CYBER THREAT MONITOR REPORT

Q1_2024-25

LEVERAGING THREAT INTELLIGENCE INDICATORS TO PROACTIVELY FIGHT CYBER THREATS

RAISE YOUR GUARD AGAINST RISING RANSOMWARE THREATS

Ransomware attacks have become more streamlined these days, and are a popular attack tool with both amateurs and experts in the cyber threat industry. It is now very easy to purchase a ransomware strain off the dark web or use the services of a Ransomware-as-a-service (RaaS) model at a very nominal rate. Ransomware has been on the rise over the past few quarters, as threat actors are adapting their attack techniques along with the evolving digital landscape, making it a difficult task for the cyber security industry to find a single protection against it.

Though ransomware breaches are not fully preventable, organizations can take steps to reduce the ransomware risk by putting as many barriers as they can between the threat actors and their critical and sensitive data. Regular vulnerability assessment also should be done to find an organizations' security stance. This can help fix vulnerabilities before the threat actor identifies the same for exploitation.

WIth enterprises having to bear the brunt of attacks and with different tailor-made Tactics, Techniques & Procedures (TTPs), and MITRE ATT&CK techniques being used, the cyber security industry has to keep pace with the ever growing threat industry to stay put.

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.

Kindly read and share the report with your colleagues. Have a safe digital experience!

Enjoy reading!

INFECTION RATE (IR)

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

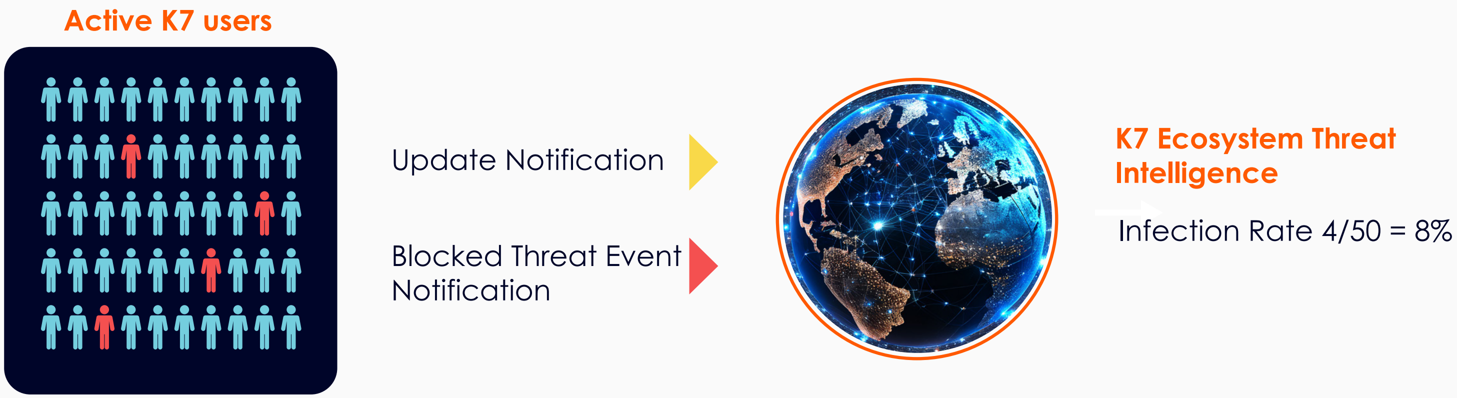
Those new to our quarterly report need to understand an important concept called "Infection Rate" (IR), which is used as the base for benchmarking cybersecurity risk for enterprises and netizens.

We use this IR factor to identify enterprises and netizens' exposure to cyber threats. IR is determined as the proportion of active K7 corporate or consumer users who encountered at least one cyber threat event which was blocked and reported to our K7 Ecosystem Threat Intelligence infrastructure (K7ETI). The higher the IR, the greater the risk.

Active users indicate users who have activated and updated their products.

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

Infection Rate (IR) of an area



Active K7 users

Update Notification

Blocked Threat Event Notification

K7 Ecosystem Threat Intelligence

Infection Rate 4/50 = 8%

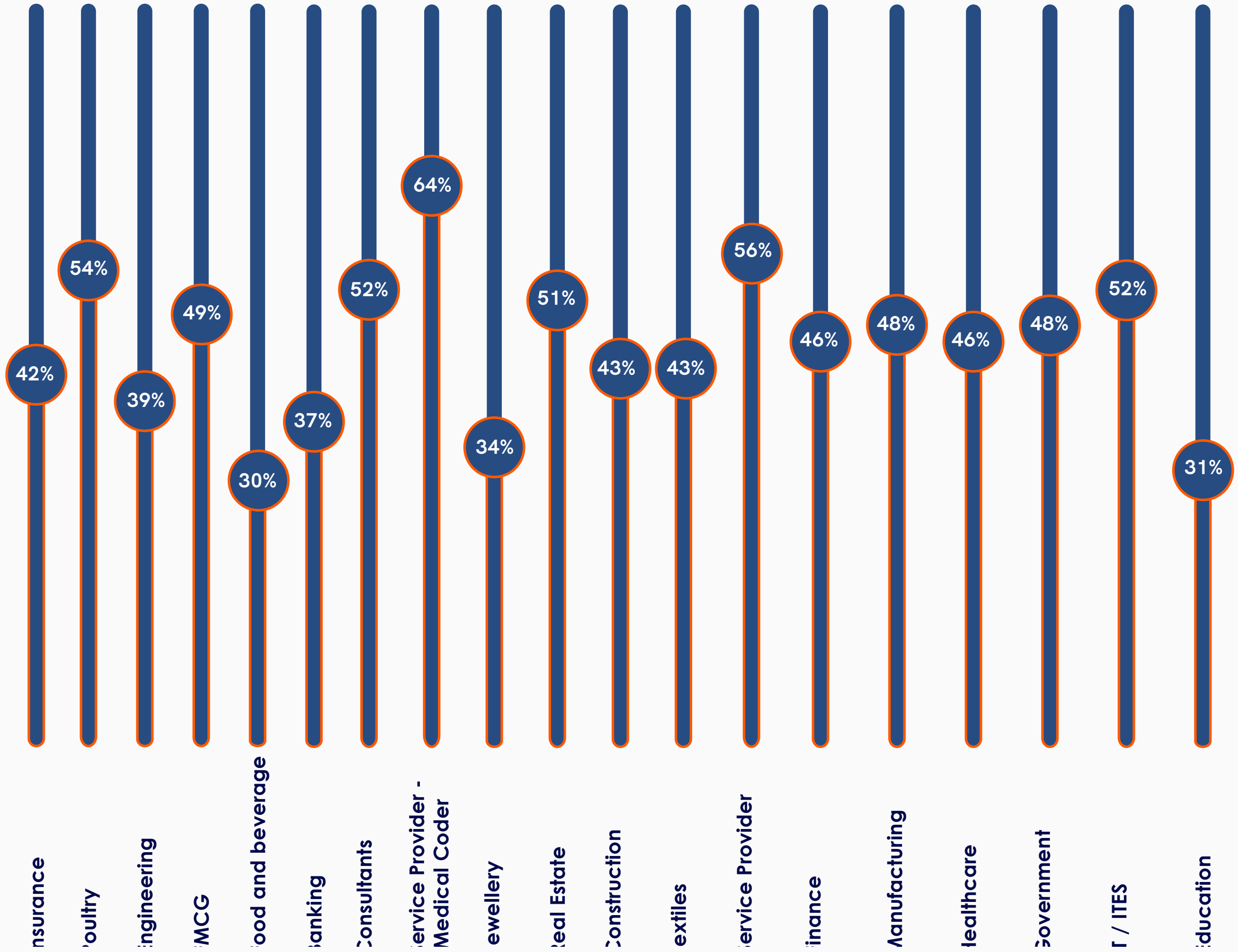
The Global IR for Q1_2024-25 was 58%

INDUSTRY THREAT LANDSCAPE

The Threat Scenario

Here, we have classified threats to Industries, based on the IR and also based on their threat percentage, which identifies the industries mostly targeted by the threat actors.

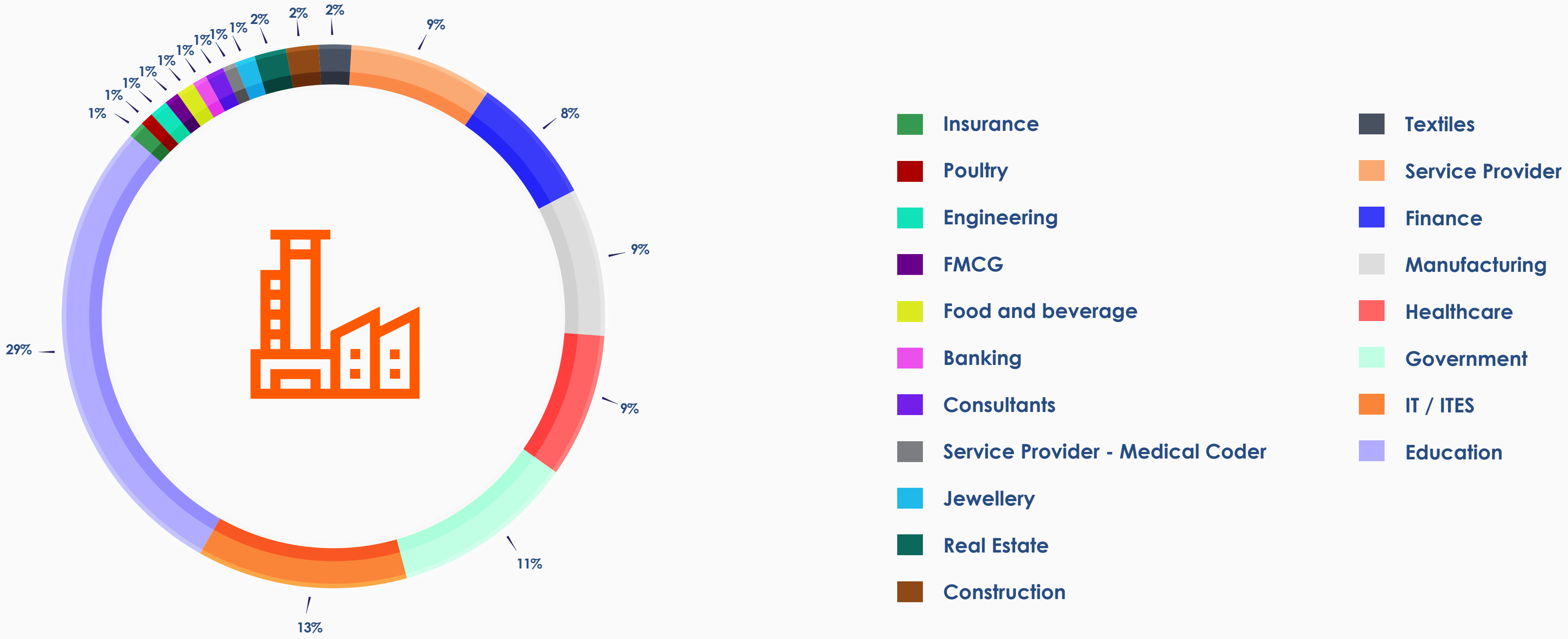
Top Industry Verticals Vulnerable to Cyber Threats



INDUSTRY THREAT LANDSCAPE

This chart depicted above lists the top industry verticals based on their IR.

