CYBER THREAT MONITOR

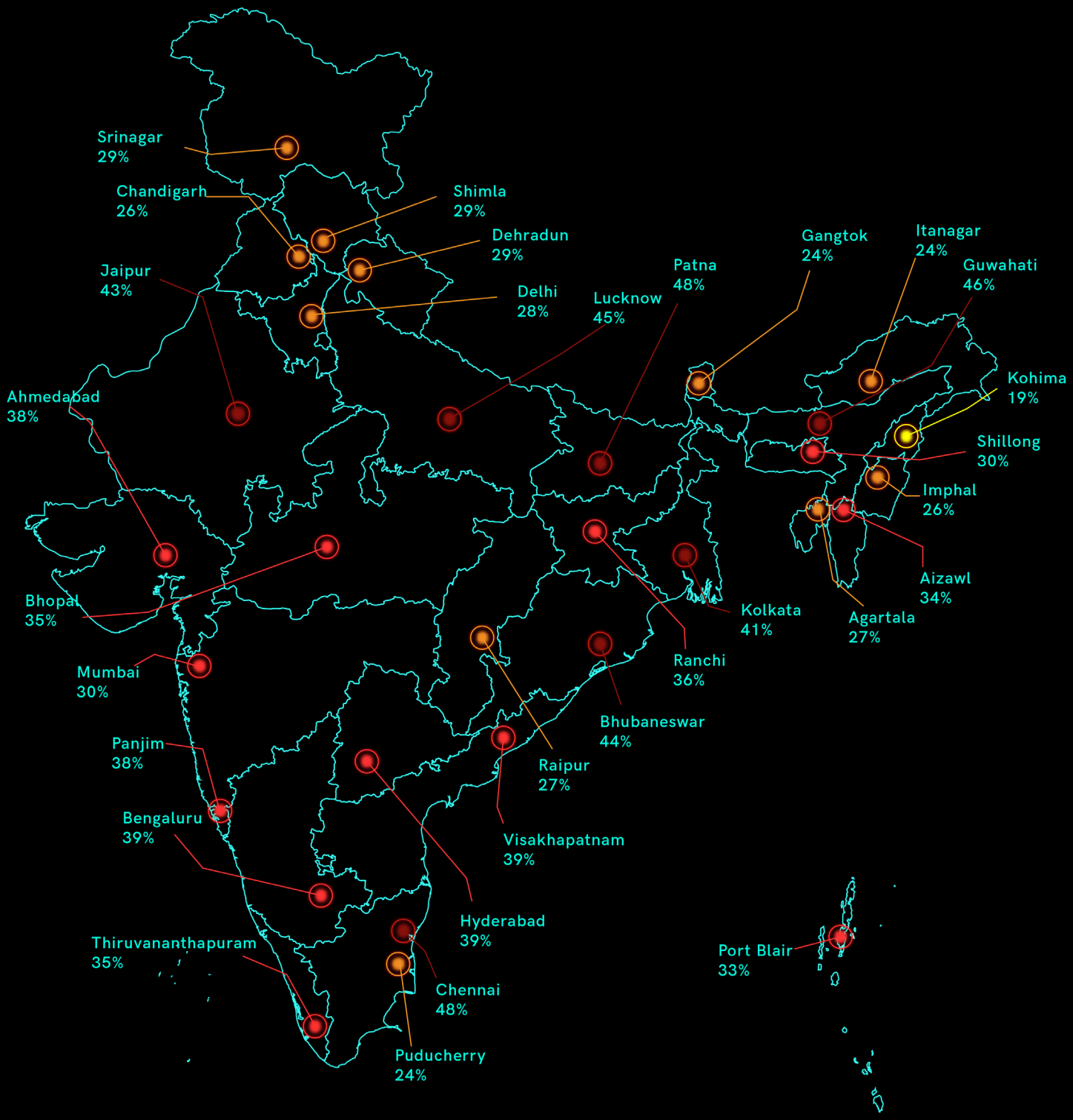
K7 LABS

Q1

2019 - 20

K7 SECURITY

CYBER THREAT MONITOR - INDIA



Map for illustrative purposes only. Not to scale.

CONTENTS

Demystifying the Cybersecurity Portrait of India 4

Regional Infection Profile 5

Infection Rate
The Metros and Tier 1 Cities Infection Rate
Infection Density

Enterprise Insecurity 11

Case Study 1: Logical Weaknesses of a WebLogic Server
Case Study 2: The Myth of Being Secure
Safety Recommendations

Vulnerabilities Galore 14

Exploitation of Loopholes

Windows Under Siege 16

Ransomware and Fileless Attacks
Windows Malware Type Breakdown
Mitigation Tips

Mac Attack 19

The Reign of Trojans
The Upsurge of Adware
Zero-day Rises
Safety Guidelines

The Mobile Device Story 23

The Territory of Trojans
Tips to stay safe

Danger in the Internet of Things 26

Mitigation Techniques

Key Takeaways 29

DEMYSTIFYING THE CYBERSECURITY PORTRAIT OF INDIA

"Welcome to the first quarterly issue of K7 Cyber Threat Monitor report! We've used K7 real-world telemetry data and K7 Labs security incident investigation data over the last quarter to help track the state of India's cybersecurity posture at both Enterprise as well as Consumer levels. We have begun with quarterly reports on the state of cybersecurity in India, to be followed in the future by similar reports for other regions in the world.

Today cybersecurity is heavily reported in the media, with all manner of stories from sophisticated attacks on large corporate entities resulting in data theft to globally spreading destructive ransomware to the theft of funds through phishing attacks on hapless individuals. However we thought we'd spice it up a bit and share our stories based on real-life scenarios, and our own interpretations of what's going on, backed by our proprietary telemetry data. Which city has the biggest cybersecurity problem? What types of threats are they facing? What were the Enterprise cybersecurity horror stories over the past quarter? We'll narrate all of this and more. Indeed, as our sources of K7 Ecosystem Threat Intelligence (K7ETI) increase, so shall the coverage.

We hope you find the content informative and useful, and, as always, we would love to hear your feedback on how we can improve."

REGIONAL INFECTION PROFILE

At K7 Security, we focus heavily on protecting at every security layer to maximise the chances of stopping malware as early as possible in its attack chain.

Of course, infection vectors which allow malware to be delivered to your device are many, but it might yet be interesting to see the proportional split of K7 active protection mechanisms which have stopped a malware attack across various high-user cities.

We would also like to measure the exposure of netizens to these various threats. Wouldn't it be interesting to determine where the cybersecurity risks are highest so that solutions can be devised to mitigate them? We have introduced a quantity called "Infection Rate" to highlight high-risk areas, and it is the quarterly city-wise Infection Rate depicted on the map of India at the beginning of this report.

Infection Rate

We define the "Infection Rate" (IR) of an area as the proportion, as a percentage, 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. The higher the IR, the greater the proportion of users who encountered at least one cyber threat event, and therefore the higher the exposure of netizens of that area to cyber risk.

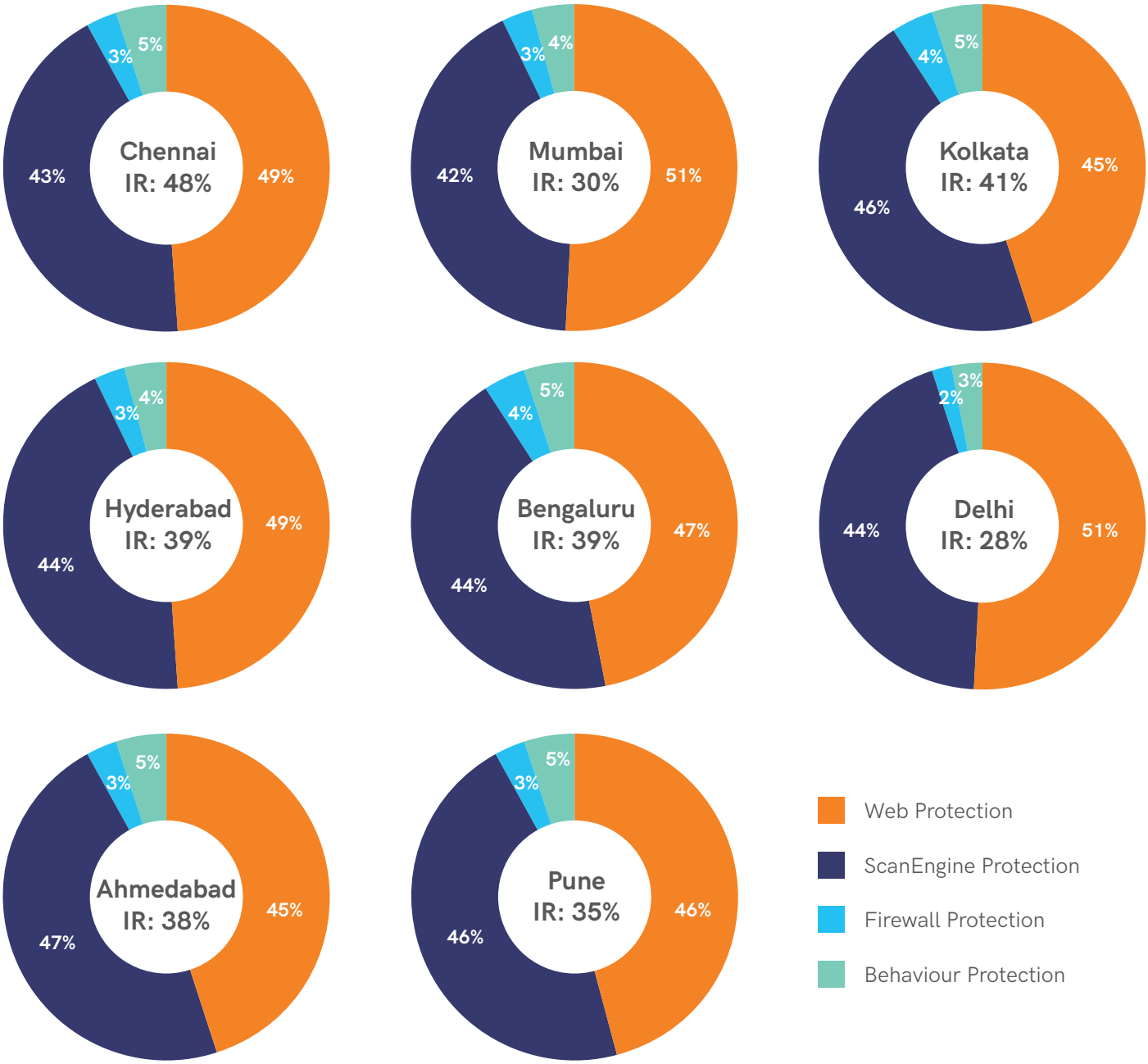
Infection Rate could, thus, give us a clue as to the cybersecurity awareness and/or cybersecurity hygiene of users in the corresponding area. Only if one knows that there is a problem can one take steps to fix it.

