CYBER THREAT MONITOR

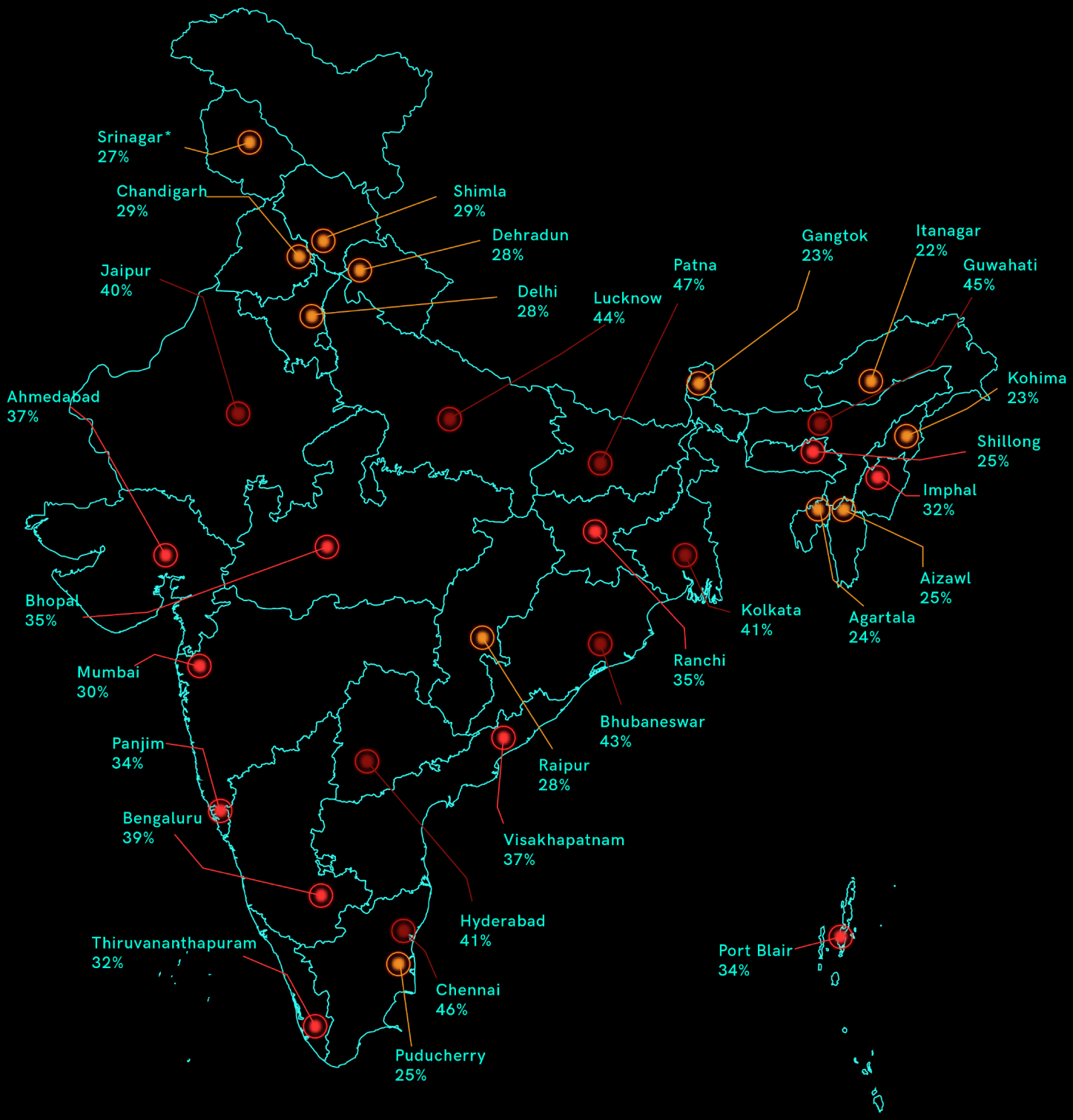
K7 LABS

Q2

2019 - 20

K7 SECURITY

CYBER THREAT MONITOR - INDIA



*-18% drop in the number of devices reporting telemetry

Map for illustrative purposes only. Not to scale.

CONTENTS

PAINTING INDIA'S CYBERSECURITY PORTRAIT

"The K7 Cyber Threat Monitor Q2 2019-20 report is an effort to offer a glimpse of the complete Indian cybersecurity landscape. Gleaned from the trends we observed during Q2 2019-20, and the millions of insights that we gained through our telemetry, received from both our consumer and enterprise customers, the K7 CTM report will detail the attacks encountered by Indian netizens over the Q2 period.

We had introduced a concept called "Infection Rate" in the Q1 2019-20 report to elaborate on the regional exposure to threats encountered by the netizens of India. In this quarter, we continue to offer granular analysis, grouped by Tier-1 and Tier-2 cities, out of which a few could be representative of their respective states.

The report also offers a detailed picture of all the prevalent threats grouped by popular platforms like Windows, macOS, Android and IoT.

As expected, Q2 2019-20 experienced an unprecedented wave of targeted cyberattacks. Adversaries used a blend of new and old tactics of social engineering, phishing and exploitation of system weaknesses for the distribution of malware and for launching targeted cyberattacks. Though the enterprises and SMEs were the bullseye for cybercriminals, consumers weren't spared either. The presence of pervasive adware in macOS and Android hints how they are still actively promoted by many cybercriminals.

We hope these insights will help organisations improve their responses towards tackling the challenges posed by the adversaries, which would also be of immense help while drafting their cybersecurity policies. This also helps consumers gain an overall insight about the existing and emerging threats and how to reduce the risks associated with the same."

REGIONAL INFECTION PROFILE

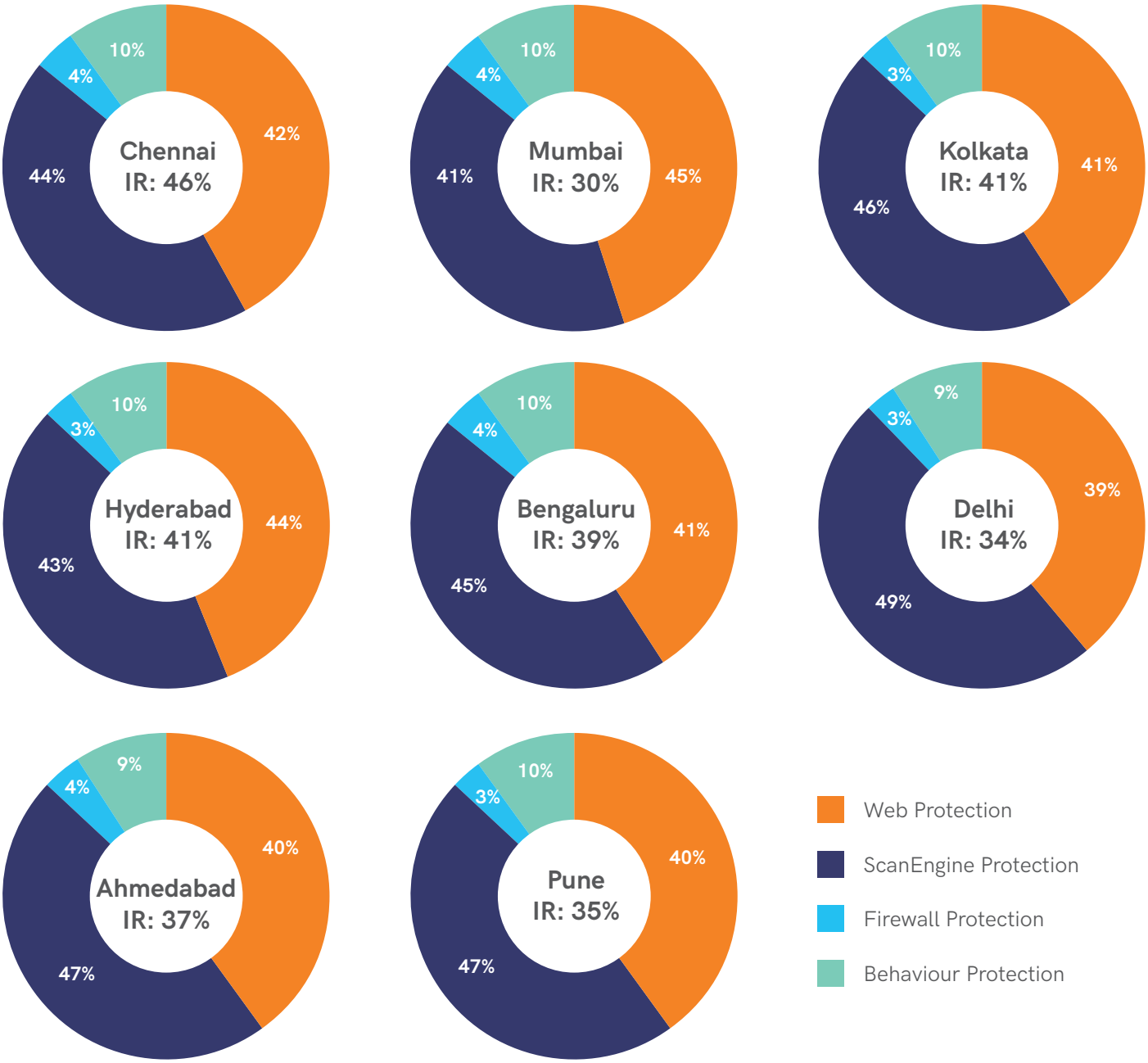
At K7 Security, we encounter cyber adversaries on a daily basis and hone our threat-countering skills to keep them at bay. In the process of detecting and thwarting numerous attacks every day, we have experienced every sort of malware and emerging threat of the cyber world. Analysing these based on their geolocation evokes myriad concepts regarding the cybercriminals' agenda, targets and sometimes even hints about their future strategies. This detailed and insightful information often helps us to detect the emerging and growing threats which would give the necessary awareness in crafting our cybersecurity policy and posture.

