Cyber Threat Monitor Report

2020-21

K7 SECURITY

Contents

Contents

Cybersecuring Our Digital Ecosystem

The year 2020 would be long remembered for a list of nightmarish reasons. Besides the Covid-19 pandemic, the ever-increasing business of disinformation, the rise of large cybercriminal gangs, and the crossover and blurring boundaries between the state-sponsored attackers and organised cybercriminals have created what seems like a digital catastrophe which would continue to compromise our personal and enterprise digital safety for years to come.

The privacy quagmire around us is continuously transforming the world into a tumultuous space. Modern and advanced technologies like IoT and IIoT (Industrial Internet of Things) are injecting more vulnerabilities alongside easing our lives to some extent. Popular smart gadgets are being used as a platform to launch sophisticated attacks on the enterprises and the end-users.

This widespread technology consumption in our everyday life makes us vulnerable to malicious attacks. Malware actors are continuously evolving their tactics, techniques and procedures (TTPs) to pave the way for more sophisticated attacks. For instance, malware actors nowadays bank on more nuanced social engineering techniques to invade into the target devices.

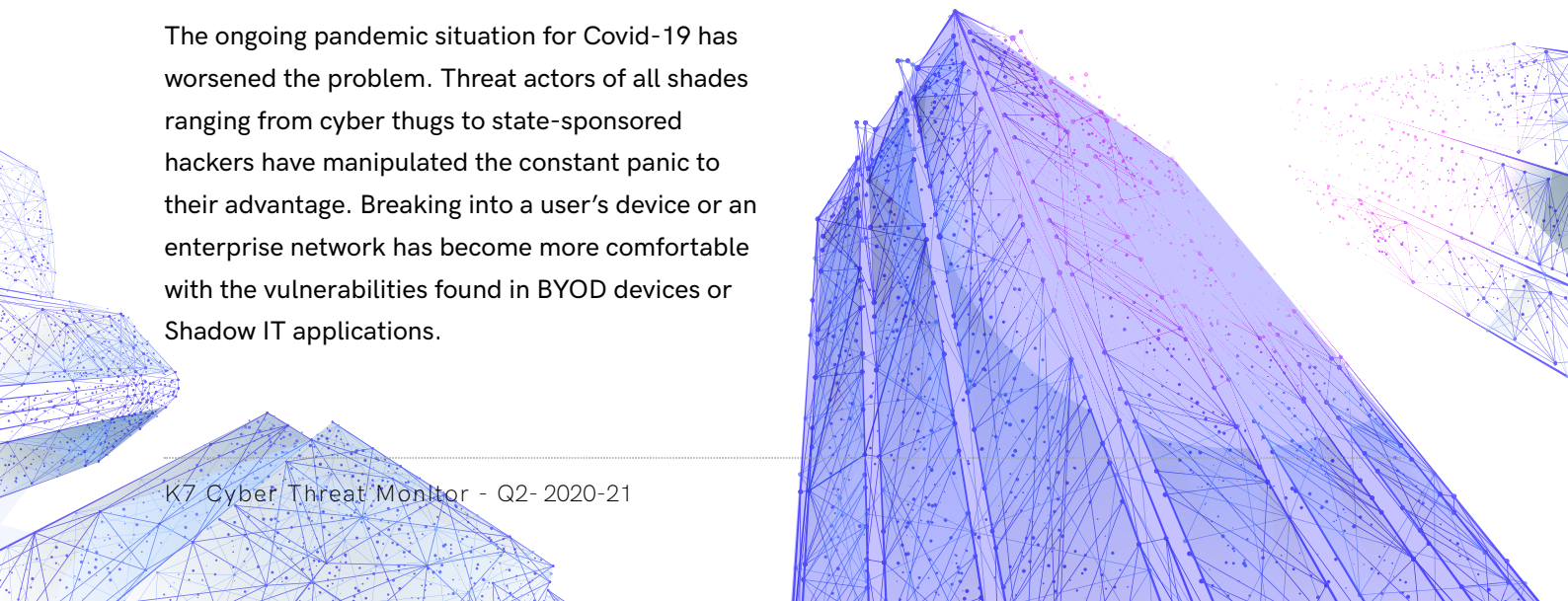
The ongoing pandemic situation for Covid-19 has worsened the problem. Threat actors of all shades ranging from cyber thugs to state-sponsored hackers have manipulated the constant panic to their advantage. Breaking into a user's device or an enterprise network has become more comfortable with the vulnerabilities found in BYOD devices or Shadow IT applications.

The increasing number of Trojans across the smartphone operating systems has become another hair-raising concern for individuals and enterprises. Threat actors are developing new deception techniques every day to obfuscate malware strains evading regular protection services like Google Play Protect. In the connected world, smart devices play an essential role in security. Unprotected smart devices are a possible entry point for threats affecting the entire enterprise.

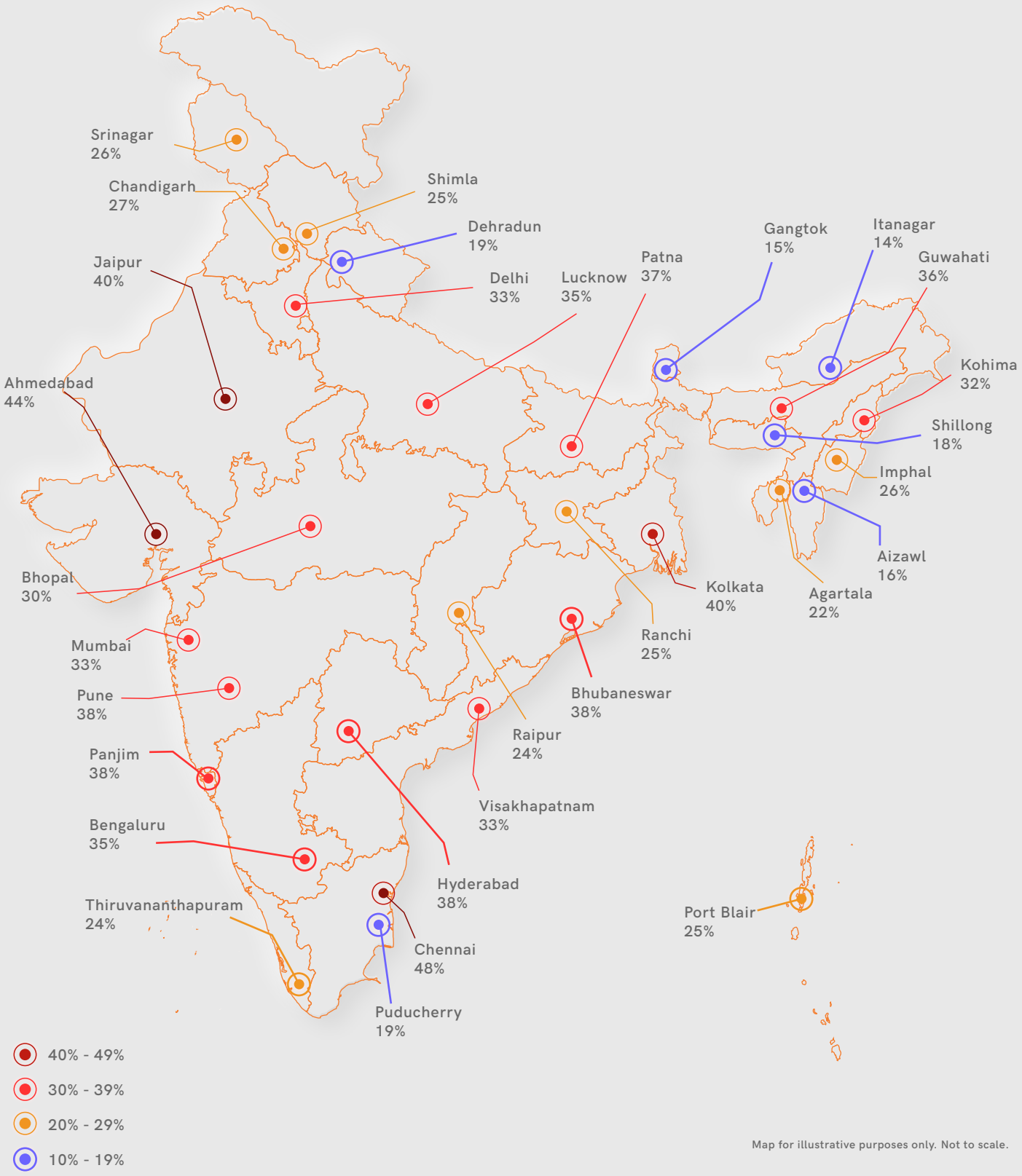
The latest K7 Cyber Threat Monitor Report Q2_2020-21 aims to present an account of all the aforementioned security-related concerns to help you understand the current threat landscape. The report also seeks to offer a heads up about all the various vulnerabilities, malware strains and the perturbing threat landscape in the country.

Besides, the report also offers a series of mitigation techniques grouped by platform and operating system to allow you to choose appropriate safeguarding techniques without a fuss.

We appreciate you sharing this report among your colleagues and friends to make them more aware of the prevalent cyber threats and to make the digital world a safer place!



CYBER THREAT MONITOR - INDIA



Map for illustrative purposes only. Not to scale.

BACK TO CONTENTS

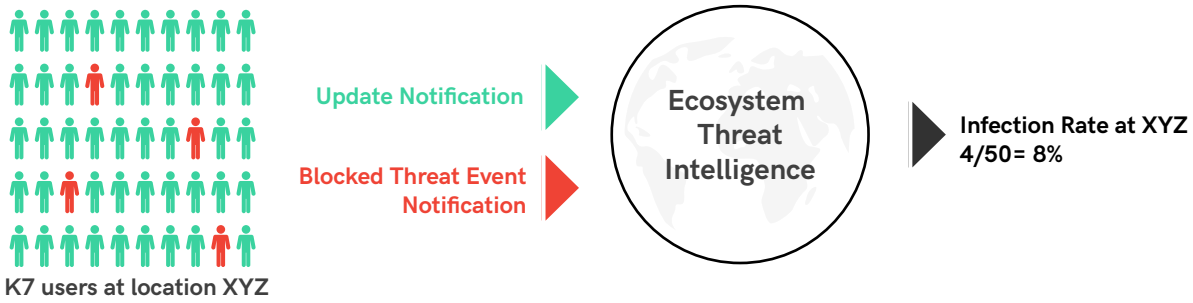
Regional Infection Profile

The increasing dependence on digitisation, both in our personal and professional spaces, has eased our life in many aspects. This transformation has helped enterprises and end-users enormously by enhancing communication, production, strategy-making and various other benefits. But as Mark Twain once said, every moon has a darker side; the massive surge of digitisation also exposes a vulnerable aspect which gets immensely exploited by threat actors to carry out their plans.

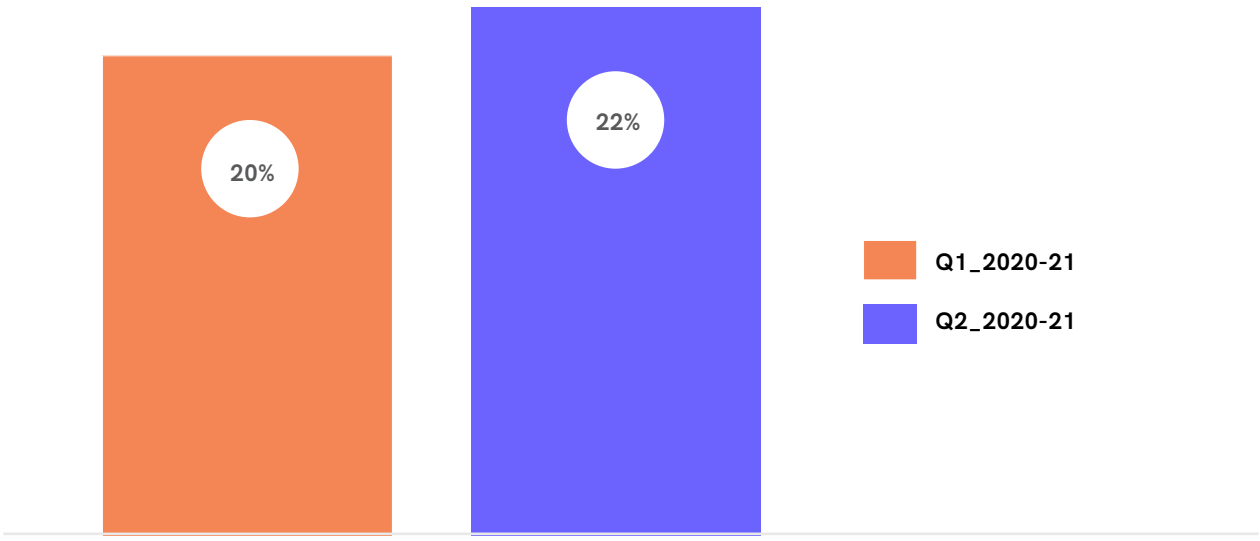
This section summarises findings gathered by K7 Ecosystem Threat Intelligence (K7ETI) and from the thwarted attacks by our malware prevention and detection engine. Let us shed some light onto the infection rates of Tier -1 and Tier-2 cities in the country.

