# Cyber Threat Monitor Report

2019-20

K7 SECURITY

# Contents


**Deciphering The Indian Cybersecurity Threat Landscape ..... 4**

**Regional Infection Profile ..... 6**

**Enterprise Insecurity ..... 8**

Case Study: Spurt In RDP Attacks ..... 9

COVID-19 Themed Attacks ..... 10

Safety Recommendations ..... 11

**Vulnerabilities Galore ..... 12**

Curveball Aka Windows Crypto API Spoofing Vulnerability ..... 12

Ghostcat Vulnerability ..... 13

Unauthenticated Meeting Join Vulnerability In Webex Meetings ..... 13

SMBghost ..... 14

Prevalent Remote Code Exploitation ..... 15

RCE Exploitation Using Shortcut Files ..... 15

RCE Vulnerability In Microsoft Exchange Server ..... 15

**Danger In The Internet Of Things ..... 16**

Healthcare Sector Wakes Up To MDhex ..... 17

Zero-Day Vulnerabilities Discovered In Cisco Discovery Protocol (CDP) ..... 18

Kr00k - The New WiFi Vulnerability ..... 18

Mitigation Techniques ..... 19

## Contents


**Windows Under Siege ..... 20**

Windows Malware Type Breakdown ..... 20

Windows Exploits ..... 21

Creeping Unnoticed: Worms Vs Viruses ..... 22

- USB Worms Vs Viruses ..... 22
- USB Advantages ..... 22
- Sophisticated USB Attacks ..... 22
- Telemetry ..... 23
- Few Tips To Stay Safe ..... 24

Obsolete OS: A Potential Malware Zone ..... 25

- The Telemetry Factor ..... 25
- Risks Of An Obsolete/Unpatched OS ..... 26

**The Mobile Device Story ..... 27**

Case Study: Cerberus Trojan Targets Mobile Devices ..... 28

The Significant Rise Of Trojan Horses ..... 29

The Adware Crisis ..... 30

Malicious Apps From Google Play Store ..... 31

Tips To Stay Safe ..... 32

**Mac Attack ..... 33**

But There Is A Catch ..... 33

The Prevalent PUPs ..... 34

The Upsurge Of Adware ..... 35

The Reign Of Trojans ..... 36

Safety Guidelines ..... 36

**Key Takeaways ..... 37**

# Deciphering the Indian Cybersecurity Threat Landscape

On our round-the-clock mission to protect our customers from all manner of adversaries, including APT attacks, and state-sponsored hackers, we have very frequently come across and combatted a diverse range of malware, intrusion strategies, relentless attack kill-chain phases and now the COVID-19 theme-based attacks targeted towards work from home users (WFH) by threat actors taking advantage of the lockdown scenario. Phishing attacks were the most common attack seen during the pandemic. In the Android platform, malicious apps disguised as benign COVID-19 apps were also seen this quarter targeting Indian banking users and across the world. And interestingly, the variety in the attacks has never failed to surprise us. Keeping pace with the latest innovations in technology and internet space, adversaries take the help of Internet forums, manipulate pen-testing tools, and purchase malware-related services from the colossal cybercrime marketplace; the Dark Web.

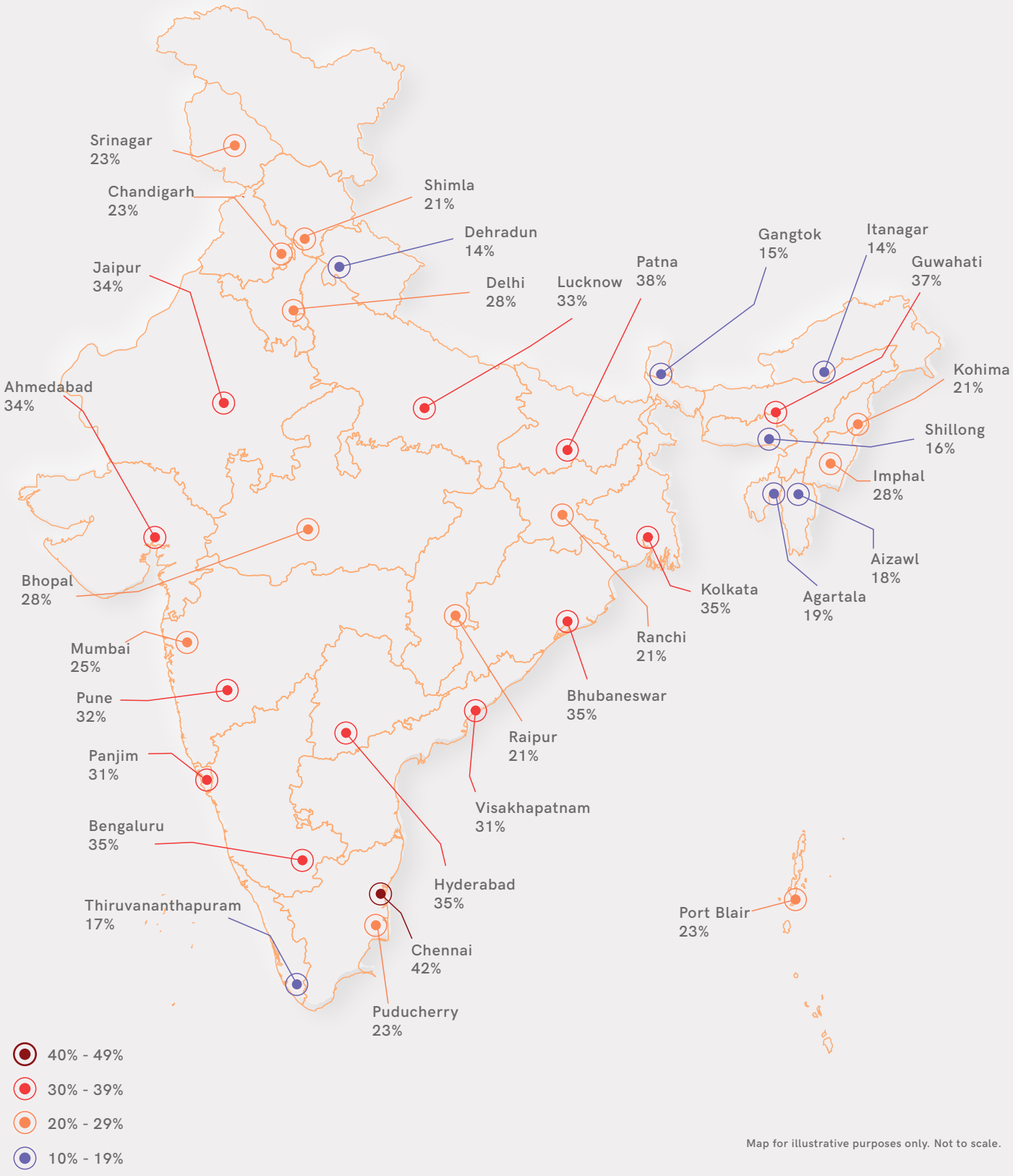
The massive pool of such available resources has encouraged many amateurs known as script kiddies or skiddies to step into the dark alleys of cybercrime. Though this growing number has increased the frequency of attacks to some extent, the pattern of attacks and victims remain predictable. The modern attackers have become extremely avaricious and seldom work for fun or merely to flex their muscles.

And every quarter, we see that the tendency of the attackers to lure more and more money from their victim's increases. The most interesting part of this rapid transformation could be perceived while looking at the trends in the attack structure. Besides making annoying PUA and adware, adversaries are now mainly focusing on enterprises irrespective of their size. So in Tier-2 and relatively small cities, they are focusing on the small scale industries where cybersecurity policies are not strictly enforced, where the human resources responsible for cybersecurity do not have adequate knowledge and know-how or where cybersecurity budgets are small.

However, in Tier-1 cities and metros, the bull's eye would be the large enterprises. Attacks in these parts of the country have been relatively sophisticated, with multiple layers and devious phishing techniques. Quite naturally, the inexorable threat actors too are adopting new tactics, techniques, and procedures (TTP) to accomplish their goals and attempt to make their attacks unstoppable. And the growing frequency of cyberespionage operated by state-sponsored hackers has made the situation even grimmer.

So we urge you to read our exhaustive report to gain extensive knowledge about the latest threat landscape. We appreciate you sharing this report among your colleagues and friends to make them more aware of the prevalent cyber threats and 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

Our society is transforming every day. And so is the world of malware. Adversaries are adopting and adapting new intrusion and evasion tactics to fly under the radar. Even though the bad actors are executing more targeted attacks, the attacks on the end-users in this quarter seem to have dropped significantly, perhaps due to them adopting better security hygiene practices. At the same time, some adware and PUPs have been transforming themselves as borderline malware. Like Software-as-a-Service, Malware-as-a-Service (MaaS) has become more affordable than ever, and helps even amateurs to perpetrate sophisticated attacks.

