K7 SECURITY

www.k7computing.com

PHISHING'S EVOLVING DISGUISE: HUMAN-CENTRIC ATTACKS

Phishing attacks are not new. It has been there since the cyber world was unleashed; just that it has become more and more sophisticated with a growing cyber population. Targeted socially engineered attacks have increased over the years in cyberspace.

Though cyber awareness campaigns have been on the rounds to help cyber users identify and learn from phishing attacks, humans still continue to be the most vulnerable in identifying whether it is a phishing threat or not.

So why are human-centric attacks still on the rise? This is primarily due to human emotions.
For instance, employees still continue to urgently reply to emails if they come from a sender with whom they are emotionally connected with. In this case, it has to do with respect. Obeying a seniors' orders is a matter of showing respect to their position and authority. So humans will think twice to check the authenticity of the email when it appears to come from a known sender.

To minimise this, organizations should start focusing on remediation, not just once their network has malware in it, but to restrict this payload from intruding into their organizations' network through socially engineered channels; by applying rules to restrict such threats from reaching the users' and also through increased cyber awareness.

We at K7 Labs offer significant protection from emerging and latest threats by closely examining and identifying such incidents and providing security at multiple layers.

Kindly read and share the report with your colleagues. Have a safe digital experience!
Enjoy reading!

Back To Contents

INFECTION RATE (IR)

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

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

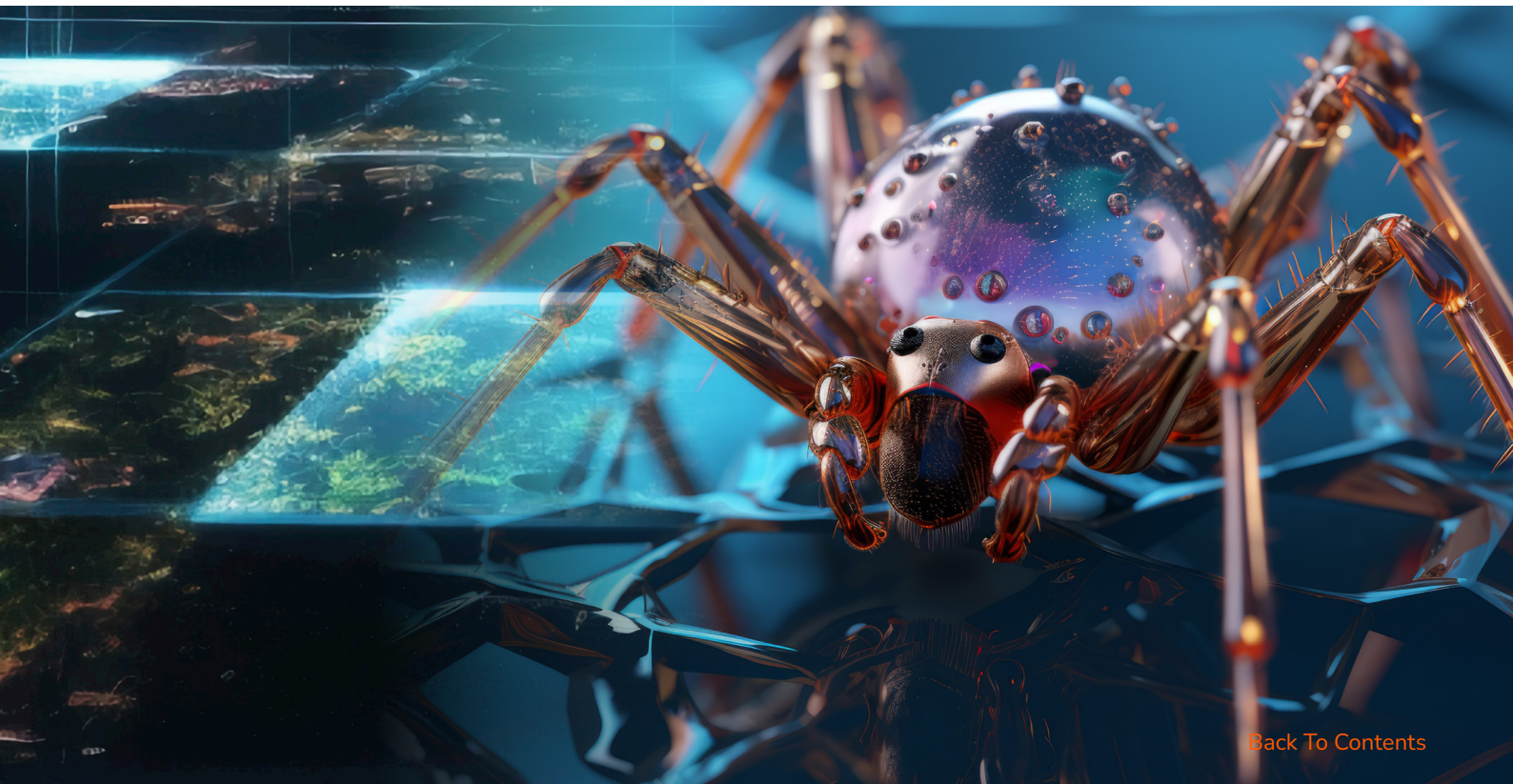
We use this IR factor to identify enterprises and netizens' exposure to cyber threats. IR is determined as the proportion of active K7 corporate or consumer users who encountered at least one cyber threat event that was blocked and reported to our K7 Ecosystem Threat Intelligence infrastructure (K7ETI).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

Active users indicate users who have activated and updated their products.

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

Infection Rate (IR) of an area

The Global IR for Q2_2025-26 was 19%

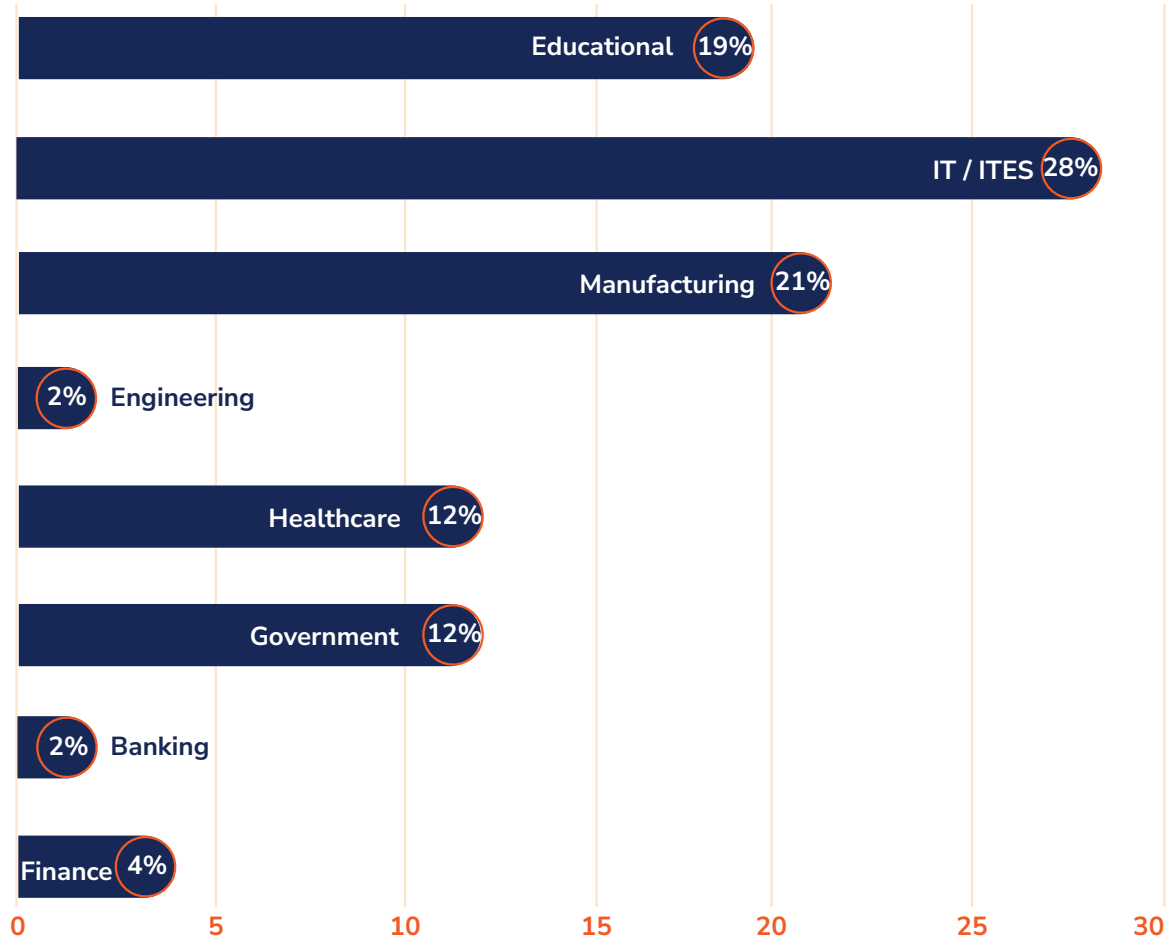


Back To Contents

VULNERABILITIES AND INDUSTRY IMPACT

The era of isolated attacks is over; we are firmly in a persistent cyber conflict driven by state-sponsored actors and highly professionalized cybercrime cartels. Our data, showing IT/ITES (28%) and Manufacturing (21%) as the most-hit sectors, is not a coincidence; it's a direct reflection of an adversary strategy focused on high-value intellectual property and supply chain choke points.

Vulnerability Impact grouped by Industry



For the C-suite and founders, this means two things: First, vulnerability debt is business debt. The continued exploitation of old flaws like MS17-010 (76%) highlights a critical failure in patching hygiene. Second, initial access vectors are becoming sophisticated. Current headlines, such as the major Jaguar Land Rover disruption in October 2025 and the surge of the Qilin ransomware group targeting critical Fortinet vulnerabilities, confirm that supply chain attacks and the exploitation of edge devices are now the main entry points. Furthermore, the DaVita healthcare attack in August 2025, compromising over 2.6 million patient records, proves that the Healthcare (12%) and Government (12%) sectors are consistently under siege.