The concept of an "Infection Rate" (IR) of an area is as illustrated below

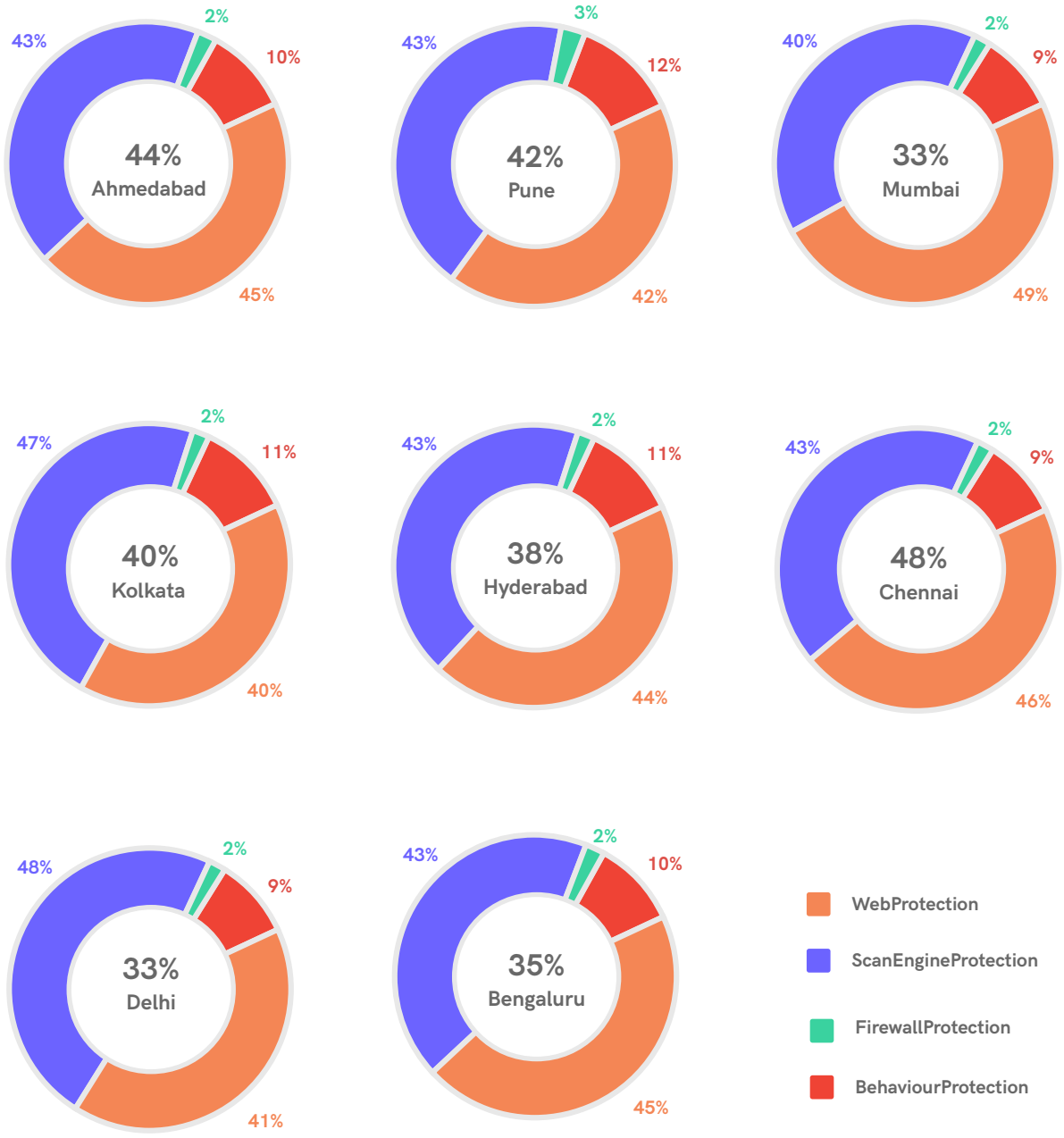
Infection Rate" (IR) of an area



The overall pan-India IR is given below.

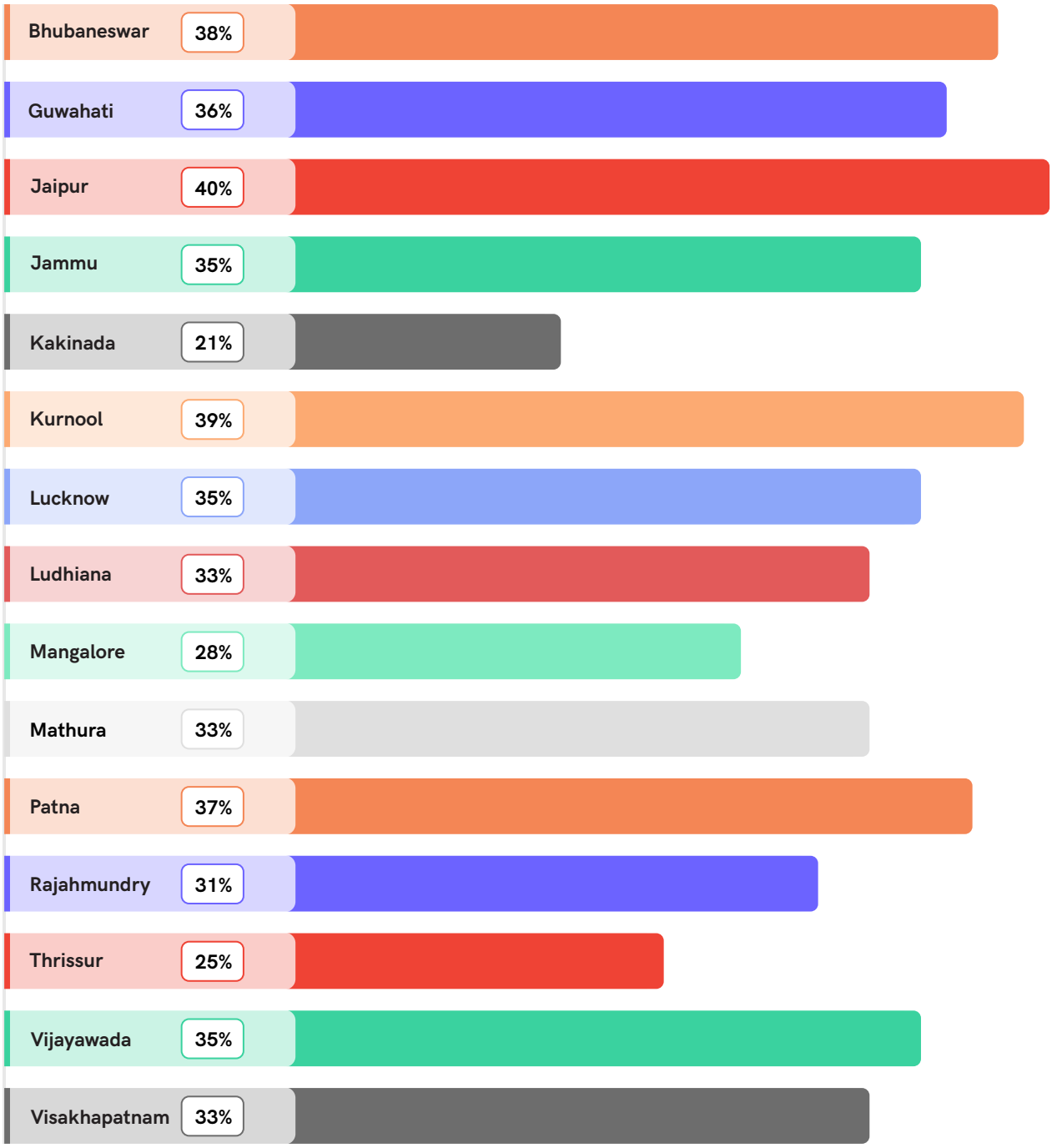


The Metros and Tier - 1 Cities - Infection Rate



The increase in IR compared to the previous quarter is an indication that the threat actors have increased their focus on the Metros and Tier-1 cities. Work-from-Home users are possibly facing the brunt of the attacks during this pandemic time.

Top 15 Infection Rates in Tier-2 Cities



Like the previous quarter, all the Tier-2 cities had an IR above the national average, as per K7ETI.

BACK TO CONTENTS

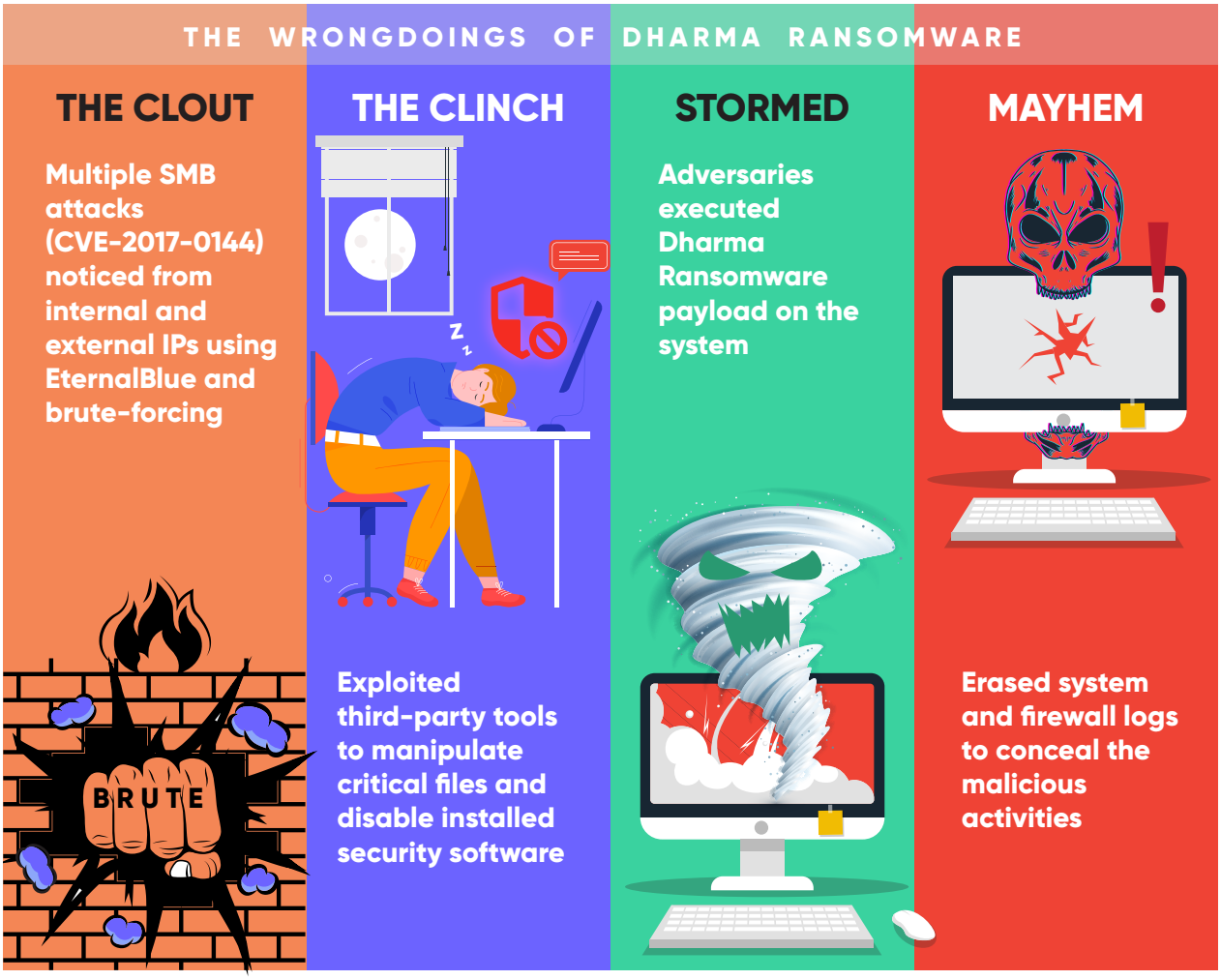
Enterprise Insecurity

The enterprise threat landscape is becoming increasingly complex. As enterprises embrace new security approaches to safeguard themselves from the prevalent attacks, the threat actors are introducing new tactics, techniques, and procedures (TTPs) to bypass or exploit the newly introduced technologies on the potential victim's network.

