K7 SECURITY

CYBER THREAT MONITOR REPORT

Q3_2023-24

www.k7computing.com

CONTENTS

COMPREHENDING OUR CYBERSPACE

While Israel is grappling with attacks by Hamas on its soil, Islamic hacktivist groups have launched a digital war on its digital infrastructure intensifying the conflict further.

A rise in politically and religiously motivated hacktivist groups targeting Israeli critical infrastructure with DDoS attacks was also seen. After Israeli organisations such as media, defence and other critical infrastructures fell victim, its age-old ally India came to its rescue by unleashing its group of hackers to defend their systems and other sensitive digital assets.

On the other hand, its holiday season in the US and the rest of the world. More cyber attacks are foreseen on countries supporting Israel and the subsequent retaliation. It is going to be a different ball game altogether for the threat actors and if played well, they are the ones who are going to benefit the most, be it money or just stopping operations.

A rise in ransomware operations; mainly due to the large attack surface and monetary benefit that it offers for the threat actors, and crypto malware; mining cryptocurrencies is very lucrative and cryptojacking is an inexpensive way to mine, are foreseen. Threat actors are also creating variants of existing malware with enhanced evasion techniques. Ransomware-as-a-service (RaaS) methodology will involve a lot of players in the field, both amateurs and professionals.

The world is reeling under chaotic times and we also foresee a rise in nation-state sponsored threat activity. Nations and organizations need to up their defences by following proper cyber hygiene practices and training their employees to stay safe from this ongoing digital warfare.

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.
Stay Alert, Stay Vigilant!

CYBER THREAT MONITOR - INDIA

Map for illustrative purposes only. Not to scale.

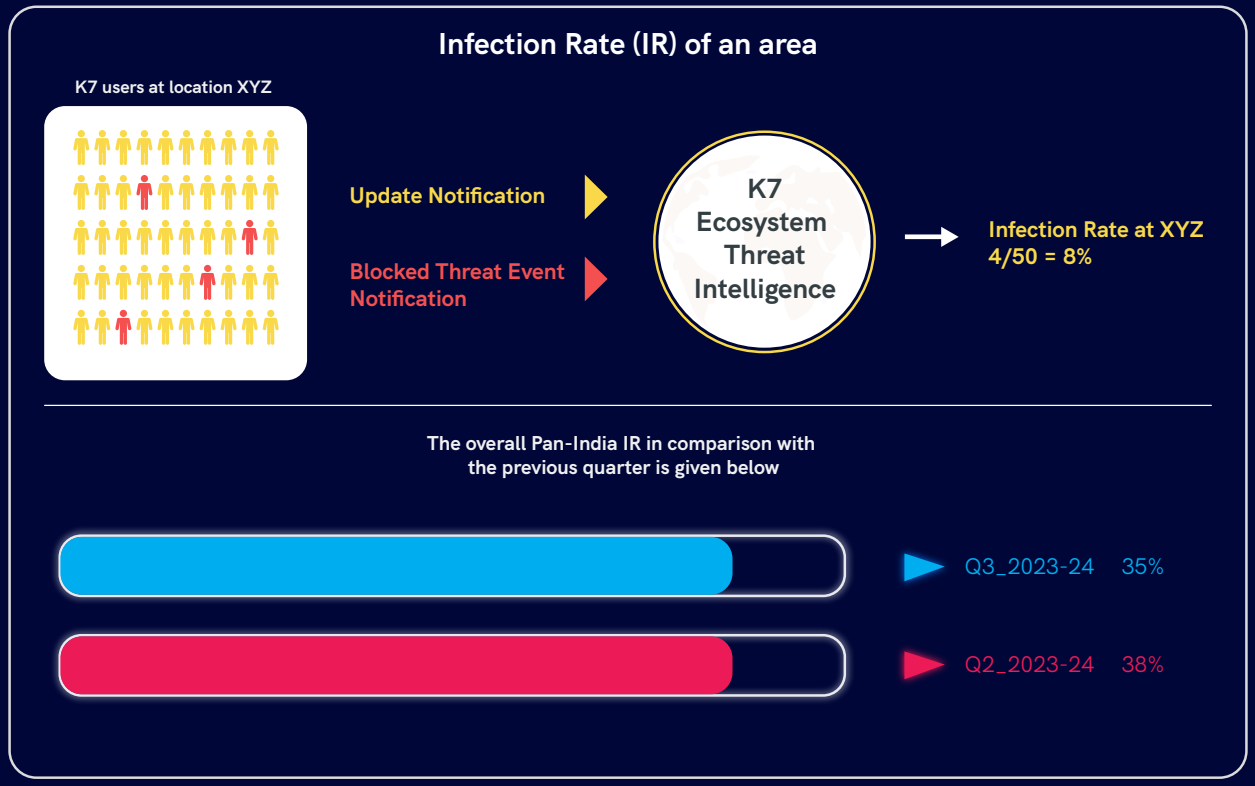
REGIONAL INFECTION PROFILE

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.

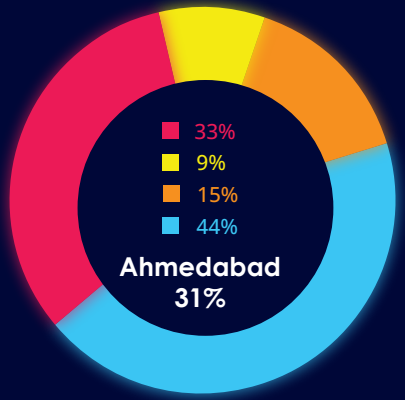
The concept of Infection Rate is better explained by the below picturization.

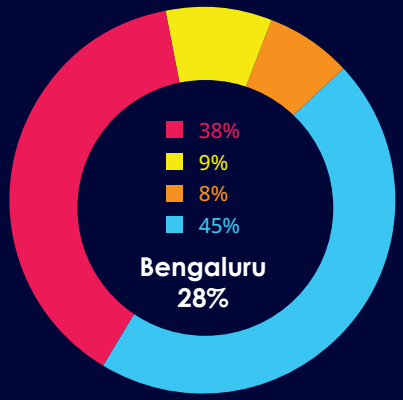


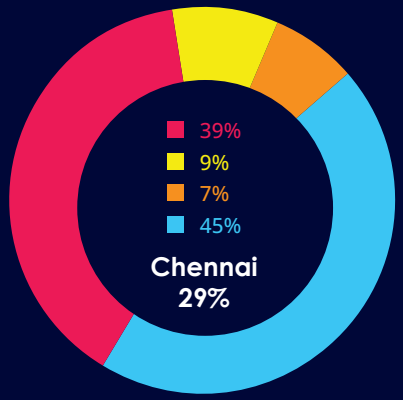
The slight reduction in the infection rate doesn't intend a much safer digital experience. This could be attributed to incidents not reported and products not activated/updated.

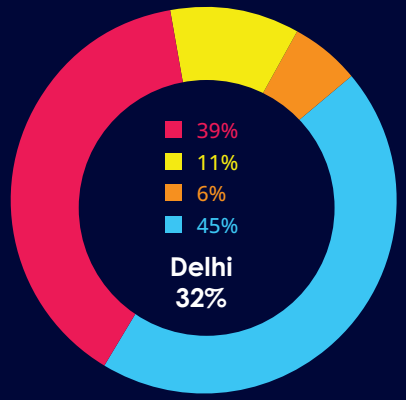
Before we delve into the threat landscape for the last quarter, we present to you a few significant IRs across metros classified based on the different levels at which the threats were blocked.

