DSCI
PROMOTING DATA PROTECTION

SECRITE

INDIA CYBER THREAT REPORT 2023

FOREWORD – DSCI

As India advances its digitalization efforts across sectors, a pervasive outbreak of cyberattacks has inflicted substantial financial losses on businesses. Cybersecurity has ascended to a strategic concern at the board level owing to the multifaceted nature of cyber threats and the escalating monetary repercussions stemming from data breaches. For the purpose of this report, DSCI in collaboration with SEQRITE analysed approximately 400 million malware detections from over 8.5 million SEQRITE endpoint installations in India. Our objective was to conduct a detailed study of India's cyber threat landscape and present our analysis very specific to Indian context covering the states, cities, and industry segments.

Malware stands as a significant peril to the integrity of digital systems, with cybercriminals engineering increasingly intricate and diverse attack methodologies. Every day, over half a million instances of malware are discovered, adding to the already staggering one billion circulating malware programs. As depicted in the report, there is a significant rise in behaviour-based detection compared to signature-based detections owing to the surge in constantly mutating malware variants such as polymorphic malware, zero-day exploits, fileless attacks. The report delves into serious threats posed by ransomware attacks. It is evident from the analysis that ransomware hit rate is higher compared to other malware categories as ransomware detection is still evolving. The geographical analysis presents the top states and cities with highest detection; however, it also underlines the fact that BYOD, work from home trends resulting in Tier II/ III cities are in the ambit of cyberattacks. The digitization drive across industry segments is exposing traditional industries such as automobiles, manufacturing, healthcare to cyber threats.

The report meticulously delineates prominent classifications of malware and their consequential impacts, providing insights into both network and host-based exploitations, Android-specific detections, zero-day vulnerabilities pertinent to the Indian context. The featured stories in the report offer in-depth narratives on prevalent cyber threats. These narratives dissect cryptojacking exploits, anti-forensic activities, advanced persistent threats, and various malicious activities targeting specific sectors and technologies.

The report concludes with a glimpse into the future, providing predictions and insights into cyber threats anticipated for 2024, empowering us to stay ahead in our security measures. It serves as a compass, guiding our actions and fortifying our cybersecurity posture.

VINAYAK GODSE
Chief Executive Officer,
Data Security Council of India

FOREWORD – QUICK HEAL

In line with the Hon'ble Prime Minister, Shri Narendra Modi's vision of cyber-safe India, at SEQRITE, the enterprise cybersecurity arm of Quick Heal, we envision a future where cyber safety is not just a privilege but a fundamental right for all. It is with great pride and a sense of responsibility that I share with you deep insights derived from the country's largest Malware analysis lab, SEQRITE Labs, in collaboration with Data Security Council of India (DSCI).

I thank the entire team at DSCI and experts at our Labs to have researched and published threat intelligence for the Indian market. This report will dive deeply into the world of ever evolving threats in the Indian context, share predictions and recommendations for individuals, businesses and government organizations to stay a step ahead of prevalent risks during current and future times.

Backed by our patents and international certifications and a legacy of nearly three decades, our award-winning solutions are truly made-in-India for the world. I am confident that with our rigorous R&D efforts, focus to innovate future-ready technologies, and round-the-clock technical support, our solutions are capable of mitigating new and emerging threats.

Our commitment to securing India goes hand in hand with our dedication towards innovation thereby creating solutions that promise a sustainable future. Our insights forged at our Labs form the cornerstone of our deep understanding of the evolving threat landscape. Recently, our team has patched two Zero Day vulnerabilities and is the only cybersecurity solution provider world over to have found a solution for Expiro Infector. In addition, we are the first and only Indian company to have been invited to collaborate with the Govt. of USA on NIST-NCCOE's Data Classification Project.

I take immense pride in our role as guardians of the critical infrastructure of our nation through our enterprise cybersecurity brand, SEQRITE. Safeguarding the digital backbone of our country is not just a responsibility; it's a commitment to ensuring the resilience of our nation in the face of evolving cyber threats.

As we navigate the ever-changing digital age, SEQRITE remains steadfast in its commitment to innovation, simplification, and securing all.

Sincerely,

DR. SANJAY KATKAR
Jt. Managing Director,
Quick Heal Technologies Limited

From CEO's Desk – QUICK HEAL

India's rapidly growing digital ecosystem has proved to be a boon to its economy and is estimated to contribute over 20% to the country's GDP by 2026. However, with digital evolution, India has also emerged as the most targeted country in terms of cyberattacks, accounting for 13.7% of all attacks worldwide. Indian government agencies witnessed 95% increase in cyberattacks in 2022, as compared to the previous year. Industries including healthcare, education, research, government, and military sectors have emerged as the most vulnerable, followed by agriculture, logistics, transportation, the energy industry at large, high-tech enterprises, pharmaceutical companies, and manufacturers of medical equipment.

Therefore, it is with great pleasure that we present to you this Threat Report, a collaborative effort between SEQRITE and DSCI, drawing on the invaluable insights from SEQRITE Labs, the country's largest Malware Analysis Lab to equip businesses with India centric knowledge and actionable recommendations to fortify their cybersecurity posture.

This report stands as a testament to the diligence and dedication of our researchers and experts, whose tireless efforts have allowed us to compile a comprehensive analysis of cyber threats in the Indian landscape. The wealth of data, statistics, and telemetry from approximately nine million endpoints forms the backbone of this report, providing a unique and detailed perspective on evolving cyber threats.

The report delves into the geographic and sectoral impact of cyber threats, shedding light on the top states, cities, and industries targeted throughout the year. From our analysis, it's evident that no region or sector is immune to the reach of these malicious attacks.

In addition, our commitment to ensuring holistic protection is reflected in the multiple layers of detection and protection mechanisms employed against sophisticated malwares. Notably, on the Android front, we've observed a significant increase in Adware and Potentially Unwanted Applications (PUAs). Shockingly, fake and malicious applications including SpyLoan and HidAdd apps hosted on Google Play Store, have been downloaded by millions of unsuspecting users. Our researchers at SEQRITE Labs have identified and got numerous such malicious apps removed from Google Play Store.

Furthermore, the influence of geopolitical events, such as the Russia-Ukraine and Israel-Hamas conflicts, have cast a shadow on the global cybersecurity landscape. Despite India's diplomatic balancing act, our government and private entities have faced cyber threats from actors supposedly affiliated with the warring parties.

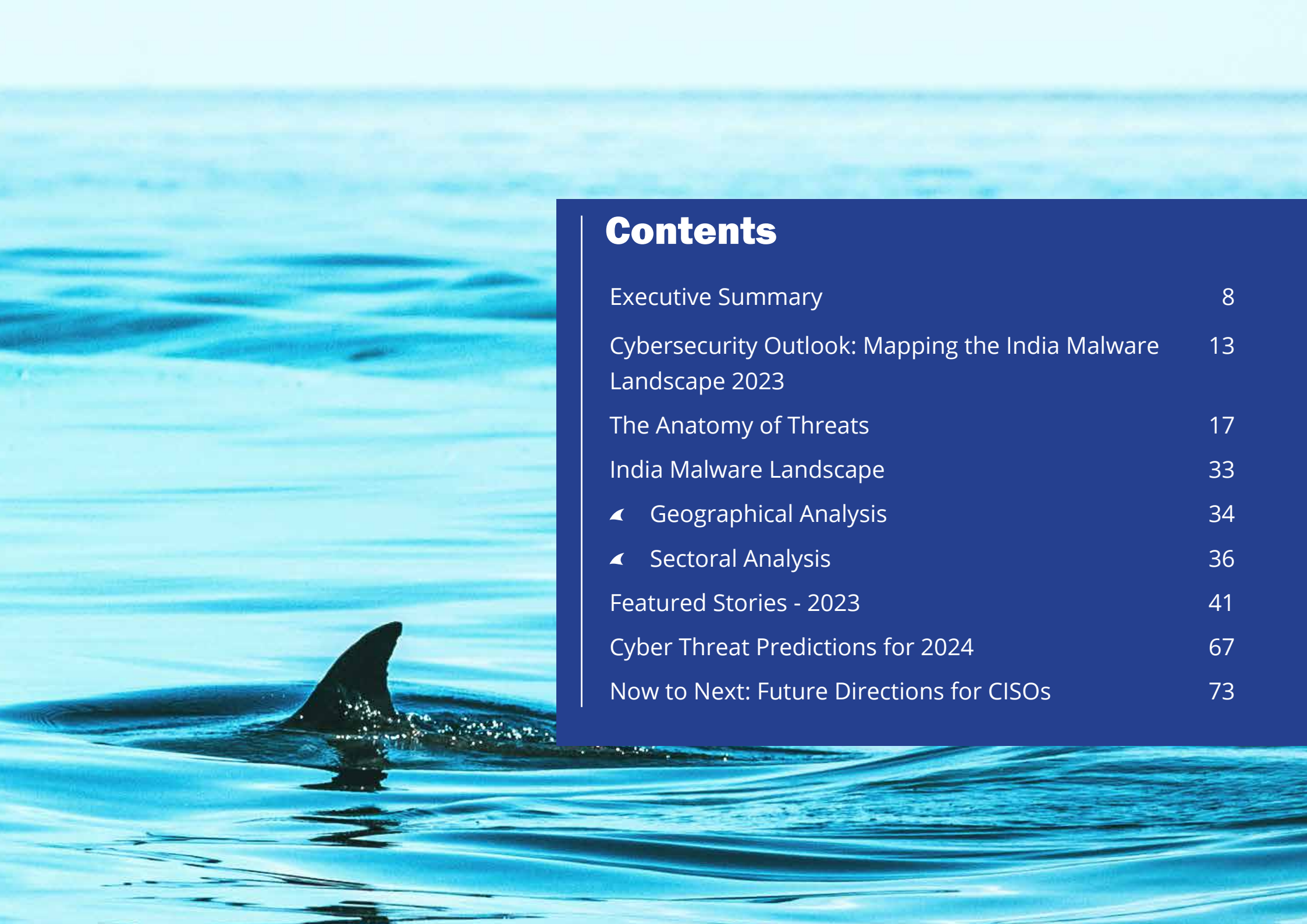
The report also uncovers cyber space violations during significant social and national events, including the G20 summit hosted by India. Central and state government websites experienced DDoS attacks, defacements, and an overall surge in attacks, aiming to tarnish the country's image during pivotal national and global occurrences.

We stand committed to simplifying cybersecurity for enterprises, government organizations and public sector entities by providing comprehensive and innovative solutions that are powered by state-of-the-art threat intelligence and play books backed by world-class service provided by the best-in-class security experts.

We extend our heartfelt gratitude to DSCI for their collaborative efforts and to the dedicated team at SEQRITE Labs for their unwavering commitment to creating excellence in cybersecurity. In light of this collective endeavor to safeguard our digital landscape, I sincerely hope that this report serves as a valuable resource for our common goal of creating a safe country and a safe world.

Sincerely,

VISHAL SALVI
Chief Executive Officer,
Quick Heal Technologies Limited



Contents

Executive Summary

The DSCI-SEQRITE India Cyber Threat report is instrumental in gaining a comprehensive understanding of the current cybersecurity landscape, particularly within the Indian context. It offers valuable insights into emerging trends related to threats, the activities of threat actors, vulnerabilities and cybersecurity incidents.

The report integrates strategic and technical components, making it accessible to both technical and non-technical audiences. It goes beyond the surface by identifying and elucidating the top threats, delving into the specifics of threat actors' motivations and attack techniques. Furthermore, the report provides a thorough exploration of specific sectors and geographies.

Key Hightlights

> 400 million detections across **~8.5 million** endpoints

Averaging **761 detections** per minute

~49 million detections stem from behaviour-based analysis, constituting **12.5%** of all

Ransomware & Malware

Ransomwares authors continually evolve their methodologies and employ sophisticated techniques to evade traditional signature-based detection.

Ransomware incident ratio
~1 per 650 detections

Malware incident ratio
~1 per 38,000 detections

Cryptojacking
Emerging as a significant threat with over 5 million detections in a year

Malware Attack Spectrum

Dominant Threats
41% Trojans & **33% Infectors**

Geographical Hotspots
15% Telangana & **14% Tamil Nadu**

City-wise Analysis
15% Surat & **14% Bengaluru**

Top Three Industries

Automobile

Government

Education

Attack Vectors

>50%
of detections are associated with removable media and network drives.

~25%
of attacks result from clicking on malicious links in emails and websites.

Mobile Threat Landscape

An average of **~3** attacks in a month per Android device

The report presents a comprehensive analysis of **malware threats** based on the data collected by SEQRITE Labs reporting **400 million** malware detections based on **8.5 million** endpoints, averaging **761 detections every minute**. The detections were examined under different subcategories, assessing the impact on various industry segments including government agencies. Additionally, the threat landscape across states and cities were explored, highlighting notable instances such as APTs in action, Cryptojacking, Ransomware attacks, the resurgence of old viruses, fake lending apps, and more.

2023 witnessed a pronounced increase in global threat vectors, largely influenced by significant geopolitical developments worldwide, including Russia's invasion of Ukraine. Specifically, within India, the G20 summit became a central stage for geopolitical events, garnering substantial attention regarding cyberattacks on India's digital infrastructure. During this period, there was a marked increase in both the frequency and sophistication of cyber threats, contributing to the proliferation of criminal activities such as extortion, espionage, and frauds on a broader scale.

Observations 2023

The current state of solutions against malwares face challenges with signature-based approaches, given the agility of malware creators in manipulating signatures. Behavioural analysis is the proactive approach that involves scrutinizing behavioural patterns associated with potential threats, recognizing the deception tactics employed by contemporary malware against traditional signature-based detection systems. Behavioural-based detection technologies constituted over **12.5% of detections in 2023 (approximately 49 million instances).**

- Next-Generation Antivirus (NGAV) solutions are equipped with behaviour-based detection components to identify these advanced malwares based on the traits. Behaviour-based detection observes system activities to differentiate between normal and abnormal behaviour, thereby aiding in the identification of potential threats. This approach utilizes Artificial Intelligence (AI) and Machine Learning (ML) to analyze large data sets and identify patterns that deviate from the norm, indicating potential malicious activities.

Ransomware persistently upholds its position as one of the most pernicious manifestations of cybercrime. A single ransomware security incident emerges for every cluster of 650 detections. Whereas the occurrence of a malware incident is considerably less frequent, materializing only once amidst a staggering **38,000 detections.**

Crypto Miners and Cryptojacking: Cryptojacking is a prevalent stratagem where an adversary deploy malevolent crypto mining software to an unsuspecting victim's device to mine cryptocurrency coins without their permission. Crypto miners are surfacing as a tenacious menace in the cyberthreat panorama. They impact all significant computing systems and can remain undetected for an extended period of time. Despite the fluctuations in cryptocurrency values throughout 2023, the large-scale deployment of crypto miners can yield substantial financial gains for threat actors. Regardless of market shifts, cryptocurrency remains paramount. Crypto mining has evolved to be more resource-demanding and consequently more expensive. Attackers have started to infiltrate multiple victims' environments to install miners and misappropriate the necessary computing resources.

- The year also witnessed detections associated with CryptoNight, a mining algorithm employed to secure networks and authenticate transactions in certain cryptocurrencies like Monero and Webchain. This included a surge in the usage of the Webchain miner and several XMRig-based miners. XMRig, a widely used open-source tool for mining cryptocurrencies including Bitcoin and Monero, is currently one of the most exploited coin miners by threat actors.

Industry Trends

- **Automotive Industry:** Over the past three to four years, the global adoption of Industry 4.0 has marked a transformative trend, witnessing extensive digitalization integration across industries. The industry, once considered relatively secure, now faces escalating cyber threats. In 2023, a notable surge in cyber-attacks targeted the automotive sector, marking a shift from its earlier perceived safety. Supply chains within the automotive industry experienced the highest number of detections, surpassing government agencies and the education sector.
- **State-Backed Threats in India:** India, particularly vulnerable to state-backed threat actors, witnessed an increased focus on government agencies and defense organizations.
- **Education Sector:** The sector contends with common threats such as phishing. Account compromise, fuelled by high turnover, is a prevailing challenge. W32.Neshta.C8 emerged as a significant threat within this sector.
- **Power and Energy Sector:** The critical power and energy sector in India, pivotal for economic growth, faces cyber threats targeting diverse verticals, including supply chain, cloud, legal, IT, and OT. The sector continues to grapple with the risk of cyber supply chain vulnerabilities, with the Expiro infector variant being particularly prevalent.
- **Healthcare Sector:** As India advances in digitizing healthcare, securing online systems becomes imperative. Nearly 60% of healthcare organizations in India encountered cyberattacks in the past year, with the Nimda variant posing a significant threat.
- **Manufacturing Sector:** Indian manufacturing firms confront heightened risks due to unsecured IoT devices in their networks. The implementation of 5G technology raises concerns about exacerbating existing security vulnerabilities. Ransomware attacks have disrupted manufacturing operations, especially impacting Small and Medium-sized Enterprises (SMEs), while sophisticated phishing attacks target SMEs within the sector.
- **Logistics, Banking, and Financial Sector:** Beyond manufacturing, the logistics, banking, and financial sectors are susceptible to cyberattacks. The financial sector's digital transformation and the rise of the platform economy have elevated cyber threats on low-value transactions.

India has been a significant target for Advanced Persistent Threats (APTs). Throughout 2023, entities associated with various nations consistently conducted computer network operations, emphasizing the vital role these operations play in fulfilling national objectives. Adversaries have carried out a variety of attacks, including destructive, espionage, and information operations characterized by a marked increase in the scope and scale of their espionage activities.

The cybersecurity landscape has been significantly influenced by the extensive integration of Android devices, constituting nearly 71% of the global market.

The cybersecurity landscape has been significantly influenced by the extensive integration of Android devices, constituting nearly 71% of the global market. The analysis conducted, based on 500K installations, reveals a discernible uptick in Adware and Potentially Unwanted Applications (PUAs), highlighting the persistent prominence of malware as a significant threat. The data indicates an average of 2-3 monthly attacks on Android mobiles, posing a substantial risk to corporate networks, especially considering the widespread utilization of mobile devices for office work.

Predictions 2024

1. Ransomware continues to pose a significant threat to organizations, with the cost of attacks expected to rise. Key trends include increased targeting of critical infrastructure and the rise of Ransomware-as-a-Service (RaaS), which lowers entry barriers for cybercriminals. Double extortion tactics are also on the rise where attackers encrypt and steal victims' data. The need for robust cybersecurity measures is underscored by the evolving threat landscape and the anticipated persistence of these threats.
2. AI-powered malware like BlackMamba poses significant threats, using AI for evasion and creating unique payloads. It uses AI to capture keystrokes, potentially infiltrating Android OS. As AI evolves, phishing tactics are expected to become more personalized and effective.
3. 'Living off the land' binaries like Powershell and Certutil pose considerable risks, being exploited to disable security measures and conduct malicious activities. The recent DarkGate malware and Cobalt Strike used these binaries to compromise systems, indicating a potential increase in such attacks in 2024.
4. Multi-Factor Authentication (MFA) fatigue attacks are a rising cybersecurity concern, where hackers inundate victims with repeated second-factor authentication requests, coercing them into granting access.
5. Looking ahead to 2024, AI-generated voice and video scams are emerging as a significant threat. These scams use advanced deep learning techniques to imitate trusted individuals, thus deceiving targets into revealing sensitive information or taking undesired actions.
6. Significant democratic events, such as elections, inevitably draw the attention of adversaries. The upcoming 2024 Indian Elections are no exception and are poised to witness a surge in cyberattacks, particularly in the form of phishing emails and malvertising. Artificial intelligence (AI) tools are increasingly being leveraged to scale up such attacks, making them more sophisticated and difficult to detect.
7. Supply chain vulnerabilities are a growing concern in cybersecurity, leading to targeted attacks with widespread consequences. The rise in such attacks call for new regulations and global collaboration between governments and private industries. Supply chains offer attackers the opportunity for one-to-many attacks, a trend expected to escalate in 2024.
8. Zero-day vulnerabilities are increasingly being exploited by cybercriminals and state-sponsored groups for persistent access to networks. This allows them to operate undetected, extract valuable information, and demand higher ransoms. The trend is expected to grow with a focus on exploiting cloud infrastructure misconfigurations.

As we move into this new era of AI-generated media, we must balance innovation with integrity and verify the source of all communication.

