Quick Heal

QUARTERLY THREAT REPORT Q1 2023

www.quickheal.co.in

About Quick Heal

Quick Heal Technologies Ltd. is one of the leading IT security solutions company. Each Quick Heal product is designed to simplify IT security management for home users, small businesses, Government establishments, and corporate houses.

About Quick Heal Security Labs

A leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

Contributors

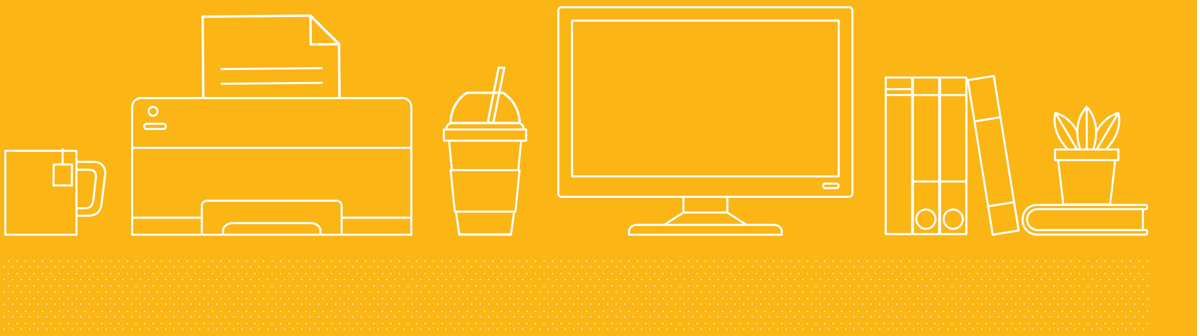
Quick Heal
Security Labs

Quick Heal
Marketing Team

Follow us

For an overview of the latest security threats and trends for enterprises, please refer to the threat report by Seqrite, enterprise security brand of Quick Heal Technologies Ltd. Visit **www.seqrite.com**

TABLE OF CONTENTS



FOREWORD

The Cybercrime frontier is a hot-bed of activity, with malicious actors continuing to evolve and adapt to new circumstances. As we deep-dive into the first quarter of 2023, several trends have surfaced. A technological landscape that is abuzz with a host of new and emerging trends threatening individuals and businesses alike.

At the forefront, Ransomware attacks continue to be a significant concern as is evident with the expansion of Royal Ransomware. Additionally, newer variants and novel attack techniques have brought to light that malware is finding ways to bypass traditional admin security measures. Furthermore, attackers are now exploiting both new and old software vulnerabilities.

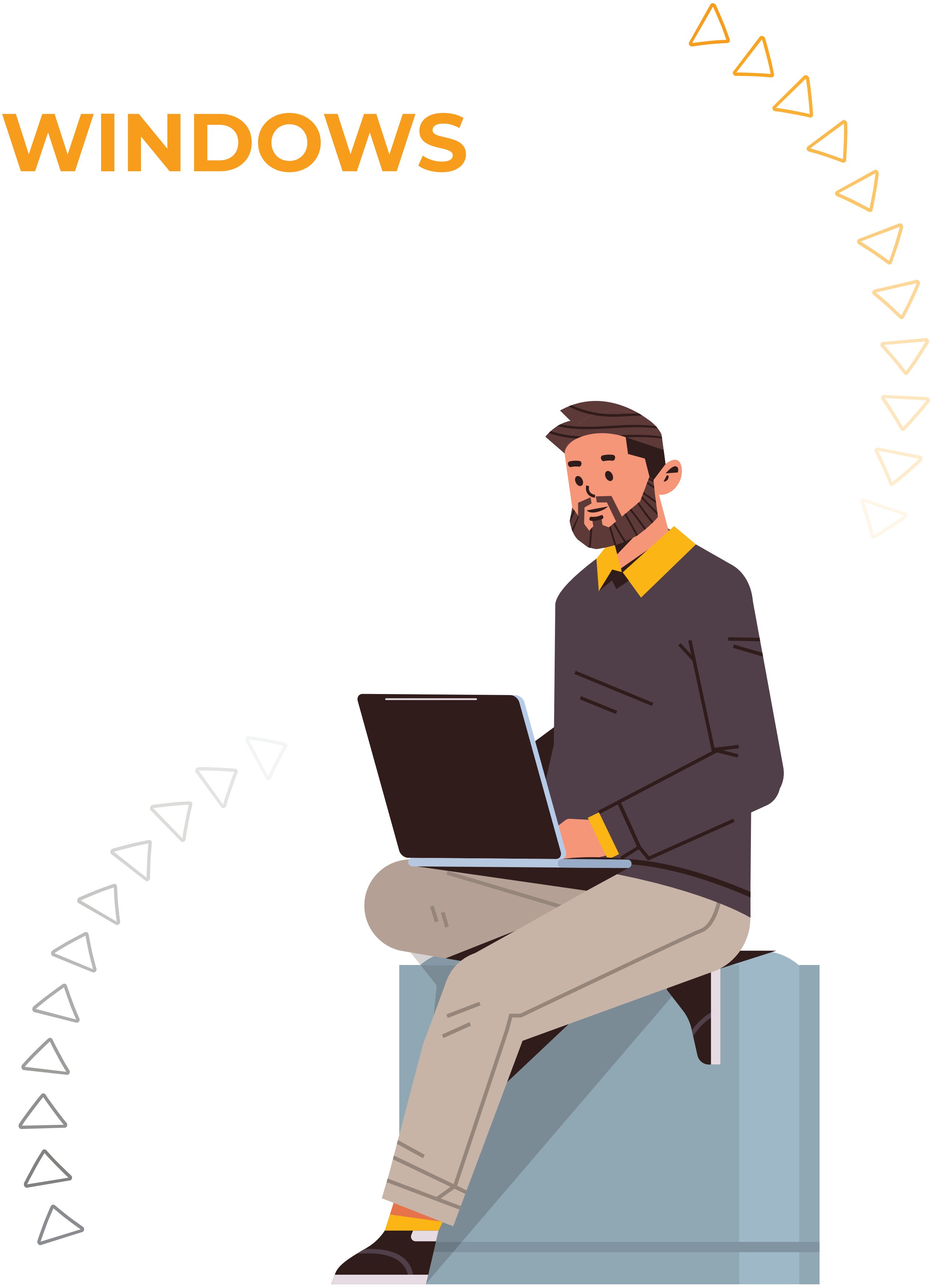
It is also noteworthy that while some types of attacks, such as Windows malware and ransomware, have gone down this time as compared to last year's first quarter, others, such as PUA and Adware, have increased.