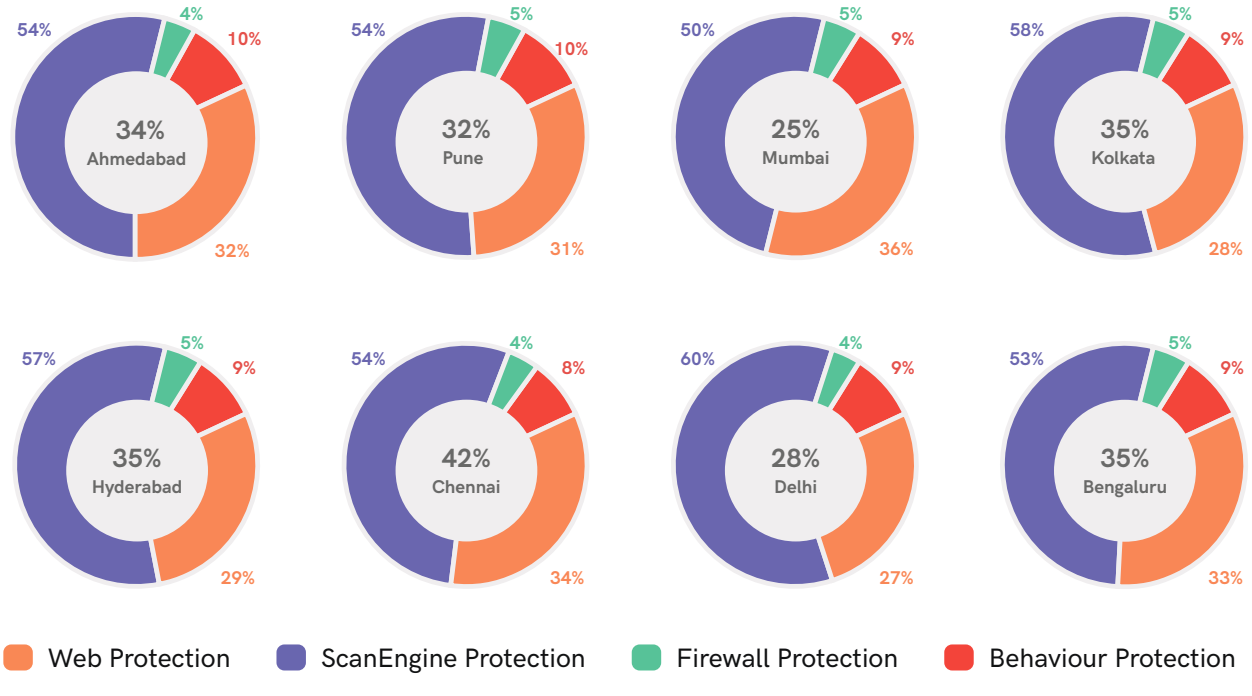
Before diving into the attack techniques and tactics seen in the wild during the quarter, it's apt that we shed some light on the threat landscape to offer some granular insight.

Infection Rate (IR) of an area is defined as the proportion of our active users who encountered at least one cyber threat event which was blocked and reported to our K7 Ecosystem Threat Intelligence (K7ETI).

The most interesting observation during the period was the apparent drop in the frequency of overall attacks. In contrast to the previous quarter, the percentage of total attacks has declined by eight percent in Q4, 2019-20 compared to Q3. Our telemetry stats reveal an overall IR of 16% in the country, but it remains to be seen if such a drop can be maintained in the longer term over the quarters to come.

As you may already be aware, the IR offers a glimpse of the regional proportions of threat activities tracked by our K7ETI. The detailed data grouped by Tier-1 and Tier-2 cities show their relative exposure to cyber threats on the various computing platforms.

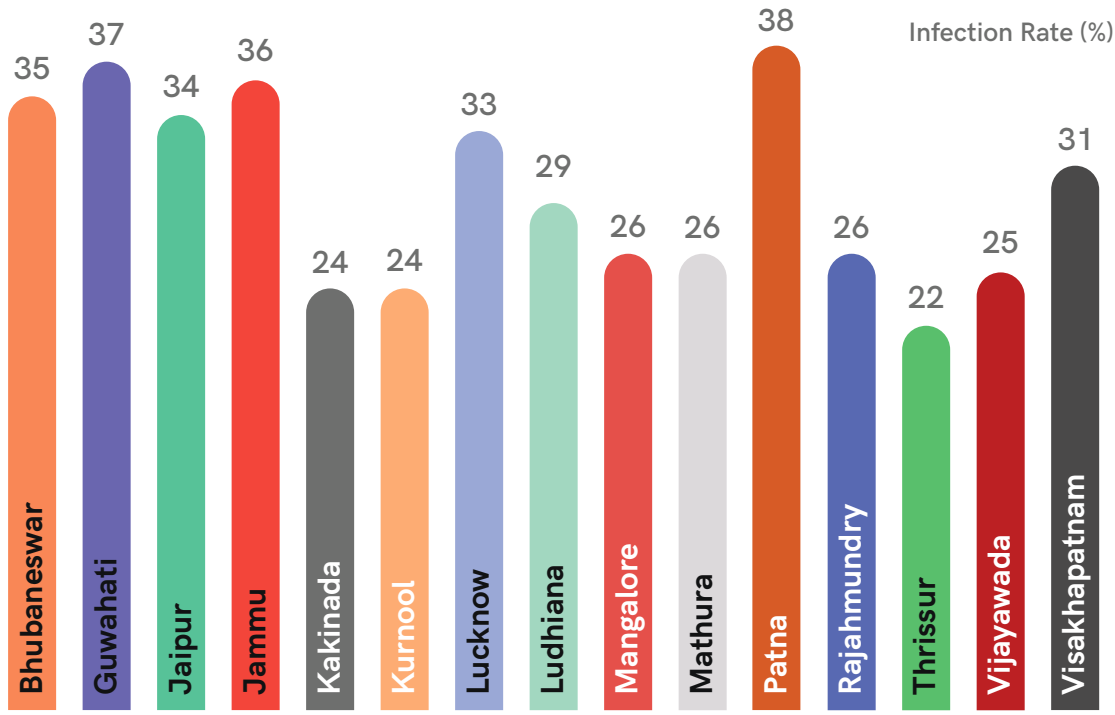
## The Metros and Tier-1 Cities - Infection Rate



As you can see from the charts, every four out of ten netizens from Chennai have encountered at least one thwarted cyber-attack. The metros, like Bengaluru, Hyderabad, and Kolkata, had an attack percentage of thirty-five percent. The IR for Pune and Ahmedabad users had reduced marginally in comparison to the previous quarter and were at 32% and 34% respectively. However, both Mumbai and Delhi, had an IR of less than thirty percent, this time.

In comparison to Q3 2019-20, the trend in Q4 2019-20 is definitely an aberration, attributed mainly to the COVID-19 pandemic panic world-wide. We need to wait and see how this pattern would emerge over the quarters to come and also in a post COVID-19 world.

## Top 15 Infection Rates in Tier-2 Cities




The trend line in the Tier-2 cities, however, remained quite significant. At least thirty-five percent of netizens from the Tier-2 cities like Patna, Guwahati, Jammu, and Bhubaneswar had faced the brunt of cyber attacks this time. With an IR of 33%, 31%, and 34%, respectively, Lucknow, Visakhapatnam, and Jaipur have experienced a decline of 9%, 5%, and 1% in comparison to the previous quarter, but only time will tell whether such a decline can indeed be maintained.

BACK TO CONTENTS

# Enterprise Insecurity

The ongoing Coronavirus pandemic has thrown the world out of gear. Threat actors are manipulating the increasing fear and anxiety amongst people to expand their victim base. The Coronavirus pandemic has compelled organisations from all over the world to allow their employees to work from home. However, many large enterprises, SMEs and SOHOs are still not prepared enough to host all of its employees remotely. Enterprises have started adopting necessary remote working protocols such as Remote Desktop Protocol (RDP) to offer access to its sensitive data and applications, and large enterprises are also leveraging proven technologies such as VPN and Endpoint security software to provide a protected digital environment to their employees.

The sudden mass requirement to embrace remote working procedures did not give enough time for the organizations to adopt a comprehensive and matured implementation of security practices. This has become a boon for the cybercriminals who have started targeting more users than ever, mainly due to unpatched vulnerabilities in these applications which could be potentially exploited. For example, a massive number of recent enterprise breaches were executed by using unpatched vulnerabilities in enterprise VPN products, even from reputed companies.

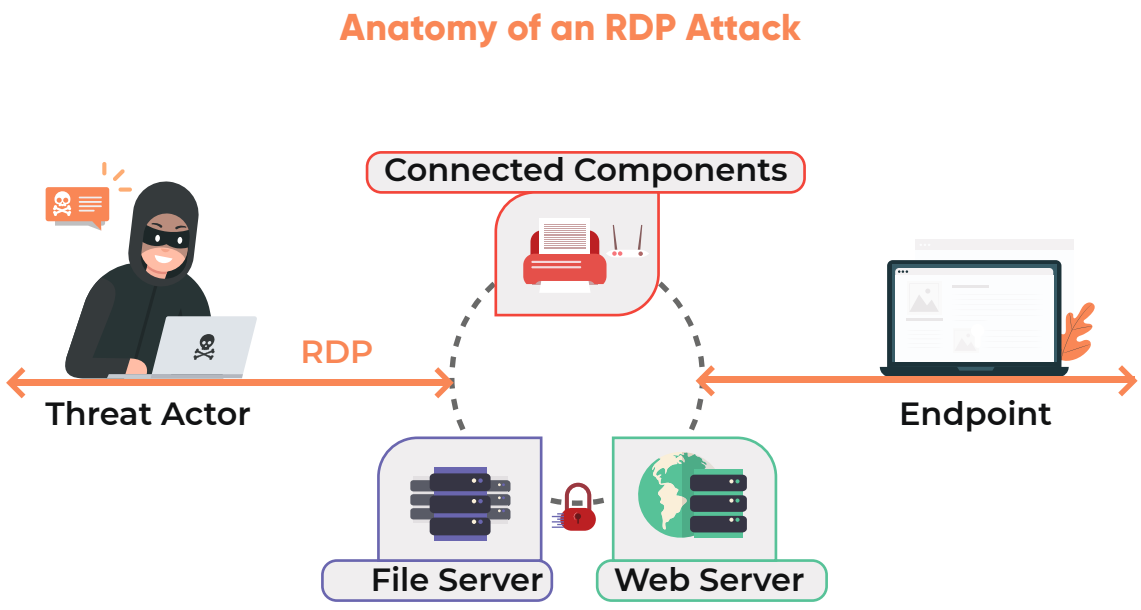
## Case Study: Spurt in RDP attacks

Remote Desktop (RDP) has always been an accessible technology across platforms providing remote access to your organisation's data for all your employees from anywhere across the world. But while using such technologies, system admins should also be cautious with its visibility over the internet. Lack of additional security features such as network-level authentication and encrypted connections may make public-facing terminal servers susceptible to unauthorized remote access and ransomware attacks, among others.

