Cyber Threat Monitor Report

2020-21

K7 SECURITY

Contents

Contents

The Need to Stay Safe in an Insecure World

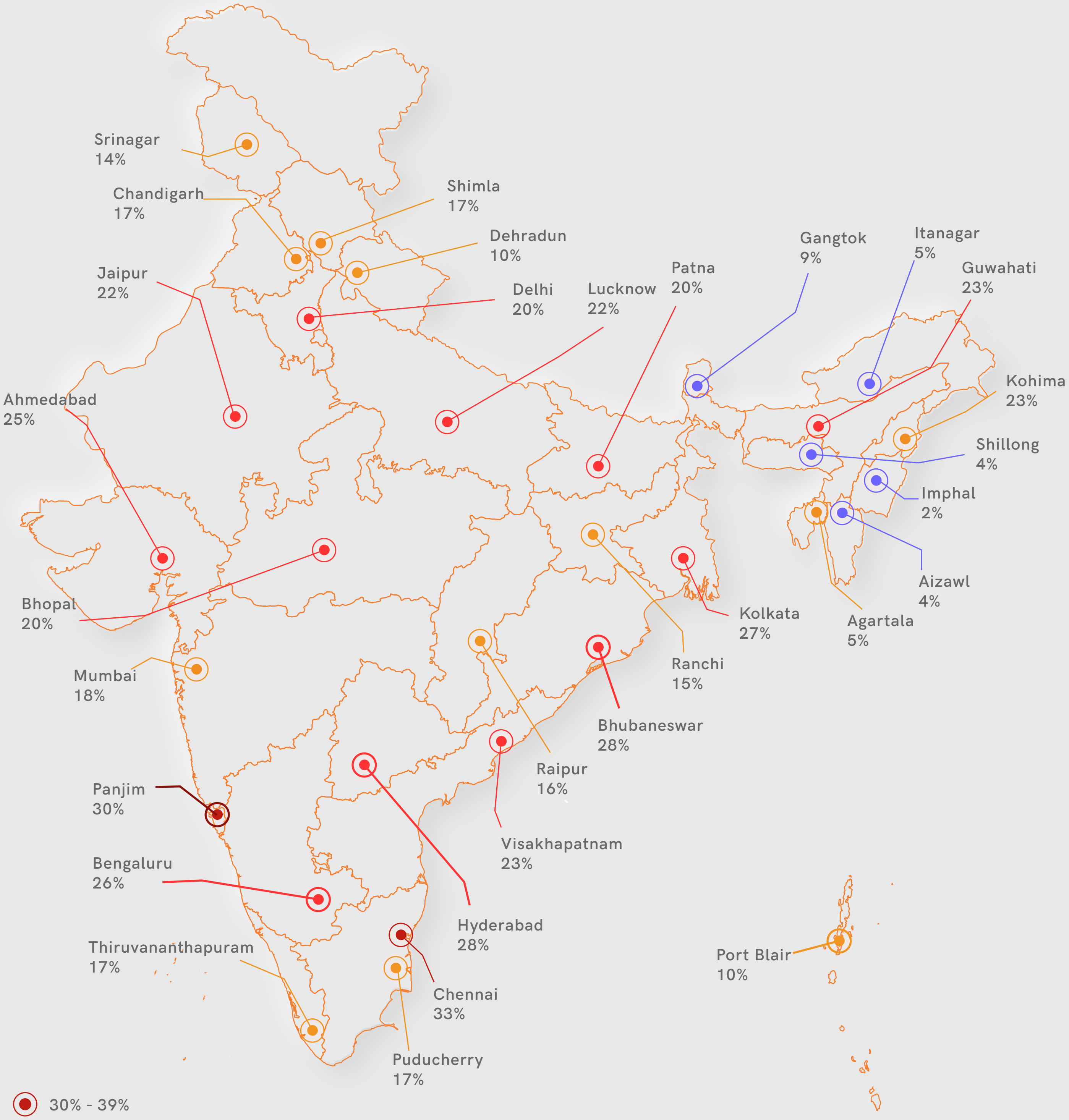
With every passing day, we are becoming more and more reliant on digital devices and the threat landscape is adapting to this with its ever expanding and evolving threat base. The attacks these days are more targeted, sophisticated and capable of evading multiple detection layers. Moreover, the attackers have also started devoting more time on reconnaissance so as to gather the acute intelligence of their targets before launching any attack.

The growth of sophisticated ransomware and several other Trojan families suggests how the future of the threat landscape looks. That doesn't indicate that the visibility of good old adware is dwindling. Multiple adware are still there on the horizon, trying to mint money on the back of naive users. To survive in this state of turmoil, it's always a good idea to nip the problem in the bud by following safety precautions.

This quarter's K7 Cyber Threat Monitor report looks into the threat landscape and explains the latest tricks of threat actors through illustrative infographics. The report also aims to provide vignettes of the prevalent threats hovering over different popular platforms. The list includes the malware strains, vulnerabilities, and exploits perturbing the digital world.

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

CYBER THREAT MONITOR - INDIA



🔴 30% - 39%

🔴 20% - 29%

🟠 10% - 19%

🔵 1% - 9%

Map for illustrative purposes only. Not to scale.

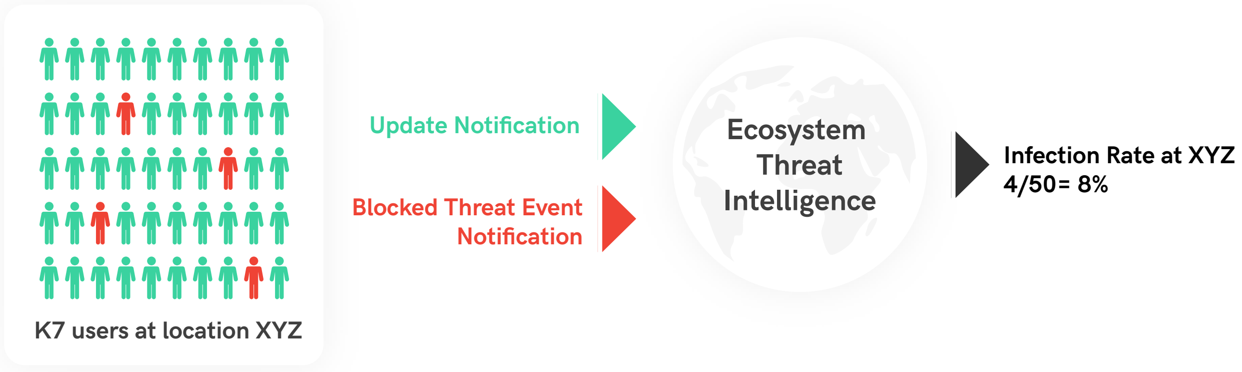
BACK TO CONTENTS

Regional Infection Profile

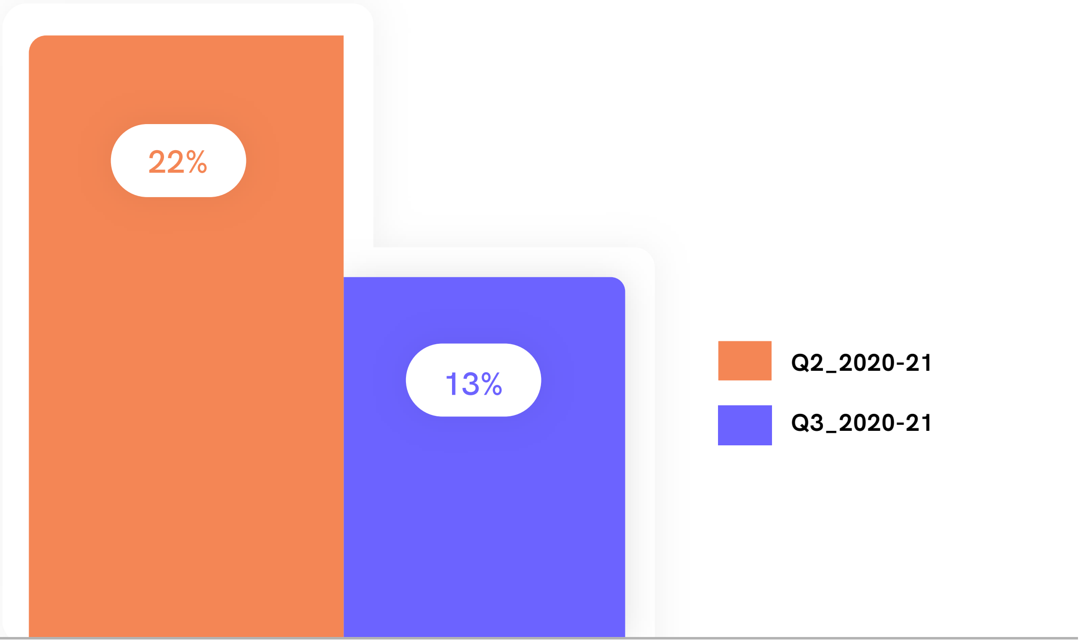
The year 2020 began on an alarming note, and the situation seemed more or less the same even by the end of the year. The influx of numerous critical vulnerabilities found on multiple sought-after products and technologies helped the threat actors immensely to launch relevant attacks. During this ongoing mayhem, the Covid-19 pandemic worked as a catalyst, offering a helping hand to deliver more phishing and other social engineering tricks.

