CYBER THREAT MONITOR REPORT

Q4_2024-25

LEVERAGING THREAT INTELLIGENCE INDICATORS TO PROACTIVELY FIGHT AGAINST CYBER THREATS

SECURING THE UNSECURED

With growing digitization, threats have simultaneously grown, albeit with a higher velocity. This is primarily attributed to a lack of education and cybersecurity awareness. Those in remote locations are not even computer literate, and now they are required to be tech-savvy in using high-end mobile phones, with all their banking accounts set to one-click access. They have access to download any software/utility from so-called secure interfaces, with no concern or belief that their phone could have been hacked or could be used for malicious activity. This is because not even educated people - be it different generations or even cybersecurity professionals are unable to identify clearly if their phone or system has been compromised. This is because the world is not savvy enough to compete with the evergrowing threat industry launching sophisticated and silent attacks.

Organizations should start investing heavily in creating a team of cybersecurity professionals with expertise in their own skill sets and using cutting-edge technology to counter cyber threats that are growing in sophistication as the world is fully moving towards relying on AI instead of human intelligence. They should also invest in a team of highly skilled professionals who need to rely solely on human intelligence to find exploitation possibilities similar to the cyber-savvy team and also to find any loopholes that may not be detected by the technological team and keep refining their test cases similar to generative AI. Moreover, the testing should be done on both hardware and software.

Amidst evolving challenges, cybersecurity has transcended traditional boundaries, encompassing individuals and organizations of all sizes. As digital transformation permeates life, the responsibility to safeguard data and systems has expanded. The increasing reliance on AI and automation emphasizes the need for a comprehensive approach integrating cutting-edge technology with human expertise. Organizations must recognize cybersecurity as an ongoing, adaptable process requiring a visionary technological framework and a vigilant human perspective. Cultivating awareness, investing in skilled professionals, and implementing robust testing protocols ensures asset protection and proactive positioning in the ever-evolving cyber threat landscape.

Back To Contents

INFECTION RATE (IR)

Those new to our quarterly report need to understand an important concept called "Infection Rate" (IR), which is used to benchmark 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 picture below better explains the concept of infection rate.

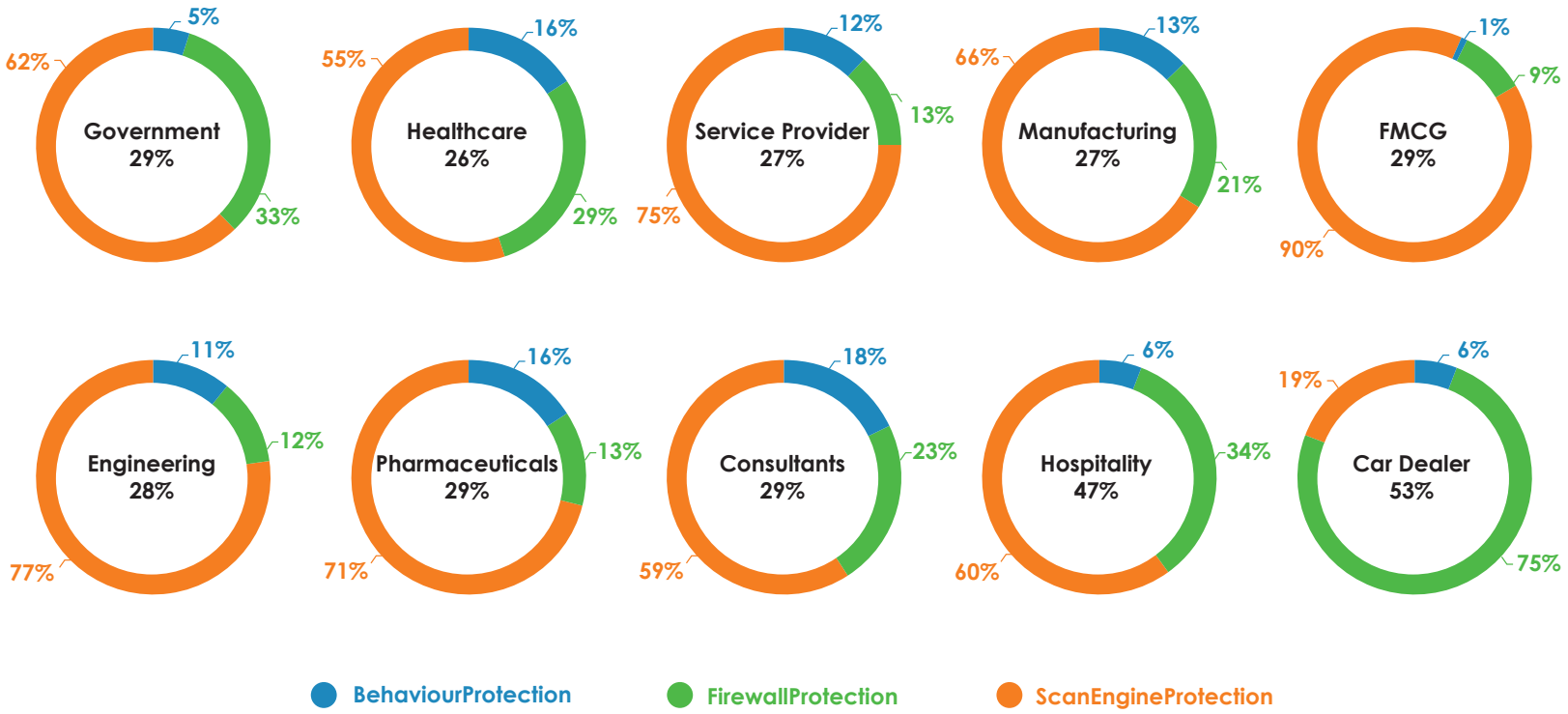
Infection Rate (IR) of an area

The Global Infection Rate (IR) for Q4_2024-25 was 26%.

A Granular View of The Industry Threat Landscape

The chart clearly demonstrates how threat actors strategically target industries perceived as more vulnerable or easier to exploit. Sectors such as hospitality and car dealerships, which may not involve extensive computer networks or SOC or CISO personnel, still appear prominently at the top of the list due to the lucrative nature of their operations. This pattern suggests that while the technology infrastructure may be limited, these industries present attractive financial opportunities. Notably, the sectors under threat tend to fluctuate quarter by quarter. In the previous quarter, industries such as FMCG, Manufacturing, and Healthcare remained more susceptible to attacks, while the Government remained the primary target. Conversely, this quarter, Pharmaceuticals and Engineering (which is often closely associated with Manufacturing and utilizes a significant number of IoT devices) has encountered a notable share of threats. This indicates that industries with critical infrastructure or valuable data continue to attract attackers. As these sectors enhance their defenses, threat actors may redirect their focus to other sectors. This evolving pattern emphasizes that no sector is entirely immune to cyber threats, and organizations must remain vigilant, as any industry could potentially become the next target in the dynamic cybersecurity landscape.