Vulnerable systems or servers running on dated operating systems are also likely to get exposed to attackers on the internet via RDP. Between February to March this year, we found an umpteen number of attacks executed on such dated systems.

Recently, we encountered one such incident where one of our valued enterprise customers reached out to us after noticing numerous suspicious thwarted login attempts in their network. Upon analysing, we found the network exposed many of its servers on the internet. And the dubious login attempts were being executed via all these publicly-accessible IPs.

We explained to the customer about how threat actors scan the internet looking for servers running vulnerable services and applications which could be exploited directly or by brute-forcing themselves into the network.




We also discussed the security best practices with them and requested them to patch and update all applications hosted on these public-facing servers. We also recommended them to swap the default RDP port for an unused port as threat actors usually look for the default RDP port number to attack.

## COVID-19 Themed Attacks

As ever, phishing attacks have remained the most favourite intrusion method for the threat actors. In the past few months, due to the COVID-19 pandemic, there has been an increase in the number of these attacks across the world. Benign looking emails with COVID-19 themes and containing malicious attachments crafted to download dangerous malware onto the users' devices are being sent to unsuspecting victims.

Many of such emails purport to arrive from reputed organisations to increase its authenticity to the victim. Moreover, these emails come loaded with mendacious information related to this pandemic. Such emails contain attachments which, when accidentally opened, download malware capable of many bad things like stealing sensitive personal and financial information and dropping other malware.

# Safety Recommendations

- We recommend you to change your default Remote Desktop (RDP) login name to mitigate brute force attacks to some extent. Ensure you follow a strong password policy as a standard
- Change the default port of RDP (3389) to another unused port. This step would better hide your RDP service from the RDP hunters who are looking to exploit vulnerable remote services
- Use a secure Virtual Private Network (VPN), wherever possible
- Change default/weak passwords on your router and firewall
- Update your firewall rules to block unwanted inbound traffic
- Follow good security hygiene and safe email handling practices
- Secure your device by keeping it up-to-date and patched for the latest vulnerabilities
- Always use the right security product such as K7 Endpoint Security to scan your devices and network

BACK TO CONTENTS

# Vulnerabilities Galore

Exploits often offer a snapshot of the threat actors' activities, about how they intruded into the vulnerable system. The availability and popularity of the internet are helping threat actors to track the latest vulnerabilities and create a new intrusion plan accordingly. The zero-day and other sinister vulnerabilities on the Dark Web have made this situation grimmer. Threat actors are also offering Malware-as-a-Service (MaaS) at a throwaway price which makes it all the more easy and advantageous to exploit vulnerabilities. This easy availability of vulnerabilities has made the administrator's job more complicated as many are getting exploited even before the concerned patches are applied. Let us now see the list of vulnerabilities in this quarter, that could be the attacker's target.

## Curveball aka Windows Crypto API Spoofing Vulnerability

Microsoft Windows has always remained the top favourite for threat actors for numerous reasons, and vulnerabilities play a crucial part in this.

In this quarter, we will be looking at the **CVE-2020-0601** vulnerability called Curveball, which allows an attacker to spoof an intermediate code-signing certificate. Code-signing certificates are needed to validate executable programs in Windows 10 and to establish the identity of websites in browsers. The exploitation of these could then lead to attackers installing malicious applications such as rootkits. This vulnerability affects Windows 10, Windows Server 2016, and Windows Server 2019.

## Ghostcat Vulnerability

Threat actors nowadays focus on all the emerging and popular platforms to target more victims. The immensely popular Apache Tomcat versions of application servers had also experienced a scourge of loopholes. In this quarter, a high-risk read/include vulnerability, **CVE-2020-1938**, has been discovered in Apache Jserv Protocol (AJP) of Apache Tomcat between versions 6.x and 9.x.

The patch has been released for the 7.x, 8.x, and 9.x but not for 6.x versions as it has reached end-of-support. A massive number of scans targeting this vulnerability had already begun. What makes this vulnerability a high-risk one is that all the versions of Apache Tomcat come shipped with the AJP connector enabled by default.

## Unauthenticated Meeting Join Vulnerability in Webex Meetings

Another threat comes from one of the most popular remote communication platforms, Webex. The Cisco owned video conferencing platform caters to many of the most prominent enterprises from all over the world and is immensely popular for the solutions it offers.

However, a newly found vulnerability has managed to create a taint in its hard-earned popularity.

**CVE-2020-3142** is a vulnerability that lets any unauthenticated user join a password-protected meeting without entering the password for a meeting. To exploit this, the attacker has to initiate remote connection attempts from a Webex mobile app. The affected versions are Cisco Webex Meetings Suite sites lower than 39.11.5 and Cisco Webex Meetings Online sites lower than 40.1.3.

## SMBGhost

Another Windows-based vulnerability that made it to the headlines was SMBGhost, aka EternalDarkness. The remotely exploitable vulnerability was capable of exploiting a flaw found in Windows System Message Block version 3's file-sharing protocol. SMBGhost or **CVE-2020-0796** is an RCE vulnerability present in the latest SMB version 3.1.1. It is a classic integer overflow vulnerability that exists in the SMB decompression module, which lets an adversary gain access to the system with current user privileges. Microsoft hurriedly launched an update for the impacted versions which are Windows 10 1903 and Windows 10 1909 client and server edition operating systems to fix the dangerous flaw.

## Prevalent Remote Code Exploitation

Remote Code Execution vulnerabilities are one of the most critical vulnerabilities available around because exploiting these could easily compromise the entire network or organisation in a very short span of time making this a vulnerability that needs to be fixed at the earliest.


### RCE Exploitation Using Shortcut Files

**CVE-2020-0729** is a remote code execution (RCE) vulnerability that could get exploited when a specially crafted malicious LNK file is processed. This specially crafted file can be placed on a remote share or a removable drive and would exploit the vulnerability once the directory gets accessed. A similar vulnerability was used in the infamous Stuxnet malware a decade ago. By using these specially crafted LNK files as bait, adversaries can easily make their way into vulnerable systems for data exfiltration, among other things.

Another RCE vulnerability, **CVE-2020-0684**, could be exploited by accessing a remote share or removable drive with a malicious LNK file. The vulnerability is an example of a classic integer overflow vulnerability that occurs while parsing the LNK file. By using a specially crafted LNK file as bait, adversaries can make their way into air-gapped systems using USB drives.

### RCE Vulnerability in Microsoft Exchange Server

**CVE-2020-0688** is a remote code execution vulnerability in the Microsoft Exchange server that could get exploited when a specially crafted malicious email gets sent to a vulnerable Exchange Server. The vulnerability lies in the Exchange Server, failing to create unique cryptographic keys properly at the time of installation. The vulnerability is critical because no user interaction is required, and the code execution happens with system-level permissions, which could allow an attacker to take complete control of the Exchange Server via a single email.

BACK TO CONTENTS

# Danger In The Internet Of Things

The burgeoning success of the Internet of Things related devices is a double-edged sword. Besides making our life easy in many aspects, a plethora of modern IoT gadgets are also riddled with flaws and vulnerabilities, inviting threat actors to invade. The stable internet connectivity helps as a conduit for sharing data, which are often accessible to the malicious actors also.

Many enterprises, irrespective of their size, overlook the security related to IoT devices compared to the other connected devices, which could result in a security disaster. However, putting necessary security measures in place could effectively protect the enterprises along with the end-users.

We encountered a pool of scary vulnerabilities during the quarter, as listed below.

## Healthcare Sector Wakes up to MDhex

GE HealthCare devices are vulnerable to 6 unpatched vulnerabilities (CVE-2020-6961, CVE-2020-6962, CVE-2020-6963, CVE-2020-6964, CVE-2020-6965, CVE-2020-6966), collectively referred to as MDhex.

The vulnerabilities could allow attackers to perform remote code execution, disable the devices, harvest personal health information (PHI), change alarm settings, and alter device functionality to the point that they become inoperable.

These vulnerabilities affected the below-mentioned devices:

- Central Information Center (CIC), versions 4.x and 5.x
- Apex Pro Telemetry Server/Tower, versions 4.2 and earlier
- CARESCAPE Central Station (CSCS), versions 1.x and 2.x
- CARESCAPE Telemetry Server, versions 4.3, 4.2 and prior
- B450 patient monitor, version 2.x B650 patient monitor, versions 1.x and 2.x
- B850 patient monitor, versions 1.x and 2.x

## Zero-day Vulnerabilities Discovered in Cisco Discovery Protocol (CDP)


A series of vulnerabilities were discovered in the CDP. Any unauthenticated user can achieve remote code execution or denial-of-service through a specially crafted packet, allowing attackers to fully take over these devices due to improper validation of the CDP messages.

