



CYBER THREAT MONITOR- INDIA

Q3

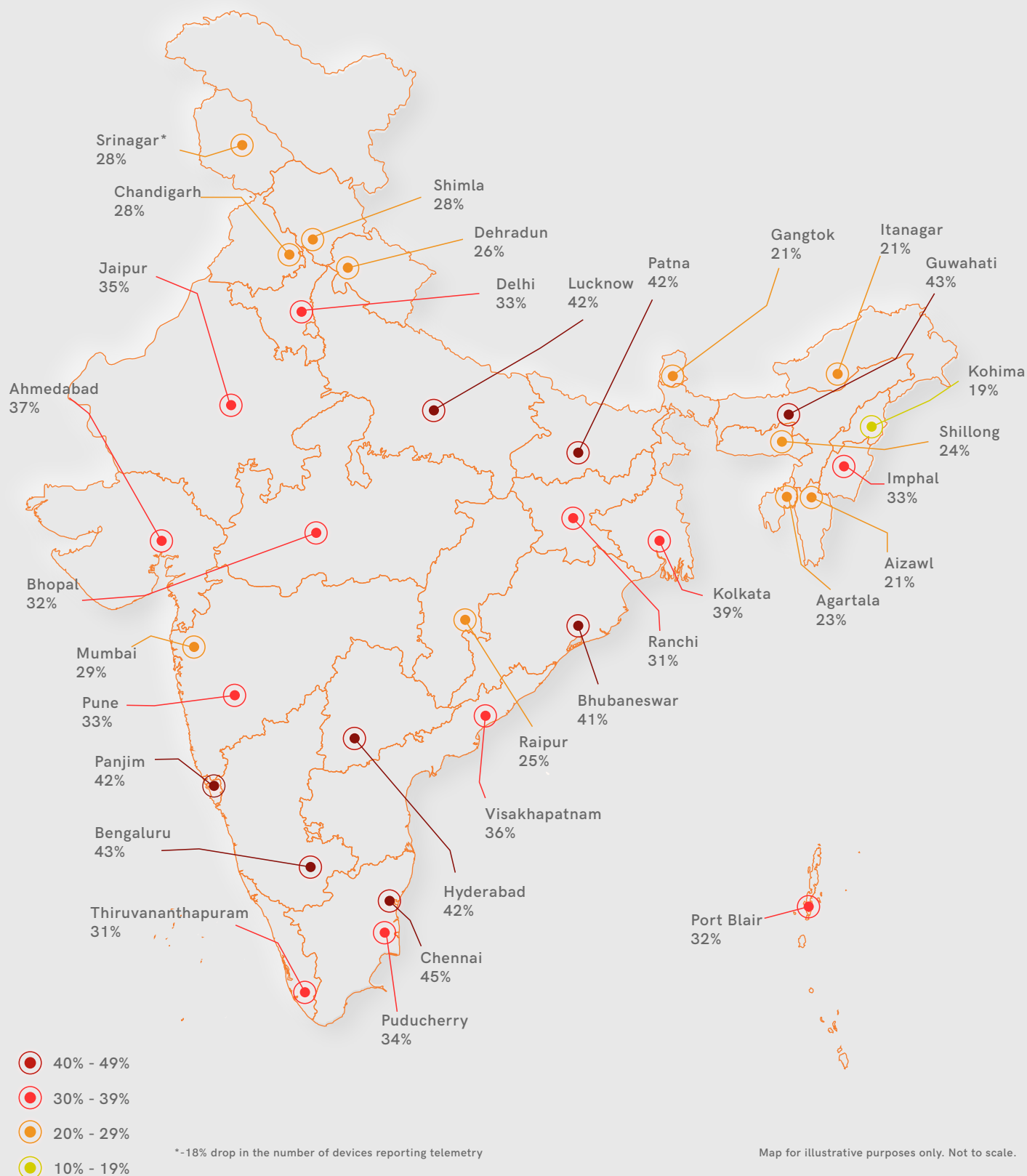
2 0 1 9 - 2 0 2 0

Exploring Indian Cyberspace





CYBER THREAT MONITOR - INDIA



Exploring Indian Cyberspace	5
Regional Infection Profile	6
Enterprise Insecurity	8
Colossus: Another RDP Attack: Case Study 1	8
Exploitation of Legitimate Pen Testing Tools: Case Study 2	9
Peekaboo: The Coinminer Attack: Case Study 3	10
Safety Recommendations	11
Vulnerabilities Galore	12
Vulnerabilities from the World of Android	12
Linux and the Enterprises	12
Windows Under Siege	13
Windows Malware Type Breakdown	13
Windows 7 Nostalgia	14
Mitigation Tips	15
Out-of-Date Security a Malware Magnet	16
The Necessity of Updating your AV	16
What Happens When you don't Update your Cybersecurity Suite?	16
Web Protection	17
ScanEngine Protection	17
Behaviour Protection and Firewall Protection	17
The Mobile Device Story	18
WhatsApp Stack Buffer Overflow Vulnerability (CVE-2019-11931)	18
WhatsApp Double-free Memory Vulnerability (CVE-2019-11932)	19
Word of Caution	19
The Adware Crisis	20
The Trojan Horses	21
Malicious Apps from Google Play Store	22
The Iniquitous Joker	23
MoqHao: Targeted Trojan attacks on Android and iOS users	24
MoqHao Victims	24
MoqHao Characteristics	24
The iOS Kill Chain	25
Tips to Stay Safe	26



Mac Attack	27
The Prevalent PUPs	28
The Upsurge of Adware	29
The Reign of Trojans	30
Cryptocurrency Exchange Targeted by a Fileless Trojan	31
Safety Guidelines	32
Danger In The Internet Of Things	33
Home Routers in Jeopardy	33
Perilous Web Server Flaw Strikes Many IoT Devices	33
Mitigation Techniques	33
Key Takeaways	34



EXPLORING INDIAN CYBERSPACE

The cyber threat world is like a game of chess where your invisible opponent attacks you, out of the blue. To avoid being systematically de-pieced, you should play all your moves in a timely fashion and intelligently. One calculated move by the adversary can make your exit with all your data, money and lots of other sensitive information with a perfect checkmate.

For being safe, sometimes you have to sacrifice some of your favourite habits, just like you do by sacrificing pawns, knights or a rook in the real chess game. But being obstinate would make you fall prey to vulnerabilities, just like a large chunk of users did in this period.

An unpatched software vulnerability is like the tiny hole in the balloon, enough to take everything away from you. On a mission to

keep the world and our beloved country safe from all the digital worries, we share cyber threat and software vulnerability details alongside the evasion techniques used by cybercriminals. And we have added plenty of that in the current edition of the Cyber Threat Monitor report with illustrated case studies.

We have hand-picked some real-life case studies from the different platforms, to explain how one silly blunder could make you the victim of cyber thugs. We would also tell you the required mitigation techniques as a defense measure against such threats!

REGIONAL INFECTION PROFILE

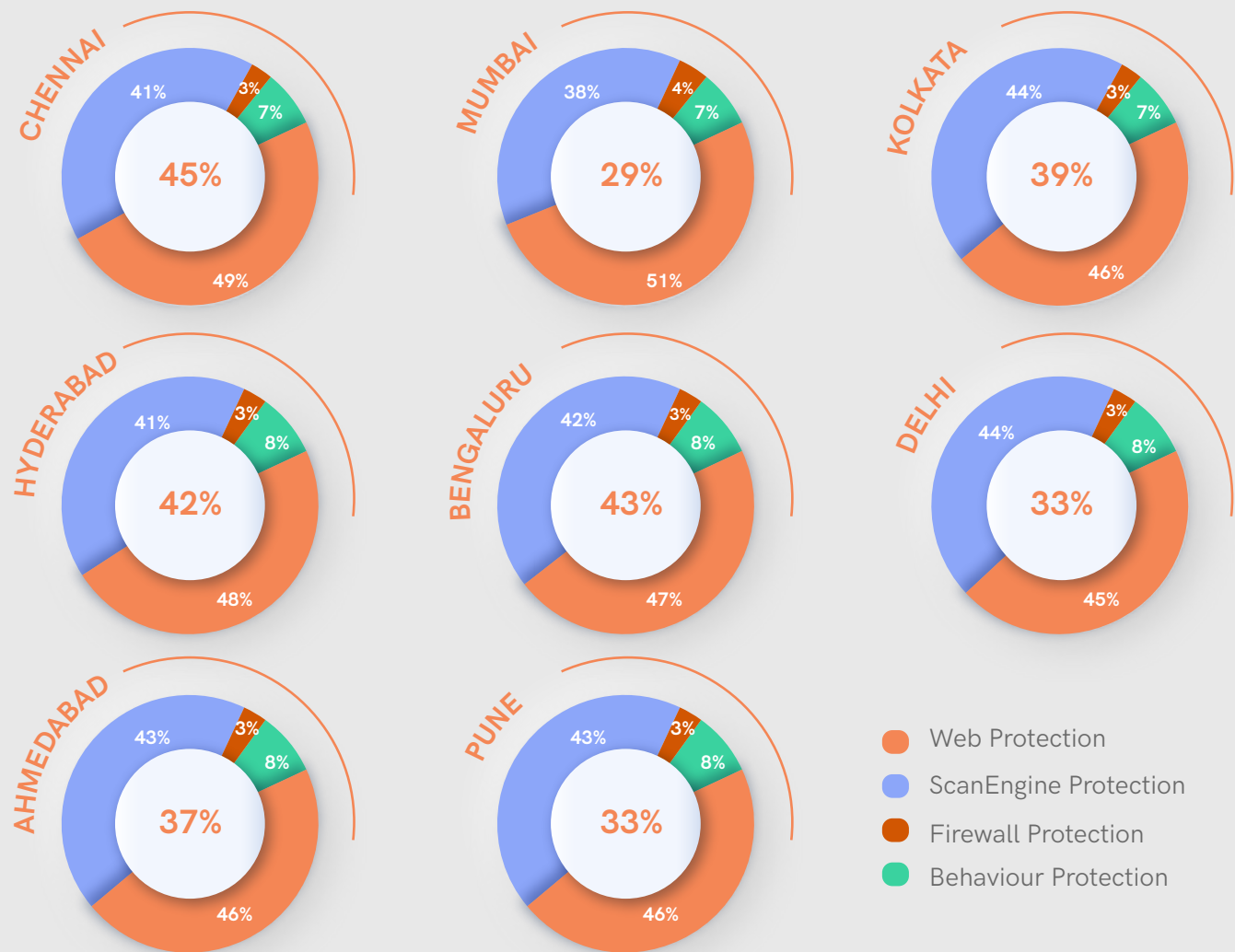


In the third quarter of 2019-20, we have noticed a considerable decline in the overall pan India cyber threat Infection Rate (IR) which is at 24%. IR is defined as the proportion of active and unique users who encountered at least one threat event which was blocked and reported to our K7 Ecosystem Threat Intelligence (K7ETI) during the specific period. This overall decline might be an outcome of cybercriminals shifting their focus towards Enterprises, SMEs and

SOHOs for minting more money, or it could be due to a quietening of activity over the holiday season.

Throughout this period there has been a steady increase in the number of attacks on enterprises. Noticing the volume of attacks, we also figured out the threat type pattern based on which the victims were targeted, categorised by cities.

The Metros And Tier 1 Cities - Infection Rate



The overall decline, however, doesn't necessarily indicate that users across the country were safer than before. Just that a few Indian metro cities like Kolkata and Delhi had

a marginal decline in the number of attacks compared to the previous quarter.

