Cyber Threat Monitor Report

2020-21

K7 SECURITY

Contents

Contents

Into the Realm of the Cyber Threat Ecosystem

Though this year started off well for our country, it has been riddled with uncertainties now owing to the fear of this COVID-19 global pandemic and the ensuing lockdown scenario. Nowadays, there are more transactions being done online rather than by going out to complete regular tasks. This has become an advantage for threat actors who want to leverage this crisis situation, to show off their nefarious skills and mint money as can be seen from the increase in Android Banking Trojans such as Cerberus, Ginp and Anubis during the COVID-19 period.

Taking advantage of the Work from Home (WFH) scenario, threat actors are trying to find new vulnerabilities in various tools such as Virtual Private Networks (VPNs) and Conferencing tools to hinder the regular working of enterprises. These tools are used mainly by enterprises of all sizes as they need to embrace this extensive digitization driven by the requirement to achieve more efficiency to boost business in terms of revenues and for scaling up further. Propelled by the new-age technologies, including connected devices (IoT and IIoT), cloud storage, and Software-as-a-Service (SaaS), the enterprises are opening up new avenues, but also more and more scope for attacks making them an easy target for the cybercriminals. Thus, this massive digitization has made the businesses all the more vulnerable.

The attackers are ramping up the frequency of attacks with new intrusion and evasion methods which are more lethal than ever before. And the vulnerabilities that exist on the network infrastructure and devices are helping them to a great extent. Targeting the employees is another good option for cybercriminals as they are the weakest link in the chain.

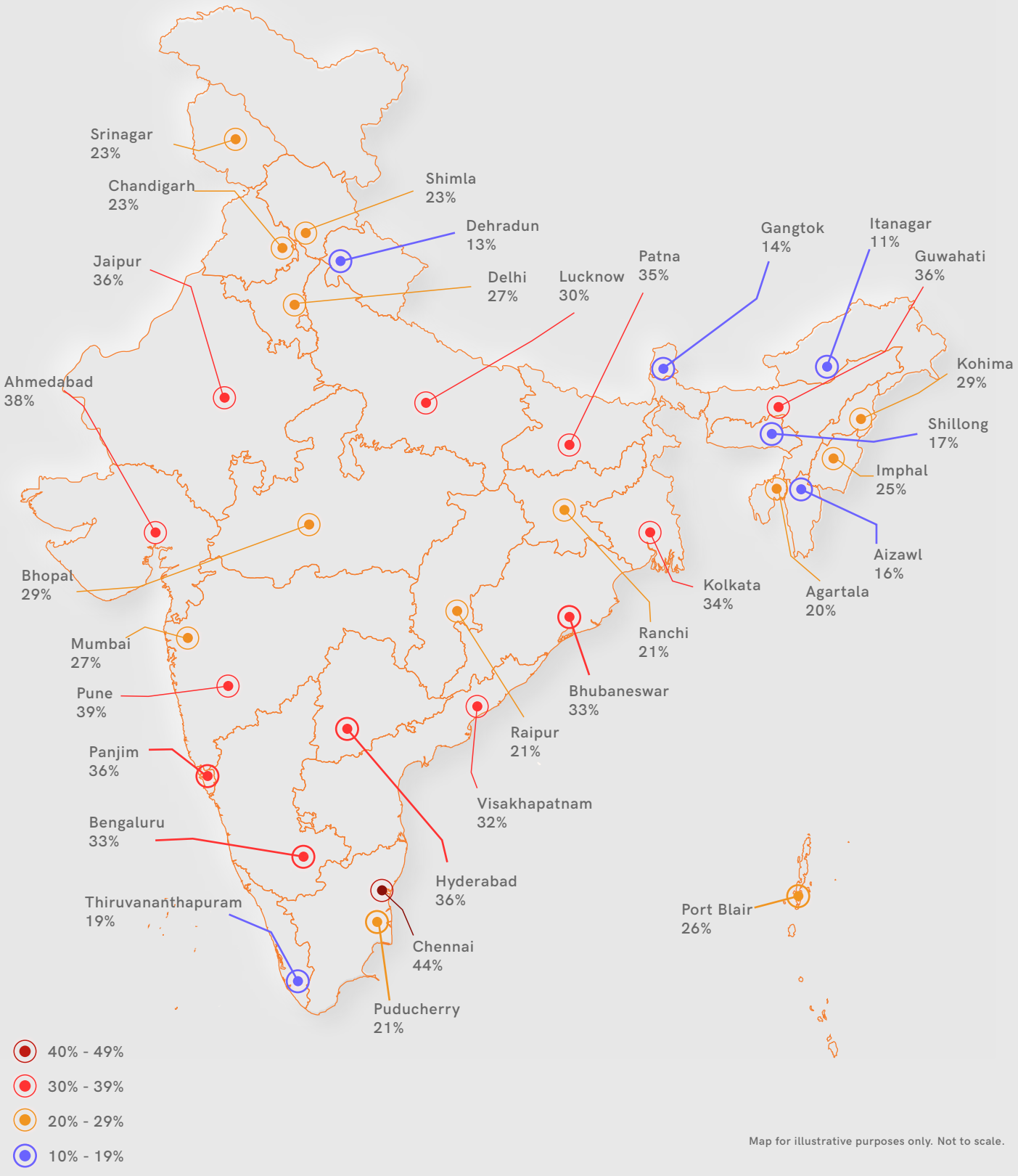
Managing the vulnerabilities is, of course, a significant requirement to remain safe on the internet. However, controlling the massive range of vulnerabilities that appear every day is quite an arduous task for enterprises. And therefore the cyberthreat landscape is transforming to an increasingly chaotic one.

However, any enterprise or end-user can avoid such potential risks by adopting a few changes in their cyber hygiene, inclusive of internet behavior and the embrace of security best practices.

Our Q1_2020-21 report outlines Windows security, macOS security, mobile security, Internet of Things (IoT), vulnerabilities, the prevalent threats, and the threat atmosphere hovering over the country. This report also includes a set of measures to mitigate business or personal data risks.

We sincerely hope this report's insights would be informative such that you become more proactive and well-acquainted with the efforts to fight against the onslaught of threats that are surfacing these days. However, if you are a K7 user please rest assured that you are in the best of hands, as we endeavour to protect you from all such cyber dangers at all times.

CYBER THREAT MONITOR - INDIA



Map for illustrative purposes only. Not to scale.

BACK TO CONTENTS

Regional Infection Profile

Unfortunately 2020 would not be remembered as a year of joy and positive feelings; rather what would stay in the minds of people is the global pandemic and the fears associated with it. Many enterprises are grappling with this rising crisis which has created havoc not only in personal lives but also in the digital world as the threat actors have effectively managed to successfully launch attacks specific to this crisis apart from their usual attacks.

For those who do not know, "Infection Rate" (IR) of an area is the proportion of K7 users in that area who encountered at least one cyber threat event which was blocked and reported to our K7 Ecosystem Threat Intelligence infrastructure (K7ETI). Our stats reveal that, at 20% this quarter, there has been an increase of 4% in the overall pan-India IR compared to the previous quarter.

Since attacks related to COVID-19 have already been extensively covered in our "**Cyber Threat Report COVID-19**" published within Q1_2020-21, we would be focusing more on the other types of attacks except for a detailed write-up on Android Banking Trojans.

Malware in the form of ransomware, Remote Access Trojan (RAT), Banking Trojans, and others has been on the rise this quarter. The adversaries are engaging themselves in attacking targets literally on every platform. As expected, many attacks were targeted instead of being random and were executed utilizing a plethora of new evading techniques.

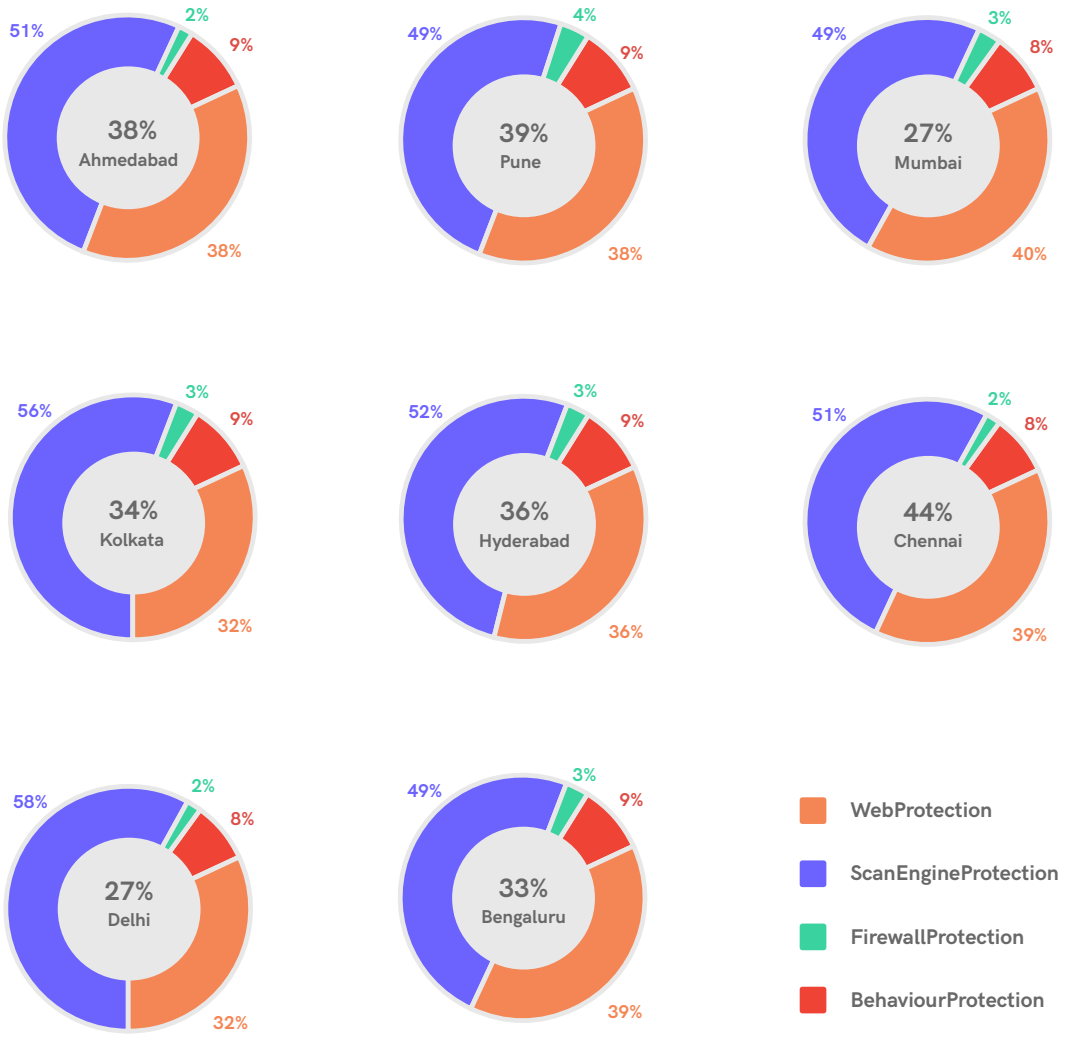
The observations also reveal numerous other attack techniques like SMiShing, remote desktops, PowerShell, Spyware, fileless attacks, drive-by activities, commodity malware, and counting.

