K7 SECURITY

Cyber Threat Monitor Report

Q1_2021-22

www.k7computing.com

Contents

Projecting The Cyber Threat Landscape

The dawn of 2021 started with a murky, pandemic-induced note, where 2020 had left us. Many of the menacing threats rolled out somewhere in 2020 were still very much active. Alongside, threat actors unfurled various other Tactics, Techniques and Procedures (TTPs), to hunt down target victims quickly.

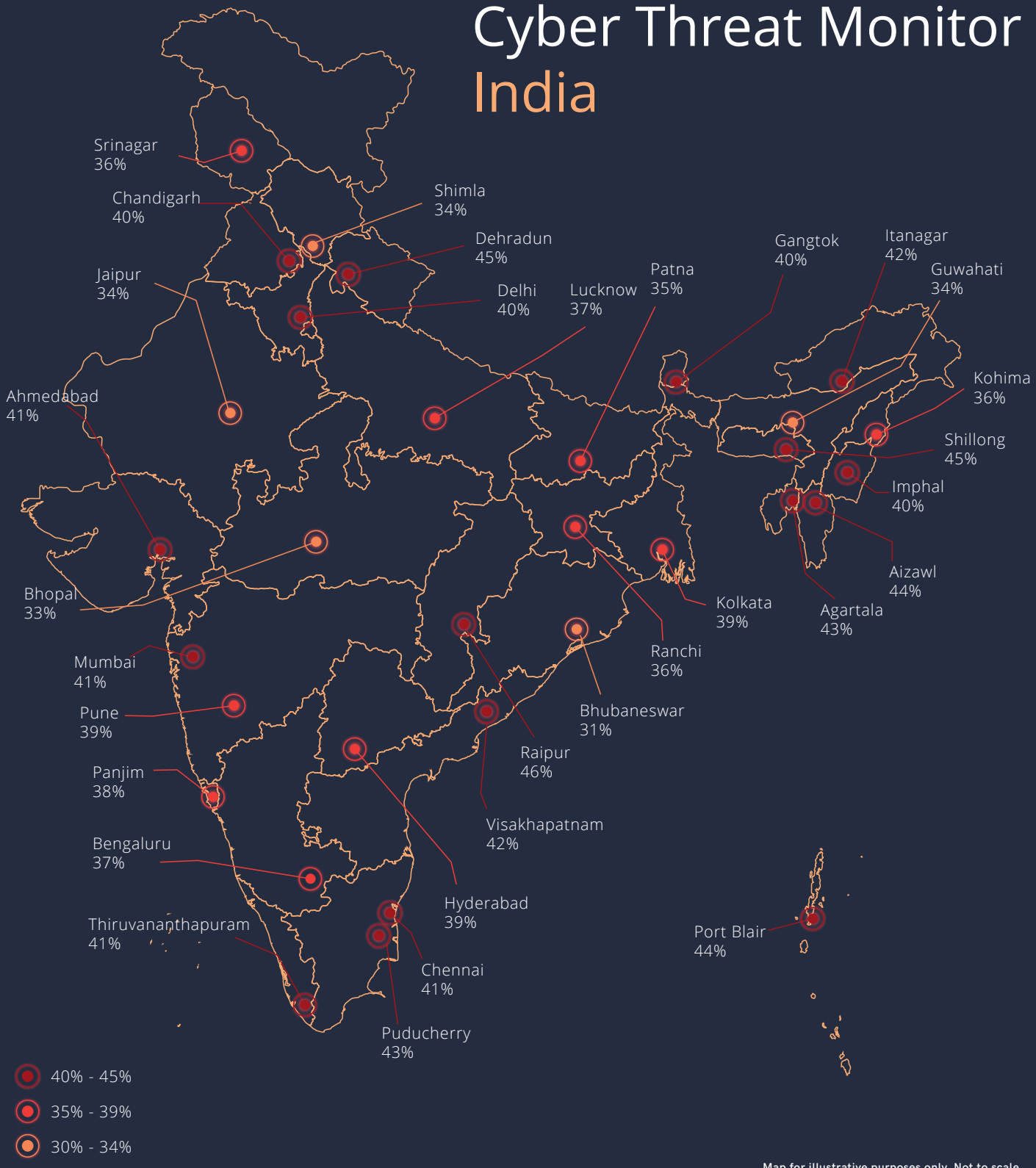
We at K7 are committed to combating this persistent onslaught of attacks to offer a cybercrime-free society. For the last 30 years, we have been working on preventing attacks on-premises and over the cloud. And the massive number of unprecedented battles let us witness millions of oncoming threat activities recorded by K7 telemetry. Keeping pace with the advancement in the threat landscape, we have refined our algorithms to present higher precision data.

The K7 Cyber Threat Monitor (CTM) report offers a snapshot into the latest threat activities, vulnerabilities and significant cyber incidents besides suggesting the best mitigation techniques to keep your organisation and yourself safe from cyber dangers.

This report brings exclusive infection rate (IR) data of all the Tier-1 and metro cities, top 10 Tier-2 cities alongside the country's state capitals. The infection rate offers a birds-eye view about the statistics of thwarted attacks to understand the frequency of threat actor activities which we believe you ought to be keenly aware of. From this quarter onwards, we have made some changes to the way the IR has been calculated and the reasons for the same have been detailed below.