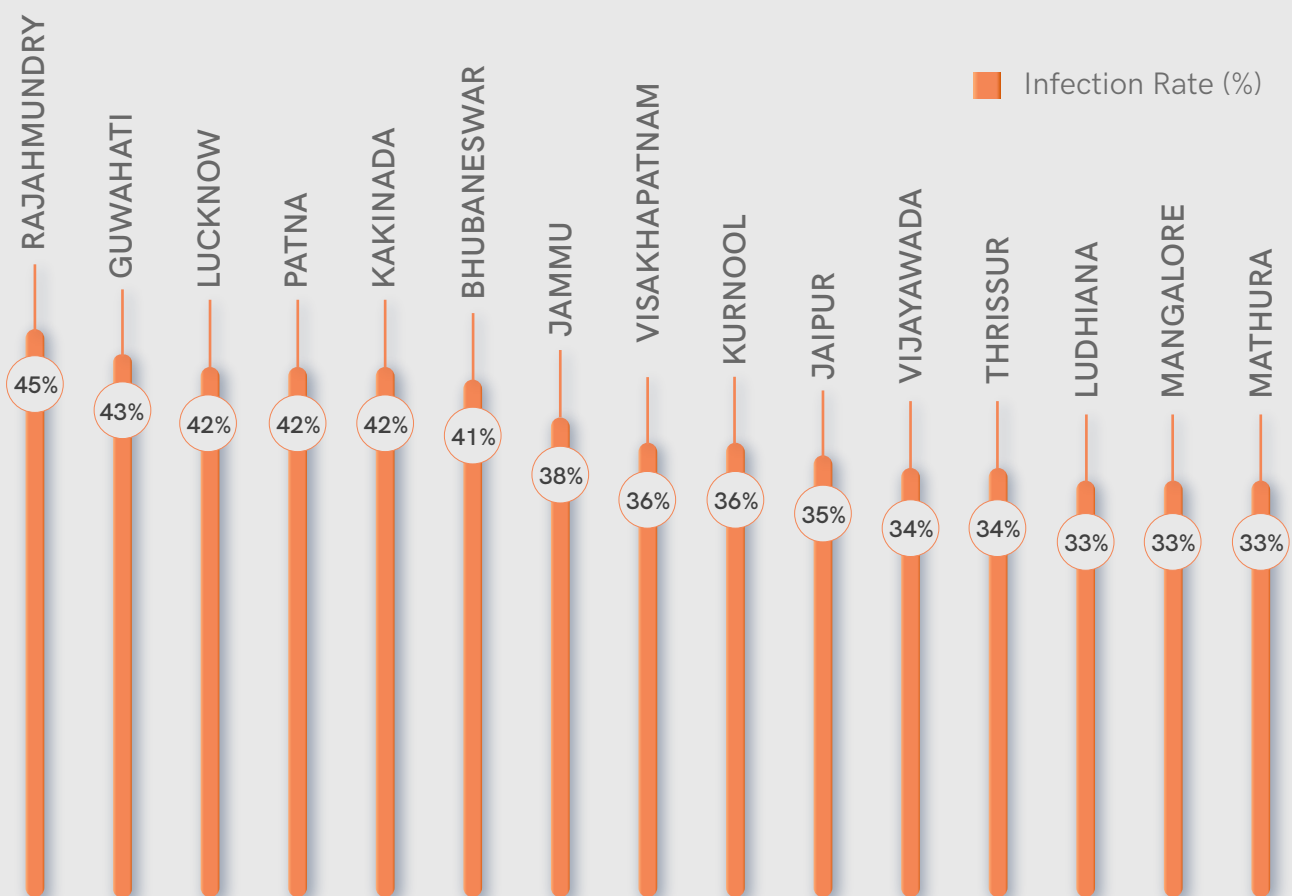


The attack portrait of Bengaluru and Hyderabad, however, were to the contrary. Cyberattacks in Bengaluru ballooned in Q3 with a four percent increase compared to the previous quarter. At the same time, over four out of ten netizens from Hyderabad experienced cyber-attacks in this period.

and Mumbai reduced by one percent each. In Kolkata and Pune, the IR reduced by two percent. Ahmedabad had the same statistics in comparison to the last quarter.

In Kolkata, Delhi and Mumbai, however, the IR had plunged. The IR in Delhi, Chennai

Top Fifteen Infected Tier Two Cities



The trend in the Tier-2 cities in India being exposed to cyber-attacks remains more or less the same as compared to the previous quarter. However, the figures in comparison to the last quarter have changed a bit. The IR in Patna, Guwahati, and Jaipur, the most affected Tier-2 cities of the previous quarter, has experienced an overall decline of five, two and five percent respectively.

Rajahmundry topped the IR list among the Tier-2 cities at 45%. This quarter also had a few new entrants to the top infected Tier-2 cities like Kakinada, Jammu and Kurnool among others with an IR of 42%, 38% and 36% respectively.

Cybercriminals continuously come up with new obfuscation and evasion tactics. In recent quarters, the target of their attacks has shifted to Enterprises and SMEs for more significant gains, with the trend continuing this quarter too. Besides exploiting the newly found vulnerabilities, cybercriminals still continue to depend on old tactics such as the Remote Desktop Protocol (RDP) and PowerShell for

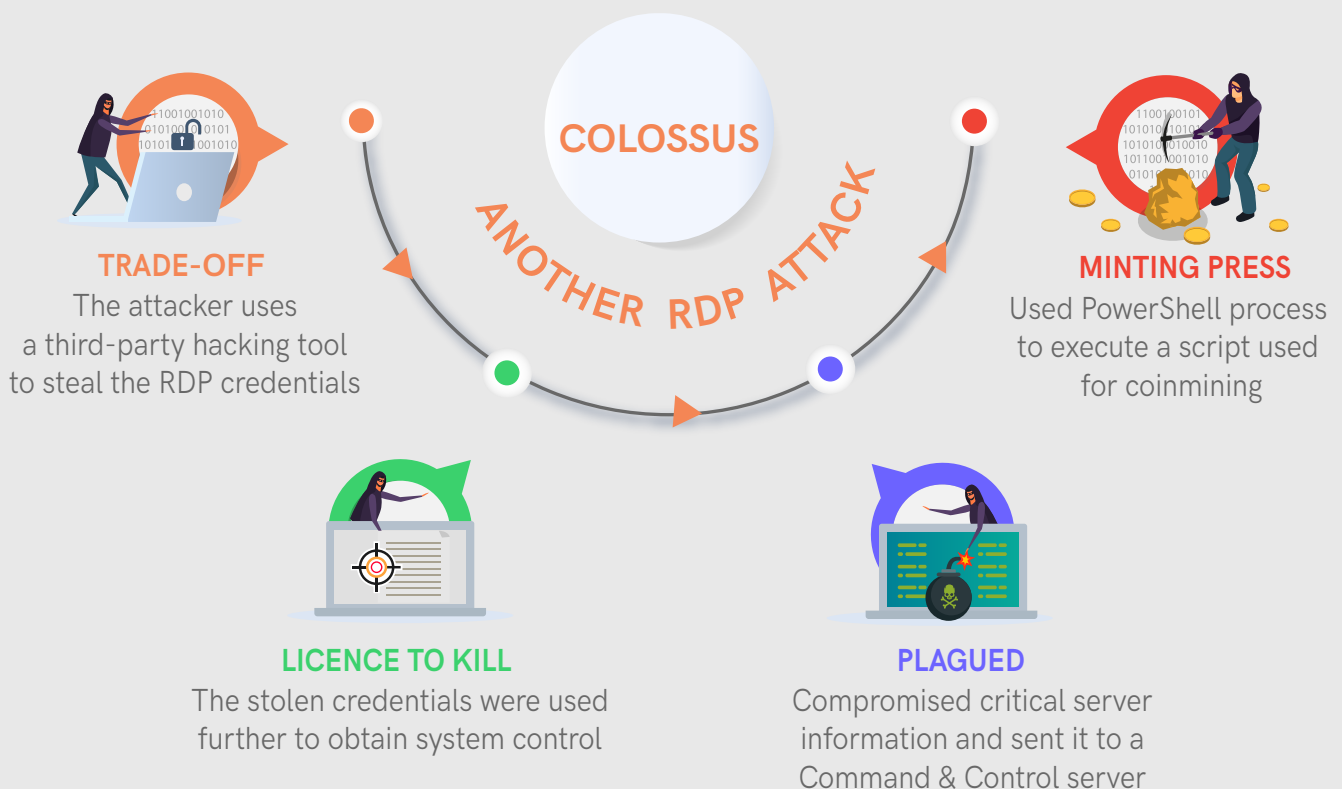
their nefarious activities, which also remained the most common form of abuse this quarter.

Given below are a few case studies which should make the organizations realise the importance of securing their network, failing which their entire organization's IT assets could be in jeopardy.

Colossus: Another RDP Attack: Case Study 1

One of our enterprise customers reported an issue about high CPU usage in an SQL server machine. On analysing all the running processes, we found a PowerShell process executing a script that was being used for coinmining. The script was also trying to establish communication with a specific IP for downloading additional software pertaining to coinmining and was also sending the customer's server information such as MAC address, domain information and hostname.

On investigating further, we found attackers abused RDP to gain entry into the affected system. During the attack, they dropped a tool for RDP connections called wfreerdp.exe and mimi.dat, part of Mimikatz, a hacktool to steal system credentials and which can be used in RDP attacks, to compromise the system. The detailed attack-flow infographic follows.





Exploitation of Legitimate Pen Testing Tools: Case Study 2

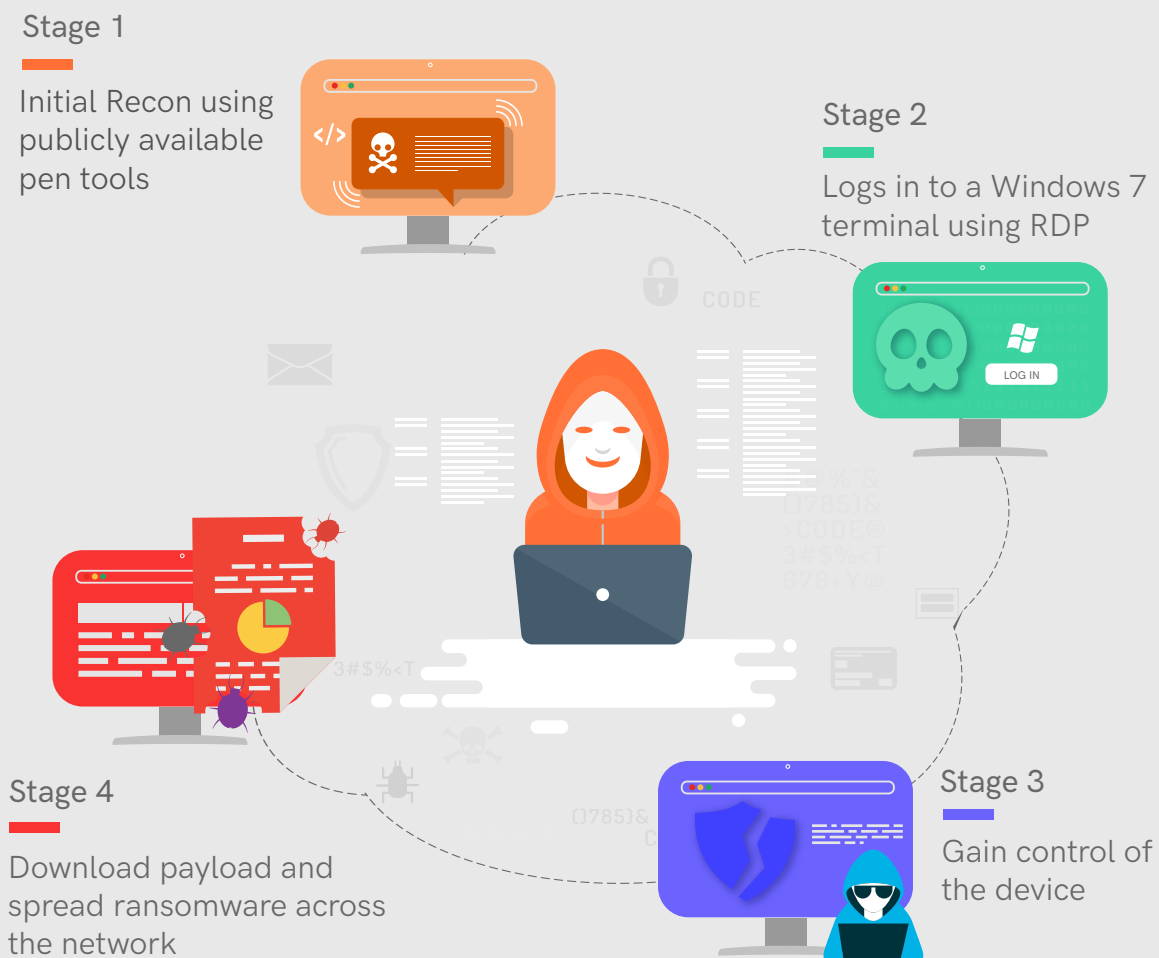
The spate of RDP based attacks, especially ransomware attacks, has been increasing over time and continues to sustain its intensity. In one such recent post-attack incident response, K7 threat researchers found a ransomware-affected Windows 7 system.

