K7 SECURITY

# Cyber Threat Monitor Report

Q1

# Contents


## Keep a Tab on these Cyber Threats

## Enterprise Insecurity

Case Study: Ransomware Mayhem across Enterprises

Safety Recommendations

## Vulnerabilities Galore

Authentication Vulnerability in BIG-IP

Spring4shell vulnerability in Java Spring Framework

LSA Spoofing Vulnerability

Server-side Injection in VMWare

MSDT prone to RCE Attacks

## Danger in the Internet of Things

Linux Kernel Double-Free Vulnerability

File Write Vulnerability in OAS platform

RCE Attacks in Carrier's ICS

Mitigation Techniques

## Windows Under Siege

Windows Malware Type Breakdown

Windows Exploits

Heuristic Host Intrusion Prevention System (HIPS)

Mitigation Tips

## The Mobile Device Story

Case Study: Fake Loan Apps on the Prowl

The Ubiquitous Trojan

The Adware Saga

Tips to Stay Safe

## Mac Attack

The Trojan Fracas

The Adware Brouhaha

A Pinch of PUPs

Safety Guidelines

## Key Takeaways

# Keep a Tab on these Cyber Threats

If anyone asks which technological innovation has changed the world, the answer would be the internet. The impact of the internet has changed every business functioning, also becoming a game changer in how people are evolving socially. But when accessing the internet, many of us skip or forget the basic thumb rule of the virtual world — online privacy, which the bad actors use to their advantage.

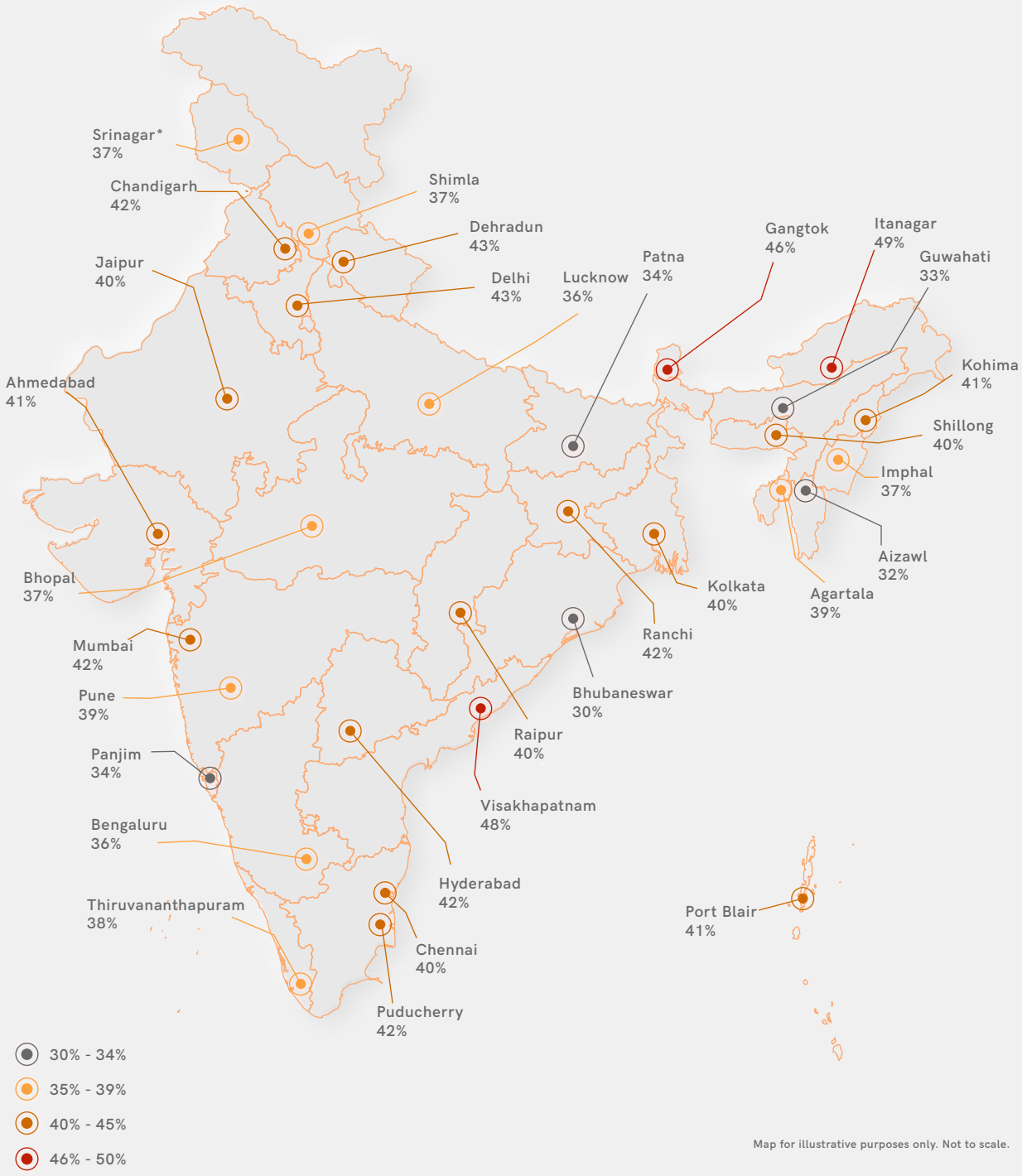
Apart from this, state sponsorship has made their ventures even more lucrative money-making machines. Threat actors these days are focusing more on rebuilding older malware and spend the saved time discovering new exploits and social engineering techniques. They also often handpick their targets according to priorities, and nobody is safe from their wrath until businesses and end-users embrace the basics of cyber hygiene alongside having sophisticated cybersecurity suites as a safeguard. The K7 Cyber Threat Monitor would help you perceive the latest trends in the contemporary threat landscape. Garnering data from tens and millions of real-life attack trends while protecting our customers, this report unravels the barometer of the threat landscape and salient mitigation tips to save you.

Furthermore, we have recently unleashed a new half-yearly threat report dedicated to the MSMEs. So do read, share the reports, and spread the good word around.

We wish you a safe online and offline life!