Alongside introducing new attack methods, the perpetrators are also banking on old but lethal malware and vulnerabilities to outdo all the defence mechanisms and keep their flags flying high. The SMBv1 series of vulnerabilities has been there for half a decade and is still alive and kicking for several reasons.

Infamous ransomware such as CrySIS (aka Dharma), Wannacry, and Petya majorly exploit at least one grand old vulnerability from the set. During the period, one of our valued enterprise customers encountered one such attack on their server machine.

The post-exploit observations are depicted below

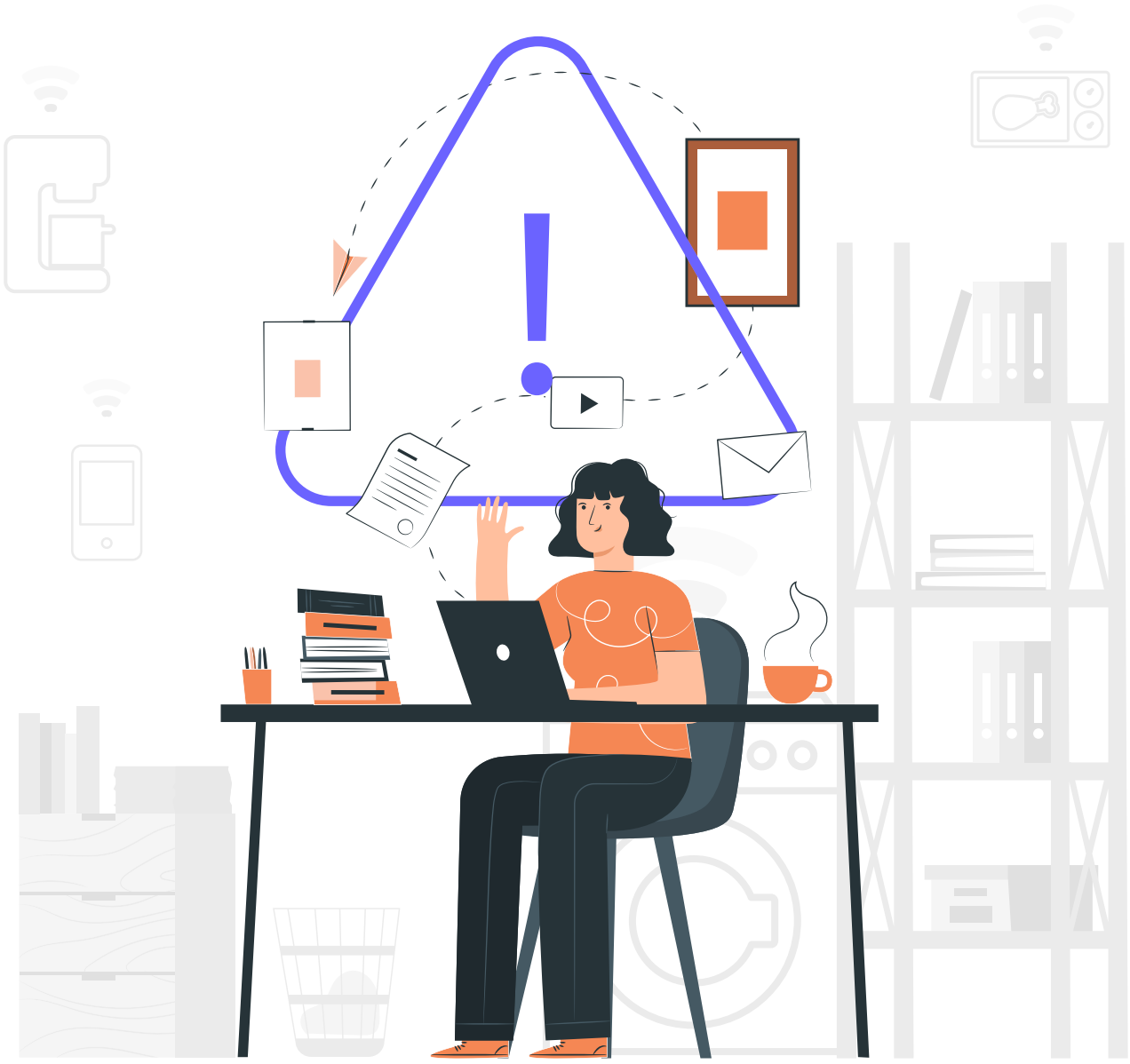


Our active K7 products have detection for this variant at multiple security layers, thereby protecting our customers from this ransomware attack.

Safety Recommendations

- Enforce strong password policy
- Ensure all your devices are patched for the latest vulnerabilities
- ALL systems in the network should have a reputable enterprise security suite, such as K7 Endpoint Security, installed and kept updated and systems should be regularly scanned
- Ensure your organization has a proper alert mechanism for any potential security breaches. If not, it is advisable to check your logs regularly

Vulnerabilities Galore



The sudden WFH scenario has sown the seed for even more vulnerabilities due to the use of several personal devices, IoT devices and Shadow IT applications. The unpatched vulnerabilities that exist in these new devices and applications have helped the perpetrators further to pounce on their targeted victims.

To understand this persistent precariousness, here is a snapshot of the most prevalent vulnerabilities we found over the quarter.

SIGRed Vulnerability

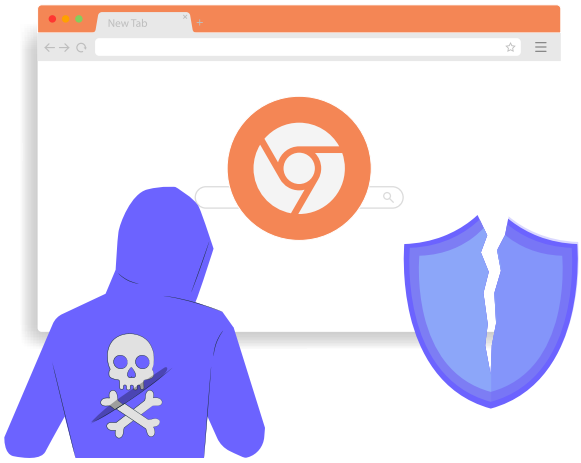
SIGRed aka **CVE-2020-1350** is a wormable remote code execution vulnerability that exists in Windows Domain Name System servers which can be triggered by specially crafted DNS queries. On successful exploitation, a malicious user can run arbitrary code on the victim's machine. It affects Windows Server versions from 2003-2019.

Microsoft rolled out a patch for the SIGRed vulnerability in July 2020 alongside 122 other vulnerabilities as part of its monthly patch Tuesday program. However, there are numerous unpatched Windows DNS servers up and running in the country without installing the patch yet.

The BootHole Vulnerability

CVE-2020-10713 is a buffer overflow vulnerability affecting the GRUB2 bootloader and impacting any system using Secure Boot. This vulnerability allows malicious users to get around Secure Boot protections and to run arbitrary code during the boot process. It affects any device supporting a GRUB2 bootloader which will include all Linux based systems and all Windows based systems that are using Secure Boot.

This major vulnerability has affected most of the devices on a network such as desktops, laptops, servers, workstations, and network appliances across industries. Any successful attack abusing the BootHole vulnerability could gain complete control over the device, including the operating system it runs on, applications, and data.



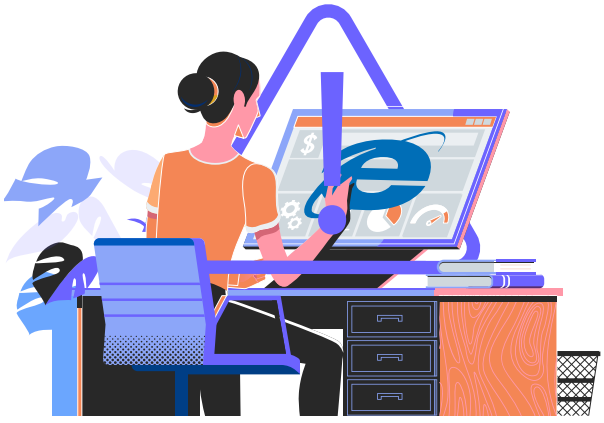
Code Execution Vulnerability in Chrome

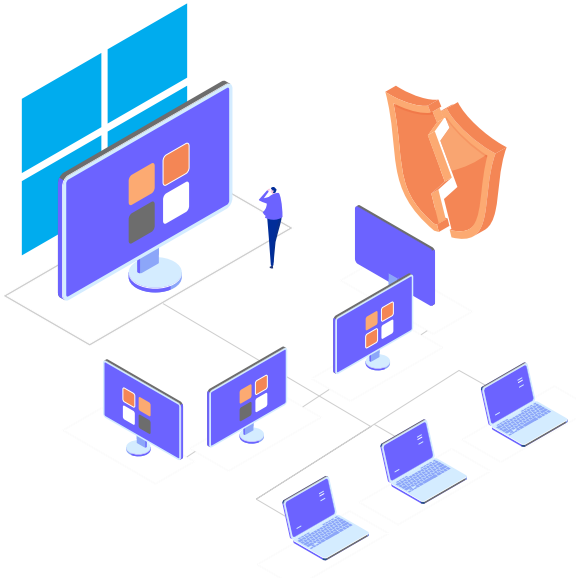
During this period, a Use-After-Free vulnerability was discovered on Google's popular internet browser Chrome versions 81.0.4044.138 (Stable), 84.0.4136.5 (Dev) and 84.0.4143.7 (Canary).

The vulnerability, CVE-2020-6492, could trigger arbitrary code execution if successfully exploited. The vulnerability is present in WebGL (Web Graphics Library), which is a JavaScript API for rendering web graphics.

IE Vulnerable to Memory Corruption

A zero-day vulnerability spotted on Microsoft Internet Explorer has created quite a buzz. CVE-2020-1380 was found to be a Use-After-Free vulnerability, affecting Internet Explorer and is being actively exploited in the wild. The vulnerability exists in IE's JavaScript Just-in-Time (JIT) engine. It affects all IE versions above 9.





Windows Domain Controller Attacked

CVE-2020-1472 (aka Zerologon), a critical vulnerability, was seen affecting Windows Domain Controllers this quarter. This is an elevation of privilege vulnerability which allows any unauthenticated attacker with network access to a Domain Controller to gain administrator privileges to the same. It exploits a flaw in Netlogon Remote Protocol which is used by Domain Controllers for various tasks such as user and machine authentication.

All Windows server versions upto Server 2019 are affected by this vulnerability.

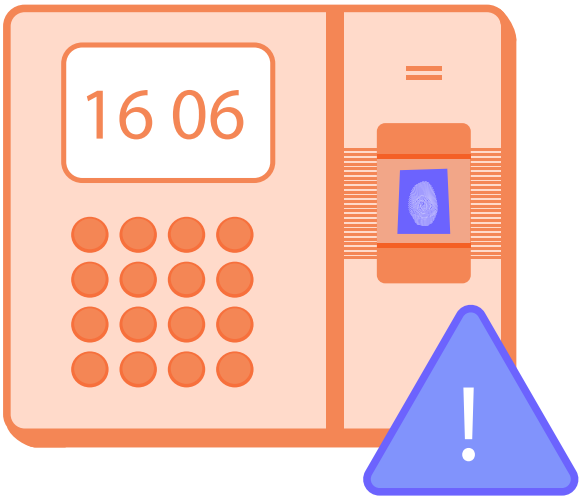
BACK TO CONTENTS

Danger In The Internet Of Things

The rampant use of connected devices in enterprises, as well as in our daily lives, has transformed many things. While smart devices have definitely helped us to ease our jobs, most of the IoT devices have been built with scant regard for security, making it easy for the threat actors to exploit these devices. IoT devices with absent or inadequate in-built security and connected to enterprise networks offer the adversaries an open door into an organization's entire network to wreak havoc.

Let us now see a few of the prominent flaws.

Critical Flaws in GeoVision's Fingerprint Scanner



CVE-2020-3928, a vulnerability that is a result of password hardcoding of a root account in GeoVision Door Access Control devices, affecting GV-AS210 version prior to 2.21, GV-AS410 version prior to 2.21, GV-AS810 version prior to 2.21, GV-GF192x version prior to 1.10, and GV-AS1010 version prior to 1.32 was found in its fingerprint scanner.

