Cyber Threat Monitor Report

2020-21

K7 SECURITY

Contents

Contents

Be Cyber Safe in this Unpredictable World

The pandemic has changed the way one looks at cybersecurity. Cybersecurity also has undergone a rapid transformation within a few months of the start of the pandemic. This can be attributed mainly to the evolving threat landscape wherein threat actors have quickly adapted to the adoption of remote working by organizations.

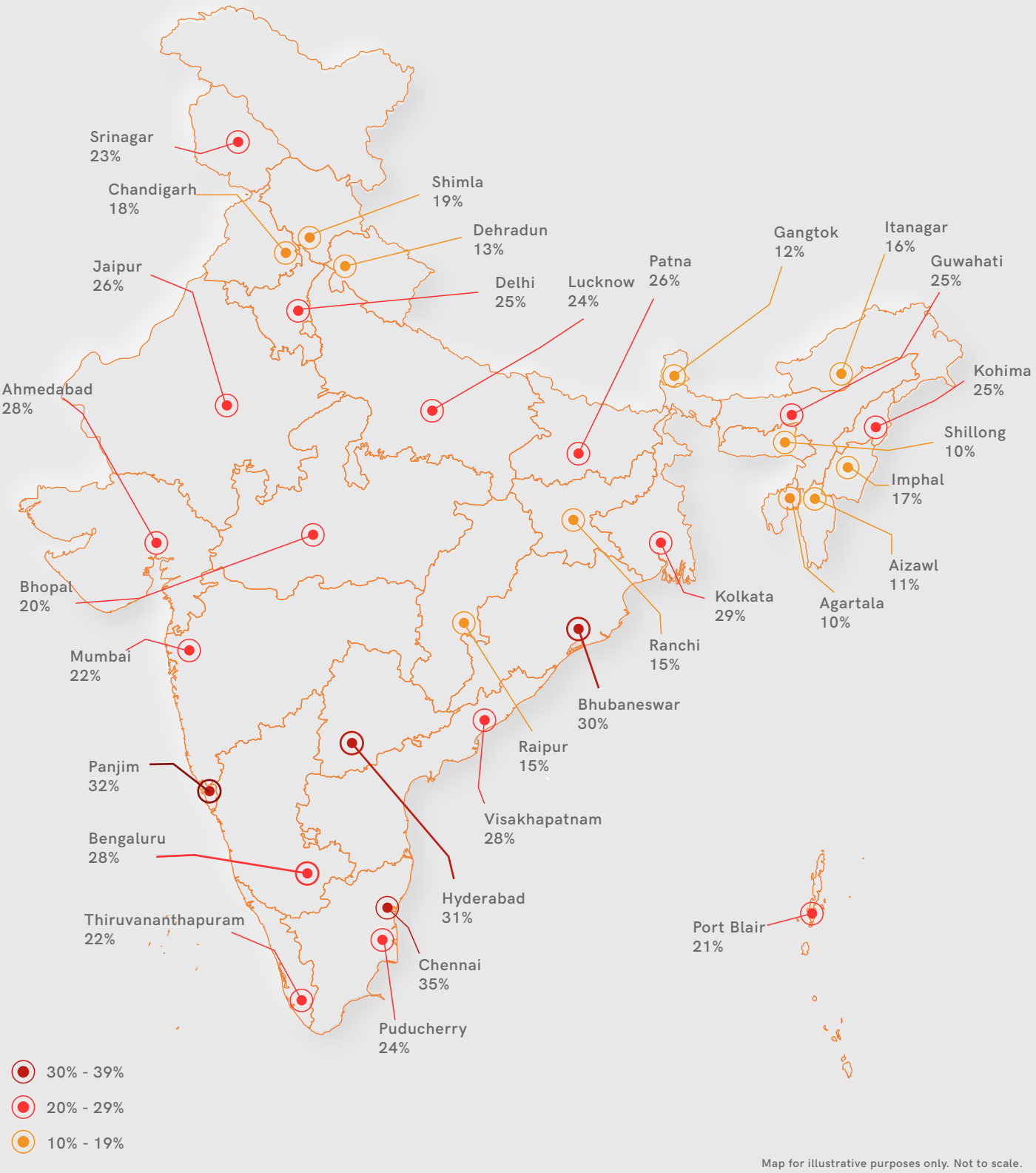
Of late, there has been an increase in both targeted and random attacks and threat actors are leaving no stone unturned in finding any loopholes to exploit. It is now becoming difficult to predict in which direction the threat landscape may steer, as the threats are evolving at a much more rapid pace than the cybersecurity response from victims.

This is mainly because cybersecurity is still not given much importance among various individuals and organizations. In our country, only a very few enterprises and SMEs have good cybersecurity practices in place, making the rest susceptible to various threats.

We at K7 are offering you a snapshot of the entire threat landscape in the country via the quarterly Cyber Threat Monitor (CTM) report. Here, we share prevalent threat statistics alongside a few didactic case studies encountered by our customers through illustrative infographics. The latest CTM report would also act as a barometer to help one understand future attack trends and patterns.

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

CYBER THREAT MONITOR - INDIA



Map for illustrative purposes only. Not to scale.

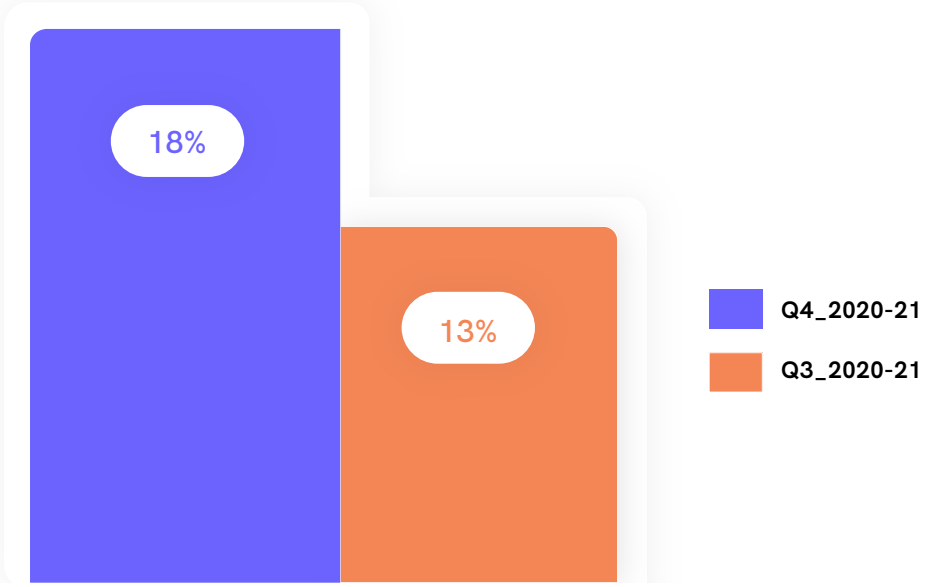
Regional Infection Profile

The modern-day perpetrators are well educated and are also in sync with new technology. They are now launching sophisticated and targeted attacks besides significantly contributing to the breach rate every quarter. Adversaries are picking and choosing the most profitable targets instead of just targeting random victims. This new trend of attacking has increased the overall infection rate.

