K7 SECURITY

Cyber Threat Monitor Report

Q3_2021-22

www.k7computing.com

Contents

Unravelling the Indian Cybersecurity Scenario

Digitalization comes with its own set of advantages and disadvantages. People are now more connected than ever before. However, threat actors try to find loopholes in the software being used by the organizations and individuals. Technology head honchos are also hinting at taking our daily lives to the metaverse where you could even get married virtually.

Threat actors are taking advantage of this increase in users' adoption of technology and are bolstering their arsenal with new and repurposed malware, social engineering, obfuscation and evasion techniques to hit the targets at an astounding rate.

The scenario is even more complex for the high-profile and high net-worth organizations and individuals who are specifically earmarked by the threat actors for churning out more money through a single attack.

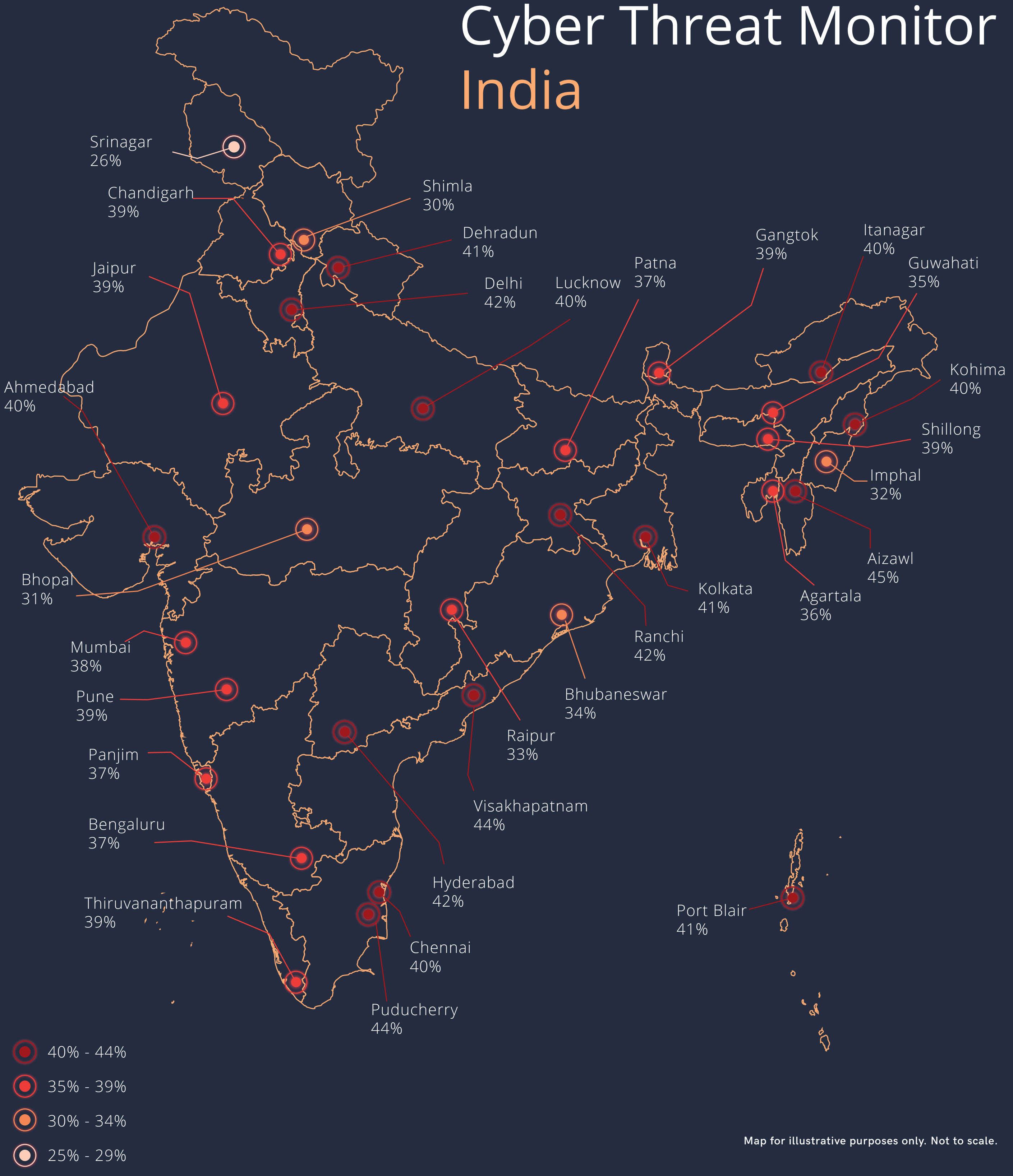
At such an alarming time, we should understand the necessity to safeguard our digital activities and assets from prying eyes and probing fingers. And owning or buying appropriate devices and solutions form just one part of the initiative to stay strong against cybercriminals. Also, one can ensure to follow some safety precautions such as ensuring to keep your devices and security applications updated and learning how to avoid social engineering, spoofed websites and phishing tricks, among other forms of internet trickery.

By being part of a cybersecurity company that protects organizations and individuals globally, K7 Labs researchers hold the best perspective to observe the threat landscape.

The latest K7 Cyber Threat Monitor report offers a snapshot of the critical analysis of all the prevalent cyber-attack techniques and trends. The actionable threat landscape report also includes the required cyber hygiene practices you should embrace to stay safe and protected.

We would appreciate you sharing this report among your colleagues and folks to raise awareness of the prevalence of cyber threats, thus helping to make the digital world a safer place!

Cyber Threat Monitor India



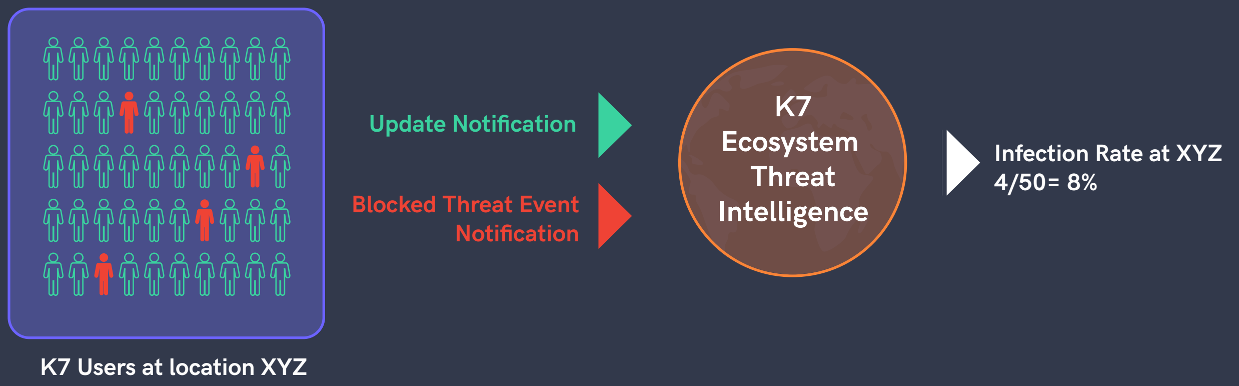
Map for illustrative purposes only. Not to scale.