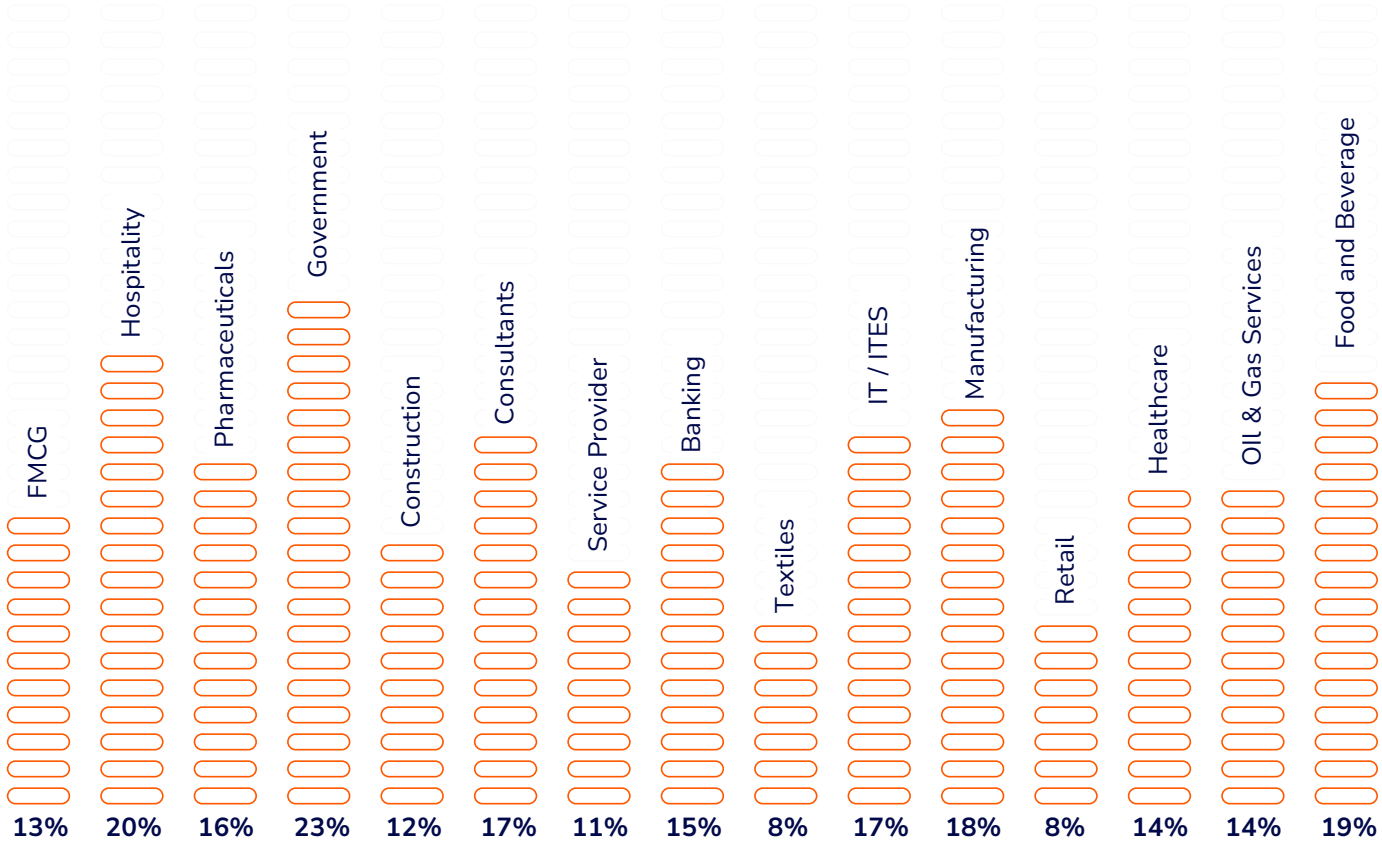
The lower proportional figures for Banking (2%) and Finance (4%) shouldn't breed complacency; instead, they signal these sectors face fewer, but far more sophisticated, low-volume, high-impact intrusions that bypass signature-based defenses.

Back To Contents

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

The Infection Rate (IR) data of significant industries serves as a stark warning, translating generalized threats into specific operational risks for CXOs and founders. The top-tier IR for Government (23%) and Hospitality (20%) confirms these sectors are high-velocity targets, prized for sensitive public data and high-volume transaction records, respectively. This signifies persistent threat actor activity and often reflects a critical lack of immediate patch deployment or robust segmentation.

Most Impacted Industries around the Globe

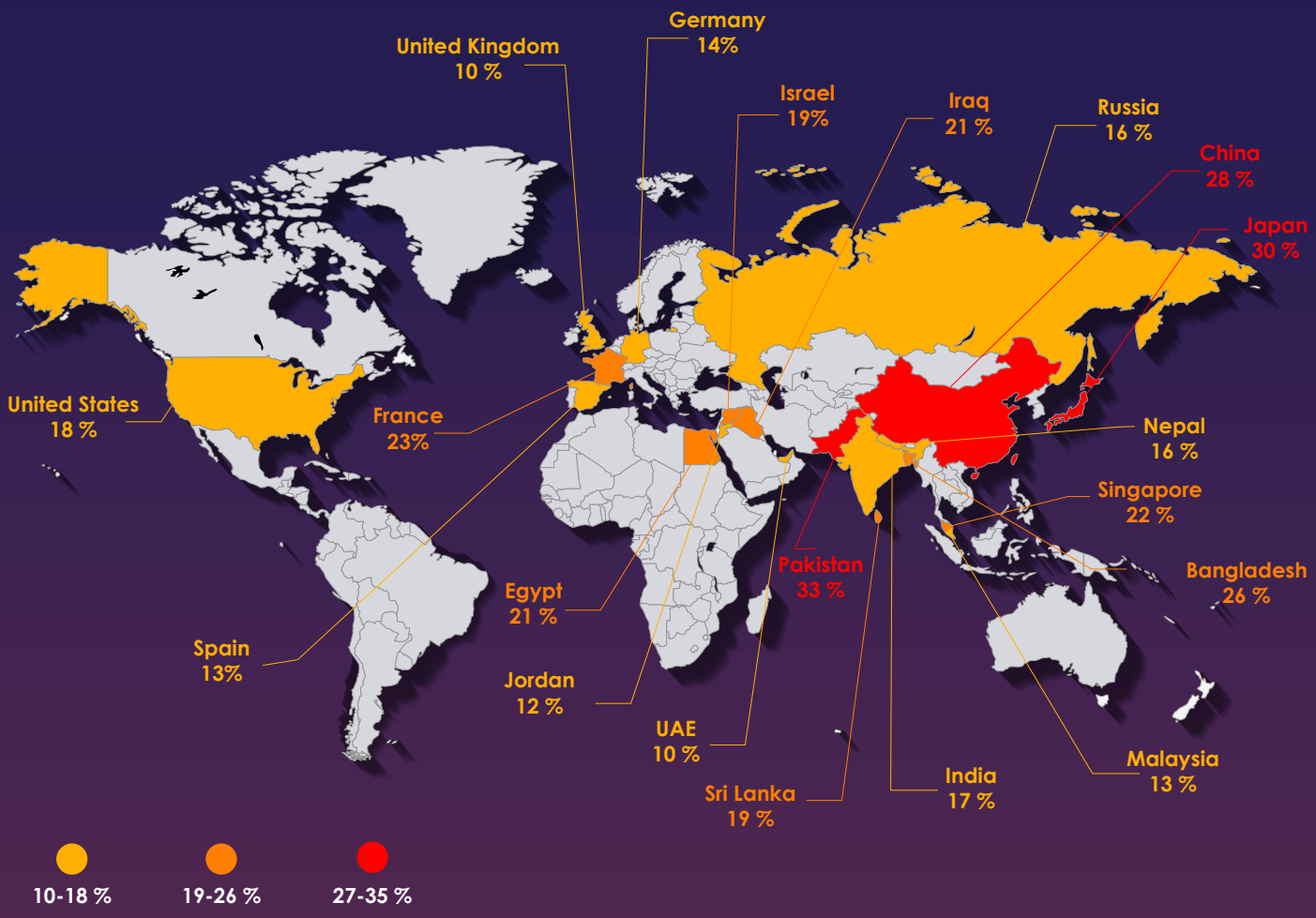


The elevated rates for Food and Beverage (19%), Manufacturing (18%), IT/ITES (17%), and Consultants (17%) highlight the pervasive threat environment across the economic engine. For these C-Level leaders, the risk is about supply chain contamination and intellectual property theft. An IR of 17% in a consulting firm, for instance, implies direct exposure of client-sensitive data. Even the seemingly modest 15% for Banking is alarming, suggesting high-volume, albeit potentially lower-impact, commodity malware is frequently finding footholds, often through employee endpoints. The lowest rates in Textiles (8%) and Retail (8%) may indicate a proportionally smaller volume of attacks, but not necessarily less severity.

Back To Contents

WORLDWIDE CYBER THREAT LANDSCAPE

The global chart reveals a stark, non-uniform risk landscape. While the US and UK hold low infection rates (18%, 10%), nations like Pakistan (33%) and Japan (30%) face a significantly amplified threat level.