**Happy reading!**

# CYBER THREAT MONITOR - INDIA

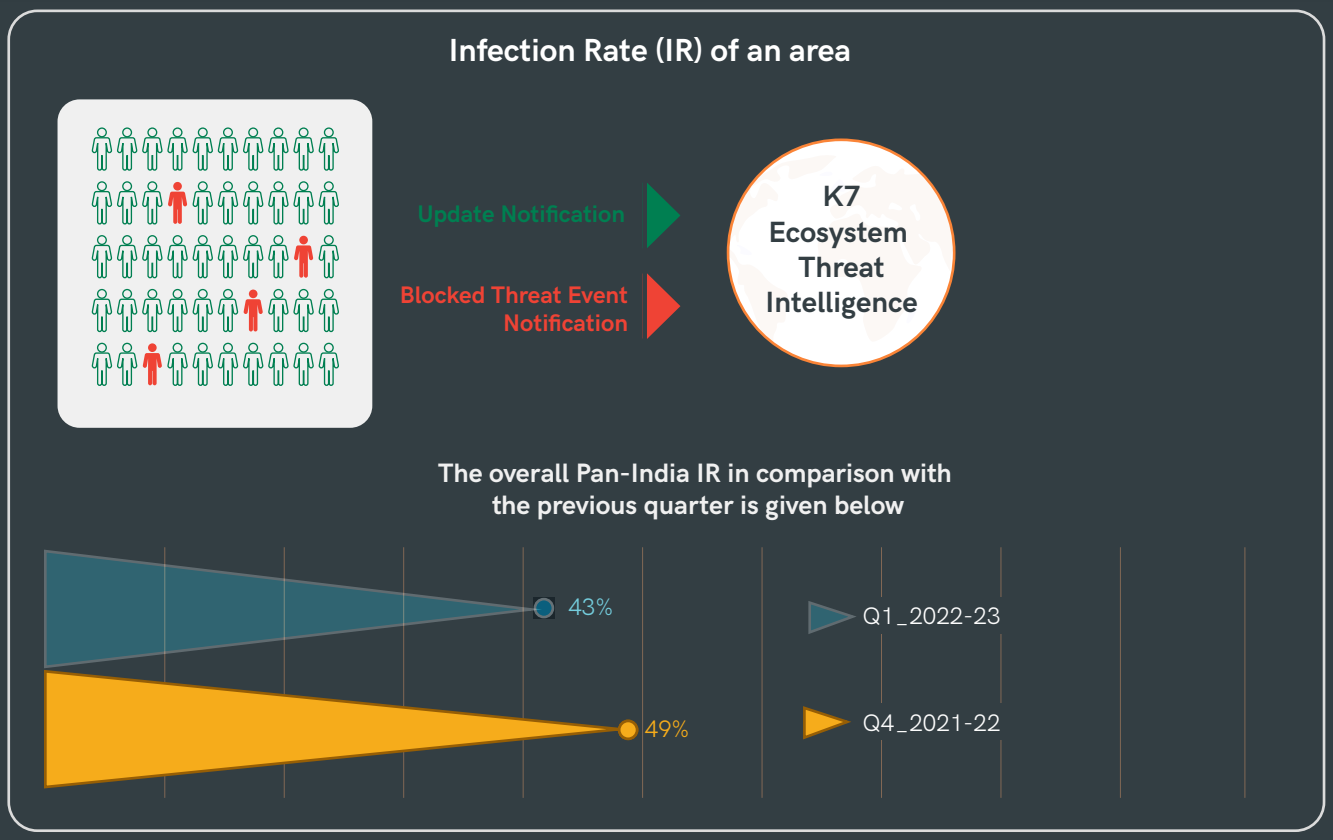



Map for illustrative purposes only. Not to scale.

# Regional Infection Profile

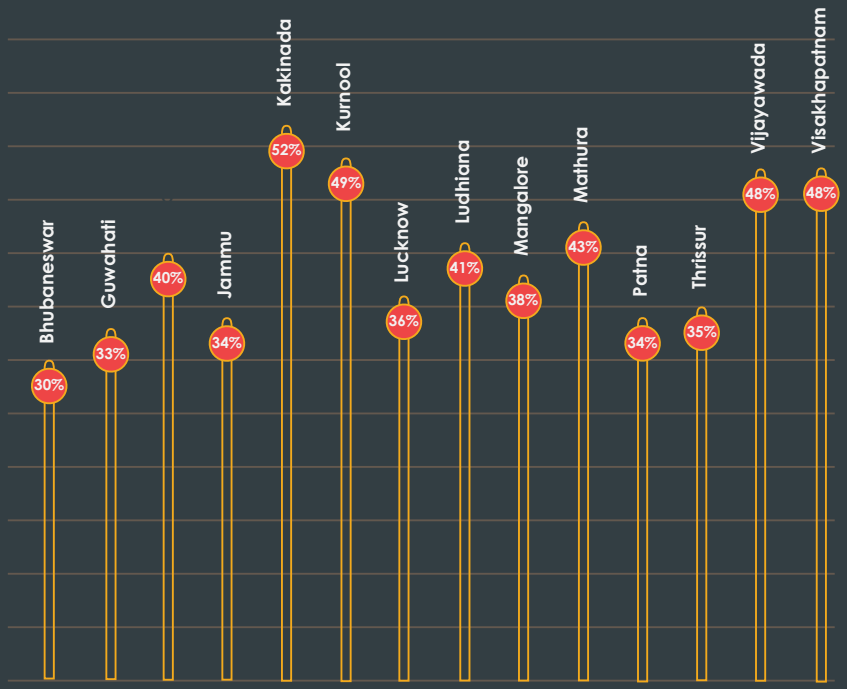
The ongoing Russia-Ukraine war and the resulting global economic slump have had unintended, but not unexpected, repercussions on the global threat landscape. Unpatched vulnerabilities have become a safe haven for threat actors to prey on enterprises and user devices alike. The geopolitical environment has helped ransomware and Ransomware-as-a-Service (RaaS) operators to take advantage of the same. Threat actors are also increasingly targeting smartphones; a fact proved by our telemetry statistics.
The countrywide Infection Rate is a snapshot of all these scattered events, showcasing the overall picture of the threat landscape.