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

During the period, our telemetry data detected that, on average, about four out of ten users encountered at least one cyber threat in the high-user cities. Not surprisingly, users in Tier-1 metro cities in the country like Chennai, Hyderabad, Bengaluru, and Kolkata have experienced regular and sustained attacks.

"Infection Rate" (IR) is the proportion of K7 users in that area who have encountered at least one cyberthreat event which was blocked and reported to our K7ETI system

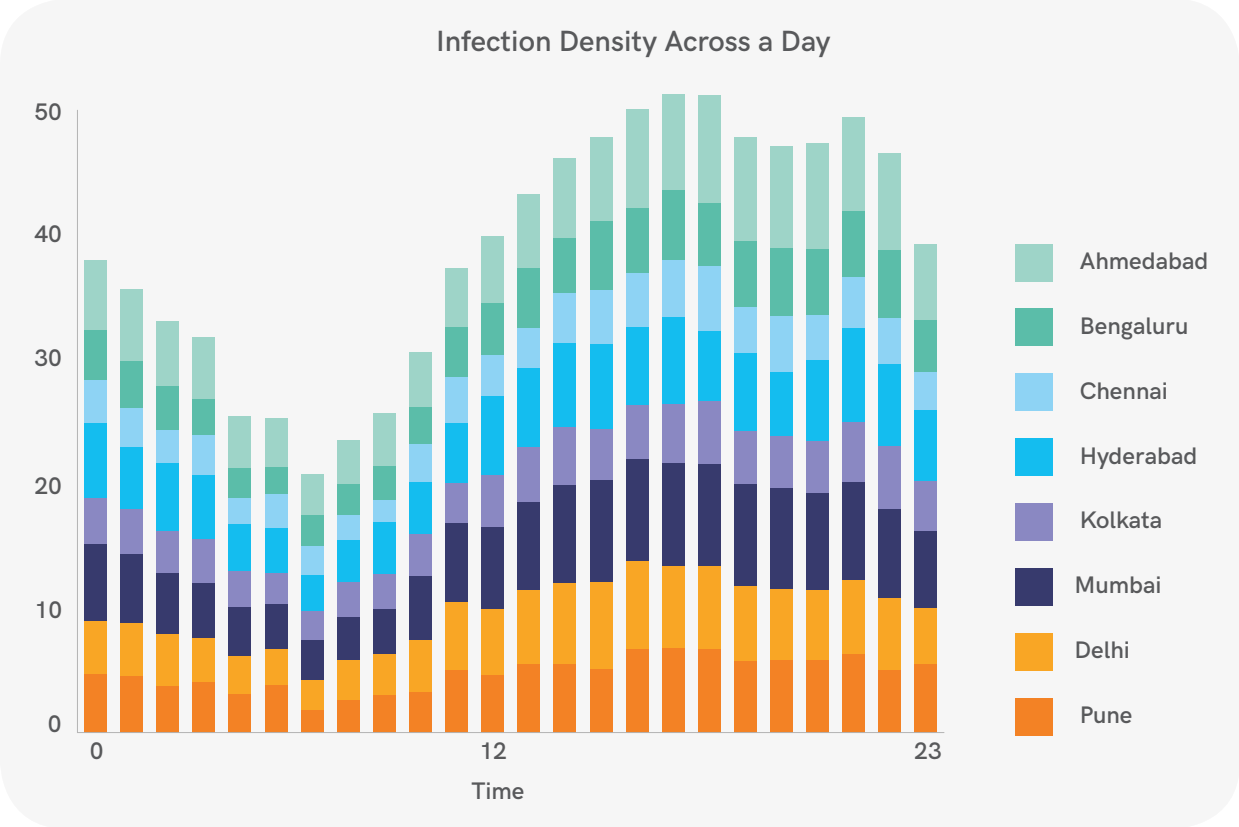
The Metros and Tier 1 Cities - Infection Rate



In this quarter, Chennai experienced the brunt of attacks, 48% of computer users having had a cyber threat encounter. Kolkata follows soon after at 41%. Cybercity Hyderabad and Bengaluru witnessed thirty-nine percent of cyber users coming under attack; it was a mere one percent less in Ahmedabad. In Pune, Mumbai, and Delhi, the Infection Rate stood a tad lower at thirty-five, thirty and twenty-eight percent respectively. We intend to track these IRs quarter-by-quarter.

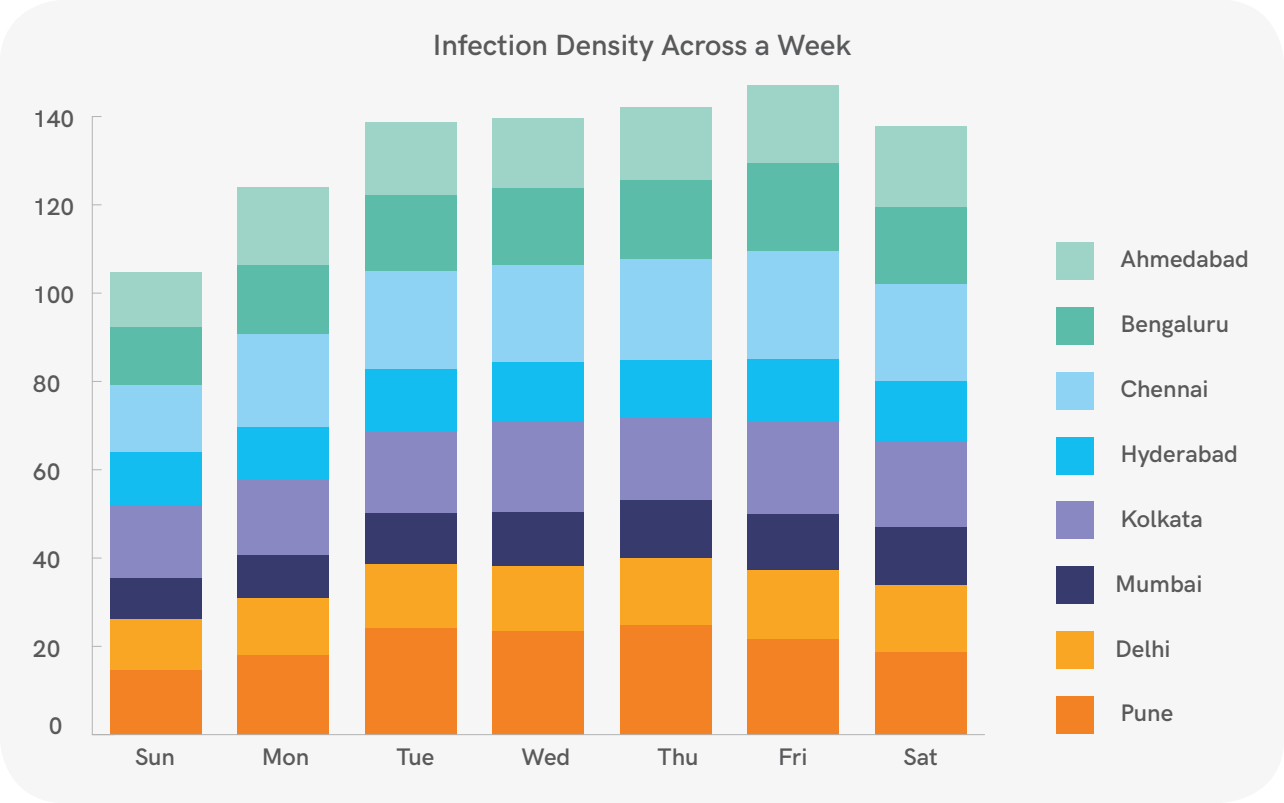
Infection Density

We decided to go a step further and determine whether there is a pattern of cyber threat event activity in these cities based on a specific time. When are users most at risk during a particular day? Does the day of the week have a bearing on cybersecurity risk?

