

CYBER THREAT MONITOR
REPORT

Q4_2023-24

CONTENTS

Delving into the Cyber Threat Scenario

Cyber Threat Monitor India

Regional Infection Profile

Infection Rate Comparison Across Platforms

Enterprise Insecurity

Safety Recommendations

Vulnerabilities Galore

Google's Memory Access Vulnerability

Security bypass Vulnerability in Windows SmartScreen

Privilege Elevation Vulnerability in Microsoft Exchange Server

Vulnerability in Microsoft Shortcut files

Microsoft Kernel's Elevation Privilege Vulnerability

Danger in the Internet of Things

Apple OS Vulnerability

Vulnerability in Ivanti Products

Write Vulnerability in Fortinet Products

Mitigation Techniques

Windows Under Siege

Windows Malware Type Breakdown

Windows Exploits

Heuristic Host Intrusion Prevention System (HIPS)

Mitigation Tips

The Mobile Device Story

The Omnipresent Trojan

The Adware Saga

Tips to Stay Safe

Mac Attack

The Ubiquitous Trojans

The Adware Uproar

A Pinch of PUPs

Safety Guidelines

Latest Security News

Resurgence of Qakbot

Ransomware in Python's flavour

Phony SMS on the rise

Last year's noteworthy Vulnerabilities

Key Takeaways

DELVING INTO THE CYBER THREAT SCENARIO

The recent surge in cyber threats presents a grave and rapidly evolving landscape. Novel social engineering scams, sophisticated phishing, and smishing tactics are not just posing significant risks but have reached an alarming all-time high nowadays. Attackers are demonstrating advanced techniques to evade traditional security controls, intensifying the situation.

The skyrocketing number of ransomware attacks adds another layer of complexity to the landscape, testing victims' technological and financial resilience. The advent of "as-a-service" models like Ransomware-as-a-Service (RaaS), Phishing-as-a-Service (PaaS), and Malware-as-a-Service (MaaS), among many others, has made the tools for conducting cyberattacks more accessible. Even those with minimal technical know-how can launch advanced cyberattacks, thanks to these "as-a-service" models that lower the entry barrier for potential cyber criminals.

Adding fuel to the fire is the fact that spyware and malware campaigns are increasingly targeting enterprises and individuals alike. Both have profound implications: the integrity of information and privacy could be hampered, signifying the need for specific defenses.

It has been quite evident that conventional cybersecurity is no longer valid. Organizations, and in essence, even individuals have no option but to be forward-leaning in acquiring and mastering an all-around approach to cyber defense that includes high-end threat detection and continuous education on new-age cyber threats. We will only strengthen our resolve to outmanoeuvre the foes against a backdrop of rising cybersecurity challenges. By being informed and prepared, we are collectively enabled to thwart the adversaries efforts and protect our digital future.

Our report offers a comprehensive overview of the threat landscape without overwhelming you with technical jargon. For more detailed analysis, read our [K7 Labs' technical blogs](#).

Share this report with your colleagues to ensure a secure digital experience.

Get informed and take action now!



Map for illustrative purposes only. Not to scale.

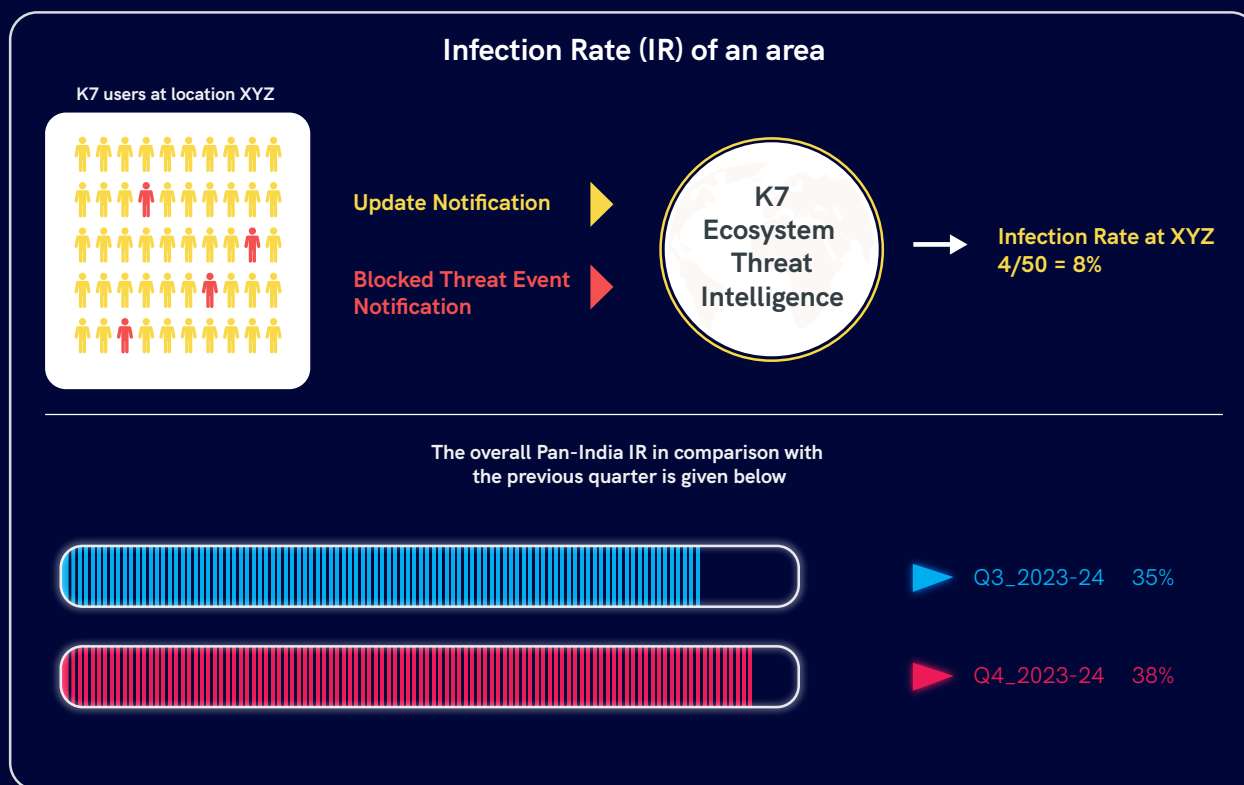
REGIONAL INFECTION PROFILE

The landscape of digital threats is constantly evolving, posing significant challenges to the security of our online lives. Designed to enlighten both newcomers and seasoned readers, our IR serves as a foundational benchmark for assessing the vulnerability of internet users to cyber threats.

Those new to our quarterly report would need to understand an important concept called "Infection Rate" (IR) which is used as the base for benchmarking a netizen's risk.

We use this IR factor to identify the netizens' exposure to cyber threats. IR is determined as the proportion of K7 users in an area who encountered at least one cyber threat event and which was blocked and reported to our **K7 Ecosystem Threat Intelligence infrastructure**. The higher the IR, the greater the risk.

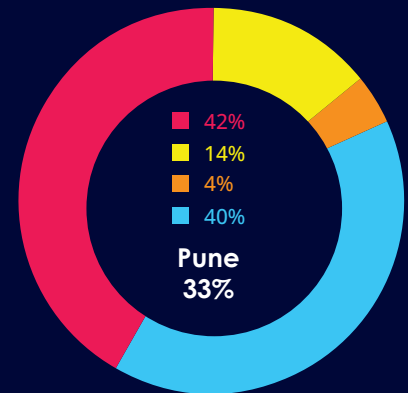
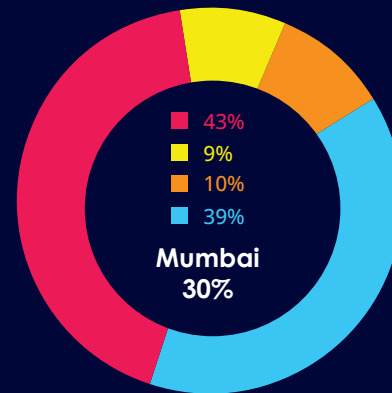
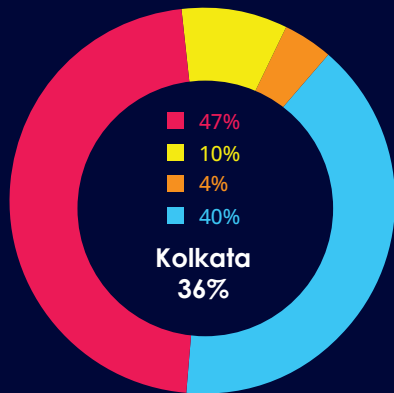
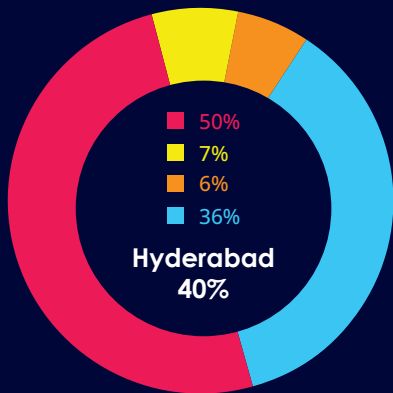
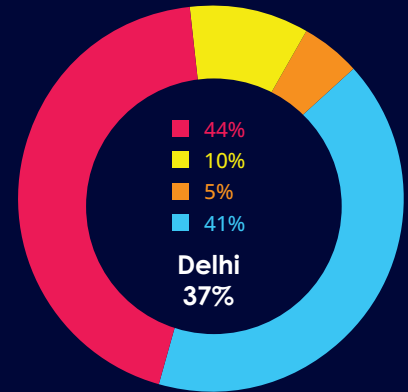
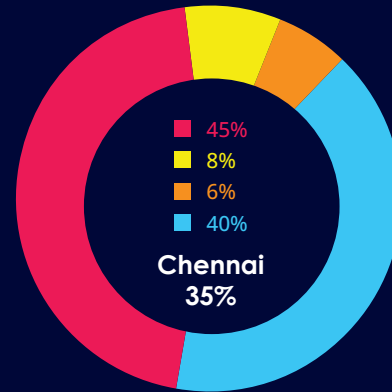
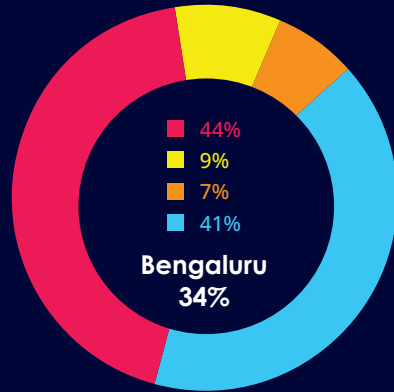
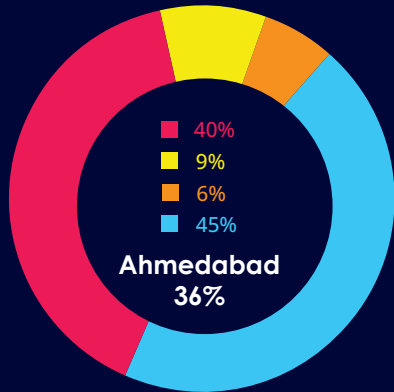
The concept of Infection Rate is better explained by the below picturization.



