K7 SECURITY

CYBER THREAT MONITOR REPORT

Q1_2023-24

www.k7computing.com

CONTENTS

DIVING INTO THE CYBER THREAT ARENA

Organizations, especially after the pandemic, are going online with their operations and hybrid in their working style. Threat actors are also evolving their Tactics, Techniques and Procedures (TTPs) to keep pace with them and are launching various cyber attacks. This poses a challenge for organizations, as with the shift to remote work, it is becoming increasingly difficult for organizations to verify trusted connectivity, becoming a boon to threat actors.

There has also been a resurgence of ransomware in 2023 which has caused a huge data breach of sensitive and confidential data. And with the popularity of the ransomware-as-a-service (RaaS) model, there is a lot of opportunity for amateurs to work in this field in tandem. We recommend organizations patch vulnerabilities with urgency to minimize the attack surface.

There has also been an increase in WMI abuse by threat actors for its use in enterprise applications and administrative scripts. Therefore, organizations are requested to constantly monitor their threat environment, do a threat assessment periodically and mitigate any risks as and when noticed.

We at K7 Labs offer significant protection from emerging and latest threats at the earliest by closely examining and identifying such incidents and providing security at multiple layers.
Our quarterly reports list case studies that ignited our interest and were found worthy of sharing, threat scenarios across major Indian cities, significant vulnerabilities, top threats in Windows, Android, and macOS platforms, and relevant mitigation techniques.

This report explains the what and how of the topics under consideration without getting into deep technical details to suit a broad readership base. However, those interested in a more detailed analysis are more than welcome to read our K7 Labs' technical blogs.

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

CYBER THREAT MONITOR - INDIA

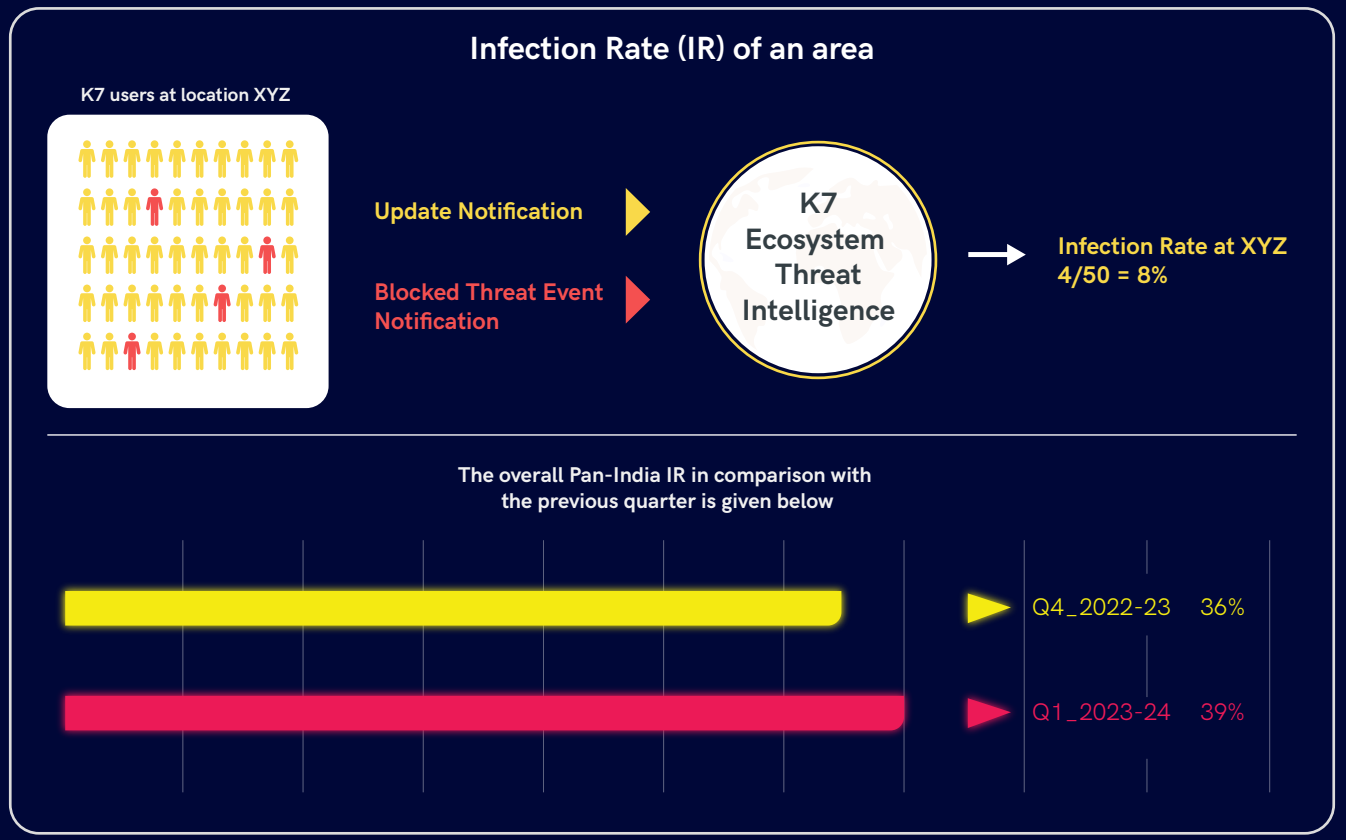
Map for illustrative purposes only. Not to scale.

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.

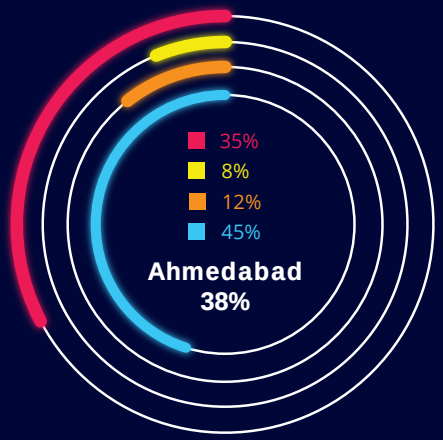
Those new to our quarterly report would need to understand an important concept called **"Infection Rate" (IR)** which is used **as the base for benchmarking a netizen's risk.**
We use this IR factor to identify the netizens' exposure to cyber threats. IR is determined as the proportion of K7 users in 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.

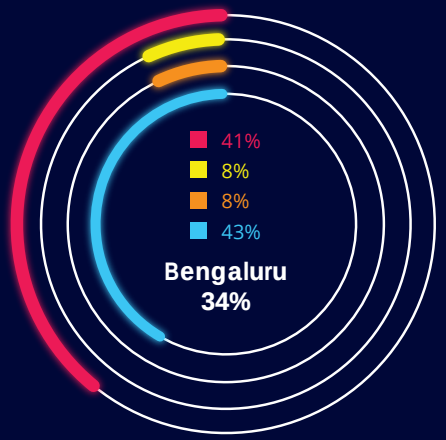
The concept of Infection Rate is better explained by the below picturization.

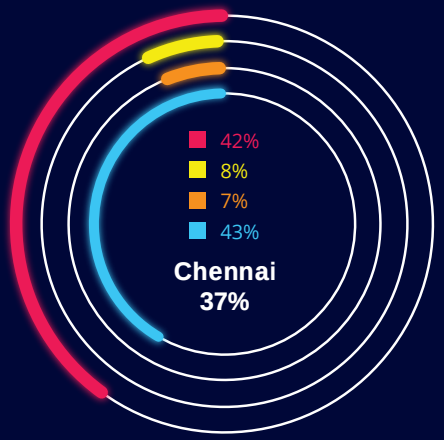


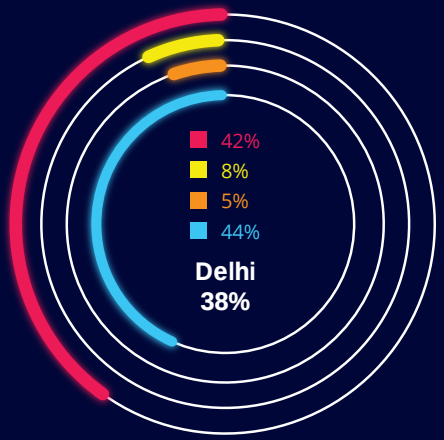
In recent months, there has been a significant surge in cyber-attacks across the globe. The abundance of potential targets, ranging from large corporations to government agencies, financial institutions, and even individuals, offers threat actors an ideal environment to exploit vulnerabilities and reap substantial gains.

