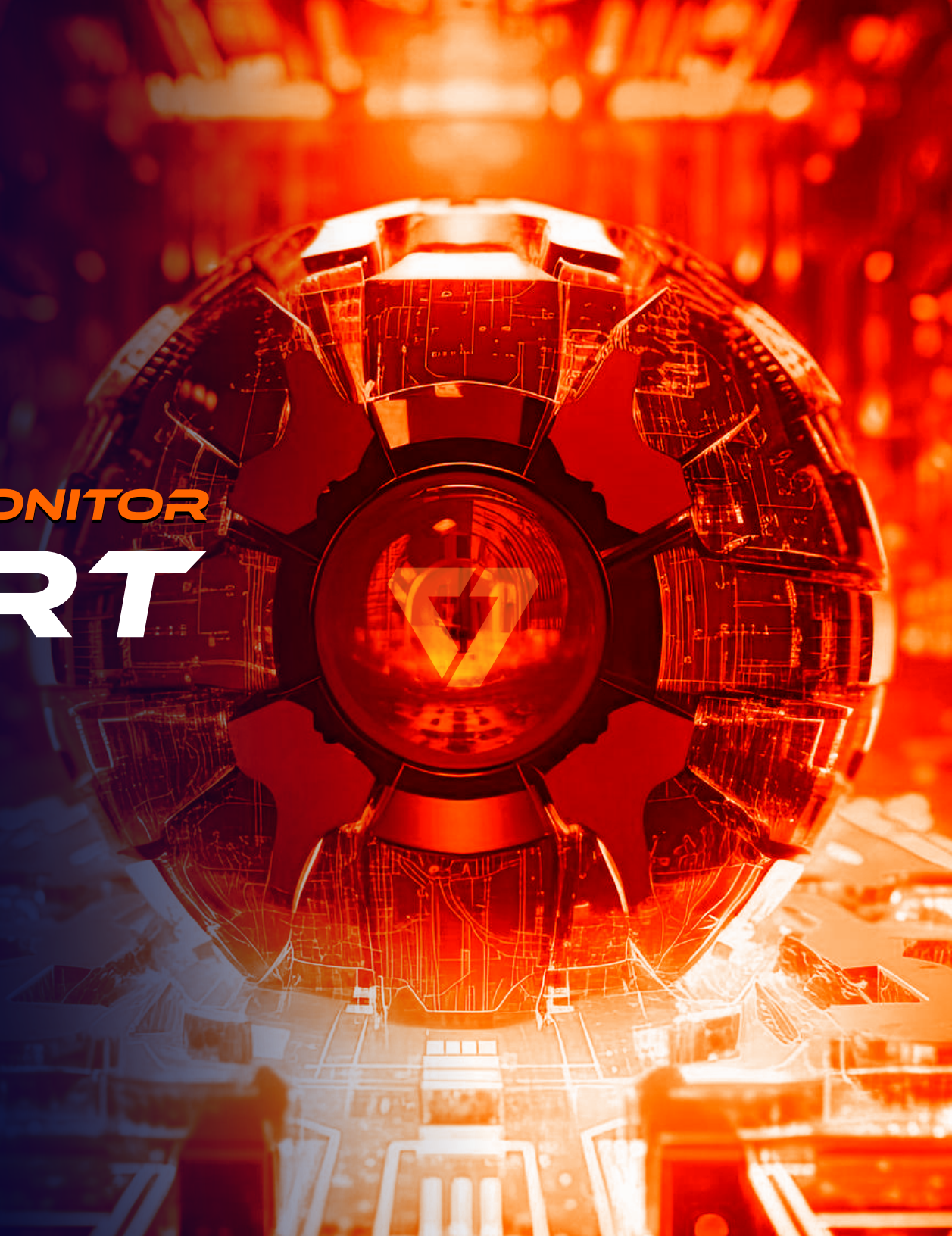
K7 SECURITY

CYBER THREAT MONITOR REPORT

Q2_2023-24



www.k7computing.com

CONTENTS

UNDERSTANDING THE CYBER THREAT LANDSCAPE

Digital interconnectedness acts like a double-edged sword. Even though it offers unprecedented opportunities across sectors, it has also widened the lid of Pandora's box for both the existing and budding cybercriminals, making things more effortless than ever while launching a cyberattack.

Take the Ransomware-as-a-Service (RaaS) model as an example. The volume of infrastructure, intelligence, time and workforce required for executing a sophisticated ransomware attack is quite impossible for an amateur in this field. Making things easy for them, ransomware groups launched RaaS to ease out the process and victimise more.

For instance, Cl0p and Lockbit ransomware groups, not only executed several significant attacks that are capable of shaking the industry, but they have also garnered hundreds of affiliates and enough intelligence to spot the latest glitch and zero-days to ensure that thwarting the onslaught remains a pipe dream for many.

Moreover, the prevalence of nation-state-sponsored cyber attacks adds a geopolitical layer to the threat landscape. Countries engage in cyber warfare, using sophisticated techniques to infiltrate adversaries' networks, steal sensitive information, or disrupt essential services.

To confront the onslaught, enterprise and MSMEs requires a multifaceted approach. As our digital realm continues to evolve, so must our awareness and defences against the ever-shifting sands of cyber threats.

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!

CYBER THREAT MONITOR - INDIA

Map for illustrative purposes only. Not to scale.

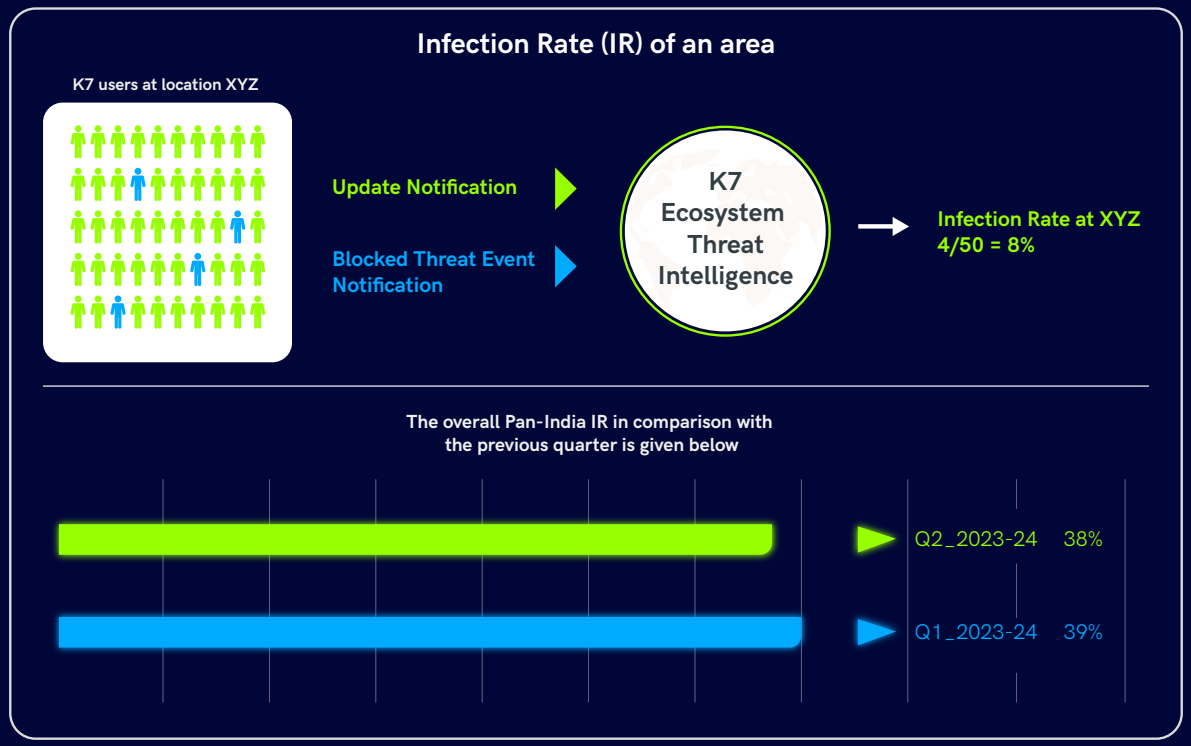
REGIONAL INFECTION PROFILE

Irrespective of its type, a security breach is a thing to worry about in every aspect of our digital life. And that's precisely what our infection rate indices indicate.