9. A concerning development in the cybersecurity landscape is the growing prevalence of the underground economy, where corporate assets are auctioned, and breach datasets are openly traded. This surge is particularly evident in the increased auctioning of corporate access and the sale of breach datasets, driven by escalating demand for services such as penetration testing, zero-day exploits and RaaS (Ransomware as a service) within the underground market. Consequently, there has been a notable rise in ransomware infections and instances of unauthorized access to sensitive networks, as acquired access is actively traded in underground forums.
10. Phishing attacks are increasing, often using personal data from social media to gain trust. As generative AI improves, it will be used more in scams, including mimicking voices. The dating app scams are also expected to rise.

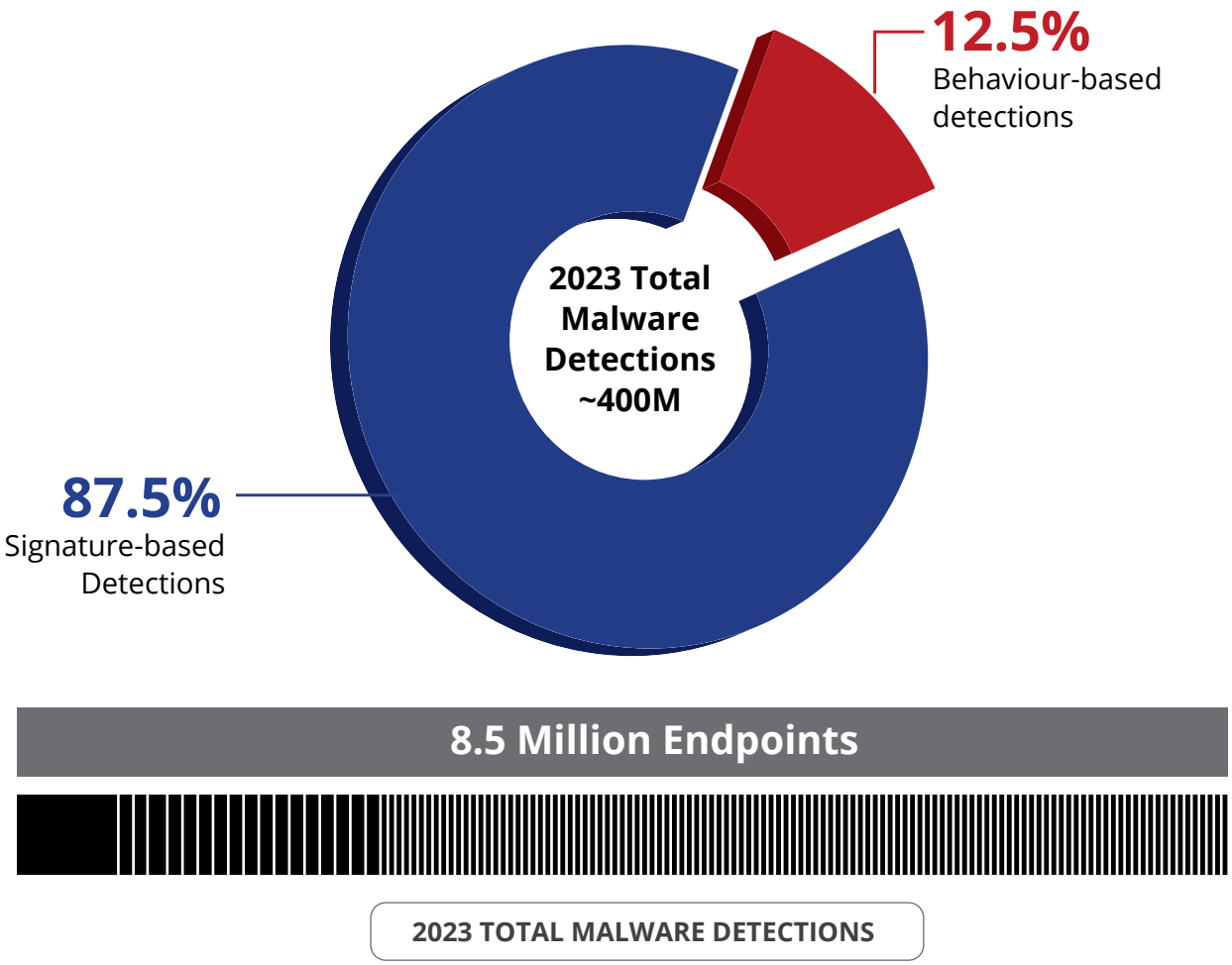
Cybersecurity Outlook:

Mapping the India Malware Landscape 2023

Malware Detection Overview

To arrive at the cyber threat landscape of India for the year 2023, a substantial 400 million instances of malware were observed across an extensive network of 8.5 million endpoints.

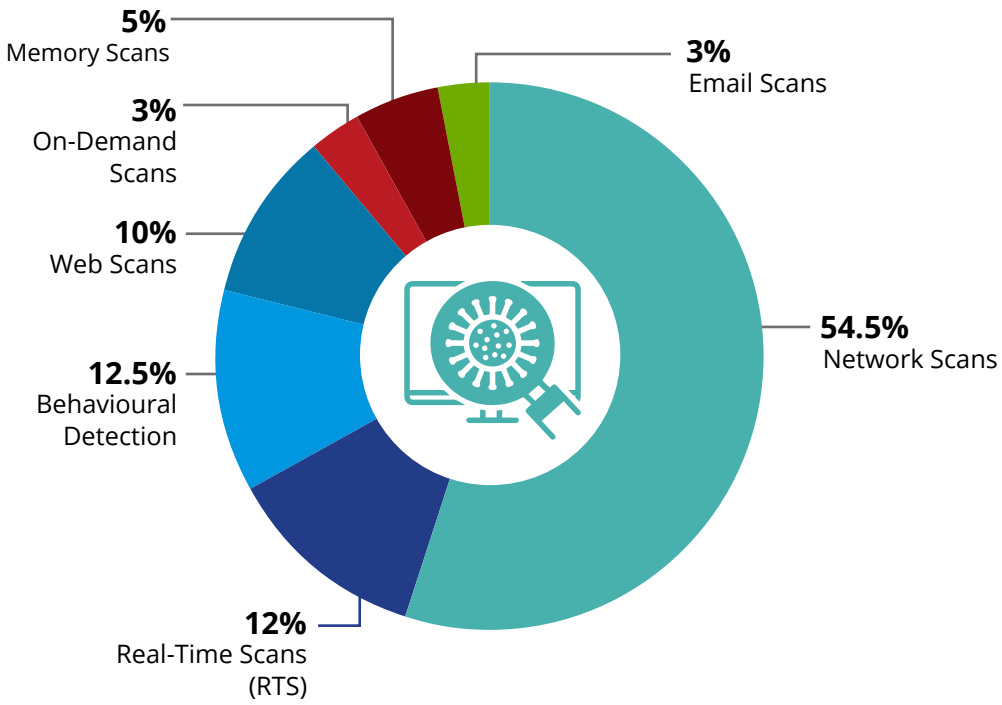
Behavioural Detection (NGAV) played a pivotal role, contributing to **49 million**[1] of the total detections.



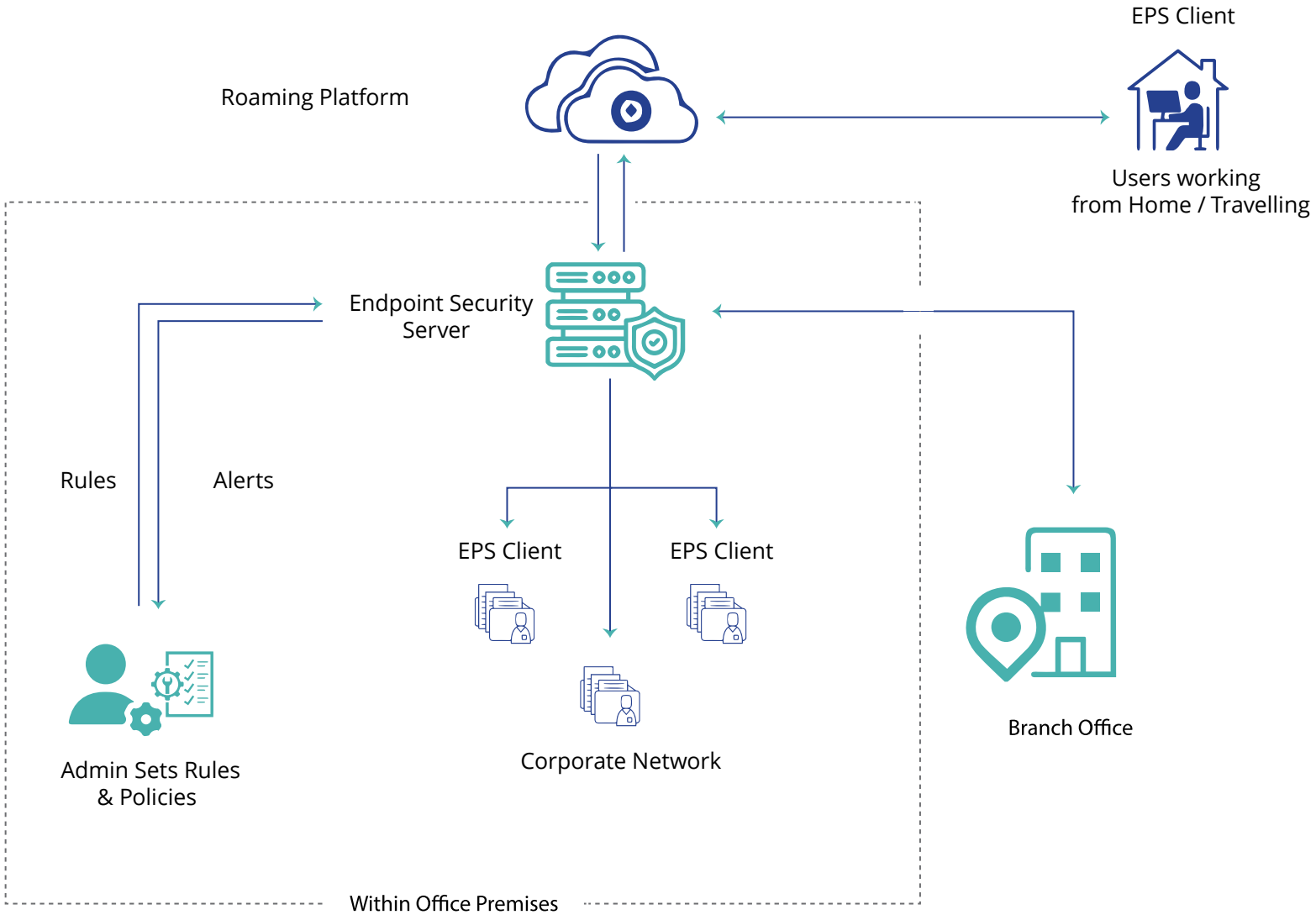
[1] These detection capabilities were arrived through SEQRITE's cutting-edge technologies including Endpoint Security Server, amongst others to provide a comprehensive approach securing both on-premise and cloud environments.

Breakdown of Scan-Wise Detections:

Scan Wise Detections Subcategory	Percentage Detections	Inferences
Network Scans	54.5%	Monitoring and safeguarding network traffic is vital.
Behavioural Detection	12.5%	Behaviour-based analytics are effective for malware detection.
Real-Time Scans (RTS)	12%	RTS promptly detects and neutralize threats, ensuring swift response and ongoing protection.
Web Scans	10%	Web scans for malware proactively safeguard users and data by identifying and mitigating online threats.
On-Demand Scans	3%	On-demand malware scans provide users with flexible, manual threat detection for added control and security.
Email Scans	5%	Email remains a vector of concern, with significant number of malware instances detected through vigilant email scanning.
Memory Scans	3%	Adversaries are actively targeting threats operating in memory.



SCAN-WISE DETECTIONS

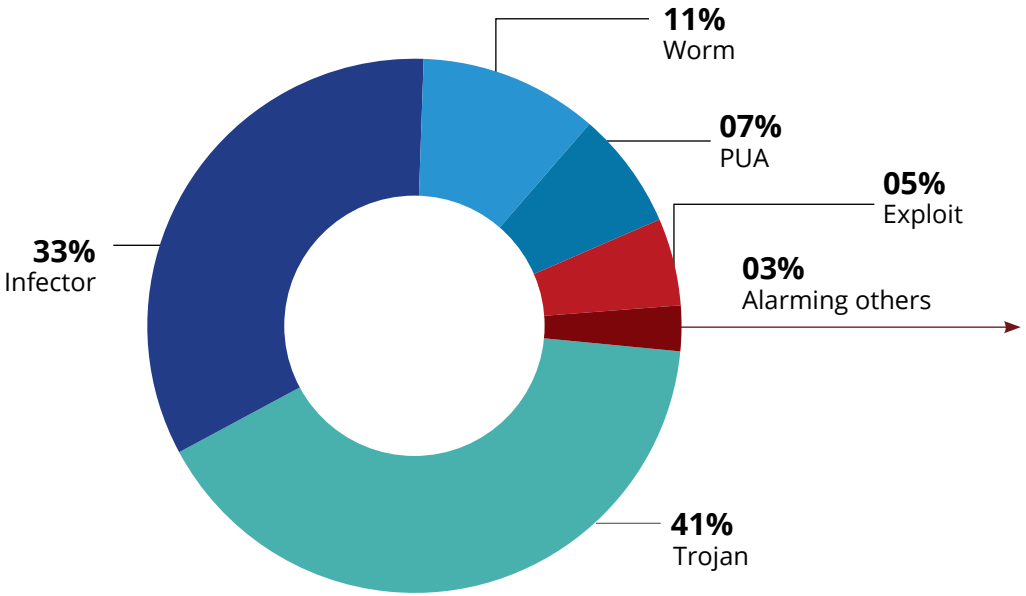


ENDPOINT ARCHITECTURE

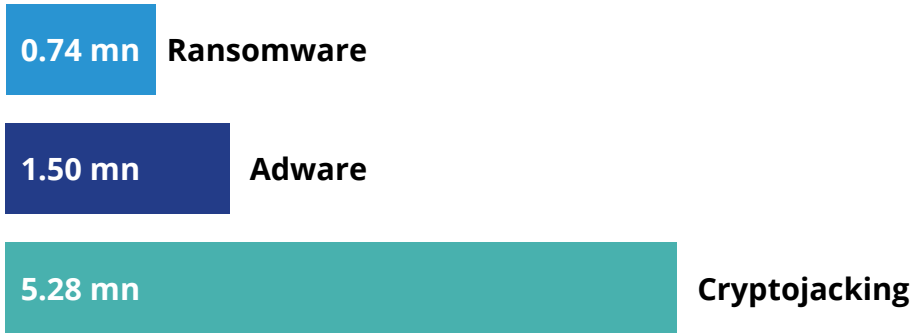
The Anatomy of Threats

Examining Malware Subtypes 2023

The section on malware subcategories elaborates on the current landscape of digital threats, sheds light on the prevalence of various malicious entities, and their potential impact on computer systems.



MALWARE SUBTYPES 2023 (DETECTIONS)



DISSECTING THE 7.53 MN DETECTIONS OF "ALARMING OTHERS FAMILY"

**The reported count reflects Quick Heal installations and is based on data spanning from October 2022 to September 2023. Users are advised to consider the limited scope of this data for comprehensive insights.*

- **Trojan (111.19 million):** The prominence of Trojan highlights the sophistication of deceptive tactics employed by cybercriminals. Users must exercise caution when downloading and installing software to avoid falling victim to such threats.

  Robust endpoint security solutions are crucial to detecting and neutralizing Trojan attacks before they can compromise sensitive data.

- **Infector (91.40 million):** Infectors pose a significant risk to the integrity of files and the overall health of computer systems.

  Regular system scans and the use of reputable antivirus software is essential to identify and eradicate infections promptly. Additionally, user education on safe browsing practices can help prevent inadvertent execution of infected programs.

- **Worm (29.62 million):** The self-replicating nature of worms necessitates a proactive approach to network security.

  Deploying firewalls, intrusion detection systems, and network segmentation can limit the spread of worms and minimize the potential for widespread damage.

- **PUA (Potentially Unwanted Application) (19.48 million):** Potentially Unwanted Applications may not be explicitly malicious, but their impact on system performance and user experience can be detrimental.

  Organizations should implement strict software controls and educate users about the risks associated with downloading and installing applications from untrusted sources.

- **Exploit (14.47 million):** Exploits targeting software vulnerabilities demand constant vigilance in terms of software updates and patch management.

  Time effective application of security patches is critical to close potential entry points for exploit-based attacks.

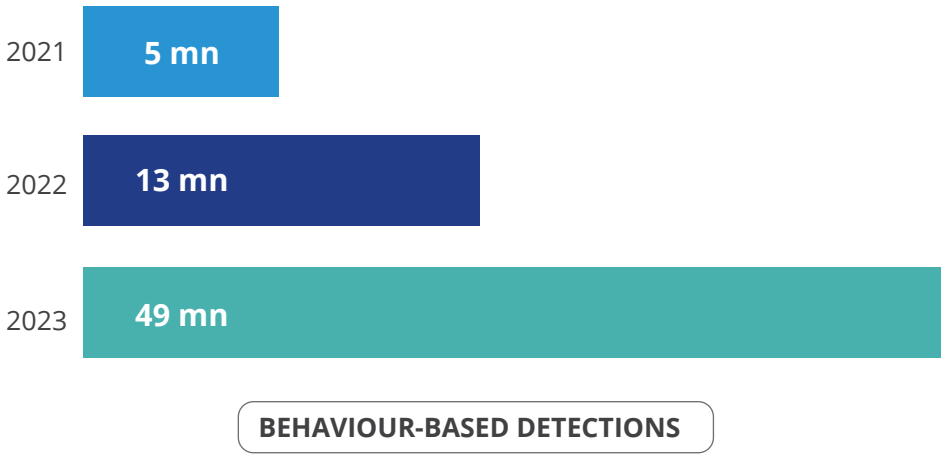
- **Alarming Others (7.53 million):** This category, comprising Cryptojacking, Adware, and Ransomware, represents a multifaceted threat landscape.

  - **Cryptojacking (5.28 million):** The prevalence of cryptojacking emphasizes the importance of monitoring system resources and utilizing endpoint security solutions capable of detecting and blocking unauthorized cryptocurrency mining activities.
  - **Adware (1.50 million):** It can be tackled by using ad blockers and security solutions capable of identifying and eliminating adware components.
  - **Ransomware (0.74 million):** Ransomware's potentially devastating impact on organizations reinforces the need for robust backup strategies, employee training on recognizing phishing attempts, and advanced endpoint protection to inhibit ransomware attacks.

Behaviour Based Detections

In the ever-evolving landscape of cybersecurity, the limitations of conventional detection techniques have prompted the integration of advanced methodologies to enhance the efficacy of anti-malware systems. Traditional approaches, such as signature-based methods, excel in identifying known malware patterns. However, their inherent limitation lies in their inability to effectively detect unknown or polymorphic malware strains that continuously mutate to evade signature recognition.

To address these challenges, machine learning methods are being seamlessly integrated with existing detection mechanisms. While heuristic-based methods offer a promising avenue for identifying new malware variants, their susceptibility to high rates of false positives and false negatives necessitates the development of more precise and adaptive detection strategies. This imperative has led to the emergence of behaviour-based detections, which focus on analyzing the dynamic actions and patterns exhibited by potential threats, thereby offering a proactive and comprehensive defense. This synergy of machine learning and behavioural analysis marks a pivotal shift towards a more resilient and responsive approach.