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

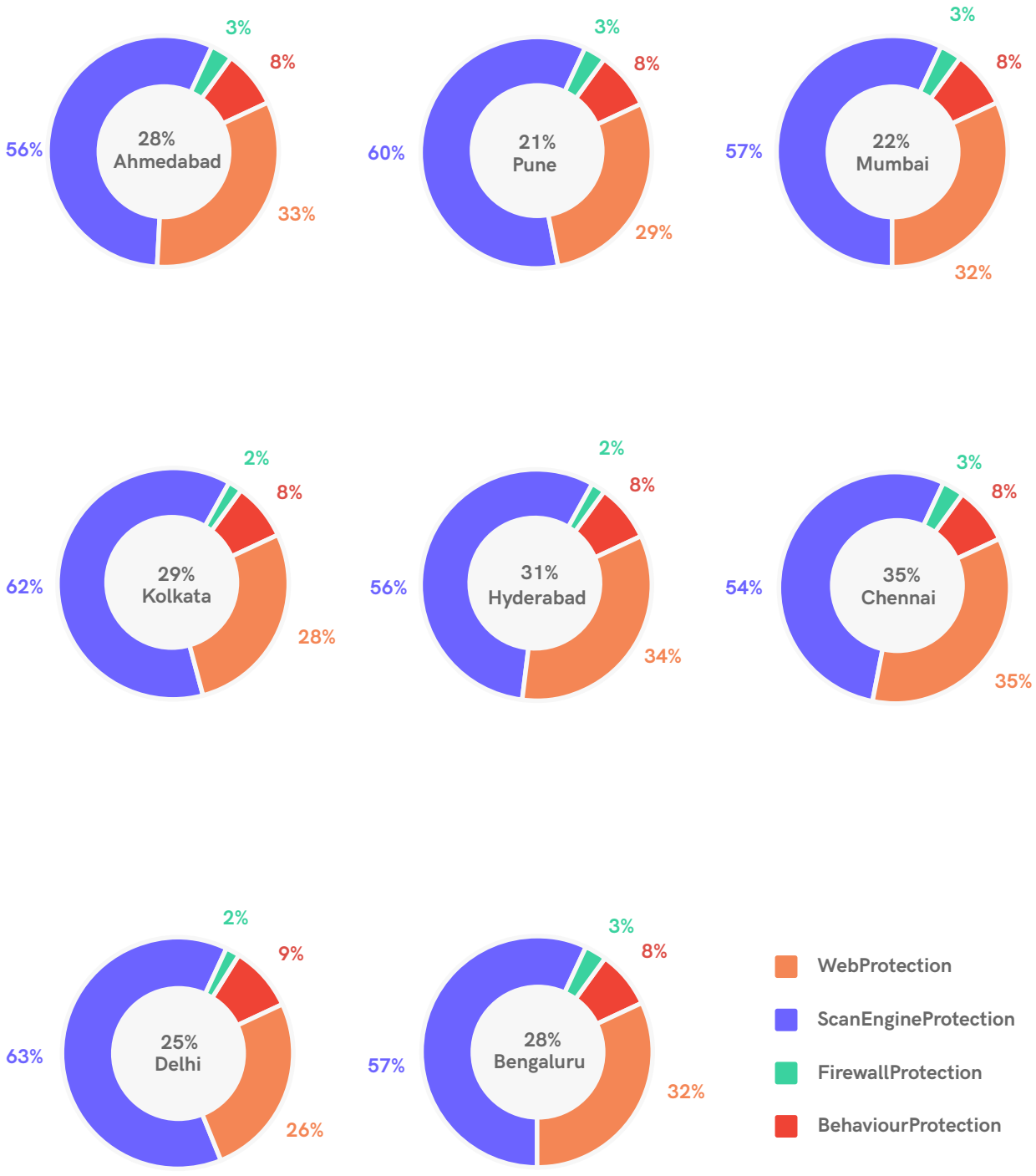
Infection Rate" (IR) of an area

The Overall Pan-India IR is given below.



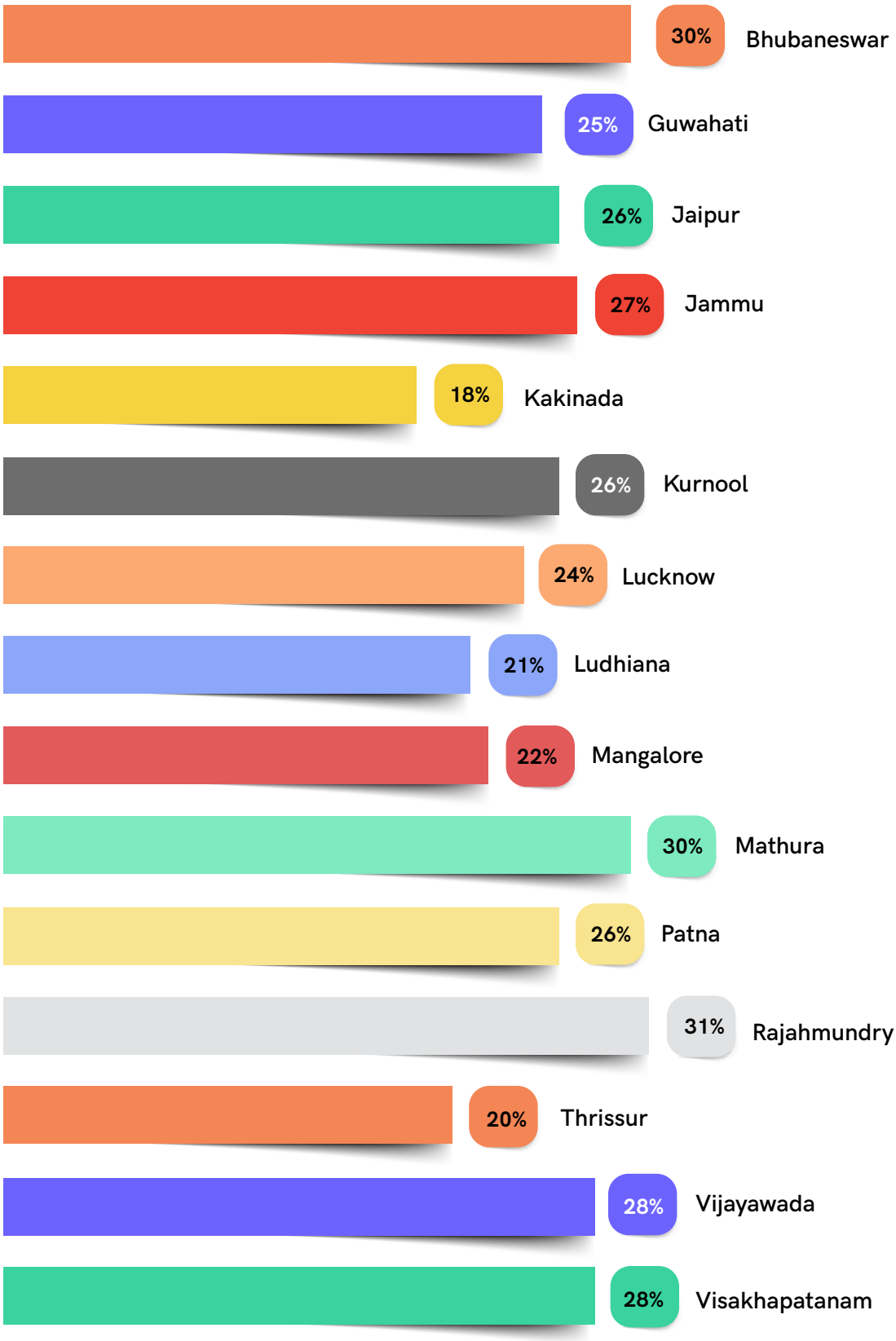
The 5% surge in the Pan-India IR conveys how the users are becoming lax towards safe cybersecurity practices. This can be seen from the increasing IR among Tier-1 and Tier-2 cities this quarter in comparison to the previous quarter.

The Metros and Tier - 1 Cities - Infection Rate



Threat actors are still using old techniques such as phishing emails and socially-engineered malware downloads, among others, as their infection vector. Users who do not practice safe cyber hygiene practices are more vulnerable and fall prey to the evil intentions of the threat actors. This quarter saw an increase in IR in almost all the Tier-2 cities which can be attributed to the laxity of the users.

