K7 SECURITY

Cyber Threat Monitor Report

Q3

Contents

Expounding the Cyber Threat Panorama

Year 2021 and the past year have been riddled with cyber attacks. Geopolitics continued to play a significant role. For instance, Russia's invasion of Ukraine saw an increase in malware, DDoS attacks among others across Ukrainian organizations and attacks spread through geographical boundaries too. From cyber warfare to hacktivism, there was all and we expect to see more such attacks in the future too considering the growing unrest between nations.

Threats targeting not only data but also putting an organization's reputation at stake were prevalent. The prominent ones were ransomware and supply chain attacks. Threat actors targeted almost all the platforms. Ransomware attacks were prevalent in the Windows platform, while Android was riddled with Banking malware. macOS platform, however saw malicious signed binaries, which bypassed Apple's security mechanism for spoofing a job vacancy opportunity. Due to the huge difference in the user base, the attack surface is comparatively lesser in number making the impact on macOS platforms smaller. However, threat actors are targeting it and proving that Apple's platform too is vulnerable albeit more difficult than Microsoft's.

The past quarter saw enterprises battling with ransomware attacks and a significant chunk of them used brute force as the attack vector to drop the payload.

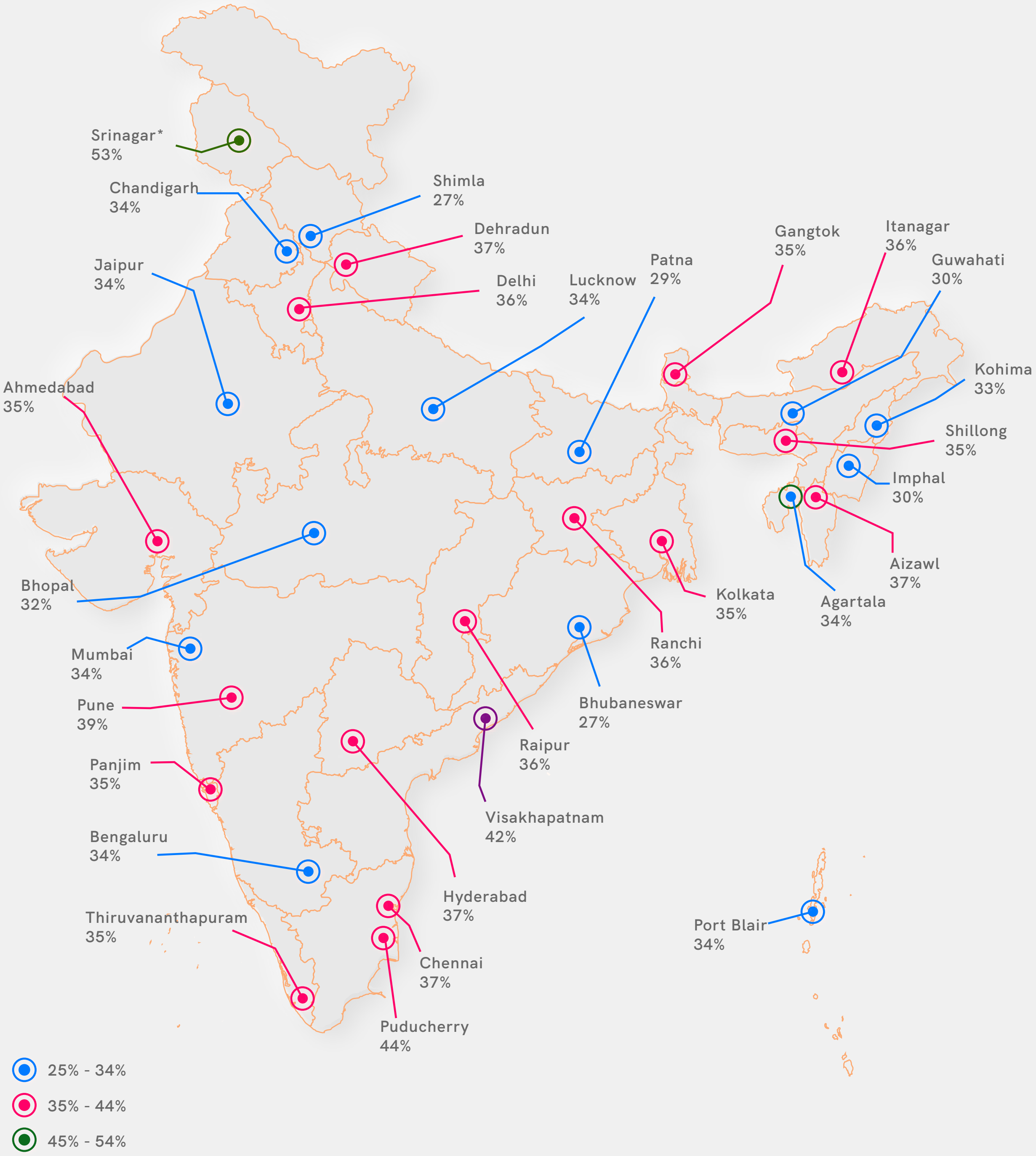
We at K7 Labs offer significant protection from emerging and latest threats at the earliest, by closely examining and identifying such incidents and providing protection at multiple layers,

Our quarterly reports list case studies that ignited our interest and found worthy to share, 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 of you who might be interested in more detailed analysis are more than welcome to read up 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

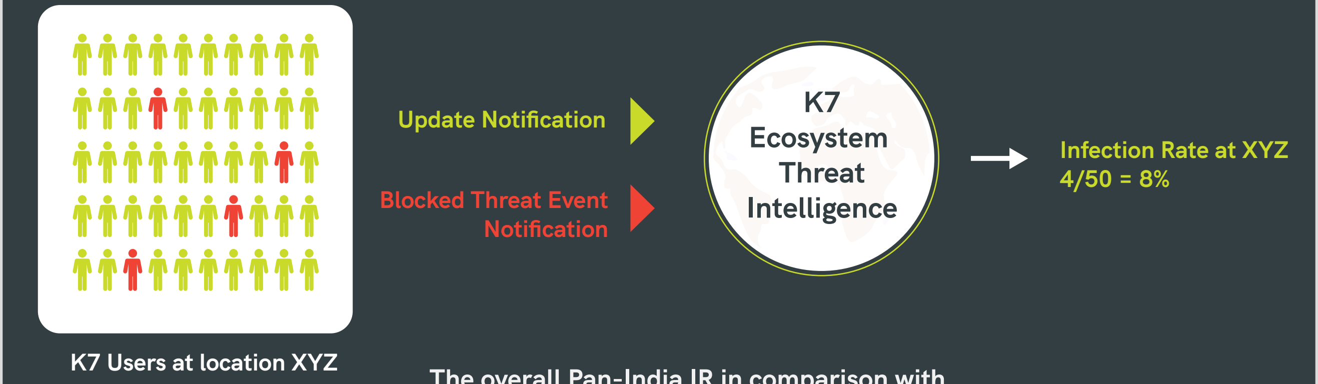
The K7 Cyber Threat Monitor (CTM) report for Q3_2022–23 offers a broad assessment of the cybersecurity threat landscape.

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 netizens' risk at K7 Labs.

