K7 SECURITY

Cyber Threat Monitor Report

Q4

Contents

Tackling your Cyber Adversaries

The post-pandemic and ongoing war between Russia and Ukraine has caused a significant shift in how attackers operate. Additionally, with the increased usage of digital platforms and transactions, the attack surface has grown large, leading to a higher risk of cyberattacks, which are also becoming more and more sophisticated and challenging to detect.

In addition, threat actors are increasingly utilizing social engineering tactics such as phishing attacks, CEO fraud, and business email compromise to infiltrate corporate networks. Such strategies have proved to be low-cost but effective for threat actors, as humans are easy to deceive.

The emergence of several AI technologies, including deepfake, proves immensely beneficial to threat actors for composing real life audio and visual content raising the potential of future social engineering.

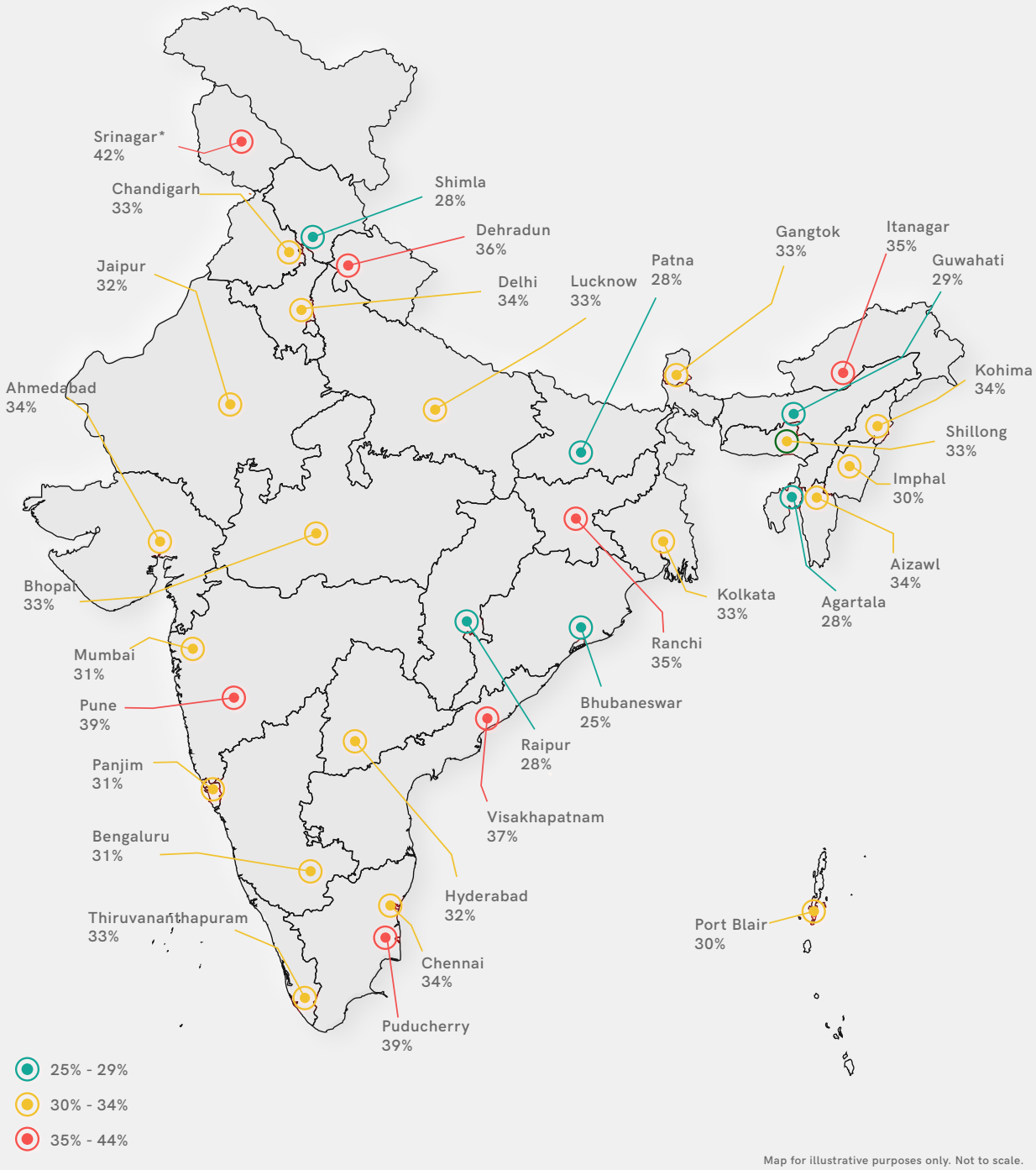
The future of cybersecurity will demand a comprehensive approach that strengthens endpoint security while implementing layered defenses, behavioural analytics, and machine learning to anticipate and block threats proactively.

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 lists 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

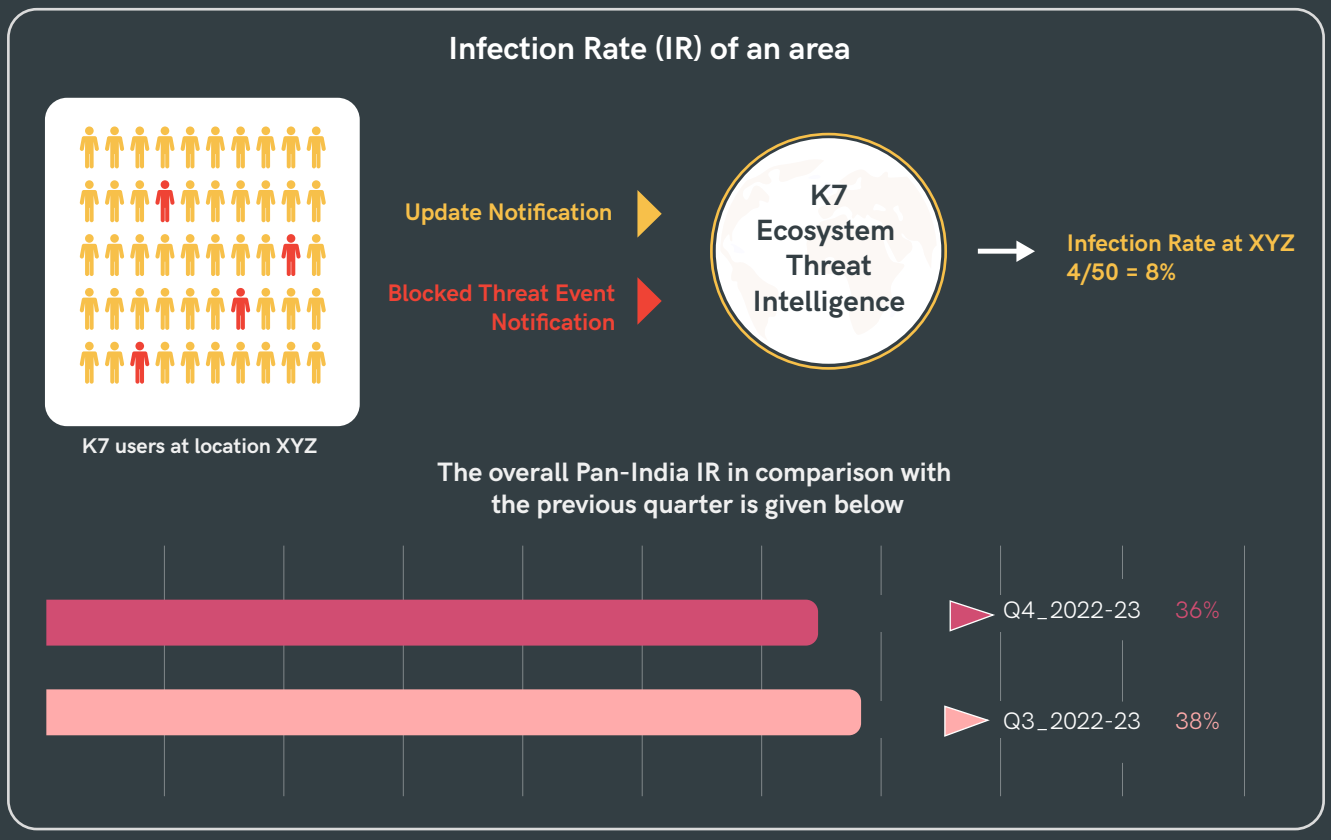
Irrespective of its type, a security breach is a thing to worry about in every aspect of our digital life. And that's precisely what our infection rate indices indicate.