Top 15 Infection Rates in Tier-2 Cities



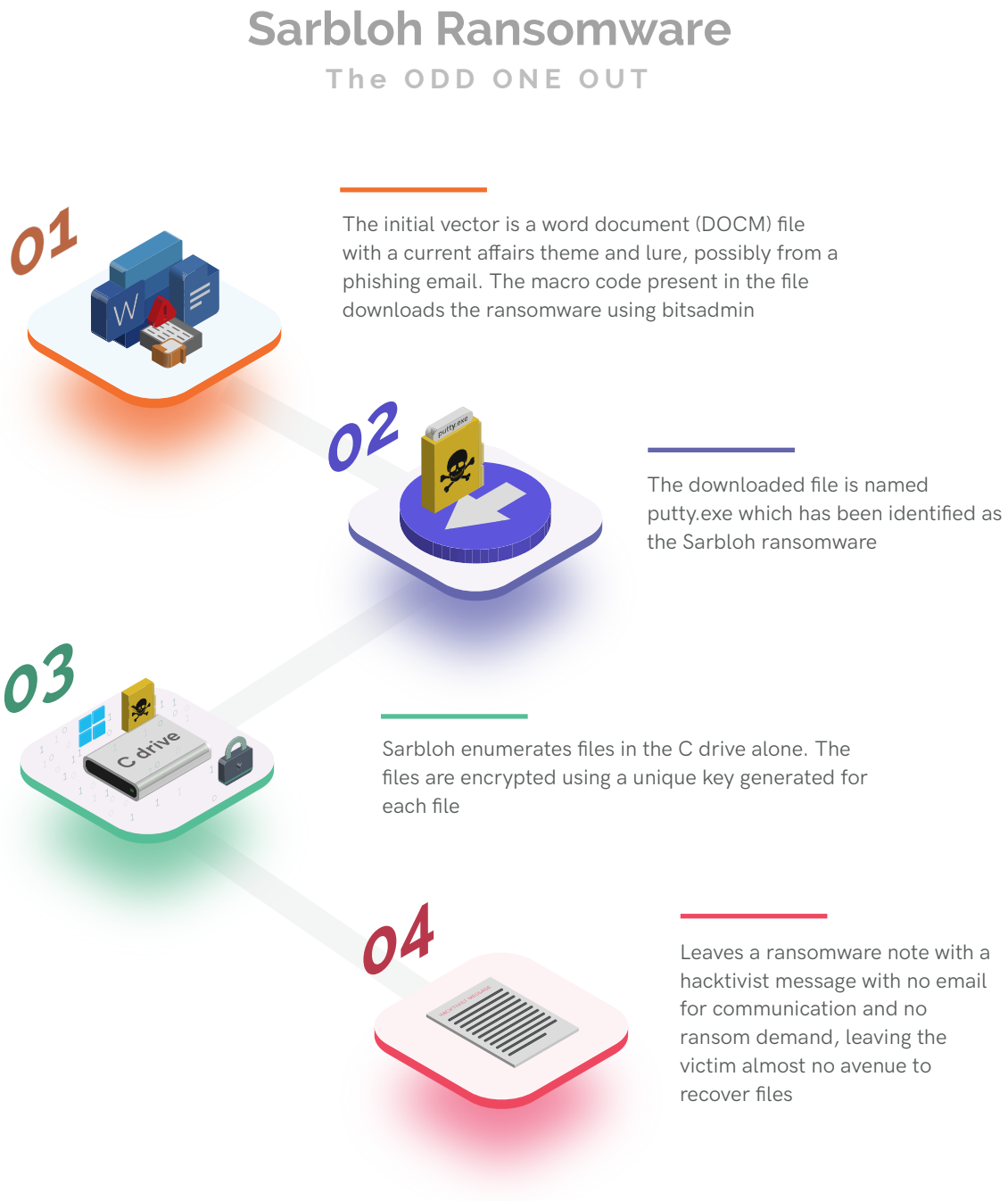
BACK TO CONTENTS

Enterprise Insecurity

In recent years, ransomware attacks have become the rage in terms of attacks on enterprises, hospitals, universities, governments, and even individuals. Modern threat actors have either developed new ransomware or refurbished older ones. The new age ransomware implements more detailed reconnaissance methods, sophisticated encryption algorithms, attacks more file types, exploits more vulnerabilities, is targeted, and also available in a Ransomware as a Service (RaaS) business model. There was also a client incident noticed this quarter wherein, apart from the ransomware payload, threat actors also used the machine to mine cryptocurrency. Let's now delve into the incidents.

Case Study 1: Sarbloh Ransomware - The ODD ONE OUT

In this quarter, we at K7 Labs came across a new ransomware dubbed **Sarbloh** whose kill-chain has been given below. What is unique about this ransomware is its **NO RANSOM** agenda, an attempt at political hacktivism instead.



Case Study 2: The Twinsword – Ransomware and Cryptojacking Together

Recently, we at K7 Labs received an incident submission wherein the attacker dropped the LockBit ransomware onto the client's machine apart from using their machine to mine cryptocurrency.

The sequence of events is outlined below:

THE TWINSWORD:
Ransomware and Cryptojacking Together

1

Attacker brute-forces RDP in the client's machine for the usernames 'administrator' and 'admin'

2

The attacker uses tools for AV evasion such as ProcessHacker and does further reconnaissance using tools like Mass Scanner and NLBrute

3

Finally, the attacker drops the LockBit ransomware payload and encrypts the files on the client's machine

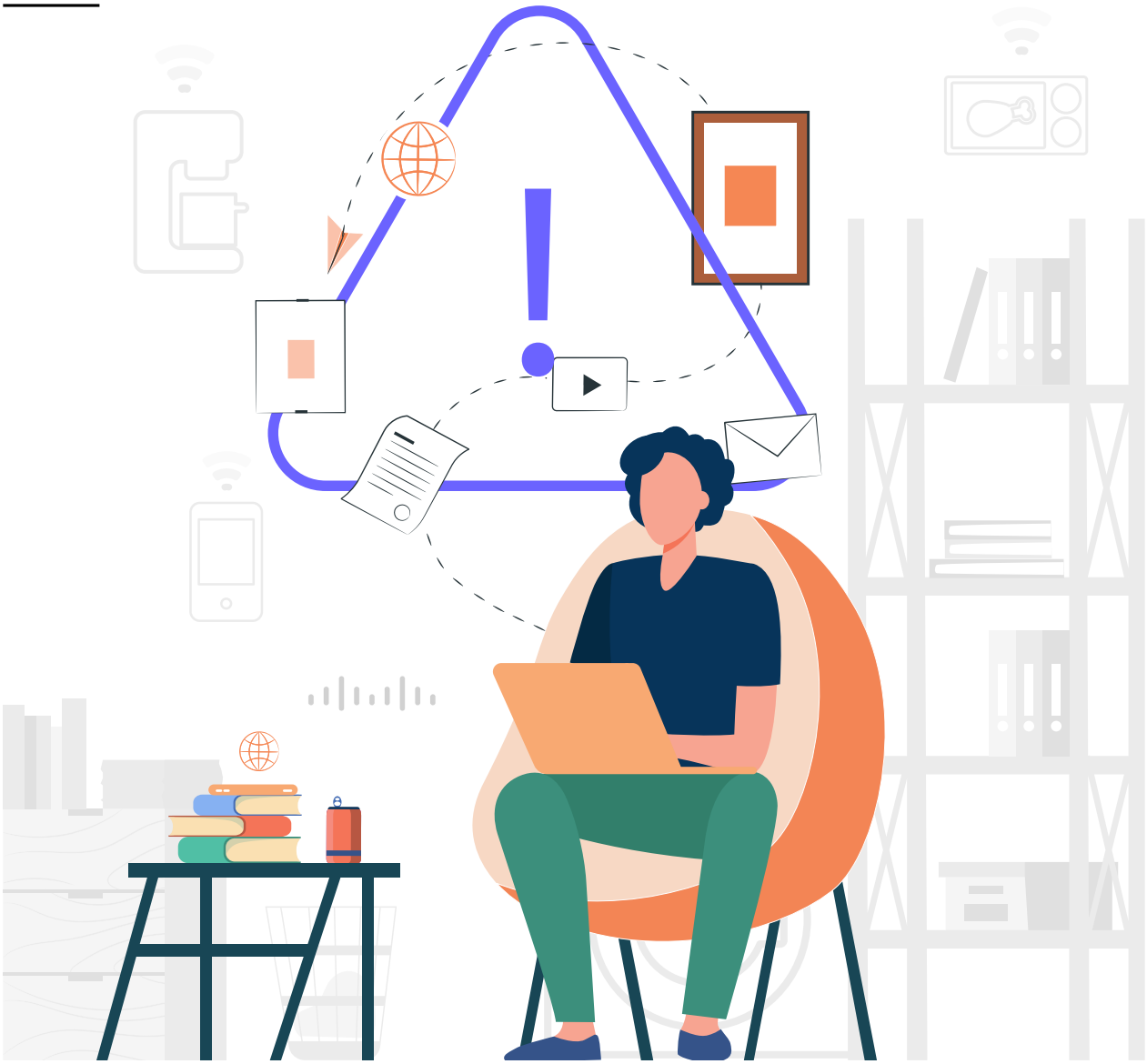
4

The attacker also drops XMRig miner and uses the client's resources for mining Monero cryptocurrency

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

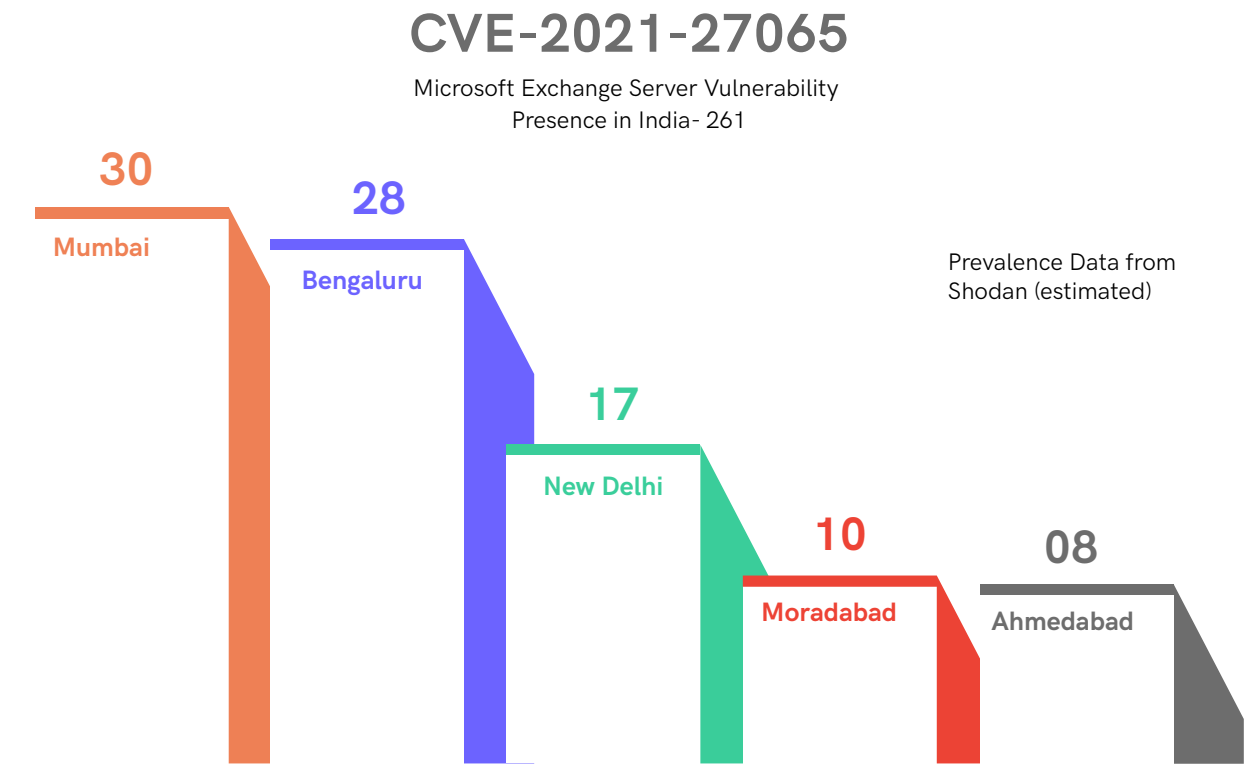


The rapidly evolving threat landscape has taught many enterprises to take digital security concerns, soaring every day, seriously. The reason behind such an exponential growth is mainly due to the unpatched vulnerabilities.

