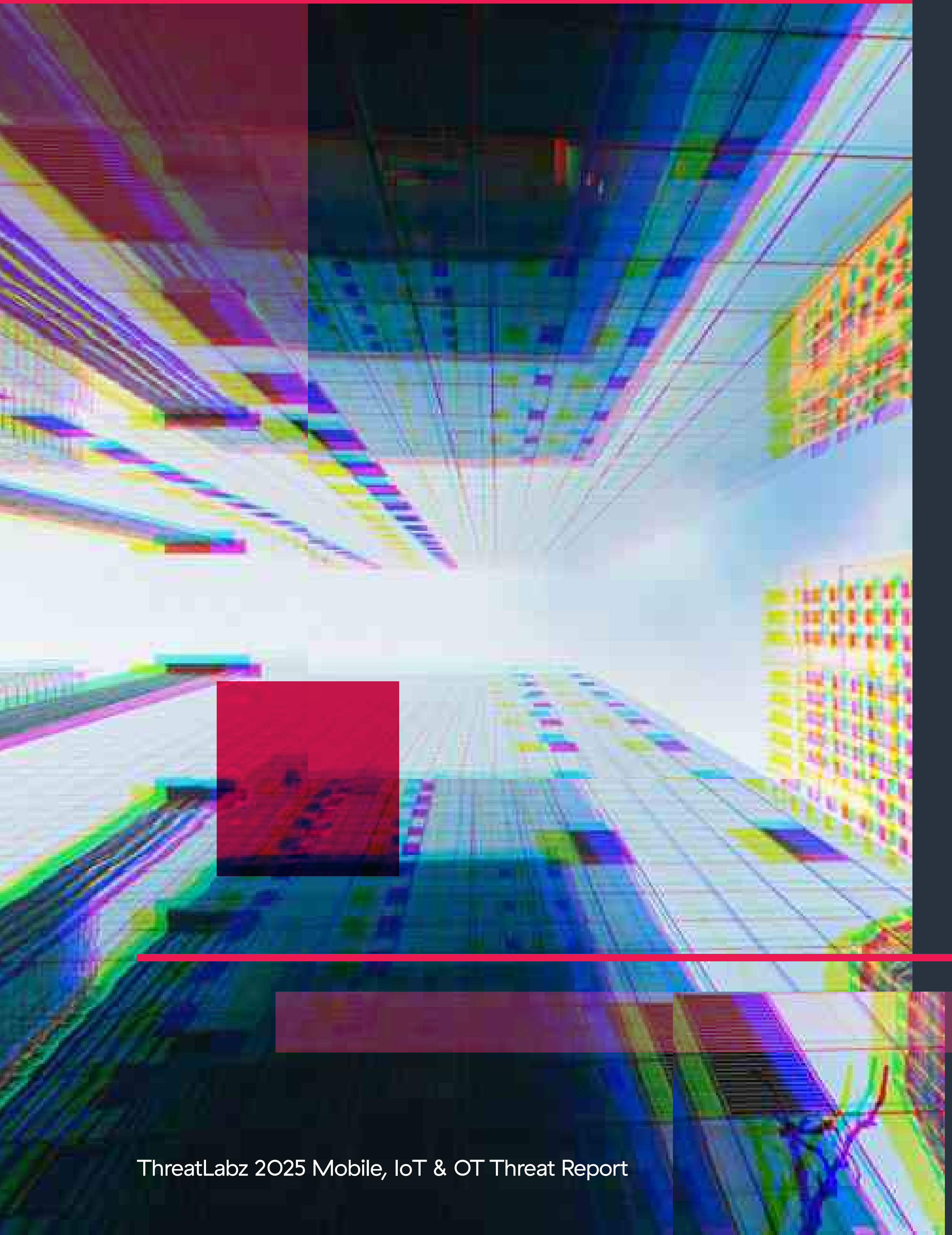
Zscaler ThreatLabz 2025 Mobile, IoT & OT Threat Report

Table of Contents



Executive Summary

Mobile, IoT, and OT systems have become the backbone of business operations today, enabling innovation and powering critical infrastructure across industries. Mobile devices now dominate global connectivity, while IoT and OT systems keep manufacturing, healthcare, transportation, and smart cities running. Cellular-connected IoT devices are central to this transformation, enabling expansive operational use cases—but simultaneously exposing organizations to new and evolving threats.