Moreover, with the introduction of ChatGPT early-on this year, the threat landscape has also become an arena of an ongoing debate. While criminals have begun employing sophisticated capabilities of Artificial Intelligence and machine learning tools to gain the upper hand, cyber security experts are also deploying the same technology to counter these attempts and keep systems safe.

Amidst this fluid landscape, it has become more important than ever for businesses and individuals to remain vigilant in their cybersecurity efforts. The importance of regularly updating security measures and staying informed about new and emerging threats cannot be emphasized more.

In our efforts to empower your digital lives and help you stay ahead of emerging threats and challenges, we have collated this report for you. Read on to gain a deeper insight and stay one step ahead of cyber threats.

WINDOWS



QUICK HEAL
Threat Report Stories Q1

(Jan-Mar 23)

01

DEEP DIVE INTO ROYAL RANSOMWARE

⚠ Criticality: **High**

Countries, States, Regions: US, Canada, UK, Brazil
Sector targeted: IT, finance, materials, healthcare, food and staples industries.

Royal Ransomware has expanded its reach to include Linux ESXi servers, which can have devastating consequences for businesses and organisations. This new strain of ransomware specifically targets virtual machines, which are critical components of many organisations' IT infrastructures. By targeting these servers, the attackers can potentially access and encrypt data from multiple virtual machines simultaneously, causing significant disruption and the possible loss of data. The success of these attacks is due in part to several critical vulnerabilities in VMware software.

The new variant of Royal Ransomware is often distributed through phishing emails, torrent sites, and malicious attachments. Once it infects a system, it encrypts all volumes, including network shared drives, and appends the "Royal" extension. In the newer variant, they have used "Royal_w" and "Royal_u," where the first is for Windows and the latter for Linux. Its unique ability to modify the encryption percentage of files, makes it more difficult to recover encrypted data.

Organisations must take proactive steps to protect their systems against such attacks, and ensure that their software and security systems are up-to-date. We recommend regular patches, along with the implementation of strong access controls, frequent backups, and secure storing of data offsite. It is essential that organisations remain vigilant, stay abreast of the latest security trends, and secure all systems against potential attacks.

02

UAC BYPASS USING CMSTP

Criticality: **Medium**

Countries, States, Regions: **Global**

One of the key challenges in any malware attack is the way attackers are able to achieve administrative privileges on the system. While this can be done through several different techniques, it is observed that attackers are more inclined towards the UAC in recent times.

User Account Control (UAC) is a built-in security mechanism that displays a prompt whether to elevate the program to an administrator mode or not. However, attackers can bypass UAC without the victim's knowledge, using techniques such as changing the registry key, DLL hijacking, or targeting genuine Windows application program COM interfaces.

One specific technique used by popular ransomware like Lock bit 3.0 and BlackCat is the use of Microsoft Connection Manager Profile Installer (CMSTP) COM objects for UAC bypass.

CMSTP is a command-line tool used to install connection manager service profiles and is a signed file normally located in "..\System32\cmstp.exe" or "..\SysWOW64\cmstp.exe." Adversaries use malicious INF files with commands to bypass UAC and gain admin privileges, or they may use CLSIDs of CMLUA, CMSTPLUA, or link CMLUA.dll at runtime to achieve the same outcome. This technique is difficult to detect and can easily bypass antivirus engines as it uses a genuine Windows application.

03

ONENOTE EXPLOITS: THE LATEST WEAPON IN CYBERCRIME

⚠ Criticality: **High**

Countries, States, Regions: India, China, European countries, America and some part of Africa
Customers affected: More than 100

In the past few months, a new malware distribution method has emerged that is causing havoc among OneNote users. The attackers have been disguising malware as a OneNote file, and sending it through email or other messaging platforms. Once the file is downloaded and opened, the malware is activated, giving the attacker access to the victim's device and potentially sensitive data.

Multiple RATs (Remote Access Trojans) like AsyncRAT, Quasar RAT, and NetWire have been seen using OneNote files. Most of these OneNote files contain batch scripts that will download the payload using PowerShell. Malware families like QBot, IcedID, and Emotet have also explored this file type. For the QBot campaign, the OneNote file contains obfuscated ".hta" files that will download DLLs. For the Emotet campaign, the infection chain is different. Here, the OneNote file contains obfuscated VBScript with a ".wsf" file extension, which is hidden from end users. This file will download Emotet DLL from a compromised website.