A buffer overflow vulnerability in GeoVision's fingerprint readers, affecting GV-AS210 version prior to 2.21, GV-AS410 version prior to 2.21, GV-AS810 version prior to 2.21, GV-GF192x version prior to 1.10, and GV-AS1010 version prior to 1.32, allows remote code execution on successful exploitation.

Critical Vulnerability in Cisco vWAAS

CVE-2020-3446, a critical vulnerability in Cisco Virtual Wide Area Application Services (vWAAS) with Cisco Enterprise NFV Infrastructure Software (NFVIS)-bundled images exists because the user accounts using the software uses default credentials. This affects Cisco ENCS 5400-W Series and CSP 5000-W Series appliances

Memory Exhaustion Vulnerability in Cisco IOS XR

CVE-2020-3566, a memory exhaustion vulnerability is present in Cisco IOS XR software due to improper handling of IGMP (Internet Group Management Protocol) packets. Attackers can exploit this vulnerability by crashing the IGMP process which is done by sending crafted IGMP traffic which in turn crashes other processes causing memory exhaustion.

All Cisco network devices running any version of Cisco IOS XR Software are impacted.

Mitigation Techniques

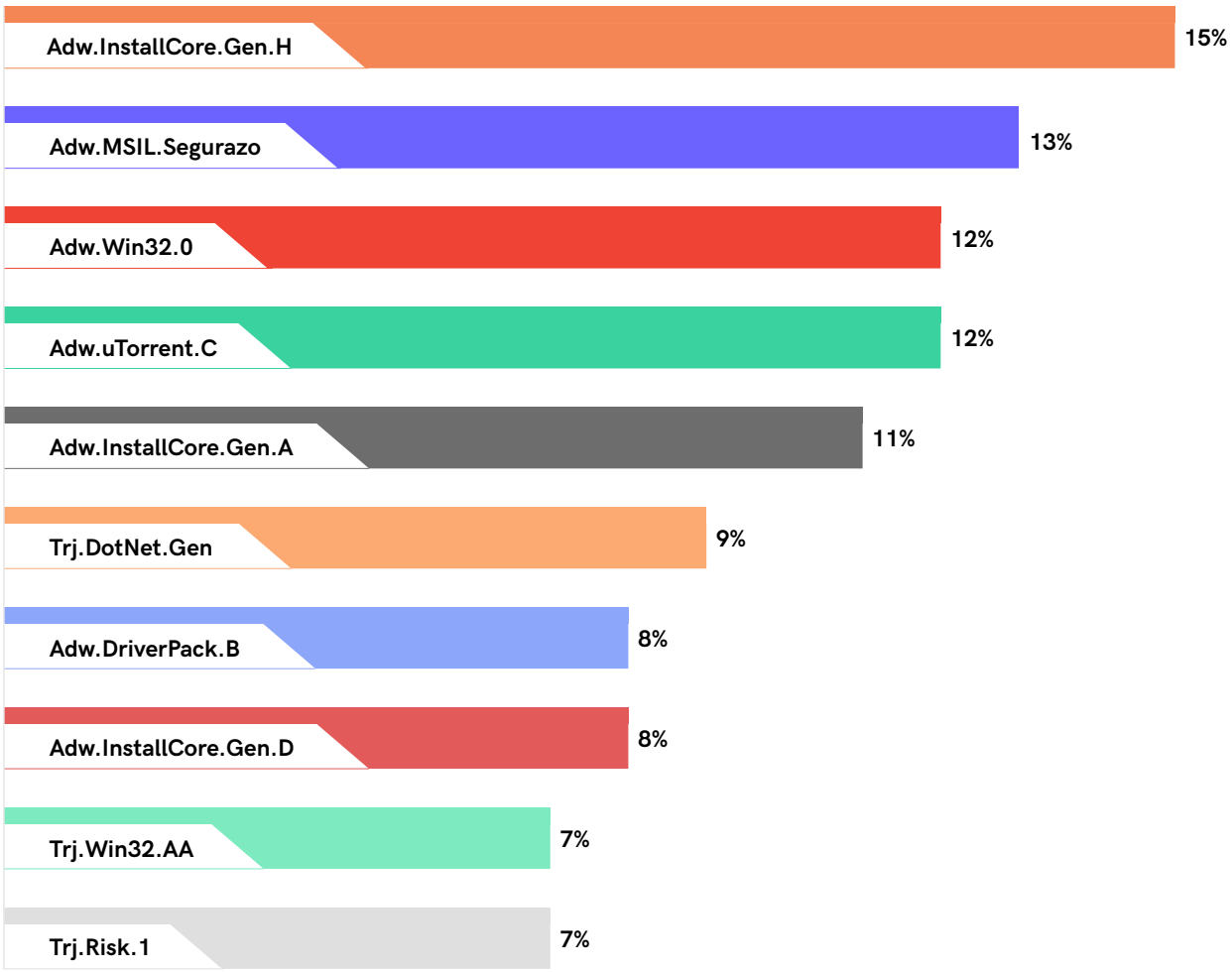
- Ensure all your devices are kept up-to-date and patched for the latest vulnerabilities
- Change your default settings
- Deactivate unused features and services to reduce the attack surface for cybercriminals
- Avoid compromising on security for cheap savings

Windows Under Siege

Windows Malware Type Breakdown

To continue its reign in the operating system industry, Microsoft puts a lot of effort to keep its users safe from the prying eyes. The maker of Windows is continuously tracking and fixing vulnerabilities with its monthly Patch Tuesday program. Despite numerous awareness campaigns on cybersecurity, the vast majority of users still do not follow proper security hygiene, thereby exposing themselves to cyberthreats.

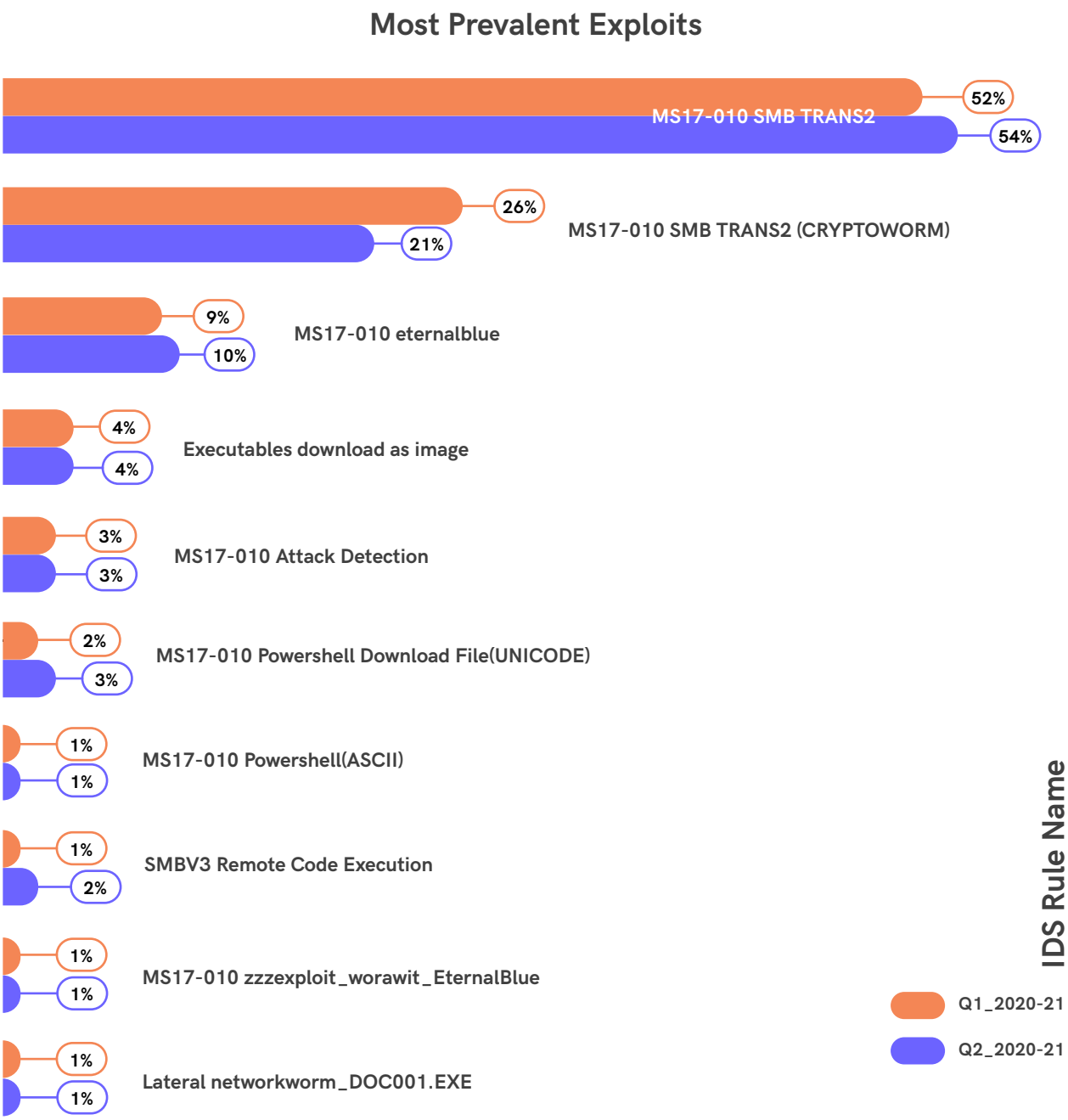
Split of Windows Top 10 Detections



In Q2_2020-21, Adw.InstallCore.Gen.H, which managed to remain active in its malicious activities, still holds the top spot for being the most prevalent among the other significant families.

Windows Exploits

The most notable find on the Windows platform is the visibility of good-old vulnerabilities which have existed for years and continue to be equally lethal to the ignorant users who have not yet applied the requisite patches. Take EternalBlue as an example. The exposure has grabbed many headlines for years concerning its nefariousness. Yet, a large number of Windows users feel updating their operating system is insignificant, risking themselves unnecessarily.



In this quarter too, SMB based vulnerabilities have continued to stay at the top of the threat list.

What Can Website Categorization Tell Us About Malicious URLs?

A URL is typically classified as malicious by AV Vendors, if it is a website created by the threat actors themselves or it is a legitimate website which has been compromised or if the website's hosting features have been abused to host malicious content. Out of curiosity, K7 Labs researchers decided to perform a cursory investigation of whether it is possible to obtain clues about the nature of such malicious URLs by forcing an evaluation of them by K7's Machine Learning-based Web Categorization feature.

Need for URL Categorization Based Access

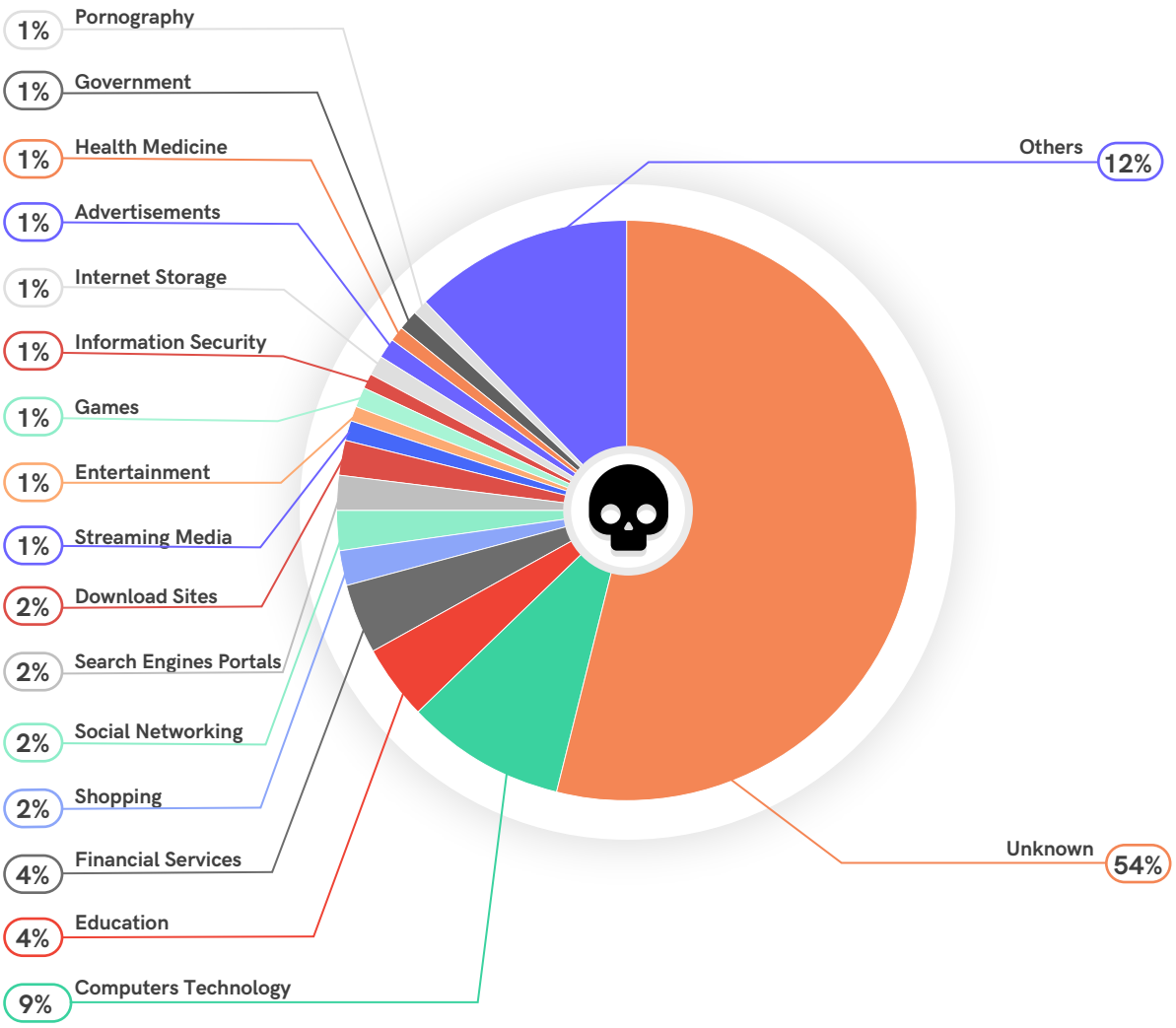
This is needed not only for an organization but also for consumers and parental control to restrict access to certain types of websites, e.g. sites hosting inappropriate content or news or shopping, etc. This is done for various reasons. An admin can restrict employees from browsing inappropriate content on the corporate network or parents could block access to improper content for their children. In the corporate context, this would certainly also help the organization in ensuring employees do not waste time, computer resources and bandwidth on sites that are not productive to the organization such as social networking, sports and the like. K7's Web Categorization feature uses various features of a website such as its content to make automated, intelligent and contextual decisions about its likely purpose so that admins can decide to block or allow classes of websites.