## The Infection Rate is picturised as follows.




As hubs of industries and enterprises, Tier-1 cities are often more prone to attacks than Tier-2 cities. However, with the increasing number of startups in Tier-2 cities and the high number of digital transactions being made, Tier-2 cities have become more preferable attack zones to the perpetrators. The rising numbers are especially noticeable around Ludhiana, Mathura, and Jaipur, alongside the previously attack-prone zones such as Visakhapatnam, Vijayawada, Kakinada, and Kurnool.

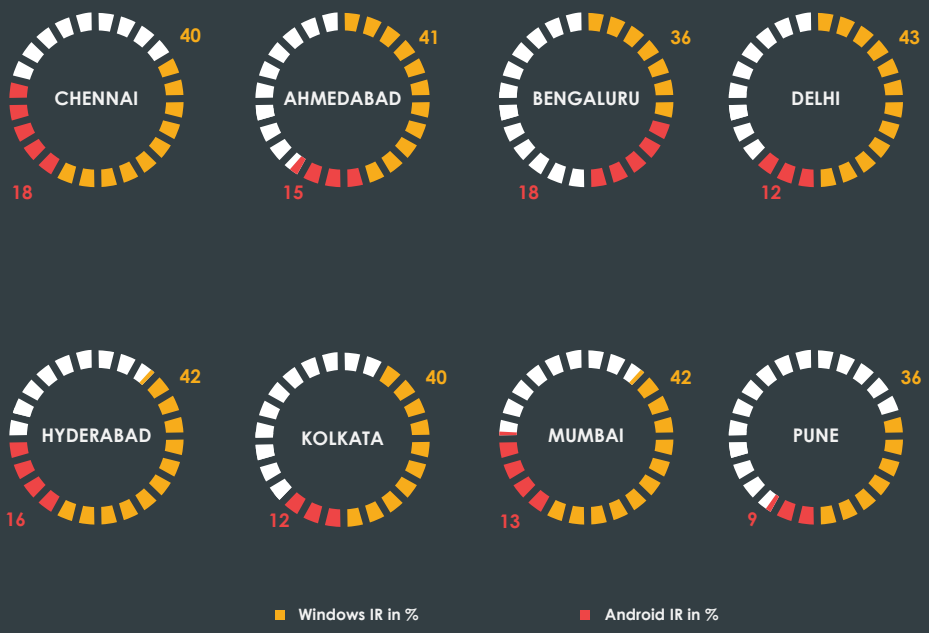
# Top 14 Infection Rates in Tier-2 Cities




## Infection Rate Comparison Across Platforms

Even though the popularity of mobile devices is soaring in contrast to desktops and laptops, most adversaries still prefer the latter for various reasons. Ransomware operators are still more active on Windows among other desktops/laptop platforms. However, the last quarter showed that there has been a significant rise in malware targeting mobile devices in comparison with the previous quarter, indicating that threat actors have started eyeing mobile devices as lucrative targets.

## Windows IR vs Android IR



# Enterprise Insecurity

The number of ransomware attacks are rising globally, and enterprises of all sizes are facing the brunt of it. The increasing number of successful attacks encourage ransomware and Ransomware-as-a-Service (RaaS) developers to invest more and increase their subscription base.

Last quarter too, there was no respite from the soaring ransomware attacks. We have presented before you one of the significant threats noticed in the quarter.

# Case Study: Ransomware Mayhem across Enterprises

One of our enterprise customers reported a ransomware attack on their network. K7 Labs researchers' analysis led to the following insights:


1. Threat actors tried bruteforcing themselves via RDP multiple days before the actual breach. It was also noticed that RDP was configured using the default port in the pivot system
2. Threat actors also tried getting into the pivot system through the publicly exposed MSSQL service
3. Evidence of security product breach was noticed, though the product itself was not fully disabled
4. Threat actors used enumeration tools, PowerShell, and WMI queries for the breach
5. Finally, attackers managed to execute ransomware,thereby encrypting the user files

# Safety Recommendations

- 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.
- Frequently audit user accounts and their permission levels. Set alerts on any unauthorised user accounts created.
- Change the password of default accounts, and disable unused accounts.

# Vulnerabilities Galore

Safeguarding their business and related data is of high priority for any enterprise. That said, most of the devices and applications being used by them come with their share of vulnerabilities, which paves a way for the threat actors who are waiting to exploit the same to breach into the network and cause colossal damage.
Last quarter, we spotted numerous vulnerabilities on critical devices and applications, which if exploited could become a gateway for the threat actors to abuse your network and devices.

We have listed a few prominent ones.

## Authentication Vulnerability in BIG-IP

CVE-2022-1388 is an authentication bypass vulnerability in iControl REST of F5's BIG-IP. This can be used by threat actors to launch remote code execution (RCE) attacks. This has been rated as a critical vulnerability having a CVSS base score of 9.8 and has been exploited in the wild.

Vulnerable versions of BIG-IP are 16.1.0 - 16.1.2, 15.1.0 - 15.1.5, 14.1.0 - 14.1.4, 13.1.0 - 13.1.4, 12.1.0 - 12.1.6, 11.6.1 - 11.6.5

## LSA Spoofing Vulnerability

CVE-26925, is a Local Security Authority (LSA) Spoofing vulnerability that allows an unauthenticated attacker to call a method on the LSARPC interface and persuade the domain controller to authenticate using NTLM.

Vulnerable versions are Windows 7, 8.1, 10,11 and Server 2008, 2012, 2016, 2019, 2022

## Spring4shell Vulnerability in Java Spring Framework

A critical vulnerability, CVE-2022-22965, in the Java spring framework results in unauthorized RCE attacks, when few objects are passed in with their class names in a HTTP request. This has been dubbed as spring4shell, for being similar to the Java based log4shell vulnerability.

Spring Framework versions 5.3.0 to 5.3.17 or 5.2.0 to 5.2.19, and older versions are vulnerable to the same.

Vulnerable products include Apache Tomcat versions<10.0.20, <9.0.62 and <8.5.78 and VMware

## Server-side Injection in VMWare

CVE-2022-22954, is an RCE vulnerability in VMWare which is due to the server-side template injection. An unauthenticated attacker with network access can trigger the same to execute an arbitrary command as the VMware user in VMware Workspace ONE Access and Identity Manager.