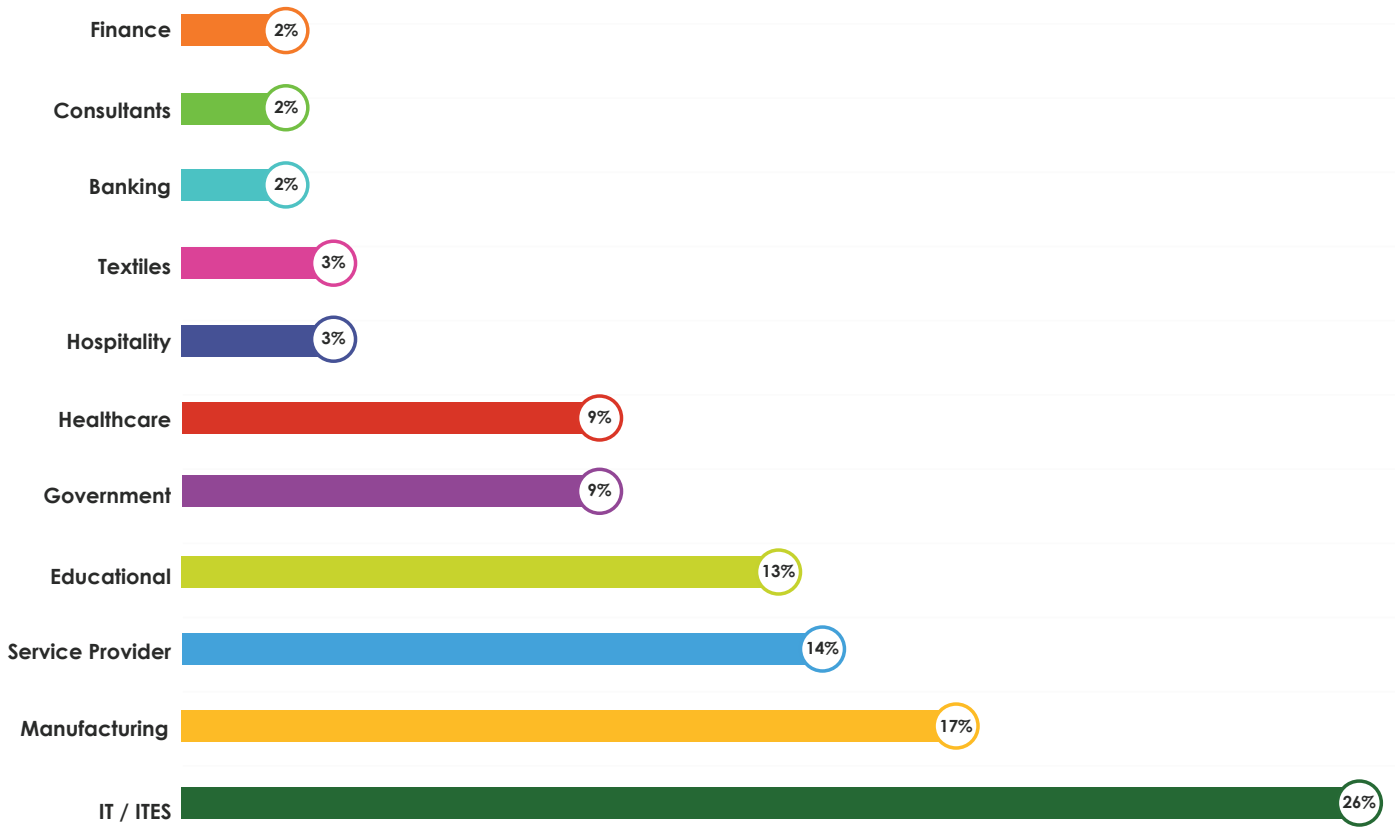
Top 10 Most Targeted Industries



VULNERABILITIES: A GLOBAL AND DOMESTIC PERSPECTIVE ON EMERGING THREATS

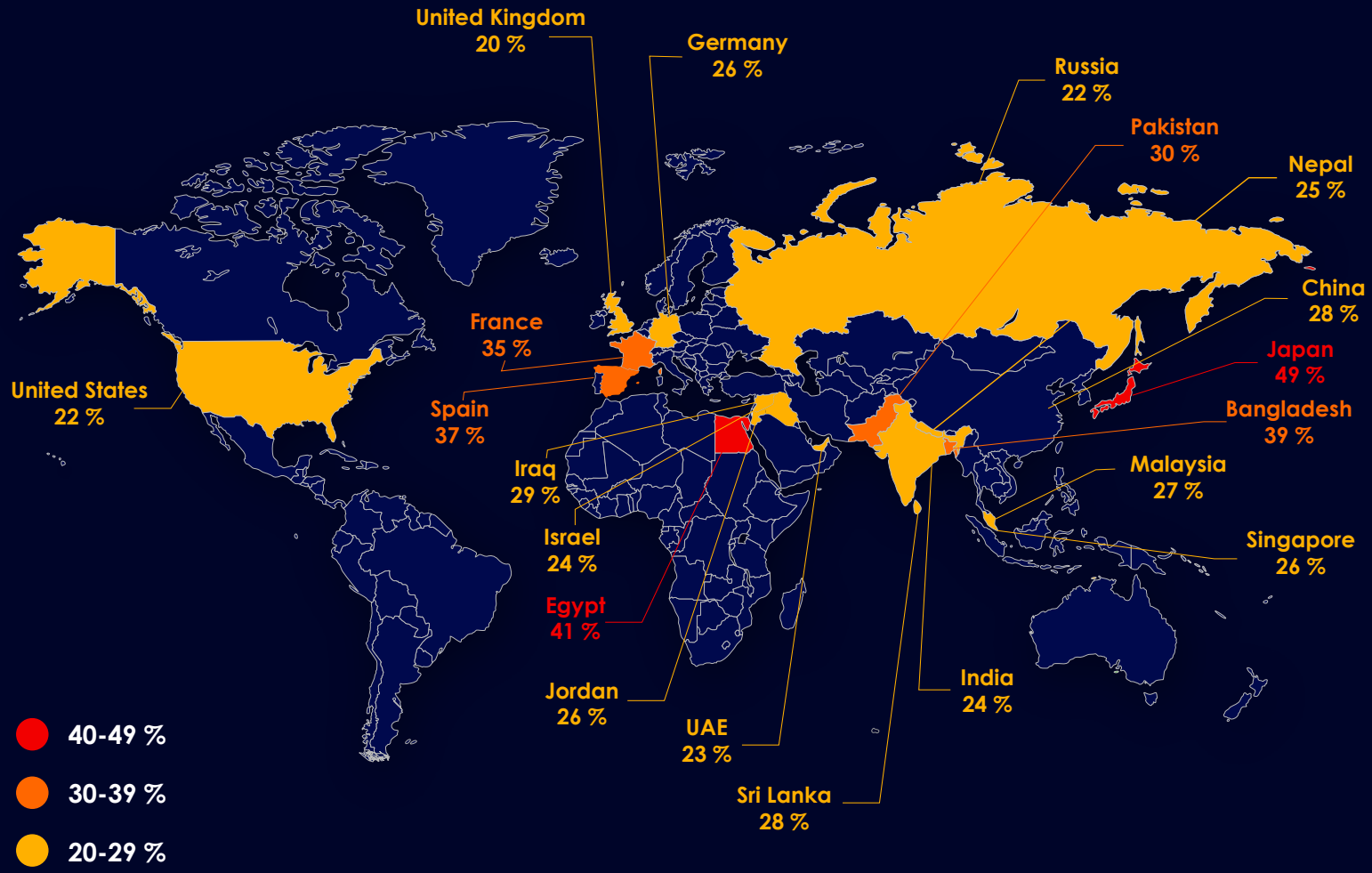
The IT/ITES industry continues to dominate as the most vulnerable sector, accounting for 26% of all cyber threats. This vulnerability stems from its heavy reliance on interconnected systems and the vast amount of sensitive data it handles. As digital transformation accelerates, these industries are increasingly targeted by cybercriminals exploiting weaknesses in software, hardware, and supply chains. Manufacturing, the second most vulnerable industry, faces 17% of cyberattacks, with disruptions to production lines and supply chains posing significant risks.
Service providers, responsible for managing critical client data and services, follow closely at 14%, while the education sector accounts for 13% of attacks. With more schools and universities shifting to online platforms, their systems become prime targets for data theft. Other industries such as government (9%), healthcare (9%), hospitality (3%), textiles (3%), banking (2%), consultants (2%), and finance (2%) also experience significant threats, but at lower percentages. The latest statistics underscore the need for heightened security measures, particularly within IT/ITES, which remains at the forefront of cyber vulnerabilities.

Vulnerability Impact grouped by Industry



Worldwide Cyber Threat Landscape

The global infection rate chart serves as a compelling indicator of the evolving cyber threat landscape, shaped by a confluence of cyber strategies and geopolitical dynamics. The data presents a revealing and somewhat unsettling portrayal of the countries most susceptible to cyber threats, providing subtle insights into the roles of threat actors and opposing nations. For instance, Japan, Egypt, France, and Spain exhibit heightened vulnerability, likely attributable to a combination of economic significance, technological infrastructure, and geopolitical factors. Other countries with substantial infection rates, such as Bangladesh, China, Pakistan, Iraq, the United Arab Emirates, Jordan and Israel further underscore regional tensions and varying degrees of digital penetration. This chart not only emphasizes the escalating global threat but also suggests the intricate motivations driving these cyberattacks.