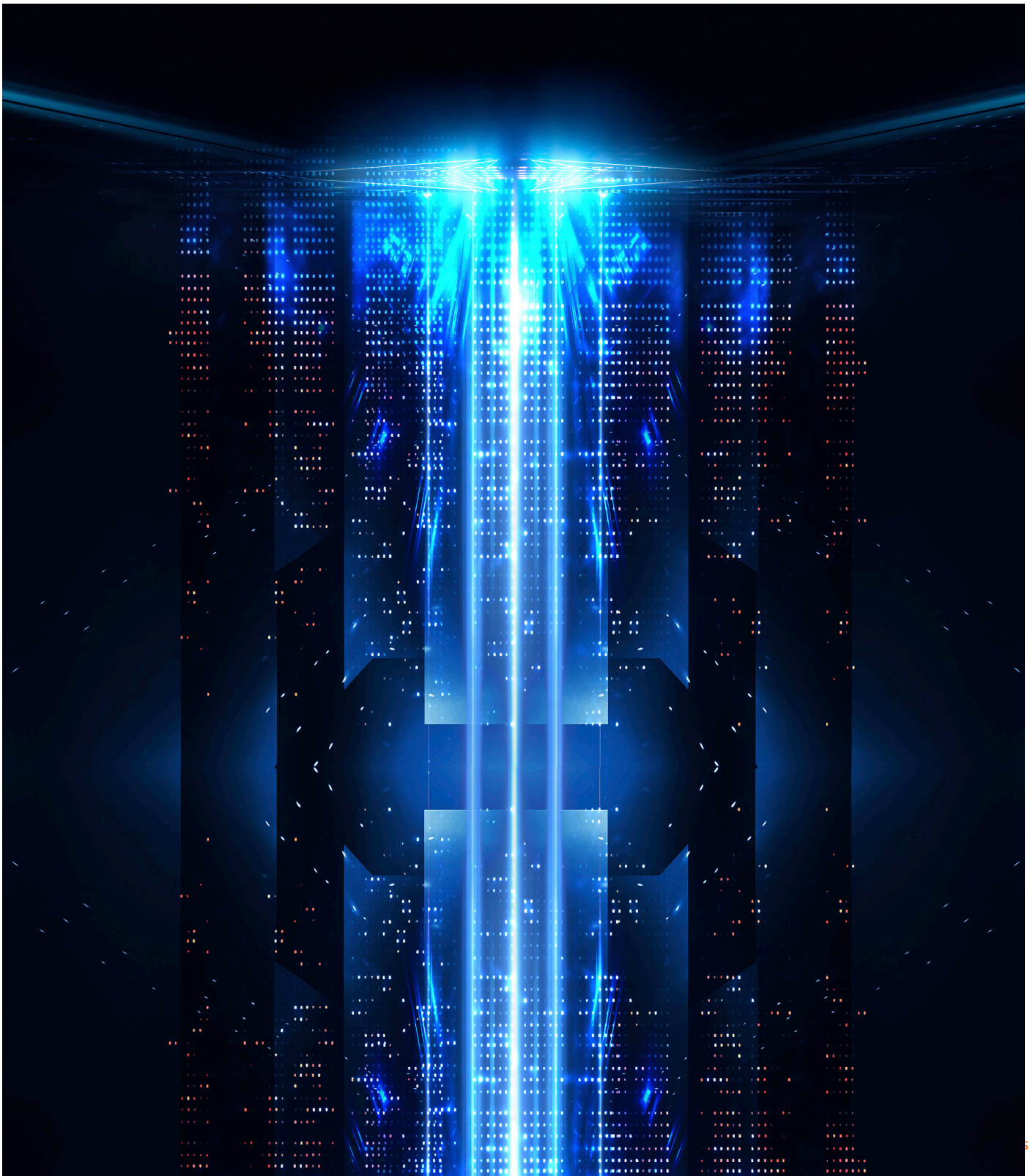
Back To Contents

WINDOWS THREAT LANDSCAPE

The question of why Windows remains the most discussed and heavily targeted operating system (OS) in the cyber threat landscape, despite the growing volume of threats targeting the Android platform, is rooted in a fundamental trifecta: market share, architectural history, and enterprise entrenchment.

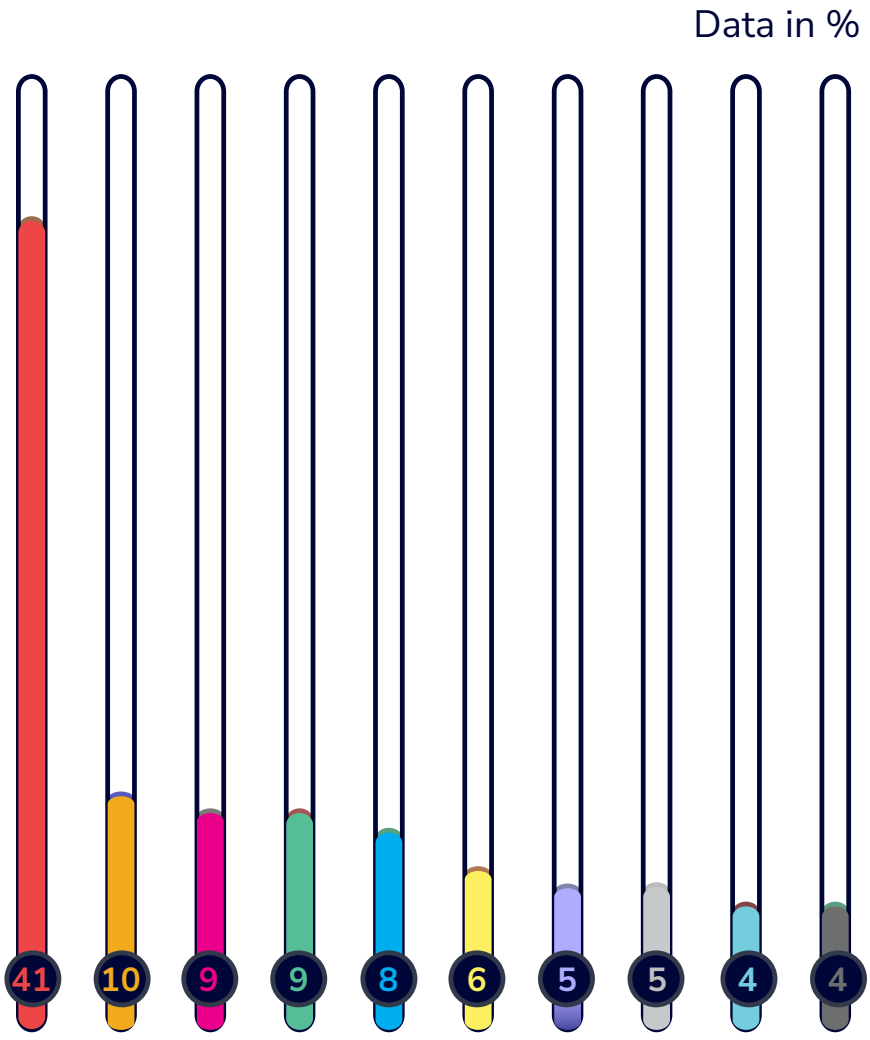
Windows' unparalleled global market share, which dominates corporate, government, and consumer desktop environments, offers threat actors the largest attack surface and the greatest return on investment (ROI).

Attacks on Windows are typically sophisticated, aimed at network lateral movement, intellectual property theft, and critical infrastructure disruption. Even as mobile adoption soars, the core business logic, critical servers, legacy systems, and proprietary applications still reside predominantly on the Windows ecosystem.



TOP MALWARE TARGETING WINDOWS SYSTEMS

The Windows malware landscape remains alarmingly dominated by adware and hack tools, indicating a pervasive threat of nuisance and unauthorized system modifications.

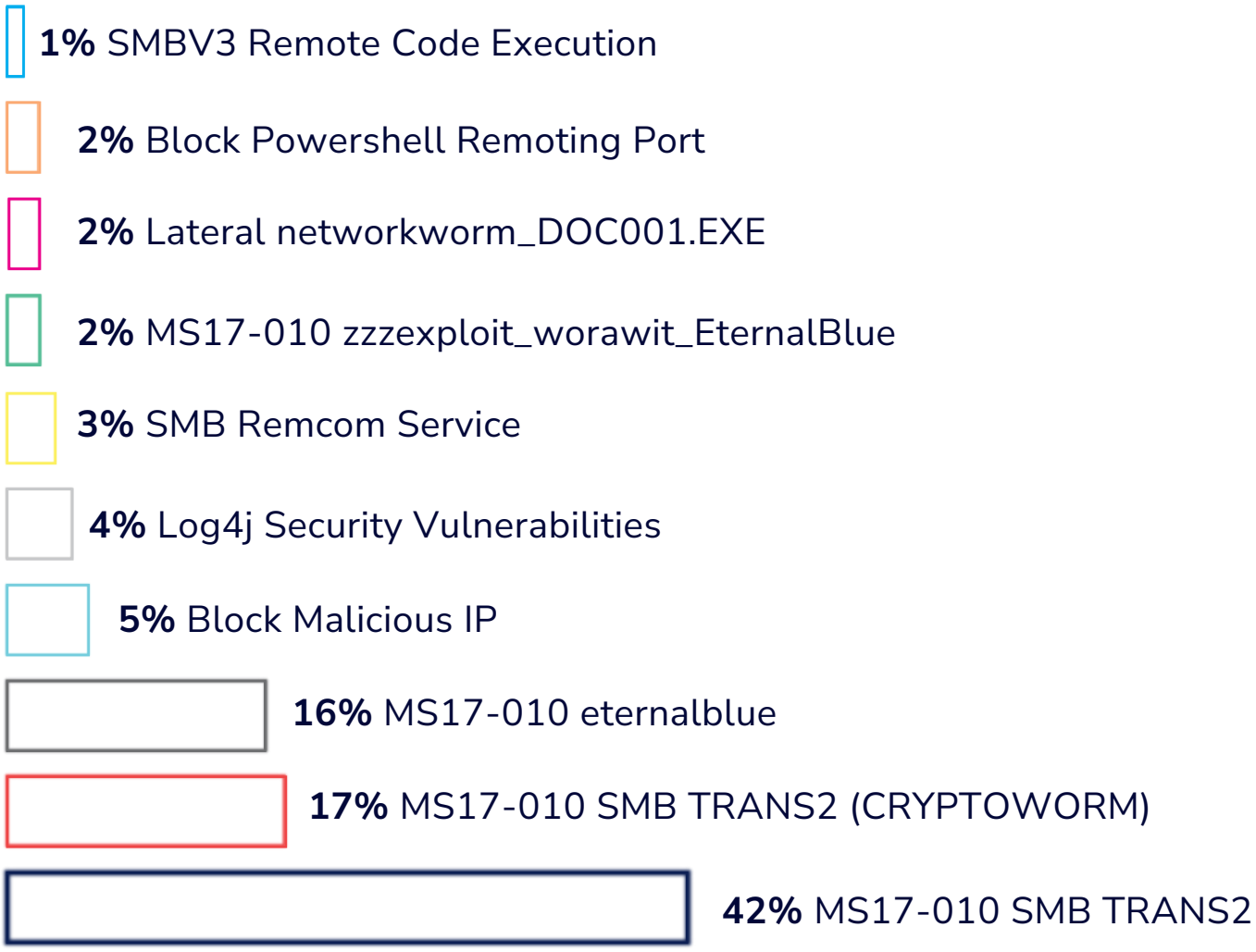


At the forefront is Adw.Win32.Cpp, accounting for a staggering 41% of detections, closely followed by the Hack.Win32.AddUser variants which collectively comprise 23%. This predominance of HackTools, often related to software 'cracking' or activation, underscores a high-risk user behavior, which threat actors, like those behind recent Infostealer and Ransomware operations (e.g., Lumma, Cl0p), are quick to capitalize on.

Back To Contents

UNPATCHED VULNERABILITIES: THE ACHILLES' HEEL OF WINDOWS SYSTEMS

The persistent and most critical threat to Windows remains the exploitation of MS17-010, an aging vulnerability in the Server Message Block (SMBv1) protocol.



This family of exploits, spearheaded by EternalBlue, dominates detections at a combined 75% (42% as SMB TRANS2, 17% as CRYPTOWORM, and 16% as eternalblue), cementing its role as the quintessential weapon for network lateral movement and mass infection.