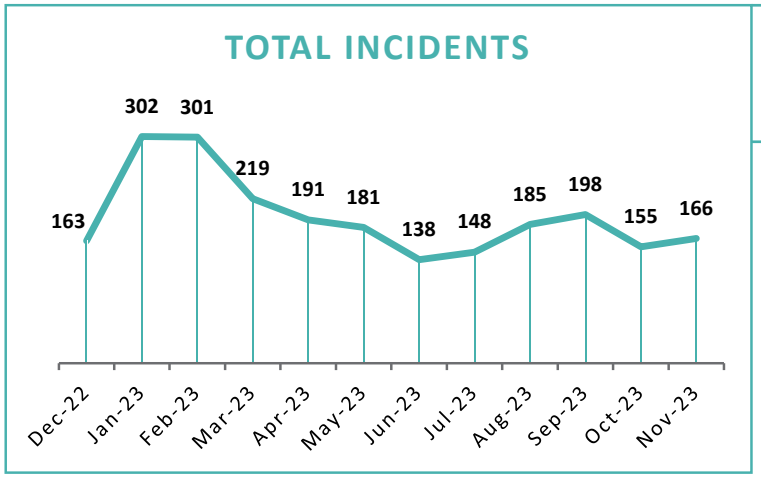
- **In 2023, over 12.5% of detections (~49 million)** are attributed to behaviour-based components. Over the years, we can see that behaviour-based detections have increased. It signifies that over the years, these technologies will evolve and would be more potent to tackle the latest malwares. Conventional static file-based detection methods have constraints to detect sophisticated malwares with custom packers and obfuscation.
- **NGAV solutions** are equipped with behaviour-based detection components to detect sophisticated malwares based on their characteristics.
- Listed below are some of the malware variants detected by **NGAV** which otherwise are difficult to detect with conventional methods.
  - **Polymorphic Malware Variants:** These malwares are known for their ability to continually alter their characteristics to evade detection. Despite being derived from known malware families, their signatures are modified with each iteration, rendering them invisible to signature-based detection systems.
  - **Code Obfuscation:** It is a strategy used to dodge detection and analysis. By making the source code extremely hard to comprehend or even illegible, it can bypass tools that perform static analysis.

- **Fileless Attacks:** These attacks employ macros, scripting engines, in-memory execution and utilizes "living off the land" binaries and leave no minimal traces on the disk.
- **Zero-Day Attacks:** These are novel or unidentified attacks that have not been recorded in signature databases yet represent significant challenge for traditional antivirus solutions.
- **LOLbins or Living Off the Land Binaries:** LOLbins are non-malicious system tools that cyber criminals can exploit to hide their malicious activities. They can execute code, perform file operations, steal passwords, and bypass detection. Often, these are Microsoft-signed binaries like Certutil and WMIC. LOLbins are challenging to detect and terminate because they use local and trusted processes. Even if detected, they should only be terminated, not quarantined, leaving the system vulnerable to further attacks until the parent process initiating the malicious operation is terminated. The only effective countermeasure is to detect them during malicious activity, terminate the process immediately, and quarantine the parent process or program. This can be achieved through deployment of NGAV Solutions.

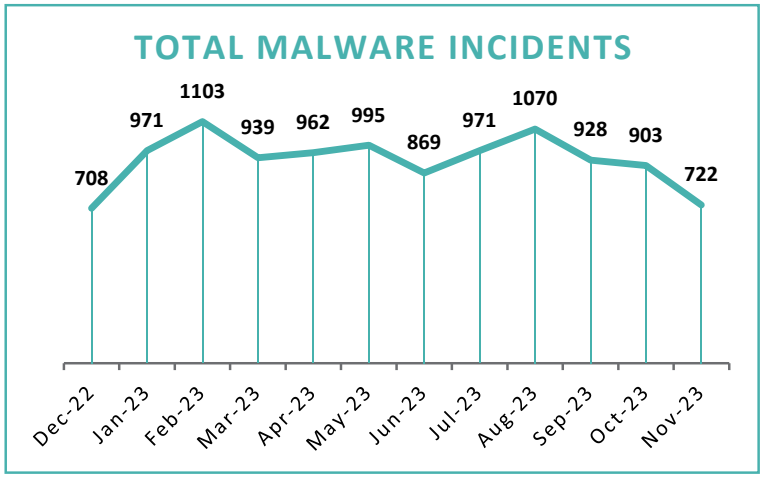
Malware and Ransomware Analysis (Year 2023)

Decrypting the Menace: Unveiling the Inherent Risks of Ransomware

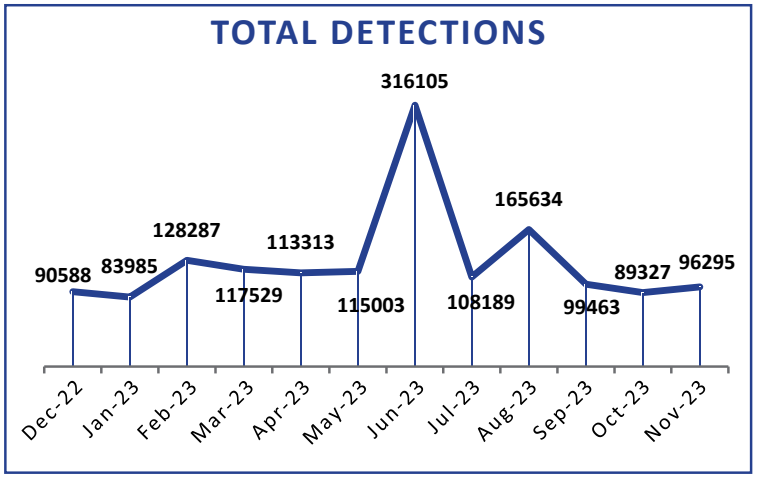
This section examines incident trends and detections from December 2022 to November 2023, focusing on the total incidents vs. total detections ratio as a key measure of detection efficiency. The prevalence of ransomware is higher due to its increased difficulty of detection in comparison to conventional malware.



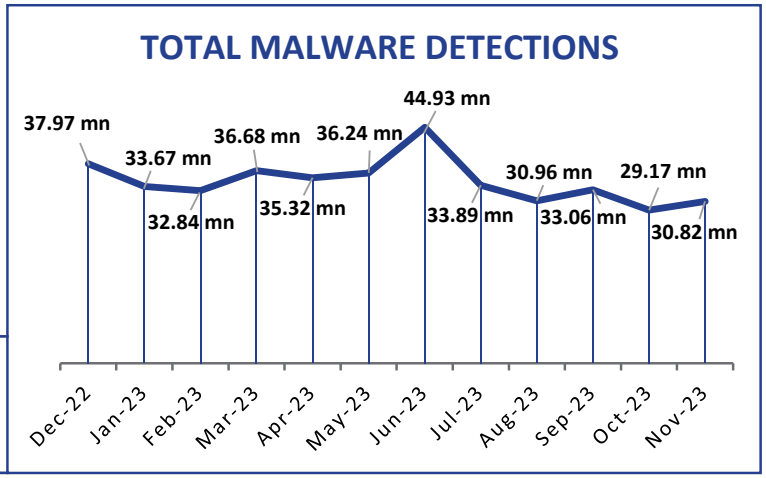
Ransomware ~1 incident per 650 detections



A lower ratio signals a more effective detection mechanism, implying a higher success rate in identifying attacks.



Malware ~1 incident per 38000 detections



~95 mn detections can be contributed to the below list of Malwares

W32.Pioneer.CZ1

Detections: 50.70 mn

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behaviour: The malware injects its code to files present on the disk and shared network. It decrypts malicious .dll present in the file and drops it. This .dll performs malicious activities and collects system information and sends it to a 'CNC' server.

Worm.AUTOIT.Tupym.A

Detections: 6.21 mn

Threat Level: Medium

Category: Worm

Method of Propagation: Malicious links in instant messenger

Behaviour: Malware drops file in system32 folder and executes it from dropped location. It connects to malicious website, also modifies browser home page to another site via registry entry. It also creates Run entry of the same dropped file for persistence.

LNK.Cmd.Exploit.F

Detections: 7.63 mn

Threat Level: High

Category: Trojan

Method of Propagation: Email attachments and malicious websites

Behaviour: Uses cmd.exe with "/c" command line option to execute other malicious files. It simultaneously executes a malicious .vbs file with name "help.vbs" along with a malicious .exe file. The malicious .vbs file uses Stratum mining protocol for Monero mining.

W32.Mofksys

Detections: 8.40 mn

Threat Level: High

Category: Worm

Method of Propagation: Removable or network drives

Behaviour: It copies itself to following paths: <System>\explorer.exe, <Windows>\svchost.exe, <Windows>\spoolsv.exe, It adds these paths to RunOnce registry. It can capture the activity like keyboard/mouse inputs, including screen capturing and pass it to the remote intruder.

Drops a copy of itself on other machines in network through writable shared drives and further uses sc.exe to remotely execute as a service.

Trojan.Starter.YY4

Detections: 7.71 mn

Threat Level: High

Category: Trojan

Method of Propagation: Email attachments and malicious websites

Behaviour: Creates a process to run the dropped executable file. Modifies computer registry settings which may cause a system crash. Downloads other malwares like keyloggers. Slows down the booting while shutting down the process of the infected computer. Allows hackers to steal confidential data like credit card details and personal information from the infected system.

Nsis.Bitmin

Detections: 3.38 mn

Threat Level: Medium

Category: Worm

Method of Propagation: Emails and malicious websites

Behaviour: It drops and replicates itself in the "%APPDATA%\temp" directory. This then extracts an inner file named "uihost64.exe" and "uihost32.exe", storing them in the Temp folder. To ensure persistence, it alters a registry key: Registry Entry: <HKCU>\Software\Microsoft\Windows\CurrentVersion\Run

HTM.Nimda.A

Detections: 2.33 mn

Threat Level: Medium

Category: Worm

Method of Propagation: Spreads through emails

Behaviour: The worm spreads by sending email attachments with name 'README.EXE'. It exploits CVE-2001-0154 by setting unusual MIME header type to HTML email containing the executable attachment. The worm infects files on victim machines and network drives.

W32.Runouce.B

Detections: 2.05 mn

Threat Level: Medium

Category: Virus

Method of Propagation: Spreads through emails

Behaviour: It sends a copy of self as an email attachment to email ids present on the victim contact lists. It drops the copy at %system% folder as 'runouce.exe' with hidden attributes. Creates mutex with name 'ChineseHacker-2'.

W32.Neshta.C8

Detections: 1.53 mn

Threat Level: Medium

Category: Virus

Method of Propagation: Removable or network drives

Behaviour: Copies virus code at the start of clean file and keeps clean file at the end of the file. Drops files at paths: <Windows>\svchost.com and <Windows>\directx.sys.

A significant portion, **over 50%, of the detected threats stem from removable media and network drives,** highlighting potential vulnerabilities in external storage and network security. Approximately, **25% of detections result from engaging with malicious links in emails and websites**, highlighting the critical role of robust email and web security measures. Additionally, around **20% of the identified threats propagate through emails using file infectors.** Of particular concern, **26% of these detections fall into the category of high-threat incidents,** warranting immediate attention.

TOP 10 FILES COMMONLY FOUND WITH MALICIOUS CODE

Top Network Based Exploits

As organizations navigate the intricacies of complex network infrastructures, identifying and comprehending the methodologies employed by cyber adversaries is crucial. This section delves into specific exploits that pose significant risks to network security.

Network Exploit	Detections
SMB/CVE-2017-0147-EC.WIN!KP.1912	175 mn
SMB/EternalBlue.UN!SP.31780	155 mn
SMB/Autoblue.UN!SP.30735	65 mn
HTTP/CVE-2017-9841.RCE!PT.42647	1.3 mn
HTTP/CVE-2021-26086.Jira!PT.44523	.1 mn
HTTP/CVE-2021-44228.RCE!AW.45158	.4 mn

Server Message Block | WannaCry ransomware attack in May 2017

Mailchimp Servers, eCommerce Modules in Drupal, Jira Server, LDAP Servers, DB Files

175 mn

SMB/CVE-2017-0147-EC.WIN!KP.1912

CVE-2017-0147 highlights an information disclosure vulnerability within the Microsoft Server Message Block 1.0 (SMBv1) server. The vulnerability originates from the server's handling of particular requests, providing an avenue for attackers to create a specifically tailored packet. Exploiting this vulnerability has the potential to lead to the disclosure of information from the server. Typically, this exploitation scenario entails an unauthenticated attacker transmitting the specially crafted packet to a designated SMBv1 server.

225 mn

SMB/EternalBlue.UN!SP.31780
SMB/Autoblue.UN!SP.30735

CVE-2017-0144, known as EternalBlue, a critical security vulnerability affecting Microsoft Windows operating systems, particularly in the Server Message Block (SMB) protocol. Exploitation of EternalBlue enables remote attackers to execute arbitrary code on a target system without user interaction. The most notable instance of this exploit was witnessed during the WannaCry ransomware attack in May 2017, where the malware rapidly spread across unpatched systems, encrypting files and demanding ransom payments. This incident underscores the significance of promptly applying security updates to mitigate known vulnerabilities.

1.8 mn

HTTP/CVE-2017-9841.RCE!PT.42647
HTTP/CVE-2021-26086.Jira!PT.44523
HTTP/CVE-2021-44228.RCE!AW.45158

HTTP/CVE-2017-9841.RCE!PT.42647

CVE-2017-9841, is a critical code injection vulnerability found in Util/PHP/eval-stdin.php; the vulnerability allows remote attackers to exploit the flaw by sending HTTP POST data beginning with a '<?php ' substring. An unauthenticated attacker, gaining access to the /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php URI, could execute arbitrary PHP code. This security risk impacts the Mailchimp and Mailchimp E-Commerce modules in Drupal, collectively used by a substantial number of sites. The vulnerability is attributed to the use of the php://input wrapper in the /phpunit/src/Util/PHP/eval-stdin.php file, with patched versions of PHPUnit addressing the issue by adopting the php://stdin wrapper.

HTTP/CVE-2021-26086.Jira!PT.44523

This detection pertains to CVE-2021-26086, a path traversal vulnerability in Jira Server and Data Center that exposes a critical security flaw. Actively exploited, this vulnerability allows remote attackers to read arbitrary files on the server by sending a specifically crafted HTTP request to the /WEB-INF/web.xml endpoint.

HTTP/CVE-2021-44228.RCE!AW.45158

CVE-2021-44228, also known as Log4Shell is critical remote code execution vulnerability affecting systems that use Apache Apache Log4j2 versions, where the JNDI features used in configuration, log messages, and parameters lack protection against attacker-controlled LDAP and other JNDI-related endpoints.

Top Host Based Exploits

This section casts a spotlight on Host-Based Exploits, a critical facet of the digital threat landscape. Examining the detections of prominent host-based exploits, including LNK.Exploit.Gen, LNK.Cmd.Exploit.F, LNK.Exploit.Cpl.Gen, LNK.USB.Exploit, and JPEG.Exploit.ms04-028, the focus laid on understanding the prevalence and impact of these exploits on individual computer hosts. Each detection represents a potential gateway for cyber adversaries to compromise system integrity and extract sensitive information. By scrutinizing these instances, the report aims to provide valuable insights into the tactics employed by attackers and equip cybersecurity practitioners with the knowledge needed to strengthen defences.

Host Based Exploits	Detections
LNK.Exploit.Gen	55,11,892
LNK.Cmd.Exploit.F	1,51,18,452
LNK.Exploit.Cpl.Gen	15,14,979
LNK.USB.Exploit	3,12,667
JPEG.Exploit.ms04-028	6,23,886

5.5 mn
LNK.Exploit.Gen

- **LNK/Pantera**, A classified trojan is a type of malware that performs activities without the user's knowledge. These activities commonly include establishing remote access connections, capturing keyboard input, collecting system information, downloading/uploading files, dropping other malware into the infected system, performing denial-of-service (DoS) attacks, and running/terminating processes.

- **Dorkbot**, a widespread botnet, specializes in stealing online payments, conducting distributed denial-of-service (DDoS) attacks, and delivering various malware types. Used globally, it poses a significant threat. Dorkbot-infected systems are weaponized for cybercrime, enabling the theft of sensitive data, initiation of DoS attacks, disabling of security safeguards, and distribution of multiple malware strains. Typically, Dorkbot spreads through malicious links in social networks, instant messaging programs, or infected USB devices. Its backdoor functionality Ex`mpowers remote attackers to download and execute files, harvest logon information, and manipulate domain access. Vigilance is crucial to thwart this pervasive threat.

- **Jenxcus** worm family poses a significant threat by granting unauthorized access and control of your PC to malicious hackers. Additionally, it has the capability to collect and transmit your personal information to these attackers. The infection commonly occurs through drive-by download attacks or by visiting compromised webpages, and it can also be introduced through the use of infected removable drives. Users should exercise caution to mitigate the risk of this intrusive and potentially harmful threat..

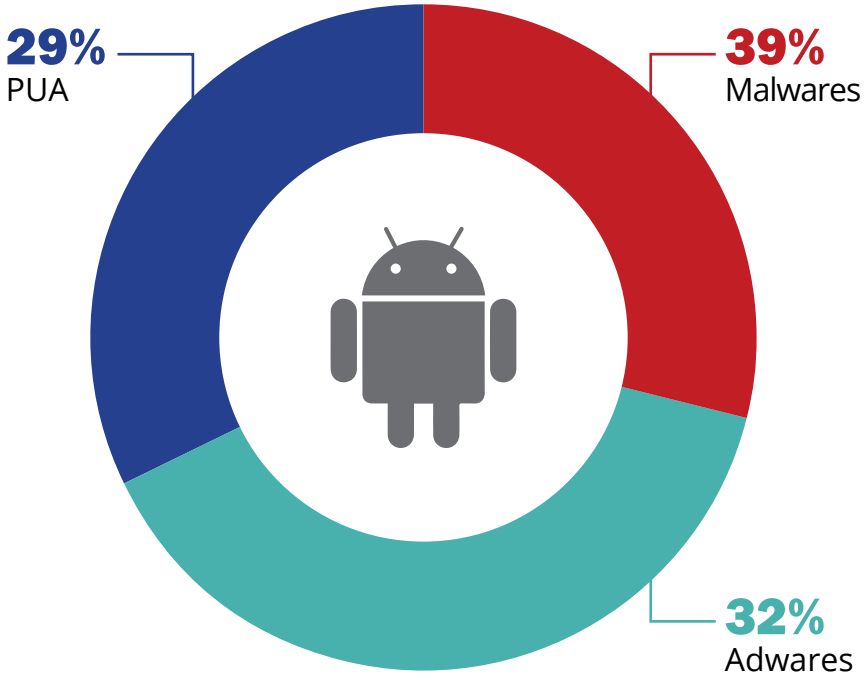
15.1 mn
LNK.Exploit.Gen

Dinihou, a worm, gains entry through removable drives and is typically introduced to a system as a file dropped by other malware or unknowingly downloaded by users visiting malicious websites. Once present, it replicates by dropping copies of itself onto all connected removable drives. Worms like Dinihou have an inherent ability to autonomously propagate to other PCs, utilizing various methods such as copying to removable drives, network folders, or spreading through email. This autonomous spread increases the risk of widespread infection and underscores the importance of proactive security measures.

1.5 mn
LNK.Exploit.Cpl.Gen

CVE-2010-2568 is a detection for malware exploiting a critical remote code execution vulnerability, CVE-2010-2568, present in specific Microsoft Windows versions. This vulnerability stems from the incorrect parsing of shortcuts, enabling the execution of malicious code upon opening an infected LNK file. Notably, this flaw was exploited by the Stuxnet threat and other malware families. This vulnerability also played a significant role in exploit kits used for cyber-espionage campaigns.

Android Detections 2023



Mobile devices continue to replace laptops and desktop computers for many functions, including electronic banking, mobile payments, messaging apps, and social networks. In fact, 60% of all Internet traffic in 2022 was generated by mobile devices.

In 2022, nearly 71% of mobile devices worldwide used the Android operating system.

In 2023, the following threats were observed:

- Significant rise in Adware and Potentially Unwanted Applications (PUAs)
- Malware continues to dominate as a threat for Android.
- Based on the analysis of 500K installations, it was observed that approximately 2-3 attacks per month are detected on Android mobiles.
- Given the extensive use of mobile devices for office work, this poses significant risk to corporate networks if these attacks go undetected in the absence of Android protection.

TOTAL ADDS UPTO 110%

500K Installation Base

Top Zero Days of 2023

This section casts a spotlight on Host-Based Exploits, a critical facet of the digital threat landscape. Examining the detections of prominent host-based exploits, including dummy text for the prevalence and impact of these exploits on individual computer hosts. Each detection represents a potential gateway for cyber adversaries - dummy to change.