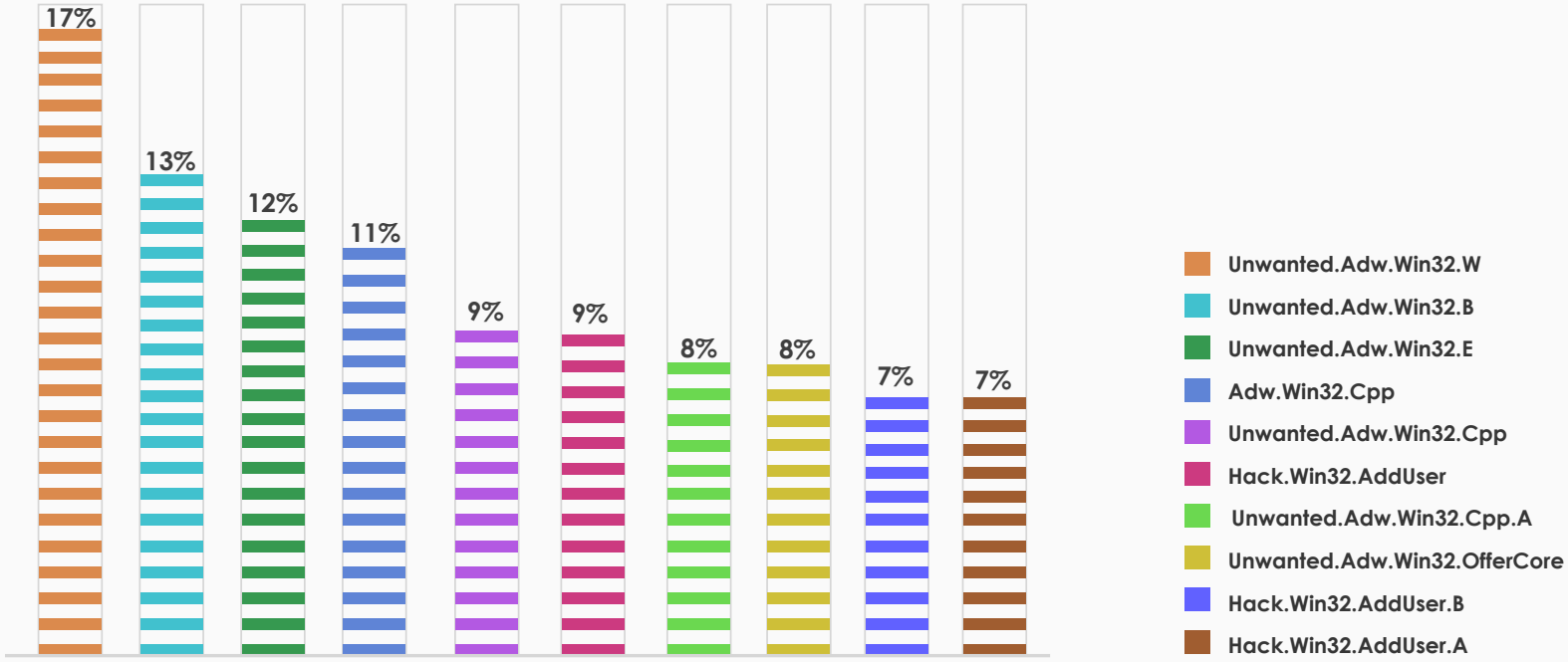
WINDOWS THREAT LANDSCAPE

Windows has long been the primary target for cybercriminals, primarily due to its widespread adoption and extensive attack surface. While there has been a recent increase in targeting of other platforms such as Linux, FreeBSD, SunOS, ESXi, and macOS; Windows remains the preferred choice for data extortion, ransomware, and malware execution. Its legacy systems, common misconfigurations, and vast user base consistently create vulnerabilities that attackers exploit through evolving reconnaissance techniques. Consequently, enterprises face a persistent challenge in balancing operational efficiency with escalating security risks.

Top Malware Targeting Windows Systems

A top-ten malware chart serves as a pivotal tool for comprehending the evolving dynamics of digital security threats. It provides a comprehensive overview of the most prevalent cyber risks, elucidating the emerging attack methodologies and vulnerabilities that organizations face. This chart not only illuminates the latest malware trends but also elucidates the tactics employed by cybercriminals to exploit vulnerabilities. By analyzing this chart, organizations can proactively identify potential threats, fortify their security posture, and prioritize defenses, thereby positioning themselves effectively in the increasingly intricate and adversarial cyber landscape.

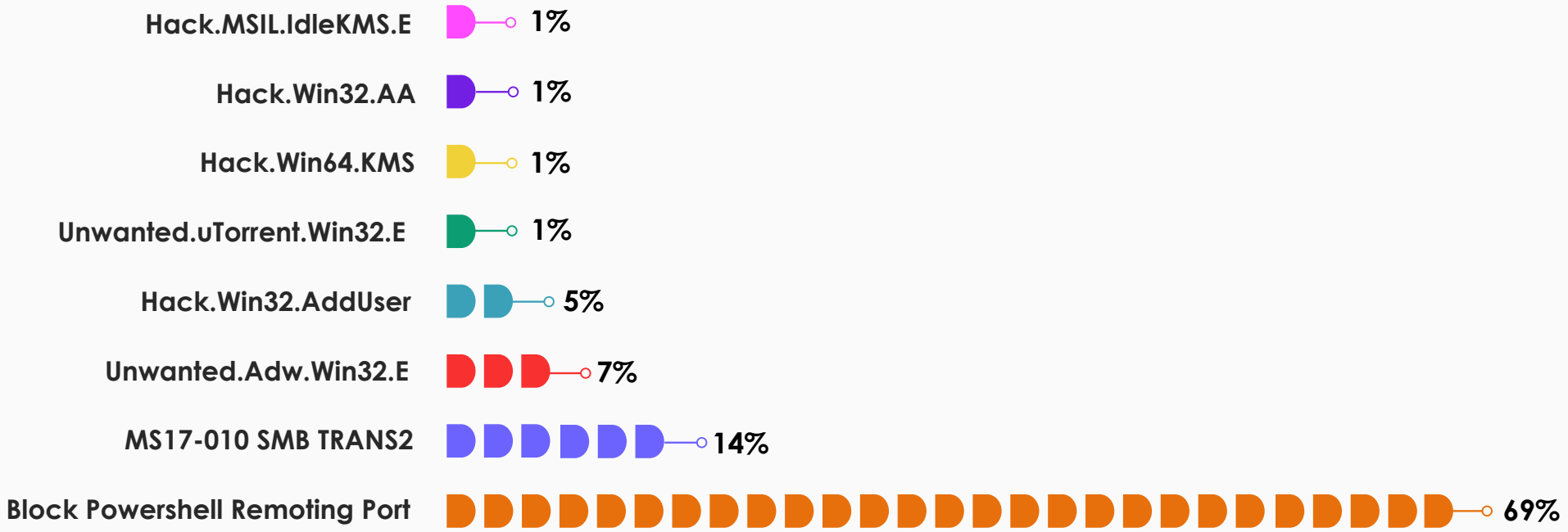
SPLIT OF WINDOWS TOP 10 DETECTIONS



Unpatched Vulnerabilities: The Achilles' Heel of Windows Systems

Every unpatched software, outdated system, and misconfigured setting presents an open invitation for cyber criminals. These vulnerabilities are not merely weaknesses; they are the most frequently exploited entry points in contemporary cyberattacks. When organizations disregard or postpone addressing these vulnerabilities, they are essentially risking their data, operations, and reputation. The consequence is ransomware attacks, data breaches, and costly disruptions that can have severe financial and reputational repercussions. As hackers continue to evolve in sophistication, the necessity for proactive vulnerability management has become imperative—it is no longer a matter of choice but a necessity for survival in an unforgiving digital environment.

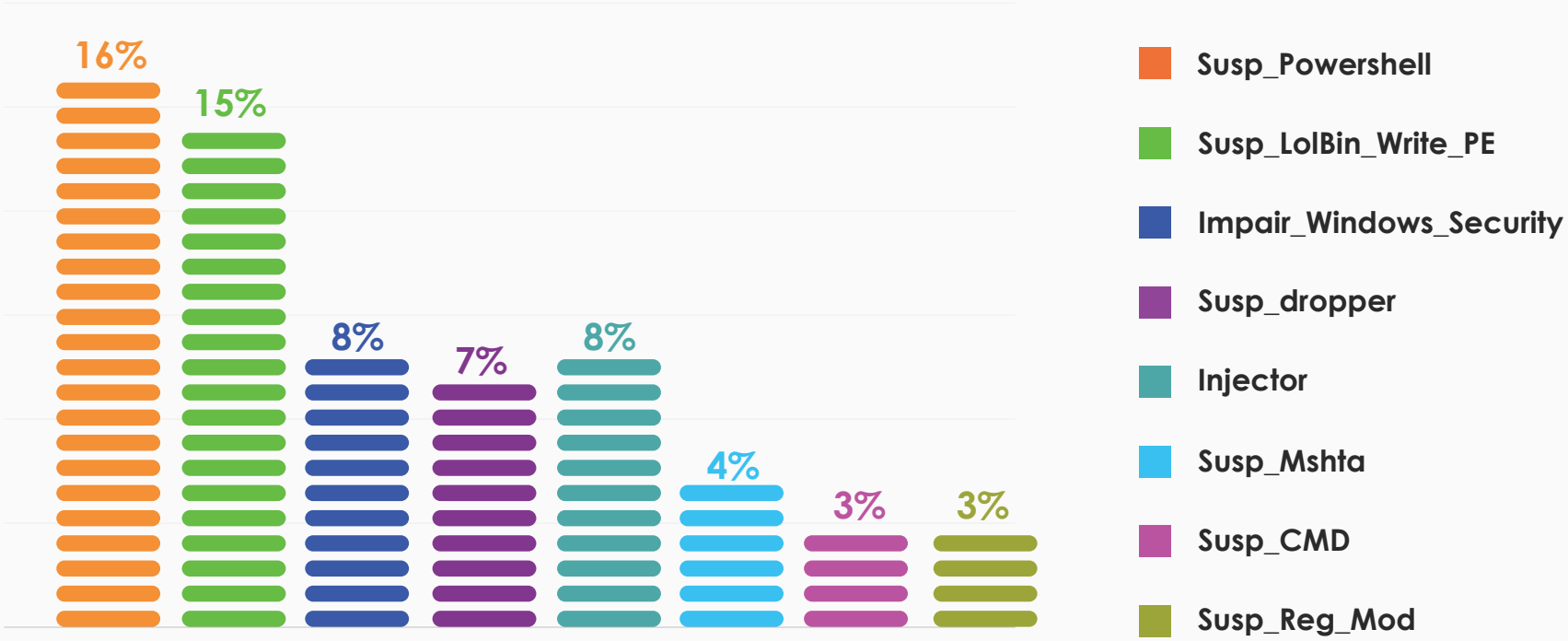
Most Prevalent Exploits



Heuristic Host Intrusion Prevention System (HIPS)