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 netizens' 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.

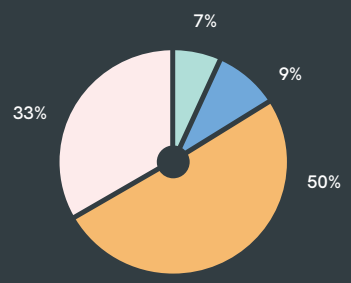
The concept of Infection Rate is better explained by the below picturization.

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

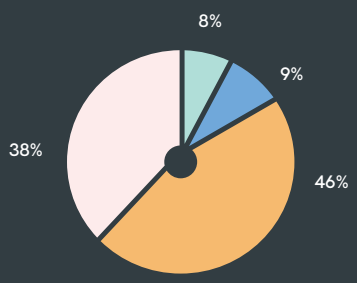


Quarter over quarter, the number plots the bigger picture involving the rise and fall of every malware, ransomware, vulnerabilities, and everything else that matters on the threat landscape. The number offers insight into all the threats discerned into various detection layers, including firewall, scan engine detection, URL, and behavioural.

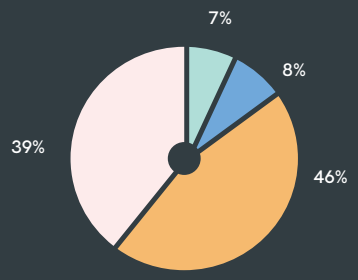
The Metro and Tier-1 Cities - Infection Rate



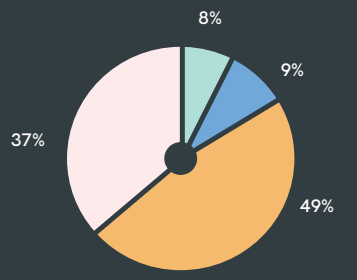
Ahmedabad
34%



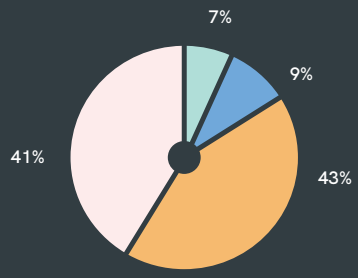
Bengaluru
31%



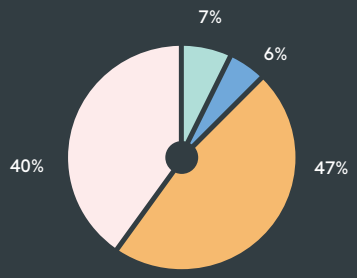
Chennai
34%



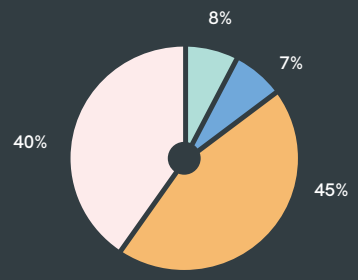
Delhi
34%



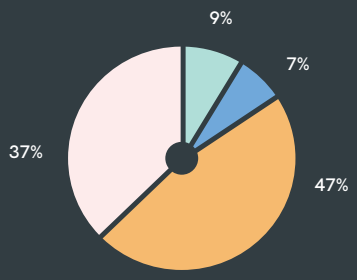
Hyderabad
32%



Kolkata
33%



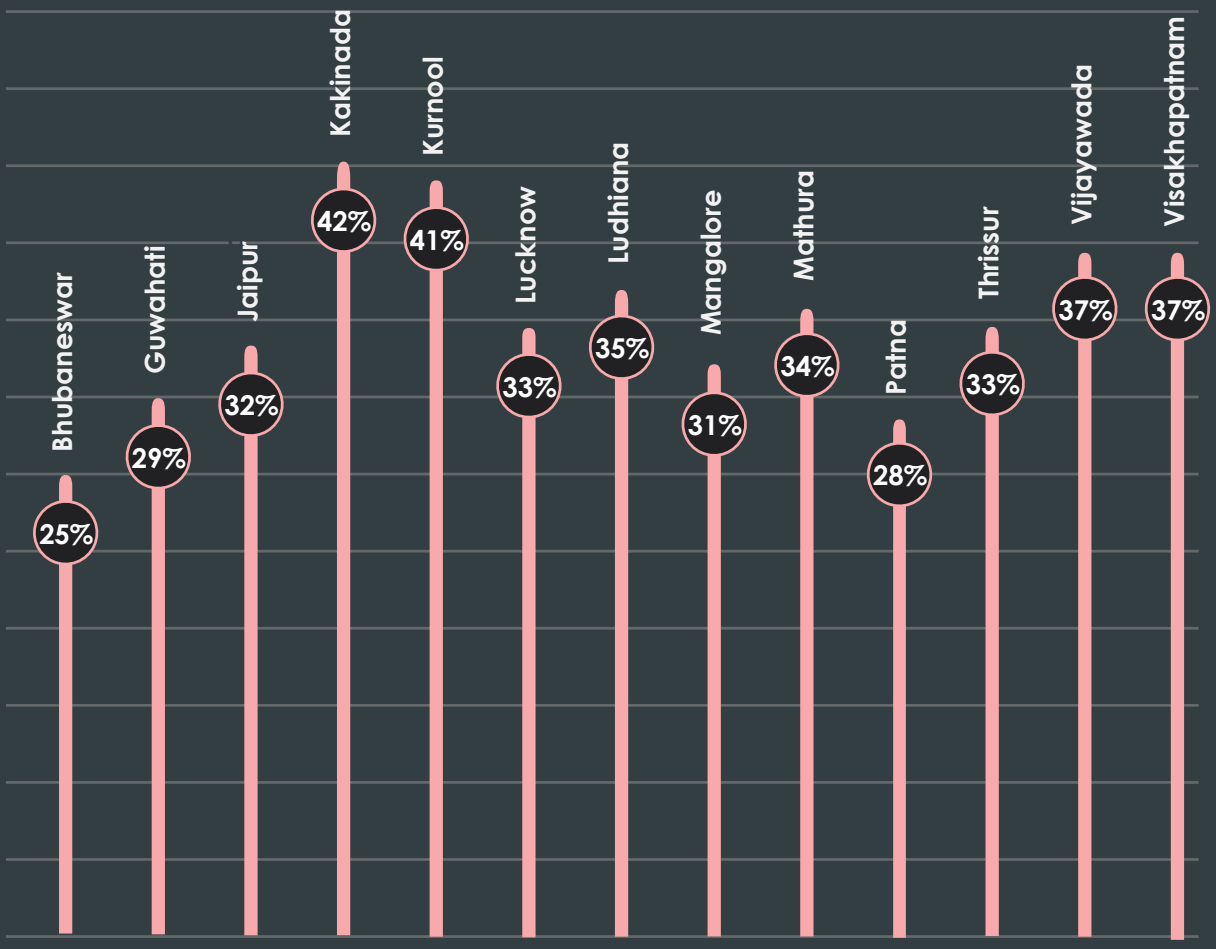
Mumbai
31%



Pune
29%

- Behaviour Protection
- Scan Engine Protection
- Firewall Protection
- Web Protection