Like in the rest of the world, Indian enterprises and end-users were hit by a range of threats. Our report reflects our findings alongside a set of practical defense tips.

But instead of diving directly to the analysis of our most significant findings grouped by platforms, we would also like to reflect on a granular view of the threat landscape in India grouped by the state capitals, Tier-1, and major Tier-2 cities.

Looking at the higher-volume attempts observed in the country between April 1 to June 30, the below chart displays that the overall attack on the Tier-1 cities has mostly increased in comparison to the previous quarter.

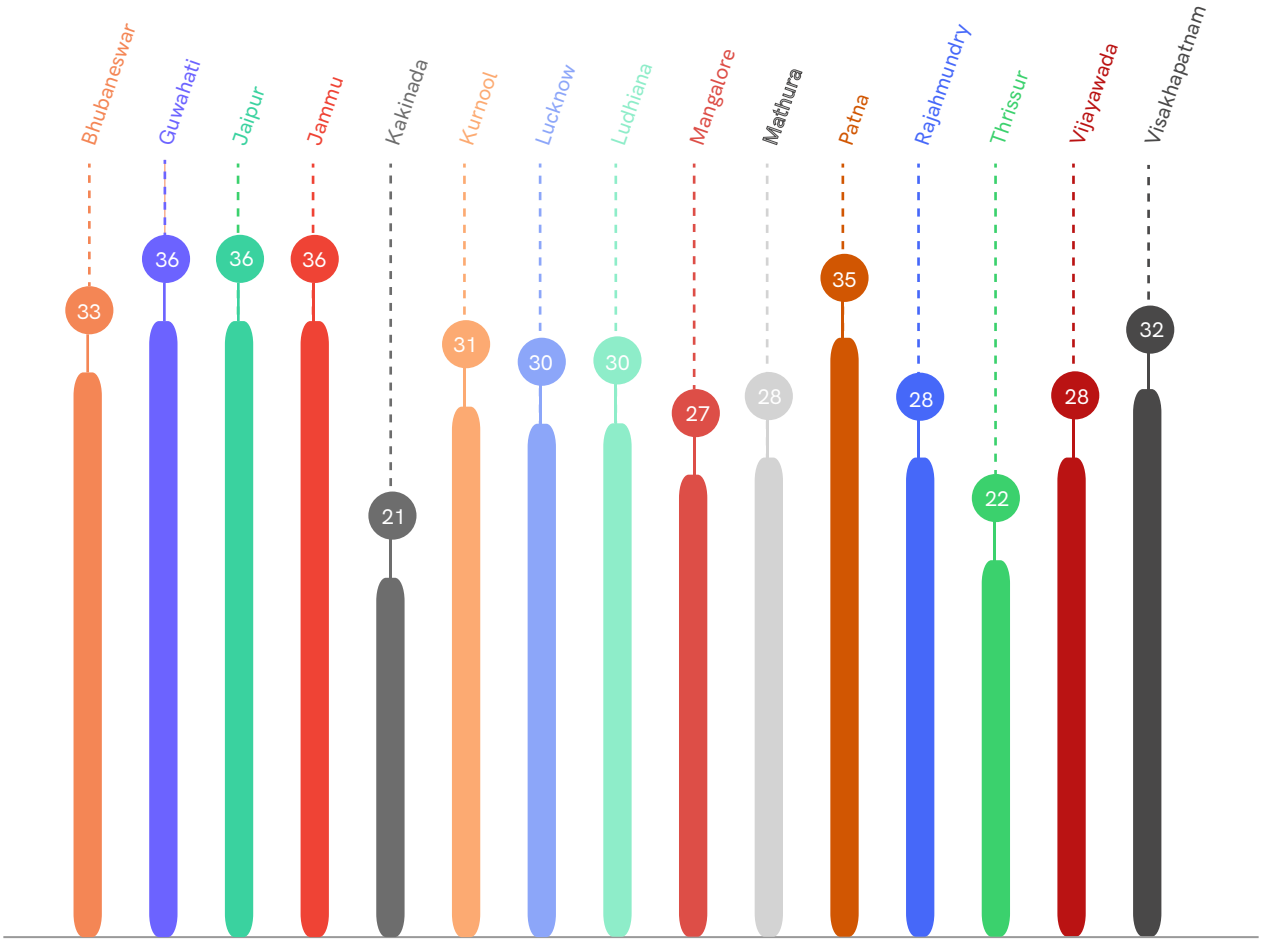
The Metros and Tier - 1 Cities - Infection Rate



Ahmedabad, Pune, and Mumbai have encountered 4%, 7%, and 2% more attacks than the previous quarter. Chennai and Hyderabad were no exceptions and had 2% and 1% more attack visibility compared to the last quarter. However, Kolkata, Delhi, and Bengaluru bucked the trend a little bit by displaying 1%, 1%, and 2% fewer attacks. This scenario does not mean that these cities were safer than the rest.

Ahmedabad in this quarter had experienced an IR of 38%, while Pune had a tad more by hitting the graph with 39% attack visibility. Chennai and Hyderabad remained the most vulnerable metro cities, and had IRs of 44% and 36% respectively. However, Kolkata and Bengaluru displayed slightly lower IRs of 34% and 33% respectively.

Top 15 Infection Rates in Tier - 2 Cities



As per K7ETI, all the Tier-2 cities had an IR above the national average. Ludhiana, Vijayawada, Visakhapatnam, Jaipur, and Mathura recorded higher IRs, increases by a range of 1%-3% compared to the previous quarter. Bhubaneswar, Guwahati, Jaipur, Jammu, Patna, Visakhapatnam, and Kurnool have had an IR visibility of more than 30%; Jaipur, Guwahati, and Jammu had faced a 36% IR, while Patna had 35% IR, which was a decline of 3% in comparison to the previous quarter.

BACK TO CONTENTS

Enterprise Insecurity

Following a nosedive in 2018, ransomware attacks have ballooned starting 2019 and have continued inflicting their wrath on enterprises worldwide in 2020 too. Unlike the previous ransomware families, the ransomware operators have become more focused on their target and attacking methods. They have also transformed themselves into business enterprises by delivering ransomware in a SaaS model, just like Salesforce or G Suite. They call it RaaS or Ransomware-as-a-Service. Upping their ransomware game, the operators are appointing affiliates with previous attacking experience to increase the frequency of attacks.

Modern Ransomware operators work like any other high-end software enterprise. Modern RaaS solutions come with high-end tools such as a dashboard to display attack status in real-time, a customer helpline, language and geolocation support, and many more. Moreover, they are also increasing the number of advertisements on the Dark Web, offering a variety of customized attacks grouped by price.

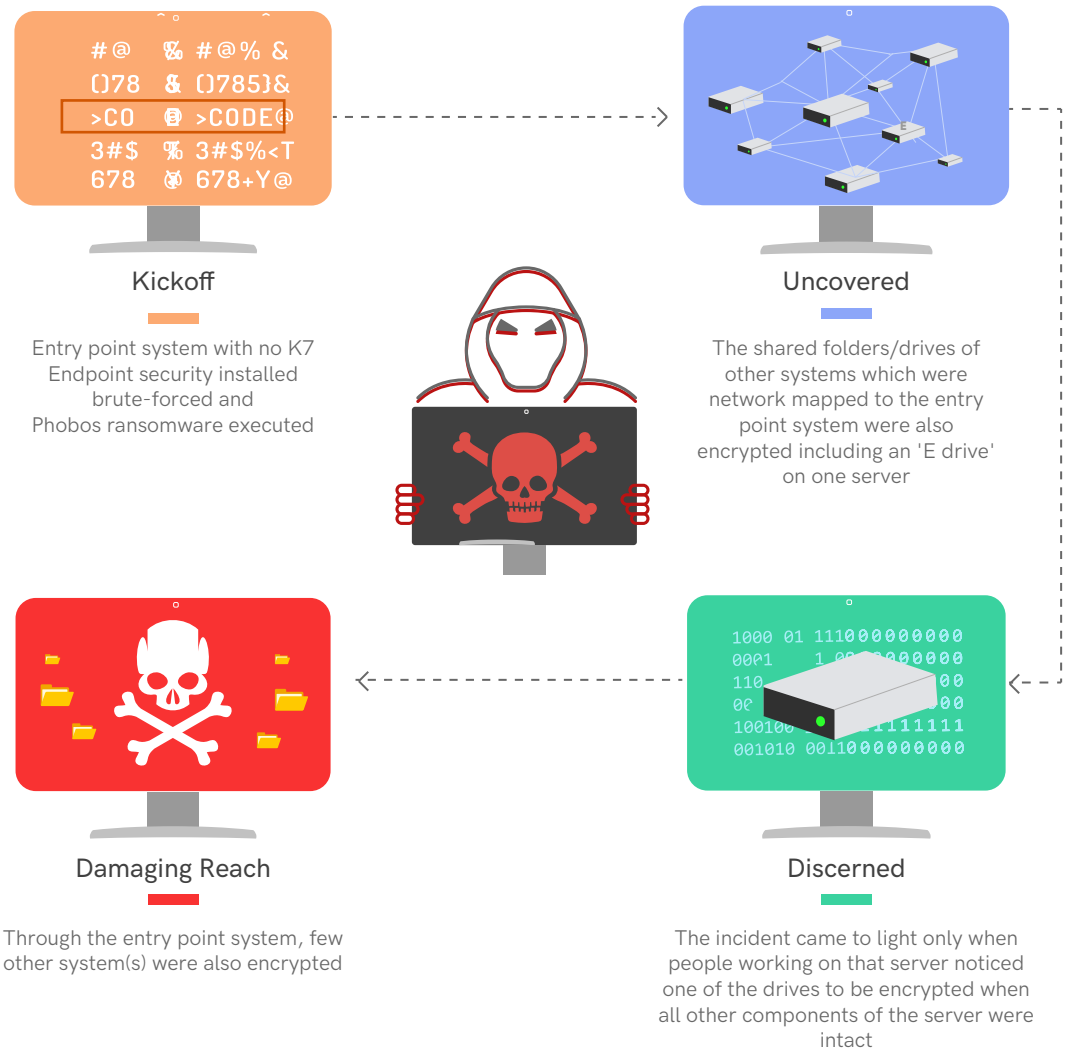
The brandishing strategies by all the notorious ransomware operators have helped immensely to increase the frequency of attacks. We have witnessed a surge in attempted ransomware attacks on our Indian Enterprise customers.