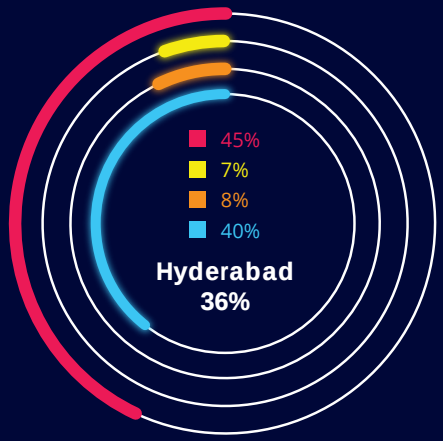
THE METRO AND TIER-1 CITIES - INFECTION RATE

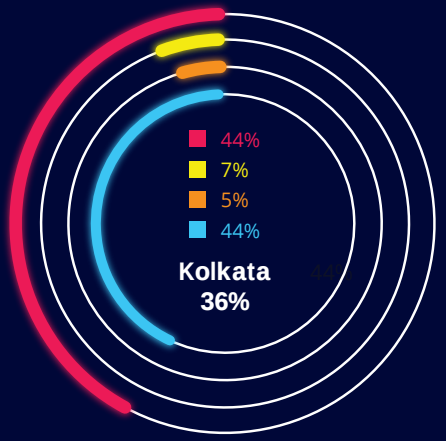


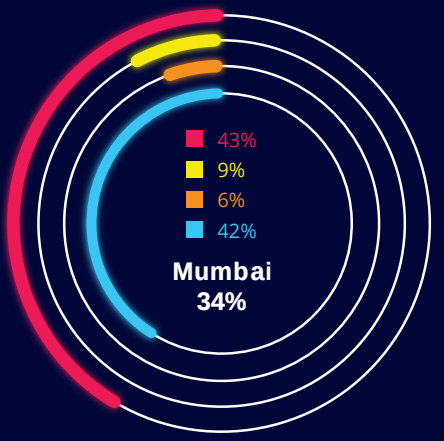


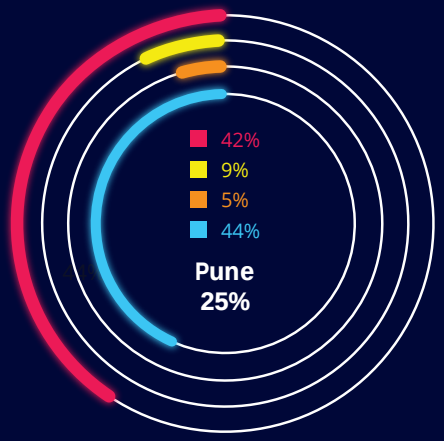






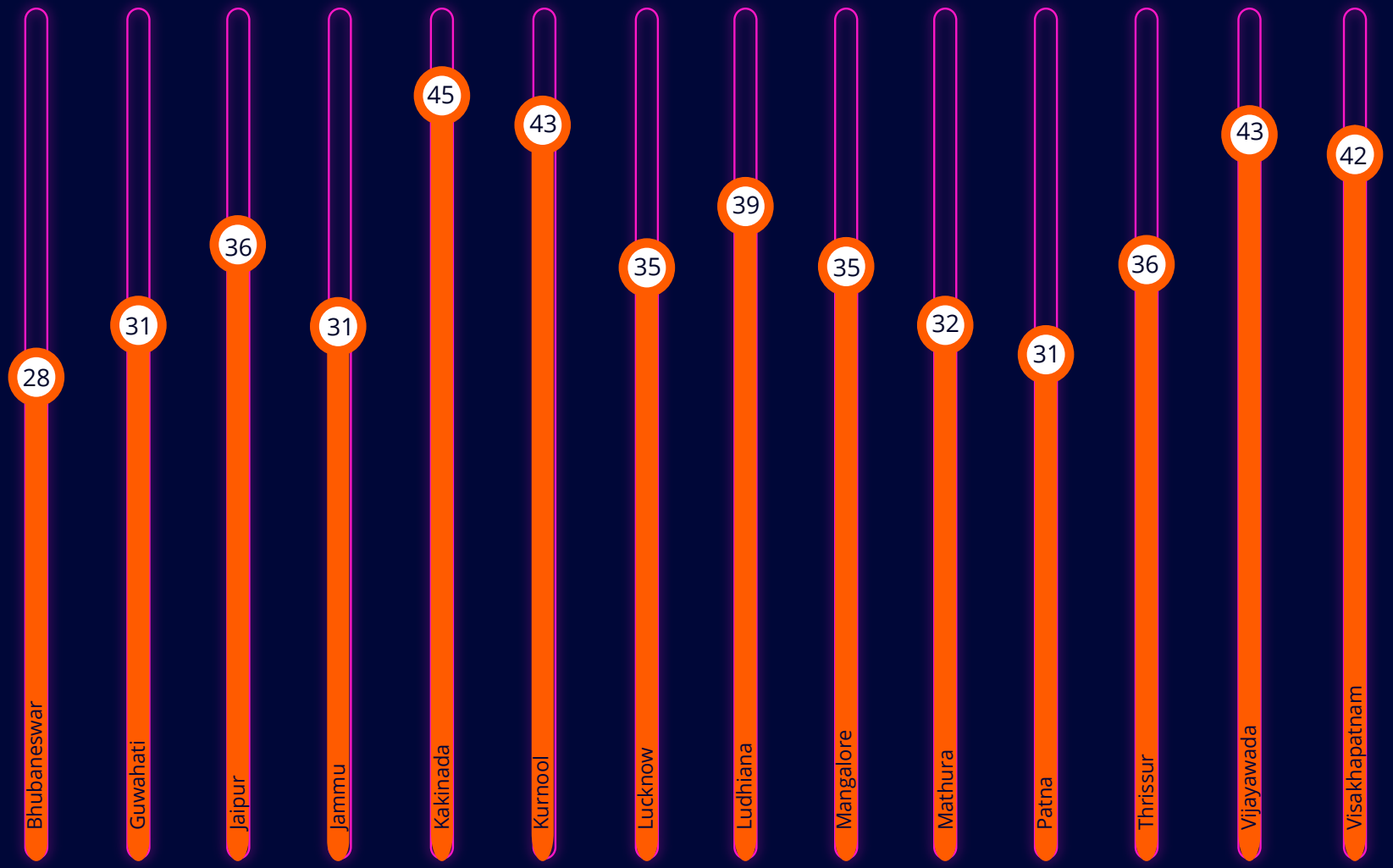






- Web Protection
- Firewall Protection
- Behaviour Protection
- ScanEngine Protection