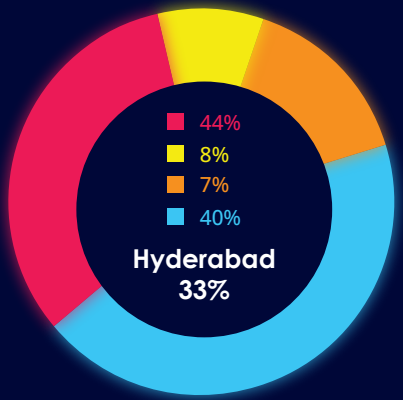
THE METRO AND TIER-1 CITIES - INFECTION RATE

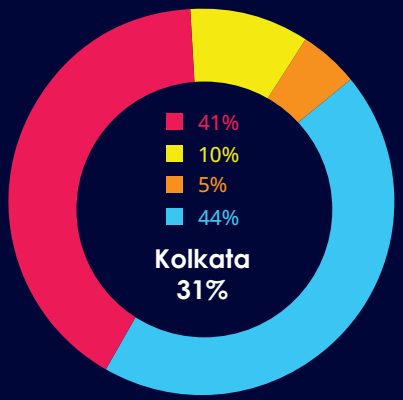


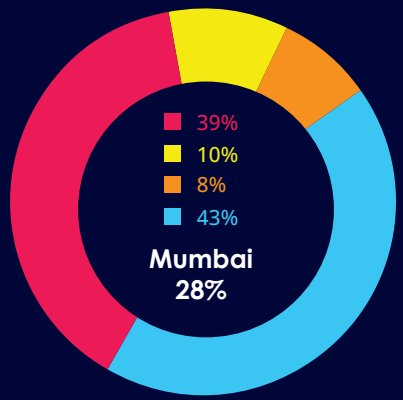


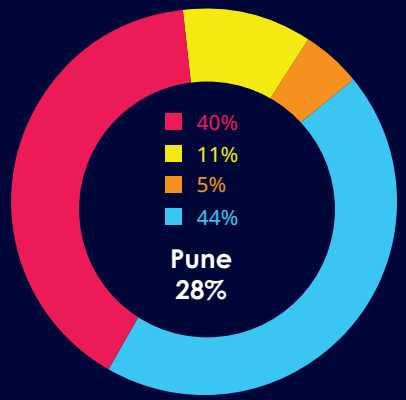






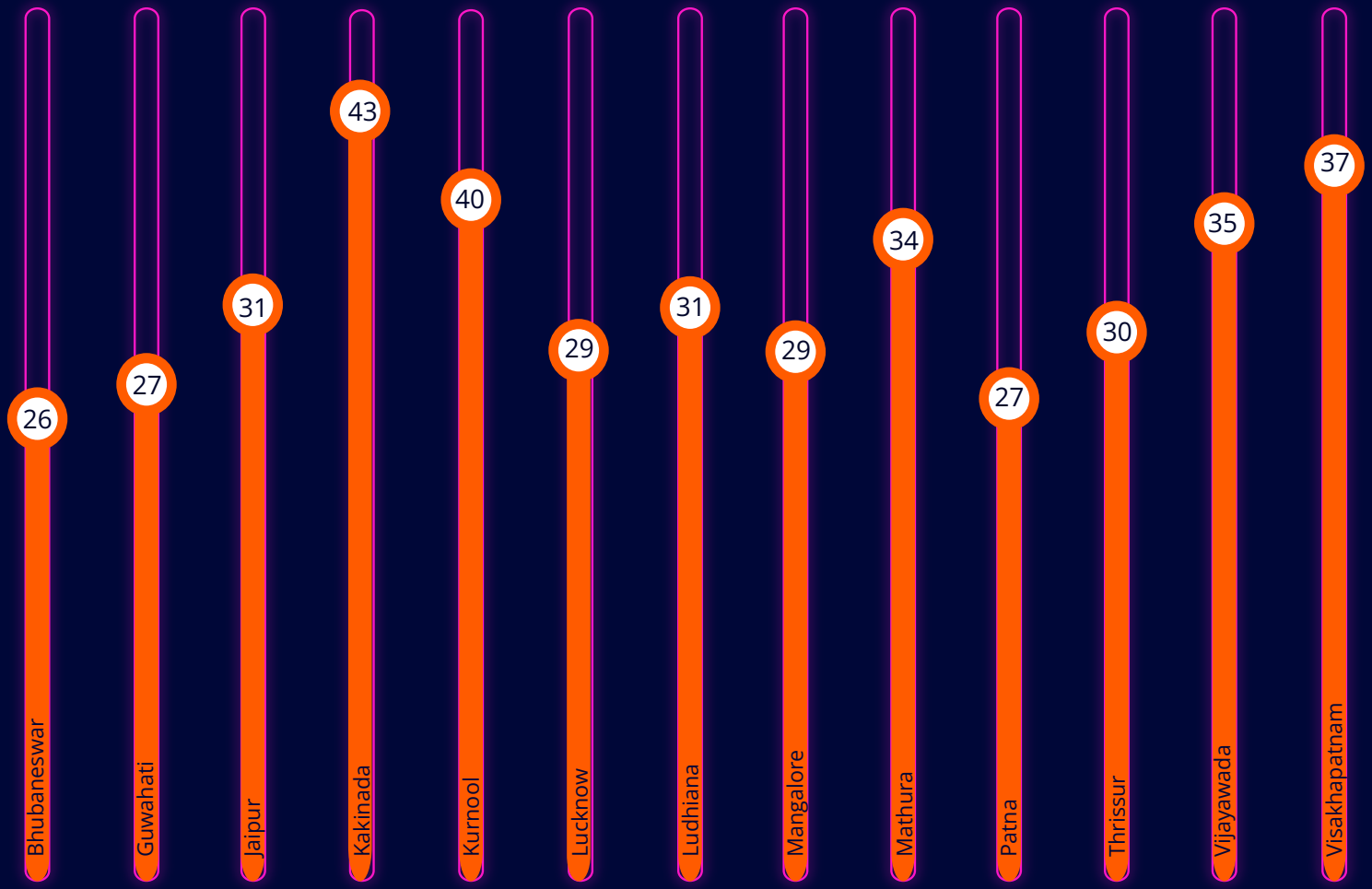






- Web Protection
- Firewall Protection
- Behaviour Protection
- ScanEngine Protection