In Q4_2020-21, we saw many such vulnerabilities that helped the adversaries launch refurbished or new attacks. Here is an insight into the most prevalent vulnerabilities glooming over this quarter.

Microsoft Exchange Server Vulnerability

Four zero-day vulnerabilities were reported this quarter in Microsoft Exchange Server. **CVE-2021-26855** allows an attacker to query the server with a specially-constructed request allowing an adversary to authenticate to the Exchange server. The remaining three vulnerabilities can be exploited only after successful authentication. **CVE-2021-26857** gives the ability to run code as SYSTEM on the Exchange Server. **CVE-2021-26858** allows the attacker to overwrite an existing file in the system with their data, and **CVE-2021-27065** allows an attacker who has gained access to overwrite a system file on the Exchange Server. There have been reports that these vulnerabilities have been chained and exploited by various adversaries.



Exists in	Technologies	Severity
Microsoft Exchange Server	Microsoft Exchange Server 2013, Mirrosoft Exchange Server 2016, Microsoft Exchange Server 2019	Critical

RCE Vulnerability in VMware

CVE-2021-21972, a remote code execution (RCE) vulnerability in vSphere Client's vCenter Server plugin, upon exploitation gives attackers the capability to execute commands with unrestricted privileges on the host OS.

Products impacted are VMware vCenter Server (vCenter Server) and VMware Cloud Foundation (Cloud Foundation).

Sudo Heap Overflow Vulnerability

A heap overflow vulnerability, **CVE-2021-3156**, has been discovered in Sudo which is present in most Unix and Linux based OSes. Any unprivileged user can exploit this vulnerability and gain root privileges.

The affected products are Sudo legacy versions from 1.8.2 to 1.8.31p2 and stable versions from 1.9.0 to 1.9.5p1 in their default configuration

Windows DNS Server Affected by Multiple RCE Vulnerabilities

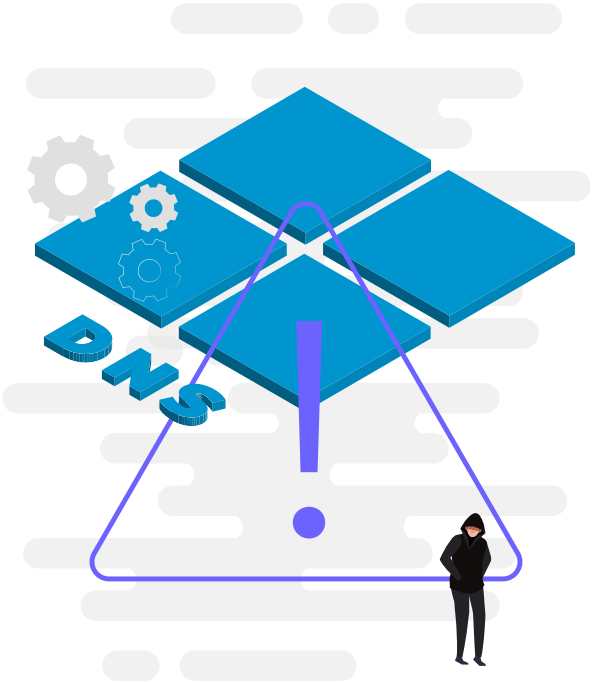
CVE-2021-24078 is an RCE vulnerability in Windows DNS Server which can be easily exploited by threat actors.

All Microsoft supported Windows Server OSes with DNS server enabled are exposed to this vulnerability.

Another RCE vulnerability, **CVE-2021-26877**, is an Out-of-Band (OOB) read vulnerability which can be exploited by updating the Zone with TXT RR that has a "TXT length" greater than the actual "Data's length".

The RCE vulnerability, **CVE-2021-26897**, can be exploited by sending consecutive Signature RRs Dynamic Updates which results in Out-of-Band (OOB) heap write.

Windows Server version 20H2, versions 1909, 2004, 2019, 2016, 2012, 2012 R2, and 2008 are vulnerable to this.



Windows Privilege Escalation Vulnerability

CVE-2021-1732, a zero-day Windows Win32k Privilege Escalation Vulnerability, has been widely exploited in the wild. On exploitation, it could be used to escape the sandbox of Microsoft IE browser or Adobe Reader to access the host OS.

The vulnerable products are the latest versions of Windows 10 and Windows Server 2019.

BACK TO CONTENTS

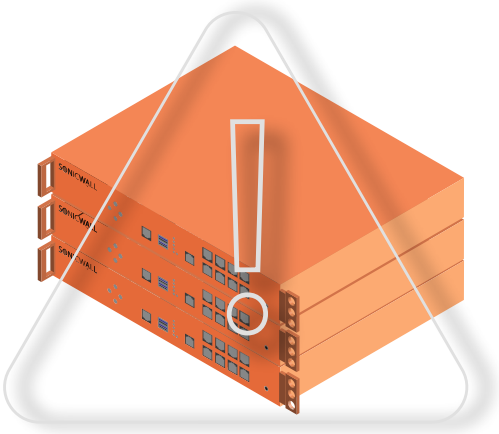
Danger In The Internet Of Things

The vulnerabilities noticed in Q4_2020-21 were potentially impacting a large number of devices as the attack surface was left wide open for the threat actors to exploit. Most users in the Internet of Things (IoT) arena were however ignorant of the approaching threats. Few significant threats have been given below.

Critical Flaws in RealTek Wi-Fi

CVE-2020-9395, a remote stack overflow vulnerability in Realtek WiFi devices, could lead to device takeover when exploited. This is due to the vulnerable RTL8195 module present on these wireless devices.

Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before v2.0.6 are vulnerable to this.



Critical Zero-Day in SonicWall SMA Devices

Security researchers have found a severe zero-day SQL injection vulnerability on SonicWall SSLVPN Secure Mobile Access (SMA) 100 series devices. **CVE-2021-20016** could get exploited due to improper neutralization of SQL commands. On successful exploitation, a remote unauthenticated attacker can gain access to the credentials on the vulnerable devices.

Physical Appliances viz. SMA 200, SMA 210, SMA 400, SMA 410 and Virtual Appliances viz. SMA 500v (Azure, AWS, ESXi, HyperV) are vulnerable to this.

Critical RCE Vulnerabilities in Netgear Switch

Severe flaws were identified in Netgear's Ethernet switch. **CVE-2020-26919** is a critical RCE residing in the switch internal management web application. Using this attackers can bypass authentication and execute code with administrator privileges.

Firmware versions prior to 2.6.0.43 are vulnerable to this.

Another critical vulnerability, CVE-2020-35220, allows the attacker to update firmware that is active by default, allowing them to upload malicious firmware updates without requiring administrative credentials.