Top Infection Rates in Tier-2 Cities

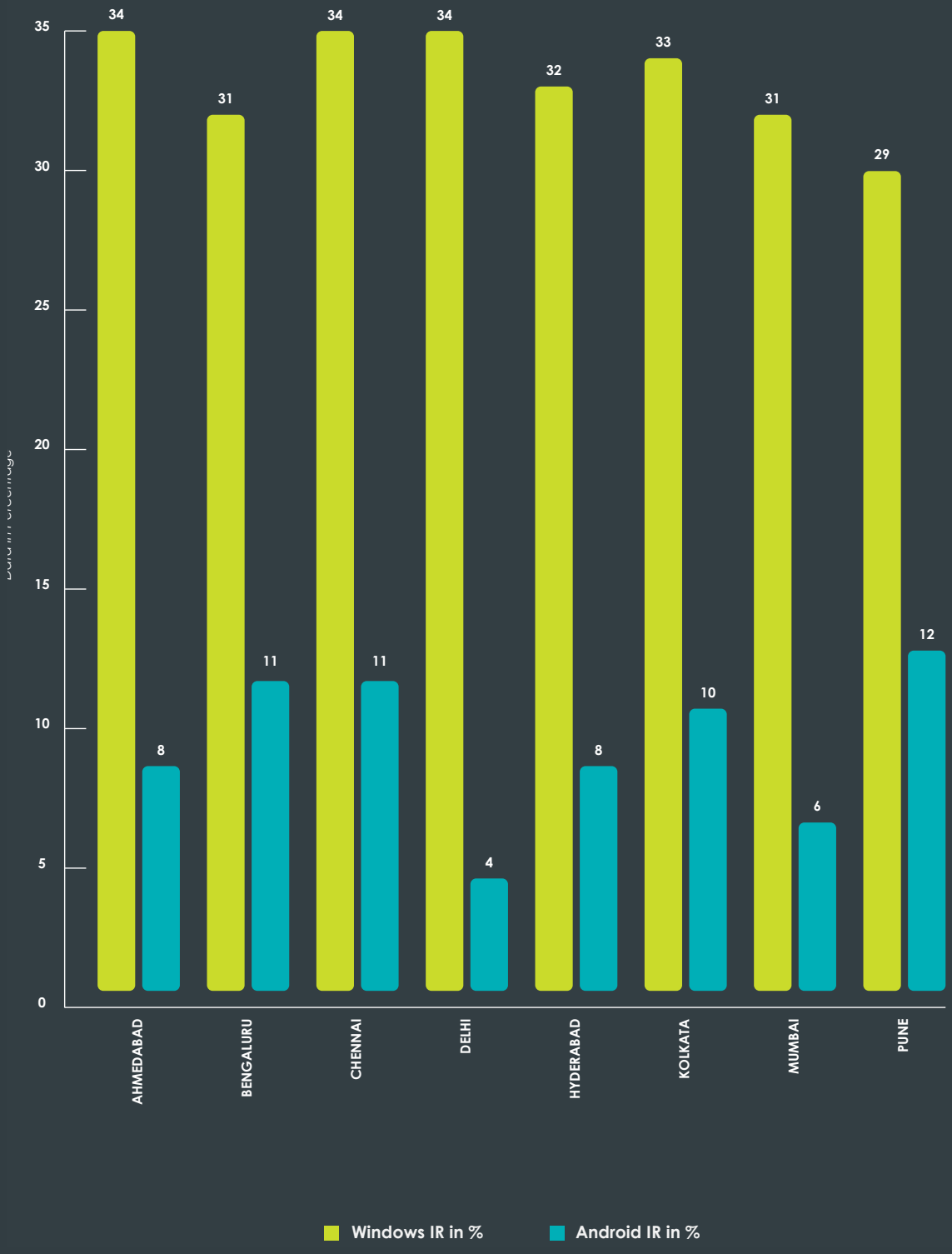


Cyber-attacks targeting netizens' lives in smaller cities have seen a noticeable rise in recent quarters. These attacks can range from stealing sensitive data to shutting down entire computer systems, causing significant financial harm to individuals and companies. Cyberattacks on smaller cities are particularly worrisome, as many may lack the resources to protect themselves adequately against these increasingly sophisticated threats.

Infection Rate Comparison Across Platforms

Both Windows and Android platforms saw a slight decrease in the infection rate, which is a very good trend. Looks like cyber-savvy users have now started to embrace cybersecurity guidelines seriously as can be seen from the stats. We hope this trend continues in the future too.

Windows IR vs Android IR



Enterprise Insecurity

Threat actors are exploring different means to gain access to a victims' system and enterprises are a lucky lure, because of the large attack surface that it could expose. Cryptojacking is one such means to achieve their target, as they can hide quietly in the background to do their malicious activities. Also, threat actors are able to mine for cryptocurrency without incurring huge costs.

Recently, we noticed one such incident at our customer's site. The attack sequence is as illustrated below.

Case Study: Crypto Mining malware disrupts Enterprise Activity

Recently, one of our customers reported alerts from our security product. K7 Labs researchers took a remote connection of the customers' system and identified the following execution sequence.

1

The Alerts

The Alerts were due to abnormal WMI activity, which created unauthorized scheduled tasks and was visible only from the registry entries.

2

Gealning Down Further

On further analysis, we gleaned that these tasks were connected to a Coin Mining website.

3

The Mole

Also, we noticed an unprotected system in the network that was creating remote schedule tasks on other trusted machines.

4

The Shield

Our security product detected all these threats and prevented the malware from executing.

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 unprotected systems and taking steps to protecting them
- Backup your critical data

Vulnerabilities Galore

As the threat landscape evolves, companies must keep up not only with technology but also with the steady influx of new vulnerabilities so as to safeguard their assets. From January through March of 2023, we identified various vulnerability patterns.

This section will discuss the most critical ones from the lot.

RTF Parser Vulnerability

In November 2022, a security researcher discovered a flaw in Microsoft Word's RTF parser, **CVE-2023-21716**, and disclosed it privately. This vulnerability was a heap corruption flaw that could allow attackers to execute remote code on a victim's device with their privileges.
Authentication was unnecessary, as attackers can send booby-trapped RTF files via email.