Let us see one such incident that affected an Enterprise customer.

Case Study: Phobos Ransomware exploits Weak Security Networks

During Q1_2020-21, one of our Enterprise customer's systems was encrypted. On analysing we found that the entry point system which the attacker brute-forced did not have our K7 Endpoint security installed and the Phobos ransomware was executed on it. Also, the shared folders/drives of other systems which were network mapped to the attacked system were also encrypted. This included an 'E drive' on one of the servers.

Exploring Phobos Ransomware



The ransomware incident came to light only when people working on the infected server noticed one of the drives to be encrypted. However, other server components were intact. Further investigation led to the discovery that through the entry point system, a few other systems were also encrypted.

Learning Lessons

The perils of internal systems needlessly exposed to the internet is a known fact. However, many system administrators ignore its risks. Exposed systems could be easily searched by a few clicks or typing-in commands in search engines like Shodan, and can be breached without much effort from the attacker. In fact, there are automated bots which can carry out the routine tasks of both network reconnaissance and initial compromise.

Not using a licensed copy of a reputed enterprise security product having a multi-layer defense system for threat prevention is another grave blunder that many system admins often repeat.

Such mistakes could allow your businesses to fall prey to cybercriminals in no time, resulting in monetary loss due to the breached data or loss by paying massive ransom money to get back all of your organization's critical data. Alongside this, such attacks badly affect enterprise productivity too, which would directly impact revenue.

As a system administrator, follow the safety recommendations given here.

Safety Recommendations

- ALL systems in the network should have an reputable enterprise security suite, such as K7 Endpoint Security, installed and kept updated, and systems should be regularly scanned
- Conduct regular security audits and vulnerability assessments in your enterprise to identify system and network weaknesses
- Set up a comprehensive breach alert mechanism in your Enterprise network
- Train your employees on cybersecurity so that they understand the cyber risks and best practices in the industry

Vulnerabilities Galore

Spotting vulnerabilities is an intrinsic part of the threat prevention cycle. Besides developing new intrusion and obfuscation techniques, threat actors often invest a considerable amount of time finding unexplored vulnerabilities in software and hardware to make the game easy for them.

These vulnerabilities usually pose immense privacy risks. The convenience of the Dark Web makes the case grimmer as adversaries sell exploits for zero-day vulnerabilities and help to launch massive attacks.

In Q1_2020-21, the threat landscape had its fair share of vulnerabilities at operating system, application software, and firmware levels. With employees working from home due to the ongoing COVID-19 crisis, threat actors are trying to find vulnerabilities and exploit services and applications to hinder smooth working and to steal confidential data. Security researchers are trying to get such vulnerabilities fixed at the earliest before the attackers can exploit and monetize them. Zoom app and Microsoft Teams exploitation are good examples to quote. Apart from these let's also look into other salient weaknesses that have been taken advantage of on Windows, Android, iOS, and IoT devices.

Zoom Client App Vulnerabilities

A partial path traversal vulnerability, CUE-2020-6110, was noticed in the Zoom client. Successful exploitation of the same could lead to arbitrary code execution implying that an attacker can execute arbitrary commands on any target user or group by sending a specially-crafted message. The vulnerability affected Zoom Client applications with version numbers 4.6.10 and 4.6.11.

Another vulnerability, CVE-2020-11469, exists in the Zoom client app that could allow an unprivileged user to get root privileges. Another massive vulnerability that was found in the video conferencing app Zoom was CVE-2020-11470. This vulnerability could lead an attacker to take control of the victim's microphone and camera access without notifying them. The affected Zoom version for CVE-2020-11469 and CVE-2020-11470 is the Zoom client app version V4.6.8 for MacOS.

Takeover Vulnerability Affects Microsoft Teams

A vulnerability in Microsoft Teams, a team collaboration platform, could allow an attacker to use a malicious GIF to sweep off the user's data and ultimately take over an organization's Teams accounts. The vulnerability lets the attacker send a GIF image bundled with a malicious payload to the victim. Once the victim opens the picture, the payload executes and circulates the same image file to other users via Microsoft Teams. In this way, the attacker could grab the tokens and messages of each user that exists on that Microsoft Teams session.

Flaws in the Android OS

Alongside apps, operating systems too have exposed a bunch of vulnerabilities to the attackers who are searching for easy prey. One such massive flaw, CVE-2020-0103, on the Android operating system could allow remote code execution, even with no additional execution privileges on the device. The vulnerability left millions of Android devices running Android version 9 and 10 exposed.

Google has patched the vulnerability with an update released in May 2020. Alongside this massive vulnerability, Google has also fixed 39 dicey vulnerabilities via this update. However, many Android phone makers offering a heavily customized version of Google's Android operating system are yet to release the patches.

Another scary vulnerability exposed in this quarter was the infamous CVE-2020-0096, aka StrandHogg 2.0. The critical privilege-escalation vulnerability had also left an enormous number of Android devices exposed to the attackers. The vulnerability lets an attacker intercept private SMS messages, photos, login credentials, GPS movements, phone conversations, and more from the victim's device. The affected devices were the ones running on Android version 9 and earlier. Google has fixed this susceptibility too through an update.

Apple JailBreak Vulnerability

Android was not the only mobile platform riddled with vulnerabilities. Apple's iPhone operating system iOS, too, was found with a vulnerability during this quarter. The zero-day vulnerability, CVE-2020-9859, was used to Jailbreak iPhones by allowing kernel-level code execution on exploitation. The affected versions are iOS devices using iOS 13.5 or prior versions.

SMB Vulnerabilities

Months after the SMBGhost, aka EternalDarkness (CVE-2020-0796) patch release, two new vulnerabilities were detected on the Microsoft's Server Message Block (SMB) protocol. Out of these two, one called the SMBBleed vulnerability, CVE-2020-1206, was an information disclosure vulnerability. The vulnerability could lead to remote code execution by combining it with the SMBGhost vulnerability. All systems running on Windows 10 and Windows Server could get exploited through this vulnerability.

Another remote code execution vulnerability in the Windows SMB protocol was CVE-2020-1301. It is caused due to improper handling of a specially-crafted SMBv1 request which results in the attacker being able to execute remote code on the victim's machine. The affected version was SMBv1. Microsoft has fixed both the vulnerabilities via its June 2020 update. The patch addresses a fix of 129 vulnerabilities beside these two.

Danger In The Internet Of Things

Alongside these vulnerabilities, hackers are going all out against the connected or IoT devices. Many such devices often remain unpatched for years, which could let hackers easily exploit the target devices to get into the target network. Q1_2020-21, too, has revealed many exploits on the IoT platforms. Here are the most significant ones from the lot.

BIAS Attacks on Bluetoothchips

Bluetooth Impersonation Attacks (BIAS) is a security vulnerability in the Bluetooth Classic, a communication protocol commonly used between low power devices to communicate. The vulnerability allows the attackers to spoof paired devices by injecting a rogue device inside an established Bluetooth pairing, masquerading as a trusted endpoint. It will enable the attackers to capture sensitive data from the other device. Multiple IoTs, phones, and laptops, with chipsets manufactured by Cypress, Qualcomm, Apple, Intel, Samsung, and CSR, are vulnerable to this attack.

Cisco IOS Routers Compromised

CVE-2020-3227 is a vulnerability in the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software. This vulnerability allows a remote attacker to execute Cisco IOx API commands without proper authorization. The affected versions are Cisco IOS XE Software releases 16.3.1 and later.

Ripple20 Flaws Affect IoT Devices

Researchers have also found out two vulnerabilities in a TCP/IP software library developed by Treck. Out of these two, CVE-2020-11896 could affect any device running on Treck with a specific configuration. The flaw could get triggered by sending multiple malformed IPv4 packets to a device supporting IPv4 tunneling. On successful exploitation, the attackers can execute code remotely. Devices that use the Treck TCP/IP library stack earlier than version 6.0.1.66 are vulnerable to the flaw.

The CVE-2020-11897 affects any device running an older version of Treck with IPv6 support. It is an out-of-bounds write flaw that can get triggered by sending multiple malformed IPv6 packets to a device. On successful exploitation, it can cause remote code execution. The flaw makes the devices with Treck TCP/IP stack before version number 5.0.1.35 vulnerable to it.