System forensics revealed that the attackers used publicly available tools for network enumeration, breaching, and to bypass security detection. These tools were later used to launch ransomware on the affected machine

and also for lateral movement.

Security admins are advised to make themselves familiar with some of the latest publicly available tools popular among attackers. They should continuously monitor their infrastructure to check for the presence of these tools on their network and their machines. The best procedure is to regularly monitor the logs to identify any suspicious/malicious activity and take the required action to remediate the same.

Exploitation Of Legitimate Pen Testing Tools





Peekaboo: The Coinminer Attack: Case Study 3

In another incident, one of our enterprise customers reported that a detection notification was being sent from multiple server machines by our Endpoint security solution every hour.

On analysing, we noticed that the AV was blocking the execution of a malicious PowerShell command which was encoded in base64 and could download coinmining malware from a malicious URL.

Digging deeper, we figured out that the Task Scheduler's registry had this malicious entry

which was scheduled to run hourly. However, this was not showing up in its GUI, as it was using the hidden task scheduler option.

We inferred that the malicious blocks must be loaded in memory and the scheduler was running from there, as the malicious schedule was still running even after removing the Task Scheduler's registry entry. After removal of the persistence entries, the customer was requested to restart the server, and the malware was gone on reboot. The full attack chain is as follows.

Peekaboo: The Coinminer Attack



Start Off: A process was initiated through a Windows Registry entry for executing a PowerShell command



Welly: The PowerShell command was capable of downloading a coinminer from a malicious URL



Dodge: The process loads itself to the system memory to evade detection



Safety

Recommendations

- Ensure a strong password policy for RDP users
- Change default settings used for configuring RDP
- Change the default port that RDP listens on
- Secure your device by keeping it up-to-date and patched for the latest vulnerabilities

VULNERABILITIES GALORE



Finding and fixing weaknesses in any software is an ongoing task. Therefore all the software, apps, browser, operating system and device driver makers spend enormous amounts of time to find out the existing flaws which could

be exploited and fix them at the earliest. But many of them get discovered by the attackers much before the developer notices or rolls out a fix, resulting in a successful cyber-attack.

Vulnerabilities from the World of Android

Sometimes vulnerabilities found in commonly used services help the attackers to victimize several people to fulfil their malicious intent. In this quarter, the vulnerability CVE-2019-2114 found in Android OS service NFC Beam, also popularly known as Android Beam, exposed millions of smartphone users to the clutches of cybercriminals. The NFC Beaming service acts as an alternative to Wi-Fi and Bluetooth for data transfer. It lets an Android user send/receive apps, images, videos and different files to another nearby device. This vulnerability allows an NFC system application to bypass the 'Install unknown apps' check while installing applications. A rogue device like a rogue payment terminal can use this vulnerability to infect devices with malware. An NFC system service in Android devices has permissions to install applications on the device. Using this vulnerability, a malicious NFC-enabled device

can send a specially-crafted request to the victims' Android device requesting it to install a malicious app. This affects Android versions 8 (Oreo) and higher.

Google patched this dangerous vulnerability through its Android patch in October 2019. Users are requested to apply the patch to protect themselves from this type of exploitation.

StrandHogg is another minacious weakness found in the Android operating system, which, when leveraged, could grant attackers access to private SMS conversations, photos, login credentials and a lot more. It allows attackers to abuse legitimate apps to deliver malware by spoofing the same. The vulnerability affects all Android versions, including the latest Android Q, aka version 10.

Linux and the Enterprises

However, Android was not the only operating system platform to hit the headlines for the wrong reasons. The good old sudo command of Linux was also found riddled with the CVE-2019-14287 vulnerability. The vulnerability allows any user permitted to execute commands, by elevating their privileges to any user other than root USING SUDO, to execute commands as a root user. This vulnerability can be exploited to bypass security and run arbitrary code. It impacts all sudo versions before 1.8.28.

Another security flaw that deserves attention

is CVE-2019-16928, a vulnerability present in Exim, a famous open-source Mail Transfer Agent (MTA), that allows remote attackers to execute arbitrary code or to crash the server. It affects versions from 4.92 up to and including the latest version 4.92.2.

Likewise, the BlackDirect vulnerability allows attackers to takeover Microsoft and Azure Accounts due to trusting unregistered URLs and perform malicious actions on their behalf. This mainly impacts Microsoft's OAuth 2.0 applications.

WINDOWS UNDER SIEGE



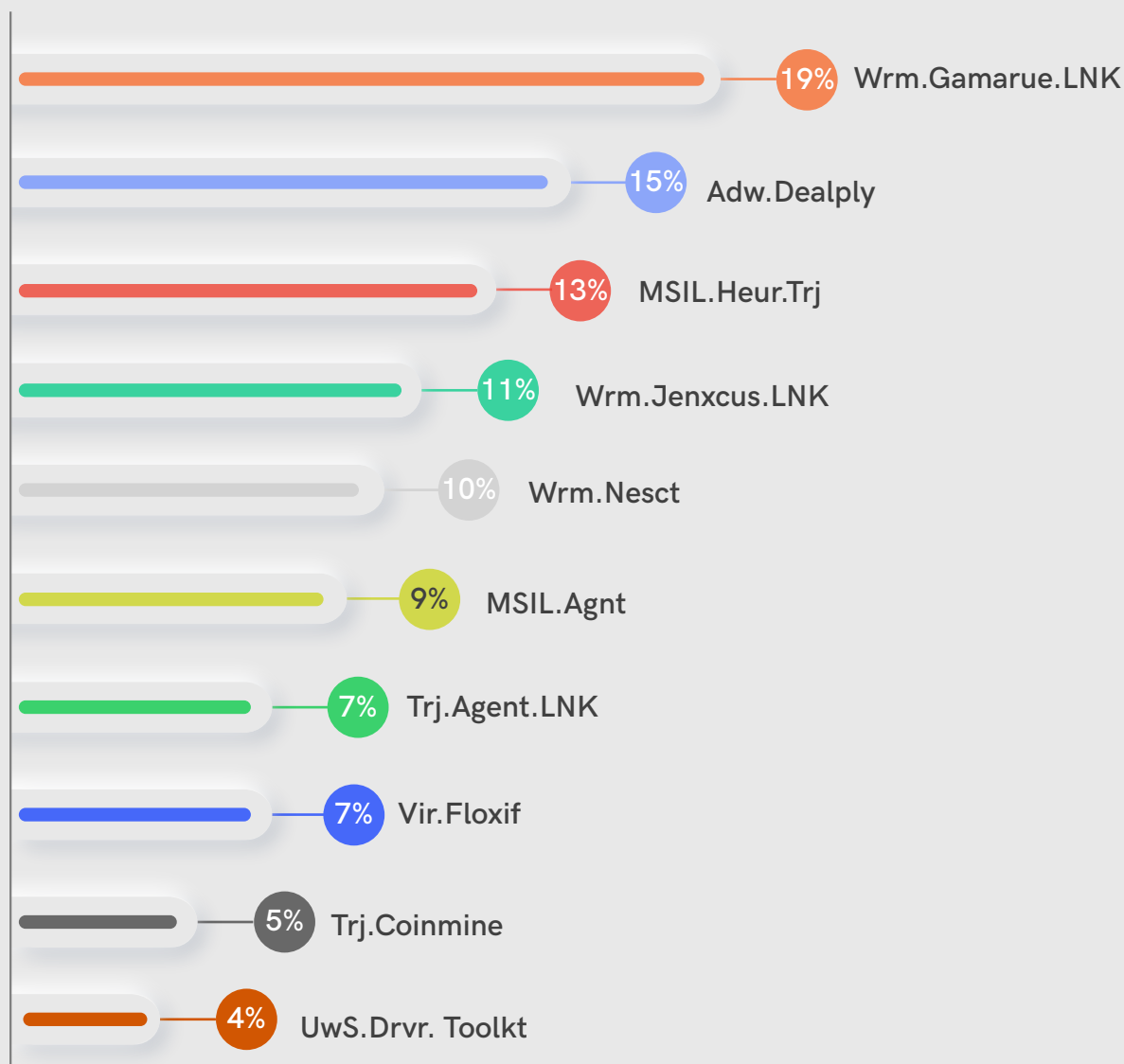
Windows Malware Type Breakdown

Despite this quarter bubbling up a few new and exciting families of malware, Wrm.Gamarue.Lnk managed to hold the throne even in Q3, even though it remained a little less prevalent than in Q2. However, almost all of the significant malware families like Adw.Dealply, Wrm.Jenxcus.LNK, Wrm.Nesct, MSIL.Agnt, and Vir.

Floxif had their own share of the prevalence pie this quarter.

The upward trend of many infamous malware families threatened both Enterprise and personal Windows users.