04

MALWARE GOES VIRAL VIA GOOGLE ADS

⚠ Criticality: **High**

Software targeted: Adobe, Zoom, AnyDesk, Notepad++, Bluestacks, ChatGPT, Spotify
Countries, States, Regions: Global

Google Ads are often used by malware authors to redirect users to phishing websites that have the potential to download and spread infection. This is done through software impersonation, which involves creating lookalike websites that host Windows installer files masquerading as legitimate software. Users are then tricked into downloading and installing these type of files, which triggers the infection sequence. They mimic popular software such as Zoom and Notepad++ and can also be spread via spam emails containing such attachments.

Another example is the MalVirt cluster of virtualized malware loaders, which implement a range of anti-analysis and anti-detection techniques to distribute malware from the Formbook family. These loaders are written in ".NET" and use the KoiVM virtualizing protector for obfuscation. In addition to these threats, the malware downloader known as BATLOADER is also seen to be abusing Google Ads to deliver secondary payloads like Vidar Stealer and Ursnif. The ads are designed to spoof legitimate apps and services, such as Adobe and Spotify, and the MSI installer files execute Python scripts containing the BATLOADER payload to retrieve the next-stage malware from a remote server. Finally, dotRunpeX is a new ".NET" injector that is actively being developed to distribute numerous known malware families, including Agent Tesla, LokiBot, and Rhadamanthys. It uses the Process Hollowing technique to infect systems and is a cause for great concern amongst cybersecurity experts.

05

EXPIRO: OLD VIRUS POSES A NEW CHALLENGE

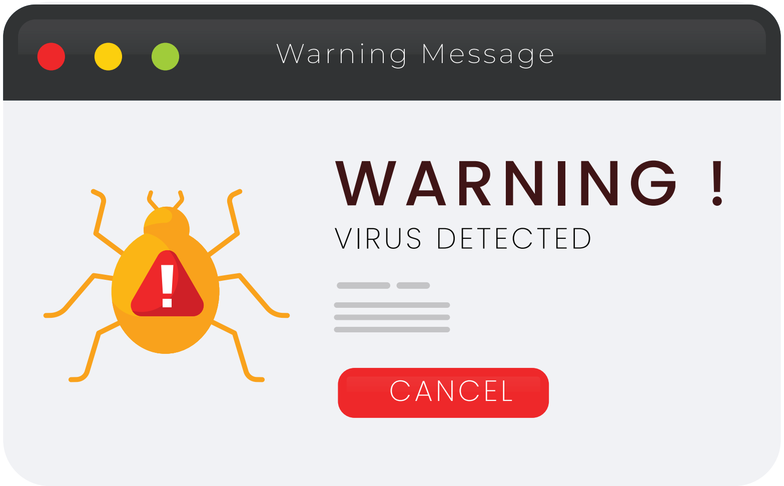
Criticality: **High**

Countries, States, Regions: **South Asia**

We have also observed a new variant of the Expiro virus that is infecting executable files on the system by appending virus code at the end of those files. This new variant of Expiro appears to patch any call in the executable section. Upon execution, the infector code is run, and the malicious call is patched with a new address to run the benign code.

It is difficult to restore the file to its original offset since the overwritten code is kept compressed and encrypted. This further gets decrypted during runtime because of the highly obfuscated decompression and decryption routines. The infection routine is implemented in such a way that the user applications will run as normal, without the user's knowledge.

This variant of Expiro has the capability to check network-mapped drives and infect executable files present on those drives as well, which may result in spreading the infection across the network. We have also observed this variant performing backdoor capabilities by connecting to remote servers. Expiro is able to receive commands from remote servers and execute them on the infected system. This includes installation of other malware on the system that could steal and upload sensitive information to the servers.



06

MYLOBOT: THE BOTNET THAT IS INFECTING DEVICES WORLDWIDE

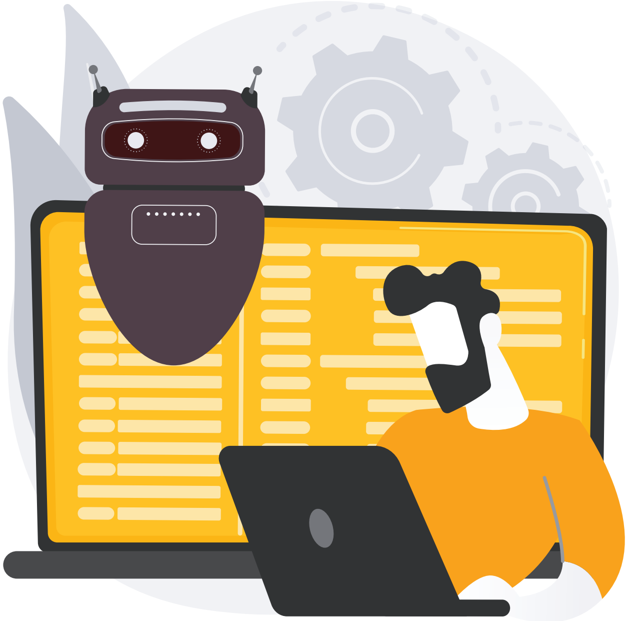
⚠ Criticality: **High**

Countries, States, Regions: **Global**
Customers affected: **50,000 daily infections**

A sophisticated botnet known as MyloBot has compromised thousands of systems, with most of them being reported in India, the U.S., Indonesia, and Iran. Currently, we see more than 50,000 unique infected systems every day, which interestingly shows a decline from a high of 250,000 unique hosts in 2020.