Cybersecurity and Infrastructure Security Agency (CISA) warned of the imminent threat this vulnerability poses as it is being exploited in the wild already.

Vulnerable versions are VMware Workspace ONE Access (Access) 20.10.0.0 - 20.10.0.1, 21.08.0.0 - 21.08.0.1, VMware Identity Manager (vIDM) 3.3.3 - 3.3.6

## MSDT prone to RCE Attacks

CVE-2022-30190, is an RCE vulnerability in Microsoft Support Diagnostic Tool (MSDT) which can be exploited by threat actors when MSDT is called from another application like Word using the MS Protocol URL.

Vulnerable products are Windows 7, 8, 10 , 11, Server 2008, Server 2012, 2019

# Danger in the Internet of Things

Many IoT device manufacturers focus primarily on unveiling new devices and do not usually fix the vulnerabilities in their older devices or previous versions of it. Retaining such older devices on your network is synonymous with inviting trouble on the web. But many businesses still use them for budget and other concerns, thus enticing the bad actors to take a chance.

Here are the toppers from the infamous list of IoT vulnerabilities during the quarter, listed as eye-openers.

## Linux Kernel Double-Free Vulnerability

A double-free vulnerability, CVE-2021-22600, in the packet network protocol implementation in the Linux kernel could lead to memory corruption, thereby allowing threat actors to execute an RCE attack.

## RCE Attacks in Carrier's ICS

A vulnerability, CVE-2022-31479, could lead to RCE attacks in Carrier's ICS. This vulnerability may allow an attacker to modify the host name with a specially crafted name allowing shell command execution during the process of core collection.

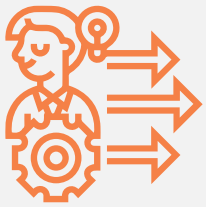
Vulnerable Products are HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.302 for the LP series and 1.296 for the EP series.

## File Write Vulnerability in OAS platform

A file write vulnerability, CVE-2022-26082, in Open Automation Software (OAS) Platforms' OAS Engine SecureTransferFiles functionality, could lead to RCE attacks by threat actors using specially crafted series of network requests.

OAS Platform is often found in Industrial Control Systems (ICS) where it is used to connect industrial and IoT devices, and SCADA systems.

OAS Platform V16.00.0112 is vulnerable to it and can be easily exploited in the wild.



# Mitigation Techniques

- Continuously monitor all IoT devices on your network and keep track of its configurations
- Ensure all your devices are kept up to date and patched against the latest vulnerabilities

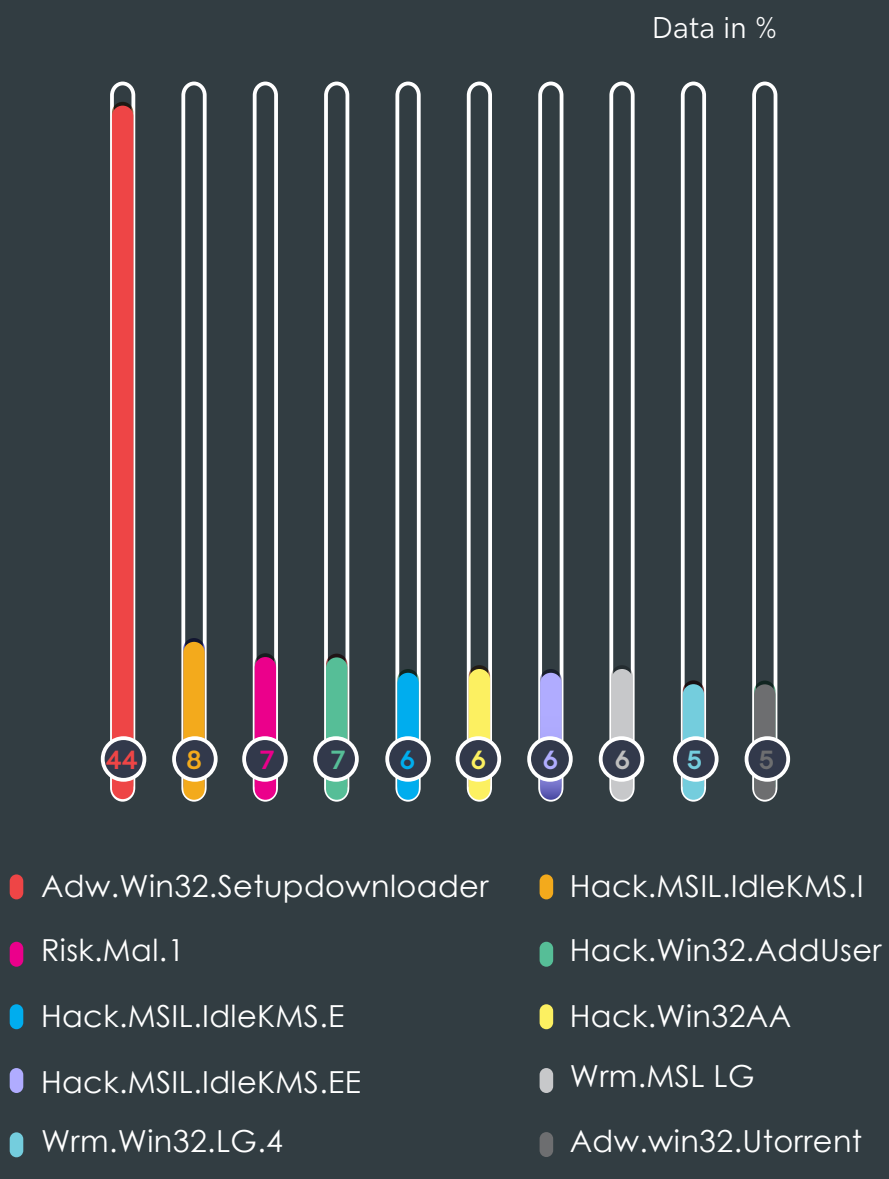
# Windows Under Siege

## Windows Malware Type Breakdown

In Q1_2022-23, we didn't see any solace from the ushering force of malware. Last quarter, Adw.Win32.Setupdownloader, a free subscription-based adware program, remained a colossal force throughout the period.