TOP INFECTION RATES IN TIER-2 CITIES

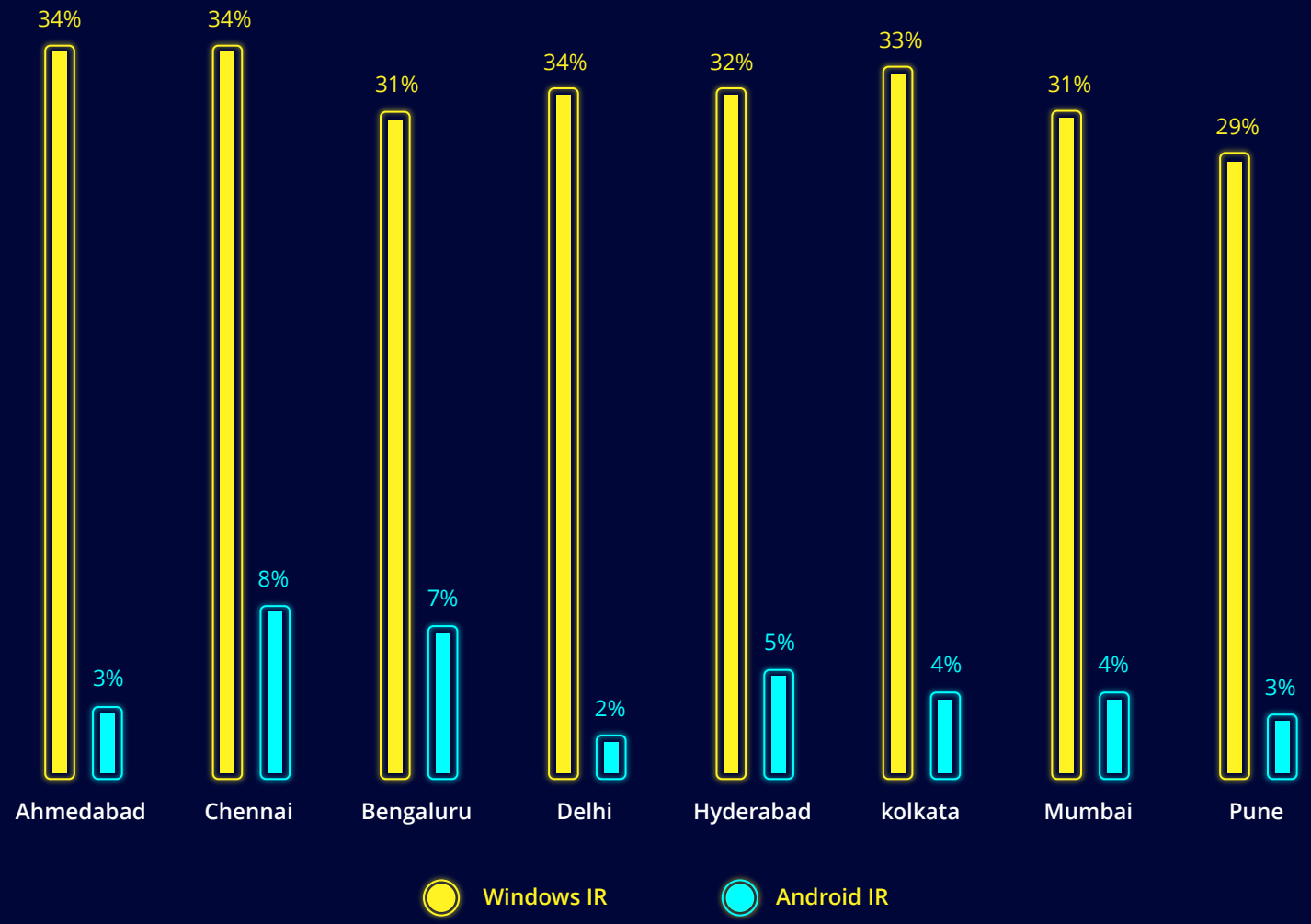


Threat actors have also started focusing more on Tier-2 cities due to a plethora of factors such as poor cyber hygiene, lack of awareness, etc.

INFECTION RATE COMPARISON ACROSS PLATFORMS

Threat actors are still focusing more on Windows-driven devices and networks in comparison to its Android counterpart. This is mainly due to its vast user base and the extensive attack surface that the Windows devices offer. That does not make Android OS any safer than Windows OS. Though there is a significant rise in mobile malware, the proportion of attacks is however relatively small compared with Windows making the mobile threat landscape appear less significant.

Windows IR vs Android IR



ENTERPRISE INSECURITY

Enterprises are prone to cyber attacks because of the vast attack surface that it offers, and with most of them still lacking proper cyber hygiene, it becomes a cakewalk for the threat actors to cause a data breach. The repercussions of the same are not just financial loss, they will have to handle the reputational loss and legal consequences of the cyber attack too.

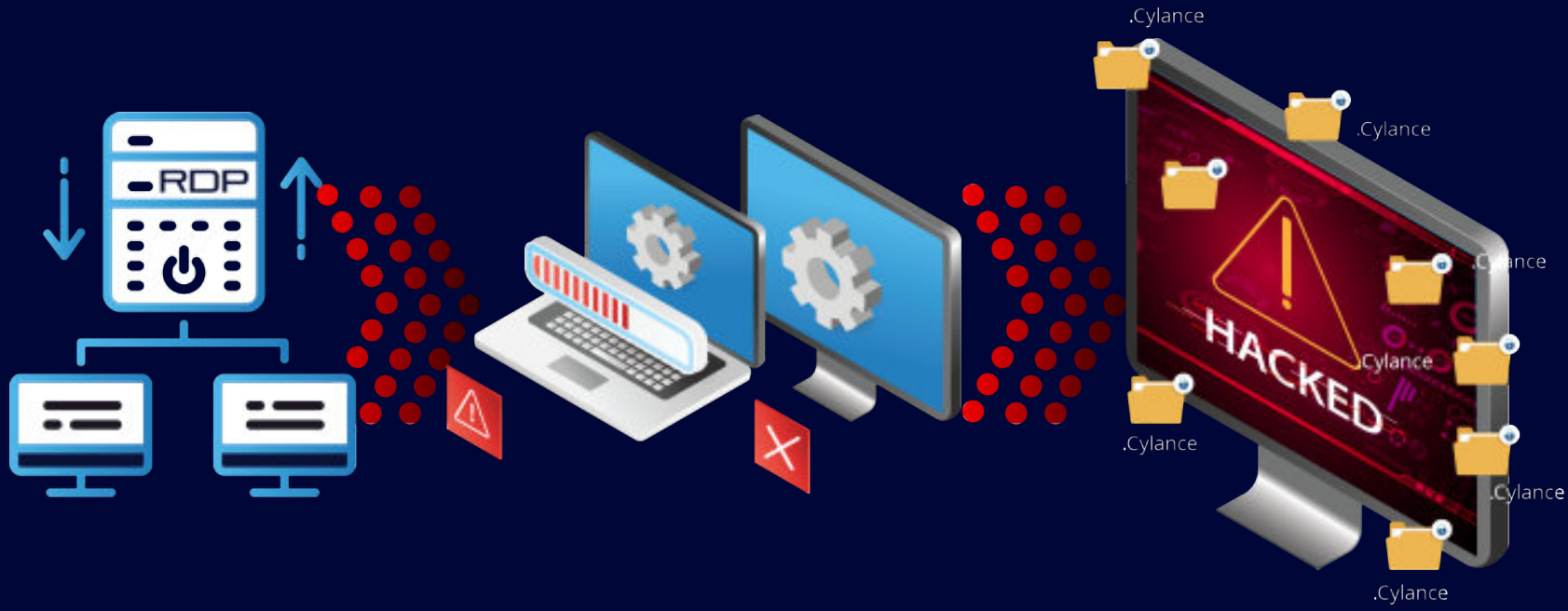
CASE STUDY: DEFAULT PORTS TARGETED BY CYLANCE RANSOMWARE

Recently, one of our enterprise customers got infected with CYLANCE ransomware, exploited through internet facing services on default ports. More details are illustrated below.

Threat actors brute force themeselves on RDP and MSSQL services running on default ports

They then used specialized tools to gain privilege and drop the ransomware on the system

All drives get infected with the CYLANCE ransomware and the files are encrypted with the ".CYLANCE" extension.



SAFETY RECOMMENDATIONS

- Enforcing use of strong passwords and multi-factor authentication (MFA)
- 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

While organizations are trying to understand the risks associated with their products and taking steps to fix them; threat actors are not giving them time and are going one step further in finding loopholes to exploit as and when they are exposed.

Listed below are a few significant vulnerabilities that we came across in the last quarter.

EoP Vulnerability in Microsoft's Win32K

The elevation of privilege (EoP) vulnerability, CVE-2023-29336 is in a core kernel-side driver used in Windows. This is an important zero-day vulnerability which has been exploited in the wild. Exploitation allows SYSTEM level privileges on the intended host.

WIndows 10, Windows Server 2008, 2012 and 2016 are the products impacted.

Secure boot Vulnerability

In May 2023, a security vulnerability CVE-2023-24932 was discovered in Secure Boot, a Boot Manager used in Windows. Once exploited, the attacker with physical access or administrative rights to the target device could install an affected boot policy and bypass Secure Boot.

Windows 10, 11 and Windows Server 2008, 2012, 2016, 2019, 2022 are the products affected by the same.

Netfilter's EoP Vulnerability

An EoP vulnerability CVE-2023-32233 was discovered in the second quarter of 2023 in Netfilter which is a framework provided by Linux Kernel. On exploitation, an unprivileged local user can escalate their privileges to root and completely compromise the system.

Linux kernels up to 6.3.1 are impacted by this vulnerability.

RCE Vulnerability in Google Chrome Web Browse

CVE-2023-3079, a vulnerability within the Google Chrome web browser can be exploited by an adversary using a specially crafted HTML page causing heap corruption which leads to remote code execution attacks. This is caused by a type confusion within the V8 JavaScript engine.

Vulnerable product versions are Google Chrome for Windows, MacOS, Linux < 114.0.5735.110.

SQL Injection Vulnerability in MOVEit

CVE-2023-34362 vulnerability allows an unauthenticated adversary to gain access to MOVEit Transfer's database, a commercial secure managed file transfer software solution, and gain access to sensitive data.