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

Cyber Threat Monitor
India

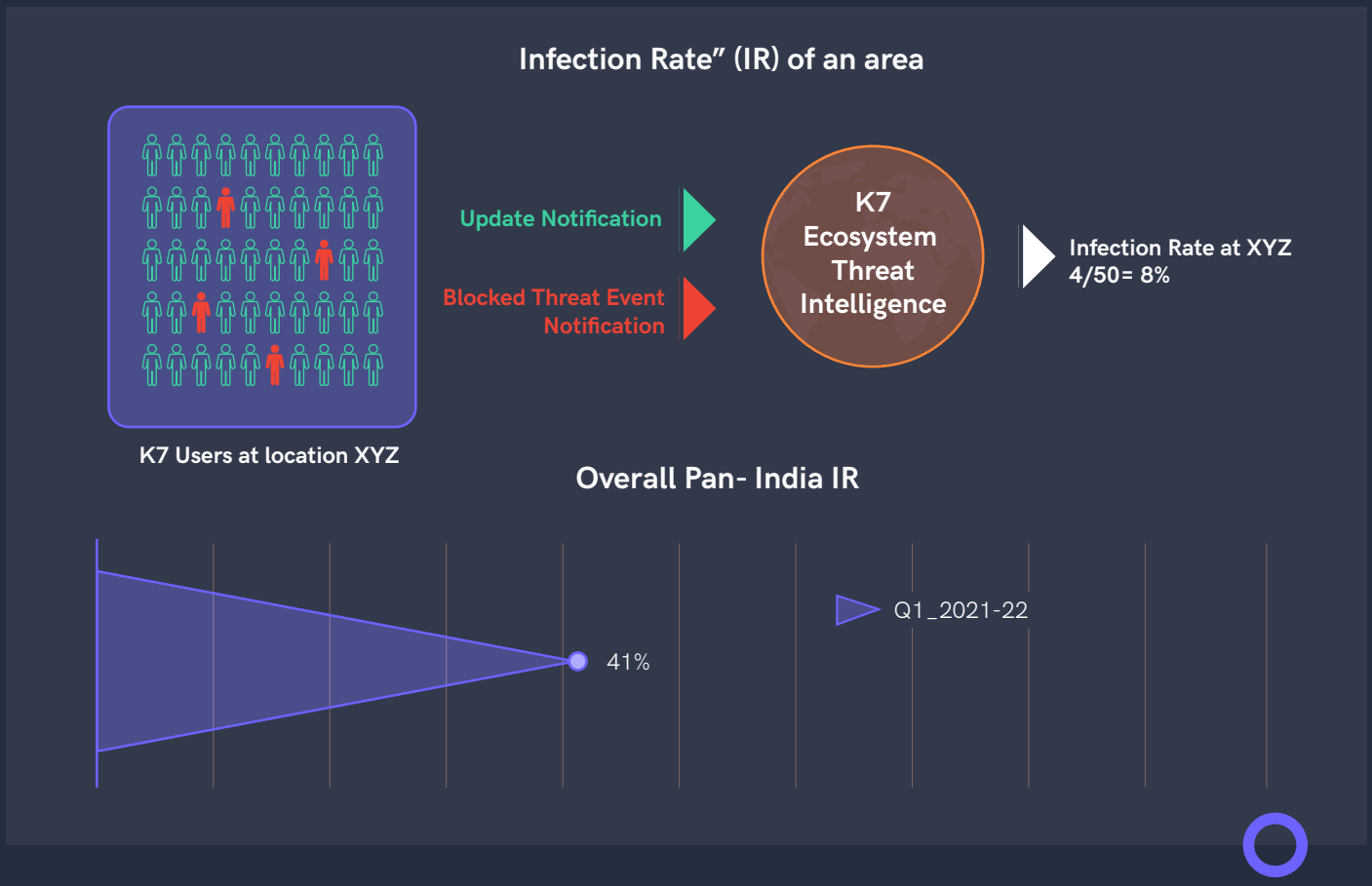


Map for illustrative purposes only. Not to scale.

Back to contents

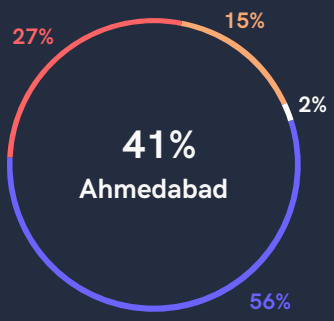
Regional Infection Profile

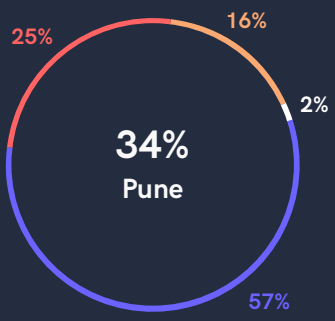
The concept of an "Infection Rate (IR)" of an area is as illustrated below.

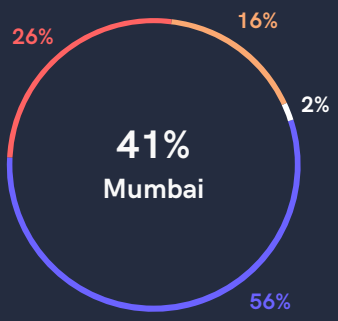


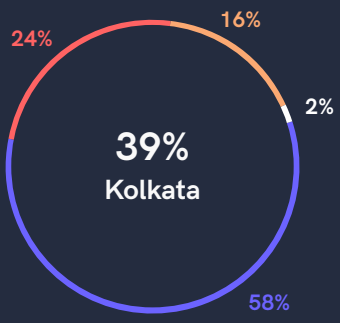
From this quarter onwards you would notice a significant surge in IR. This is due to a statistical remapping of user locations reported to our K7 Ecosystem Threat Intelligence (K7ETI) to adjust for occasionally tenuous geolocational (NAT-ed IPv4-based) data. This has been done to enhance precision and accuracy of geolocation data, which has revealed much higher concentrations of threat events.