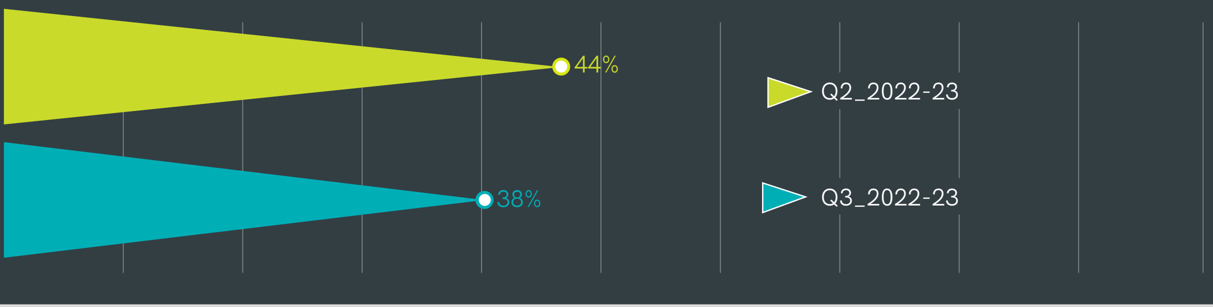
We use this IR factor to identify the netizens' exposure to cyber threats. IR is determined as the proportion of K7 users in an area who encountered at least one cyber threat event and which was blocked and reported to our K7 Ecosystem Threat Intelligence infrastructure. The higher the IR, the greater the risk.

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

Infection Rate (IR) of an area



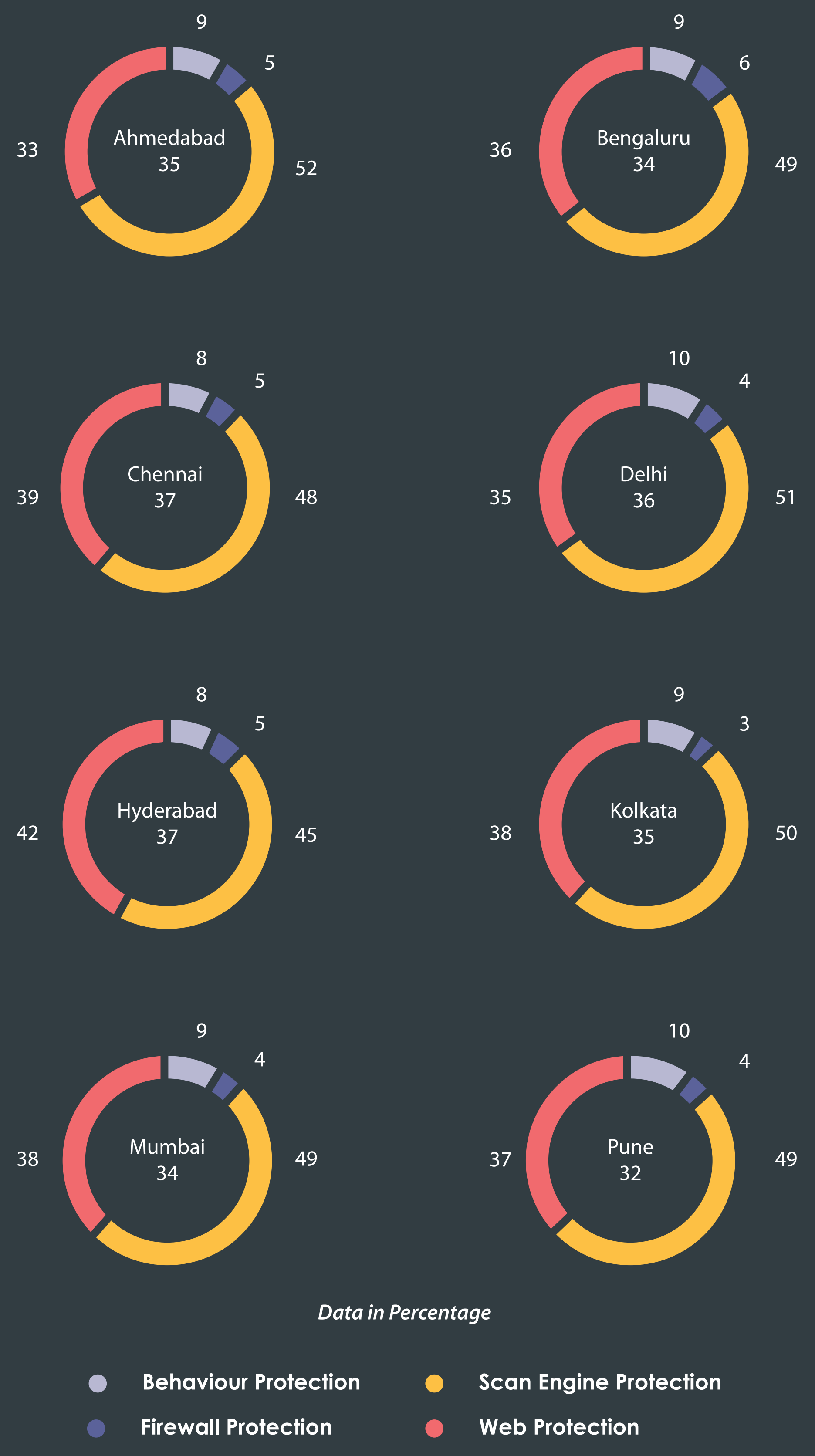
The overall Pan-India IR in comparison with the previous quarter is given below



As can be seen from the chart, there has been a 6% drop in IR in comparison to Q2_2022-23. This could be attributed to incidents not reported and products not activated/updated. Or maybe, just maybe, the threat actors went on vacation as well.