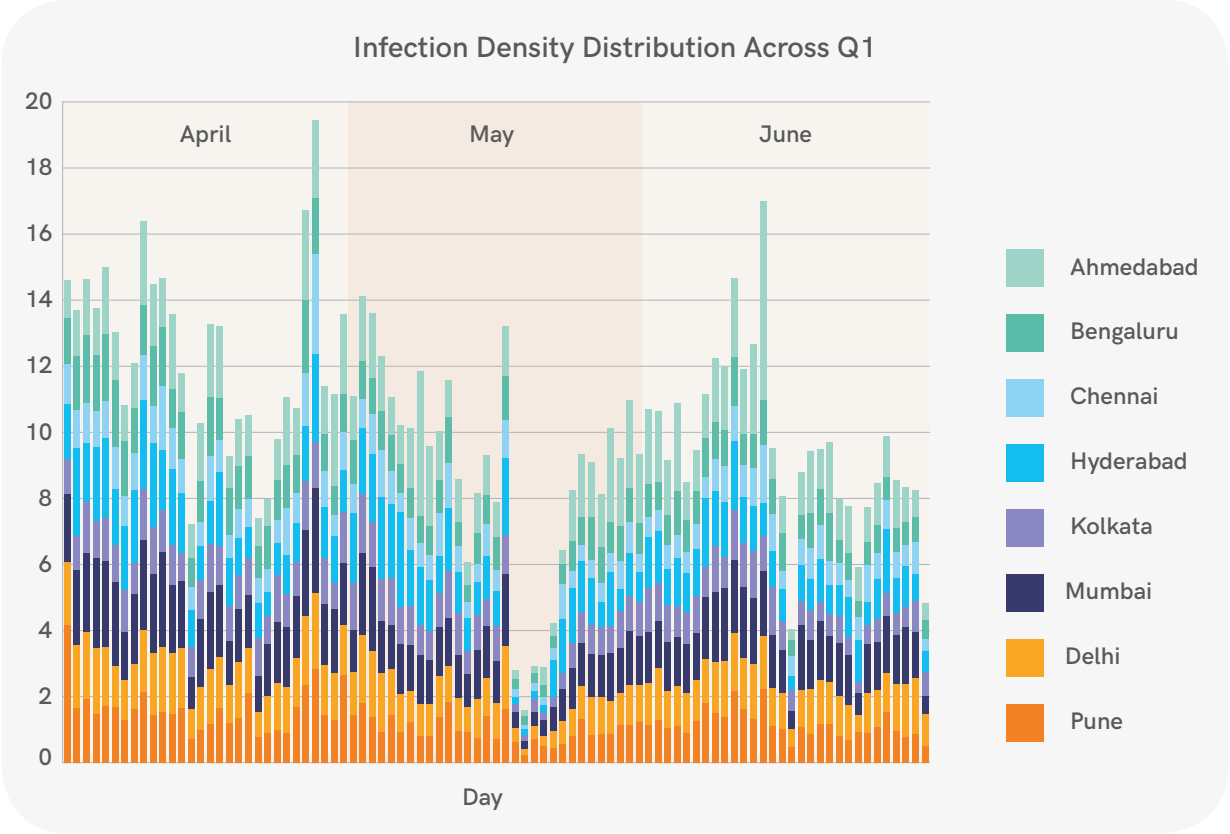


We introduced another quantity called "Infection Density" (ID) which is defined as the cumulative average volume of threat events at a particular point in time, whether a specific hour of the day, or a day of the week. We begin to notice some interesting patterns that are suggestive of either a lack of cybersecurity awareness or cybersecurity hygiene, including risky browsing habits, or both, and these patterns vary from city to city.

From the hourly breakdown of Infection Density, we see that typically, overall, the cyber riskiest hour in the metros is around 4 pm and the cyber safest is around 6 am. As might be expected, the waking hours, when netizens are accessing their devices, involve the highest cyber risk exposure.

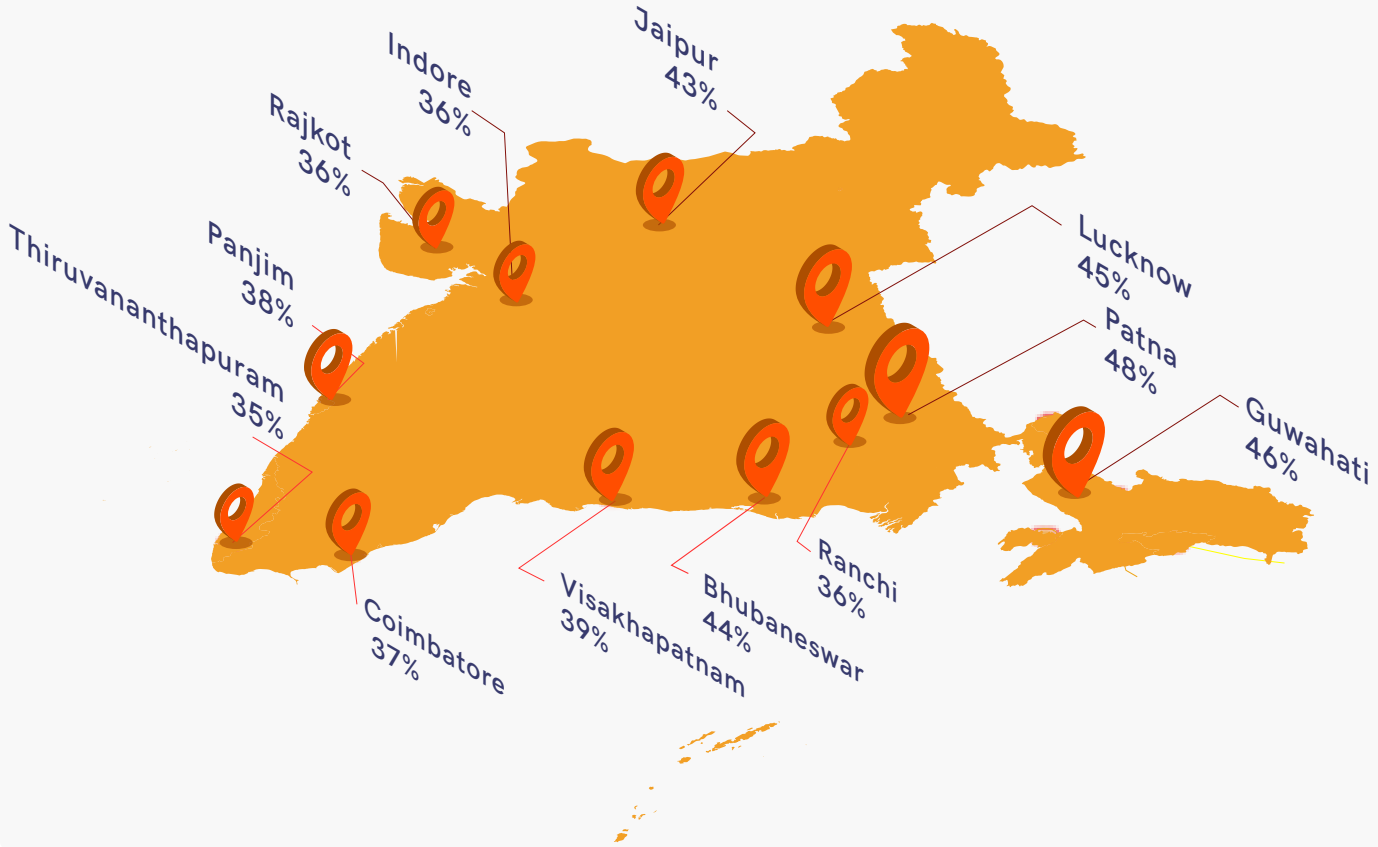


Surprisingly, when we stand back a little bit to see the weekly trends, we observe that, overall, Friday entails the highest cyber risk, and Sunday the lowest. Of course, Sunday could involve family time for netizens or outdoor activities, reducing their time for cyber misadventures, and perhaps even cybercriminals have their day off. Cyber risk exposure then steadily rises from Monday across the working days of the week.



Looking at days across the entire quarter, we get to see days with peaks of Infection Density and also dips. The dips correspond closely with weekends and public holidays when netizens either use their devices much less or use them in very predictable ways such as to stream movies or access social networking platforms.

TOP INFECTED TIER 2 CITIES

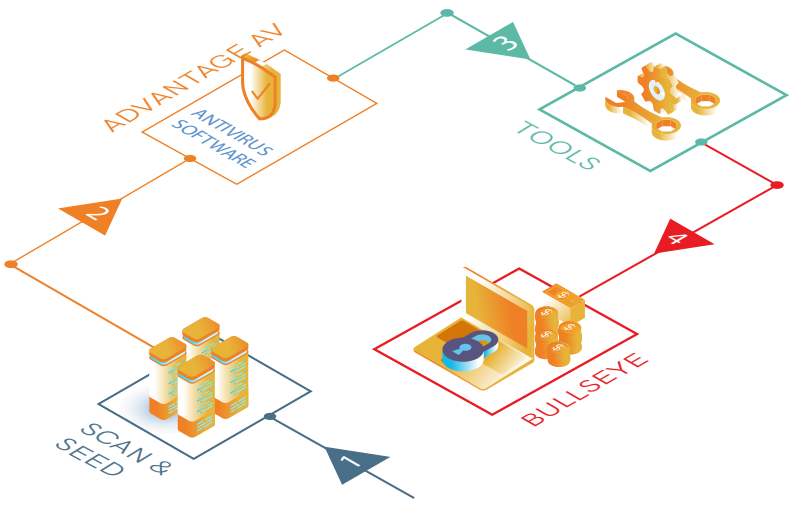


Interestingly, the Tier-2 cities such as Patna, Guwahati, Lucknow, and Bhubaneswar weren't any safer than Tier-1 cities. In fact, on average, they seem to be worse off. Could that be due to an awareness gap about cybersecurity? Patna experienced the highest percentile of cyberattacks during the period, identical to Chennai, and more than Hyderabad, Bengaluru, Mumbai, and Delhi.