Split Of Windows Top 10 Malware



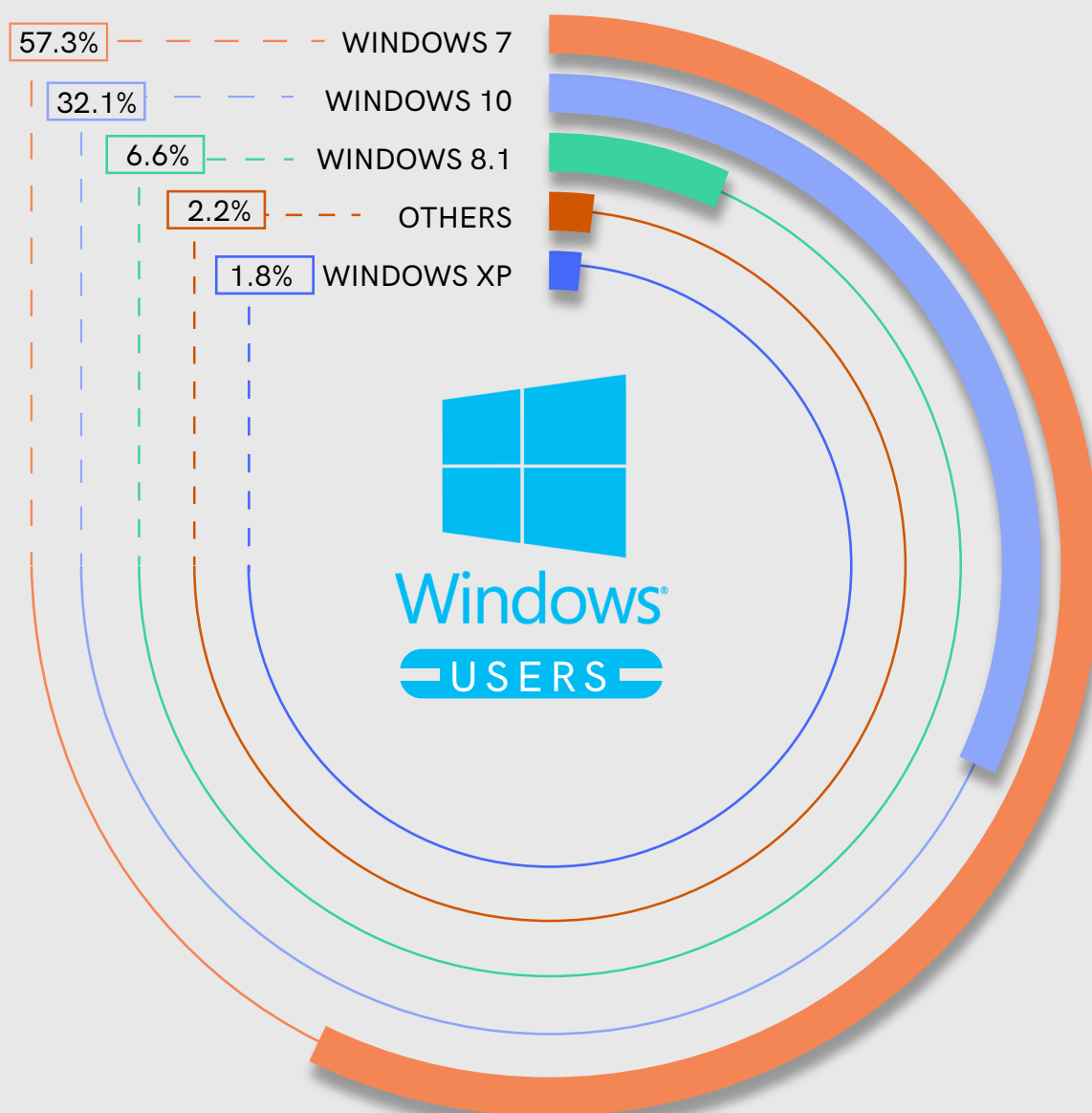


Windows 7 Nostalgia

In this quarter we saw that around 60% of our active users are still using Windows 7. The percentage is significant especially given the official announcement of support withdrawal by Microsoft. This means Windows 7 users won't be getting security updates from Microsoft anymore. However, a few enterprises are using Windows 7 by compulsion as many of

their tailored software is Windows 7 based. A large chunk of Windows 7 users still prefer this version over Windows 10 because of its ease-of-use and lower resource requirements. However, since there won't be any official support anymore, bad actors would proactively target the Windows 7 consumers by exploiting the existing vulnerabilities.

MS Windows OS Breakdown By Users

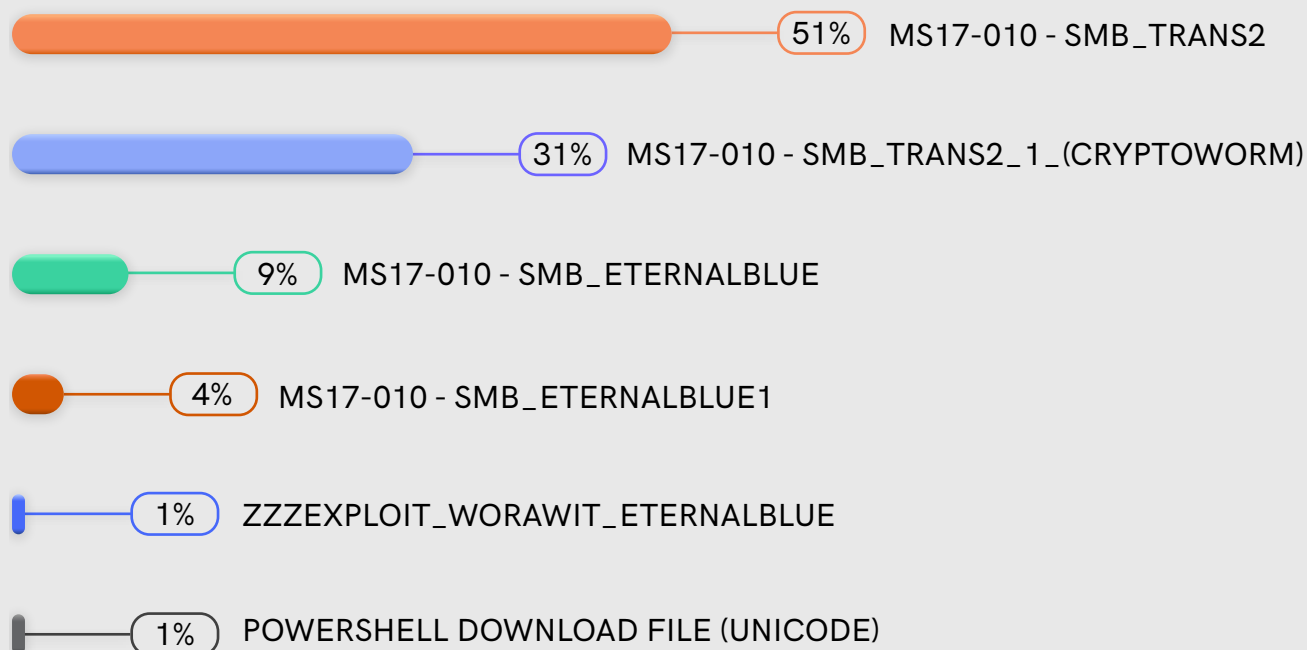




From the K7 Telemetry stats, we found a large number of attacks exploited various SMB-based vulnerabilities. Notably, the top amongst them is a dated vulnerability which was fixed many years ago. The stats show that there are

still many machines that exist at large which are yet to be patched for such vulnerabilities. The chart below describes the most prevalent vulnerabilities getting exploited in the wild.

Most Prevalent SMB And EternalBlue Variants



Mitigation Tips

- Keep your OS and Anti-Virus up-to-date
- Disable ports that are not being used
- Enforce a strong and complex password policy and ensure that the same password is not used for different accounts
- Use a password manager and multi-factor authentication for all the services you use
- We suggest users move to Windows 10, so as to receive continuous support from Microsoft and to stay safe from the latest as well as older vulnerabilities
- Users also need to turn on the K7 auto-update feature to receive protection from all the latest threats



Out-of-Date Security a Malware Magnet

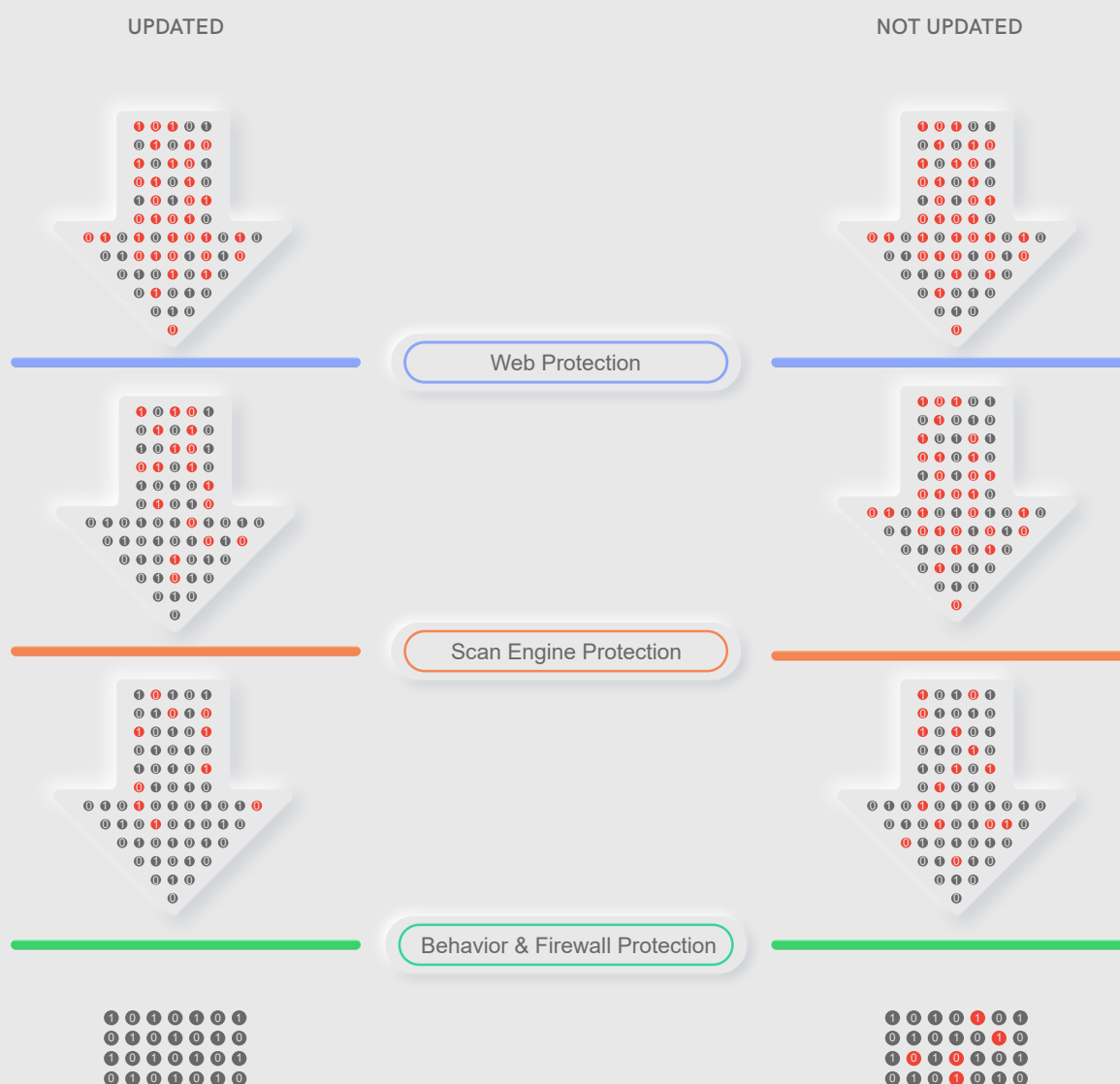
The Necessity of Updating your AV

Keeping yourself up-to-date has always been a necessity, but never more so than now, whether it is for climbing up the career ladder or keeping yourself safe from the cyber threats that are wreaking havoc in people's lives. A dated cybersecurity or AV suite makes you vulnerable to existing and emerging cyber threats, giving you all the more reason to stay

up-to-date.

Cybersecurity product installs which receive the latest definitions are deemed up-to-date, whereas product installs which do not are deemed non-up-to-date, and are at great risk of malware infections.

What Happens When you don't Update your Cybersecurity Suite?





Deep inside every cybersecurity suite exists a set of protection layers for detecting malware in the wild. Each of these layers is responsible for inspecting the various activities happening on the system and blocking malware according to established patterns (we call them signatures). The layers are commonly known as Web Protection, ScanEngine Protection, Behaviour Protection and Firewall Protection. Let's analyze what happens when users allow their security product to expire or turn off updates for some reason such that they no longer receive the latest protection definitions.