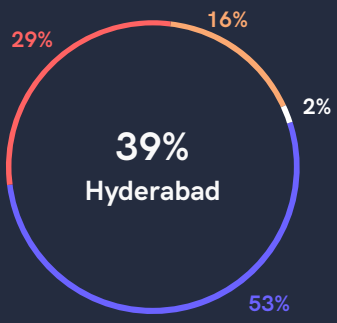
The Metros and Tier - 1 Cities - Infection Rate

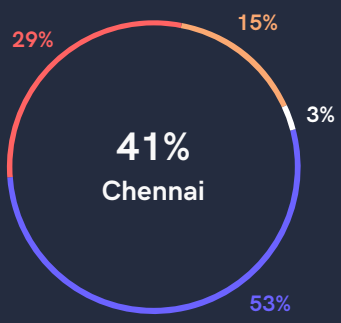


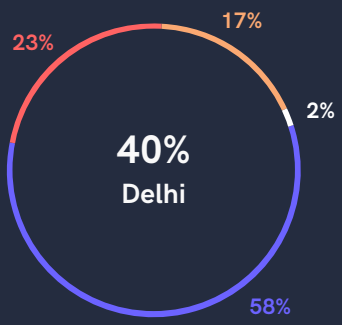


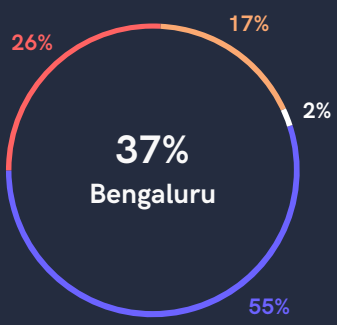






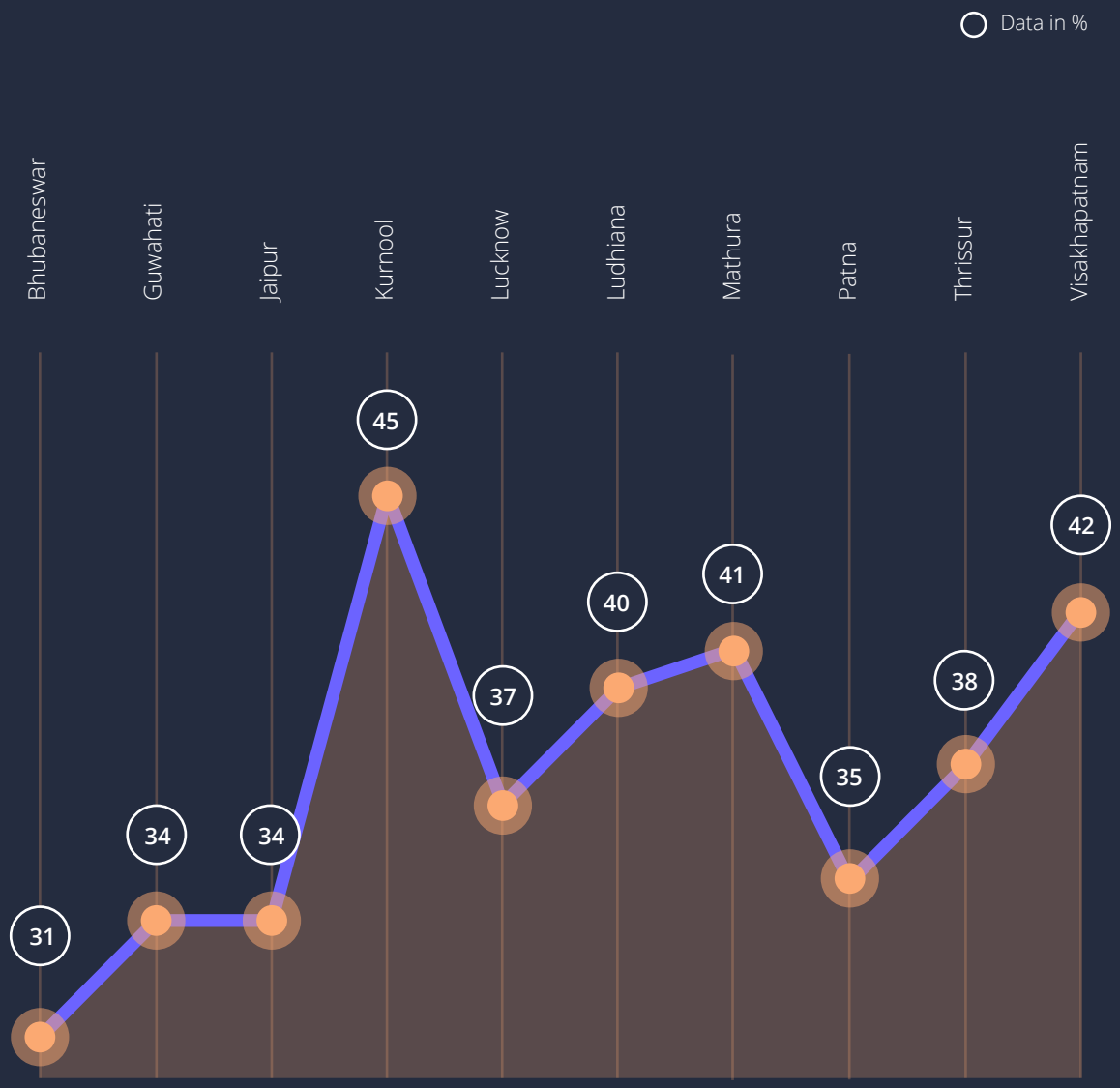






Behaviour Protection Firewall Protection ScanEngine Protection Web Protection

Top 10 Infection Rates in Tier - 2 Cities



The recalibrated IR, as described earlier, indicates a more precarious cyber threat situation in all the cities.

Enterprise Insecurity

Enterprises have long been a prime target for threat actors. And the severity is becoming grimmer with every passing day. With time, the threat actors are becoming sophisticated in their infection and attack methods, posing a formidable challenge to industry cybersecurity. This quarter we noticed one such malware whose execution strategy has been given below.