A higher IR value signals an elevated risk level, underscoring the necessity for vigilant cybersecurity measures. Understanding the contemporary threat landscape through the lens of the IR not only informs us about the current state of cyber threats but also empowers us to take the necessary steps to protect ourselves.

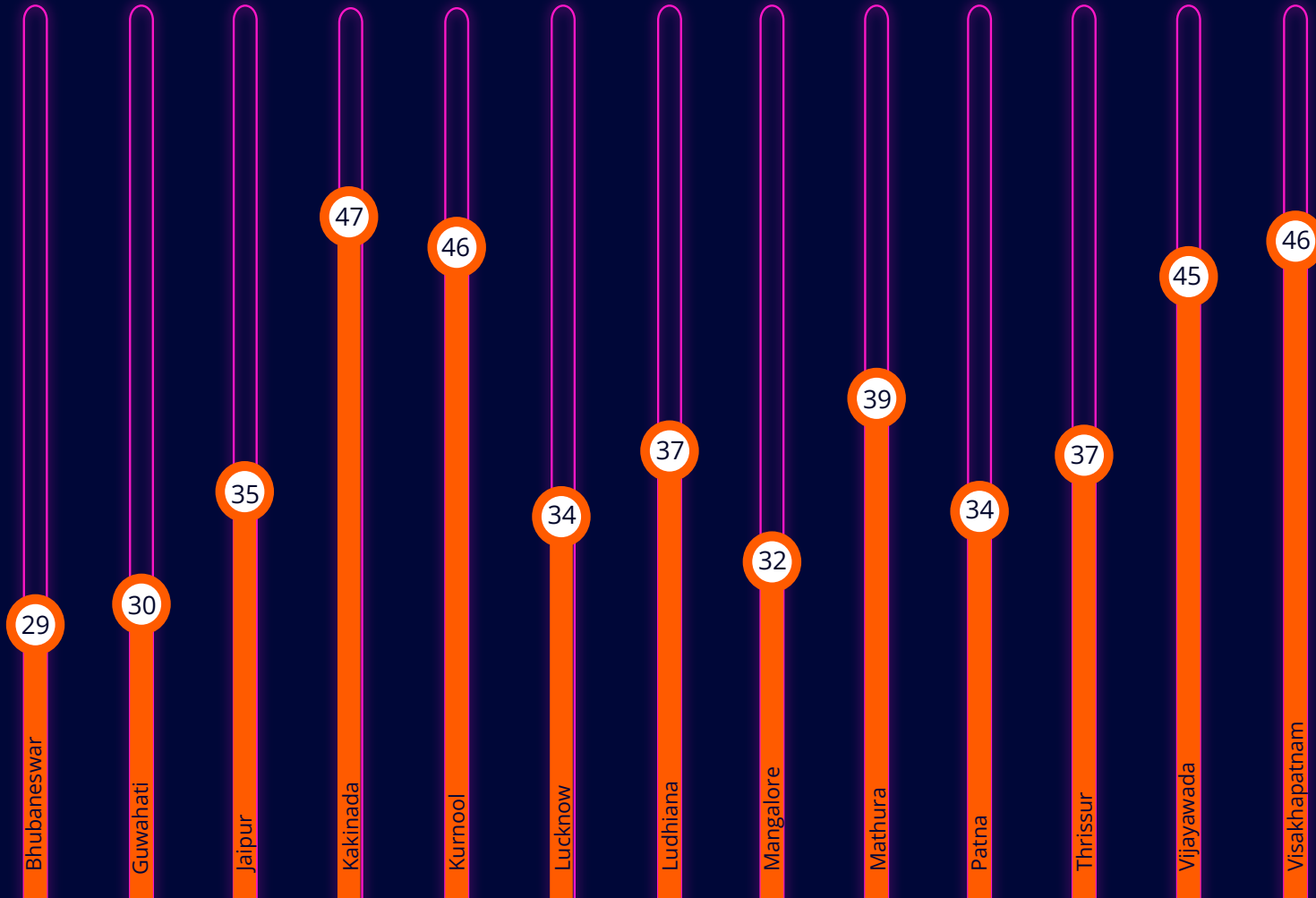
Before we delve into the threat landscape for the last quarter, we present to you a few significant IRs across metros classified based on the different levels at which the threats were blocked.

THE METRO AND TIER-1 CITIES - INFECTION RATE



- Web Protection
- Behaviour Protection
- Firewall Protection
- ScanEngine Protection