TOP INFECTION RATES IN TIER-2 CITIES

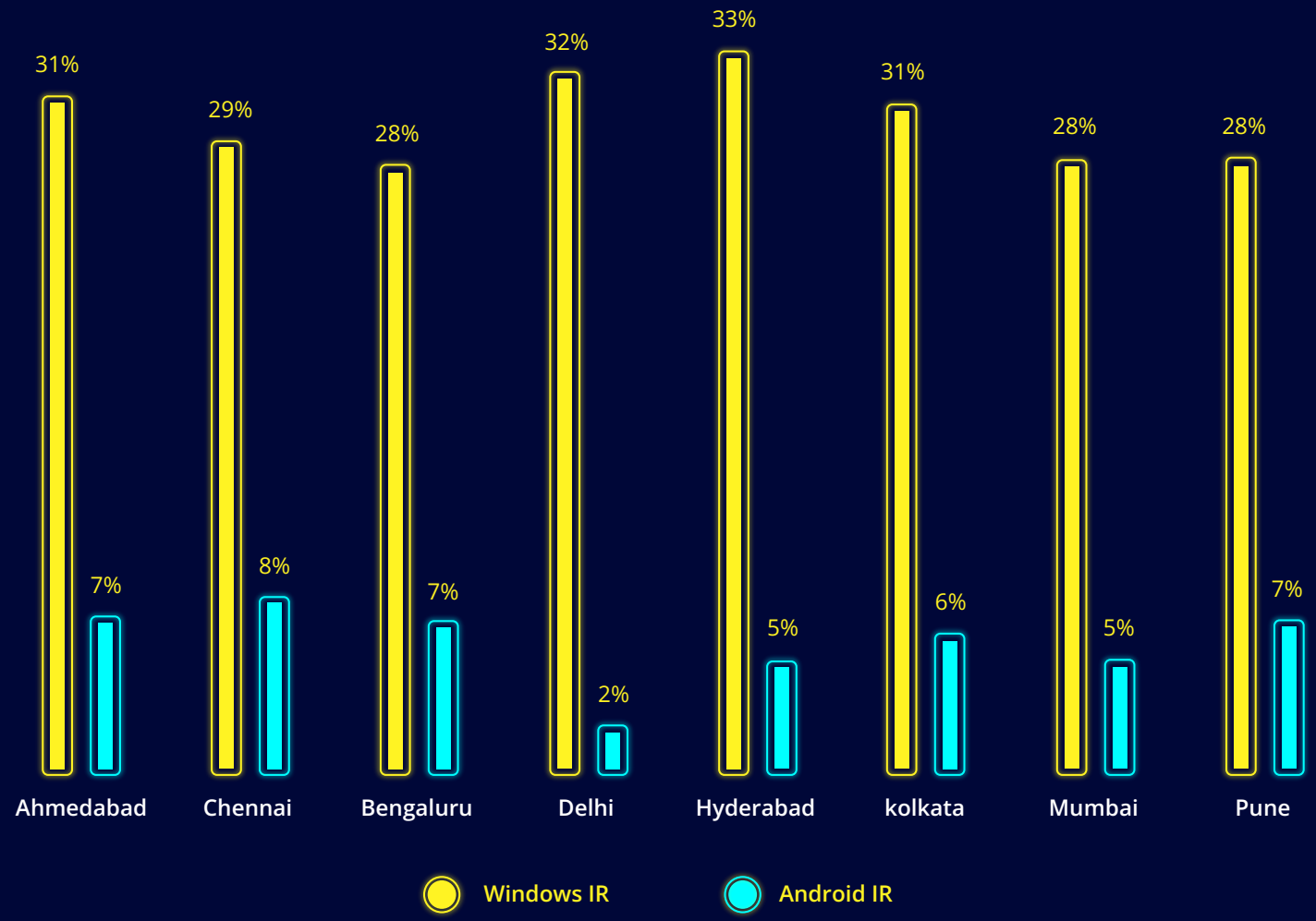


Threat actors have also started focusing more on Tier-2 cities due to a plethora of factors such as poor cyber hygiene, lack of awareness, etc.

INFECTION RATE COMPARISON ACROSS PLATFORMS

Even though Windows is a closed-source system, its enormous user base presents a lucrative chance for cybercriminals seeking notoriety and bragging rights.

Windows IR vs Android IR



As the chart reveals, threat actors are also targeting Android users, major Indian cities like Ahmedabad, Bengaluru, Chennai, and Pune witnessing a reasonable volume of attacks. This simply reflects the differing tactics employed by threat actors on each platform.

ENTERPRISE INSECURITY

Cryptomining malware can jeopardize the availability and security of a network or system and can stall an enterprises' operations. It co-opts the victims' computing resources to mine cryptocurrencies. It is resource intensive and happens without the knowledge of the victim. It hides on your network and steals the computing resources, thereby slowing down the entire network.

Recently, one of our enterprise customers complained of frequent pop-up notifications from our security product, about a malicious file detected while it was being copied from the local network. This file was deployed in one of the internet facing SQL servers which was poorly protected and was spreading laterally across the network.

The kill chain is as below

LemonDuck: Not Yet Ducked Out

SAFETY RECOMMENDATIONS

- Deploying tools to monitor your organizations' network
- Enforcing least privilege access
- 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

Vulnerability in Skype's Business Products

CVE-2023-41763, an information disclosure vulnerability, allows an attacker to elevate their privileges.

- Vulnerable products include
  - Skype for Business Server 2015 CU13 < 6.0.9319.869
  - Skype for Business Server 2019 CU7 < 7.0.246.530

Wordpad's Information Disclosure Vulnerability

CVE-2023-36563, in Microsoft Wordpad works by convincing a user into opening a malicious file, which allows the disclosure of NTLM hashes. A thing to note is that Wordpad is no longer being updated and will be removed from the future Windows releases.

- Vulnerable products include
  - Windows 10 and 11
  - Windows Server 2008, 2012, 2016, 2019 and 2022.

SmartScreen ByPass Vulnerability

CVE-2023-36025, tricks an user into clicking on a malicious URL, by which an adversary may be able to bypass Windows Defender SmartScreen checks and their associated prompts.

- Vulnerable products include
  - Windows 10 and 11.
  - Windows Server 2008, 2012, 2016, 2019 and 2022.

Google Chrome's Buffer Overflow Vulnerability

CVE-2023-5217, allows a remote attacker to potentially exploit a heap corruption via a crafted HTML page.

- Vulnerable products include
  - Google Chrome

RCE Vulnerability in Microsoft's Excel

CVE-2023-36041, convinces a victim to open a specially crafted file from a website, leading to local attack on their computer allowing threat actors to gain high privileges which include read/write and delete functionality.

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

- Vulnerable products include
  - MS office 2019 & 2016.
  - 365 Apps for Enterprise.
  - Office LTSC for Mac 2021.
  - Office LTSC 2021.

DANGERS IN THE INTERNET OF THINGS

IoT devices are primarily designed with connectivity in mind. Many organizations have a lax attitude towards cybersecurity especially with these connected devices. Moreover, they are particularly vulnerable to data theft primarily because most of the devices do not encrypt data during transit or storage.
Listed here are a few notable vulnerabilities from the last quarter that was exploited in the wild.

Sophos Command Injection Vulnerability

CVE-2023-1671 in Sophos Web Appliance allows execution of arbitrary code.

- Vulnerable products include
  - Sophos Web Appliance < 4.3.10.4

Privilege Escalation Vulnerability in Bluetooth module

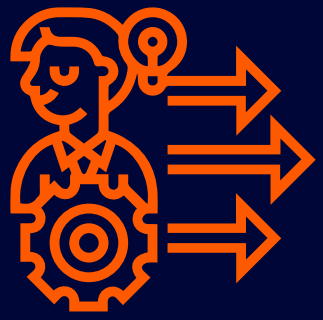
CVE-2023-45866 is a remote privilege escalation vulnerability in the Bluetooth module i.e. bluez, available in Android, iOS, macOS and Linux operating systems. With this an attacker can connect to a discoverable host without user confirmation and may be able to inject keystrokes by spoofing a keyboard.

- Vulnerable products include
  - Android OS version less than or equal to 10.
  - macOS less than or equal to 14.1.1.
  - Ubuntu less than or equal to 23.10.
  - iOS less than or equal to 17.1.1.

Vulnerability in Apple Products

While processing web contents, an out-of-bounds read vulnerability **(CVE-2023-42916)** and memory corruption vulnerability **(CVE-2023-42917)** in WebKit of Apple products, allows disclosure of sensitive information and can also lead to arbitrary code execution.
Vulnerable products include