Case Study: Resurgent Glupteba Backdoor

The Glupteba malware was boisterous only until 2020, followed by a lull in activities. Then, quite surprisingly, we noticed a recent surge in its visibility via our K7 telemetry. This malware was seen spreading its mayhem via EternalBlue exploits. The execution sequence is sketched below:

The Resurgence of Glupteba

Safety Recommendations

- Keep all your devices, including your OS, updated and patched for the latest vulnerabilities
- Do not open suspicious documents. Also do not enable macros, especially if the file received is from an unknown source
- Change all your default credentials
- ALL systems in the network should have a reputable enterprise security suite, such as K7 Endpoint Security, installed and kept updated

Vulnerabilities Galore

There is no denying that vulnerabilities are increasing at an alarming rate. You can check the CVE database yourself to understand the massive proliferation. The ramification of this paradigm shift is affecting the industry, both public and private, and all netizens.

The sustained splurge asserts that newer, more robust multi-layer detection methods are required, along with necessary policy changes to thwart attacks.

To understand the ongoing rapid escalation of vulnerabilities across platforms, we highlight the most notorious vulnerabilities that bombarded the threat landscape in this period

HTTP Protocol Stack Vulnerability

A vulnerability, **CVE-2021-31166,** in the HTTP protocol stack could lead to wormable remote code execution (RCE). To exploit this, an unauthenticated attacker can send specially crafted packets to a targeted server utilizing the HTTP Protocol Stack. On successful exploitation it leads to arbitrary code execution in the context of the logged on user. The vulnerable versions are Windows 10 and Server versions 2004 and 20H2.

SonicWall Email Security Vulnerability

CVE-2021-20021, a vulnerability in SonicWall Email Security, can be exploited by sending a specially crafted HTTP request to a target system. On successful exploitation an unauthenticated attacker can create an admin user. Vulnerable products are SonicWall On-premise Email Security (ES) 10.0.9 and earlier versions, and Hosted Email Security (HES) 10.0.9 and earlier versions.

Virtual SAN Health Check Vulnerability

The **CVE-2021-21985** vulnerability is due to insufficient input validation in the Virtual SAN Health Check plug-in of vSphere Client which is enabled by default in vCenter Servers. On successful exploitation this vulnerability could lead to remote code execution on the target machine. Vulnerable products are vCenter Server 7.0, 6.7 and 6.5.

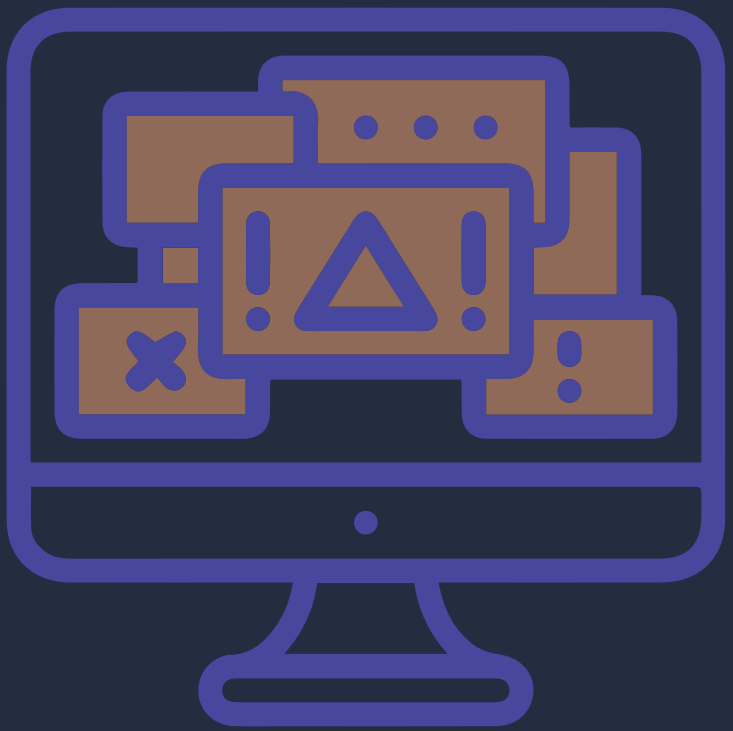
RCE Vulnerability in Microsoft's Browser Engine

CVE-2021-33742 is an RCE vulnerability in Windows MSHTML, which is Microsoft's proprietary browser engine. This is used by legacy applications that are dependent on Internet Explorer. On successful exploitation, this vulnerability could lead to arbitrary code execution in the context of the logged in user. Vulnerable OS versions are Windows 10, Windows Server 2019, Windows Server 2016, Windows 7, Windows 8.1, Windows Server 2008, Windows Server 2012

Privilege Escalation Vulnerability in Windows NTFS

A privilege escalation vulnerability, **CVE-2021-31956,** has been identified in Windows NTFS. This vulnerability was exploited in the wild along with Windows Notification Facility (WNF) to execute malware with admin privileges on compromised Windows systems.

Vulnerable OS versions are Windows 10, Windows 8.1, Windows 7, Windows server 2008, Windows server 2012, Windows server 2016, Windows server 2019.

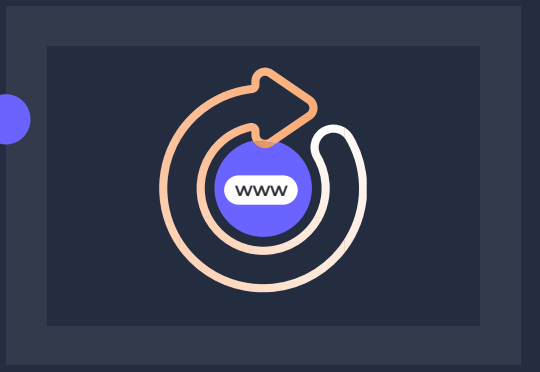


Danger in the Internet of Things

Besides the menacing list of software vulnerabilities, the period also indicated that IoT devices remain riddled with copious weaknesses. The most extensive vulnerabilities are as follows.