		Method	Target	Description
1	CVE-2023-34362	SQL Injection	MOVEit Transfer	Transfer database if exploited by unauthorized individuals
2	CVE-2023-36884	Remote Code Execution	Windows HTML and Microsoft Office	Run scripts remotely and get beyond established system defenses
3	CVE-2023-3460	Privilege Escalation	User registration and account management plugin in the WordPress CMS	Creates users on WordPress websites running vulnerable versions of the Ultimate Member WordPress Plugin with admin privileges.
4	CVE-2023-38831	File extension Spoofing	Winrar	Contains executable content to process desired actions
5	CVE-2023-23397	Privilege Escalation	Windows Microsoft Outlook	Authenticate as the intended user and launch relay attacks

CVE-2023-34362: SQL Injection in MOVEit Transfer

- The discovery of a zero-day vulnerability in MOVEit Transfer has brought attention to the potential risks of unauthorized access as MOVEit Transfer is widely recognized as a secure and popular managed file transfer program utilized by enterprises to safely transfer data using protocols such as SFTP, SCP, and HTTP-based uploads. A SQL injection vulnerability can grant them access to the **MOVEit Transfer database if exploited by unauthorized individuals.** This vulnerability is actively targeted, with attackers leveraging HTTP or HTTPS channels to exploit unpatched systems.

CVE-2023-36884 : remote Code execution in Microsoft Office and Windows HTML

- A major security flaw in Windows HTML and Microsoft Office has been identified as CVE-2023-36884. It represents a particular kind of threat called "Remote Code Execution," which basically gives an attacker a way to **run scripts remotely and get beyond established system defenses.** The exploit involves creating Microsoft Office documents with malicious intent in order to run remote malware.

CVE-2023-23397 : Microsoft Outlook Privilege Escalation

- The Windows Microsoft Outlook client has a vulnerability called CVE-2023-23397 that may be exploited by sending a specially crafted email that sets off an automatic trigger when the Outlook client processes it. The exploit can be activated without any involvement from the user.
- The Net-NTLMv2 hashes of the targeted user will be exposed if the vulnerability is exploited. The **threat actor might then use this to authenticate as the intended user and launch relay attacks** against additional systems that support NTLMv2.

CVE-2023-38831: File extension Spoofing in WINRAR

- CVE-2023-38831 is an RCE vulnerability in WinRAR prior to version 6.23. The problem arises because a ZIP archive may contain both a harmless file (such a regular.JPG file) and a folder with the same name as the harmless file. When an attempt is made to retrieve only the benign file, the **contents of the folder which can contain executable content** are processed.

CVE-2023-3460: A Privilege Escalation Vulnerability in Ultimate Member WordPress Plugin

- A well-known user registration and account management plugin in the WordPress content management system has a privilege escalation vulnerability that allows **malicious actors to create users on WordPress websites running vulnerable versions of the Ultimate Member WordPress Plugin with admin privileges. It can yield in serious repercussions such as the WordPress website being completely taken over or compromised.**

India Malware Landscape

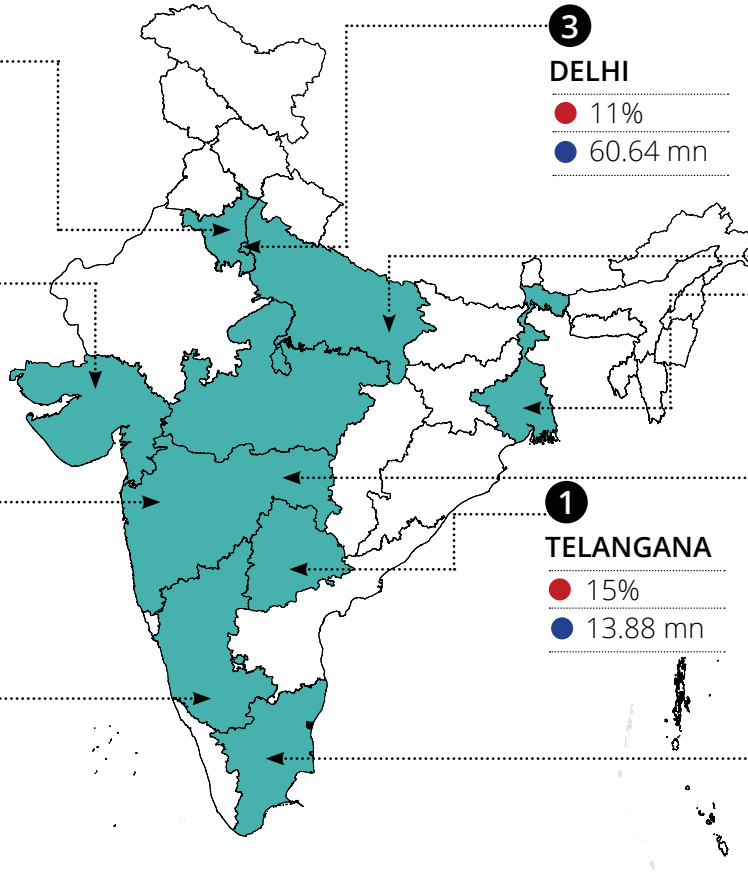
India Malware Landscape: Geographical Analysis

Top 10 States with Highest Malware Detections

~ 70% of the total detections originate from these states.

290 mn Detections

- The number of detections varies across different states of India, depending on the installation base, the availability of computing devices, and the presence of IT/ITeS industries.
- Telangana and Tamil Nadu have the highest ratio of detections per installation, while Maharashtra, Gujrat and Delhi have the highest absolute number of detections.
- Gujarat and Madhya Pradesh show an increase in detections, reflecting the emergence of new IT/ITeS hubs in these states.



7 HARYANA
08%
11 mn

3 DELHI
11%
60.64 mn

9 UTTAR PRADESH
07%
21.53 mn

4 GUJARAT
11%
51.99 mn

8 WEST BENGAL
08%
27.90 mn

6 MAHARASHTRA
09%
71.68 mn

1 TELANGANA
15%
13.88 mn

10 MADHYA PRADESH
07%
9.26 mn

5 KARNATAKA
10%
23.69 mn

2 TAMIL NADU
14%
20.14 mn

% age Detections/Endpoint Detections

Source: https://www.surveyofindia.gov.in/pages/outline-maps-of-india

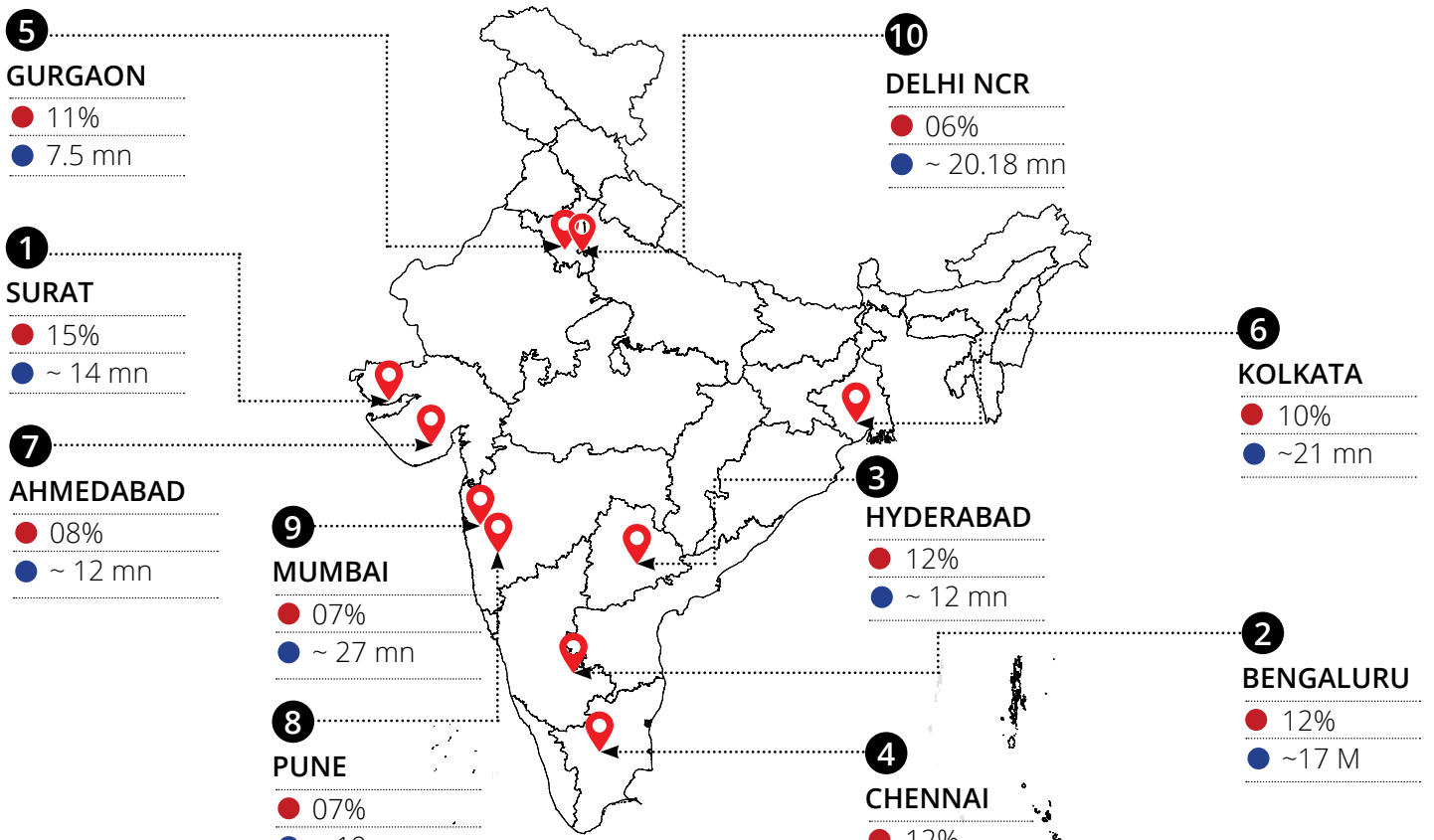
Disclaimer: The data that has been rationalized and the insights provided are depicted as per SEQRITE installation base.

Top 10 Cities with Highest Malware Detections

~40% of the total detections originate from these cities.

160 mn Detections

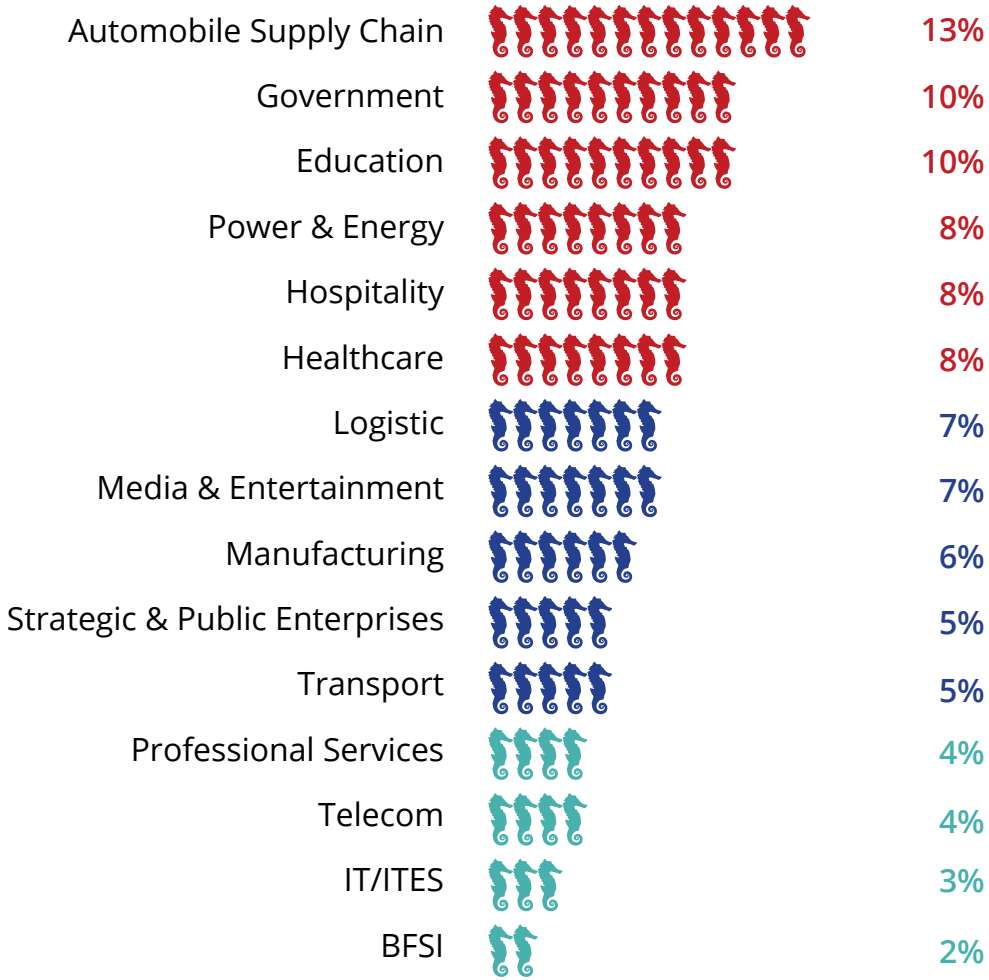
- A city-wise analysis reveals that Mumbai, Pune, Chennai and Bangalore have the highest number of detections in absolute terms. Surat and Ahmedabad, which have emerged as new IT/ITeS hubs, have high detections relative to their installation base.
- The top 10 cities account for more than 50% of the detections, while the remaining detections are spread across tier II and III cities and towns in India. This may be due to the rise of work-from-hometown culture amid the pandemic.



Source: https://www.surveyofindia.gov.in/pages/outline-maps-of-india

Disclaimer: The data that has been rationalized and the insights provided are depicted as per SEQRITE installation base.

India Malware Landscape: Sectoral Analysis



INDUSTRY-WISE PERCENTAGE DETECTIONS PER INSTALLATION BASE

The **Automotive Supply Chain, Government and Education** are the top three industry segments with the **highest malware detections** per installation base across the industry.

The automotive industry, which was once relatively immune to widespread and notorious threats, has become a prime target for malicious actors who seek to disrupt operations, steal sensitive data, and compromise supply chains. In 2023, we observed an escalation in both the volume and the impact of cyber-attacks on the auto industry.

India is one of the most vulnerable countries to state-sponsored threat actors, especially those targeting government agencies.

Some of these cyber attacks are orchestrated by state-backed actors on strategic occasions such as the G20 summit.

The Education sector faces common attack vectors such as phishing and user account compromise. User account compromise is prevalent in this sector, as it manages a variety of accounts for staff, third-party contractors, educators, students, alumni, etc., with a high turnover rate. The most dominant threat in the education sector was W32. Neshta.C8, a malicious software that poses a formidable challenge to educational institutions.

The **Power and Energy sector** in India is a critical component of the country's economic growth story, making it a lucrative target for cyber attackers that can cause significant service disruptions and physical damage to infrastructure. The attackers target different departments such as supply and procurement, cloud and infrastructure, legal, IT and OT. Cyber supply chain risk visibility is essential to mitigate threats in this sector. The revived new variant of Expiro infector has the highest detections in this sector.

As India progresses towards digitalizing the healthcare sector, it has become imperative to secure the online systems. According to a new study by Sophos, a UK-based cybersecurity firm, reported by the Economic Times, nearly 60% of healthcare organizations in India have experienced a cyberattack in the past 12 months. Nimda variant was the most prominent threat with the highest detections in the Healthcare and Hospitality segment.

Indian manufacturing firms faced increased risks from unsecured IoT devices connected to the network, more than any other sector. Manufacturing organizations believe that 5G adoption will exacerbate security gaps. The sector suffered ransomware attacks that halted manufacturing operations. The SMEs in this segment endured sophisticated social engineering phishing attacks.

In addition to manufacturing, the logistics, banking and financial sectors are also under the radar of cyber-attacks. The financial sector is leading the digital transformation and with the platform economy in action, attacks on low-value transaction businesses are also relevant. Lending apps that request access to sensitive information surged in India during this period.

Automobiles

~6 in every 10 detections

~11,800 Endpoints

2,17,000+

Trojan.NSIS.Miner.SD

Trait: Gains access via hacked sites/links, installs from malicious sources, auto-runs on startup, alters system files/registry, degrades performance with resource-intensive bitcoin mining, and opens a backdoor for other malware.

Government

~2 in every 10 detections

~2,84,000 Endpoints

30,4000 +

Remoteadmin.Remoteexec

Trait: Enables remote installation, execution, and updates of applications, programs, and files on Windows network systems.

Education

~4 in every 10 detections

~1,58,000 Endpoints

8,53,000+

W32.Neshta.C8

Trait: It self-extracts data, executes a dropped binary, and establishes autorun at Windows startup.

Power & Energy

~5 in every 10 detections

~2000 Endpoints

13,000 +

W32. Expiro.R3

Trait: Infects files by appending its virus code to the files. Enters the system from cracked softwares, Drive-by-download, Malvertising campaigns etc. Steals browser certificates and passwords & store at

%AppData%|<random_hex_values>.bin. Creates mutexes

Logistics

~2 in every 10 detections

~3,900 Endpoints

11,000+

Trojan.YakbeexMSIL.ZZ4

Trait: Employs multiple techniques: extracting code, creating memory, dropping/executing binaries, using Windows utilities, keystroke logging, autorun at startup, file attribute manipulation for false deletion appearance, self-replication, altering Explorer settings, encrypting files, and obstructing access to the victim's workstation.

Media & Entertainment

~1 in every 10 detections

~13,800 Endpoints

10,500+

Trojan.Rdpwrap

Trait: Introduces a vulnerability, allowing potential hackers to infiltrate and deploy Trojan horse software for unauthorized data access and control.

Manufacturing

~1 in every 10 detections

~2,20,000 Endpoints

3,32,000+

PIF.StucksNet.A

Trait: Deploys a .LNK file as a shortcut to its main executable, leveraging CVE-2010-2568 to execute arbitrary code on victim machines, a vulnerability famously exploited in Stuxnet.

BFSI

~5 in every 10 detections

~47000 Endpoints

87,000+

W32.Pioneer.CZ1

Trait: Infects files, deploys a malicious DLL, and sends system information to a remote server.

Transport

~4 in every 10 detections

~1600 Endpoints

4700+

Script.Trojan.A3676696

Trait: Quarantine to prevent spreading or removes files entirely as per F-Secure security settings.

Professional Services

~2 in every 10 detections

~2,85,000 Endpoints

5,02,000+

Trojan.KillAv.DR

Trait: Drops a file and can deliver and execute well-known malware like Skype spy or antivirus service killers; it also transmits victims' IP addresses and related data to the malware authors, often disguising itself with icons resembling genuine Windows applications.

Telecom

~7 in every 10 detections

~1600 Endpoints

7,000+

Nsis.Bitmin

Trait: Mines cryptocurrency, avoiding performance issues and intrusive ads, highlighting the need for its prompt removal to safeguard the system.

IT/ITES

~1 in every 10 detections

~69,900 Endpoints

48,500+

Worm.AUTOIT.Tupym.A

Trait: The malware drops and executes a file in the system32 folder, establishes a connection to a malicious website, alters the browser's start page via registry modification, and creates a persistent Run entry for the dropped file.

Strategic & Public Enterprises

~2 in every 10 detections

~4800 Endpoints

12,600+

Trojan.Shadowbrokers

Trait: Exploits specific SMB vulnerabilities, named after the group that disclosed them, the ShadowBrokers (aka Equation group).

Featured Stories 2023

Cryptocurrency Conundrum:
Unveiling the Enigma of Cryptojacking Exploits

- **Criticality:** High
- **Sectors Targeted:** All
- **Countries Affected:** Worldwide

Cryptojacking is illegal cryptomining, cybercriminal secretly uses someone else's resources, without their knowledge or permission, to mine cryptocurrencies. Large-scale Cryptojacking is emerging as a popular trend in the world of cyber crime.

Engaging in mining activities does not require extensive technical expertise, as the essential tools are frequently open-source or easily accessible for purchase. The emergence of cloud mining has heightened the risk of increased incidents. Moreover, the algorithm utilized in Cryptojacking is remarkably efficient with CPUs, negating the necessity for a GPU. This efficiency enables malicious actors to deploy miners such as XMRig across devices.

This encompasses utilizing cloud services, such as using Kubernetes clusters for mining the cryptocurrency Dero, and even targeting Android devices.

Over the past year, there has been an observed increase in hits from the NiceHashMiner payload, reaching a peak in the month of July 2023. Rise in cross-platform malware is also observed.