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

Infection Rate" (IR) of an area

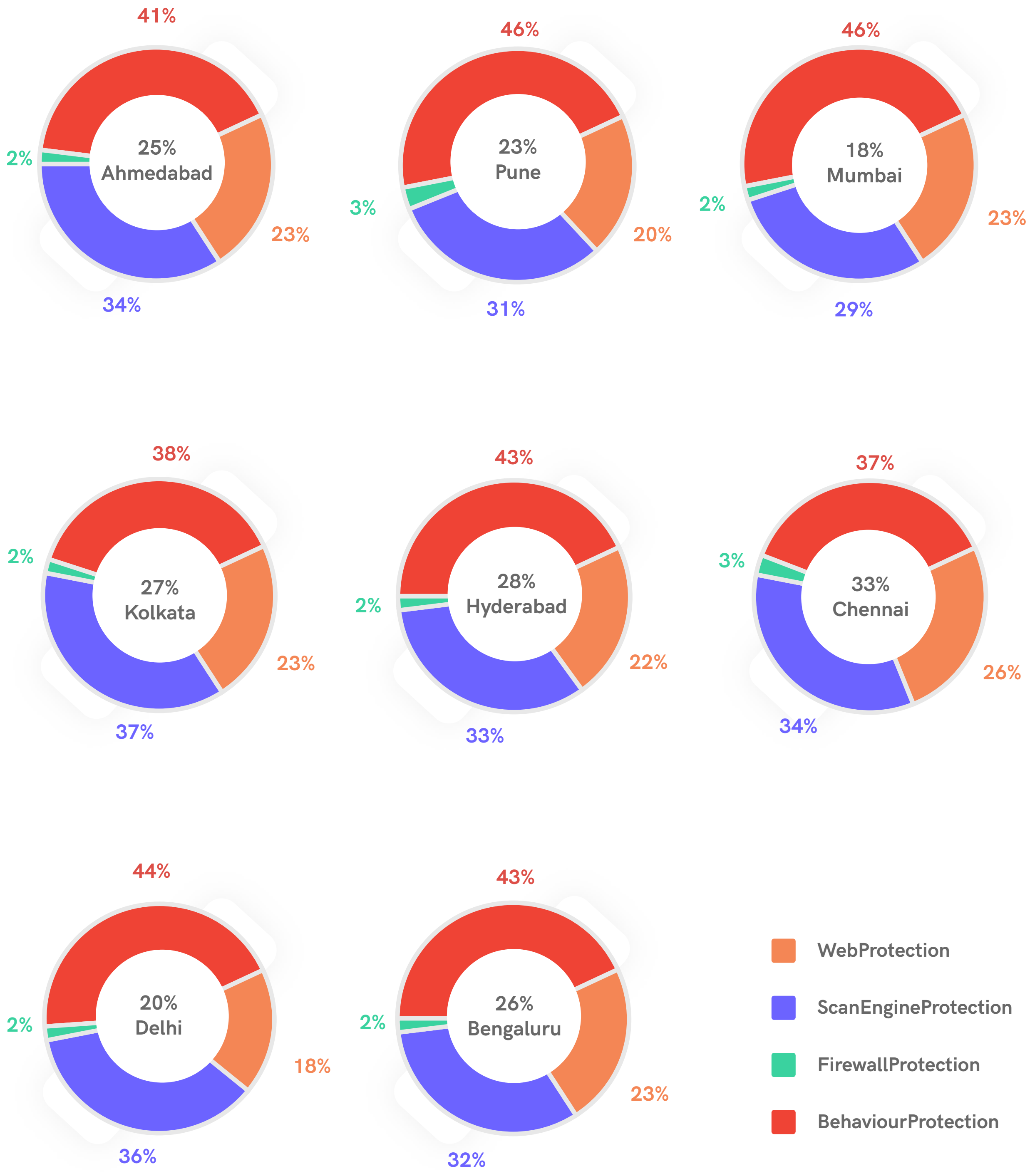


The Overall Pan-India IR is given below.



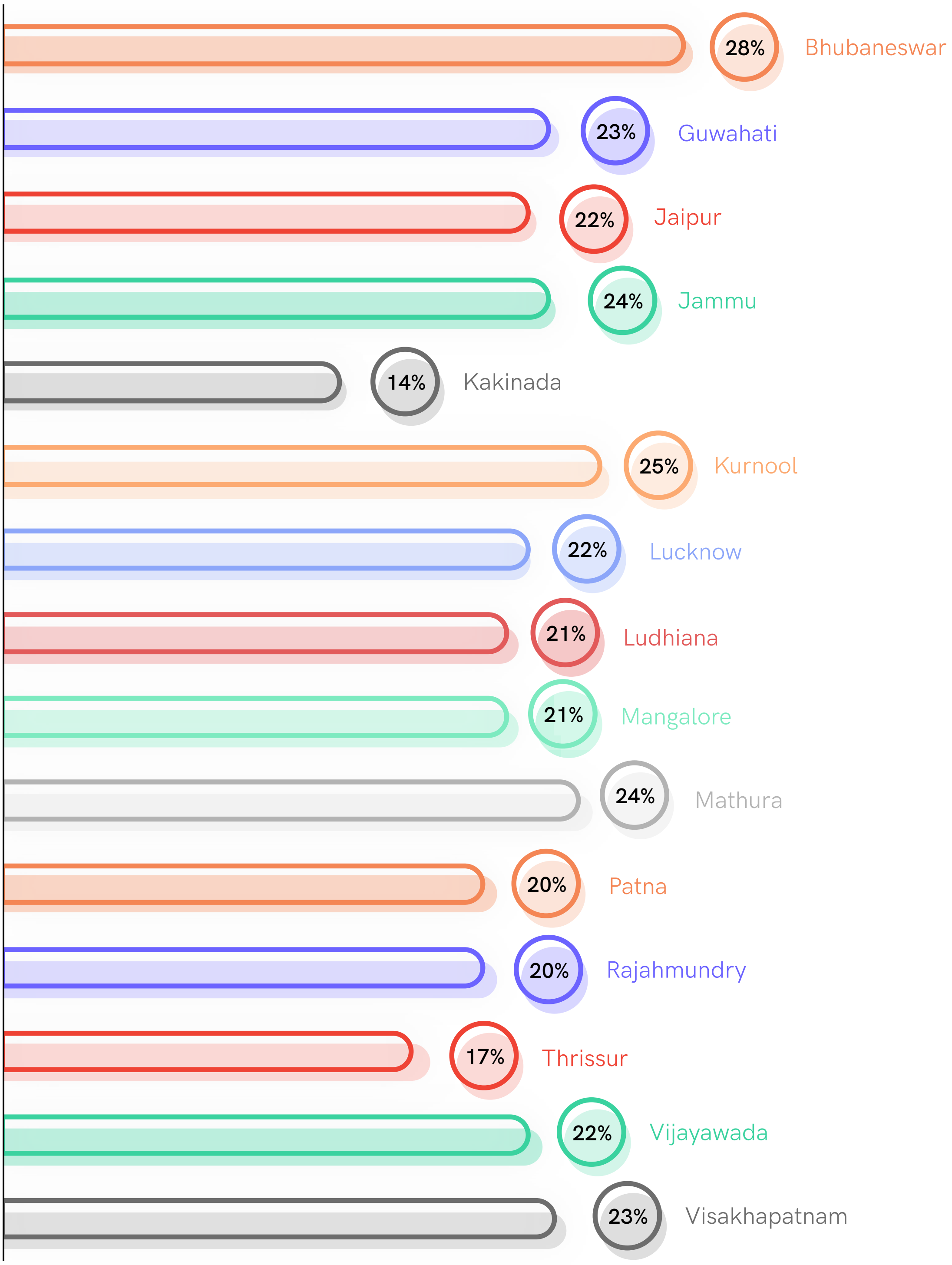
Metros and Tier-1 cities often bear the brunt of attacks in any given period as they are well-connected, the hub of several profitable enterprises and offices. And with an average IR of 25% and above, the scenario does not look favourable for users.

The Metros and Tier - 1 Cities - Infection Rate



The increasing mass digitisation, begun well before the pandemic but accelerated by it, has changed the threat landscape in Tier-2 cities as well. These have become more attack-prone. However, the good news is that the netizens here have perhaps become a little more cyberaware, as can be seen from the decreasing IR in all the cities in comparison to the previous quarter. However, we would need to observe such trends across multiple consecutive quarters to arrive at any conclusive judgement on the matter.