Industry-wise Threat Percentage



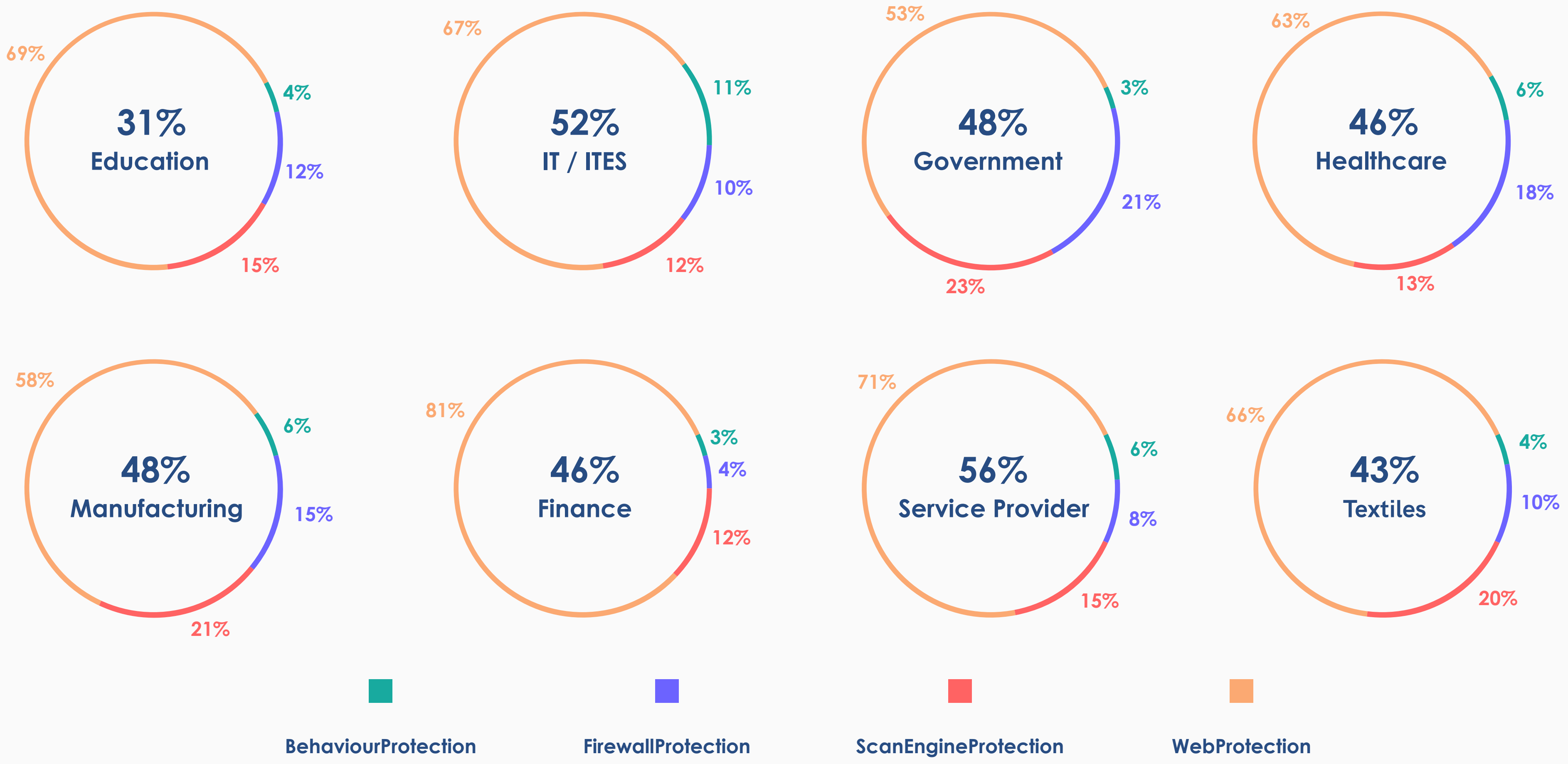
This pie chart reveals the industries that are a favorite target for threat actors. From the chart, we can decipher that the Education sector has been the most affected. This is especially after the pandemic, when students had to rely on e-learning and various communication platforms to collaborate and communicate. Given a very short time to get the entire system up and running, the primary motive was connectivity rather than cyber security in mind. Similarly, the IT/ITES sector had only a short recovery period to get back to business without any major outages from their end. The sector, therefore, had to allow their employees to use their own systems and mobiles for doing official business also, again with a scant regard to cyber security.

Threat actors target government organizations as they hold sensitive data about their citizens and also data pertaining to national security. They also target organizations from where they can extract a lot of money, and those where their operations cannot be halted, especially in industries like Healthcare, which cannot afford to put their patients' lives at stake.

This threat percentage graph shows the proportion of threats across industry verticals, and is different from the IR chart shown above, which depicts the proportion of malware infections in a given industry vertical.

THE LAYERED SPLIT

We have listed below the top industries vulnerable to cyber threats based on the different levels at which the threats were blocked.



The WebProtection layer offers protection to active users from internet-borne cybersecurity risks that can damage devices, systems, and networks, expose users to online harm, and cause undesired actions or events.

The ScanEngineProtection layer has various signatures to protect users against all known threats. Users are required to update their product to the latest scan engine so as to stay protected from the latest threats. This blocks all artefacts deemed malicious, both real time or on-demand.

The FirewallProtection layer is usually an organization's first line of defense against malware and data breaches. All traffic traveling into and out of the network is scanned for signs of malicious activity and blocked.

The BehaviourProtection layer focuses on an artifact's actions on your device. For instance, when the artifact is executed, rather than relying on known attributes like file names or hash values.

As we can see from the layered detection chart, most of the threats were blocked by our Firewall rules, when the artifact performed some action on the device or threats from the internet.

INTERPRETING USER BEHAVIOUR

1. Corporate users are still very much susceptible to cyber attacks via phishing emails, especially if the emails purportedly come from their higher-ups such as CEO, CTO among others
2. Most of their staff still do not follow safe internet browsing, such as being cautious about the links they click, downloads they install and execute, among others
3. Though our security product blocks malicious packets from gaining access to the network, organizations need to make sure that they update their firewall rules and our product regularly to receive the latest definitions so as to stay protected from cyber threats

Enterprises can make themselves less susceptible to cyber attacks by making sure the following points are taken into consideration.

1. Secure entry points to your network

   Mobile networks, IoT (Internet of Things) devices, and cloud storage are susceptible entry points. Enterprises should make sure all external-facing systems should be secured to prevent unauthorised access to their network and data breaches.

2. Email security

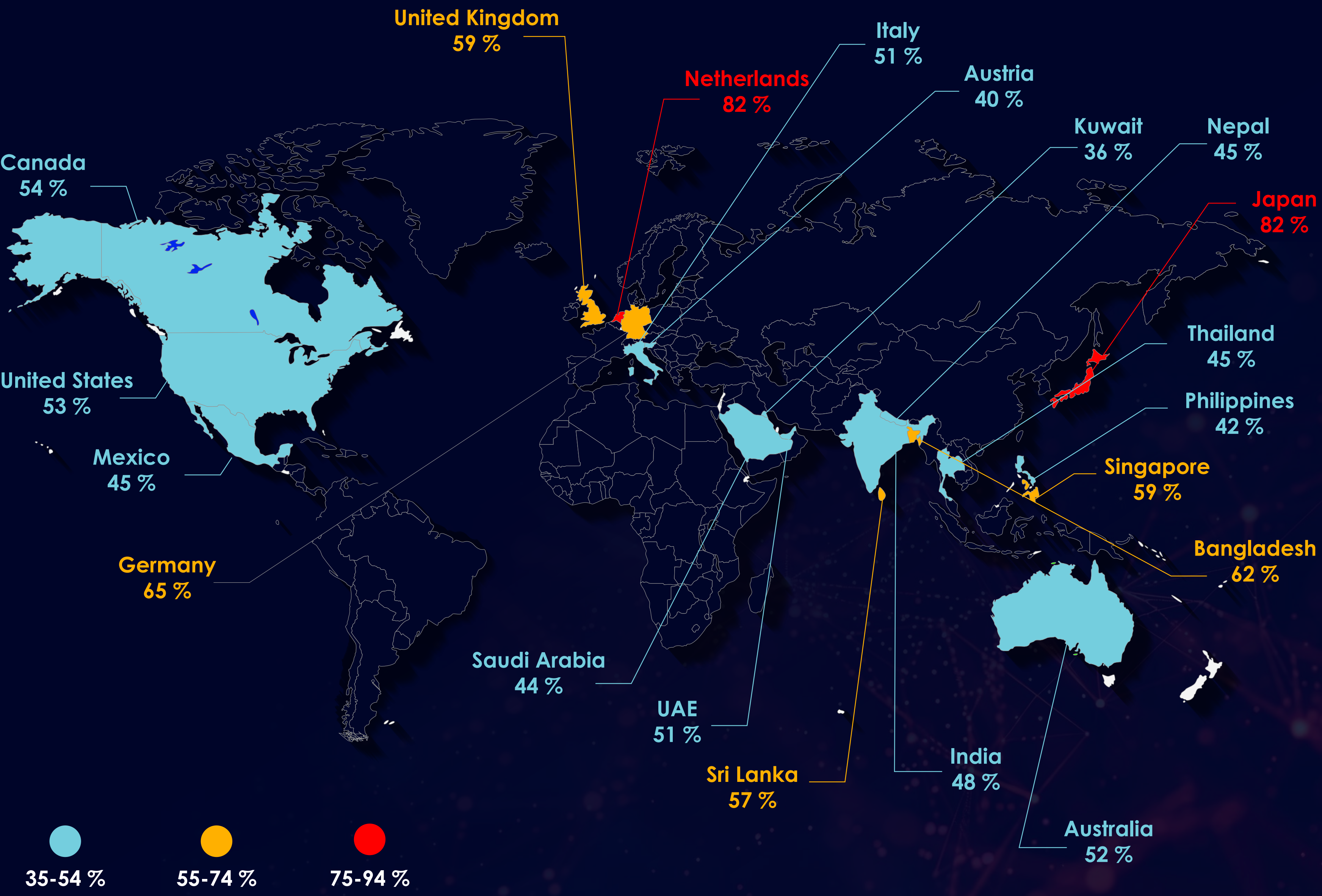
   Phishing emails are one of the most common ways threat actors use to gain access to enterprises' networks and data. Scanning all emails having links and attachments for malware and quarantining the same before they reach your staff's inbox and training your staff to identify phishing emails is very essential.

3. Vulnerable systems and out-of-date software

   Antivirus not activated and updated for the latest definitions, misconfigured firewall rules, unpatched operating systems, and unsecured networks, servers, and software put your organization at risk, which should be taken care of.

CYBER THREAT LANDSCAPE - WORLD

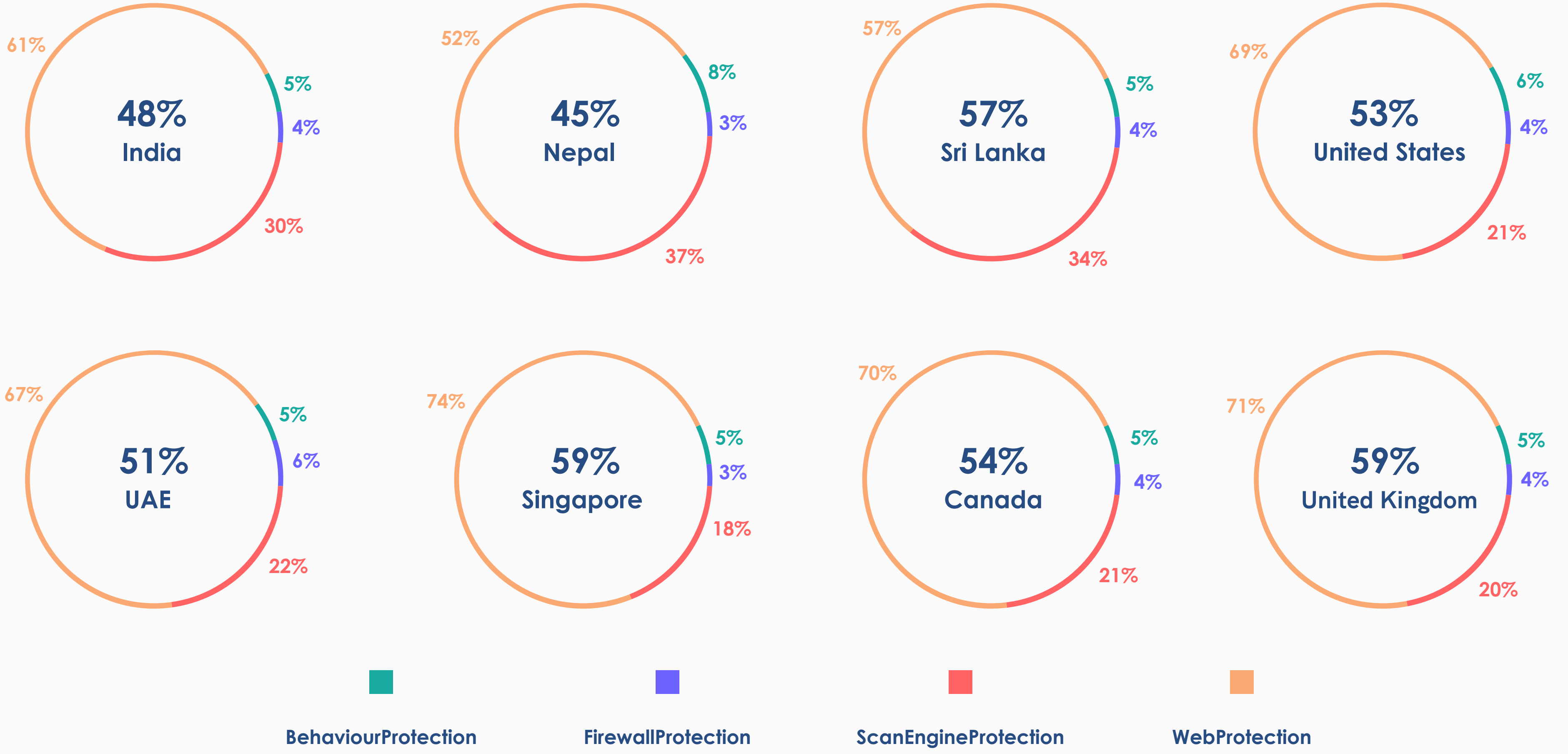
Countries that are technologically advanced, have a large economy, and populated countries experience the most threats due to their large attack surface, as when connectivity increases, it makes it easier for threat actors to laterally move across an entire network.