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.

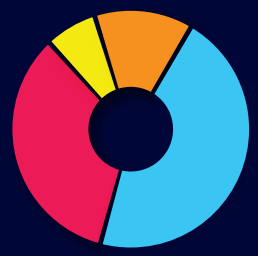
The concept of Infection Rate is better explained by the below picturization.



The slight reduction in the infection rate doesn't intend a much safer digital experience. This could be attributed to incidents not reported and products not activated/ updated.

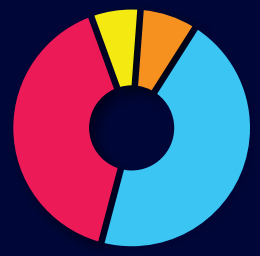
Before we delve into the threat landscape for the last quarter, we present to you a few significant IRs across metros classified based on the different levels at which the threats were blocked.

THE METRO AND TIER-1 CITIES - INFECTION RATE



34%
7%
13%
46%

Ahmedabad
36%



40%
7%
7%
46%

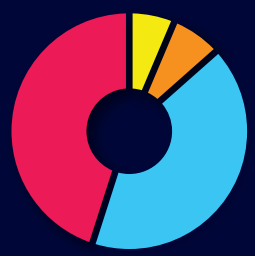
Bengaluru
31%

42%
6%
7%
45%

Chennai
35%

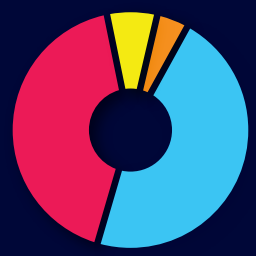
40%
8%
6%
47%

Delhi
34%



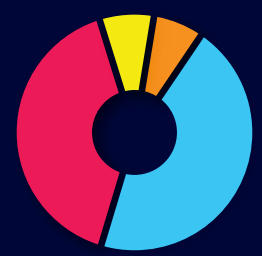
46%
6%
7%
41%

Hyderabad
36%



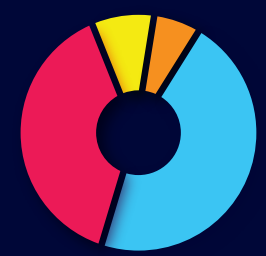
42%
7%
4%
46%

Kolkata
35%



41%
8%
6%
46%

Mumbai
32%



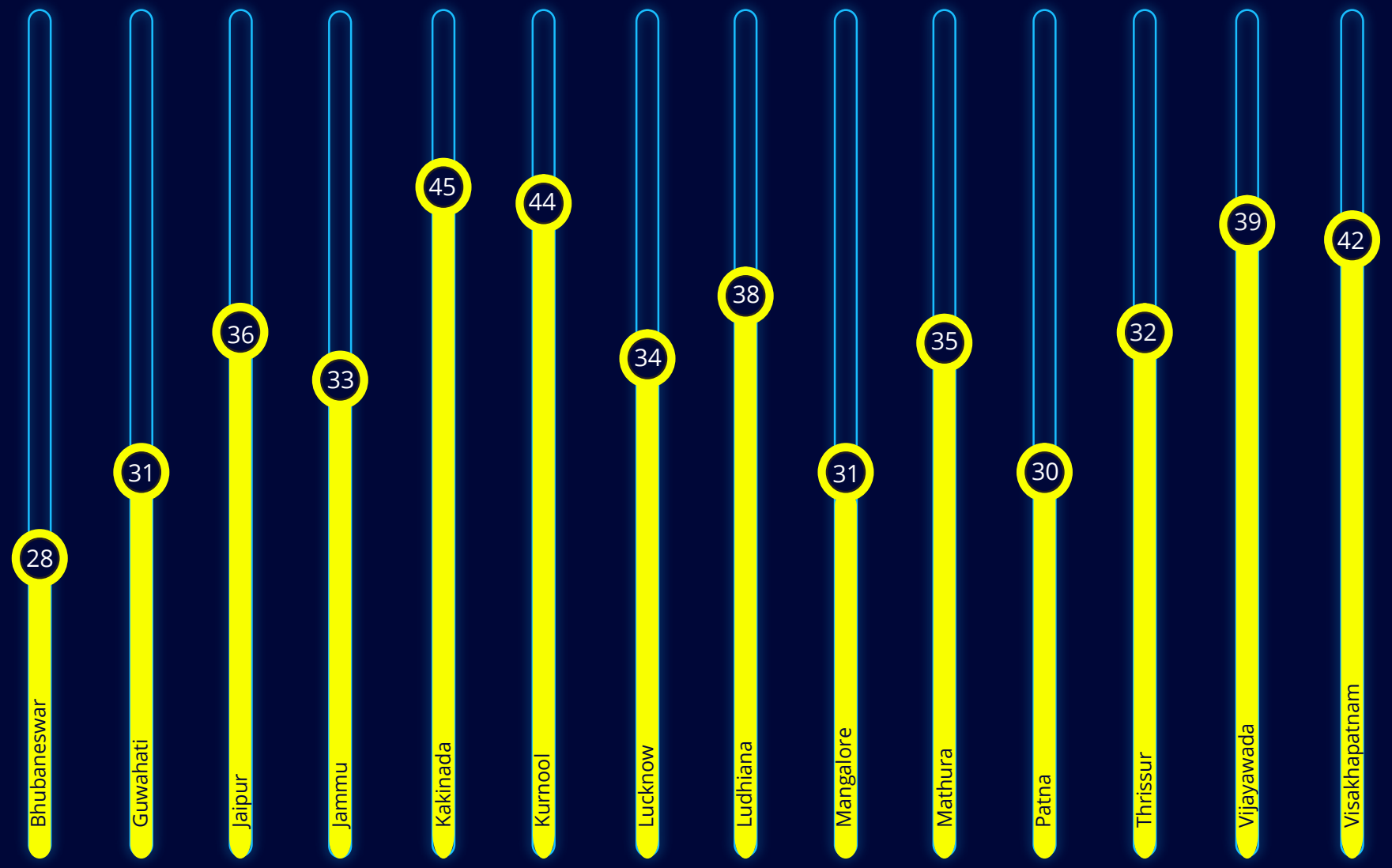
40%
8%
6%
47%

Pune
31%

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

TOP INFECTION RATES IN TIER-2 CITIES

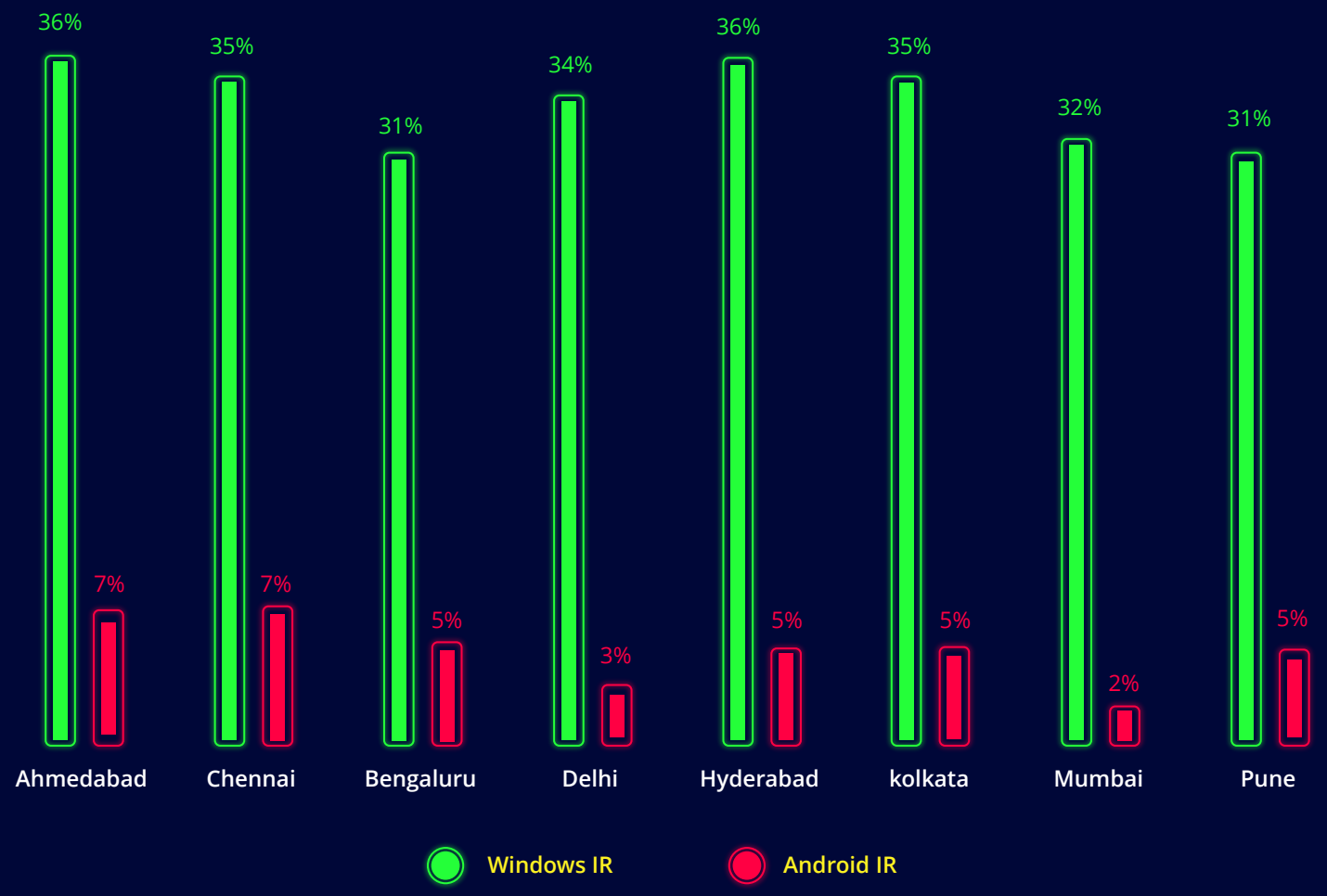
Now let us look at the risk factor of netizens in the Tier-2 cities.



INFECTION RATE COMPARISON ACROSS PLATFORMS

The attack percentage on the Windows platform is way higher than on Android because of its vast user base, However, K7 Labs researchers continue to see a spurt in attacks on the mobile platform too, not too significant because of a comparatively smaller user base.

Windows IR vs Android IR



ENTERPRISE INSECURITY

PowerShell is a widely used command-line tool and scripting language that system administrators use to automate tasks and manage systems. However, it is also being used by threat actors to launch attacks.

Threat actors prefer PowerShell as it is easier to deploy a fileless attack/infection which makes it harder to detect as it can execute commands, scripts and binaries directly in memory. Also, it can establish remote connectivity on nearly any Windows device.

Recently one of our enterprise clients was a victim of ransomware attack wherein threat actors used PowerShell as their attack vector.

SAFETY RECOMMENDATIONS

- Enforcing least privilege access
- 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

Unpatched software leaves your devices vulnerable to known bugs. Also, it becomes easier for threat actors to infiltrate your organization's network, deploy malware, gain unauthorized access and steal data of critical and sensitive nature.

A few significant vulnerabilities that have been exploited in the wild have been listed below.

Security Bypass Vulnerability in Microsoft Applications