Top 15 Infection Rates in Tier-2 Cities



BACK TO CONTENTS

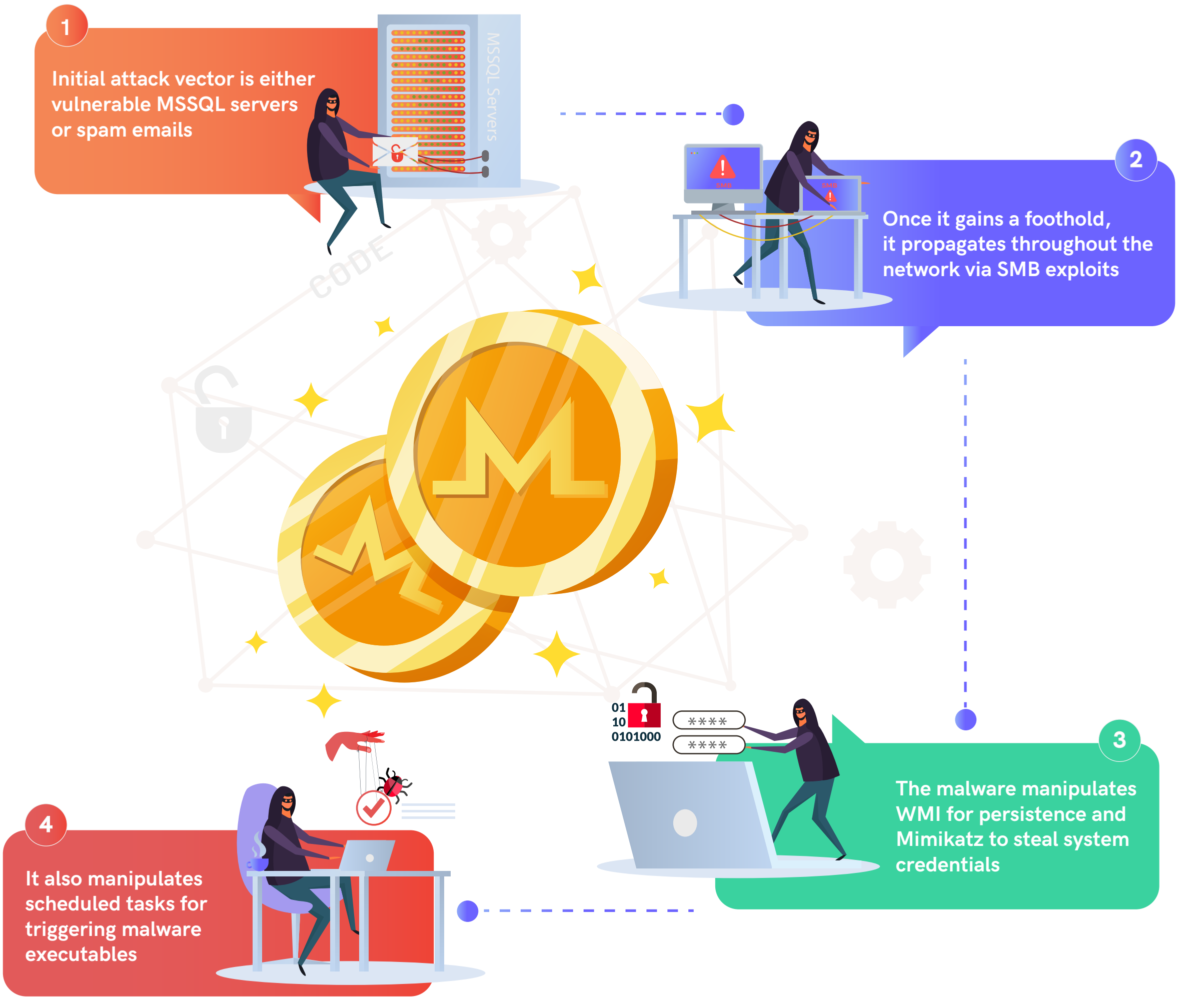
Enterprise Insecurity

It is almost a year since Covid-19 smote the world, and we are still very much within a Pandemic. Cyber threats are not far behind. While enterprises across the world are experiencing a surge of ransomware, we also saw a continued influx of other malware attacks such as cryptominers. Though being outshone by the ubiquitous ransomware, cryptomining malware did remain quite visible and concerning.

During this period, one of our valued customers reported that their DNS (Domain Name Server) configuration was being changed periodically without any intervention from their side. Our investigations revealed that the culprit was a Coinminer malware.

Our analysis of the malware has been delineated below.

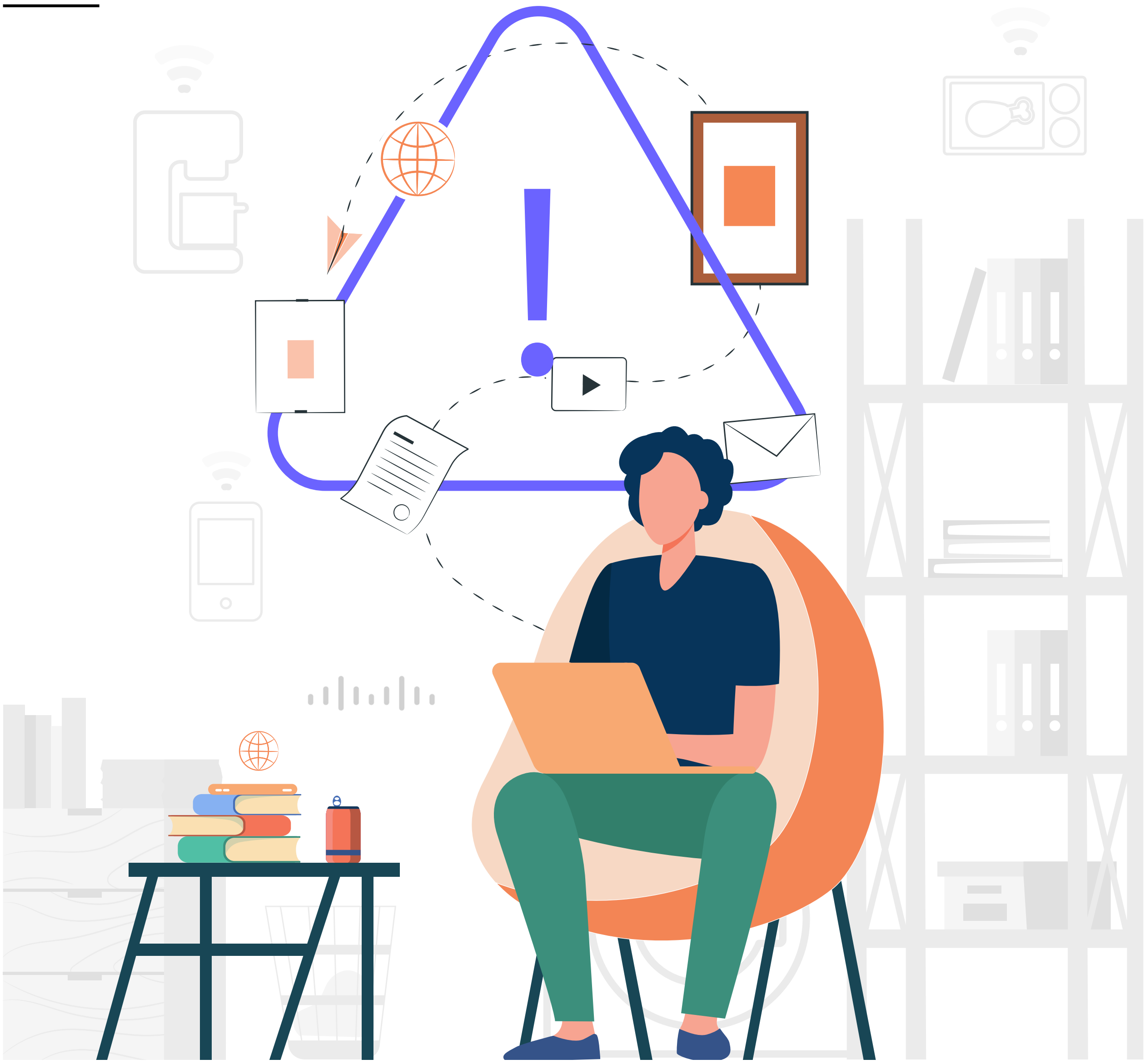
The Pursuit of MrbMiner


1
Initial attack vector is either vulnerable MSSQL servers or spam emails
MSSQL Servers
CODE
2
Once it gains a foothold, it propagates throughout the network via SMB exploits
3
The malware manipulates WMI for persistence and Mimikatz to steal system credentials
01
10
0101000
****
****
4
It also manipulates scheduled tasks for triggering malware executables

Safety Recommendations

- Keep all your devices including your OS updated and patched for the latest vulnerabilities
- System administrators should regularly check the event logs for any anomalous activities
- ALL systems in the network should have a reputable enterprise security suite, such as K7 Endpoint Security, installed and kept updated
- Ensure to quickly respond to critical cybersecurity infrastructure alerts. Also make sure all other alerts are acted upon and resolved ASAP

Vulnerabilities Galore



Despite myriad efforts from the device and software manufacturers to offer glitch-free solutions, vulnerabilities do and will continue to exist. The easy availability of search engine tools like Shodan is helping the threat actors to hunt down vulnerable systems that can be exploited at will. Exploit kits are also making the job easier for the threat actors.

In Q3_2020-21, the visibility of vulnerabilities across platforms was grimmer than ever. Besides the operating systems and application software, the device firmware also had their fair share of glitches which were exploited and monetised by the threat actors. Let’s take a look at the most salient vulnerabilities spotted during the period.

SUNBURST Backdoor - Supply Chain Attack

Attackers connected to a backdoor embedded in the SolarWinds' Orion Platform software allowing them to compromise the server on which the Orion products run. A majority of the impacted systems are present in private networks.

Sunburst Backdoor

Supply Chain attack

Presence in India

Prevalance data from Shodan (estimated)

55

Exists in

SolarWinds Orion Platform

Severity

☠ Critical

Technologies

Orion Platform 2019.4 HF5, version 2019.4.5200.9083

Orion Platform 2020.2 RC1, version 2020.2.100.12219

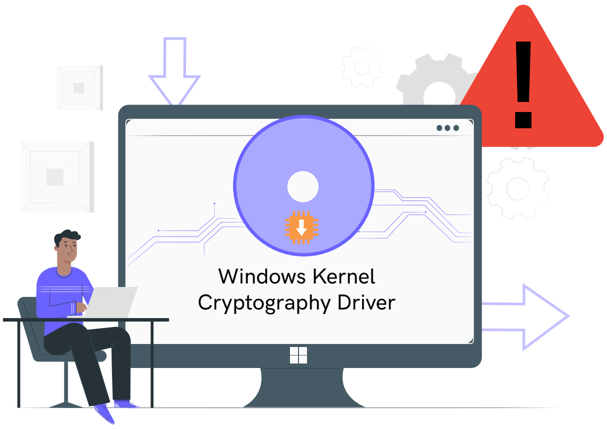
Orion Platform 2020.2 RC2, version 2020.2.5200.12394

Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432

Ghost Join Vulnerability in Cisco Webex Meetings

The vulnerability **CVE-2020-3419** in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to join a Webex session without appearing on the participant list. This vulnerability is due to improper handling of authentication tokens by a vulnerable Webex site.