TOP INFECTION RATES IN TIER-2 CITIES

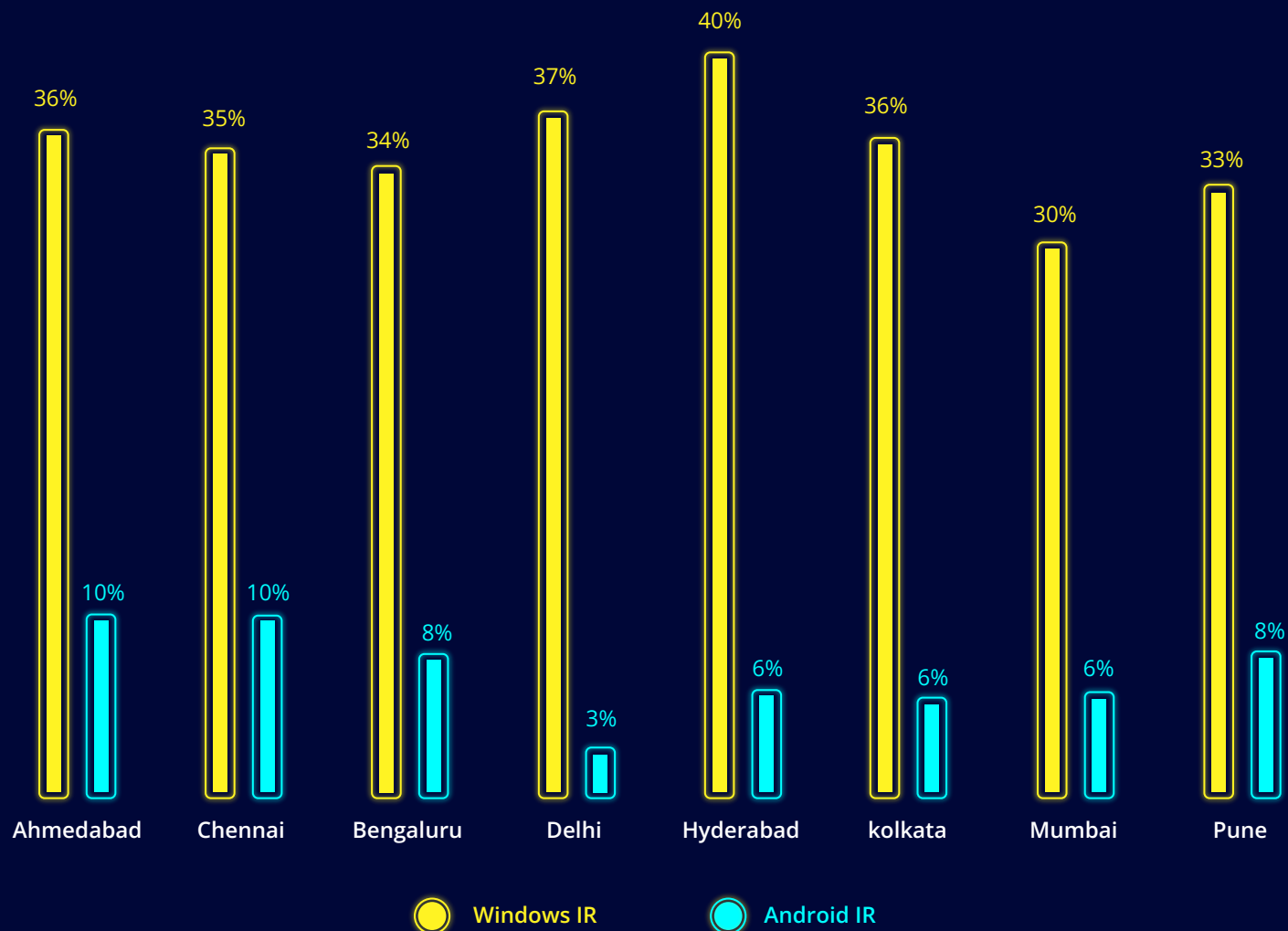


Tier-2 cities, once considered less lucrative targets, are increasingly attractive to cybercriminals due to their expanding digital footprint, inadequate knowledge of cyber hygiene, and potential for cascading disruptions.

INFECTION RATE COMPARISON ACROSS PLATFORMS

While Android threats are on the rise, Windows' massive installed base and legacy vulnerabilities continue to make it a prime target for cybercriminals.

Windows IR vs Android IR



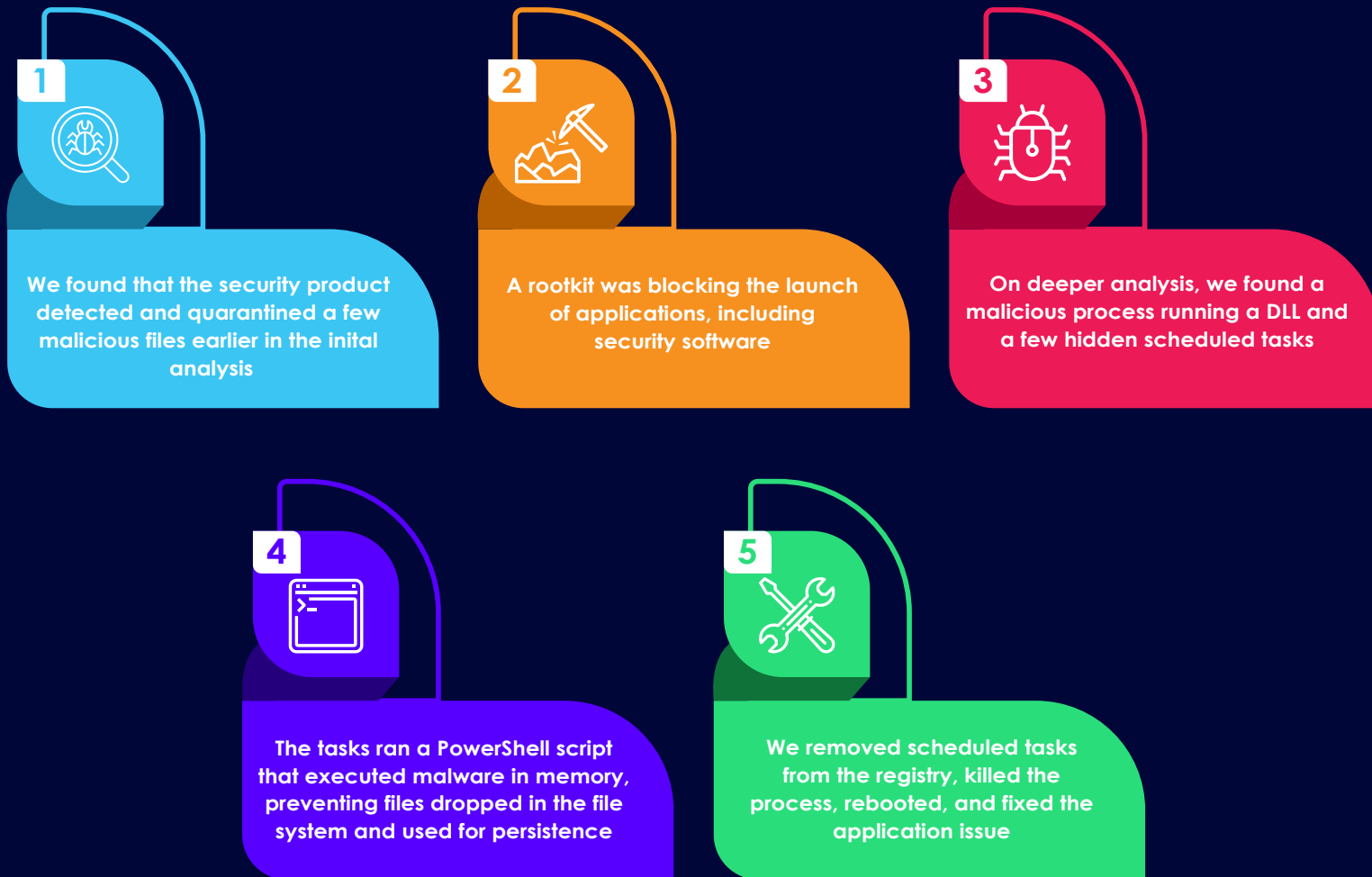
However, K7 Labs researchers have observed an uptick in mobile malware also. This trend suggests that cybercriminals are increasingly recognizing the growing mobile landscape and may shift their focus in the future.

ENTERPRISE INSECURITY

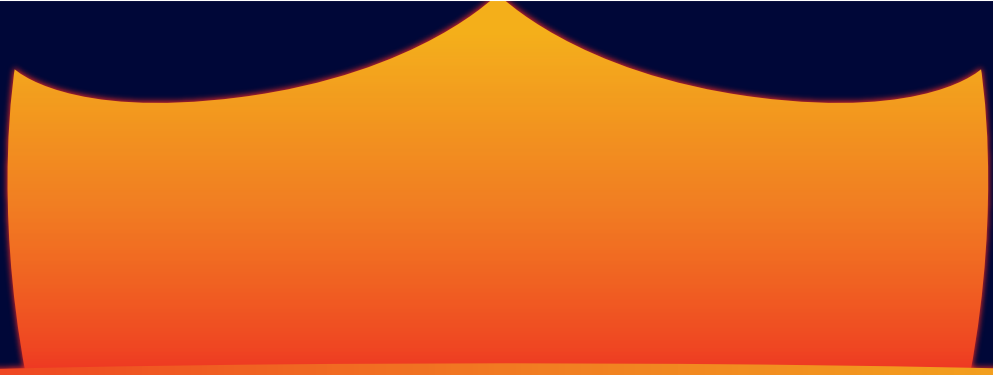
Enterprises have been a target of threat actors mainly due to the large attack surface and monetary benefits it offers.

Recently, one of our customers reported that they were unable to open some of their applications. The kill-chain is as given below.

Case Study: The Rootkit R77 Mayhem



SAFETY RECOMMENDATIONS

- 
- Enforcing use of strong passwords and multi-factor authentication (MFA)
 - Logging PowerShell activity
 - Keeping your devices updated and patched against the latest vulnerabilities
 - Protecting your devices by using a high-quality security software such as K7 Endpoint Security and keeping it up-to-date

VULNERABILITIES GALORE

Most of the devices are vulnerable in some way or the other.. These can be exploited by threat actors if not identified and fixed in a timely manner..

Listed below are a few of the significant vulnerabilities that have been exploited in the last quarter

Google's Memory Access Vulnerability

CVE-2024-0519, an out-of-bounds memory access vulnerability in Google chromium V8 allows a remote attacker to craft a HTML page to potentially exploit heap corruption in V8 Javascript and WebAssembly engine.

- Vulnerable products
 - Google Chromium < 120.0.6099.216

Security bypass Vulnerability in Windows SmartScreen

A security feature bypass vulnerability, **CVE-2024-21351** in Microsoft Windows SmartScreen allows an attacker to send a malicious file to the user and convinces them to open it, allowing an attacker to inject code into SmartScreen and potentially gain code execution, leading to data exposure, system unavailability and more.

- Vulnerable products
 - Windows server 2016, 2019 and 2022.
 - Windows 10 and 11.

Privilege Elevation Vulnerability in Microsoft Exchange Server

A privilege elevation vulnerability, **CVE-2024-21410**, in Microsoft Exchange Server allows an attacker to use a leaked Net-NTLMv2 hash against the vulnerable Exchange server and authenticate as a victim to perform operations on the server on behalf of the victim.