Using **CVE-2023-35311,** an adversary tricks an user into clicking on a malicious URL bypassing Microsoft Outlook Security Notice prompt.
Vulnerable products include

- Microsoft Outlook 2013, 2016
- Microsoft Office 2019, 2021
- Microsoft 365 Apps

Using **CVE-2023-32049,** an adversary tricks an user into clicking on a malicious URL bypassing Open File - Security Warning Prompt..
Vulnerable products include

- Windows 10, 11
- Windows Server 2016, 2019, 202

Untrusted Data Vulnerability in Adobe ColdFusion

CVE-2023-26359, results in code execution in the context of the current user.
Vulnerable product versions include

- Below ColdFusion 2018 Update 16
- Below ColdFusion 2021 Update 6

WinRAR ZIP file Processing Vulnerability

CVE-2023-38831, allows remote attackers to spread malware by crafting ZIP archives that serve as carriers for various malware families.
Vulnerable product versions include

- Below WinRAR 6.23

Heap Based Buffer Overflow Vulnerability in Google Chrome

CVE-2023-4863 in Google Chromium WebP Codec allows a remote attacker to perform an out-of-bounds memory write by using a crafted HTML page.

Vulnerable product versions include

- Google Chrome for Mac and Linux < 116.0.5845.187
- Google Chrome for Windows < 116.0.5845.188

DANGERS IN THE INTERNET OF THINGS

IoT devices are particularly vulnerable to data theft primarily because most of the devices do not encrypt data during transit or storage. This implies that threat actors can easily steal user's credentials and other sensitive information transmitted to and from the device.

RCE Vulnerabilities in Apple Products

CVE-2023-41604 leads to arbitrary code execution while processing a maliciously crafted image.
Vulnerable product versions include

- Below iOS 16.6.1
- Below iPadOS 16.6.1
- Below macOS Ventura 13.5.2

CVE-2023-37450 leads to arbitrary code execution while processing web content.
Vulnerable product versions include

- Below Safari 16.5.2
- Below iPadOS 16.6
- Below iOS 16.6
- Below macOS 13.5
- Below tvOS 16.6
- Below watchOS 9.6

Logic Error issue in Android Framework

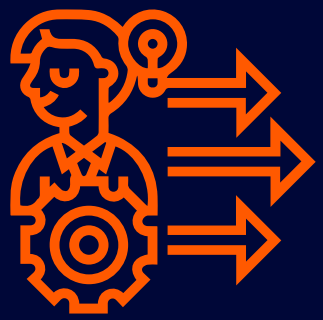
CVE-2023-35674 in onCreate function of WindowState.java in Android Framework launches a background activity which could lead to local privilege escalation with no additional execution privileges needed.

Vulnerable product versions include

- Android 11, 12, 12.1, 13

Authentication issue in Cisco's VPN feature

CVE-2023-20269, an improper separation of authentication, authorization and accounting in the remote access VPN feature of Cisco Adaptive Appliance Software and Cisco Firepower Threat Defense Software, allows an unauthenticated, remote attacker to perform a brute force attack in an attempt to identify valid username and password and establish a clientless SSL VPN with an unauthorized user.