Mitigation Techniques

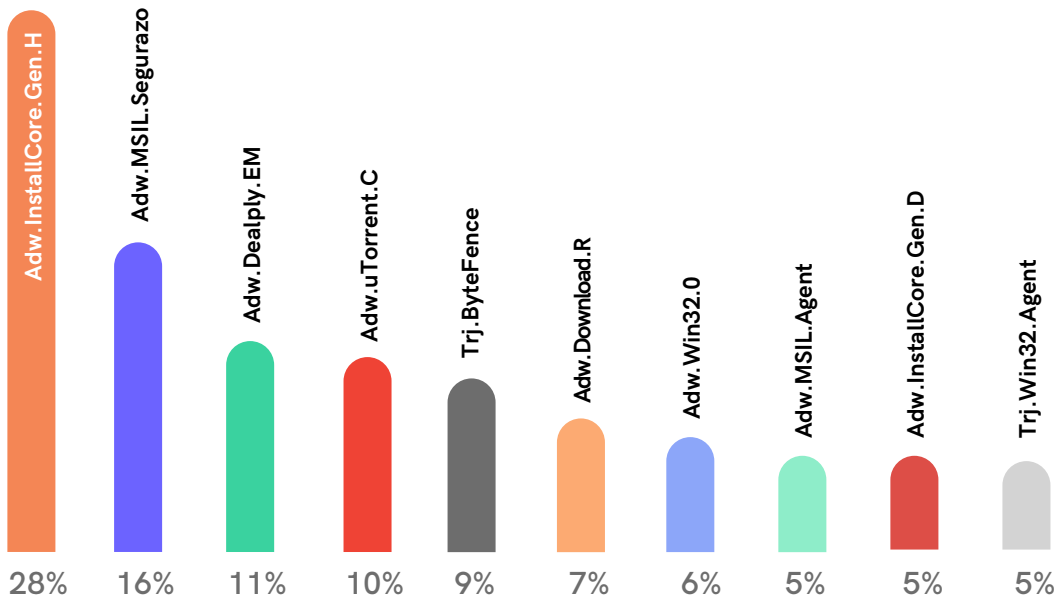
- Ensure all your devices are patched for the latest vulnerabilities
- Monitor for any data breaches regularly by thoroughly checking the logs
- Change your default settings
- Deactivate unused features and services to reduce the attack surface for cybercriminals

Windows Under Siege

Windows Malware Type Breakdown

Telemetry on Windows malware in the country for the first quarter of 2020-21 was a tad different from what we have experienced so far. In this period, many new malware families surfaced on the K7ETI system, hinting that the attackers were on a roll with newer evasive malware to inflict more damage on their victims. However, a few of them belonged to similar families which have remained visible for the past few quarters.

Split of Windows Top 10 Detections



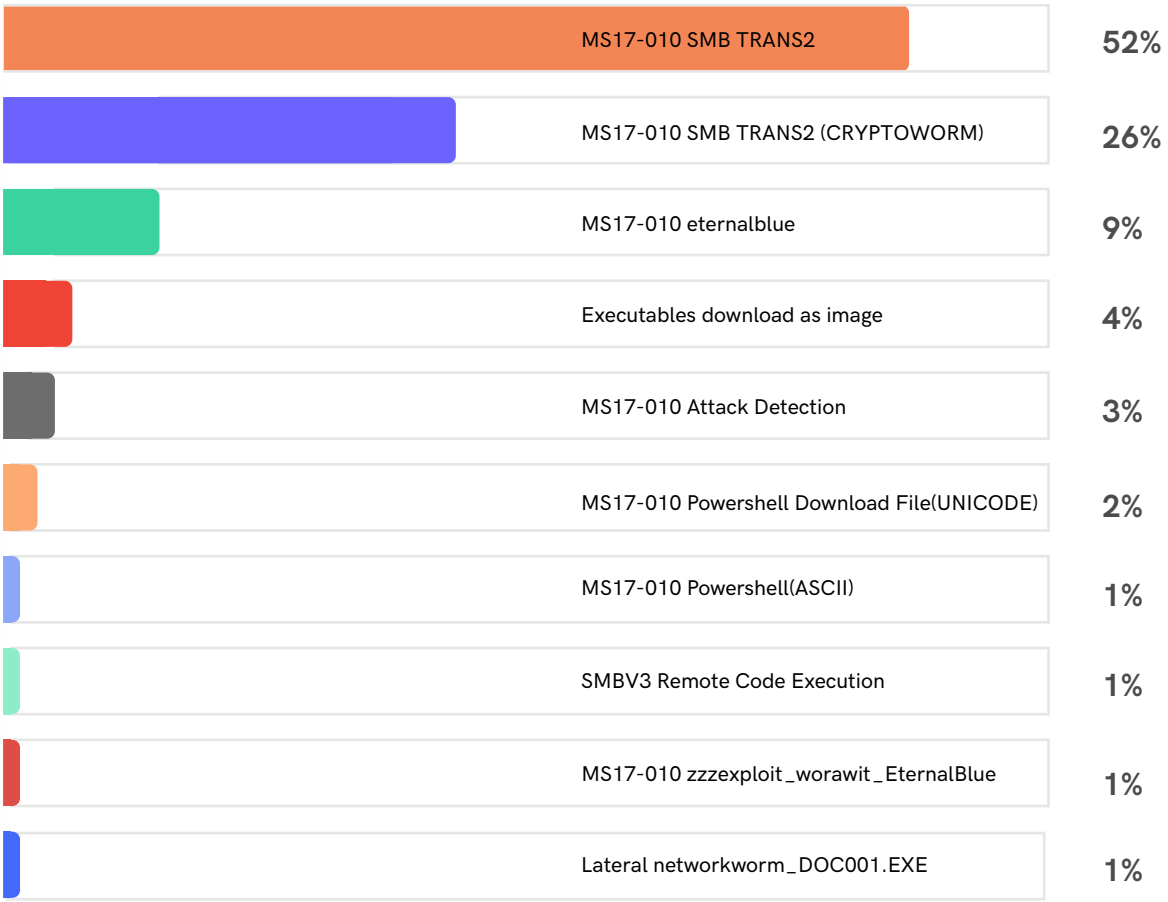
For instance, the first four most visible detections are from prevalent adware families. Such adware comes in the form of bundlers initiated to install adware and potentially unwanted applications (PUAs) alongside legitimate applications. For instance, Adw.MSIL.Segurazo installs a dubious antivirus on the system, which would be impossible to uninstall by a regular user. The adware is known for generating phony system scan results and compels the user to pay for software from untrustworthy vendors to fix the problem.

The infamous three most visible detections spotted during the period were Adw.InstallCore.Gen.H, Adw.MSIL.Segurazo, and Adw.Dealply.EM having a visibility of 28%, 16%, and 11%.

Windows Exploits

Quite like the previous quarter, the visibility of exploits on the Windows platform majorly belonged to the SMB family. The prevalence of EternalBlue based exploits during the period implied that there were still a significant chunk of users who are using dated, unpatched operating systems around the country.

Most Prevalent Exploits



The other two frequently visible exploits were related to PowerShell and suspicious Executable downloads. While the adversaries have long preferred PowerShell for a myriad reasons, Executables download as image is comparatively new in the top lot, using the latest obfuscation methods to bypass gateway/edge reputation-based blocking.

Mitigation Tips

- Keep your devices updated and patched for the latest vulnerabilities
- Change all of your default settings
- Train your employees to look out for signs of a potential breach
- Follow good security hygiene

The Mobile Device Story

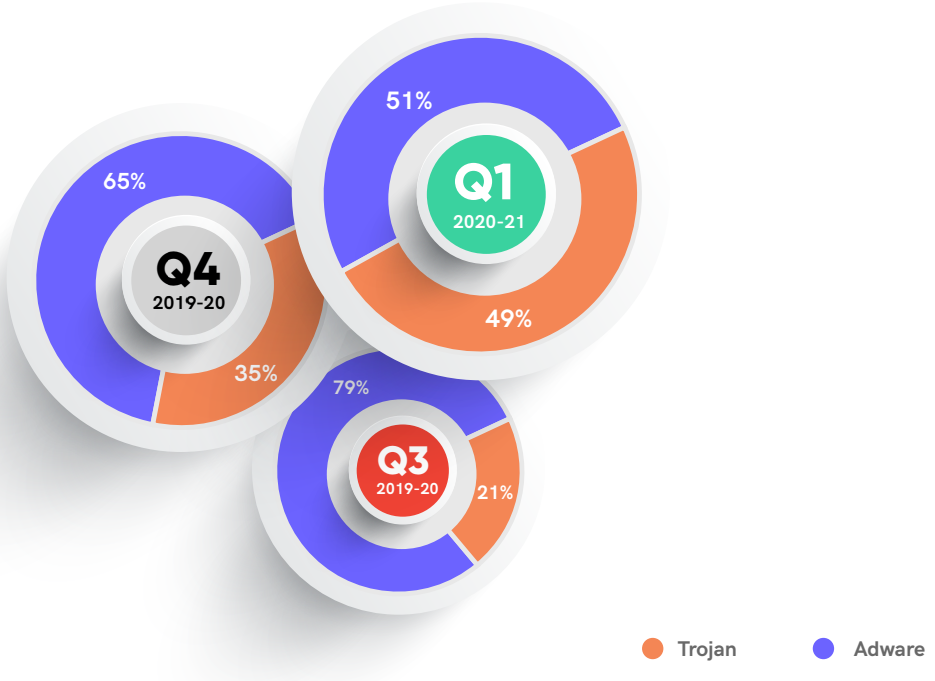
In these COVID-19 days, threat actors have been keeping us on our toes, or ought we to say "on our fingers", more than before, by either creating new malware or revamping existing malware for mobile devices. Android Banking Trojans such as Cerberus, Ginp and Anubis ruled the roost during this period as has been covered already in our **COVID-19 report** mentioned earlier.

This quarter has also seen almost every sort of threat, ranging from SMiShing schemes, adware, fake apps, downloaders, information stealer, and many more. Moreover, scamsters have invested in many legitimate-looking popular apps which collect user's data without their consent for making profit and/or execute many other offensive strategies such as cyber espionage.

We at K7 have also found an obvious sign of the transforming nature of the adversaries targeting the mobile platform, especially Android. With every passing quarter, the money-minded attackers transform their attack strategies and armours to make more money than before.

Instead of following the old route of adware, they are leveraging more power to make dangerous Trojans that come with a more layered approach and better obfuscation techniques to evade detections. Let us see the proportional split of adware and Trojans over the quarters.