THE QUARTERLY TRENDS AND STATISTICS

Top Susceptible Countries to Cyberthreats

We have listed below the top countries based on the different levels at which the threats were blocked, and preferred by threat actors.

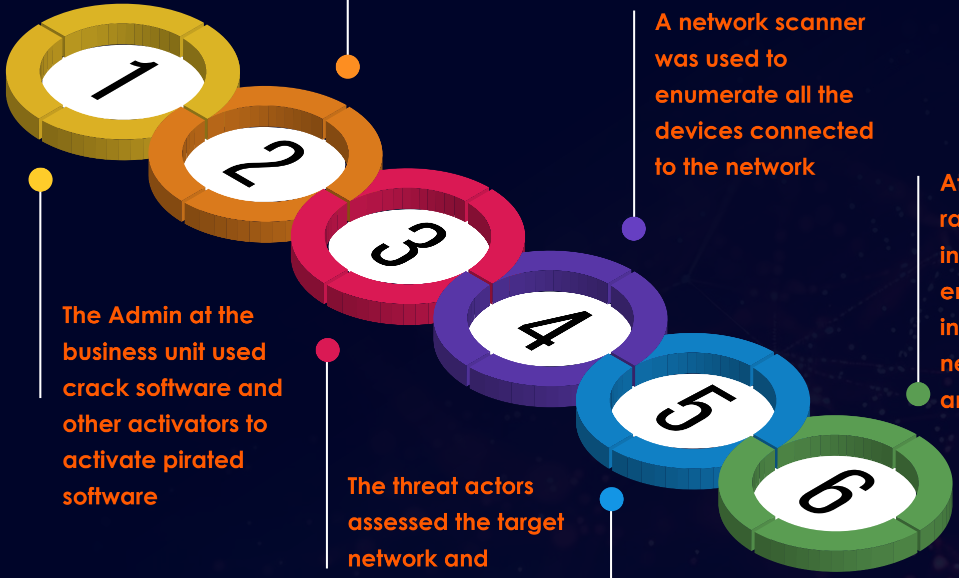


ENTERPRISE INSECURITY

There has been a spike in ransomware attacks across enterprises globally. Organizations need to be aware of the techniques used by the attackers and update their defenses to stay safe in this cyber environment.

Recently, a business unit was impacted by a ransomware attack.
The ransomware strain was identified to be that of the Crytox family.

The kill chain is as depicted below



The Admin at the business unit used crack software and other activators to activate pirated software

Threat actors tracked the business unit, by tracking the activators

The threat actors assessed the target network and exploited a vulnerability in the MS Exchange Server to gain a foothold in the network

A network scanner was used to enumerate all the devices connected to the network

Mimikatz, a Windows password revealer tool, was used to acquire user credentials

Attackers then ran the ransomware payload in the system, encypting all the files, including the network-shared folders and shared drives

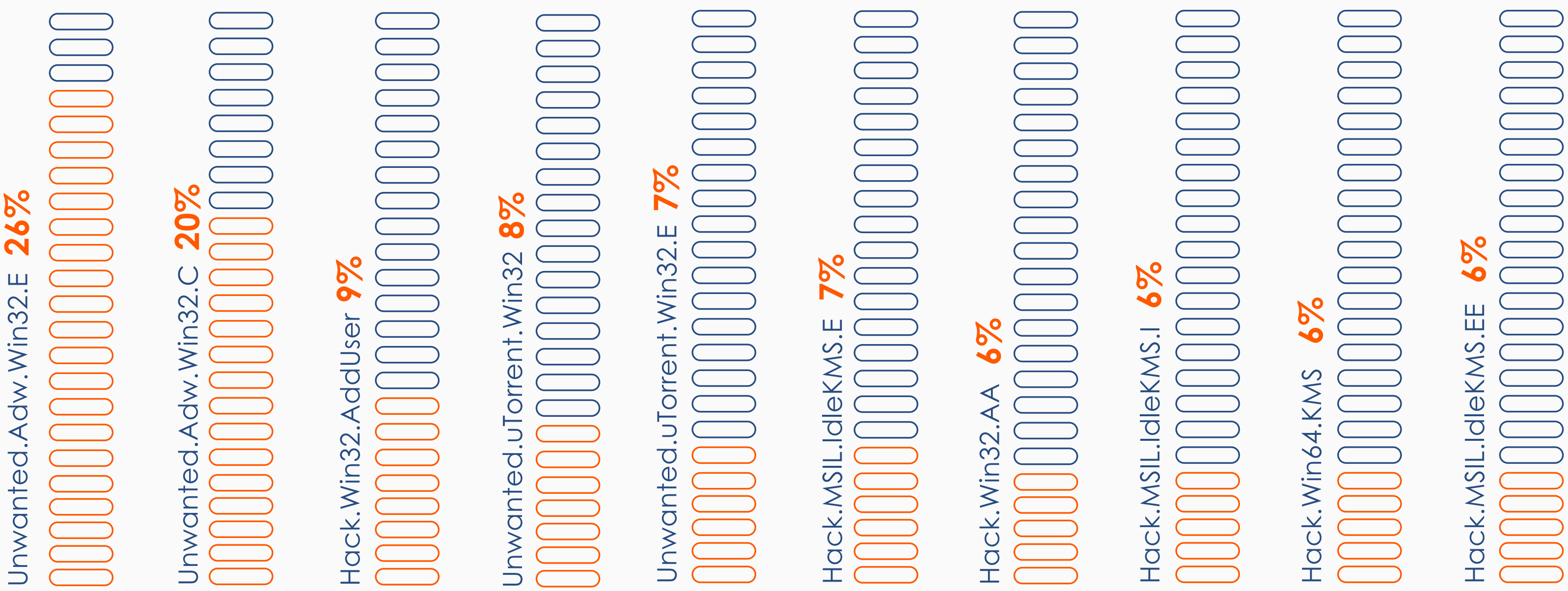
WINDOWS THREAT LANDSCAPE

Threat actors target enterprises with plenty of money as most of the attacks are financially motivated. Also, because of a data breach, a lot of their sensitive data could be leaked, which would also cause a reputational loss, making the organizations agree to the threat actors' demands. With Windows being the most used OS, and having a large user base, makes it convenient for adversaries to exploit the still unpatched vulnerabilities to gain access to their network and do the intended damage.

Windows Malware Type Breakdown

Windows operating systems are used almost everywhere, be it in businesses, schools, and homes. This popularity makes it an easy target for threat actors who are using sophisticated Tactics, Techniques and Procedures (TTPs) to launch their attacks. This creates a challenge for organizations to safeguard their systems and data. With the growth of internet-connected devices, threat actors are using social-engineering techniques, among others, to exploit unpatched vulnerabilities and penetrate into the organization's network.

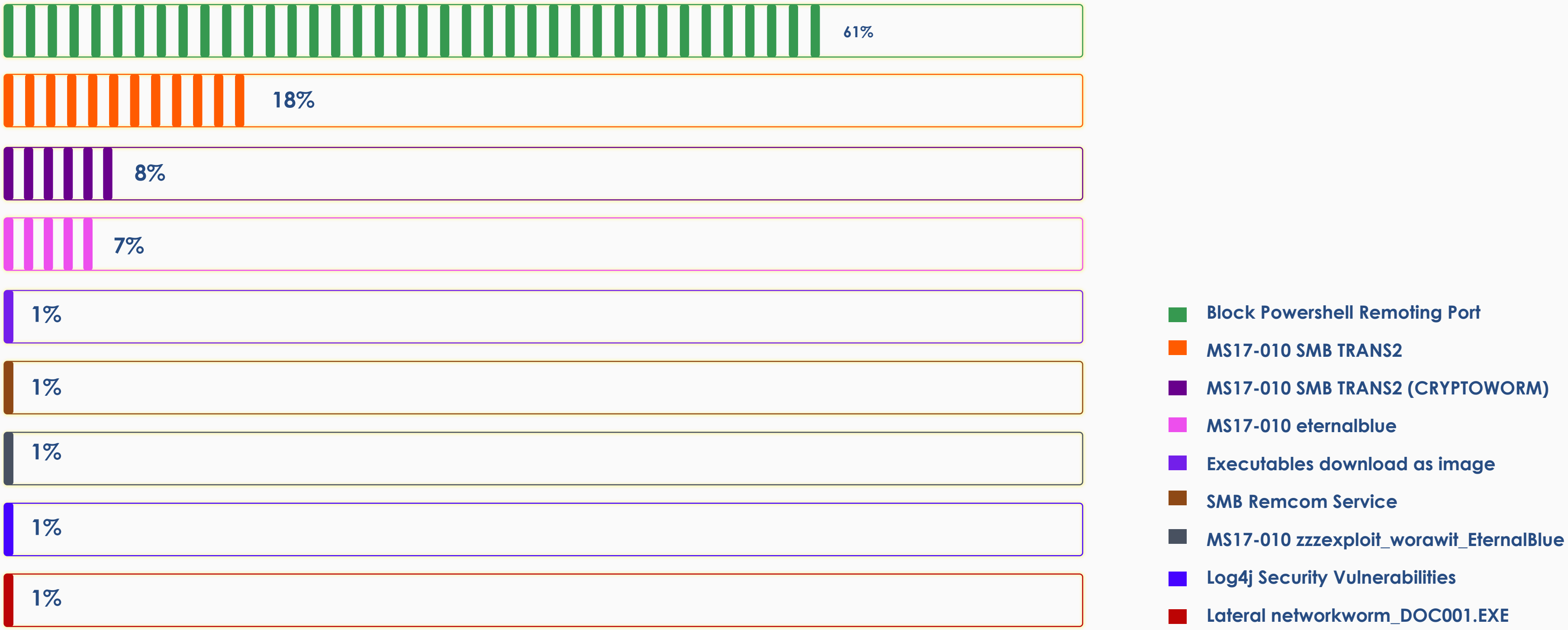
SPLIT OF WINDOWS TOP 10 DETECTIONS



Windows Exploits

It is practically impossible to make a 100% unhackable device. Even if you try to, one needs to compromise on utility vs security. Microsoft is trying to create this balance, and they are doing their best in fixing known vulnerabilities with their "Patch Tuesday" program.

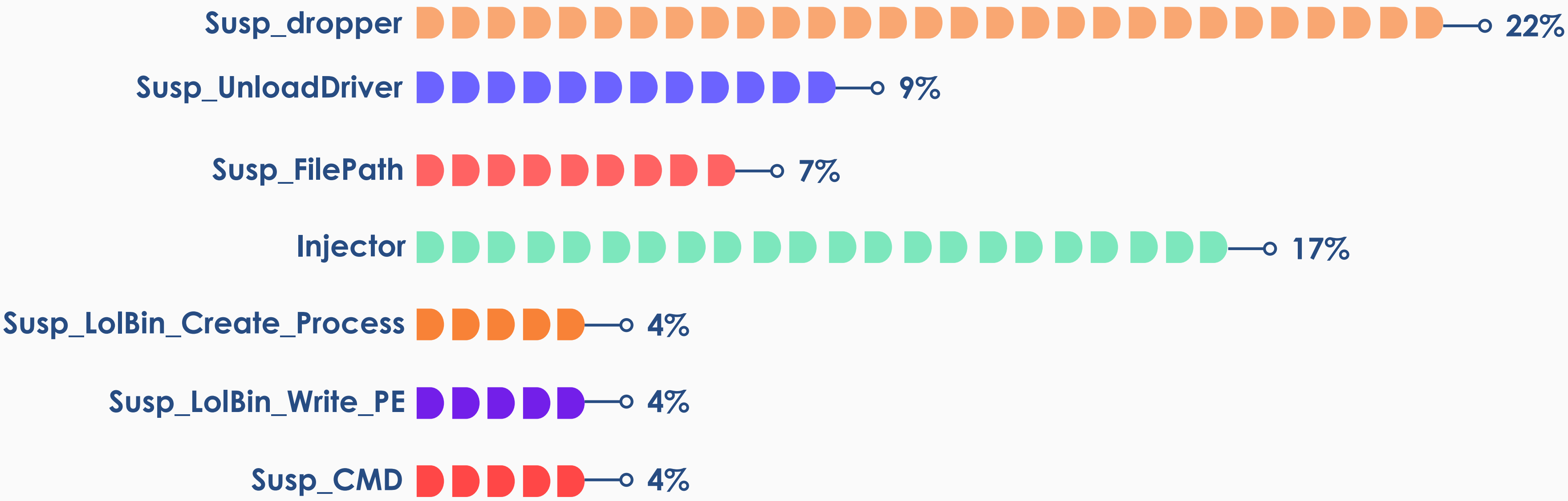
Most Prevalent Exploits



While Microsoft has significantly improved Windows security over the years, its unpatched legacy vulnerabilities, like those in SMBs and PowerShell, have massively contributed to the constant escalation in various Windows devices being targeted. Cybercriminals have increasingly utilised PowerShell for malicious activities, such as delivering malware or executing various attack techniques. PowerShell's versatility and deep integration with the Windows operating system make it an attractive choice for attackers.