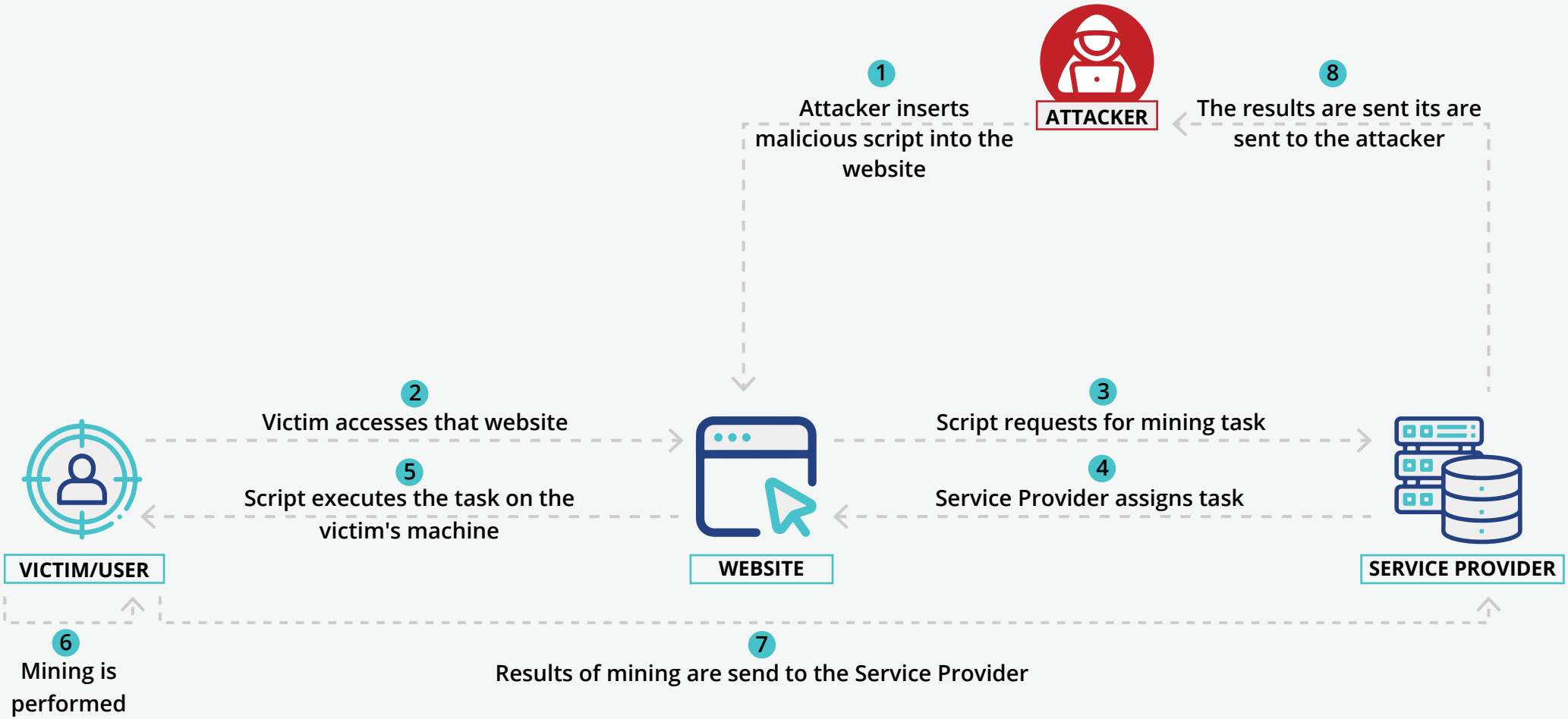
Security professionals should be vigilant for the following malware associated with Cryptojacking attacks: HonkBox (MacOS), Scrubcrypt (targets Oracle WebLogic Servers and bypasses Windows Defender protections), Lucifer Trojan (targets both Windows and Linux), and QubitStrike Campaign (targets Jupiter Notebooks).

37%
Annual increase in cases

14.3m
Detections

XMRig
prominent Malicious Actor

Cross-Platform
Malwares



Uncovering LockBit Black's Attack Chain and Anti-forensic activity

- **Criticality:** High
- **Sectors Targeted:** Healthcare, Finance, Manufacturing, Transportation and Government agencies.
- **Countries Affected:** United States, United Kingdom, Canada, Japan, Germany, India.

Since the dissolution of the Conti ransomware group, the LockBit group has emerged as a dominant force in the cybersecurity landscape. This transition is marked by the adoption of new extortion techniques and the implementation of a groundbreaking bug bounty program. The LockBit 3.0 variant, subject to thorough investigation and analysis, exhibits a high infection vector and a sophisticated attack chain characterized by significant anti-forensic measures.

LockBit's 3.0 variant, specifically the Black variant, has been observed engaging in anti-forensic activities. These activities include the simultaneous clearing of event logs, termination of multiple tasks, and the deletion of services. The group uses various tactics for initial network access, such as SMB brute-force attacks from diverse IPs, allowing for lateral movement across the victim's network to execute the ransomware payload.

The group uses the sys-internal tool PSEXEC to execute malicious BAT files on a single system, leaving traces indicative of modifications to RDP and authentication settings, along with the simultaneous disabling of antivirus solutions. PSEXEC is also leveraged for lateral movement within the victim's network. The malware employs encryption with a multi-threaded approach, selectively targeting shared drives. Encrypted files bear the distinctive ".zbzdbs59d" extension, hinting at the generation of each payload with a random static string.

The encryption utilizes a multi-threaded approach, exclusively targeting shared drives. To execute the payload successfully, a valid key must be passed along with the command-line option '-pass.' Encrypted files bear the distinctive ".zbzdbs59d" extension, suggesting that the builder generates each payload with a unique, randomly generated string. It is vital that each payload is accompanied by a valid key for file encryption.

In instances where Admin privileges are lacking during execution, the malware uses CMSTPLUA COM to circumvent the UAC prompt, leveraging the legitimacy of the Windows Connection Manager Service. Anti-debugging techniques are also observed, along with the tactic of changing the wallpaper. Despite the builder being leaked, LockBit 3.0 has ascended to the forefront of the Ransomware-as-a-Service (RaaS) model. This is attributed to the introduction of its bug bounty program and the adoption of innovative extortion tactics. Remarkably, the threat has persisted even as malicious actors create their own variants based on the leaked builder.

Initial Access
SMB Brute Force of unprotected systems

Execution
of Malicious BAT scripts

Initial Access
PsExec to run the ransomware

Encryption
of Shared Drives

01
After initial access via SMB brute forcing, **malicius BAT files are** executed to modify authentication settings and disabling AV - openrdp.bat, mimon.bat, auth.bat etc.

02
Pseudo code for decrypting PE Sections. TEXT, DATA, and PDATA are 3 sections decrypted in memory.

03
Privilege escalations - UAC Bypass using **CMSTPLUA**

04
Thread Hide From Debugger. This hinders dynamic analysis by inhibiting debug information from the current ransomware thread to reach the attached debugger.

05
Logs are disabled by setting multiple registry subkeys to value 0. *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels* *Specifically, Windows Defender is disabled for evasion.

09
Ransomware Note on Screensaver

08
Files are encrypted by creating multiple threads where each filename is replaced with a random string generated and appending the extension to them. With full encryption completed under 2 minutes

07
Before encryption, the ransom note is created in every directory except the Program Files and the Windows directory, which are not encrypted

06
Process terminated includes SecurityHealthSystray.exe and the mutex created during execution was 13fd9a89b0eede2627293472 8b390e06

Fake applications disguised as legitimate ones

- **Criticality:** High
- **Targets:** Android Users
- **Countries Affected:** India

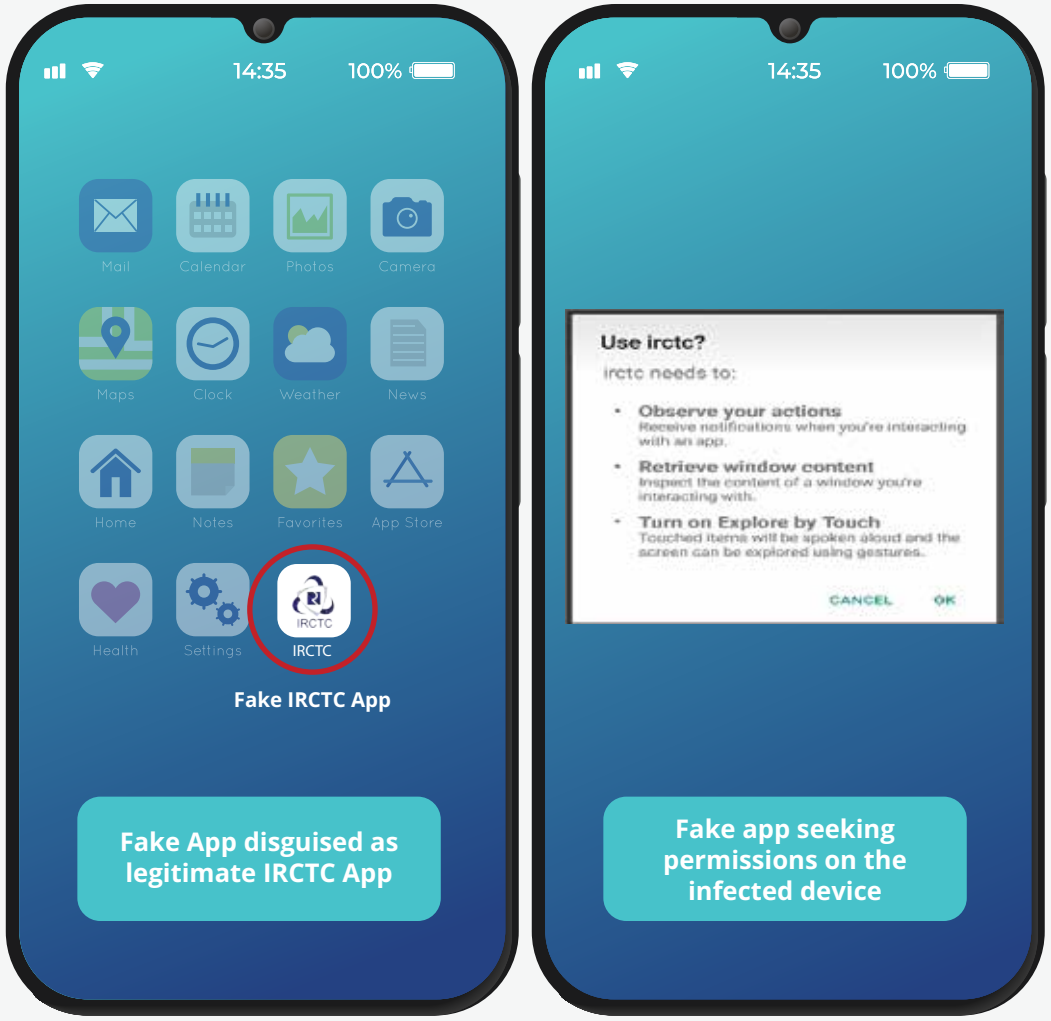
In a recent alert, the Indian Railway Catering and Tourism Corporation (IRCTC) cautioned users about a malicious Android app, irctcconnect.apk, that circulated on messaging platforms like WhatsApp and Telegram. The fraudulent app, masquerading as an official IRCTC app, posed a serious risk to users by functioning as spyware.

The deceptive app was capable of stealing Facebook and Google credentials, extracting codes from Google Authenticator, tracking GPS and network locations, recording videos using the Camera API, and collecting information about installed applications on users' devices.

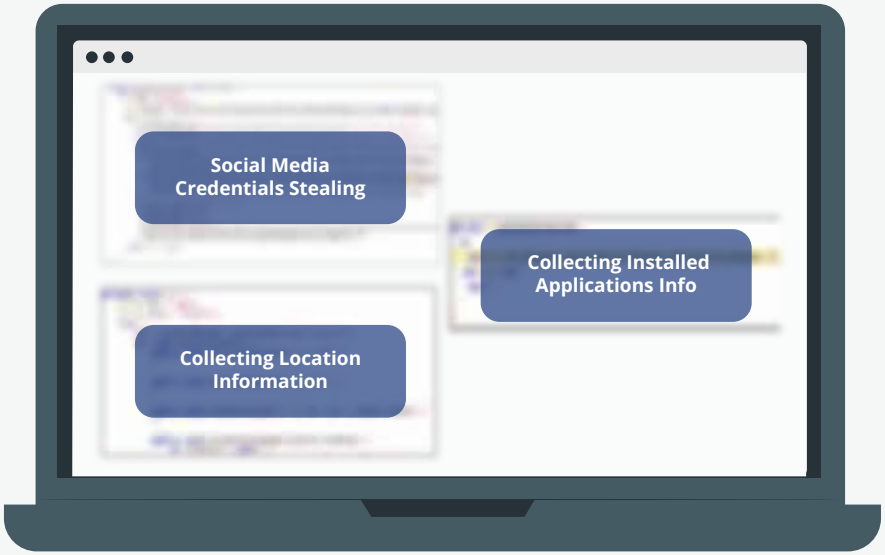
IRCTC's advisory emphasized the app's malicious nature and warned users against downloading it. The phishing links, distributed widely, impersonated IRCTC officials to trick users into revealing sensitive net banking credentials, including UPI details and credit/debit card information.

Antivirus programs have the capability to identify and detect malicious applications, specifically those that share similarities with "Android.SpyNote.GEN."

On Screen



Behind the Screen



Indicator of Compromises (IOCs)

Android.SpyNote.GEN.

1. 45c154af52c65087161b8d87e212435a
2. c01566f5feb7244ed4805e2855ebdc400
3. c77435e6e77152d24e86eb75e1f04d75

Battling the death trap of malicious loan apps

- **Criticality:** Medium
- **Targets:** Android Users
- **Countries Affected:** India

In the age of instant finance at our fingertips, loan apps have reshaped how we access funds. However, beneath the convenience lies a concerning trend—malicious apps that are being linked to tragic outcomes. A spate of tragic deaths has occurred in the last 2-3 years PAN India. The reason: seemingly genuine loan applications with sinister motives behind them. Victims comprise individuals who opted to take loans from such apps but ended up committing suicide instead, driven by harassment, blackmail, and abuse by operators of these loan apps.

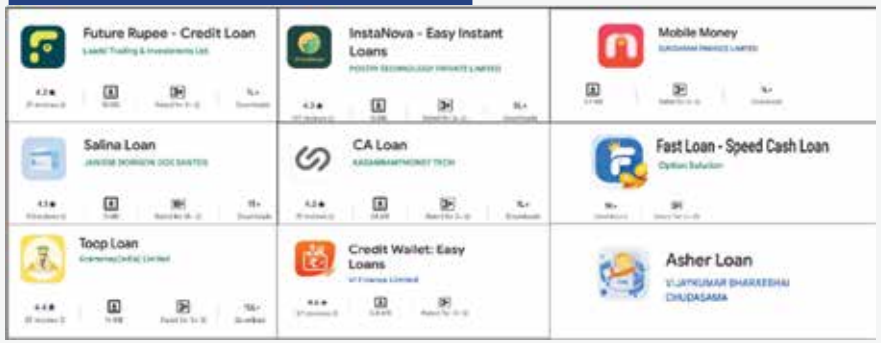
These applications offer small loans without requiring much paperwork but, in turn, charge heavy interest rates and often resort to extortion through morphed photographs and cyberbullying. Many of these apps compel users to share unnecessary information, including contact details, photographs, location, and more. Subsequently, the operators behind these apps use these details to harass the victim with defamatory messages and manipulated photographs sent to their contacts, and so on. This unwarranted harassment leads to some users experiencing depression and attempting suicide out of fear of public humiliation. These applications request permissions, and a few of these permissions are unnecessary, such as android.permission.BLUETOOTH and android.permission.READ_CALL_LOG.

Countermeasures

Google has been proactive in removing 3500 such applications from their Play Store and mandated that developers to take measures such as set the application category to ‘finance’, mention the minimum and maximum period of repayment, mention maximum annual percentage rate which may include interest and other fees. In addition to this, Google has also restricted loan apps which require repayment in full within 60 days. Personal loan applications are no longer allowed to access sensitive data, such as photos and contacts.

Reserve Bank of India (RBI) has also published guidelines that states that Regulating Entities (RE) should ensure that their DLA (Digital Lending Applications) should not access mobile phone resources like media, contact list, call logs or telephony functions.

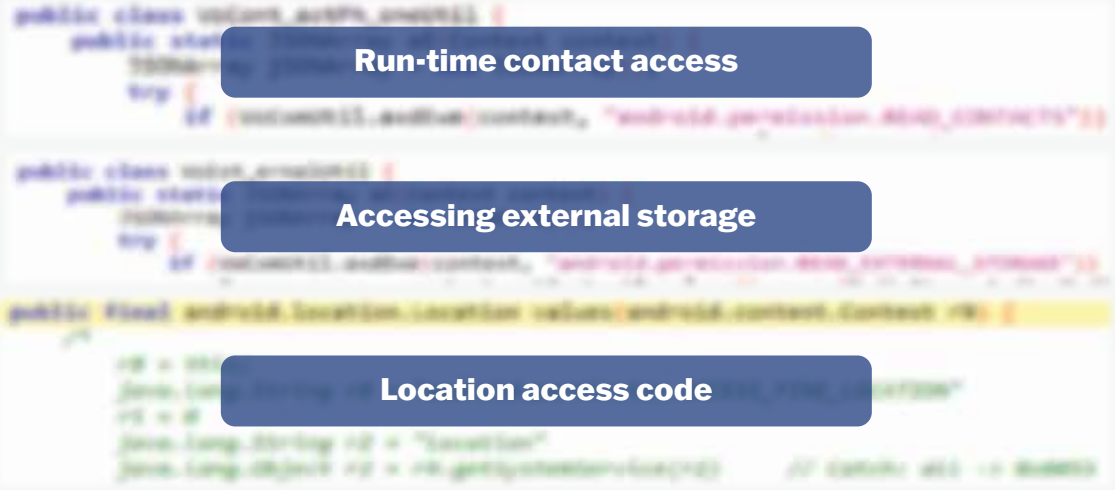
Reported Loan applications



Permissions declared by App

- READ_SMS
- CAMERA
- READ_PHONE_STATE
- ACCESS_COARSE_LOCATION
- READ_CALL_LOG
- BLUETOOTH
- INTERNET
- ACCESS_WIFI_STATE
- CHANGE_WIFI_STATE

Process followed by these applications to retrieve sensitive information



Indicators of compromise(IoC)

Application Name	Package Name
Future Rupee – Credit Loan	com.future.cash.rupee
InstaNova – Easy Instant Loans	com.wavfge.magfin
Mobile Money	com.mobile.money.cash
Salina Loan	com.salina.loan.mountain
CA loan	com.assistance.career.loansindia
Fast Loan- Speed Cash Loan	com.fastloan.cashloan.instantloan.loanapp
Toop Loan	in.azme.high.top.loan
Credit Wallet: Easy Loans	com.ceditwallet.now
Asher Loan	com.asher.loan.cocla

Expiro: Old virus poses a new challenge

- **Criticality:** High
- **Sectors Targeted:** Power and Energy
- **Regions:** South Asia

Expiro is no stranger in the family of viruses, having existed since 2011. However, over the last one and a half years, a sudden surge in Expiro cases has been witnessed, primarily targeting regions in India. Two different versions of Expiro, one involves a multiple-layered, complex code to retrieve patched code from the infected file, and the other version modifies the imports of the clean file. Despite the differences, both versions share the common goal of infecting executable files on the system by appending virus code at the end. Upon execution, the infector code is run, and the malicious call is patched with a new address to execute the benign code. Restoring the file to its original offset proves challenging due to the compressed and encrypted nature of the overwritten code, which gets decrypted during runtime through highly obfuscated decompression and decryption routines.

The infection routine is executed in a manner that allows user applications to run seemingly normally, unbeknown to the user. This Expiro variant possesses the capability to check network-mapped drives, infecting executable files on those drives and potentially spreading the infection across the network. Additionally, observations indicate this variant performing backdoor capabilities by connecting to remote servers. Expiro can receive commands from these servers, executing them on the infected system, including the installation of other malware capable of stealing and uploading sensitive information.

Power and Energy sector had maximum detections of Expiro attacks

Source

The infection vector:

- Cracked or patched version of software
- Driven-by-download: File download upon visiting an infected website
- Dropped by some other malware, USB drives, Malvertising campaigns, etc.