Adware vs Trojan Proptional Split



From the comparison chart, we can understand that the adversaries are not only relying on malvertising apps to monetize their efforts but are also developing Trojans to effect their malicious intentions. And like on Windows or other popular platforms, they bank on social engineering via phishing, SMiShing, fraudulent apps, and other techniques to get into the victim's device to install their payloads.

The number of adware and Trojans on the Android platform have drastically swapped their positions in just over a year. Looking at the comparison graph, you can see the percentage of adware found in Q3_2019-20 was 79%, which has come down to 51% in less than a year. The 28% plunge of adware indicates how the Android threat landscape in the country is shaping up differently. The adware slump also shows how the visibility of Trojans has increased from 21% to 49%.

Most of these Trojans are crafted to stay hidden inside the user's device to harvest financial credentials, and other sensitive user information and to execute other malicious intentions of the attacker. They often use cunning social engineering tricks to get into the device and do the damage.

Apart from this, in this quarter something that has become more important and is being strictly enforced by the Government of India is data privacy, though this is one of the persistent cybersecurity goals. Data privacy is about how a user's information is handled, based on its importance, by the organization having access to that data. WIth the growing tensions between India and China, the Indian government has taken a strict stand on how the data should be used. This has led to a ban of 59 Android apps with links to China due to possible data leakage and access to Indian users' data by the Chinese government. Let us see the deeper implications of that order.

GoI Order on Data Privacy Impacting Apps

The Government of India banned 59 apps with links to China that impact data privacy based on the recommendations of Indian Intelligence agencies. The Government has claimed that these Chinese mobile applications are being used to exfiltrate Indian user information to servers based in China. Following the ban, both the official app stores of Android and iPhone have pulled out the listed apps.

The official order released by the Indian Cybercrime Coordination Centre at the Ministry of Home Affairs has claimed that the Indian Computer Emergency Response Team (CERT-IN) has received a plethora of complaints about the banned apps regarding data privacy and security.

The list of banned Chinese apps includes some big names such as ByteDance's social media platform TikTok. Other popular Chinese apps in the banned list are ShareIt, UC Browser, Mi Community, WeChat, UC News, Viva Video, Helo, UC Browser, BeautyPlus, Club Factory and a lot more.

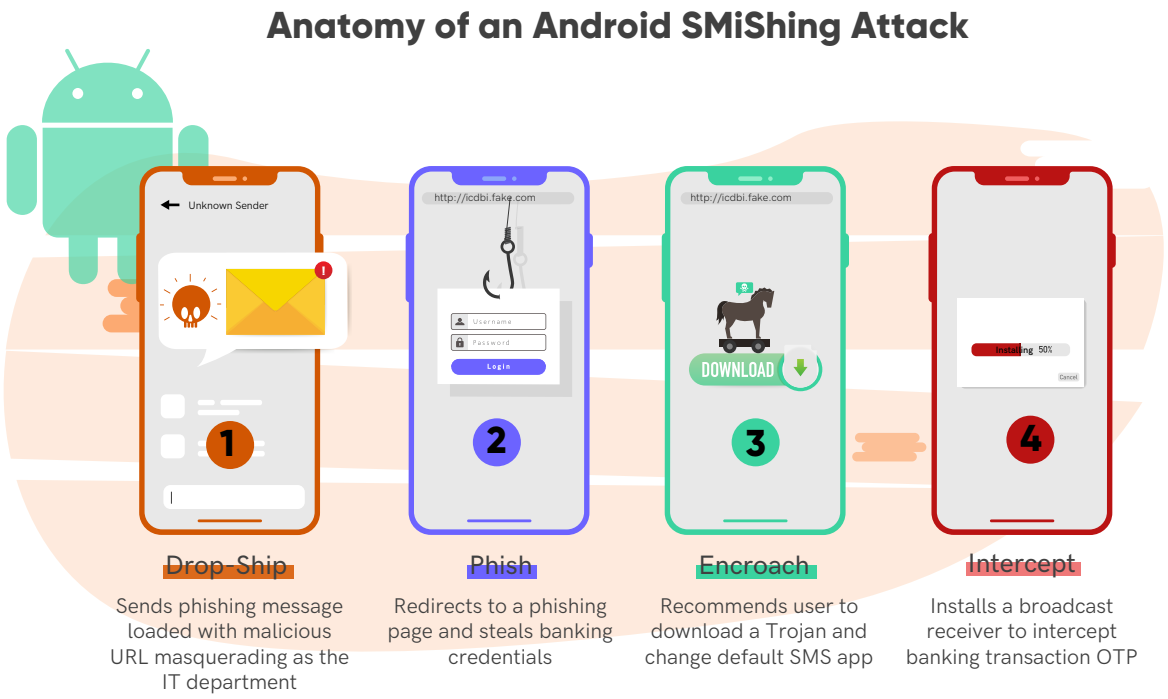
The 59 apps listed may not be exhaustive as there could be other data privacy-compromising apps from mobile manufacturers that are pending a thorough investigation.

However, it is to be noted that the app uninstallation process itself might not be that easy as it could vary depending on whether an app version from the device manufacturer or OEM is downloaded from the official Google Play/third-party store or whether the same app comes pre-installed on the device.

High profile users' data could be more at risk, leading to cyber espionage among other cyber attacks. So users are advised to read the data privacy policy of the app to be installed on their device to know what information would be shared and in which location it would be stored.

Case Study: Rising SMiShing Attacks on Indian Users

Recently, one of our colleagues received an SMS from BW-INFMSG. The sender, masquerading to be from the Income Tax Department of India, urges the recipient to click on a malicious link to submit a formal request for the payment of their overdue tax refund for a certain amount. Once the user clicks on the link, it redirects them to a phishing page impersonating the Income Tax Department of India. The site asks the victim to select the bank preference. Once selected, the victim gets prompted to enter the User ID, password and any other data related to do a fund transfer for the selected bank.



In addition, the victim gets a prompt asking to enter more personal and sensitive information as well.

Once the victim completes the above process and clicks on Submit, the victim gets redirected to another web page which recommends installing a malware APK (Android application installer PacKage) disguised as a part of the verification process.

If the victim installs the APK file, the app installed in the name of "Certificate" requests specific permissions to stay in stealth mode. The granted permissions also ensure that any instances of the APK do not appear on the device notification bar.

Alongside, the app also requests the user's permission to become the default SMS app and other SMS-related permissions such as sending or receiving SMS messages. With these permissions and registered receivers, the malware app intercepts all incoming messages and collects One-Time Passwords (OTPs) from the bank with no obstruction and without the user's knowledge.

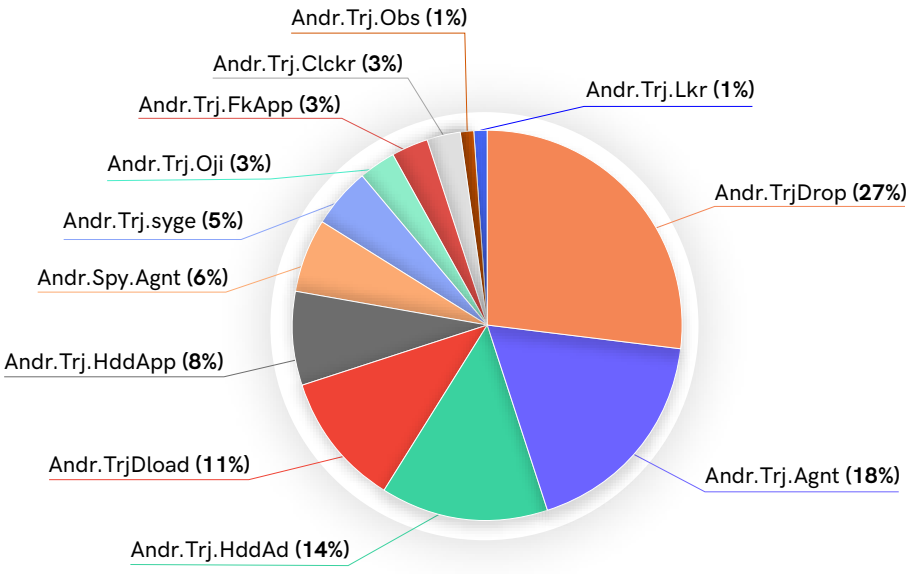
Once set, the attacker silently forwards the money to their own accounts, and aborts the SMS notification to the user so that the victim would never know about the surreptitious transaction.

The attacker also harvests other user information such as email address, device model, and device admin status, which get forwarded to another suspicious URL.

The Eventual Rise of Trojans

The upswing of Trojans remained noticeable in Q1_2020-21. Out of the total number of Android attacks in the country, 49% of the victims were hit by Trojans in the quarter.

Most Prevalent Trojan Types



The most commonly observed Trojan was Andr.TrjDrop with a 27% presence out of the total number of Trojan attacks. Though Andr.Trj.Agnt slumped from 24% to 18% it continued to hold the second spot this quarter. Andr.Trj.HddAd, the third spot holder in the most visible Trojan list, has upped its presence from 7% to 14%.