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

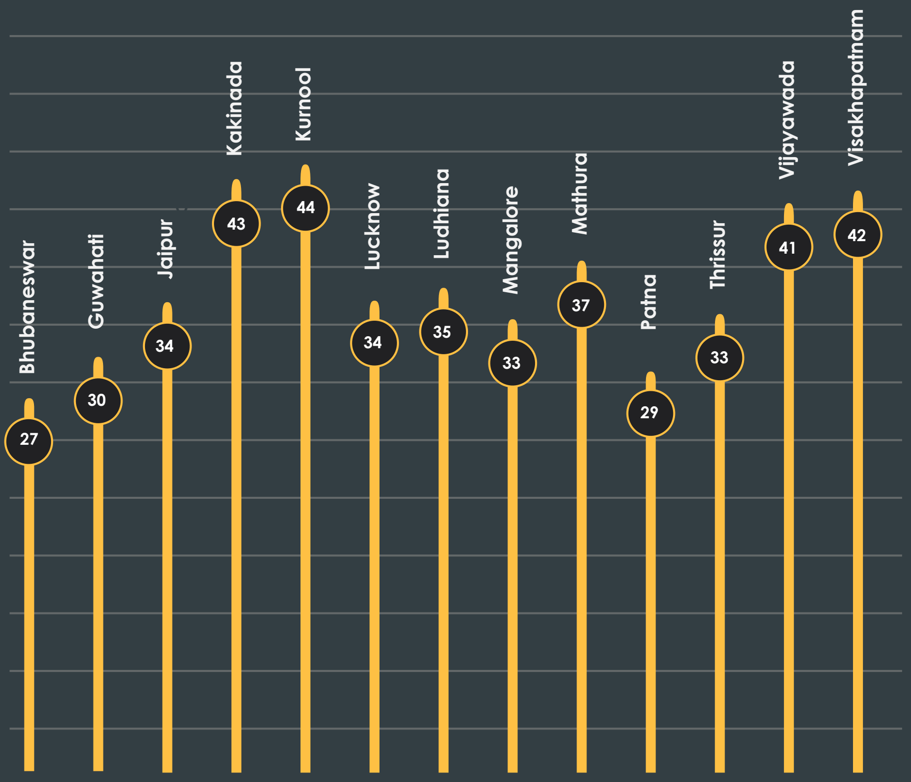


Data in Percentage

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

Back to contents

Top Infection Rates in Tier-2 Cities

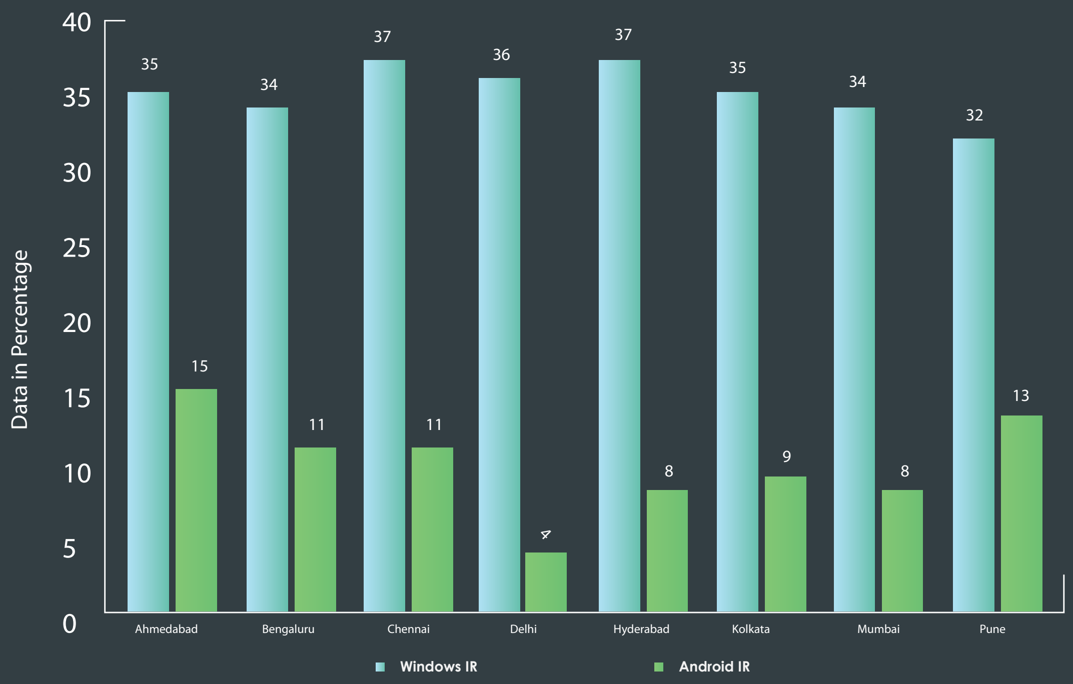


Data in Percentage

Infection Rate Comparison Across Platforms

Even though most cybercriminals target Windows-based workstations because of the comparatively large user base and hence the bigger reach they will achieve, K7 Labs has also witnessed significant malware assaults on Android devices each quarter which includes phishing, banking trojans, spyware and downloaders among others.

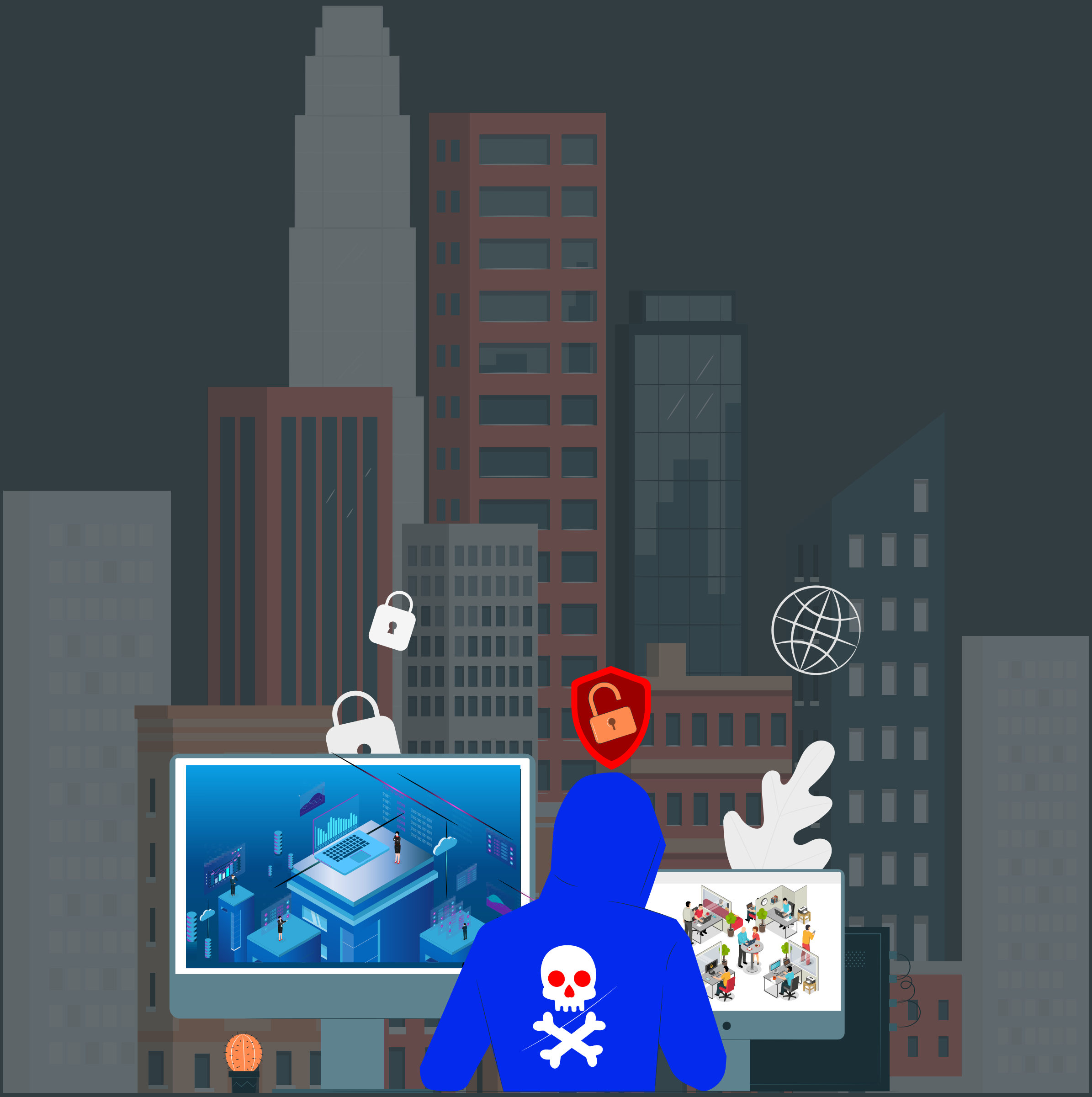
Windows IR vs Android IR



Enterprise Insecurity

Enterprises have always been the target for ransomware attacks because of the huge monetary benefit that can be achieved. The infection vector to drop ransomware payloads ranges from phishing, credential abuse to exploitation of vulnerabilities.

