K7 SECURITY

Cyber Threat Monitor Report

Q4_2021-22

www.k7computing.com

Contents

Cyber Threats Under Our Magnifying Glass

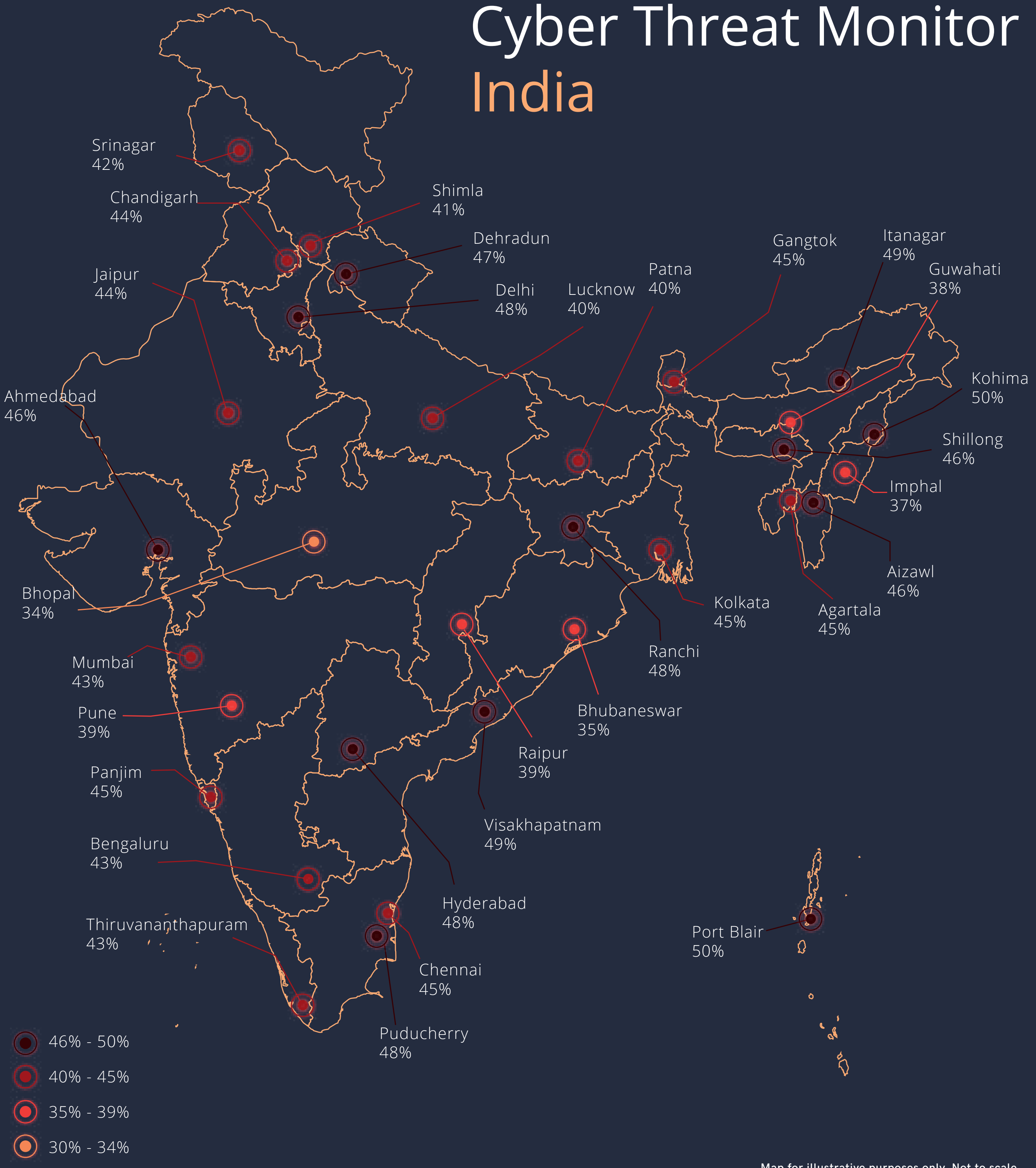
Amid the world's chaotic situation, the threat actors too are creating mayhem by multi-folding their attacks. Nation-state threat actor activities are increasing as a new weapon of modern warfare and nowadays, threat actors are also seen to upload ransomware kits, exploit kits, phishing kits and other malware kits onto the dark web for sale at "reasonable costs" making it easier for amateur adversaries to plan attacks and earn quick money. From our telemetry statistics, we gleaned that in Q4_2021-22, the proportion of attacks was 49%, exceeding by 7% in comparison to the previous quarter.

Threat actors these days are getting more and more sophisticated with their attack, obfuscation and intrusion techniques. Social engineering techniques such as phishing are also being weaponized more, resulting in more successful attacks. To survive in this state of turmoil, it's always a good idea to nip the problem in the bud by adopting necessary safety precautions.

K7 Labs has spent many hours in research and detection of malware, which has been put to use in compiling this report. The latest K7 Cyber Threat Monitor report not only offers a snapshot of the critical analysis of all the prevalent cyber-attack techniques and trends in the last quarter but also offers an insight into the present and future threat landscape. This actionable threat landscape report also includes the required cyber hygiene practices one should embrace to stay safe and protected.

We recommend you to share this report among your colleagues, friends and family members to raise awareness of the prevalence of cyber threats, thus helping to make the digital world a safer place!