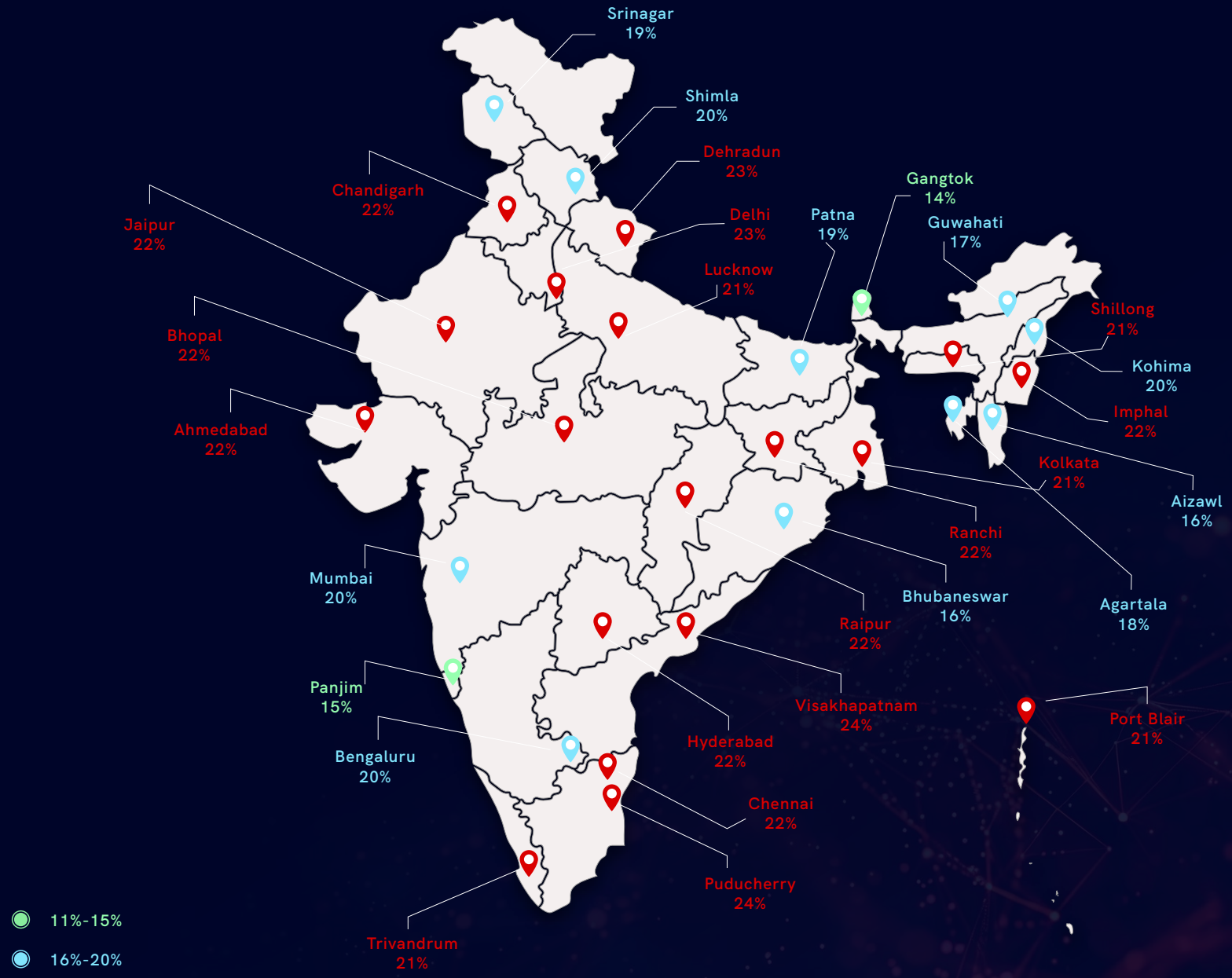
Heuristic behavioral detection provides fundamental security by identifying threats based on patterns and actions, rather than predetermined signatures. It's effective against zero-day exploits and rapidly evolving malware, as it detects novel threats in real-time. By prioritizing behavior over signatures, it offers a proactive defense against attackers' evolving tactics.

Windows Heuristic Behavioural Detection



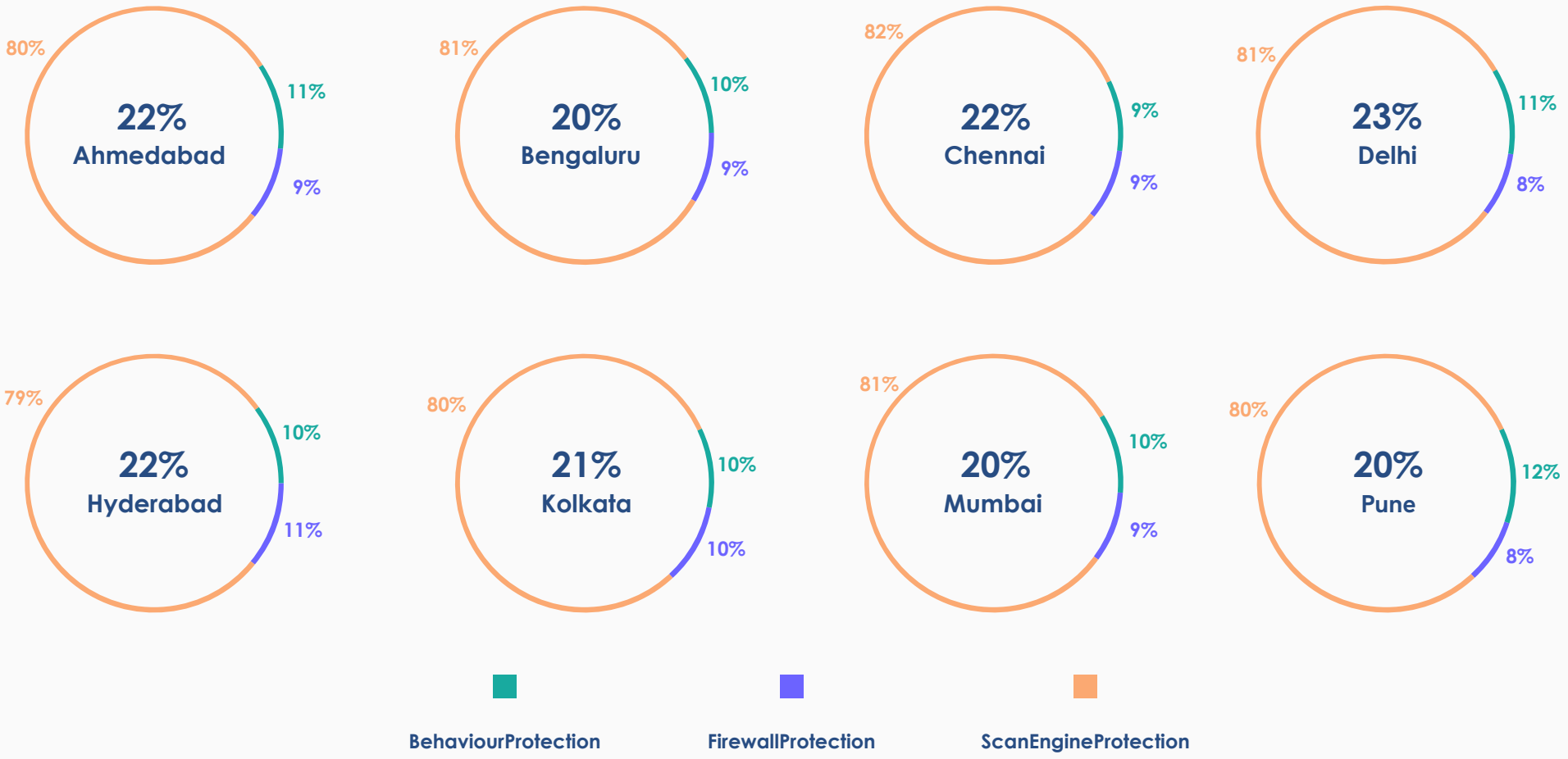
The rise of PowerShell and LOLBins in writing PE files, as evidenced by the two most prevalent strains in double figures, highlights a concerning trend in modern cyberattacks. These techniques allow attackers to execute malicious code undetected by traditional detection methods, leveraging legitimate system tools for discreet and efficient execution. This shift in tactics involves exploiting trusted system functionalities to bypass security measures and persist in compromised environments.