MyloBot, which emerged in 2017, is known to employ a multi-stage sequence to unpack and launch the bot malware. Notably, it also sits idle for 14 days before attempting to contact the command-and-control (C2) server to sidestep detection.

The primary function of the botnet is to establish a connection with a hard-coded C2 domain embedded within the malware and await further instructions. When Mylobot receives an instruction from the C2, it transforms the infected computer into a proxy. The infected machine will be able to handle multiple connections and relay traffic sent through the C2 server. Analysis of MyloBot's infrastructure has revealed several connections to a residential proxy service called BHProxies.



07

CHATGPT: THE LATEST WEAPON IN CYBERCRIMINALS' ARSENAL?

⚠ Criticality: **High**

Countries, States, Regions: **Global**

OpenAI's release of ChatGPT, the new interface for its Large Language Model (LLM), was received with an instant flurry of interest in AI and its possible uses. However, ChatGPT has added major seasoning to the modern cyber threat landscape, as it quickly became apparent that code generation through it could help less-skilled threat actors effortlessly launch cyberattacks.

A thread named "ChatGPT – Benefits of Malware" soon appeared on a popular underground hacking forum where experiments with ChatGPT were being discussed to recreate malware strains and techniques described in research publications along with write-ups about common malware. As an example, the publisher shared the code of a Python-based stealer that searches for common file types, copies them onto a random folder inside the Temp folder, zips them, and uploads them to a hardcoded FTP server.

However, at this point it remains to be seen how widespread the use of ChatGPT will be among cybercriminals, and whether it will lead to a significant increase in the overall volume of cyberattacks. Nonetheless, this development underscores the need for increased vigilance and security measures to protect against emerging threats in the cyber landscape.

WINDOWS

- 87 Million Windows Malware detected in Q1 2023
- 29 Million Windows Malware detected in Mar’23
- 0.96 Million Malware daily average detected in Q1 2023