Regional Infection Profile

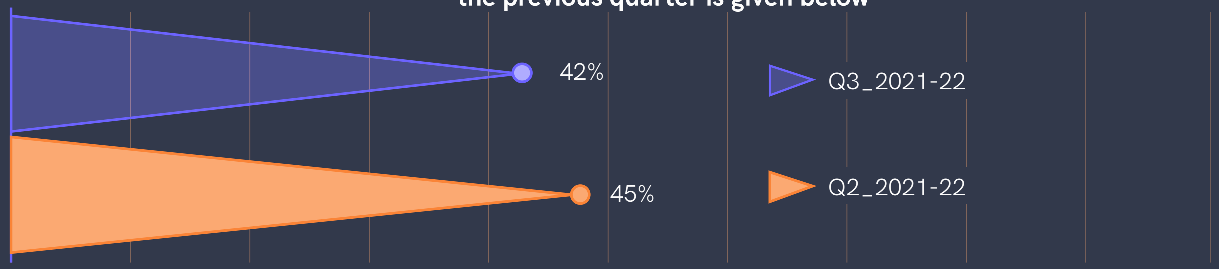
Over the past 31 years, K7 Computing has safeguarded hundreds of enterprises across sizes and end-users by delivering state-of-the-art cyber threat detection and mitigation solutions. K7 telemetry collects hundreds of terabytes of data and is scrutinised by our skilled threat researchers at K7 Labs. The K7 Cyber Threat Monitor report offers an analytical rundown observed during Q3_2021-22.

To better understand the present condition of the domestic threat landscape, we have designed a concept called Infection Rate (IR). The idea is picturised as follows.

Infection Rate (IR) of an area

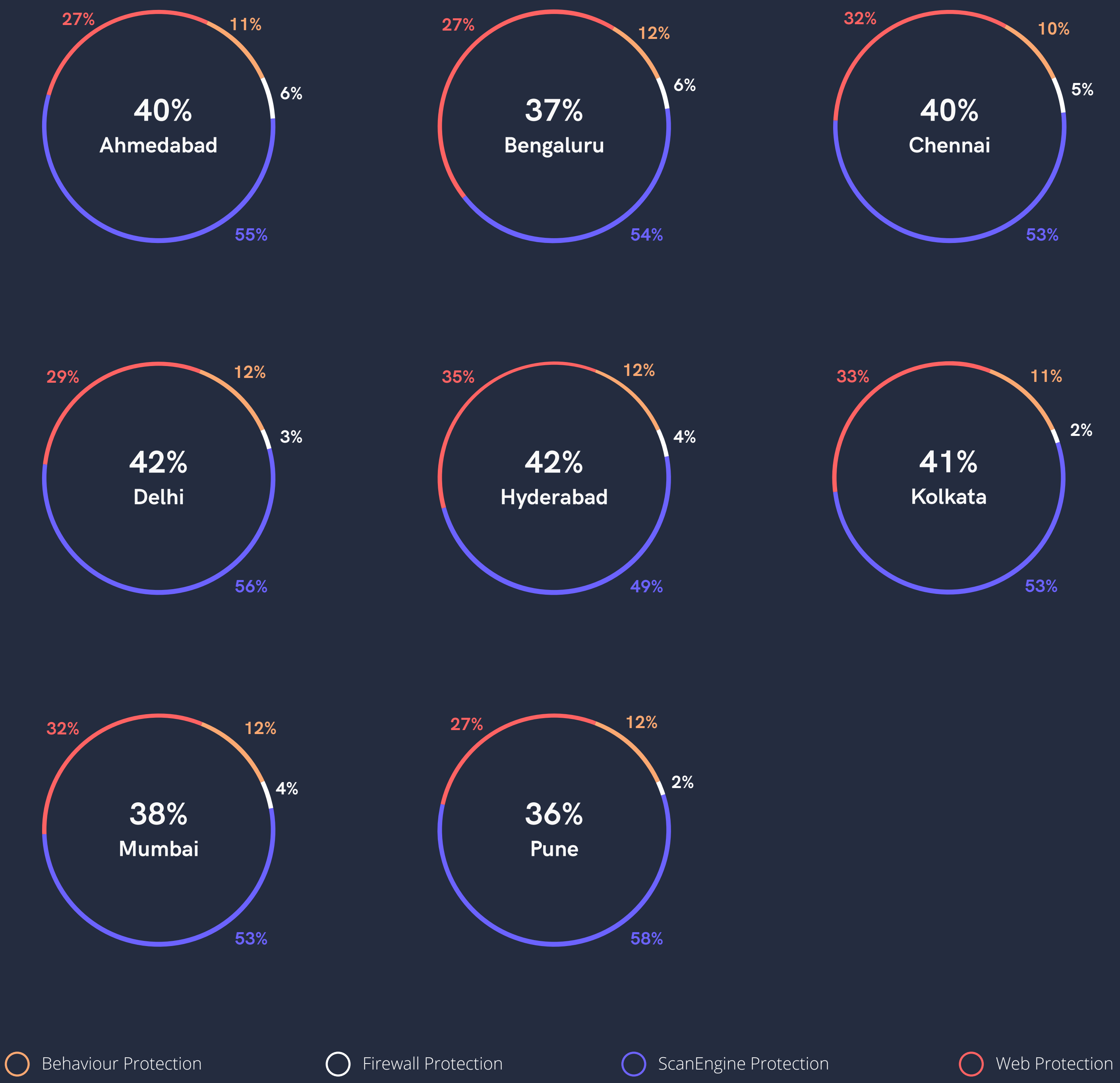

Update Notification
Blocked Threat Event Notification
K7 Ecosystem Threat Intelligence
Infection Rate at XYZ 4/50= 8%
K7 Users at location XYZ

