
# CYBER RISK MONITOR

K7 SECURITY

# CONTENTS

# THIS REPORT IS ABOUT...



Today, cybersecurity is no child's play. Adversaries are becoming more sophisticated day-by-day, adopting new technologies to evade the strongest defence measures to victimise users across regions, platforms, devices and demographics. It is important to focus on learning and understanding the modus operandi of cybercriminals to enhance holistic defence mechanisms.

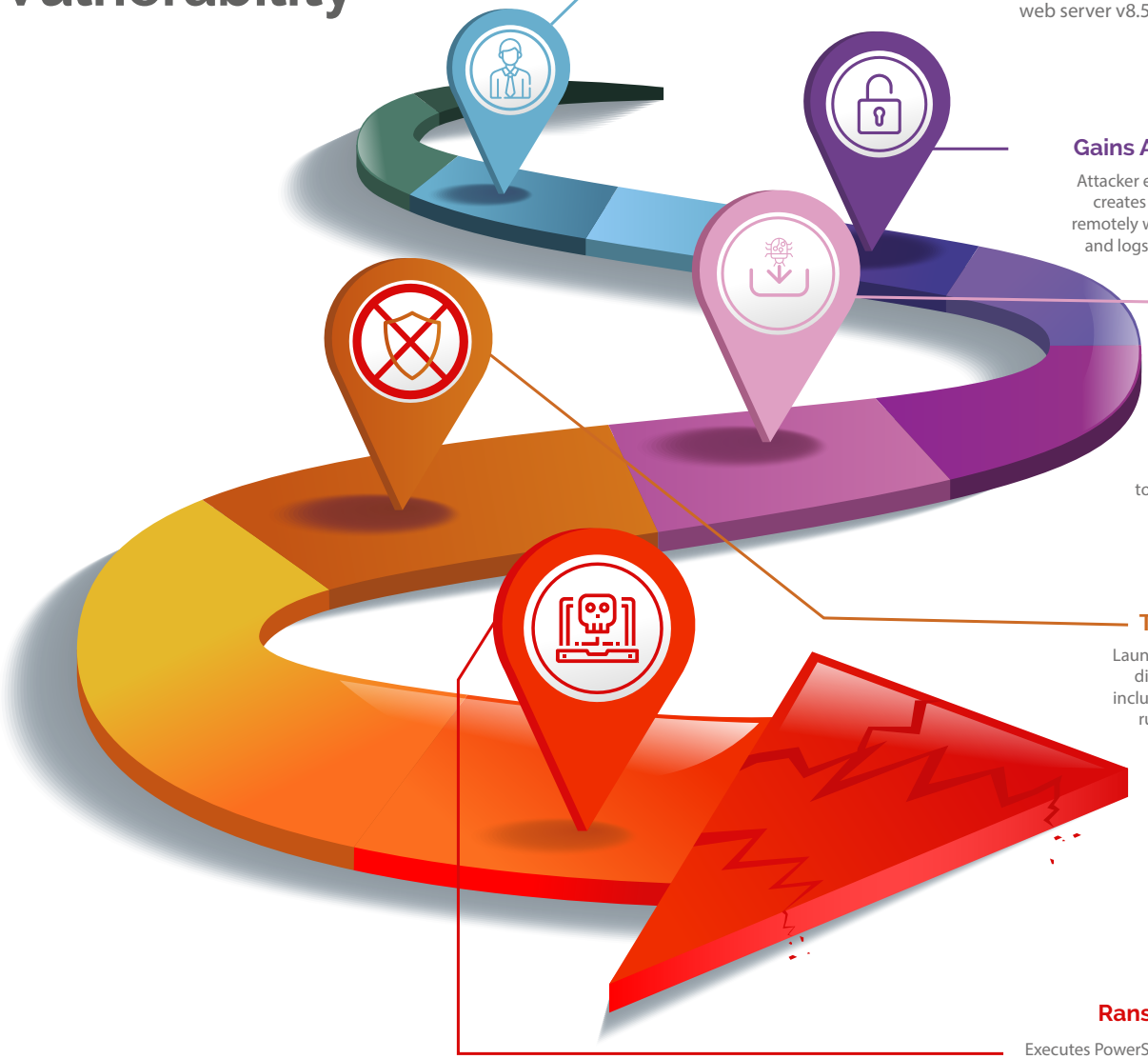
In this report we will take a closer look at some of the telemetry and experiential data compiled by our K7 Labs experts to portray the challenges faced by users and enterprises within India, providing insights into some real-life scenarios and explaining how to defend oneself or one's organisation against such threats.

In the last few months, K7 Labs researchers tracked numerous cyberattacks involving enterprises. Interestingly, many of these attacks occurred due to misconfigured or mismanaged servers, more than enough for attackers to carry out their acts with ease.

## Case Study 1: Exploiting Unpatched Vulnerability

In our first case study, the attacker penetrated the network by exploiting an unpatched vulnerability on a server exposed to the internet to gain access to the organisation and damage their entire network. Our initial analysis revealed that the administrator skipped installing a critical SMB server patch (security update for Microsoft Windows SMB Server – reference number 4013389). To summarise Microsoft's description of the security patch, it fixes a system backdoor vulnerable to remote code execution attacks. The rest of the Tactics, Techniques and Procedures (TTPs) of the attacker are described in the infographic.

# UNPATCHED
# Server Vulnerability



### Administrator skipped installing a critical SMB server patch

The server was not behind a robust firewall resulting in a few ports, including 80, 137 and 445, were accessible over the internet with IIS web server v8.5 hosted on port 80.