MITIGATION TECHNIQUES

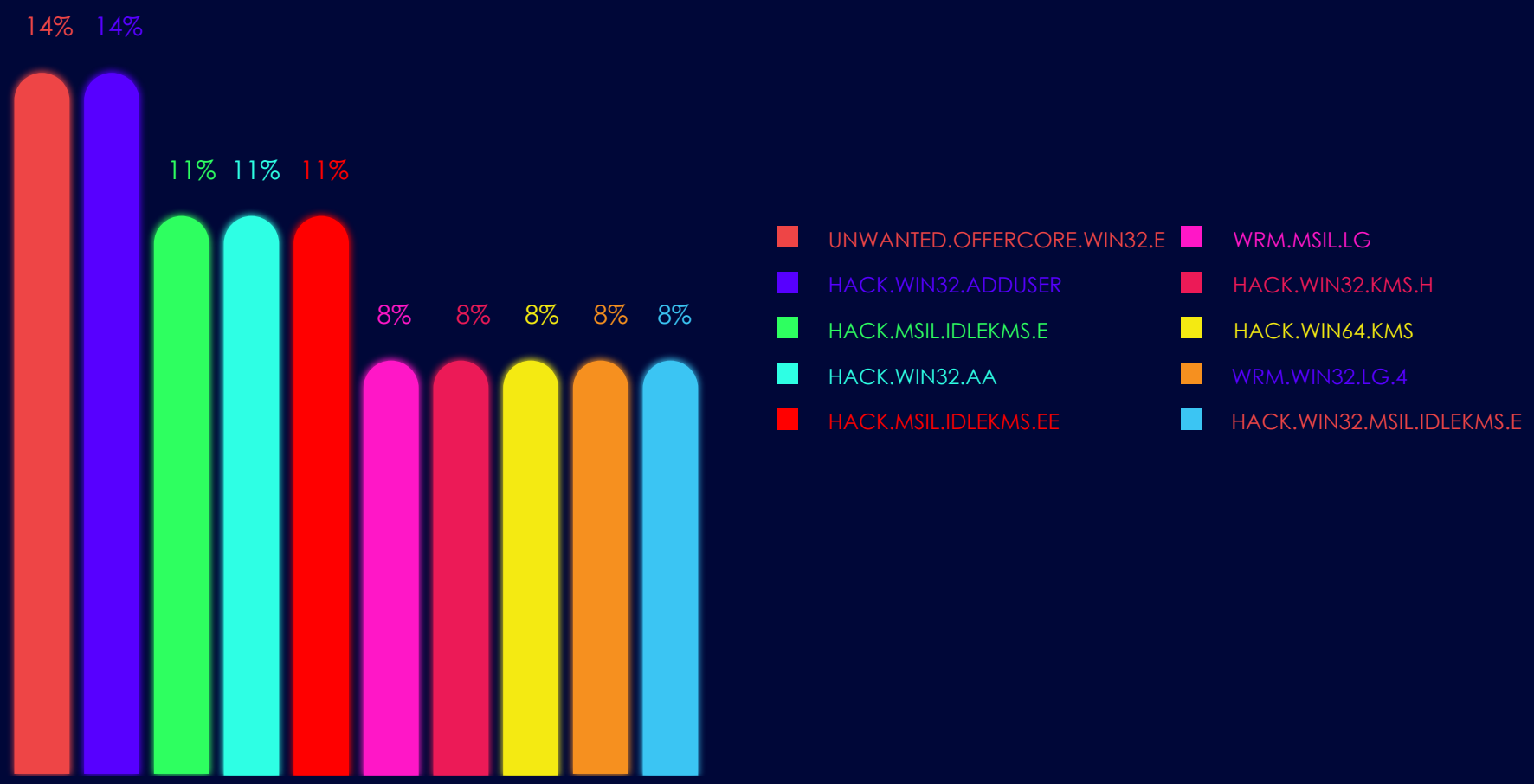
- Encrypt your connections
- Ensure you set a unique and strong password for each of your devices in the network
- Connect your devices to only a secure and trusted network

WINDOWS UNDER SIEGE

Windows Malware Type Breakdown

Being the most used platform on earth, it always bears the brunt of novel attack methods. Also, most of the time, the applications that users download are via a standard internet browser, a connection which is more vulnerable to attacks.

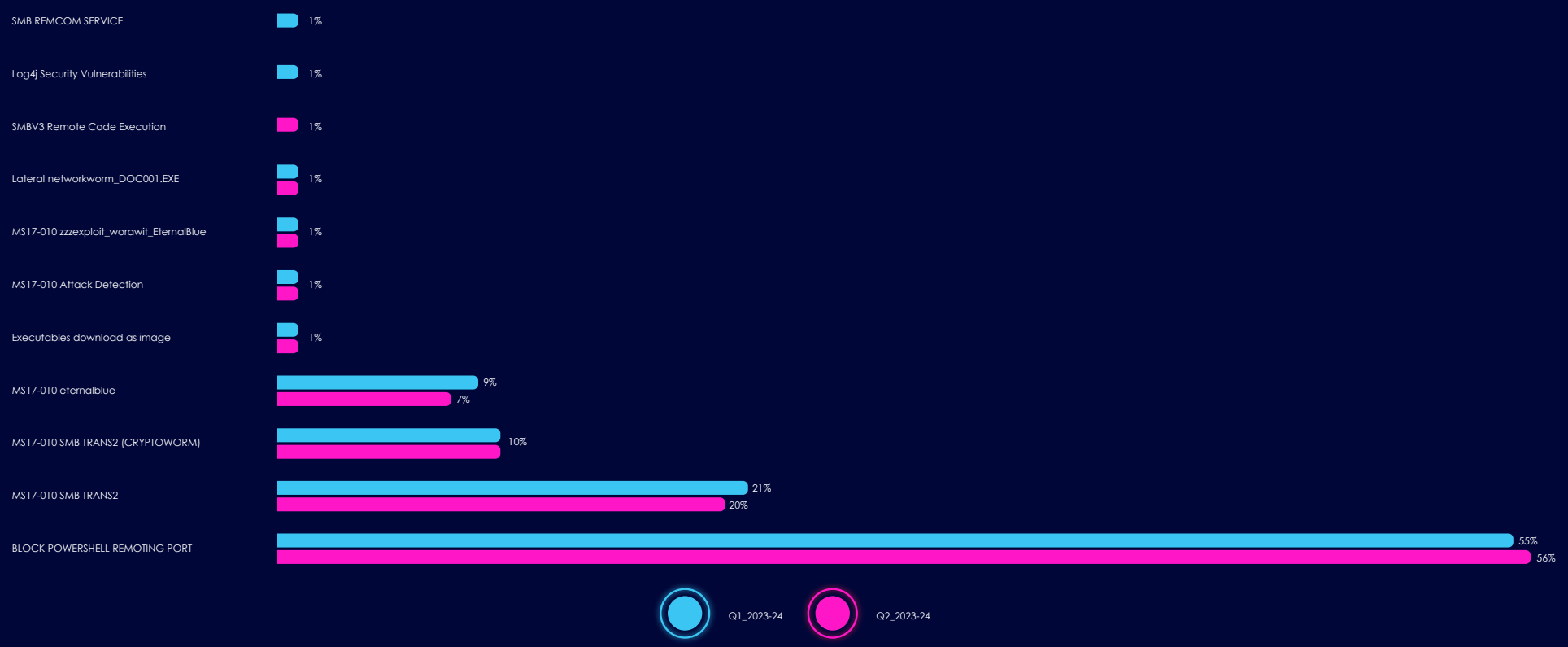
Split of Windows Top 10 Detections



WINDOWS EXPLOITS

Since Windows has a larger market share, it is a bigger target for threat actors. PowerShell has been exploited the most. Being the popular built-in command-line tool in Windows, it allows extensive functionality and flexibility, allowing adversaries to execute complex scripts and commands that can be obfuscated, making it harder for security tools to detect the malicious activity.