All Cisco Webex Meetings sites prior to November 17, 2020, Webex Meetings 40.10.9 and earlier for iOS and Android, Webex Meetings Server 3.0MR Security Patch 4 and earlier and 4.0MR3 Security Patch 3 and earlier are vulnerable to this.



Privilege Elevation Vulnerability in Windows Kernel

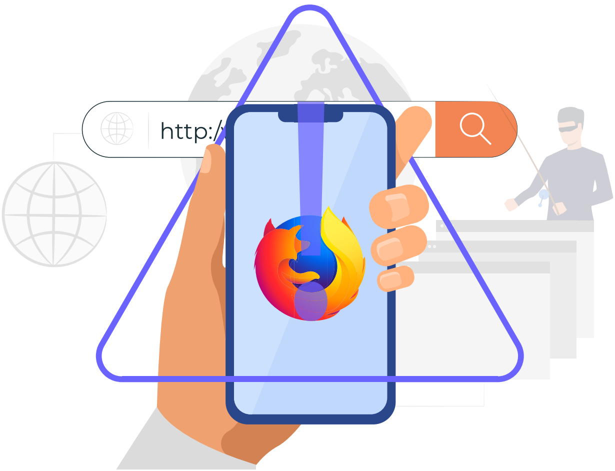
The integer overflow vulnerability, **CVE-2020-17087**, in Windows Driver leads to local privilege escalation and sandbox escape which is due to the way the Windows Kernel Cryptography Driver (cng.sys) processes input/output control.

This affects all Windows versions up to Windows 10.

File Stealing Vulnerability on Firefox Browser

The vulnerability **CVE-2020-15647** in Firefox for Android allows attackers to steal cookies and local files. This is due to the way Firefox uses 'content://' URIs.

It affects all Android users using Firefox versions prior to v68.10.1.



RCE Vulnerability in Windows SMB

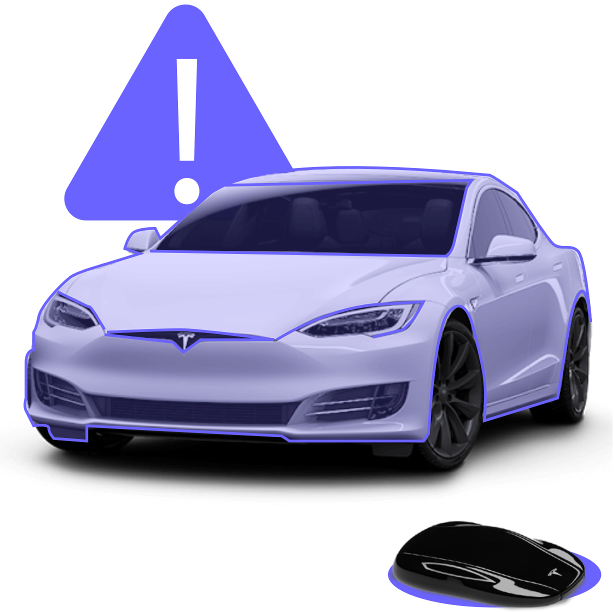
A remote code execution (RCE) vulnerability, **CVE-2020-17096**, exists in Windows SMB v2 drivers. Perpetrators could trigger this vulnerability via specially crafted requests and achieve privilege elevation for local users or remote code execution (RCE) for remote users.

It affects all Windows operating system versions.

BACK TO CONTENTS

Danger In The Internet Of Things

Besides the vulnerabilities mentioned above, the adversaries were equally active, finding the gaps that exist on IoT devices, waiting to be exploited for intruding into the target networks. During this period too, there were a series of vulnerabilities on various IoT platforms.



Keyless Entry System Vulnerabilities on Tesla Cars

Major security flaws were discovered in the Tesla Model X keyless entry system. The first vulnerability was identified in the key fob where the Bluetooth Low Energy (BLE) interface allows remote updates for the software running on the BLE chip. The second vulnerability was in the implementation of the pairing protocol between the key fob and the car.

All Tesla Model X cars have been affected by this.

BleedingTooth Vulnerability

Cybersecurity researchers have also found out a vulnerability on BlueZ, which is a Linux Bluetooth Stack. Dubbed BleedingTooth and having a CVE identity of **CVE-2020-12351**, this gets triggered due to improper input validation in BlueZ, and could thereby allow an unauthenticated user in range to potentially enable privilege escalation.

It impacts all devices with Linux kernel versions that support BlueZ.

RTA Vulnerability

CVE-2020-25159 is a stack overflow vulnerability that was discovered in the Real Time Automation's (RTA) 499ES Ethernet/IP (ENIP) stack which is one of the most widely used ICS protocols. Successful exploitation of this vulnerability could cause a denial-of-service condition, and a buffer overflow may allow remote code execution.

This vulnerability affects all RTA's ENIP stack versions prior to 2.28.

Mitigation Techniques

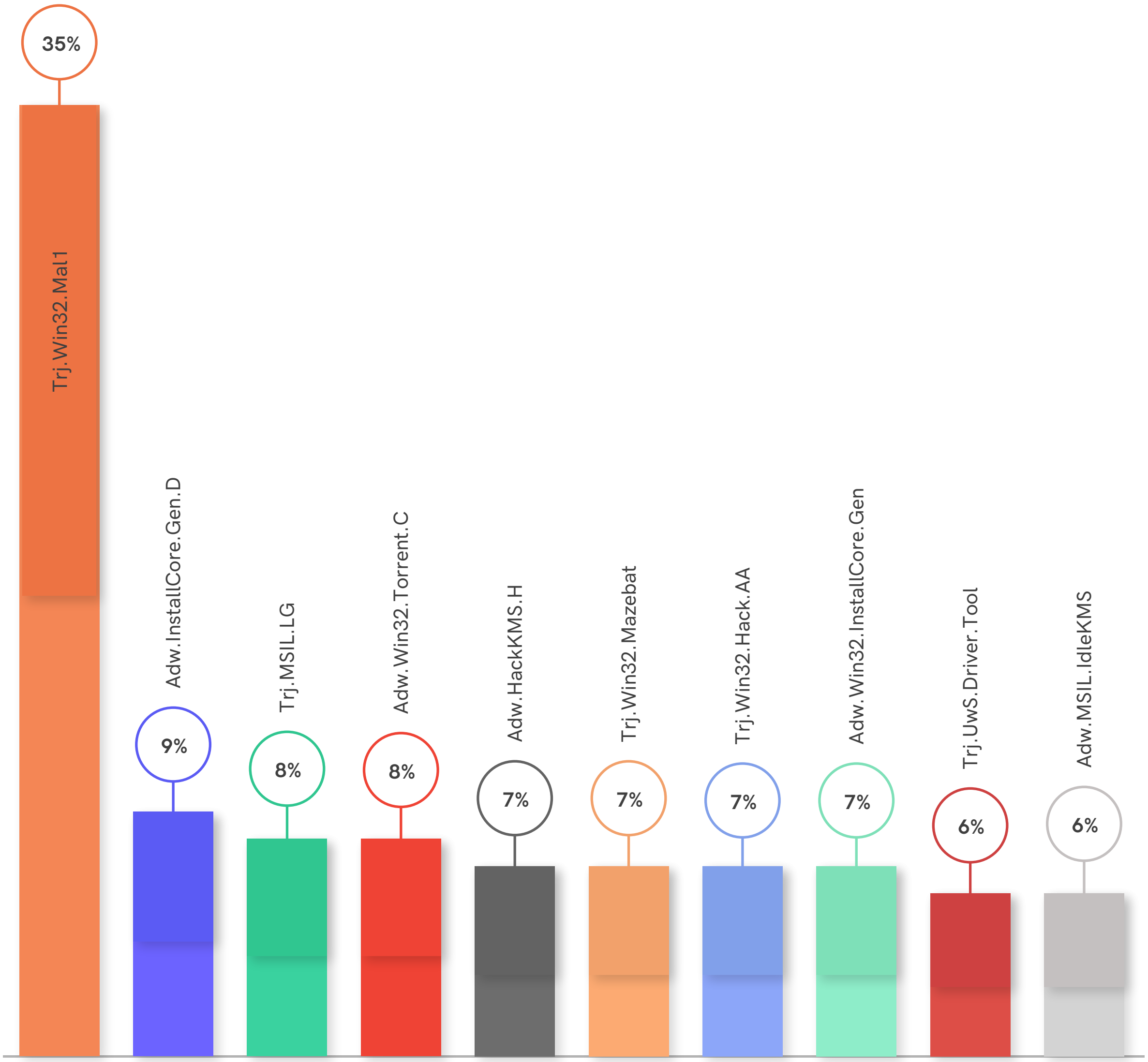
- Ensure all your devices are kept up-to-date and patched for the latest vulnerabilities
- Reconfigure your default settings so that attackers cannot easily guess or brute-force access
- Deactivate unused features and services to reduce the attack surface for cybercriminals

Windows Under Siege

Windows Malware Type Breakdown

In the third quarter of the financial year 2020-21, Trojans remained a colossal force, while adware subsisted together, minting money via exploiting the victims