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.



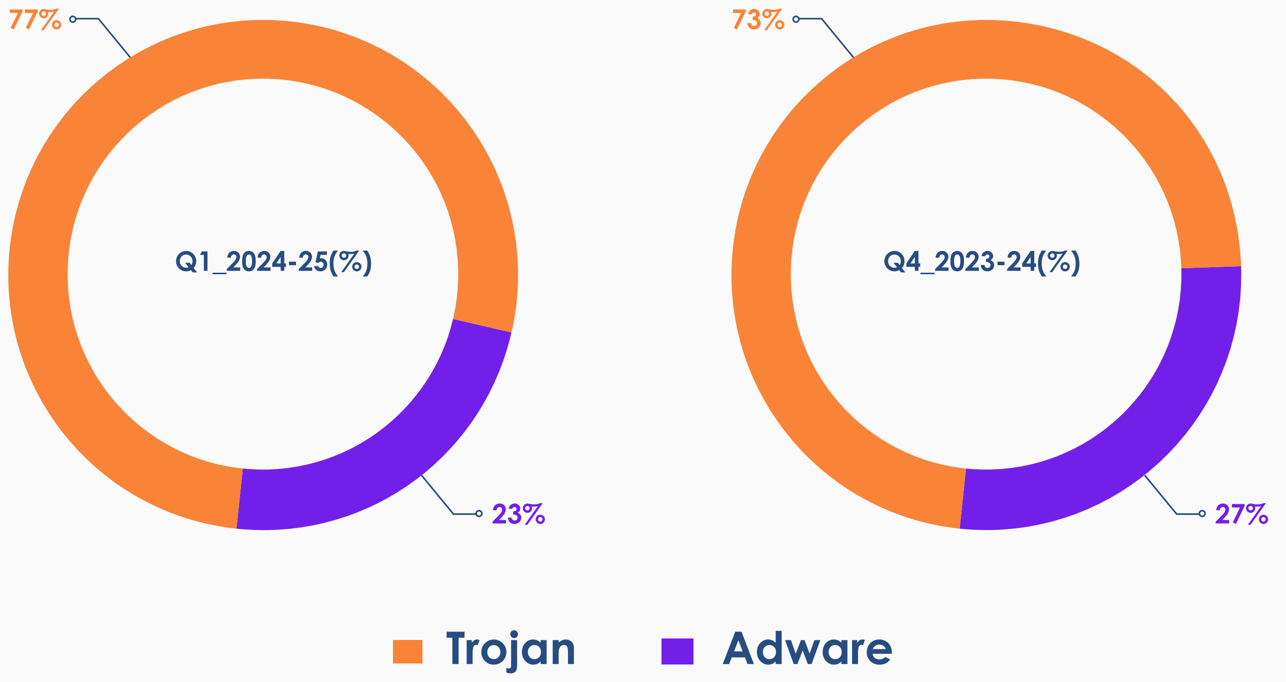
Last quarter, Injectors and Droppers were the most prevalent. Injectors are malware that use legitimate file names or locations to hide behind trusted names so as to evade detection. Injectors, as the name indicates, inject code into processes, typically legitimate and trusted services. This is also usually done to evade AV detections, or gain privilege elevation, or both. Droppers are used by threat actors in multi-stage attacks where additional malicious payloads are downloaded or dropped.

MOBILE THREAT LANDSCAPE

Mobile devices extend an enterprise's periphery and can be a delicate link in the defence line. The unstoppable growth of malware in the mobile space is primarily due to the rise in apps catering to various smartphone users' needs. Threat actors exploit this by targeting victims with fake and trojanized versions of legitimate apps, raising grave concerns about data security and user privacy.

Phishing, fake apps, and other prevalent Android-based cyber threats are widespread, significantly impacting the mobile threat landscape.

Adware vs Trojan Proportional Split

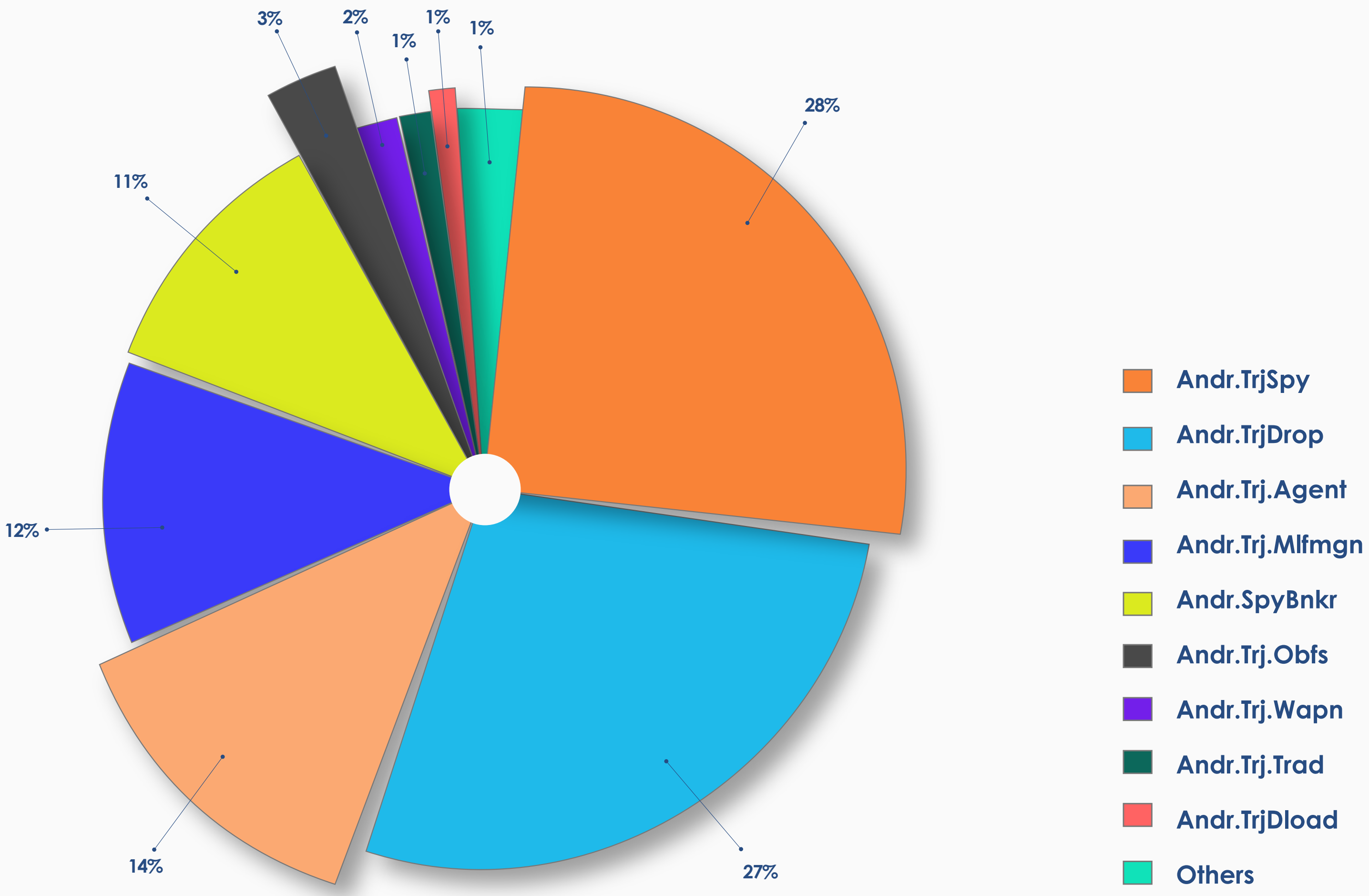


The comparison between two consecutive quarters underscores the dynamic nature of mobile threats. Trojan attacks have soared by 4% while adware attacks have tanked by 4%, revealing how Trojans and adware collectively impact the Android threat landscape.

THE OMNIPRESENT TROJAN

Trojans' visibility on the Android platform is soaring due to their evolving complexity and ability to bypass traditional security measures. This increase highlights their sophisticated tactics, such as mimicking legitimate apps and exploiting system vulnerabilities, making them a growing menace.

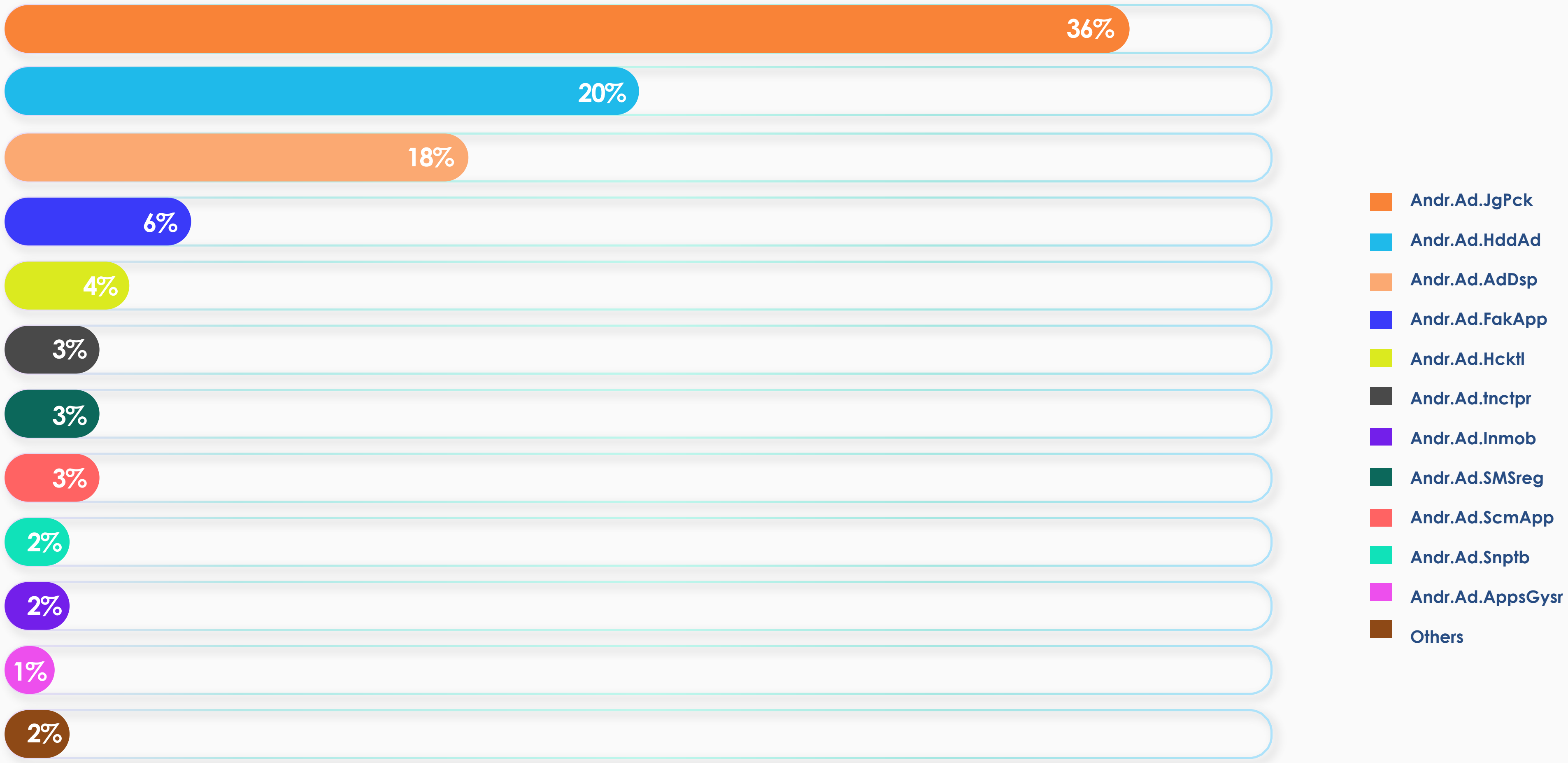
Most Prevalent Trojan Types



THE ADWARE SAGA

There have not been many changes in the adware space in the past few quarters. Andr.Ad.JgPck, Andr.Ad.HddAd, and Andr.Ad.AdDsp are the three families retaining the top spot, indicating that threat actors are prevalently launching several campaigns using these three adware families.