This flaw affects many Microsoft products, including Microsoft SharePoint Server Subscription Edition. Microsoft Office 2019, 2021, and Microsoft Word 2013 and 2016. Since "Preview Pane" is an attack vector, opening the file is not a requirement for exploitation. Attackers must convince users to open or preview a Word document.

In February 2023, Microsoft released a patch via its Patch Tuesday program. It recommended its users to avoid the preview pane and utilize the Office File Block Policy to block RTF files from unknown sources.

DoS Attacks on OpenSSL

CVE-2023-0286 is an OpenSSL vulnerability that can be exploited for denial-of-service (DoS) attacks that was present in a widely-used cryptographic library due to the way it manages X.509 certificates. Only applications that utilize a custom implementation for obtaining a Certificate Revocation List (CRL) over a network will likely be affected.

This vulnerability may permit an attacker to provide arbitrary pointers for a memcmp call, which can result in them viewing the contents of system memory or executing a denial-of-service attack. The vulnerability has been discovered in OpenSSL versions 3.0.8, 1.1.1t, and 1.0.2zg and has been appropriately addressed.

BIG-IP prone to RCE Attacks

CVE-2023-22374, a format string vulnerability exists in BigIP iControl SOAP, allowing an authenticated attacker to crash the iControl SOAP CGI process or potentially execute arbitrary code. A successful exploit could permit a threat actor to remotely trigger code execution on the device as the root user.

Abusing this vulnerability in appliance mode of BIG-IP could help a threat actor to overlap a security boundary successfully. F5 has fixed the issue and has a hotfix available. However, if you can't use the hotfix, F5 recommends only letting trusted people use the iControl SOAP API so that threat actors can't access the device.

Security Vulnerability in Linux command line

Binwalk, a Linux command-line security tool for analyzing and extracting firmware images, contains a security vulnerability that could enable remote code execution. This vulnerability arises from a path traversal issue originating from the Professional File System (PFS) extractor plugin merging with Binwalk in 2017. User interaction is necessary because opening a "malicious file with Binwalk using extract mode (-e option)" triggers the vulnerability.

The flaw is considered high severity (CVSS 7.8) and has been identified as **CVE-2022-4510**, affecting Binwalk versions ranging from 2.1.2b to 2.3.3. Although PFS is a rare file system format found mostly in embedded devices, Binwalk does remain a popular tool for security analysts.

Privilege Elevation in Microsoft Outlook

CVE-2023-23397 is an elevation of privilege vulnerability in Microsoft Outlook which has been exploited in the wild since April 2022.

An attacker could exploit this vulnerability by sending a specially crafted email setting Calendar Reminder which triggers automatically when processed by the Outlook client. This will leak the Net-NTLMv2 hash of the victim to the attacker who can then relay this to another service and authenticate as the victim.

Vulnerable products are Microsoft Outlook 2013, 2016; Microsoft Office 2019, 2021; Microsoft 365 Apps for Enterprise.

Dangers in the Internet of Things

Regardless of pattern or objective, threat actors want to get initial access to a network. Many IoT devices simplify this process by storing the default password in the device's firmware. In conjunction with weak IoT devices, existing exploits enable threat actors to obtain access while maintaining stealth, as the entry is made using genuine credentials and does not necessarily raise alarms. These choices are especially advantageous for attackers since they are already associated with high privileges, making privilege escalation unnecessary.

This overview shows the most significant security flaws discovered in popular IoT devices.

Susceptible Fortinet Products

CVE-2023-25610 describes a buffer underflow in FortiOS and FortiProxy administrative interface. An unauthenticated, remote attacker can exploit this vulnerability by sending specially crafted requests. Depending on the targeted device, this may result in either a denial-of-service on the GUI or execute arbitrary code on the device.

Vulnerable products are -
- FortiOS - 7.2.0-7.2.3, 7.0.0-7.0.9, 6.4.0-6.4.11, 6.2.0-6.2.12, 6.0
- FortiProxy - 7.2.0-7.2.2, 7.0.0-7.0.8, 2.0.0-2.0.12, 1.2, 1.1

WebKit Vulnerabilities across Apple's Product Series

Tracked as **CVE-2023-23529** and happens when WebKit processes maliciously generated web content. The bug might theoretically allow a remote attacker to build a specially designed web page, fool the victim into opening it, cause type confusion, and execute arbitrary code with the highest privileges on the target machine.

WebKit vulnerabilities are additionally noteworthy since they affect every third-party web browser for iOS and iPadOS due to Apple's constraints requiring browser makers to utilize the same rendering technology.

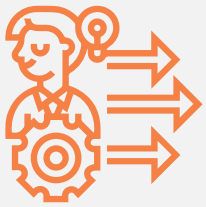
Apple has addressed the issue in macOS Sierra 13.2.1, iOS 16.3.1, iPadOS 16.3.1, and Safari 16.3.

Internet to Baseband RCE Attacks in Exynos Modems

Last quarter, researchers reported eighteen 0-day vulnerabilities in Exynos Modems produced by Samsung Semiconductor. Four most severe **(CVE-2023-24033, CVE-2023-26496, CVE-2023-26497 and CVE-2023-26498)** of these eighteen vulnerabilities allowed for Internet-to-Baseband remote code execution vulnerabilities.

These vulnerabilities allow an attacker to remotely compromise a phone at baseband level with no user interaction, and requires only the attacker to know the victim's phone number.
Samsung Semiconductor's advisories provided the list of Exynos chipsets that are affected by these vulnerabilities. Affected products include -

- Mobile devices from Samsung, the S22, M33, M13, M12, A71, A53, A33, A21s, A13, A12 and A04 series;
- Mobile devices from Vivo, the S16, S15, S6, X70, X60 and X30 series;
- The Pixel 6 and Pixel 7 series of devices from Google;
- Any vehicles that use the Exynos Auto T5123 chipset.



Mitigation Techniques

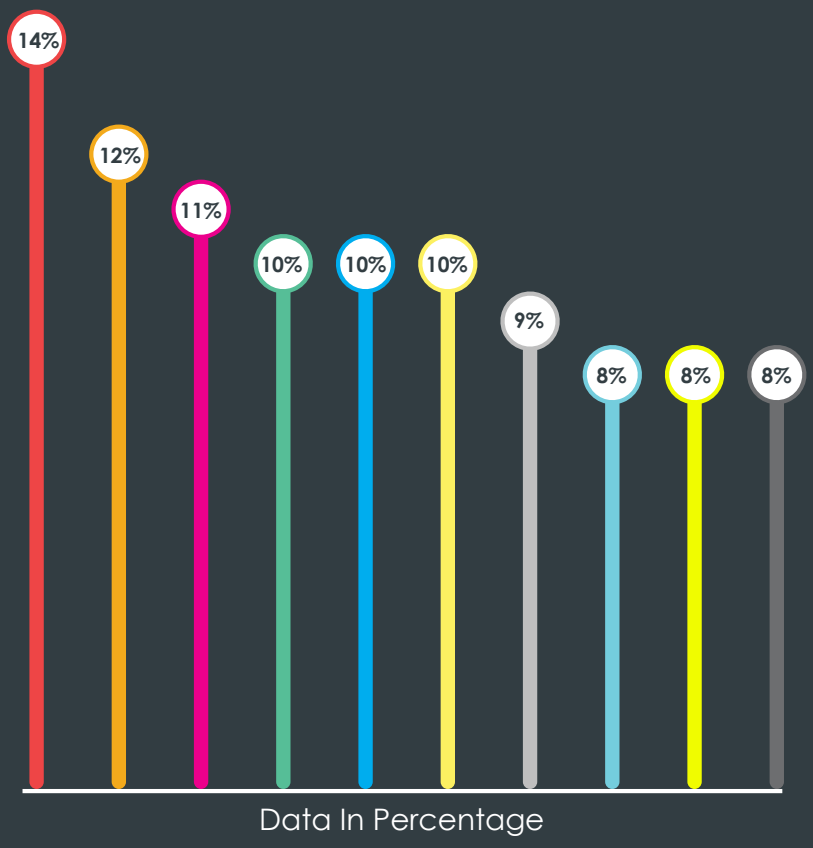
- Secure your linked devices and networks
- Regularly monitor and upgrade your IoT devices and network as soon as a fix has been implemented for any security risk(s) under consideration