Researchers from K7 Labs investigated telemetry evidence of pan-India threat events from non-up-to-date devices over the Q3 period. The very first thing to understand clearly is that there are malware infections found on systems which are not updated. Let's dive into the difference updates or lack of them make to each protection layer.

Web Protection

Web Protection is the first layer of defense in all K7 cybersecurity (CS) suites. It is responsible for blocking malware and related attacks coming via browsing the internet. For instance, Web Protection blocks the user from inadvertently navigating to a malicious website or visiting a link in a phishing email, thereby stopping these attacks in their tracks.

The Web Protection layer enhances its signature database numerous times in a single day to detect and block the latest malicious websites. Users who do not update the CS suite would naturally miss out on such critical updates, thereby falling prey to cyberattacks that are now allowed to penetrate deeper, implying that an impaired Web Protection would be far less likely to prevent malware from being downloaded onto their system. The telemetry evidence clearly indicates a badly-injured Web Protection layer on non-up-to-date systems.

ScanEngine Protection

Our researchers saw a spike in the proportion

of blocks at the ScanEngine Protection layer when the CS suite is not updated. The data shows that some of the malware which were not blocked at the impaired Web Protection layer are detected by stretched and strained generic and heuristic detections previously available in the product. In reality this is a bad sign as it indicates the presence of malware inside the machine which should have been stopped at Web Protection layer, if it were fully-fit by being up-to-date. Our researchers are certain that any dated system would typically harbour more hidden malware, which would have been detected and blocked if the product were up-to-date.

Behaviour Protection and Firewall Protection

Both Behaviour Protection and Firewall Protection, when they are up-to-date, help immensely to detect newly-coded or revamped malware based on their dynamic behaviour characteristics. If the CS suite doesn't get updated, these layers are stretched to rupture, being much more heavily dependent on the heuristic protection features available in the product which have not been refined via updates. The telemetry analysis for non-up-to-date systems reveals the end result; only some of the malware which should have been blocked at the earlier protection layers of Web Protection and ScanEngine Protection, to stop their spread, are now being blocked by whatever remains of the dynamic protection features due to an expired product, giving further strong evidence of the likelihood of hidden malware in the non-up-to-date scenario, a great danger indeed.

So, how much malware must be lurking undetected and unblocked on non-up-to-date systems? It's a scary question which could be avoided by keeping cybersecurity products up-to-date at all times!

THE MOBILE DEVICE STORY



Smartphone security has become increasingly important these days mainly because of the personal and business information stored on these devices. Cyberattacks compromising users' sensitive information has been on the rise in the last few months. But unsurprisingly the number of malicious cyberattacks couldn't manage to surpass adware infections. Our

K7 Telemetry recorded seventy-nine percent presence of adware among the total number of reported cases, which was interestingly three percent less than the previous quarter, and the frequency of Trojan attacks had increased from eighteen percent in the last quarter to twenty-one percent of the total infections in this quarter.

The Presence Of Adware Vs Trojan



Besides the enormous presence of adware, Potentially Unwanted Programs (PUPs), and Trojans, many vulnerabilities in popular apps manifested in large numbers during this period. The infamous WhatsApp stack buffer overflow and double-free vulnerability were

seen in this quarter. In case you're curious to know a bit more about the vulnerabilities that were exploited to execute the kill chain, here are some brief details about both the vulnerabilities.

WhatsApp Stack Buffer Overflow Vulnerability (CVE-2019-11931)

The infamous WhatsApp stack buffer overflow could allow cybercriminals to execute Denial-of-Service (DoS) or Remote Code Execution (RCE) attacks by exploiting a specially crafted MP4 (video) file. For the vulnerability to be taken advantage of when this file is sent to the user, the auto-download feature had to be turned on.

iOS versions prior to 2.19.100, Enterprise Client versions prior to 2.25.3, Windows Phone versions before and including 2.18.368, Business Android versions prior to 2.19.104 and Business iOS versions prior to 2.19.100. However, there has been no reported case of this WhatsApp vulnerability being exploited in the wild so far.

This affects Android versions prior to 2.19.274,



WhatsApp Double-free Memory Vulnerability (CVE-2019-11932)

Like the previously explained WhatsApp vulnerability, CVE-2019-11932 also allows the attacker to execute a DoS or RCE attack, thereby gaining control of the device. This vulnerability is exploited via a specially crafted GIF image that is sent to the targets, provided the attacker is in the user's contact list. The

GIF file is downloaded automatically without any user interaction and is saved in the media gallery. The bug gets triggered when the victim subsequently shares a media file to any of the members in his or her contact list. This vulnerability affects Android versions before 2.19.244.

Word of Caution

WhatsApp has already fixed both the vulnerabilities through an update. However, the vulnerability still exists in those devices running on dated WhatsApp versions.

Users are advised to update the WhatsApp installed on their devices, if not already up-to-date, and also to disable the auto-download feature in WhatsApp to stay safe.

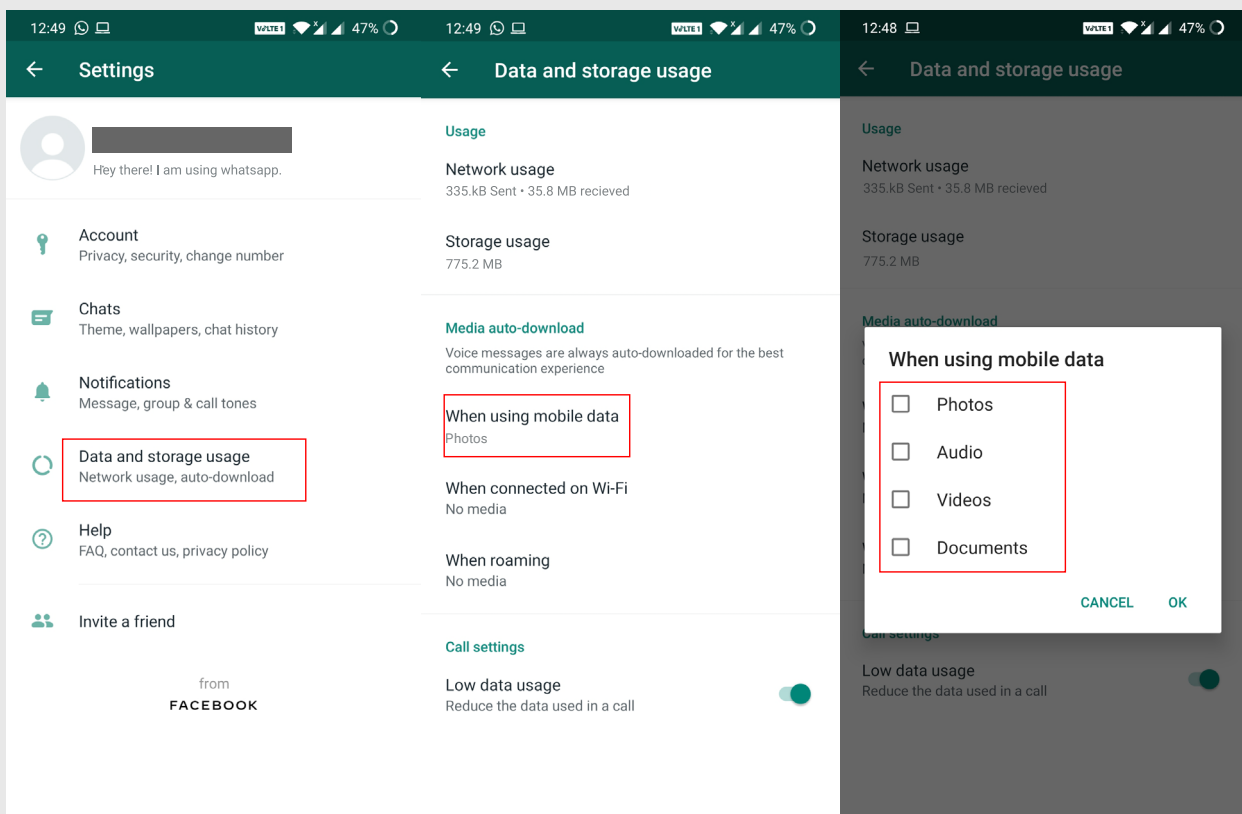
The auto-download feature of WhatsApp can be disabled as follows (also depicted in the image below):

1. Navigating to WhatsApp's hamburger menu, which appears on the top-right corner of the app

2. Navigating to "Settings"

3. Clicking on "Data and storage usage"

4. Uncheck all the checkboxes that appear under all options for "Media auto-download", i.e. "When using mobile data", "When connected on Wi-Fi" and "When roaming"



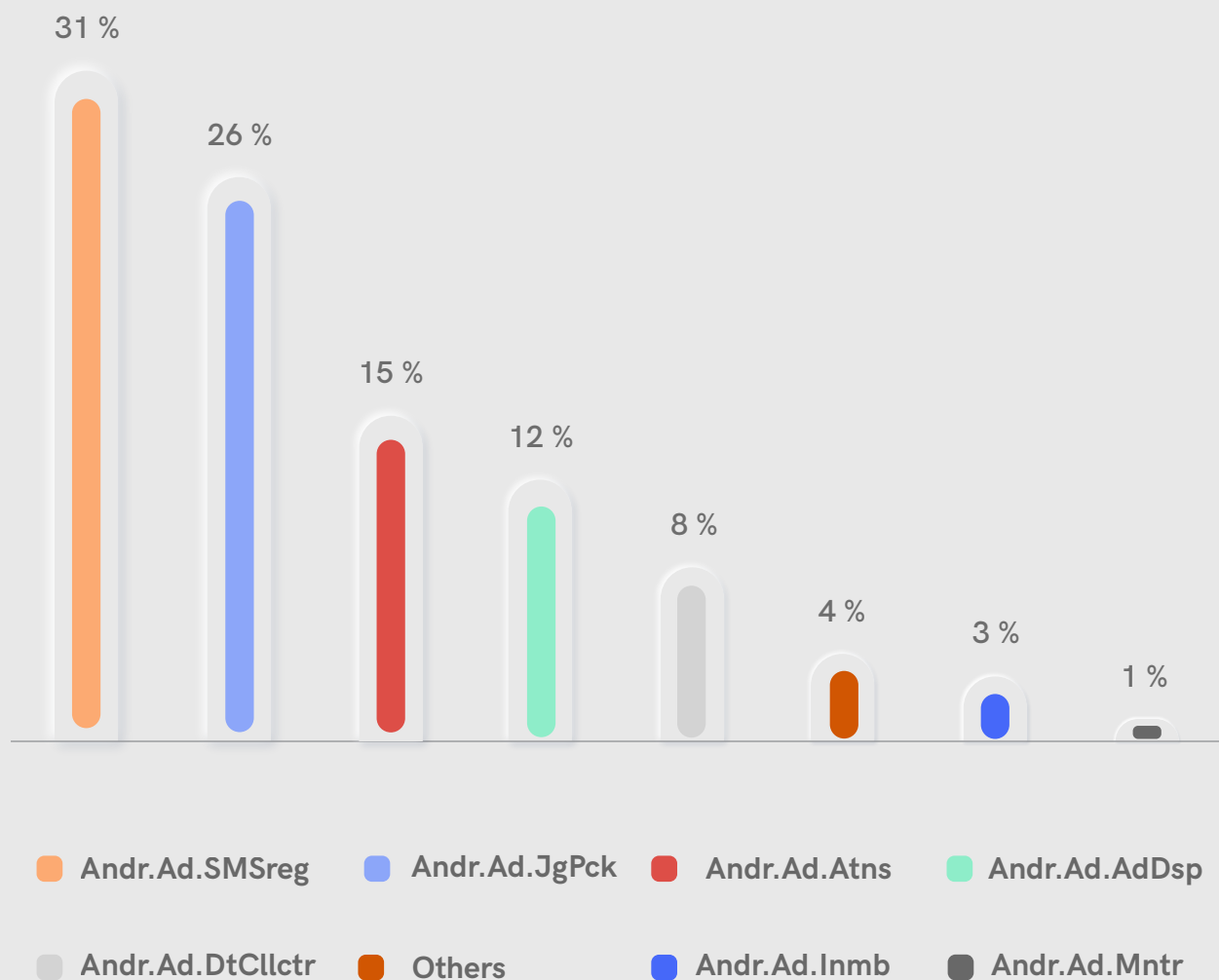


The Adware Crisis

We flagged and tracked a surfeit of adware in the previous quarter and the trend continues this quarter as well. Known for their easy money-making capability by victimising users, adware is becoming more and more ubiquitous with time. Instead of stealing important credentials,

including financial ones, adware simply churns out money by pushing advertisements into users' devices and in some cases even auto-clicking on ads without their consent.