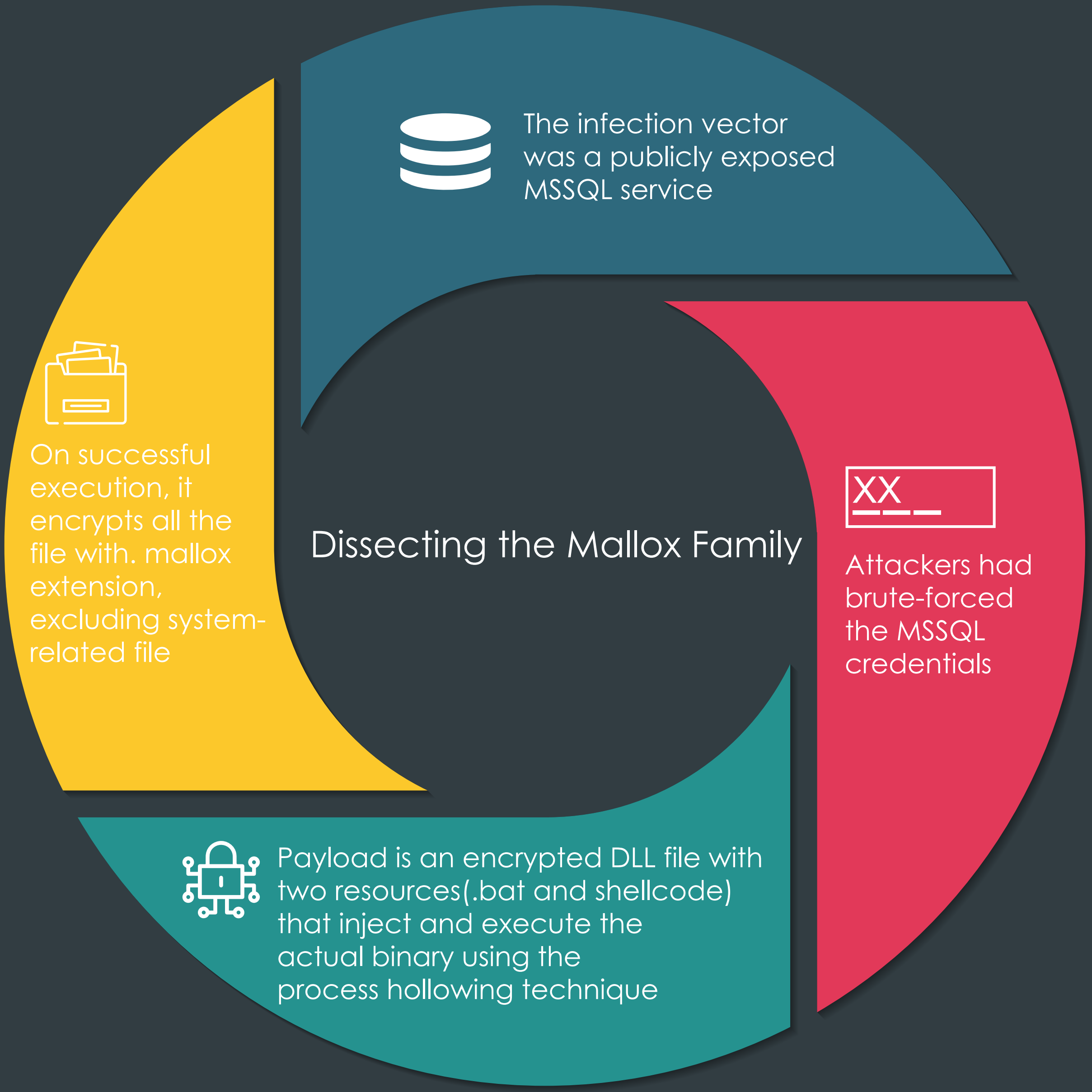
However, attackers still continue to use old techniques such as brute force to gain access into the vulnerable network, mainly due to a high success rate. However, this does require a lot of time and effort in comparison to other sophisticated techniques. Also, brute forcing need not be manual, it could also be done using bots.



Case Study: Dissecting the Mallox Family

Over the past few weeks, many of our customers had been hit by the Mallox ransomware variants. The threat actors choose their victims by targeting vulnerable servers and applications using brute forcing.

The kill-chain is depicted below:


Dissecting the Mallox Family
The infection vector was a publicly exposed MSSQL service
Attackers had brute-forced the MSSQL credentials
Payload is an encrypted DLL file with two resources(.bat and shellcode) that inject and execute the actual binary using the process hollowing technique
On successful execution, it encrypts all the file with. mallox extension, excluding system-related file

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
- Reduce your attack surface by identifying and patching vulnerable assets
- Keep a backup of all critical data
- Train your employees on good cyber hygiene practices

Vulnerabilities Galore

Vulnerabilities mainly exist due to improper coding, poor design and configuration issues. Organizations need to identify, prioritise and work on fixing vulnerabilities so as to safeguard their networks and data from any breach or accidental leaks.

This section lists some of the key vulnerabilities that should be patched at the earliest.

Privilege Elevation and RCE Vulnerability in Exchange Server

CVE-2022-41040 is an unauthenticated Server Side Request Forgery vulnerability in Microsoft Exchange Server frontend that allows adversaries to bypass authentication.

CVE-2022-41082 is a Remote Code Execution (RCE) vulnerability in Microsoft Exchange Server backend. This allows adversaries to run arbitrary commands in vulnerable servers.

Vulnerable product versions are Microsoft Exchange Server 2013, 2016, 2019.

VMWare Authentication bypass vulnerability

CVE-2022-31685 is an authentication bypass vulnerability that exists in VMware Workspace ONE Assist wherein a malicious actor can gain administrative access without the need to authenticate to the application.

Vulnerable product version is VMware Workspace ONE Assist - 21.x, 22.x.

Buffer Overflow Vulnerability in OpenSSL

CVE-2022-3602 and CVE-2022-3786 are buffer overflow vulnerabilities in X.509 certificate verification wherein an attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes on the stack causing a Denial of Service.

Vulnerable product version is OpenSSL version 3.0.0.

Dangers in the Internet of Things

IoT adds a lot of value for both businesses and end users alike. With value comes a lot of data generated from these devices and when there are unpatched vulnerabilities in them, it offers a lot of opportunity for threat actors to exploit.

Let us now get into a few significant vulnerabilities.

Cross Site Request Forgery vulnerability

A Cross Site Request Forgery vulnerability, **CVE-2022-41622,** present in F5 BIG-IP and BIG-IQ wherein attackers can launch an RCE attack thereby compromising the complete system.

Vulnerable product versions are BIG-IP - 17.0.0, 16.1.0-16.1.3, 15.1.0-15.1.8, 14.1.0-14.1.5, 13.1.0-13.1.5 and BIG-IQ - 8.0.0-8.2.0, 7.1.0.

Fortinet authentication bypass vulnerability

CVE-2022-40684 is an authentication bypass vulnerability found in Fortinet components FortiOS, FortiProxy and FortiSwitchManager. An unauthenticated adversary can add an SSH key to the admin user and then access the affected system as admin via SSH.

Vulnerable product versions are FortiOS - 7.0.0-7.0.6, 7.2.0-7.2.1, FortiProxy - 7.0.0-7.0.6, 7.2.0 and FortiSwitchManager - 7.0.0, 7.2.0.

Out-of-bounds write vulnerability in Apple products

CVE-2022-42827 is an out-of-bounds write vulnerability present in Apple products which allows an application to execute arbitrary code with kernel privileges.