### Gains Admin Privilege

Attacker exploits vulnerability, creates two user accounts remotely with admin privileges, and logs on to the IIS server.

### Helper Tools

Installs third-party tools including Process Hacker.

### Tool Execution

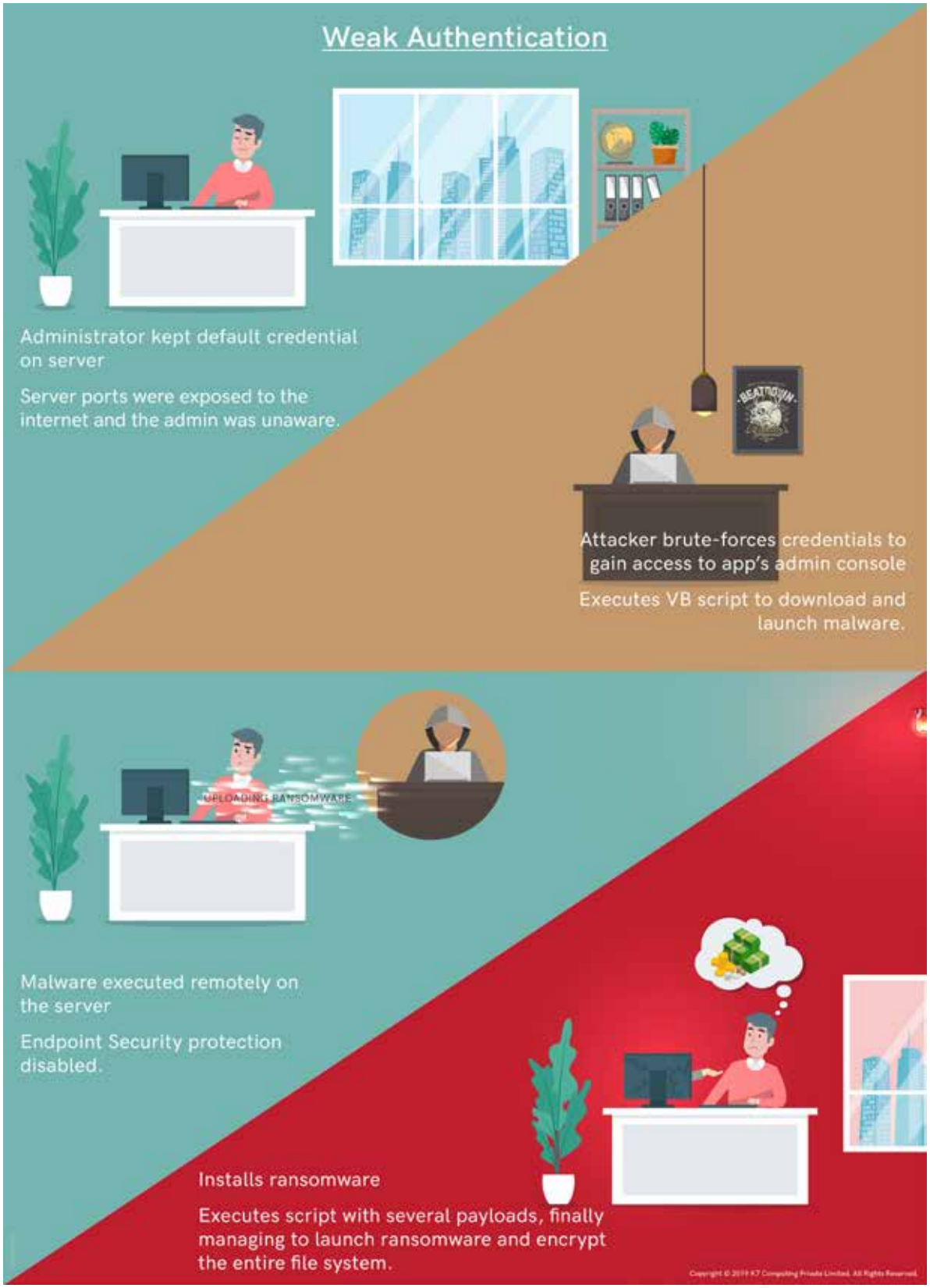
Launches installed utilities to disable myriad services including security protection running on the server.

### Ransomware

Executes PowerShell script with multiple payloads connecting to several IPs to download a variant of GandCrab ransomware.

## Case Study 2: Brute-Forcing Weak Password

In the second breach scenario, the attacker managed to gain admin privileges on the server due to its weak authentication. The system administrator had not changed the default credentials for the server application, and was utterly unaware of several network ports being exposed to the internet. Once the server was brute-forced, the attacker executed a tailored version of ransomware to encrypt its entire file system. Moreover, the server was found hosting a Minecraft game service as an internet scanning bot. A scanning "bot" is a program that continually scans the internet for vulnerable systems, and once found, it exploits vulnerabilities to transfer and install malicious code.


Weak Authentication
Administrator kept default credential on server
Server ports were exposed to the internet and the admin was unaware.
Attacker brute-forces credentials to gain access to app's admin console
Executes VB script to download and launch malware.
UPLOADING RANSOMWARE
Malware executed remotely on the server
Endpoint Security protection disabled.
Installs ransomware
Executes script with several payloads, finally managing to launch ransomware and encrypt the entire file system.

## Suggested Mitigations

In both the case studies, misconfigured servers (and sometimes services too) allowed the attackers to compromise servers. Furthermore, in the second case study, the system administrator was not even aware of publicly-exposed network ports on the server that helped the attackers to intrude and take control of the network, and didn't take timely action on the malware blocking notifications on the K7 Enterprise Console.