Windows Under Siege

Windows Malware Type Breakdown

The Windows platform has always been a target of cyber attacks because of its large user base. Threat actors not only create new malware or modify existing malware code to evade detection but also exploit vulnerabilities in the OS and/or other installed applications. The following chart displays certain significant detections.

Split of Windows Top 10 Detections

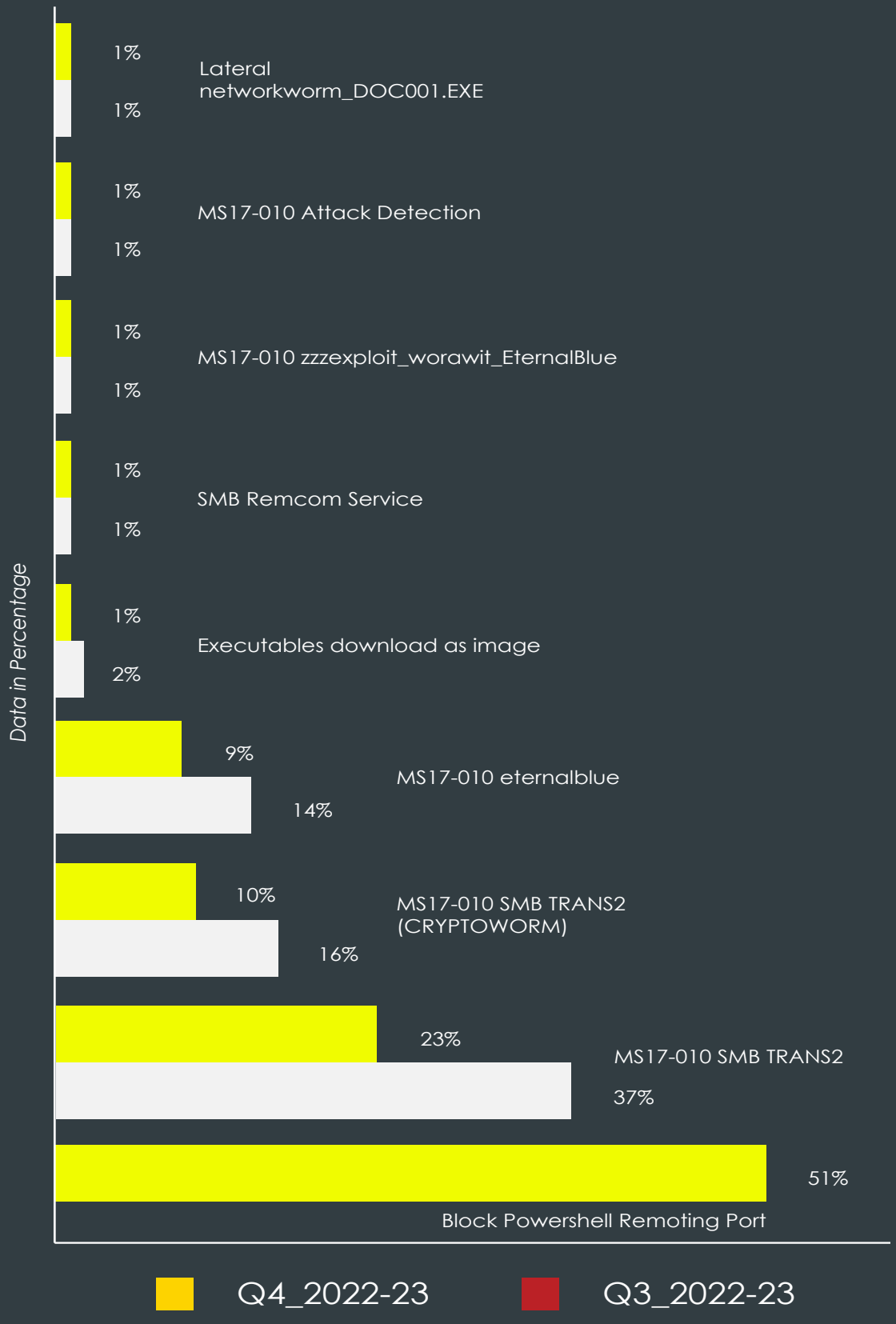


- Hack.MSIL.IdleKMS.I
- Hack.Win32.AddUser
- Hack.MSIL.IdleKMS.E
- Hack.Win32.AA
- Hack.MSIL.IdleKMS.EE
- Wrm.MSIL.LG
- Wrm.win32.LG.4
- Hack.Win32.IdleKMS.E
- Adw.win32.Setupdownloader
- Hack.Win32.KMS.H

Windows Exploits

Though Microsoft regularly patches the vulnerabilities in its operating systems and requests users to apply the patch through its Patch Tuesday programme, enforcing discipline is difficult mainly due to its vast user base. The prevalence of dated vulnerabilities is one such example.