- Vulnerable products
 - Microsoft Exchange Server 2019 Cumulative Update 14 < 15.2.1544.004
 - Microsoft Exchange Server 2019 Cumulative Update 13 < 15.2.1544.004
 - Microsoft Exchange Server 2016 Cumulative Update 23 N/A

Vulnerability in Microsoft Shortcut files

CVE-2024-21412, a security feature bypass vulnerability in Microsoft Internet Shortcut allows an attacker to send and convince the user to open the malicious file to bypass the displayed security checks and exploit the vulnerability.

However, there is no evidence of this vulnerability being exploited in the wild.

- Vulnerable products
 - Windows 10, 11, Server 2019, Server 2022

Microsoft Kernel's Elevation Privilege Vulnerability

CVE-2024-21338 in Microsoft's Windows Kernel allows privilege elevation. The Appid.sys contains an exposed IOCTL with insufficient access control vulnerability within IOCTL dispatcher that allows a local attacker to run a specially crafted application and achieve privilege escalation onto the system.

- Vulnerable products
 - Windows 10, 11, Server 2019, Server 2022

DANGERS IN THE INTERNET OF THINGS

Most of the connected devices are vulnerable with no major importance given to cybersecurity making it easier for threat actors to breach and gain access to Personal Identifiable Information (PII) and other sensitive data.

Few of the significant vulnerabilities exploited in the wild are given below

Apple OS Vulnerability

A type confusion vulnerability, **CVE-2024-23222**, in multiple Apple product's OS, allows remote code execution while processing a malicious crafted web content.

Vulnerable products -

- Vulnerable products -
 - iOS - Versions after (>) 16.0 and before (<) 16.7.5 - Versions after (>) 17.0 and before (<) 17.3
 - tvOS - Versions before (<) 17.3
 - macOS - Versions from including (>=) 14.0 and before (<) 14.3 - Versions from including (>=) 13.0 and before (<) 13.6.4 - Versions from including (>=) 12.0 and before (<) 12.7.3
 - iPadOS - Versions after (>) 16.0 and before (<) 16.7.5 - Versions after (>) 17.0 and before (<) 17.3

Vulnerability in Ivanti Products

A command injection vulnerability, **CVE-2024-21887** in web components of Ivanti connect secure and policy secure allows a low-privileged user to execute arbitrary commands on the appliances by sending a specially crafted HTTP request.

A server-side request forgery vulnerability, **CVE-2024-21893**, in the SAML component of Ivanti connect secure, policy secure and neurons for ZTA. allows an unauthenticated attacker to access certain restricted resources.

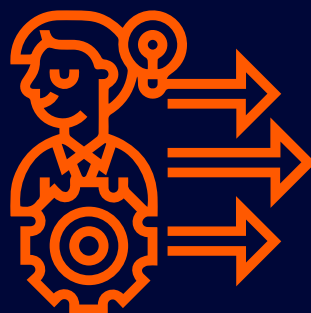
- Vulnerable products -
 - All supported version of - 9.x and 22.x

Write Vulnerability in Fortinet Products

An out-of-bounds write vulnerability, **CVE-2024-21762**, in FortiNet FortiOS and FortiProxy, allows a remote unauthenticated attacker to send a crafted HTTP request and execute arbitrary commands on the victim's network.

Vulnerable products -

- Vulnerable products -
 - FortiOS Versions:-
 - 7.4.0 <= Versions <= 7.4.2
 - 7.2.0 <= Versions <= 7.2.6
 - 7.0.0 <= Versions <= 7.0.13
 - 6.4.0 <= Versions <= 6.4.14
 - 6.2.0 <= Versions <= 6.2.15
 - 6.0.0 <= Versions <= 6.0.17.
 - FortiProxy versions:-
 - 7.4.0 <= Versions <= 7.4.2
 - 7.2.0 <= Versions <= 7.2.8
 - 7.0.0 <= Versions <= 7.0.14
 - 2.0.0 <= Versions <= 2.0.13
 - 1.2.0 <= Versions <= 1.2.13
 - 1.1.0 <= Versions <= 1.1.6
 - 1.0.0 <= Versions <= 1.0.7



MITIGATION TECHNIQUES

- Encrypt your connections
- Ensure you set a unique and strong password for each of your devices in the network
 - Connect your devices to only a secure and trusted network
 - Regularly check your device permissions and connections

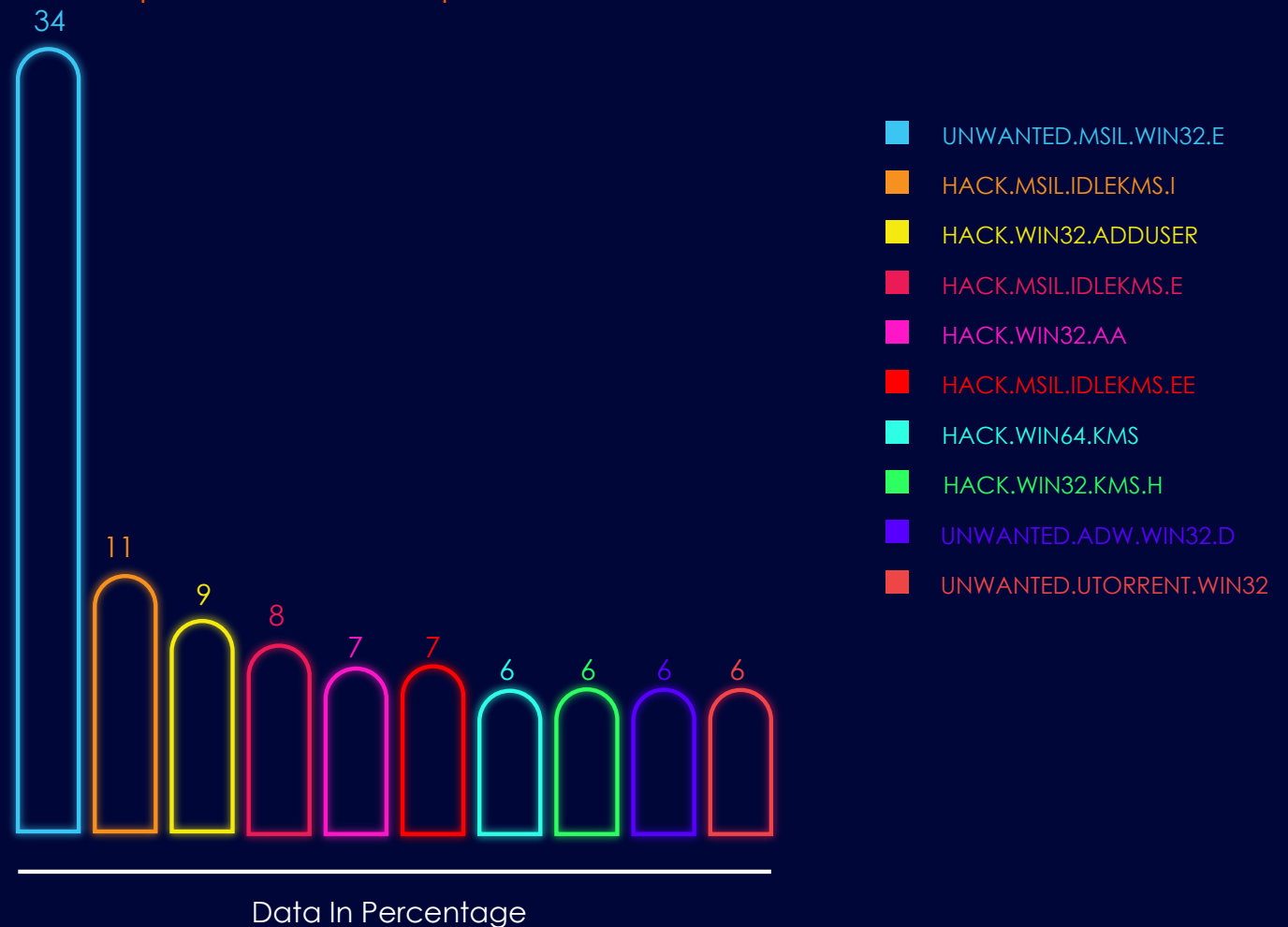


WINDOWS UNDER SIEGE

WINDOWS MALWARE TYPE BREAKDOWN

In this ever-evolving cyber domain, the Windows operating system emerges as a focal point of contention, under siege from an array of sophisticated malware threats. The latest analysis reveals a concerning trend: a continuous and aggressive onslaught targeting bustling corporate giants as well as solo entrepreneurs. Adversaries can execute complex scripts and commands that can be obfuscated, making it harder for security tools to detect malicious activity. Such persistent aggression necessitates a deeper investigation into the Windows platform's vulnerabilities.