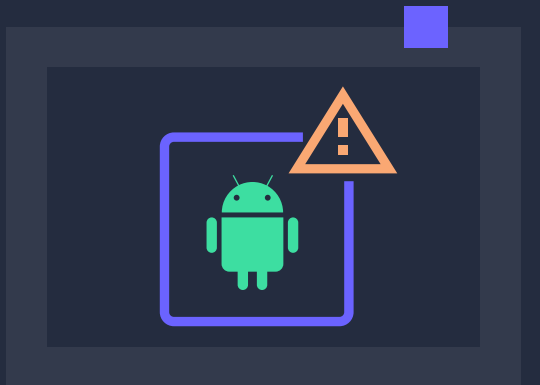
Fragattacks

It is a collection of vulnerabilities present in WiFi devices since 1997 due to a design flaw in the WiFi standard, which can be exploited by attackers who are within the device's range. This vulnerability can be used to exfiltrate sensitive data that is being transmitted from the vulnerable devices. It affects a lot of devices that are using the WiFi security protocols from WEP to WPA3.



WebKit Buffer Overflow Vulnerability

CVE-2021-30666, a buffer overflow vulnerability, can be exploited using maliciously crafted web content. This vulnerability can be exploited to achieve remote code execution on the vulnerable devices. Vulnerable devices are iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3, and iPod touch (6th generation) with iOS version older than 12.5.3.

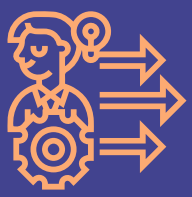


Android OS Vulnerabilities

CVE-2021-0507, is an RCE vulnerability that exists in the System component in the Android OS.

An elevation-of-privilege vulnerability, **CVE-2021-0516**, was also identified in the Android System Component. This vulnerability can be exploited by an attacker to achieve admin privileges.

Vulnerable devices are Android versions 8.1, 9, 10, and 11.



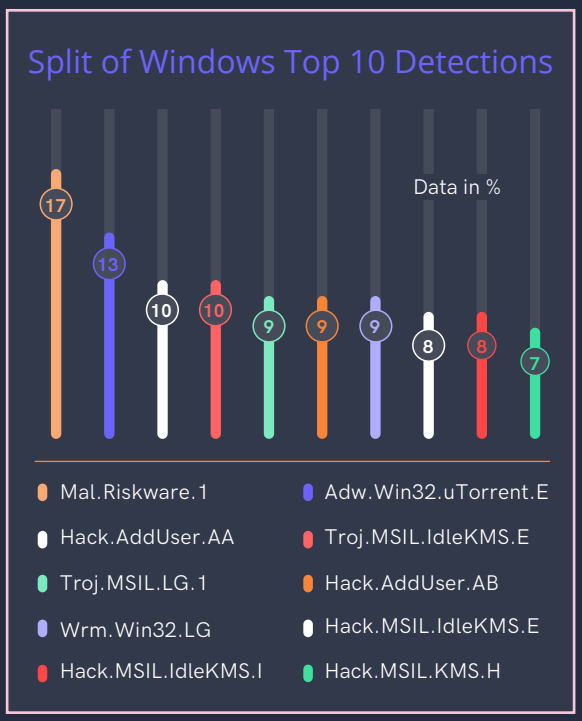
Mitigation Techniques

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

Windows under Siege

Windows Malware Type Breakdown

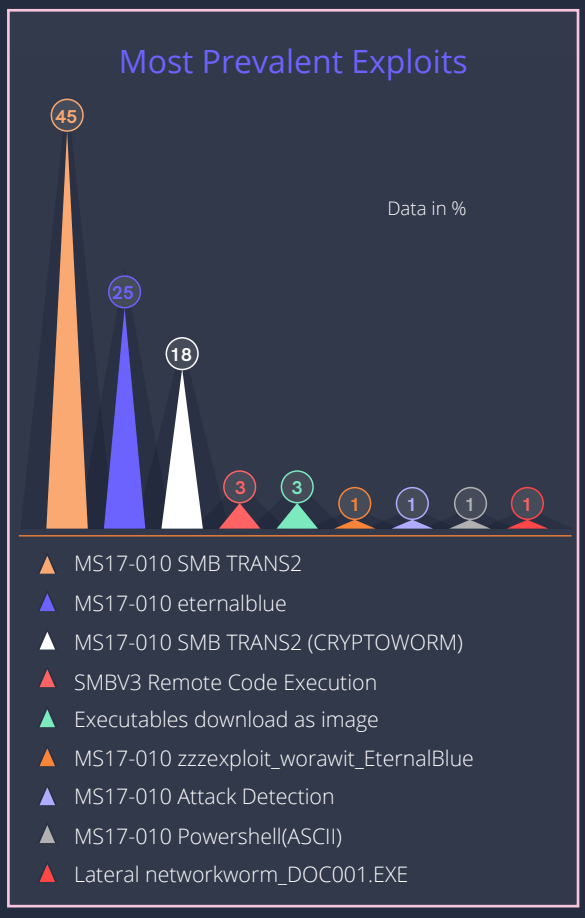
This quarter also, our telemetry detected various malware, adware, and hack tools subsisting together and targeting the users.



Mal.Riskware.1 and Adw.Win32.uTorrent.E topped the Windows threat landscape list, while the rest of the Windows adware and malware also retained their significant share during the period.

Windows Exploits

Even after Microsoft has released many updates for its Windows operating system, older unpatched versions still exist in the market for various reasons. This gigantic visibility of vulnerable computers enables the adversaries to continue exploiting the dated vulnerabilities and intrude into the victims' system to do the necessary damage.