"Infection Rate", described as the regional percentage of threat events reported to our K7 Ecosystem Threat Intelligence (K7ETI) infrastructure can be used as a barometer to measure the exposure of netizens grouped by state capitals, Tier-1 and Tier-2 cities to threats, i.e. those who encountered at least one threat event during the period.

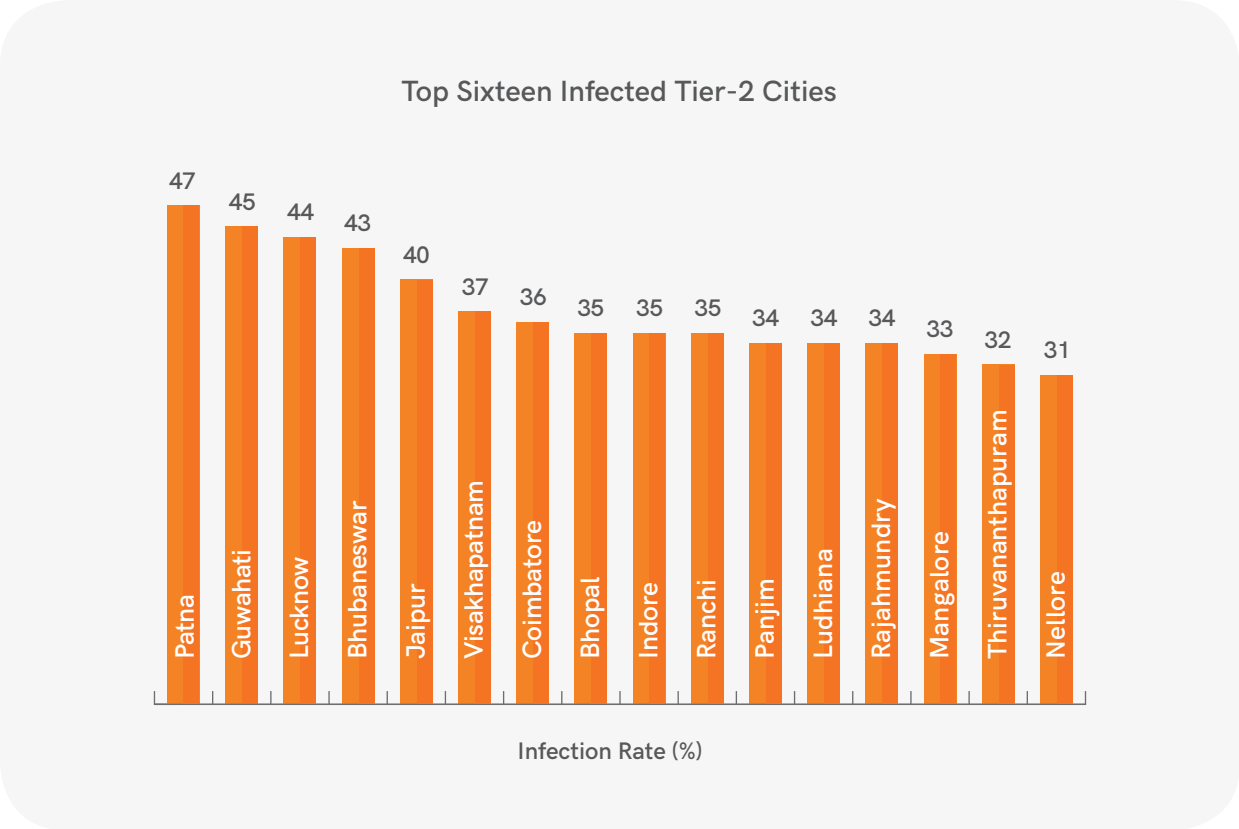
The figures highlight high-risk areas, and it is this quarter's state-capital-wise infection rate that is depicted on the map of India at the beginning of this report.

The statistics may be suggestive of high-user cities. During the period, our telemetry data indicates that, on average, approximately three out of every ten Indian users encountered one or more cyberattacks. By comparison to the previous quarter, many of the high-user cities have experienced a similar number of sustained attacks.

The Metros and Tier 1 Cities - Infection Rate



Attacks in Delhi ballooned in Q2 with a 6% increase in the quarter-on-quarter infection rate. The IR in Cyber City Hyderabad is 41% from 39% recorded last quarter. Bengaluru and Pune experienced 39% and 35% of cyberattacks, similar to the previous quarter. Despite a 2% decrease in infection rate from the last quarter, Chennai still remains most vulnerable at 46%. Kolkata follows soon after at 41%. Ahmedabad, at 37%, witnessed a 1% drop in infection rate compared to the previous quarter, and Mumbai had an identical thirty percent.