Vulnerable product versions are MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1) and MOVEit Cloud versions 15.0.0.0 - 15.0.2.39, 14.1.0.0 - 14.1.6.97.

DANGERS IN THE INTERNET OF THINGS

With the number of connected devices growing at a rapid pace, so is the huge amount of data that is generated by it. With this comes a plethora of opportunities for threat actors to exploit the not so secure devices, which are mainly built only with rapid development and utility in mind and with lax attitude towards cybersecurity.

PaperCut Vulnerability exposes victim's system to ransomware

The remote code execution (RCE) vulnerability, CVE-2023-27350 allows threat actors to bypass authentication on vulnerable PaperCut NG 22.0.5 (Build 63914) installations and thereafter execute arbitrary code with SYSTEM privileges.

Vulnerability in Apple's products

CVE-2023-28204 is a vulnerability in WebKit's browser engine that supports Apple's web browsers, allowing processing of malicious crafted web content leading to exposure of sensitive information.

CVE-2023-32373 is an RCE vulnerability which when exploited allows arbitrary code execution while loading maliciously crafted web pages.

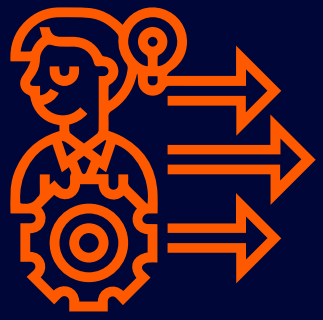
CVE-2023-32409 is a sandbox escape vulnerability that allows an attacker to break out of Web Content sandbox.

iOS and iPadOS products having versions below 16.5 are impacted.

Buffer Overflow in Fortiguard products

CVE-2023-27997 vulnerability allows an attacker to execute arbitrary code or commands by sending specially crafted requests to vulnerable devices.

Vulnerable product versions include FortiOS-6K7K versions 6.0.10 - 7.0.10, FortiOS versions 6.0.0 - 7.2.4 and FortiProxy versions 1.1, 1.2, 2.0.0 - 2.0.12, 7.0.0 - 7.0.9, 7.2.0 - 7.2.3.



MITIGATION TECHNIQUES

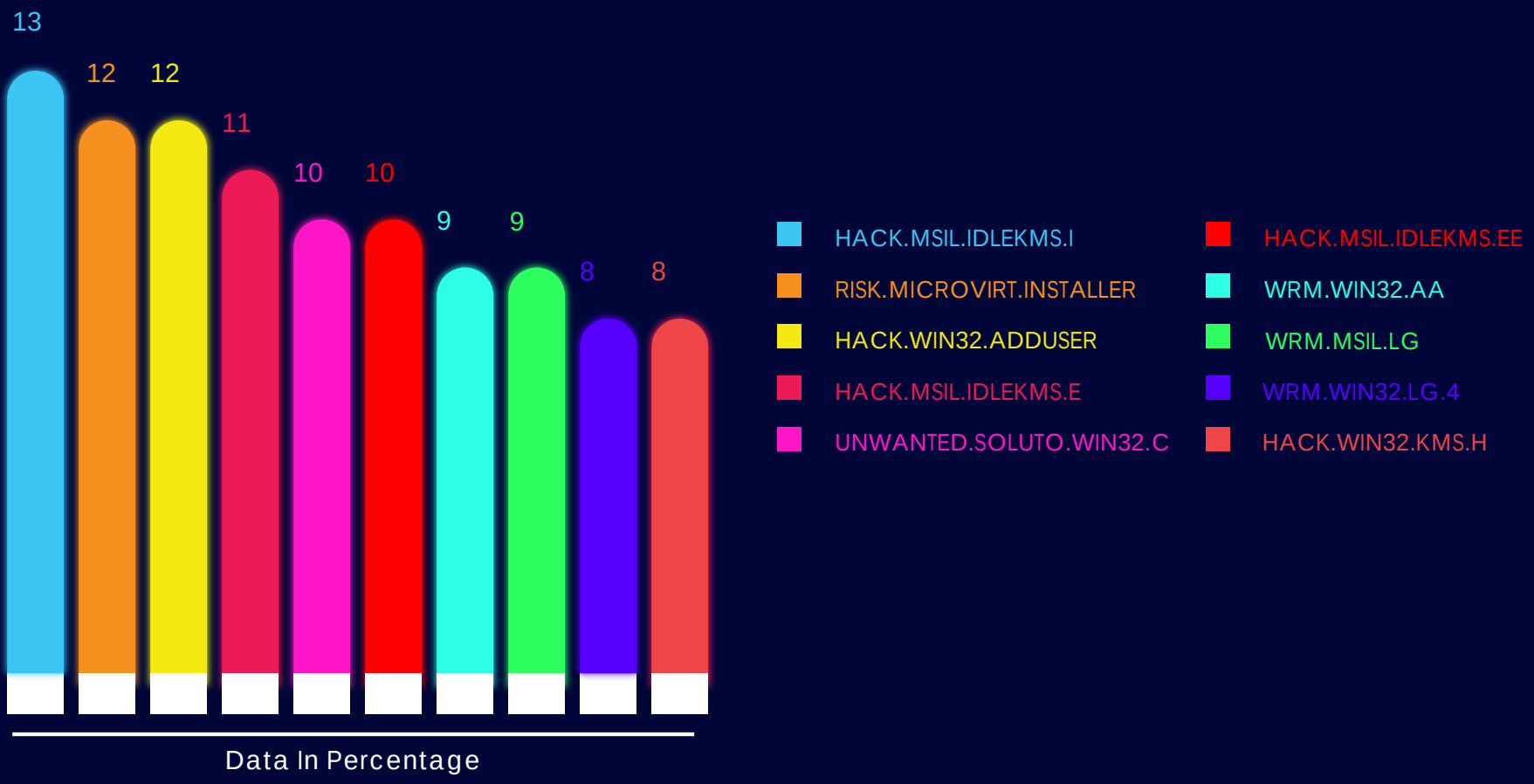
- Secure all devices connected to your network
- Identify IoT risks and mitigate them as soon as possible

WINDOWS UNDER SIEGE

Windows Malware Type Breakdown

Windows has dominated the desktop and laptop market for years, making it an attractive target for cybercriminals seeking to exploit vulnerabilities and gain unauthorised access. The following chart displays certain significant detections.

Split of Windows Top 10 Detections

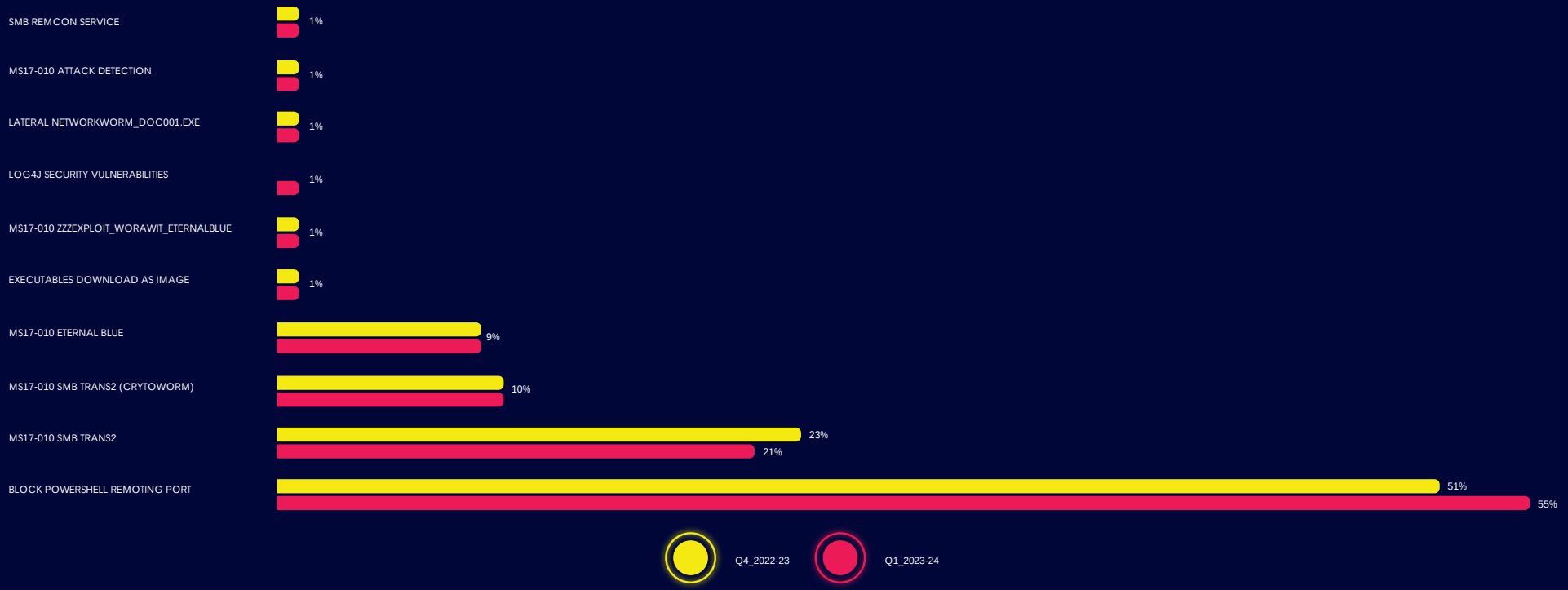


WINDOWS EXPLOITS

While Microsoft has significantly improved Windows security over the years, the unpatched legacy vulnerabilities in it, like the ones in SMBs and PowerShell, have massively contributed to the constant escalation in various Windows devices being targeted.