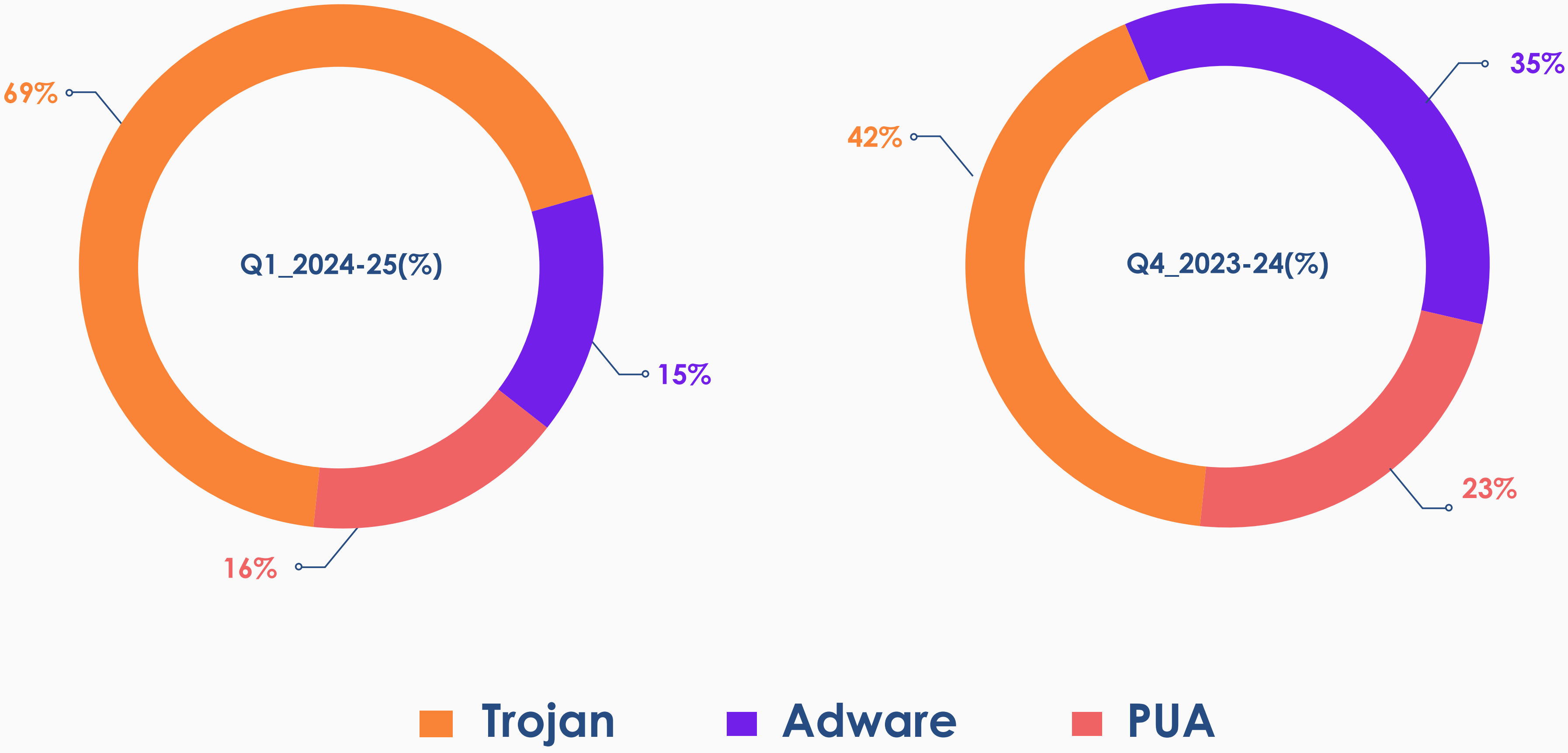
Trend Line Showing the Adware Plague



MAC THREAT LANDSCAPE

Threat actors are increasingly targeting macOS platform users due to their perceived affluence and the growing market share of Apple devices. These cybercriminals constantly evolve their tactics to exploit new vulnerabilities, making it challenging for users to stay protected. The surge in visibility of trojan attacks on macOS systems is because of sophisticated methods used that bypass traditional security measures.

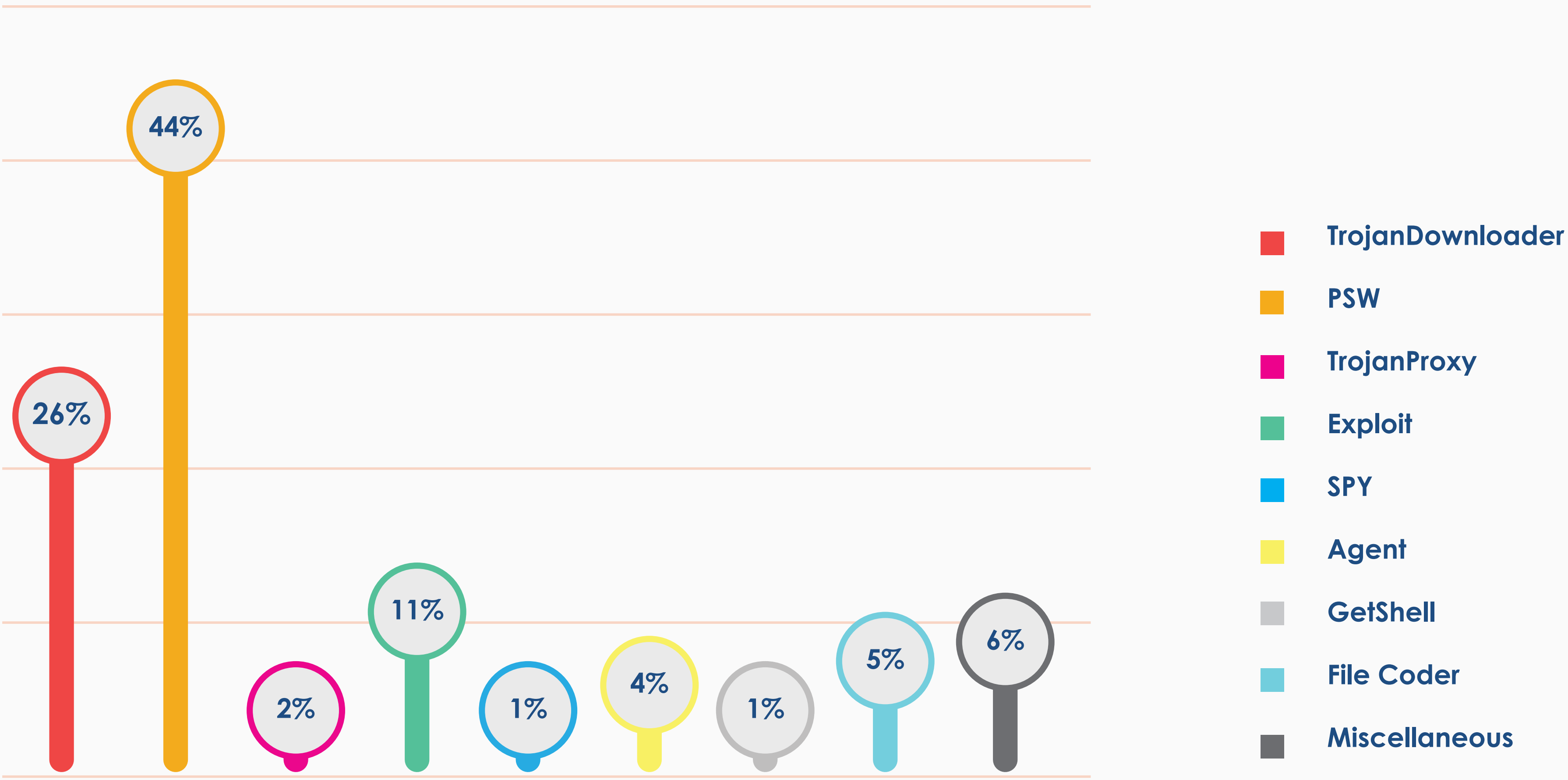
Trojan, Adware, and PUA Proportional Split



THE UBIQUITOUS TROJANS

Even though we saw a massive upsurge in the frequency of trojan attacks, the macOS space was riddled mainly with two trojan families—PSW and TrojanDownloader. The PSW family of trojans, an acronym for Password Stealing (mal)ware, focuses on silently retrieving user credentials, posing a grave threat to users' privacy and security.

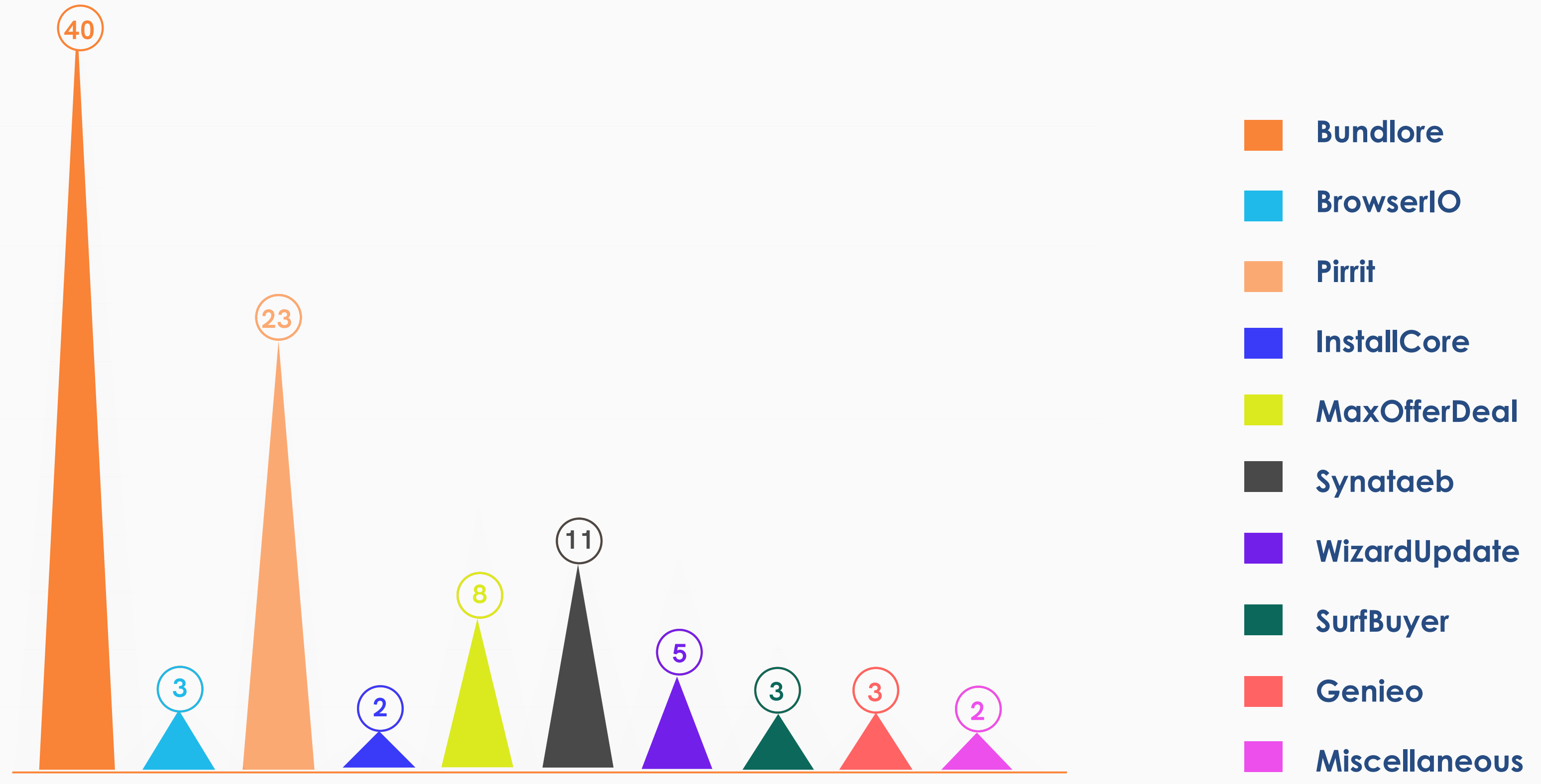
Trojan Detection Trend Line



THE ADWARE BROUHAHA

In the macOS threat landscape, the adware space was dominated by two prominent families: Bundlore and Pirrit, which accounted for over half of all adware attacks. These adware variants are notorious for their persistence and ability to evade detection, often bundling with legitimate software to infiltrate systems.