Mitigation Techniques

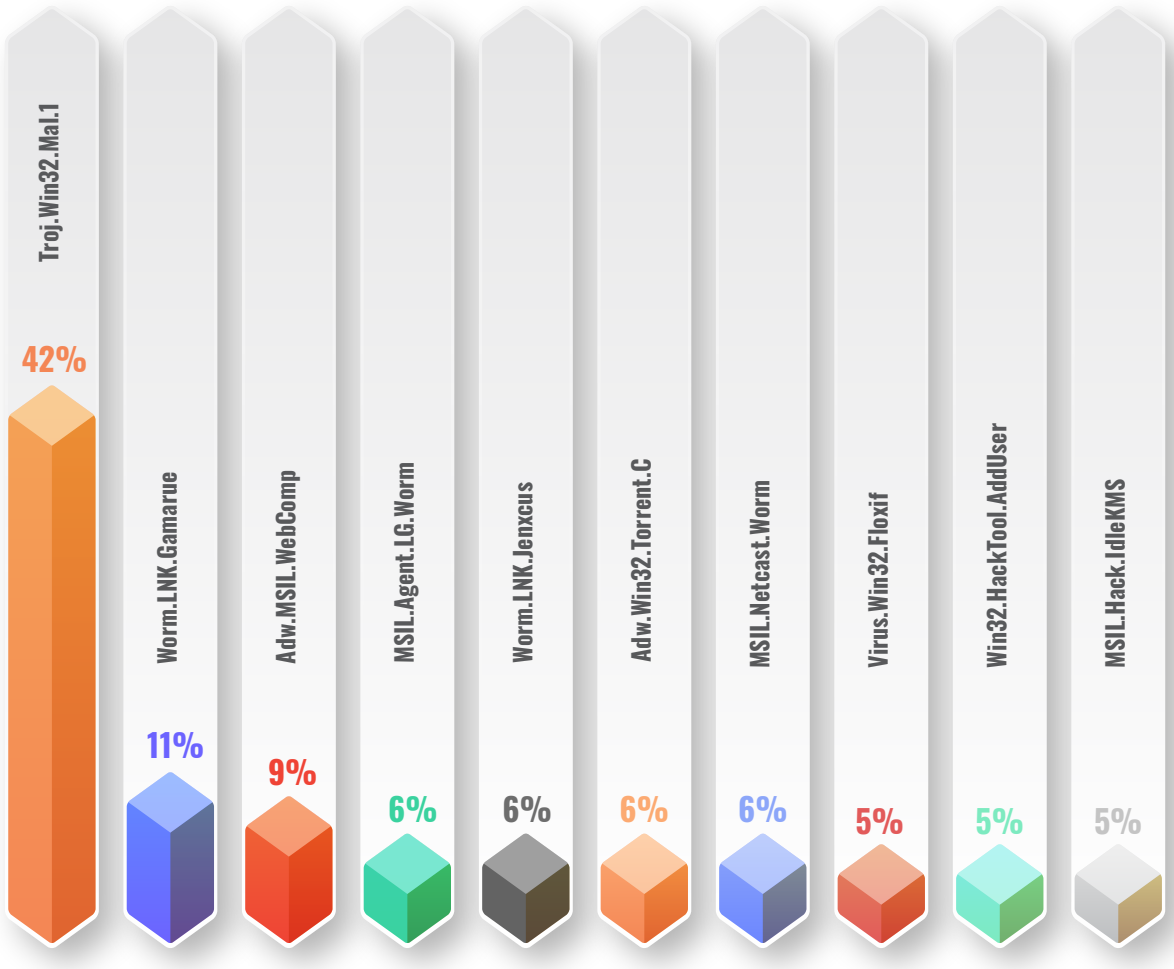
- Continuously monitor all IoT devices in your network and keep a track of their configurations
- Ensure all your devices are kept up-to-date and patched for the latest vulnerabilities

Windows Under Siege

Windows Malware Type Breakdown

Like in Q3_2020-21, this quarter also saw Trojans occupying a significant portion of the threat landscape. Adware was not so significant according to our rich K7 Ecosystem Threat Intelligence (K7ETI) data.

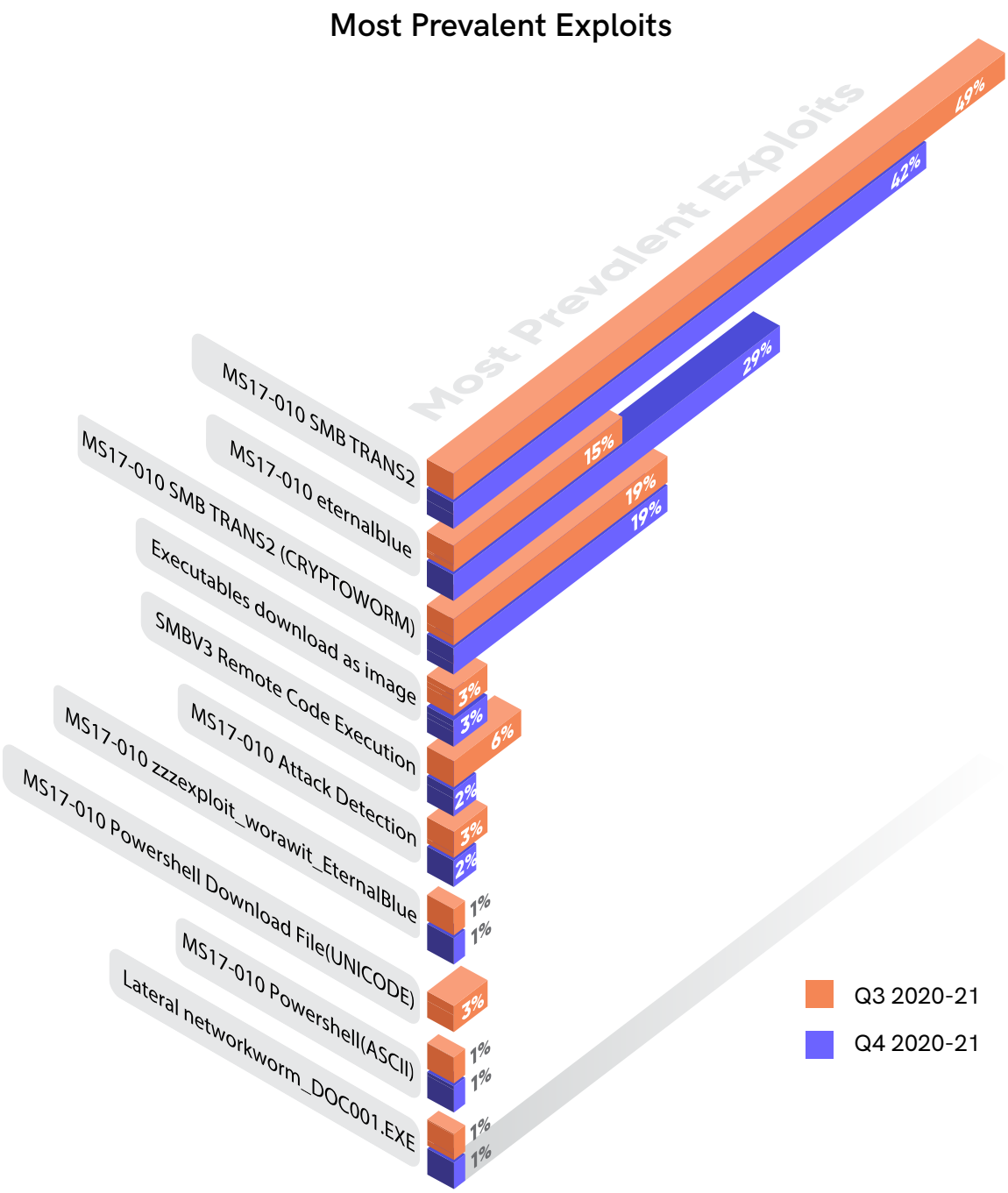
Split of Windows Top 10 Detections



Besides Trojans, this quarter also saw worms being used by threat actors to infect those users who have not protected their devices.

Windows Exploits

In this quarter, SMB exploits have diminished to some extent, however, they still remained a very significant threat that could not be ignored. Simultaneously, the EternalBlue exploit still proves to be the best bet around for the threat actors as long as users devices are still unpatched.



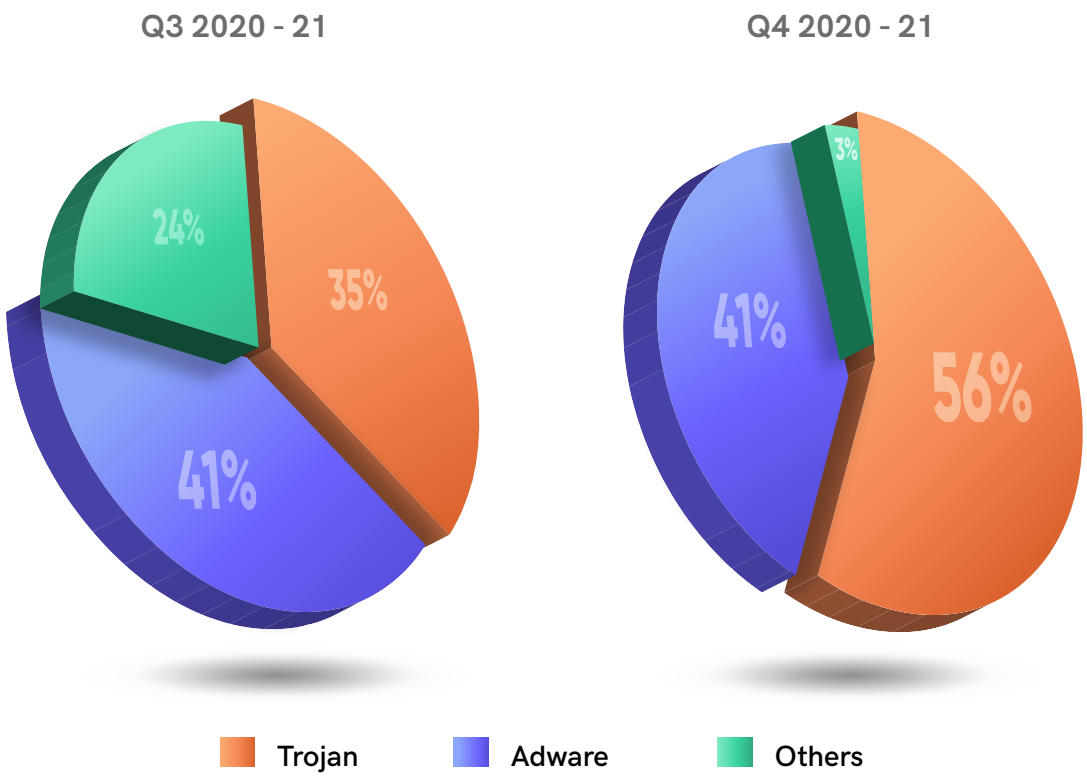
Mitigation Tips

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

The Mobile Device Story

Android has grown rapidly in the consumer space and hence has also become a significant part of the global threat landscape. In the past few years, the threat actors have increased their activity on the Android platform by rolling out numerous malware strains to exfiltrate users' private information or cause financial loss. The adversaries have manipulated the latest trends and demands as a lure to trap their victims.