**To overcome the problem, we recommend a few key best practices:**

- Check the server's network and security settings to ensure its security before exposing it to the open internet
- Unused ports and services on the server must be blocked or disabled

# CYBER THREAT TYPE BREAKDOWN

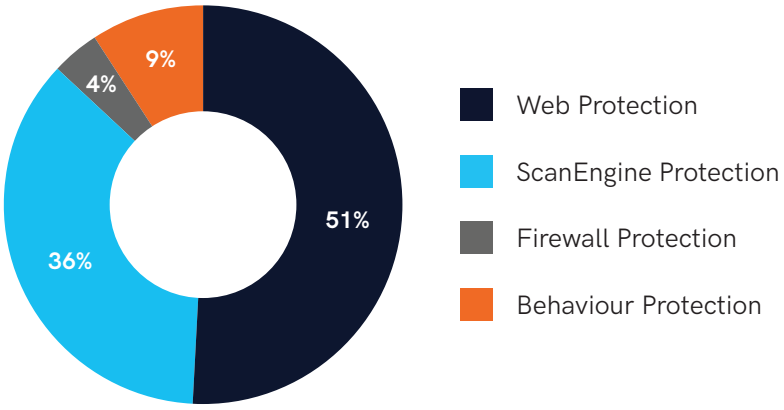


K7 Labs has tracked a significant spike in the frequency of cyber attacks across India over the last few years. The attackers have become more smart and lethal, adopting a variety of subversive ruses to fool users.

K7 Security focuses heavily on providing protection at every security layer to maximise the opportunities for stopping malware at various strategic stages in its attack chain.

## Attack Type Breakdown

According to K7 Labs telemetry data, web-based attacks remained the dominant form for mushrooming malicious programs floating in the cloud across the nation. During the last quarter, the number of web-based attacks was more than half of the total number of blocked threat events spotted in the country.



## Why So Many Web-based Cyber Attacks?

# MOBILE SECURITY SPACE



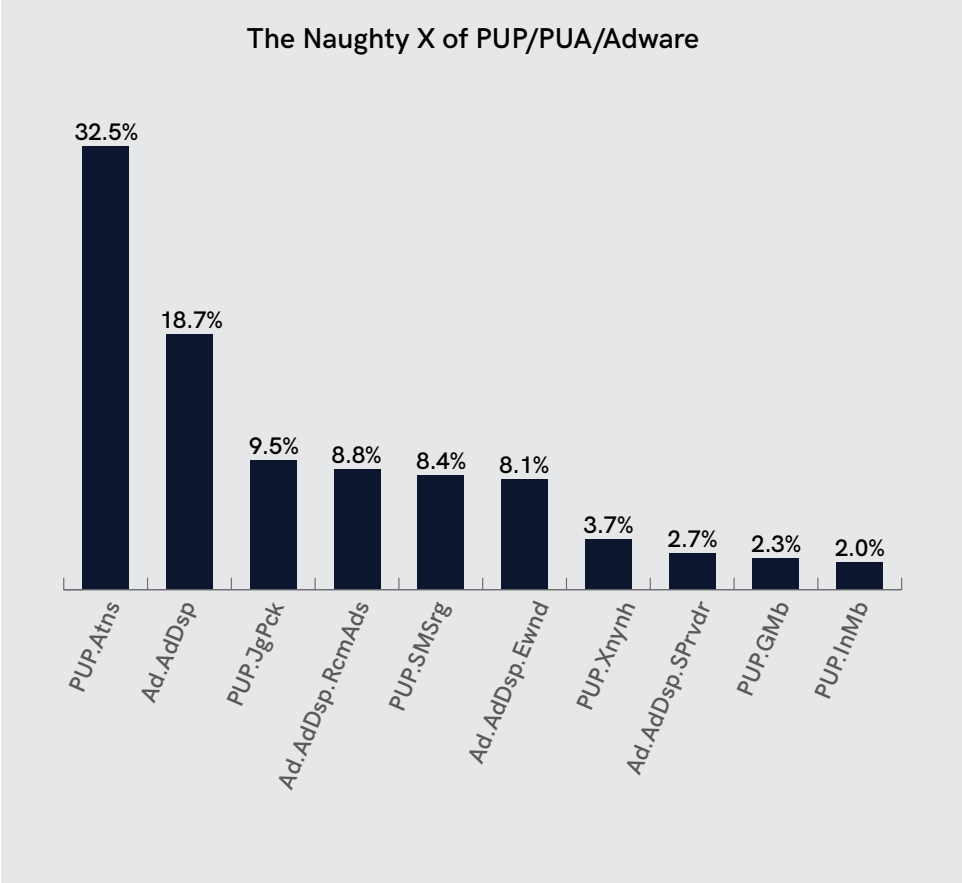
Cybercriminals are increasingly training their efforts towards breaking into your Android mobile devices using malware-loaded apps designed to exploit loopholes. In this section, we present the findings of our K7 Labs Mobile Security Team.

Initially, malware Android application packages (APK), especially legitimate apps injected with malicious code to bamboozle and attack users, were available only through scrappy app stores, but adroit cybercriminals have found ways to roll out these malicious apps on the Google Play store as well.