Cyber Threat Monitor
India

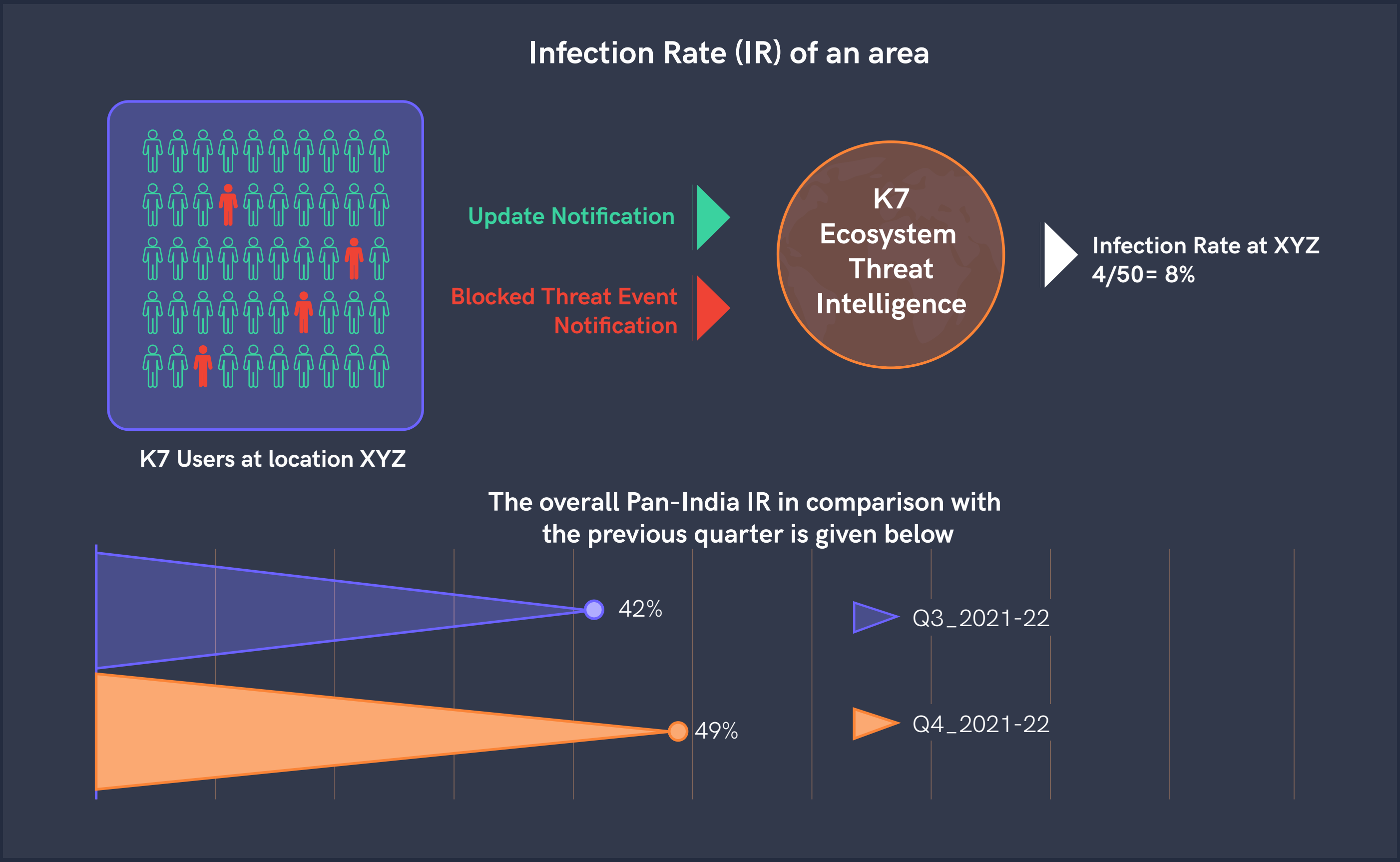


Map for illustrative purposes only. Not to scale.

Regional Infection Profile

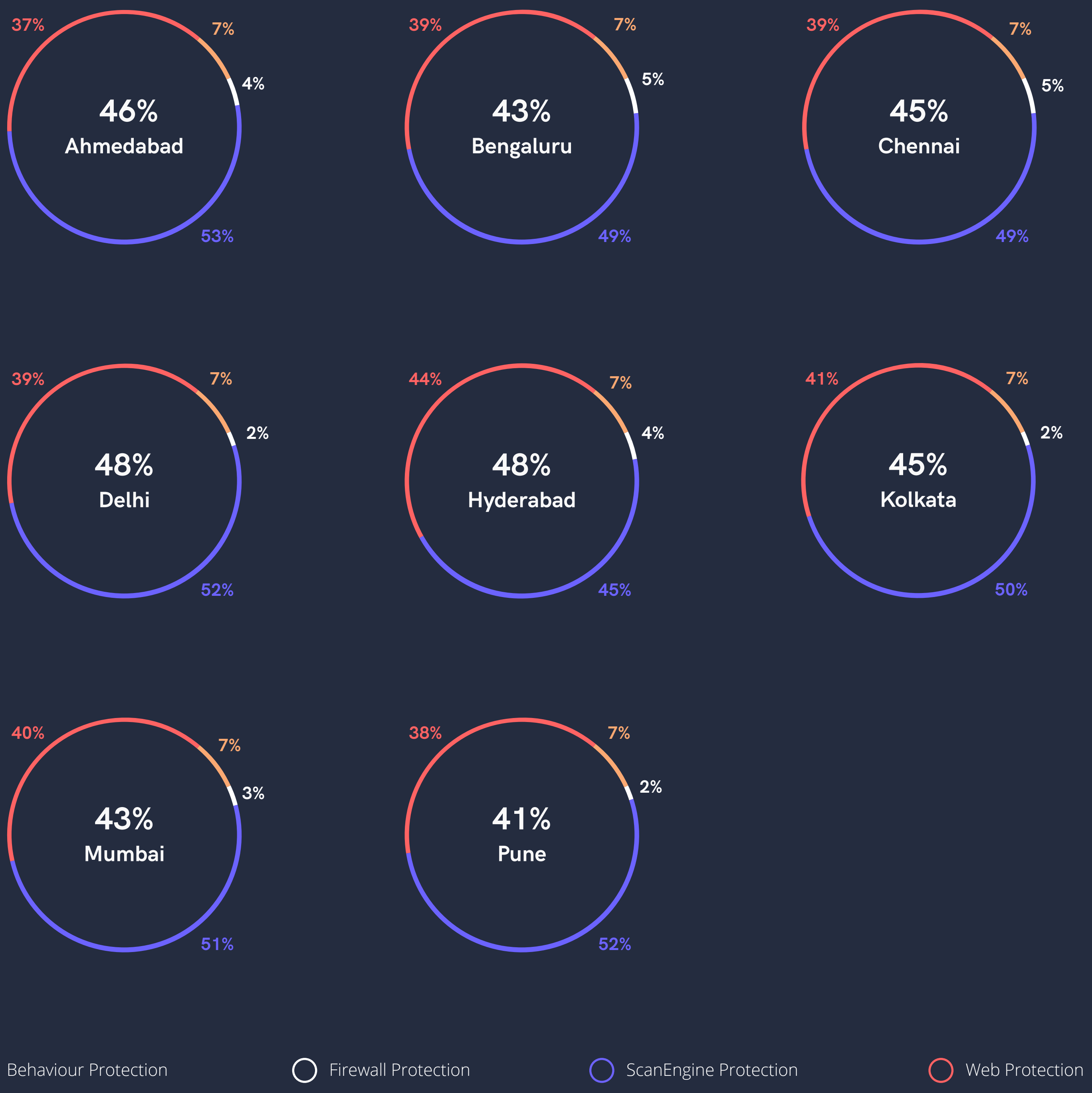
Infection Rate (IR) is a critical benchmark we use for an analytical overview of the countrywide threat landscape. In addition, our telemetry develops a detailed dataset to offer a snapshot of the quarterly threat landscape stemming from various detection layers including URL-based, engine and firewall level as well as behavioural.

The Infection Rate is picturised as follows.