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



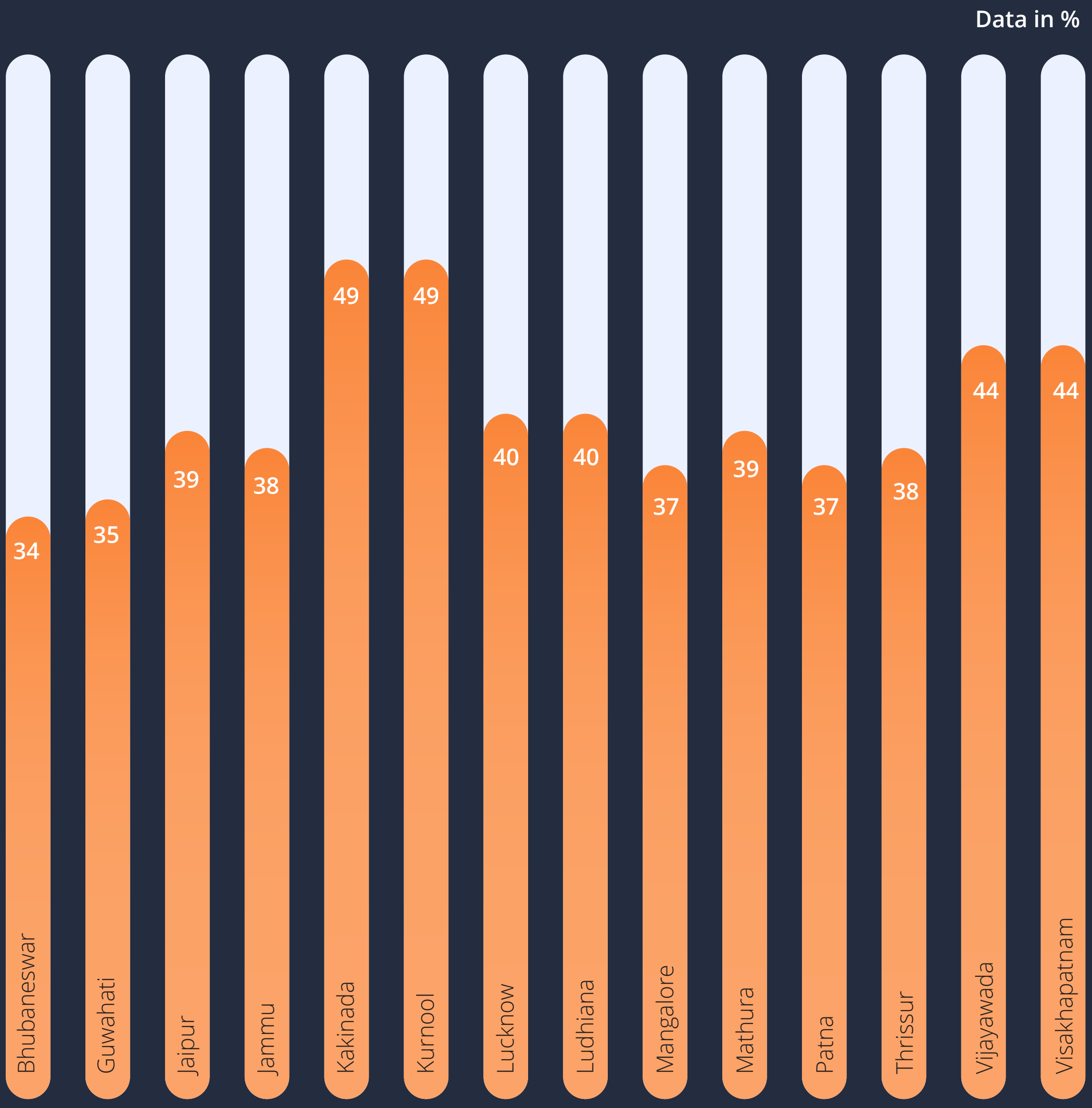
Though the infection rate has reduced compared to the previous quarter, a plethora of new threats alongside old threats behind the cloak of new ones has surfaced across platforms. And the steady escalation can be overviewed on the state capitals, Tier-1 and Tier-2 cities charts.

The Metros and Tier - 1 Cities - Infection Rate



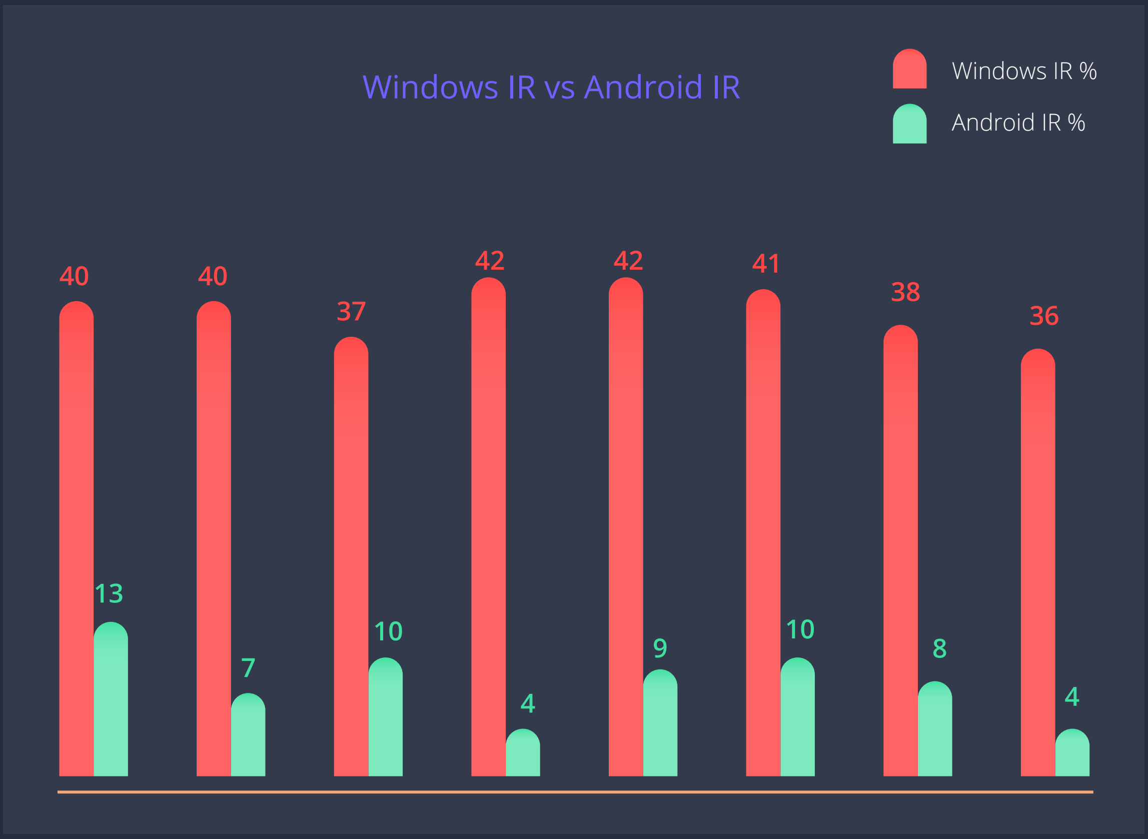
The thwarted attacks observed on the Tier-2 cities shows the increasing menace of the adversaries across all places

Top 14 Infection Rates in Tier - 2 Cities



Infection Rate Comparison Across Platforms

Besides the enormous growth of malware targeting the Windows operating system across enterprises and among end-users, the Android threat landscape is also swelling rapidly in both volume and complexity. Moreover, the threat actors are adopting new obfuscation and distribution methods to build malware for myriad reasons. And the massive surge is reflected in our telemetry too.



Stemming from the statistics, we can glean the steady rise of Android malware in tandem with their Windows brothers. Besides tricking the victims via camouflaged apps triggered through the third-party app stores and often even Google Play, the threat actors actively execute phishing email distribution and SMiShing campaigns to hunt down more victims. And with the growing number of smartphone users and crypto investors in and around the country, the activities could heighten further in the near future.