Malware

A malware site is typically one that hosts malicious content. Usually users accidentally access these malicious websites or are lured to them by clicking on links in a spam email or SMS or social media post, etc. One common reason could be typosquatting. For instance, the typosquatting variant of Google is 'Goggle.com' which is a fraud site. Another important factor is that many of these malicious sites look absolutely legitimate even if they use supposedly secure HTTPS, which may then not raise even an iota of doubt among users.

Let us now delve deeper into the subcategories of URLs already classified as Malicious.

Malicious URL Occurrences



Unknown: Indicates that the feature content was insufficient to make a decision on the nature of the site. It could be a newly registered domain or a domain which is just a few days old, parked and waiting to be populated. Threat actors frequently register domains to host their malicious content. Though this sub-category is of high risk to users among the other defined categories, a hacked domain could pose a higher risk to users as they might not know that the website they know and trust has been compromised.

Shopping: If this is an online shopping portal that has been compromised, it could mean easy access to your online financial transaction information when you do a purchase.

Social Networking/Download Sites/Streaming Media/Internet Storage: These types of websites are commonly used to host malware by threat actors who abuse the website's "cloud" content hosting features.

Financial Services: Could be compromised sites associated with Banking, Insurance and the like or could be sites designed to lure unsuspecting would-be customers of "financial services".

Adult Sites: Pornography sites frequently host both malware and adware. In addition, many adults could be coaxed into revealing their confidential and personal information which can later be used to victimise them. A deeper behind-the-scenes dive into our CTM Infection Rate stats depicted in the "Regional Infection Profile" section indicates the

blocking of several adult sites, malware and adware contributing significantly to the overall numbers.

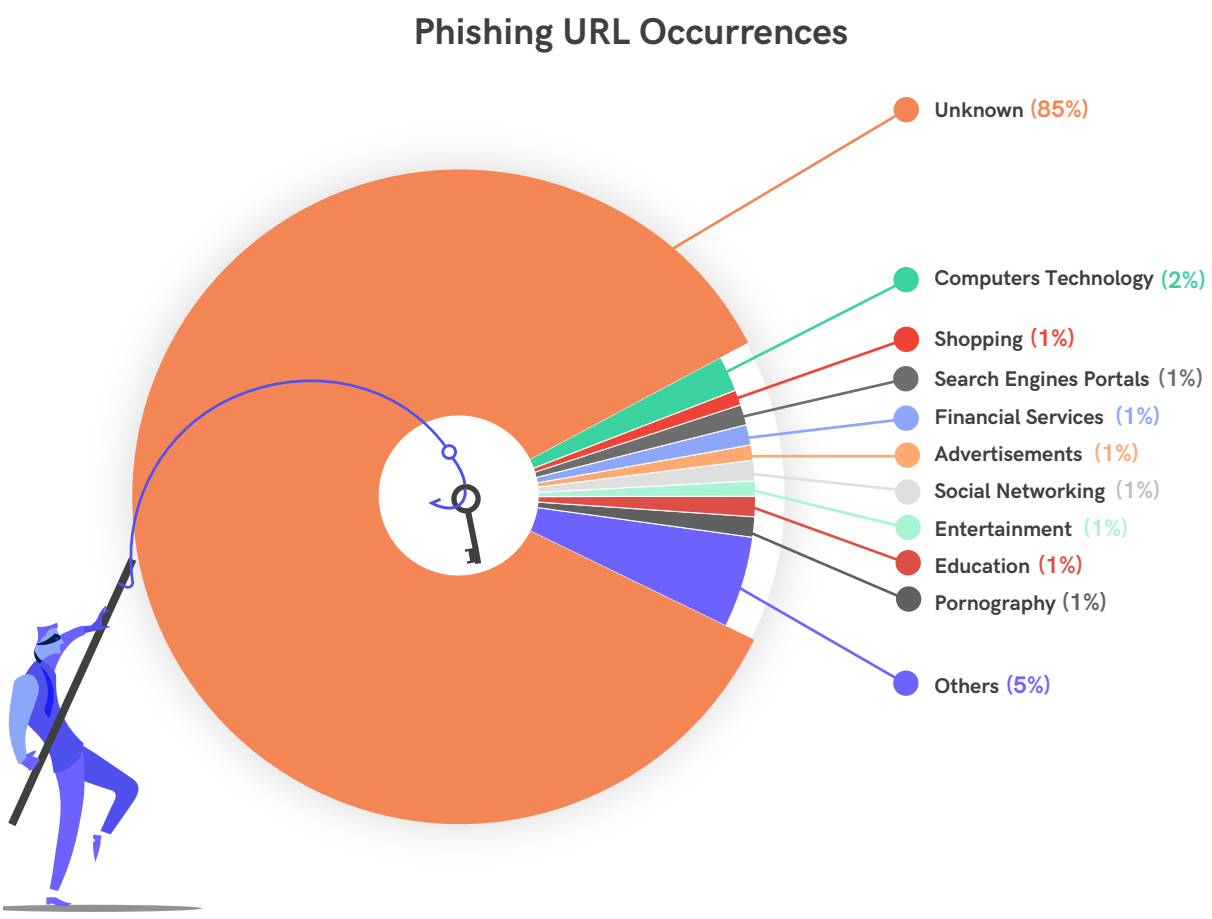
Games: Children could be easy targets if malware/ adware were deployed on a supposed gaming site. Some malware authors may be focusing on children, so an interesting and attractive game is an easy lure.

Health Medicine: These could either be dubious sites offering various "remedies" or, once again, compromised legitimate sites in the Healthcare sector. This sector has become a prime target mainly due to the sensitive personal information they have access to.

Phishing

Phishing websites often appear as an exact replica of a legitimate site to visitors. Here, they are confidence-tricked into providing their credentials or other sensitive information, such as credit card data, to the threat actors. Social engineering is used as a lure for fooling users into clicking the URLs.

In this case, most of the time, the users click on the URL with their full consent, without realising that they have taken the bait and have fallen into the trap laid by the threat actors. These websites can also be accessed by typosquatting as explained earlier.



The very high proportion of the "Unknown" subcategory would imply that most phishing URLs are hosted on domains owned by threat actors wherein core areas of the URL may hold insufficient features to classify into known categories.

Being Safe from the UnSafe

The Web is being used as a quick and easy way to deliver malware and harass victims. Therefore there is also a need to not only differentiate between malicious and clean URLs but also to categorize them accordingly as a way of restricting access to certain types of websites. Organizations are therefore advised to blacklist such categories, and if this is not possible, do a thorough check on the website and ensure access only if it is clean and appropriate.

Users are also requested to do their part by being more aware of such malicious links. We at K7 protect our users by sifting through a large number of URLs on a daily basis and categorizing them accordingly. Enterprise users are advised to install a reputed security product such as K7 Endpoint Security and keep it updated to stay safe from cyber threats. Consumer users can install K7 Ultimate Security and keep it up-to-date to avail of K7's Web Cat feature.

Mitigation Tips

- Ensure that the website you intended to visit and the one shown in the address bar are the same, especially sites that require you to part with sensitive information such as your login credentials
- Ensure you access sites that are secure, starting with "https://" and ensure there is a padlock symbol in the address bar. Please note that the 's' in "https://" does not by itself guarantee safety. This can only be used as a basic check to ensure encrypted web traffic
- Ensure that all the sites that you traverse from the landing page that require you to submit your PII or sensitive information such as credit card details are secure

The Mobile Device Story

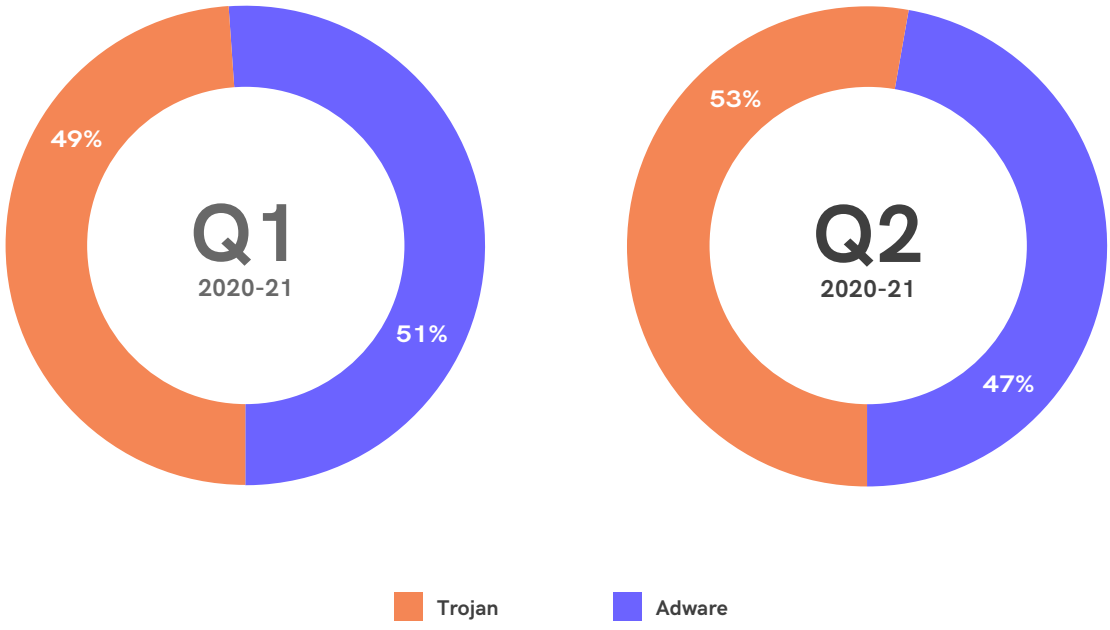
Our huge dependency on smartphones has encouraged numerous software providers and developers to unveil a multitude of apps that make life easier for its users. No wonder the bad actors also have joined the bandwagon to make wads of cash among other malicious intentions.

For instance, Joker and BlackRock, the two most inimical Trojans out there in the Android cosmos this quarter, have managed to blight a vast number of Android devices around the world. Both these sophisticated Trojans have come up with innovative swindling techniques such as leveraging Google accessibility service privileges and masquerading as the most popular apps.

Recently, Google has banned and taken down Joker infected apps from its Play Store. However, such malware-ridden apps are easily available for download from third-party app markets, proving advantageous for the threat actors' intentions.

In Q2_2020-21, the Android space has seen an increase in Trojans in comparison to the good old adware.