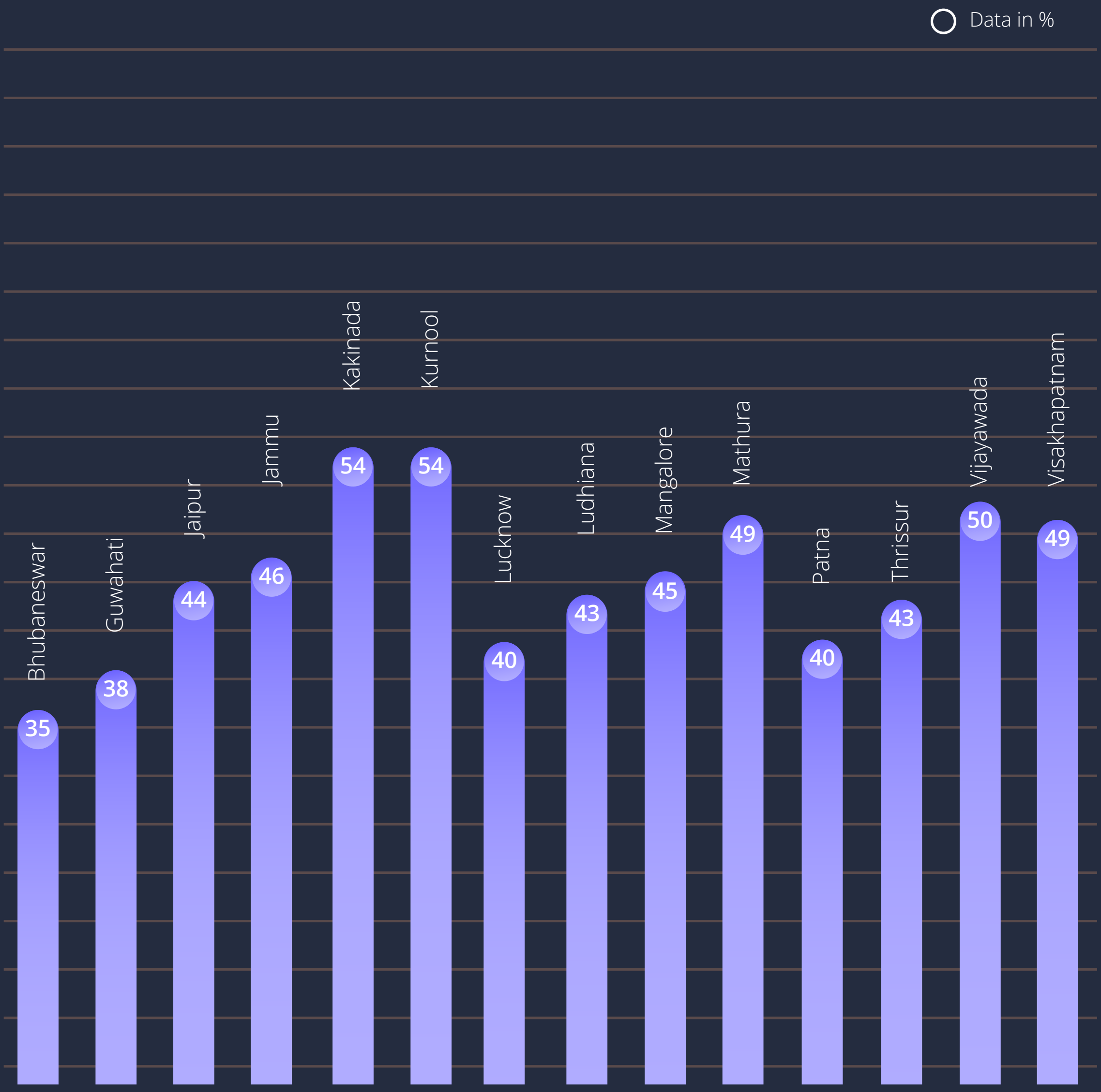
As you can see, the IR index in the last quarter has risen by 7%.

The Metros and Tier - 1 Cities - Infection Rate



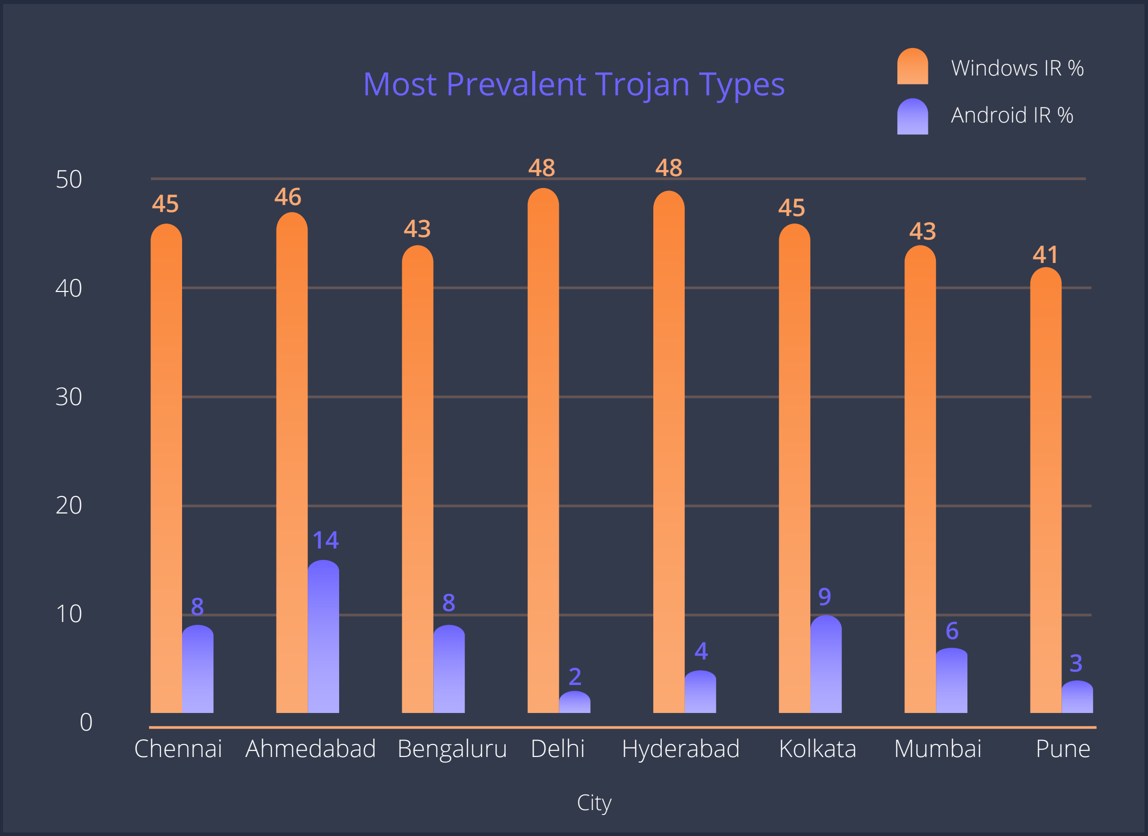
The frequency of attacks has also risen further in Tier-1 and Tier-2 cities. However, the most noticeable aspect in the Tier-2 city chart is the steady increase of malware attacks in smaller Tier-2 cities such as Kurnool, Kakinada, Vijayawada, and Visakhapatnam.

Top 14 Infection Rates in Tier - 2 Cities



Infection Rate Comparison Across Platforms

Detecting and analysing the massive volume of threats flocked around the huge number of Windows and Android users is definitely a herculean task. Windows platform being a proprietary software, threat actors would try to challenge themselves to exploit the same, so that they can get name and fame in comparison to Android platform, which is an open source project. This difference reflects in the statistics too.



As you can see on the chart, the Android users of Ahmedabad, Bengaluru, Chennai, and Kolkata faced more attacks as compared to other metros. The numbers don't mean the attack volume was comparatively lesser.