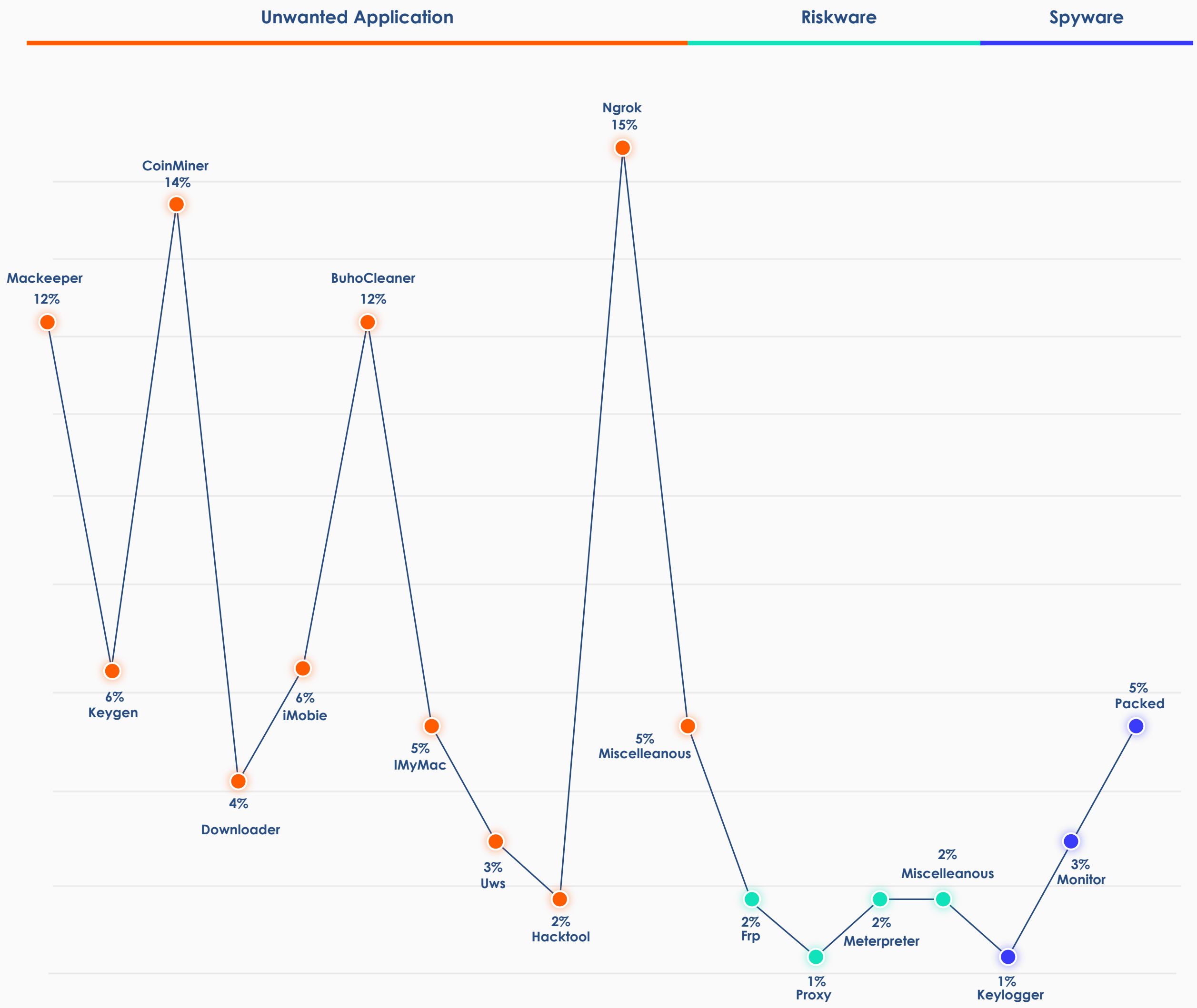
The Trend Line of Adware Variant Detections



A PINCH OF PUPS

Last quarter, Ngrok, Coinminer, and Mackeeper dominated the macOS Potentially Unwanted Programs (PUP) landscape. This prevalence is attributed to its aggressive marketing tactics and the blurring lines between utility and intrusion, making it a central figure in our analysis. Though Ngrok is claimed to be a secure remote access tool, it has also been seen to be misused by threat actors to bypass network protection and hence flagged by security products as unwanted application.

Most Prevalent PUP Types



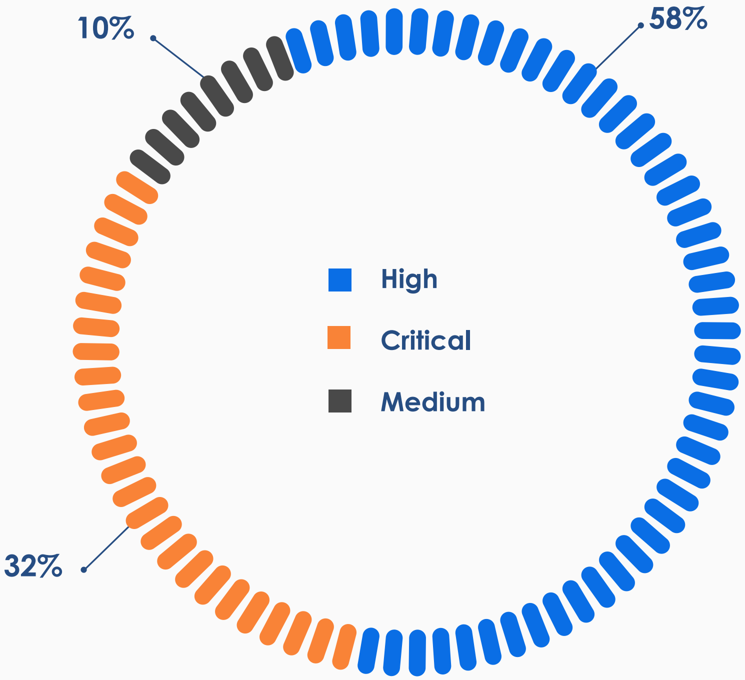
VULNERABILITIES THREAT LANDSCAPE

It is advisable for organizations to conduct regular vulnerability assessments to safeguard their network from data breaches and prevent any financial and reputational losses that can occur due to a successful exploitation. However, the time gap between identifying the vulnerability and fixing it, is being taken advantage of by the threat actors who exploit their network before the actual fix is rolled-out or the suggested patches are applied.

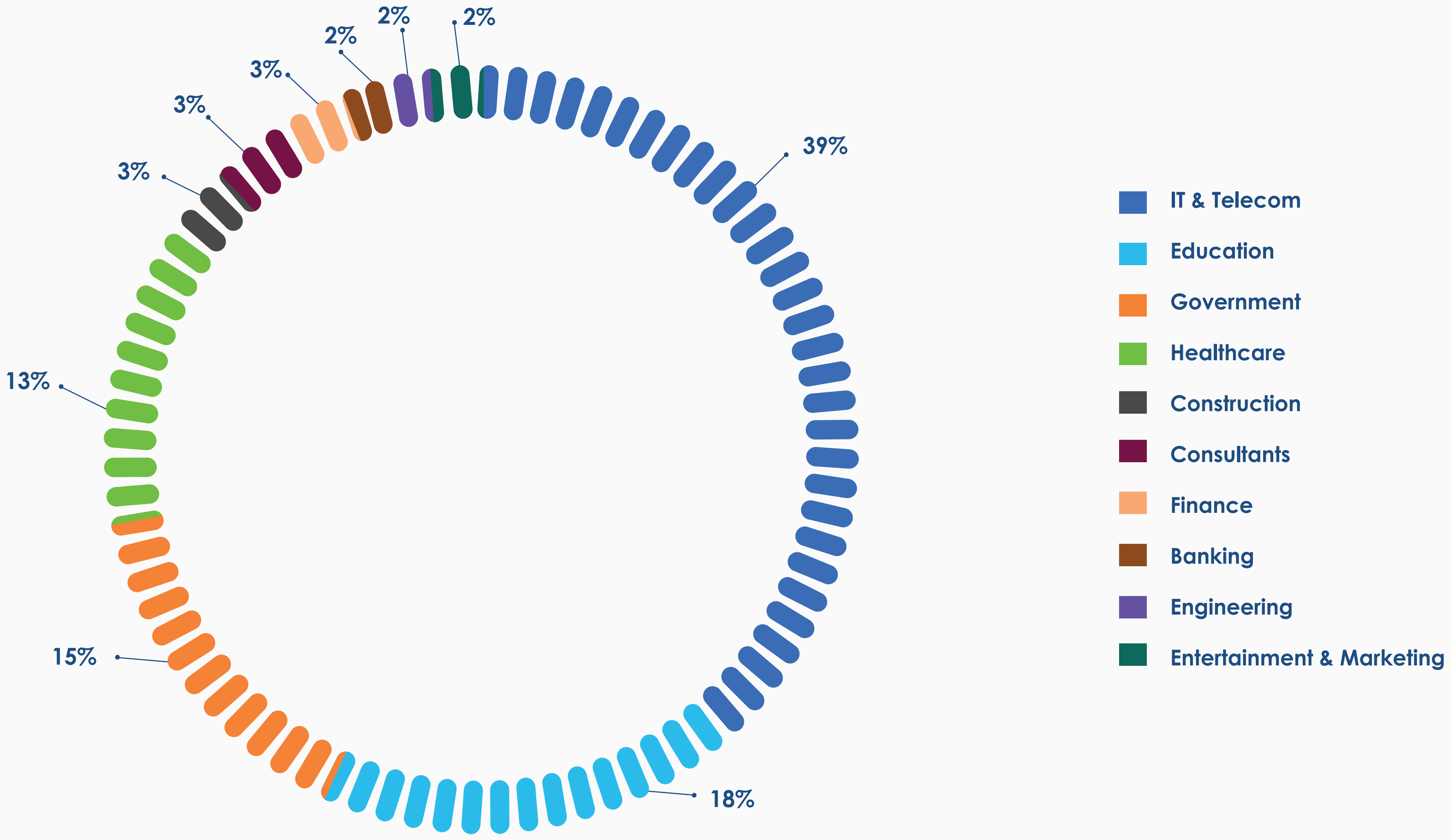
CVE Analysis

The vulnerabilities exploited in the wild have been categorized based on the impact it had on the environment, be it financial, reputational, or operational loss.

The pie chart offers a broad view of the vulnerability distribution as tracked by K7 Labs.



Most Exploited Industries



Most of the sectors are exploited using social engineering attacks such as phishing, or because of the large attack surface, as the potentially vulnerable points that have been exposed to the internet are usually not taken care of for a myriad of reasons like time, the budget allotted for cyberthreat management and some of the organizations believing their data may not be a target for threat actors, which is not the case, or just sheer negligence, resulting in a data breach.

SIGNIFICANT VULNERABILITIES FOR THE QUARTER

Listed below are a few of the vulnerabilities from last quarter that have been exploited and deserve attention.

Chrome's Sandbox Vulnerability

A remote code execution (RCE) vulnerability, CVE-2024-5274, in Google Chrome's sandbox allows threat actors to craft an HTML page to exploit it due to a type confusion issue in its V8 JavaScript engine.

Vulnerable Products:

- Google Chrome versions below 125.0.6422.112

Linux Kernel's Privilege Vulnerability

CVE-2024-1086, a use-after-free vulnerability in the Linux Kernel's netfilter: nf_tables component allows a threat actor with basic access to escalate their privileges to root, compromising system security.

Vulnerable Products:

- Linux Kernel 3.15 to 6.1.76
- Linux Kernel 6.2 to 6.6.15
- Linux Kernel 6.7 to 6.7.3

Bypass Vulnerability in Microsoft's Products

CVE-2024-30040, a security feature bypass vulnerability in Microsoft 365 and Microsoft Office's MSHTML platform, allows threat actors to execute arbitrary code if they can convince the user to open a malicious file. This bypasses Object Linking and Embedding (OLE) mitigations designed to protect users from malicious files.

Vulnerable Products:

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems

PAN-OS Vulnerable to Attacks

CVE-2024-3400, a command injection vulnerability in Palo Alto Networks' PAN-OS software, allows unauthenticated remote code execution. Threat actors gain root privileges by exploiting the curl command used in its telemetry functionality, enabling them to inject shell commands via HTTP POST requests by manipulating the SESSID cookie parameter.

Vulnerable Products:

- Palo Alto Networks PAN-OS 10.2.0 - 10.2.9
- Palo Alto Networks PAN-OS 11.0.0 - 10.0.4
- Palo Alto Networks PAN-OS 11.1.0 - 11.1.2

Threat Actors gain access to NAS Devices

CVE-2024-3273 is a vulnerability due to a backdoor account having hard coded credentials leading to command injection in multiple D-Link Network Attached Storage (NAS) devices' HTTP GET Request Handler. This allows a remote threat actor to execute arbitrary commands, potentially leading to unauthorized access to sensitive information, modification of system configurations, or denial of service conditions.