CYBER THREAT LANDSCAPE - INDIA



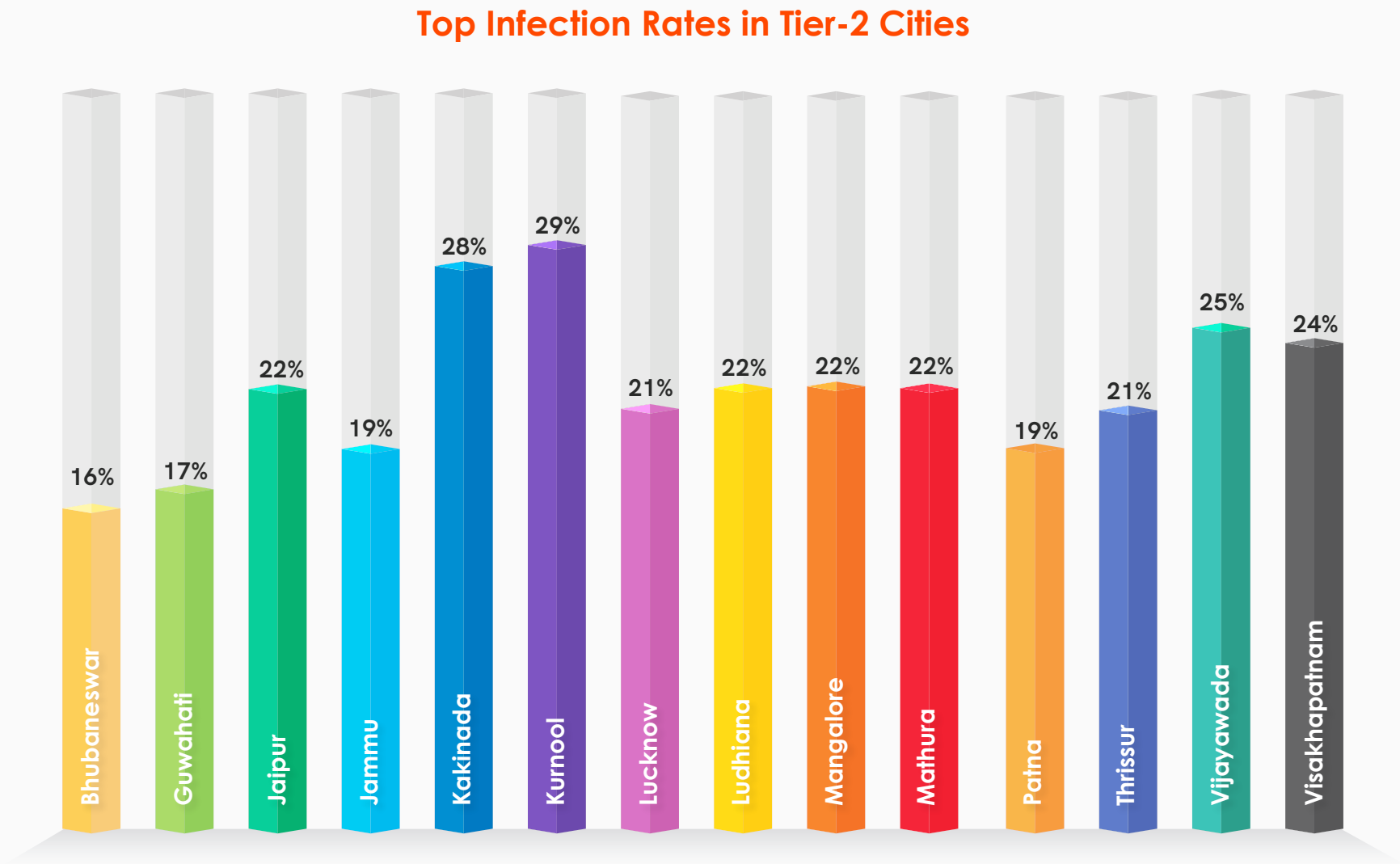
Map for illustrative purposes only. Not to scale.

THE METRO AND TIER-1 CITIES - INFECTION RATE



Top Infection Rates in Tier-2 Cities

Tier-2 cities have become a new focus for cybercriminals due to the affordability of smartphones and laptops, and the expanding digital accessibility. This combination of factors, along with residents' limited cybersecurity awareness, makes them vulnerable to online threats. They lack the knowledge to identify or defend against common cybercrimes.



ENTERPRISE INSECURITY

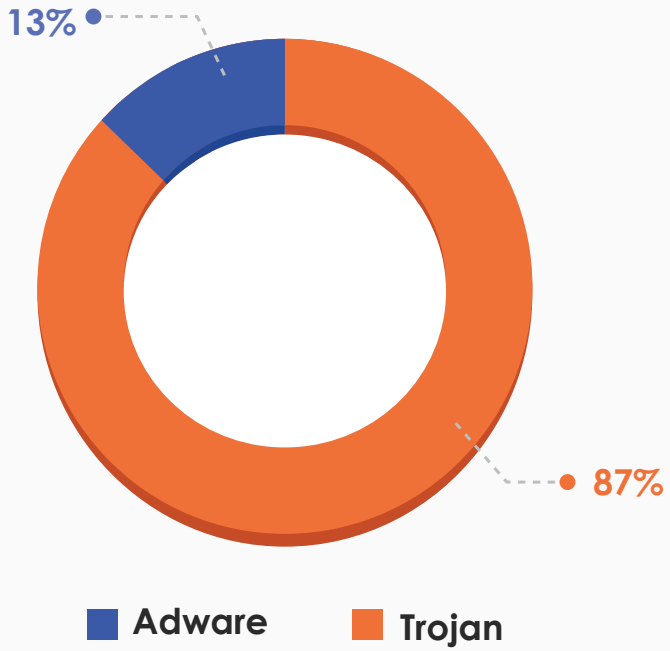
Ransomware strains from its original source have been doing the rounds for quite some time. Makop ransomware is one such ransomware having its base code from the Phobos ransomware, with payment requests in bitcoins.

Makop Wrath Unfolded

THE MOBILE DEVICE STORY

The Android threat landscape continues to evolve at an alarming pace, with a surge in novel and existing Trojan strains targeting users across diverse sectors. These Trojans have become increasingly sophisticated, employing diverse tactics to evade detection while relentlessly pursuing sensitive data. Unlike earlier variants, contemporary Trojans often transcend financial theft, focusing on a broad spectrum of privacy breaches, including credential theft and unauthorized data access. These advanced threats are designed to be persistent, adapting to user behavior and bypassing conventional security measures with ease.

Adware vs Trojan Proportional Split



Enterprise Risks in the Mobile Threat Landscape

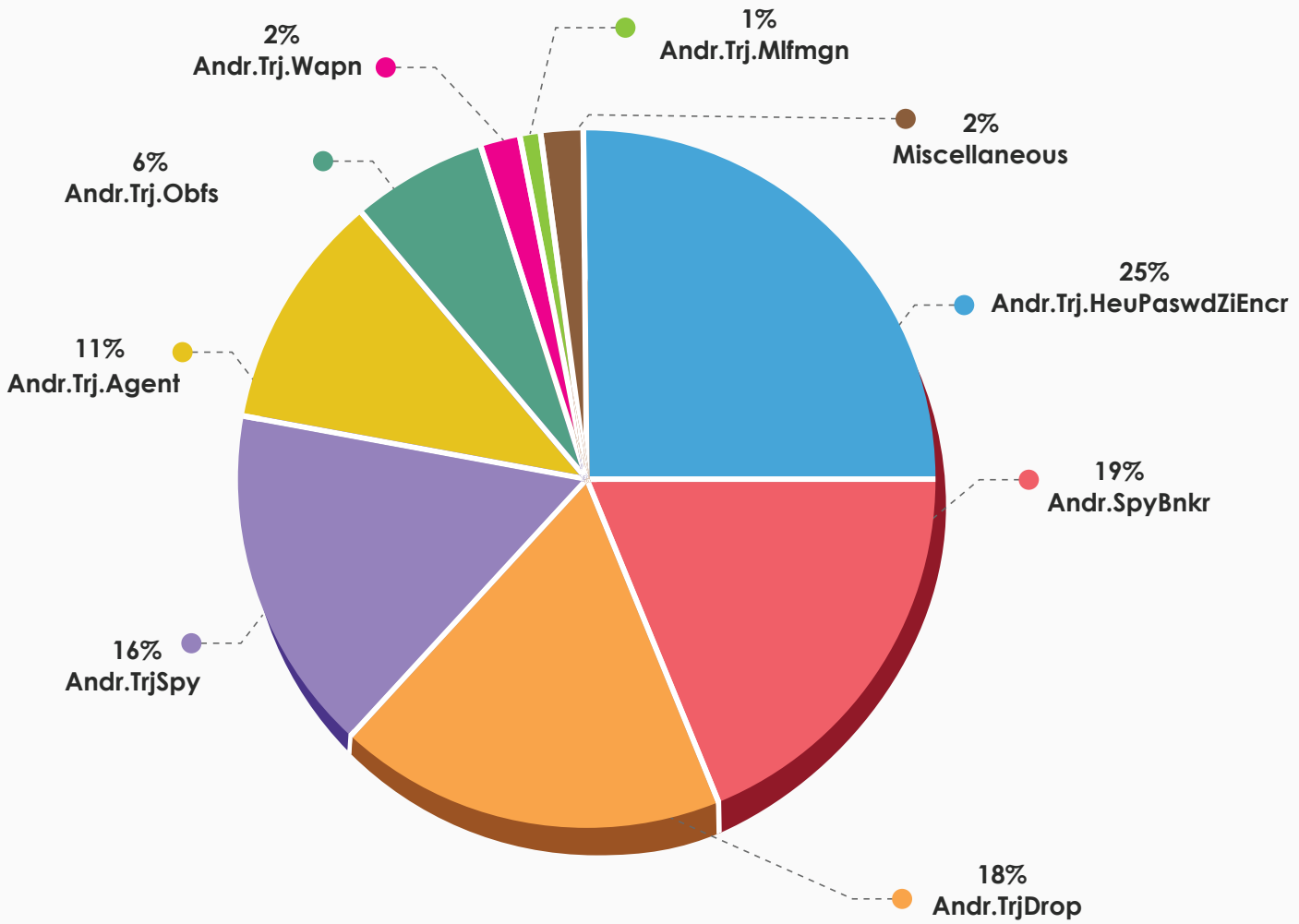
- Smartphones as a Gateway: Smartphones serve as a critical link between personal and professional networks, positioning them as prime targets for cybercriminals.
- Increased Vulnerability: A single compromised mobile device can provide attackers with direct access to organizational systems.
- Severe Consequences: Such an attack can expose sensitive corporate data, disrupt business operations, and lead to significant financial and reputational damage.