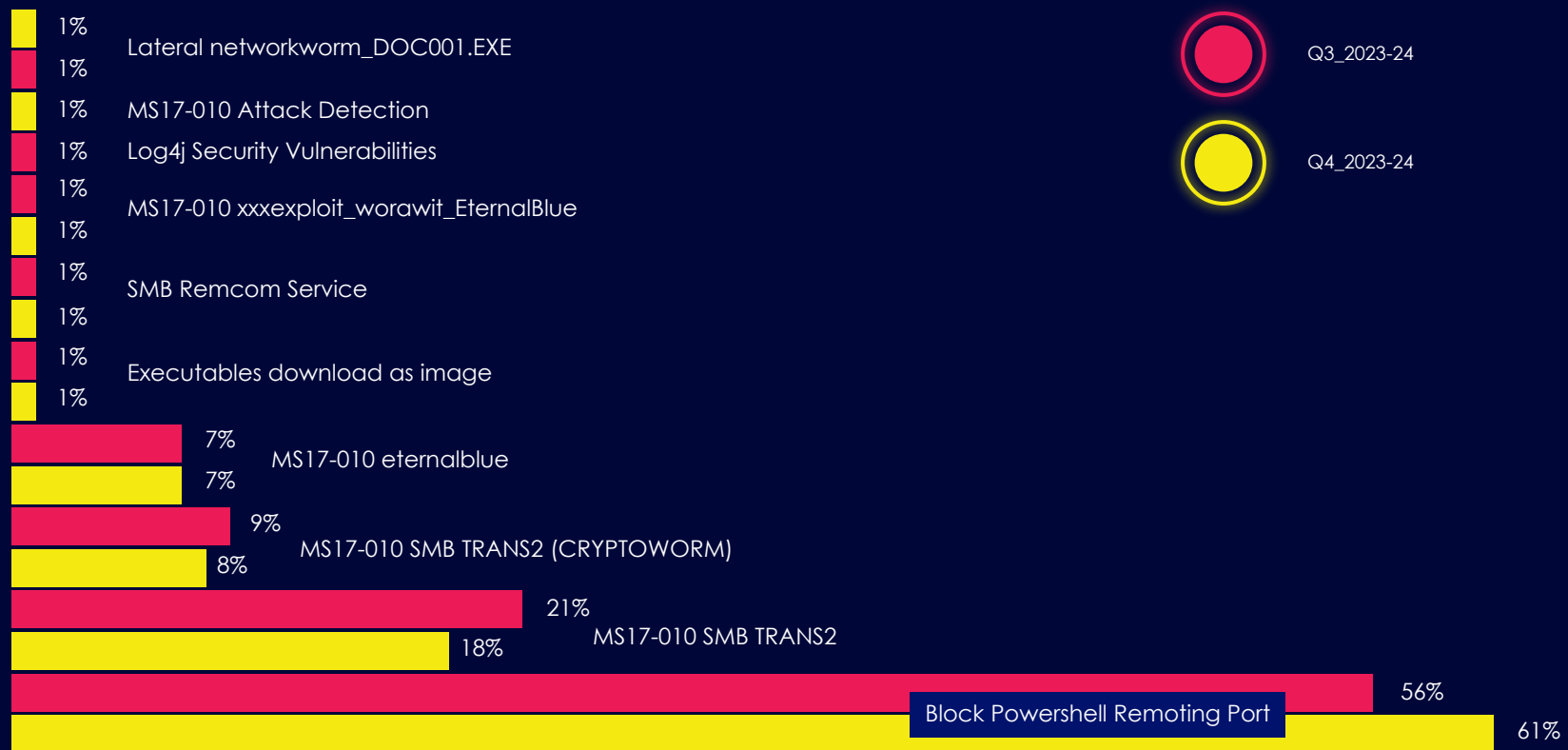
Split of Windows Top 10 Detections



WINDOWS EXPLOITS

With its longstanding dominance in the desktop and laptop market, Windows presents an alluring target for cybercriminals. Threat actors tirelessly seek to exploit system weaknesses, thereby gaining unauthorized access to critical information and infrastructure. The significance of these vulnerabilities is underscored by notable detection metrics, which highlight the urgent need for robust cybersecurity measures.

Most Prevalent Exploits

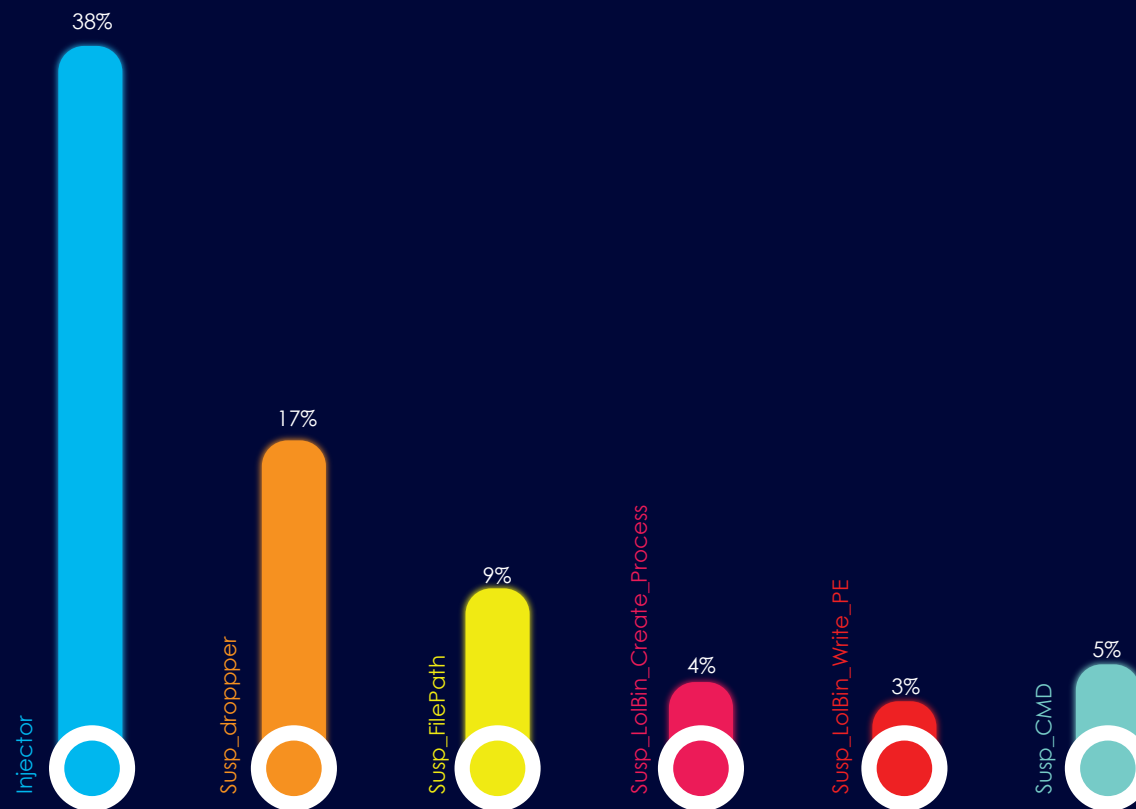


While Microsoft has significantly improved Windows security over the years, its unpatched legacy vulnerabilities, like those in SMBs and PowerShell, have massively contributed to the constant escalation in various Windows devices being targeted. Cybercriminals have increasingly utilised PowerShell for malicious activities, such as delivering malware or executing various attack techniques. PowerShell's versatility and deep integration with the Windows operating system make it an attractive choice for attackers.

HEURISTIC HOST INTRUSION PREVENTION SYSTEM (HIPS)

Heuristic behavioural detections are a way of detecting threats for which we might have not added a signature as yet. This detection layer is ideal for both defending against new threats (0-days) as well as being very effective against new variants of existing malware families. Let us see what our heuristic behavioural technology has detected in the last quarter.

Windows Heuristic Behavioural Detections



In Q4_2023-24, Injectors and Droppers retained their place as in Q3_2023-24. Injectors are malware that use legitimate file names or locations to hide behind trusted names so as to evade detection. Injectors, as the name indicates, inject code into processes, typically legitimate and trusted services. This is also usually done to evade AV detections or gain privilege elevation or both. Droppers are used by threat actors in multi-stage attacks where additional malicious payloads are downloaded or dropped.