We explained in our previous CRM report about how the older operating system versions like Windows 7 or Windows 8 and unpatched software are making the users more vulnerable to cyberattacks. Here are two case studies we observed recently to illustrate how adversaries are exploiting vulnerabilities and weaknesses to deploy lethal attacks.

Case Study 1: Logical Weaknesses of a WebLogic Server

In our first case study, the attacker penetrated the network by exploiting a remote code execution vulnerability (CVE-2019-2725) in Oracle WebLogic Server (versions 10.3.60. and 12.1.3.0). Our analysis revealed that the system admin had skipped installing the required patch which Oracle had rolled out on 26 April 2019. The vulnerability allows unauthenticated, remote code execution in the network, meaning that a hacker who successfully exploits the weakness would be able to control the device on the network from a remote location. The detailed attack process is as follows.



1 SCAN & SEED

Attacker scans internet for WebLogic servers vulnerable to CVE - 2019-2725, gains unauthorised control and seeds sodinokibi ransomware via a PowerShell script

2 ADVANTAGE AV

Anti-Virus promptly deletes Sodinokibi ransomware files

3 TOOLS

Disabling system-installed Anti-Virus using third party tools and unpatched vulnerablity eventually succeeding

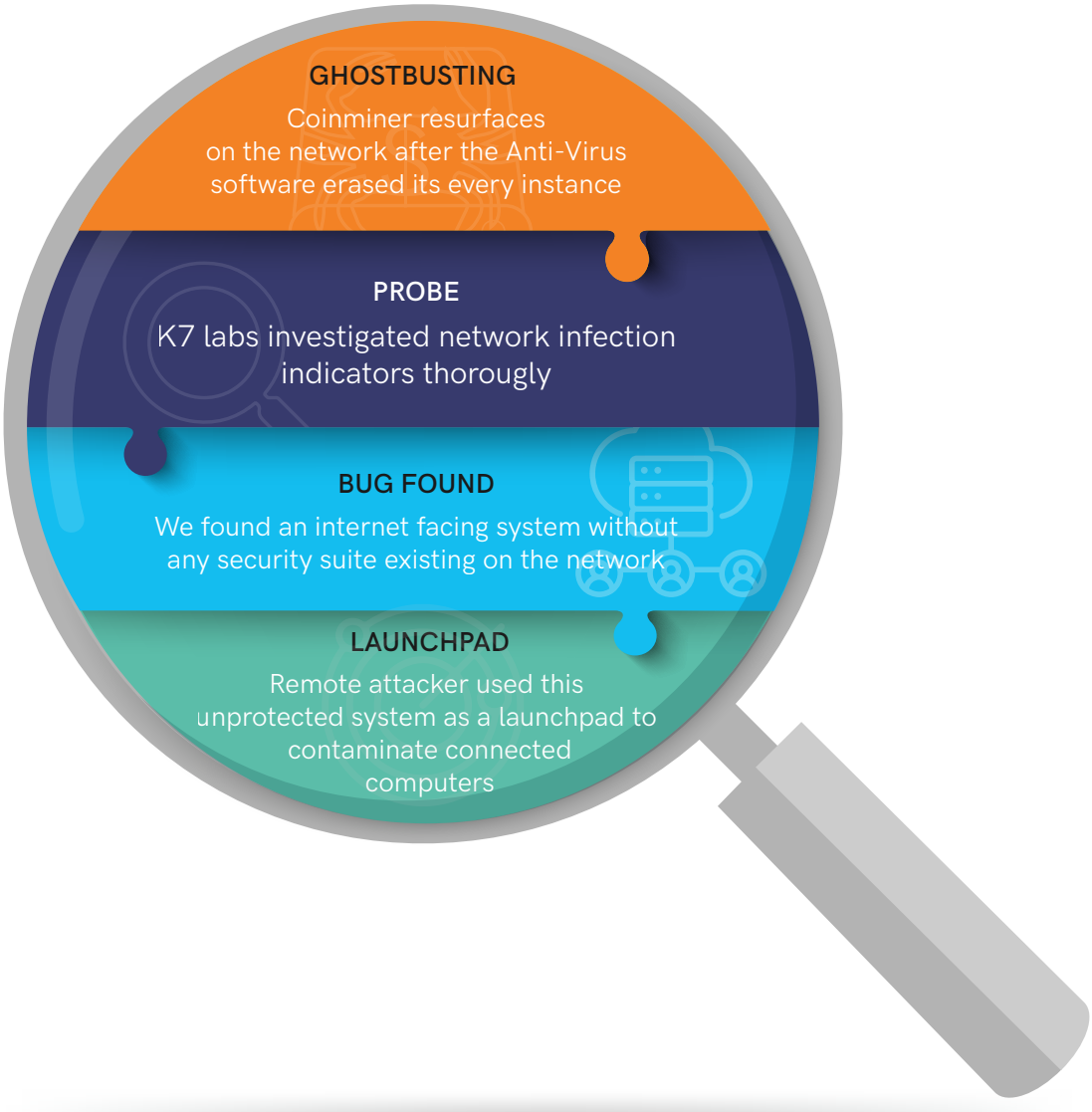
4 BULLSEYE

Sodinokibi ransomware is executed and all footprints wiped via scripts

Interestingly, many other servers surfaced on the K7 Labs telemetry radar which are yet to patch Oracle WebLogic vulnerabilities CVE-2019-2725 and CVE-2019-2729 (NB: CVE-2019-2729 too allows unauthenticated, remote code execution in the network).

Case Study 2: The Myth of Being Secure

Through our second cyber breach scenario, we tell you an even more scary story. Installing up-to-date security software in every system intertwined on a network comes under the basics of cybersecurity. Skipping such measures can make your network vulnerable to a myriad of cyberattacks, and so it happened in the case of the victim network we are presently discussing. In this case, the security software repetitively detected and deleted coinmining malware, which subsequently reappeared. In our initial investigation, we found an unprotected internet-facing system existing on the network. The attacker compromised the system remotely and used it as a Launchpad to attempt to contaminate other protected systems on the network.



Safety Recommendations

- The administrator should actively patch their OS and applications. (NB: CVE-2019-2725 is a critical bug with a high severity CVSS rating of 9.8/10 which means it must be patched ASAP).
- The administrator should not be lax in monitoring system logs and security notifications, especially about malware detected on the network.
- The administrator should not assume that the network won't be hacked because it doesn't hold any significant data that might interest malicious actors. Many attack tactics are automated and are not a targeted attack on a specific entity, so anyone with an unpatched vulnerability is a potential victim or collateral damage.
- Availability of off-the-shelf attack-tool packages and network enumeration tools make it essential for admins to monitor and filter data coming in and out of each system.
- The second case study reminds us of the adage: "All of us are safe or none of us are". Having even a single unprotected system in the same network environment as the other critical systems is asking for trouble.

VULNERABILITIES GALORE

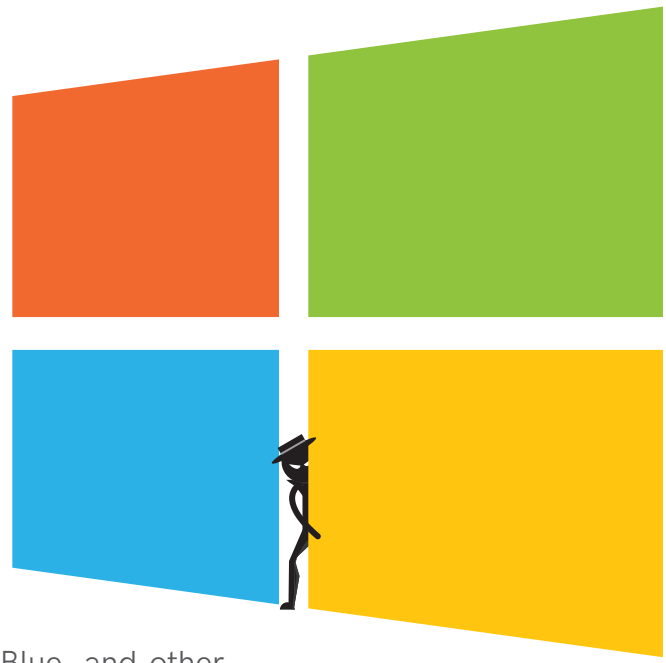
Exploit trends for any given period delineate the actual picture about what adversaries are doing to identify and victimise vulnerable systems. In this quarter, we found many such vulnerabilities exploited by cybercriminals, including APT groups, to accomplish their missions.

We observed a spike of ransomware attacks amongst enterprises all around. Old school ransomware like Wannacry is still doing the rounds, while more recent competitors like LockerGoga, Gandcrab, and Sodinokibi are also climbing up the cyber breach ladder.