Adware vs Trojan Proportional Split (%)



In this quarter, we saw a significant rise in Trojans when compared to adware. Also, there was no difference seen in the adware threat share in comparison to the previous quarter. Trojans are more targeted these days along with specific intent and capabilities and often get used as a part of multi-layer cyber attacks while adware is mainly used to earn profit for the developers. The uncategorised attacks share has also reduced to a noticeable extent, hinting that attackers are becoming very clear in their attack strategies.

Case Study: The Lure of Fake TikTok

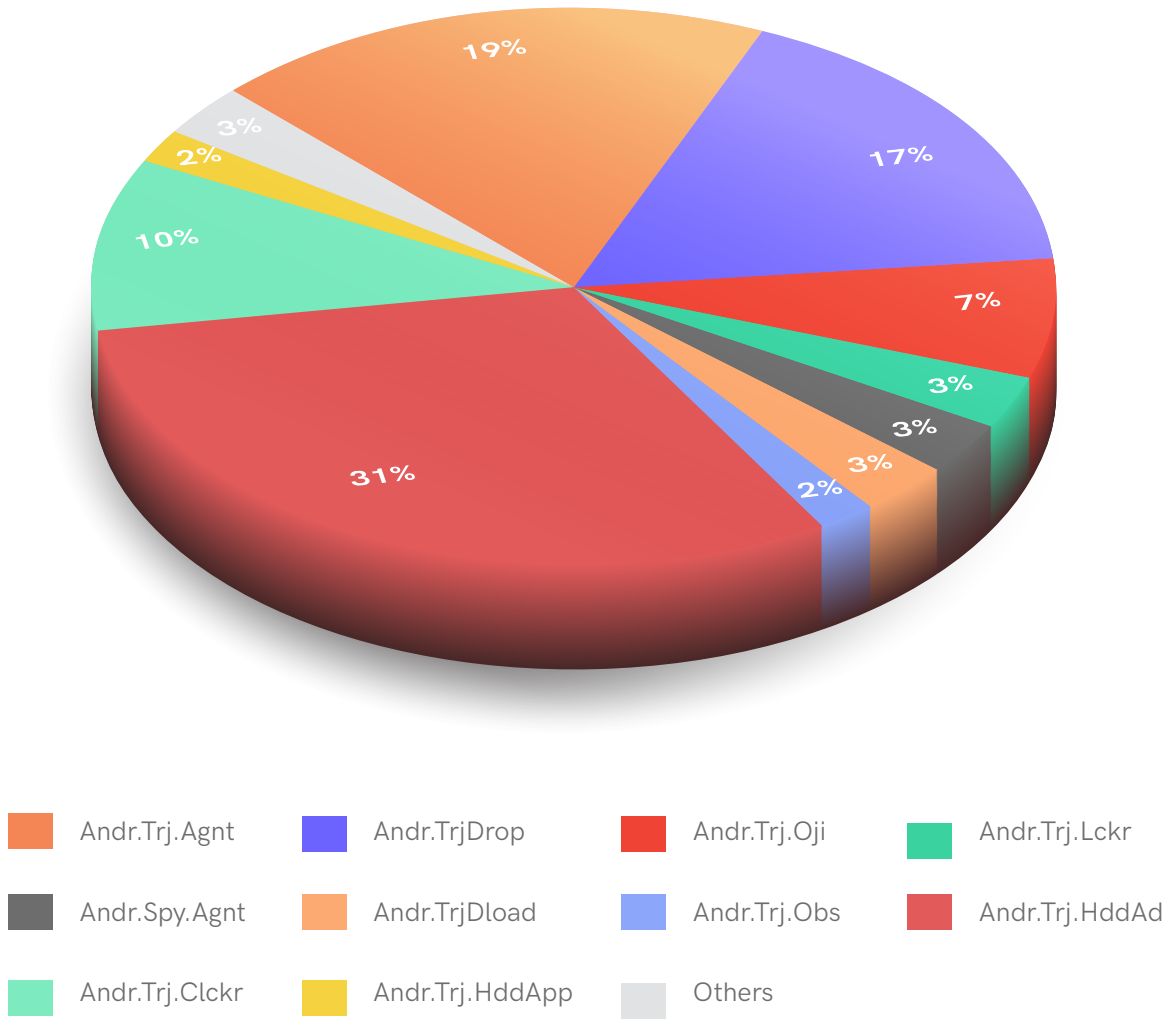
This quarter, we at K7 Labs received reports from users that the **tiktok.apk,** one of the apps banned by the Government of India (GoI) is being falsely detected as a Trojan. Taking a closer look revealed the fact that it is actually a fake app spreading mainly in the name of tiktok.apk. In this case, adversaries have availed the users' interest in one of the banned apps, TikTok, to trick them in installing this fake version.

The kill-chain is as shown below:

The Trojan Brouhaha

Throughout Q4 of 2020-21, we at K7 Labs saw a dramatic surge in several Trojan families' frequency, disguising themselves as legitimate apps in a few scenarios. Alongside, the threat actors constantly used tools for reconnaissance, incorporated new functionality and obfuscation techniques to bypass protection methods.