Vulnerable product versions are iOS < 15.7.1, iPadOS < 15.7.1, macOS < 12.6.1, tvOS < 16.1 and watchOS < 9.1.

Mitigation Techniques

- Secure your linked devices and networks
- Regularly monitor and upgrade your IoT devices and network as soon as a fix has been implemented for any security risk(s) under consideration

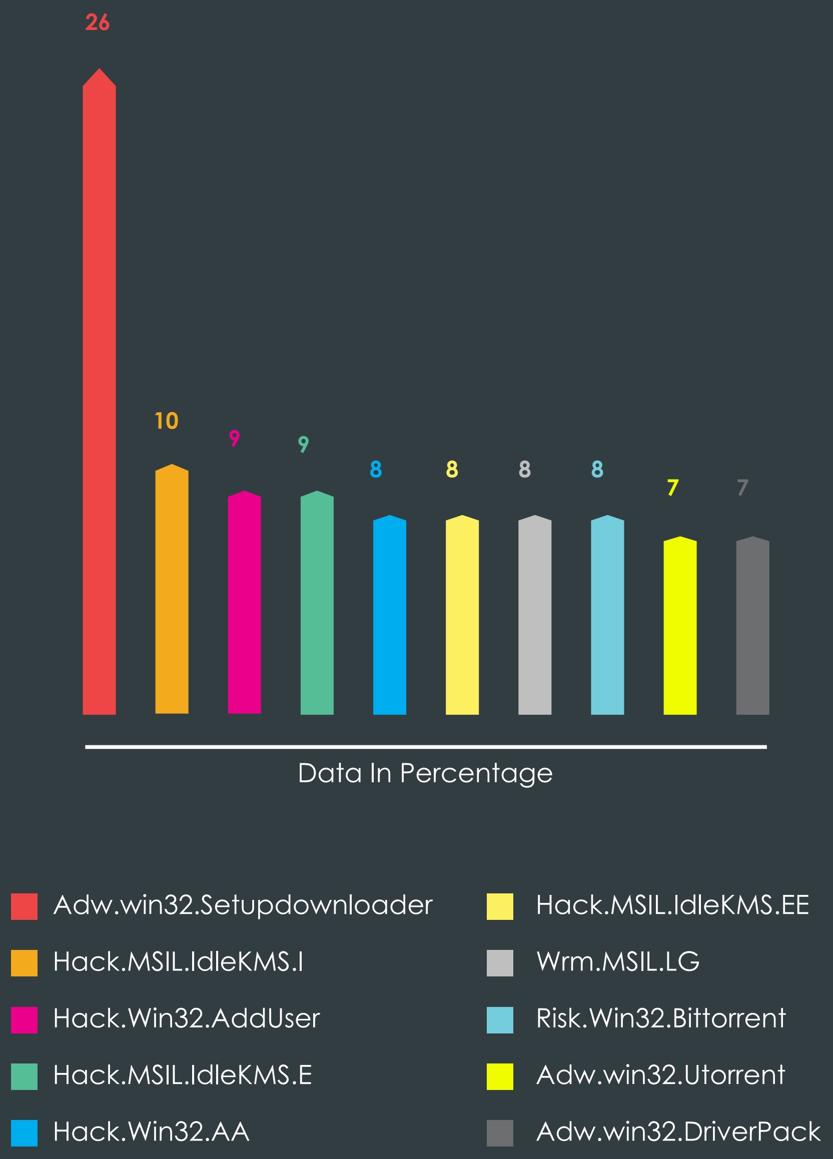
Back to contents

Windows Under Siege

Windows Malware Type Breakdown

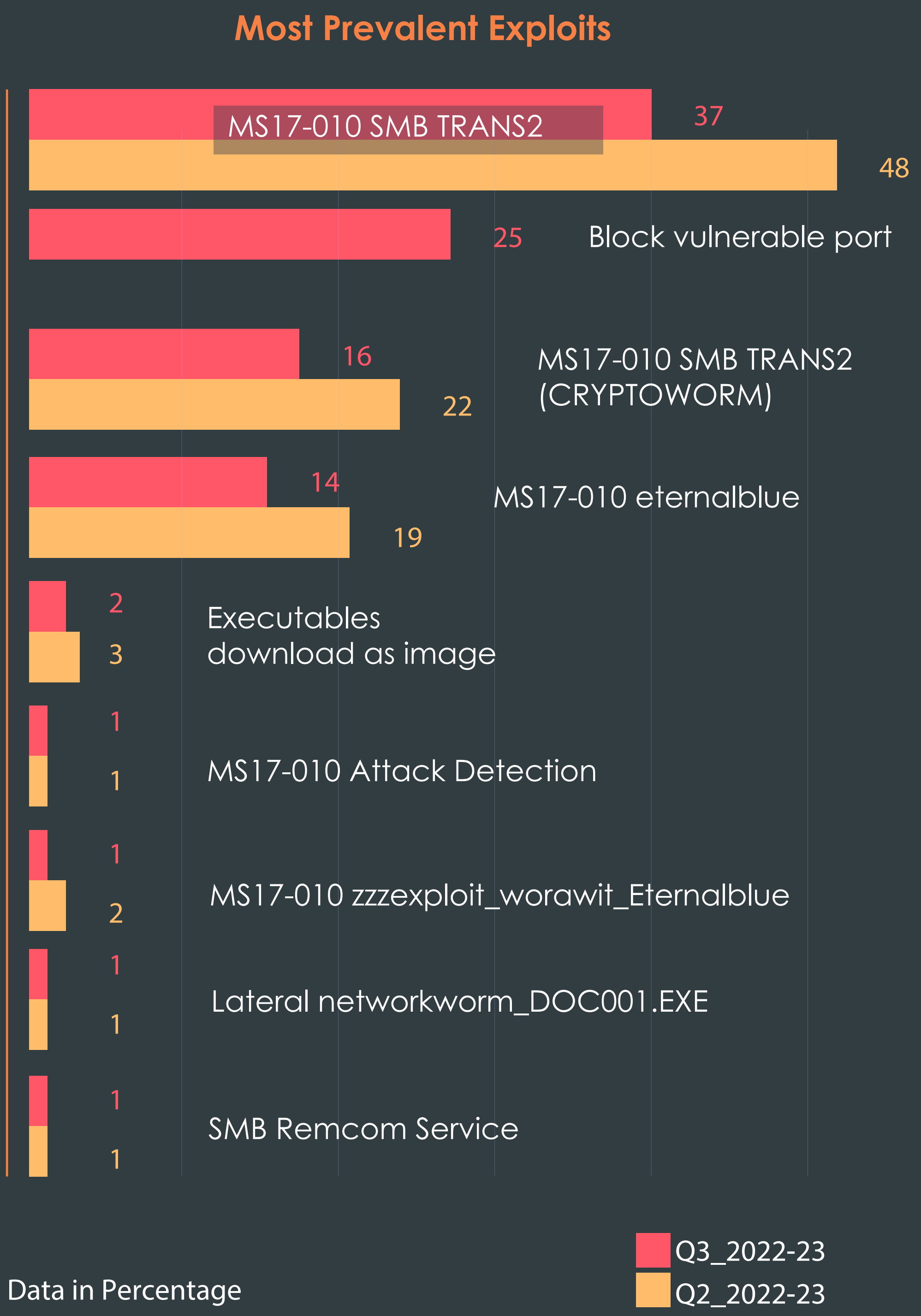
Being the most widely used operating system in use today, Windows is subject to the most recent and advanced attacks. The bad actors put forth a comparable effort to get beyond security gateways and launch further assaults. This is in addition to the effort taken to create new malware strains.