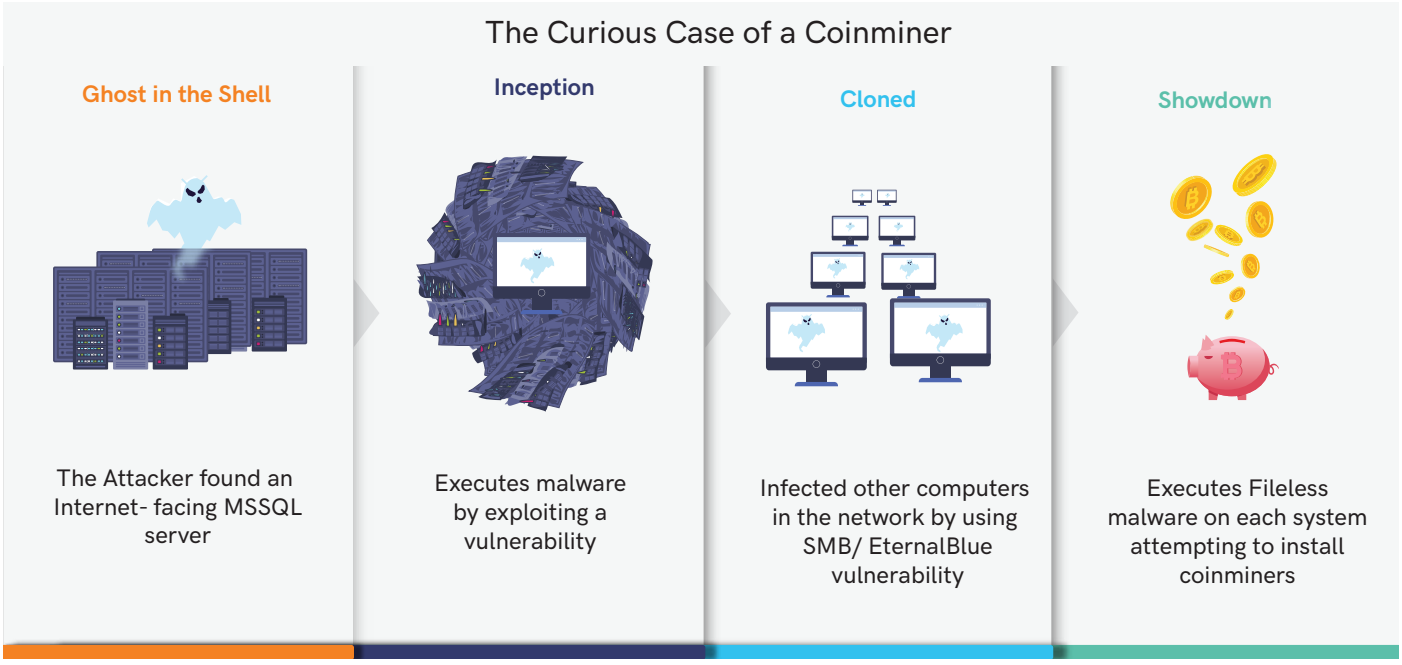
It is surprising to see how the infection rate is spiking up every quarter in most of the popular Tier-2 cities. Patna still holds the highest percentile of cyberattacks at 47% compared to the rest of the Tier-2 cities, and higher than any Tier-1 city. Guwahati, Lucknow, Bhubaneswar and Jaipur witnessed a massive forty-five, forty-four, forty-three and forty percent of the cyber users coming under attack. Alongside, other Tier-2 cities also faced repeated attacks, showing how cybercriminals are indiscriminate about smaller city-based prey, some of them perhaps considered collateral damage. It might be because of the low Internet data cost, easy and affordable availability of devices which can be used to exploit, and most certainly insufficient cybersecurity awareness amongst netizens.

In Q2 2019-20 cybercriminals have introduced new attack methods and sophisticated malware, along with old-school malware techniques like phishing and exploitation of vulnerabilities found in public-facing systems.

Many system vulnerabilities, including that exploited by the infamous EternalBlue (for which a patch is available), persist in many of the enterprise, SME and SOHO networks. From the multitude of infiltration and infection cases that we observed, let's highlight two case studies which demonstrate how cybercriminals have exploited the weaknesses that exist in networks to launch sophisticated attacks, effecting a complete takeover.

Case Study 1: The Curious Case of a Coinminer

In one scenario observed by K7 Labs, a malicious PowerShell script was trying to download and execute a coinmining malware which promptly got blocked by K7 Endpoint Security. Initially, it looked as if the script was getting triggered through Task Scheduler, however, we were unable to find related entries in scheduled tasks. Upon further analysis, we found that it was a fileless malware, as it was loaded from a standard OS repository and executed in memory, whilst its disk-based traces were removed from the repository. The detailed attack flow is given below.

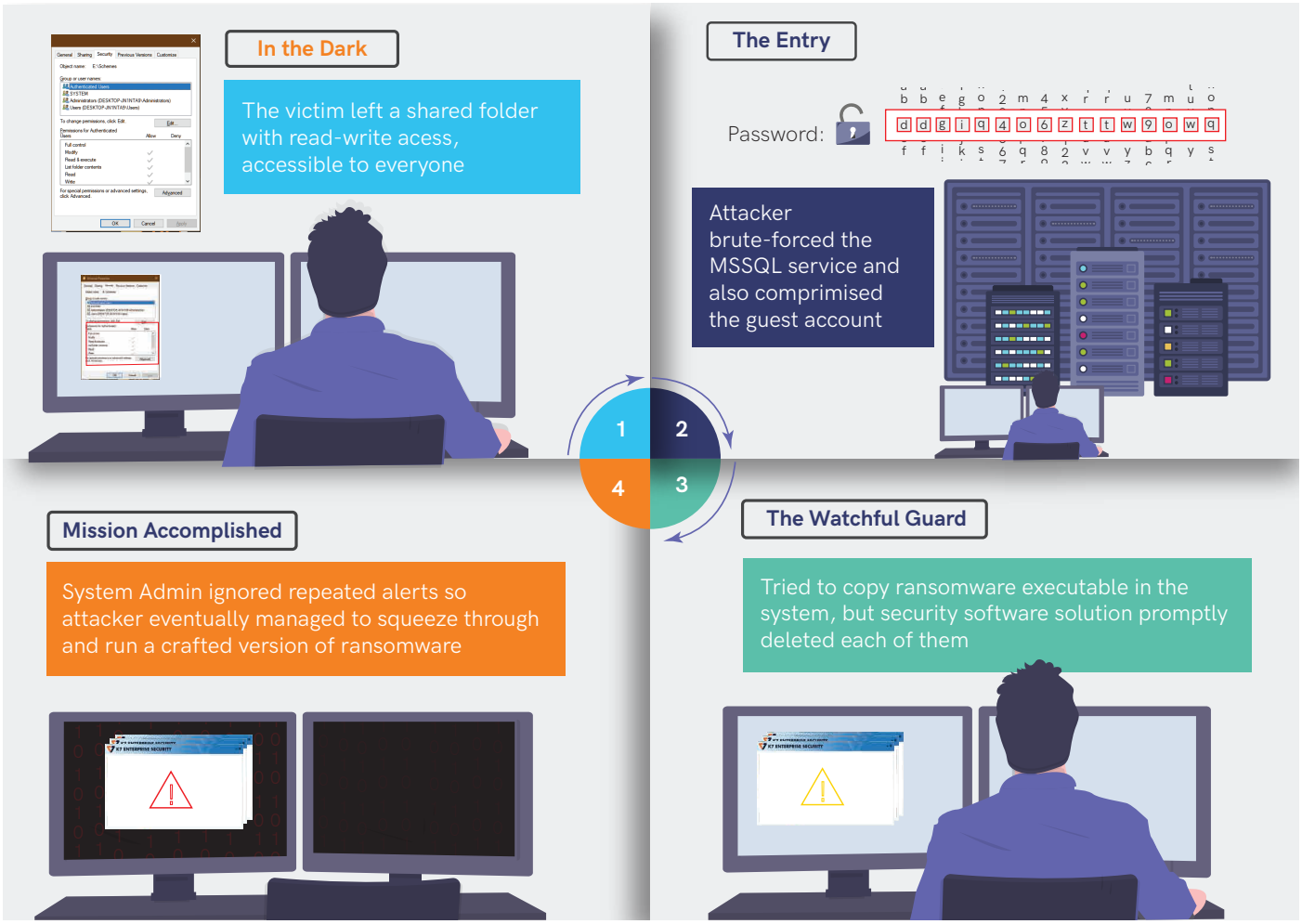


Case Study 2: Anatomy of a Ransomware Outbreak

In another scenario, we observed a ransomware infected machine. On checking the security product logs, we found that there were as many as 167 malware detections within the two-day period prior to the ransomware attack.

Further analysis revealed that the customer had a publicly-shared folder, offering full readable and writable access. The adversaries had used it as a storage repository for their malicious stockpile that could then be used as a launchpad for attacking other entities on the Internet.