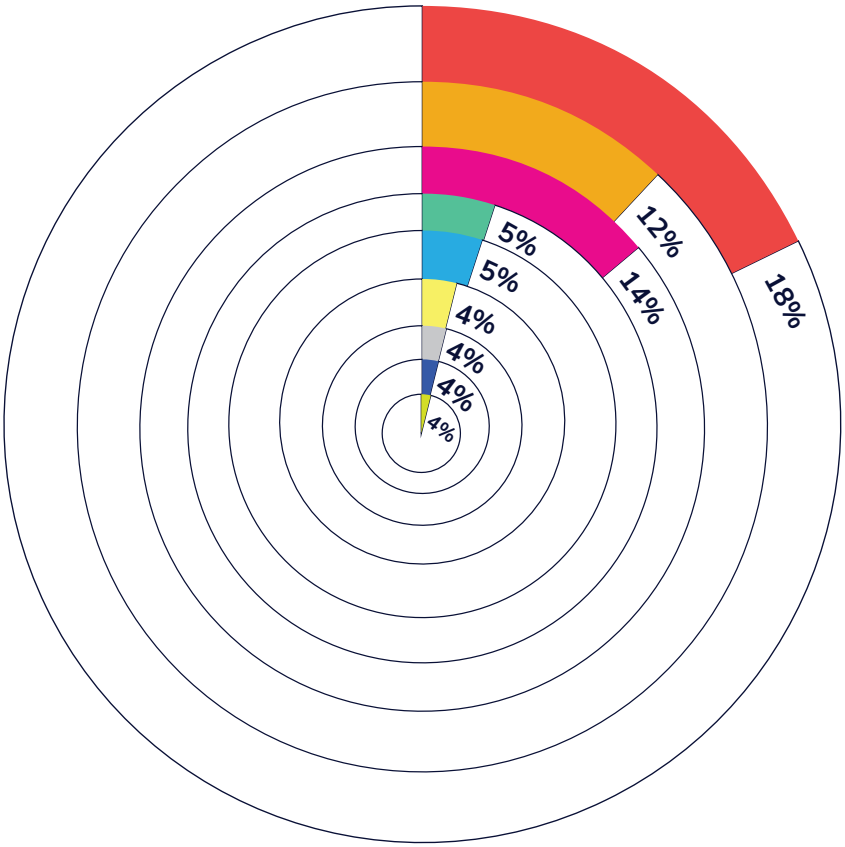
Despite being patched years ago, its high prevalence fuels devastating ransomware campaigns like WannaCry and NotPetya, underscoring a systemic failure in patching hygiene across enterprises globally. Addressing this legacy exposure is non-negotiable for fundamental cyber resilience.

Back To Contents

HEURISTIC HOST INTRUSION PREVENTION SYSTEM (HIPS)

Behavioral Heuristic Detections reveal a clear focus on the post-exploitation kill chain, where attackers leverage native tools for stealth.

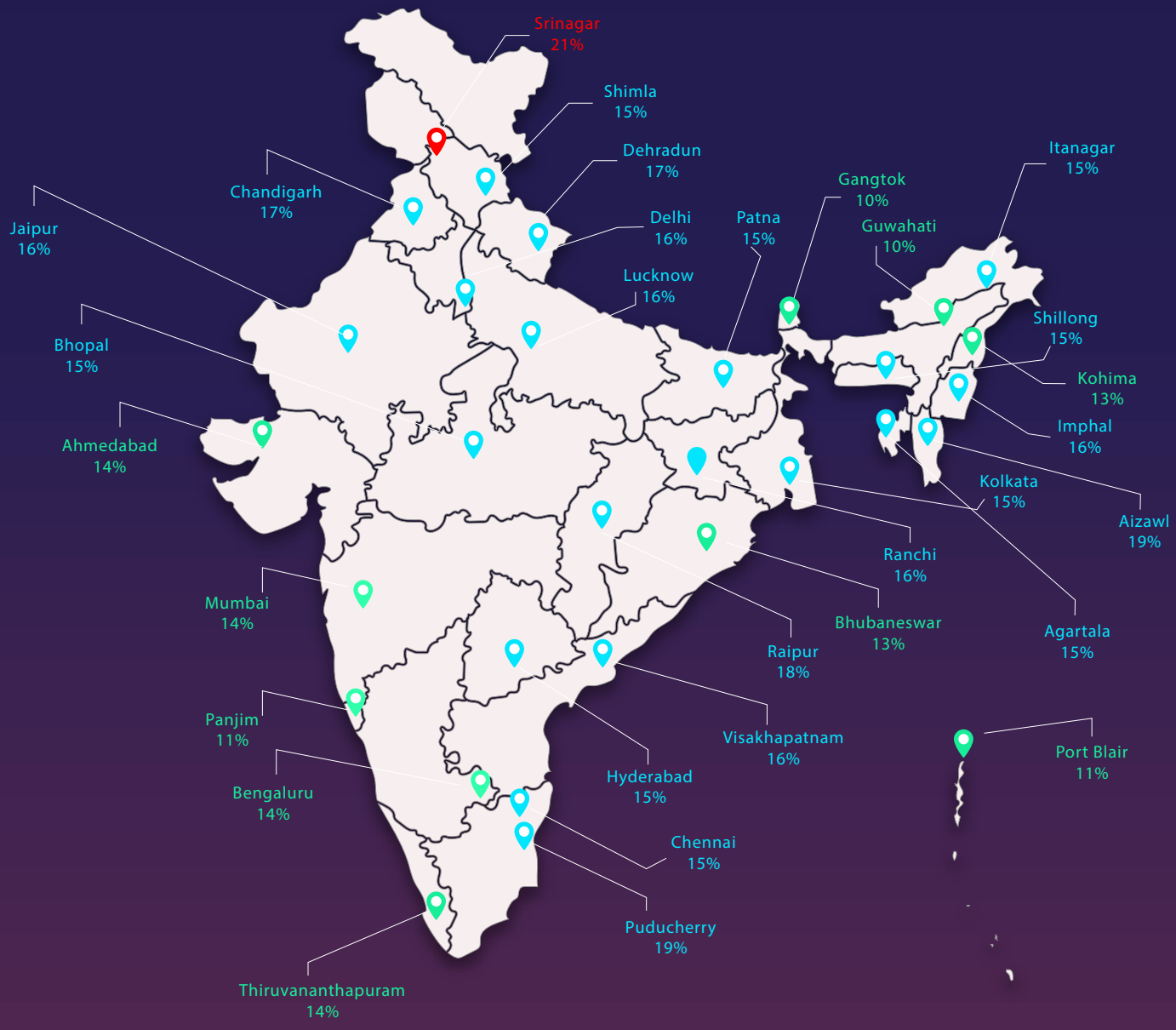
Windows Heuristic Behavioural Detection



Susp_Powershell (18%) remains the single largest indicator, confirming the dominant role of scripting for command execution and evasion. Coupled with Susp_dropper (14%) and Susp_LolBin_Write_PE (12%), which signal the use of legitimate binaries ("Living-off-the-Land") to deliver and write malicious executables, this data confirms a strategic shift toward fileless and hands-on-keyboard activity that bypasses traditional signature-based security layers.

Back To Contents

CYBER THREAT LANDSCAPE - INDIA



- 10%- 14%
- 15%- 19%
- 20%- 24%

Map for illustrative purposes only. Not to scale.

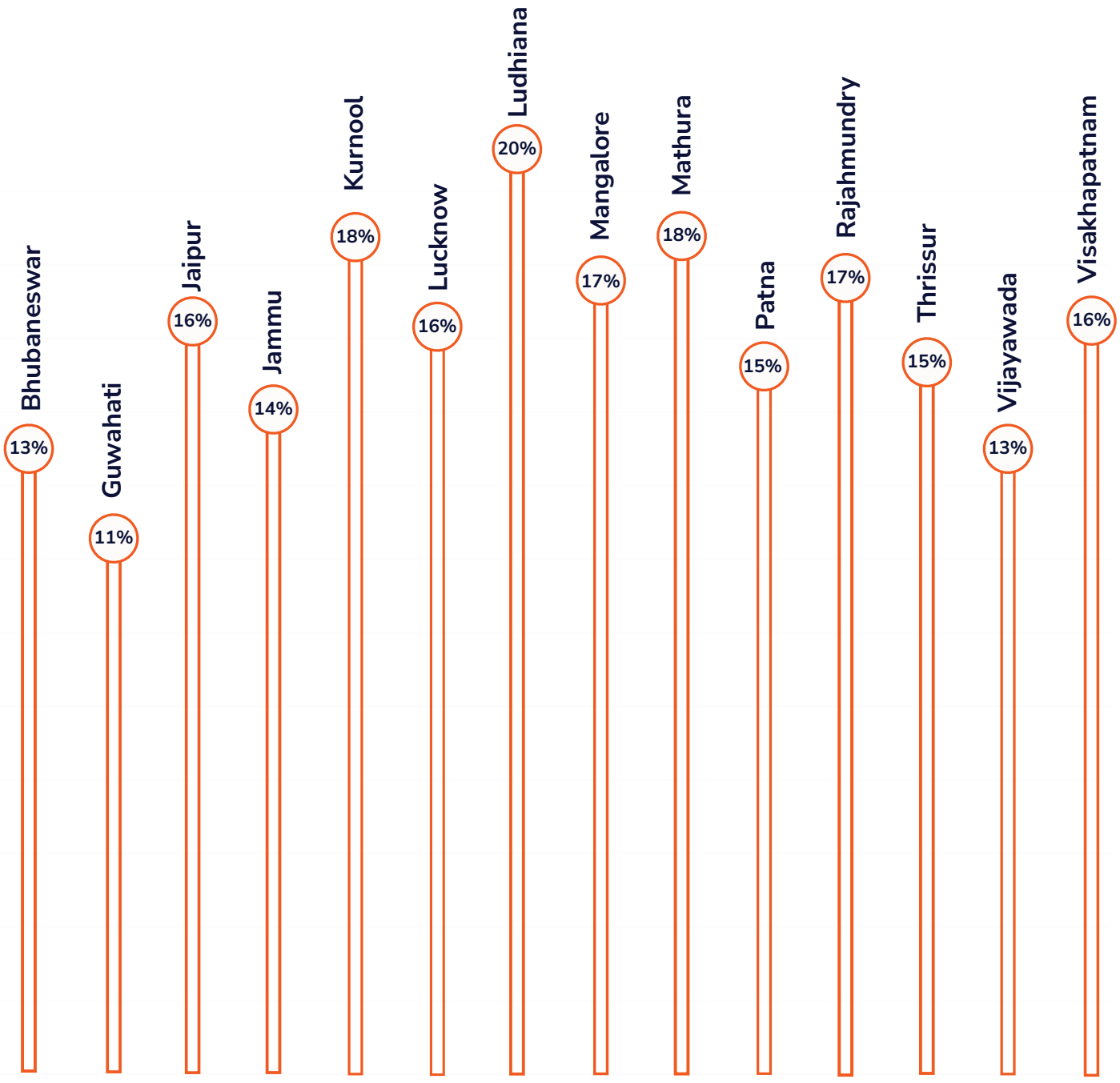
Back To Contents

THE METRO AND TIER-1 CITIES - INFECTION RATE

Our detection data across major Indian cities tells a straightforward story: Signature-based defenses, specifically our ScanEngineProtection, are the heavy lifters. They're catching over 80% of threats. This dominance isn't a badge of superior strategy, though; it just reflects the sheer, overwhelming volume of known, circulating malware we face. It's the front door holding back the common riff-raff.