Infects both 32-bit and 64-bit executable files. The new variant of Expiro is a type of "Appender" virus, that infects files by inserting virus code at the end of the file, specifically the last section of the executable file.

File Infection Process

- The new variant of Expiro patches a call in the executable section that further jumps to the last section, at an offset where the malicious virus code is present. The code to calculate and select which Call to patch is highly obfuscated.
- Upon analysing multiple files of this variant, it was found that the decompressed buffer for most of the infected files remains same and the wrapper keeps changing.
- After successful decompression and decryption, the infected application is launched, and it starts infecting other executables present in the system.
- Due to the use of obfuscated call patching routine and encrypted virus code data, it is challenging to clean infected codes with complete accuracy.

Risks posed by Expiro

Expiro possesses capabilities to accept commands from its controller and execute them on the infected systems.

With successful commands delivered to victims, Expiro can:

- Install other malwares (like keyloggers, spywares, ransomware, etc.)
- Steal and upload sensitive information
- Disable security software from the systems
- Hijack servers
- Establish itself to act at a later point in time

DarkRace Ransomware:
A deep dive into its techniques and impact

- **Criticality:** High
- **Sectors Targeted:** Manufacturing, Financial, Transportation, Science & Technology
- **Regions:** Europe and United States

Brief:

DarkRace ransomware is a derivative of the infamous Lockbit ransomware, incorporating heavily from its leaked source code.

How it spreads:

- Cracked Software Infiltration: The ransomware discreetly enters systems through cracked software installations using obfuscator technology.
- Phishing Email Attacks: DarkRace employs social engineering in phishing emails, deceiving users into activating exploit kits and initiating ransomware attacks.

This section below delves into the key characteristics and tactics employed by DarkRace, shedding light on its intricate functionalities.

Mutex Checks: Efficient Resource Utilization and Stealth Operation

DarkRace implements Mutex checks on infected systems, a strategic measure to prevent multiple infections on the same system. This not only ensures efficient use of resources but also mitigates the risk of detection arising from excessive activity. By employing Mutex checks, DarkRace operates stealthily, enhancing its overall effectiveness in compromising targeted systems.

Runtime Decryption: Unveiling Crucial Information Dynamically

The ransomware incorporates runtime decryption mechanisms for XML data, encompassing critical information such as the ransom note, whitelisted files, folders, and extensions. This dynamic decryption approach allows DarkRace to adapt its tactics during runtime, maintaining flexibility and further complicating efforts to counter its malicious activities.

Encryption using Salsa20: Speed and Security in File Compromise

DarkRace leverages the Salsa20 stream cipher, renowned for its speed and security, as the encryption algorithm of choice. This robust encryption method is employed to encrypt files on the victim's system, appending a random extension to them. This deliberate action renders the files inaccessible until a ransom is paid to acquire the decryption key, adding a layer of complexity to recovery efforts.

Post Encryption Measures: Heightened Security Evasion and Covering Tracks

Post-encryption, DarkRace adopts additional measures to make recovery more challenging. This includes the deletion of shadow copies, hindering traditional recovery methods. Going a step further, DarkRace terminates processes that might interfere with its operation or could potentially be used to recover encrypted data. After executing its malicious activities, the ransomware takes the drastic step of deleting its own files and restarting the system. This deliberate act adds an extra layer of complexity, making it exceptionally challenging for cybersecurity experts to trace its activities and develop effective countermeasures.

Mutex Checks

- Prevents multiple infections on the same system for efficient resource utilization.
- Avoids detection by limiting excessive activity.

Runtime Decryption

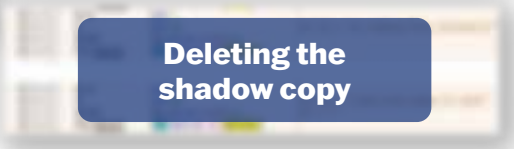
- Decrypts XML data, revealing information like ransom notes and whitelisted files.
- Enhances flexibility and adaptability in handling encrypted content

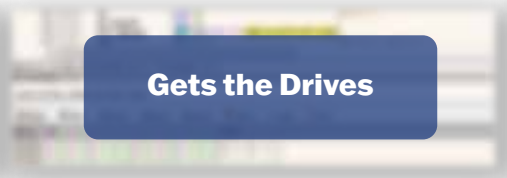
Encryption with Salsa20

- Utilizes the salsa20 stream cipher for swift and secure file encryption.
- Appends a random extension to files, rendering them inaccessible until ransom payment.

Post Encryption Measures

- Deletes shadow copies to hinder recovery efforts.
- Terminates interfering processes, covering its tracks, and restarts the system for added evasion.





Critical Zero Day Vulnerability in MOVEIT transfer

- **Criticality:** High
- **Sectors Targeted:** Government, Finance, Media, Aviation, Healthcare
- **Countries Affected:** United States

MOVEit Transfer is widely recognized as a secure and popular managed file transfer program utilized by enterprises to safely transfer data using protocols such as SFTP, SCP, and HTTP-based uploads. This specific vulnerability, referred to as “CVE-2023-34362”, heightens the risk of unauthorized access and exploitation of elevated privileges within the system.

It initiates from a SQL injection vulnerability that could grant unauthorized individuals access to the MOVEit Transfer database if exploited.

The vulnerability is actively targeted, with attackers leveraging HTTP or HTTPS channels to exploit. After successfully exploiting the vulnerability, the attacker deploys a web shell (human.aspx), a hidden entry point for future access.

Through this deployed web shell, the threat actor gains continued backdoor access to the compromised system, establishing a means for continuous control. Subsequently, they initiate data exfiltration activities, secretly extracting sensitive information without authorization.

Certain patterns of requests are frequently observed when attempting to implant malicious web shells.

These patterns often serve as indicators of compromise. The software provider quickly develops a patch to fix the identified vulnerability, ensuring users can update their MOVEit Transfer installations and protect their systems from potential exploitation.

Observed patterns of requests

GET / - on port 443
POST /guestaccess.aspx - port 443
POST /api/v1/token - port 443
GET /api/v1/folders - port 443
POST /api/v1/folders/[PATH/files upload Type-resumable - port 443 ← File Upload
POST/machine2.aspx - port 80
POST/moveitisapi/moveitisapi.dil - port 443 ← SQL Injection
POST /guestaccess.aspx - port 443
PUT /api/v 1/folders/[PATH/files uploadType-resumable& fileId-[FILEID] - port 443 ← File Upload
POST/machine2.aspx - port 80
GET /human2.aspx - port 443 ← Access Webshell

Steps for prevention

Update MOVEit Transfer:
- Upgrade to patched versions: MOVEit Transfer 2023.0.1, 2022.1.5, 2022.0.4, 2021.1.4, 2021.0.6.

Disable HTTP and HTTPS Traffic:
- Modify firewall rules to block incoming traffic on ports 80 and 443, preventing potential attacks on MOVEit Transfer.

Remove Unauthorized Files and Users:
- Delete "human2.aspx" and scrutinize and eliminate

OneNote Exploits:
The latest weapon in cybercrime

- **Criticality:** High
- **Sectors Targeted:** Windows Users
- **Regions:** India, China, European Union, United States, & Africa

OneNote, with a significant installation base worldwide and extensive use for note maintenance is facing a new malware distribution method that raises concerns among users. Malicious actors are disguising malware as OneNote files and distributing them through email and other messaging platforms. These malicious spam (Mal spam) emails masquerade as various documents, including DHL shipping notifications, invoices, ACH remittance forms, mechanical drawings, and shipping documents.

The attackers embed malicious Visual Basic Script (VBS) attachments into OneNote notebooks. When an unsuspecting user double-clicks on these attachments, the malware is launched. Notably, various Remote Access Trojans (RATs) like AsyncRAT, Quasar RAT, and NetWire have been observed using OneNote files for their distribution. Many of these OneNote files contain batch scripts that download the payload using PowerShell. Additionally, malware families such as QBot, IcedID, and Emotet have explored this file type.

In the case of the QBot campaign, the OneNote file contains obfuscated ".hta" files that download DLLs. Conversely, in the Emotet campaign, the infection chain is different. The OneNote file contains obfuscated VBScript with a ".wsf" file extension, cleverly hidden from end users. This file, in turn, downloads the Emotet DLL from a compromised website.

This sophisticated attack methodology poses a high level of criticality, especially given the widespread use of OneNote globally. Users are urged to exercise caution, particularly when receiving unexpected documents or files through email or messaging platforms to mitigate the risk of falling victim to this threat.

The Surge of BazaCall and Caller-Driven Malware Attacks

BazaCall has emerged as a potent technique since 2021, employing phone calls to entice targets into clicking malicious links and unknowingly installing malware.

Modus Operandi: Phishing emails with provided phone numbers lure victims into making calls, where operators convince them to grant remote access. Simultaneously, network operators exploit this access to clandestinely install backdoors.

- Affiliated ransomware groups leverage this method, recruiting callers proficient in multiple languages for vishing campaigns using "Callback Phishing".
- Evolving BazaCall tactics have seen the deployment of notorious malware strains like BazaarLoader, Trickbot, and IcedID, with a focus on the US, Canada, and select Asian countries.
- Underground forums witness a growing demand for individuals skilled in caller-based techniques. Some operators, working on bulk orders, strategically utilize toll-free numbers to avoid SIM blocking, underscoring the adaptability of this malicious approach.

Corporate Implications:

- Corporate entities must be alert to the rising threat of caller-based services, recognizing them as a new vector for malware infiltration.

Threat actor seeking caller services

I am looking for Callers for Ratting Mobile Carrier Store PC's Namely USA and UK Countries. Candidate must be Fluent in English and have Prior Experience in this Profession as well as must be Good in Social Engineering. You will be Provided Direct Link to the RAT Stub .exe File which You should be able to Convince the Store Employees to Download the File and Execute it. Monetary Compensation can be Discussed and Agreed upon. Interested Candidates can Contact me on my Telegram.

Also 1 am open to work with People who are into sim-swapping, Ratting Mobile Store PC's, etc. I have FUD RAT Stubs and looking for People who can RAT Mobile Carrier Store PC's. Profit will be Shared among us 50/50.

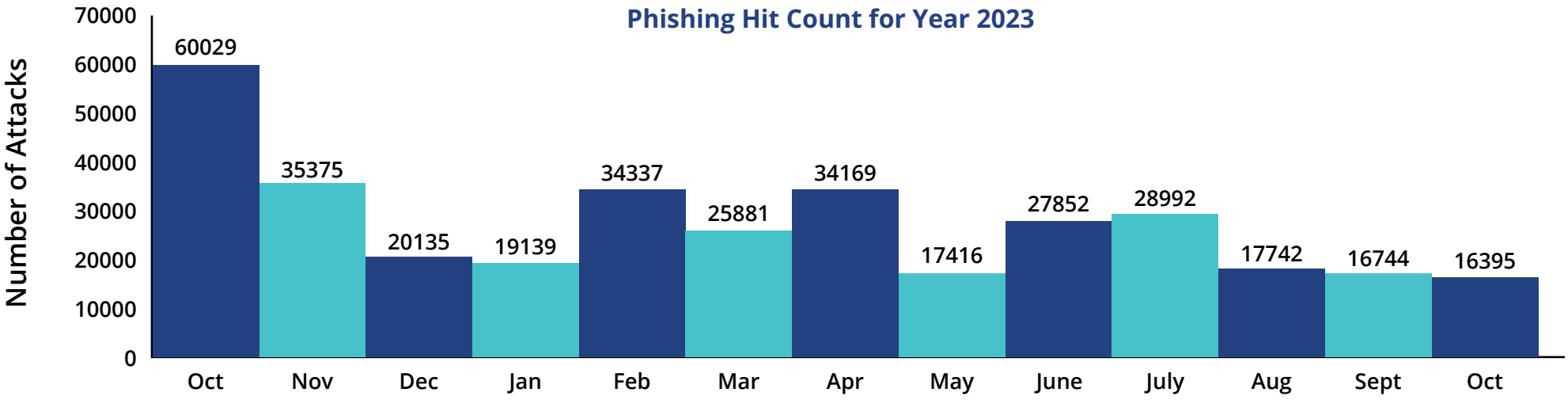
Affiliates of Threat Actors reaching out Targets

Hello,

We received an inquiry concerning an invoice correct? I was unable to locate your account with the information you sent out. Could you send over the phone number or email address attached to the account so that we can look into it for you?

Spam Mail randomization

{Health Policy: soft copy
{Insurance Database is Updated or invoice



WordPress Bookly Plugin Vulnerability:
CVE-2023- 1172 and CVE-2023-1159

- **Criticality:** High
- **Sectors Targeted:** All
- **Countries Affected:** Worldwide

A widely used WordPress plugin by over 60,000 websites is the "WordPress Online Booking and Scheduling Plugin – Bookly". Bookly streamlines online bookings and automates the reservation process. However, like many other WordPress plugins, it is vulnerable to exploitation by attackers. It allows unauthenticated attackers to inject malicious scripts, potentially compromising a site owner's entire site when they access the calendar tooltip from the plugin.

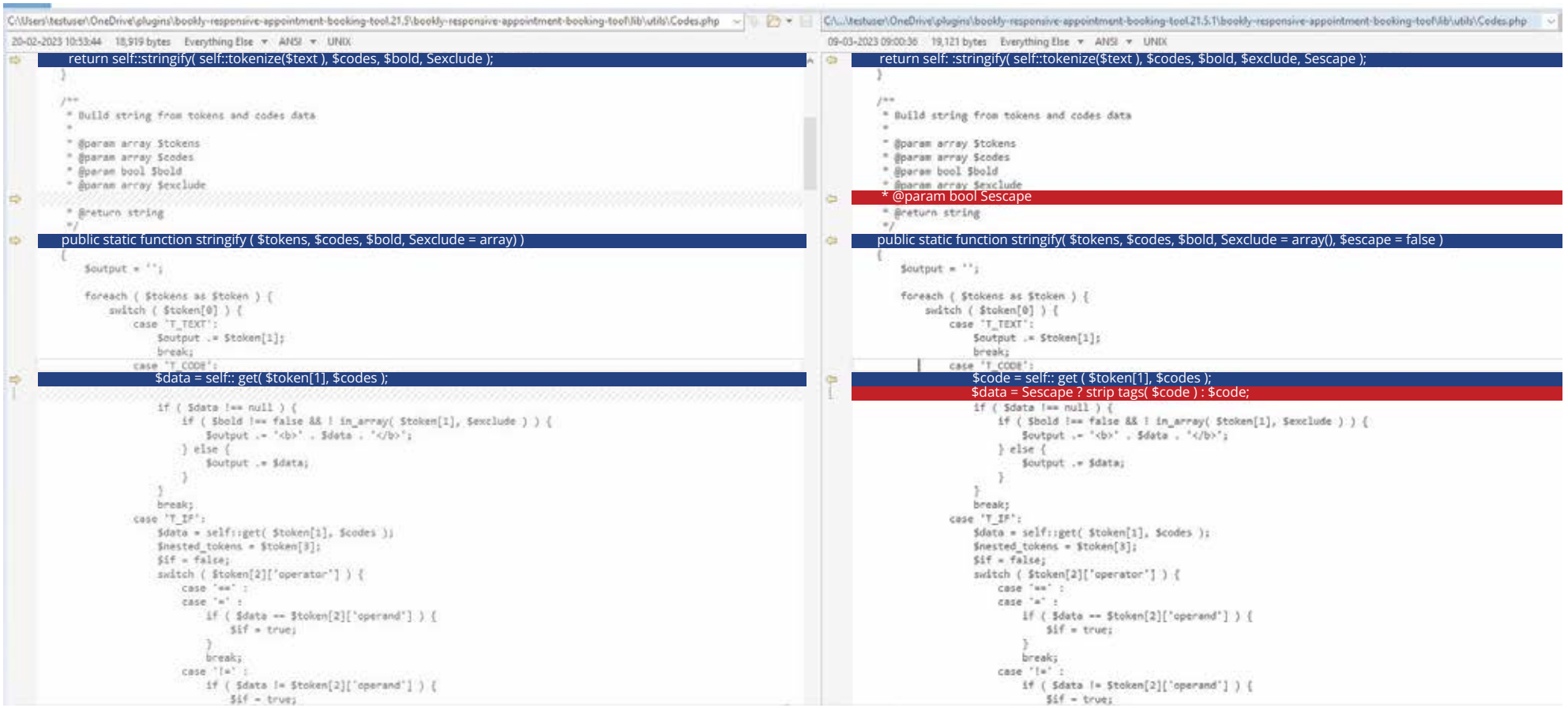
In March 2023, SEQRITE Labs uncovered two security vulnerabilities in the Bookly plugin for WordPress impacting users worldwide.

The first vulnerability, CVE-2023-1172, is a high severity Cross-Site Scripting flaw resulting from inadequate input sanitization and output escaping in the full name value. Unauthorized attackers can globally exploit this, injecting arbitrary web scripts onto pages, posing a significant risk with every user visit.

The second vulnerability, CVE-2023-1159, classified as medium severity, is a Cross-Site Scripting issue stemming from insufficient input sanitization and output escaping in the 'Service Title' field. Authenticated attackers with administrative privileges can leverage this vulnerability in multisite installations or where the "unfiltered_html" feature is disabled. They can insert web scripts into pages, which execute when users access the affected pages.
Both vulnerabilities have a global reach, with CVE-2023-1172 being of higher severity, emphasizing the critical need for users to address these security concerns promptly.

Research discovered that the Bookly plugin's "Full name" field was vulnerable to stored cross-site scripting (XSS) attacks. The plugin reuses the user's "Full name" input in multiple files, significantly increasing the risk of security breaches if the input is not properly sanitized and escaped to prevent malicious code injection.