The affected devices include Cisco NX-OS switches, Cisco IOS XR routers, Cisco NCS Systems, Cisco 8000 IP Cameras, Cisco Firepower Firewalls, and Cisco IP Phone 7800 and 8800 Series.


## Kr00k - The New WiFi Vulnerability

The world's most popular WiFi chipsets, Broadcom and Cypress, have been affected by a vulnerability that allows unauthorized decryption of WPA2-encrypted traffic. It is believed that more than a billion devices could be exploited by this vulnerability.

# Mitigation Techniques

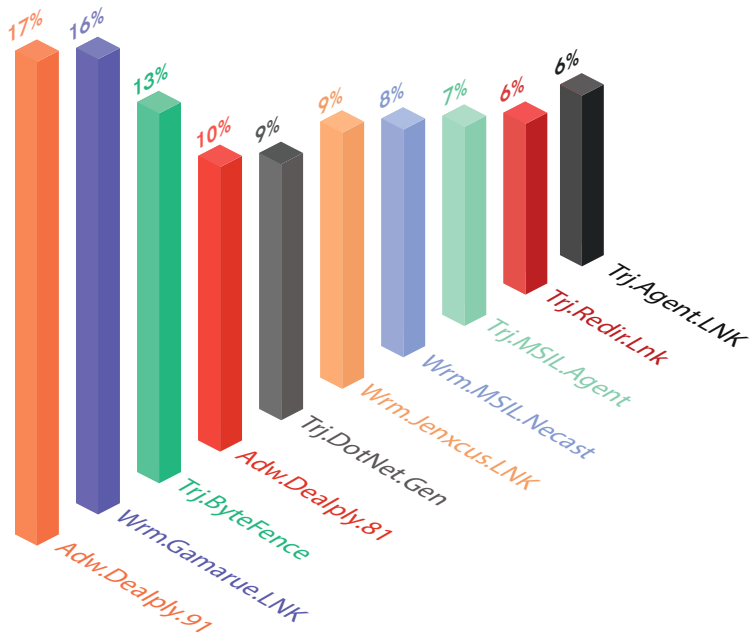
- Ensure all your devices are patched for the latest vulnerabilities
- Do not connect to untrusted SMB servers
- Do not expose your SMB service on the internet unless required
- Restrict the use of USB devices in your environment, and while using them follow good USB hygiene
- Monitor for any data breaches by thoroughly checking the system logs
- Train your employees to look out for signs of an attack
- Change your default settings
- Deactivate unused features and services

# Windows Under Siege

## Windows Malware Type Breakdown

Looking at the variety of malware during this particular period offers an interesting observation. The proportion of the different malware families observed offers glimpses of adversaries' intent and capabilities. We have listed the top malware affecting our Windows users as it has been the most targeted operating system since its inception.

### Split of Windows 10 Malware

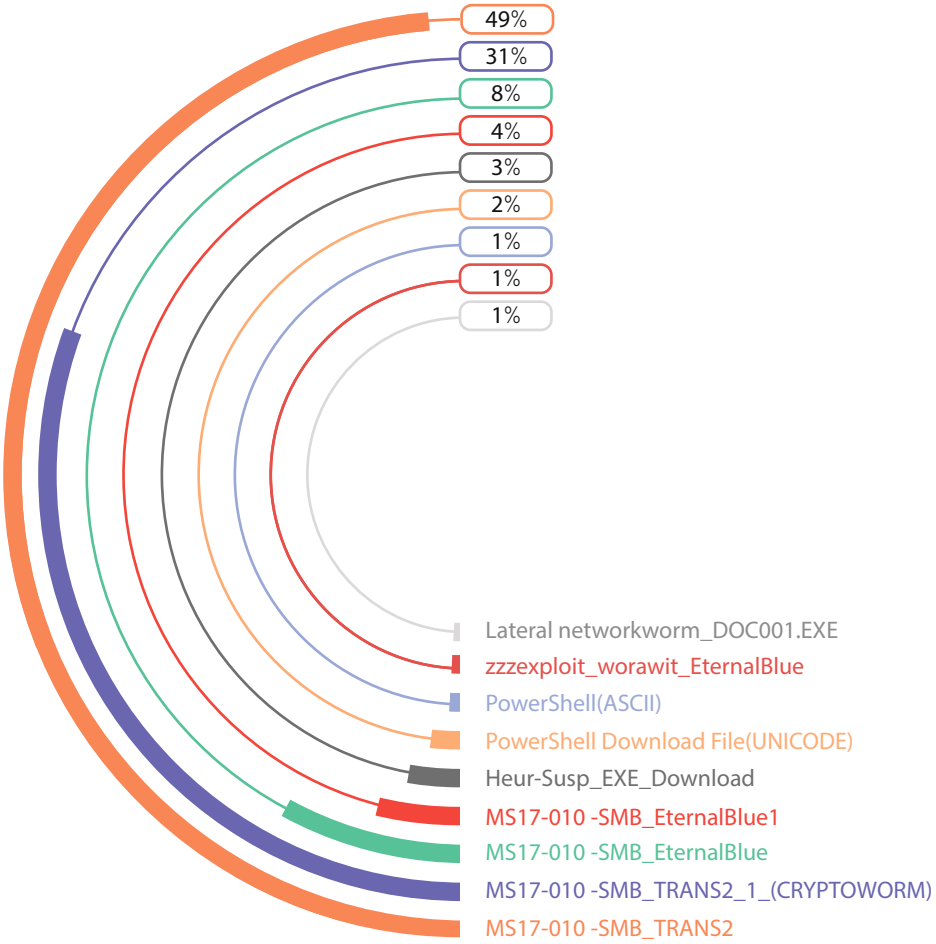



The three most prevalent Windows threats Adw.Dealply.91, Wrm.Gamarue.LNK, and Trj.ByteFence have recorded a presence of 17%, 16%, and 13% respectively. Despite a sudden plunge of 3%, Wrm.Gamarue.LNK still remained prevalent this quarter too. The Adw.Dealply adware families were, however, seen quite often in different avatars and remained most significant. As can be seen from the chart, the top spot of the most active ten malware has been occupied by Adw.Dealply and the variants have collectively occupied the highest spot in the prevalence scale when compared to any other threat family.

## Windows Exploits

From the stats, we can glean that the SMB-based vulnerabilities continue to be the most exploited type by the malware operators this quarter. All the top four vulnerabilities attempted to be exploited over the period were based on SMB, while PowerShell based vulnerabilities held two spots on the leaderboard.

### Most Prevalent Exploits




The continuous visibility of EternalBlue based vulnerabilities over several quarters clearly shows that a large chunk of users still use dated Windows operating system versions despite several words of caution. Even though Microsoft has already released the patch long ago, the patch hasn't been installed by all users, thus unintentionally inviting the bad actors.

# Creeping Unnoticed: Worms vs Viruses

Like how there are health risks in sharing towels, there are security risks when you share USB sticks across systems, especially if you are not protected by a robust security product. Some of the risks associated with these are data theft and malware installation.

Let's look at the most prevalent old USB worms and virus artefacts that have been reported to us via our telemetry system time and time again and see what the data tells us.

## USB Worms vs Viruses

While USB worms (aka autorun worms) spread by taking advantage of the plug-and-play feature available for USB devices, which allows data transfer without user intervention; viruses (aka "file infectors") attach themselves to executable programs and spread whenever you run the infected program.

And if the AutoRun feature is enabled, it would automatically launch installers and other programs when the device is merely plugged in. However, an embedded virus in a file could still infect the system when the file is opened, even if AutoRun is disabled.

Now, let us look at the reasons why USB sticks are a convenient mode of malware transfer for the threat actors.

## USB Advantages

The popularity of USB based worms has not waned since USB storage devices are convenient and used by many people, easy to handle due to their small size, easily available, portable, and inexpensive. It is relatively trivial to distribute malware on these devices. It is also easy to spread the infection to a clean USB drive from an infected computer.

USB drives could also be infected while loading it with default software if proper quality control measures are not taken.