The attacker had initially brute-forced the MSSQL service and also compromised the guest account feature, which was in an enabled state, and used it as the pivot system (A pivot system is an initial target machine which lets the adversary get a foothold into the network, from where the attacker can target other connected machines) with freshly minted variants of the ransomware which eventually managed to get executed by camouflaging itself with an effective benign cloak.



Safety Recommendations

- Ensure that the OS and all services running on the server, be it web servers, mail servers or SQL servers, are up-to-date and patched for the latest vulnerabilities.
- Admins must NOT ignore security software notifications. They should be prompt in responding to the same. This would help them to detect and prevent attempts to compromise the system in time.

VULNERABILITIES GALORE

Every quarter, K7 Labs sees hundreds of newly-discovered vulnerabilities which are used to execute multi-stage zero-day attacks, spread malware or otherwise to strengthen the adversaries' arms to wreak havoc on enterprise targets or end-users.

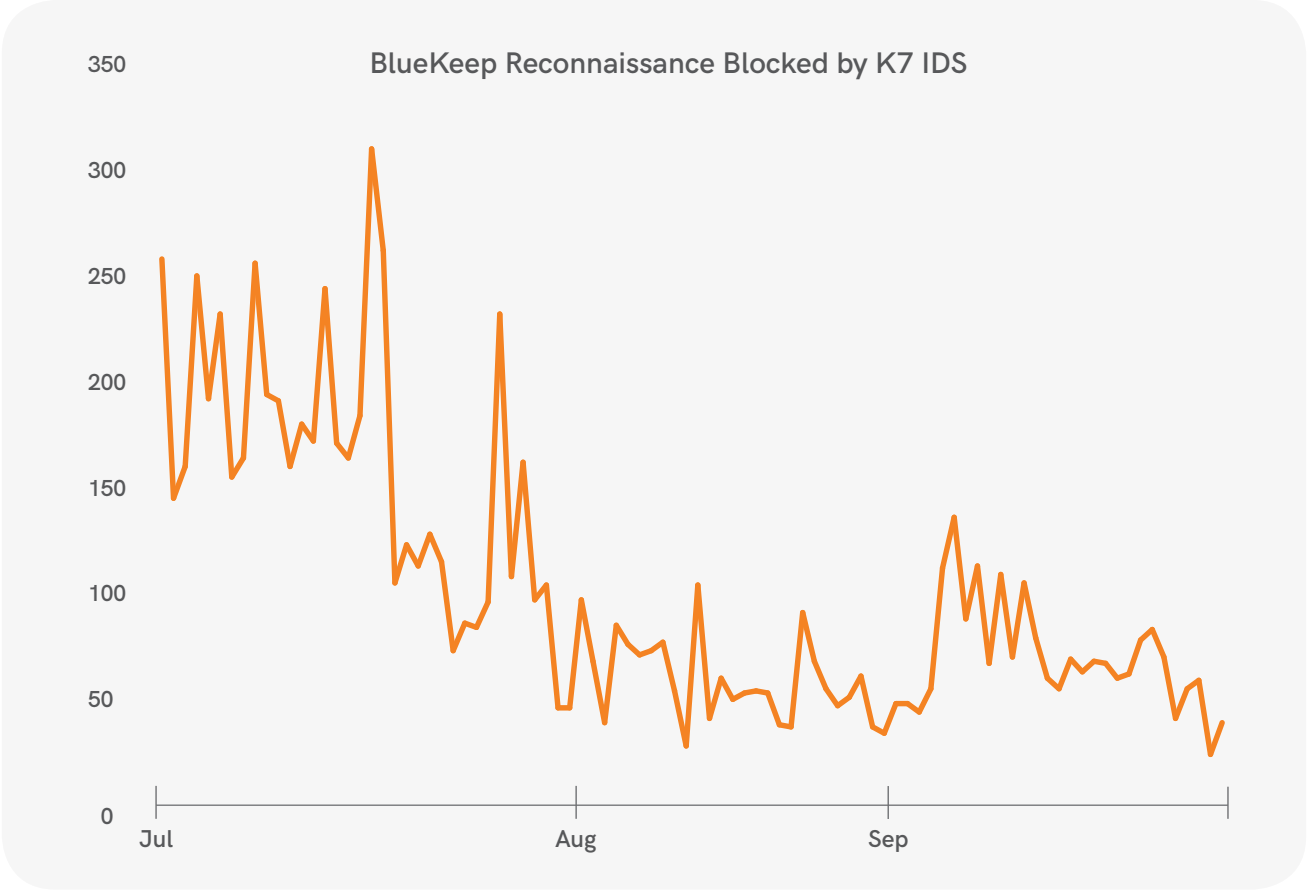
This quarter too had its fair share of vulnerabilities impacting both Windows and iOS systems. Let's dive deeper into a few of these.

Exploitation of Loopholes

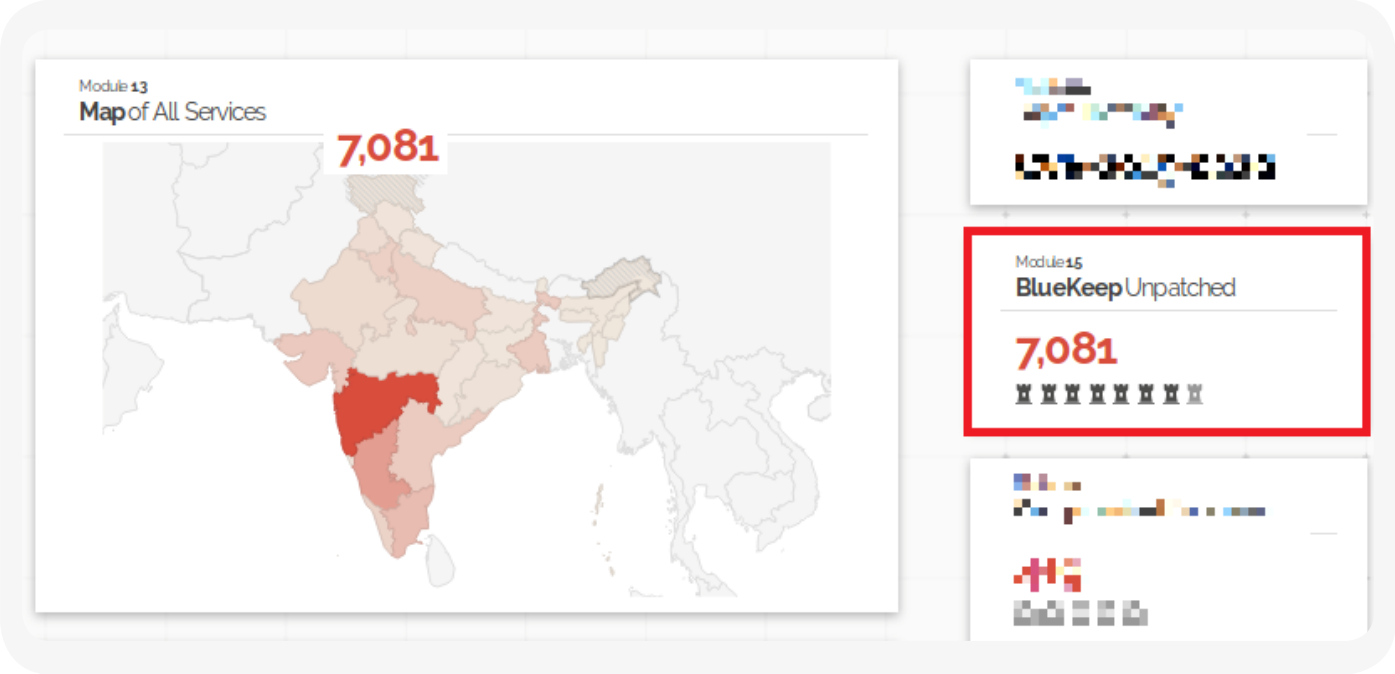
The iOS vulnerabilities CVE-2019-8624, CVE-2019-8646, CVE-2019-8647, CVE-2019-8660, and CVE-2019-8662, found in the iMessage service that exists in iPhone and Siri components. The scariest part about these vulnerabilities is that none of them requires any interaction from the target's end to invoke remote code execution, making each extremely advantageous for the adversaries. To exploit these vulnerabilities, the attacker merely needs to send a specially-crafted message to the victim's device. Upon exploitation, the vulnerabilities CVE-2019-8624 and CVE-2019-8646 could help to provide remote access to victims' files without user interaction. Apple has patched all five of them, alongside a few other severe vulnerabilities in Apple's iMessage and the Safari browser.