Adware vs Trojan Proportional Split



The preponderance of Trojans seen during the period was mainly for harvesting financial credentials, Personally Identifiable Information (PII) of the victims among a myriad other elements of value. Of late, cybercriminal groups have also started targeting smartphone users for mobile espionage.

The List of Fishy Apps and Ban Saga

Carrying forward the trend of banning apps, the Indian government has banned apps in Q2_2020-21 also, citing security issues. However, threat actors have started creating similar malicious versions of such popular apps to lure users. For instance, this quarter has seen a rise in fake TikTok apps, which had been one of the most popular apps.

Case Study: Fake TikTok App Targets Android Users

The latest ban on TikTok has created ripples among the social media app aficionados. While a significant part of its users has already deviated to substitutes, many TikTok users are still on the lookout for alternatives to get back their access.

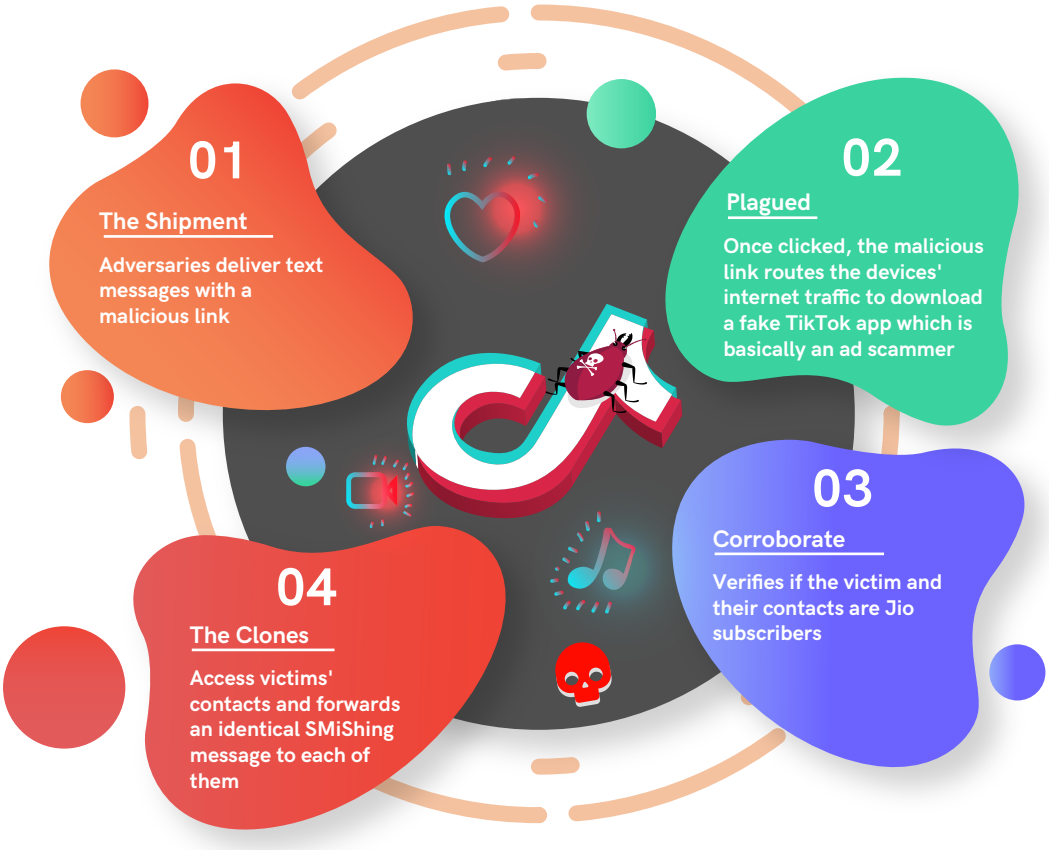
The malicious actors, who look forward to such massive craving, have already started taking advantage of it by rolling out several malware-riddled fake apps to swindle numerous users.

Our K7 Android security researchers have found multiple instances of these apps. Most of such malware get crafted to bamboozle victims.

One such recent malware targeted Reliance Jio telecom subscribers specifically. This fake TikTok app, an ad scammer, does not seem to do much more than display a fake TikTok login screen to the victims.

Here is how it works:

Anatomy of a Fake TikTok App

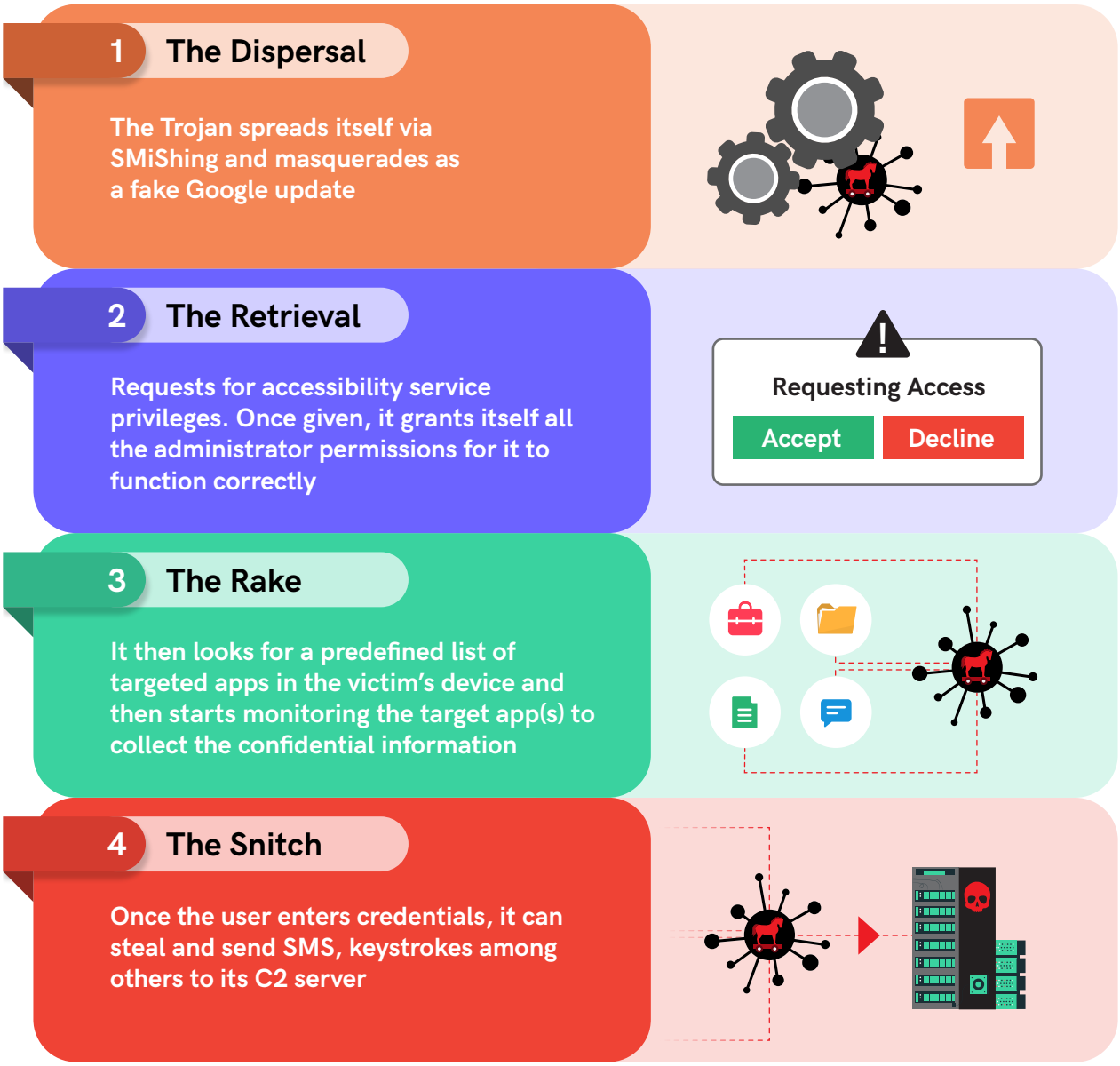


BlackRock: An Info Stealing Android Malware

During this quarter, we came across a variant of the Lokibot Banking Trojan, BlackRock, which managed to make quite a few headlines for its stealthy nature and devastating strategy. This Android-based Banking Trojan is capable of robbing banking and other login credentials from the victims' device. This Trojan has been derived from the code of the Banking Trojan Xerxes.

For easy understanding, here's how the BlackRock malware works.

The Wrath of BlackRock

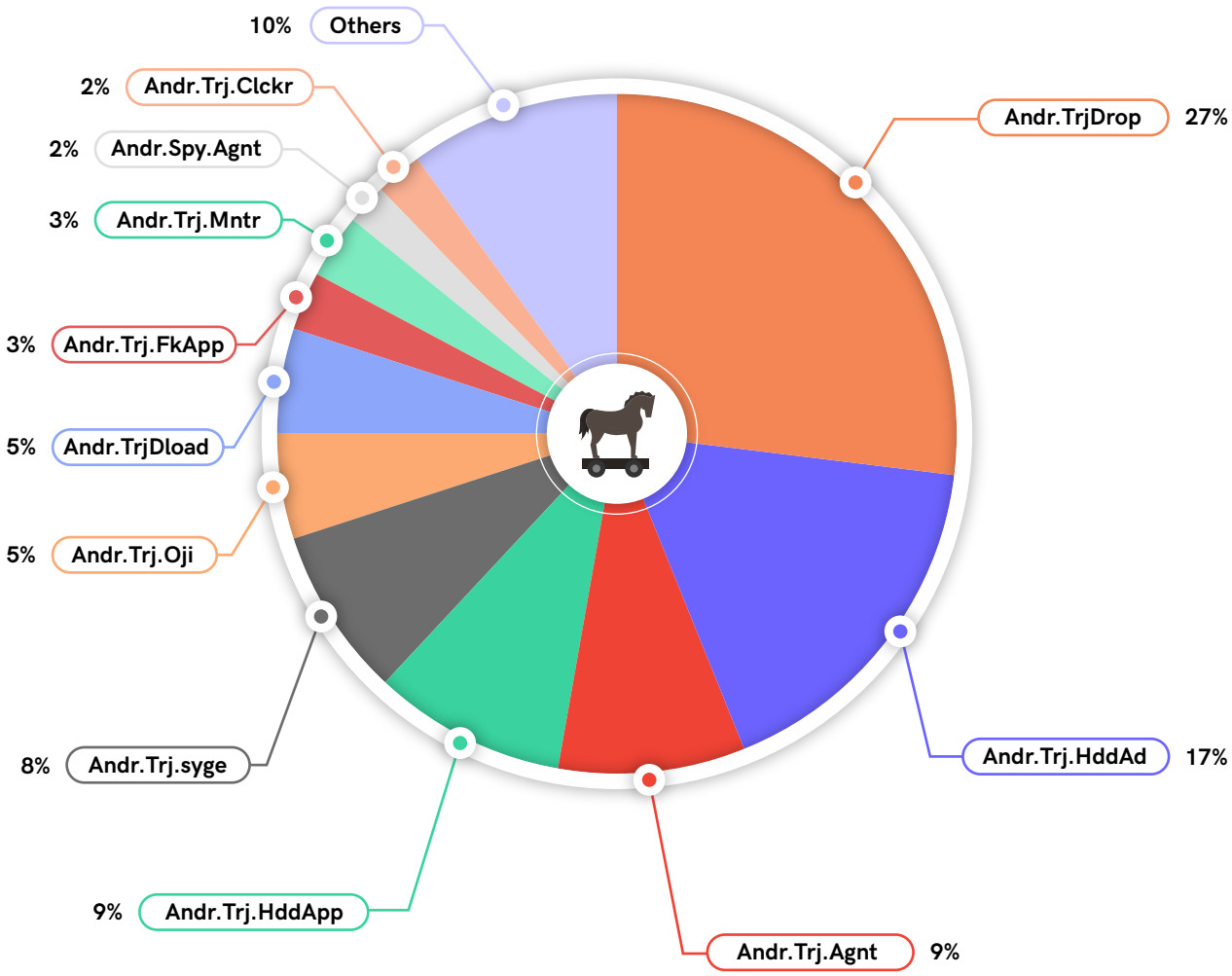


The predefined list of target apps (carried within the app's code) falls under the categories of Banking, Lifestyle, Music, News among others, including a few Indian Banking apps.

The Omnipresence of Trojans

The spurt of Trojan attacks remained ubiquitous in the country during Q2_2020-21 wherein over half the percentage of infected smartphone users experienced a Trojan-type attack.