Back To Contents

TOP INFECTION RATES IN TIER-2 CITIES



Across India's Tier-2 cities, the average infection rate is alarmingly high, with rates peaking near 20 in cities like Ludhiana and Mathura. This spread, driven by the sheer volume of known threats, shows cyber risks are pervasive, hitting smaller urban centers with significant intensity.

Back To Contents

ENTERPRISE INSECURITY

Case Study: Purplefox installed using exposed SMB shares

SMB shares are used by enterprises to access their data on a remote system as if they were on local devices. However, this traffic can be exploited by threat actors to deploy malware.

In one of our enterprises' networks, Purplefox malware was attempted to be installed using SMB.

The kill-chain is as detailed below:

Threat actors discover SMB shares exposed to the internet, beaconed by multiple Keygens and KMSAuto being used by customers

Threat actors then bruteforce themselves into the enterprise's network

Network settings are change for installing the RDPWrap application for better remote access

Firewall is turned off, and threat actors reassign the server's port numbers

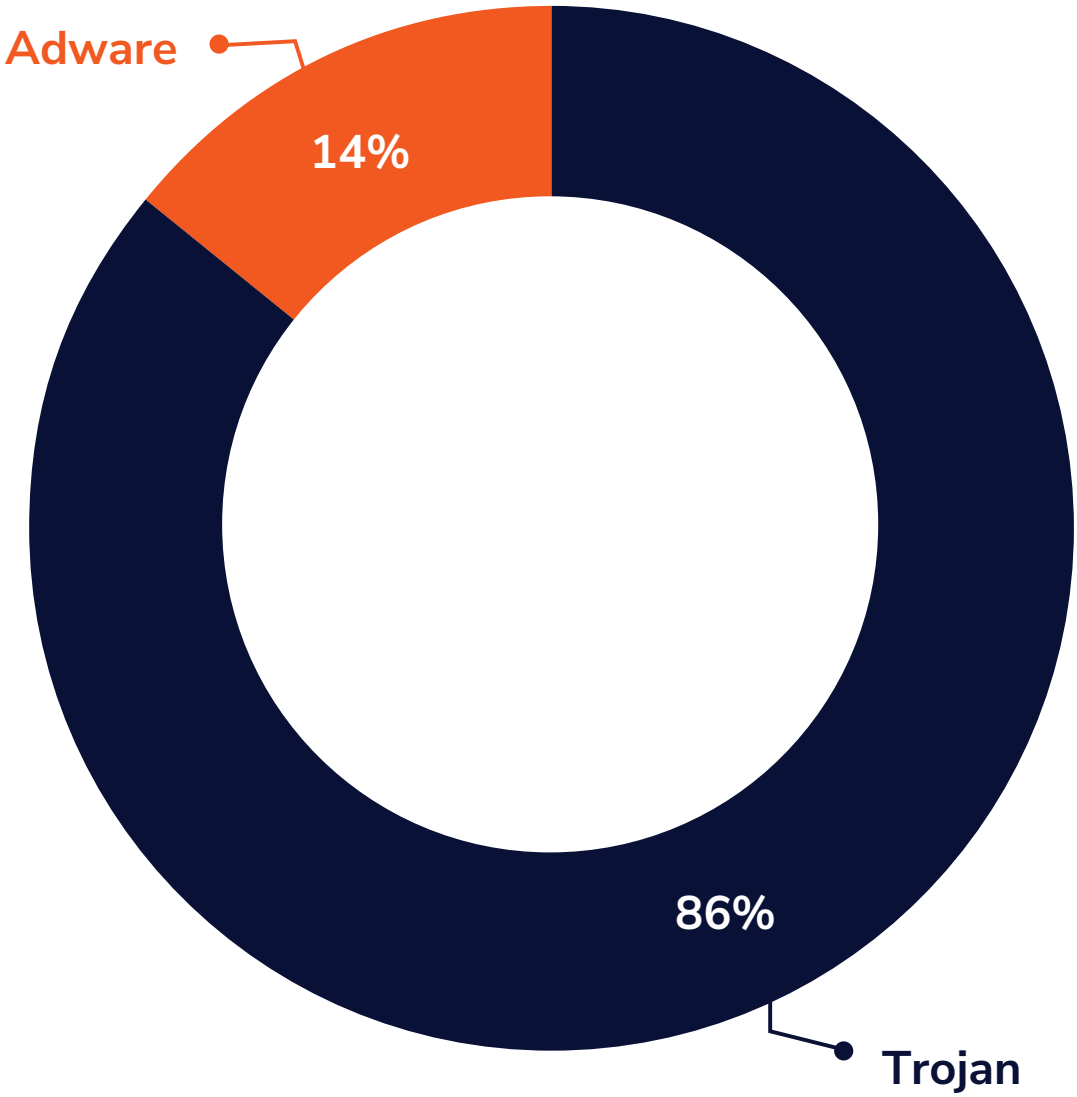
The PAExcel tool is then used to remotely create a service, which in turn downloads the Purplefox malware

Back To Contents

THE MOBILE DEVICE STORY

For CXOs, C-level leaders, and decision-makers within SMBs, the current Android threat landscape demands vigilant strategic oversight.

Adware vs Trojan Proportional Split

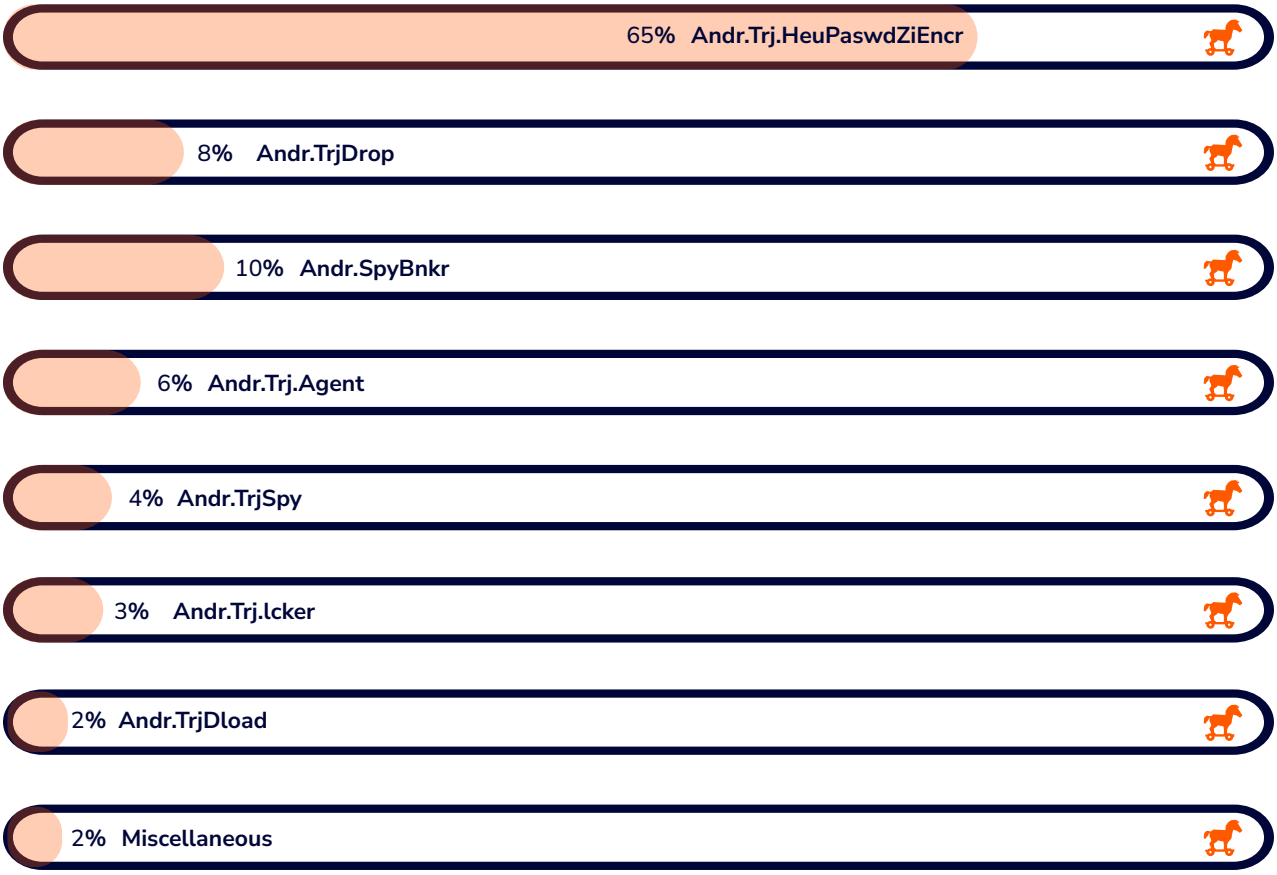


Trojans now account for 86% of detected threats, a clear indication that adversaries are favoring attack vectors capable of breaching both corporate and smaller business defenses to access critical data. This surge in Trojan activity presents notable risks not only to large enterprise assets but also to the operational continuity and reputational health of SMBs, which often lack extensive security resources. By contrast, adware's footprint is only 14%, signaling more effective detection mechanisms or a calculated shift by attackers toward more lucrative payloads.