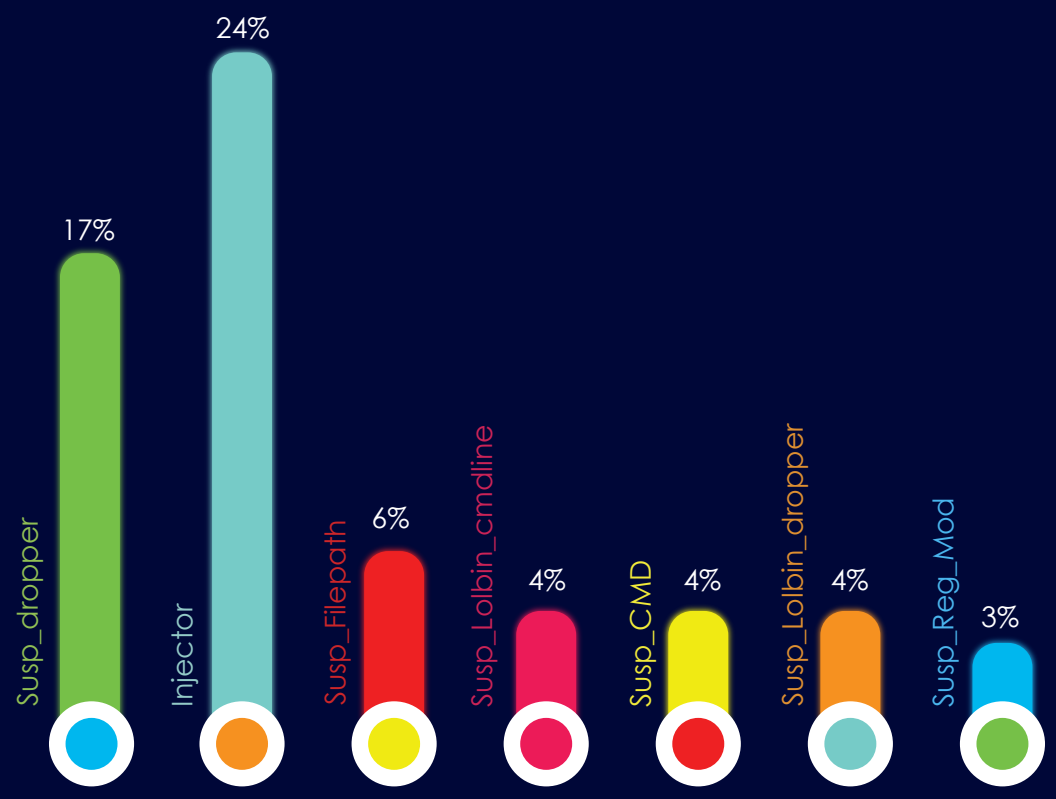
Most Prevalent Exploits



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



Droppers continued to occupy a significant chunk followed by Injectors - malware that use legitimate file names or locations to hide behind trusted names so as to evade detection. Droppers are used by threat actors in multi-stage attacks where additional malicious payloads are downloaded or dropped. 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. Registry modifications are done by threat actors for persistence and execution of malware.

MITIGATION TIPS

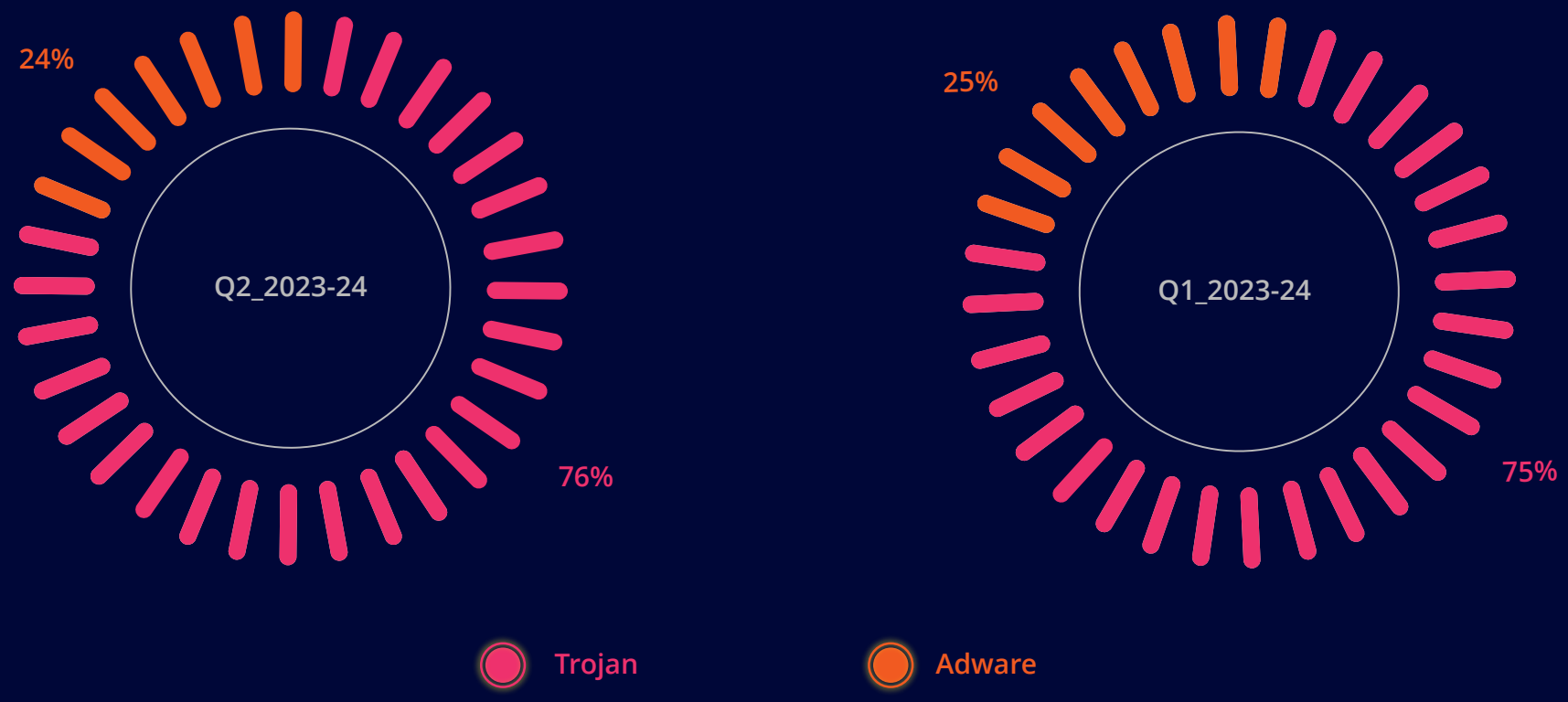
- Use an account without administrator privileges wherever possible
- Set up your operating system to enable auto-updates by default
- Backup your data on a regular basis

THE MOBILE DEVICE STORY

The unstoppable growth of malware in the mobile space is primarily because of the rise in apps catering to various needs of a smartphone user. Threat actors make use of this opportunity to target victims with fake and trojanized versions of the original apps raising grave concerns about data security and user privacy.

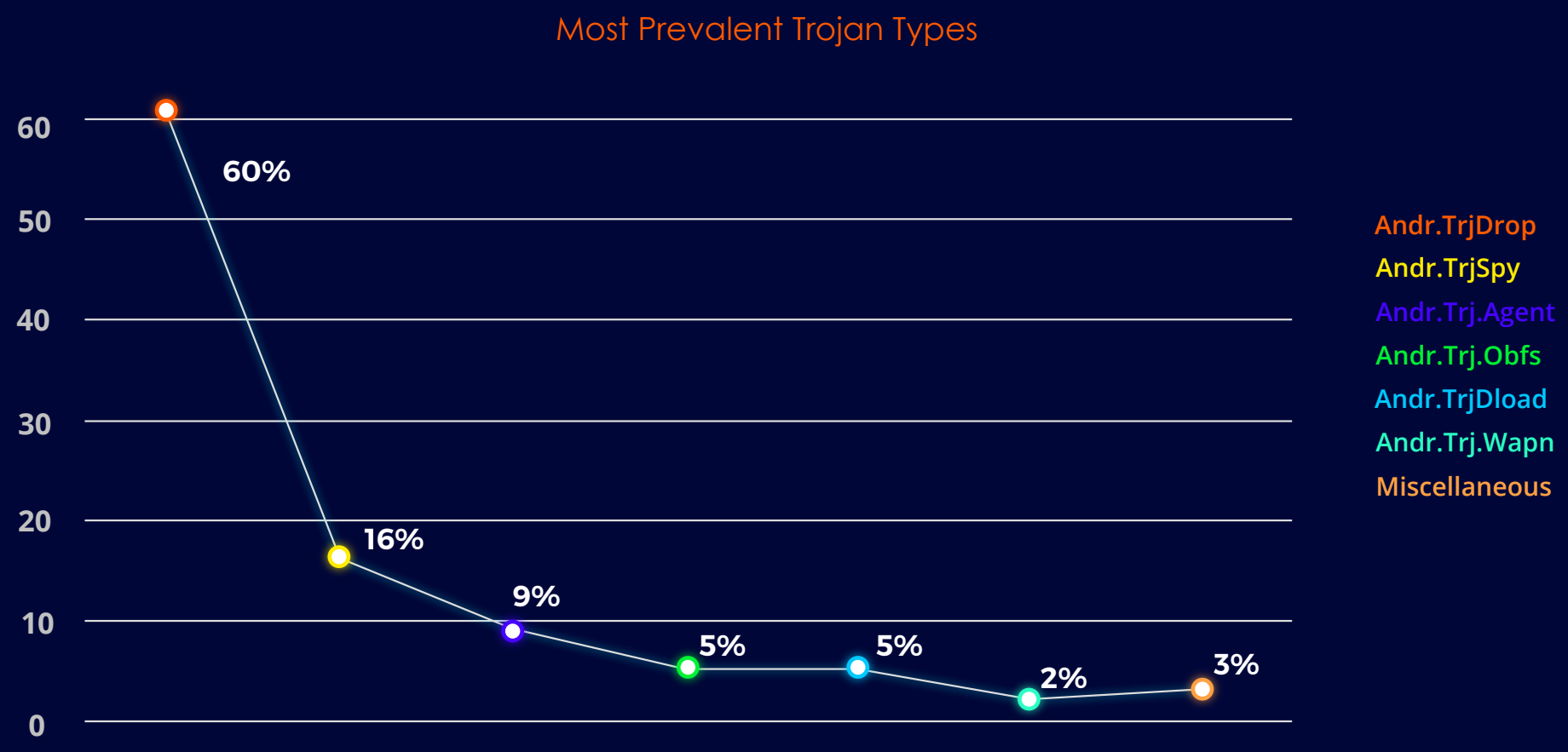
However, the astounding growth of such perilous activities doesn't hint at any decline in adware's existence.