Most Prevalent Trojan Types

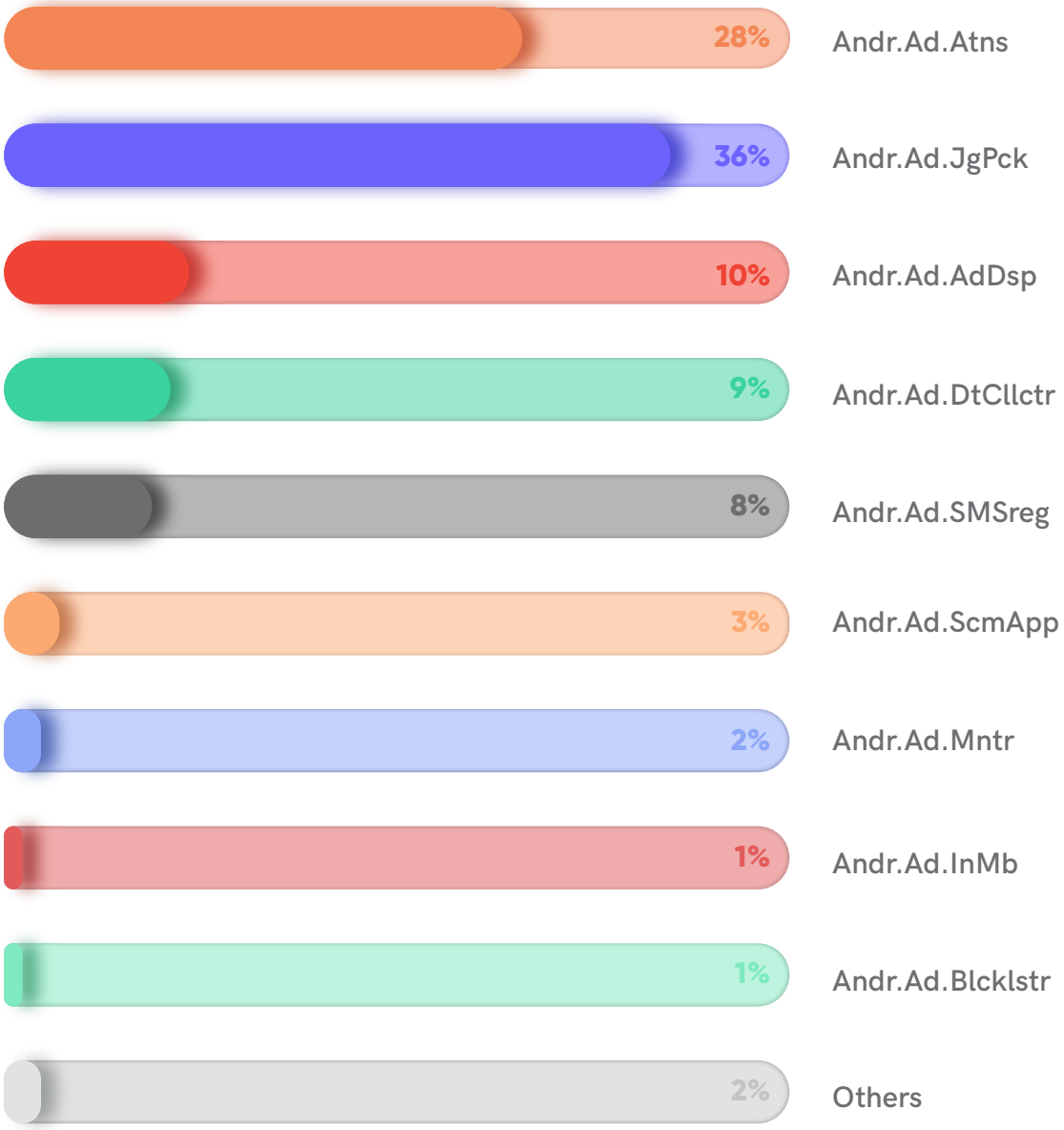


The most glaring observation during the period was how a few Trojan families continued their reign on the Android threat landscape. This quarter, the threat actors were seen using mainly the top 4 families to victimise hundreds and thousands of Android users worldwide.

The Ubiquitous Adware

Despite Trojans' dominance on the Android threat landscape, adware families too have kept their presence alive via a few old and popular strains. These adware continuously transformed their attack strategies and appeared in various new avatars to generate easy money for the bad actors.

Trend Line Showing the Adware Plague



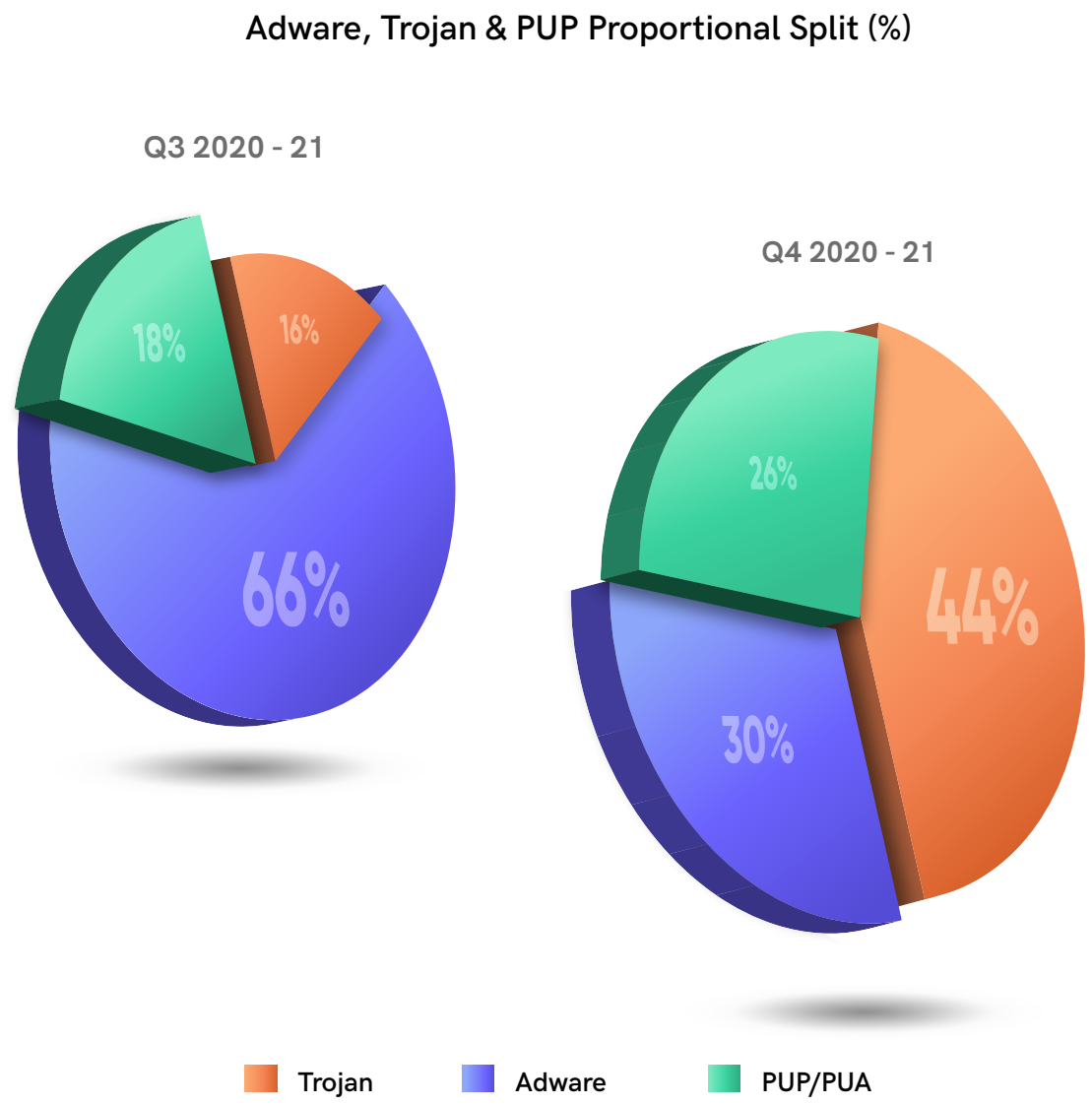
Andr.Ad.JgPck has been topping the charts for the past few quarters.

Tips to Stay Safe

- Avoid apps banned by the GoI
- 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

Besides targeting a large number of Windows and Android users this quarter, perpetrators are also using new attack techniques and infection vectors against macOS users as threat actors have begun to realise that like Windows and Android, Mac devices are no longer safe as they were purported to be.

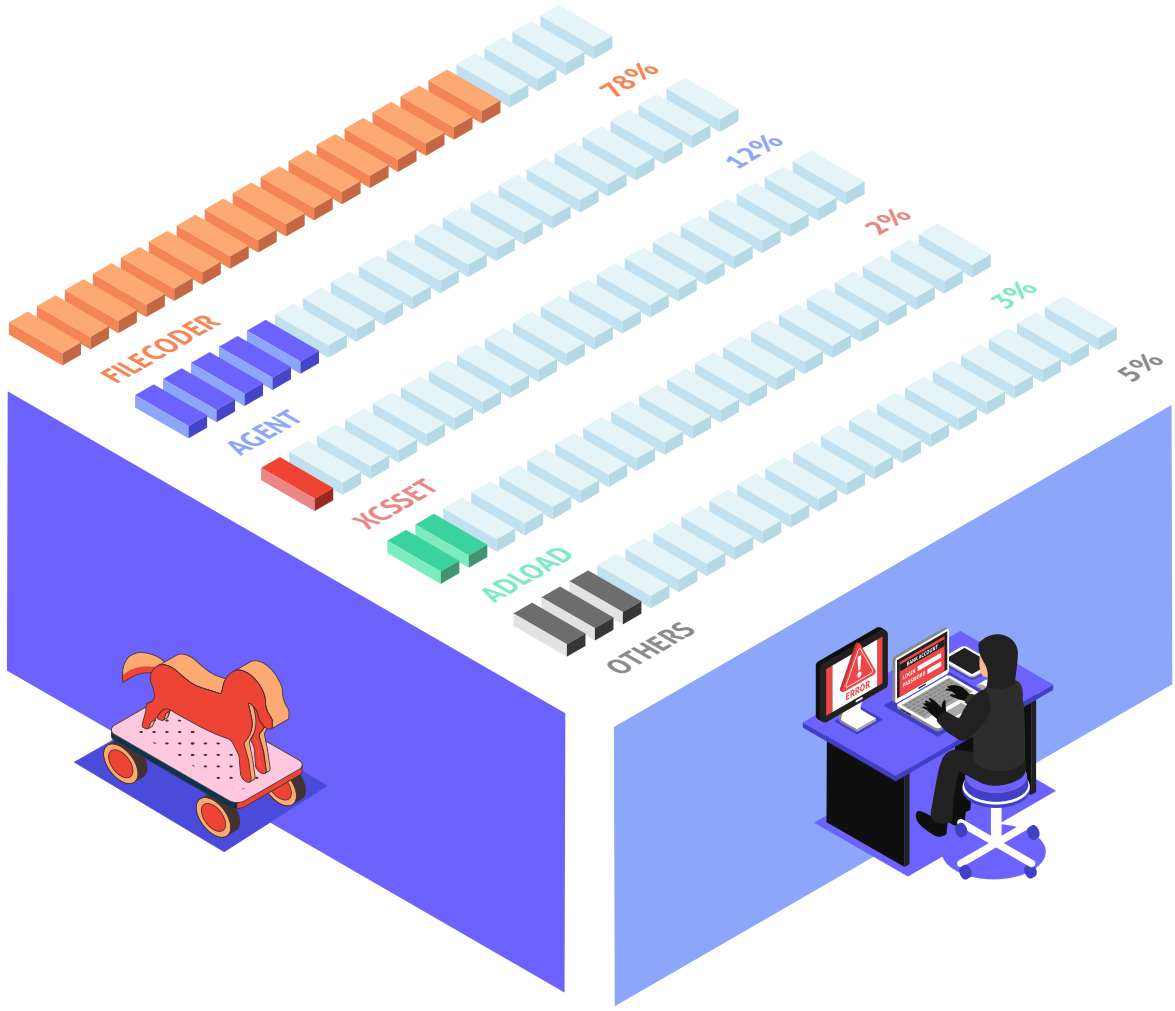


We saw a substantial proportional surge of Trojans this quarter in comparison to adware which has seen a drastic decline. The rising statistics of PUP/PUA shows how threat actors are leveraging them to swindle an innumerable number of victims.