MITIGATION TIPS

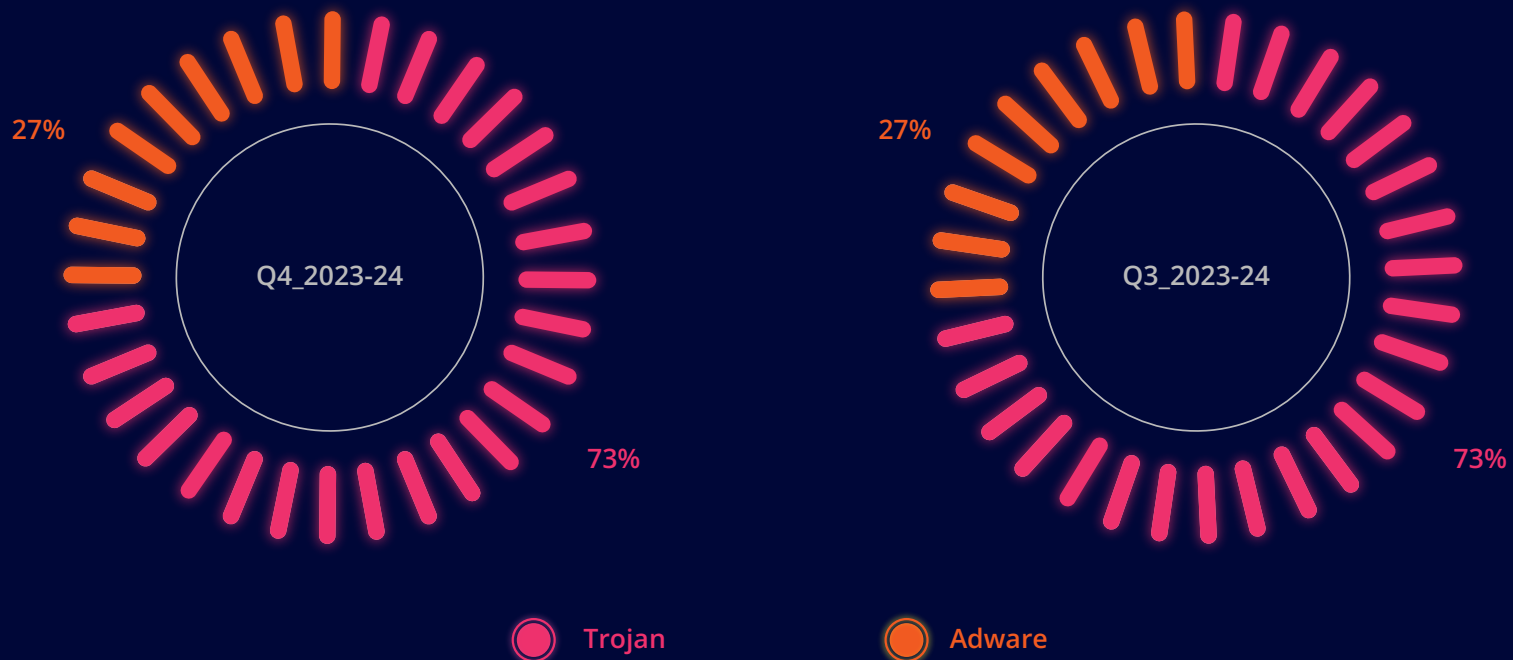
- Use an account without administrator privileges wherever possible
- Set up your operating system to enable auto-updates by default
 - Be cautious when installing any software
 - Backup your data on a regular basis



THE MOBILE DEVICE STORY

The Android threat landscape has rapidly evolved, presenting urgent new challenges to users' mobile security. The reasons behind the prevalence of trojans and adware is due to the widespread use of Android devices, the increasing sophistication of social engineering tactics, and the vulnerabilities in third-party app stores and apps. This uptick in malicious activities underscores the adaptability and persistence of threat actors and highlights significant implications for Android security, necessitating enhanced defensive measures from both users and corporations. This evolving threat landscape demands constant vigilance and adaptation to safeguard against the ingenious tactics employed by cybercriminals, setting a crucial agenda regarding the same for the tech community in the coming months.

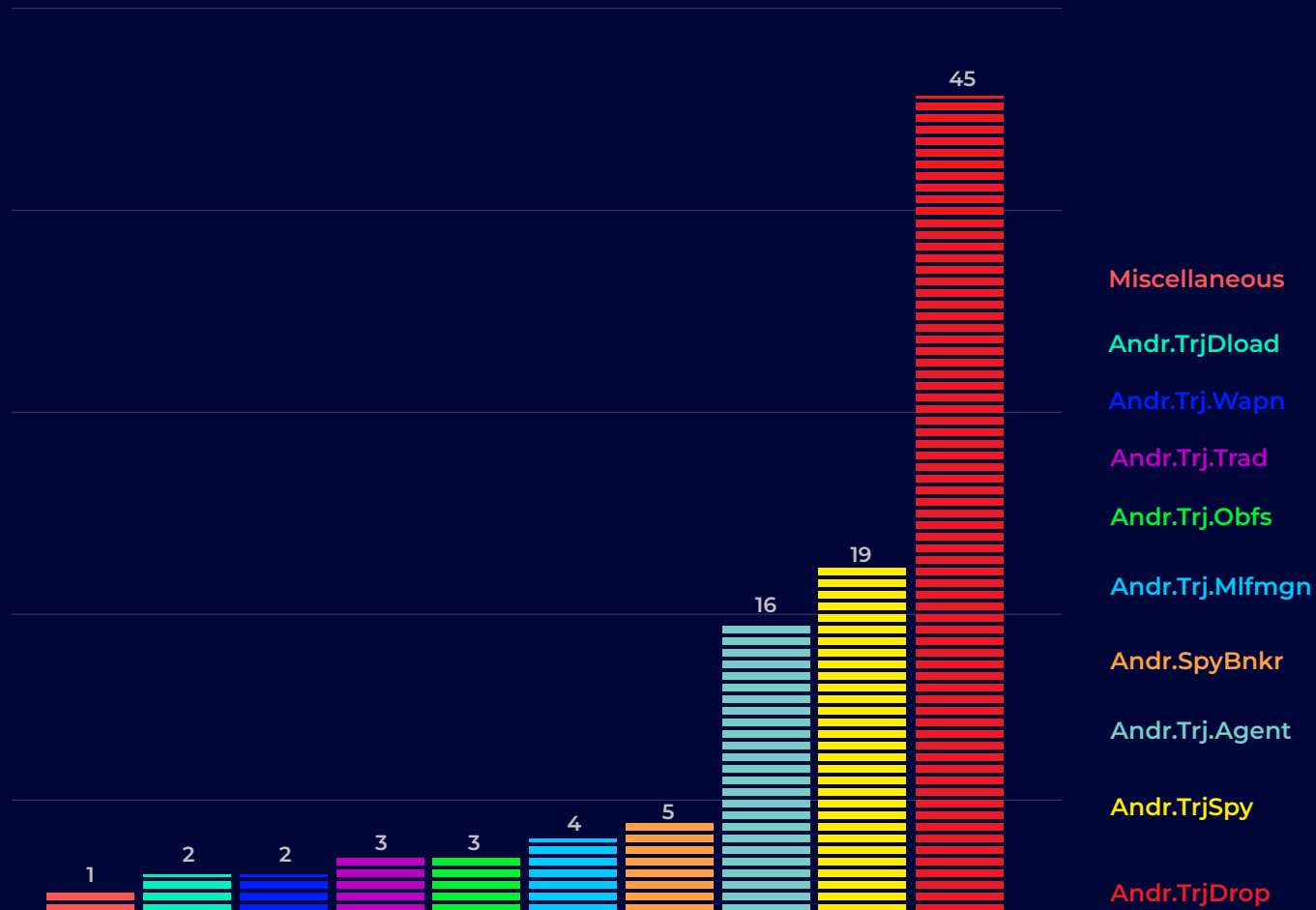
Adware vs Trojan Proportional Split



THE OMNIPRESENT TROJAN

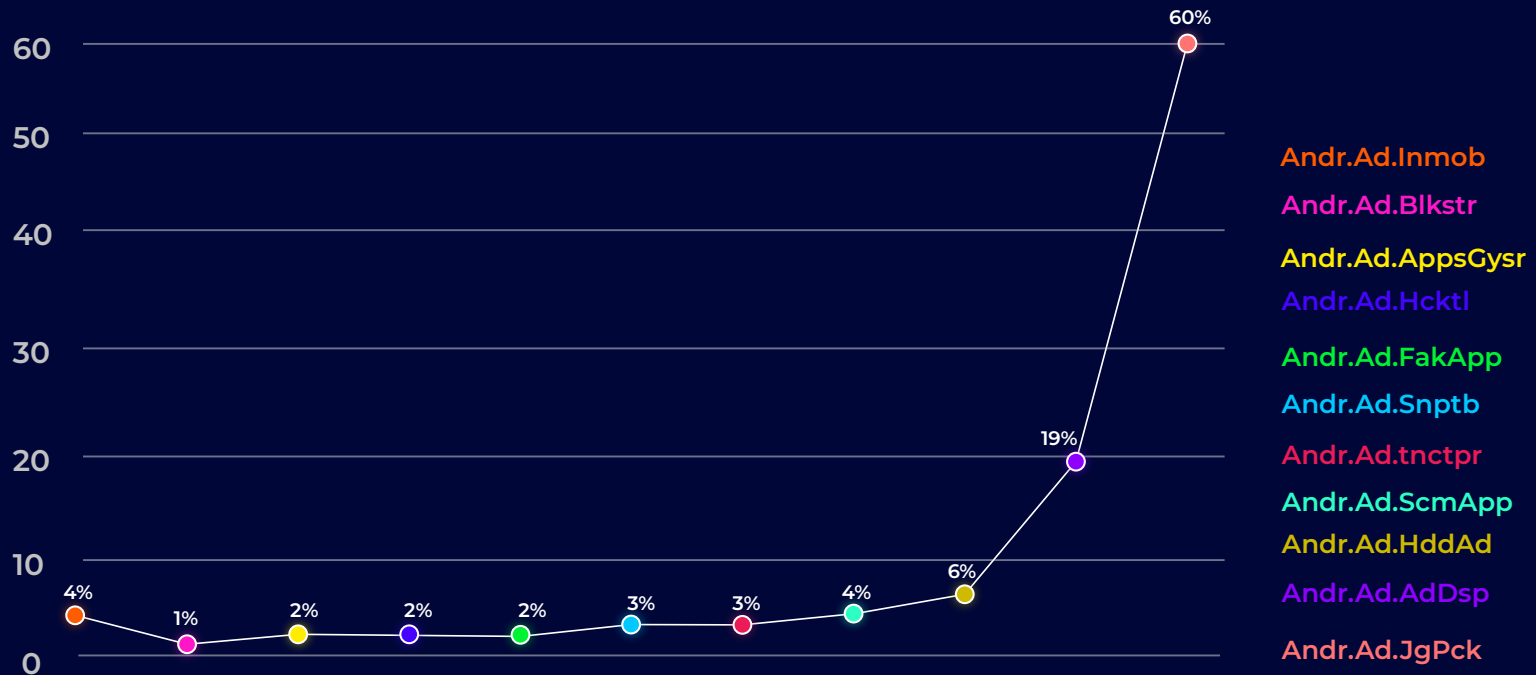
The prevalence of Andr.TrjDrop, Andr.TrjSpy, and Andr.Trj.Agent attacks have notably increased, indicating a sophisticated effort by cybercriminals to compromise Android devices. These types of malware have been instrumental in infiltrating devices, leading to the theft of sensitive information and the deployment of further malicious payloads, jeopardising personal and corporate data security.