Mitigation Tips

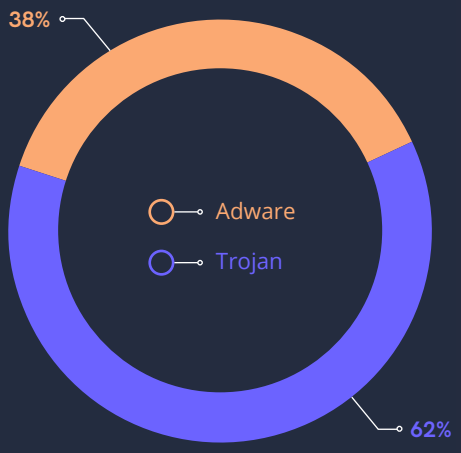
- Keep your devices updated and patched for the latest vulnerabilities
- Follow the principle of least privilege while granting access to your employees
- Enforce a robust password policy

The Mobile Device Story

Financially motivated cybercriminals trigger malware, phishing, and copious social engineering techniques to the handheld devices for intruding into an organization's network as part of a comprehensive strategy resulting in an uptick in the Android threat landscape.

The latest Android threat landscape has been continuously evolving and bad actors are coming up with new threats, making life difficult for the netizens.

Adware vs Trojan Proportional Split

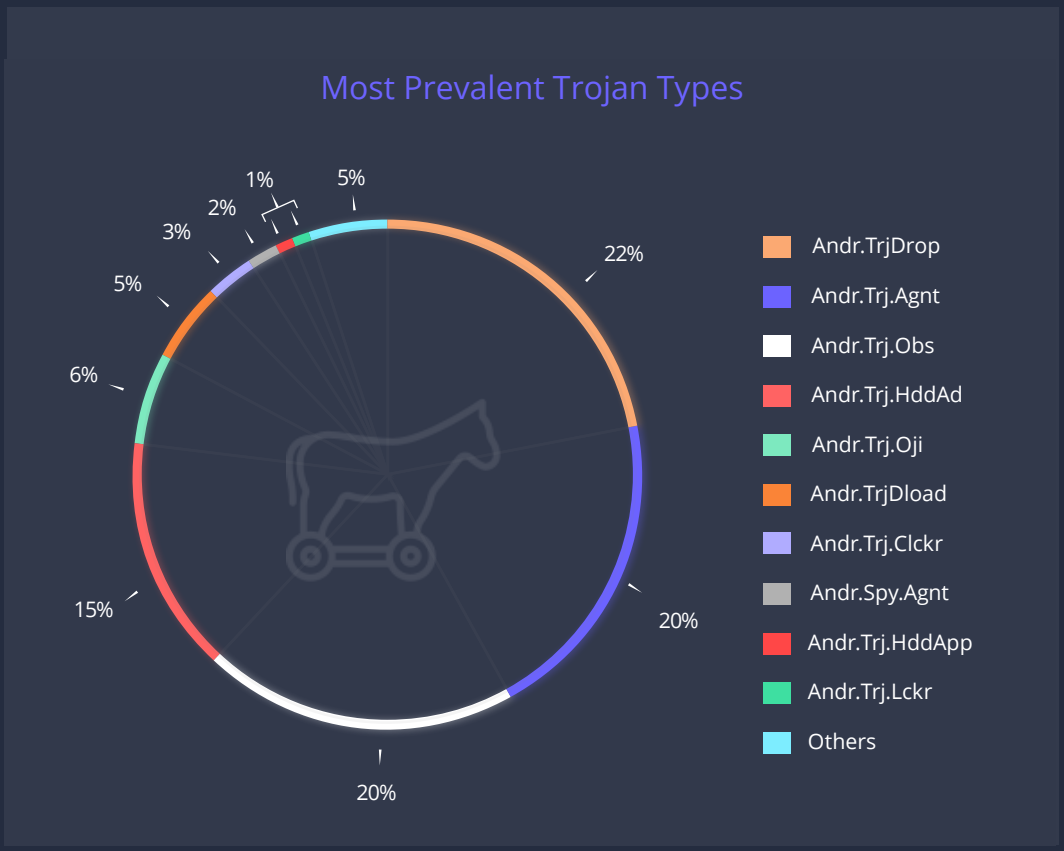


Apps play a critical role in the smartphone threat landscape. Despite the efforts of Google and Apple, threat actors keep an eye on downloading trends and develop fake apps masquerading as authentic ones to fool the users. Take the WhatsAppPink theme, for instance. The app looks exactly like the genuine WhatsApp with a new avatar. People looking for changes in their existing WhatsApp theme would undoubtedly fall prey to it. And what happens next? Check the infographic.

Case Study: Never Ink the New WhatsappPink

The Ubiquitous Trojan

The Covid-19 pandemic has increased the use of mobile devices for various purposes, resulting in a sharp uptick in Banking Trojan families. Alongside the rampant growth of Advanced Persistent Threats (APTs) activity, threat actors are using Mobile Remote Access Trojans, info stealers, fake mobile apps, and even ransomware to achieve their money-motivated intentions quickly.