Back To Contents

THE OMNIPRESENT TROJAN

The Wicked Trendline of Trojans

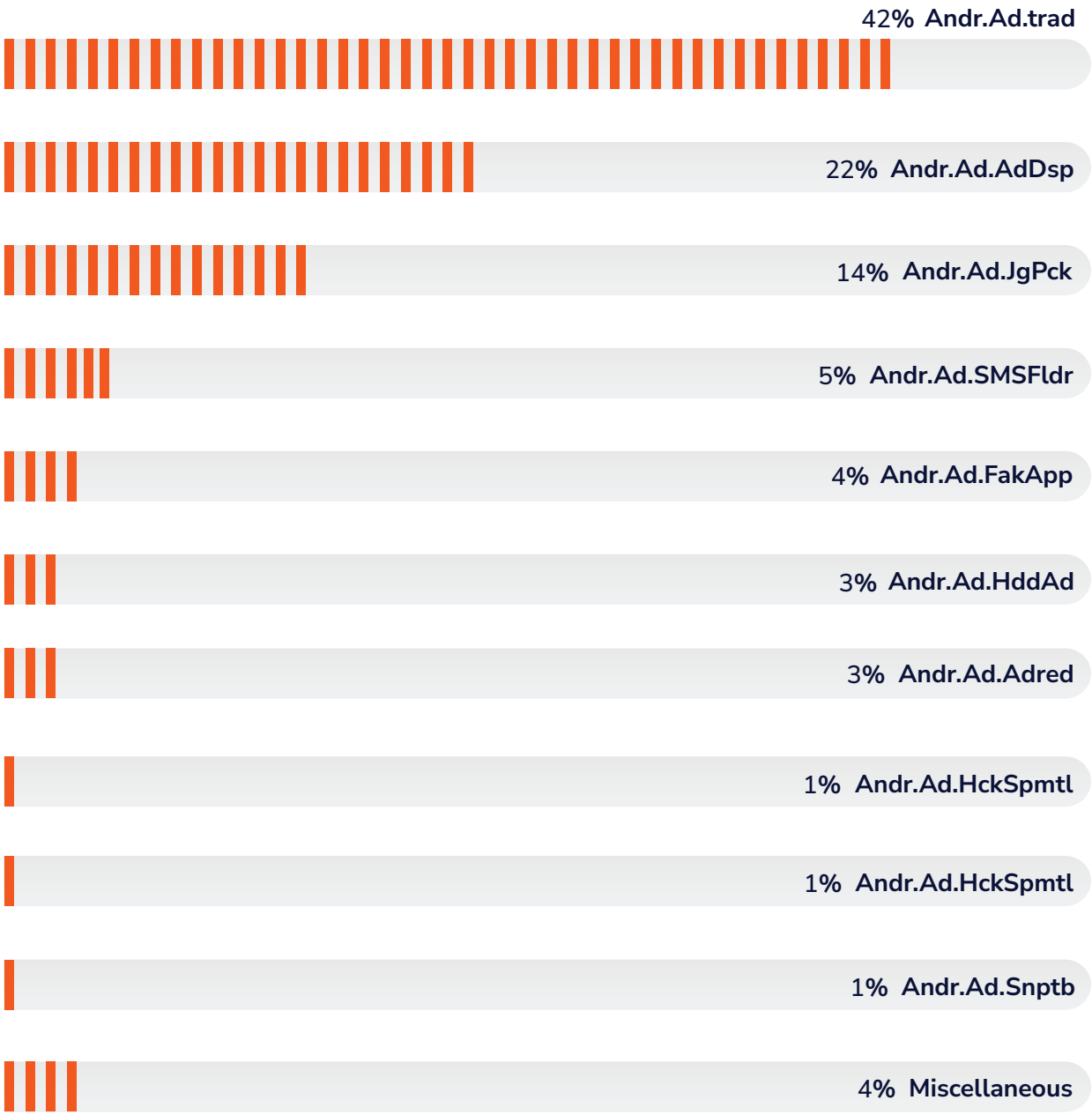


The Trojan ecosystem is dominated by specialized threats, each posing a distinct risk to corporate and personal data. Password-stealing Trojans, identified as Andr.Trj.HeuPaswdZiEncr accounts for a significant 65% of detections, making credential theft the primary attack vector. Banking spyware (Andr.SpyBnkr) follows at 10%, directly targeting financial information. Other notable families include Droppers (Andr.TrjDrop) at 8% and Agents (Andr.Trj.Agent) at 6%, which install further malware and create persistent backdoors. Spyware, Lockers, and Downloaders represent smaller but still critical threats. This distribution reveals a strategic shift toward multifaceted attacks that begin with compromising user credentials to enable deeper intrusions.

Back To Contents

THE ADWARE SAGA

Most Prevalent Adware Types



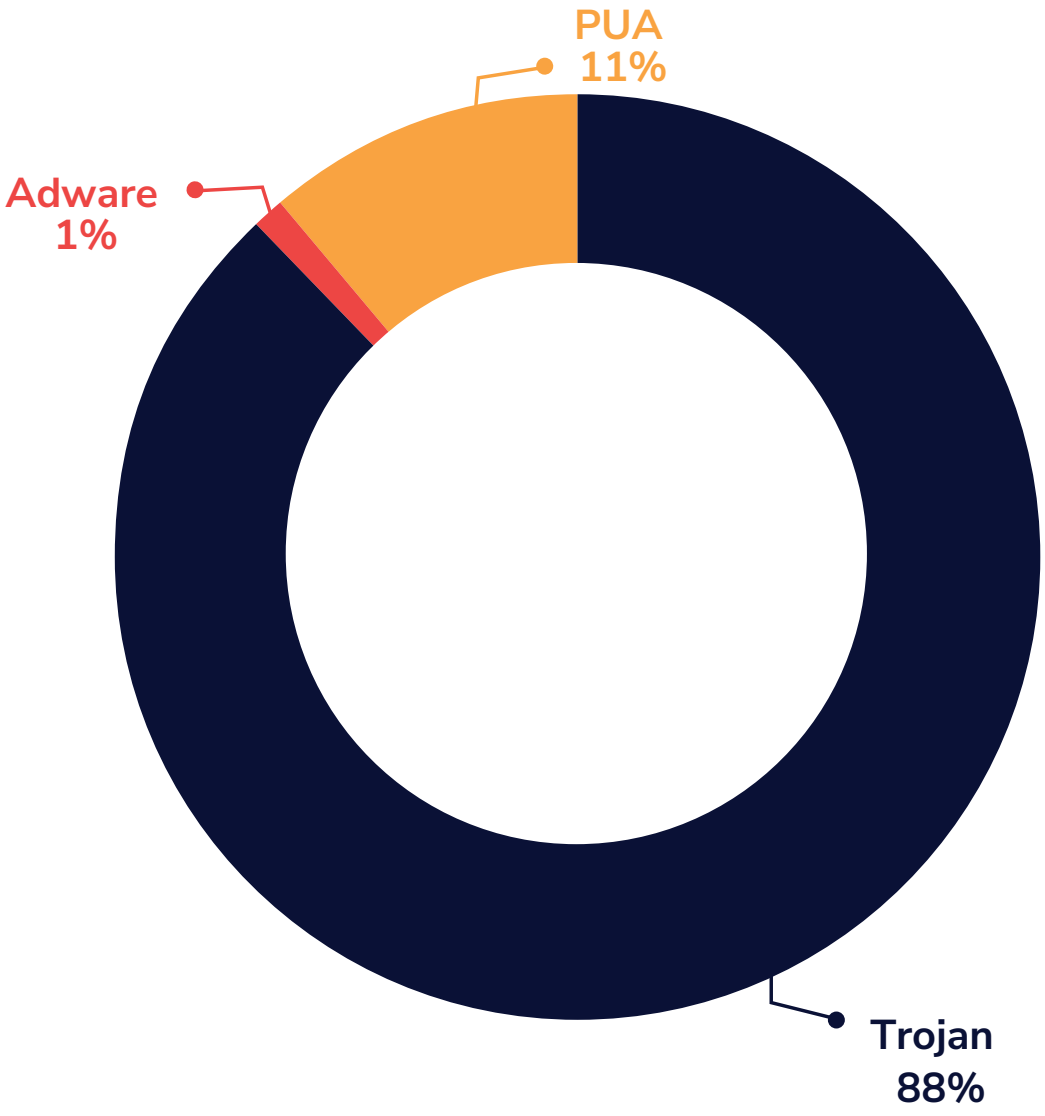
While Trojans represent the most severe threat, the adware landscape reveals its own set of risks that demand strategic attention. Traditional ad-displaying variants (Andr.Ad.trad) lead at 42%, but more concerning are the sophisticated families, such as Andr.Ad.AdDsp (22%) and Andr.Ad.JgPck (14%), which often employs deceptive tactics to serve aggressive or malicious ads. This breakdown illustrates that even lower-priority threats are evolving, using stealth and persistence to disrupt user experience and potentially serve as a gateway for more significant security breaches. Acknowledging these adware vectors is crucial for a comprehensive mobile security posture that protects brand reputation and operational integrity.

Back To Contents

THE MAC ATTACK

macOS, once seen as a stronghold of security, now faces a rapidly evolving threat landscape that demands vigilant oversight from organizations of all sizes, including both large enterprises and SMBs. Trojans dominate at 88% of all detected threats, reflecting a targeted shift by adversaries toward stealing credentials and compromising sensitive business data. Potentially Unwanted Applications (PUAs) have dropped sharply to 11%, while adware is nearly obsolete at just 1%, marking a notable departure from previous threat patterns.

Trojan, Adware and PUA Proportional Split



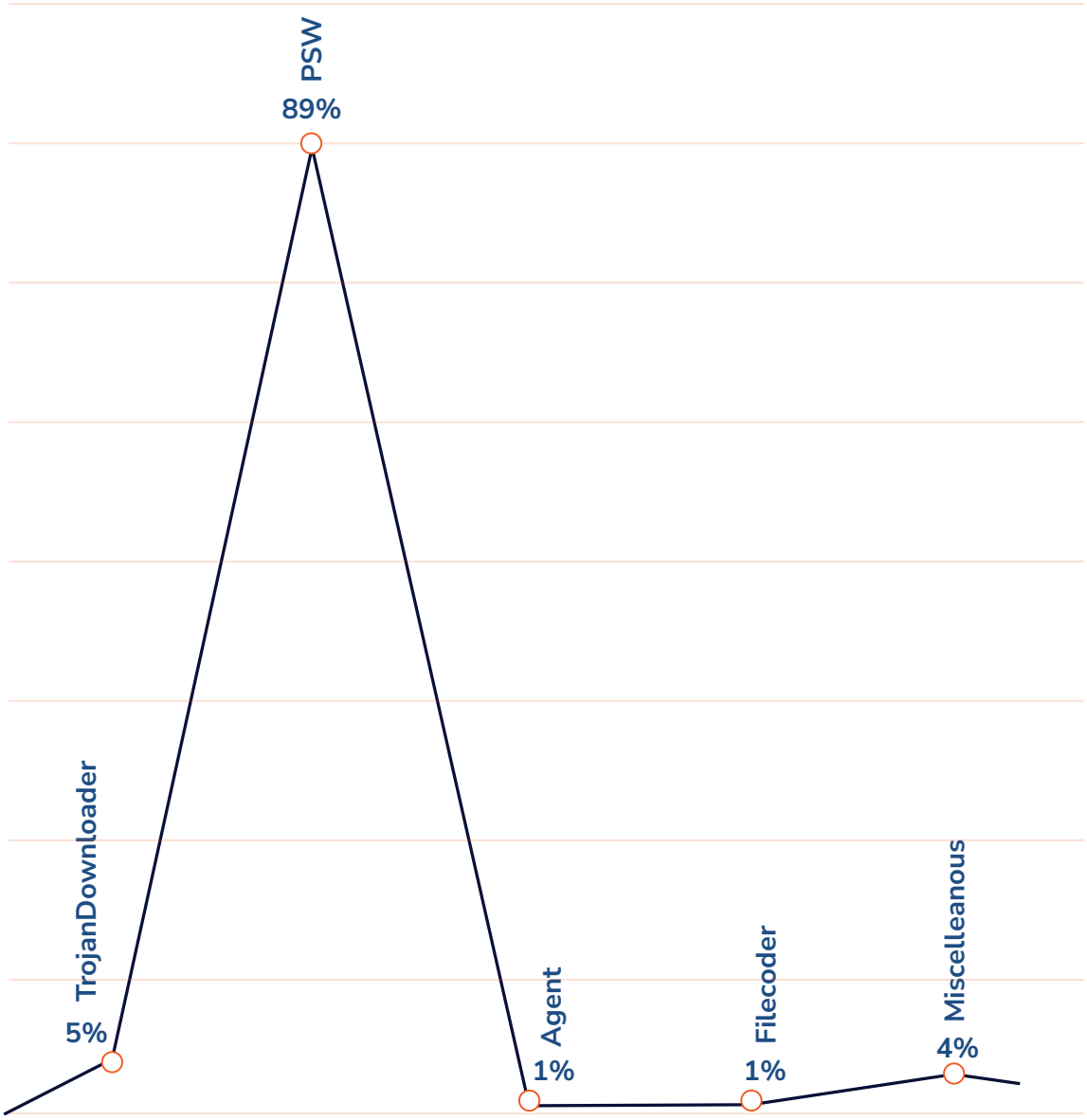
For CXOs, C-level leaders, and SMB decision-makers alike, these developments underscore the urgent need to review and strengthen security frameworks regardless of organizational scale. The landscape has moved beyond low-risk nuisances; sophisticated, Trojan-driven attacks now represent the primary threat to both corporate and SMB digital assets. Protecting your organization and its reputation demands proactive investment in robust detection, swift incident response, and ongoing user awareness initiatives to address the realities of modern macOS threats. This data signals a timely call to action: defending critical infrastructure and sensitive data requires vigilance, a clear strategy, and leadership commitment from the boardroom to the front lines of every business.