The Trojan Hubbub

According to our K7ETI stats, few Trojan families occupied the major share this quarter.

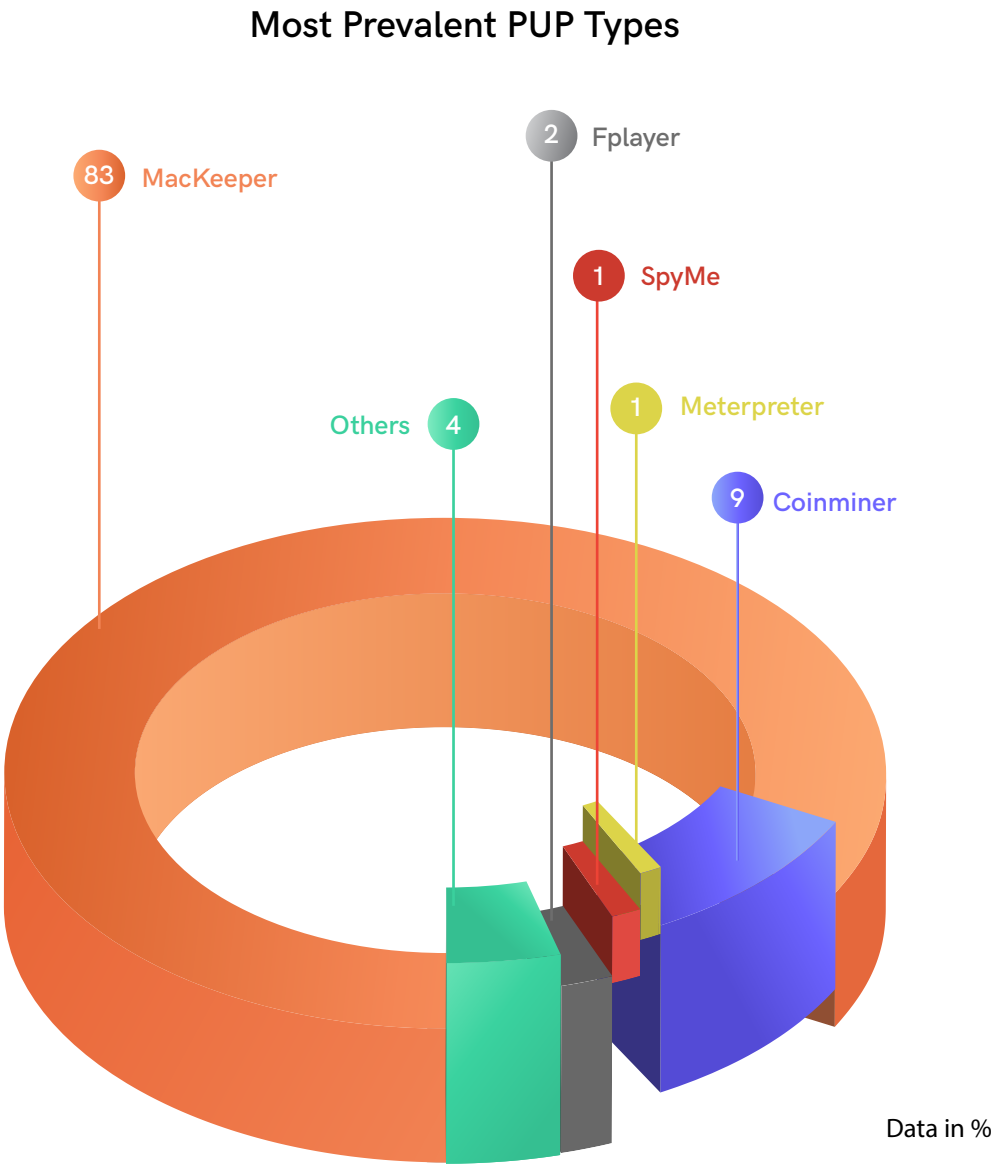
Trojan Detection Trend Lines



As we can see, the Trojan space was majorly occupied by the Filecoder Trojan type, followed by various downloaders. Other Trojan families remained comparatively less visible during this period.

The Spurt of PUPs

The steady growth of Potentially Unwanted Programs and Applications (PUP/PUA) hints at how the threat actors are evolving in every malicious category and developing more sophisticated and spurious apps to outwit the security standards and app review policies.

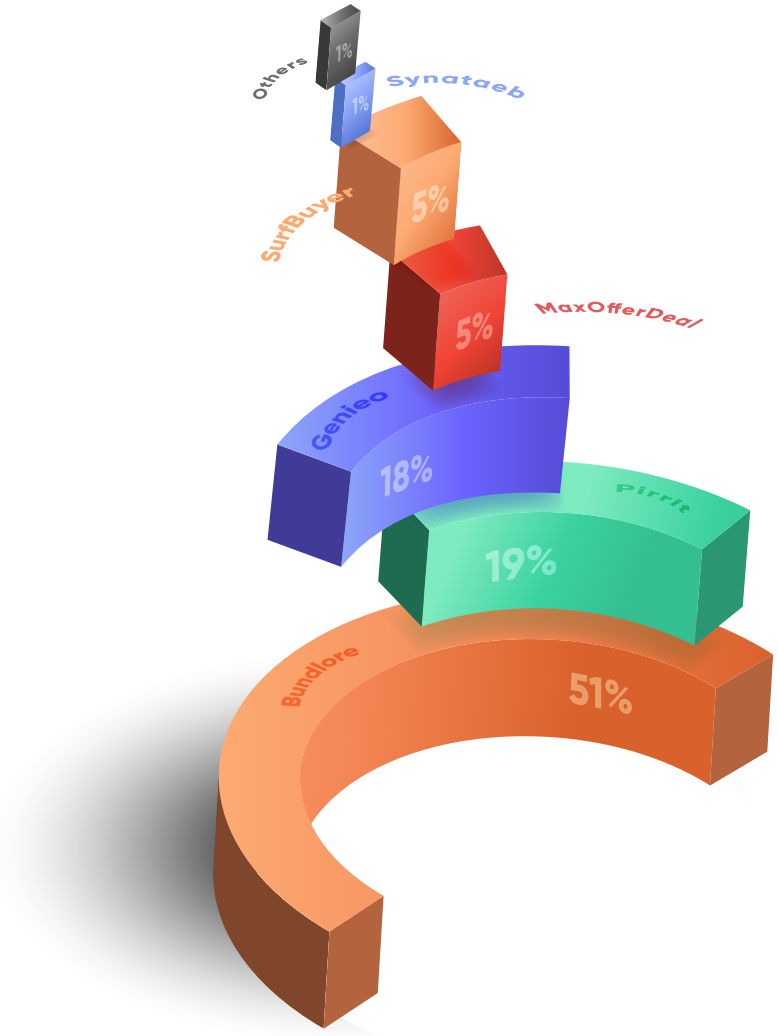


Continuing its exceptional visibility in the past few quarters, MacKeeper tops the chart with a mammoth visibility of 83%.

The Adware Saga

Despite the diminishing numbers, classic adware like Bundlore, Genieo, and Pirrit have continued to keep the flag flying. However, there were no new adware families found in this period, hinting that the adversaries might be banking more on Trojans and PUPs.

The Trend Line of Adware Variant Detections



Continuing the trail of its visibility in the past few quarters, Bundlore managed to hold the significant share during this period. Other notable adware during the period were Genieo, Pirrit, and MaxOfferDeal.

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

These days adversaries are regularly introducing innocent-looking vectors, reconnaissance methods and malware strains which helps in staying stealth from AV vendors, thereby posing a huge risk to both individuals and organizations. During this tumultuous period, every individual and organisation should aim to protect themselves from cyber crimes by embracing necessary safety precautions so as to secure their digital lives. We recommend the below-mentioned steps to safeguard yourselves.

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
Do not open documents from unknown or suspicious sources. Also, do not enable macros in documents received from such sources	Avoid apps banned by the GoI
Secure all entry and exit points of your network	Do not download apps from unknown sources or third-party app stores

April 2021