Enterprise Insecurity

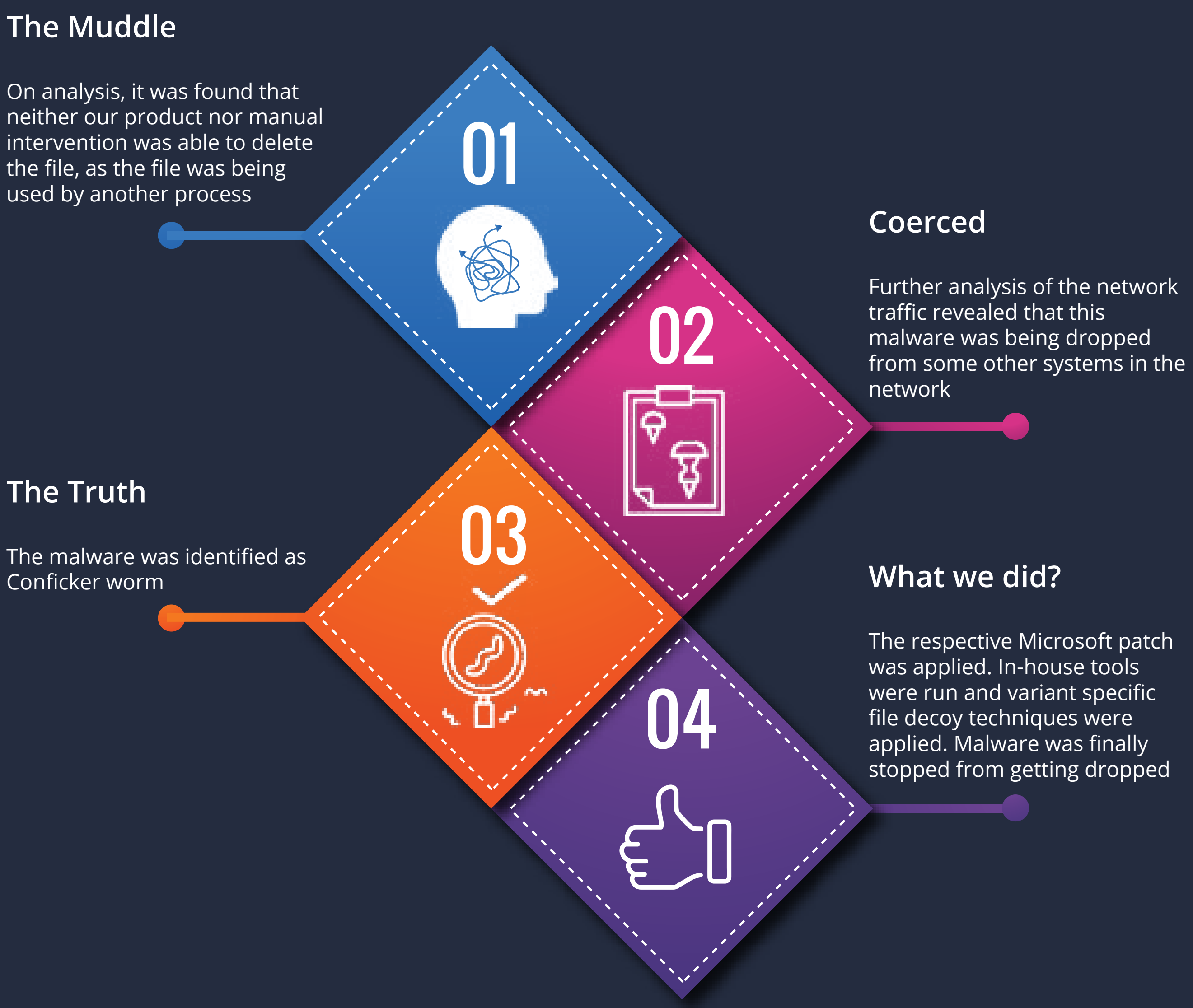
Any cyber breach on an enterprise causes more than data and financial loss. A successful cyberattack could shake-up an entire organization as it causes enormous operation downtime, supply chain slowdown, reputation damages, etc.

Of late, many enterprises are seen to have embraced required security measures to thwart oncoming attacks. They have started implementing multi-factor authentication, cloud data encryption, OS/application updates, and other critical safety measures.

However, the attack statistics are still skyrocketing due to some unpatched loopholes, such as retaining or connecting vulnerable computers or servers to the enterprise network, thereby offering the adversaries an increased attack surface to abuse and intrude to execute mayhem.

Case Study: Conficker's Covert Attack

In the last quarter, an enterprise customer of ours had reported about repeated malware alerts popping-up on their systems on a file in the Windows system area. Let us now look at the sequence of events as to how our K7 Labs researchers analysed and removed the malware from the network.



The Muddle

On analysis, it was found that neither our product nor manual intervention was able to delete the file, as the file was being used by another process

Coerced

Further analysis of the network traffic revealed that this malware was being dropped from some other systems in the network

The Truth

The malware was identified as Conficker worm

What we did?

The respective Microsoft patch was applied. In-house tools were run and variant specific file decoy techniques were applied. Malware was finally stopped from getting dropped

Safety Recommendations

- Secure your devices by keeping them 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

Back to contents

Vulnerabilities Galore

The security effectiveness of any enterprise can be gauged by the existence of flaws in the network. Though many organizations have started adopting good cyber security practices, threat actors have also started adopting new and innovative techniques to fool the users and intrude into the organizations' network to do their malicious activities.

Last quarter too, there were many new security flaws and loopholes in operating systems, networks, and application software like in previous quarters. The respective developers have already fixed many of these flaws by rolling out patches and updates. However, many organizations are yet to patch these vulnerabilities, leaving their network/systems in jeopardy.

Here are the most infamous vulnerabilities from the list.

System Level Vulnerability in Microsoft's DNS Server

CVE-2022-21984 is a system level code execution vulnerability in Microsoft's DNS server. This vulnerability is network-based. On successful exploitation, the attacker gains control over the Active Directory server, if DNS and AD are configured in the same server, thereby giving the attacker control over the entire network.

Vulnerable products are Windows 10, Windows 11 and Windows Server 2022.

Predominant Vulnerabilities in Adobe Software

CVE-2022-24086 is an improper input validation vulnerability that is actively being exploited in the wild, which when successful would allow an unauthenticated attacker to execute code on the remote's victim machine.

CVE-2022-24087 is another improper input validation vulnerability that is caused due to insufficient patching of CVE-2022-24086 vulnerability.

Vulnerable Products are Adobe Commerce and Magento Open Source versions 2.4.3-p1 (and earlier) and 2.3.7-p2 (and earlier).

Vulnerability in Chrome

CVE-2022-0609 is an use-after-free zero-day vulnerability in Chrome that is being actively exploited in the wild, which when successful could lead to corruption of valid data and execution of arbitrary code on vulnerable systems. This can also be used to escape the browser's security sandbox.

Vulnerable products are Google Chrome versions before v98.0.4758.102 and Microsoft Edge versions before v98.0.1108.55.

Windows SMB v3 RCE Vulnerability

CVE-2022-24508 is an SMB v3 Remote Code Execution (RCE) vulnerability in Windows.

This is yet another vulnerability in the Compression module of SMB and impacts Windows versions above Windows 10 20H1. A similar vulnerability was seen in 2019 dubbed as SMBghost and similar mitigation was employed..

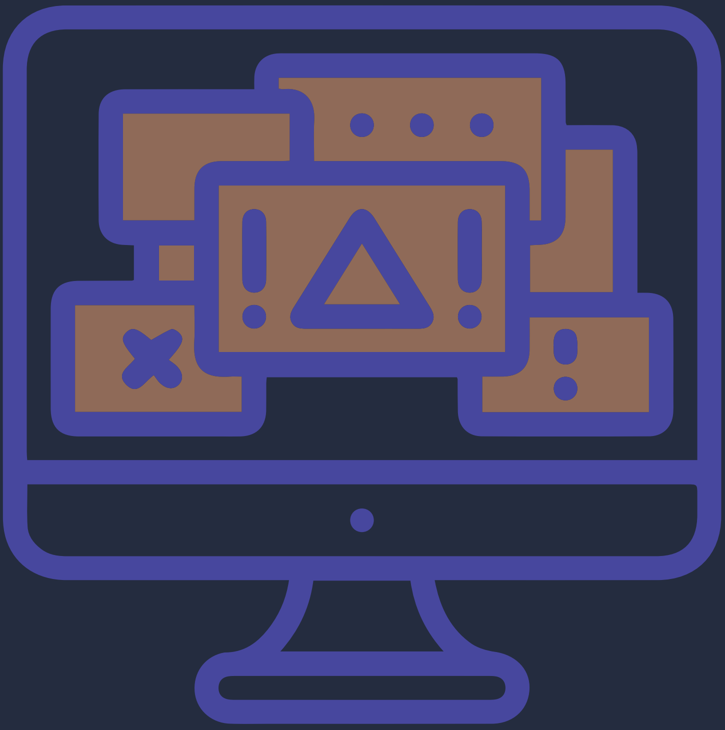
This requires an authenticated attacker to send a specially crafted packet over the network to a targeted SMBv3 server.