- Vulnerable products include
  - iOS
  - iPadOS
  - macOS



MITIGATION TECHNIQUES

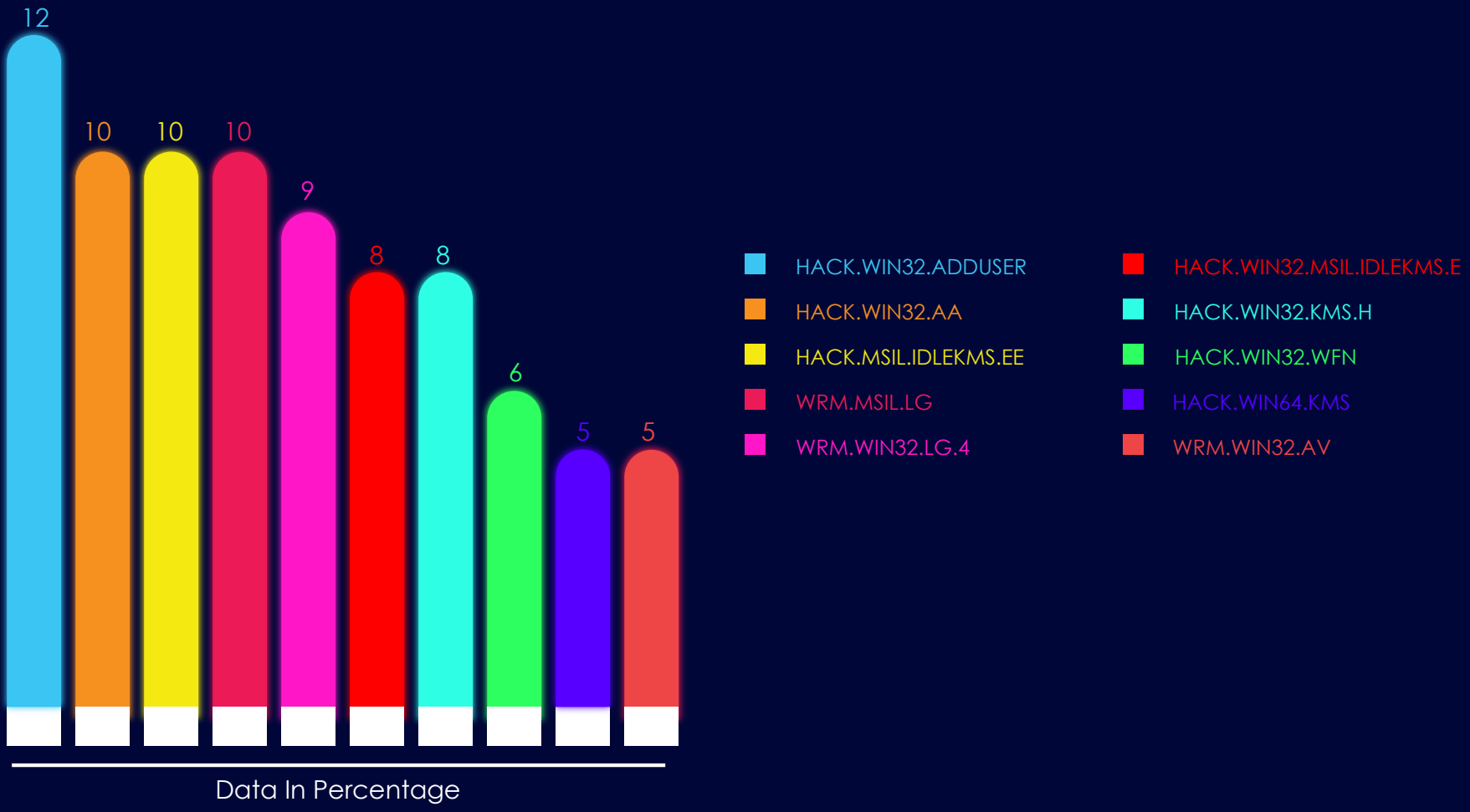
- Encrypt your connections
- Ensure you set a unique and strong password for each of your devices in the network
- Connect your devices to only a secure and trusted network
- Regularly check your device permissions and connections

WINDOWS UNDER SIEGE

Windows Malware Type Breakdown

The battle lines remain firmly drawn in the cyber realm, with Windows users caught in the crossfire. Our latest data paints a worrying picture: a relentless, quarter-on-quarter barrage of threats aimed at corporations and unsuspecting individual users. This pervasive targeting warrants a closer look:

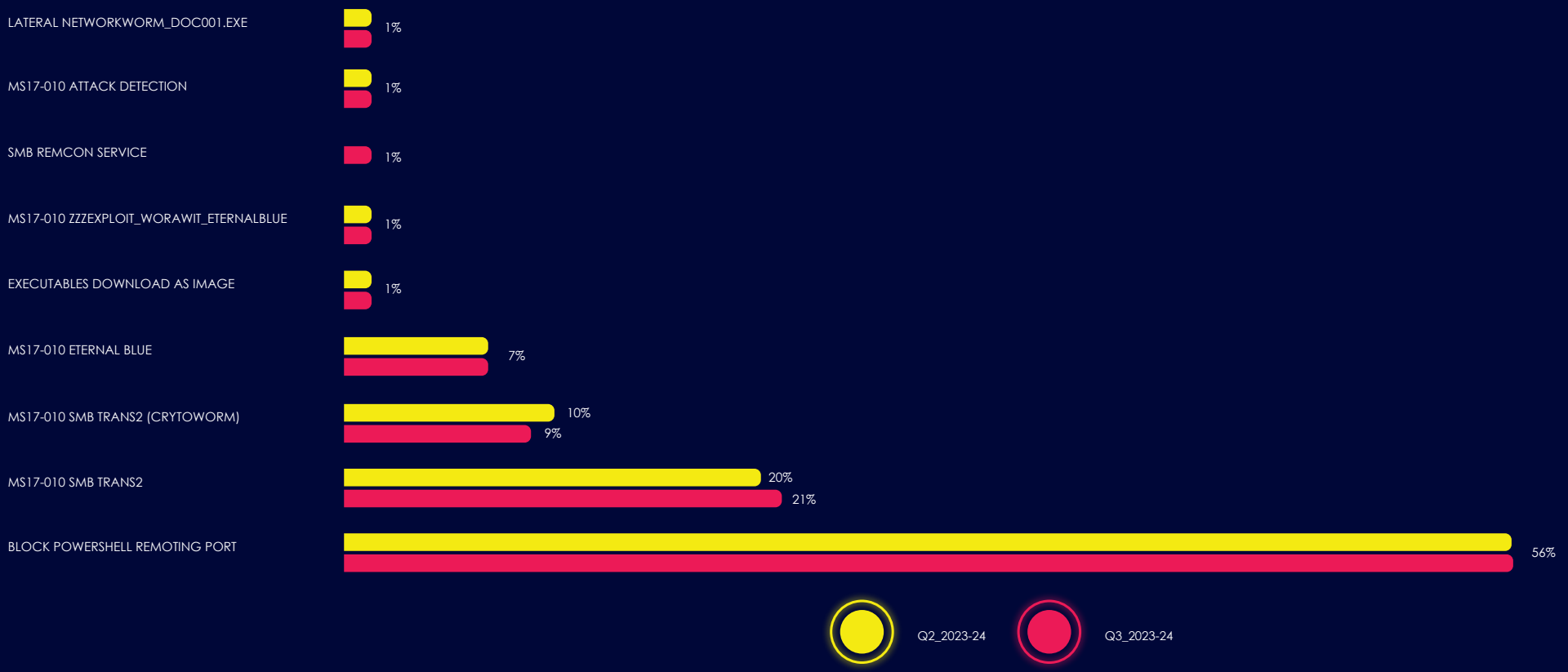
Split of Windows Top 10 Detections



WINDOWS EXPLOITS

Organisations of all sizes, from bustling corporate giants to solo entrepreneurs, were in the threat actors' sight. Malware campaigns exploited vulnerabilities in critical infrastructure, seeking to disrupt operations and extort sensitive data.