## Sophisticated USB Attacks

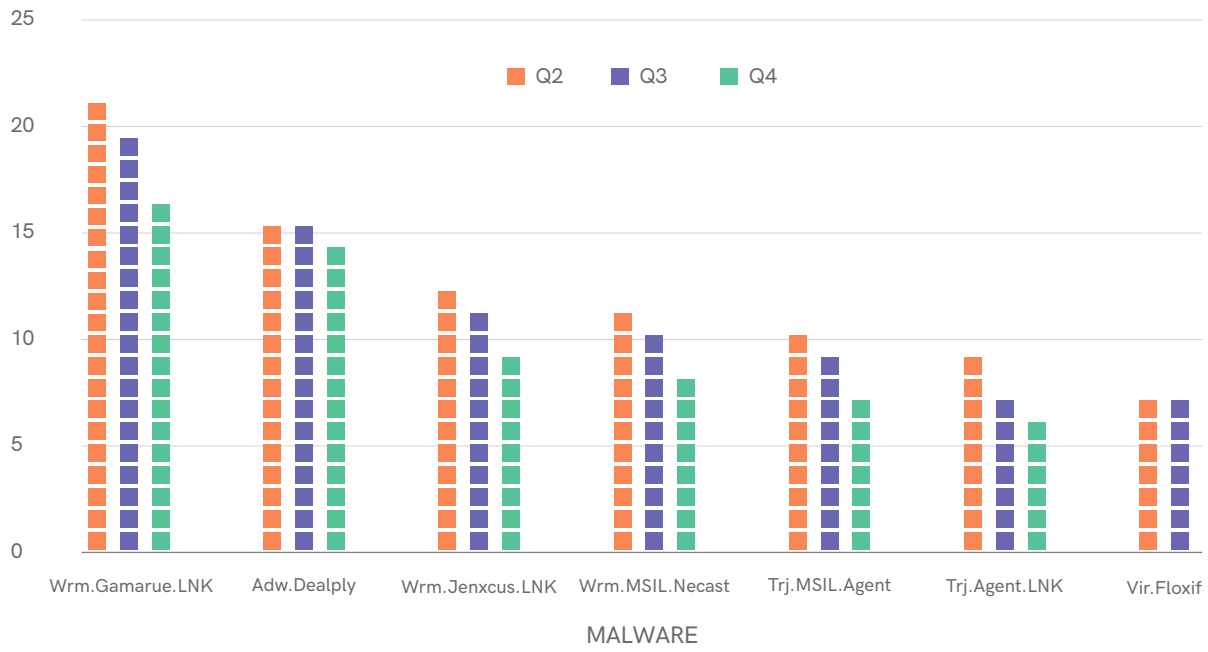
Nowadays, USB sticks carry crypto-mining malware too. USB malware spreads exclusively through devices that plug into the USB port of computers. These could be used for targeted attacks on systems disconnected from the internet, e.g. power plants, nuclear facilities, etc. The infamous Stuxnet worm that targeted Iranian organizations via an infected USB drive is a prime example of how USBs can be used to deliver malware across air gaps.

## Telemetry

Telemetry stats from the quarters Q2, Q3 and Q4 2019-20 reveal that the proportion of users who had an encounter with the same families of USB worms and viruses across quarters has remained consistently high. Among the top 10 malware listed in our quarterly reports, the USB worm families of Gamarue and Jenxcus were among the top 5, and the Floxif virus was among the top 10.

We also gleaned that among the most prevalent worms and viruses, the percentage of users who have shown repeated infections of the same malware was around 30%.

### Top Threats Proportional Split (%) for 2019-20




On looking deeper into the metadata related to these threat events, we believe that many users are not following satisfactory security hygiene practices. Many appear to be plugging in their USBs on their system after perhaps using it on an infected system with no security product installed or sharing their USBs with others who are not very security conscious.

In the case of viruses, we have observed that some users' backups themselves contain infected files, and each time the backup is accessed, the files get reported by the security product, again and again.

As can be seen from our stats, the USB worms Gamarue and Jenxcus have been prevalent across all the 3 quarters, as shown in the chart above. However, we can see that the Floxif virus has fallen off the radar in Q4 2019-20, possibly due to users practising better security hygiene.

Since we have been getting repeated infections every quarter, for reasons mentioned above, henceforth, we intend to filter out these repeated detections, which skew our data, from our top 10 stats in order to more accurately represent threat distributions in the wild.

# Few Tips to Stay Safe

- Ensure AutoRun feature is in a disabled state, and manually launch programs in the flash drive only after a complete scan of the drive by a reputed and robust Anti-Virus product like K7 Total Security
- Keep your Anti-Virus up-to-date
- Backup your critical data
- Ensure that all your backups, including cloud-based ones, are malware free
- Avoid sharing your USB sticks
- Do not use your USB sticks on untrusted systems
- Physical security needs to be in place so that random USB devices are not plugged into air-gapped systems. Also, block unused USB ports on such systems
- Train your employees and make them aware of common threat vectors
- Follow the principle of least privilege and restrict access to critical systems

Practising good cyber hygiene, including restrictions for removable devices and installing a reputable security product, is the best way to minimize security risks that could attack your systems.

## Obsolete OS: A Potential Malware Zone

People these days want to follow and keep up with the trends. Be it in technology, like owning the latest gadget, being up-to-date with the latest cybersecurity related topics or be it in going green or being a fashionista and the like; trend has become a buzzword these days.

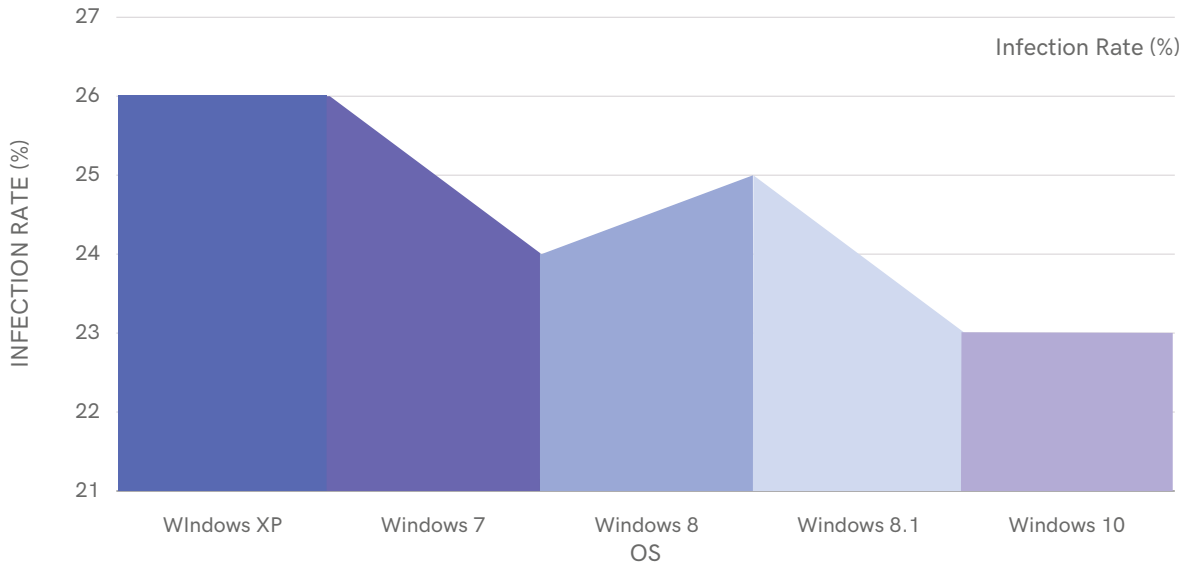
However, when it comes to choosing an operating system, many among us don't seem to give much importance to keeping our OS updated and with the latest trend, thereby putting our devices and the connected peripherals at risk.

Here, we would look into our telemetry stats and the multiple risk factors associated with an obsolete/unpatched OS in spite of having up-to-date security and apps on your device.

### The Telemetry Factor

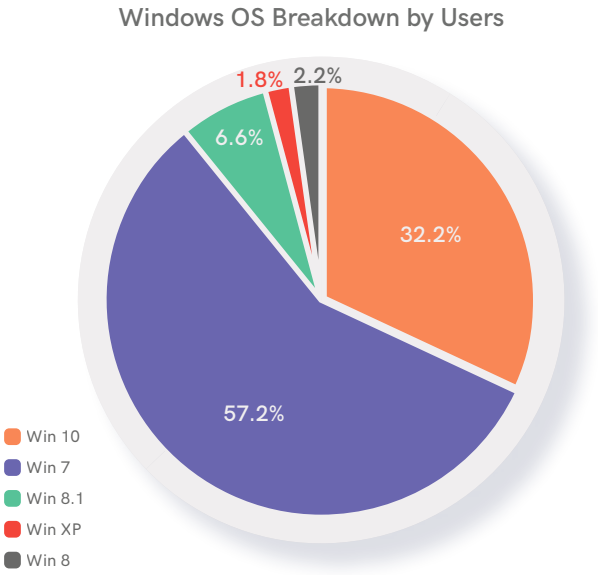
Let us now analyse what our telemetry stats that were reported to our K7ETI tell us about the IR for an obsolete/unpatched OS.

**OS vs Infection Rate (%) for 2019-20**




From our data, we gleaned that all the existing operating systems were significantly vulnerable to threats, as can be seen from the Infection Rate chart. However, it is also to be noted that Windows 10 has been the least susceptible to threats compared to other typical Windows OS. Regardless of OS, to protect ourselves, we need to apply the latest security patches that are made available by Microsoft for each Windows version.

## Windows OS Breakdown by Users




We have depicted the proportion of our active user base who are using a particular flavour of Windows. We can see that almost 60% of our active users are still using Windows 7. This percentage is significant considering the fact that Microsoft has officially withdrawn support for the same. For a variety of reasons, this enormous chunk of users still prefers using obsolete operating system versions such as Windows 7. A significant number of users even use Windows XP. Microsoft has already stopped releasing updates and patches for these Windows versions and does not offer any user support even in case of an emergency.

However, we at K7 always care for our customers and still provide full support for users who have not yet migrated from Windows 7, for a few more years, and we still support you on Windows XP too. However, we always recommend our users to upgrade their operating system at the earliest to stay fully protected.

### Risks of an Obsolete/Unpatched OS

Using an outdated operating system does bring many problems for users, including putting them on the cybercriminals prey list. The vulnerabilities that exist on an unpatched operating system are easy targets for the threat actors to infiltrate into the victims' device, and in such a scenario, even having an updated security suite might not be enough to protect the victim as the effectiveness of the same might be hampered.

Listed below are some of the things that the threat actors can use your device for, amongst other dangers:

- As a backdoor to the device and the rest of the devices in your network
- To encrypt your data by dropping ransomware
- To breach your data

These threats could impact your devices, even if your apps and security products are up-to-date because the threat actors could exploit the existing operating system vulnerabilities at scale.