Trojan Takeover Looms

Despite the upsurge of new Trojan strains in the Android threat landscape, older varieties remain dominant.

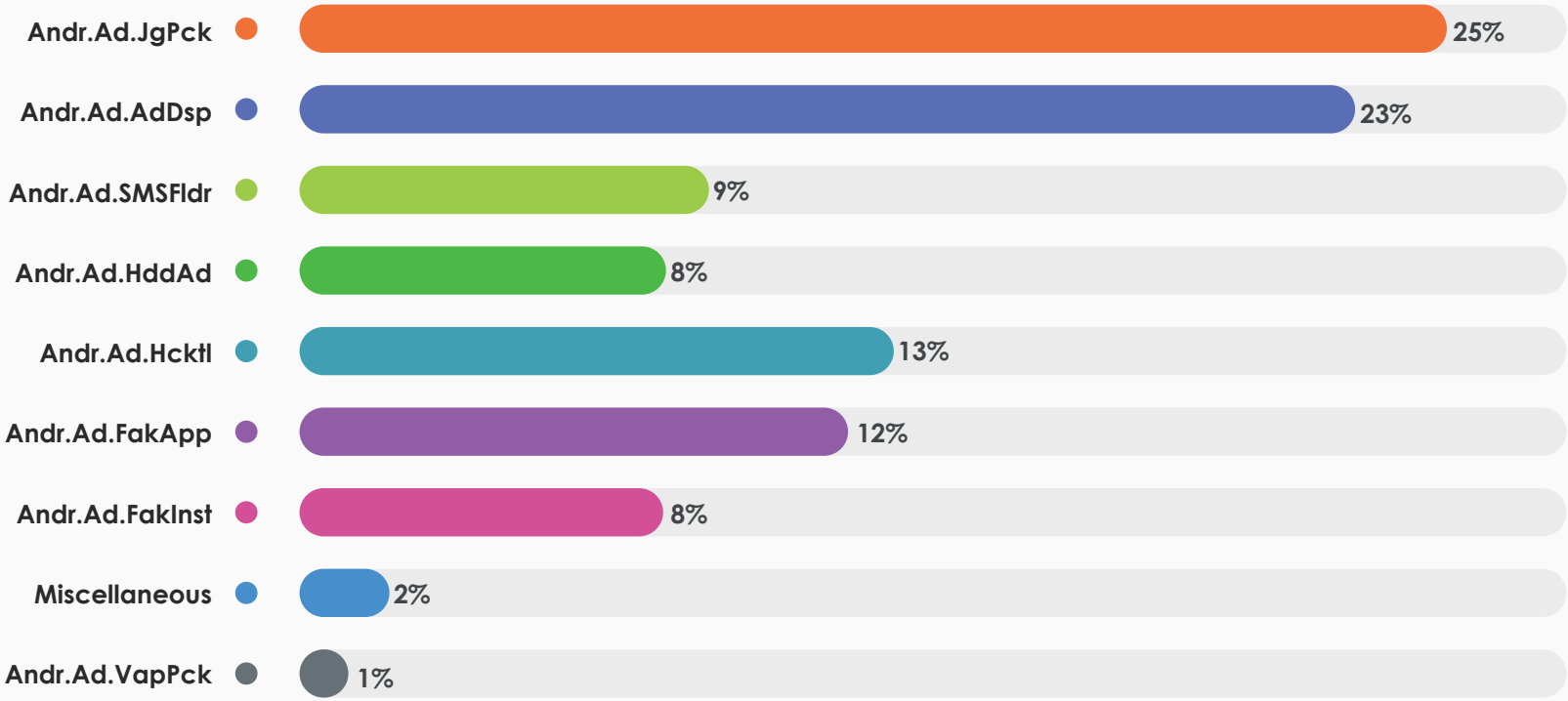
Trojans designed for password theft, bank-related fraud, and dropper deployment continue to dominate the threat landscape. Spyware and agent Trojans, which exploit compromised devices by attaching more malicious installers, also maintain their position at the top of the threat chart. This persistent success suggests that threat actors are not only adept at these types of attacks but also continuously refine and re-purpose existing tactics. Remarkably, older Trojans remain highly effective, leveraging well-established methods that consistently yield results. This demonstrates that attackers continue to find value in refining and recycling familiar techniques rather than pursuing entirely novel strategies.

The Wicked Treadline of Trojan



The Colossal Role of Adware

Most Prevalent Adware Types

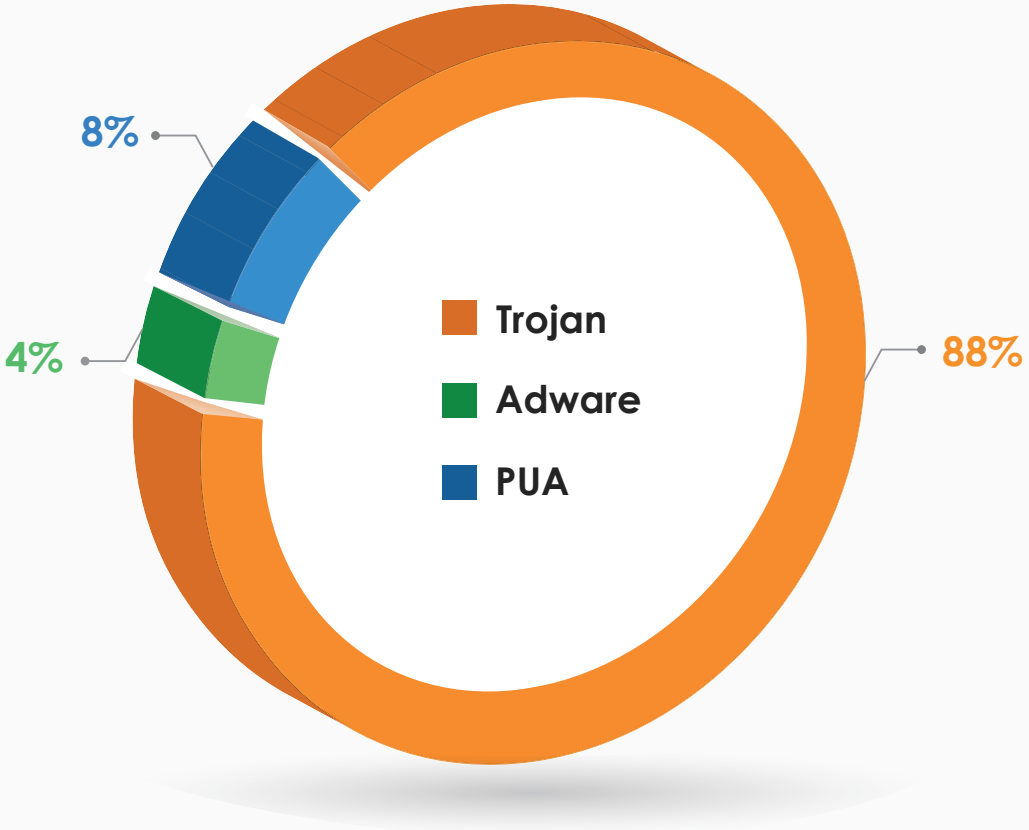


- Minimal Visibility, Significant Impact: While Adware's visible presence is small compared to Trojans, it plays a critical role in the threat ecosystem.
- Credential Theft and Scams: Many Adware strains steal user credentials or facilitate prevalent scams, contributing to more complex attack chains.
- Broader Attack Campaigns: Adware often acts as a precursor to more serious malicious activities, making it a critical vector in mobile security threats.

THE MAC ATTACK

Despite the continued prominence of Windows operating system as a significant target for various cyber threats, macOS is increasingly gaining attention in the contemporary cybersecurity landscape, impacting businesses of all sizes. Quarter after quarter, macOS threats have rapidly evolved, with Trojans notably surging to account for an astonishing 88% of all detected malware. This surge underscores the paramount importance of vigilance and preparedness for micro, small, and medium-sized enterprises (MSMEs), as well as enterprises alike.