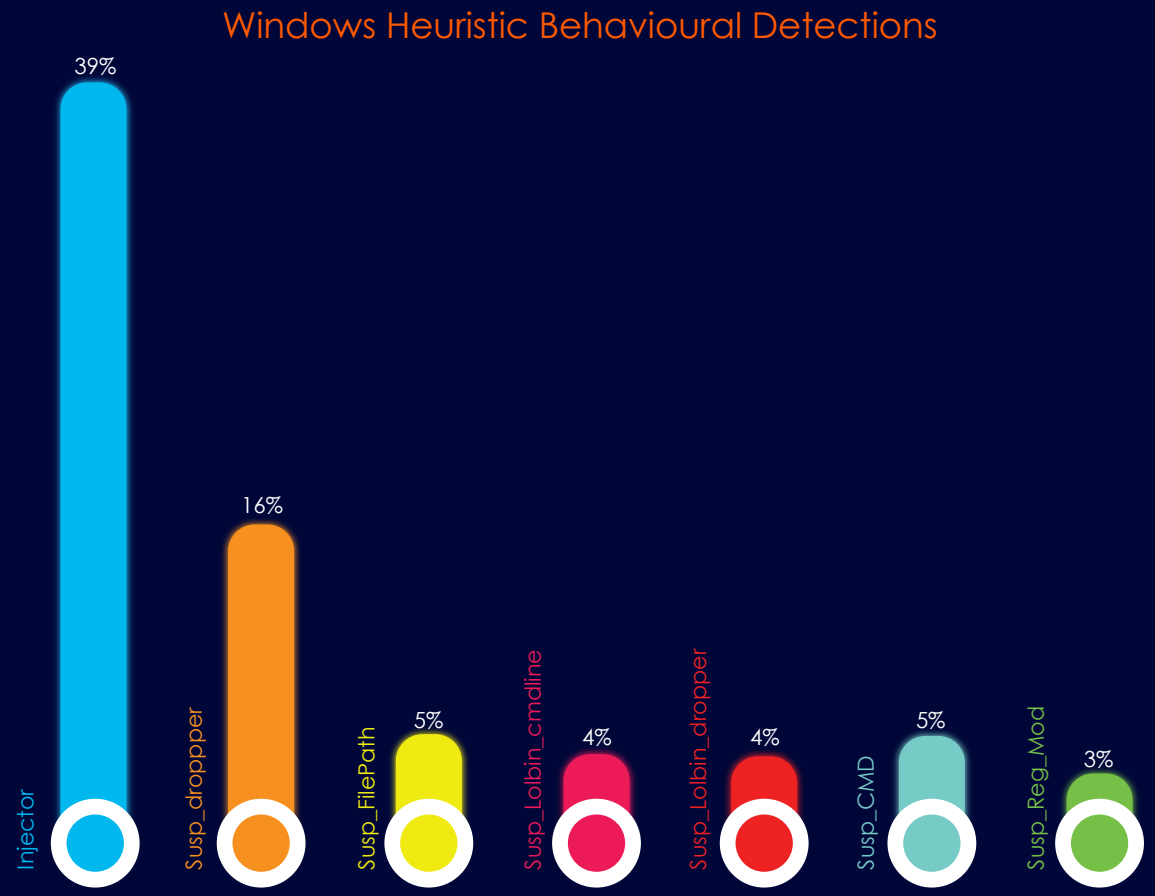
Most Prevalent Exploits



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.



This time Injectors increased by a significant percentage in comparison to the previous quarter. 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, retained their place and are used by threat actors in multi-stage attacks where additional malicious payloads are downloaded or dropped. Registry modifications are done by threat actors for persistence and execution of malware.

MITIGATION TIPS

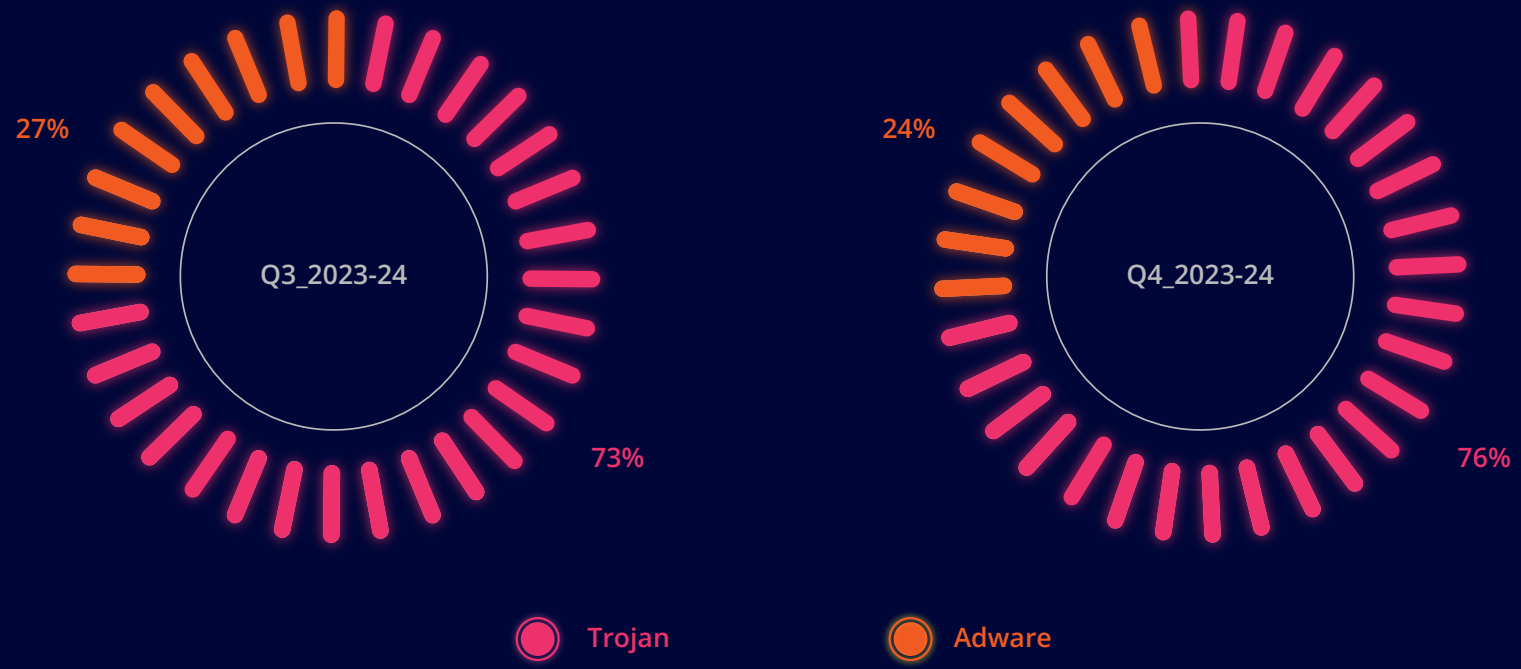
- Use an account without administrator privileges wherever possible
- Set up your operating system to enable auto-updates by default
- Be cautious when installing any software
- Backup your data on a regular basis

THE MOBILE DEVICE STORY

Imagine your phone not as a sleek device but as a vault overflowing with personal and financial treasures. Banking apps, social media accounts, even shopping receipts—everything's just a tap away. This allure of readily accessible data makes Android users prime targets for malicious actors seeking financial gain, identity theft, or cyber espionage.

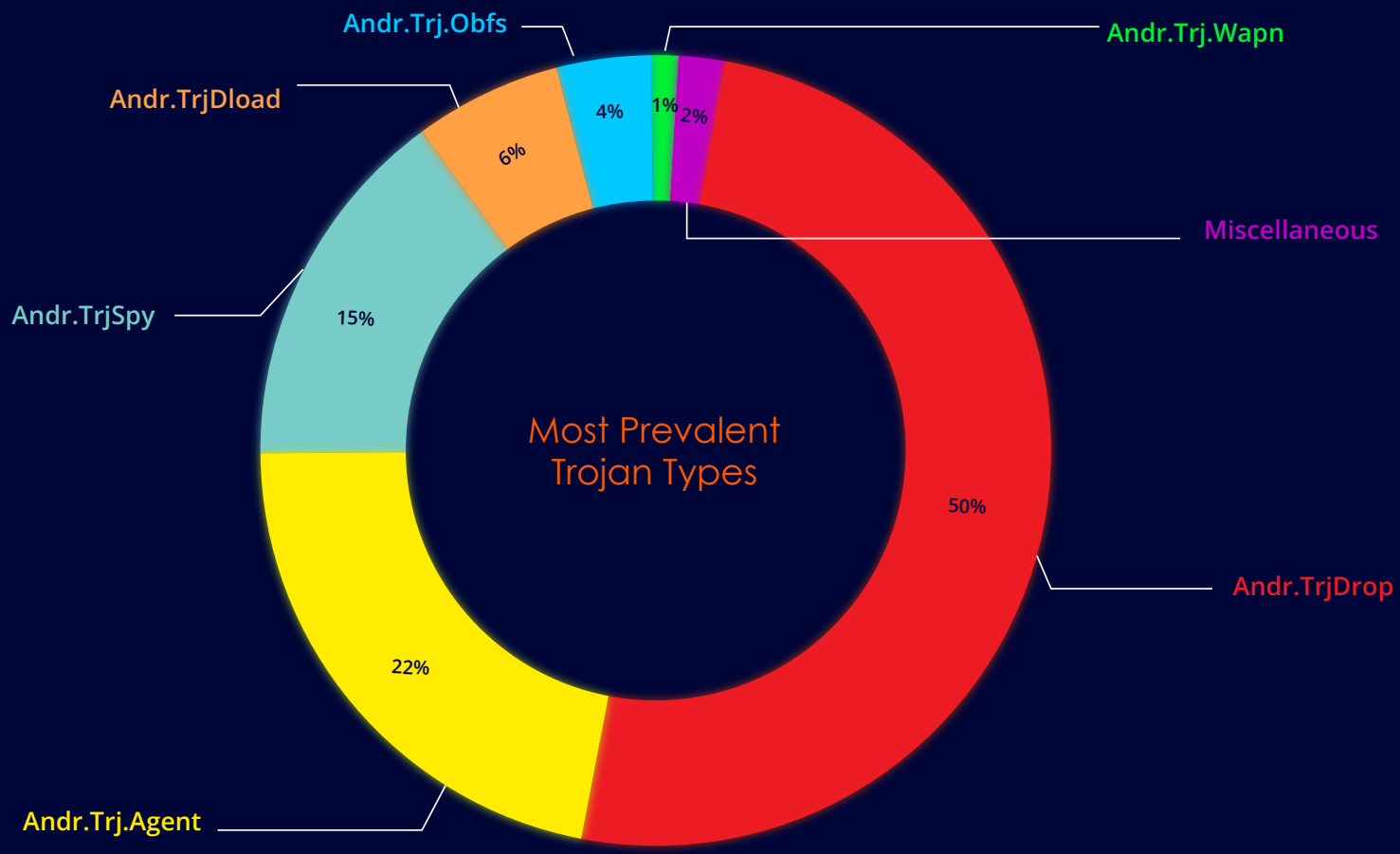
But the treasure chest analogy only tells half the story. Unlike Apple's tightly controlled App Store, the Android landscape thrives on diverse, often unregulated third-party stores. While this openness fosters innovation, it also creates a breeding ground for malware disguised as innocuous games, productivity tools, or even fitness trackers. These rogue apps slip through the cracks of less stringent security checks, infiltrating devices and wreaking havoc.