Trend Line Showing The Adware Plague



All the major adware noticed in the previous quarter remained prevalent in this period too. Interestingly the Andr.Ad.SMSreg holds the crown even after a major plunge in visibility from forty-one percent recorded last quarter to thirty-one percent this quarter. Adware

like Andr.Ad.Atns, Andr.Ad.JgPck, Andr.Ad.AdDsp remained prevalent with a visibility of 15%, 26%, and 12% respectively. It was then followed by Andr.Ad.DtClctr, Andr.Ad.Inmb, and Andr.Ad.Mntr with a presence of 8%, 3%, and 1% respectively.

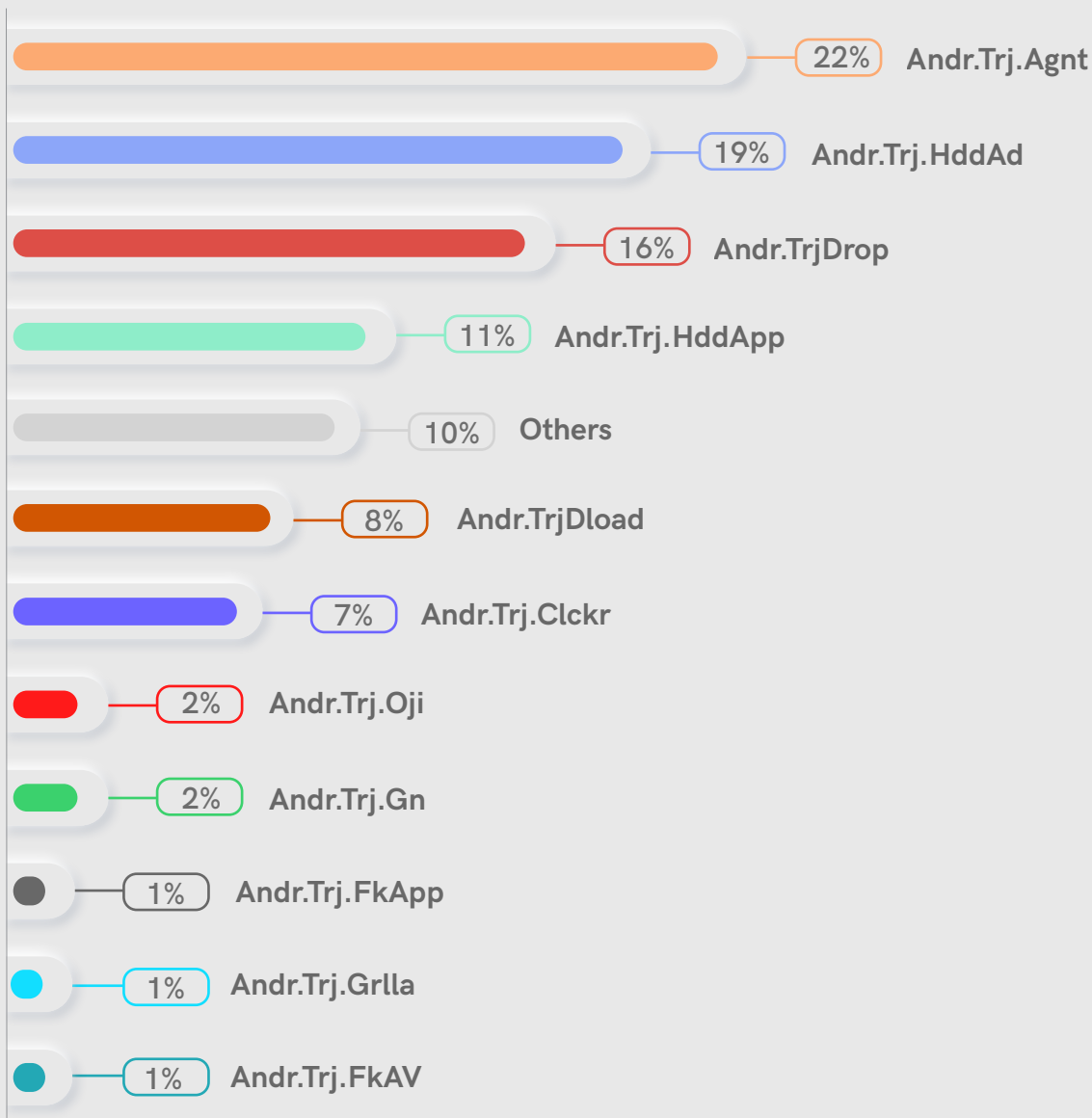


The Trojan Horses

The trendline of Android Trojans in the period remained quite predictable with a significant presence of the most popular Trojans of recent times. Andr.Trj.Agent, Andr.Trj.Drop, Andr.Trj.

HddApp and Andr.Trj.HddAd remained more prevalent than the others.

Most Prevalant Trojan Types



Andr.Trj.Agent reigned the Trojan arena with a visibility of 22%, which is 2% higher than the previous quarter. The Andr.Trj.Drop, Andr.Trj.HddApp, and Andr.Trj.Dload have plummeted by 2%, 5%, and 7%, respectively, compared to the previous quarter. Despite this, they still managed to hold positions just below the

top spot with a visibility of 16%, 11% and 8% respectively. Andr.Trj.HddAd (the infamous Hiddad adware) and Andr.Trj.Clckr were prevalent at 19% and 7% respectively.

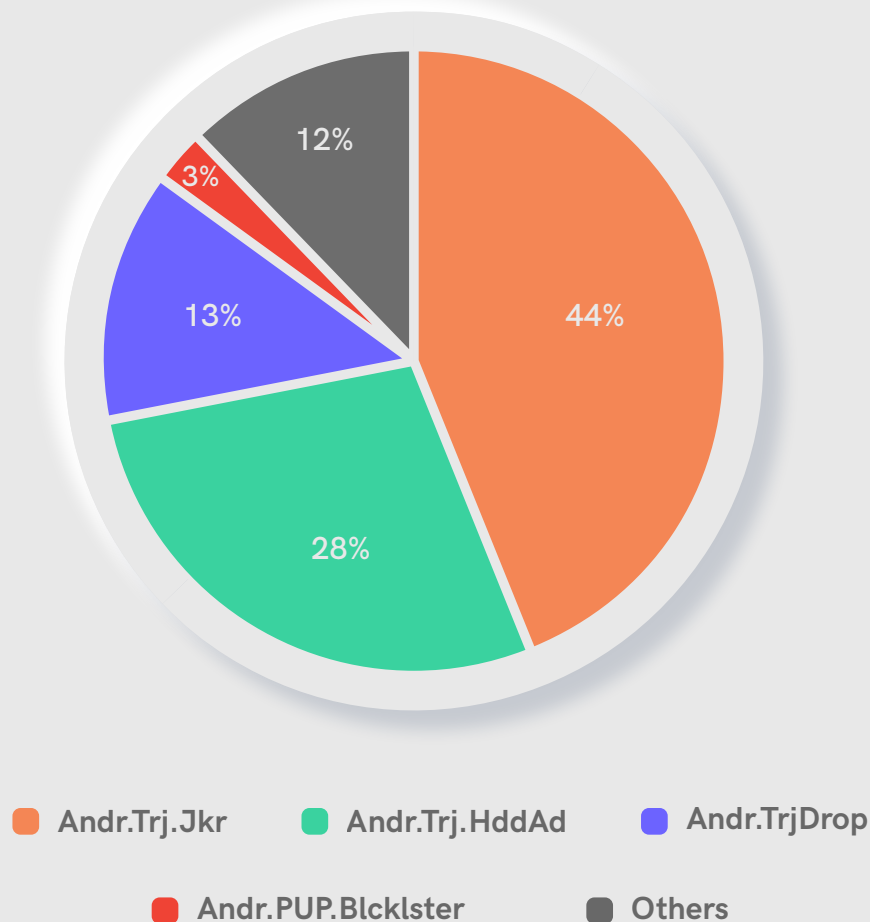


Malicious Apps from Google Play Store

Our researchers have encountered an umpteen number of malware riddled apps on several Android app markets including Google Play. The visibility of such a massive amount of malware in the official App Store hints at how the unscrupulous malware authors have

learned the art of hijacking benign apps and injecting malicious code into them to escape the standard vetting methods.

Visibility Of Malware Riddled Apps In Google Play Store



Take the Joker malware for instance. This Android Trojan does justice to the name, associated with the infamous nemesis of the superhero Batman. The Trojan malware has

reportedly infected more than 30 apps having over 2 lakh downloads, targeting mainly Asian and European users.



The Iniquitous Joker

Among the malicious apps from Google Play, Joker reigned over the overall mobile malware industry throughout the quarter. This notorious malware used various disguising methods to stay undetected and do the necessary damage to accomplish its evil intent.

Nicknamed Bread, the Joker Trojan identifies the victims' mobile location and later swindles them by subscribing to premium services

without their knowledge. The malware ensures that it stays within the advertisement framework and infects only users belonging to countries present in its hardcoded list. This hardcoded list includes India, Australia, Belgium, Brazil, China, France, Germany, Ireland, Italy, Malaysia, Singapore, United Arab Emirates, United Kingdom, etc. It also has an additional check to ensure that it does not affect users from the US and Canada.

DISSECTING THE JOKER



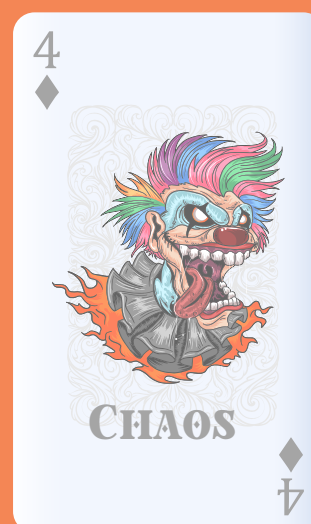
Stays within the advertisement framework while performing malicious tasks



Picks and chooses victims from specific geographical locations



Connects to the C&C server and downloads the second-stage payload



Subscribes to numerous paid premium services without victims' authorisation

Once it validates the country code, the malware downloads a DEX (Dalvik Executable) file as a second-stage payload from its Command & Control server. The second-stage payload simulates automatic interaction with advertisement websites. It also harvests the victim's contact list, SMS messages and device

information. It then accesses the user's text messages to get the authorisation code to verify the subscription. After that, it waits for a confirmation SMS message code and later submits the extracted code to the advertising offer's web page to authorise the premium subscription.