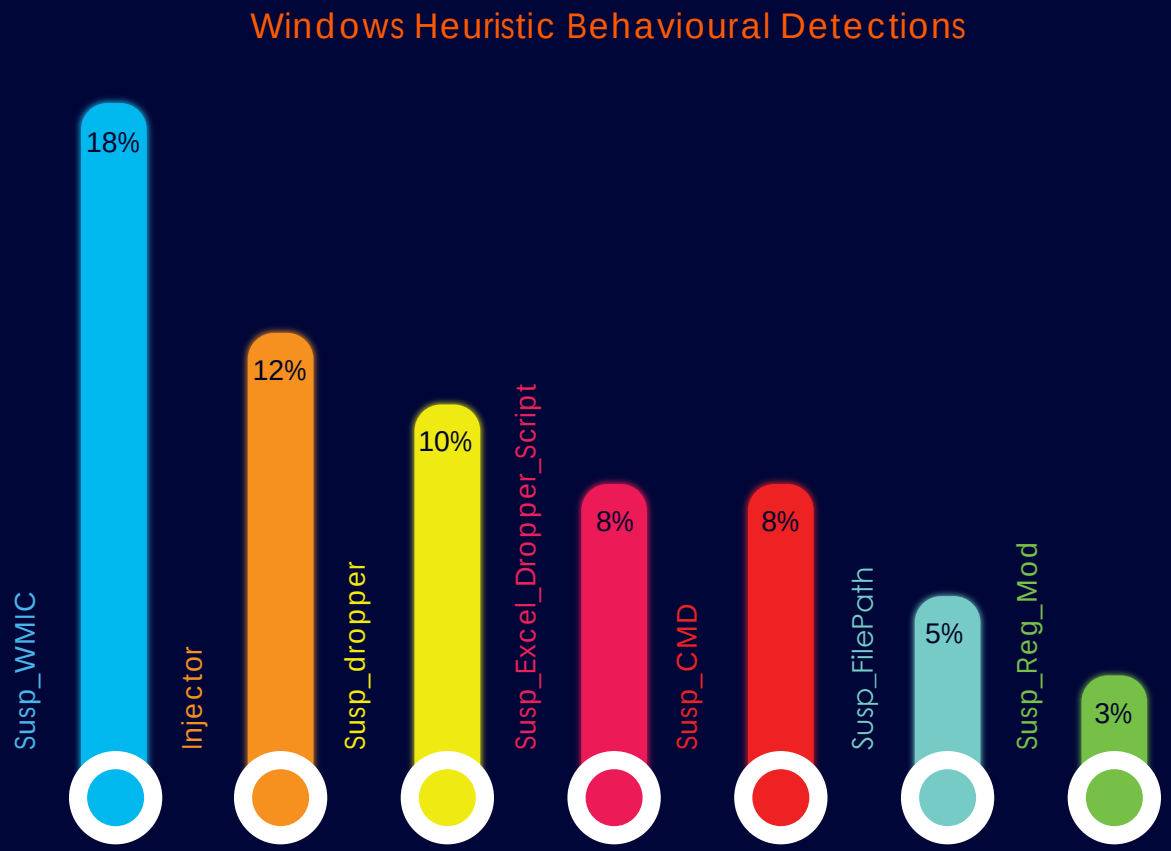
Cybercriminals have increasingly utilised PowerShell for malicious activities, such as delivering malware, or executing various attack techniques. PowerShell's versatility, and deep integration with the Windows operating system make it an attractive choice for attackers.

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.



Threat actors abusing WIndows Management Instrumentation (WMI) is on the rise. WMI is being used by them to interact with local and remote systems and execute malicious commands and payloads. 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.

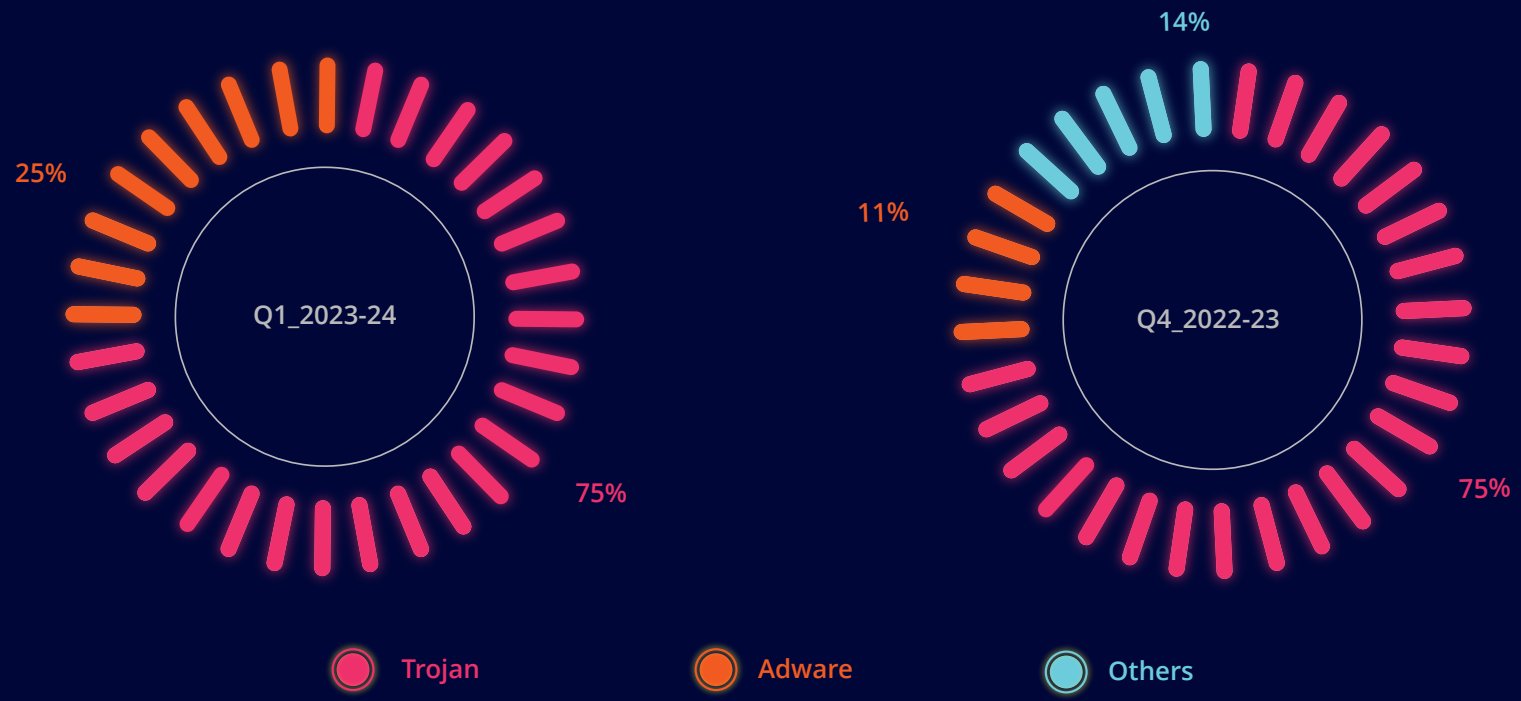
MITIGATION TIPS

- Enable remote access only when you need it, keep it disabled otherwise
- Set up your operating system to enable auto-updates by default
- Backup your data on a regular basis