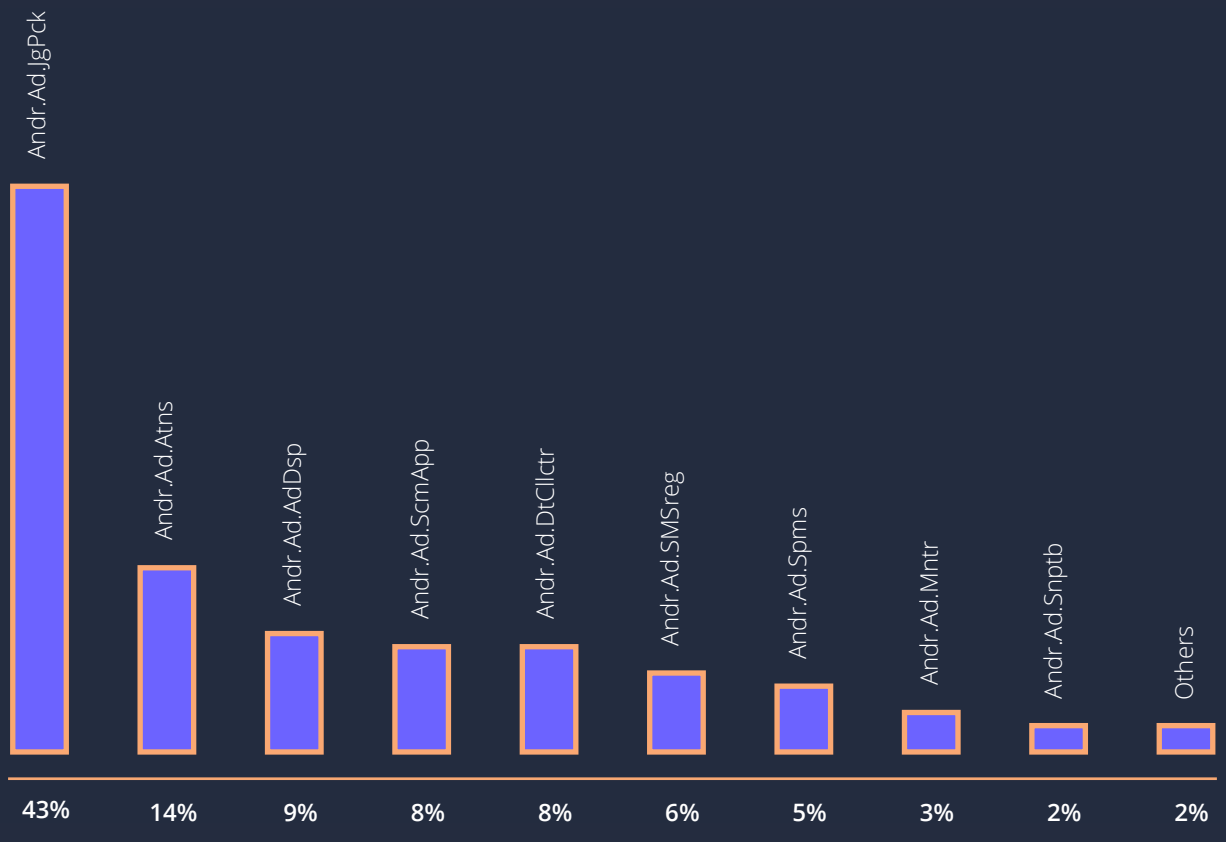


To substantially increase the attack numbers, threat actors relied on social engineering techniques to misguide the users into installing malicious apps.

The Significance of Adware

The continuous surge of Trojans didn't indicate any withering in the presence of adware. Popular adware persists in the Android arena, masquerading as popular apps on the Google Play Store and third-party app stores.

Trend Line Showing the Adware Plague



Nowadays, threat actors use adware for easy money-making without users' authentication.

Tips to Stay Safe

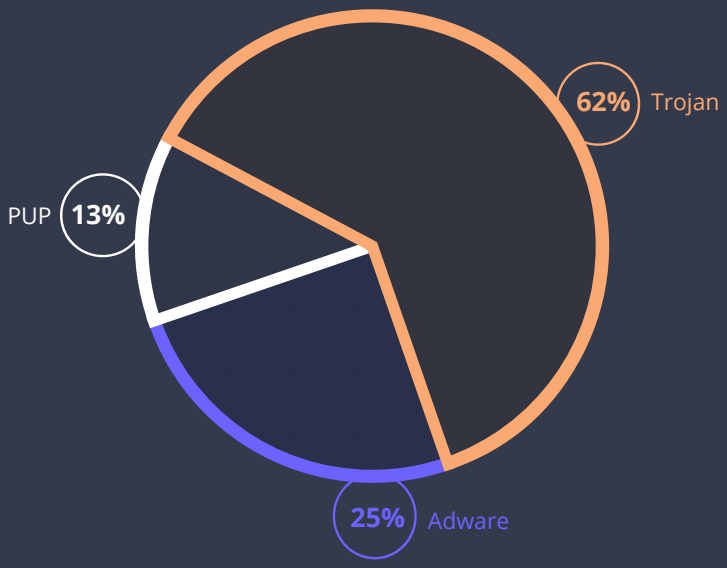
- Do not get mislead by fake messages
- Do not download apps from unknown sources or third-party app stores
- Keep your OS and devices updated and patched for the latest vulnerabilities
- Install a robust security product like K7 Mobile Security to stay protected from the latest threats and update it regularly

Mac Attack

While conventional adware and PUPs are trudging through an ongoing disruption in organisations globally, a few old-school Trojans are doing the rounds in the macOS arena. The novel macOS ransomware EvilQuest and spyware Xcsset have re-emerged from the past and are triggering a colossal disruption among macOS users.

From the stats we can glean that the proportion of adware is also indicative of how adversaries are targeting macOS users with a significant internet engagement.

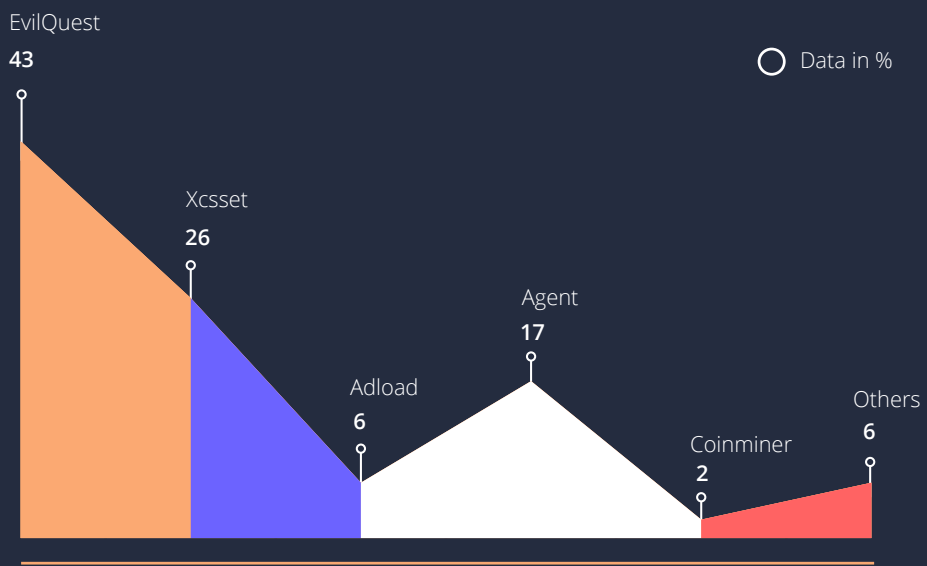
Adware, Trojan & PUP Proportional Split



The Trojan Brouhaha

Despite the massive occupancy of Trojans in the macOS threat landscape, a handful of families executed steady attacks on macOS users.