Adware vs Trojan Proportional Split



THE OMNIPRESENT TROJAN

What makes Trojans the scourge of the Android landscape? Their versatility, for one. From granting remote access to your phone, turning it into a puppet for hackers, to exploiting zero-day vulnerabilities, invisible cracks in the system ripe for exploitation, Trojans wield a diverse, ever-evolving toolkit.

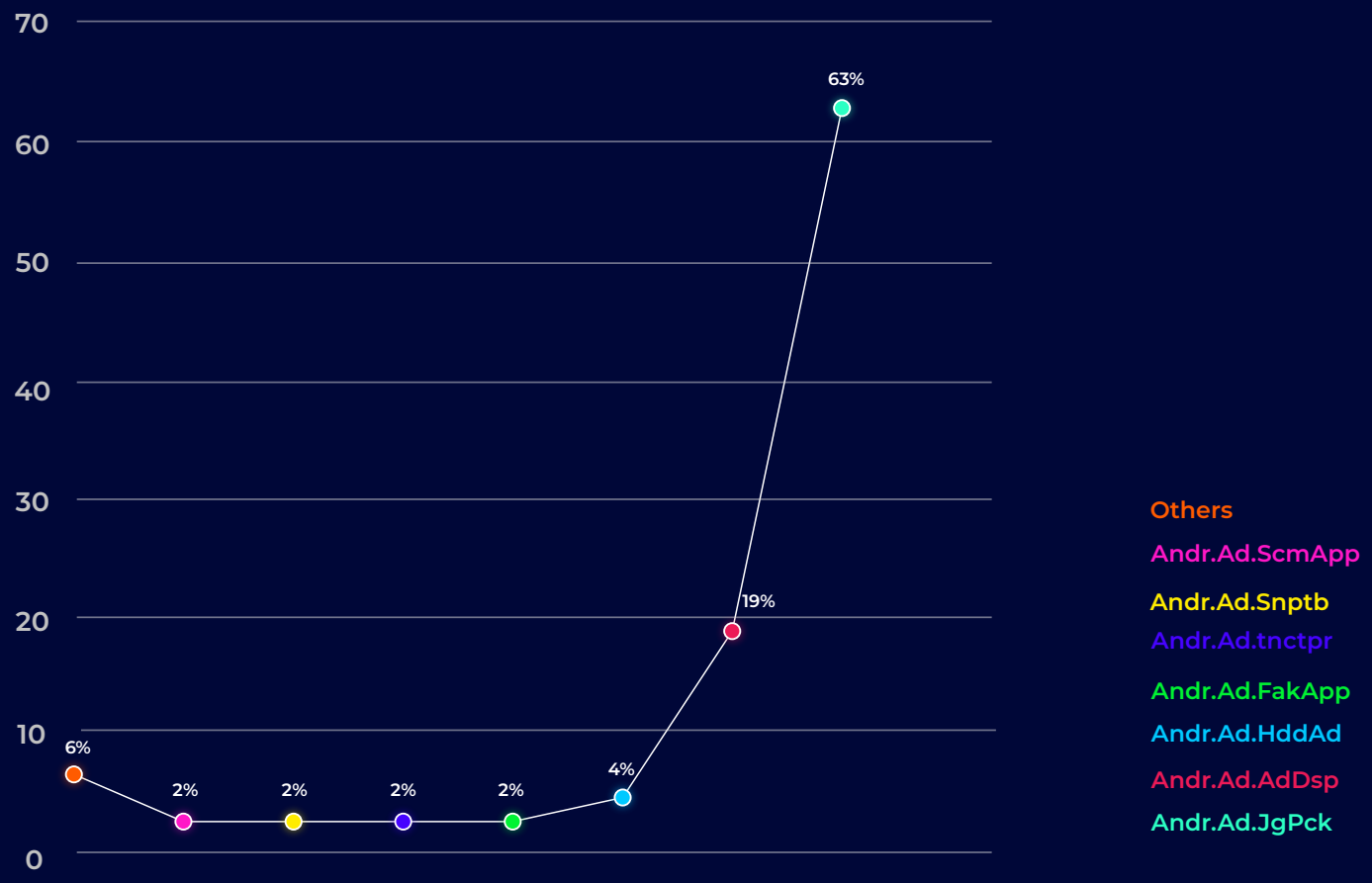


Droppers, Agents, and Spyware played a crucial role in contributing to the swell in the mobile threat landscape.

THE ADWARE SAGA

There was a slight increase in adware's presence last quarter. The same adware families continued to be prevalent this time too, in comparison with the previous quarter. Andr.Ad.JgPck topped the chart this time too with a significant increase. Adware can not only be annoying, but can affect your mobile device's performance and security.