Another exploit that is doing the rounds is a year-old privilege escalation vulnerability in Windows (CVE-2018-8453) which is mostly being exploited by the evasive Sodinokibi ransomware, earlier used by APT groups like FruityArmor.

In July 2019, K7 Labs observed a spike in the frequency of BlueKeep (a Remote Desktop Vulnerability(RDP) which allows for remote code execution in Windows OS) reconnaissance activities that were blocked by our Intrusion Detection System (IDS), which started to decline significantly in the latter half as shown in the figure below. The peaks were noticed soon after Microsoft issued a critical fix addressing CVE-2019-0708 (BlueKeep).



In India alone 7081 devices are publicly-exposed to the BlueKeep vulnerability. There would be a surge in the total number of vulnerable devices, if we were to consider the unpatched devices that exist on the internal networks. The figure below shows the list of vulnerable devices in India, courtesy of Shodan.



The infection rate would likely skyrocket if any malware successfully exploits this vulnerability that exists in these publicly-exposed devices.

DejaBlue, a BlueKeep-like RDP exploit, is also on the prowl! The wormable vulnerability "DejaBlue" (CVE-2019-1181 and CVE-2019-1182) is a remote code execution (RCE) on RDP which does not require an attacker to authenticate to the system and can wreak havoc on all supported versions of Windows client and server systems except Windows Server 2008. With the availability of this vulnerability, Remote Desktop Protocol Service has become vulnerable again. Along with the BlueKeep RDP vulnerability, which is effectively used to contaminate Windows XP and Windows 2003 systems, DejaBlue makes the entire range of Windows products susceptible.

Like many new vulnerabilities, DejaBlue too requires no user interaction. An adversary can send a request to open the RDP port and gain control of the system without requiring further authentication details. An exploit for BlueKeep has been made public very recently, which is a forewarning about the upcoming threats. Users are advised to update their OS, applying patches for these vulnerabilities ASAP, and enable network-level authentication to steer clear of such critical RDP vulnerabilities.

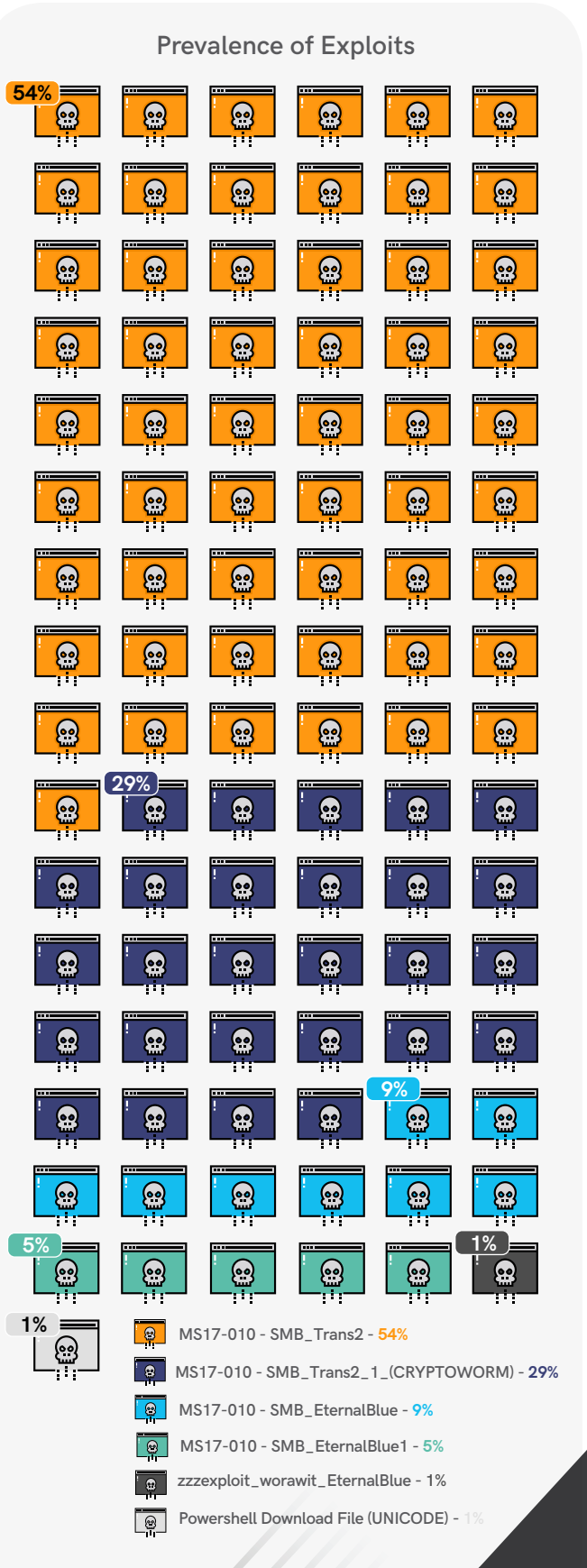
Unpatched Virtual Private Networks (VPNs) Under Attack!!

Hackers are increasingly attempting to attack SSL VPNs manufactured by both Fortinet and Pulse Secure because of an RCE vulnerability which does not require an attacker to authenticate to the system. CVE-2018-13382, which was found in Fortinet's VPNs, does not use the usual validation procedures to access a system, and this can be easily exploited by manipulating specific input values on the login page, by which any user's password can be easily modified. Similarly, CVE-2019-11510 and CVE-2019-11539 were found in Pulse Secure's VPN. CVE-2019-11510 is a file-reading vulnerability allowing sensitive information disclosure, while CVE-2019-11539 allows an attacker to execute arbitrary commands on the web server compromising the confidentiality and integrity of data; attackers can gain access inside the private VPN network if it gets exploited. We have been observing extensive reconnaissance and exploitation of these vulnerabilities.

The Windows SMB (Server Message Block) vulnerability MS17-010 has been doing the rounds since March 2017 and has plagued an innumerable number of networks since then. In October 2017, Microsoft rolled out the necessary patch, but cybercriminals are continuing to hunt down potential victims who are yet to patch this vulnerability. In Q2 these attacks were detected and blocked by K7's Intrusion Detection System (IDS) which has been installed in millions of devices around the world.

EternalBlue, the most prevalent vulnerability from the SMB Exploit variety, is still considered the favourite of cybercriminals. Alongside, we intercepted several other SMB varieties which are supposedly used by different types of ransomware.

Interestingly, this exploit only affects machines running outdated Microsoft operating system versions, hinting that a plethora of users are yet to upgrade to Windows 10.



Windows Malware Type Breakdown

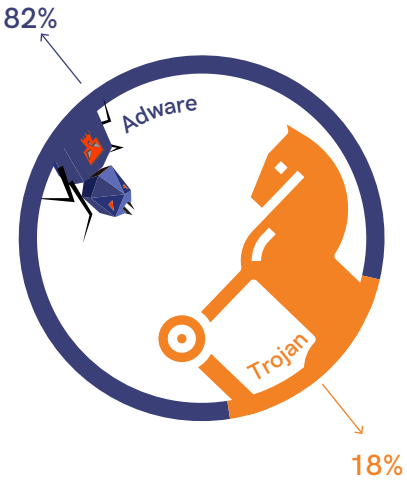
Following the past trends, Wrm.Gamarue.LNK (21%), associated with worm-like spreading via USB storage devices, remains the top malware threat for Windows users, followed by Adw.Dealply (15%). The malware that topped the list in Q1 2019-20 are still widely prevalent.