Back To Contents

THE PREVALENCE OF TROJANS

An analysis of Trojan variants targeting macOS reveals a striking focus on password-stealing malware (PSW), which accounts for 89% of all Trojan-related detections. This highlights a deliberate effort by attackers to obtain credentials, which are key access points to sensitive corporate and personal data.

Trojan Detection Trend Lines



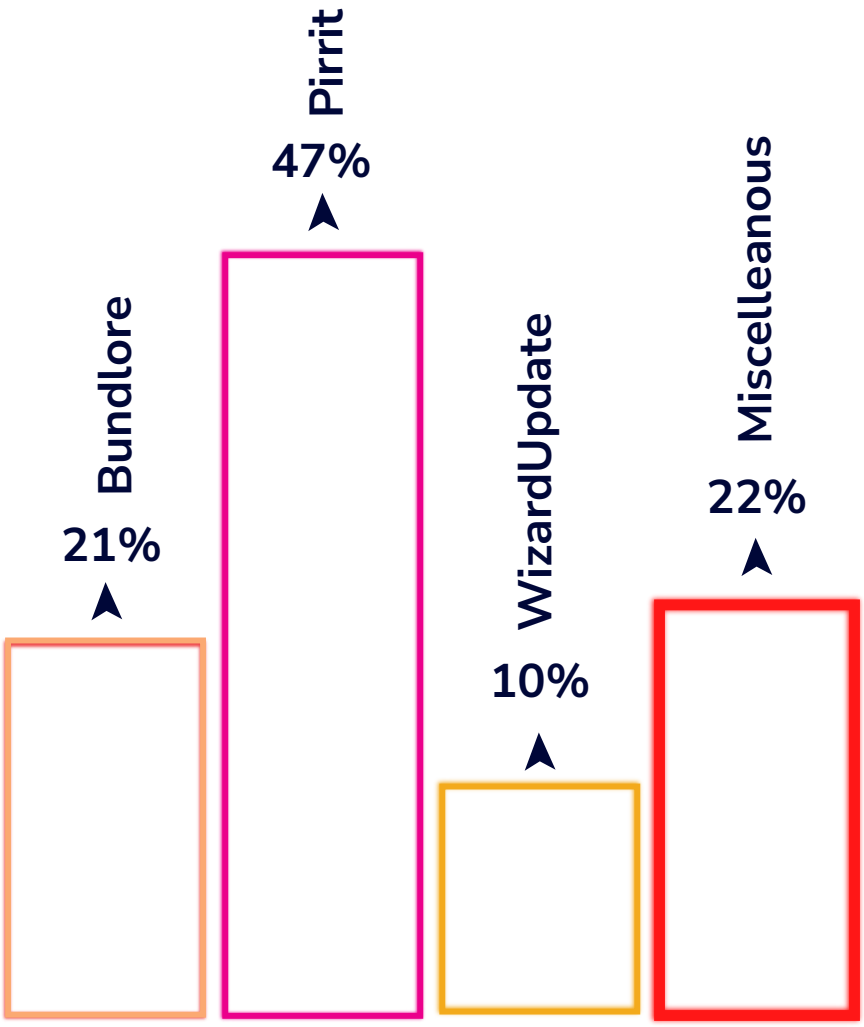
Other variants, such as TrojanDownloaders (5%), serve as delivery mechanisms for additional malware, creating ongoing risks within systems. Smaller segments, such as Agents and Filecoders (each at 1%), enable remote control and data encryption, posing a threat to operational continuity.

This distribution shows attackers prioritize credential theft as the primary entry point for deeper, more damaging network intrusions. For businesses, these findings underscore the importance of robust access controls and multi-factor authentication to mitigate this significant threat.

Back To Contents

THE ADWARE BROUHAHA

The Trendline of Adware Variant Detections

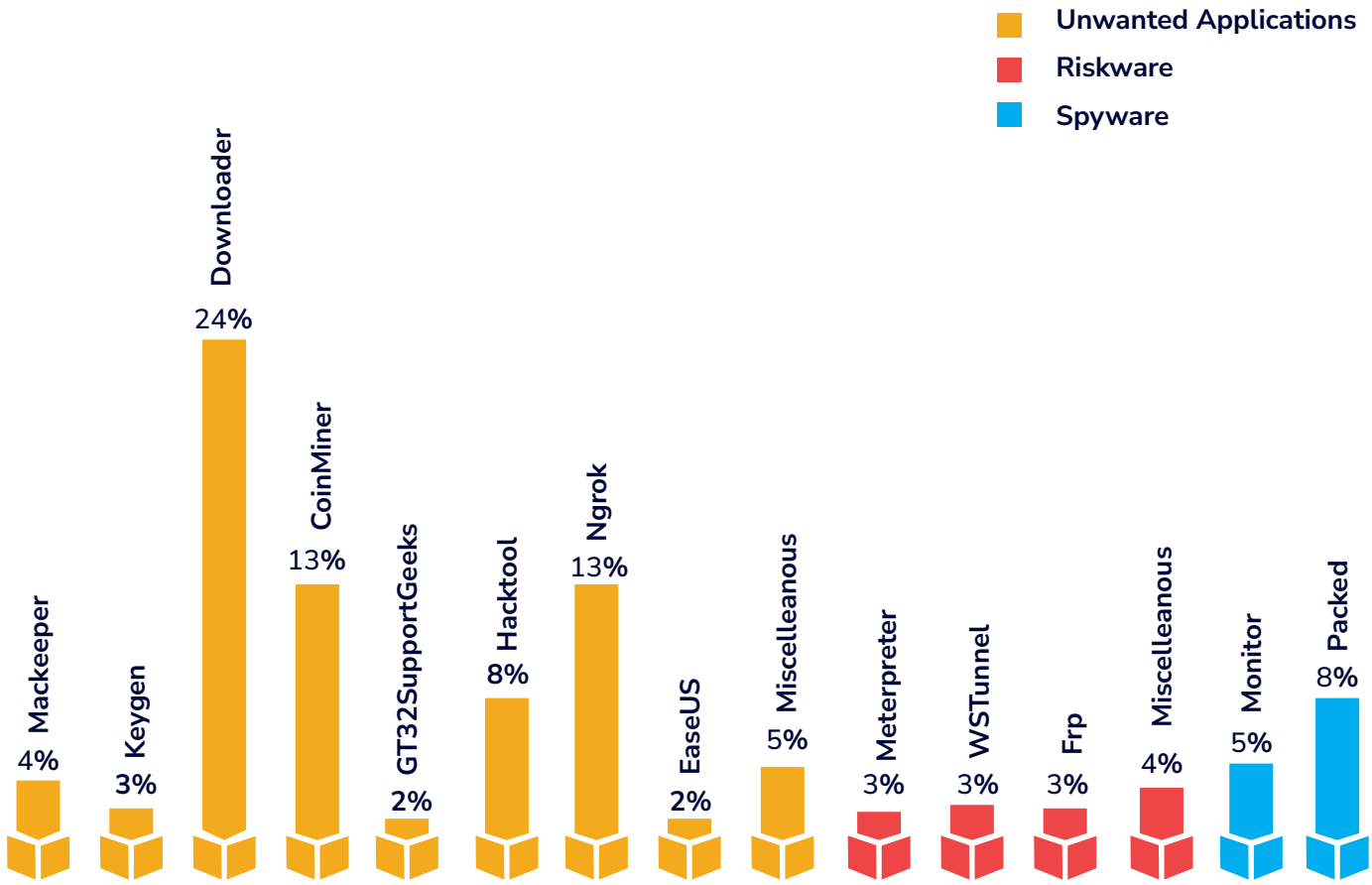


While Trojans represent the more severe macOS threats, the adware landscape presents persistent risks that business leaders should not underestimate. The Pirrit adware family is the most dominant, accounting for 47% of detections, known for its aggressive ad-injection capabilities that can disrupt user workflows and expose systems to further risks. Following this, Bundlore at 21% and WizardUpdate at 10% are also significant, often disguising themselves as legitimate software updates to gain entry. Although adware may seem like a low-level nuisance, its presence can degrade system performance and serve as an entry point for more malicious payloads, making it a relevant factor in your organization's overall security posture.

Back To Contents

THE SHARE OF PUPS

Most Prevalent PUP Types



While often overshadowed by Trojans, Potentially Unwanted Applications (PUAs) introduce significant backdoor risks that demand strategic oversight. Within this category, Downloaders are the most prevalent at 24%, acting as gateways for more malicious software. In comparison, CoinMiners and reverse-tunneling tools like Ngrok (both at 13%) directly siphon corporate resources and create hidden network access points. Furthermore, the presence of Riskware, such as Meterpreter, and Spyware, including Monitors and Packed executables, indicates that PUAs are often a precursor to active data exfiltration and corporate espionage, making their detection critical for protecting intellectual property and operational integrity.