Vulnerable operating systems are Windows 10, Windows 11 and Windows Server 2022.

RCE Vulnerability in Microsoft Exchange Server

CVE-2022-23277 is a RCE vulnerability in Microsoft Exchange Server. This requires an authenticated attacker to send a specially crafted packet over the network to a vulnerable server. Since 2021, we have seen a lot of vulnerabilities reported in Exchange Server.

Vulnerable products are Microsoft Exchange Server 2013, Microsoft Exchange Server 2016 and Microsoft Exchange Server 2019.



Danger in the Internet of Things

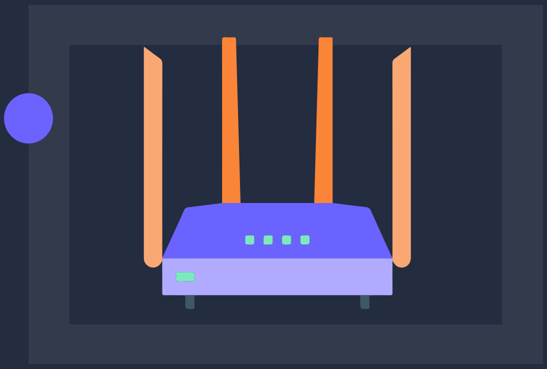
The skyrocketing usage of IoT products across enterprises and end-users have eased many complex tasks. But many of these devices are riddled with vulnerabilities resulting in an insecure network that could get compromised easily. Hence system admins and users should be aware of the exposed vulnerabilities to take necessary action immediately.

In **Q4_2021-22,** there were many such vulnerabilities in several IoT solutions. Let us look at the most prominent ones.

Zero-day in WebKit Browser Engine

CVE-2022-22620 is a zero-day vulnerability in the WebKit browser engine which on successful exploitation can lead to arbitrary code execution on the vulnerable devices. This vulnerability is actively being exploited in the wild.

Vulnerable products are Apple devices using version earlier to macOS Monterey 12.2.1, iOS 15.3.1 and iPadOS 15.3.1



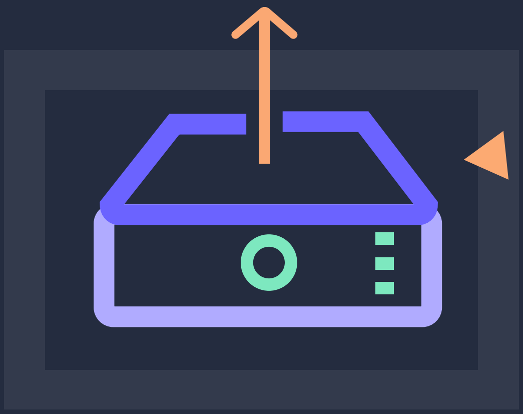
Significant Cisco Router Vulnerabilities

CVE-2022-20699 is a vulnerability in Cisco routers due to insufficient boundary checks when processing specific HTTP requests. Successful exploitation of this vulnerability could lead to unauthorised users executing code on the remote device with root privileges.

Vulnerable products are Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers SSL VPN

CVE-2022-20700 is another vulnerability in Cisco routers due to insufficient authorization which on successful exploitation could lead to privilege escalation on the vulnerable device.

Vulnerable products are Cisco Small Business RV Series



Vulnerability in APC Smart-UPS devices

CVE-2022-22806 and **CVE-2022-0715** are unauthenticated TLS authentication bypass vulnerabilities in APC Smart-UPS devices that can lead to Remote Code Execution (RCE) attacks using a network firmware upgrade. On exploitation, an attacker can remotely take over the devices and execute arbitrary code on them.

This could be used to physically damage the device itself or other assets connected to it.

Vulnerable devices are SMT Series ID=1015: UPS 04.5 and prior, SMC Series ID=1018: UPS 04.2 and prior, SMTL Series ID=1026: UPS 02.9 and prior, SCL Series ID=1029: UPS 02.5 and prior, SCL Series ID=1030: UPS 02.5 and prior, SCL Series ID=1036: UPS 02.5 and prior, SCL Series ID=1037: UPS 03.1 and prior, SMX Series ID=1031: UPS 03.1 and prior

Mitigation Techniques

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

Windows Under Siege

Windows Malware Type Breakdown

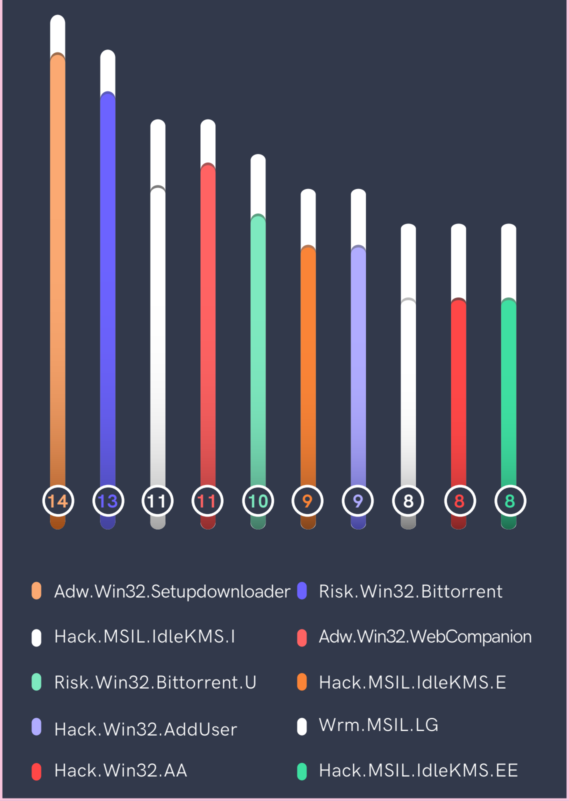
From the statistics that we are seeing quarter-on-quarter, Windows users do not seem to have a respite from threats. Not only organisations across sizes were targeted, even end-users were not spared and were also targeted for various intents.

Windows Exploits

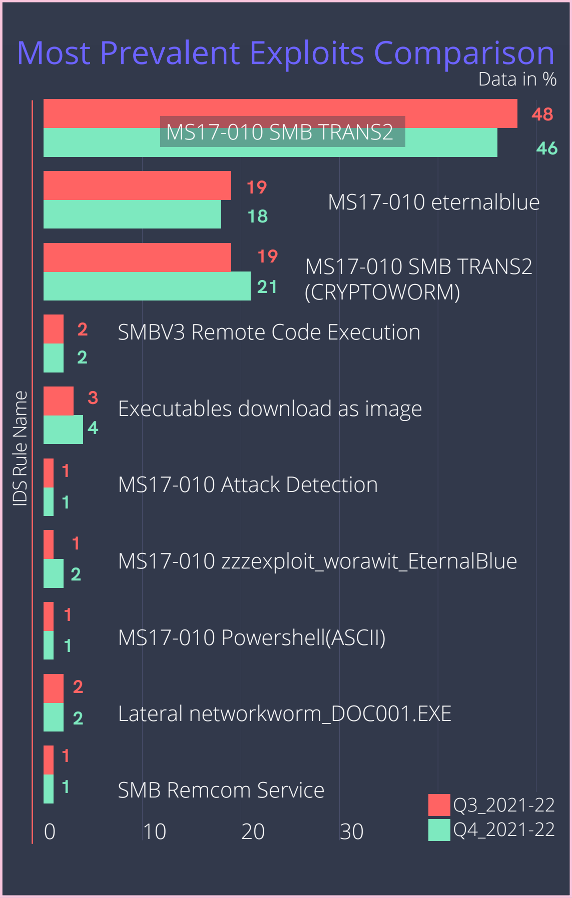
Threat actors proactively weaponise the new and existing unpatched vulnerabilities and abuse them to their advantage.