Back to contents

Enterprise Insecurity

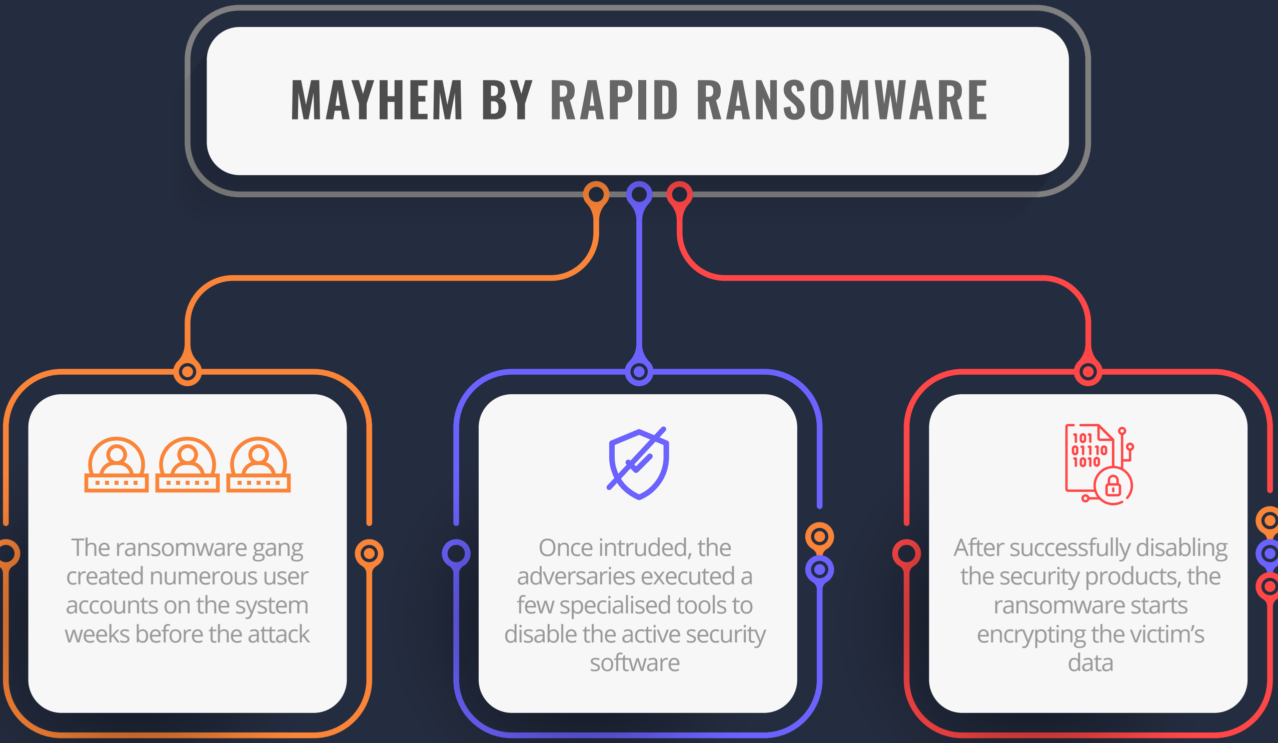
As the year 2021 has come to a close, we can glean that the cyber threat landscape has been plagued by increasing chaos and disruption. Alongside other existing threats, ransomware has been seen to be relentlessly on the rise. Furthermore, the increasing dependence on portable devices such as smartphones and the Internet of things (IoT) makes the scenario even more complex as users are not adopting the necessary security measures, thus making themselves susceptible to attack.

Case Study: Mayhem by Rapid Ransomware

During the period, one of our enterprise customers reported a ransomware attack on their network. We found that the ransomware variant "**Rapid**" encrypted all their network storage drives when their systems were accessed remotely. To intrude and compromise the system, the ransomware gang executed some intriguing steps.

The initial vector was brute force by the threat actors, on the organization's servers having public IP, with different usernames and passwords. After gaining access, the username and passwords were changed.

Here is how the attack unfolds-



The ransomware gang created numerous user accounts on the system weeks before the attack

Once intruded, the adversaries executed a few specialised tools to disable the active security software

After successfully disabling the security products, the ransomware starts encrypting the victim's data

Safety Recommendations

- Secure your devices by keeping them up-to-date, patched against the latest vulnerabilities, and protected by up-to-date, high-quality security software such as K7 Endpoint Security
- Frequently audit user accounts and their permission levels. Set alerts on any unauthorized user accounts created
- Change the password on default accounts

Vulnerabilities Galore

Finding out security holes in operating systems, firmware, software libraries, APIs, and application software has become commonplace nowadays. Happily, most software providers roll out immediate patches to promptly control the damage. But many times, it becomes too little too late for many users out there because of ignorance or other reasons. The timeframe between the vulnerability discovery and patching is sufficient for threat actors to exploit the same.

This quarter too had its own share of significant vulnerabilities which have been detailed below.

Vulnerability in Java-based logging library

CVE-2021-44228, is a vulnerability in Log4j, a popular Java-based logging library, which is a part of Apache logging services. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

Vulnerable versions are Log4j <= 2.16.0

PAN Buffer Overflow Vulnerability

CVE 2021-3064, a buffer overflow vulnerability, was identified in a security appliance from Palo Alto Networks (PAN). This vulnerability has a working exploit which on execution against vulnerable devices could lead to unauthenticated Remote Code Execution on the devices.

Vulnerable versions are PAN-OS 8.1 prior to 8.1.17.

Windows Installer elevation-of-privilege vulnerability

CVE-2021-41379 is a Windows Installer elevation-of-privilege vulnerability which was patched during the November Patch. However, a bypass to the patch was identified which on exploitation results in elevation of privilege from a regular user to system administrator. This vulnerability is actively being exploited in the wild.

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

Use-After-Free Vulnerability in Chrome

CVE=2021-4102 is a high severity vulnerability in Chrome being actively exploited in the wild. This is a use-after-free vulnerability that on exploitation can result in corruption of valid data or even remote code execution on the victim's device.

Vulnerable versions are Chrome prior to v96.0.4664.110 and Microsoft Edge (Chromium based) prior to v96.0.1054.57.

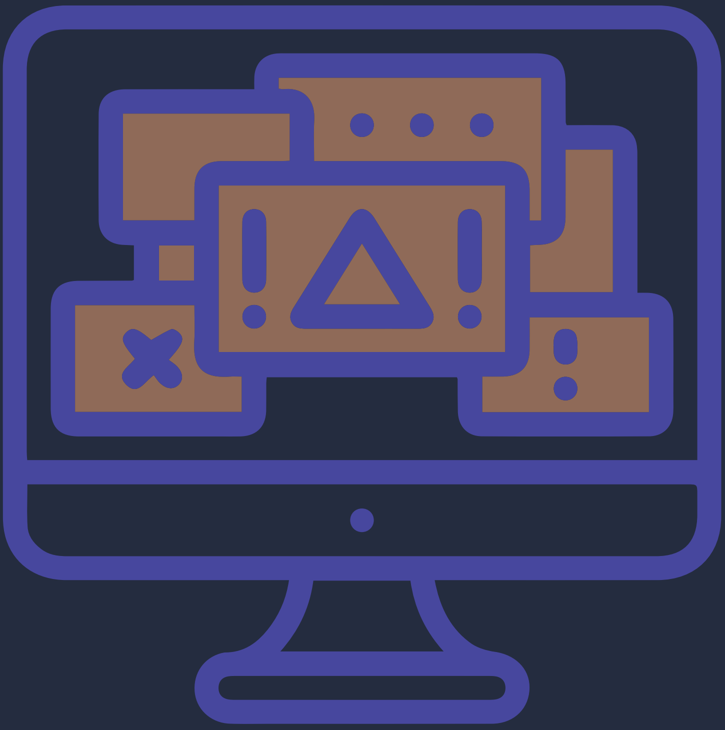
Active Directory Domain Services Elevation of Privilege Vulnerability

CVE-2021-42278, a vulnerability in Active Directory with which an attacker can tamper with the SAM Account Name. On successful exploitation an attacker can spoof the SAM Account Name.