Windows Detection Statistics Q1 2023

Malware

87 Million

Per Day: 0.97 Million

Exploit

4.68 Million

Per Day: 51, 414

Ransomware

0.10 Million

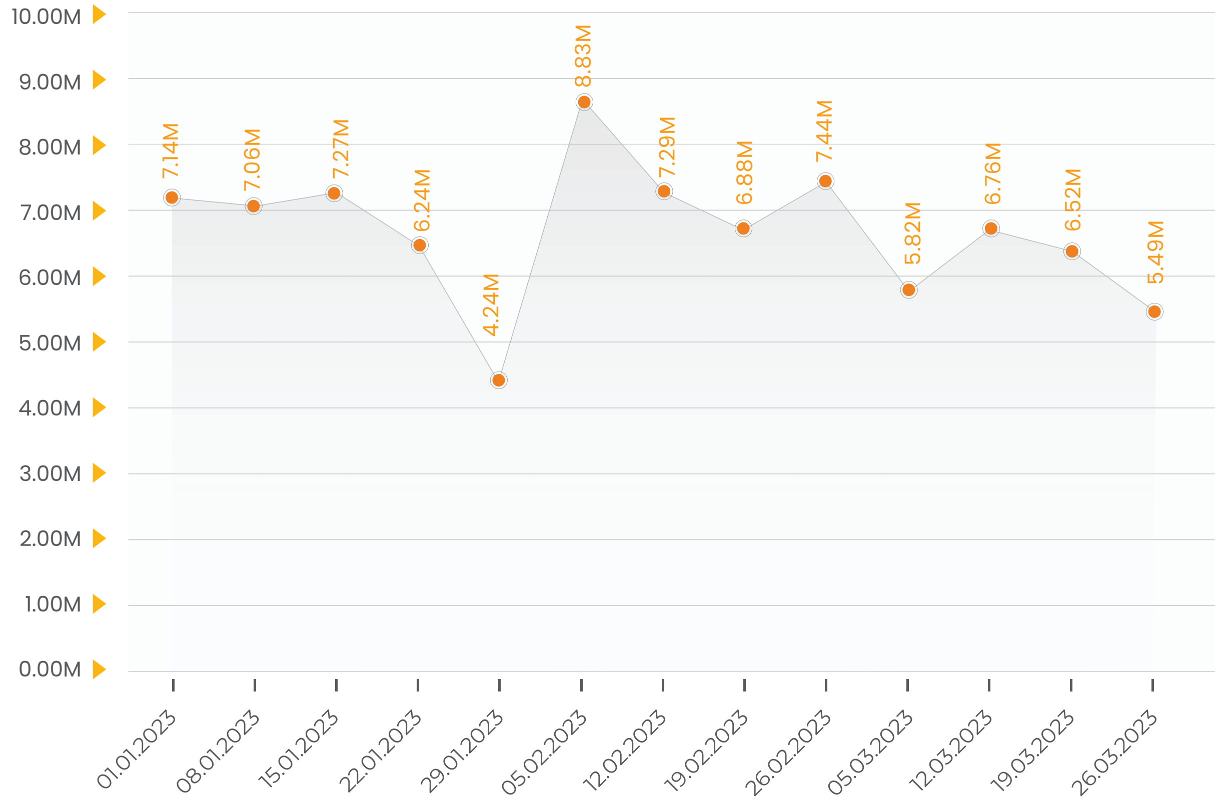
Per Day: 1100

PUA & ADWARE

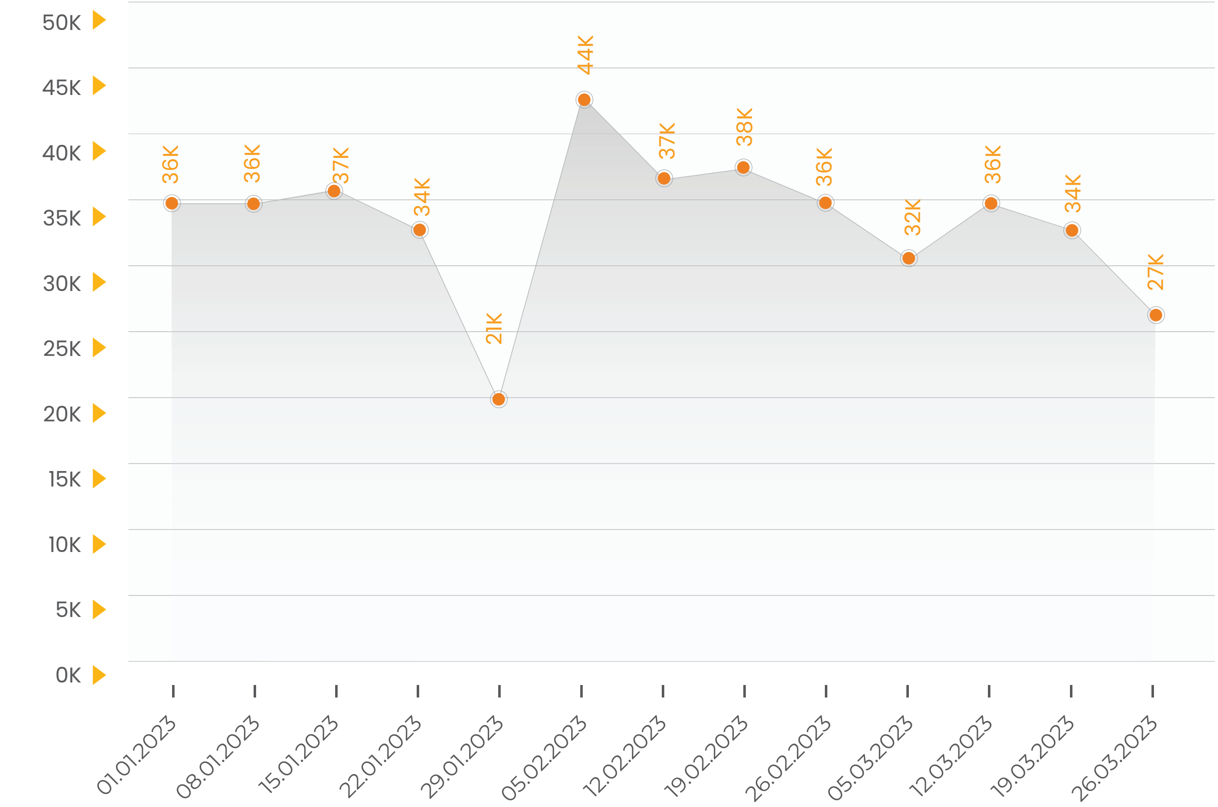
5.06 Million

Per Day: 55, 590

Detection Statistics Week-Over-Week

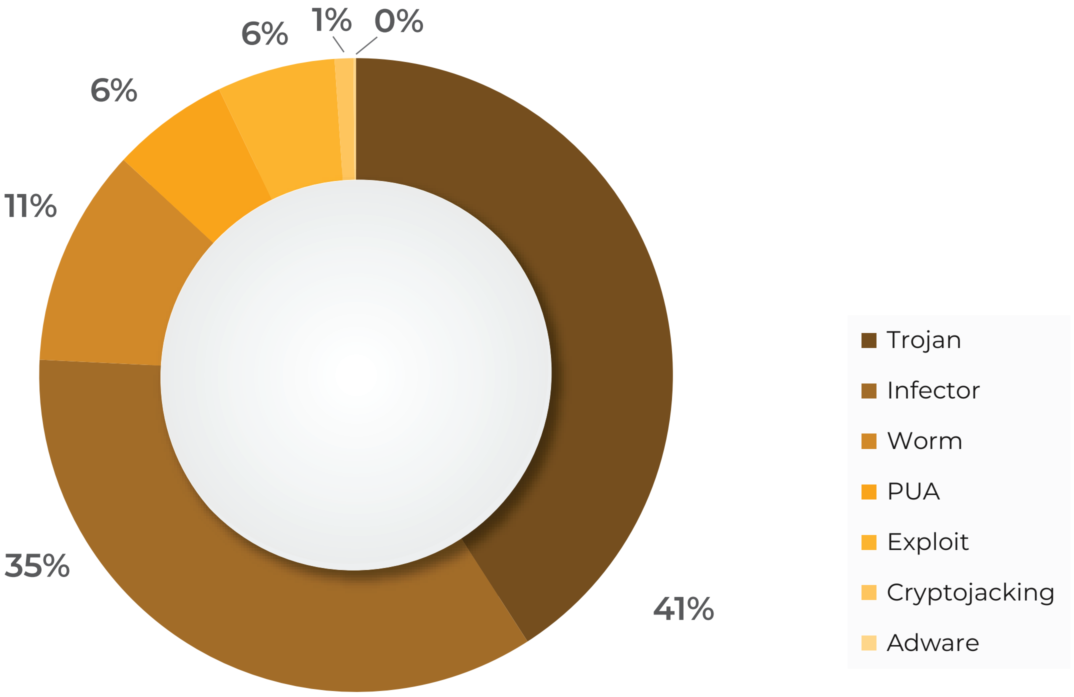


Ransomware Week-Over-Week

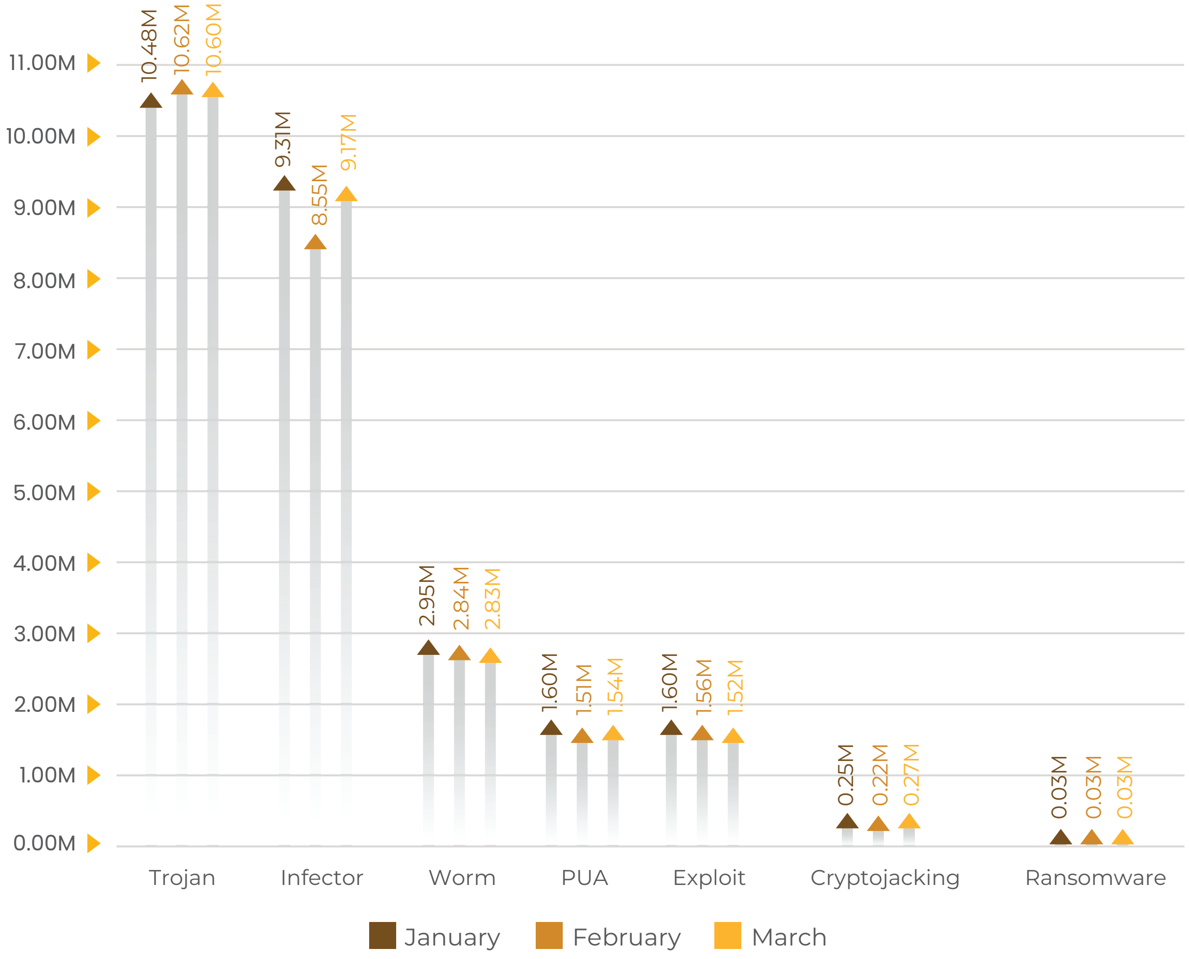


Detection Statistics **Category Wise**

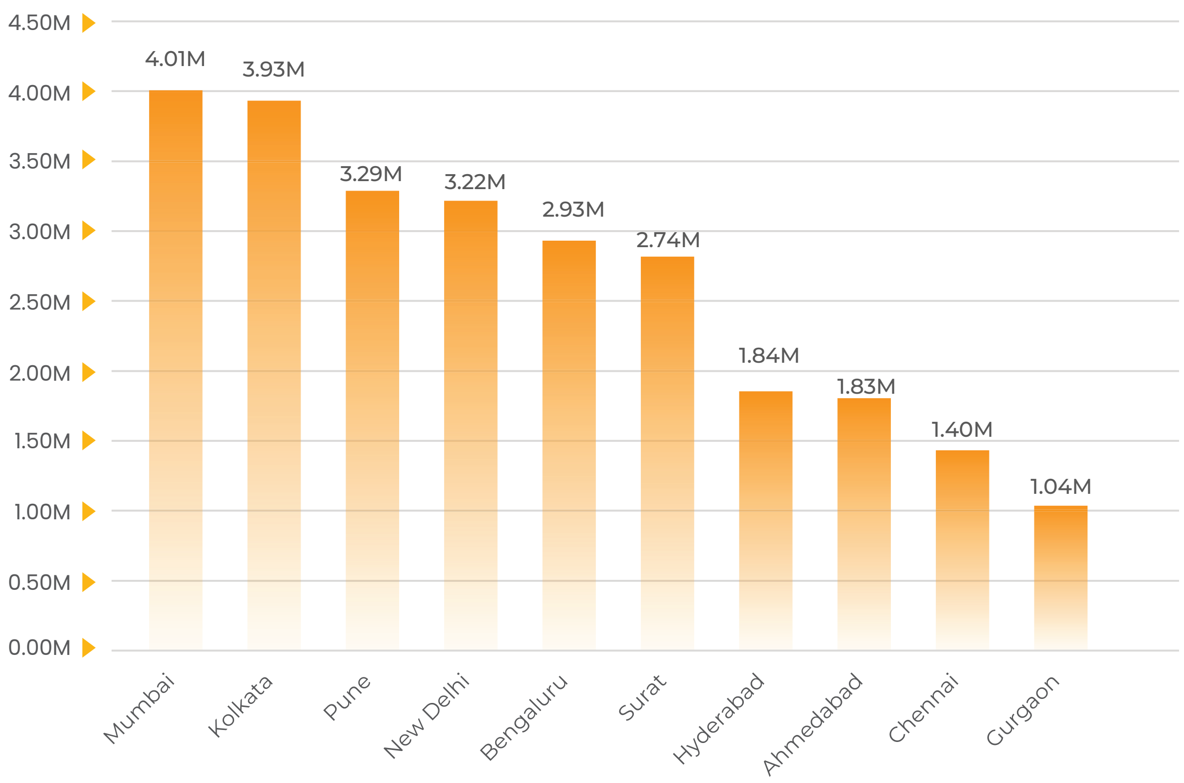
A) Malware Categorization



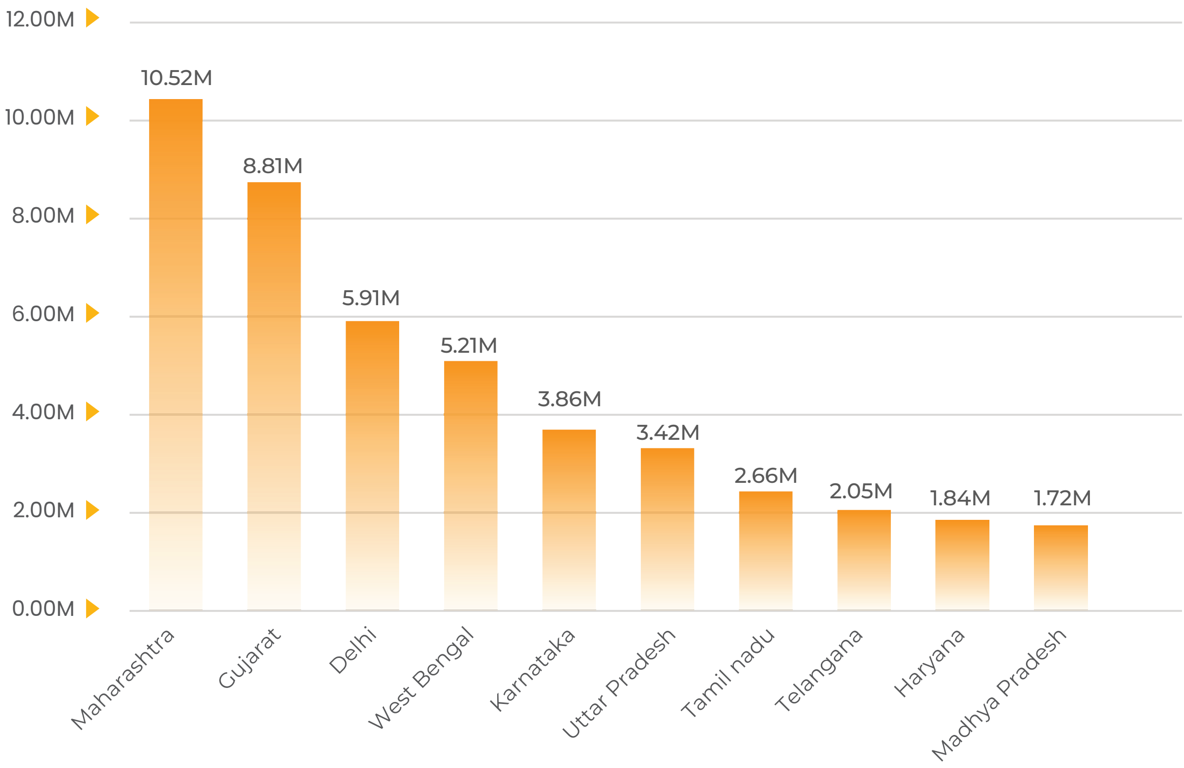
B) Month-wise Categorization



Top 10 Affected Cities



Top 10 Affected States



ANDROID

QUICK HEAL
Android Stories Q1

↓ (Jan-Mar 23)

01

FAKECALL: BANKING MALWARE STRIKES VIA VISHING

⚠ Criticality: **Medium**

Countries, States, Regions: South Korea

Threat actors are continuously improving their techniques to trap users. Lately "Vishing" is a technique that is being widely used. It involves social engineering through fake calls that are initiated under Banking Trojans.

First, it uses a bank icon or customer support icon to get into the user's device. When the victim tries to connect to the customer support of the bank, it disconnects the call and opens a fake page which makes it seem that the call is still going on with the legit customer support. Meanwhile, the call is connected with the threat actor or a pre-recorded conversation is played. Victims often fall for this scam, and end up revealing their personal and financial information.

This technique has the capability to capture live audio and video streams from the device’s camera and send them to C&C servers. It uses different anti-analysis and obfuscation techniques to avoid detection.