In order to stay safe from the malicious actors, users are advised to upgrade their operating system whenever available and possible, and keep their security product such as K7 Total Security and apps up-to-date as a protective measure against threats in the wild.

BACK TO CONTENTS

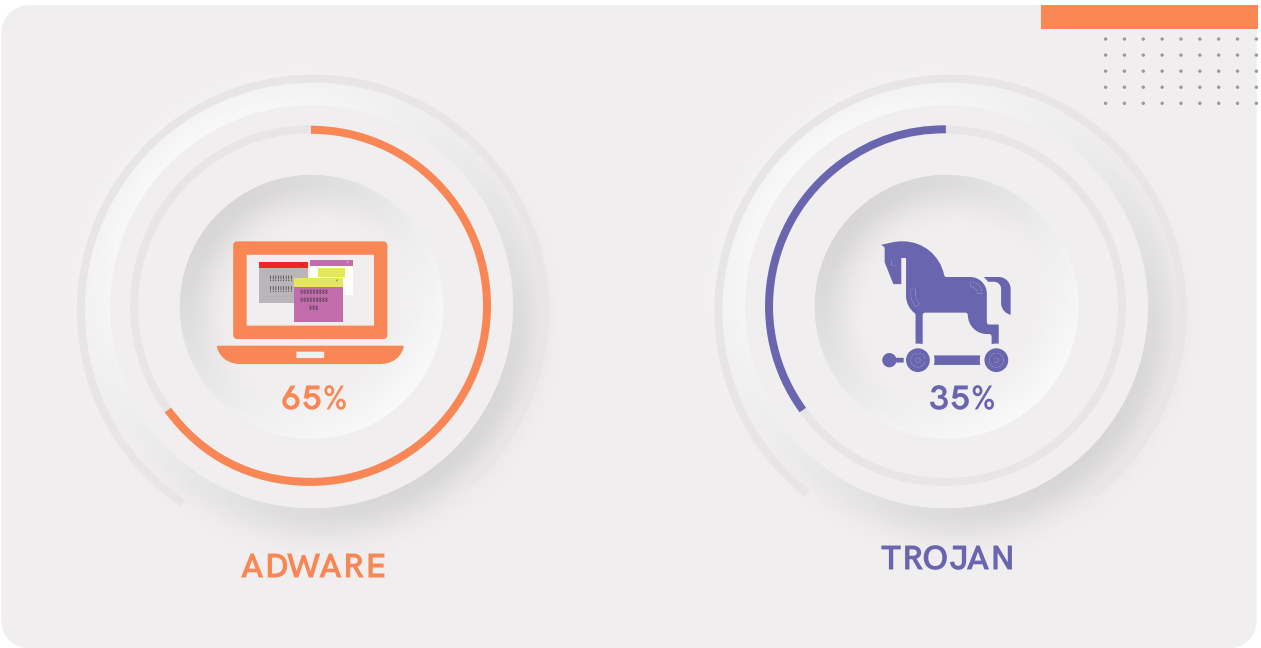
# The Mobile Device Story

Gone are the days when malware attacks were solely associated with Windows driven desktop and laptop computers. The mushrooming of smartphones and umpteen other reasons have made the smartphone market a lucrative hotspot for the threat actors. And the prevalent number of malware families affecting Android and iOS platforms is definitely a cause for concern.

The Android and iOS threat landscapes have always experienced a massive pervasive growth of adware-related apps in comparison to Trojans. The reason is easy to explain - easy money.

However, in this quarter, we have found that the frequency of more nefarious cyberattacks has surpassed the number of adware. In contrast to the previous quarter, the number of Trojan infections has increased by fourteen percent.

## The Presence of Adware vs Trojan

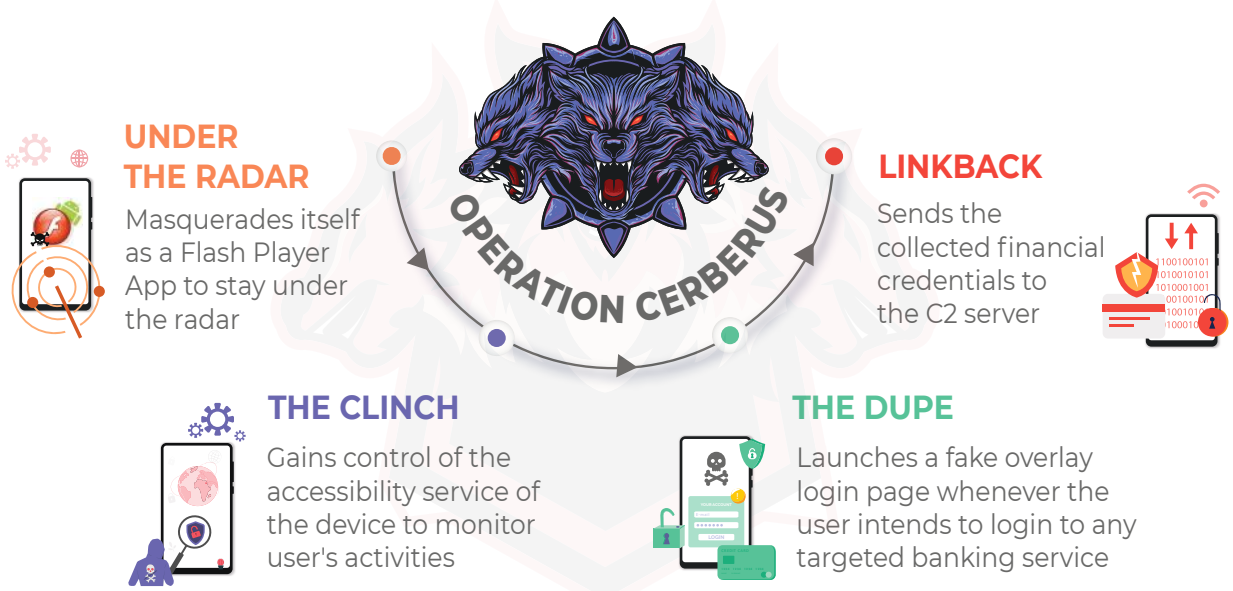



The stats show that while a large number of threat actors have moved towards highly targeted attacks on large, medium, and small scale enterprises, a small number of them are still involved in pushing adware based apps onto the victim's devices for making some easier money.

Threat actors are increasingly rolling out complex Trojan based apps that steal victim's banking credentials. The notorious Operation Cerberus Banking Trojan was primarily seen during Q4 2019-20 targeting Indian banking users.

## Case Study: Cerberus Trojan Targets Mobile Devices

This Banking Trojan disguises itself as a benign COVID-19 app, covid-19.apk which is capable of stealing credentials and sensitive user data. This malware has targeted more than 250 banking and cryptocurrency applications across the globe. Some of the Indian banks that have been targeted by this malware are Axis bank, ICICI Bank, Indian Bank, HDFC Bank, to name a few.



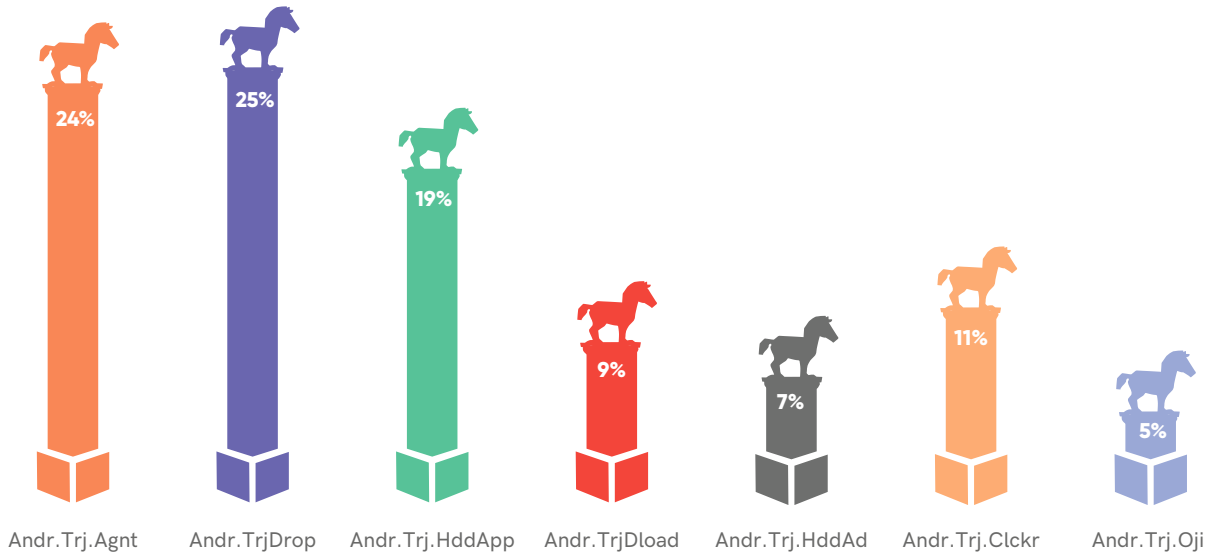

Once this app is installed on the device, it first ensures that it gains control of the accessibility service of the device to monitor the user's activities stealthily. It also masquerades itself as a genuine Flash Player Application and hides its icon to stay unnoticed. Whenever the victim opens any banking app, the Trojan opens a fake overlay screen, a phishing login page of that targeted application, where it asks the user to enter their confidential information. This malicious app also has Remote Access Trojan (RAT) and key-logger functionalities which steals confidential information when the user inputs account credentials by logging keystrokes, recording sound and saving the log file to send it to the Command & Control (C2) server. It also disables "Google Play Protect" to prevent its removal.