The presence of Adw.Win32.Setupdownloader is especially noticeable since its existence had increased trifold in comparison with the previous quarter.

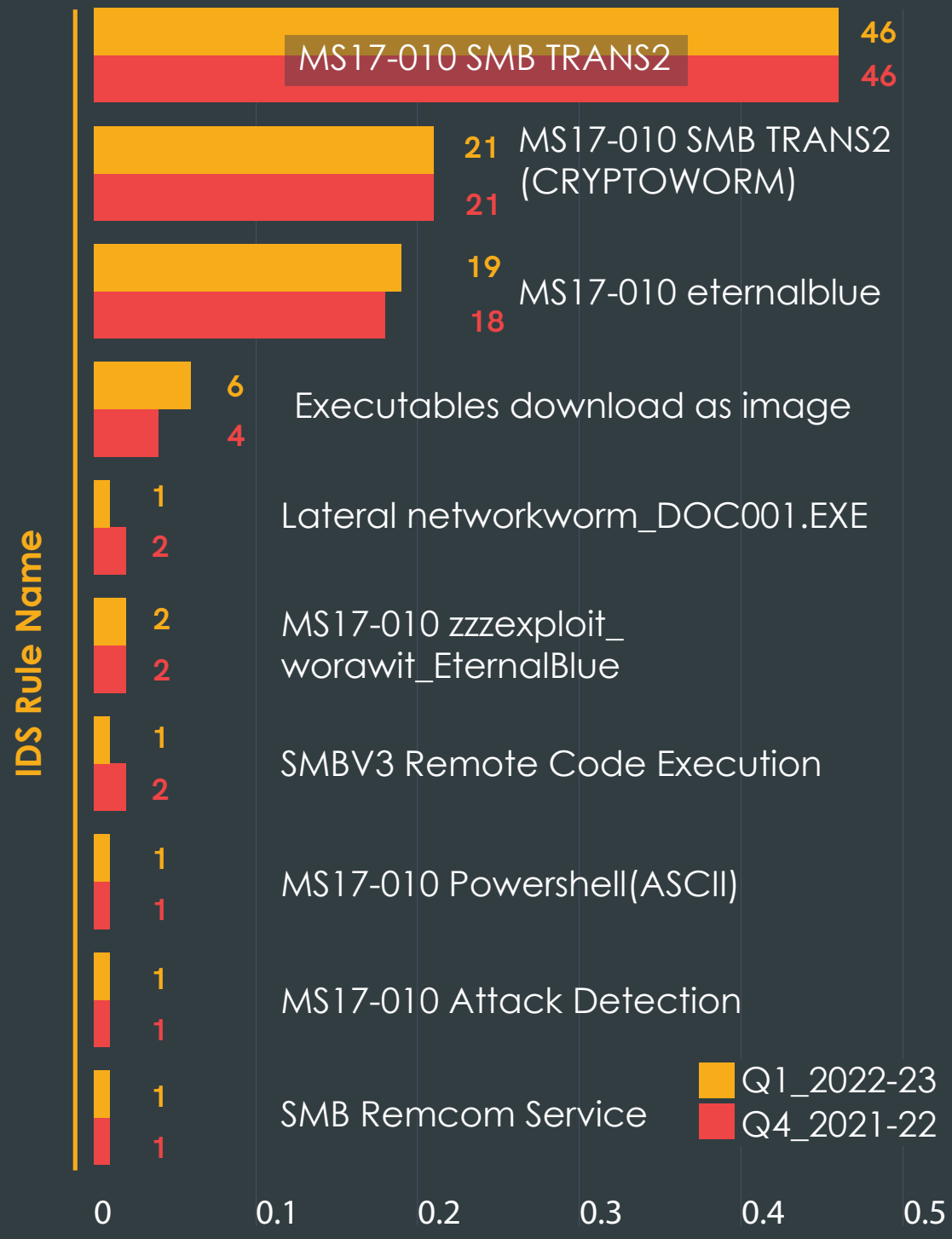
### Split of Windows Top 10 Detections



# Windows Exploits

Microsoft, being the owner of the most popular OS, puts multiple efforts to safeguard its devices by releasing regular patches to weigh down the abundance of Windows vulnerabilities. Despite these steps, there seems to be no respite from exploitation of these vulnerabilities.