Exploitation of Loopholes

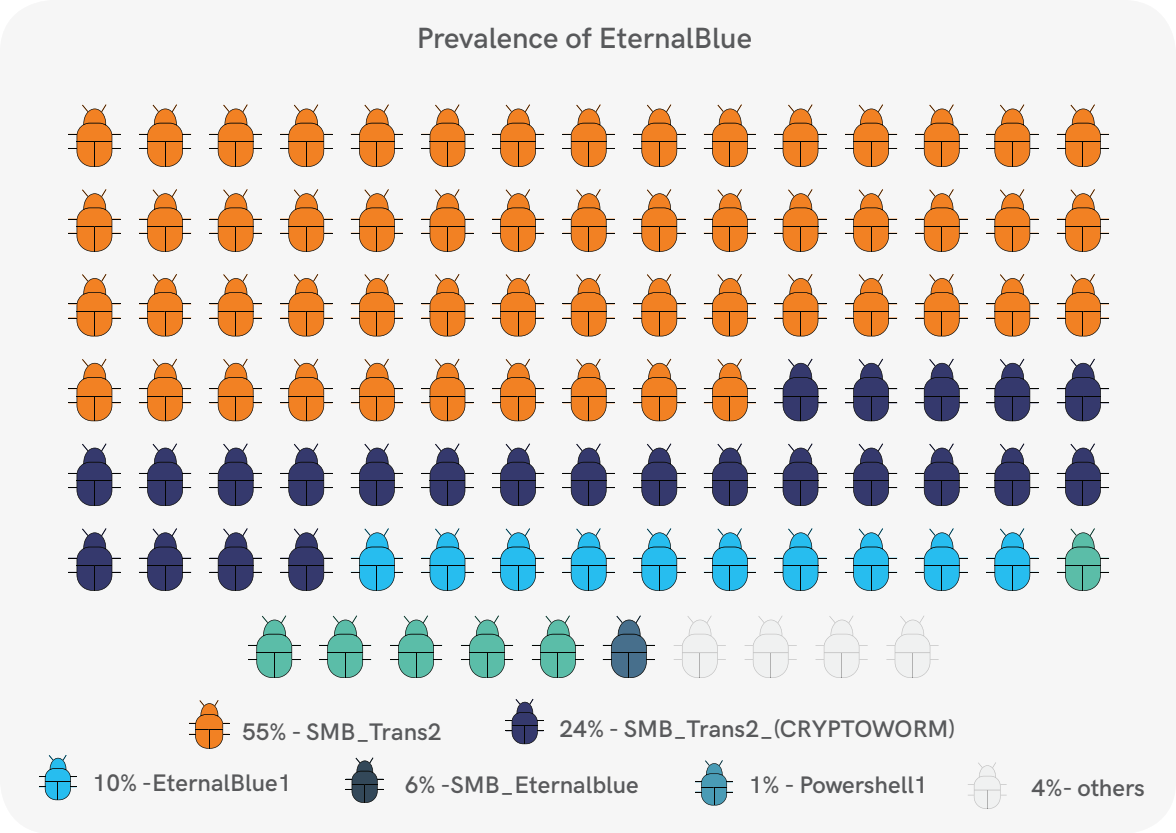
A critical wormable Windows RDP (Remote Desktop Protocol) exploit for a vulnerability assigned reference CVE-2019-0708, codenamed Bluekeep, has become the source of many cyberattacks targeting enterprises. We found several shreds of evidence that cybercriminals are actively exploiting this vulnerability. The Bluekeep vulnerability impacts older Windows operating system versions, including Windows Server 2008, Windows Server 2008 R2, Windows 7, which Microsoft intends to retire next year, and Windows XP. In short, the exploit exists in the kernel driver handling RDP, which can be manipulated by an adversary by sending specially crafted requests over RDP virtual channel MS_T120.

Moreover, as the cherry on top, a security firm has recently unleashed a penetration tool armed with a fully working exploit for the same vulnerability.



Another exploit which has been doing the rounds for a couple of years and is still actively preferred by the cyberthugs is EternalBlue. This exploit has been lethal, spreading disastrous ransomware attacks like WannaCry, banking Trojans like Emotet and Trickbot, and coinmining malware. This notorious exploit manipulates several vulnerabilities existing in the Microsoft Server Message Block 1.0 (SMB1), and is capable of taking advantage of dated Windows versions like Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 2012, Windows 8.1, Windows Server 2012 R2, alongside Windows 10 Version 1507, 1511 and Windows Server 2016.

The following chart indicates the prevalence of several SMB-based exploits blocked by K7's Intrusion Detection System (IDS), including EternalBlue, and other MS17-010 tagged vulnerabilities exploited in the wild.


Prevalence of EternalBlue
55% - SMB_Trans2
24% - SMB_Trans2_(CRYPTOWORM)
10% -EternalBlue1
6% -SMB_Eternalblue
1% - Powershell1
4%- others

Ransomware and Fileless Attacks

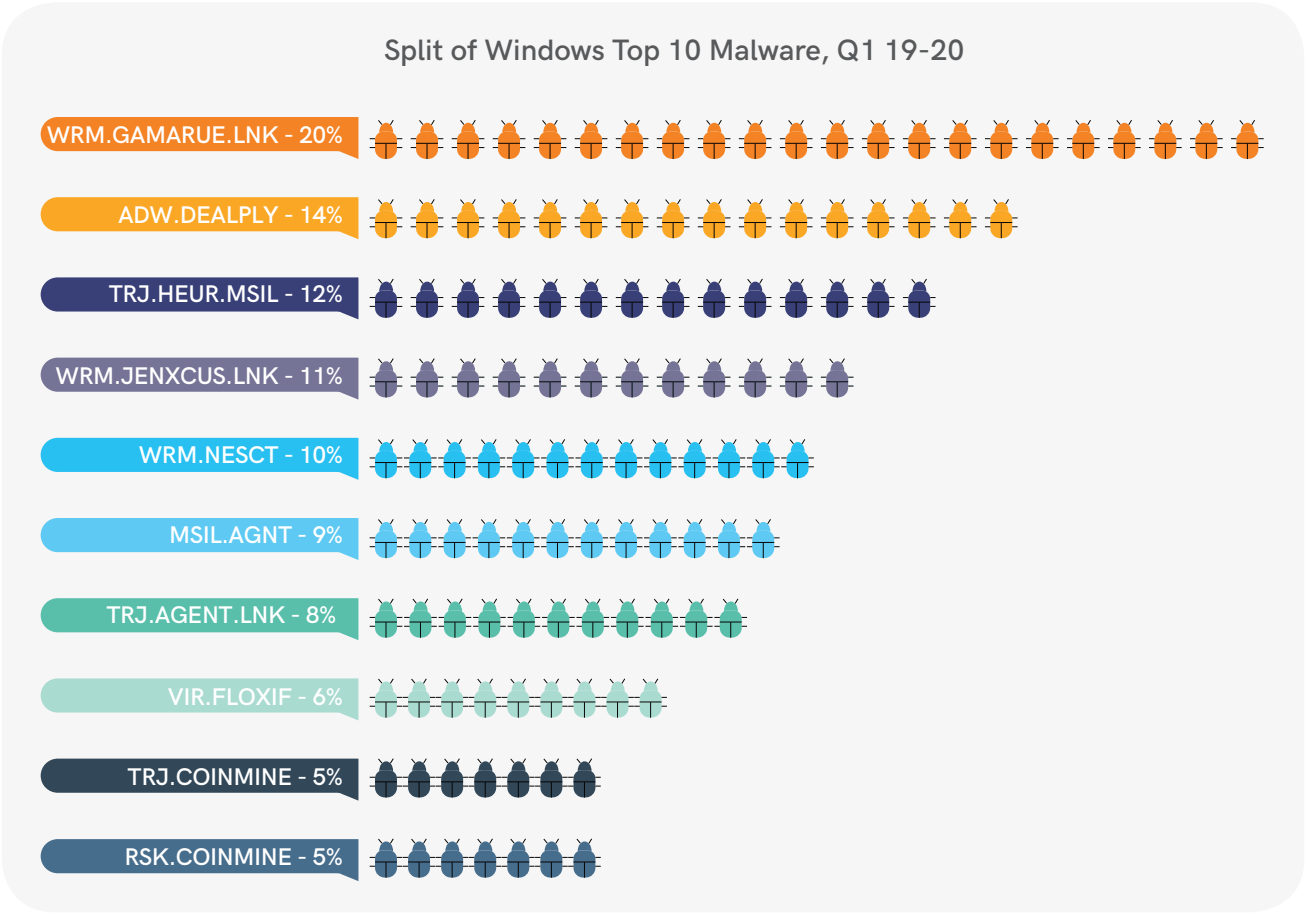
The gruelling rise of ransomware attacks is an ever-growing problem. After the arrival of Ransomware-as-a-Service (RaaS), ransomware attacks have started to grow at an alarming rate. Primarily hoodwinking by email, fake websites, plugins, and malicious advertising, and also by using the network and server-side vulnerabilities, threat actors trigger successful ransomware attacks. During the past quarter, 13 percent of our total behavioural blocks were identified as Generic Ransomware by the heuristic anti-ransomware feature built into K7 security products. This massive chunk of attacks proves that ransomware is still rampant.

Modern ransomware are using numerous advanced camouflage techniques to evade detection but get blocked in other protection layers of our security product. This is why multi-layered security is vital.

The upsurge of fileless attacks too is apparent given the evidence from our telemetry. We have seen more than 1000 unique instances of blocking abuse of PowerShell alone in attempted fileless attacks. This number is expected to rise as cybercriminals attempt to reuse pre-installed Windows components, such as PowerShell, to execute their nefarious designs, minimising artefacts, which can be more easily identified by security products.

Windows Malware Type Breakdown

Wrm.Gamerue.LNK, a component of a worm, remained the most prolific type of malware artefact we tracked. Gamarue infects your computer and external devices you connect to it, offers remote access of your computer to threat actors, and is capable of a dozen other malicious tasks. The list is also brimming with different versions of Trojans, Potentially Unwanted Programs, Adware, Coinminers and a slew of Deceptors, which trick users into parting with their cash, although they don't quite make the Top 10. Interestingly, Vir.Floxif, a file infector, has made the Top 10, indicating the resilience of this old-style malware which are still effective in spreading themselves far and wide.