THE MOBILE DEVICE STORY

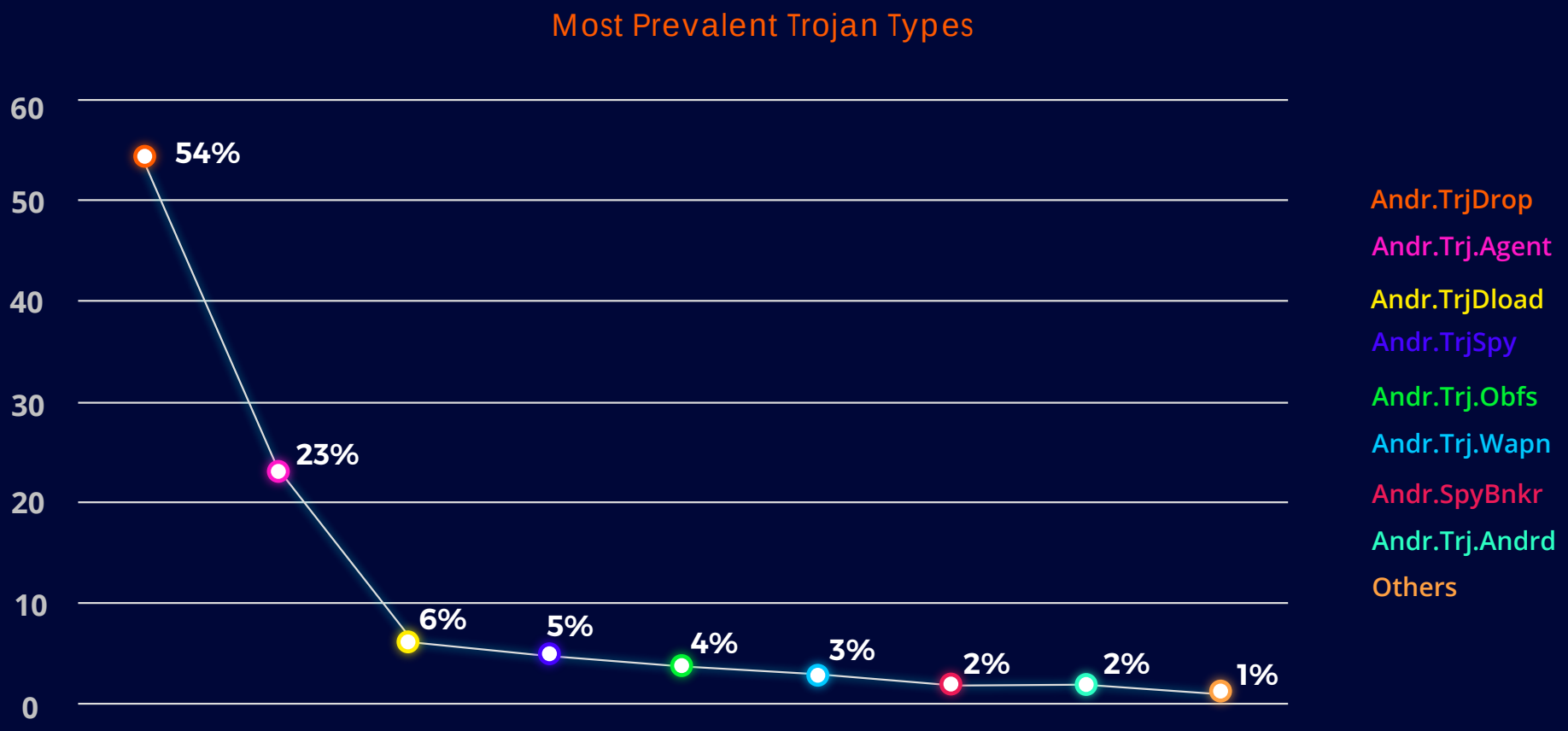
Organizations, businesses and individuals alike are facing mobile threats that use multiple attack vectors targeting vulnerable smartphones and the human element. While the vulnerable devices are a gateway to several malware-ridden apps and sites, the human element is vulnerable to sophisticated phishing, smishing and several other social engineering scams.

Adware vs Trojan Proportional



THE OMNIPRESENT TROJAN

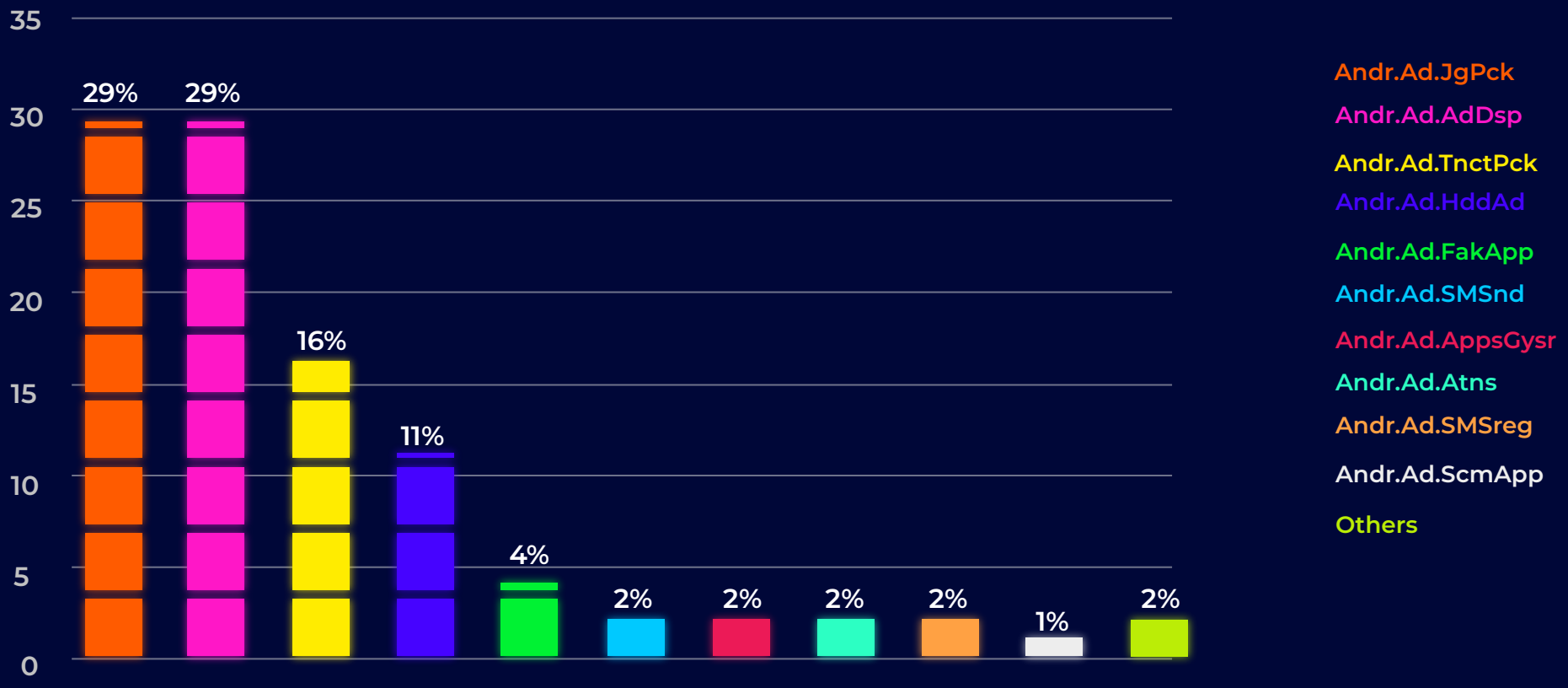
Continuing its trend in its prevalence since the last few quarters, sophisticated trojans have veiled behind the agents, downloaders and droppers to do its malicious intent.



THE ADWARE SAGA

Last quarter also saw most of the older families, such as Andr.Ad.JgPck, Andr.Ad.AdDsp, Andr.Ad.HddAd occupying over half of the total adware space.