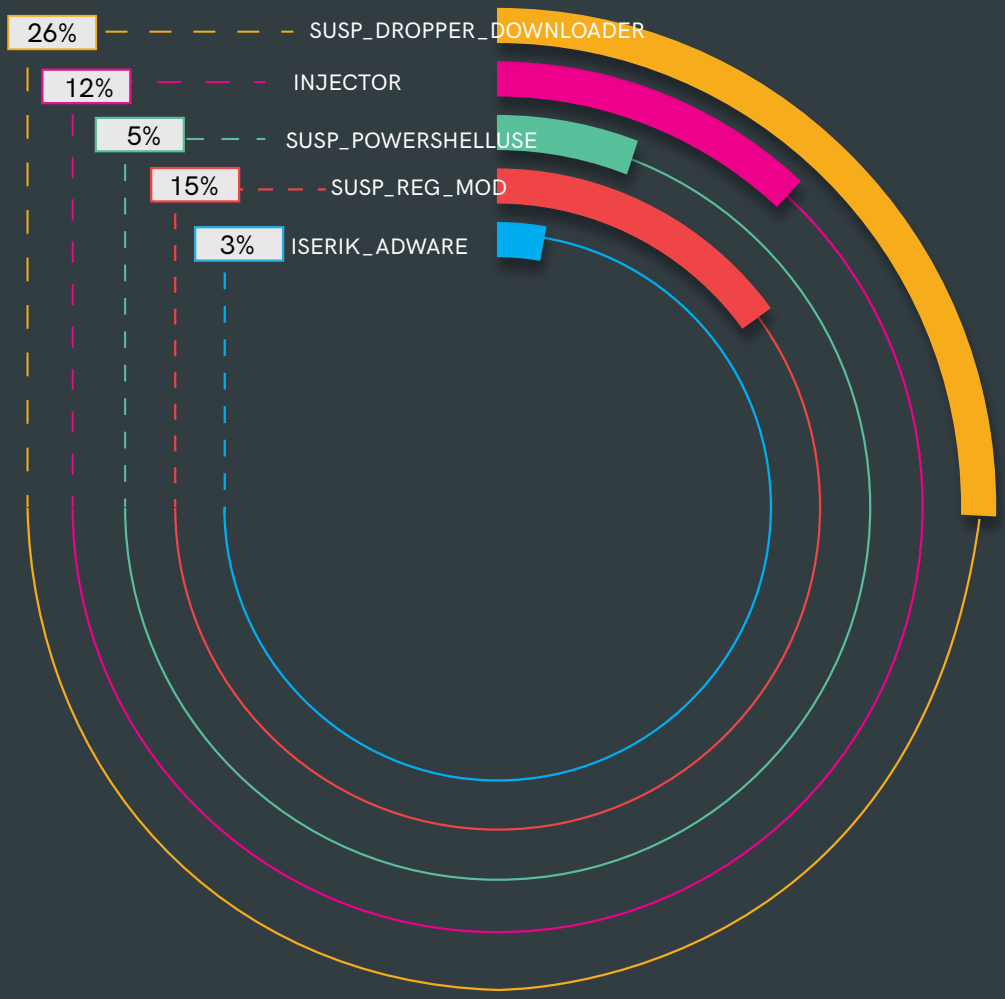
## Most Prevalent Exploits



# 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 highly 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/Downloaders occupied a significant chunk followed by Registry Modifiers and Injectors. 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 OS services. This is usually done to evade AV detections and for privilege elevation. Our behavioural detection also identified malware that were hosted as malicious scripts on websites abusing PowerShell and Windows command shell.

# Mitigation Tips

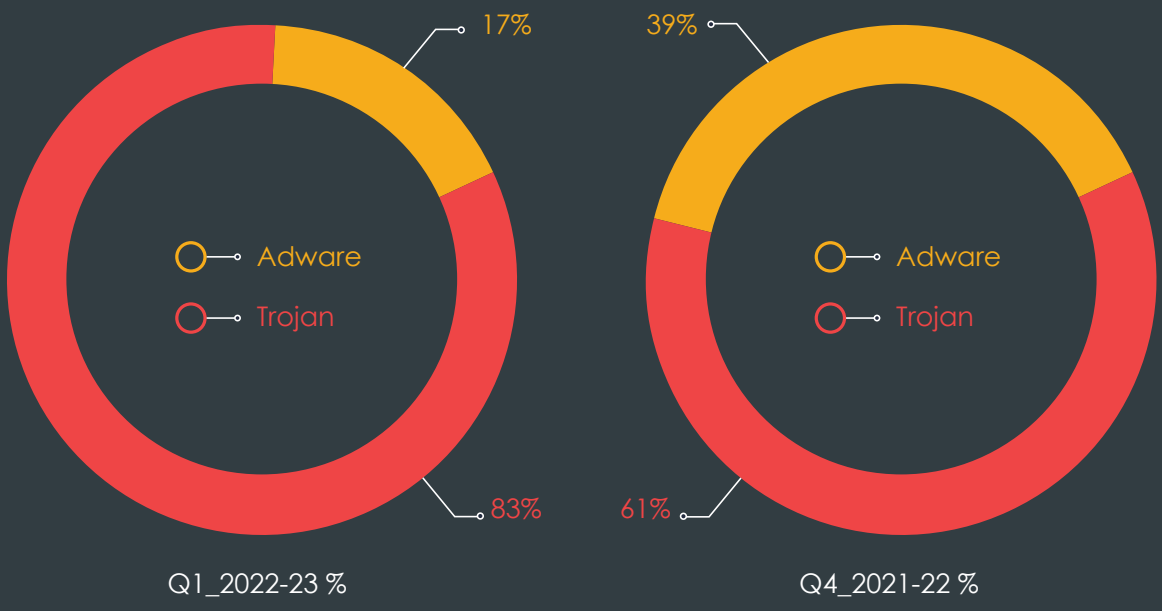
- Keep your devices and its software updated and patched against the latest vulnerabilities
- Perform risk assessments to determine vulnerabilities
- Avoid clicking on pop-up windows.especially, the ones asking you to download apps

# The Mobile Device Story

With time, as more and more users are strengthening their cyber defenses, so have the threat actors adapted to the same by using  more innovative, sophisticated and targeted attacks. The comparison graph below displays how the threat actors focus more on developing Trojans masquerading as legitimate-looking apps to heighten their menace.

In many of our previous editions of the CTM report, we have rung the caution bell on how fake apps are doing the rounds on Google's Play Store and other third-party websites.

## Adware vs Trojan Proportional Split




Q1_2022-23 %

Q4_2021-22 %

# Case Study: Fake Loan Apps on the Prowl

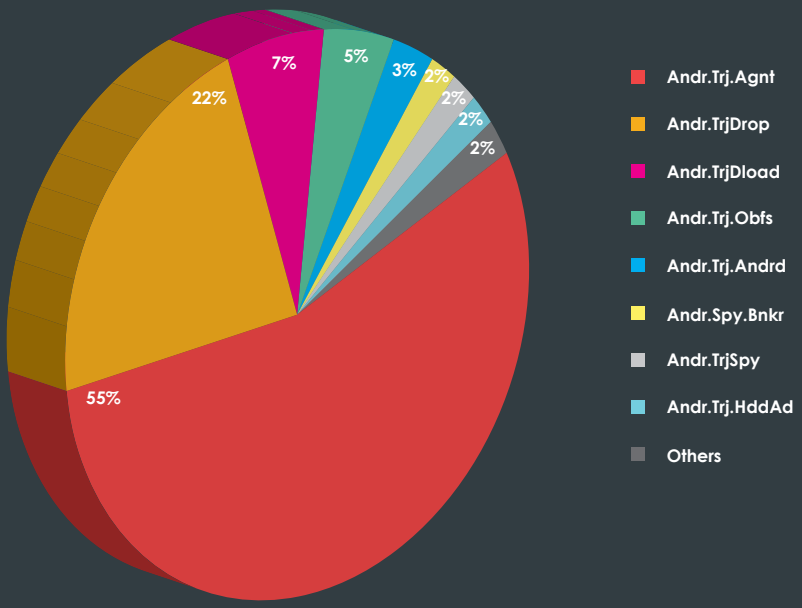
Recently, we came across something similar wherein fake instant loan apps were seen duping users. Though this does not come as a bolt out of the blue for the user, we are duty-bound to warn you of such apps. So let us now delve into the details.