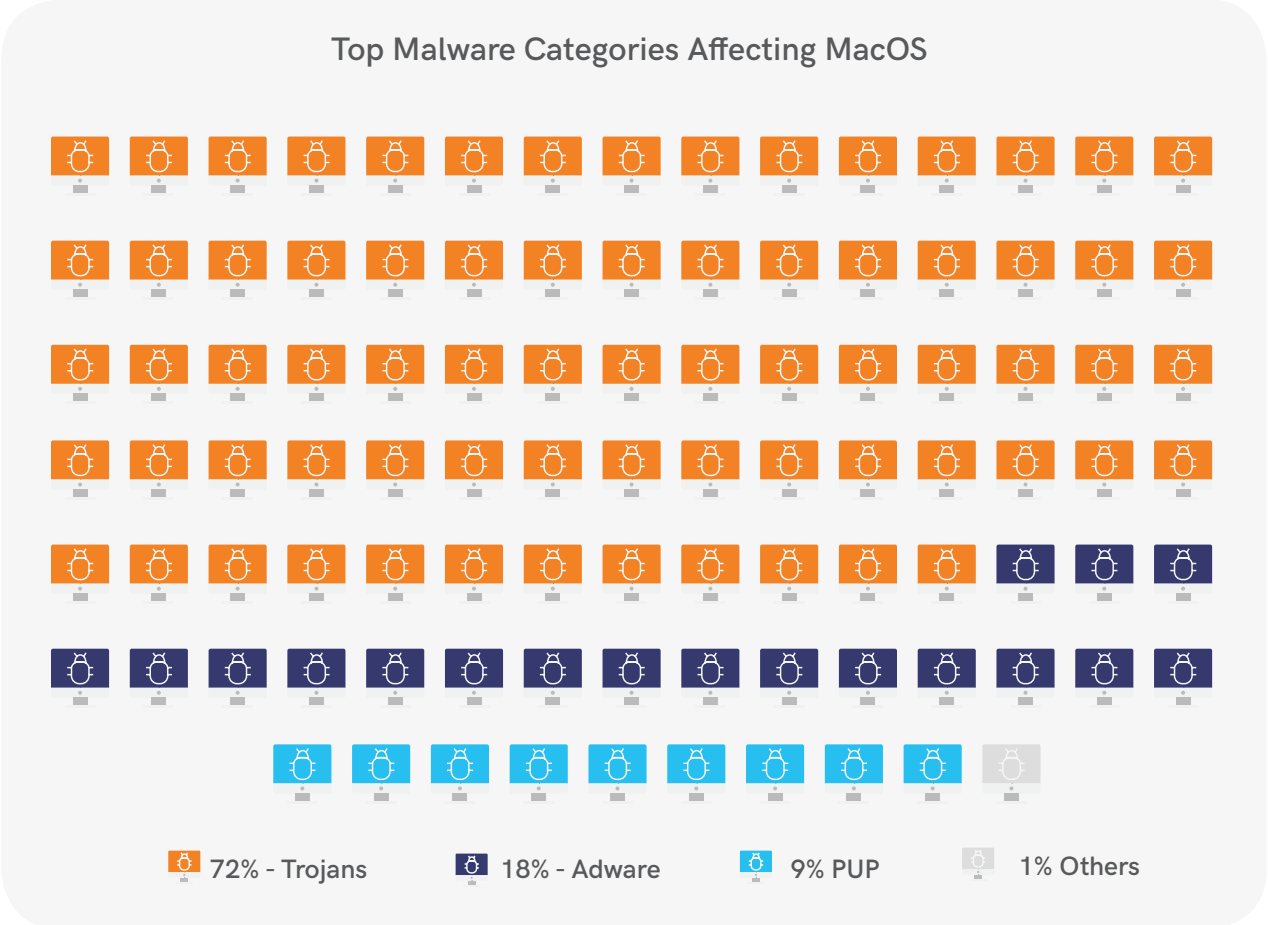
Mitigation Tips

- Install available patches and keep Windows up-to-date.
- Follow a regime for creating and maintaining an active password policy.
- Always use a strong and complex password for user authentication.
- Always use group policies to control the security settings of an enterprise environment.
- Change the system default RDP port.
- Avoid installing any third-party software. If necessary, download only through some trusted domain.
- Never use or encourage anyone to use a pirated operating system or software.
- Never click or forward any email links from any unacquainted source.
- Always lock down your system while you're away from your desk.
- Install a reputable Anti-Virus product, like K7 Endpoint Security or K7 Total Security, and keep it active and up-to-date.

MAC ATTACK

Cybercriminals are increasingly targeting Apple's homegrown operating system, macOS. Traditionally it has been the Windows OS which has been at the bullseye of most cyberattacks, but we have observed that macOS too is now under increasing attack. The closed nature of macOS doesn't seem much of a help as malware authors are developing Trojans, PUPs, adware, coinminers, spywares, keyloggers, and worms which are successfully compromising macOS users.

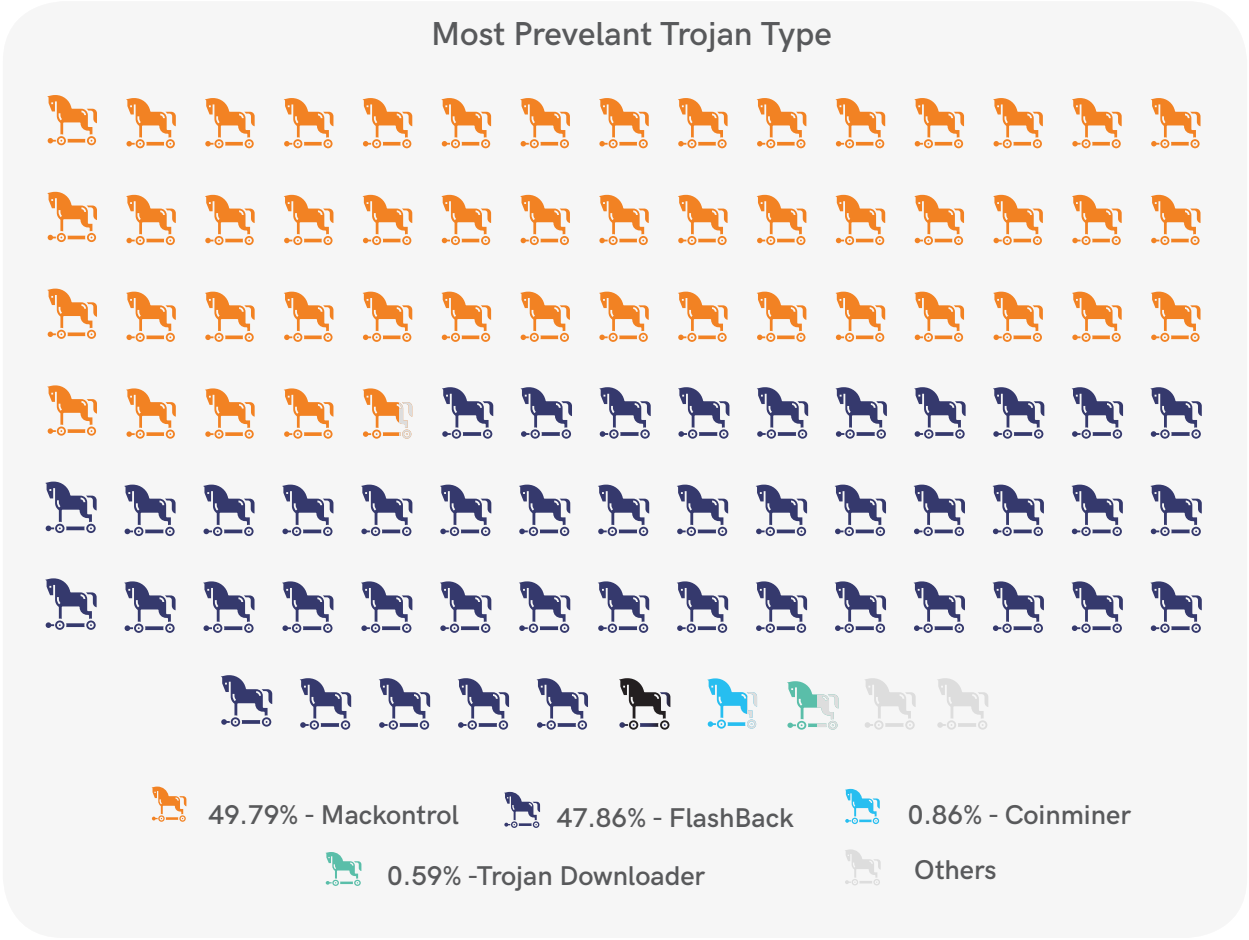
During the period K7 Labs has blocked a plethora of malware, out of which about 72% are categorised as different versions of Trojans. Of the total number of malware identified, around 18% is adware, while the Potentially Unwanted Programs (PUP or Potentially Unwanted Application/PUA) remained at 9%. Other categories of Trojans detected were of a small percentage, as depicted below.



The Reign of Trojans

Like on other platforms, adversaries are transforming their attack strategies for macOS users. Unlike before, coinminer and spyware attacks have decreased below 1% while the backdoor apps have spiked up (~50%), and ranked ahead of the others is the most visible botnet Trojan Flashback (48%) in this period. Malware masquerading as downloaders remained static, but exploits (0.01%), spyware (0.16%) and agent apps (0.12%) had surprisingly low visibility.