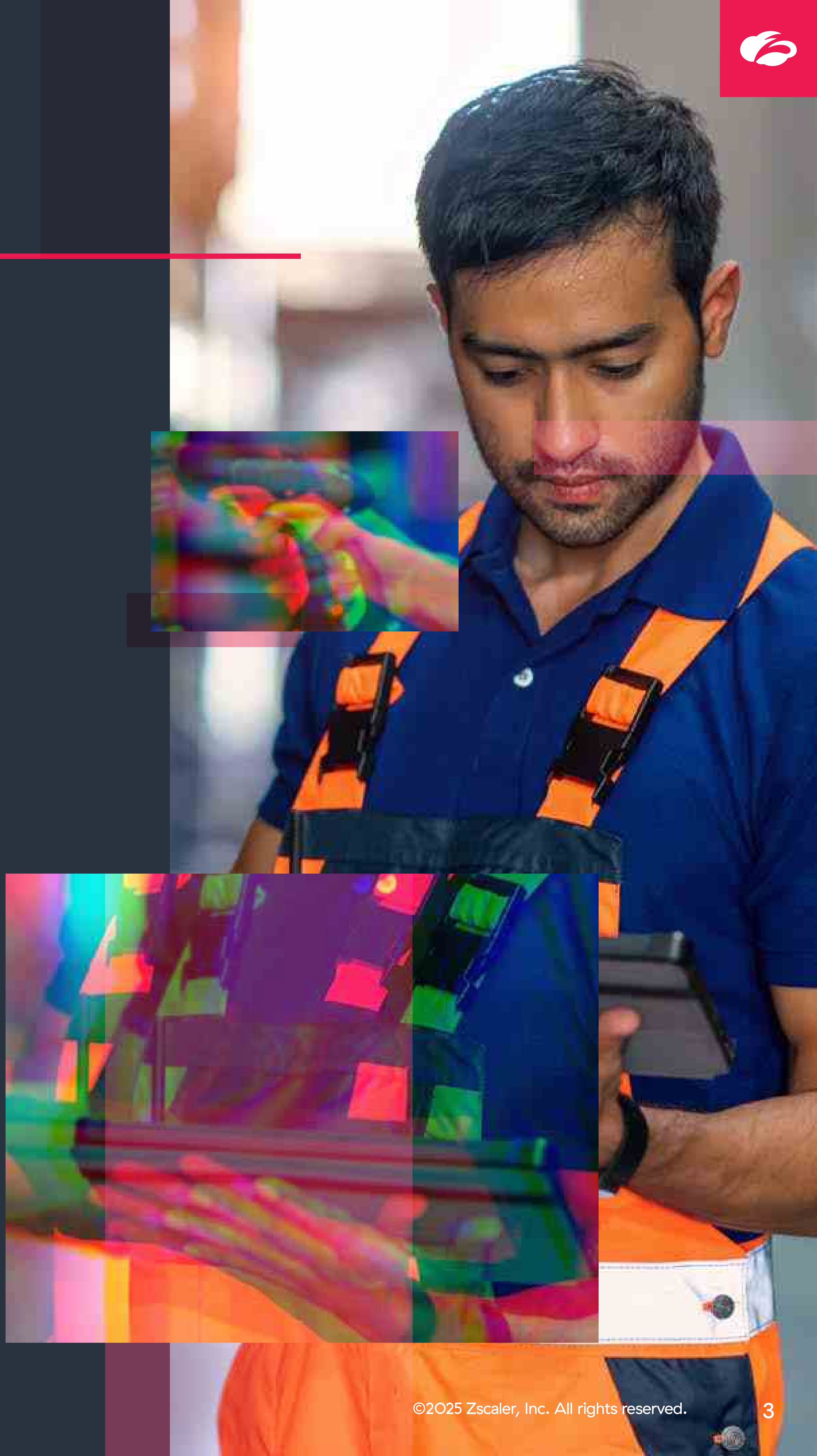
Threat actors are taking advantage of this expanding web of connectivity and interdependence, targeting vulnerabilities in mobile devices, IoT systems, and legacy OT environments. Over the past year, notable attacks ranged from sophisticated Android malware campaigns to nation-state operations like Volt Typhoon and Salt Typhoon, which exploit public-facing infrastructure for espionage, sabotage, and disruption. This threat activity is amplified by IoT botnets that automate attacks across unpatched or misconfigured devices. At the same time, connectivity gaps, high latency, and weak SIM protections within cellular-connected ecosystems compound the risks, creating a shadow attack surface that is difficult to detect and defend.