Most Prevalent Exploits

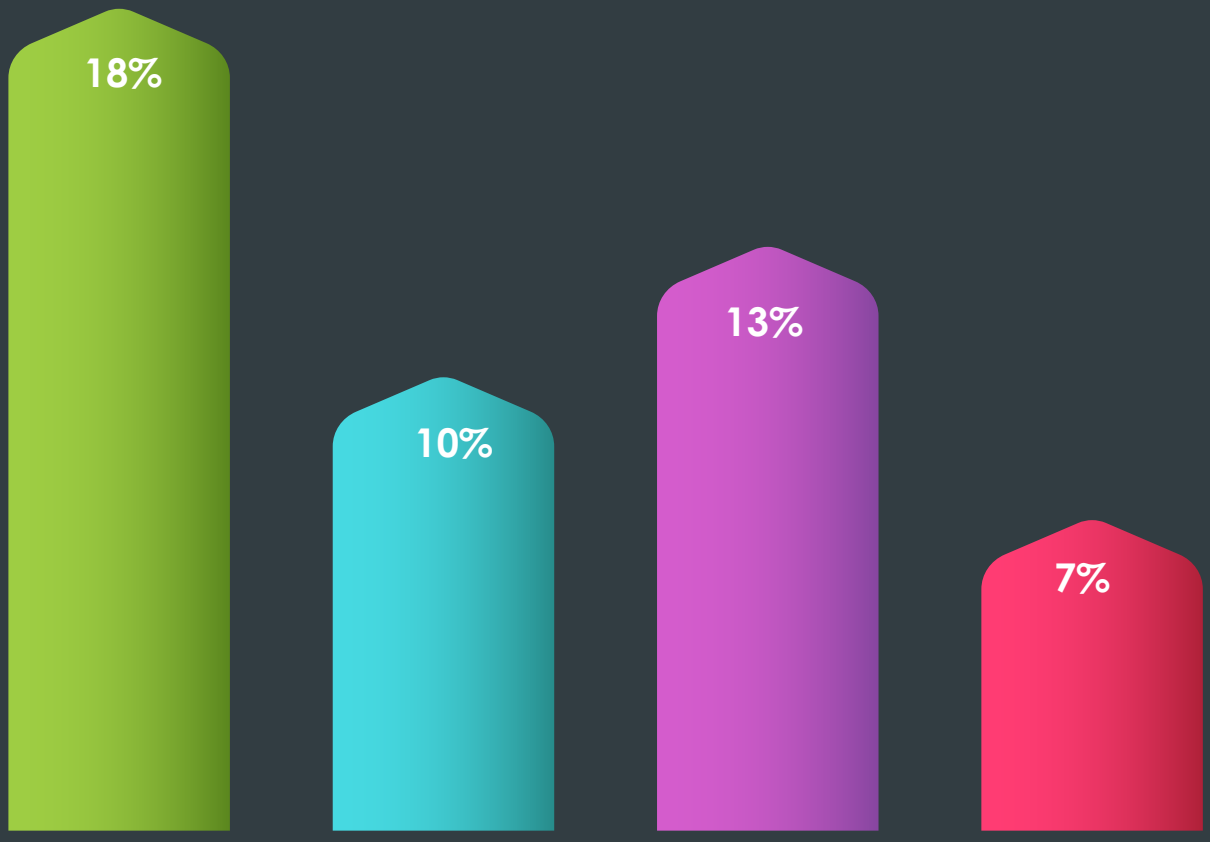


Heuristic Host Intrusion Prevention System (HIPS)

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.

Windows Heuristic Behavioural Detections



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.

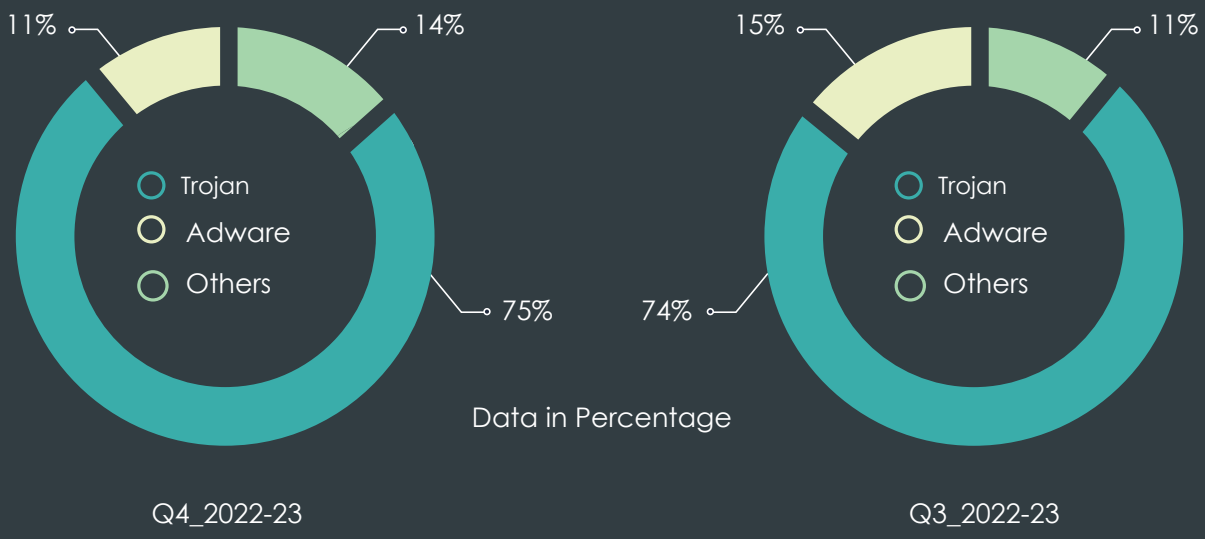
Mitigation Tips

- 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

The Mobile Device Story

Malware attacks on mobile devices have seen a spike with the increase in usage of smartphones among users. Smartphones have become an appealing target for attackers because they hold sensitive personal and financial data as everything is available at the click of a button. In addition, the usage of third-party app stores and the absence of security upgrades from device manufacturers or carriers makes it simpler for threat actors to exploit vulnerabilities on these devices.