Interestingly a dated backdoor app dubbed MacKontrol was the most visible malware. This malware is known to be used in targeted attacks. It arrives on the system via a specially-crafted MS Word document which exploits the ancient CVE-2009-0563 vulnerability. This backdoor app collects system information and sends it to a remote server, and also accepts control commands to open a remote shell, delete or download a file, and can even shutdown or restart the system through a remote attacker. Since the vulnerability it exploits had been patched a long time ago, we're surprised to notice its persistence in doing the rounds.



Flashback too is an obsolescent botnet. It redirects the browser to a rogue website while surfing the internet. Once the user visits the rogue website, the java applet exploits the vulnerability and drops the malicious payload on the system. Once installed, Flashback can harm the user by installing other malware, helping in cybercrime activities like identity theft, and slowing down the infected system's performance. The significant reduction in coinminers might be an outcome of the official shutdown of numerous cryptocurrency exchanges or maybe just an aberration.

The Upsurge of Adware

Adware remains the most ubiquitous threat to the macOS platform.

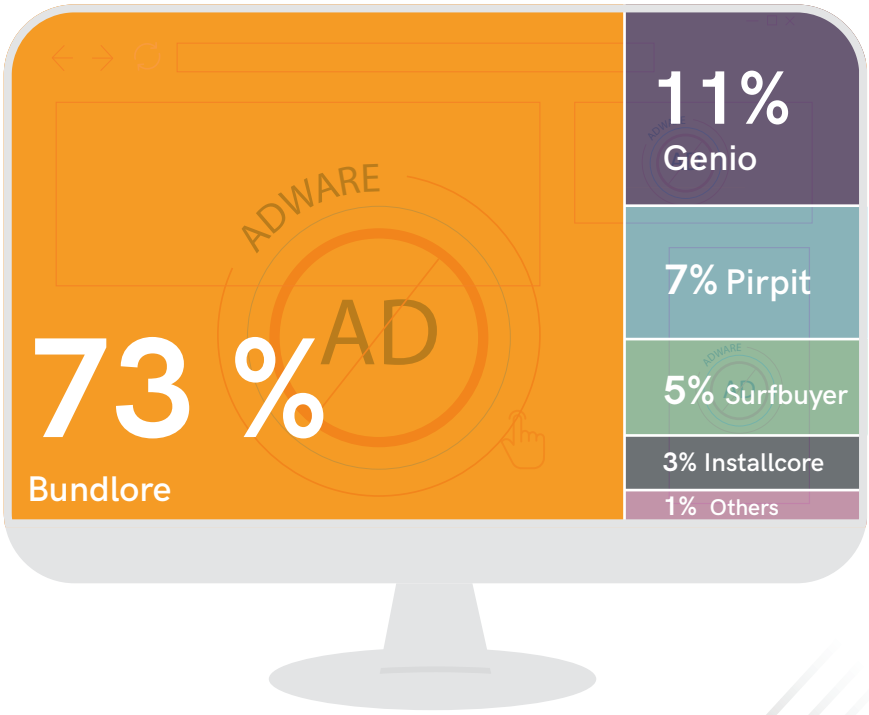
Adware applications like Bundlore, Genieo, Pirrit, and SurfBuyer were noticeable.

Cybercriminals found numerous techniques to attempt to hide their wares from analysis. We noticed numerous adware in the wild using encryption techniques to hide. A few of them even succeed in evading Gatekeeper, macOS' default security app.

One such Python-based suspicious app we found was written to inject advertisements and was obfuscated at several stages.

The following adware has masqueraded themselves as apps and tricked users into installing them.

Most Common Adware Variant Detections



For instance, Bundlore appears in the form of an installer for legitimate software. The installer usually bundles dangerous software such as spyware, adware, and various other harmful components. Adware like CinemaPlusPro, FlashMall, MyShopCoupon and many others pop up on your Mac display due to a BundLore infection. Once clicked, they can install more unwanted software on the system.

PUP/PUA apps categorised as unwanted applications usually gain notoriety for their deceptive marketing strategies. Besides impacting the system performance, they sometimes crash legitimate apps and surreptitiously install other dangerous software onto the systems without the user's knowledge.

Zero-day Rises

With the rising popularity of macOS powered devices, cybercriminals, especially notorious APT groups, are taking more interest in the platform. For instance, the Bangladesh Bank heist and Sony hack famed Lazarus group has taken down the DragonEx cryptocurrency exchange through a Mac remote attack. Besides, malware developers are crafting savage malware by exploiting zero-day vulnerabilities. Two recent targeted attacks involving zero-day flaws found on macOS GateKeeper and Firefox hint about the coming days.

Safety Guidelines

The most crucial step to protect systems from different sorts of cyberattack is to be aware of the problem and safeguarding techniques. Here are a few safeguarding procedures every macOS user should follow to block any cyberattack:

- Install applications only from the official App Store of macOS. We recommend you to stay away from any third-party app stores.
- Tweak your system settings to ensure your device updates itself whenever any new security update is available.
- Install a reputable Anti-Virus software, like K7 Antivirus for Mac, from a trusted vendor.
- Never click on any attachments or URLs embedded inside emails, unless you're pretty sure about the sender's intention.
- Activate TimeMachine backup on your system and use it once a month to back up your system data.

Over the past few months, we have seen a long list of Android Potentially Unwanted Programs (PUPs)/Potentially Unwanted Applications (PUAs) and Trojans manifest themselves. Instead of executing attacks through specially-crafted applications, threat actors now prefer to develop veiled apps available through both official and unofficial app stores. For better penetration, threat actors prefer to deliver deceptive PUPs under specific categories which are immensely popular among users, e.g. photo editors, beautification filter apps, music players and equalisers to name but a few. Alongside, fake monitors or spying apps and fake Anti-Virus apps are also two popular app categories used by cybercriminals to infect the users' devices. During the quarter, we found PUPs/ PUAs in Google Play Store as well.

The Android Security Mashup

Digging further, we found the threat actors used packers like Jiagu, DingXProtect, and TencentProtect to hide unhealthy codes within the apps.

Alongside these highly visible PUAs, we noticed an interesting PUP disguised as an app from the famous Indian network provider "Jio" spread itself aggressively in the country. The PUP claims to offer new and exclusive offers for Jio mobile users. Dubbed Jio-4G-Offer, here's how the app behaves.

SCENE 1

TRICKS VICTIM THROUGH A CAMOUFLAGED APP FROM 3RD PARTY MARKET

SCENE 2

WITHOUT VICTIM'S KNOWLEDGE

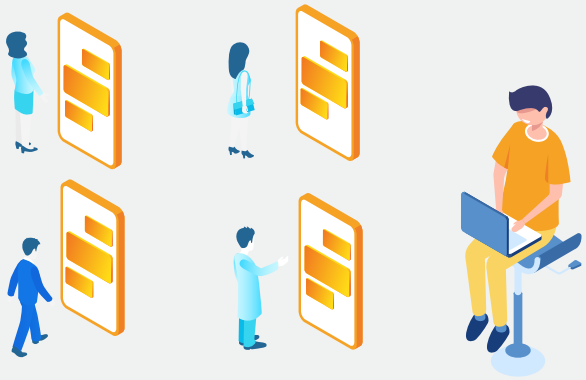
COLLECTS ALL THE CONTACTS ARCHIVED ON THE VICTIM'S DEVICE

SCENE 3

FILTERS ALL THE JIO MOBILE NUMBERS THAT EXIST IN CONTACT LIST

CLIMAX

PUSHES PHISHING MESSAGE SENT TO EACH JIO USER FOUND IN THE LIST



The Territory of Trojans

According to our telemetry data, Trojans disguised as legitimate apps took a sneaky swipe in a few regions and remained a more effective tool for executing attacks and targeting users' devices.

An Android Trojan named Andr.Troj.Agnt remained the most prevalent in comparison to its malware playmates. This Trojan is capable of stealing and transmitting device data to remote servers and can turn the device into a Distributed Denial of Service (DDoS) bot, allowing it to be controlled remotely by hackers. The Trojan can also hide by suppressing the creation of an app icon and listing itself with a generic name in the installed app list. Sometimes it can also impersonate a system app to avoid identification.