Key findings from the Zscaler ThreatLabz 2025 Mobile, IoT & OT Threat Report reveal the magnitude of these converging risks:

- **Android malware transactions grew by 67% year-over-year**, fueled by spyware and banking malware designed to target trusted marketplaces and hybrid work environments.
- **IoT botnet activity remains dominated by Mirai, Mozi, and Gafgyt malware families**, accounting for 75% of all malicious IoT payloads by exploiting router and edge device vulnerabilities to expand botnet reach and move laterally.
- **239 malicious Android applications were collectively downloaded 42 million times on the Google Play Store**, illustrating how attackers bypass app store protections to infect endpoints.

The findings call for enterprises and public sector organizations to prioritize proactive security strategies, including deploying zero trust frameworks, using AI-driven threat detection, and implementing segmentation across IoT/OT and cellular-connected networks. These measures reduce the attack surface, limit lateral movement, and help defend against increasingly sophisticated threats targeting mobile devices, IoT ecosystems, and mission-critical infrastructure.

This report provides actionable insights and guidance to help organizations securely adopt cellular-powered IoT and OT systems and ensure their connected ecosystems remain a source of innovation—not a point of compromise.



Key Findings

Top Mobile Trends

Android malware transactions grew by 67% year-over-year, fueled by spyware and banking malware designed to target trusted marketplaces and hybrid work environments.

239 malicious Android applications were collectively downloaded 42 million times on the Google Play Store, illustrating how attackers bypass app store protections to infect endpoints.

A new backdoor called Android Void malware has infected 1.6 million Android-based TV boxes, primarily in India and Brazil, enabling threat actors to download and install third-party software onto the devices.

India remained the top target, accounting for 26% of mobile attacks, followed by the United States (15%) and Canada (14%).

Manufacturing, Energy, Oil & Gas, and Retail & Wholesale were the most targeted industries, with Energy attacks rising 387% and Healthcare sector attacks increasing by 224.39% compared to last year.