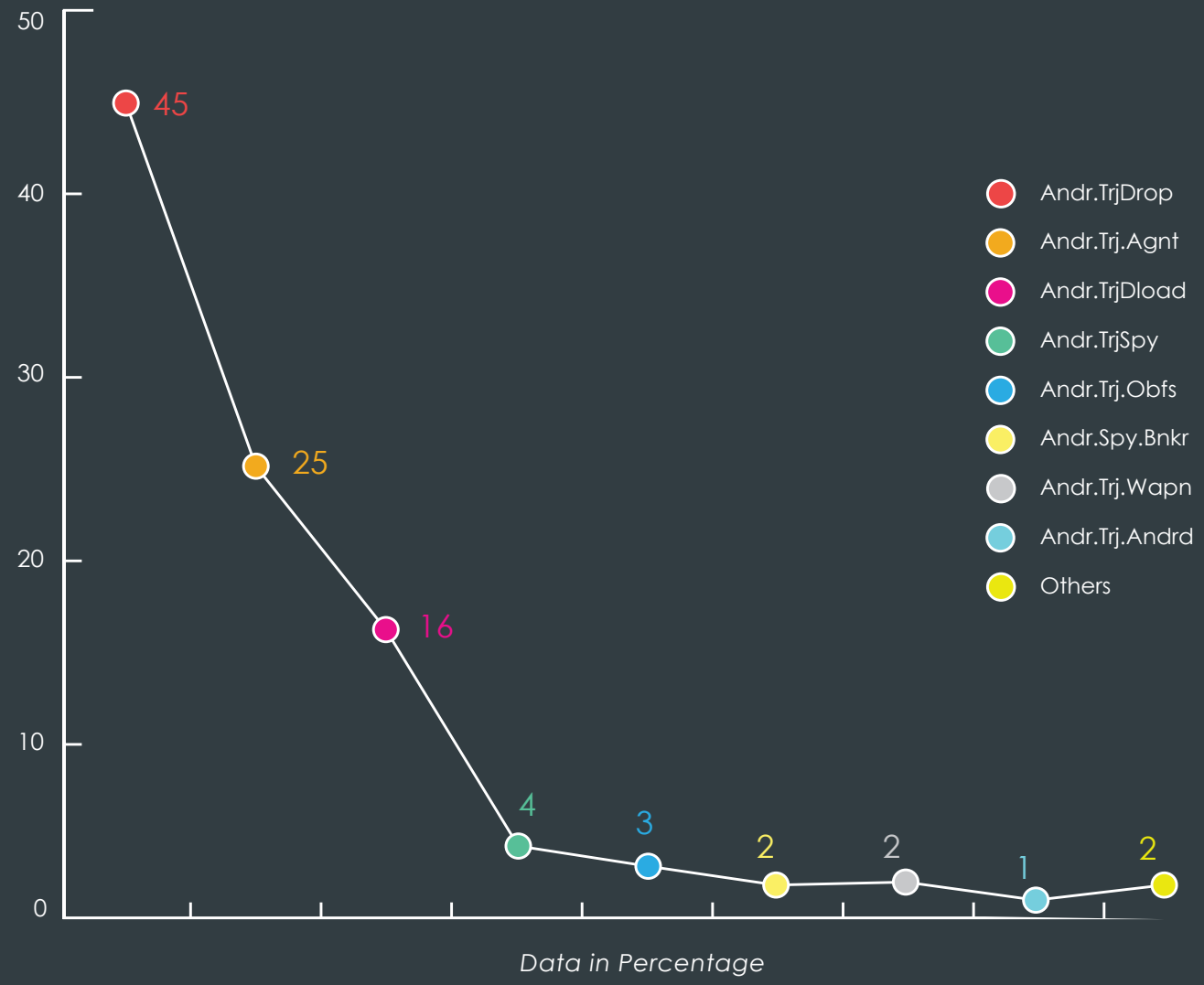
Adware vs Trojan Proportional Split



The Omnipresent Trojan

Trojans have been used as a means to attack smartphones for carrying out the threat actors' malicious intents such as remote access, 0-day exploits, data theft, and much more.

Most Prevalent Trojan Types

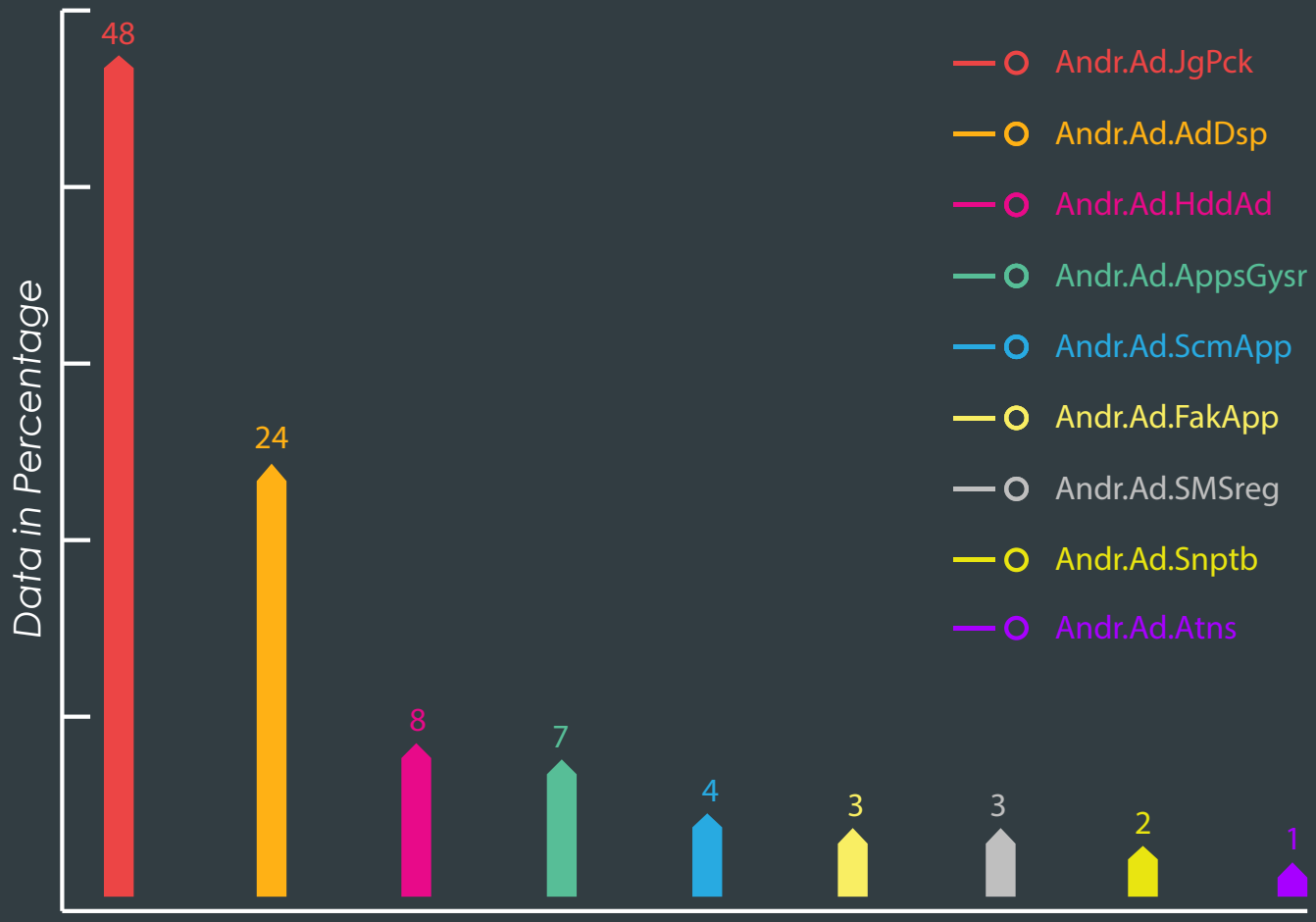


Agent and malware downloaders have remained a popular choice among threat actors for their ability to offer a convenient way to deliver malicious payloads to their targets while remaining undetected by security software. The massive share of malware downloaders and agents in the previous quarter reflects the same.

The Adware Saga

The decreasing popularity of adware is seen from our telemetry numbers. However, older families continue to rule the roost, helping the threat actors to make easy money.