Adware vs Trojan Proportional Split



THE OMNIPRESENT TROJAN

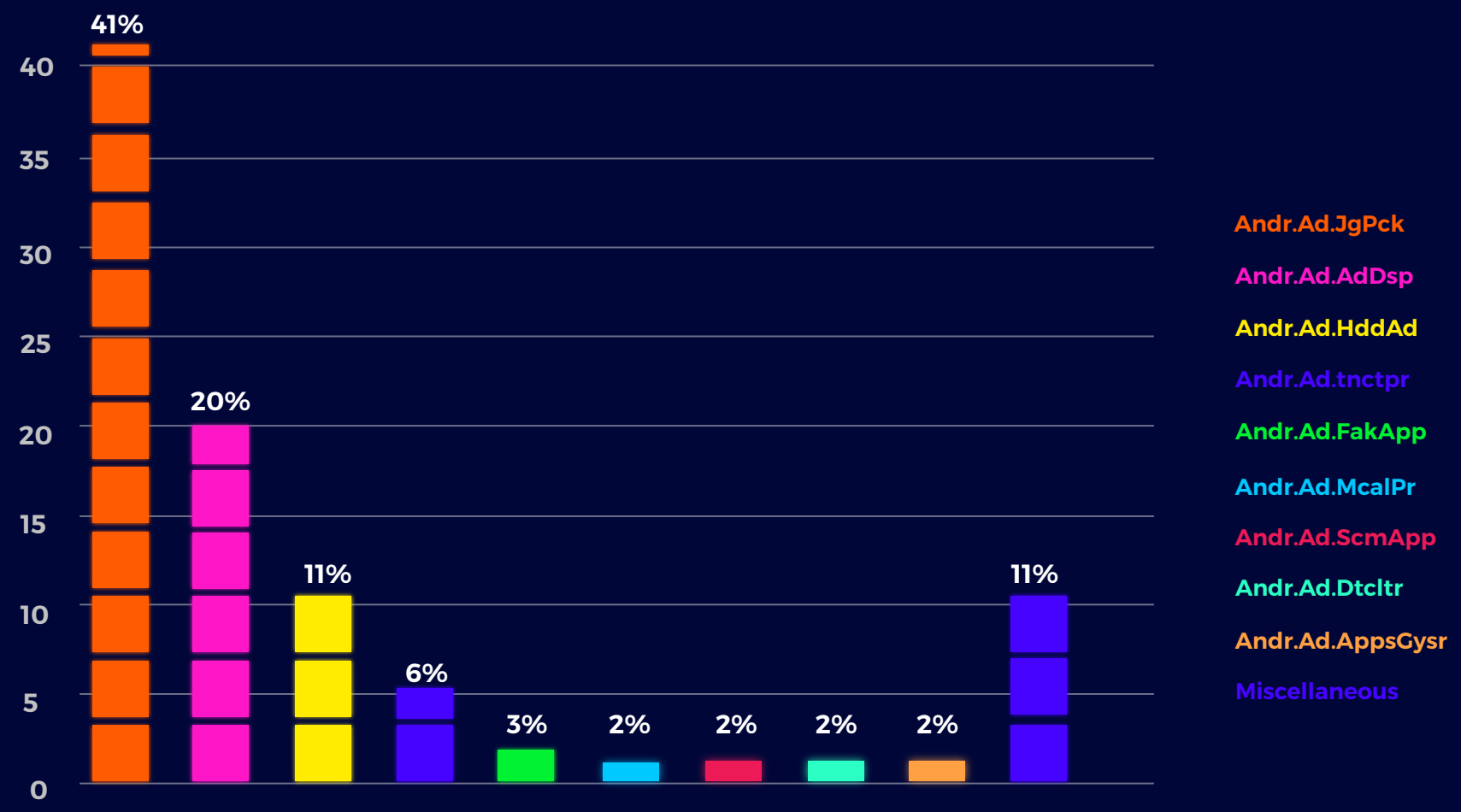
The most noticeable observation in this quarter was the mushrooming of spyware activities even after Trojan droppers retained their massive presence in the mobile threat landscape.



THE ADWARE SAGA

Last quarter too, saw the prevalence of existing adware families like Andr.Ad.JgPck, Andr.Ad.AdDsp, and Andr.Ad.HddAd.