The vulnerability has been fully resolved in plugin version 21.5.1. It is strongly recommended that WordPress site owners update their site to the latest patched version of the plugin (currently version 21.6 at the time of writing) to prevent potential attacks.



```
return self::stringify( self::tokenize($text ), $codes, $bold, Sexclude );
}

/**
 * Build string from tokens and codes data
 *
 * @param array $tokens
 * @param array $codes
 * @param bool $bold
 * @param array $exclude

 * @return string
 */
public static function stringify ( $tokens, $codes, $bold, Sexclude = array) )
{
    $output = '';

    foreach ( $tokens as $token ) {
        switch ( $token[0] ) {
            case 'T_TEXT':
                $output .= $token[1];
                break;
            case 'T_CODE':
                $data = self:: get( $token[1], $codes );

                if ( $data !== null ) {
                    if ( $bold !== false && ! in_array( $token[1], $exclude ) ) {
                        $output .= '<b>' . $data . '</b>';
                    } else {
                        $output .= $data;
                    }
                }
                break;
            case 'T_IF':
                $data = self::get( $token[1], $codes );
                $nested_tokens = $token[3];
                $if = false;
                switch ( $token[2]['operator'] ) {
                    case '==' :
                    case '=' :
                        if ( $data == $token[2]['operand'] ) {
                            $if = true;
                        }
                        break;
                    case '!=' :
                        if ( $data != $token[2]['operand'] ) {
                            $if = true;
```

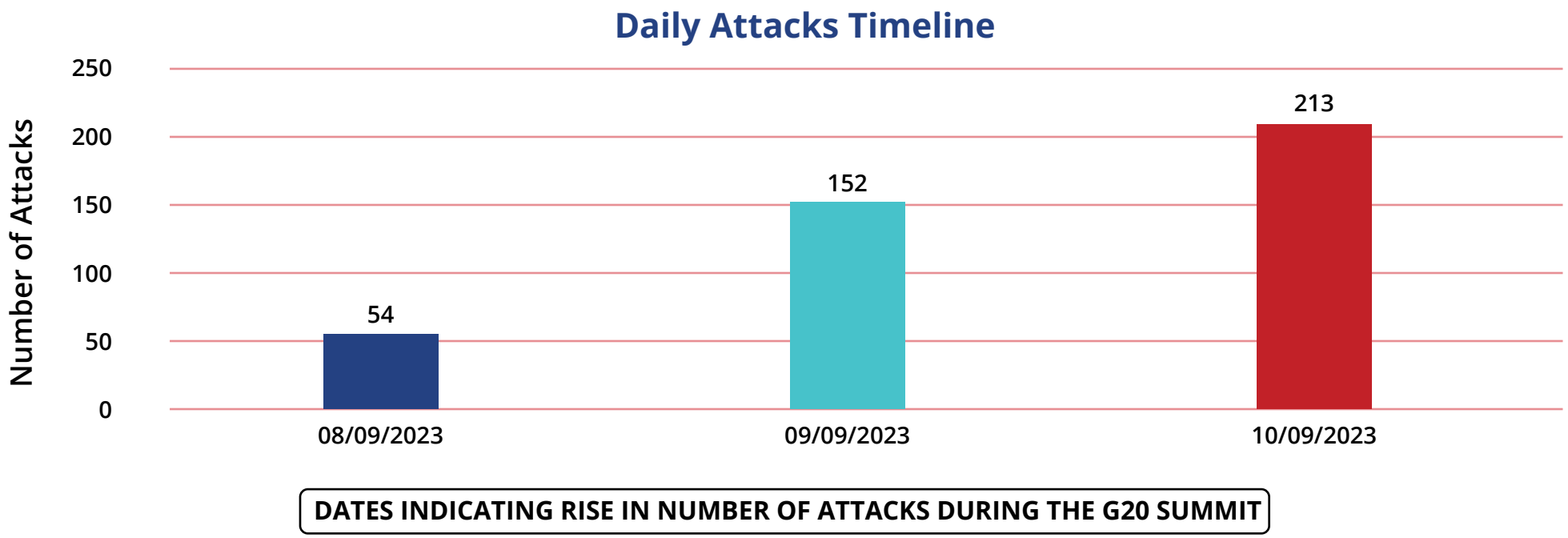
```
return self: :stringify( self::tokenize($text ), $codes, $bold, $exclude, Sescape );
}

/**
 * Build string from tokens and codes data
 *
 * @param array $tokens
 * @param array $codes
 * @param bool $bold
 * @param array $exclude
 * @param bool Sescape
 * @return string
 */
public static function stringify( $tokens, $codes, $bold, Sexclude = array(), $escape = false )
{
    $output = '';

    foreach ( $tokens as $token ) {
        switch ( $token[0] ) {
            case 'T_TEXT':
                $output .= $token[1];
                break;
            case 'T_CODE':
                $code = self:: get ( $token[1], $codes );
                $data = Sescape ? strip tags( $code ) : $code;
                if ( $data !== null ) {
                    if ( $bold !== false && ! in_array( $token[1], $exclude ) ) {
                        $output .= '<b>' . $data . '</b>';
                    } else {
                        $output .= $data;
                    }
                }
                break;
            case 'T_IF':
                $data = self::get( $token[1], $codes );
                $nested_tokens = $token[3];
                $if = false;
                switch ( $token[2]['operator'] ) {
                    case '==' :
                    case '=' :
                        if ( $data == $token[2]['operand'] ) {
                            $if = true;
                        }
                        break;
                    case '!=' :
                        if ( $data != $token[2]['operand'] ) {
                            $if = true;
```

RESOLVING THE ISSUE: A LOOK AT THE PATCH

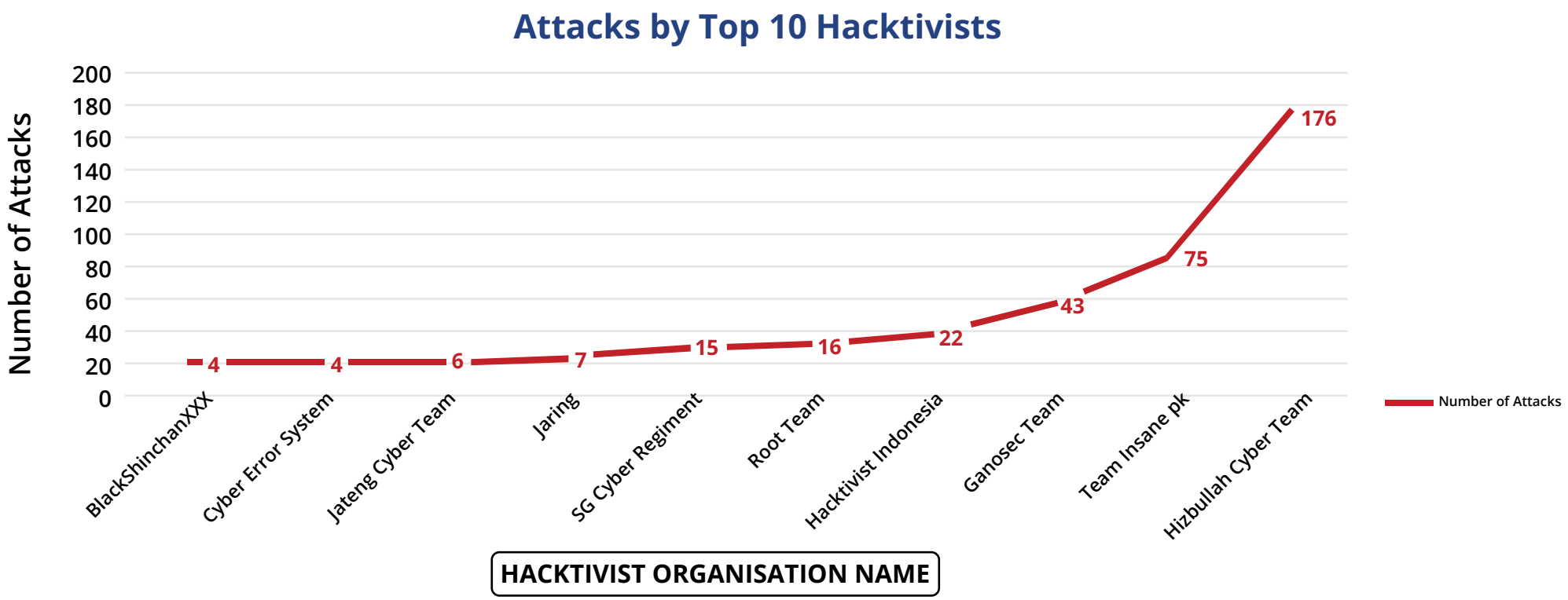
Multiple Hacktivist groups target India during the G20 Summit

Hacktivist groups from neighbouring countries had announced plans to attack websites of private and public entities in India during the G20 Summit. More than 30 hacktivist groups targeted around 600+ government and private entities through DDoS attacks, defacements, and data leaks.

The most targeted sectors were government, followed by finance, technology, public, and education industries. Similar coordinated attacks are anticipated next year during India's General Elections, Paris Olympics, etc.



DATES INDICATING RISE IN NUMBER OF ATTACKS DURING THE G20 SUMMIT


Attacks by Top 10 Hacktivists
Number of Attacks
200
180
160
140
120
100
80
60
40
20
0
4
4
6
7
15
16
22
43
75
176
BlackShinchanXXX
Cyber Error System
Jateng Cyber Team
Jaring
SG Cyber Regiment
Root Team
Hacktivist Indonesia
Ganosec Team
Team Insane pk
Hizbullah Cyber Team
HACKTIVIST ORGANISATION NAME
Number of Attacks

Decoding the Dynamics of Advanced Persistent Threats

Advanced Persistent Threat (APT) groups stand out due to their sophisticated techniques and specific target. This section outlines key details about prevalent APTs, expanding on their tactics and targets.

SideCopy: Initiating Complex Chains of Infection

- **Description:** SideCopy, distinguishes itself by distributing its own malware. The group employs a nuanced approach, often initiating attacks through malicious LNK files. These files set off a sophisticated chain of infection, leveraging multiple HTAs and loader DLLs, ultimately culminating in the deployment of final payloads.
- **Target:** SideCopy primarily targets Telecom, Power, and Finance sectors, showcasing a strategic focus on critical infrastructure and financial entities.

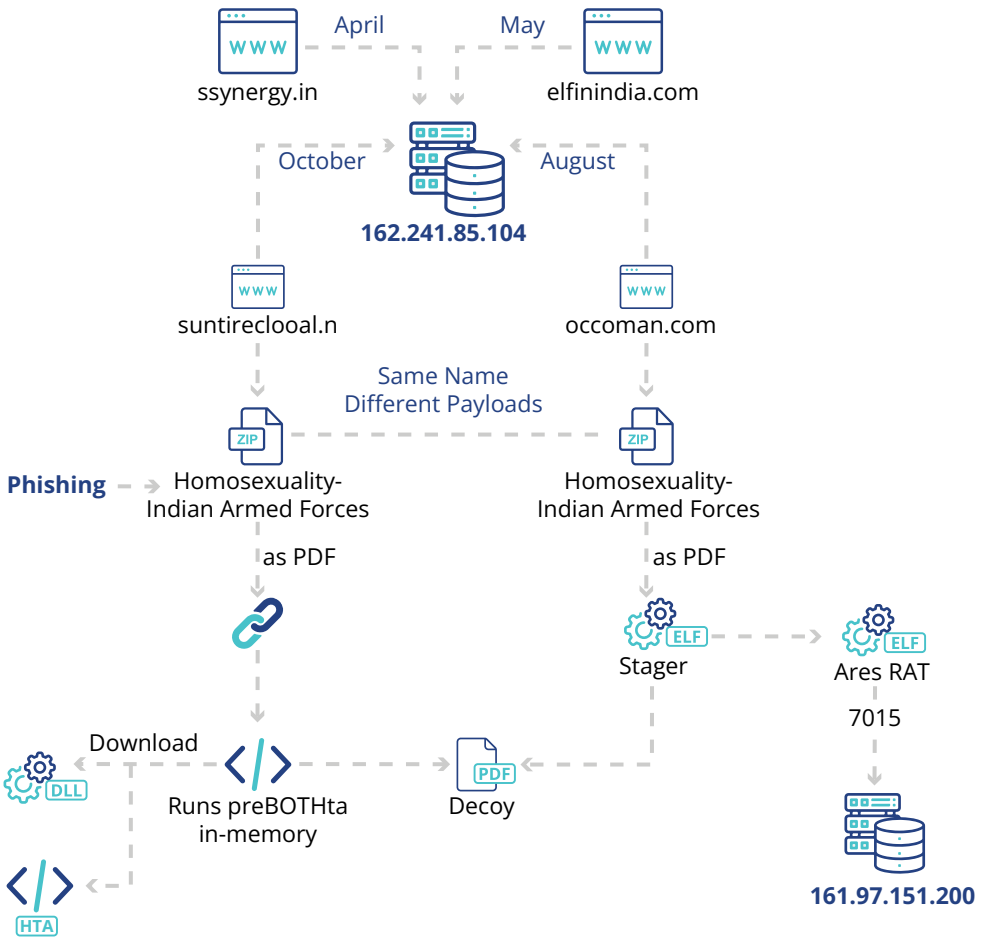
RedFoxtrot: A Prolific Actor in Asian Cyber Espionage

- **Description:** RedFoxtrot, active since at least 2014, specializes in targeting government and telecom sectors across Asian countries.
- **Target:** RedFoxtrot predominantly focuses on Defence Institutes and the Telecom Sector, aligning its activities with geopolitical developments.

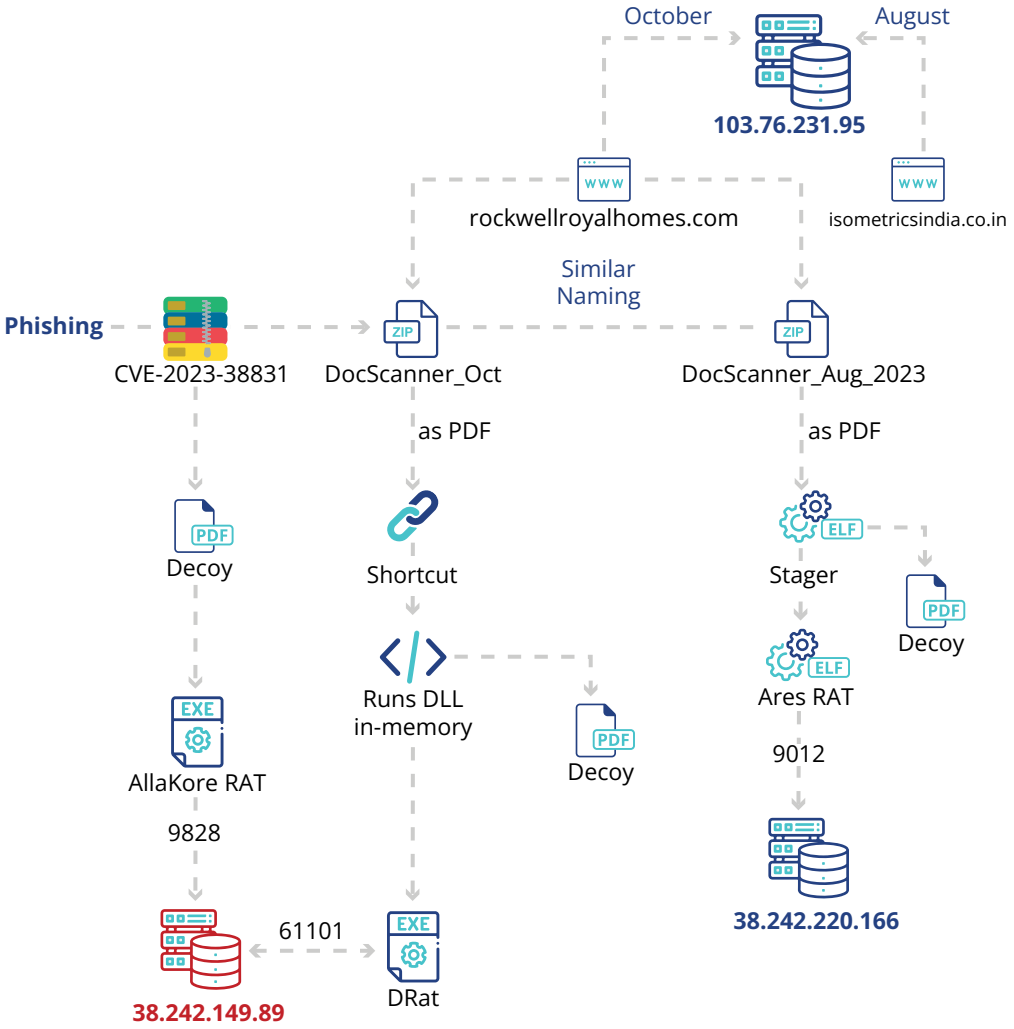
Transparent Tribe: Evolving Scope and Strategic Campaigns

- **Description:** Transparent Tribe is an APT group traditionally concentrated on Indian defence ecosystem. However, it is now targeting educational institutions and students in the Indian subcontinent. The group's malware arsenal includes the Crimson RAT, a consistent tool in its campaigns.
- **Target:** Transparent Tribe has its sights national information assets showcasing a multifaceted approach that encompasses government and critical infrastructure entities.

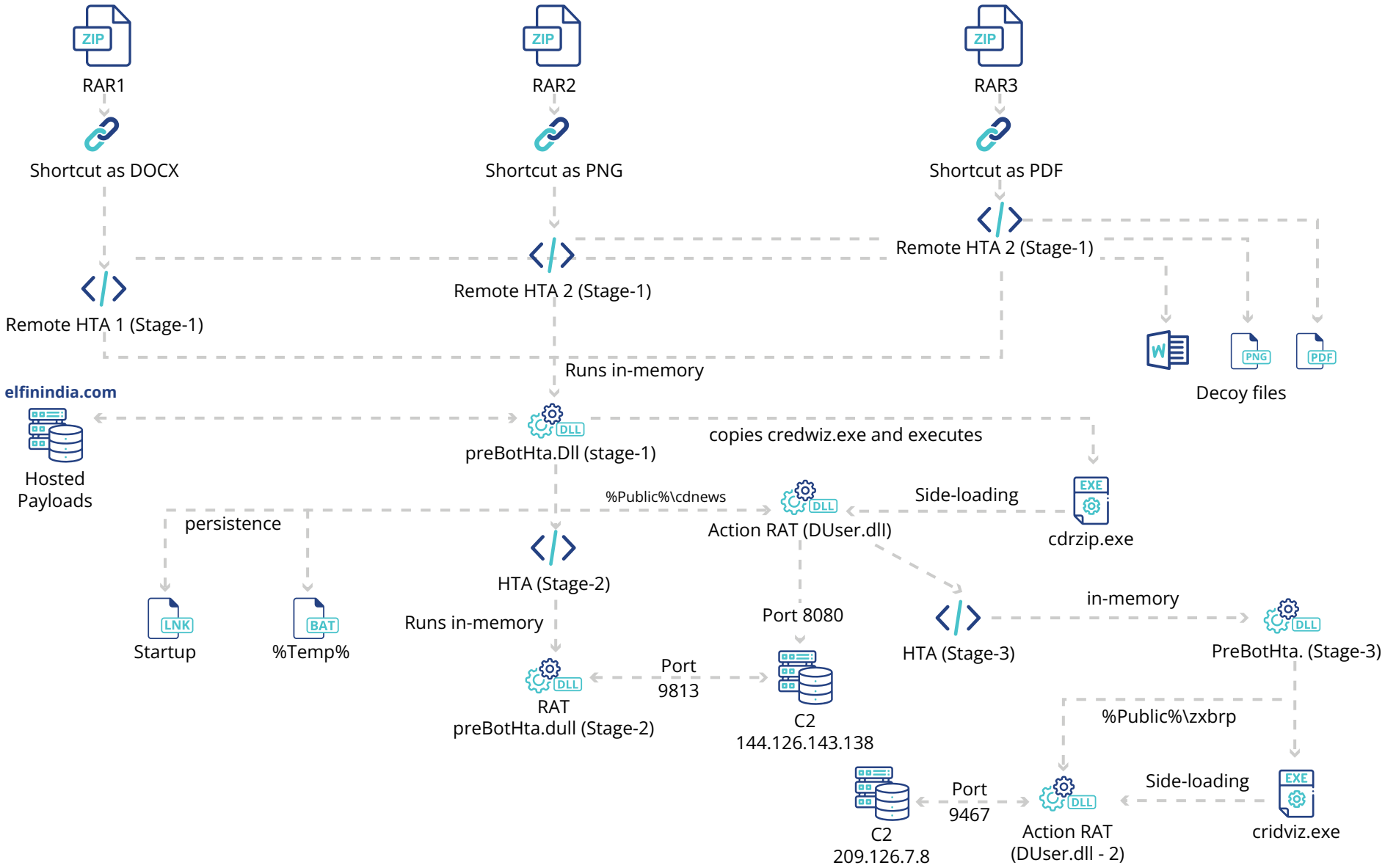
Depicting SideCopy - Infection chain-1 with the same IP



Depicting SideCopy - Infection chain-2 with IP sharing with domains and C2



Depicting SideCopy: Double Action, Triple Infection, and a New RAT



Expert Quotes

"We are experiencing continuous evolution in cybersecurity through confluence of technologies. As the banking sector embraces digital transformation and innovation, it faces increasing and evolving cyber threats from various actors who want to exploit systems, data, and customers. Implementing strong and adaptive cybersecurity solutions can safeguard assets, comply with regulations, and ensure reputation and trust. Cybersecurity is not just an operational issue, but a strategic necessity for the banking sector."

Mahesh Kulkarni, Managing Director, Barclays

"While the pandemic is over, the acceleration of perimeter-less digital world is here to stay. Beyond essential technologies such as endpoint protection, firewalls, and web security, businesses are progressively embracing the Zero Trust security paradigm to navigate the evolving reality. Organizations are witnessing benefits of corelating security events across control planes and using the collective insights in securing access and assets via Zero Trust implementations. Customers are increasingly opting for one-stop solutions that offer robust security research capabilities integrated into individual solutions on a shared security platform. This approach streamlines and simplifies Security Operations and provides end-to-end orchestration, aligning with the current trends in cybersecurity."

Ashish Pradhan, Chief Technology Officer, Quick Heal Technologies Limited

"Most rogue applications necessitate users to grant access to text messages, images, and contacts during installation, and in some instances, even camera access. The applications subsequently duplicate contact lists and photos, utilizing them to harass the victims.
The Reserve Bank of India (RBI) and Google have acknowledged the existence of these "illegal loan applications" that offer loans at "prohibitively high-interest rates" and employ "predatory recovery practices". The RBI has established guidelines for loan recovery, and Google has delineated rules for such applications on the Play Store.
Based on my understanding, SEQRITE Labs has shared with Google and the RBI a list of such applications that access the contact list, camera, location, and text messages of users, which are later used to threaten the users. Users need to exercise precaution on access permission requested by App during installation."