1. On downloading and installing fake loan/cash advance apps from the Play Store, it lends the desired amount of money to the user as agreed and it asks for a set of permissions like camera, contacts
2. On granting the permissions, it proceeds to collect contacts, images and videos from the users' device for threatening them in future
3. The loan agent then uses abusive language for extorting money from the user, even after the victim has paid back the loan amount

## The Ubiquitous Trojan

In Q1_2022-23, Andr.Trj.Agnt topped the charts meaning threat actors are using malicious apps to execute without the user's knowledge and steal information. Andr.TrjDrop followed next in the line, indicating that threat actors are still creating apps that contain other malicious apps within it.

### Most Prevalent Trojan Types




## The Adware Saga

Despite the steady plunge in visibility, adware families such as Andr.Ad.JgPck, Andr.Ad.AdDsp, and Andr.Ad.Atns have managed to retain their space in the Android threat landscape. And it was Andr.Ad.JgPck that topped the charts in the last quarter too.

### Trend Line Showing the Adware Plague

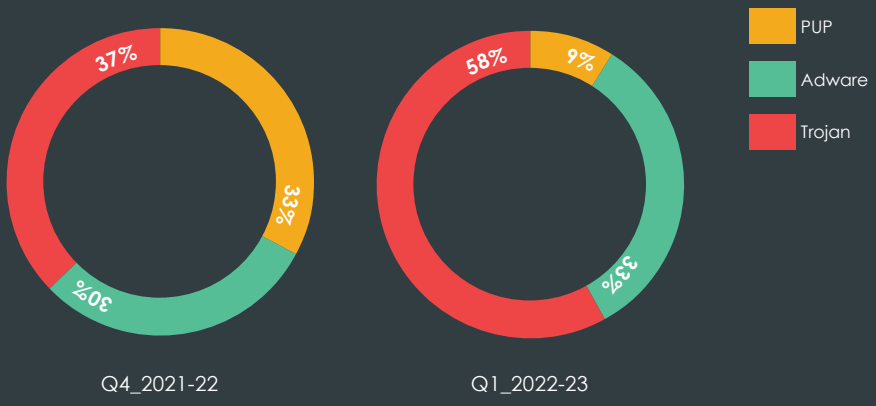
# Tips to Stay Safe

- Avoid installing apps from 3rd party app stores and/or unknown sources
- Carefully read the user reviews before downloading any app
- Be aware of what information the app collects from the user's device.
- Protect your device and data with a reputed security product like K7 Mobile Security and keep it up to date to protect yourself from the threats lurking around

# Mac Attack

There is nothing new about the continuous uptick of threats in the macOS threat landscape. Instead, the proportion of attack types display a riveting fact - threat actors eyeing macOS are rapidly shifting their focus from adware and PUP to various Trojan families as shown below.

## Trojan, Adware & PUP Proportional Split



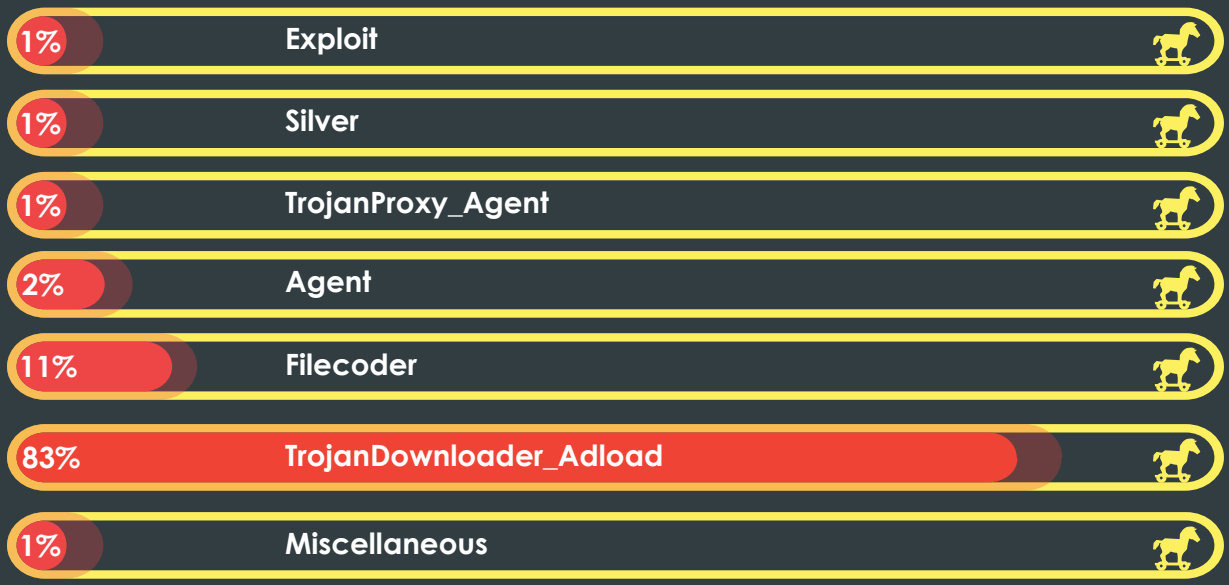

The comparison chart shows a significant decline in PUPs and a slight increase in the adware visibility.

## The Trojan Fracas

Interestingly, the massive surge of Trojans in the macOS space is because of TrojanDownloader.Adload. This downloader malware has been dominating its presence even in the past few quarters and does not seem to show any sign of stopping anytime soon.

The burgeoning proportion of Adload also depicts the growing dependence on downloader malware to victimise users and open a backdoor for various nefarious purposes.