Most Prevalent Trojan Types

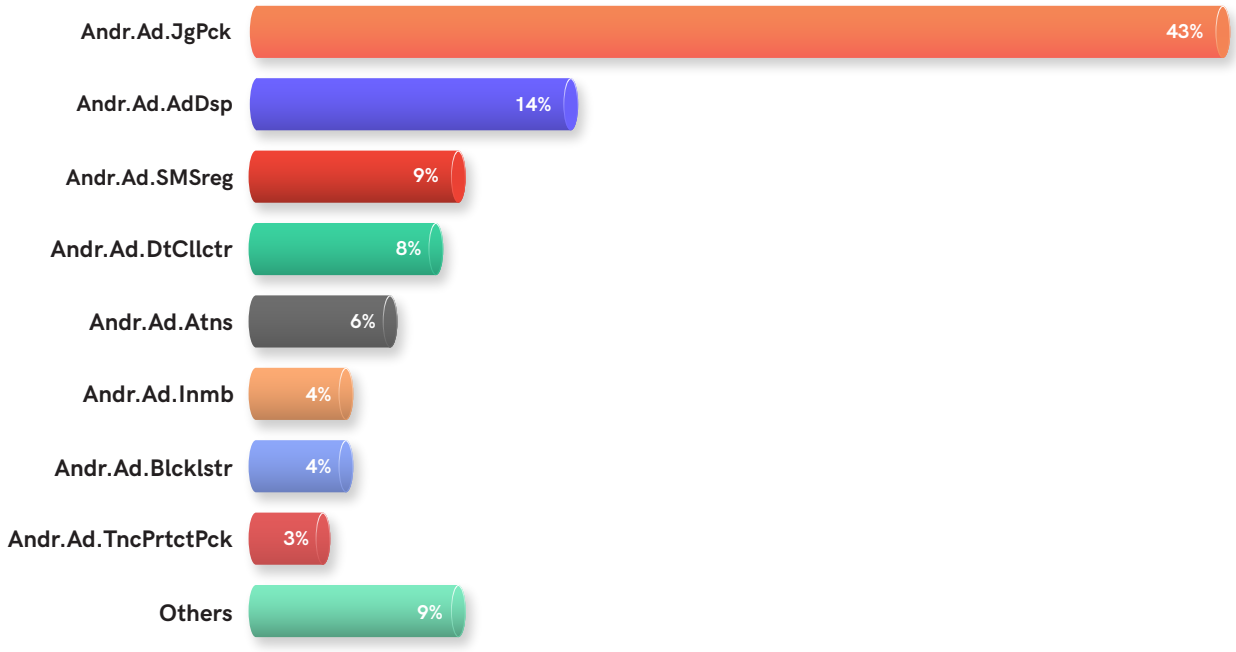


Despite the steady spike in the frequency of Trojan attacks, there are not enough new families seen during the period. In this quarter also, Andr.TrjDrop has maintained its reign over the rest of the malware strains.

The Subsisting Existence of Adware

Despite the continuous proportional plunge in presence, the visibility of adware is still significant. The idea behind adware, to make easy money, would continue to remain the prime reason behind its existence, and possibly in the years to follow.

Trend Line Showing the Adware Plague



The most prevalent adware of the previous two quarters Andr.Ad.JgPck has topped the chart in the current period too.

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
- Ensure the "Install unknown apps" option is not enabled on your Android devices. Remember never to download apps from any third-party app stores
- Install a robust security product such as K7 Mobile Security to stay protected from the latest threats

BACK TO CONTENTS

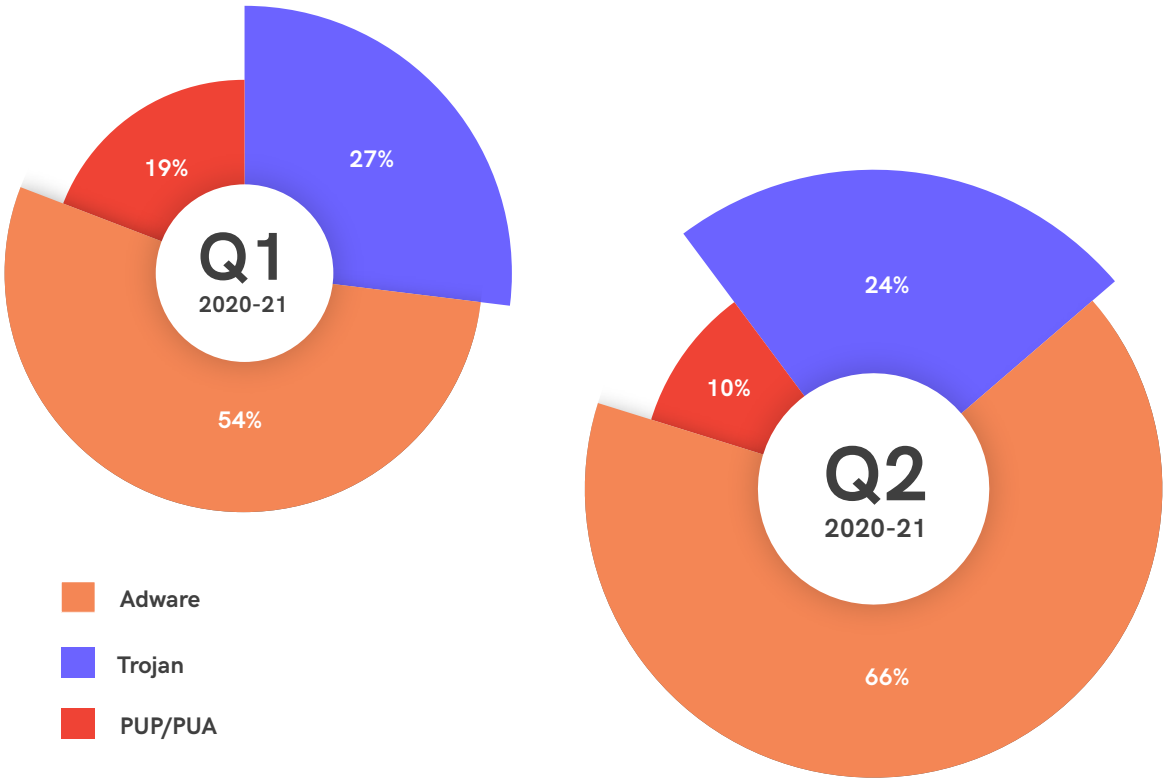
Mac Attack

The concept of casting the net wide to trap more victims and reap more money has long become a cliche. Unlike the malware barometer on Windows or Android platforms, the attacks on macOS have waned. However, the plateauing of threats has another, darker story to relate. Attacks on the macOS front have become more targeted with a higher degree of success.

Take the instance of EvilQuest, for example. The nefarious malware package bundles ransomware and spyware, and aims to exfiltrate the victim's data. The in-memory code execution or fileless abilities, and its intention behind the veil of ransomware hints at the changing threat landscape.

Besides such highly-active Trojans, the adversaries are leveraging adware more than before to make some quick bucks. The growth of Potentially Unwanted Applications (PUP/PUA) is experiencing a steady decline, probably because of the strict software review policies of Apple.

Adware, Trojan & PUP Proportional Split



*The Trojan percentage for Q2 does not include EvilQuest, as it has the major share which could skew the results

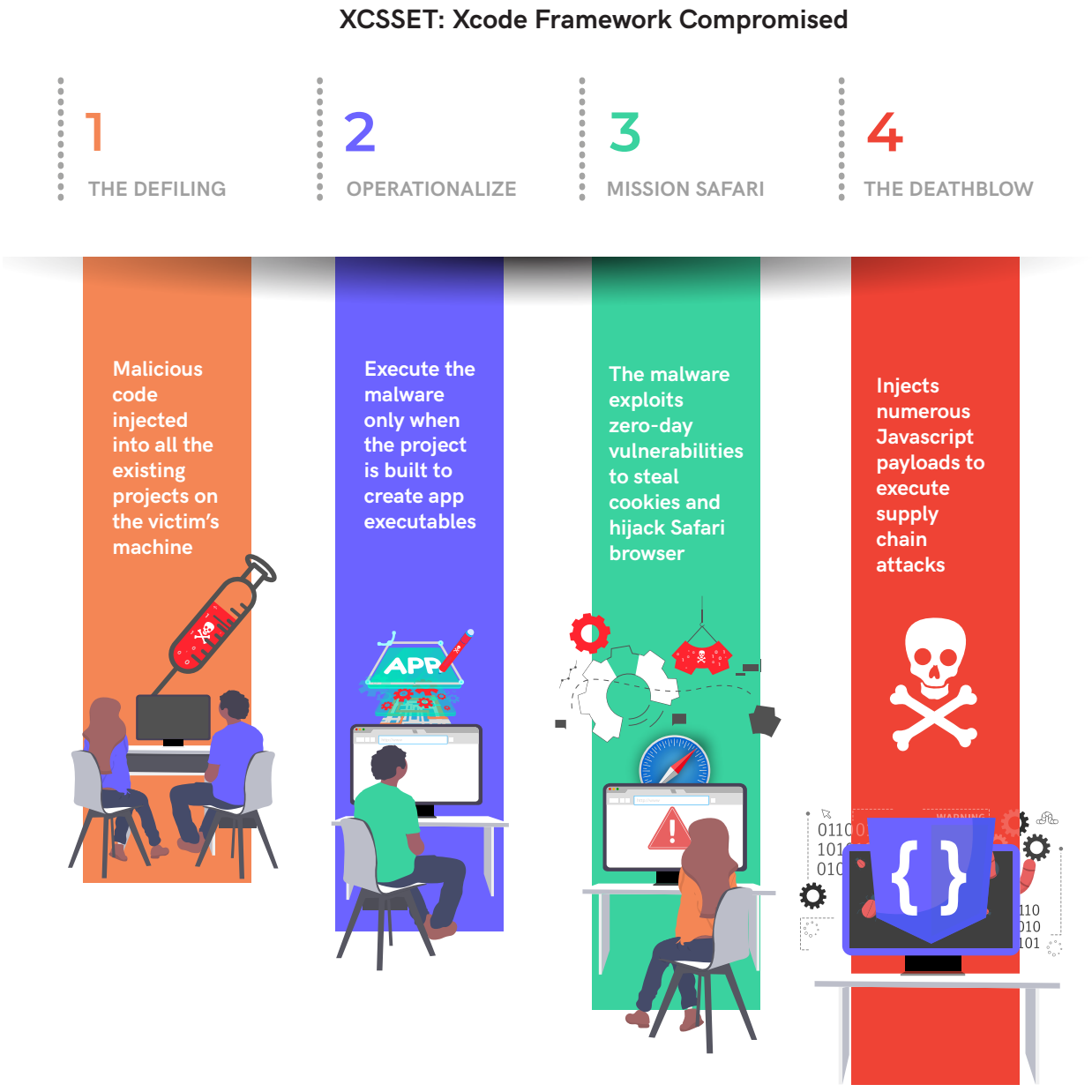
As you can see in the comparison graph above, along with its footnote, the transition doesn't indicate that the mayhem of Trojans on macOS is diminishing. Instead, the threat actors have launched more sophisticated, targeted and effective Trojan attacks in Q2_2020-21.

XCSSET Exploiting Xcode Projects

The growing popularity of the macOS is no secret. This massive uptick has also encouraged threat actors to ramp up their attack frequency with innovative methods.

Take the latest XCSSET, for example, the freshest macOS malware intended to hit Xcode, a free integrated development environment (IDE) for developing software and apps, to ensure maximum damage by proliferating automatically to maximum macOS driven computers. This would compromise all the projects being built on a developer's machine. Once the developer rolls out the infected Xcode projects as apps, they would unwittingly forward the malware to a plethora of other macOS driven computers.

The malware kill chain is as depicted.