It's pretty uncanny to see that the SMB and EternalBlue based vulnerabilities are still getting abused. This shows that despite several warnings from developers and security vendors, admins and users ignore installing available patches on time, thus offering an initial vector of compromise.

Split of Windows Top 10 Detections

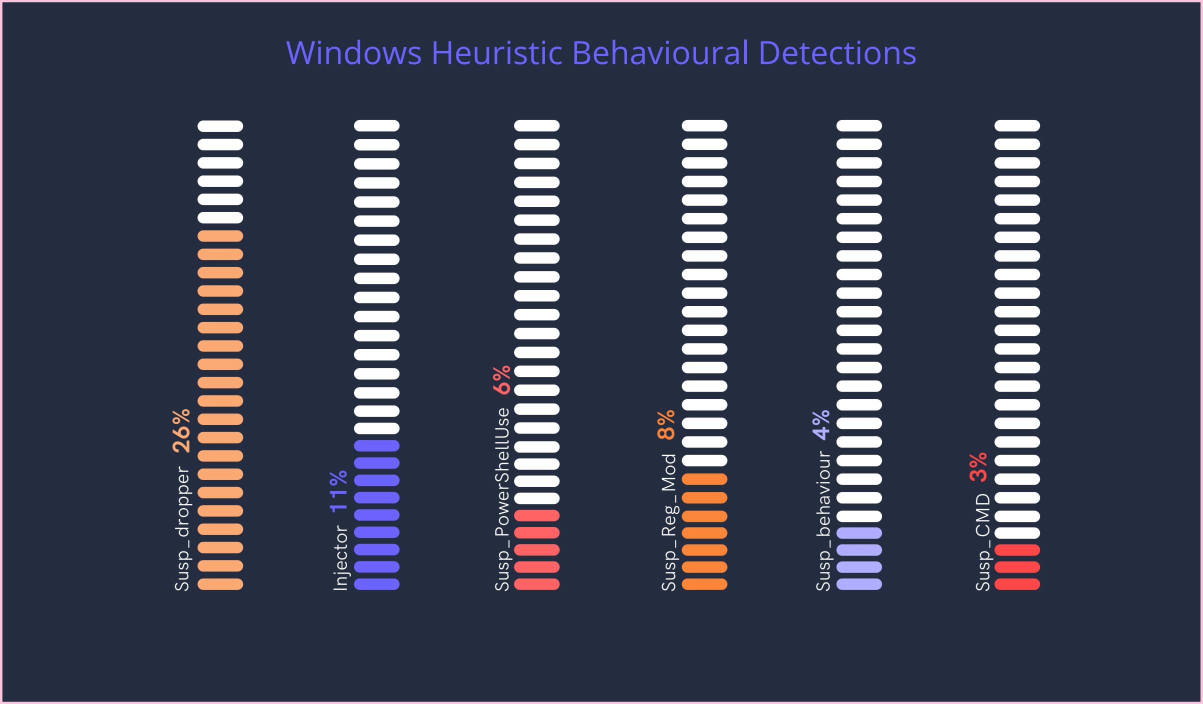


Most Prevalent Exploits Comparison



Heuristic Host Intrusion Prevention System

Heuristic behavioural detections are a way of detecting threats for which we might have not added a signature as yet. Ideal for new threats but can even be used for detecting newer variants of existing malware families. Let us see what our heuristic behavioural technology has detected in the last quarter.



Droppers occupied a significant chunk followed by Injectors and Registry Modifiers. Our behavioural detection also identified malware that were hosted as malicious scripts on websites abusing PowerShell and Windows command shell. A small percentage of the detections were those of malware trying to evade detection by hiding their artefacts.

Mitigation Tips

- Keep your devices updated and patched against the latest vulnerabilities
- Follow the principle of least privilege while granting access to your employees
- Enforce a robust password policy

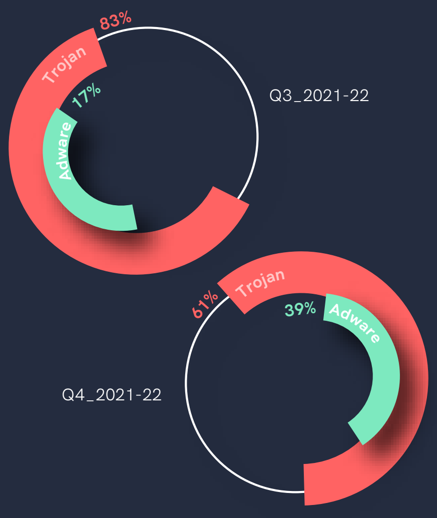
Back to contents

The Mobile Device Story

A smartphone is like a swiss army knife as it offers the ability to do almost all of the things that can be done virtually. However, since it may contain all your contacts, account credentials, financial data including credit cards, calendars, photographs, videos, and conversations it becomes a potential target for threat actors.

In **Q4_2021-22**, there was a significant presence of Trojans in comparison to Adware, though the percentage of Trojans has dwindled compared to the previous quarter.

Adware vs Trojan Proportional Split

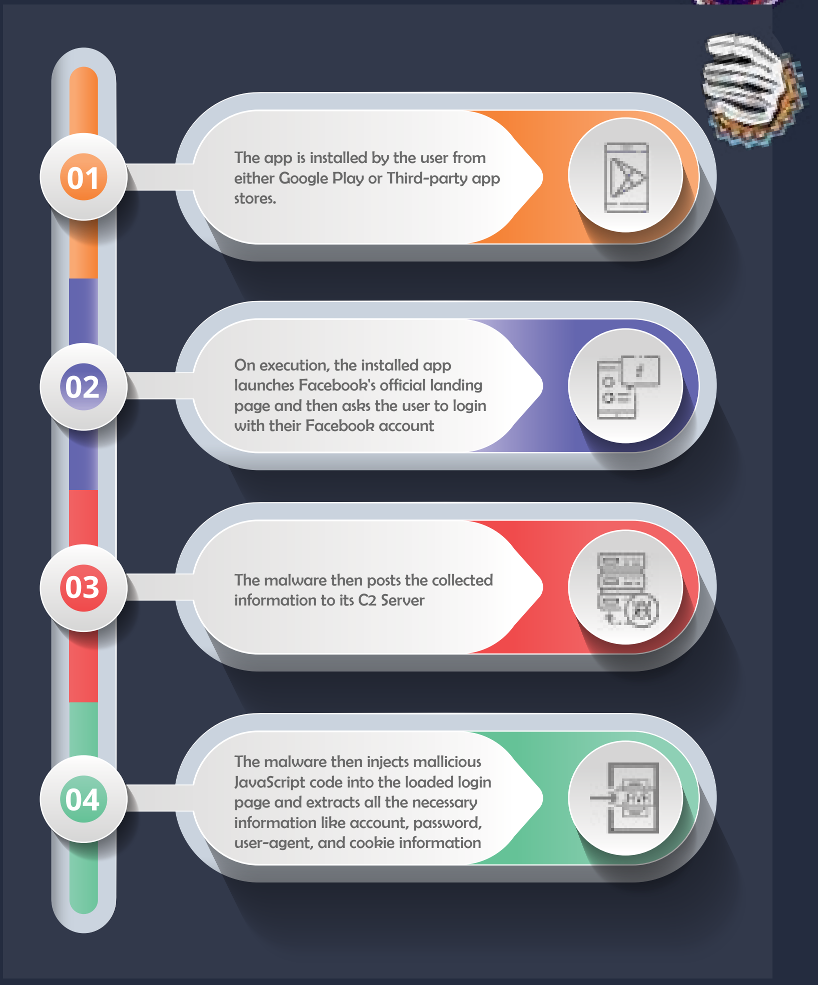


The perpetual growth of the smartphone market has impressed threat actors to consider it as one of the most potential vectors. Threat actors have been seen to constantly employ new tricks to lure users, while still wanting to maintain their old tried-and-tested tactics.