Trend Line Showing the Adware Plague



TIPS TO STAY SAFE

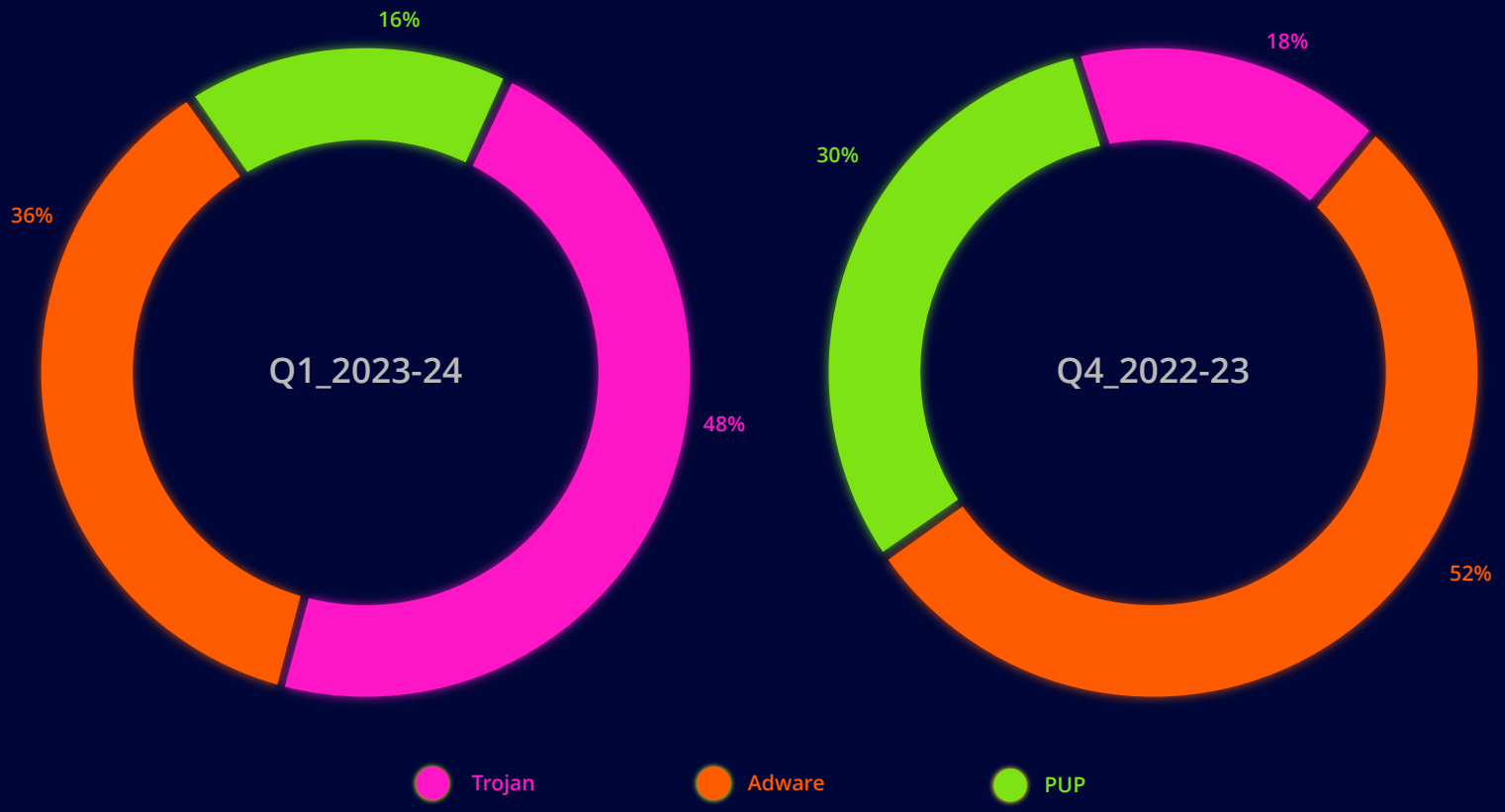
- Always be extra cautious before downloading and installing any app
- Do not download or install apps from unknown sources or third-party app stores
- Keep your OS and devices updated and patched against the latest vulnerabilities
- Install a robust security product like K7 Mobile Security to stay protected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

MAC ATTACK

Trojans are often designed with specific malicious intent, such as stealing sensitive information, distributing ransomware, or conducting financial fraud. These activities can bring significant economic gains to attackers. In contrast, adware and potentially unwanted programs (PUPs) often rely on ad revenue or user data collection, which may not be as lucrative.

Moreover, in recent years, Apple has significantly improved security measures on macOS, making it more challenging for adware and PUPs to infiltrate the system. As a result, malware developers have shifted their focus to developing trojans that can bypass these enhanced security measures.

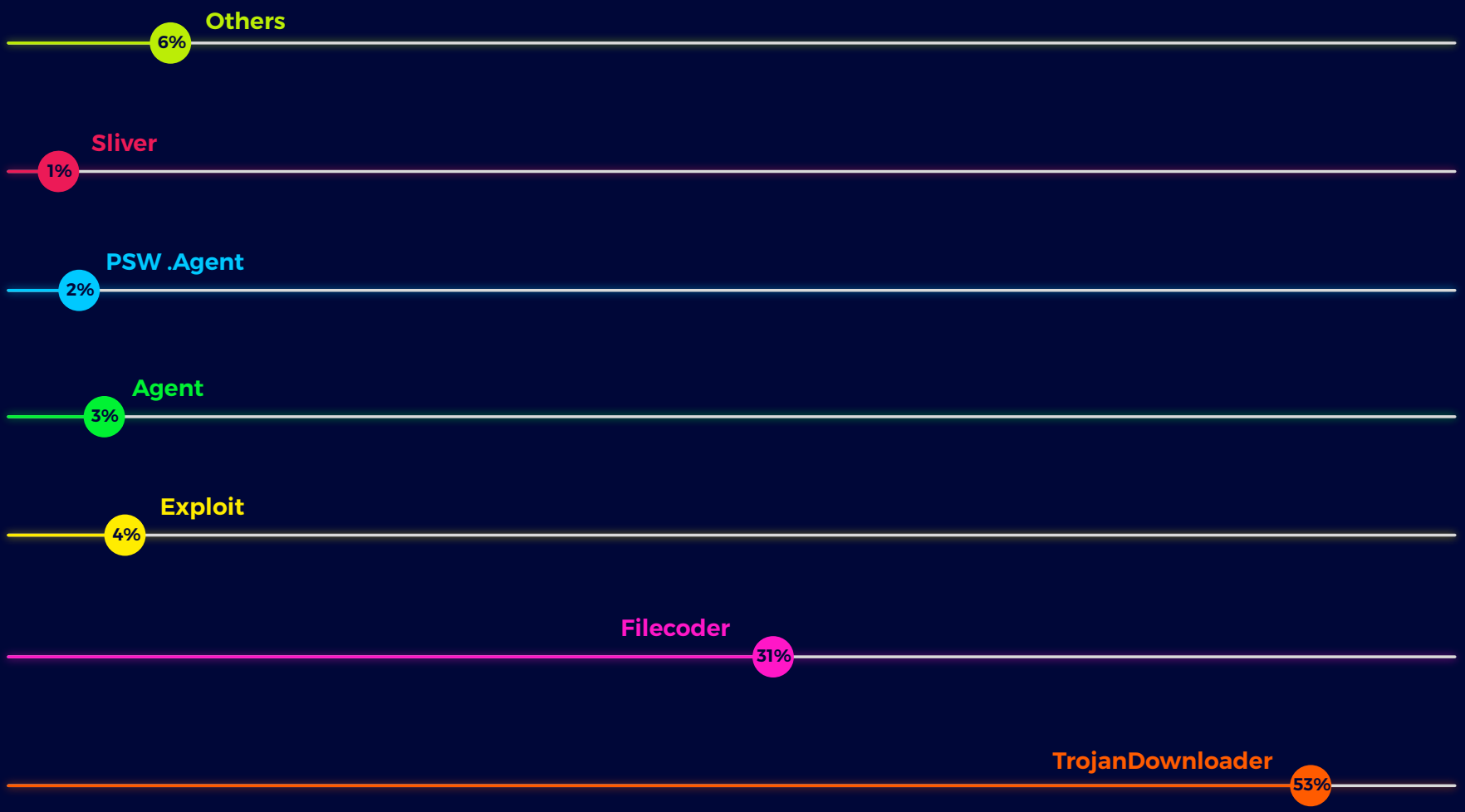
Trojan, Adware & PUP Proportional Split



THE UBIQUITOUS TROJANS

Downloaders serve as a gateway for other malware, allowing cybercriminals to gain unauthorised access to systems or steal sensitive information. These trojans are highly profitable and incentivise attackers who create and distribute them in large numbers, resulting in its massive presence on the macOS platform.