MoqHao: Targeted Trojan attacks on Android and iOS users

Noticing the growing popularity of digital banking services around the world, cybercriminals are increasingly focusing on targeted cyberattacks on both Android and iPhone users. The MoqHao Trojan attack is one such attack that remained prevalent during the period.

MoqHao Victims

We at K7 noticed a plethora of MoqHao attacks on Android and iOS. In brief, MoqHao is a sophisticated and evolving cross-platform phishing campaign which has been around for quite some time now despite notifications to law enforcement agencies and JPCERT/CC from Japan. There were many reports of MoqHao targeting diverse conglomerates in logistics and telecommunications industries in Japan, Singapore and Korea and traces of MoqHao malware samples were also found targeting Indian language (e.g. Bengali, Gujarati and Hindi) speakers.

MoqHao Characteristics

This banking/phishing Trojan has been around since 2015 and is spread via smishing or DNS hijacking. The malicious payload comes specially crafted for Android and iOS. This is achieved using a script-laced browser component which has been a critical attribute of this Trojan.

The Android MoqHao payload's ultimate goal has so far been data exfiltration, including banking credentials, and spying on the victim's activities. The modus operandi of this targeted Trojan is as follows.

A fake "Delivery failure notice" SMS containing a link to the URL for re-initiating the delivery is sent to the user. When the user clicks on the link, it redirects to a phishing website of a logistics company. The script in the browser identifies the OS of the smartphone from which the URL is accessed, and depending on the OS the infection chain varies.

The Android Kill Chain is depicted on the next page.



MoqHao Kill Chain

1. Trojan in Disguise



The malware disguises itself as a legitimate app (e.g. a logistics app) and gets downloaded/installed on the victim's device

2. Retrieving PII

It retrieves user's information like name, location, DOB, etc., and forwards them to C&C



3. Connect



Once executed, the malware connects to an existing social media account of the C&C address

4. Backport

The malware decodes/decrypts the profile info of the social media page to extract the C&C address. Also forwards the collected data to the extracted C&C in encrypted format



5. Unfurl Further

Forwards a link-embedded SMS to all the existing contacts to spread the infection further



The iOS Kill Chain

- When the MoqHao script identifies an iOS device, a phishing page, for instance "security<hidden>-apple.top", prompts the user to download a signed malicious iOS configuration profile (.mobileconfig.xml)
- Once installed, the phishing site opens automatically in the browser. It collects either the "device attributes" of the compromised device like UDID, IMEI, ICCID, version and product which are then

passed on to the threat actors or runs a browser-based cryptomining script in the background

- Note, webcryptomining on iPhone devices existed only for a short period, where the user will see a blank page on their devices, while the cryptomining happens in the background that shoots up the CPU usage of the device. However, the mode of infection is now back to phishing



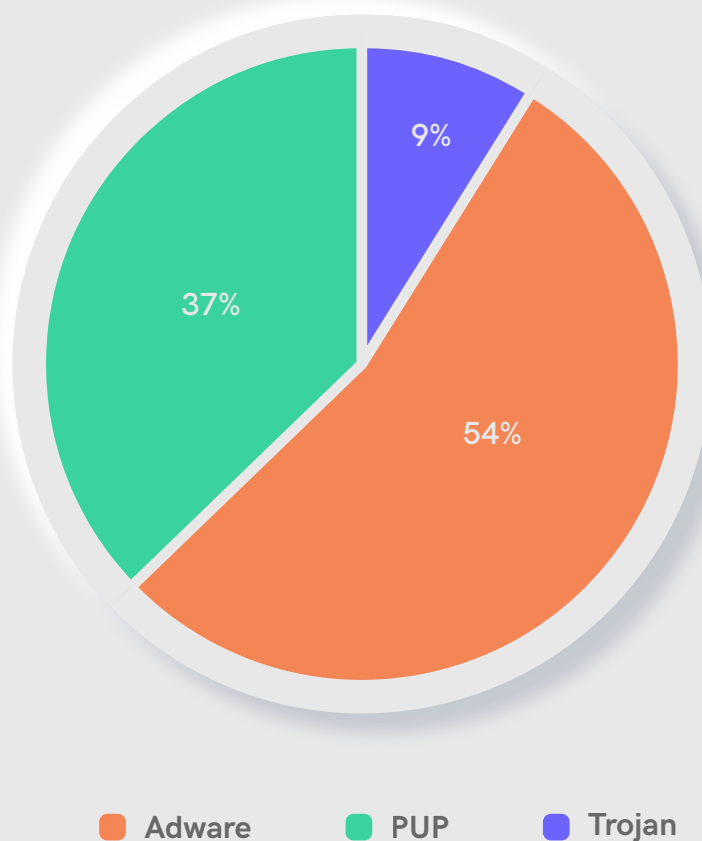
Tips to Stay Safe

- Make sure all the apps are patched for the latest vulnerabilities
- Download apps only from the official App Store
- Update your WhatsApp to the latest version and disable auto-download of any media in WhatsApp, even if it is from any member in your contacts list
- Secure yourself with a robust mobile security app such as K7 Mobile Security (Android and iOS)

The growing popularity of macOS driven machines in the SOHOs, SMEs, and large Enterprises, and the possible profits that could be got by targeting these systems have attracted the cybercriminals towards it, resulting in an increase in the frequency of attacks on Mac machines in Q3, 2019-20. While the frequency of Trojan attacks has decreased dramatically

this quarter, the amount of benign-looking adware and Potentially Unwanted Programs (PUPs) have made more noise than expected.

Top Malware Categories Affecting macOS



The statistics received from the sample inflow count are given here. The number of Trojan attacks has declined drastically and is at nine percent, while, the attacks from PUPs has spiked up to thirty-seven percent. The number of adware attacks recorded was considerably

large with a percentage of fifty-four percent during the quarter. Also, a large number of adware attacks that were reported could be attributed to just a few families.



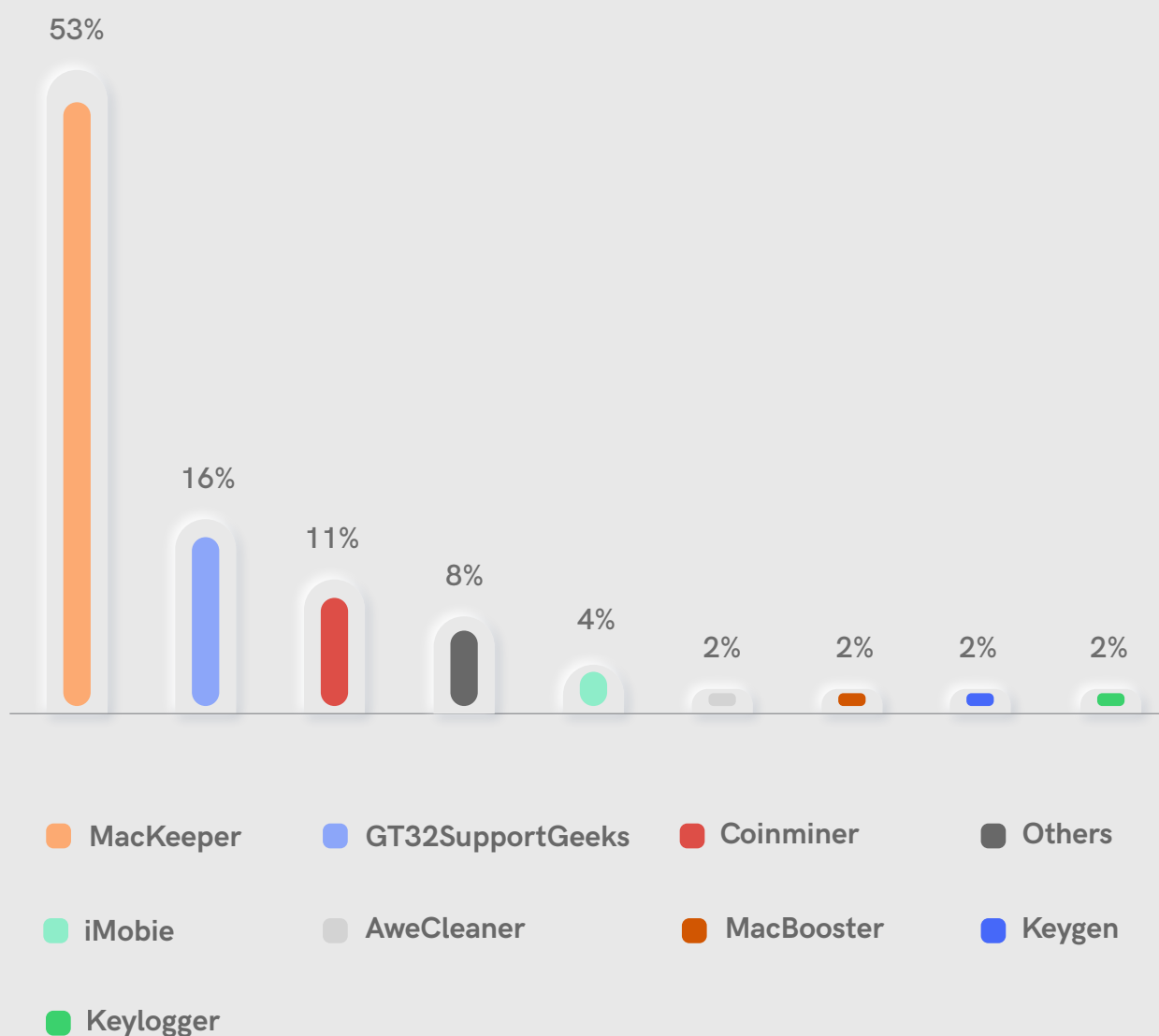
The Prevalent PUPs

PUP apps which are unwanted applications are usually quite infamous for their misleading and deceptive methods employed to infect a user's device. Once they gain a foothold on the victim's system, these apps may install malicious software without the user's permission, crash legitimate apps, consume a large amount of system resources impacting the system performance, among other issues.

MacKeeper and GT32SupportGeeks remained more prevalent than the other existing PUPs, with fifty-three and sixteen percent respectively. But more importantly, the proportion of Coinminer

attacks has significantly increased, by 8%, during this quarter, compared to what was observed in Q2. The reason behind this might be because of the unutilised robust hardware specification features available in most of the macOS powered machines, making it easy for cybercriminals to install cryptominers on such machines which would be more likely to churn out more currency when compared to conventional Windows-powered machines. Alongside, there were PUPs like AweCleaner, iMobie, MacBooster, Keygen, and Keylogger which showed their presence this quarter.