CVE-2021-42287 is also a vulnerability in Active Directory with which an attacker can impersonate a domain controller.

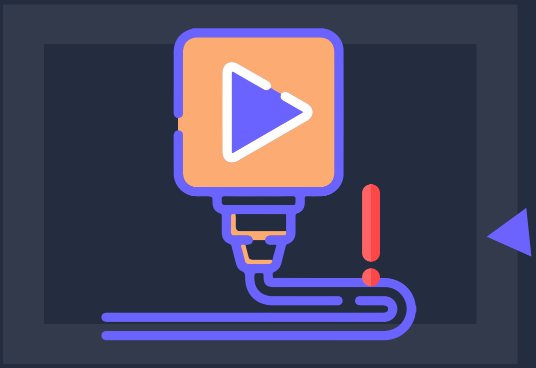
Vulnerable versions are Windows Server 2004, 2008, 2012, 2016, 20H2, 2019, 2022

Chaining these two vulnerabilities, an attacker can elevate privileges to domain admin. These are being exploited in the wild.



Back to contents

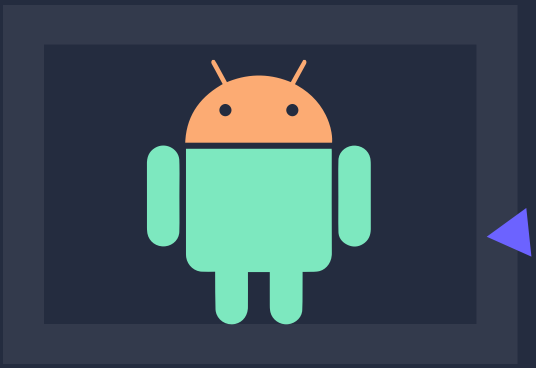
Danger in the Internet of Things



SOHO Universal Plug-and-Play Vulnerability

CVE-2021-34991 is a vulnerability in Netgear's Small Offices/Home Offices (SOHO) routers which leads to unauthenticated RCE. This is a buffer overflow vulnerability present in the Universal Plug-and-Play (UPnP) upnpd daemon of the router.

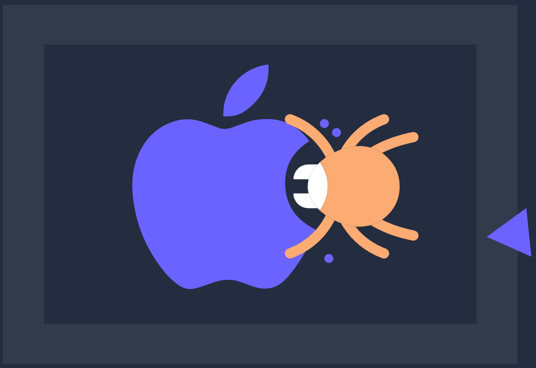
Affected devices are AC1450 - 1.0.0.36, D6400 - 1.0.0.104 and many more Netgear devices that are running the vulnerable UPnP daemon.



Use-After-Free Vulnerability in Android

CVE-2021-1048 is a use-after-free (UAF) vulnerability in the Android Kernel which on exploitation allows privilege escalation on the victims' devices. This vulnerability is currently being exploited in the wild.

Android devices having security patch level 2021-11-06 or lower are affected.



Kernel Level Vulnerability in iOS

CVE-2021-30955 is a kernel-level vulnerability in iOS, which on exploitation can execute arbitrary code with kernel privileges. This vulnerability is due to a race condition bug.

Vulnerable version is iOS 15.2.

Mitigation Techniques

- Using firewalls and IDS/IPS devices to allow only whitelisted connections and traffic
- Segment networks to ensure traffic flows only where it's required.
- Configure OT devices to restrict use of default ports and credentials

Windows Under Siege

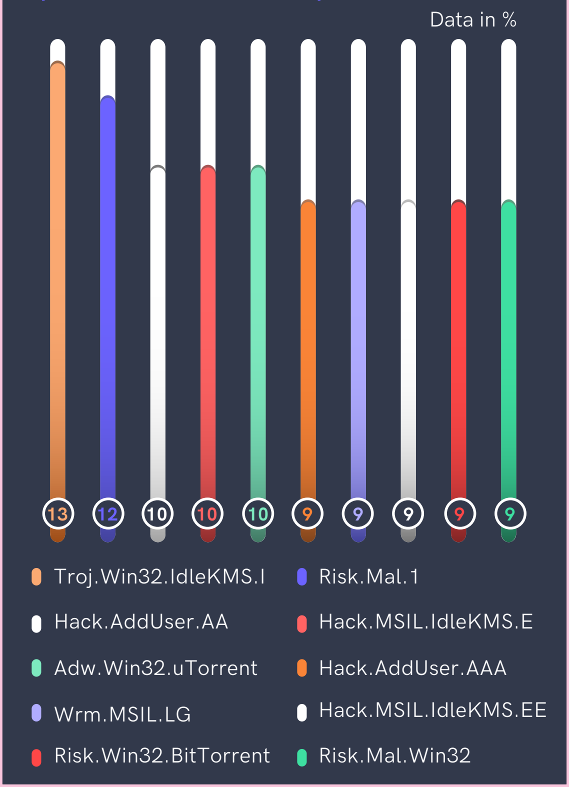
Windows Malware Type Breakdown

Being the most popular operating system on earth, the Windows platform encounters the newest and most sophisticated threats. Moreover, the rapid digitisation across enterprises has encouraged the threat actors further to heighten their menace. Besides developing new malware variants, the baddies put similar efforts to repurpose, refine, and build innovative tools and ways to bypass security gateways and unleash further attacks. Here's how they impacted our periodical Windows telemetry.

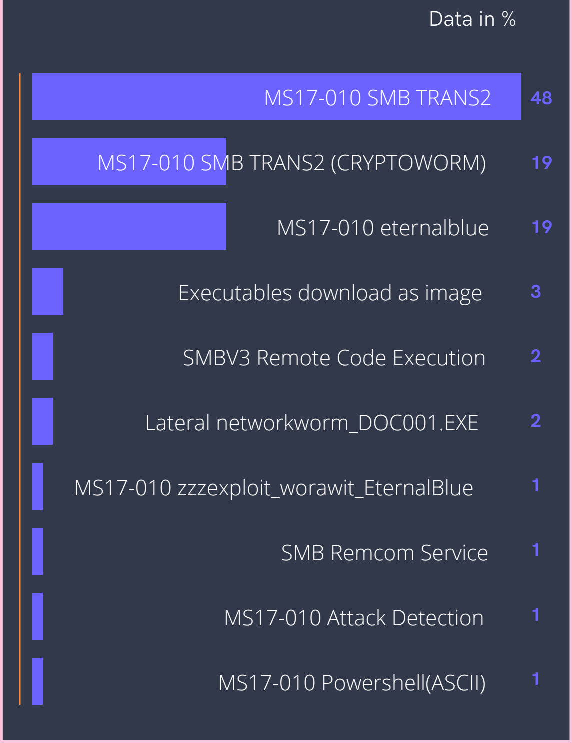
Windows Exploits

Vulnerabilities are a prime concern for all software developers as their software can be easily exploited thereby causing monetary and reputation loss. However, despite releasing patches and regular warnings by the developers and security platforms, users often ignore the necessity to get safeguarded. So let's take a look at how threat actors abused several vulnerabilities to accomplish their mission.