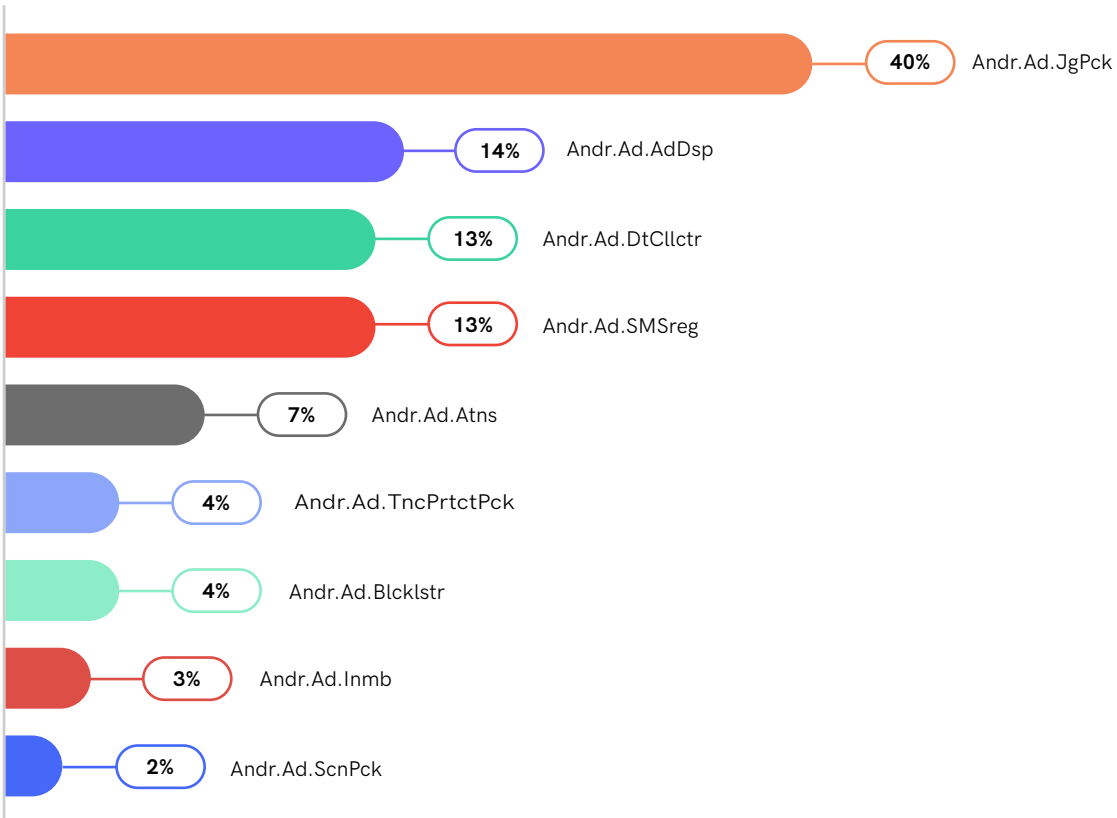
Another prevalent Android Trojan Andr.TrjDload, too, has recorded a 2% increase in its momentum in contrast to the previous quarter.

Alongside this, we also spotted a few new Android Trojan families during the period, such as Andr.Trj.syge, Andr.Trj.Obs, and Andr.Trj.Lkr.

The Significance of Adware

Despite the steady decline in numbers, individual adware families have held their sway for some time. For instance, Andr.Ad.JgPck has maintained its margin and recorded 3% more visibility than in the previous quarter. The presence of Andr.Ad.JgPck seemed relevant since this infamous adware has strengthened its presence steadily during the previous two quarters too.

Trend Line Showing the Adware Plague



Despite holding the second spot, another prevalent adware family Andr.Ad.AdDsp has weakened its presence by 16% from the previous quarter. Andr.Ad.Atns has also recorded a visible plunge from 14% in the last quarter to 7% during this period.

Other prevalent adware are Andr.Ad.DtClltr and Andr.Ad.SMSreg.

Android Trojan Trends Amidst COVID-19

Nowadays, people have started sanitizing even their smartphones for the fear of getting infected with the deadly coronavirus. However, if you do not want your digital experience to go haywire, it is equally important to be careful about your online activities that you do with your phone such as the apps that you download, transactions that you make, the websites that you visit and the activities that you do there.

Threat actors have started taking advantage of this pandemic to expand their victim base and revenue, and for this they have decided to make mobile devices as a storehouse for Trojans. From fake apps that claim to provide information on the current pandemic situation to apps faking protection measures claiming to safeguard users from getting infected, we have seen it all. For easily capitalizing on their revenue front, Banking Trojans have become their best bet these days considering the fact that all the transactions are being made online as people do not step out for the fear of getting infected in the real world. These Trojans spread by using COVID-19 situation as a ruse.

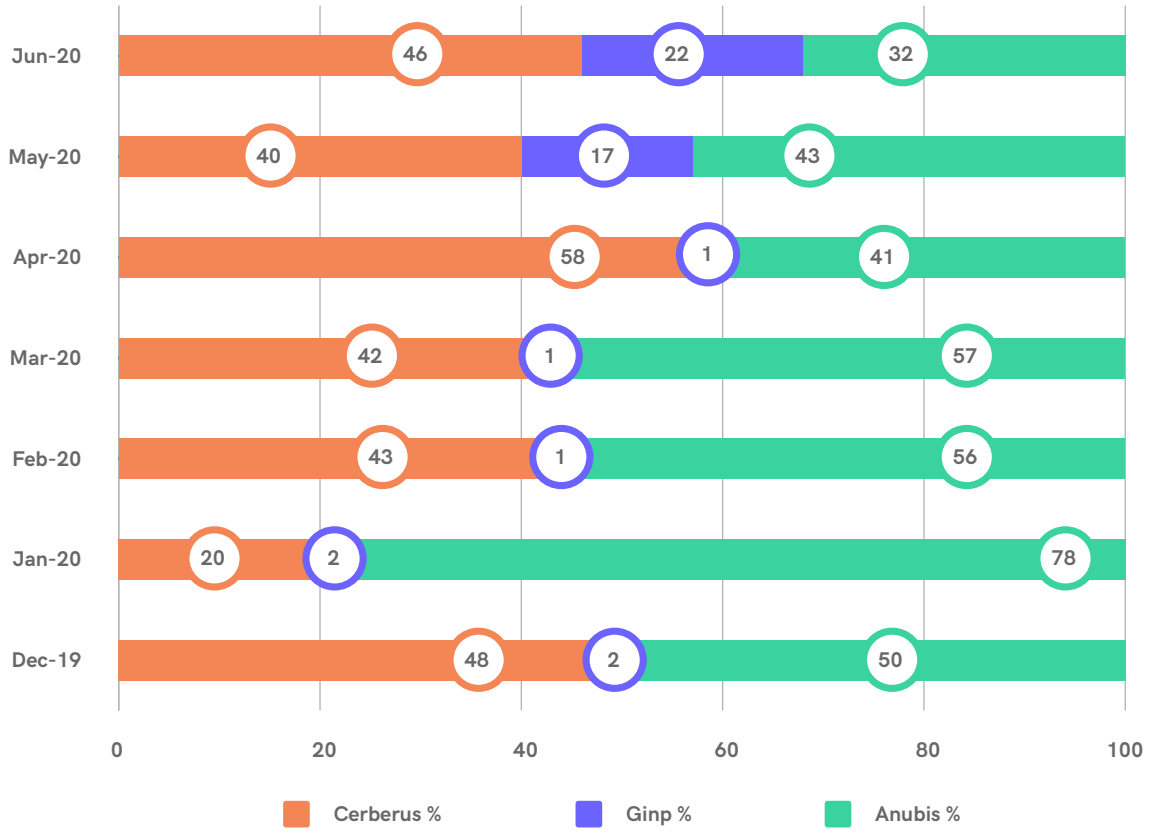
Here, we will be looking at the surge in Android Banking Trojans amidst this pandemic, using which threat actors gain access to confidential information of the users when they transact online.

Stats

Stats reveal that there has been a considerable increase in the number of Trojanized Banking apps that have escaped security checks from the official App Store, and snuck their way onto the user's device. The most infamous few have been Cerberus, Anubis and Ginp. These Trojans try to deceive the users into installing the infected app by pretending to give COVID-19 information.

While Cerberus promises to be a "Coronavirus tracker" and uses the screen overlay technique to steal credentials and sensitive user data, it also has Remote Access Trojan (RAT) and keylogger functionalities. The Ginp Trojan disguises itself as the app "CoronaFinder" and promises to provide the location information of coronavirus-infected people around the user on the payment of a small amount; it then proceeds to steal financially-sensitive information. The Anubis Trojan masquerades as a "Coronavirus statistics" app and hides itself to steal the user's sensitive information.

Android Trojan Trends Amidst COVID-19



*Data has been round-off to the nearest decimal

*Jun-20 data is still 15-Jun

The chart shows the proportion of malicious banking apps against the total listed for a particular month.

We have tracked these banking malware from Dec-19, the time when COVID-19 was first reported to the World Health Organization (WHO) till mid Jun-20.

We can glean from the statistics depicted above that there has been a steep increase in Banking malware during June, considering the fact that the stats for Jun-20 is only till the middle of the month, in contrast to the other months under consideration.

The proportion of apps affected by Banking Trojans such as Cerberus and Anubis in both Google Play store and third-party markets has shown a considerable increase in Jun-20 when compared to Dec-19, the official confirmation of the start of this deadly pandemic.

This can be attributed to the fact that the threat actors have started taking more and more advantage of the "Work from Home" scenario and the increased use of smartphone based transactions done by users for all necessities. We believe that this trend may continue or even increase further in the coming months and possibly even in a post-COVID world

How do such malicious apps succeed in entering onto a victim's device and doing their malicious behaviour?

Here are few of the most commonly-used techniques amongst many:

- By disabling Google Play Protect
- By disguising themselves as benign apps or using a system name for the app, making it difficult to uninstall
- By hiding the app icon in the launcher
- By posting fake positive reviews of apps by masquerading as the victim and luring users into installing their apps

How are such malicious apps identified?

- Google Bouncer, a Google Security service that exists to verify an app's maliciousness or unwanted behaviour status even before it is made available in Google Play for users to download
- Google Play Protect tries to protect users from apps that steal data, secretly monitor or harm users, or are otherwise malicious
- Users reporting malicious app behavior to Google for removal of those apps
- Nefarious apps being reported by Anti-Virus vendors

With the rise in COVID-19 spread and the numbers of Android users, developing malware for this mobile OS using COVID-19 as a ploy, has become a profession rather than a hobby for the bad actors. Users are therefore advised to be on guard while downloading seemingly benign apps related to COVID-19. In particular, refrain from being deceived by fake reviews posted by threat actors to increase the app rating.

K7MS detects all the above listed Banking Trojan variants generically.