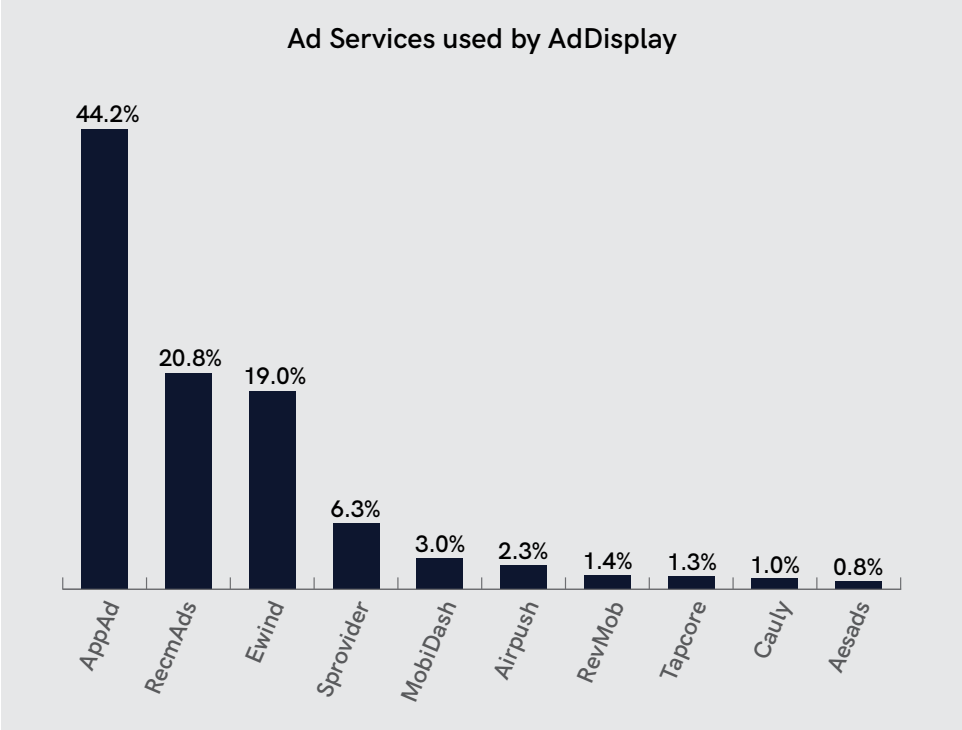
Being an open source platform, Android attracts numerous users and malware authors alike. Sometimes it is tough to identify suspicious activities usually exhibited by Potentially Unwanted Programs (PUP)/ Potentially Unwanted Applications (PUA).

For example, many Android users download apps via many external websites and third-party app stores. Usually, these apps are not listed in the Google Play store, instead being hosted through many unsecured external websites and third-party app stores, which makes it difficult to know about their suspicious nature at the time of download since there is no prior reputation-based information.

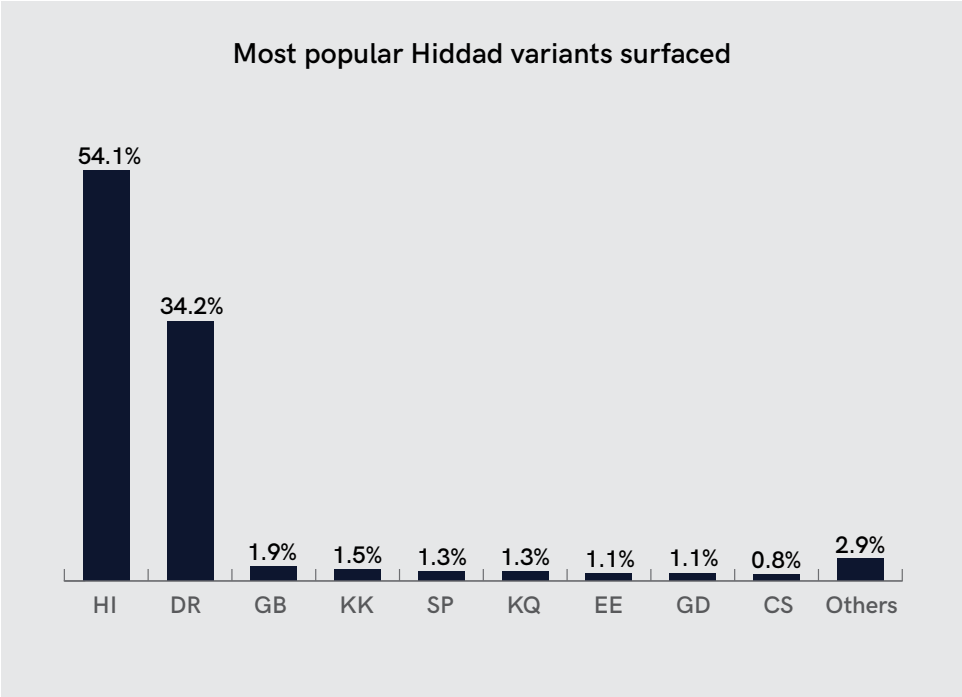
The following PUAs have masqueraded themselves as official/legitimate apps in third-party app stores and tricked users into downloading and installing them.



For instance, the primary intention of Andr.Ad.AdDsp is to promote advertisements and force the user to click on them. These ad banners catapult the users to download another app on the device or redirect to other app download links. We found they either use advertising services like, but not limited, to Andr.Ad.AdDsp.Arpsh, Andr.Ad.AdDsp.AppAd etc., or advertising frameworks/SDKs like Andr.Ad.AdDsp.Mbdsh to hide their malicious behaviour.