Split of Windows Top 10 Detections

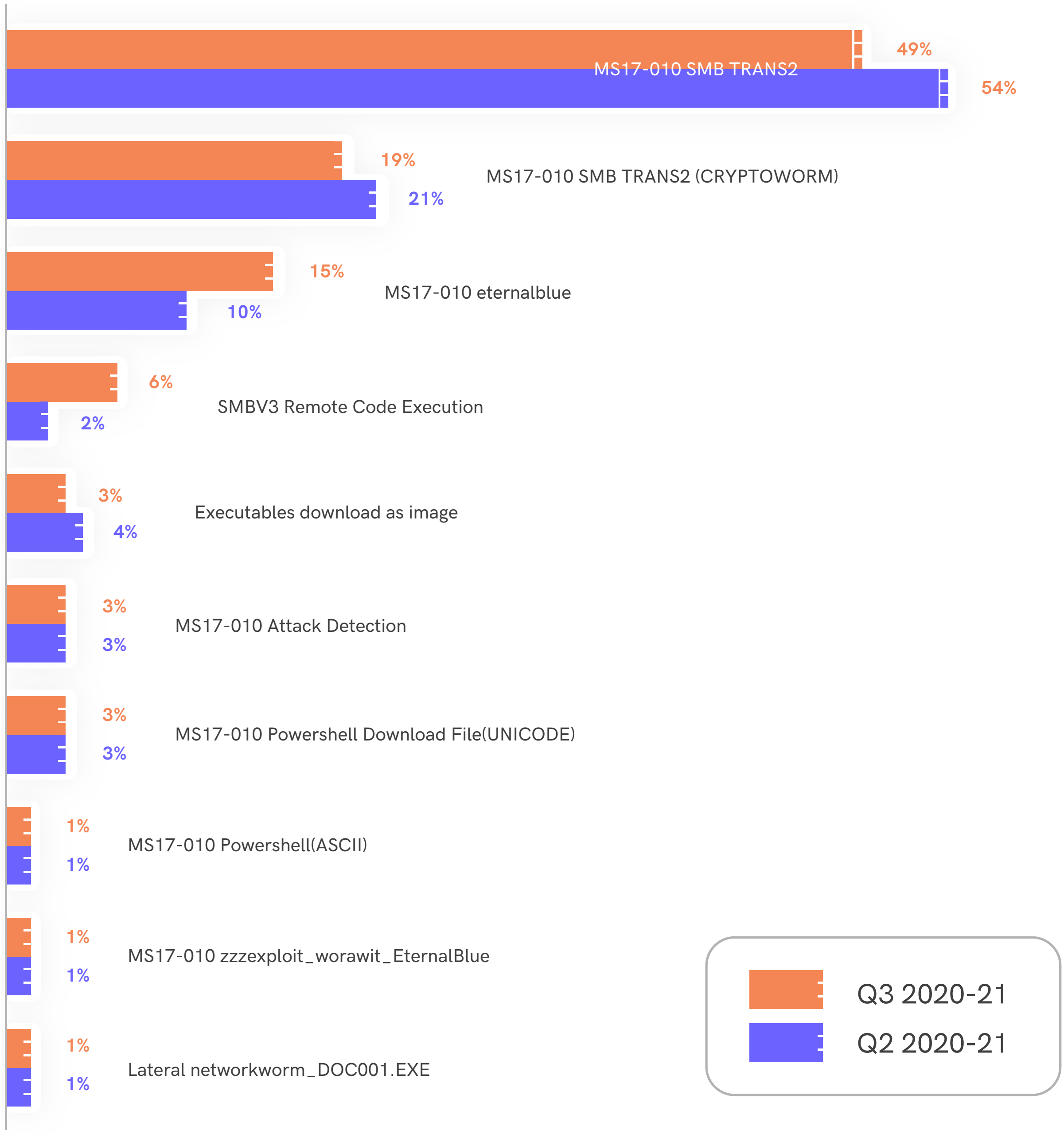


Trj.Win32.Mal1 has remained the most active Trojan family, while others haven't managed to reach double-digit presence.

Windows Exploits

Microsoft Windows is known to be potentially vulnerable. Though Microsoft releases patches on a regular basis, threat actors keep finding more and more vulnerabilities which can be exploited. This quarter too, MS17-010 SMB TRANS2 has been the most prevalent. Apart from this particular exploit, other SMB-based vulnerabilities including Eternal-Blue still rule the roost, hinting at the laxity of users in securing their systems by failing to apply the relevant patches.

Most Prevalent Exploits



Mitigation Tips

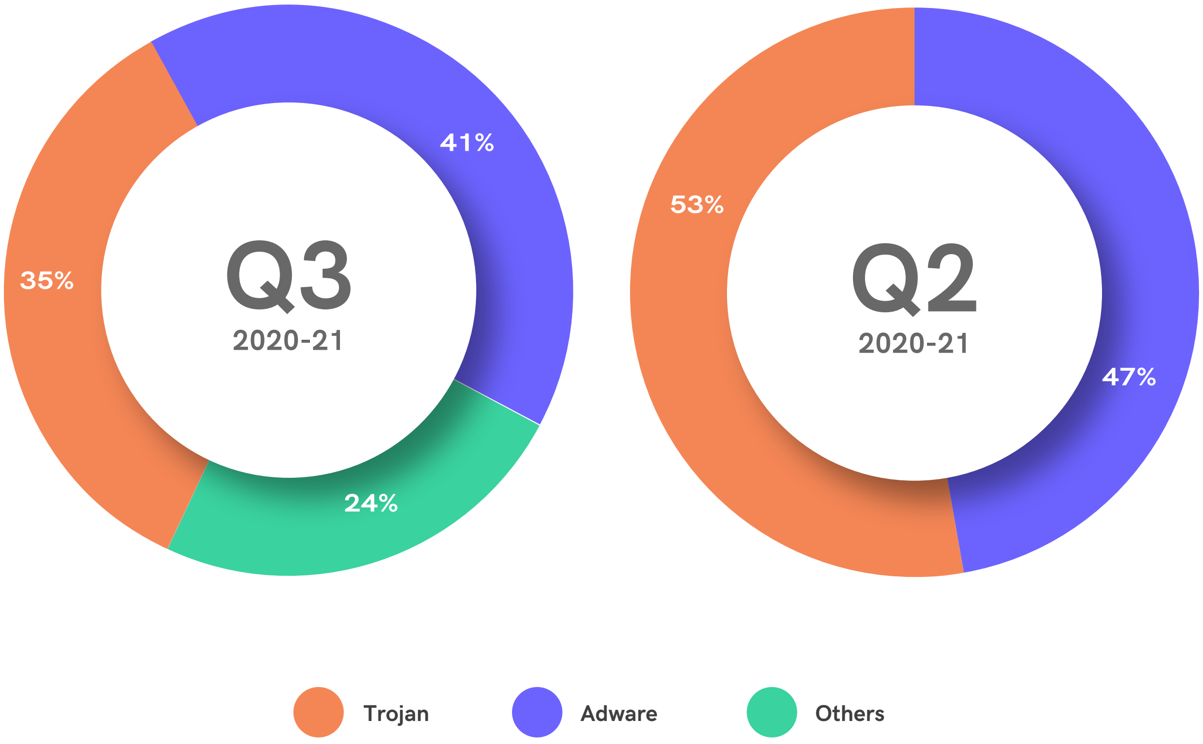
- Follow principle of least privilege
- Ensure to properly log, monitor and remediate threat events
- Effective cybersecurity training program should be in place

The Mobile Device Story

The year 2020 had been a tumultuous year for the experts and teams concentrating on mobile security. Many new or reincarnated malware have maneuvered various social engineering and deception techniques to make their way into the official and third-party app stores.

However, the proportion of adware and Trojans has seen a decline in comparison to the previous quarter. This however does not mean users are safer than before, considering the fact that there is a portion of threats that have not been classified clearly but still occupies a significant proportion of the threats seen.