Quick Heal detects this malware and other variants of Android.Fakecall

02

BANKING MALWARE EVOLVES: NEW VARIANTS WITH NEWER CAPABILITIES

⚠ Criticality: **High**

Countries, States, Regions: Brazil, US, Canada

Variants of existing banking malware have been a major threat for this quarter as well.

Pixpirate banking malware is one such variant that has been targeting Brazilian bank payment apps. We have observed that it asks for accessibility permission and uses JavaScript for its working. It also intercepts SMS, prevents un-installation, and displays rogue ads via push notifications.

Another variant is Xenomorphs. These appear to hav evolved into a new version which has added multiple new capabilities. It is now able to completely automate the entire fraud chain to become a more powerful, and dangerous banker malware, with devastating impact.

Quick Heal detects these banking malwares - Android.Banker, Android.Hqwar and Android.Agent.

03

SUBSCRIBER TROJAN : HARLY

⚠ Criticality: **Medium**

Countries, States, Regions: Global

Similar to the Joker malware, threat actors modify legitimate apps, insert malicious code, and then upload them to the Google Play store. These are infected with malicious payload and different methods are used to decrypt it. They usually have the capability to collect information about the user’s device, or any related to the mobile network and more. The application configures the list of subscriptions for signing up after switching on the Carrier Internet service on the mobile.

Quick Heal detects this malware and other variants of Android.Harly.

04

ALERT: SPYLOAN APPS NEED IMMEDIATE ATTENTION

⚠ Criticality: **Medium**

Countries, States, Regions: India, Brazil and Mexico.

Loan applications operate by offering small loans without requiring much paperwork, but charge heavy interest rates. In return, they get access to the user's contact details, SMS, storage, and camera access which makes it possible for them to harass the user into repaying the loan.

Recognizing this menace, RBI has issued new guidelines to prevent such applications from accessing irrelevent information about users. Google Play Store has also come up with a new policy for such loan applications.

Quick Heal is able to warn users by detecting such Potentially Unwanted Applications (PUA) and detects them as Android.Spyloan

Android Malware Detections for Q1 (Jan-Mar 23)

Malware	Adware	PUP
9688	9557	8670
Per Day: 106	Per Day: 105	Per Day: 95

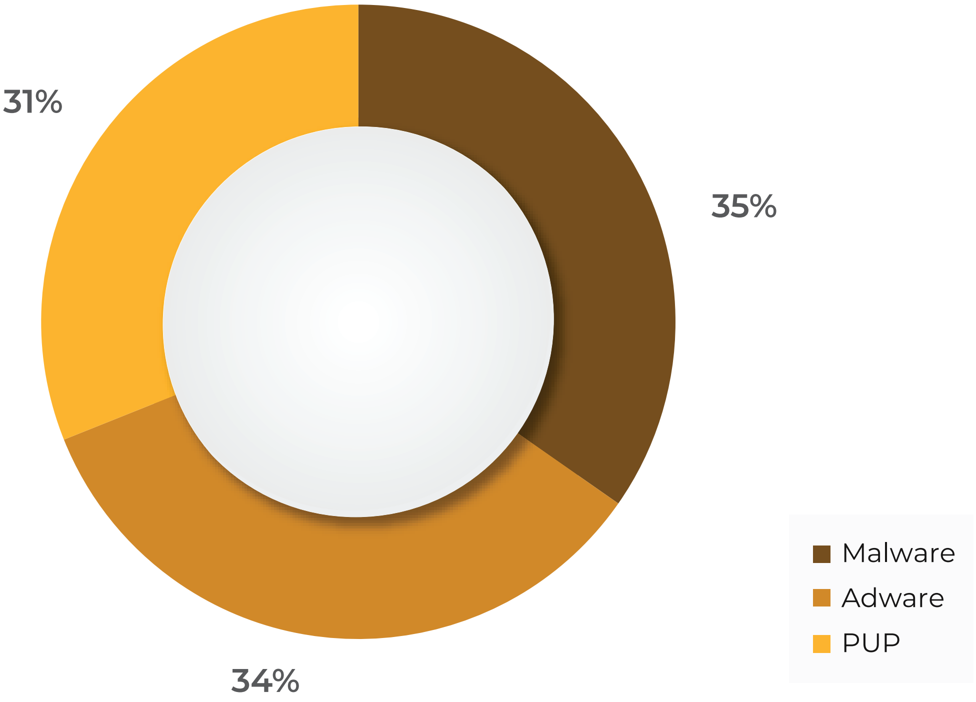
35%

of total Android detections

in Q1 2023 were Malware.

Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q1 2023.



INFERENCE

As technology evolves and expands, so does the cyber crime terrain grow in sophistication. This clearly emphasizes the need for more sophisticated cybersecurity strategies and makes it crucial that individual users and businesses maintain up-to-date security measures to prevent data breaches.

Moreover, cybercriminals are becoming bolder and more daring in their attempts to extort money from their victims. Attackers are exploiting both new and old software vulnerabilities. As if that weren't enough, we're also seeing a shift in the types of attacks that are being employed.

With cybercriminals diversifying their tactics and targeting new areas of vulnerability the first quarter of 2023 was evident that businesses and individuals need to get their A-Game on.

The need of the hour is to level-up digital protection in this ever-changing technological landscape. We hope this report helps you gain a deeper understanding of the threats and challenges that lie ahead and take the necessary steps to safeguard your digital assets.

Quick Heal Technologies Limited
Marvel Edge, Offcie No.7010 C & D, 7th Floor,
Viman Nagar, Pune 411014, Maharashtra, India.

+91 20 66813232 | www.quickheal.com | info@quickheal.com