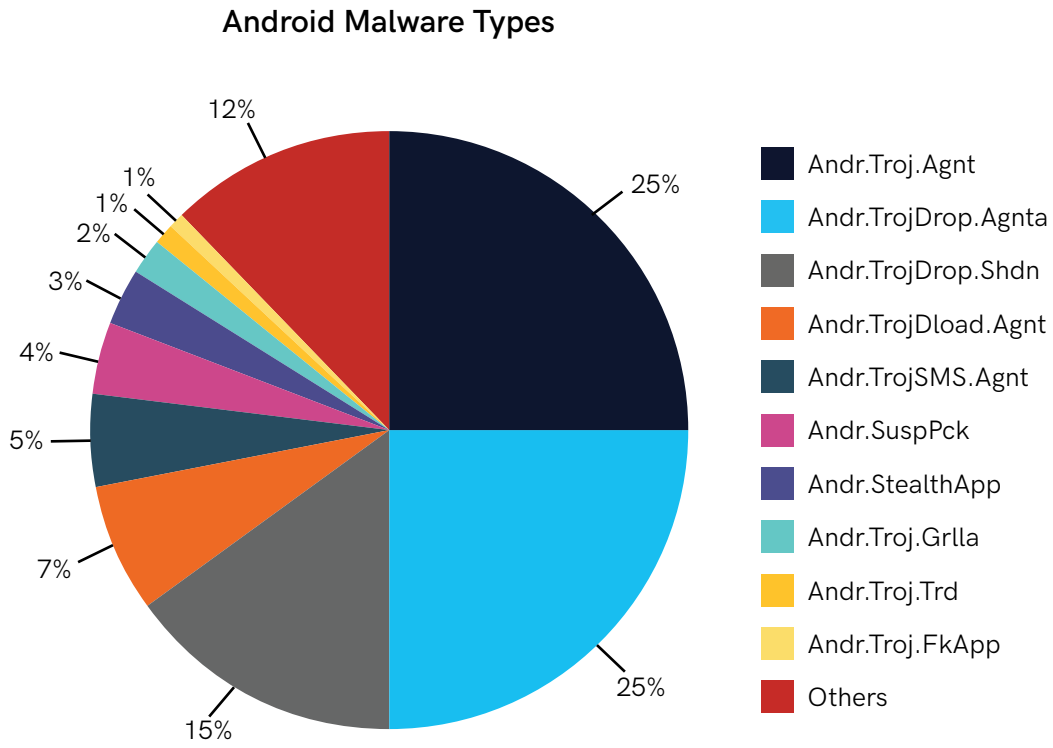


Another infamous adware dubbed Hiddad increases its trustworthiness in the Google Play store by coercing the user for an excellent rating to increase its visibility under a particular category. Interestingly, this variant has garnered more popularity in the last few months.




We at K7 Labs also discovered a spike in the number of camouflaged apps, referred to in the security industry as "Agent Apps", which are responsible for seeding malware onto the victims' device.

We found numerous instances of these apps in the country, though we have not yet ascertained whether these apps are downloaded from the Play Store or from third-party stores.