Adware vs Trojan Proportional Split

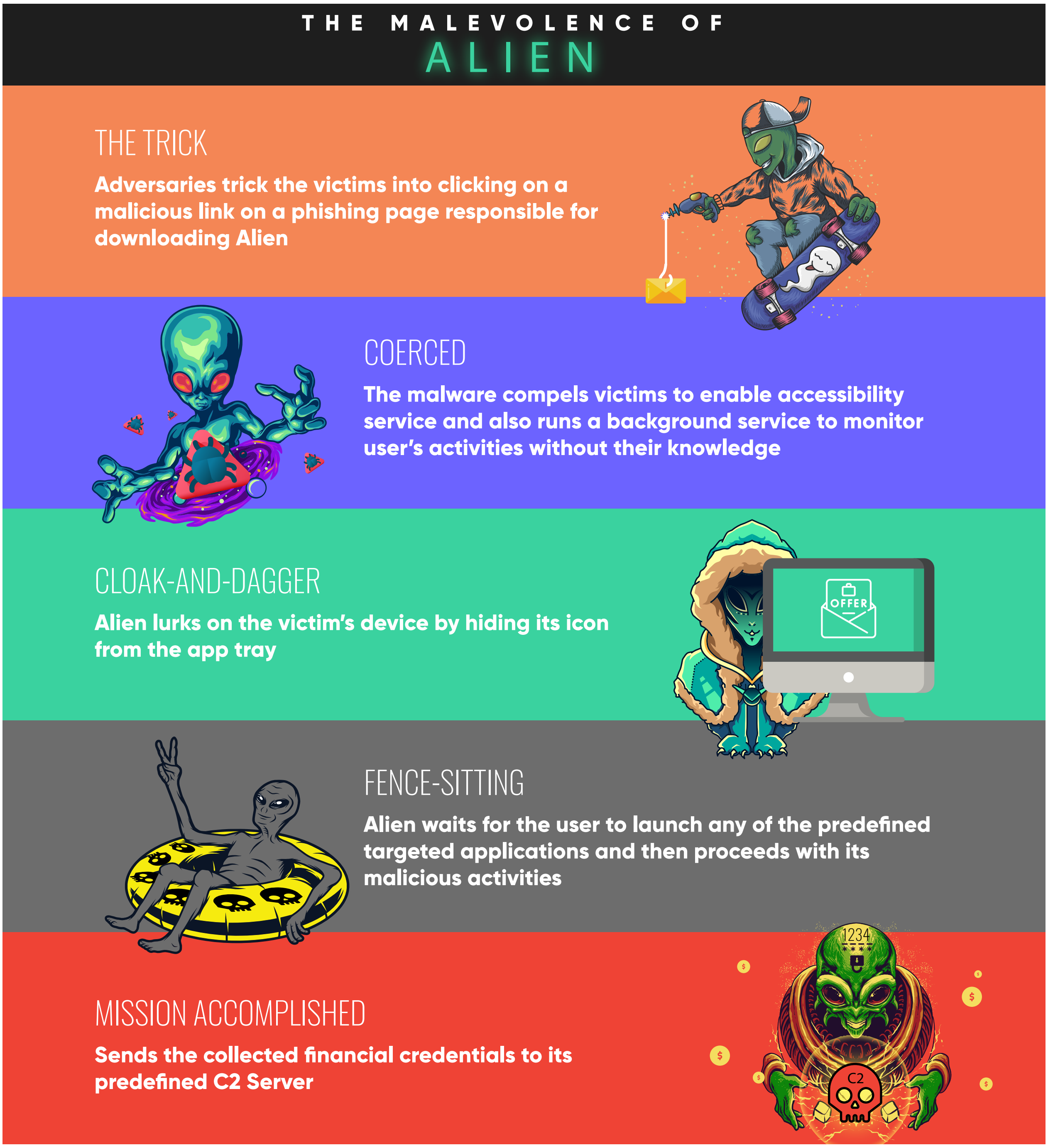


The threat actors have become smarter and are developing further intrusion and obfuscation techniques to thwart malware detection methods. As a result, the definition of traditional malware is getting blurred, unleashing a new generation of threats over the threat landscape.

Case Study: The Malevolence of Alien

During the period, Alien, the infamous and parasitic child of Cerberus, continued the mayhem by stealing banking credentials, executing screen overlay attacks, disabling Google Play Protect, intercepting messages, retrieving device information, harvesting the contact list among many other malicious activities. Some of the targeted applications in India are apps of Indian banks such as Axis bank, ICICI Bank, Indian Bank, HDFC Bank, to name a few.

The kill-chain is as depicted below:



THE MALEVOLENCE OF ALIEN

THE TRICK

Adversaries trick the victims into clicking on a malicious link on a phishing page responsible for downloading Alien

COERCED

The malware compels victims to enable accessibility service and also runs a background service to monitor user's activities without their knowledge

CLOAK-AND-DAGGER

Alien lurks on the victim's device by hiding its icon from the app tray

FENCE-SITTING

Alien waits for the user to launch any of the predefined targeted applications and then proceeds with its malicious activities

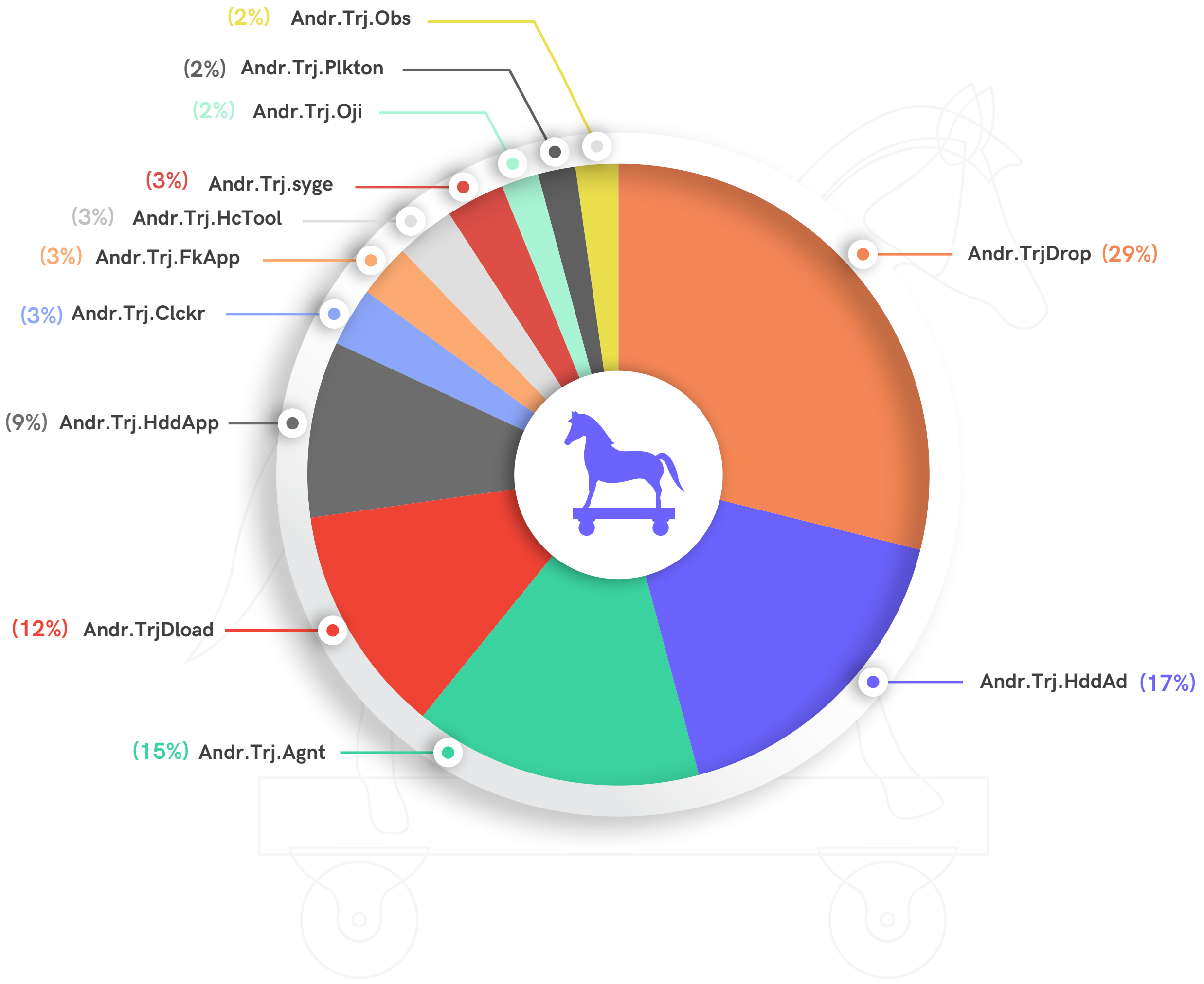
MISSION ACCOMPLISHED

Sends the collected financial credentials to its predefined C2 Server

The Ubiquitous Trojans

Exploiting the fear, panic, and misinformation caused by the ongoing Covid-19 pandemic, adversaries have potentially triggered various Trojans via manipulating legitimate apps. During the third quarter of 2020-21, we found a plethora of ransomware, information stealers, fake installers and many more.