Both enterprise customers and end-users also observed old-school malware during this period. Besides these top two malware, there were a large variety of Trojans, Potentially Unwanted Programs, adware, deceptors, and a bunch of coinminers also surfaced during this period.

Mitigation Tips

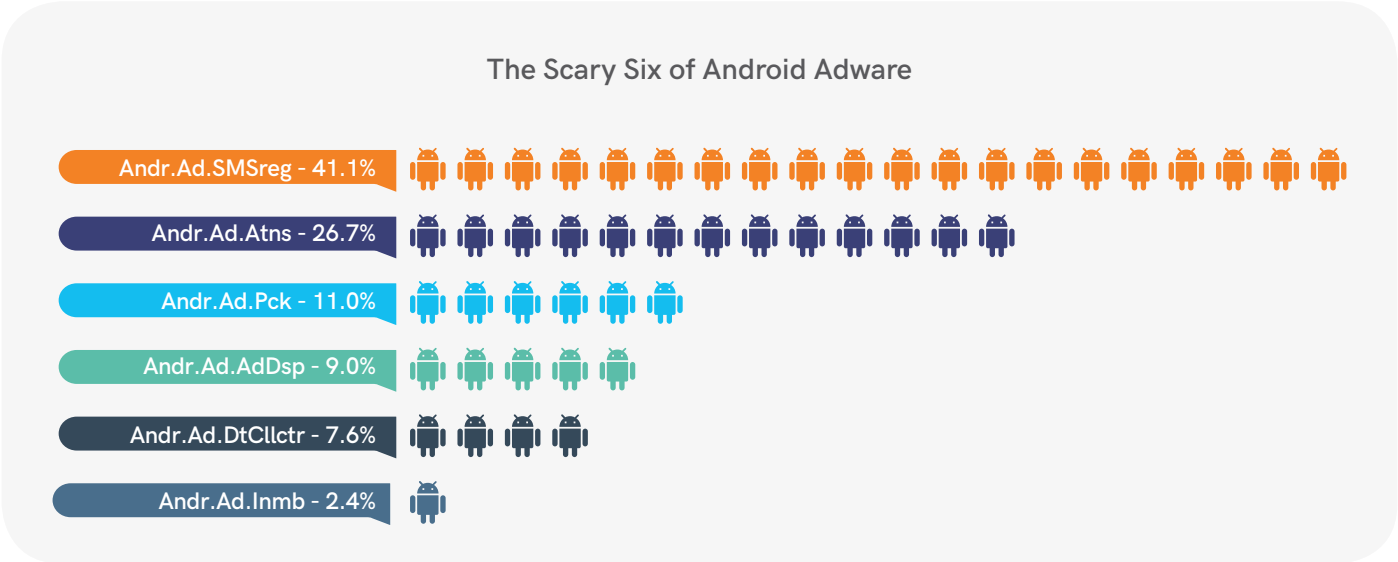
- Users are required to keep their OS up-to-date and patched for the latest vulnerabilities.
- Change default RDP ports.
- Use strong password policy.
- Use a reputable Anti-Virus product, like K7 Total Security, and keep it up-to-date.

THE MOBILE DEVICE STORY

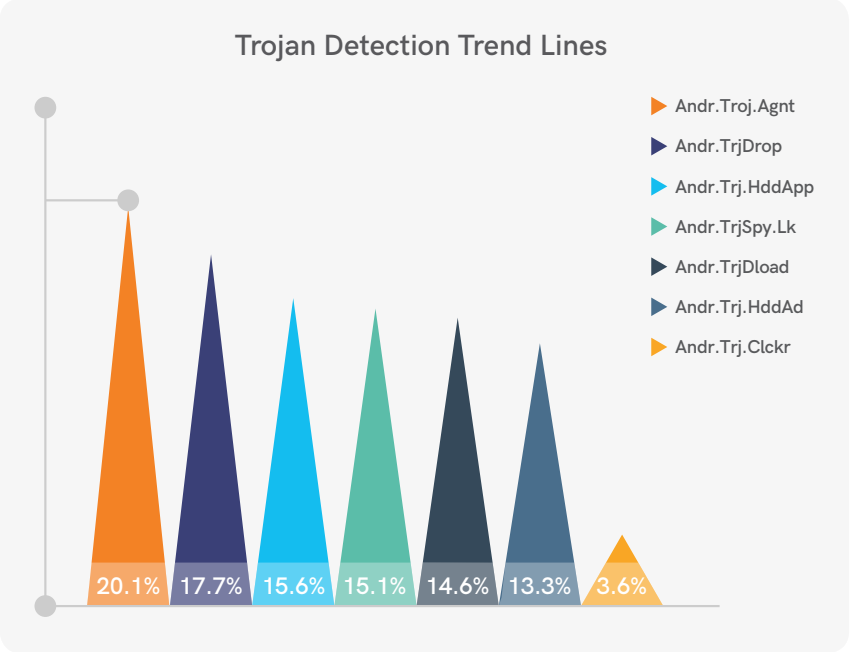


The Android threat landscape by the 2nd quarter of 2019-20 has highlighted all sorts of infamous threats, from spyware to adware, fake-apps, ransomware and downloaders pretending to be authentic apps to befool and victimize users. While many of the notorious Trojans and adware have strengthened their presence, we have also found a few new Android malware families in this quarter.

Adware continued to dominate in Q2 2019-20. It looks like this type of cyber threats has remained a growing "sweet spot" for cybercriminals. Though they sound entirely innocent by their names, some adware root the device unbeknownst to the user and spy on them by staying in stealth mode. In the ever-evolving market of cybercrime, some adware target the user with tailor-made ads after collecting the victim's online behaviour data.



Android.Adware.SMSreg (Andr.Ad.SMSreg) had flexed its muscles in the Android arena with a presence of 41.1%, an increase of 24.4% in comparison to the last quarter. It was followed by another adware called Android.Adware.Autoins (Andr.Ad.Atns) with a presence of 26.74%, which was a rise of 11% in comparison to the previous quarter. It was then followed by Android.Adware.Packed (Andr.Ad.Pck) and Android.Adware.AdDisplay (Andr.Ad.AdDsp) adware families, with a presence of 11% and 9% respectively.



Though both Android.Trojan.Agent (Andr.Trj.Agnt) and Android.Trojan.Dropper (Andr.TrjDrop) have recorded a drop of 19.85% and 19.29% respectively, they still managed to hold the top spot in the Android Trojan malware category. This quarter, Android.Trojan.HiddenApp (Andr.Trj.HddApp) and Android.Trojan.Downloader (Andr.TrjDload), have recorded more visibility with an increase of 12.53% and 1.18%, respectively. Ranked sixth in our telemetry with 13.28% out of the total malware reported, Android.Trojan.Hiddad (Andr.Trj.HddAd) is still a cause for serious concern for Android consumers.

Case Study 1: Agent Smith and the Android Matrix

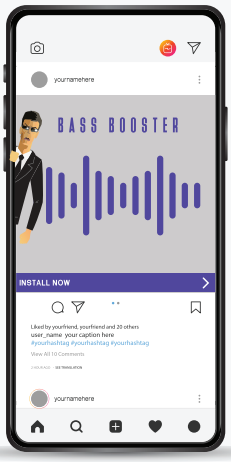
The name of the notorious Android malware "Agent Smith" is believed to be inspired by the antagonist from the famous movie "The Matrix". This malware has created havoc all over the world, especially in Asian countries, and particularly in India. Out of its 25 million victims around the world, 15 million targets are Indian.

The malware coder was not only inspired by the name but was also equally obsessed with the behaviour and used an identical strategy to victimize the target devices. Agent Smith targeted most of the Android devices running on Android version 7.0 or below.

Agent Smith had replaced popular apps like WhatsApp, Flipkart, Jio Play, JioChat, Opera and Hotstar, to name a few, with fake ones on the users' device without their interaction.