Trojan, Adware, and PUA Proportional Split

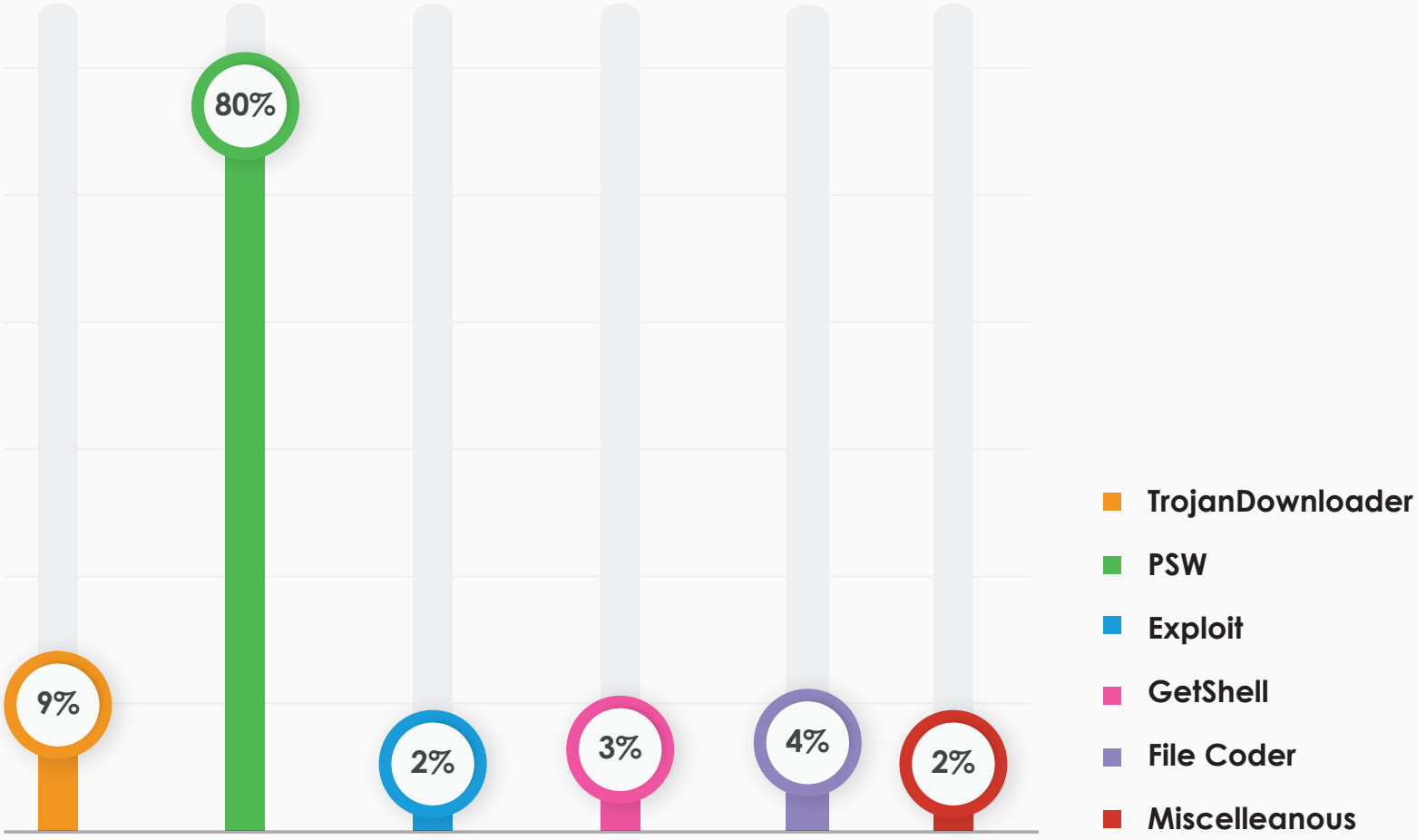


On the contrary, common annoyances such as adware and potentially unwanted programs (PUPs) have significantly diminished, now comprising only 4% and 8%, respectively. However, the growing discourse on darknet forums regarding techniques to circumvent macOS security, harness AI for malware creation, and deploy sophisticated social engineering strategies serve as a clear imperative for businesses to proactively fortify their defenses. Furthermore, the proliferation of macOS malware-as-a-service (MaaS) indicates that threats against Apple's ecosystem are not only escalating but also becoming more accessible and deployable for cybercriminals.

The Ubiquitous Trojans

Analyzing recent Trojan trends reveals concerning patterns among cybercriminals, particularly the pervasive and persistent use of PSW Trojans.

Trojan Detection Trend Line

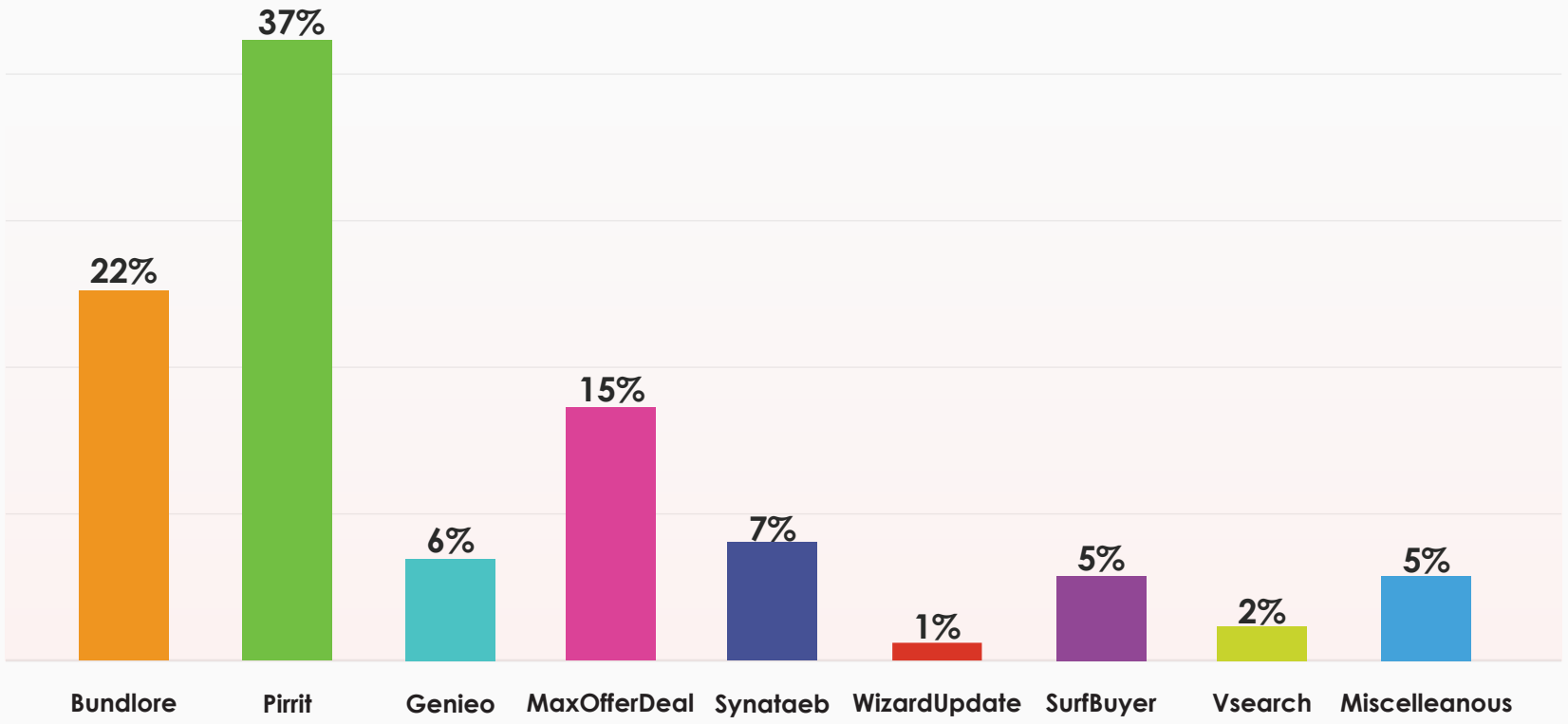


These Trojans strategically target critical macOS security features, specifically focusing on harvesting credentials saved within browsers and macOS keychains. Their intrusive capabilities also include capturing detailed system information, logging keystrokes, taking screenshots, extracting login credentials from email clients such as Apple Mail and popular messaging applications, modifying system preferences, and installing persistent launch agents to automatically execute upon system startup. These tactics represent a calculated effort by threat actors to compromise macOS systems profoundly, emphasizing the imperative for proactive and robust cybersecurity measures.

The Adware Brouhaha

Despite its diminishing visibility, adware still plays a role in macOS threats, albeit with a reduced footprint. The decline in adware prevalence suggests that cybercriminals are shifting their focus toward more lucrative Trojan-based campaigns.

