight to root control of the system.

MITRE T1190: Exploit Public-Facing Application

MITRE T1068: Exploitation for Privilege Escalation

ACTION: Upgrade to a fixed software release to remediate this vulnerability.

APPLE MULTIPLE OS

CVE-2026-20700 | CVSS 7.8 | Memory Corruption → Execute Arbitrary Code

IMPACT: Attackers with memory write capability may be able to execute arbitrary code.

MITRE T1203: Exploitation for Client Execution

ACTION: Patch all Apple devices with the latest update.

MICROSOFT OFFICE AND MICROSOFT WORD SECURITY FEATURE BYPASS VULNERABILITY

CVE-2026-21509 | CVSS 7.8 | Reliance on untrusted inputs → Security Feature Bypass

CVE-2026-21514 | CVSS 7.8 | Reliance on untrusted inputs → Security Feature Bypass

IMPACT: Allows an unauthorized attacker to bypass a security feature locally by tricking users into opening malicious documents.

MITRE T1566.001: Phishing- Spearphishing Attachment

MITRE T1204.002: User Execution- Malicious File

ACTION: Apply Microsoft January and February 2026 Office security updates.

MICROSOFT DESKTOP WINDOW MANAGER (DWM)

CVE-2026-20805 | CVSS 5.5 | Improper handling of memory addresses → Information disclosure of the address of a remote ALPC port

IMPACT: Disclosure of sensitive user-mode memory information, which may assist further exploitation.

MITRE T1082: System Information Discovery

MITRE T1046: System / Network Discovery (memory structure discovery)

ACTION: Apply Microsoft January 2026 Patch Tuesday security updates to fix improper memory handling in Desktop Window Manager.

MICROSOFT REMOTE DESKTOP SERVICES

CVE-2026-21533 | CVSS 7.8 | Improper Privilege Management → Elevation of Privilege

IMPACT: Allows an authorized attacker to elevate privileges locally.

MITRE T1068: Exploitation for Privilege Escalation

ACTION: Apply Microsoft February 2026 Patch Tuesday security updates.

GOOGLE CHROME

CVE-2026-2441 | CVSS 8.8 | Use-after-Free in CSS → Execute Arbitrary Code

IMPACT: Attackers may execute arbitrary code inside a sandbox via a crafted HTML page

MITRE T1203: Exploitation for Client Execution

ACTION: Update Chrome to the latest stable version.

DELL RECOVERPOINT FOR VIRTUAL MACHINES

CVE-2026-22769 | CVSS 10.0 | Use of Hard-Coded Credentials → Privilege Escalation

IMPACT: An unauthenticated remote attacker may gain unauthorized access to the underlying operating system and achieve root-level persistence.

MITRE T1078: Valid Accounts

MITRE T1068: Exploitation for Privilege Escalation

ACTION: Apply Dell's fix to block this attack.

Back To Contents

MONGODB DENIAL OF SERVICE

CVE-2026-25611 | CVSS 8.7 | Asymmetric Resource Consumption → Denial of Service

IMPACT: Unauthenticated messages can exhaust available memory and crash a MongoDB server.

MITRE T1499: Endpoint Denial of Service

ACTION: Update the MongoDB server with the required patch.

AMAZON AWS-LC (LIBCRYPTO)

CVE-2026-3336 | CVSS 8.7 | Improper Certificate Validation → Authentication Bypass

CVE-2026-3337 | CVSS 8.2 | Observable Timing Discrepancy → Authentication Bypass

CVE-2026-3338 | CVSS 8.7 | Improper Verification of Cryptographic Signature → Authentication Bypass

IMPACT: Allows an unauthenticated user to bypass signature verification when processing PKCS7 objects and bypass authentication.

MITRE T1553: Subvert Trust Controls

MITRE T1557: Adversary-in-the-Middle

ACTION: Applications using AWS-LC should upgrade to AWS-LC version 1.69.0.

IOT VULNERABILITIES

Qualcomm Snapdragon Multiple Platforms

CVE-2026-21385 | CVSS 7.8 | Integer Overflow → Memory Corruption

IMPACT: Integer overflow in the graphics component that causes memory corruption during memory allocation.

MITRE T1203: Exploitation for Client Execution

MITRE T1068: Exploitation for Privilege Escalation

ACTION: Upgrade to the latest security patch.

FORTINET MULTIPLE PRODUCTS

CVE-2026-24858 | CVSS 9.8 | Improper Access Control → Authentication Bypass

IMPACT: Gain unauthorized administrative access to organizations' Fortinet devices

MITRE T1078: Valid Accounts

MITRE T1556: Modify Authentication Process

ACTION: Upgrade to a fixed release and disable the FortiCloud SSO feature.

IVANTI ENDPOINT MANAGER MOBILE (EPMM)

CVE-2026-1281 | CVSS 9.4 | Command Injection → Remote Code Execution

IMPACT: Allow attackers to achieve unauthenticated remote code execution via a code injection technique

MITRE T1059: Command and Scripting Interpreter

ACTION: Apply the latest security patch provided by Ivanti.

Back To Contents

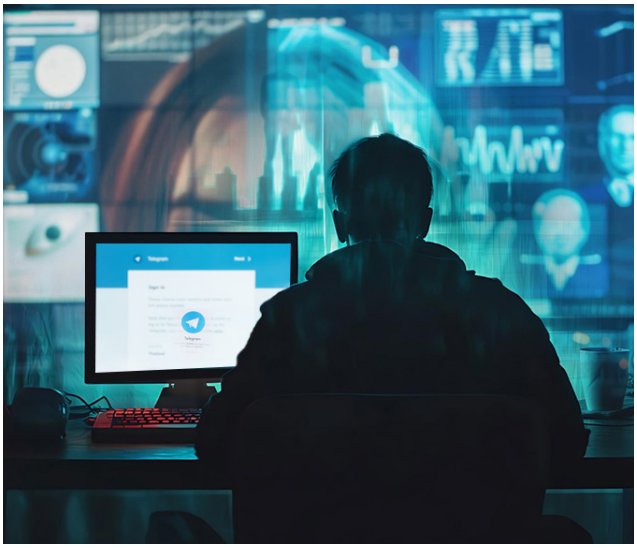
LATEST SECURITY NEWS

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

Typosquatted Websites

This blog is about how attackers are abusing Telegram though social engineering to distribute malware disguised as legitimate software bypassing security defenses.

Refer Telegram Campaign for details



Resoker: A Telegram Based Remote Access Trojan

- Resoker, a new Remote Access Trojan (RAT) is controlled through the social media app Telegram.
- It allows an attacker to monitor and control an infected system remotely by using the Telegram bot API to silently receive commands and send data back.
- The malware includes several features—persistence, privilege escalation, system monitoring, and techniques to avoid detection—making it a potentially dangerous threat.

Refer Resoker for details

Snake Keylogger

Gibcrypto, a new addition to the ransomware landscape, uses multiple stealthy tactics to bypass security checks provided by Microsoft and the victims' data cannot be retrieved even if the ransom is paid to the threat actors.

Refer Gibcrypto for details

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, in which cyber operations are integral to statecraft, eroding global trust and stability. The biggest threat to resilience is the lack of enforcement to patch vulnerabilities as soon as patches become available, as shown by legacy exploits like MS17-010 still accounting for 70% of all detections years after patches became available. Social engineering techniques are still a favorite option for adversaries as victims are still naive to keep up with the sophisticated techniques being used by threat actors to lure naive users.

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 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

K7 SECURITY

www.k7computing.com