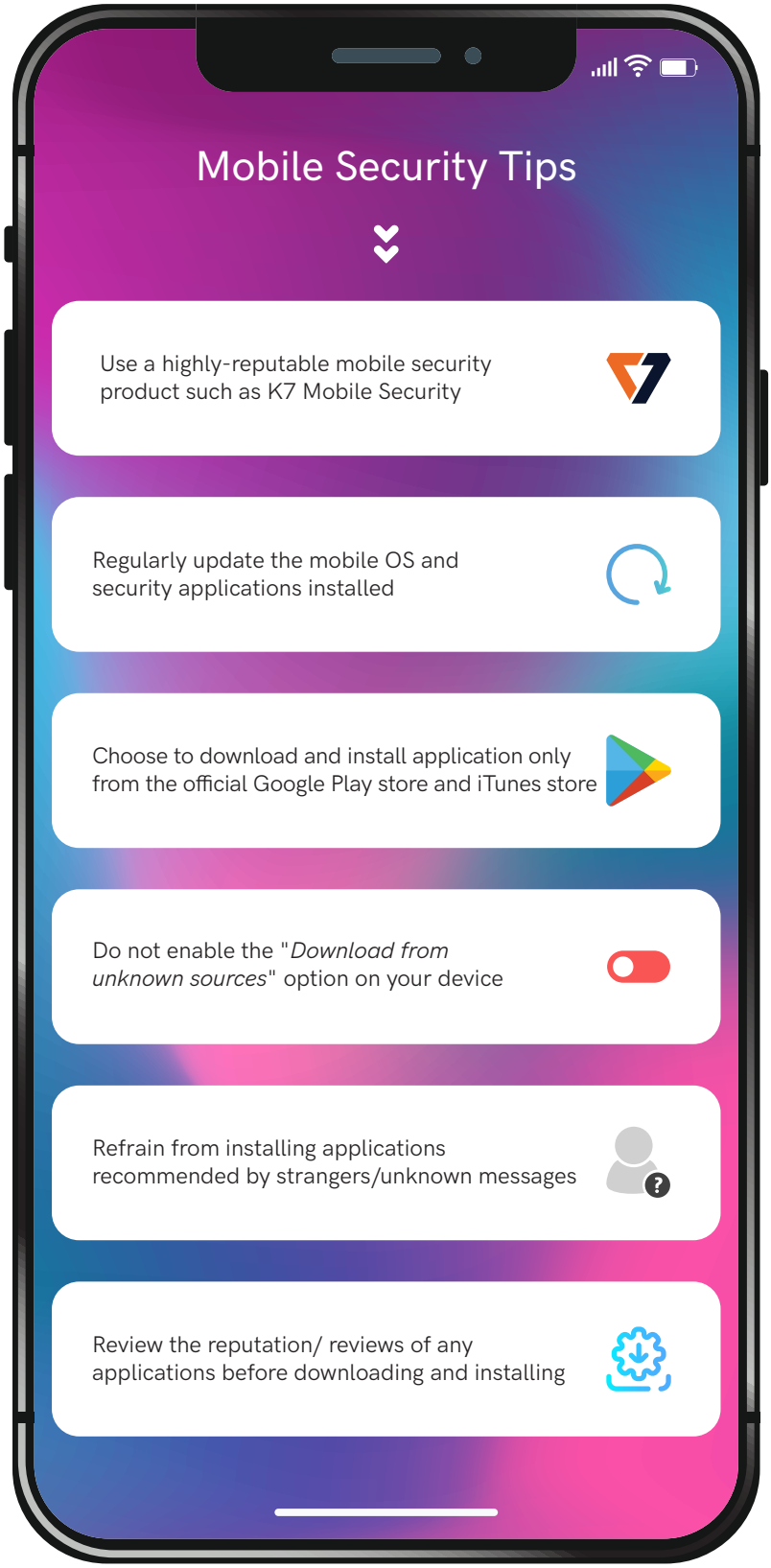



We noticed 8.44% of apps had installed themselves as system apps so that the user can't uninstall them easily.

Many of our users also encountered a certain number of apps (mostly Hiddad variants) pretending to be Google-service related apps like -

- Google Calendar Sync Adapter
- Google Videopro
- Google Apps
- Google Search

Besides games, the most alluring social engineering category for the malware developers remained video downloaders, porn content providers, internet-speed/sound boosters and gallery apps.


Mobile Security Tips
Use a highly-reputable mobile security product such as K7 Mobile Security
Regularly update the mobile OS and security applications installed
Choose to download and install application only from the official Google Play store and iTunes store
Do not enable the "*Download from unknown sources*" option on your device
Refrain from installing applications recommended by strangers/unknown messages
Review the reputation/ reviews of any applications before downloading and installing

# EXPLOITATION OF LOOPHOLES



The trend in vulnerabilities reveal what cybercriminals use for identifying and compromising target systems. Adversaries usually trigger one or more exploits for gaining control over a system or a network full of devices.

We at K7 Labs are actively tracking this space and protecting a plethora of networks and stand-alone devices from a variety of attacks. In this section, we depict a few real-life scenarios which will shed some light on a few key vulnerabilities being heavily used to compromise users' security around the country.

## The Rise of RDP Exploitation

RDP (Remote Desktop Protocol) offers excellent flexibility and power to control a system remotely. However, if the RDP access and usage are not regulated, controlled and monitored correctly, it can make the network prone to ransomware and other attacks.

In recent times we have noticed a spike in the number of ransomware attacks beginning with compromising RDP access, especially to servers. The K7 Labs Vulnerability Research Team found a massive chunk of servers in India were not secure. No wonder attackers were able to identify vulnerable RDP instances and attack unsecured RDP network ports to gain administrative control over the servers.

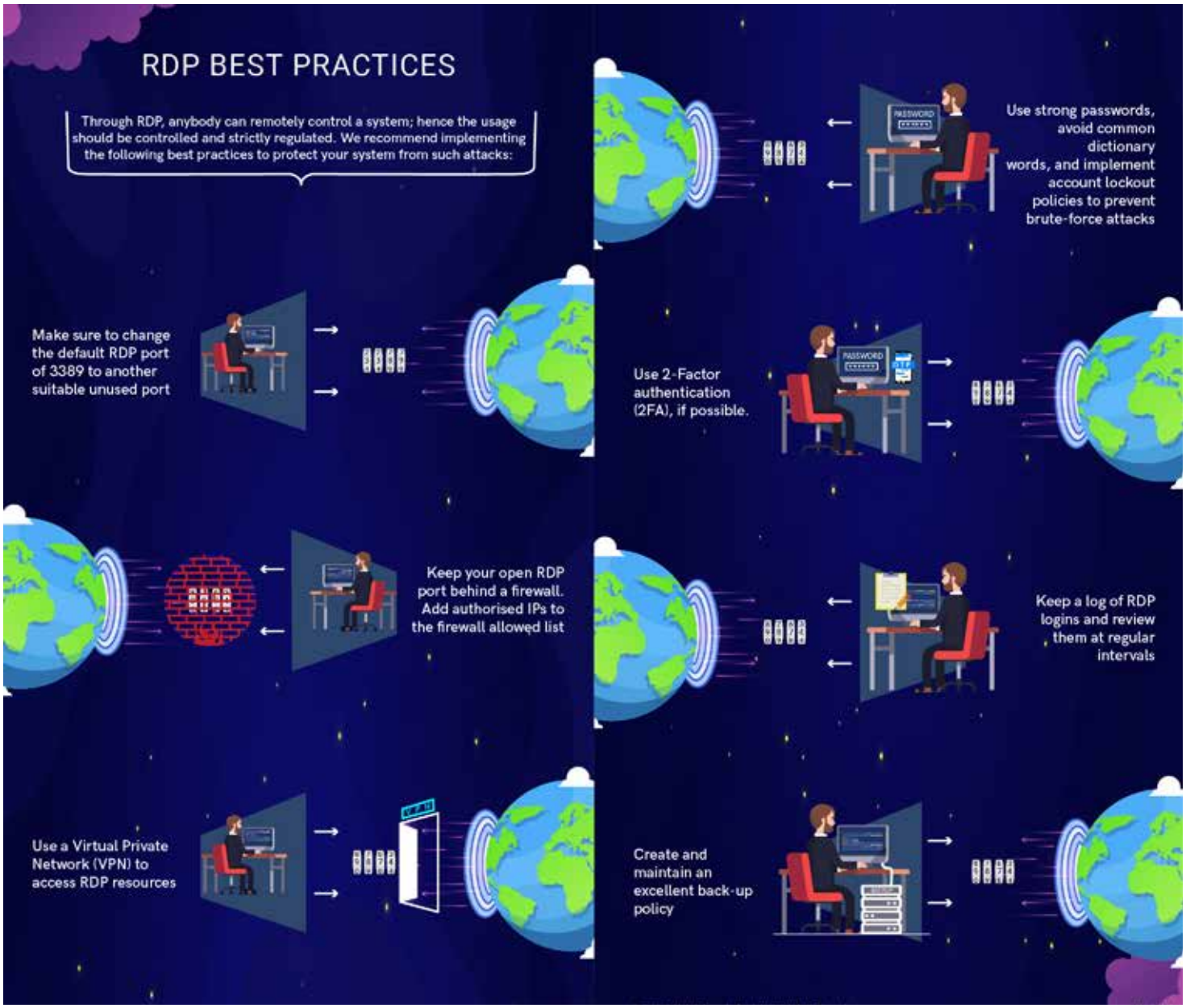
In many cases we found that numerous unused ports were left open, making the job easy for attackers to execute brute-force attacks, gain administrative control and execute malicious scripts to disable existing security software.