Split of Windows Top 10 Detections



Windows Exploits

Despite several awareness campaigns alongside the Patch Tuesday programme, innumerable users still need to pay more attention to applying patches to their dated and unpatched systems.

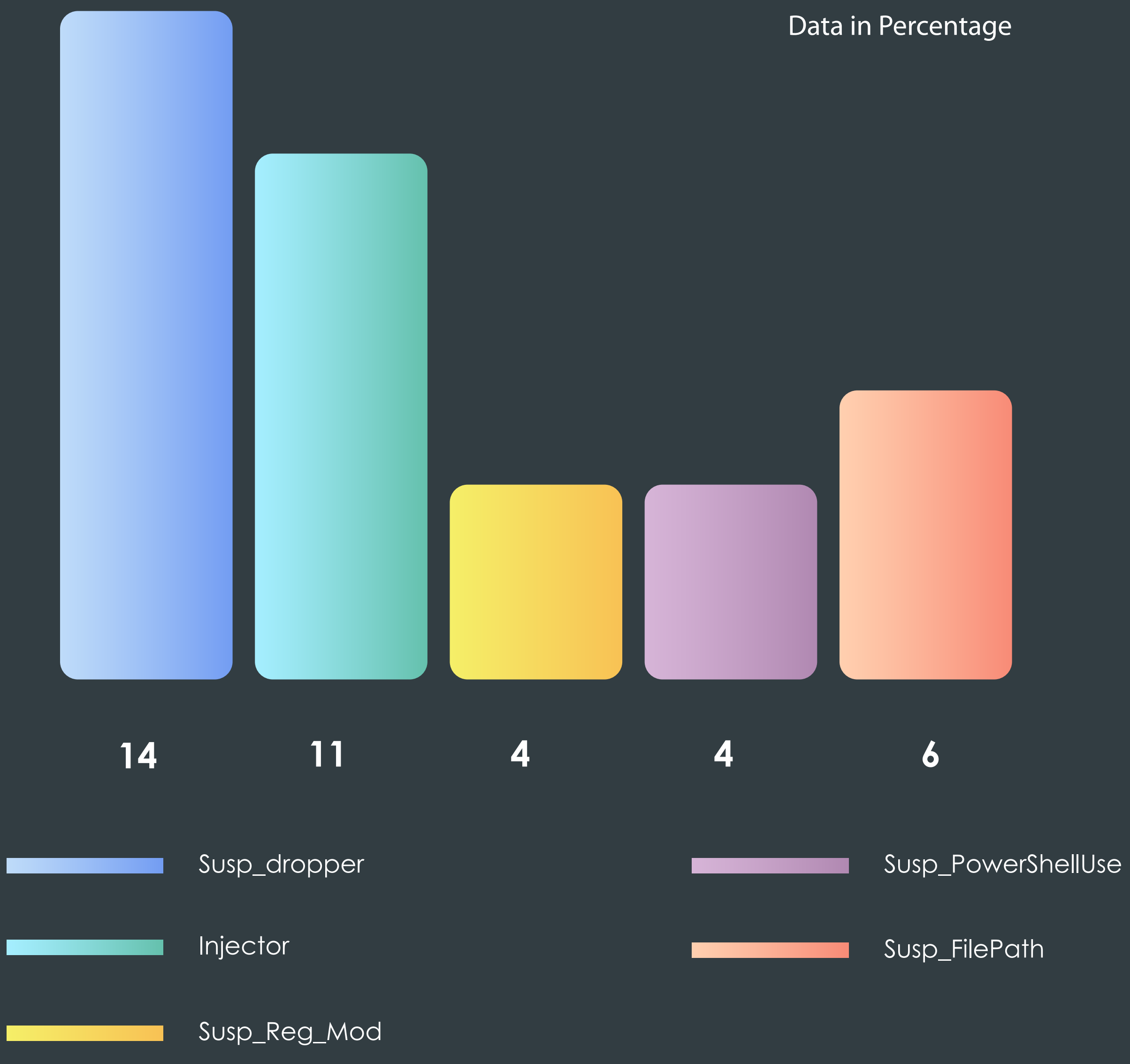


Heuristic Host Intrusion Prevention System (HIPS)

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 occupied a significant chunk followed by Injectors and those 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. Our behavioural detection also contextually identified malware abusing PowerShell and Windows command shell, as well as based on the different persistence techniques employed.

Back to contents

Mitigation Tips

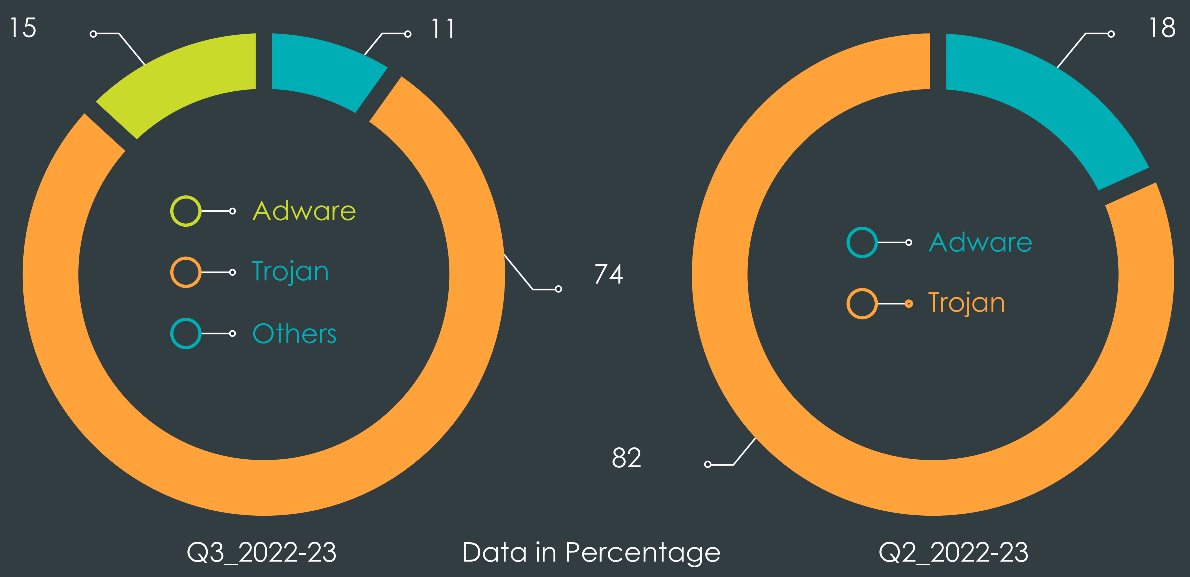
- Keep your devices updated and patched against the latest vulnerabilities
- Consider implementing a zero trust security model
- Secure your sensitive data by encrypting and storing them in a safe storage

Back to contents

The Mobile Device Story

With so many employees now connected to their companies' networks and data via their mobile devices after the pandemic started, smartphones have become the goldmines of confidential data, including both personal data, which includes banking credentials, expense and earning logs, and business data for the threat actors.