Trend Line Showing the Adware Plague



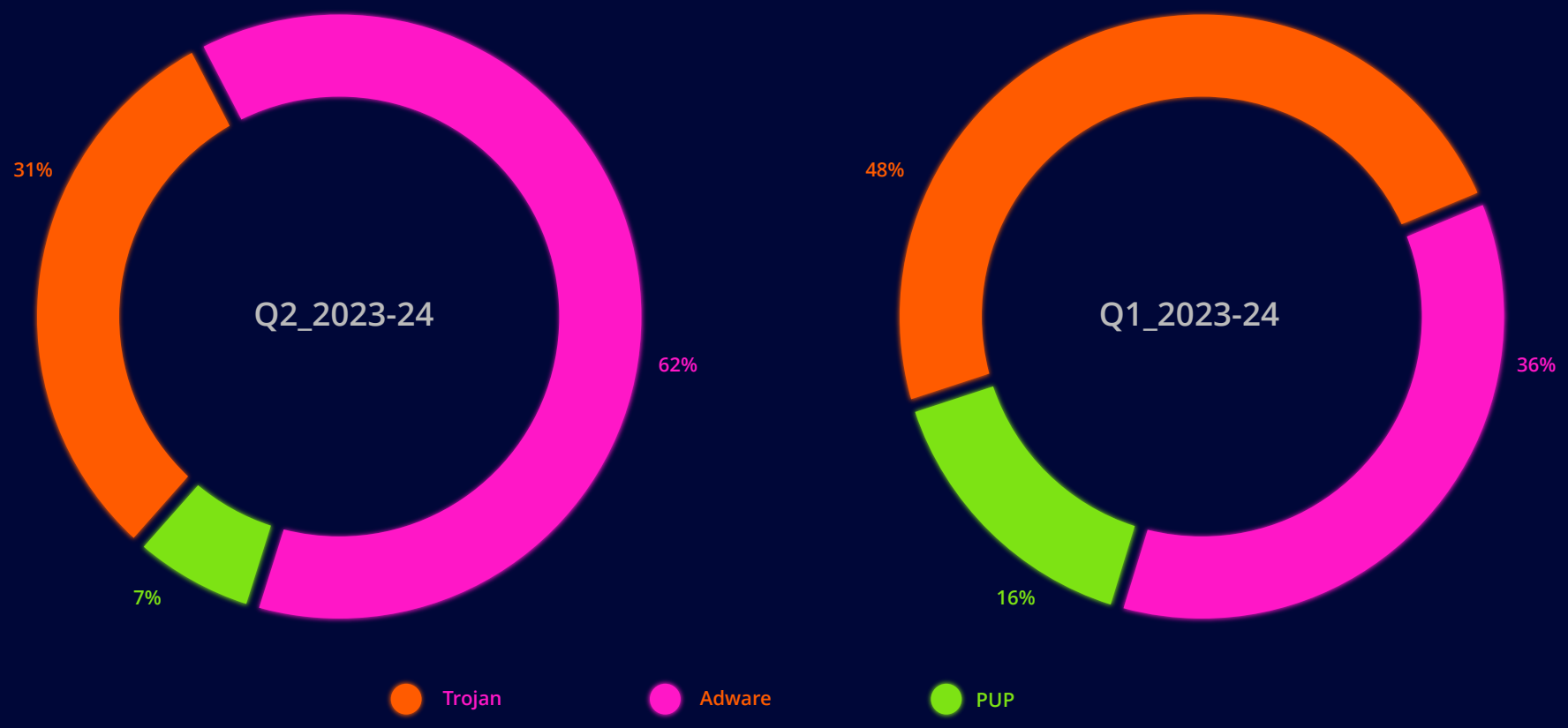
TIPS TO STAY SAFE

- 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

Threat actors are focusing more and more on the macOS space due to the rising popularity of Apple products. Mac users, most of them from high income groups, have a lot of personal and financial information which is an attractive target for threat actors, considering the monetary and reputational loss that can be created because of a data breach.

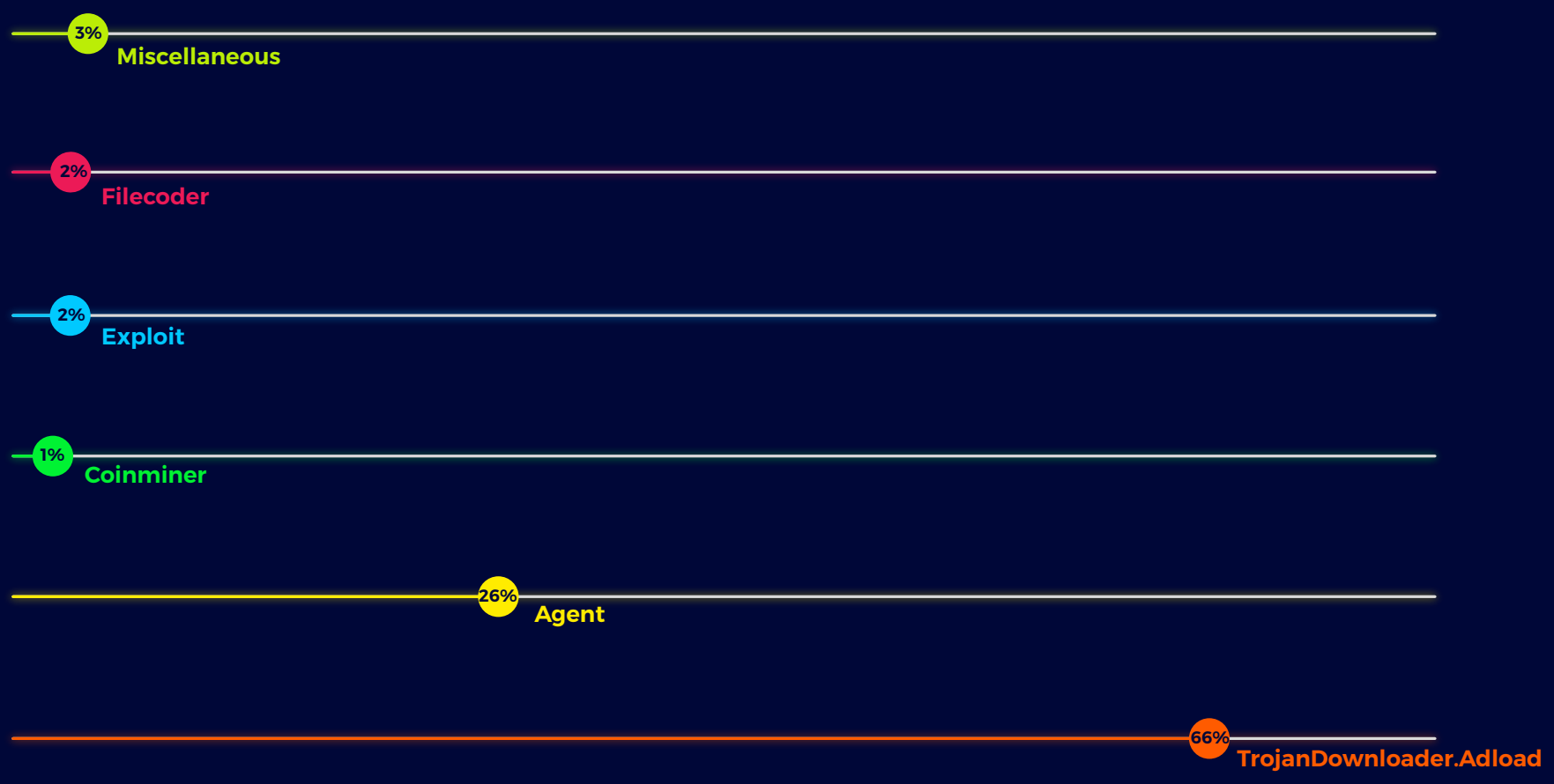
Trojan, Adware & PUP Proportional Split



THE UBIQUITOUS TROJAN

Even though the presence of trojans has shrunk significantly in contrast to the previous quarter, there is still a high number of popular trojan types in the macOS threat landscape.