Most Prevalent PUP Types





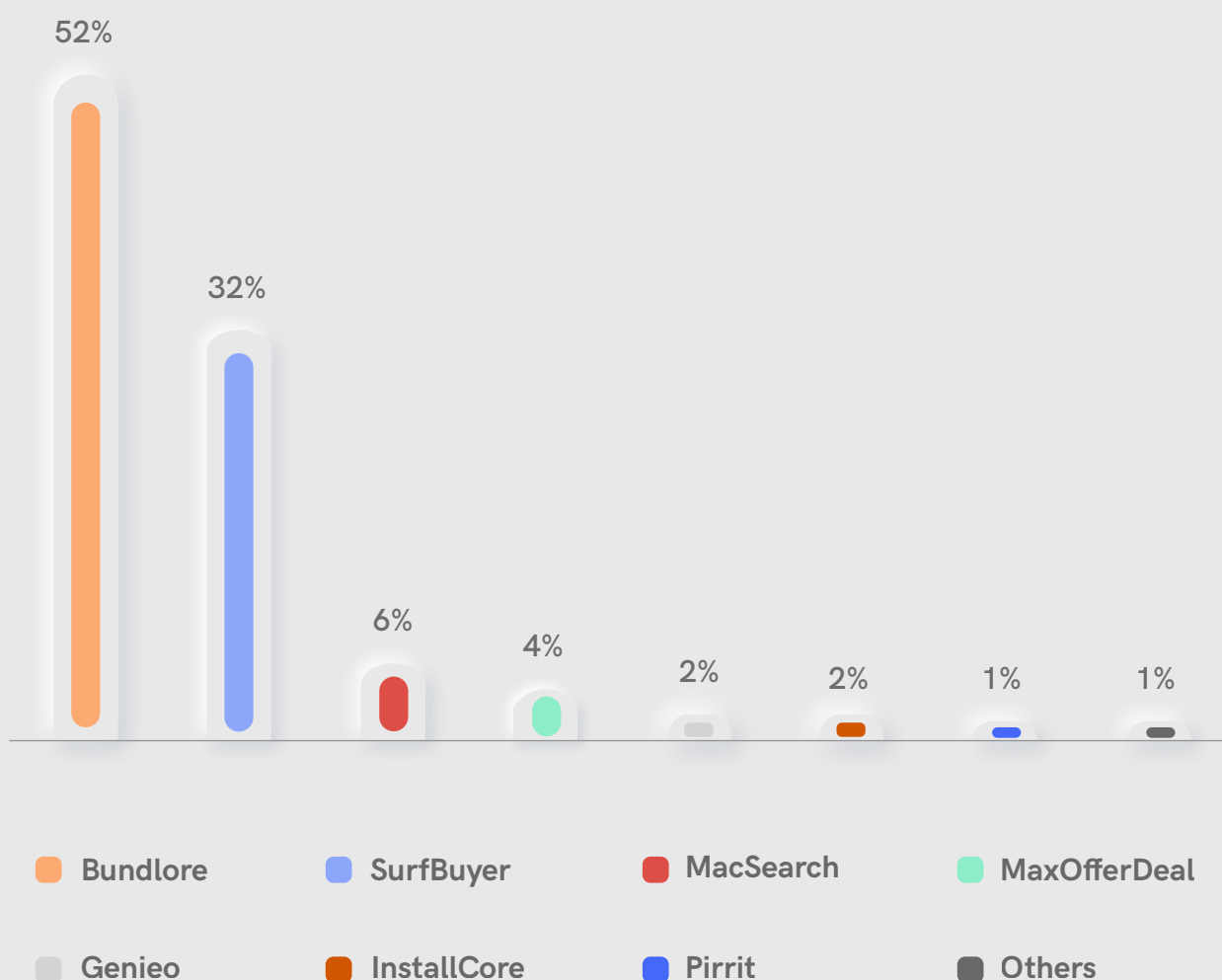
The Upsurge of Adware

During this quarter, adware remained the most ubiquitous form of malware. To dupe victims, they come up with numerous techniques to infect and remain stealthy. Notorious adware often poses as a legitimate app installer so that a large number of users download the same onto their devices. For instance, Bundlore and SurfBuyer, the two most infamous adware during this quarter, masquerade themselves as legitimate software installers to get inside the user's system. The installer usually bundles

dangerous software such as spyware, other adware, and various other potentially harmful components.

Adware like MacSearch, MaxOfferDeal, Genieo and the like have also made their presence felt this quarter. Interestingly, all of them have one thing in common, which is that they masquerade themselves as legitimate apps and trick users into installing them.

The Trend Line of Adware Variant Detections



In this period, Bundlore remained the most prevalent adware during the fiscal quarter with an overall attack share of fifty-two percent, while SurfBuyer, MacSearch, and MaxOfferDeal recorded thirty-two, six and four percent of

the attack percentage respectively. The other visible adware during Q3 2019-20 were Genieo (2%), InstallCore (2%), and Pirrit (1%).

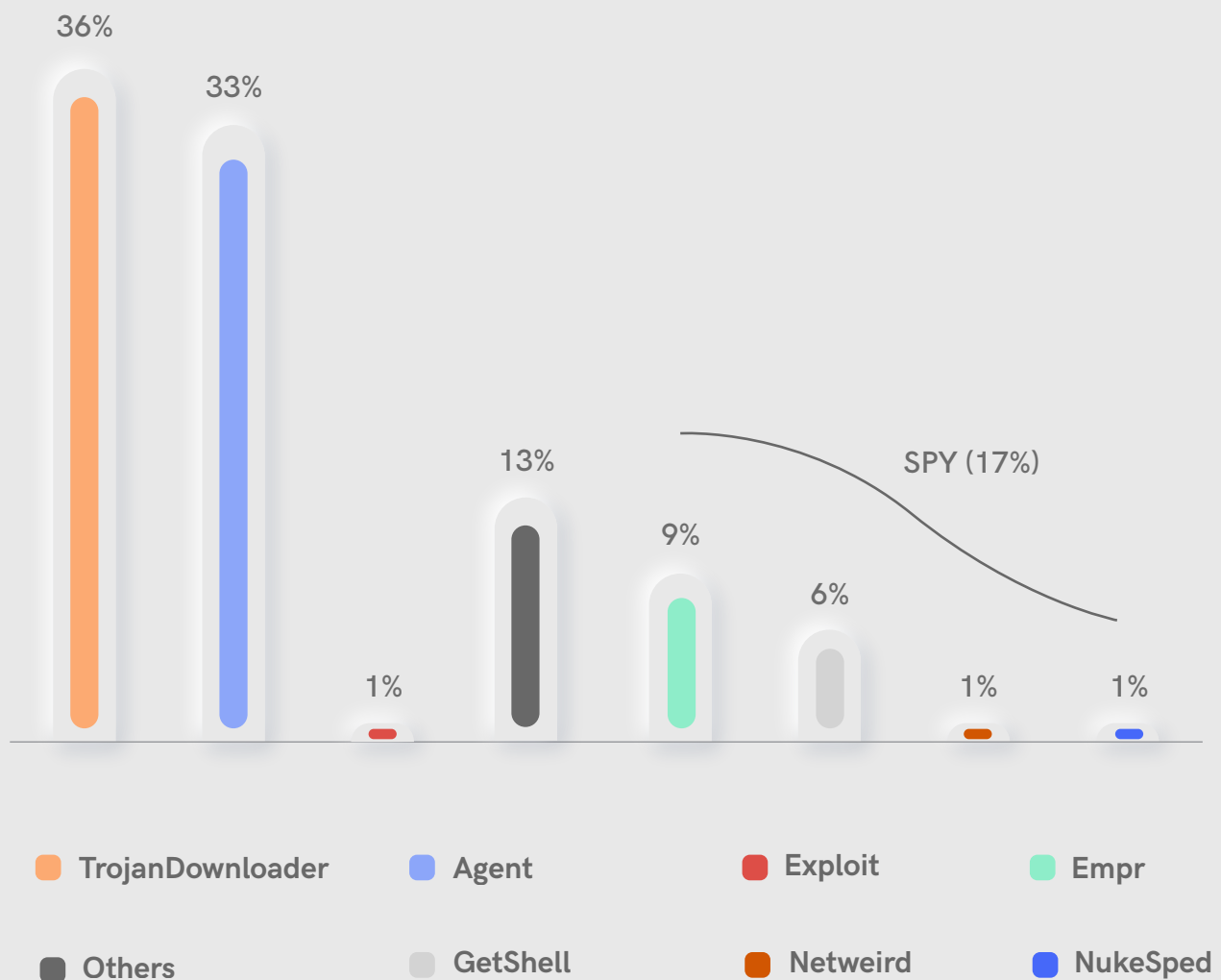


The Reign of Trojans

Trojan attacks continued their trend for the past few months, even though their share has drastically reduced. While TrojanDownloader and Agent count as the top two Trojan types, as they were the most prevalent, the percentage

of Exploits has reduced to a mere 1%. However, spy apps such as Empr, GetShell, Netweird and NukeSped had a total share of 17 percent among all the attacks in Q3.

Trojan Detection Trend Lines





Cryptocurrency Exchange Targeted by a Fileless Trojan

During this period, one of our researchers at K7 Labs, Dinesh Devadoss, came across an interesting cryptocurrency program in the wild with a few Trojan-like behaviours. On digging deeper, he found that the app had similarities with the malware developed by Lazarus, the North Korean APT group infamous for executing several high-profile targeted cyberattacks.

To gain more insights about the malware, our researcher shared the malicious sample via the social networking platform Twitter. Other researchers from around the world analysed the malware and deployed appropriate defences following our researcher's valuable lead. The cyber-attack chain is given below.

- In short, the attack begins with a social engineering trick asking the potential victims to install a cryptocurrency app from a fake website
- Once the victim installs the app, it downloads the first payload carrying the Trojan itself and infects the device
- Later, the Trojan downloads the second-stage payload, which remains active in the RAM without writing the payload onto the disk, which makes it a classic example of a fileless attack. This step would help it to evade any file-based detection by AV software



The malware is a significant instance revealing how APT groups like Lazarus are increasingly focusing on macOS machines, and unlike

traditional malware, are using fileless techniques to attempt to stay hidden.



Safety Guidelines

- Do not access/install any unknown/unsigned applications
- Ensure you keep your devices up-to-date and patched for the latest vulnerabilities
- Use a reputable security product, like K7 Antivirus for Mac and ensure it is up-to-date. Scan your devices regularly and whenever you install any new application, even if it is from the official App Store

DANGER IN THE INTERNET OF THINGS



Home Routers in Jeopardy

A series of D-Link routers namely DIR-655, DIR-866L, DIR-652, and DHP-1565 were affected by a remote code execution vulnerability. The CVE-2019-16920 vulnerability present in these routers, as a result of a command injection

vulnerability, can allow an adversary to bypass authentication, and inject and execute arbitrary commands and code on the device.

Perilous Web Server Flaw Strikes Many IoT Devices

A critical unauthenticated code execution vulnerability CVE-2019-5096 exists in the way GoAhead, a web server application for embedded devices, handles HTTP requests. This vulnerability could get exploited by attackers who use crafted HTTP requests to execute malicious code on vulnerable devices and take control over them.

on GoAhead based web servers could lead to a Denial-of-Service (DoS) attack. A specially crafted HTTP request can lead to an infinite loop in the process which leads to 100 percent CPU utilization resulting in DoS.

Both these vulnerabilities affect GoAhead versions v5.0.1, v4.1.1, and v3.6.5.

Another vulnerability CVE-2019-5097 present



Mitigation Techniques

- Ensure all your devices are patched for the latest vulnerabilities
- Change your default settings
- Deactivate unused features and services
- Do not connect to untrusted open Wi-Fi networks

KEY TAKEAWAYS

Analysing an innumerable number of threats under different categories leads us to conclude that both the threat actors and the evasion tactics used by them would continue to evolve in the near future as well.

When it comes to security, we would like to ensure everyone around us is safe, and as a precaution, we have a few suggestions for you to take away.

	
Enterprise	Consumer
1 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 updated.
2 Change your default Remote Desktop Protocol (RDP) settings and use strong authentication	Avoid accessing/installing any unknown applications
3 Migrate Windows 7 users to Windows 10 ASAP. Avoid dated OS versions	If you are using Windows 7, migrate ASAP to Windows 10



Copyright © 2020 K7 Computing Private Limited, All Rights Reserved.

This material has been compiled by K7 Labs. This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners. Email us at k7viruslab@labs.k7computing.com.

www.k7computing.com