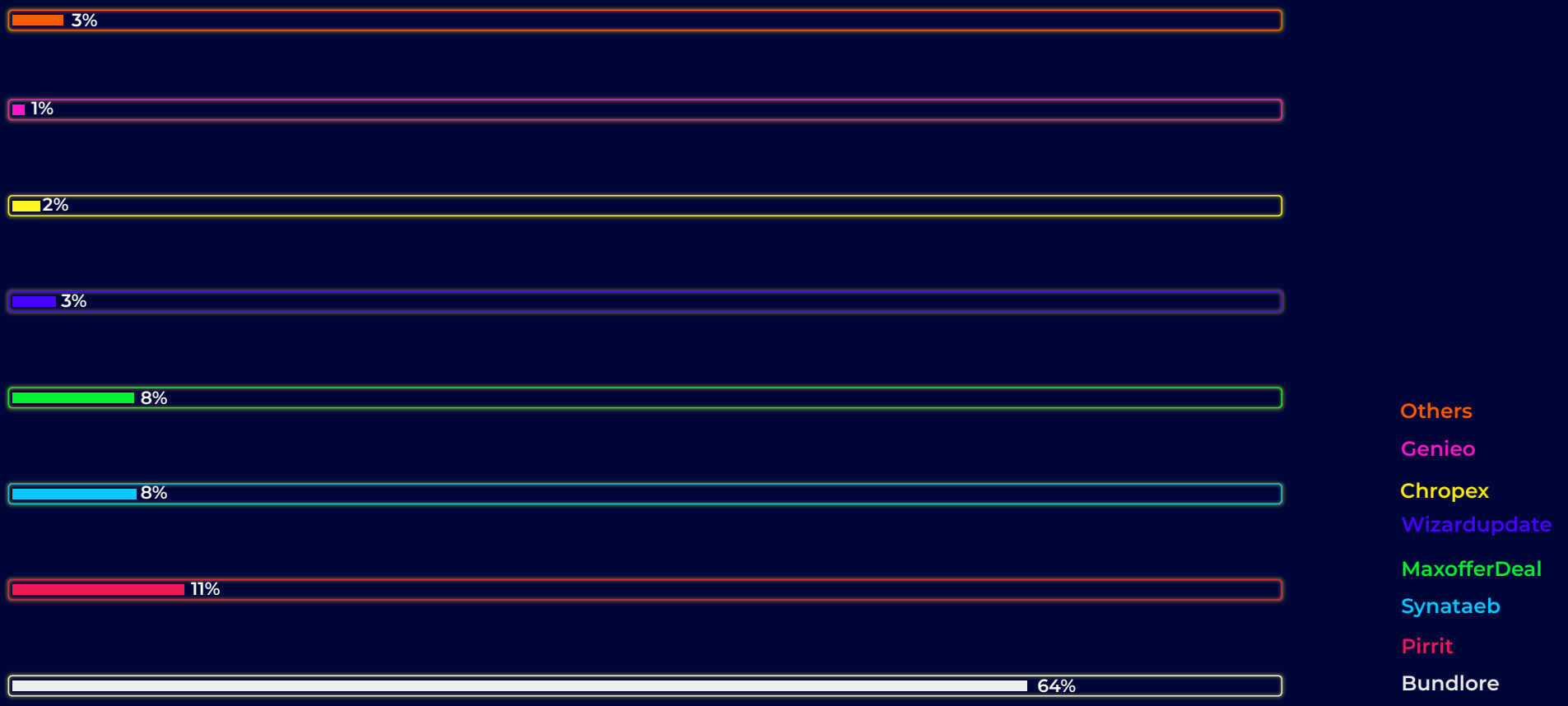
Trojan Detection Trend Line



THE ADWARE UPROAR

Even after occupying a significant slice of attacks on the macOS platform, no significant changes are noticed in the adware section. Bundlore still topped the list with two other prevalent families - Pirrit and Synataeb.

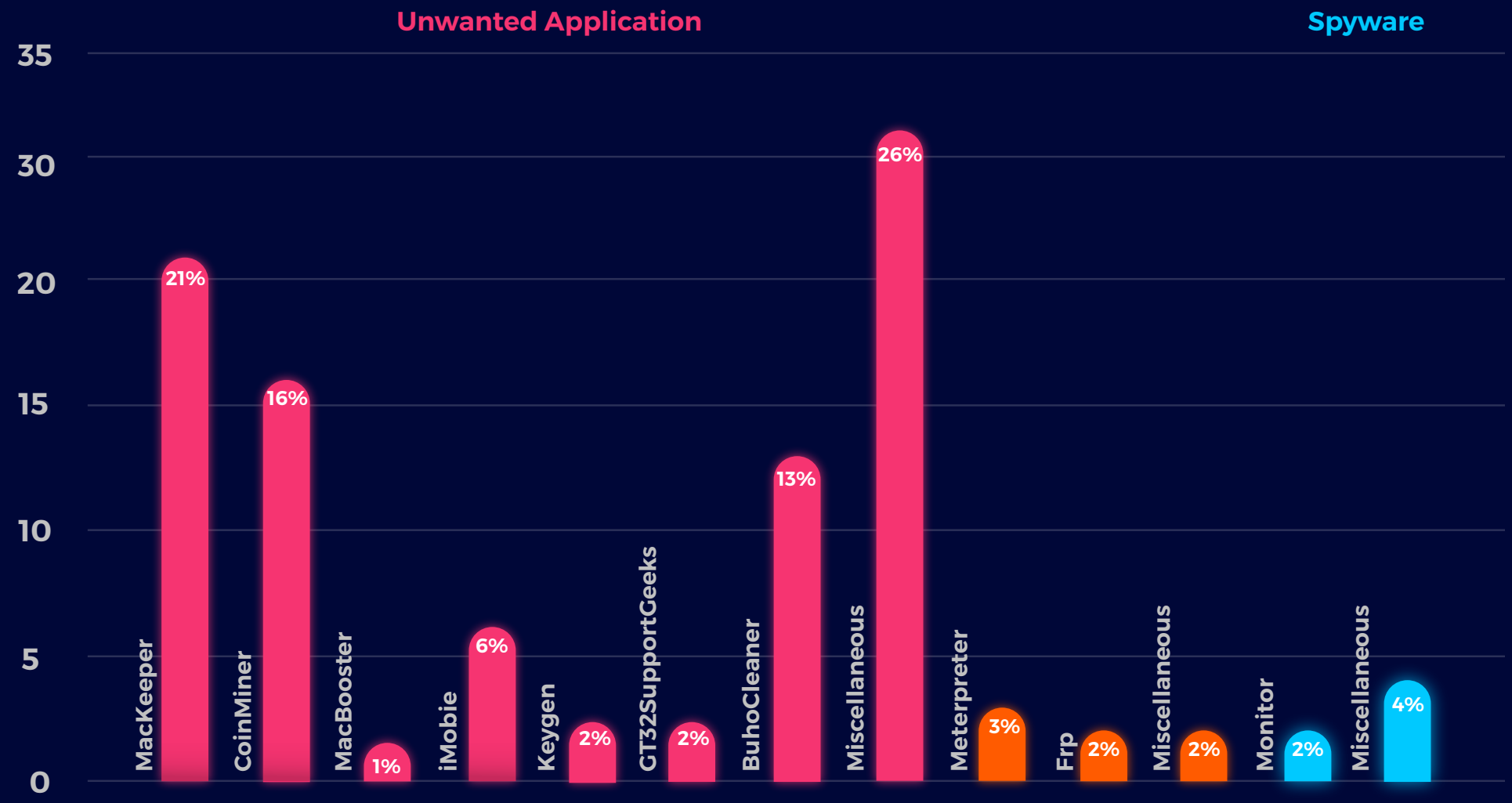
The Trend Line of Adware Variant Detections



A PINCH OF PUPS

Free system cleaners such as MacKeeper, and BuhoCleaner are still getting their fair share of victims, in spite of PUPs diminishing trend in comparison to trojans and adware.

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

KEY TAKEAWAYS

Cyber threats in today's digital world are getting more and more sophisticated. Investing in a robust and multi-layered cybersecurity system is one way to protect yourself from such dangers. In light of the prevalence of cyber threats, it is crucial to implement security measures and adhere to it.

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
Protect your business by switching to a zero-trust driven framework	Only use the official app store for app downloads and installations
Encrypt and backup your sensitive and critical data	Secure your sensitive information

www.k7computing.com