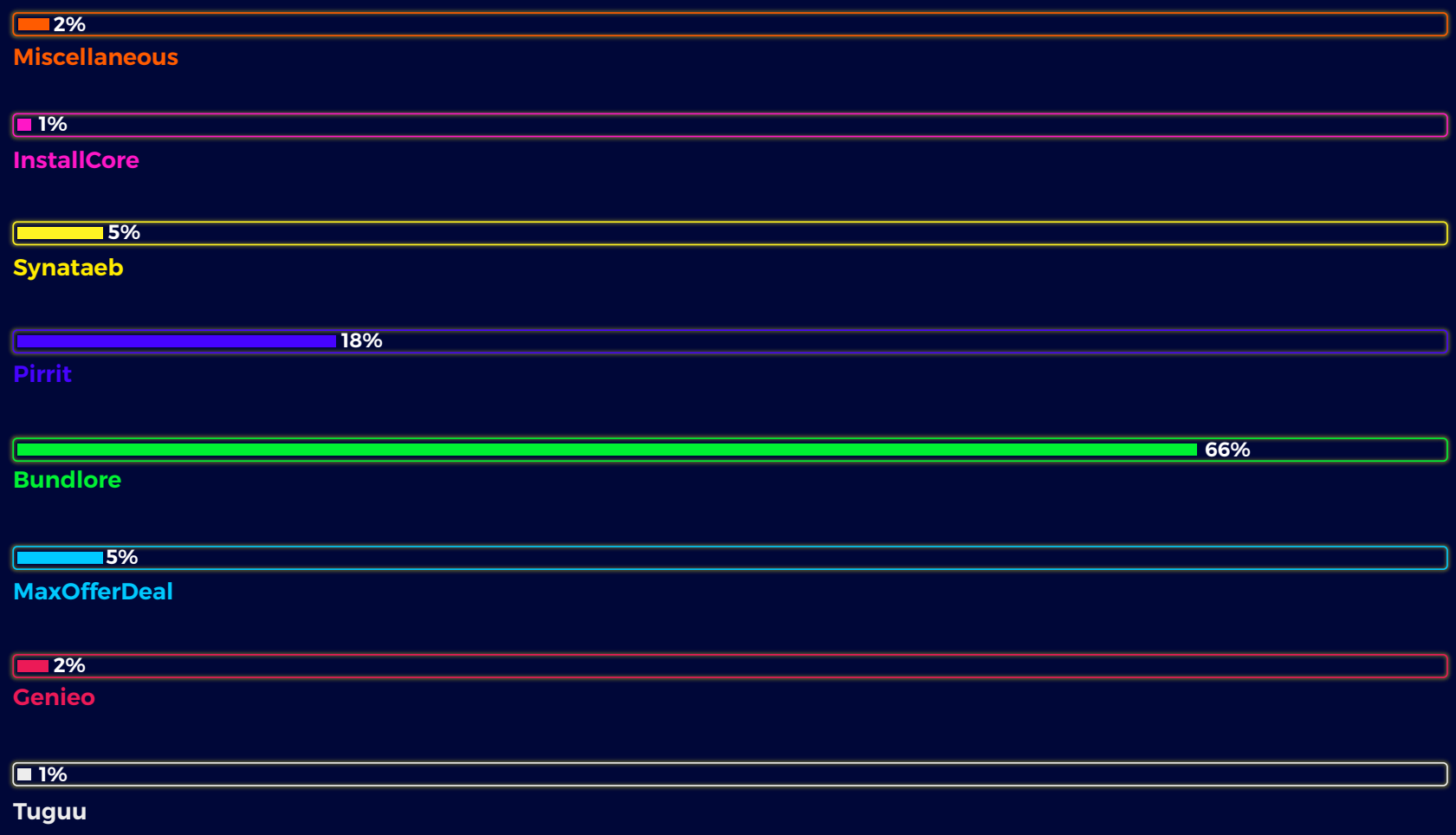
Trojan Detection Trend Line



THE ADWARE UPROAR

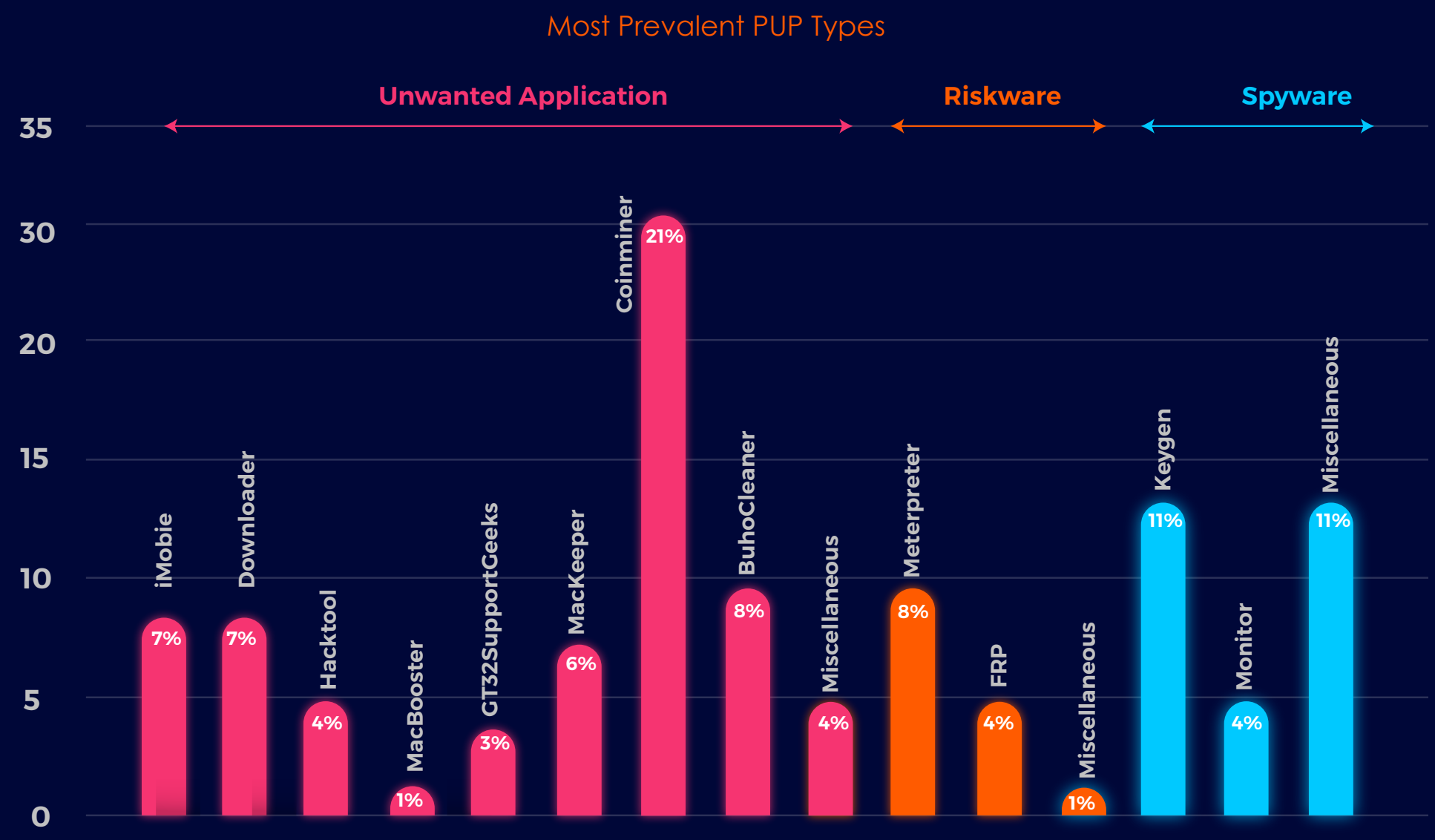
Interestingly, two seasoned adware families, Bundlore and Pirrit, maintain their significance, resulting in more adware attacks on macOS users.

The Trend Line of Adware Variant Detections



THE SIGNIFICANCE OF PUPS

Last quarter saw a significant rise in riskware and spyware in spite of PUPs diminishing trend in comparison to trojans and adware.



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

BLOG DIGEST

This report also includes a summary of some of the prominent blogs published in the last quarter.

CLOP Ransomware seen exploiting CVE-2023-34362

A vulnerability in the MOVEit file transfer application, which enables secure transfer of files between organisations and their customers using SFTP, SCP and HTTP-based uploads, allows an adversary to gain administrative access, exfiltrate data and execute arbitrary code.

CLOP ransomware group has been exploiting this across high-profile government, finance, media, aviation and healthcare organisations.

Akira Ransomware muddling with Linux

This blog is about a cross-platform ransomware dubbed Akira, that spreads across networks, targeting both Windows and Linux machines.

This threat group operates a Tor website inspired by a retro-themed aesthetic, where they publicly disclose the pilfered data if their ransom demands are not met. Moreover, their website also offers a chat feature, facilitating communication between the victims and the perpetrators, using the unique ID given in the ransom note.

Crypto Stealing Scams

This blog is about the Go language based malware, which is being used by threat actors these days as it is not only easy to code but also has a single codebase which can be used to generate multiple variants for multiple OSes, having the same base functionality. Also some features of this Go programming language makes its code difficult to reverse engineer.

Clip Banker, a Go malware, has been primarily used to steal cryptocurrency, particularly by using a Telegram bot. It operates stealthily, often infiltrating users' systems without their knowledge.

RomCom RAT: An Untold Anecdote

Threat actors behind RomCom, largely unattributed, have been active ever since Russia's invasion of Ukraine. RomCom RAT is a Remote Access Trojan, designed to take control of a victims' network by spoofing and deploying fake versions of legitimate applications on the victims' system so as to gain initial trust.

Reports reveal that there have been geopolitically-motivated attacks on Ukrainian military institutions and those countries supporting Ukraine, using this malware

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

KEY TAKEAWAYS

Businesses and consumers must be on guard against the growing number of attacks that leverage established and emerging threats. Training your staff and securing your endpoints will go a long way in protecting your organization from such threats .We recommend installing a reputable security product and following good cyber hygiene practices to help deter potential attackers.

Enterprise	Consumer
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	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
Conduct risk assessments on a regular basis	Only use the official app store for app downloads and installations
Encrypt and backup your sensitive and critical data	Keep your OS and software updated and patched against the latest vulnerabilities

K7 SECURITY

Q2

2023-24

OCTOBER 2023

www.k7computing.com