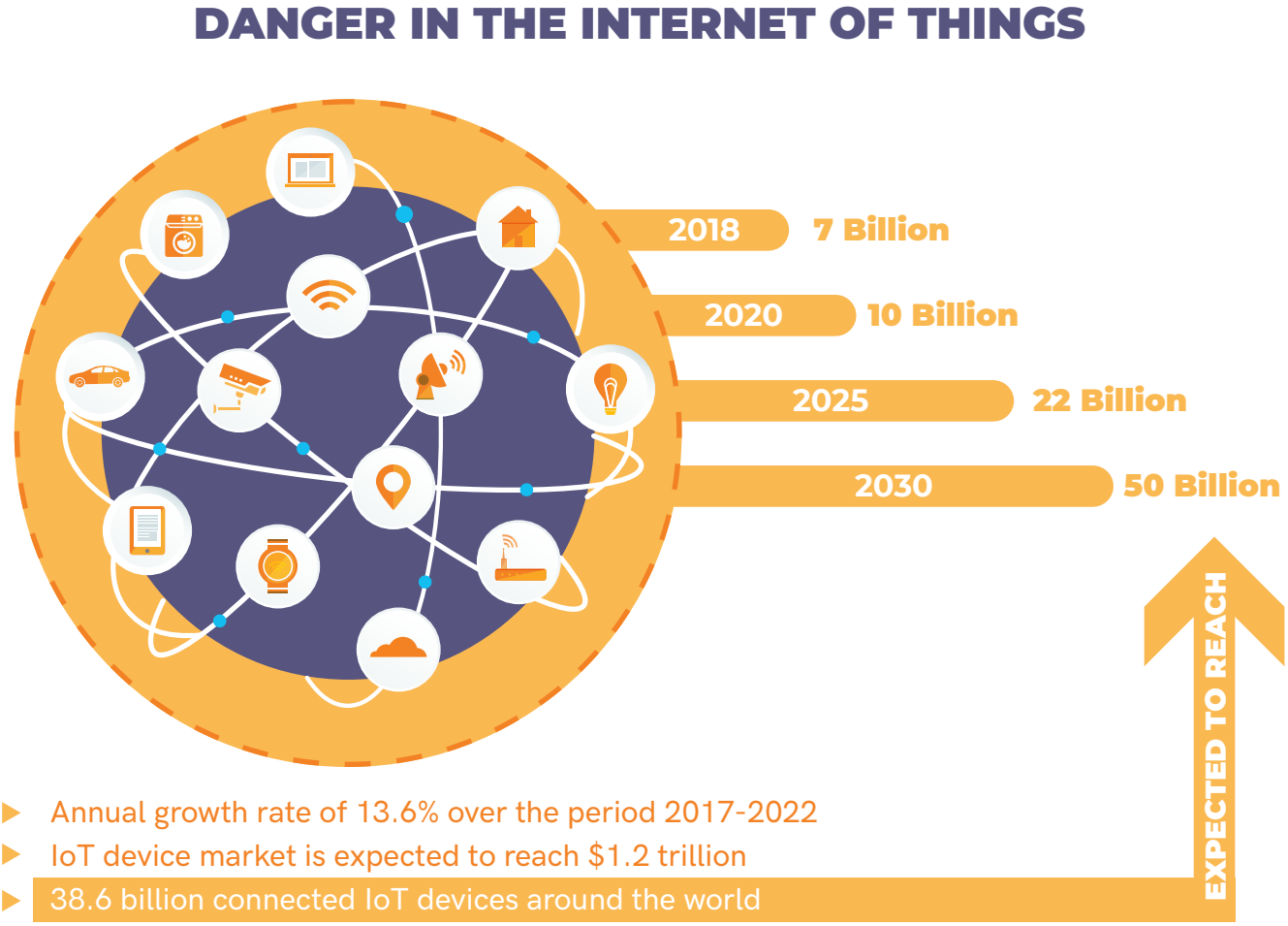
Two other noteworthy Trojans spotted during this period were Andr.TrojDload.Agnt and Andr.TrojDrop.Agnt. As the names denote, these Trojans are capable of downloading or dropping other malicious apps on to a victim's device.

Tips to Stay Safe

- Install apps only from the official app stores (Google Play Store in the case of Android and Apple store for iOS).
- Refrain from downloading applications that you do not need.
- Always verify the reputation of the application by checking the reviews available before downloading it.
- Never install apps recommended by strangers.
- Carefully analyse the messages or alerts received before installing any app, especially related to permissions that an app is asking for on the device.
- Regularly update the mobile OS and security application installed to stay clear of mobile malware.
- Install a top-notch mobile security app such as K7 Mobile Security to block all kinds of infections.
- Avoid using free Wi-Fi hotspots, in particular those that are not password-protected, especially for sensitive financial transactions.
- Delete apps that are flagged by a security product and never ignore any malware/unusual behaviour alert from security products.

DANGER IN THE INTERNET OF THINGS

There's an undeniable upsurge of IoT (Internet of Things) devices around us. Smart devices that promise to make life easier are growing manifold in both the personal world, in enterprises and, of course, in the smart cities of the future. Recent Research claims that there were 7 billion IoT devices around the world in 2018. This huge number is expected to grow to 10 billion by 2020 and 22 billion by 2025. The count includes both consumer and enterprise IoT devices and purportedly excludes smartphones, tablets, and laptops. The International Data Corporation (IDC) forecasts that, with an annual growth rate of 13.6% over the period 2017-2022, the IoT device market is expected to reach $1.2 trillion, while Strategy Analytics claims there will be 38.6 billion connected IoT devices around the world, expected to reach 50 billion by 2030.



Obviously, such an eye-popping expansion in connected devices in the consumer, retail, and enterprise sectors expand the attack surface, encouraging threat actors to exploit IoT vulnerabilities in several critical and damaging cyberattacks.

Most IoT attacks are currently related to the hijacking of devices, including your typical household Wi-Fi routers, using them as a part of a botnet to launch large-scale Distributed Denial of Service (DDoS) attacks to take down entire targeted networks. An important fact is that routers are very much part of the set of IoT devices likely to be ubiquitous; wherever one might find Wi-Fi networks, e.g. your home, your office, the train station, airports, hotel rooms. Cybercriminals also take possession of the IoT devices via various methods to install coinmining malware which consume system resources to mine digital cryptocurrencies. It is important to note that devices infected with coinminers may not show any visible suspicious activity except offering snail-slow performance and heating up often.

On the other hand, a massive number of IoT device manufacturers and users are still ignorant about the necessity of optimised security, thus inviting massive-scale attacks.

Following the horrorsome Mirai botnet debuted in August 2016, numerous variants of it have been spotted in the wild. All these variants usually come with the sole intention of infecting IoT endpoints, especially home routers, using them for executing malicious activities without the owners' knowledge.

In 2017 BrickerBot launched a nationwide attack affecting over 60,000 BSNL and MTNL modems and routers across India. The BSNL authorities claimed that the malware had attacked modems where users had not bothered to change the device's default credentials, i.e. the credentials used to access and set up the brand new device out-of-the-box. Another common issue would be the use of common or weak passwords which allow easy credential brute-forcing for an attacker to obtain unauthorised remote access to the device and control it at will.

Though the Mirai developer has been arrested, its source code released to the public inspired fellow threat actors to develop similar sophisticated botnets. Tori-Botis, the IoT botnet powered with six different persistence techniques and a capacity to infect multiple computer architectures, is a good example of this.

In 2018, VPNFilter, a multi-stage malware, compromised more than a million home, small office and NAS devices. IoT botnets like VPNFilter and Hide and Seek usually infiltrate the device using brute-force tactics and launch attacks in multiple stages. Alongside routers and Android-powered smartphones, lakhs of smart TVs, DVRs, close-circuit cameras and many other embedded devices connected to Wi-Fi are infected worldwide through these botnets.

Considering the disruptive power of IoT botnets, state-sponsored threat actors or APT groups are increasingly using similar attacks to take down several IIoT (Industrial Internet of Things) networks such as large banking bodies, government enterprises, hotel chains, manufacturing companies, and utilities and natural resource companies. Many IoT devices, such as printers, lack essential security features to protect them against cyber threats which, at times, makes them the weakest link exploited in the attack chain. Running a quick query using an Open Source Intelligence portal called Shodan, we found nearly half of the printers connected to a home network in India have a weak password, alongside IP cameras and smartphones. We also found that many printers in the country are directly reachable over the internet.

However, we have reason to believe that routers are the most vulnerable IoT devices existing in the country, followed by printers, NAS, IP cameras, media players, set-top boxes, and smart TVs.

Mitigation Techniques

The large variety of IoT botnets indicate that threat actors are becoming more sophisticated and resourceful with their attack vectors and choice of target. Hence users and enterprises should adopt necessary safeguards to ensure adequate protection of the entire network containing IoT devices. Here is a list of recommendations:

- Buy IoT appliances and routers from reputable device manufacturers with decent security features.
- Never use default configurations. Configure the routers properly.
- Use a complex and different password for each of your IoT gadgets, and update these passwords at regular intervals.
- Update the device firmware whenever available. You should also keep a tab on other IoT gadgets and update/patch each of them.
- Install a firewall in front of your network and configure it properly to prevent unwanted traffic flow, and block non-essential ports and services.
- Block unwanted ports and disable non-essential services on your devices.
- Filter both incoming and outgoing data traffic on all existing channels in the network.
- Maintain a list of all external blacklisted IPs which can be provided by reputable threat intelligence providers such as K7 Security
- Establish and maintain a vulnerability and patch management program.

KEY TAKEAWAYS

The National Infection Rate for Q1 2019-20 is roughly 30%, based on K7 Security's proprietary telemetry data, meaning that almost 1 in 3 Indian users were under cyberattack during the period. In this report we covered several types of attack that K7 Labs has tracked, across platforms and devices, backed by real threat-event data, and we recommended several best practices to remain safe whether you're an enterprise or a consumer.

Here is a summary of our top 3 recommendations by user segment, keeping in mind, as usual, that what is relevant for consumers is perhaps even more critical for enterprise users.

	Enterprise	Consumer
1	Ensure all systems existing on the network are up-to-date with respect to critical security patches for OS and applications, and, of course, endpoint security software	Install apps only from trusted domains (Windows) and from the official mobile app stores (Android and iOS)
2	Monitor network and system logs and security notifications to deal with any malicious activities on the network. Never ignore security alerts	Activate auto-update to ensure the OS and applications installed on your devices are up-to-date. Never use or encourage anyone to use pirated operating system or third-party software
3	System Admins should actively monitor and filter data coming in and out of each system to spot anomalies	Never click or forward any email links coming from unacquainted sources

CONFIDENCE IN AN INSECURE WORLD

K7 SECURITY

www.k7computing.com

Aug 2019