Back To Contents

VULNERABILITIES GALORE

In today's landscape, a security vulnerability isn't just a misconfiguration or a missing patch; it's a live, ticking clock. When exploitation is active—when adversaries are already leveraging these weak points—the only metric that matters is speed.

This section doesn't simply catalog our system weaknesses. Instead of another lengthy technical breakdown, we present a strategic decision tool: a crisp, executive-level comparison matrix designed specifically to cut through the noise and accelerate our threat response. Think of it not as a spreadsheet, but as your immediate roadmap to defense.

16 SIGNIFICANT VULNERABILITIES OBSERVED BY K7 LABS IN Q2 2025-26

Aligning CVSS scores with specific threats, it empowers decision-makers to prioritize patching, allocate resources effectively, and strengthen their cybersecurity posture.

K7 THREAT LEVEL 1 [9.0-10.0]

Critical Infrastructure (Initial Access + Privilege Escalation)

CISCO ISE NETWORK INFRASTRUCTURE

CVE-2025-20281 | CVSS 10.0 | API Input Validation Faliure → Command Injection → Root RCE
CVE-2025-20337 | | CVSS 10.0 | Untrusted API Input → Unsanitized Code Execution → Root RCE
Impact: Unauthorized power granting total control, data theft, and system disruption
MITRE T1190: Exploit Public-Facing Application
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Emergency patches required

WING FTP SERVER

CVE-2025-47812 | CVSS 10.0 | Null Byte Truncation → Code Injection → RCE
Impact: Null byte injection bypasses security checks by truncating file paths prematurely
MITRE T1059: Command and Scripting Interpreter
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Upgrade required to version 7.4.4+

MICROSOFT SHAREPOINT

CVE-2025-53770 | CVSS 9.8 | Deserialization → RCE
Impact: Unauthenticated remote code execution, granting full SharePoint server compromise
MITRE T1055: Process Injection
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Immediately apply Microsoft security updates, rotate machine keys, and enable AMSI

Back To Contents

FORTINET FORTIWEB SECURITY APPLIANCE

CVE-2025-25257 | CVSS 9.8 | SQL injection → Database breach
Impact: Unauthenticated SQL injection allows execution of queries and compromise
MITRE T1190: Exploit Public-Facing Application
MITRE T1552: Unsecured Credentials
ACTION: Patch the system and change database credentials

TREND MICRO APEX ONE SECURITY CONSOLE

CVE-2025-54948 | CVSS 9.8 | Improper Neutralization of Special Elements → Compromise
Impact: Allows total compromise of the security management server
MITRE T1059: Command and Scripting Interpreter
MITRE T1068: Exploitation for Privilege Escalation
ACTION: Apply critical vendor patches and restrict public network access to the console

CRUSHFTP FILE TRANSFER

CVE-2025-54309 | CVSS 9.8 | AS2 validation → Admin access
Impact: AS2 flaw enables remote, unauthenticated attackers to gain full administrative control
MITRE T1190: Exploit Public-Facing Application
MITRE T1078: Valid Accounts
ACTION: Upgrade CrushFTP to the latest patched version and enable DMZ

CITRIX NETSCALER VPN/ADC

CVE-2025-7775 | CVSS 9.2 | Memory overflow → RCE/DoS
Impact: Unauthenticated RCE or Denial of Service on critical Citrix network gateway appliances
MITRE T1190: Exploit Public-Facing Application
MITRE T1068: Privilege Escalation
ACTION: Apply vendor patch and disable unnecessary IPv6 services

K7 THREAT LEVEL 2 [7.0-8.9]

Enterprise Systems (Execution + Defense Evasion)

APPLE IMAGEIO FRAMEWORK

CVE-2025-43300 | CVSS 8.8 | Buffer overflow → Memory corruption
Impact: Buffer overflow corrupts memory, potentially leading to arbitrary code execution
MITRE T1566: Phishing (Malicious Images)
MITRE T1203: Arbitrary Code Execution
ACTION: Apply vendor security patches to prevent memory access

MICROSOFT SHAREPOINT

CVE-2025-49704 | CVSS 8.8 | Code generation → Arbitrary execution
Impact: Allows authorized attackers remote code execution
MITRE T1055: Process Injection
MITRE T1068: Privilege Escalation
ACTION: Apply security updates, rotate machine keys, and enable AMSI/antivirus protection

Back To Contents

GOOGLE CHROME BROWSER

CVE-2025-6558 | CVSS 8.8 | Input validation → Sandbox escape
Impact: Input flaw allows sandbox escape, potentially granting full system access
MITRE T1203: Arbitrary Code Execution
MITRE T1211: Defense Evasion
ACTION: Apply the vendor patch and disable unnecessary features for defense

CVE-2025-6554 | CVSS 8.1 | Type confusion → Memory manipulation
Impact: Type confusion enables memory manipulation, leading to arbitrary code execution
MITRE T1203: Arbitrary Code Execution
MITRE T1055: Process Injection
ACTION: Apply vendor security patch to prevent memory corruption

WINRAR ARCHIVE TOOL

CVE-2025-8088 | CVSS 8.4 | Path traversal → Code execution
Impact: Path traversal enables arbitrary file manipulation, leading to code execution
MITRE T1566: Phishing (Malicious Archives)
MITRE T1027: Obfuscated Files or Information
ACTION: Immediately patch input sanitization to block directory traversal attempts

GIT VERSION CONTROL

CVE-2025-48384 | CVSS 8.0 | Arbitrary File Write → RCE
Impact: CRLF flaw allows file manipulation, enabling data tampering and injection
MITRE T1195.001: Compromise Software Dependencies and Development Tools
MITRE T1005: Data from Local System
ACTION: Immediately validate and sanitize all input to prevent CR/LF injection

CITRIX NETSCALER VPN/ADC

CVE-2025-5777 | CVSS 7.5 | Memory over-read → Data exposure
Impact: Exposes session tokens and user credentials from memory, enabling VPN hijacking
MITRE T1005: Data from Local System
MITRE T1552: Unsecured Credentials
ACTION: Patch the NetScaler appliance, then terminate all active sessions

K7 THREAT LEVEL 3 [4.0-6.9]

MICROSOFT SHAREPOINT

CVE-2025-49706 | CVSS 6.5 | Authentication bypass → Unauthorized Access
Impact: Enables network spoofing, granting unauthorized access, often chained with RCE
MITRE T1078: Valid Accounts
MITRE T1550: Use Alternate Authentication
ACTION: Immediately apply security patches and rotate keys

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.

An Android App could reroute calls to Attackers

A malware targeting Indian banking users, has the capability to forward their calls to threat actors and do their malicious activities.

Refer Spybanker for details

Cmimai – A Silent Stealer

This talks about Cmimai, a stealer Trojan that quietly gathers system info and browser data along with periodical screenshots; and then sending it to Discord.

For more details refer Silently Dangerous

BQTLock - Encrypting data using double-extortion mode

BQTLock, a Ransomware-as-a-Service (RaaS) is marketed on the dark web and social platforms like X and Telegram and encrypting files and demanding ransoms in Monero (XMR), operating under a double-extortion mode.

Refer BQTLock for more info

Deploying RAT through LNK Files

A simple deceptive .lnk hides a powerful Remote Access Trojan (RAT) — allowing attackers to steal data, execute remote commands, share screenshots and act as per the attacker commands while being persistent via win login entry.

Refer LNKTrojan for more info

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

Back To Contents

CYBER THREATS EXECUTIVE BRIEFING: Q2 2025-26

1. Executive Summary

This briefing outlines key findings from the Q2 2025-26 Cyber Threat Report. Cyberattacks are evolving into persistent threats, driven by advanced state-sponsored groups and professional cybercriminals. The growing issue of "vulnerability debt," unaddressed software weaknesses, poses a significant risk to operations and financial stability across the global threat landscape. Adversaries are exploiting these flaws to target intellectual property and disrupt supply chains. Immediate action is required to strengthen our defenses and reduce these risks.

2. Background

The current threat landscape features coordinated attacks targeting specific industries, exploiting both legacy and new vulnerabilities to maximize impact. High-profile incidents like the Jaguar Land Rover supply chain attack and the DaVita healthcare breach demonstrate that no sector is immune. This briefing translates broad threat data into actionable risks for our organization, enabling informed decision-making.

3. Key Findings

Targeted Attacks by Industry: Industries such as IT/ITES (28%) and Manufacturing (21%) are primary targets due to their critical roles in the supply chain and valuable intellectual property. Healthcare and Government also face consistent attacks. Even Finance (4%), with lower attack volumes, experiences sophisticated intrusions designed to evade standard defenses.

Exploitation of Old Vulnerabilities: Widespread use of outdated vulnerabilities, such as MS17-010 (76% of related incidents), highlights systemic issues in patch management. This "vulnerability debt" is the most significant risk for network breaches and ransomware attacks.

Platform-Specific Threats:

- Windows: Remains the most targeted platform for enterprise attacks, focusing on credential theft and lateral movement.
- Android & macOS: Increasingly targeted with sophisticated Trojans (86% of Android threats, 88% of macOS threats) aimed at stealing credentials and compromising corporate data.
- Global Risk Variance: Certain regions face a higher threat level than others. Countries like Pakistan (33% infection rate) and Japan (30%) are disproportionately affected compared to the UK (10%) and the US (18%). This disparity directly impacts global operations and third-party risk management.

4. Business Implications

The findings present clear risks to our business:

Operational Disruption: Attacks on supply chains or Manufacturing can lead to production downtime, revenue loss, and reputational damage.

Financial and Legal Exposure: Ignoring "vulnerability debt" increases the risk of costly ransomware incidents, regulatory fines, and lawsuits.

Loss of Competitive Advantage: The theft of intellectual property, such as proprietary designs or strategies, can harm our market position.

5. Recommendations

To address these risks, we recommend the following actions:

- Prioritize Vulnerability Management: Implement a rigorous, time-bound patch management program. Treat critical patches with the same urgency as financial system outages to eliminate legacy "vulnerability debt."
- Strengthen Access Controls: Enforce multi-factor authentication (MFA) across all critical systems, especially for remote access and privileged accounts, to prevent credential theft.
- Invest in Advanced Detection: Deploy security solutions that focus on behavioral analysis rather than traditional signature-based tools to improve detection of modern, fileless attacks.
- Reassess Third-Party Risk: Evaluate the security posture of key partners and suppliers, particularly in high-risk regions, to mitigate supply chain vulnerabilities.

6. Conclusion

The evolving cyber threat landscape presents a strategic challenge that demands executive attention. By prioritizing cybersecurity as a core business function and implementing the recommendations above, we can safeguard our assets, enhance resilience, and protect our competitive edge.

Back To Contents

K7 SECURITY

Copyright © 2025 K7 Computing Private Limited, 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 authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners. Email us at k7viruslab@labs.k7computing.com.

www.k7computing.com