The Trend Line of Adware Variant Detections

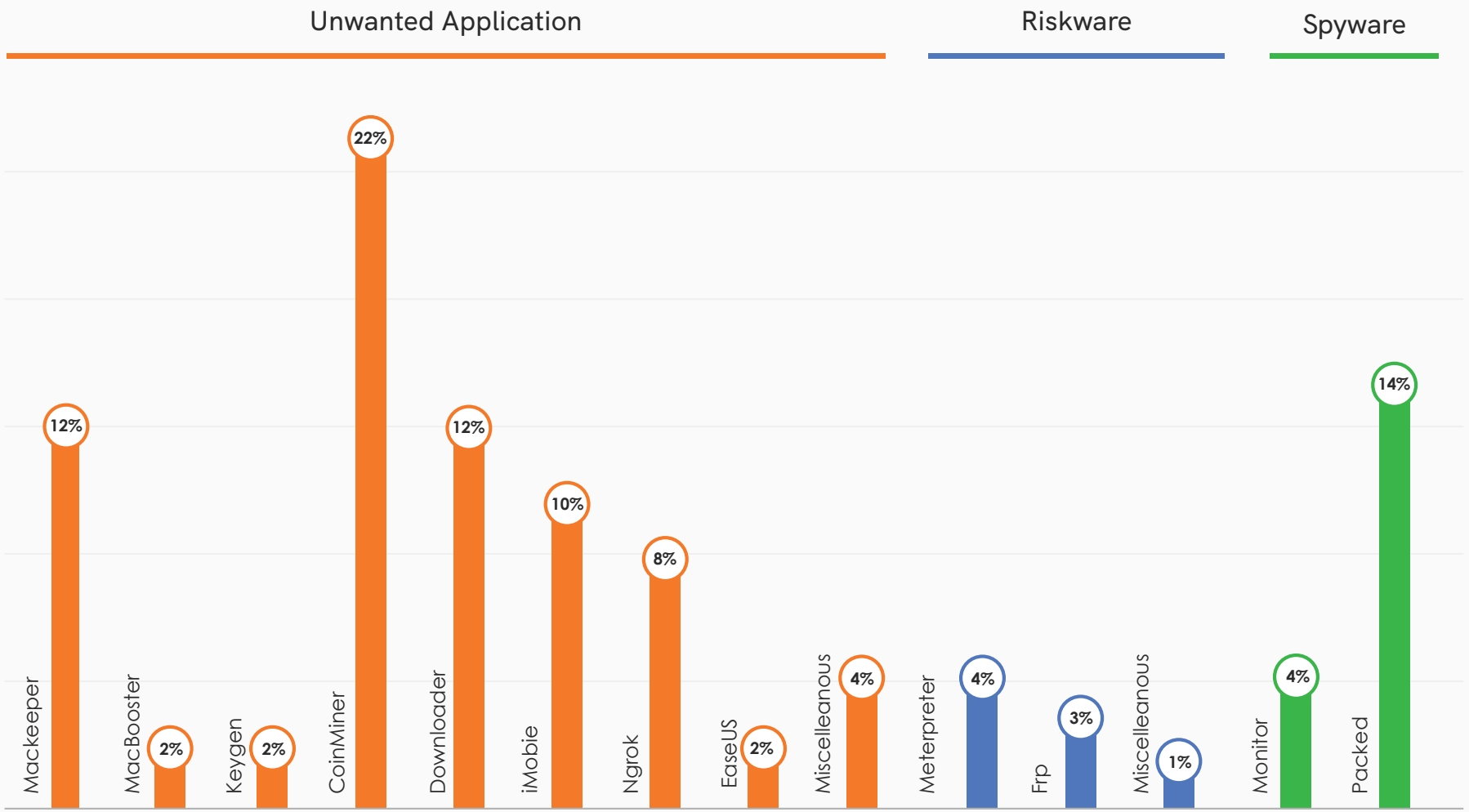


However, three adware families—Pirrit, Bundlore, and MaxOfferDeal—continue to maintain a significant presence, accounting for 37%, 22%, and 15% of detections, respectively. These adware strains infiltrate systems through deceptive software bundles, browser hijackers, and aggressive pop-up campaigns, degrading user experience and exposing systems to additional risks. Their sustained presence indicates that while Trojans dominate the macOS malware landscape, adware remains a persistent nuisance, serving as both a revenue stream for cybercriminals and a potential gateway for more insidious threats.

The Share of PUPs

Diverse detections in the potentially unknown programs (PUP) showcases that groups of threat actors focus on malicious activities, including establishing persistent remote access, executing arbitrary commands remotely, coin mining, spying among others.

Most Prevalent PUP Types



A PEEK INTO A FEW SIGNIFICANT VULNERABILITIES

Threats seem to be the most pervasive and prevalent attacks these days. However, what is often overlooked by enterprises is that the primary reason for threat attacks to happen is because of unpatched vulnerabilities. Vulnerabilities serve as the gateway for threat actors to breach an enterprise and its network chain. Organizations should adopt a more proactive approach than a reactive one in their fight against cyber threats and investing more on vulnerability patching could become a game-changer in the cybersecurity industry.

7-Zip Mark-of-the-Web Protection Breached

CVE-2025-0411 with a CVSS base score of 7.0, allows a remote attacker to bypass the Mark-of-the-Web protection mechanism with the help of user interaction like visiting a malicious page or extracting a malicious file, and may be able to execute arbitrary code in the context of the current user.

Vulnerable versions:

- 7-Zip versions prior to 24.09.

Neutralisation Vulnerability in MNC Console

CVE-2025-26633 is an important improper neutralisation vulnerability in Microsoft Windows Management Console(MNC) enabling an unauthorized attacker to execute code over a network by convincing a user to open a crafted link or file sent via email enticement or hosted on a website.

Vulnerable versions:

- Windows 11 Versions 22H2, 23H2, 24H2 for ARM64-based Systems, x64-based Systems.
- Windows 10 and Versions 1607, 1809, 21H2, 22H2 for 32-bit Systems, x64-based Systems.
- Windows Server 2008, 2012, 2016, 2019, 2022, 2025.

NTFS Bugs

CVE-2025-24993, a remote code execution vulnerability in Microsoft Windows New Technology File System(NTFS), enables an authorized attacker to execute code remotely by tricking a local user on a vulnerable system into mounting a specially crafted virtual hard disk(VHD) for exploiting heap-based buffer overflow. It is rated important with a CVSS base score of 7.8.

CVE-2025-24984 is an information disclosure vulnerability in Microsoft Windows New Technology File System(NTFS), allowing an unauthorized attacker to disclose sensitive information inserted in a log file of Windows NTFS by physically accessing the target computer to plug in a malicious USB drive and potentially read portions of heap memory. It is rated important with a CVSS base score of 4.6.

Vulnerable versions:

- Windows 11 Versions 22H2, 23H2, 24H2 for ARM64-based Systems, x64-based Systems.
- Windows 10 and Versions 1607, 1809, 21H2, 22H2 for 32-bit Systems, x64-based Systems.
- Windows Server 2008, 2012, 2016, 2019, 2022, 2025.

Microsoft Windows Win32 Kernel Subsystem vulnerable to privilege escalation

CVE-2025-24983, causes an authorized attacker to win a race condition gaining SYSTEM level access locally. The vulnerability is rated important and has a CVSS base score of 7.0.

Vulnerable versions:

- Windows 10 and Versions 1607 for 32-bit Systems, x64-based Systems.
- Windows Server 2008, 2012, 2016.

IoT VULNERABILITIES

SonicWalls' Deserialization Vulnerability

CVE-2025-23006 in SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) allows a remote unauthenticated attacker to execute arbitrary OS commands by exploiting deserialization of untrusted data while pre-authentication. The vulnerability has been rated critical with a CVSS base score of 9.8.

Vulnerable versions:

- Version 12.4.3-02804 (platform-hotfix) and earlier versions

Authorization Vulnerability affects Apple OS

CVE-2025-24200, an incorrect authorization vulnerability in Apple iOS and iPadOS, allows a physical attacker to disable USB Restricted Mode on a locked device with a medium rating having a CVSS base score of 6.1

Vulnerable versions:

- iOS 18.3.1
- iPadOS 17.7.5, 18.3.1

PAN-OSs' Bypass Vulnerability

CVE-2025-0108, an authentication bypass vulnerability in Palo-Alto Networks PAN-OS, enables an unauthenticated attacker with network access to the management web interface allowing it to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts.

It has been rated high with a CVSS base score of 8.8.

Vulnerable versions:

- PAN-OS 11.2 :- < 11.2.4-h4, < 11.2.5
- PAN-OS 11.1 :- < 11.1.2-h18, < 11.1.4-h13, < 11.1.6-h1
- PAN-OS 10.2 :- < 10.2.7-h24, < 10.2.8-h21, < 10.2.9-h21, < 10.2.10-h14, < 10.2.11-h12, < 10.2.12-h6, < 10.2.13-h3
- PAN-OS 10.1 :- < 10.1.14-h9

OUR VERDICT

This Q4_2024-25, though there has not been much changes to the way the attack has been launched and with the industries impacted, we are noticing a slight shift to more lucrative industries even if their attack surface is not much. Threat actors may get more benefits from these industries with less resource, time and money spent. Not just that, these industries being niche players, they will be more particular in meeting the threat actors' demands for the fear of losing rich clientele.

Furthermore, the evolution underscores a growing sophistication in cybercriminal tactics, with attackers increasingly exploiting specialized sectors handling high-value transactions or sensitive data. These sectors, including healthcare, pharmaceuticals, and engineering, may mistakenly perceive themselves as lower-risk due to their size and operational focus. This misjudgment frequently leads to inadequate security measures, inadvertently facilitating cybercriminals' access to significant breaches.

To effectively counter such threats, these specialized businesses must devise targeted cybersecurity strategies tailored to their unique operational vulnerabilities. Vital actions include bolstering staff awareness, conducting periodic comprehensive risk assessments, and implementing adaptive security frameworks to promptly identify and respond to potential threats. Collaborating actively with cybersecurity experts and investing in sophisticated threat intelligence solutions will further fortify defenses, ensuring both data security and enduring client trust in an increasingly complex cyber milieu.

ABOUT US

K7 Security is a cybersecurity pioneer with over 30 years' expertise in preventing cyberattacks, and one of a few global cybersecurity providers with a proprietary scan engine. K7's Enterprise Security solutions include endpoint and network security solutions that protect any size and type of business without affecting device or network performance and are designed to protect modern organisations with a remote or hybrid workforce, and cybersecurity services that provide assured compliance and threat defence.

CYBER THREAT MONITOR REPORT

Q4_2024-25

K7 SECURITY

www.k7computing.com