Vulnerable Products:

- DNS-320L Version 1.11, Version 1.03.0904.2013, Version 1.01.0702.2013,,
- DNS-325 Version 1.01
- DNS-327L Version 1.09, Version 1.00.0409.2013
- DNS-340L Version 1.08

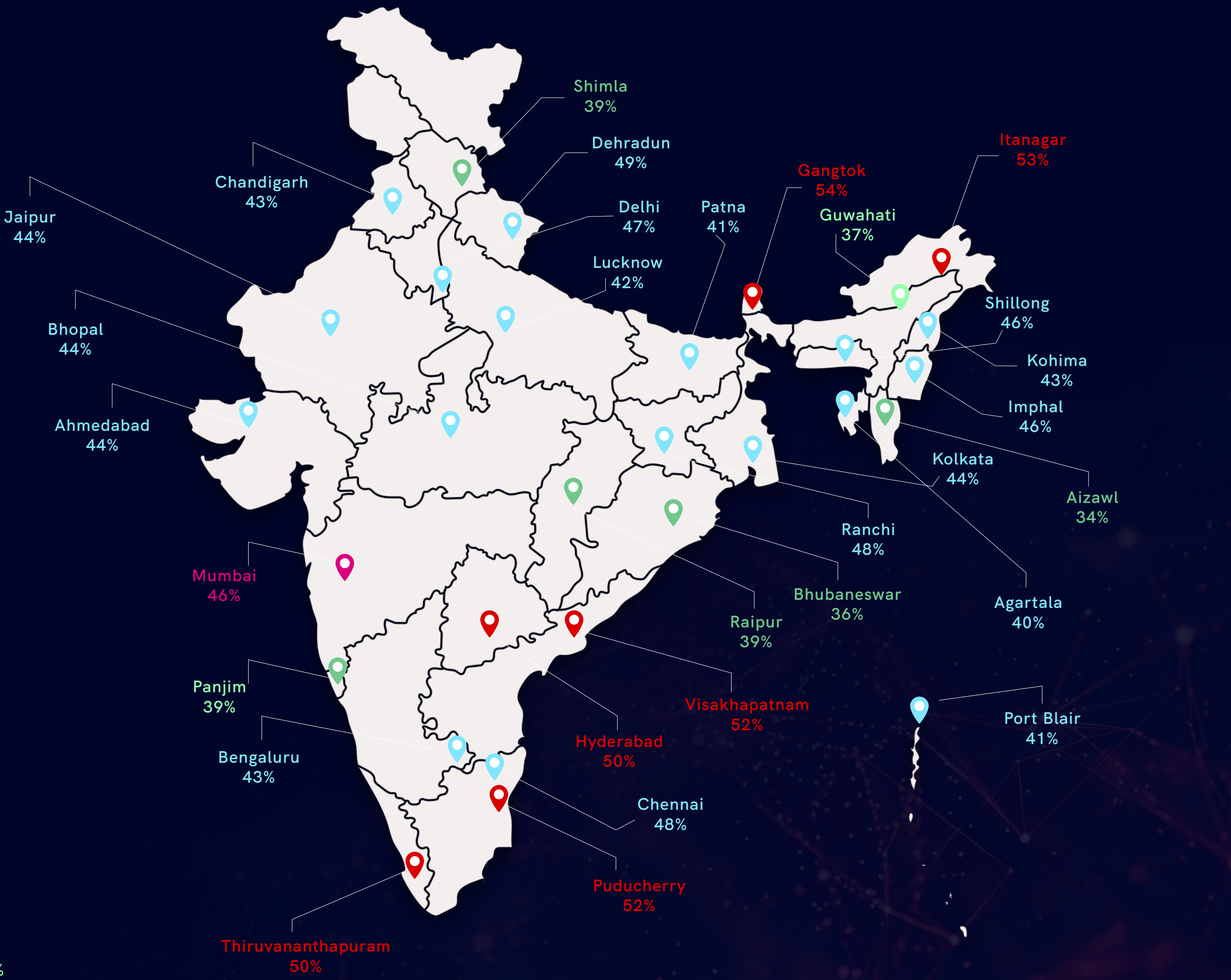
Vulnerability in Apple's OS

A memory corruption vulnerability, CVE-2024-23225, in the iOS kernel, allows attackers to bypass kernel memory protections.

Vulnerable Products:

- iPadOS before 16.7.6
- iPadOS 17.0 - 17.4
- iPhoneOS before 16.7.6
- iPadOS 17.0 - 17.4
- macOS 12.0 - 12.7.4
- macOS 13.0 - 13.6.5
- macOS 14.0 - 14.4
- tvOS before 17.4
- visionOS before 1.1
- watchOS before 10.4W

CYBER THREAT LANDSCAPE - INDIA



🟢 30%- 39%

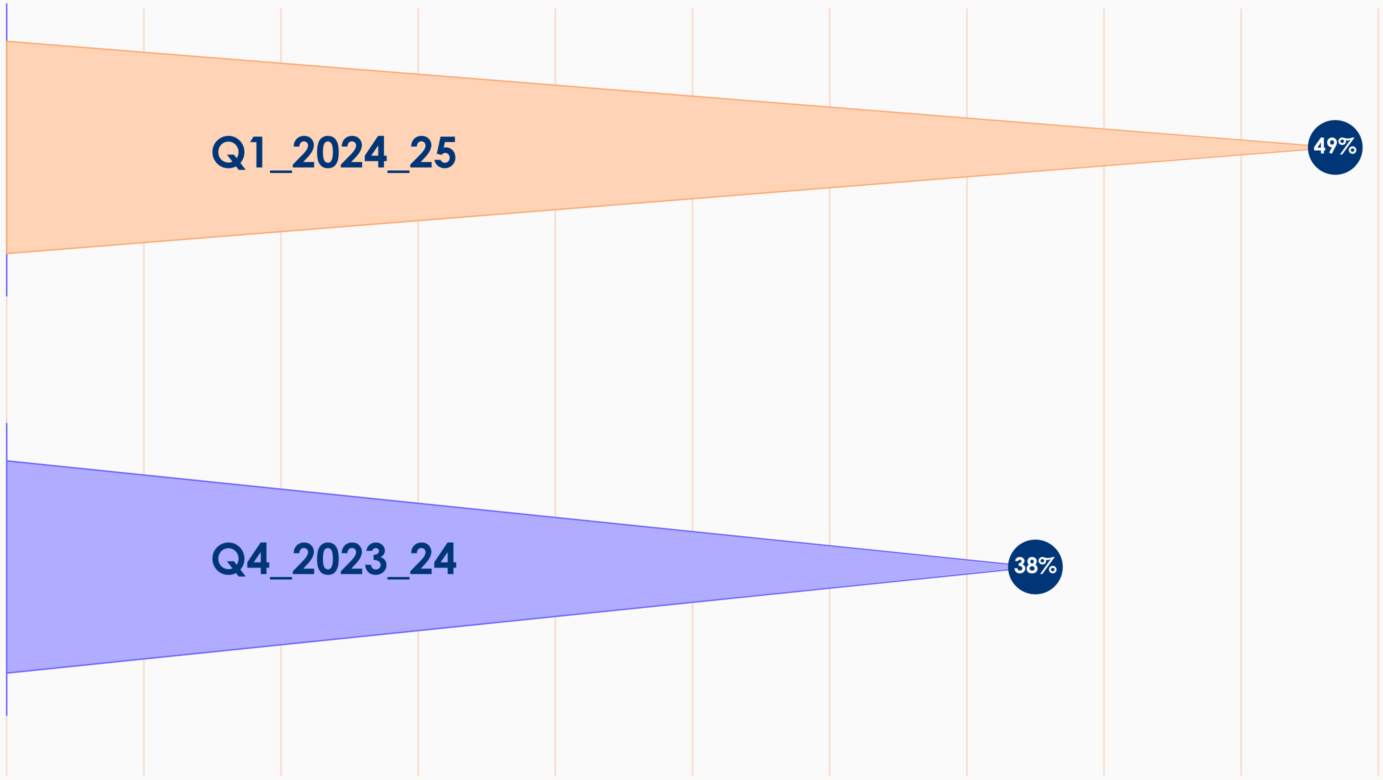
🔵 40%- 49%

🔴 50%- 59%

Map for illustrative purposes only. Not to scale.

THE QUARTERLY TRENDS AND STATISTICS

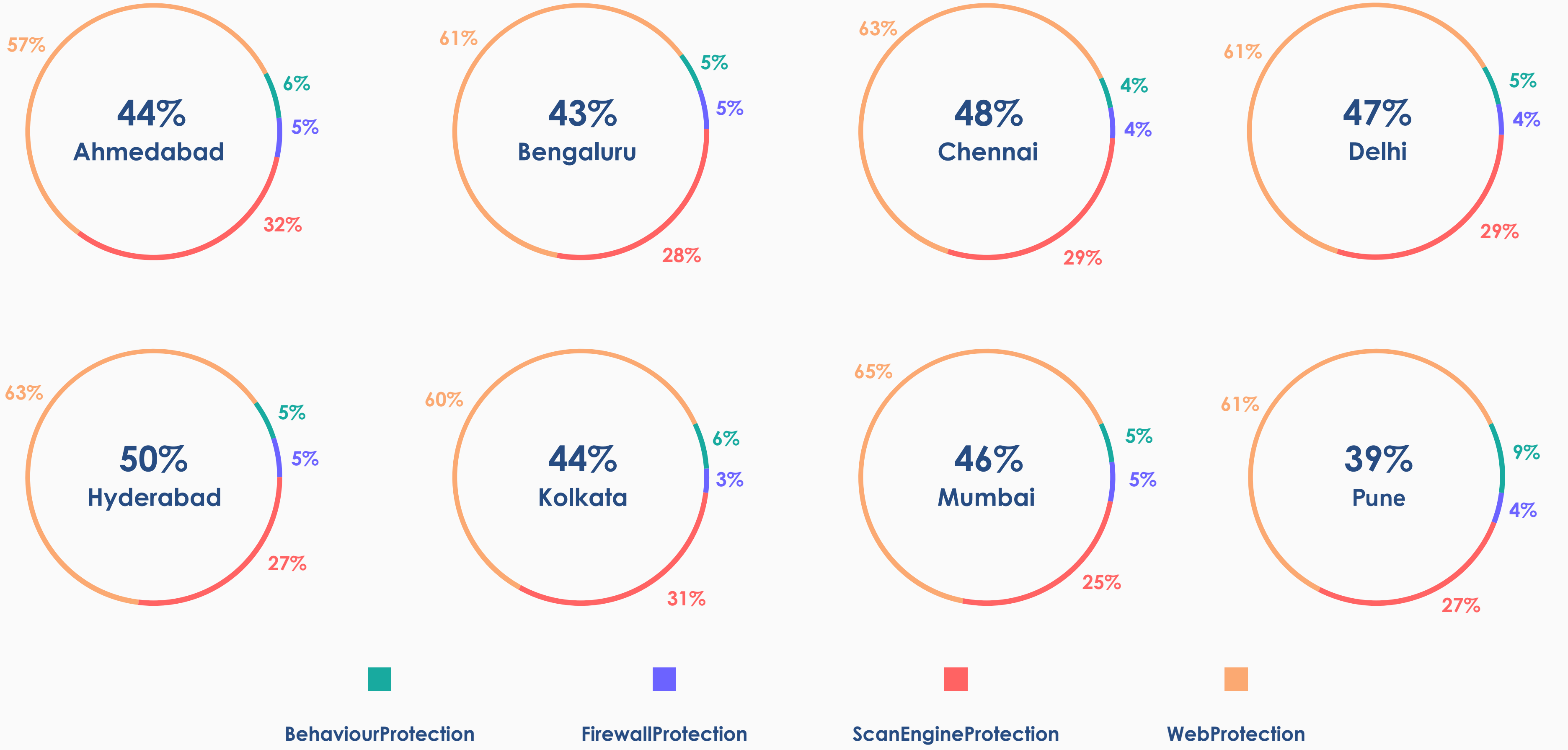
The Overall Pan-India IR in comparison with the previous quarter is given below