Trojan Detection Trend Lines

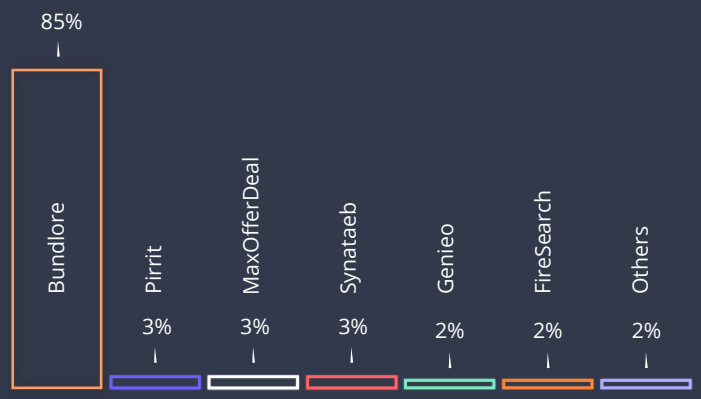


As you can see, EvilQuest and Spyware Xcsset occupied the majority of the Trojan space.

The Diminishing Adware

In this quarter, adware has plummeted a bit to indicate the ongoing trend. However, adversaries still bank on a variety of adware for making quick funds.

The Trend Line of Adware Variant Detections

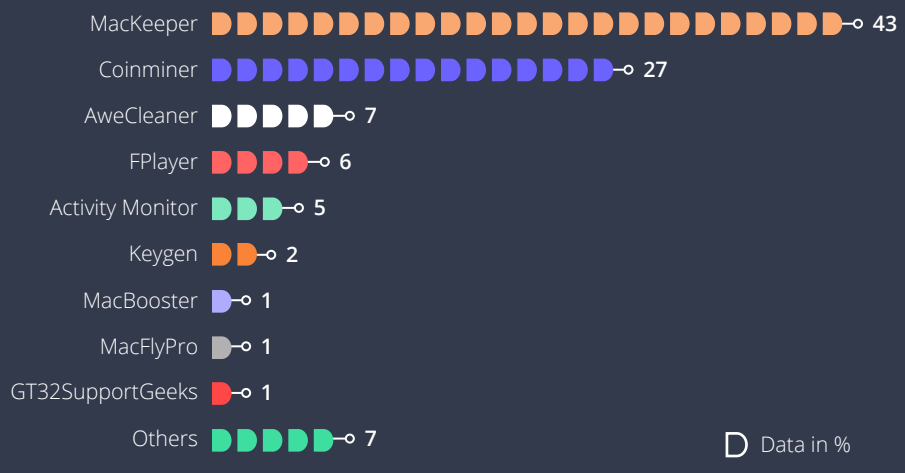


Bundlore leads the presence race with a significant difference from the other visible adware.

A Trickle of PUPs

The pervasiveness of various Trojan families in the macOS arena has adversely affected the PUP space too. However, the diminishing presence hasn't affected the predominant ones.

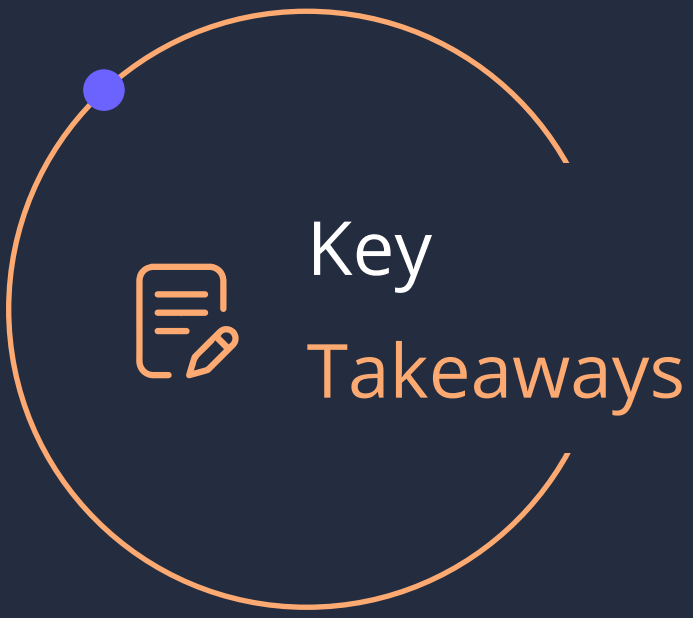
Most Prevalent PUP Types



The shady utility software MacKeeper, along with a bunch of Coinminers, have perpetually maintained their reign over the macOS space.

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



Key Takeaways

To combat the present-day threat actors, organisations and individuals should embrace a proactive approach to stay ahead in the battles against cybercriminals and their new attack trends. The policy should focus more on preventing attacks instead of adopting a remediation approach.

Here are a few mitigation tips you must embrace to stay ahead in the war against digital evil.

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

Do not open documents from unknown or suspicious sources. Also, do not enable macros in documents received from such sources

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

Consumer

Secure your device 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 it up-to-date

Do not fall prey to fake messages either via social media or through email or SMS

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

K7 SECURITY

www.k7computing.com

Jul 2021