Trend Line Showing the Adware Plague



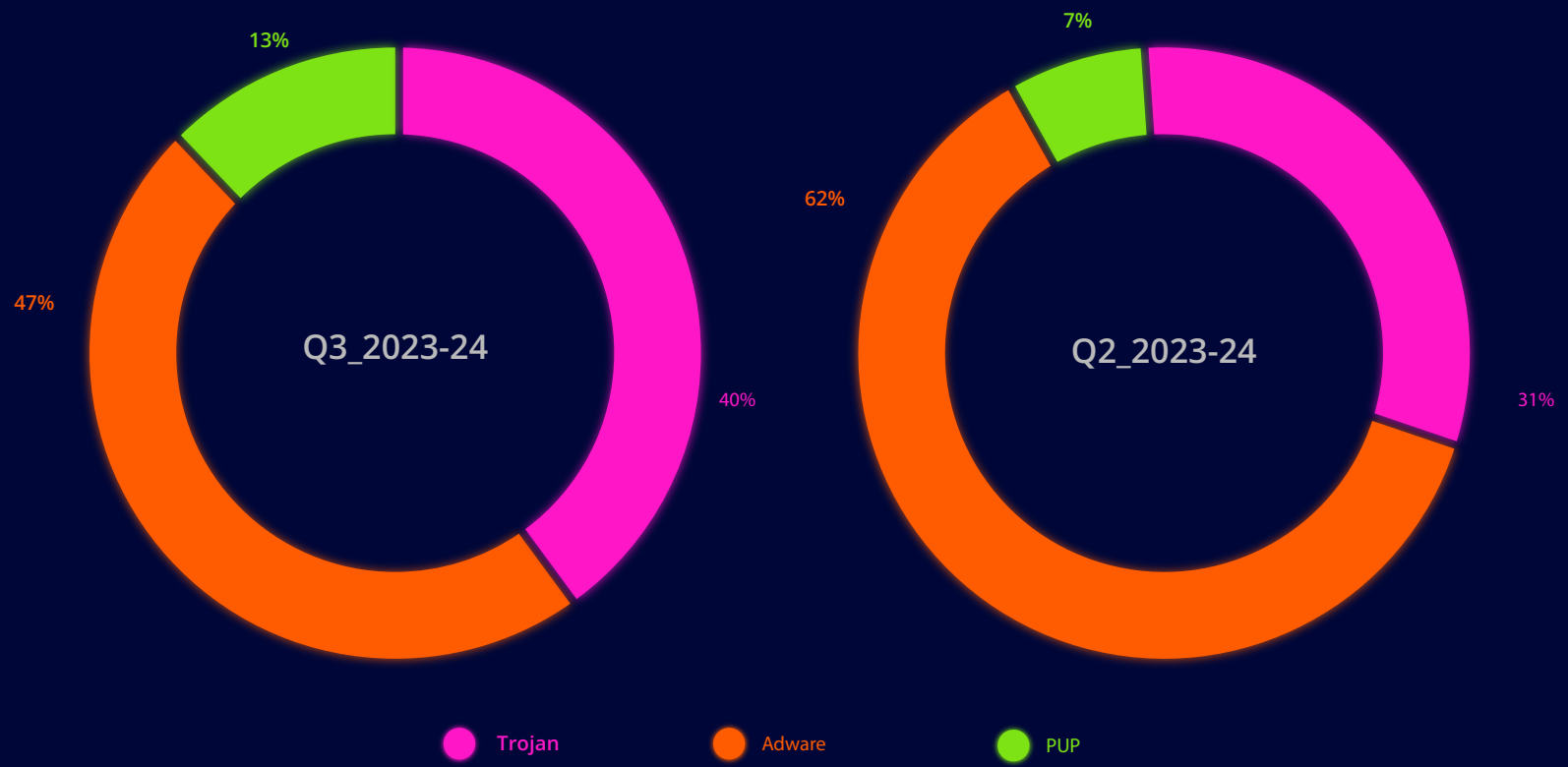
TIPS TO STAY SAFE

- 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

The rise in popularity amongst users has attracted threat actors to increasingly focus on Apple's ecosystem. Whether through sophisticated phishing campaigns masquerading as legitimate software downloads, benign adware-riddled free apps, or malware cleverly disguised as innocuous apps, the once-unbreachable fortress is now facing a rising tide of threats.

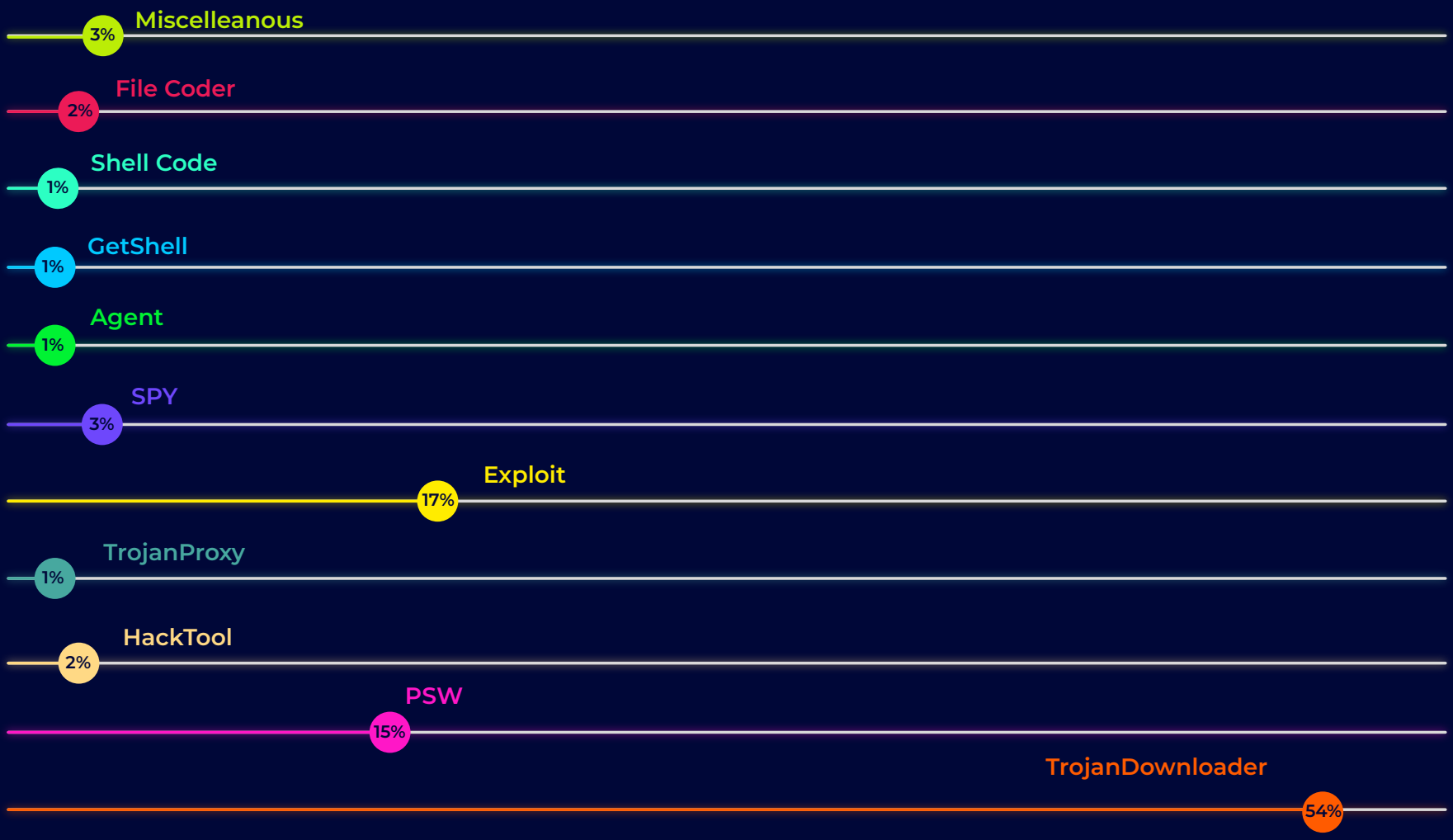
Trojan, Adware & PUP Proportional Split



THE UBIQUITOUS TROJANS

TrojanDownloader is the most significant contender, holding over half of the attacks that surfaced and were thwarted during the quarter.