Split of Windows Top 10 Detections

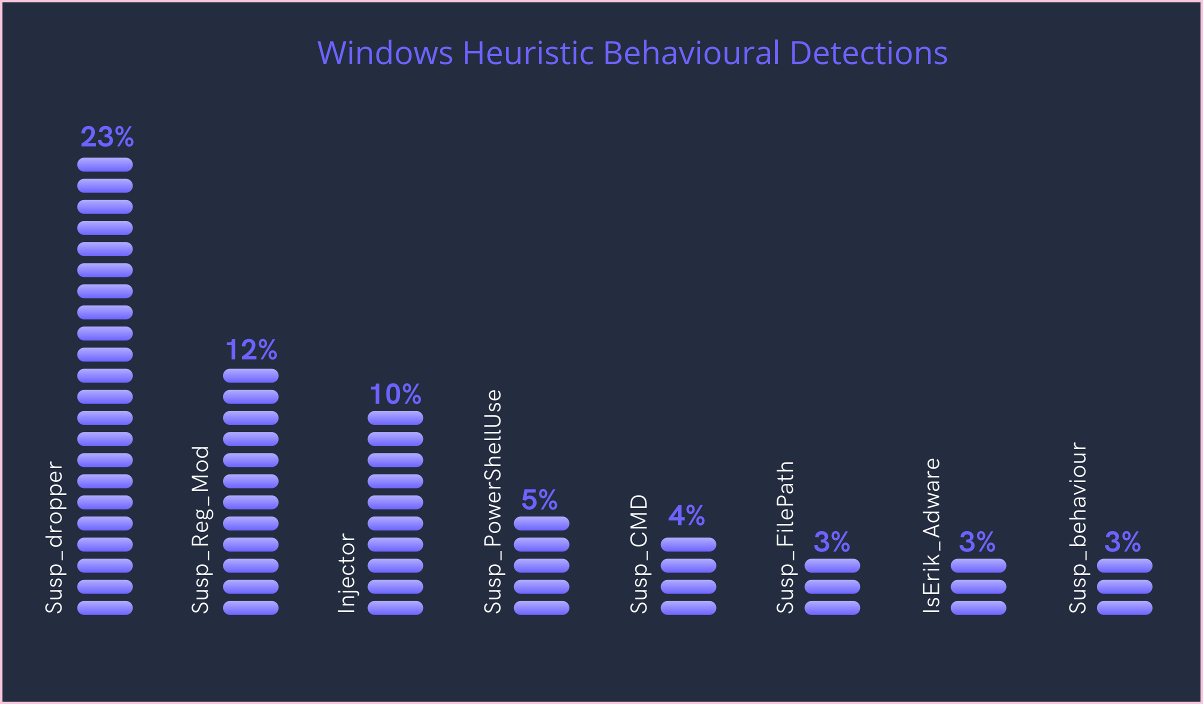


Most Prevalent Exploits



Host Intrusion Prevention System Heuristics

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



Droppers occupied a significant chunk followed by registry modifiers and injectors. Our behavioural detection also identified malware that were hosted as malicious scripts on websites abusing PowerShell and suspicious Windows process execution. A small percentage of the detections were those of malware trying to evade detection by using suspicious file paths and also of adversaries hiding their artifacts.

Mitigation Tips

- Beware of free software such as free utility programs which may come bundled with malware
- Ensure to patch all known vulnerabilities, as malware can be dropped through the same
- Be wary when you click on links on any website

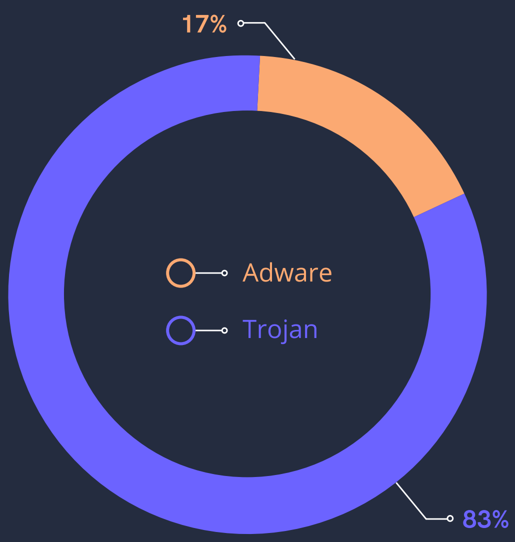
Back to contents

The Mobile Device Story

The increasing global digitisation across spheres has made us more connected than ever. However, the immense surge in digital footprint has an adverse effect too. For example, following the Covid-19 pandemic, we saw a massive increase in financially motivated malware attacks.

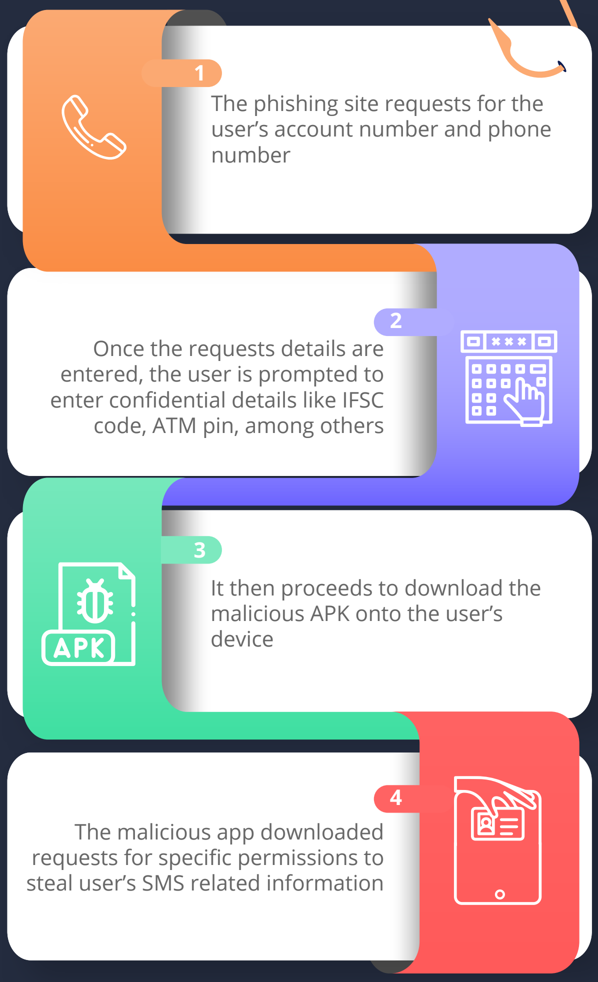
Threat actors are developing new Trojans loaded with more diverse and extensive propagation, obfuscation and attack methods. And a majority of these Trojans target digital banking and cryptocurrency consumers.