## The Significant Rise of Trojan Horses

The Android threat landscape in the last quarter of the financial year has experienced all sorts of popular Trojans, including fake apps, Banking Trojans, spyware, downloaders, and keyloggers masquerading as legitimate apps to deceive the victims into installing them.

This changing trend line of the existence of Trojans in the Android arena is interesting. Unlike the previous quarter, the threat actors have been seen using a few specific Trojans instead of using a diversified number of malware riddled apps.

### Trojan Detection Trend Lines




In contrast to the previous quarter, on analysing the stats received from K7 Telemetry, we found a significant rise in a few specific Android malware families such as Andr.Trj.Agnt, Andr.TrjDrop, Andr.Trj.HddApp, and Andr.Trj.Clckr. Other infamous Android Trojans such as Andr.TrjDload and Andr.Trj.Oji have also increased their momentum at a steady pace.

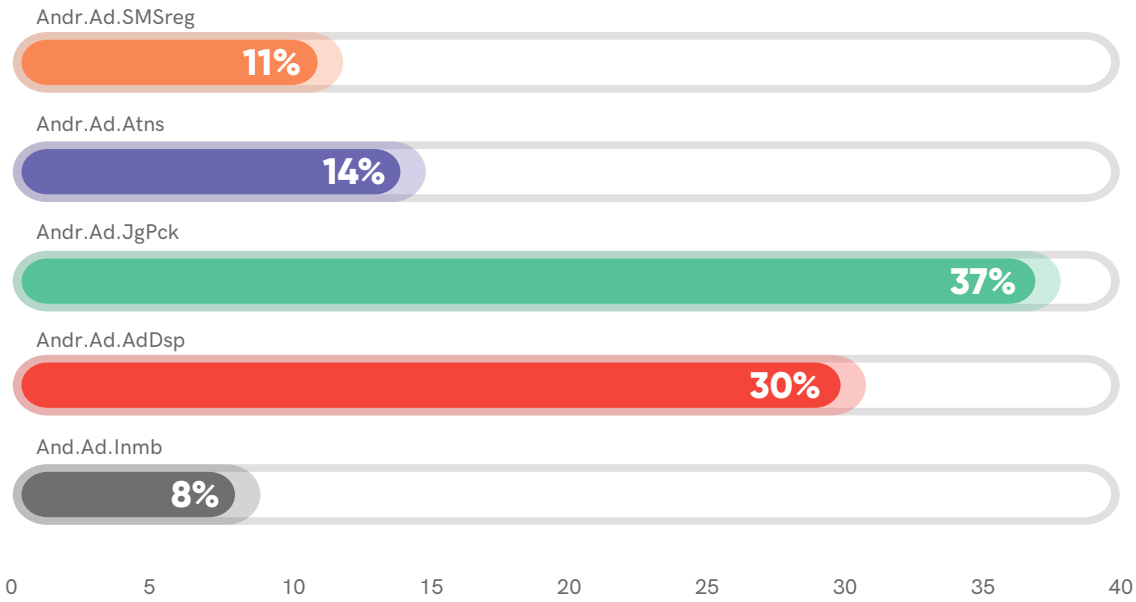
While Andr.Trj.Agnt has recorded a spike of two percent, Andr.TrjDrop has seen a spike of up to nine percent in comparison to the previous quarter. This quarter Andr.Trj.HddApp, Andr.Trj.Clckr, Andr.Trj.Oji and Andr.TrjDload have recorded more activity with an increase of eight percent, four percent, three percent, and one percent respectively.

Surprisingly, Andr.Trj.HddAd, popularly known as Hiddad, has plummeted by twelve percent, compared to the previous quarter. These statistics are quite significant in the Android threat landscape as we have been experiencing a ubiquitous influence of this ad-distributing malware since the past few quarters.

## The Adware Crisis

Despite a sharp decline, adware still reigns the Android threat landscape with a notable margin. During the period, we have encountered notorious adware such as Andr.Ad.JgPck, Andr.Ad.AdDsp, Andr.Ad.Inmb, Andr.Ad.Atns and Andr.Ad.SMSreg.

### The Fiery Five of Android Adware




Looking at the countrywide adware trend, the Andr.Ad.JgPck remained the most prevalent family of adware during this period, with a surge of eleven percent from the previous quarter. The Andr.Ad.AdDsp is at number two and also holds thirty percent of the total proportion of adware reported, an increase of eighteen percent.

The Andr.Ad.Atns and Andr.Ad.SMSreg have accounted for fourteen percent and eleven percent of all reported Android threats in the country.

## Malicious Apps from Google Play Store

Examining the global evolution of malware riddled apps on the third-party app markets and Google's official App Store, our threat researchers have found a massive rise of Andr.Trj.Jkr, aka Joker. The Trojan has infiltrated tens and hundreds of legitimate Android apps. This Trojan adopts umpteen cloaking and obfuscation techniques to generate malware-infected apps pitted against Google's defence techniques.

### Visibility of Malware Riddled Apps in Google Play Store


Other widespread malware like Andr.Trj.HddAd, Andr.TrjDrop and Andr.PUP.Blcklster, too, have camouflaged many legitimate apps with their malicious codes. Most of these Trojans and PUPs have mastered the art of disguise as a ruse.

# Tips to Stay Safe

- Install apps only from the Google Play Store
- Avoid clicking on unknown links delivered via SMS, emails and the like
- Always disable "Install unknown apps" on your Android devices
- Keep your security product up-to-date and scan all your apps with a reputable security product such as **"K7 Mobile Security"**

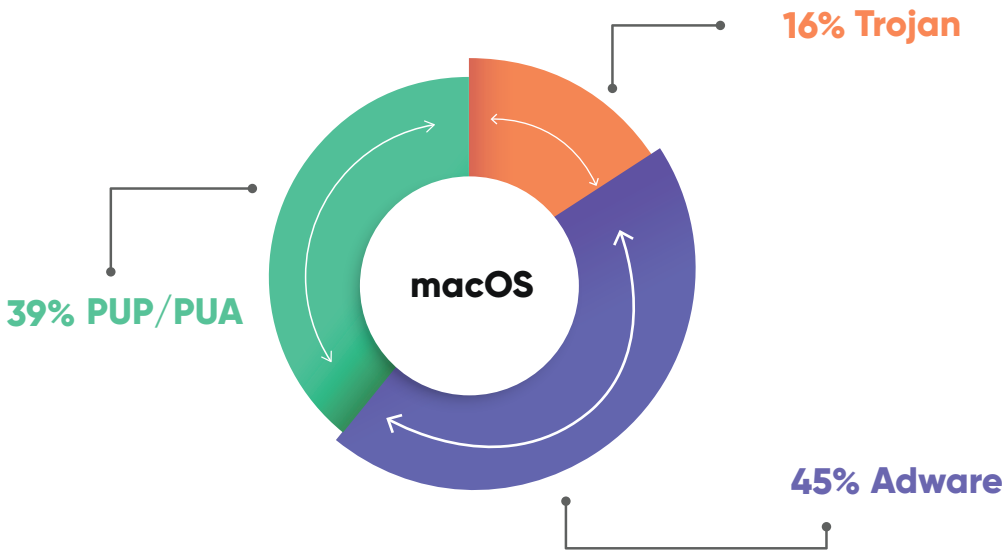
# Mac Attack

The evolving popularity of macOS-powered computers has encouraged the adversaries to try their luck in hacking these devices as well. The pervasive growth of new malware families in this platform offers enough evidence for this. In recent times we have experienced a shedload of new threats, attack methods, and multiple new camouflaging techniques. Besides designing new malware or restructuring an old one with new evasion techniques, adversaries are also offering a plethora of new malware on the Dark Web.

## But There is a Catch

Though the frequency of attacks has increased considerably on the macOS driven machines, the proportions and types of attacks are drastically different in contrast to those on other operating systems such as Windows. In this period too, we found oodles of Potentially Unwanted Programs (PUPs) and adware in comparison to malicious Trojans. This pattern has remained consistent over several periods, and it seems like it has become the new normal for this platform.

### Top Malware Categories Affecting macOS

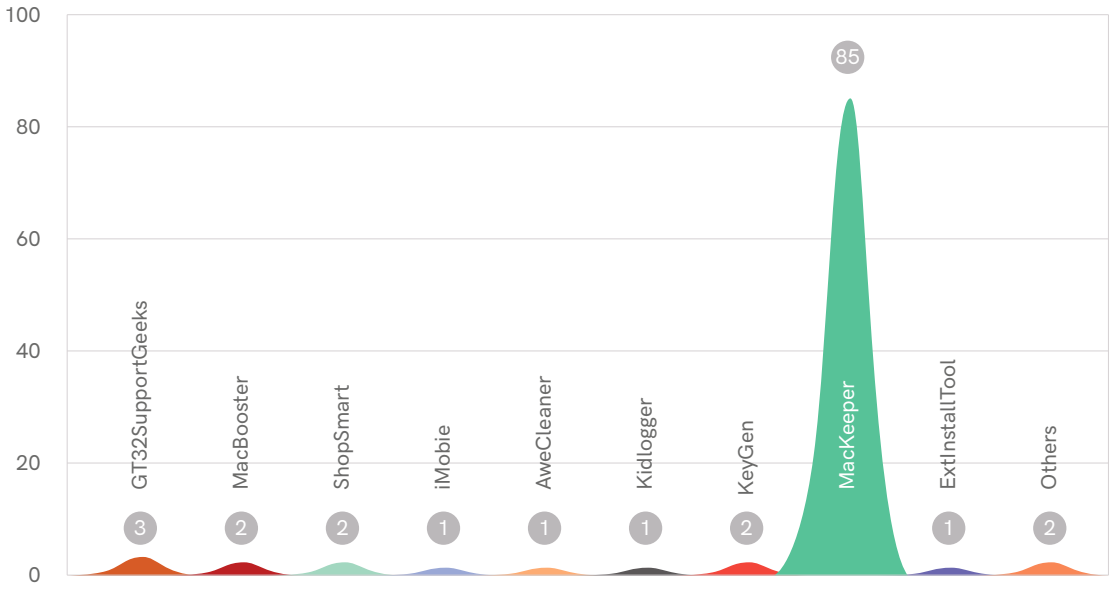



However, in contrast to the previous quarter, the frequency of adware has reduced by 9%, while the PUP and Trojan have shot up by 2% and 7% respectively. However, PUP and adware still stands out from the number of Trojan attacks.