Most Prevalent Trojan Types



The Android ecosystem has witnessed a notable surge in adware attacks, particularly those associated with Andr.Ad.JgPck and Andr.Ad.AdDsp is marking a concerning trend. This prevalence can be attributed to the expansive reach and profitability of adware for cybercriminals, coupled with the vulnerability of numerous Android devices due to irregular updates and security patches. The continuous evolution of these adware variants, leveraging sophisticated techniques to evade detection, signifies a growing challenge within the digital environment.

Trend Line Showing the Adware Plague





TIPS TO STAY SAFE

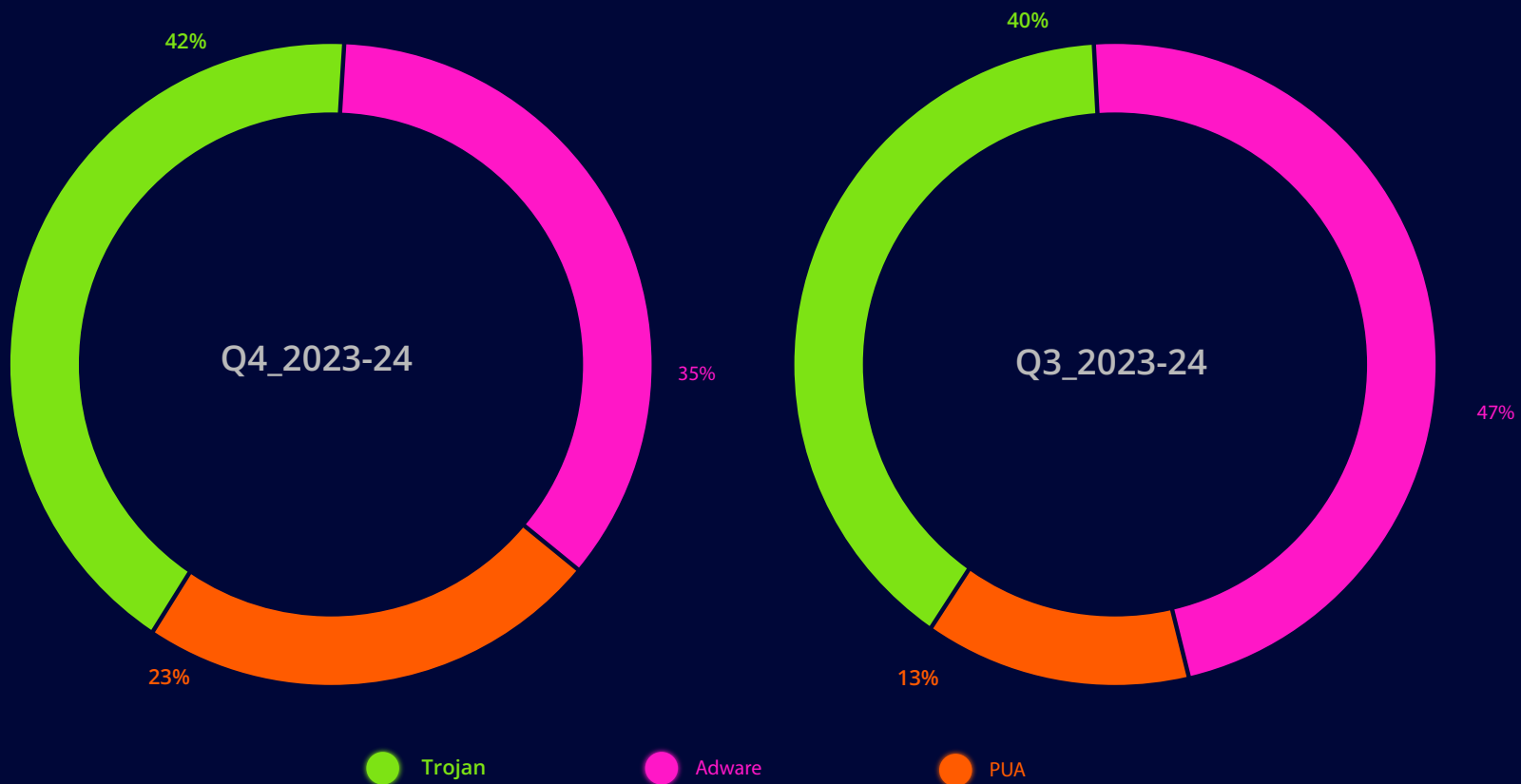
- Always be extra cautious before downloading and installing any app
- Do not download or install apps from unknown sources or third-party app stores
- Keep your OS and devices updated and patched against the latest vulnerabilities
- Install a robust security product like K7 Mobile Security to stay protected from the latest threats and update it regularly



MAC ATTACK

As the macOS user base expands so does the need for heightened vigilance against evolving threats. Based on our telemetry data, this briefing is a crucial help to understand the shifting threat landscape for macOS devices. It explores the evolving tactics cybercriminals are deploying to target Apple users and provides a glimpse into the future security challenges we may face.

Trojan, Adware & PUP Proportional Split



THE UBIQUITOUS TROJANS

Last quarter underscores the concern about the escalation of Downloaders on macOS devices. Cleverly disguised in various convincing forms to piggyback malware and install further threats has surged, accounting for over half of all detected trojan activity.