Most Prevalent Trojan Types

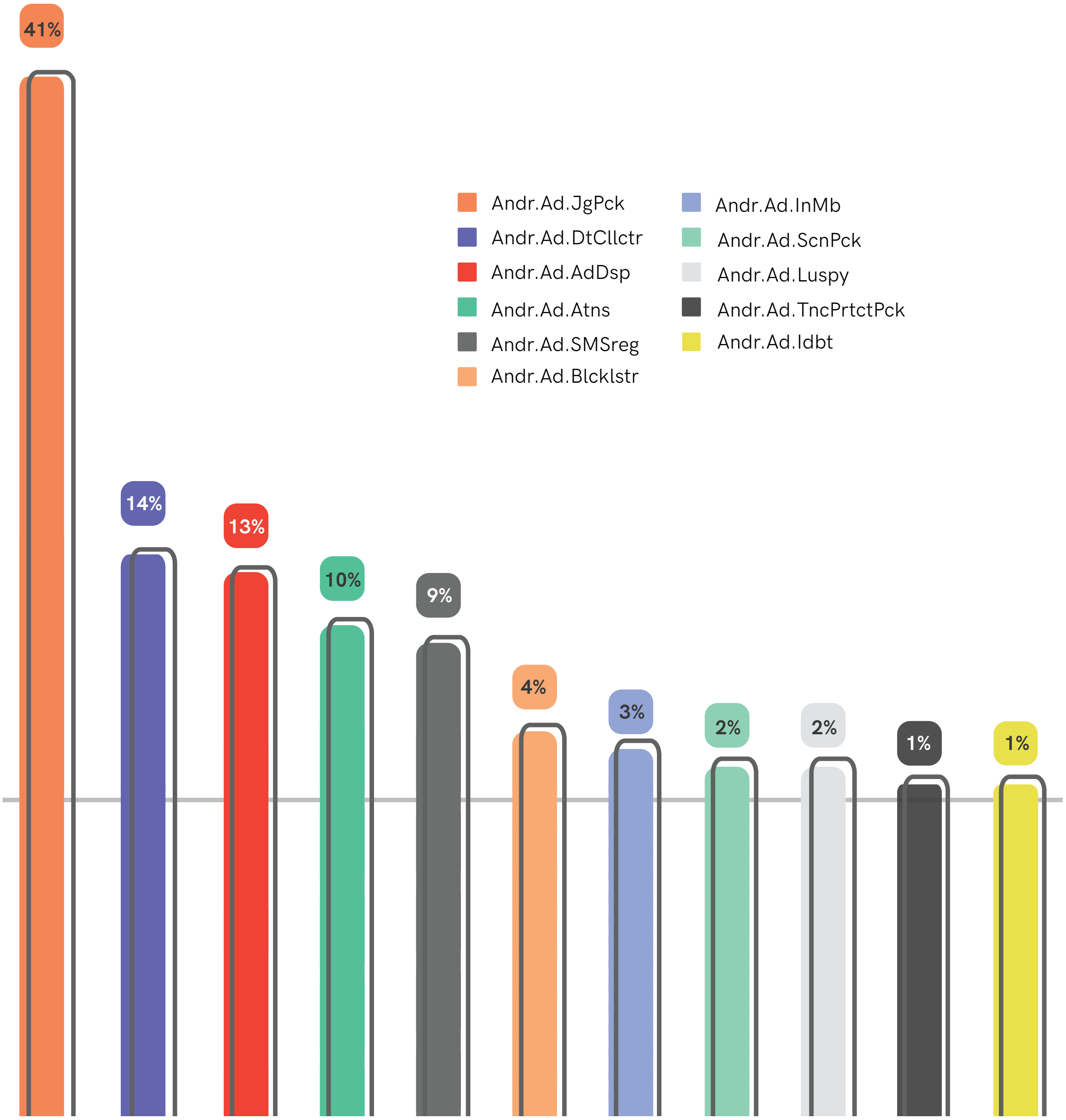


The most noticeable observation during 2020-21 was the static presence of the top three prevalent Trojan families across quarters. The statistics hint that the scenario has remained essentially unchanged with slight modifications to outsmart the target victims.

The Significance of Adware

Besides mass producing several Trojans and other malware, perpetrators also spent effort in developing adware to swindle users and generate funds by pushing advertisements without authorisation.

Trend Line Showing the Adware Plague



Interestingly, in this quarter too, Andr.Ad.JgPck topped the chart.

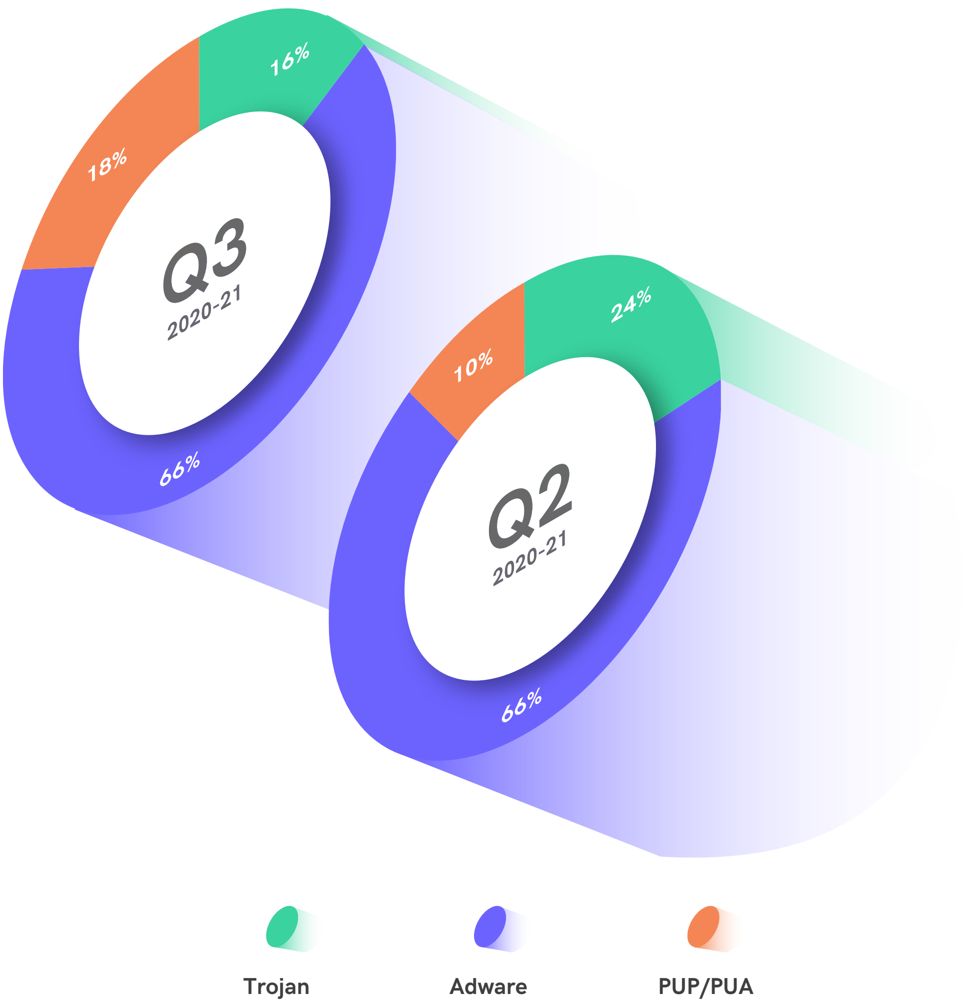
Tips to Stay Safe

- Do not click on any unknown links, especially short links, that you are not sure of
- Check if the link starts with "https://" and also ensure you are clicking on the right link before sharing any banking related information
- 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

As we are still trudging through the colossal disruption spawned by the ongoing Covid-19 pandemic, the threat landscape is getting as clear as day. Perpetrators have been repeatedly targeting the users who have increased their online presence these days.

Adware, Trojan & PUP Proportional Split



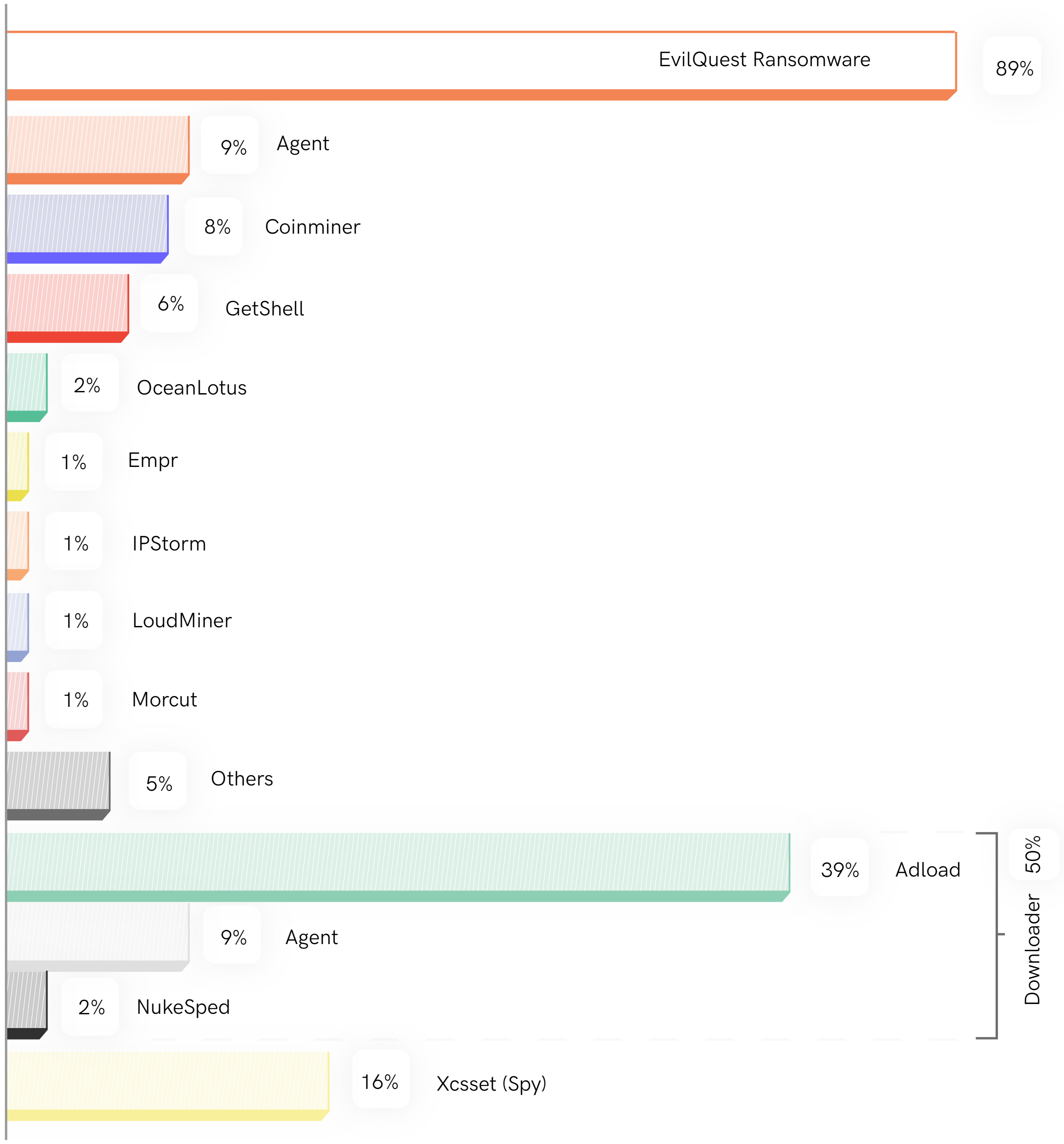
*The Trojan percentage for Q2 and Q3 does not include EvilQuest, as it has the major share which could skew the results

From the comparison chart, we can see a decline in the proportion of Trojans this quarter. This does not, however, mean that the Mac threat landscape was safe from Trojanized attacks as can be seen from the footnote.