Trend Line Showing the Adware Plague



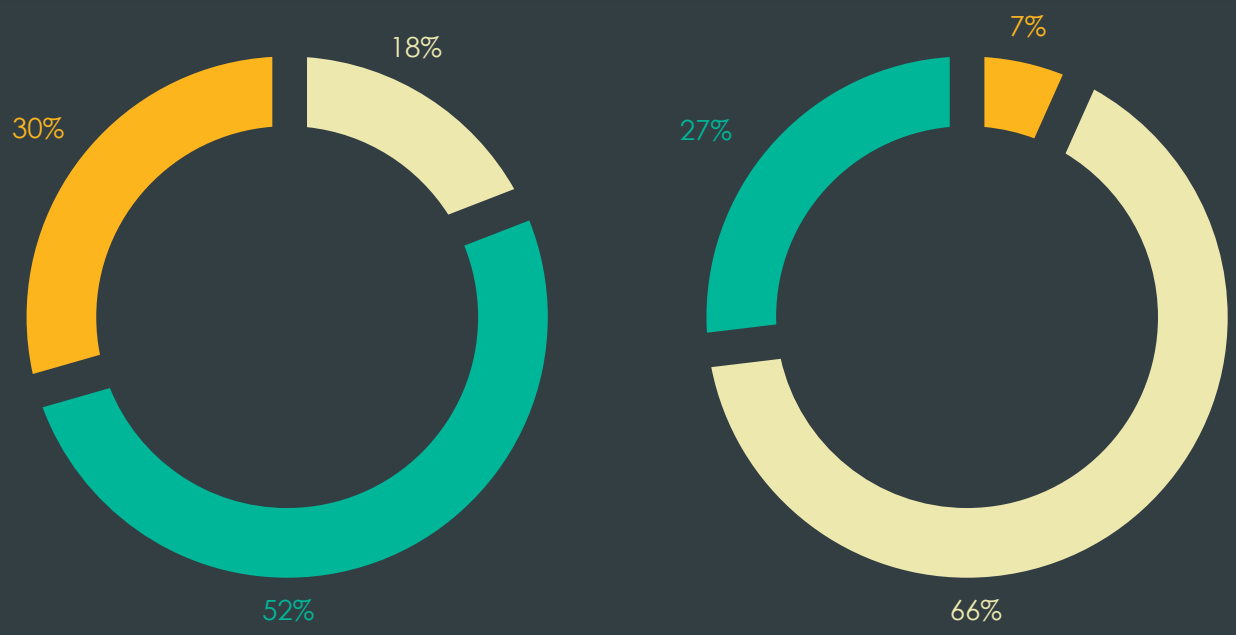
Tips to Stay Safe

- 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

Threat actors have started focusing on Mac user space mainly due to the rise in the usage of Apple's PC and laptops of late. Another significant reason behind the increasing number of attacks is because of the valuable personal and financial information that can be gleaned from the same. Also, macOS users are mostly high-income earners, which may make them attractive targets for cybercriminals looking to exploit for financial gain.

Trojan, Adware & PUP Proportional Split



Apple's uncompromising stand in the app and data sharing controls has undoubtedly helped the threat landscape to witness the diminishing proportion in Trojans share across the quarter.

The Diminishing Trojans

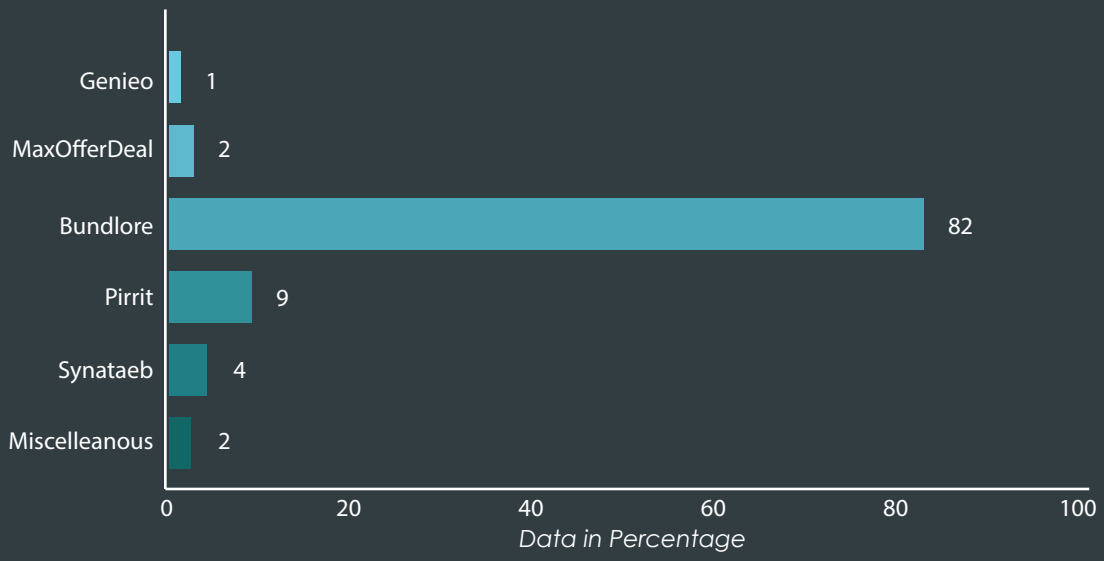
Even though the overall numbers have plummeted last quarter, the presence of Adload has increased significantly, raising a cause for concern.

Trojan Detection Trend Lines

The Adware Brouhaha

Bundlore has held the top spot on the macOS threat landscape for several quarters, with an increasing presence last quarter. The number also hints at how Apple computer users still fall prey to threat actors' tactics and techniques.

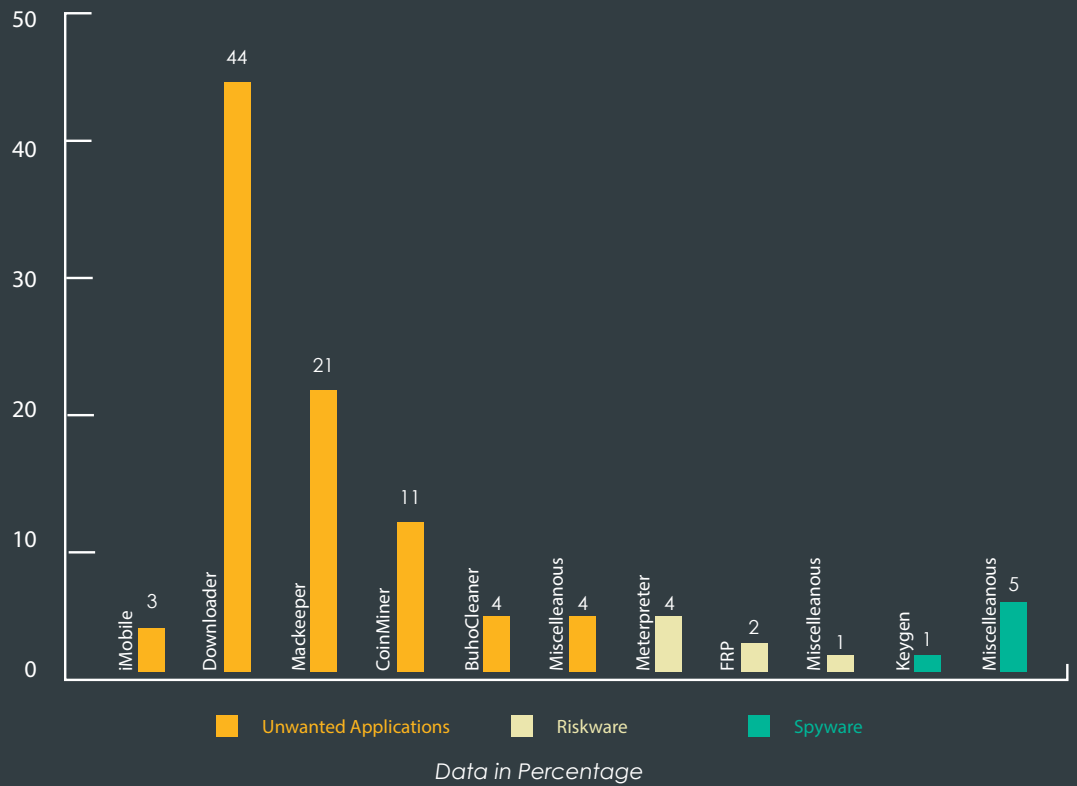
The Trend Line of Adware Variant Detections



A Pinch of PUPs

PUP's presence has remained relatively high despite Apple's extensive steps to safeguard the macOS software store. Downloaders still get much attention, but those masquerading as system cleaners and performance boosters like MacKeeper 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

Key Takeaways

Almost every quarter, enterprises seem to be bearing the brunt of cyber attacks. To safeguard themselves, they should opt for a security by design approach which also includes installing a reputable security product and following good cyber hygiene practices some of 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

Q4

APRIL 2023

www.k7computing.com