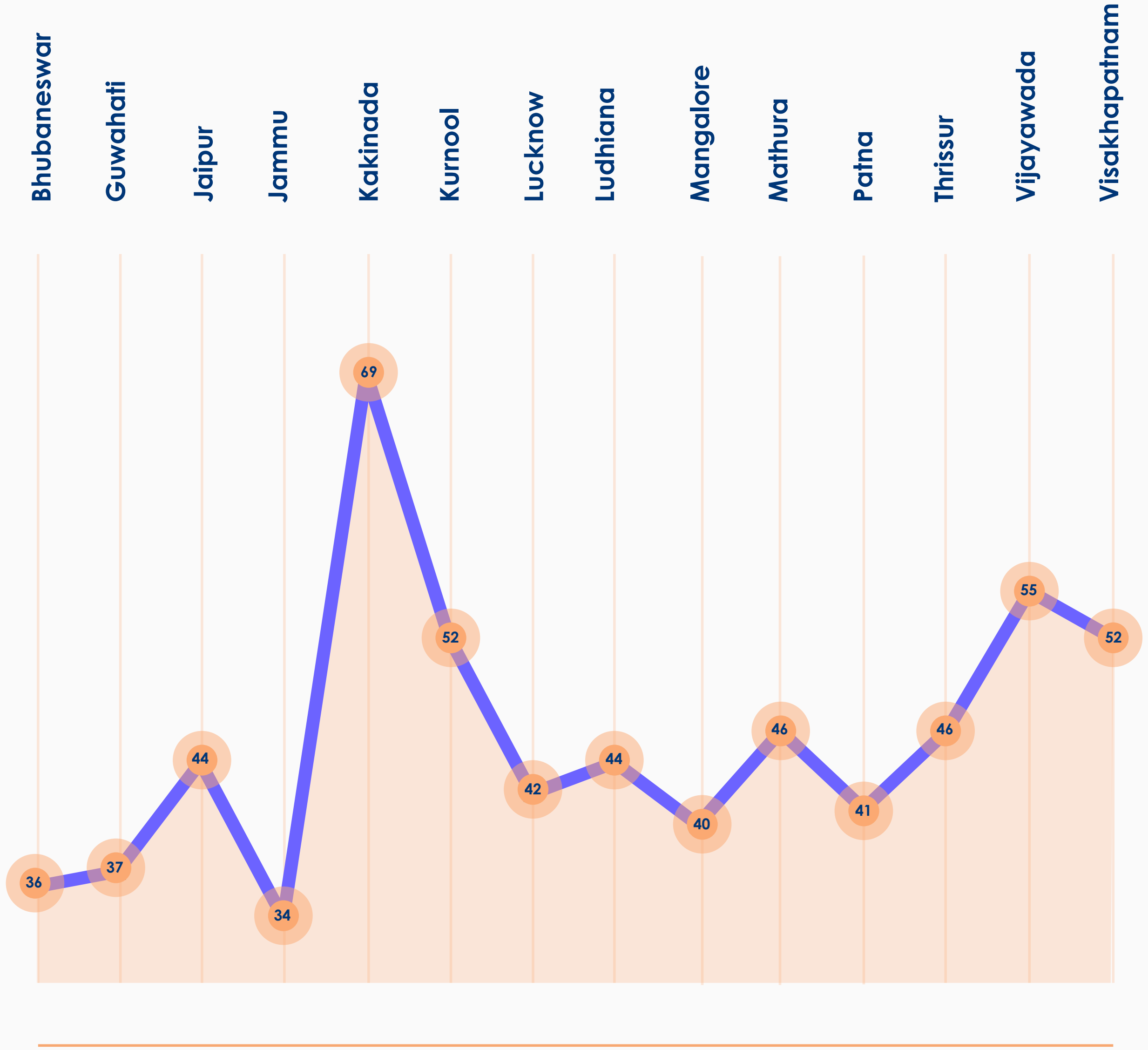
We now present a few significant IRs across metros classified based on the layer where the threats were actually blocked.

Back To Contents

THE METRO AND TIER-1 CITIES - INFECTION RATE



TOP INFECTION RATES IN TIER-2 CITIES

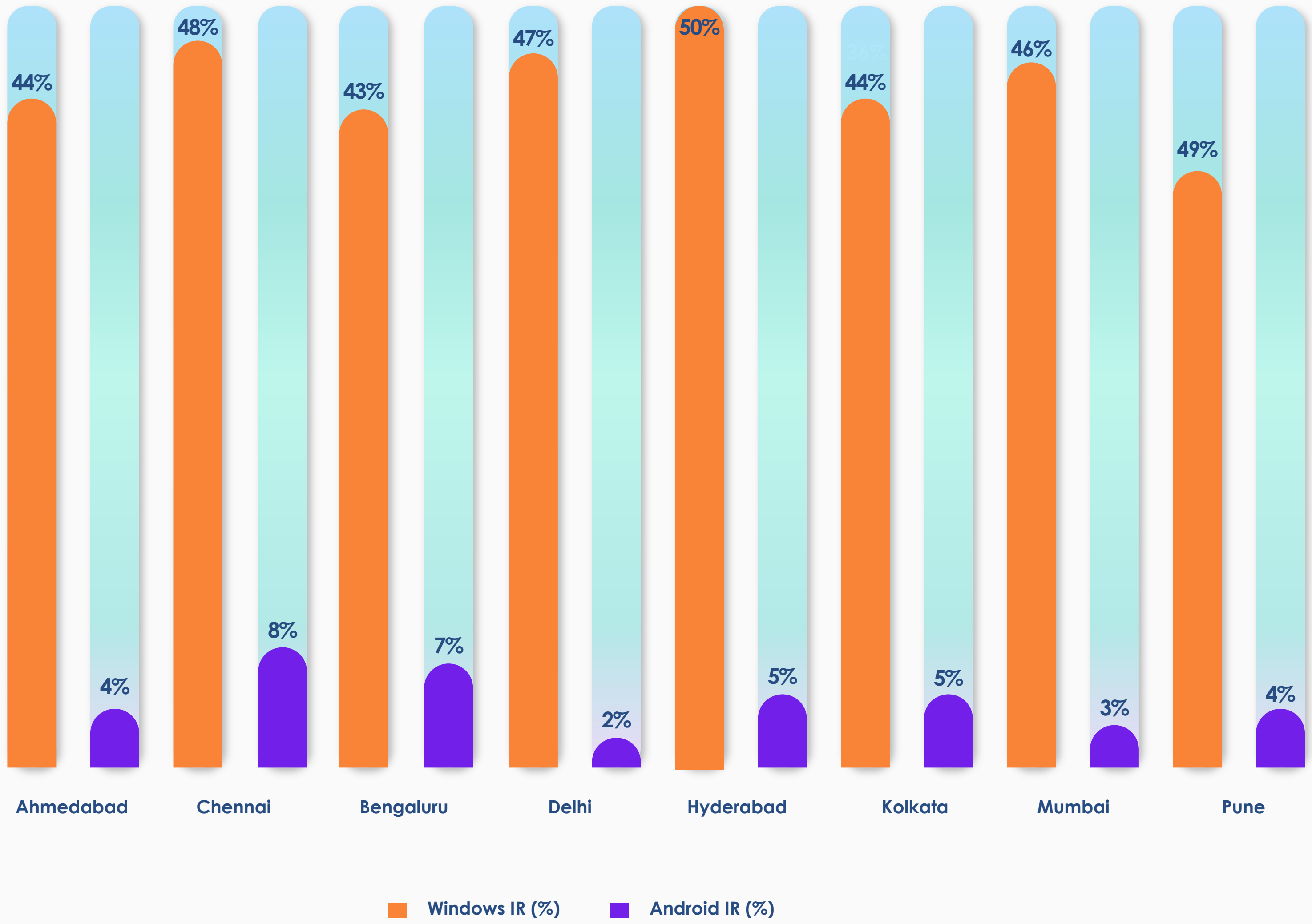


Tier-2 cities, once considered less lucrative targets, are increasingly attractive to cybercriminals due to their expanding digital footprint, inadequate knowledge of cyber hygiene, and potential for cascading disruptions.

INFECTION RATE COMPARISON ACROSS PLATFORMS

Despite the widespread use of Windows, an increasing number of users are turning to Android devices for their daily activities. While Android threats are on the rise, Windows' massive installed base and legacy vulnerabilities continue to make it a prime target for cybercriminals.

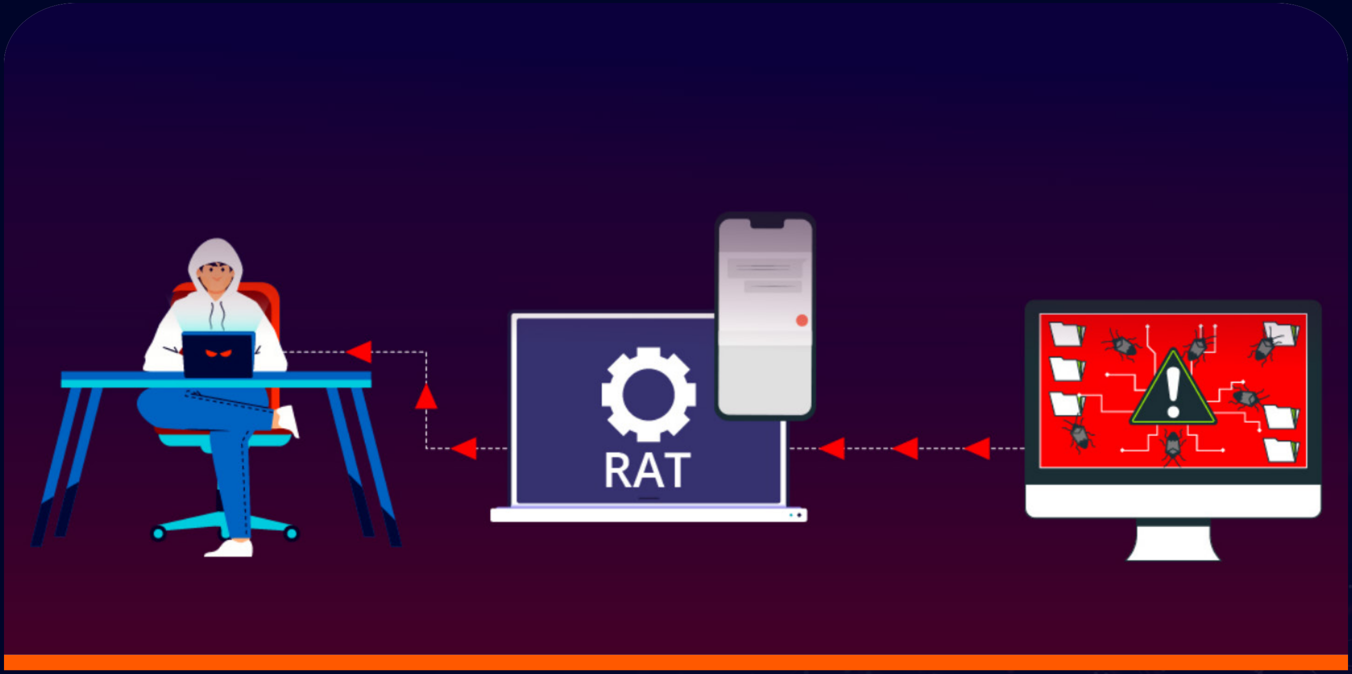
Windows IR vs Android IR



LATEST SECURITY NEWS

This section lists the latest happenings in the cyber world. For more details, please read our blogs on the same.

SpyMax – A Bane for Telegram Users



SpyMax, a spyware, steals Personal Identifiable Information (PII) and other sensitive data from an user and sends the same to a remote attacker. A phishing campaign was seen to specifically target Telegram users.

For More details refer "SpyMax – An Android RAT targets Telegram Users"

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

OUR VERDICT

The first quarter of FY 2024-25 has seen a concerning downturn in the fight against increasing cyber threats, highlighting the pervasive nature of the threat landscape and the urgent need for enhanced cybersecurity measures across sectors.

Today's cyber threats go beyond traditional IT and cybersecurity boundaries, impacting society, politics, economics, and geopolitics. Ransomware, phishing, and exploiting vulnerabilities are wreaking havoc across various sectors. Ransomware attacks are incredibly destructive, paralyzing entire networks and demanding enormous ransoms for service restoration. Phishing attacks are becoming more sophisticated, fooling even the most cautious users and resulting in significant data breaches and financial losses.

The most important step that an organization can take to protect themselves, their customers, and vendors is to protect their networks and data. Securing their networks with proper firewalls and using strong passwords is one major step that should be taken for their data security.

As cyber threats continue to evolve in numbers and sophistication, apart from implementing a zero-trust security framework, protecting your customers and vendors, taking a backup of sensitive data, and reducing your attack surface, the need of the hour is cyber awareness and making cybersecurity a national priority.

Organizations are thereby requested to conduct regular risk assessments to evaluate any potential vulnerabilities in their network, policies, procedures and technologies and get them fixed at the earliest before possible exploitation by the threat actors.

Organizations are also requested to implement proper cyber hygiene practices and follow them strictly for a safe digital experience.

Back To Contents

ABOUT US

K7 Computing is one of the earliest and most accomplished cyber security companies protecting more than 25 million clients worldwide against threats to their IT environment. Backed by more than 30 years of cybersecurity expertise. K7 Security offers best-in-class solutions & products.

K7 Labs is a leader in threat research, threat intelligence and in enforcing and applying excellent standards in cyber security. With a wide range of expertise across the Lab, you can be rest assured that you are in safe hands if you have chosen our K7 Security Product.

COVERING ENTERPRISE NEEDS WITH K7 ENDPOINT SECURITY (K7 EPS)

K7 Endpoint Security (K7 EPS) provides cost effective anti-malware capabilities for enterprises without the high purchase price, complex deployment models, or expensive renewal and maintenance costs found in other vendor solutions. Highly scalable, K7 EPS offers quick deployment and granular and centralised control over applications, devices, and networks.

K7 EPS anticipates, detects, and blocks cyberthreats, ensuring uninterrupted operations and protecting confidential business information. Designed to satisfy the needs of the modern enterprise, K7 EPS scales to protect any size of business operations and does not need an extensive in-house IT team for deployment or management.

Our in-house K7 Cerebro Engine is an ultrafast and scalable scanning engine which is capable of detecting not only existing threats but also emerging threats by using artificial intelligence and machine learning. Its proactive approach can detect and prevent the most advanced attacks, ensuring protection from zero-day attacks.

Back To Contents

CYBER THREAT MONITOR REPORT

Q1_2024-25

K7 SECURITY

www.k7computing.com