## The Prevalent PUPs

Among the PUPs, MacKeeper topped the chart with a presence of 85%, implying that most of the macOS users have been targeted by this infamous PUP. Most of these PUPs, including the MacKeeper, are crafted to generate money by flashing advertisements on the victims' display.

### Most Prevalent PUP Types



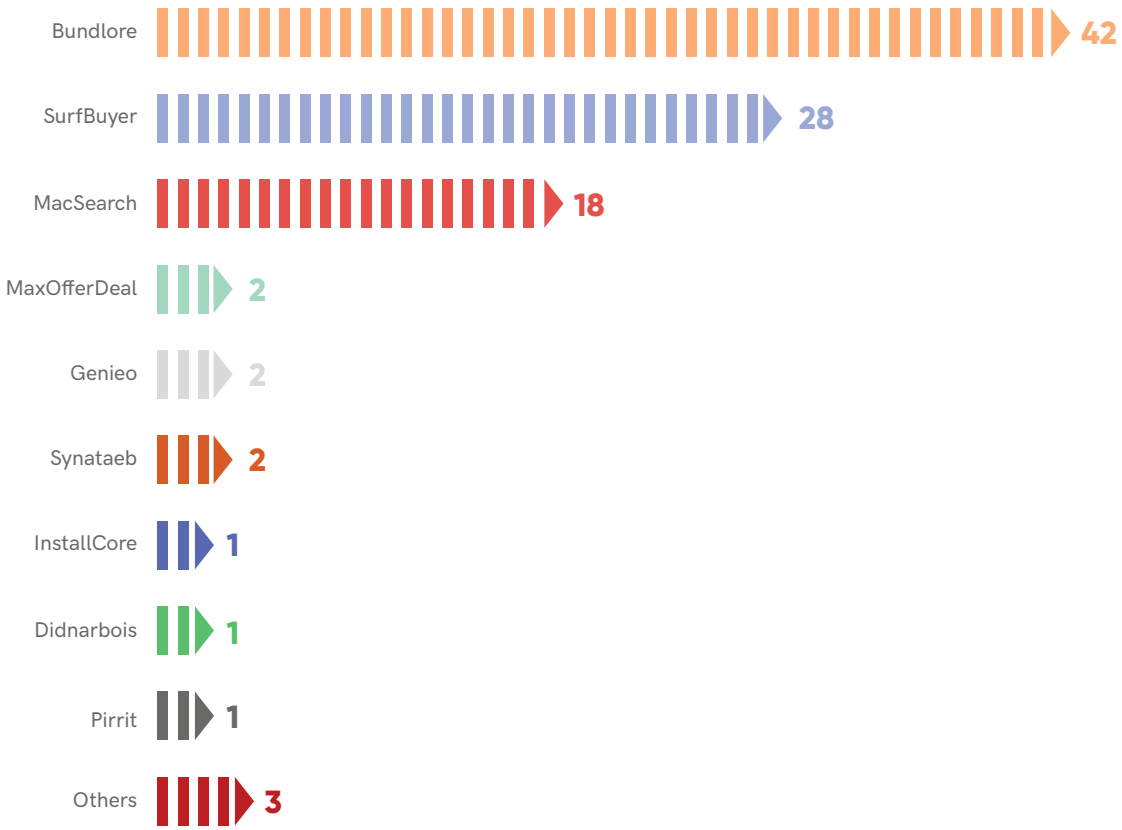

But there is a significant difference. The PUPs and adware load scary advertisements such as false malware alerts to force you to pay for a solution psychologically. These apps frequently open the system browser and launch many other hidden tasks to slow down the devices' performance, and they don't let you uninstall the program from your device.

Since Apple maintains a strict reviewing policy for each of the apps on its platform, these programs usually take the help of browser plugins to get into the system and do the damage.

## The Upsurge of Adware

Even after the substantial decrease compared to the previous quarter, adware still holds the top spot with the arrival of many new varieties. The presence of the top two adware, Bundlore and Surfbuyer, has nosedived from 52% to 42% and 32% to 28% respectively, in comparison to the previous quarter.

### The Trend Line of Adware Variant Detections

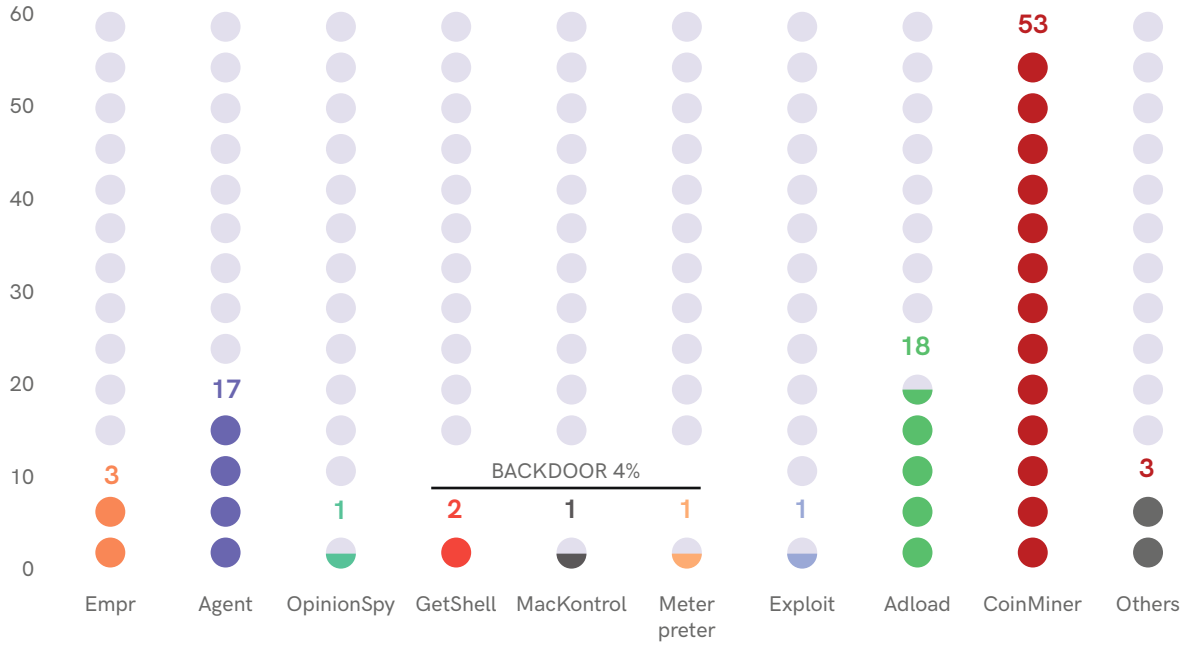



Interestingly, MacSearch, the third most popular adware, has increased its presence from 6% to 18%. Many new adware, too, has entered the macOS market with devious intentions. Such adware apps usually come as a bundler and carry an extra load of spyware, PUP, or other application with mendacious intentions.

## The Reign of Trojans

Despite the increase in the number of adware and PUP, the biggest surprise on the macOS threat landscape remains the increase of CoinMiner's popularity. Threat actors have probably understood that the outstanding hardware of most of the macOS driven machines could help them to mint more crypto money.

### Trojan Detection Trend Lines




Two other significant Trojans were Adload and Agent with a visibility of 18% and 17% respectively. Adload, known as an advertisement downloader, bombards the victims' device with lots of malicious advertisements, scam pages, fake notifications, and PUP installers while Agent is used mainly to be a part of the infection chain such as to aid in another malware installation process.

## Safety Guidelines

- 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

Reading the trendline of the cybersecurity threat landscape, anybody can make out that Remote Access Tools, spyware, keylogger, Trojan, PUP, ransomware, scareware, and other forms of malware are not going away. Apart from these attacks, we also feel that the COVID-19 themed cyberattacks are here to stay with us at least for a few more months to come and maybe around even after the pandemic is contained. And the malicious actors would pursue their agenda to innovate new luring strategies to make a dent on your system.

So to stay safe from such prevalent threats, we have given a set of precautions to shield yourself.

| 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 |
| Use a Virtual Private Network (VPN), wherever possible | Installs apps only from the official App Store |
| Upgrade your obsolete Windows OS to Windows 10 to receive latest updates and user support | Do not click on unknown links and links that you are not sure of as they could also be COVID-19 themed hoax emails (phishing scams) |

BACK TO CONTENTS

K7 SECURITY

www.k7computing.com



JUNE 2020