One such malevolent technique in the smartphone arena is to deploy malicious replicates of popular Android Apps in the Play Store.

Case Study: Facestealer aka The Credential Hijacker

Last quarter, we came across one such band of malicious apps tagged as Facebook Credential stealer, alias Facestealer. The sequence of events is portrayed below.



01 The app is installed by the user from either Google Play or Third-party app stores.

02 On execution, the installed app launches Facebook's official landing page and then asks the user to login with their Facebook account

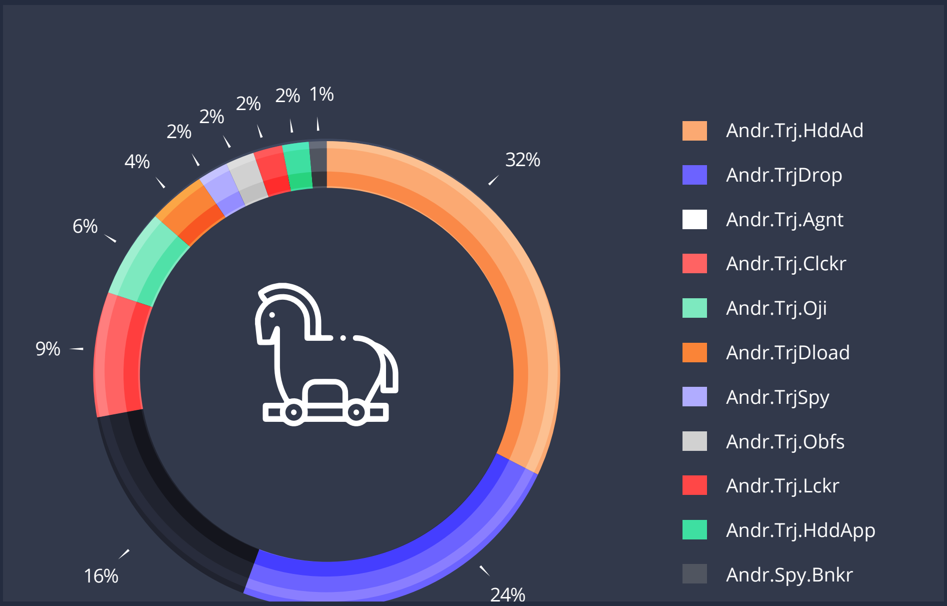
03 The malware then posts the collected information to its C2 Server

04 The malware then injects mallicious JavaScript code into the loaded login page and extracts all the necessary information like account, password, user-agent, and cookie information

The Ubiquitous Trojan

The continuous growth of Trojans implies threat actors are getting more and more sophisticated and preferring targeted attacks to churn more money. Smartphones are also the most effective attack vector for executing large-scale cyberattacks on enterprises. In this quarter, Andr.Trj.HddAd had a significant increase and topped the charts, followed by Andr.TrjDrop which saw a slight decline in comparison to the previous quarter.

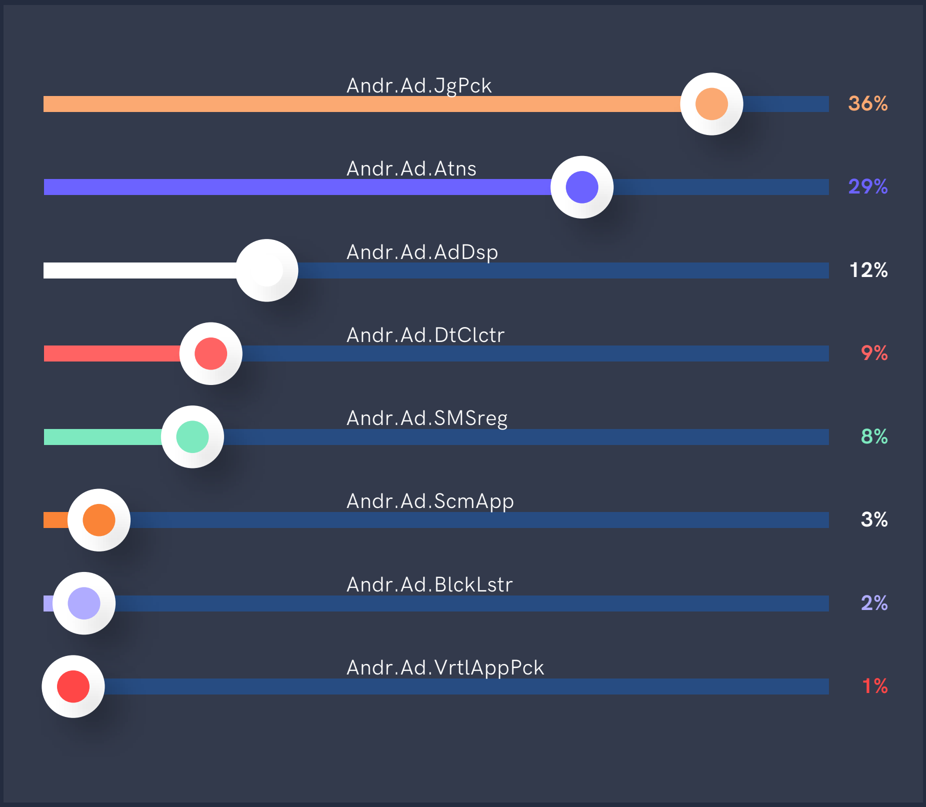
Most Prevalent Trojan Types



The Adware Saga

Though downloading adware onto the users' device is no longer a lucrative revenue-earning model, last quarter did see an increase in adware signifying that threat actors are still considering this as an option to make money. The chart below shows the statistics.

Trend Line Showing the Adware Plague



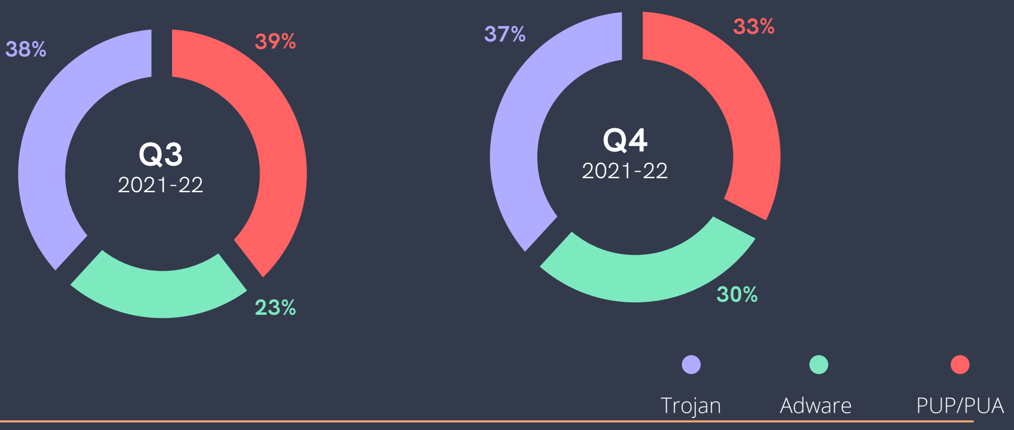
Tips to Stay Safe

- Always be extra cautious and read the user reviews before downloading and installing any app
- Do not download 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

Despite Apple's stricter cybersecurity controls on all of its devices, many attack groups have started to develop malware for the macOS platform. Though these numbers still only score a small percentage compared to malware targeting Windows users, they have been steadily increasing over the last few years.