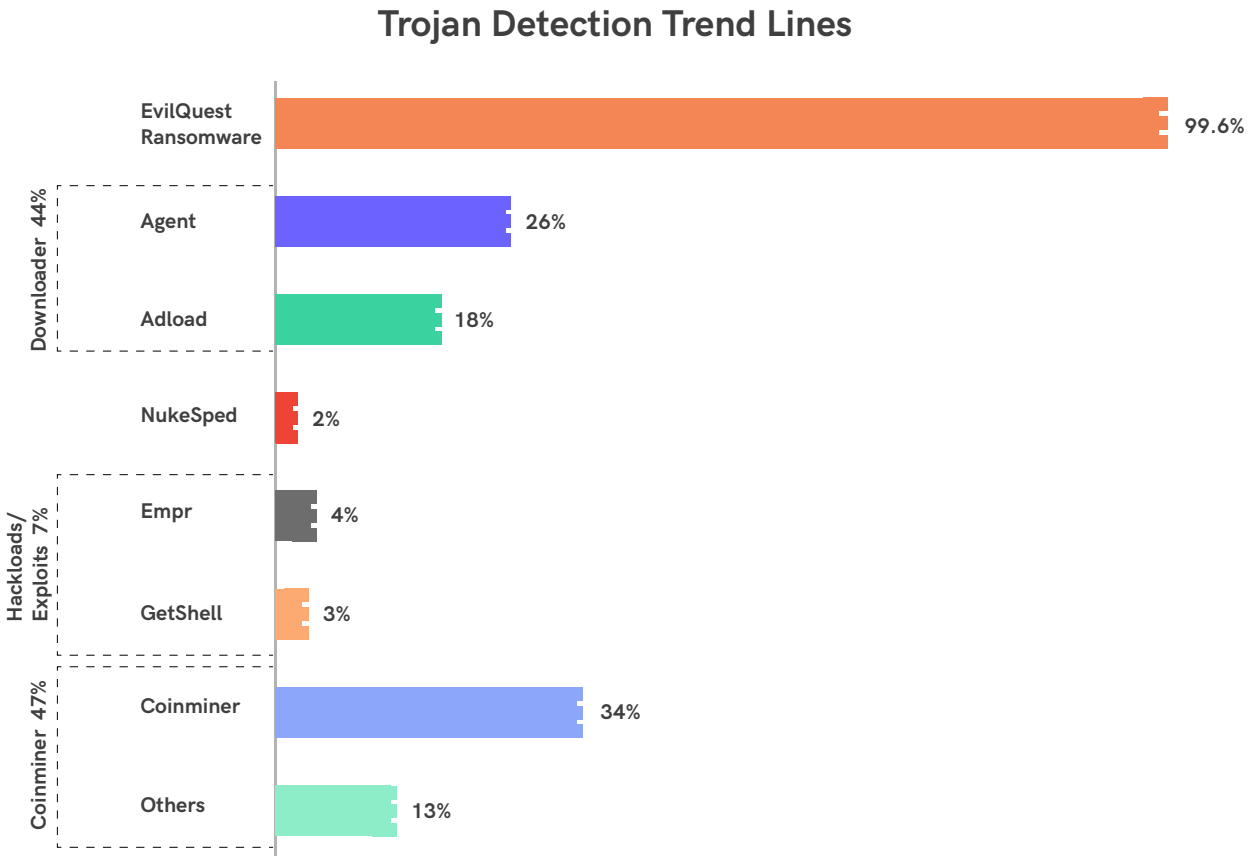
Notarized Adware: Blunder by Apple

Apple started notarizing applications to protect its users from malicious apps thus improving their confidence in using the apps. Once notarized, Mac's "Gatekeeper", macOS' in-built security screening software, allows the app to run. However, one such adware, Shlayer, also got vetted by Apple as clean, causing a buzz in macOS security circles since it poses a threat to users.

This has been fixed in its subsequent update.

The Furore of Trojans

The variety of Trojans active in Q2_2020-21 remained quite interesting. The range was scattered from Ransomware to Downloaders and Hacktools to Coinminers. Interestingly the dominant presence among Trojans was grabbed by one single ransomware called EvilQuest, the very first strain of which was identified by our K7 Labs Researcher Dinesh Devadoss; this ransomware isn't showing any signs of retiring anytime soon.

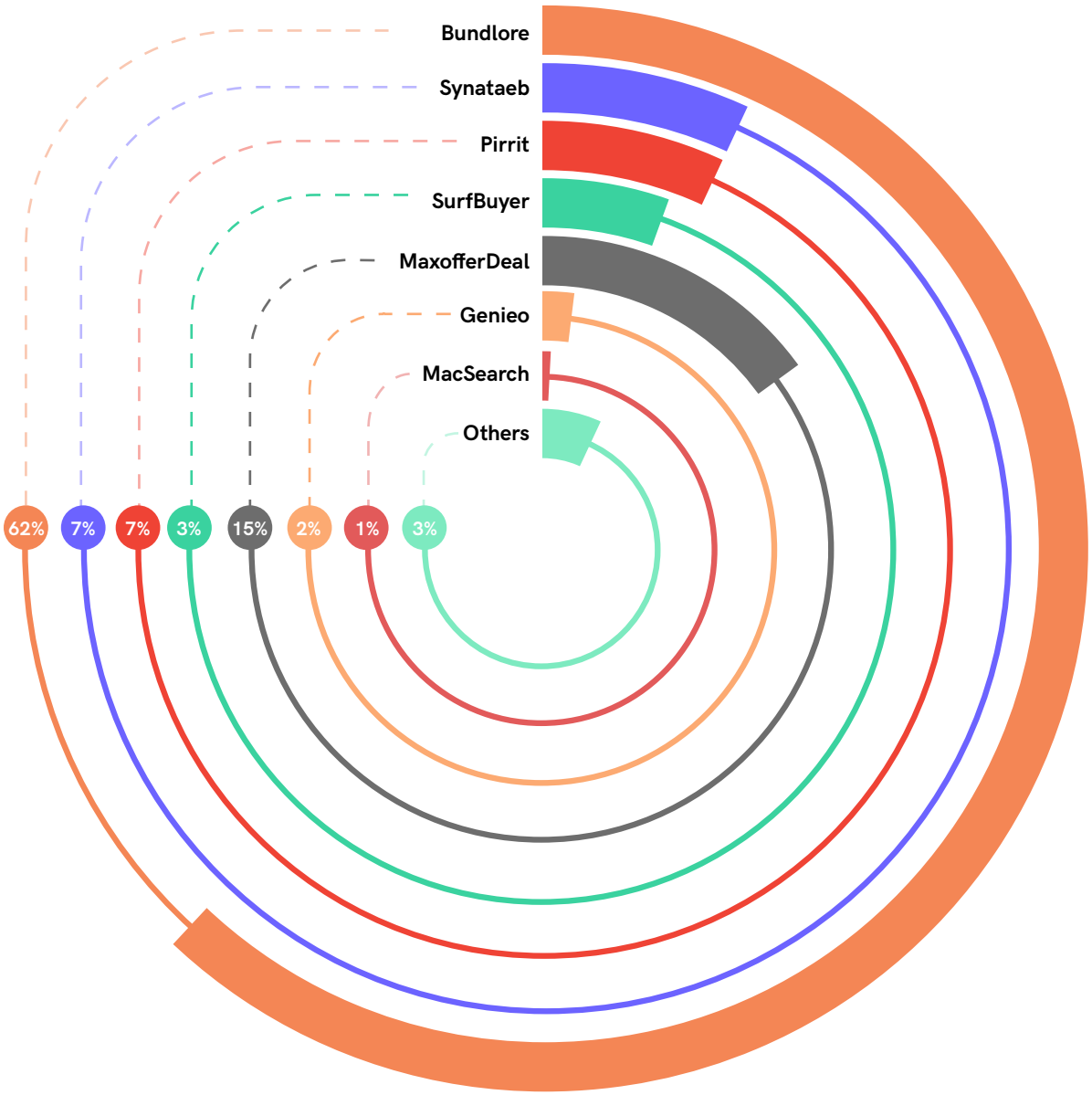


Another interesting discovery in Q2_2020-21 was the growth of Coinmining malware in comparison to Q1_2020-21. The significant growth in Coinminers this quarter possibly indicates that the numbers could rise further in the future too, especially during these pandemic times.

The Upsurge of Adware

Interestingly macOS is the only platform, for now, where we see a constant proportional rise in adware. The key reason behind this is that adware is an easy way to make money, without the need to make complicated malware which could prove expensive for the threat actors, considering the fact that there are fewer potential victims in comparison to the Windows OS, and also due to the effort expended by its developers in protecting its users.

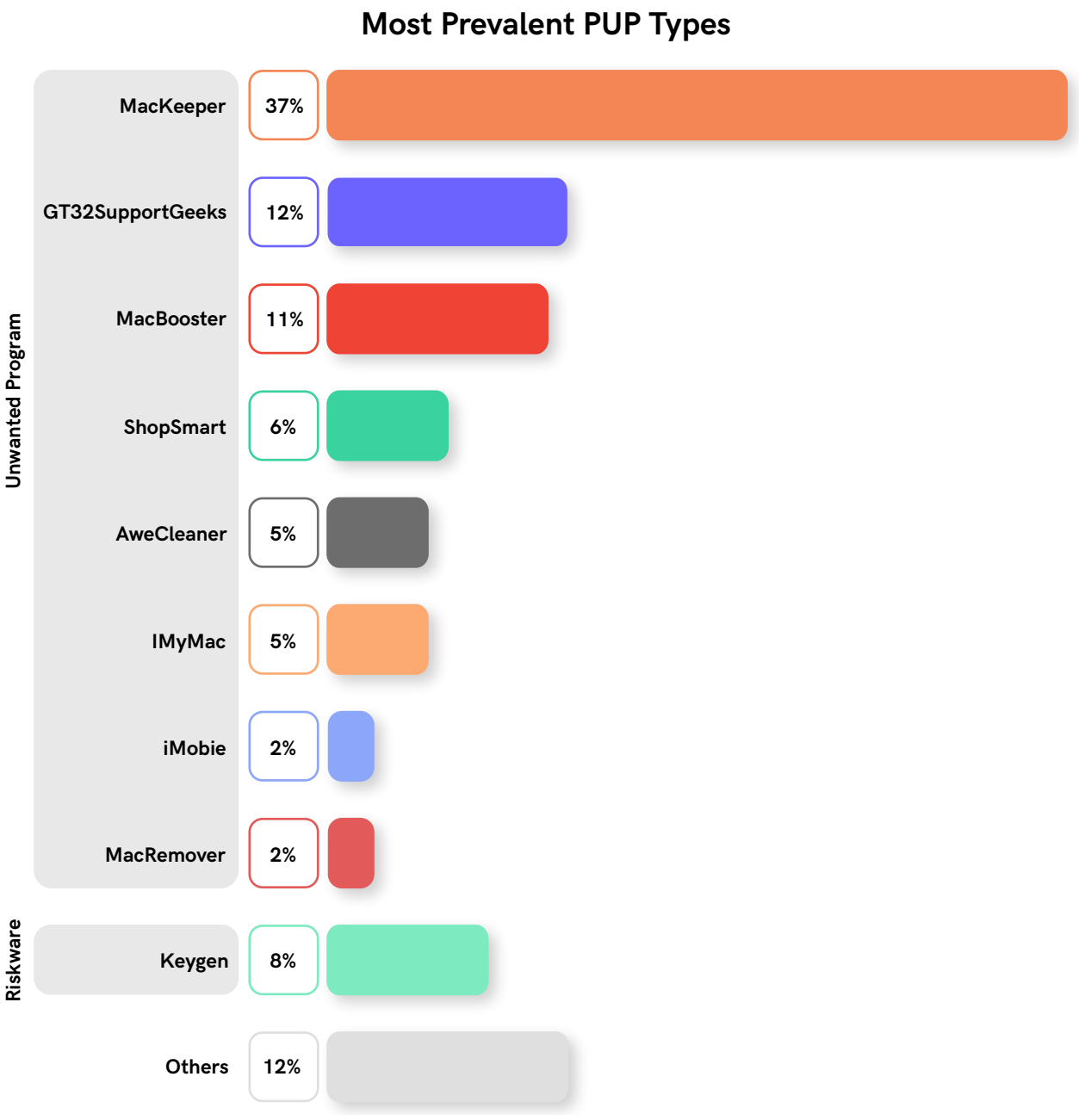
The Trend Line of Adware Variant Detections



Bundlore remained prevalent this quarter too.

The Pulse of PUP

There is not much innovation in the macOS PUP department. Most of the active PUP/PUA strains found in Q2_2020-21 have been active for quite a long time.



MacKeeper reigned supreme this quarter too.

Safety Guidelines

- Make sure your macOS is updated and patched for the latest vulnerabilities
- 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 frequency of cyberattacks is continuing to grow, and the trend is not going to decline in the foreseeable future. Attacks on organisations and end-users are mushrooming, as the perpetrators are coming up with new malware and deceptive techniques everyday.

To stay protected against these persistently-oncoming threats, enterprises and consumers should embrace the necessary safety measures as summarised (by no means exhaustive) below.

Enterprise	Consumer
Secure your devices by keeping them up-to-date and patched for the latest vulnerabilities, and protected by up-to-date, high-quality security software such as K7 Endpoint Security	Secure your device with a reputable security product such as K7 Total Security for Windows, K7 Antivirus for Mac and K7 Mobile Security (Android and iOS), and keep it up-to-date
Regularly assess your network for possible breaches	Installs apps only from the official App Stores
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

BACK TO CONTENTS

K7 SECURITY

www.k7computing.com

OCT 2020