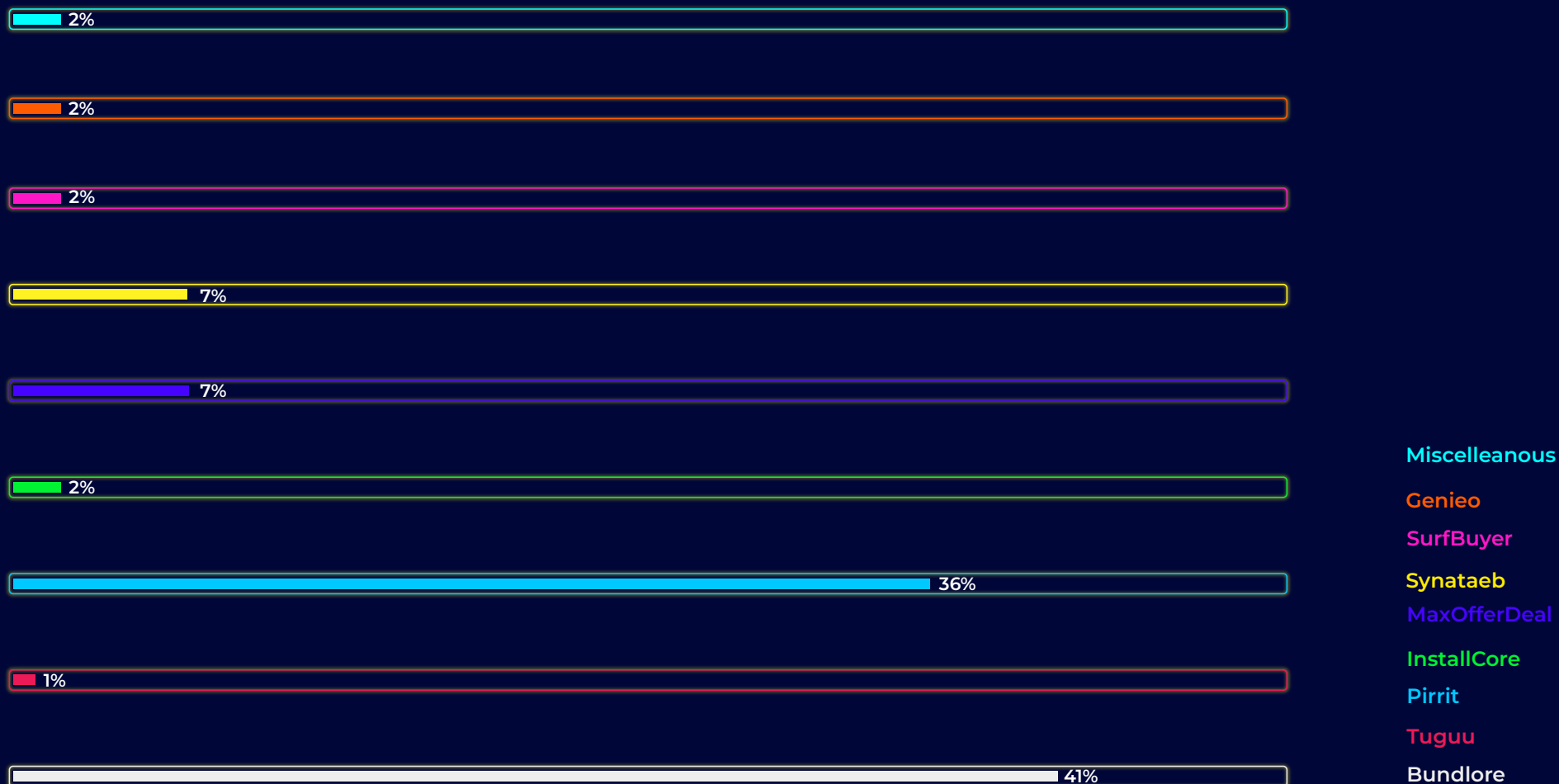
Trojan Detection Trend Line



THE ADWARE BROUHAHA

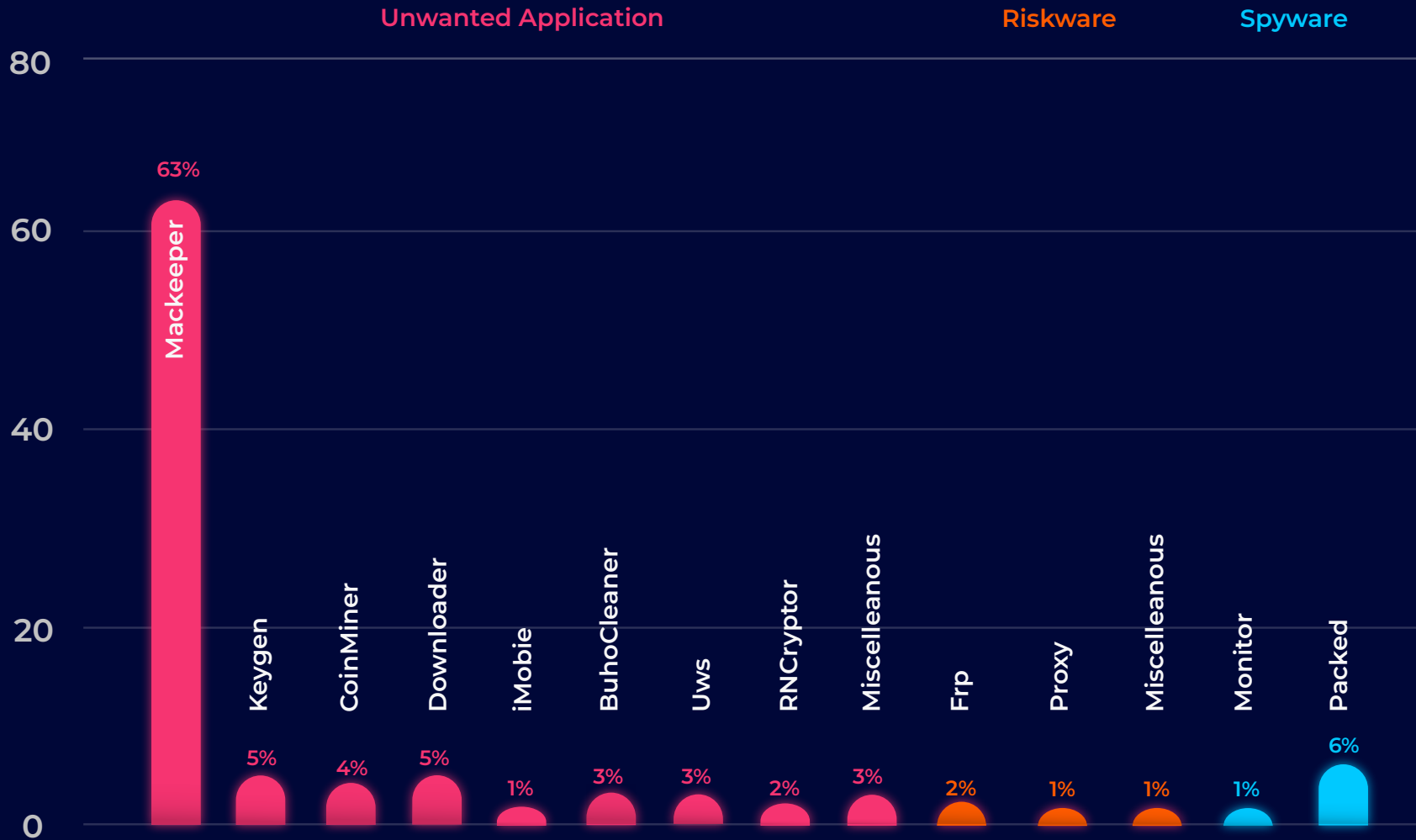
In the ever-evolving landscape of macOS cybersecurity, two formidable threats-Bundlore and Pirrit-have emerged as the primary culprits in last quarter's surge of adware attacks. Together, these entities command a significant portion of the threat surface and pioneer sophisticated techniques for infiltrating and disrupting user experiences.

The Trend Line of Adware Variant Detections



Last quarter, MacKeeper significantly dominated the macOS Potentially Unwanted Programs (PUP) landscape, a name that has become synonymous with users' challenges. This prevalence is attributed to its aggressive marketing tactics and the blurring lines between utility and intrusion, making it a central figure in our analysis.

Most Prevalent PUP Types





SAFETY GUIDELINES

- Keep your macOS updated and patched against the latest vulnerabilities
- Ensure scanning all your applications even if it is being downloaded from the official App Store
- Install a reputable security product like "K7 Antivirus for Mac" and keep it updated to protect yourself from the latest threats

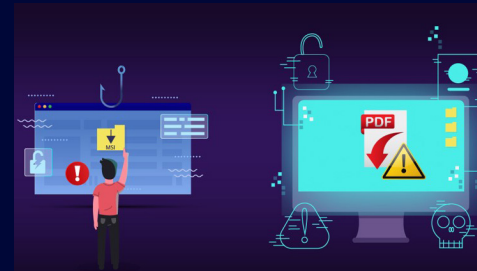
LATEST SECURITY NEWS

This section is a round up of the latest threats to the cyber world.

Resurgence of Qakbot

Qakbot is a banking Trojan that steals sensitive data. It has reappeared again, a few months after disruption, with phishing emails as the modus operandi. This malware was seen to specifically target the hospitality sector.

For more details refer [Qakbot Returns](#)



Ransomware in Python's flavour

Threat actors are targeting users with malware such as ransomware to encrypt their data and demanding a huge sum of money for getting their data back. Of late, they are using scripting languages like Python to develop malicious code, marking the rise of scripted ransomware.

Refer [Python's Byte: The Rise of Scripted Ransomware](#) for details



Phony SMS on the rise

Cybercriminals have been tricking users into downloading fake mobile apps by sending them phony text messages. This eventually compromises devices' security leading to stolen personal data and credit card information.

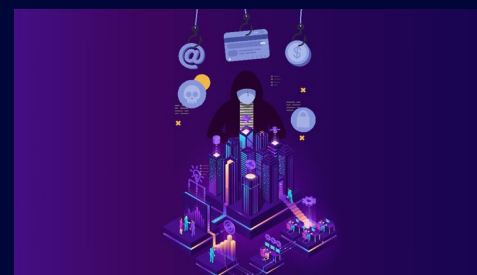
Refer [Suspicious Text Messages Alert](#) for more info



Last year's noteworthy Vulnerabilities

An organization's security posture is rated by the number of unpatched vulnerabilities it has. K7 Labs lists the most significant vulnerabilities of 2023 that have been exploited in the wild.

Click [2023 Top Vulnerabilities](#) for details



Subscribe to our [K7 Labs Technical Blogs](#) to know more about the latest happenings in cybersecurity.



KEY TAKEAWAYS

In the face of escalating cyber threats, it's imperative for both individuals and organizations to fortify their digital defenses. From enhancing security postures to investing in education and reputable security solutions, the necessity to protect data against a spectrum of established and emerging threats cannot be overstated. This approach is not merely preventive but essential for maintaining the integrity and trustworthiness of digital infrastructures in an era marked by relentless cyber assaults.

Enterprise

Secure your devices by keeping them up-to-date, patched against the latest vulnerabilities, and protected by up-to-date, high-quality security software such as K7 Endpoint Security

Empower employees with regular, updated training on recognizing and responding to cyber threats, emphasizing the importance of security best practices

Encrypt and backup your sensitive and critical data

Consumer

Secure your devices with a reputable security product such as K7 Total Security for Windows, K7 Antivirus for Mac, and K7 Mobile Security (Android and iOS), and keep them up-to-date

Enabling MFA adds an extra layer of security to your accounts, significantly reducing the risk of unauthorized access

Educate yourself on the latest malicious schemes and practice cautious online behaviour, such as verifying emails and avoiding clicking on suspicious links

Q4

2023-24

Copyright © 2024 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.