Adware vs Trojan Proportional Split



Case Study: Targeted SMiShing Attacks on Indian Banking Customers

Our researchers at K7 Labs recently encountered one such phishing campaign to lure Indian banking customers. This phishing page disguises itself as the official Customer Care site of the bank and intends to steal users' banking credentials. Here is how it executes its menace.



1 The phishing site requests for the user's account number and phone number

2 Once the requests details are entered, the user is prompted to enter confidential details like IFSC code, ATM pin, among others

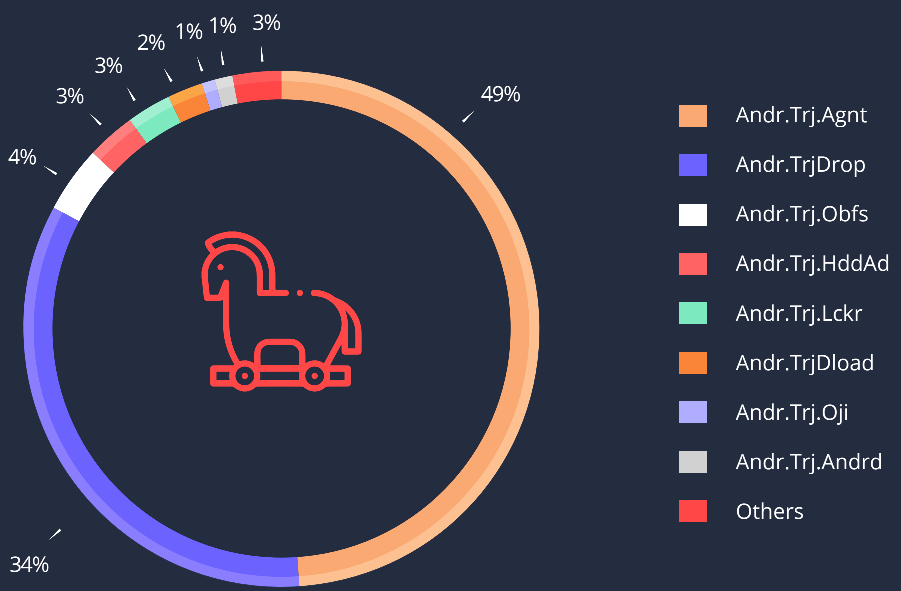
3 It then proceeds to download the malicious APK onto the user's device

4 The malicious app downloaded requests for specific permissions to steal user's SMS related information

The Ubiquitous Trojan

The increasing herd of Trojans on mobile platforms are persistent in nature, motivated and continuously evolving to evade security shields. For instance, we can glean that the frequency of agent and malware droppers has soared to a substantial amount, hinting at more sophisticated and intriguing attacks.

Most Prevalent Trojan Types

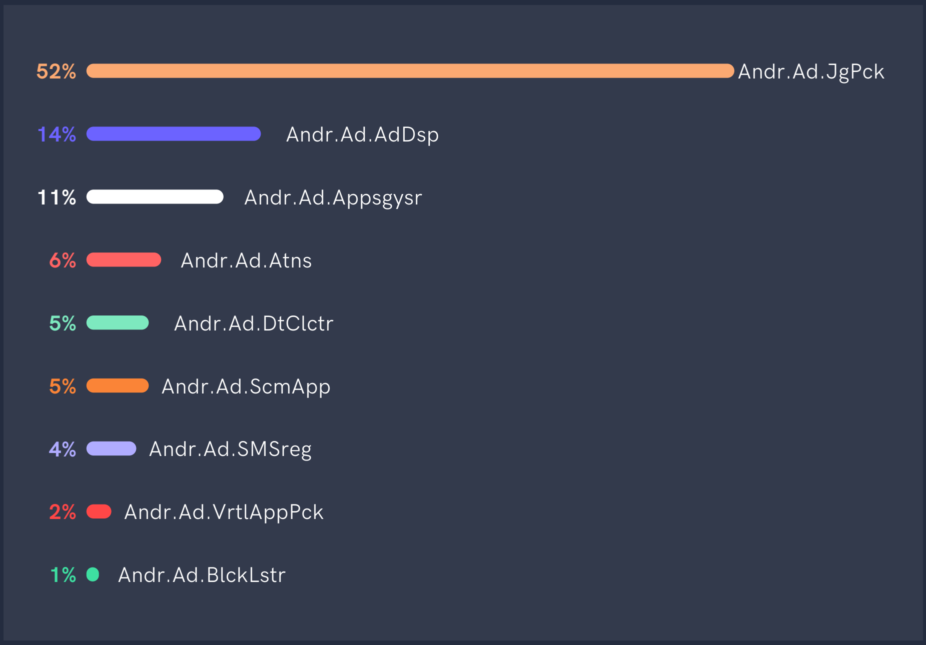


The Decline of Adware

The increase in Trojans and other malware has resulted in a significant proportional reduction in adware, although sometimes the boundary between malware and adware is very blurred indeed.

And not surprisingly, Andr.Ad.JgPck and Andr.Ad.AdDsp have managed to hold their reign in this quarter too.

Trend Line Showing the Adware Plague



Tips to Stay Safe

- Stay alert and avoid downloading 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

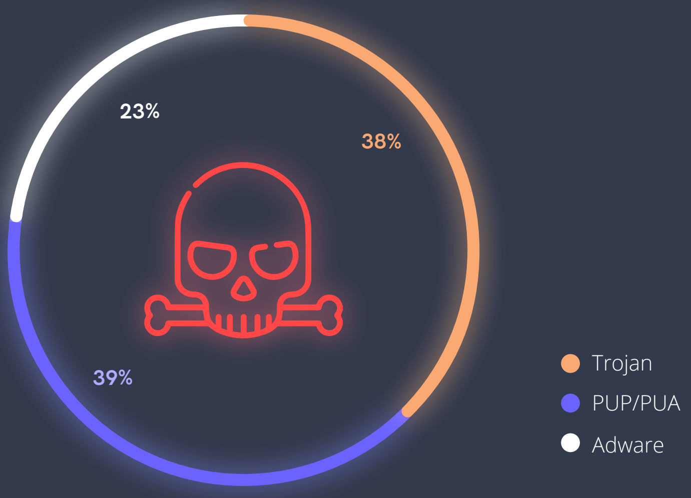
Back to contents

Mac Attack

Market share is a prime factor that drives OS targets in the threat landscape. Years ago, the lean user base of macOS discouraged the threat actors from investing significant time and resources to develop and leverage malware. However, the growing adoption of macOS computers among enterprises and end-users has transformed the scenario.

Despite Apple's immense effort and massive budget for platform security, threat actors are successfully leveraging attacks via phishing emails and various social engineering methods.