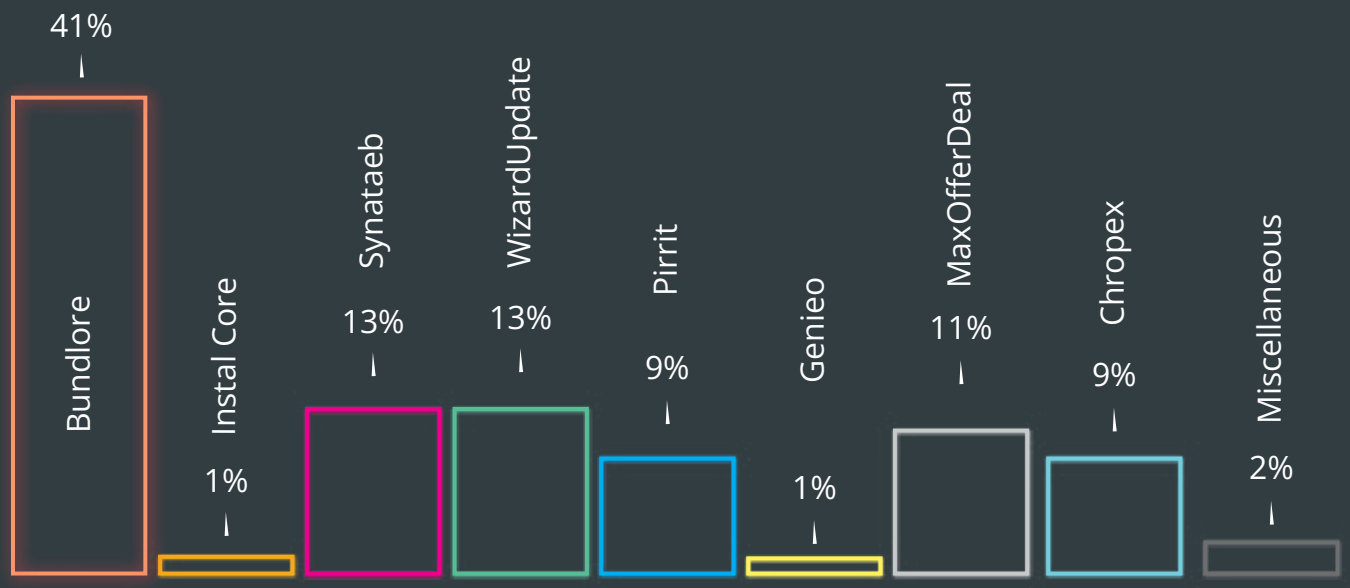
## Trojan Detection Trend Lines



## The Adware Brouhaha

Like the visibility of Trojans, the adware visibility is also dominated by the infamous adware Bundlore. This quarter's other three shady adware were Synataeb, WizardUpdate, and MaxOfferDeal.

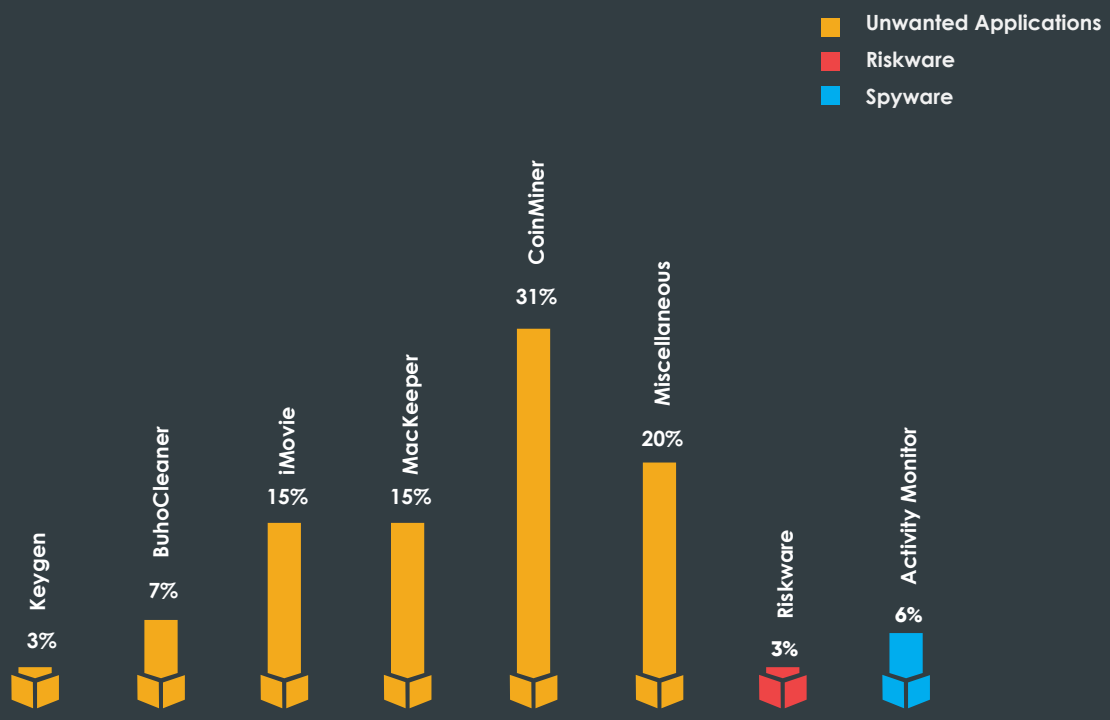
### The Trend Line of Adware Variant Detections




## A Pinch of PUPs

Even with the plunging numbers, PUP visibilities are not shrinking in reality. Instead of triggering PUPs directly on a strictly-controlled macOS platform, the sophisticated threat actors use downloader Trojans to deliver PUPs, among other malware. CoinMiners are another popular PUP used for minting cryptocurrencies illicitly.

### 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

Threat actors have myriad ways to target networks and devices. To avoid being trapped, having a reputable security suite is the primary degree of caution that one can take. Apart from this, there are other precautionary measures you have to embrace to ensure safety in your business and personal life.

Here are a few of them.

## 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

Implement an exhaustive security management framework

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

Invest in a good cyber defense for your mobile

Perform regular audits to check what information your apps are accessing

K7 SECURITY

JULY 2022



www.k7computing.com