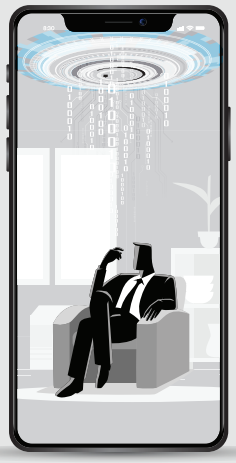
Agent Smith's malware infection happens in four main stages. The detailed pictorial representation of how the infection chain works is described below.

DOWNLOAD



The attacker lures the user to install a dropper application that pretends to be a free game or entertainment application

CAMOUFLAGE



The dropper decrypts and installs the malicious files

THE CURATED LIST

Malware downloads list of the "Prey apps" from C2 server, and crosschecks if the compromised device has any of the apps from the downloaded list

CLONE FACTORY

Injects each identified target app with malicious module by exploiting the Janus vulnerability

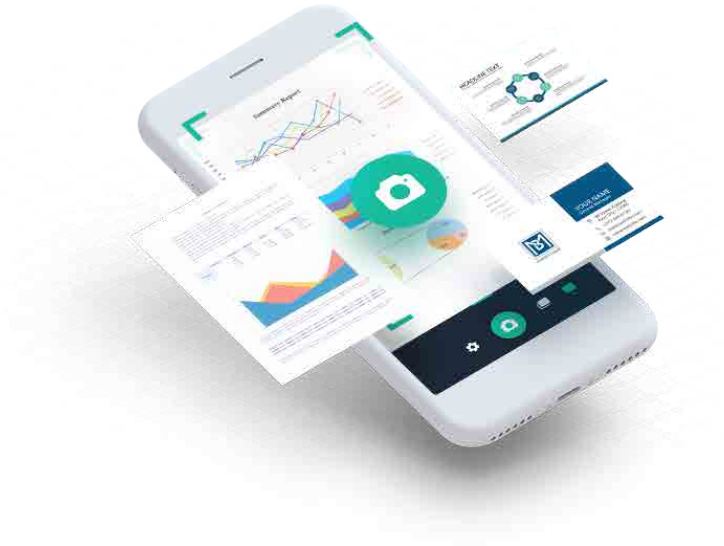
About the Janus vulnerability (CVE-2017-13156) - upon exploitation this allows attackers to modify the code in applications without affecting their cryptographic verification signatures. Google fixed this vulnerability in Android Oreo.

Case Study 2: CamScanner - Unsuspecting App Turns Malicious

CamScanner was considered as the world's leading mobile scanning app, once upon a time. With over 100 million downloads via Google Play Store, this app lets your phone act as a fully-fledged portable scanner. The app can scan documents and convert them into a PDF/JPEG file. This app was a legitimate one until version 5.11.7.20190708 was unleashed on the Play Store.

This version of the app comes with an advertising library containing a malicious dropper. This module is a Trojan-Dropper which extracts and executes another malicious module. The dropped malware is a Trojan downloader which would download more malicious modules.

These malicious modules display intrusive ads and sign users up for paid subscriptions without their knowledge.



Tips to Stay Safe

- Secure yourself with a powerful mobile security app such as K7 Mobile Security.
- Ensure your OS and all other applications are updated with the latest security patches.
- Scan all your applications with a reputable Anti-Virus product, even if it is downloaded from the official App Store.

Nowadays, it is not surprising to see that no platforms are safe from increasingly sophisticated and targeted cyberattacks. Cybercriminals are actively looking for unexplored and unpatched exploits, weaponizing them to launch multi-staged sophisticated attacks. Besides, they are gradually fine-tuning social engineering methods to hoodwink victims more quickly.

Planned Coinbase Heist Foiled

A sophisticated multi-staged cyberattack on the cryptocurrency exchange Coinbase, hit the headlines recently.

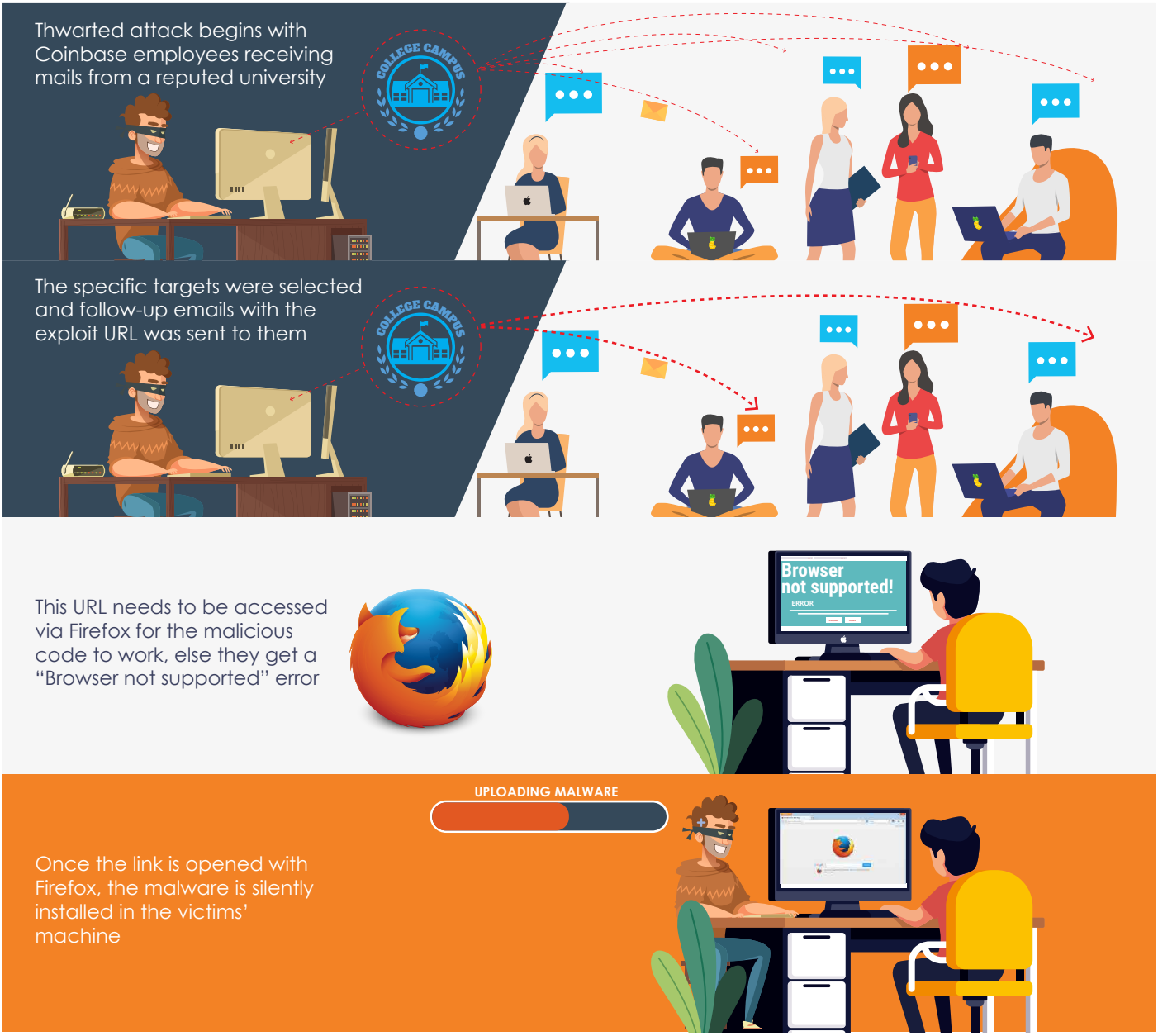
The attempt begins with attackers using spoofed email IDs of a reputed university to target Coinbase employees.

It all began with a convincing email to 200 Coinbase employees. The senders of the email even had matching fake social networking profiles for increased believability. The email looked legitimate and passed all the existing security checks. Subsequently, the hackers sent a series of emails in the following weeks to narrow down on a few high-value targets. These high-value targets received an email with an exploit URL which needs to be accessed via Firefox, else the targets receive an error message saying "Browser not supported" and are forced to install the latest version of Firefox. Once they open the link in Firefox, the malware would be installed since the landing page would have an exploit that installs the malware.