Ransomware gangs, like those behind the CrySIS and Samsam families, target enterprises by executing brute-force and dictionary-based attacks through open RDP ports to gain unauthorised remote access.

RDP-based attacks have become a dominant type of cyber threat in the country. The number of such attacks is likely to spike until network administrators and users become more cautious about system security.

## RDP Safeguards

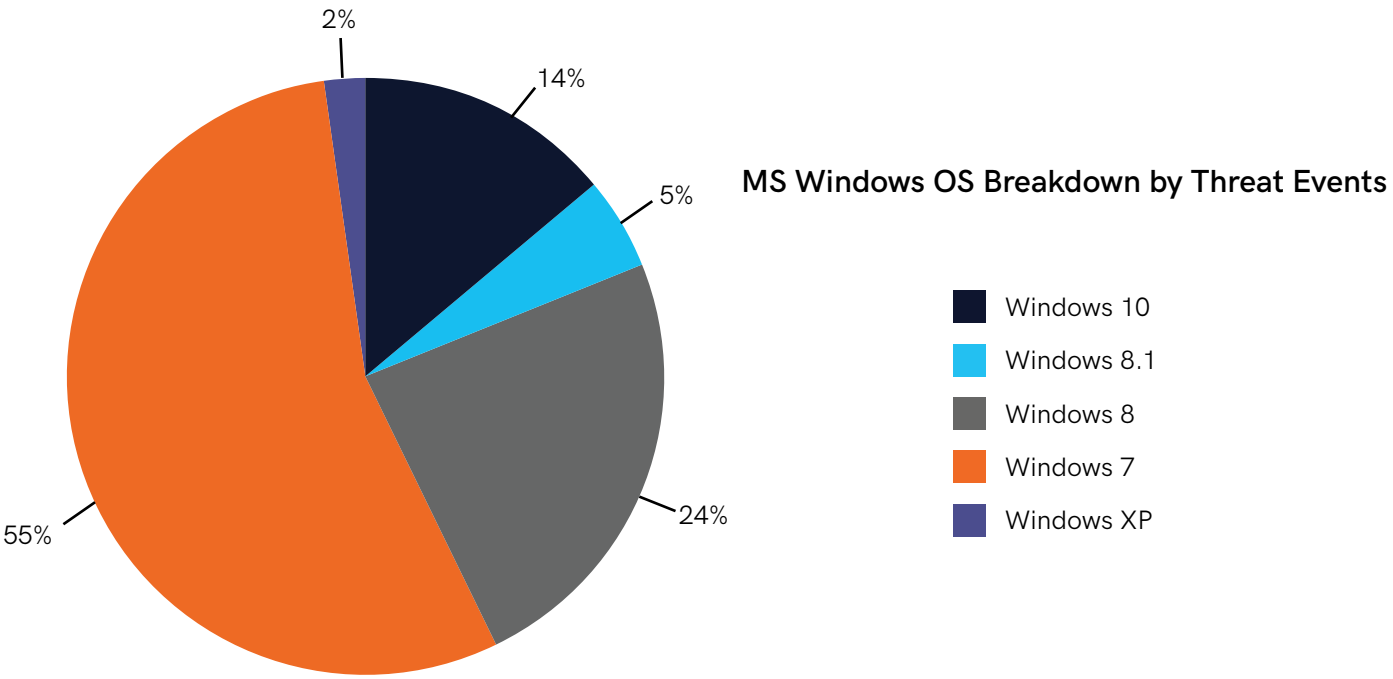
Since RDP allows remote control of a system, its access and usage should be strictly controlled and monitored. We recommend implementing the following best practices to protect your system from such attacks.



## Unpatched Operating Systems

Installing regular patches and updates is necessary for every user to remain safe. Unpatched vulnerabilities make the system far more prone to cyber attacks.