Adware Trojan & PUP Proportional Split

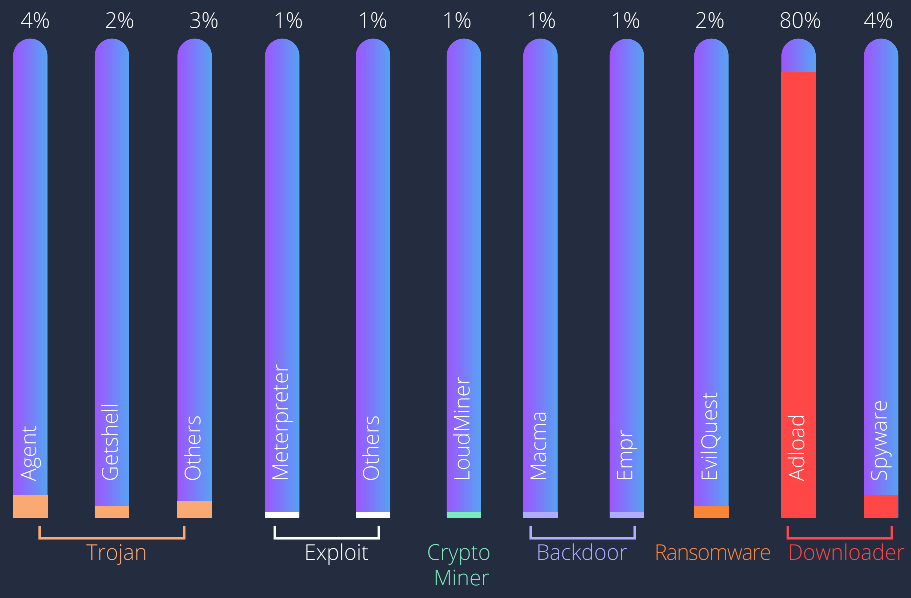


Though there has been a significant decrease in Trojans, the macOS platform is riddled with various avatars of adware and Potentially Unwanted Applications/ Programs (PUA/PUP). The rising number of attacks is quite impactful.

The Trojan Fracas

Unlike other platforms, exploits and a few specific families of Trojans remained prevalent on the macOS threat landscape. However, the statistics are pretty interesting because the numbers are way higher than the ransomware attacks on the space.

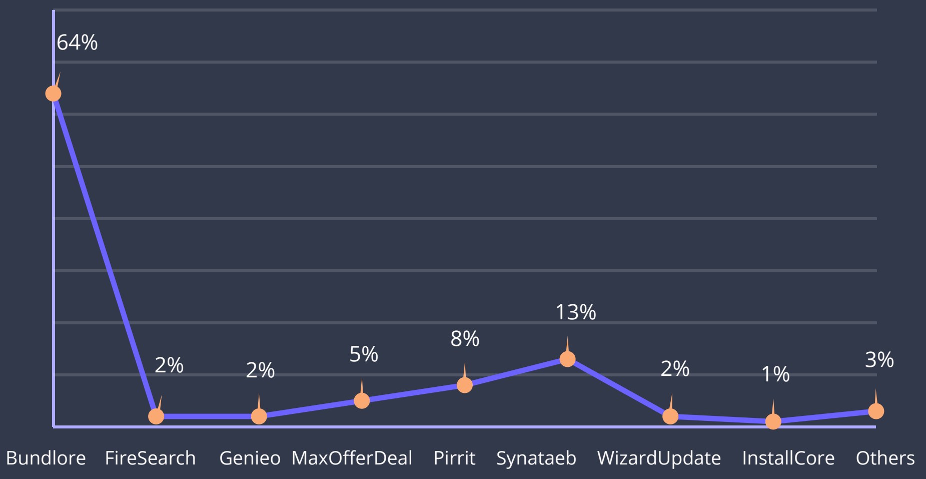
Trojan Detection Trend Lines



The Adware Saga

Adware has remained a prime concern for macOS users even in this quarter. We could still see all the old school variants hovering over the macOS space, out of which Bundlore holds a significant chunk.

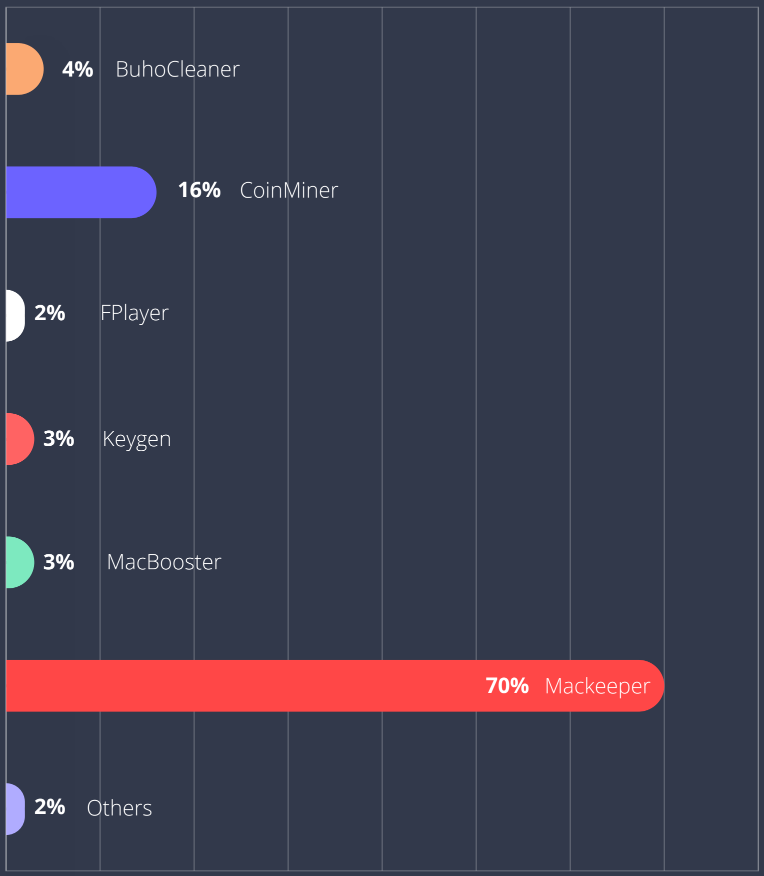
The Trend Line of Adware Variant Detections



A Trickle of PUPs

Despite the immense security measures adopted by Apple to secure the macOS app store, the PUP visibility doesn't indicate any significant decline. Instead, notorious PUPs disguised as system cleaners and performance boosters are still ruling the roost besides the substantial visibility of coinminers and pirated app key generators.

Most Prevalent PUP Types



Safety Guidelines

- Keep your macOS updated and patched for 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

Back to contents

Key Takeaways

Everyday the digital landscape is getting riskier than ever before. The growing number of vulnerabilities and social engineering opportunities due to the exponential growth of social media platforms offer more options to the adversaries. Buying a complete, multi-layered cybersecurity system is a necessary solution to it, but not every organization is willing to invest in their cybersecurity, making them very susceptible to threats.

Here are a set of safe practices you must follow to get shielded against the prevalent cyber hazards.

Enterprise

Secure your devices by keeping them up-to-date, patched for the latest vulnerabilities, and protected by up-to-date, high-quality security software such as K7 Endpoint Security

Organizations should do frequent vulnerability assessments and penetration testing so as to gauge the cybersecurity posture of their company. It will also be an advantage for the company if they start investing in the threat intelligence data that they are collecting.

Keep your network up-to-date and patched for the latest vulnerabilities

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

Do not download 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

Jan 2022