The attempt was foiled by Coinbase by blacklisting all the samples that they had with them at that time, revoking all credentials on the affected machines and locking all accounts of compromised users. They also shared the exploit code with the Mozilla security team which patched both vulnerabilities in the same week that the code was shared. They also reached out to the affected university and assisted them in securing their infrastructure, and collected more information about the attackers' behaviour, thereby degrading their ability in continuing with their campaign.

Following is a visual illustrating the strategies of the involved adversaries.

EduSmoke Coinbase Attack

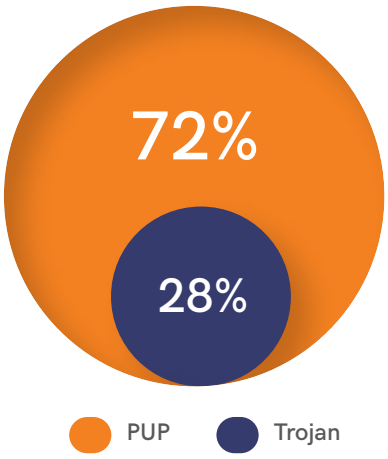


K7 Labs tracks the threat actors responsible for this attack under the name "EduSmoke". The naming convention has been so derived because the group's spearphishing emails always claim to come from an educational institution (Edu) and from the name of an artefact in its malicious applications (Smoke).

Prevalent PUPs

The macOS platform was also riddled by numerous versions of Potentially Unwanted Programs (PUP) and Trojans. But surprisingly, unlike the previous quarter, the number of PUPs observed was greater than that of traditional Trojans. It hints that adware and unwanted applications which generate consistent revenue for the developers are on the rise.

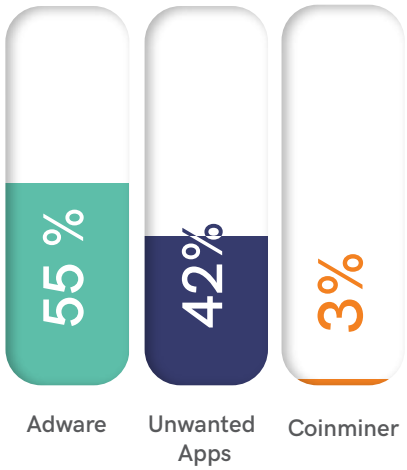
Most Prevalent Malware Types



These applications usually infect the user's device with the mission of flashing advertisements which may entice user's to click on the same so that the perpetrators can make money. These categories of apps are comparatively less harmful than the Trojans in their intent, but PUPs, like different sorts of activity loggers, come with a bucket load of suspicious activities. Alongside activity loggers, coinminers, adware, unwanted applications are also on the list.

During this quarter, K7 Labs has blocked numerous threats, categorised as PUP, out of which 55.3% are classified as different types of adware. The second most surfaced threat under the PUP category are different types of unwanted applications, with a proportion of 41.5% out of the total number of PUPs surfaced. Mackeeper remained the most visible PUP malware at 36%. Other categories of PUP detected were having a small percentage.

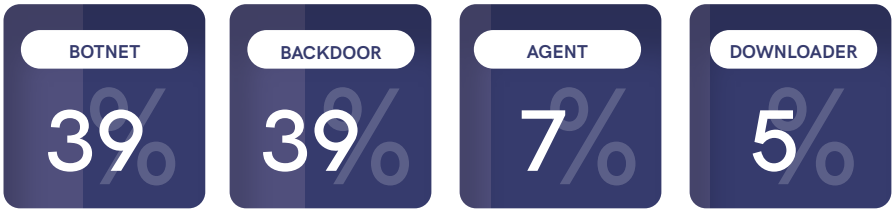
Most Common PUP Variant Detection



The most interesting observation by K7 Labs in this quarter is how cybercriminals are effectively using old-school malware by blending them with new strategies. For example, MacKontrol and Flashback have taken top spot for two consecutive quarters.

Being categorised as backdoor malware, MacKontrol has recorded a visibility of 38.7%, 11.1% less compared to the last quarter. Used mostly for targeted attacks, MacKontrol abuses the ancient MS-Word vulnerability CVE-2009-0563.

Split of Top 4 macOS Trojans



The other high-visibility Trojan, FlashBack, a botnet, is seemingly in decline now. However, we have received samples pertaining to the same in Q2 2019-20, and with a visibility of 39.4%, it topped the list under the Trojan malware category.

The most-talked-about malware type, "Ransomware", is on the wane (0.38%). Whatever the reason may be, the mystery behind its surprising disappearance might be resolved in the coming quarters.

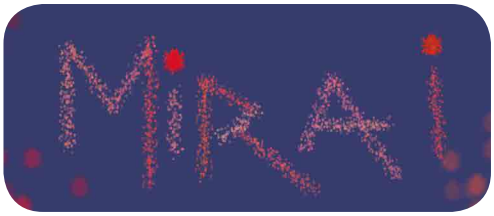
Safety Guidelines

- Ensure your OS and installed apps are up-to-date with the latest security patches.
- Avoid clicking on any links from unknown sources.
- Install a reputable Anti-Virus software, like K7 Antivirus for Mac, ensure it is kept up-to-date, and scan your device regularly so as to protect yourself from the latest threats.

DANGER IN THE INTERNET OF THINGS

At the beginning of this quarter, a Mirai-like botnet was seen in the wild, abusing unpatched vulnerabilities in RealTek and GPON routers, as the source code for the botnet was made publicly available. Digging down, we found they were abusing recently-discovered vulnerabilities which could allow attackers to bypass the devices' authentication mechanism and also allow attackers to access someone else's device and make changes, regardless of where the device is geographically located. These vulnerabilities were more than a year old and affected only unpatched IoT devices.

Echobot, a newer variant of the Mirai IoT botnet, had been spotted using over 50 exploits to take advantage of RCE vulnerabilities that exist in various IoT devices. Each of these exploits abuse well-known vulnerabilities targeting unpatched devices such as routers, cameras, Network-attached Storage systems (NAS), DVRs, servers, smart home hubs, and so on. The malware propagates by attacking these unpatched IoT devices by picking the right exploit from its arsenal. The code has been made publicly-available, which makes it easy for anyone to pick up this malicious code, modify it accordingly and spread it further in the wild.



Telestar Digital GmbH (IoT) radio devices were affected by the telnet backdoor in the last month of Q2 2019, which created a catastrophe. Millions of these devices became susceptible to RCE vulnerability CVE-2019-13473. This vulnerability allows attackers to infect the device with malware (ransomware/ rootkits/destructive scripts), add the device to a botnet or send their audio streams to the affected devices.

Mitigation Techniques

- Ensure you patch all your IoT devices for the latest vulnerabilities.
- Scan your network regularly and identify all your IoT devices. It makes it slightly easier to identify a security breach.
- Do not use default configurations for any of your devices. Ensure you maintain a good password policy and use a unique strong password for each connected device and any admin consoles for them.
- Disable Universal Plug and Play.

KEY TAKEAWAYS

	Enterprise	Consumer
1	Ensure that the OS and all services running on the servers are up-to-date and patched for the latest vulnerabilities. Also maintain a continuous backup of critical data	Secure yourself with a reputed security product such as K7 Total Security for Windows, K7 Antivirus for Mac and K7 Mobile Security (Android and iOS) and ensure it is kept up-to-date
2	Admins are recommended to check and immediately act upon any threat notifications to avoid any system compromises	Never click on attachments or links in any emails coming from unacquainted sources, and refrain from forwarding them
3	Safeguard multiple areas of the network to protect your organization's assets against cyberattacks	Scan all your applications even if they are downloaded from the official App Store

CONFIDENCE IN AN INSECURE WORLD

K7 SECURITY

www.k7computing.com

Dec 2019