A large number of users in the country still rely on older, unsupported operating system versions of Microsoft Windows, many of them despite knowing the associated risks. From K7 Labs telemetry data concerning threat blocking, we found around 86% of affected Indian users are still far away from Microsoft's most secure OS which is Windows 10.




Around two percent of affected users are still using versions of Windows XP even after the end of support. Some of the known critical vulnerabilities in WinXP are CVE-2013-0810, CVE-2013-3863, and CVE-2009-1929. More than half of the affected Indian users (55%) are still using versions of Windows 7. Microsoft has already stopped its mainstream support in 2015 and announced the end of extended support in January 2020.

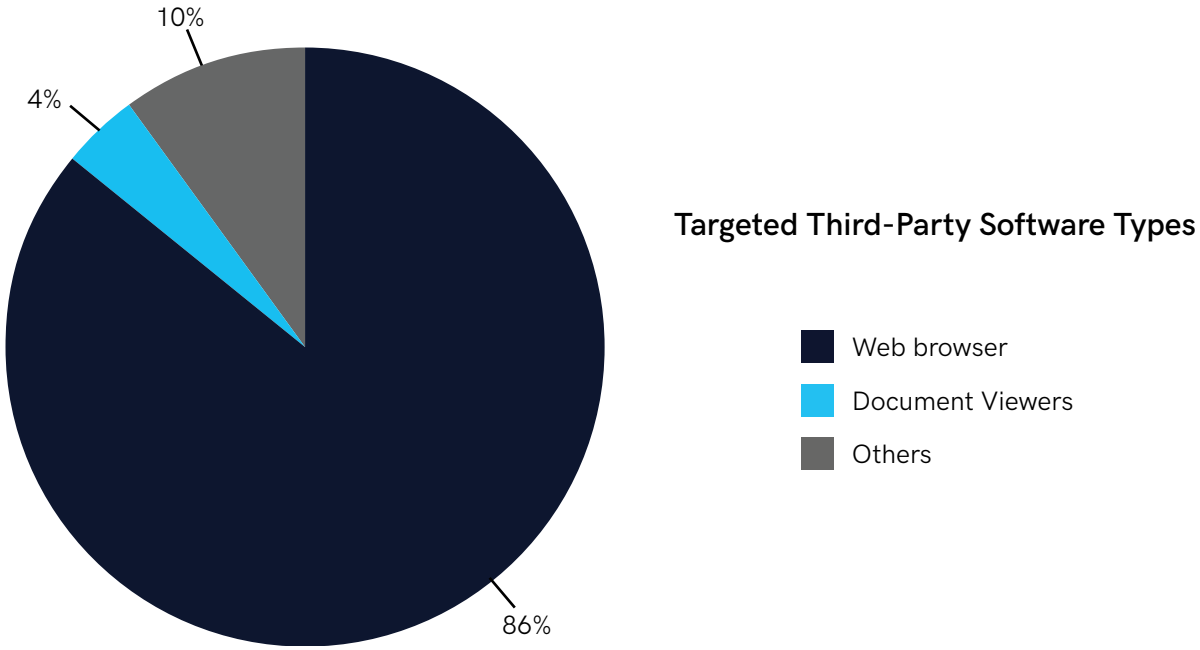
Not surprisingly, a high proportion, around 29%, of affected users are on Windows 8 and 8.1. Microsoft stopped mainstream support of Win 8 and 8.1 back in January 2018 and has announced an end to its extended support by January 2023.

Using all these dated operating system versions is highly risky even when the system is within the internal network as malware can pivot to internal networks from other internet-enabled devices on the same Local Area Network (LAN). In addition to upgrading their operating system, users must also install patches whenever available, especially for critical vulnerabilities.

## Vulnerable Third-Party Software

Exploitation doesn't restrict itself only to dated operating system versions. In reality, there are also numerous exploitable vulnerabilities existent in application software, utility tools, internet browsers, document viewers, runtime environments, etc. Triggering any such exploits can allow the adversaries to execute successful attacks, some of which may even be zero-day-based.

We have been blocking hundreds of attempts to exploit such vulnerabilities affecting a range of users.




According to our telemetry data, a significant chunk of blocked attacks was trying to snoop into the system by manipulating the web browser. Eighty-six percent of these were targeting various popular web browsers. We also observed a smaller proportion of blocks, 4% and 10% respectively, on attempts to exploit document viewers and other applications.

As always, keep all software on the system up-to-date by applying the requisite security patches whenever available.

# OUR RECOMMENDATIONS



K7 Security's proprietary telemetry data shows that many Indian users are under cyber attack. In this report we covered several types of attacks that K7 Labs has tracked, backed by real threat-event data, and we have recommended several best practices to remain safe whether you're an enterprise or a consumer.

Let us wrap up by summarising our top 3 recommendations by user segment, keeping in mind that what is relevant for consumers is also typically crucial for enterprise users.

| | Enterprise | Consumer |
|---|---|---|
| 1 | Apply critical security patches, especially on public-facing servers, and keep endpoint security software up-to-date | Avoid unsupported Microsoft OS like Windows XP. Upgrade your Windows OS version to fully-licensed Windows 10 |
| 2 | Employ strong authentication, especially for public-facing services such as RDP and WebApps | Keep all OS and installed software, especially cybersecurity software, up-to-date on both PCs and smart devices |
| 3 | Upgrade Microsoft Windows OS users to fully-licensed Windows 10 | Download Android or iOS apps only from their official app stores |

# CONFIDENCE IN AN INSECURE WORLD

K7 SECURITY



May 2019