Tips to Stay Safe

- Keep your devices updated and patched for the latest security vulnerabilities
- Do not click on links in SMS, emails and the like sent to you, especially by unknown senders
- Exercise caution even while installing apps from the official App Store
- Disable "Install unknown apps" on your Android devices. Remember to never download apps from any third-party app store
- Download apps only after knowing what information is collected and shared
- Watch out for fake reviews such as checking if a lot of reviews were posted on the same date, reading the reviewer's profile, etc.
- Check app permissions during installation. Abort the process if unnecessary privileges are asked
- Practice good security hygiene
- Scan your device regularly
- Install a robust security product such as K7 Mobile Security to stay protected from the latest threats.

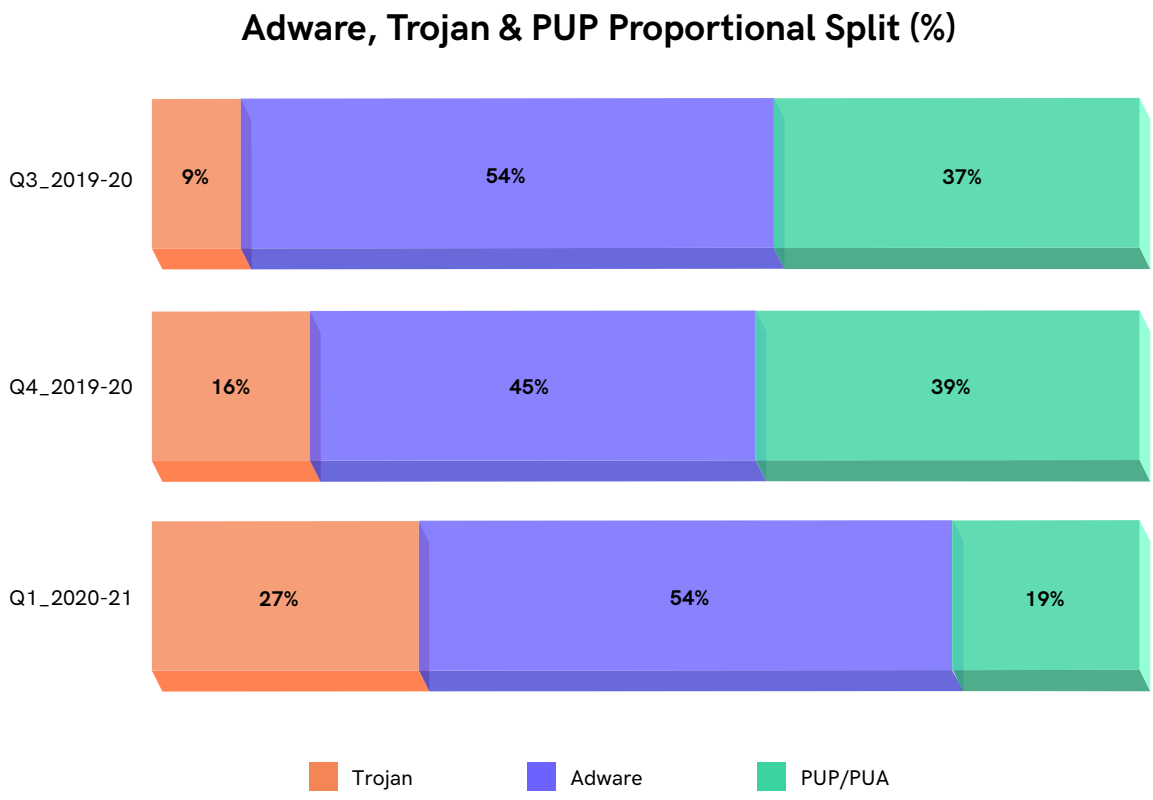
Mac Attack

macOS is popular among computer users for reasons such as stability, attractive GUI and also for claiming to be less malware-prone, among others. To prove their mettle, the threat actors want to break the chains of this so-called safety net, and want to victimize users of this OS too. The adversaries are constantly developing malware to attack individual macOS powered machines or networks to make money, accumulate sensitive financial information or to mine cryptocurrency, and are quite successful at that.

However, the momentum of mining any cryptocurrency on the macOS platform has dwindled significantly. In contrast, the frequency of various sorts of Trojans and ransomware has spiked up to a surprising extent.

The growth doesn't mean the decrease of adware on this platform. Looking at the statistics from previous quarters, we found a clear indication of how adware's popularity has remained uninterrupted.

Based on the statistics from the previous few quarters, we have found out how the adversaries are evolving in the macOS arena. However, in Q1_2020-21, they are putting fewer efforts into making Potentially Unwanted Programs (PUPs) and have started focusing more on either developing Trojans or adware.



From the stats comparison list, we can see how the Mac threat landscape would evolve going forward. There was a 7% increase in Trojan attacks in Q4_2019-20 in comparison to Q3_2019-20; and in Q1_2020-21, the surge continued with a growth of 11% in comparison to the prior quarter.

Apart from new malware, the adversaries are using revamped versions of existing malware with sophisticated intrusion techniques and obfuscation methods to stay undetected until accomplishing their missions.

The Wickedness of EvilQuest

For instance, EvilQuest, the latest ransomware in the wild was spotted by K7 threat researcher Dinesh Devadoss. Dinesh's revelations give several interesting facts about the ransomware strain. The newest ransomware is quite unlike existing macOS ransomware.

The instances of EvilQuest revealed that the attackers put the ransomware installer inside several pirated software installers. These installer files are quite popular among torrent hosts and online forums across the internet.

According to Dinesh's findings, the ransomware file comes disguised as a Google Software update. Later, other researchers' contributions revealed that the ransomware is capable of hiding itself inside other popular streams of software such as security, music, etc.

Apart from encrypting all the user data with AES encryption, EvilQuest can terminate certain running Anti-Virus programs on the system apart from employing Anti-Debug and Anti-VM techniques.

Dacls RAT and Lazarus

Lazarus is quite a big name in the cybercrime industry for its cyber espionage and destructive activities. The state-sponsored hacker group has been active for more than a decade, compromising hundreds and thousands of enterprise servers through its destructive malware. Wannacry is one such ransomware, which devastated enterprises globally in 2017.

Another very effective malware by this North Korean based hacker group was a Remote Access Trojan (RAT) called Dacls.

Interestingly, the Dacls RAT was already launched, targeting the systems and networks running on Windows and Linux based distros. But a few of the latest instances have proved that the RAT is also targeting macOS users.

Deriving its name from its file name and hard-coded strings, Dacls follows a modular approach with a capability to strengthen its nefarious capacity through added plugins. The modular approach lets malware execute customized attacks by delivering numerous malicious payloads tailored for the target victim.

The Dacls RAT for macOS users is capable of controlling the victimized Mac computers remotely. Following the compromise, the adversaries could read, write or delete archived system files remotely, execute commands, and a lot more.

The Dacls RAT for macOS comes with seven plugins, out of which six were already familiar from its Linux version. Each plugin comes with a configuration section that gets loaded while initializing the plugin.

Workings of Dacls RAT

This RAT comes bundled with a two-factor authentication app repacked from an open-source application available on Github. The app file is an executable that hides its plugin, and Command and Control (C2) server information inside its config file. The config file also stores critical device information such as PUID, Pwuid and a lot more.

Once the Remote Access Trojan (RAT) manages to infect the system, it waits for the machine to reboot. On reboot, Dacls modifies the program list (plist) file used by the system's startup launch applications LaunchAgents and LaunchDaemon.

Post network reconnaissance, the Trojan communicates to C2 servers to send the system logs through a proxy.

The Multi-OS Attack Campaign

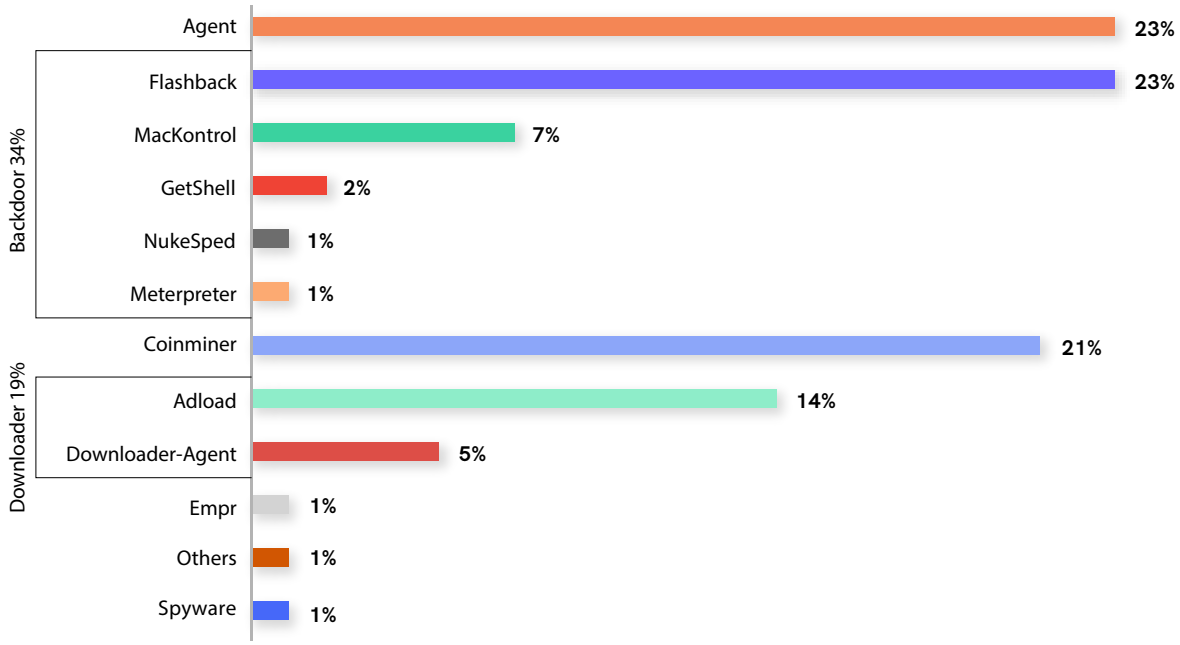
Interestingly, Dacls is not the only malware to target multiple operating system users. With the inception of the modular malware approach in 2019, malware authors nowadays don't restrict their targets to a specific operating system. They instead develop attacks targeting the most popular operating systems to increase the frequency of attacks and their bank balance.