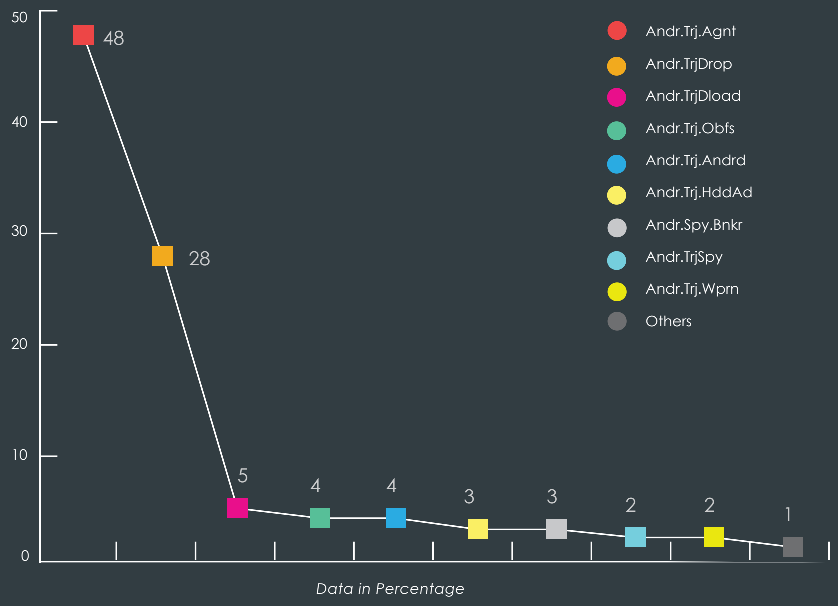
Adware vs Trojan Proportional Split



The Ubiquitous Trojan

In Q3_2022-23, there were few notable changes to the mobile threat landscape in comparison to the previous quarter. Trojans presence decreased by eight percent. However, Andr.Trj.Agnt and Andr.TrjDrop continued to remain prevalent this past quarter too. Detections of Andr.TrjSpy and Andr.SpyBnkr variants indicate Spyware was also prevalent as threat actors stand to gain a lot from users' sensitive data.

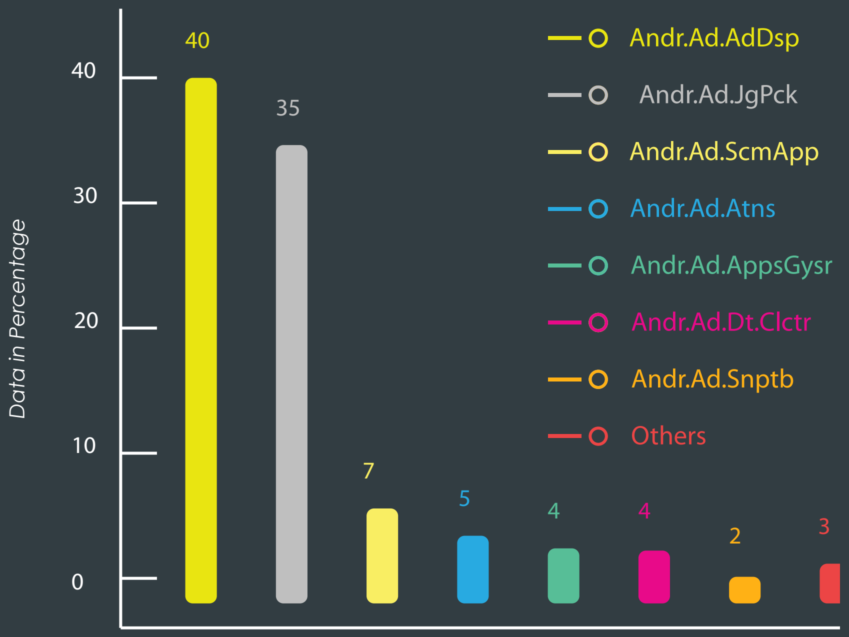
Most Prevalent Trojan Types



The Adware Saga

In Q3_2022-23 too, there has been a decrease in the Adware families' prevalence in comparison to the previous quarter. Apart from the apps still ruling the roost, we also saw data stealing apps which collect users' sensitive data for doing nefarious activities. Apart from these, we also saw users still falling prey to scamming apps

Trend Line Showing the Adware Plague



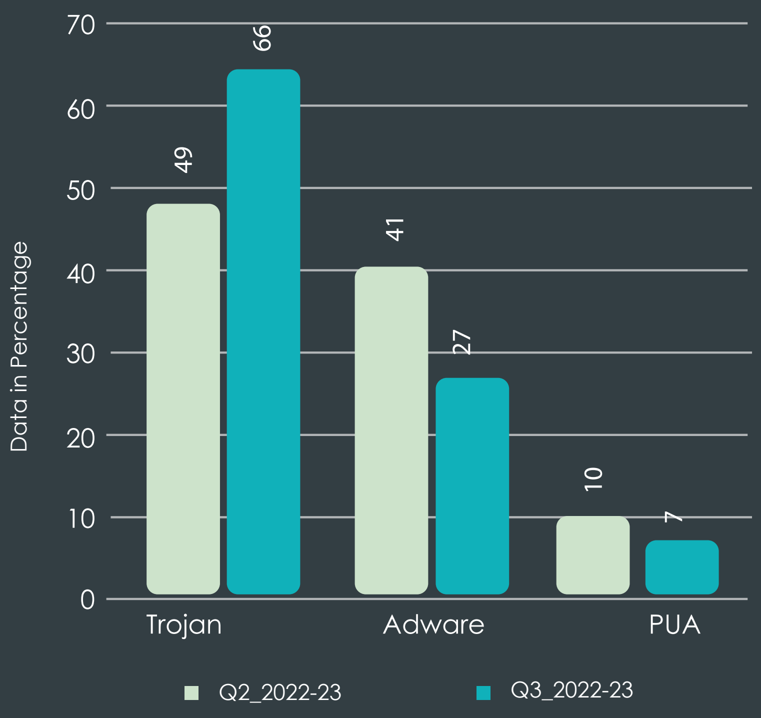
Tips to Stay Safe

- 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

macOS is considered to be more robust and comparatively less prone to attacks. However, threat actors are exploring this space to find loopholes not just in their OS but also if there are any security check lapses when providing an approval for any software.

Trojan, Adware & PUP Proportional Split



The comparison chart clearly shows not just an increase in the Trojan space but also a noticeable decline in the Adware and PUA front.

Though the threat landscape of macOS is not as vast as Windows it is not deemed as more safer than its counterparts. The rate at which macOS users are getting infected by malware is increasing year on year. Attackers are finding different techniques to infect it. One such method is explained below.

Attacks employing signed binaries

A long standing method that attackers have been repeatedly using is having signed binaries to bypass Apple's security mechanisms. We have noticed in the recent past as to how a signed malware when executed distracts the user by showing a pdf file informing the user about a job vacancy in a crypto exchange. However, in the background, it drops a couple of other executables which get executed and connects to a C&C server. Following which a payload is requested. This opens a backdoor to the infected machine and the machine can later be abused by the attacker. Read more technical details about this attack mechanism here.

This similar pattern of behaviour (a signed binary displaying a PDF and dropping PE in the background when executed) has occurred in the middle of this year too, however, this time around the company and the C&C were different.