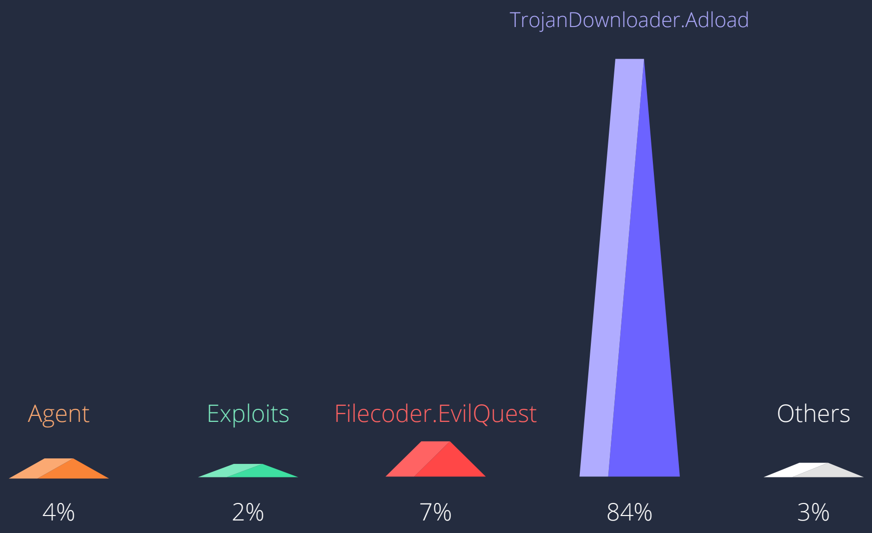
Trojan, Adware & PUP Proportional Split



The Trojan Fracas

The Trojan space seems to have shifted dramatically from **Q1_2021-22** wherein EvilQuest had a significant presence of 43% in comparison to **Q4_2021-22**. where the share dropped drastically to 7%. This quarter too, the threat actors seem to have favoured downloader Trojans to install malicious programs on the device without users' consent..

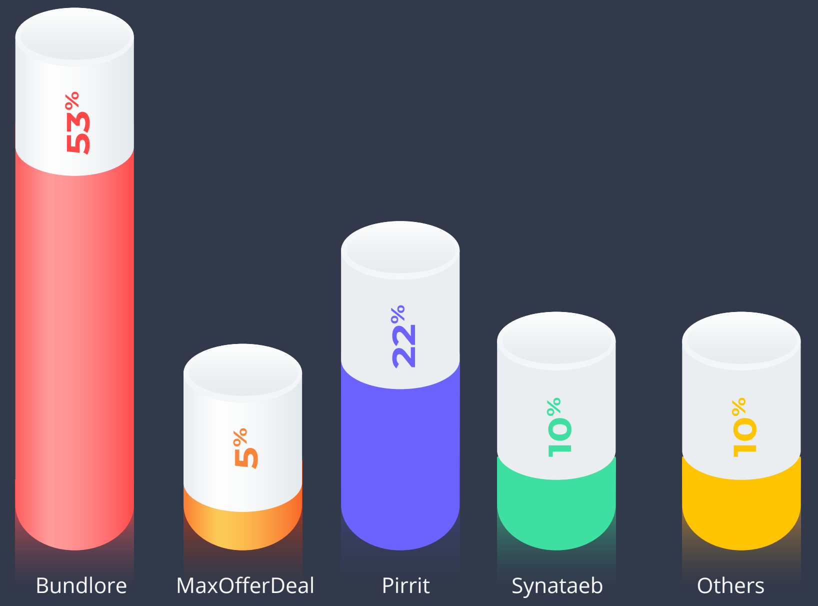
Trojan Detection Trend Lines



The Adware Brouhaha

In **Q4_2021-22** too, Bundlore (an Adware dropper) remained the key driving force behind the substantial growth of adware signifying that threat actors are relying on adware to do their malicious intent..

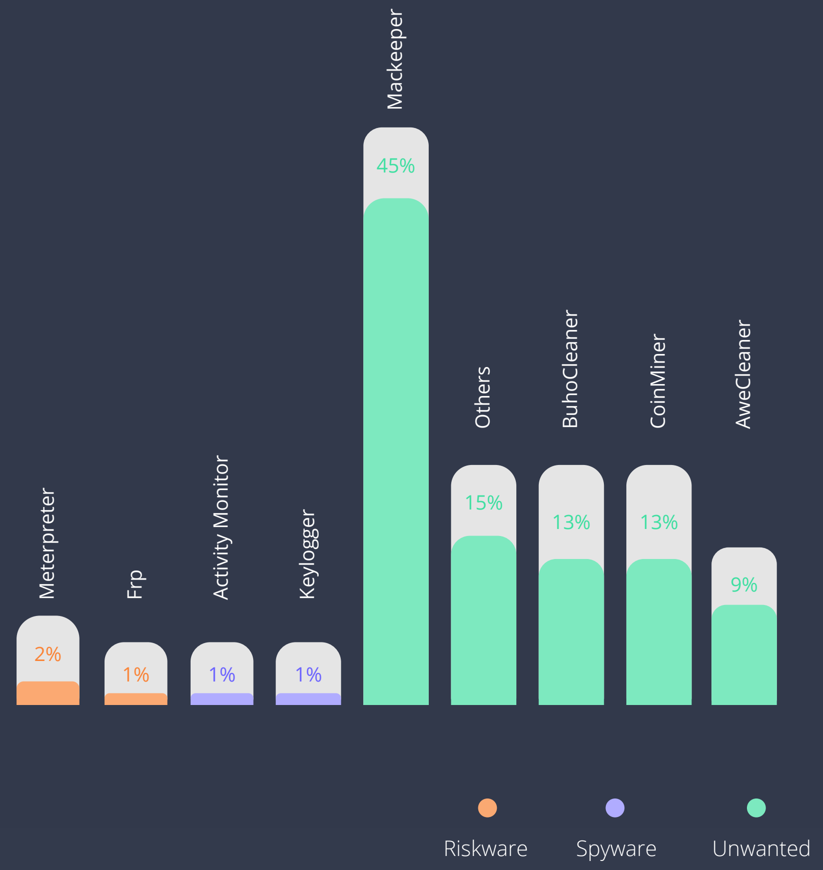
The Trend Line of Adware Variant Detections



A Trickle of PUPs

Despite the decline in the presence of PUPs, Mackeeper still ruled the roost along with system cleaning and coin mining apps.

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

As adversaries are broadening their frequency of attacks, enterprises and end-users should be geared up to circumvent this onslaught. Besides practising basic cyber hygiene in everyday digital life, they should also be careful about social engineering traps and posting sensitive information online. Besides, K7 Computing recommends the following essential practices to keep threat actors at bay.

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

Regularly audit your user accounts for any unauthorized user accounts created

Regularly assess your network to avoid possible breaches

Consumer

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

Do not download and/or install apps from unknown sources or third-party app stores

Keep your OS, applications and devices updated and patched against the latest vulnerabilities

Back to contents

K7 SECURITY

www.k7computing.com

April 2022