And with its steady rise in popularity, macOS has become one of the most targeted operating systems for cyber attackers following Windows OS.

The Reign of Trojans

Looking at the Trojan attacks, statistics offer many exciting revelations. While the coinminer attacks have recorded a massive drop of 32% compared to the previous quarter, the backdoor attacks have shot up by a considerable extent. Flashback, MacKontrol, GetShell, MeterPreter, and NukeSped have taken up 34% of the share this time, which is 30% more than in Q4_2019-20.

Trojan Detection Trend lines

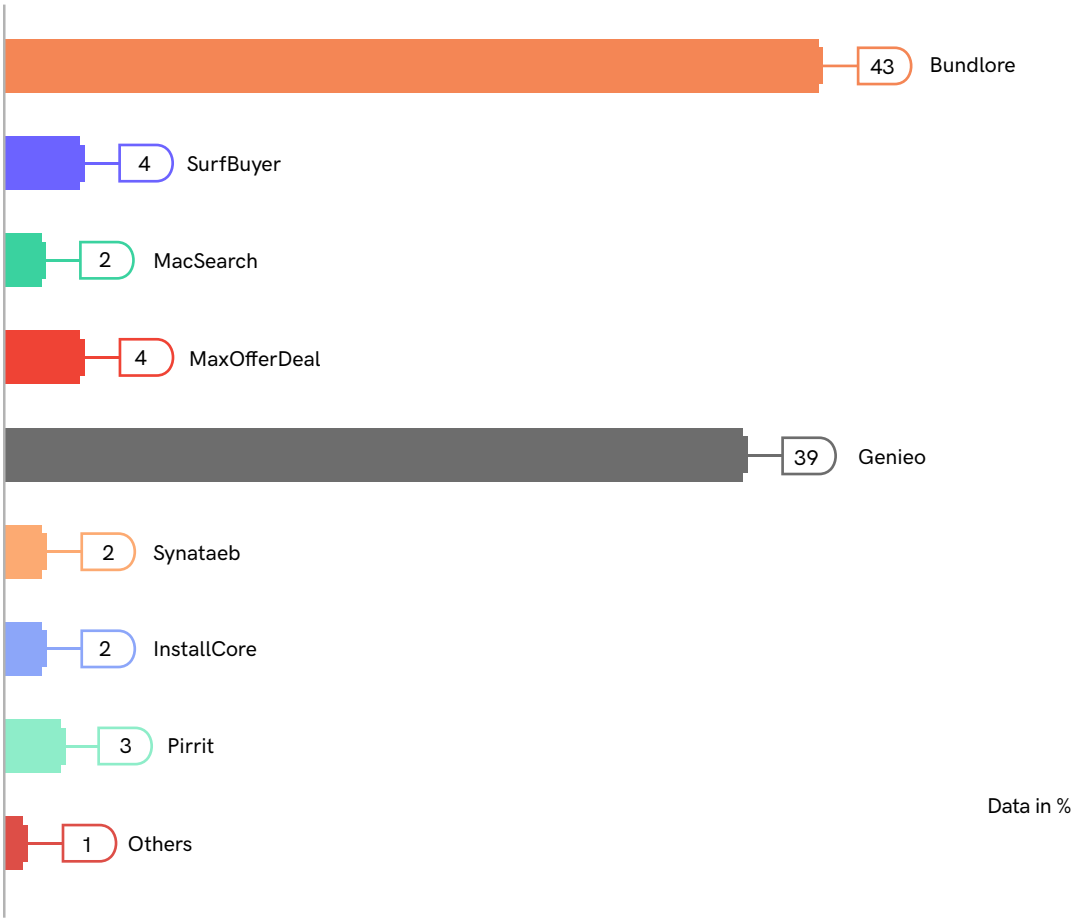


The Agent Trojan maintained its visibility in this period too, and managed to spike up its volume of attack from 17% to 23% in this quarter. The steady increase reveals how threat actors are actively victimizing end-users via injecting malware through Agent-type Trojans. Flashback, a prominent backdoor, has shared the top spot with Agent with a 23% presence. The infamous advertisement downloader, Adload, was 4% less visible in this period.

The Upsurge of Adware

The steady upward trend of Trojans has not yet impacted the visibility of adware. The top adware from the previous quarter, Bundlore, has managed to hold the crown with another 1% increase in visibility. But other infamous adware such as SurfBuyer and MacSearch have lost their reign. However, Genieo has recorded a massive increase of 37% in contrast to the last quarter and accounted for a presence of 39%.

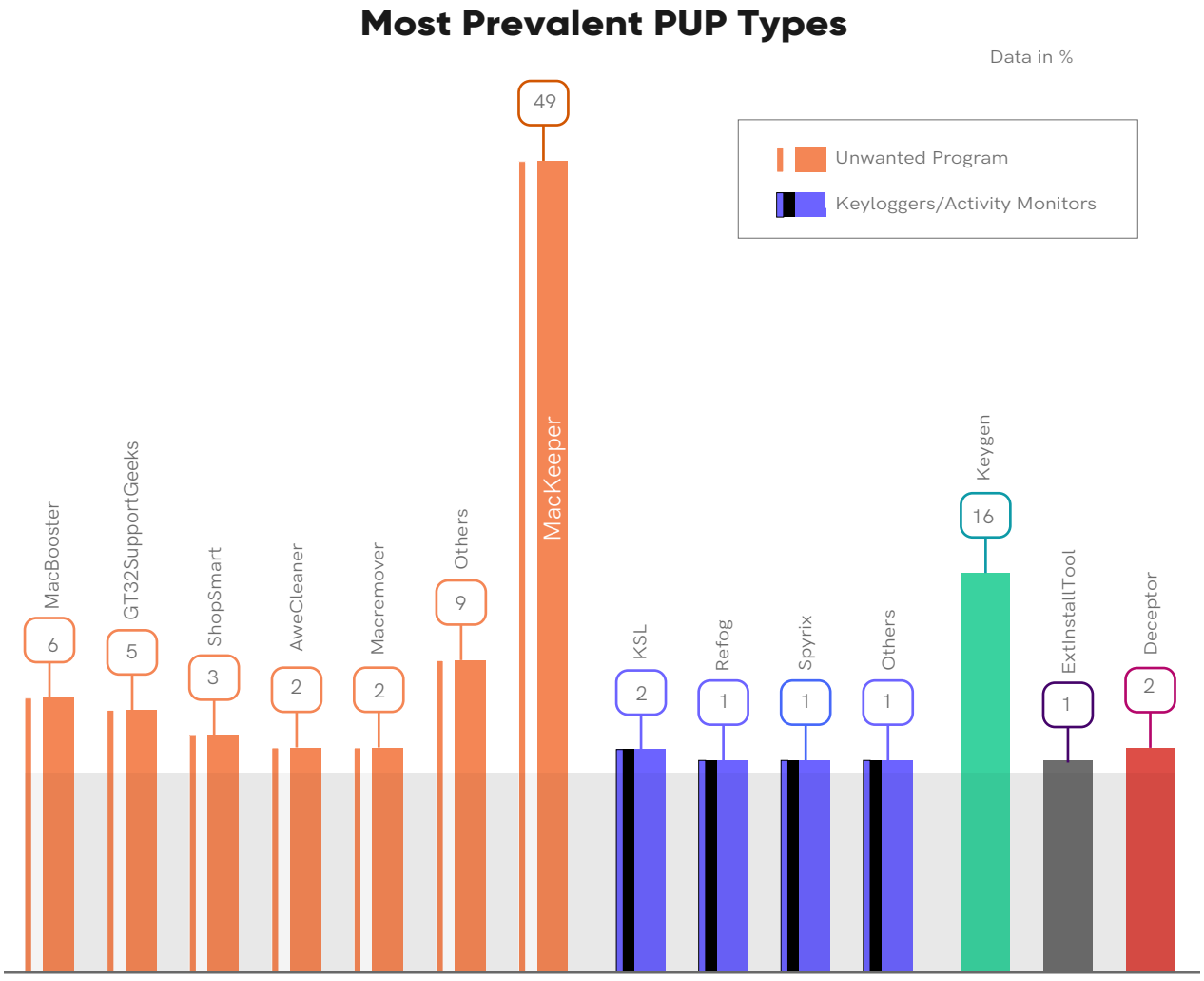
The Trend line of Adware Variant Detections



Though Genieo mostly behaves like adware, it is notoriously known for activities such as browser hijacking and modifying environment variables to ensure the system becomes unstable after uninstalling it.

The PUP Trend Line

The top PUP spot is still firmly in the hold of MacKeeper even after a massive plunge of 36% from the previous quarter. In this period, we found a large variety of Potentially Unwanted Programs (PUPs), out of which many belonged to the keyloggers or activity monitor categories. In the guise of utility software, these PUPs record the victims' keystrokes to steal financial credentials, snoop into their online/offline activities, and later send the data to the attackers. Keyloggers are also often used by the attackers as a part of cyber espionage.



These PUPs or PUAs also serve several other activities on behalf of the attacker and hamper the smooth working of devices.

Safety Guidelines

- Keep your macOS updated and patched for the latest vulnerabilities
- Say "No" to pirated software
- Ensure scanning all your applications even if it is being downloaded from the official App Store
- Install a reputable security product like "K7 Antivirus for Mac" and keep it updated to protect yourself from the latest threats
- Ensure to back up all your data and make sure it is malware-free

Key Takeaways

The alarming rate of cybercrime incidents around us should encourage caution from both enterprises and consumers. The frightening increase of phishing, business email compromise, malware, and other forms of highly sophisticated attacks demonstrates a multifold growth rate in favour of the bad guys.

To counter the onslaught of cyber attacks on the enterprises and individuals, one must follow a set of recommendations to toughen your digital security posture.

Enterprise	Consumer
Secure ALL 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
Regularly assess your network for possible breaches	Installs apps only from the official App Stores and be wary of apps that could impinge on your data privacy
Back up your critical data and ensure they are malware-free	Do not click on unknown links and links that you are not sure of

K7 SECURITY

www.k7computing.com

JULY 2020