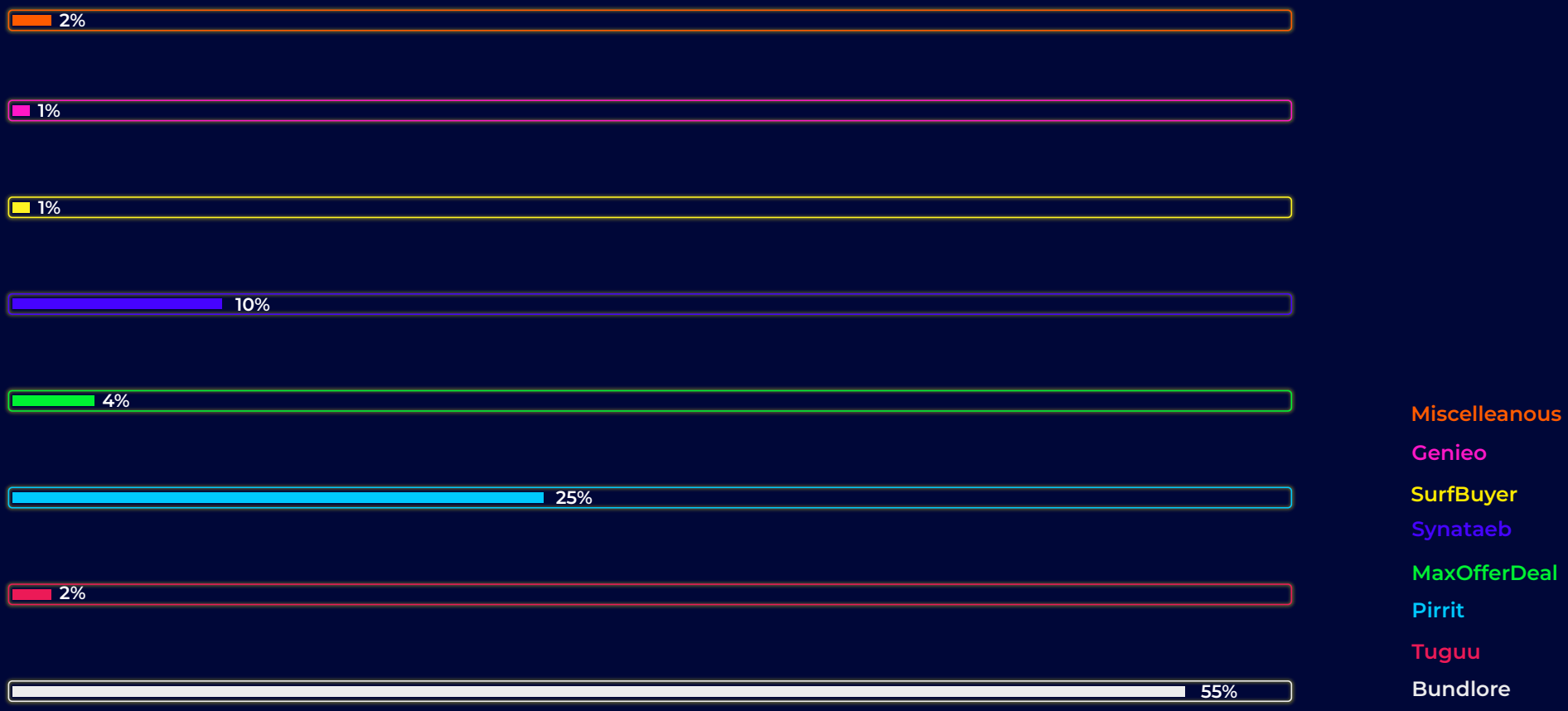
Trojan Detection Trend Line



THE ADWARE BROUHAHA

The most interesting observation from the macOS space is how two adware families, Bundlore and Pirrit, continuously held on to the reign even after several alerts.

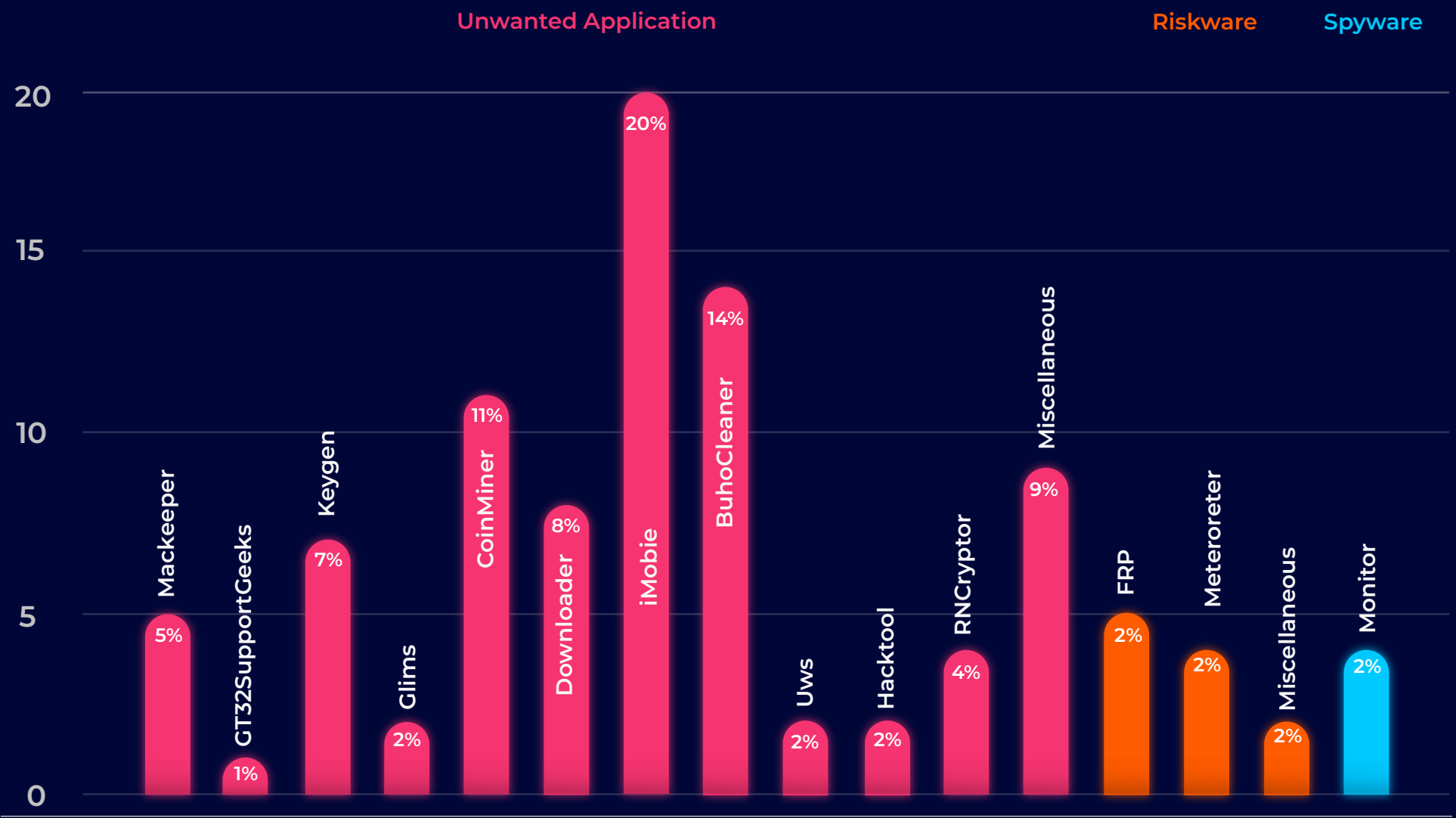
The Trend Line of Adware Variant Detections



A PINCH OF PUPS

From the chart below, apps masquerading as system cleaners or key generators continue to remain prevalent.

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.

Rusty Droid spells trouble for Android users

Threat actors use varied tactics to take complete control of a victim's device. One such is by disguising themselves as legitimate apps to dupe innocent victims. Here a Remote Access Trojan (RAT) dubbed Rusty Droid masquerades as a Chrome browser for Android that has capabilities to track a victim's financial activities, steal sensitive information, and initiate calls to premium-rate numbers, resulting in monetary and reputational losses for the victim. For more details refer
Rusty Droid: Under the Hood of a Dangerous Android Rat

This dangerous "Serpent" will steal your data

our researchers have analysed one stealer malware dubbed "Serpent" which steals credentials, and sensitive information from various applications and browsers, stays stealth and use a simplified method for data theft. Info stealers have been there for long and are a pervasive threat to the cyber world. And, as it evolves in sophistication, threat actors have been trying to reduce its footprint. Refer Uncovering the "Serpent" for more details.

How Mallox ransomware evades a Windows OS protection feature

We at K7 Labs, have discovered a ransomware evading Antimalware Scan Interface (AMSI) to stay stealth from AV Products. AMSI sends a buffer for sanning wherein third parties like AVs can subscribe, to receive this buffer for scanning and action. The ransomware in question, Mallox, runs and additional code for avoiding AMSI before running its regular code.

For more details refer Mallox Evading AMSI.

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

KEY TAKEAWAYS

Navigating the treacherous online terrain can feel daunting, especially for businesses and individuals who want to keep their data safe. Here's a quick guide to guarding your security posture, tailored for both enterprises and consumers:

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
Establish a secure network for all your endpoints	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

www.k7computing.com