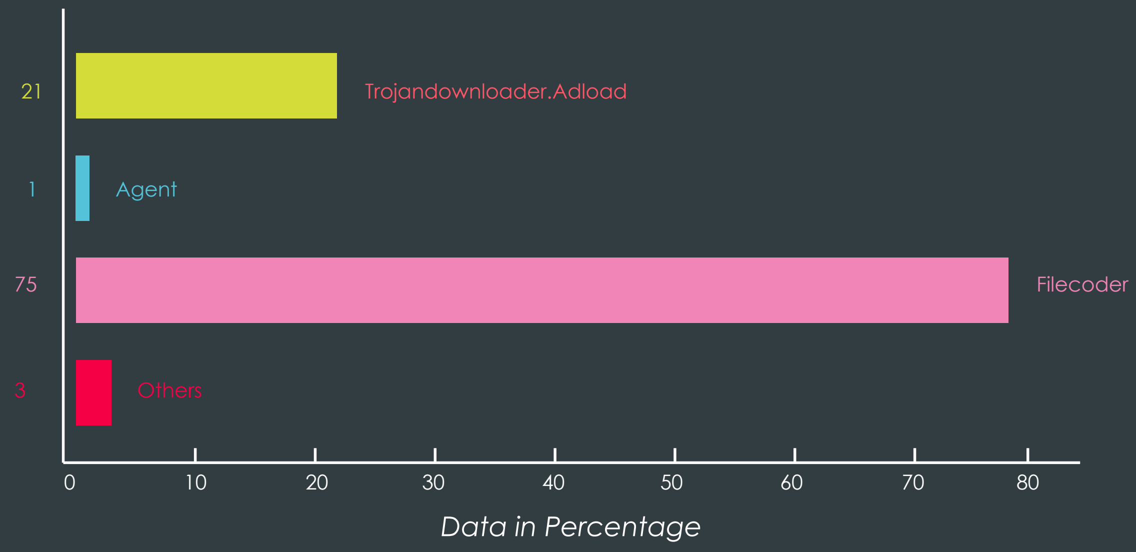
We have been seeing this trend of signed malware being used to infect macOS users dated back to 2021.

In one of the above cases the developer ID & the certificate which was used to sign the binary was revoked only around August this year, infecting many vulnerable users in the meantime.

The Trojan Fracas

The past quarter saw ransomware taking the top spot with Filecoder being prevalent. This was followed by TrojanDownloader.Adload which creates a backdoor on the affected system and maintains stealth by evading detection by security products.

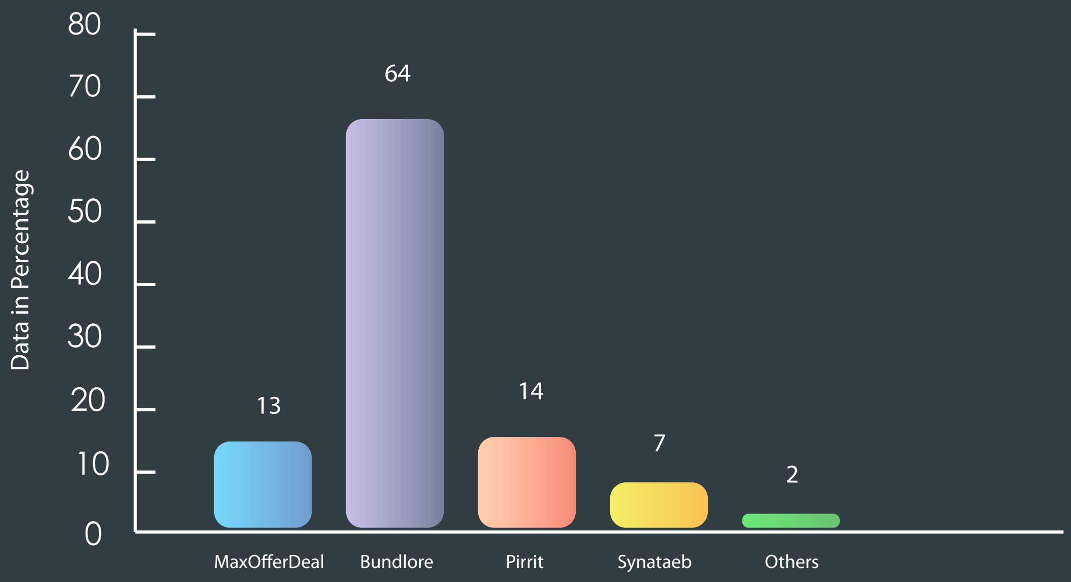
Trojan Detection Trend Lines



The Adware Brouhaha

Bundlore retained its number one position, showing that macOS malware authors are relying on droppers such as these to install adware onto the victim's devices. Apart from this, there were adware such as MaxOfferDeal and Pirrit that annoy users with unnecessary pop-ups and advertisements.

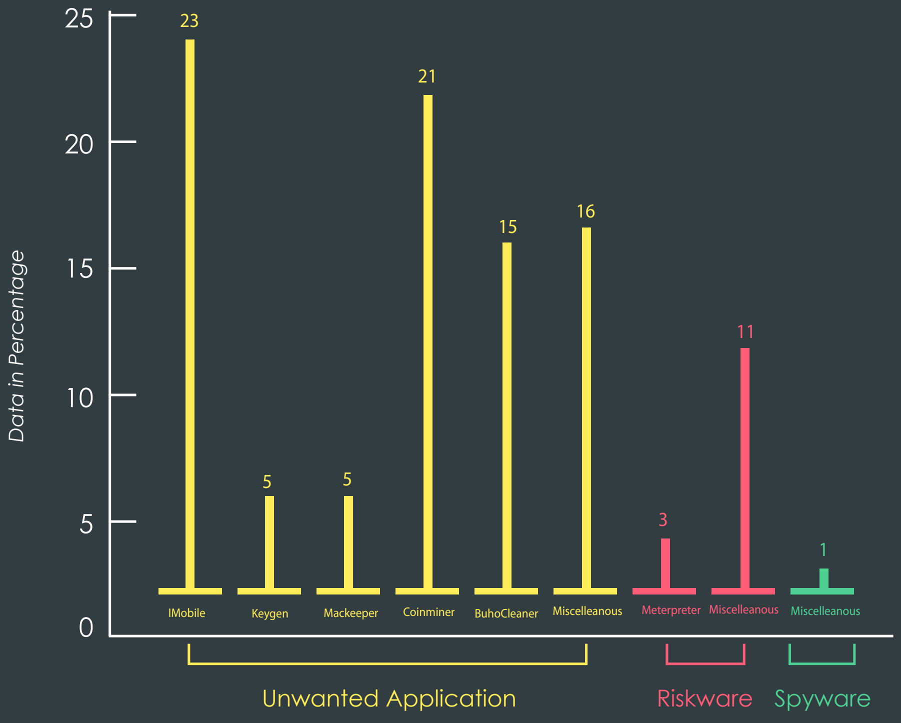
The Trend Line of Adware Variant Detections



A Pinch of PUPs

Last quarter too, there has been a visible decrease in PUPs being used. iMobie topped the charts, posing as a system optimizer and displaying unwanted ads and possible redirects to malicious websites. There was also a noticeable decline in the BuhoCleaner app even though it promised users to optimize their macOS performance. CoinMiner also saw a steady decline in its reach.

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

Last quarter, it was the enterprises which bore the brunt of cyber attacks. Raising their guard has become the number one priority. Organizations should focus more on employee training. Apart from these, one needs to install a reputable security product and follow some safety precautions which we have listed below.

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

Secure your endpoints

Regularly audit your network

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

Think twice before you click on links or downloading files

Secure your sensitive information

K7 SECURITY

Q3

JANUARY 2023

www.k7computing.com