The Trojan Brouhaha

In Q3_2020-21, we see an innumerable variety of Trojans serving different malicious intent.

Trojan Detection Trend Lines

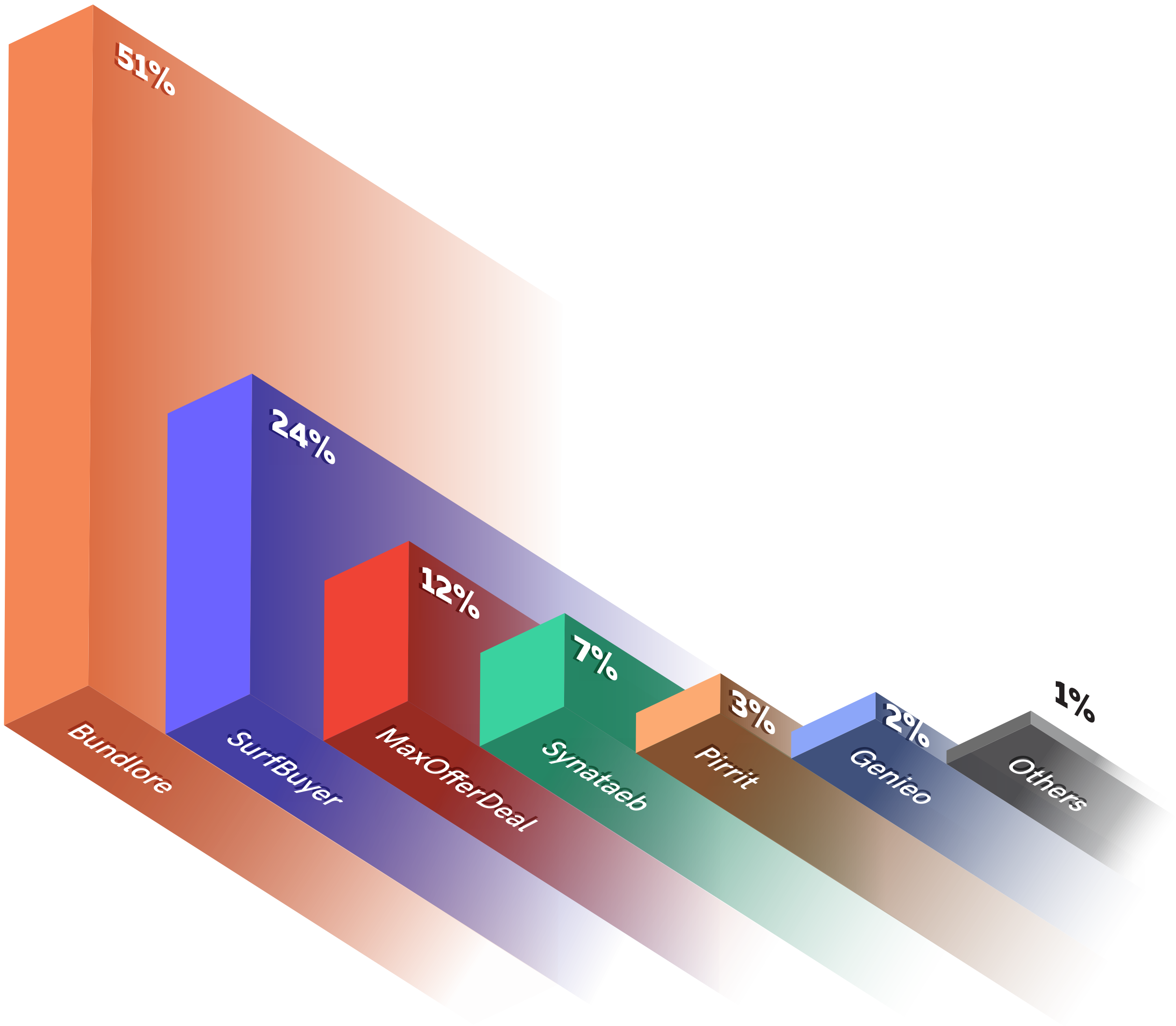


Excluding EvilQuest ransomware which occupied a significant place, the category was primarily occupied by many downloaders, spyware and coinminers.

The Upsurge of Adware

Adware has managed to keep its firm presence in the macOS threat landscape for the past few quarters. This quarter is no different and we are sure the next wouldn't be either.

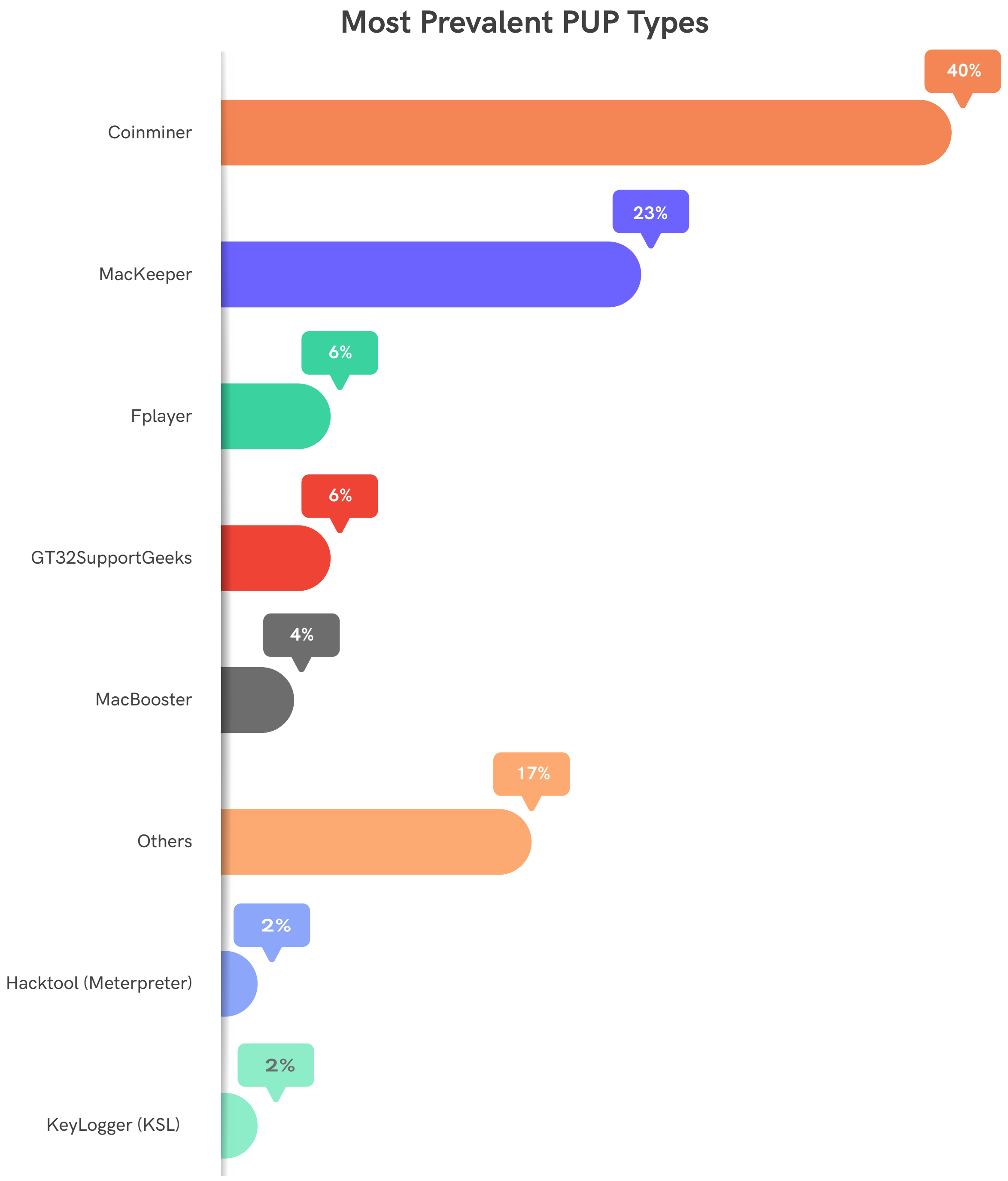
The Trend Line of Adware Variant Detections



Bundlore is the most prevalent this time too. This adware not only displays unwanted advertisements for monetizing purposes but also installs products offered by affiliates.

The Pulse of PUP

Despite the significant presence of adware on the macOS threat landscape, the PUP visibility has also heightened further this quarter. The robust app reviewing policy of the macOS developer couldn't even dent these swelling numbers.



The stats reveal the prominent presence of miners which has significantly reduced the relative statistical impact of MacKeeper.

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
- Ensure to back up all your data and make sure it is malware-free

Key Takeaways

The long list of perilous malware and vulnerabilities trends outlined in this report indicates that the threat landscape would get even more complicated with the rising number of organised, sophisticated, and well-funded cyberthreat groups. Tackling these challenges thereby becomes a herculean task for both the organisation and the individual. As a global leader in cybersecurity and having seen and mitigated a variety of threats, we have suggested a few safety measures to stay protected.

Enterprise	Consumer
Secure your devices by keeping them up-to-date and patched for the latest vulnerabilities, and protected by up-to-date, high-quality security software such as K7 Endpoint Security	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
System administrators should regularly check the logs for any unusual activities, and promptly and effectively act upon security alerts	Do not click on unknown links and links that you are not sure of
Keep your network up-to-date and patched for the latest vulnerabilities	Stay cautious and ensure you are entering your financial credentials on the correct link

BACK TO CONTENTS

K7 SECURITY

www.k7computing.com

Jan 2021