Sameer Ratolikar, Chief Information Security Officer, HDFC Bank

"Artificial intelligence (AI) is transforming the world in many ways, from enhancing productivity and efficiency to enabling new forms of creativity and innovation. However, AI also poses significant challenges and risks for the cyber security landscape, as it can be used by malicious actors to launch sophisticated attacks, evade detection, and exploit vulnerabilities. One of the main challenges that AI poses for cyber security is that it can increase the scale, speed, and complexity of cyberattacks. On the other hand, AI also offers opportunities for enhancing cyber security and resilience. For instance, AI can help defenders to detect and respond to cyberattacks faster and more effectively, by analyzing large volumes of data, identifying anomalies and patterns, and providing actionable insights and recommendations. Furthermore, AI can help defenders to improve their situational awareness and decision making, by providing them with a comprehensive and dynamic view of the cyber environment, as well as with predictive and prescriptive analytics.

AI is a double-edged sword for cyber security, as it can be used for both good and evil purposes. Therefore, it is essential to develop and implement ethical principles and best practices for the design, development, deployment, and use of AI systems in the cyber domain. Additionally, it is important to foster collaboration and coordination among various stakeholders, such as governments, industry, academia, civil society, and international organizations, to ensure that AI is used responsibly and securely for the benefit of humanity."

Sanjay Agrawal, Chief Product Officer, Quick Heal Technologies Limited

An organization is only as safe as the intelligence of their NGAV, EDR or XDR. Every organization wants to safeguard itself against known and also against unknown threats. Therefore, these solutions should enable organizations with their strong detection capabilities to bring visibility, which is equally important as prevention. These NGAV, EDR or XDRs are the current and future security technologies to get protection against advanced threats by stitching the events together to complete the context and actionable information.

Sandeep Bansal, Sr. Director Global Security, Concentrix

"SEQRITE Labs research has clearly identified an increase in use of sophisticated mechanisms by malware authors. While we are proud to acclaim being the first and only company in achieving cleanup solution for Expiro infector, we are also cognizant of the fact that the complexities and AV-evading techniques employed by malwares are going to increase in coming time. Ransomware is not limiting themselves to data theft and monetary gains and is increasingly being used to cause sabotage on the target systems. From last several quarters, we have been observing an acute increase in activities of APT groups like SideCopy and Transparent Tribe targeting our national cyber assets, including Government entities and Indian defense organizations.

In addition to increasing vigilance across clear and dark net, it's the need of the hour to deploy proactive measures, including Malware Labs, to have quick turnaround time in identifying any malicious files or IoCs that may have sneaked into the network. The innovative technologies aided by machine learning algorithms assist SEQRITE Labs to keep our customers protected against the growing menace of malwares."

Jaswinder Singh, Director – Engineering, SEQRITE Labs, Quick Heal Technologies Limited

"In the dynamic landscape of cyber threats, particularly phishing attacks targeting the Banking Sector, leadership plays a critical role. As threat actors adopt more sophisticated tactics, our defence strategies must evolve in tandem. Reinforcing cybersecurity measures, fostering information sharing, implementing proactive threat detection and effective incident response mechanism are not mere practices but imperative strategies. In this era of digital transformation where technology underpins financial institutions, robust cyber risk management is not just crucial; it is the cornerstone of modern business resilience. As leaders in the banking sector, let us navigate this intricate landscape with vigilance, innovation, and an unwavering commitment to safeguarding client trust."

Satish Lele, CISO, The Cosmos Co-op. Bank Ltd.

Cyber Threat Predictions for 2024

Zero-days attacks APTs and Ransomware group

MFA Fatigue Attacks

LoLbins- a nightmare for Threat Researchers

AI-Powered Malware

Ransomware and Digital Extortion

Deep Fake fo Deceptive Social Engineering

Exploiting Vulnerable Supply Chains

Hacktivism continues into 2024

Auction of corporate access and sale of breach datasets

Event based attacks – Elections, Olympics etc.

Phishing/Vishing attacks & Dating App Scams

AI-Powered Malware and the Future of Cyberattacks

- The emergence of polymorphic malware like BlackMamba has underscored the potential threats posed by AI-powered cyber-attacks. BlackMamba, a malicious keylogger utilizing AI for evasion, employs generative AI to create unique malware payloads, connecting with OpenAI to generate Python code for keylogging applications. The resultant standalone keylogger executable uses AI to capture and transmit keystrokes, with the potential to infiltrate Android OS. Threat actors leverage Google Play Store updates and chatbots to generate random, undetectable payloads, evading antivirus systems.

- AI's role in cyber-attacks extends beyond evasion, presenting a broader impact on the efficiency and sophistication of cyber threats. Automated and streamlined attack processes increase the scope of potential victims while enabling the creation of more sophisticated evasion techniques. The data analysis capabilities of AI enable the identification of vulnerabilities and potential targets, paving the way for the development of persuasive attacks. As AI continues to evolve, the advanced phishing tactics will become more personalized and effective. It will lead to a probable increase in successful phishing and spear-phishing-related breaches.

LoLbins- a nightmare for Threat Researchers

- The cybersecurity landscape confronts a significant challenge with the advent of LoLbins, presenting a particular concern for threat researchers. Recent security breaches underscore the substantial risk posed by 'living off the land' binaries, including widely-used applications such as Powershell and certutil. These legitimate tools, routinely employed by system administrators, can be exploited to disable security measures and execute malicious activities. Both the DarkGate malware and the well-known Cobalt Strike effectively leverage LoLbins to compromise systems. Given these developments, an impending surge in 'living off the land' attacks is expected, carrying potentially profound implications into 2024.

2024 Elections: Cyber Threats Ahead

- As technology continues to shape electoral processes globally, there is an increasing imperative for robust cybersecurity measures. With elections anticipated in early 2024, a rise in cyber threats and attacks is expected. These threats are projected to manifest in the form of phishing emails and malvertising, likely themed around the election campaign. Phishing emails may exploit heightened political interest, while malvertising could capitalize on the extensive reach of election campaigns. The overall threat landscape is foreseen to intensify during this period, emphasizing the critical need for strong cybersecurity measures. Vigilance is crucial for both individuals and organizations to ensure their digital security infrastructure is well-prepared to counter potential threats.

Exploiting Vulnerabilities in Cybersecurity Supply Chains

- The frequency of cyber-attacks on supply chains is experiencing an upward trend, prompting a call for new regulations. Globally, there is a growing push for collaboration between governmental entities and private industries in response to the escalating imperative to identify and combat threat groups. Anticipation surrounds further developments in the year 2024, signalling the ongoing evolution of supply chain vulnerabilities and the pressing need for proactive cybersecurity measures.

Understanding MFA Fatigue Attacks: A Growing Threat in Cybersecurity

- A multi-factor authentication (MFA) fatigue attack, also known as MFA Bombing or MFA Spamming, is a cyberattack tactic where hackers inundate a target victim with repeated second-factor authentication requests via email, phone, or registered devices. The aim is to coerce the victim into confirming their identity through these notifications, unwittingly granting access to the attackers trying to breach their accounts or devices. These attacks often follow other social engineering methods, like phishing, which are used to obtain the victim's initial login credentials, or they may involve stolen credentials acquired from the dark web and other sources.

- Modern MFA systems typically support push-notification-style authentication. After the user enters their initial credentials (first-factor authentication), they receive a push notification requesting confirmation of their second-factor authentication, often via their mobile device's control. This simplified authentication approach has contributed to the growing popularity of MFA fatigue attacks among hacker groups. A notable example is Uber breach by the infamous hacking group Lapsus$, highlighting the potential consequences of such attacks, including the deployment of ransomware that holds corporate resources or sensitive data hostage in exchange for a ransom.

Deep Fake for Deceptive Social Engineering

- As we look ahead to 2024, a new form of social engineering is emerging as a significant threat: AI-generated voice and video scams. These scams employ advanced deep learning techniques to imitate the voices and faces of trusted individuals, deceiving targets into revealing sensitive information, sending money, or taking actions they wouldn't otherwise consider. In the rise of deepfakes and AI-generated media with the power of advanced algorithms, virtually anyone can create and manipulate realistic images and videos, fabricating scenarios or events that never occurred. This capability has far-reaching implications, as it can be exploited to spread misinformation, fake news, or propaganda.

- The deceptive nature of these scams lies in their exploitation of our inherent trust in familiar voices and faces, making it challenging for individuals to discern the authenticity of the communication. As we move into 2024, it is advised to tread carefully in this new era of AI-generated media, balancing innovation with integrity, and always verify the source of any communication received.

Ransomware and Digital Extortion on the Horizon

- Ransomware remains a significant threat to organizations of all sizes, with the average cost of an attack expected to rise in the future. Several key trends are shaping the ransomware threat landscape. Increased targeting of critical infrastructure is evident. Ransomware attackers are increasingly targeting critical infrastructures such as hospitals and power grids where large ransoms are often paid for swift system restoration.

- The rise of RaaS (Ransomware-as-a-Service) is enabling immature cybercriminals to offer ransomware attack tools and required infrastructure. This business model facilitates the proliferation of ransomware attacks by lowering entry barriers. Additionally, the use of double extortion tactics is on the rise, with ransomware attackers steal and encrypt victims data. The dual threat provides attackers with increased leverage to extort ransoms from their victims. It emphasises the need for robust cybersecurity measures to safeguard against the growing threat of ransomware and digital extortion. Looking forward, there is an anticipation that the threat will persist at an elevated magnitude, fueled by the unprecedented number of extortion incidents witnessed in 2023.

Rise in Hacktivism

- In the ongoing landscape of hacktivism in 2024, the trend initiated in 2022 and 2023 persists with a notable increase in the number of hacktivist groups. These groups continue to play a significant role, particularly in supporting various factions amid conflicts such as the Russia-Ukraine and recent Israel-Hamas disputes.

- The tactics exercised by these hacktivist groups encompass a range of activities, including distributed denial-of-service (DDoS) attacks, data leaks, and website defacements. The trajectory suggests that hacktivist activities will diversify further. The collaboration and partnership between hacktivist groups are expected to expand, leading to more aggressive targeting of nations. Additionally, advanced persistent threat (APT) groups are anticipated to intensify their efforts to gather intelligence on neighbouring nations, adding another layer of complexity to the evolving landscape of cyber conflicts.

Increase in attacks during the Paris Olympics and the US Elections

- In anticipation of the Paris Olympics and the US elections, there is a foreseen surge in cyber threats, as cybercriminals intensify their efforts to exploit these high-profile events. This poses significant concerns, especially regarding the increased likelihood of cybercriminals deploying sophisticated phishing campaigns aimed at stealing sensitive financial information. These campaigns may masquerade as official communications related to the Olympics or electoral processes, exploiting unsuspecting individuals or organizations.

- Beyond financial motives, there is a heightened risk of targeted attacks on strategic entities such as NATO and other nations during the Olympics. The motives behind these attacks may range from political espionage to more extensive influence operations, emphasizing the need for heightened cybersecurity measures.

Exploitation of zero-days for persistence by APTs and Ransomware groups

- The exploitation of zero-day vulnerabilities for the purpose of achieving persistent access remains a growing. This trend is anticipated to escalate, not only with the involvement of nation-state threat actors but also as individual cybercriminals increasingly recognize the strategic value of zero-days.

- The emergence of more zero-day attacks are expected, driven by both state-sponsored groups seeking advanced capabilities and cybercriminals aiming to enhance their operations. The primary objective for threat actors utilizing zero-days is to establish and maintain persistent access within a victim's network. This prolonged access allows them to operate cautiously, avoiding detection mechanisms while surreptitiously extracting valuable information over an extended period. The exploitation of zero-days is particularly advantageous for ransomware groups. By validating and ensuring persistent access, threat actors can demand higher ransom amounts from victim organizations. The extended dwell time within a network often goes unnoticed, allowing ransomware incidents to unfold silently until a ransom is demanded and, in some cases, paid by the victim.

- As part of their evolving tactics, threat actors are anticipated to intensify their focus on targeting cloud environments. Exploiting misconfigurations in cloud infrastructure provides a pathway for threat actors to establish persistence and move laterally within these environments. The increasing reliance on cloud services makes them attractive targets, and threat actors will exploit any vulnerabilities to achieve their goals, whether it be for espionage, data exfiltration, or ransomware attacks.

Uptick in auction of Corporate Access and sale of Breach Datasets

- Propelled by the constant evolution of sophisticated malware and the expanding array of services provided by underground brokers, the industry is witnessing a surge in the auction of corporate access and the sale of breach datasets. Within the intricate ecosystem, various services such as penetration testing, bulletproof hosting, initial access and zero-day brokers, as well as phishing and caller services, are experiencing a substantial uptick in demand.
- Ransomware affiliates, in particular, are increasingly availing themselves of these underground services to enhance their capabilities. By utilizing sophisticated evasion algorithms embedded in emerging malware, threat actors seek to remain elusive to traditional security measures. The demand for services like penetration testing and zero-day exploits is driven by the quest for novel and effective methods to infiltrate systems and networks.
- This ecosystem of services operates as a undercover marketplace where ransomware affiliates actively search for their next victims. The objective is to increase the infection rate by leveraging a range of services that facilitate initial access and deployment of ransomware payloads. The interconnected nature of these services creates an environment conducive for the exchange of information and capabilities among cybercriminals.
- One of the alarming consequences of this trend is the auctioning of corporate and government access. Threat actors, facilitated by these underground services, gain unauthorized entry into sensitive networks, and the acquired access is then traded in underground forums. Simultaneously, compromised breach datasets are offered for sale, providing malicious actors with valuable information for orchestrating subsequent attacks.

Android Predictions

Generative AI for Malware Development

- The utilization of chatGPT and other chatbots in software development raises concerns, particularly in expediting the creation of fraudulent applications. Although there are restrictions on the malicious use of ChatGPT, it remains susceptible to misuse. Threat actors have been observed selling Chatbot services, such as FraudGPT, WormGPT, DarkBART, on the dark web, indicating a potential rise in their usage for nefarious activities.
- Looking ahead, the misuse of chat-bots is expected to grow, offering threat actors an efficient means to develop fake applications easily. The availability of these services, specifically tailored for malicious purposes, includes activities such as phishing, social engineering, exploiting vulnerabilities, and creating malware. This rise in malicious chat-bots could be driven by the need for threat actors to expand their operations to different regions where language skills may be a barrier.
- Considering that major tech companies generate a significant portion of their revenue from advertising, there is a potential for online ads linked with malware to be propagated through chatbots.

Rise in the use of Adversarial techniques for weakening Detection Systems

- Security Researchers use various technological approaches to detect and classify Android malware. Such approaches can be categorized as static, dynamic, and mixed forms of analyses, which are performed using machine learning. These techniques mainly perform static feature extraction such as bytecode, sound,

images, log records, code execution paths, control flow graphs, and data flow graphs. Some of them also developed by using algorithms such as logistic regression, Support Vector Machine and random forest. There is significant research work going on the use of quantum machine learning for malware detection and classification.

- Threat actors use adversarial example attacks to make such systems useless. Some of them are exploratory attack, data poisoning attack and evasion attack. These attacks are normally launched by providing mutated malware samples to the existing malware detection systems so that malicious applications would falsely be classified as benign ones. Injecting deliberately falsified data into victim's training set is generally called the data poisoning attack. The evasion attack is in which input data is deliberately modified to evade detection by making the machine learning algorithm classify malware samples as benign applications.

Increased use of technology in Vishing attacks and Dating App scams

- The ongoing surge in phishing attacks, combined with the simplicity and success of Vishing, signals the emergence of evolving threats. Vishing, known for its simplicity and high success rate, requires minimal technological investment and basic information, typically found on social media. The prevalent form of phishing involves impersonating figures like officials or coworkers to trick victims into divulging sensitive information, often leveraging personal data acquired from previous cyber-attacks or social media.

- As generative AI advances, it poses a growing risk, enabling the creation of more effective scams by identifying and reproducing patterns without manual input. This technology, utilizing algorithms, allows attackers to mimic voices, drawing from readily available patterns on platforms such as social media, YouTube, and interviews. The implications of AI-driven threats extend across various organizations.

New ways for Threat Actors to reach Users' Device

- Major players in the technology industry are strategically planning to enable direct app downloads through social media platforms in the EU by 2024. This initiative aligns with the EU's Digital Markets Act, which mandates mobile platforms to allow alternative methods for app downloads. The proposed benefits include heightened conversion rates for app install ads, as developers can host their Android apps directly on platforms like Facebook without relying on traditional app stores. However, concerns arise about potential vulnerabilities to malware infiltrating users' phones through this novel app entry point. While these industry developments show promise for developers and user engagement, the ongoing challenge remains to address potential security risks associated with these alternative app distribution channels.

Now to Next:
Future Directions for CISOs in 2024

In the dynamic landscape of cybersecurity, CISOs must steer their strategies based on prevailing and emerging trends. The following section outlines key directives for CISOs to strengthen their preparedness against evolving threats:

Vigilance Against Advanced Persistent Threats (APTs)

- Maintain a heightened state of alertness and preparedness in the face of advanced persistent threats (APTs) utilizing multi-vector attacks, zero-day vulnerabilities, and sophisticated malware. Prioritize the establishment of comprehensive monitoring and incident response capabilities to swiftly detect and contain these threats, mitigating potential damage to systems and data.

Robust Ransomware Defense Strategy

- Devise and implement a resilient defense strategy specifically tailored to combat ransomware. This strategy should encompass regular backups of critical data, network segmentation, rapid detection, and the isolation of affected systems. A crucial component is the development of a well-prepared and tested incident response plan to effectively mitigate the impact of potential ransomware attacks.

Adherence to Cyber Regulations and Compliance

- Keep abreast of the ever-changing cyber regulations and compliance requirements within the industry and jurisdiction. It is imperative to ensure that security policies and practices align seamlessly with existing and forthcoming standards and mandates, guaranteeing continual compliance and resilience in the face of evolving regulatory landscapes.

Integration of Emerging Technologies

- Embrace the transformative potential of emerging technologies and innovations, including artificial intelligence, quantum computing, 5G, and the Internet of Things. CISOs should proactively leverage the benefits and opportunities presented by these technologies. Simultaneously, they must exercise caution and awareness of the new risks and challenges introduced to cybersecurity and resilience measures.

Collaboration and Coordination

- Foster collaboration and coordination among CISOs and security professionals in your industry and region. Cultivate an environment of shared information, insights, and best practices. By building a collaborative ecosystem, CISOs can collectively enhance their organizations' cybersecurity posture and response capabilities, staying one step ahead of evolving threats.

In navigating these strategic imperatives, CISOs can proactively address the intricacies of the cybersecurity landscape, ensuring resilience and adaptability in the face of emerging challenges.

Authors & Contributors

DSCI

Authors

Prasad Deore, Senior Director
Neha Mishra, Associate-Technical Research

Contributor

Amit Kr. Ghosh, Sr. Manager – Communications

SEQRITE

Authors

Jaswinder Singh, Director of Engineering
Shayak Tarafdar, Engineering Manager
Priyabrata Dash, Engineering Manager

About DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by nasscom®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: www.dsci.in

About SEQRITE

SEQRITE is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, SEQRITE delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. SEQRITE is the Enterprise arm of the global cybersecurity brand, Quick Heal Technologies Limited, the only listed cybersecurity products and solutions company in India.

We are the first and only Indian company to have solidified India's position on the global map by collaborating with the Govt. of the USA on its NIST NCCoE's Data Classification project. We are differentiated by our easy-to-deploy, seamless-to-integrate comprehensive solutions providing the highest level of protection against emerging and sophisticated threats powered by state-of-the-art threat intelligence and playbooks backed by world-class service provided by best-in-class security experts at India's largest malware analysis lab – SEQRITE Labs. We are the only Indian full-stack company aligned with CISMA architecture recommendations offering award-winning Endpoint Protection, Enterprise Mobility Management, Zero Trust Network Access, and many more. Our Data Privacy Management solution enables organizations to stay fully compliant with the DPDP Act and global regulations.

Today, 30,000+ enterprises in more than 76 countries trust SEQRITE with their cybersecurity needs. For more information, please visit https://www.seqrite.com.

DATA SECURITY COUNCIL OF INDIA

Nasscom Campus, 4th Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries, contact: E: info@dsci.in | W: www.dsci.in

DSCI_Connect dsci.connect dsci.connect data-security-council-of-india dscivideo