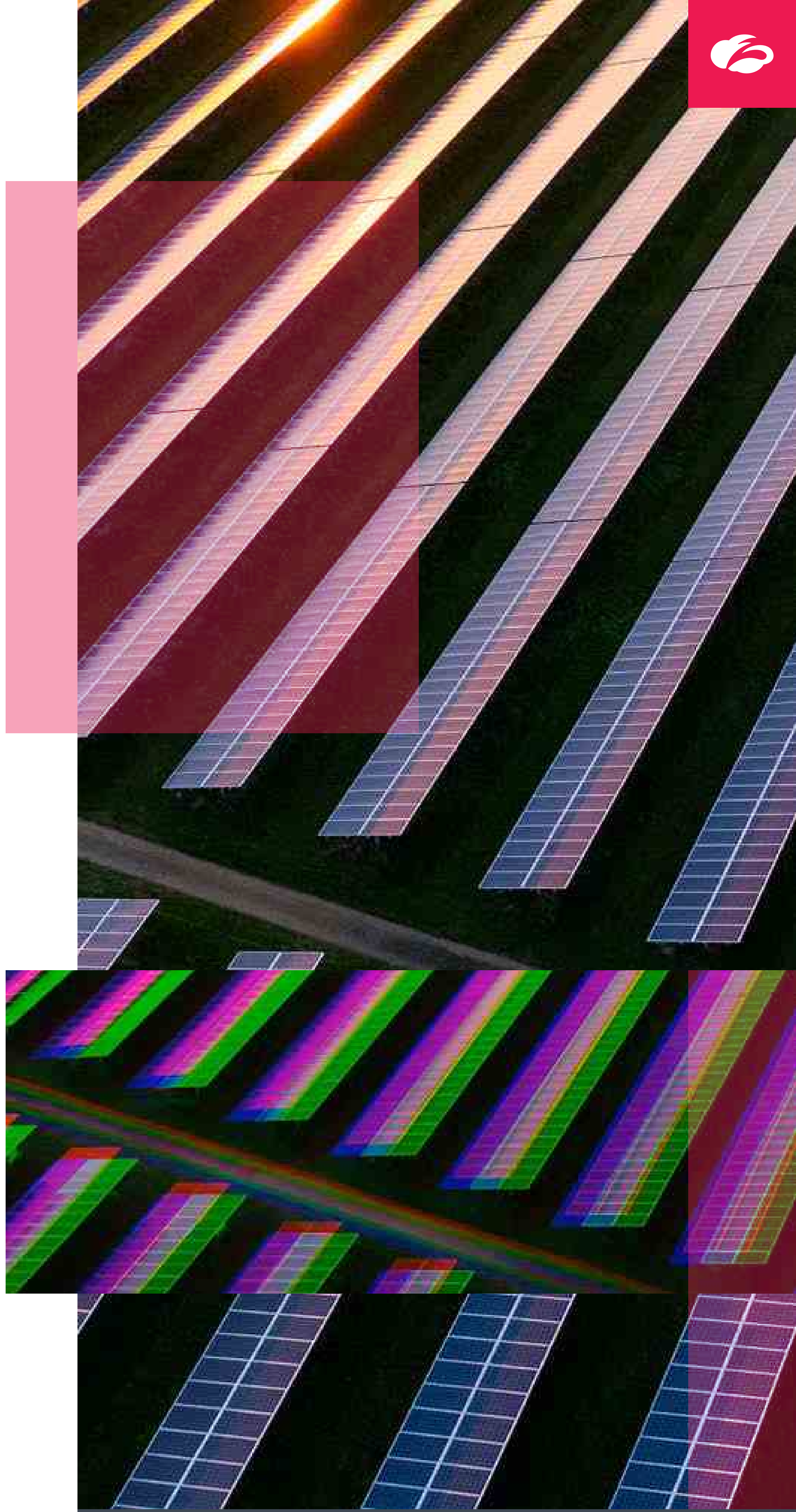
Top IoT Trends

The majority of IoT malware is linked to the Mirai and Mozi malware families. Roughly 40% of blocked transactions are linked to the Mirai family alone, while Mozi has overtaken Gafgyt as the second top malware family. Together, Mirai, Mozi, and Gafgyt account for roughly 75% of all malicious payloads.

Routers remained the most targeted IoT devices this year, accounting for over 75% of all attacks—primarily driven by command injection vulnerabilities. Attackers aggressively exploited these flaws to execute unauthorized commands, often using routers as entry points for botnet expansion and malware delivery. DVRs, NVRs, and cameras followed as frequent targets, underscoring the continued exploitation of exposed network and surveillance devices in IoT botnet campaigns.

The US remains the top target for IoT attacks, with 54.1% of activity. However, Hong Kong (15.1%), Germany (6.6%), India (4.5%), and China (4.1%) have emerged as growing hotspots, reflecting a shift in botnet infrastructure and global targeting. This diversification highlights attackers' evolving strategies to exploit IoT vulnerabilities across a wider geographic landscape.

The Manufacturing and Transportation sectors jointly bear the brunt of IoT attacks, with a combined 40% of all IoT malware attacks and equal 20% shares. This marks a shift from Manufacturing's standalone dominance last year. Additionally, attacks surged in the Arts & Entertainment and Education sectors, signaling a widening threat landscape as attackers increasingly target industries with growing IoT adoption.



Mobile Overview

Threat actors are increasingly adapting their techniques to exploit the modern workforce's reliance on personal mobile devices in hybrid and remote work settings. With 51% of U.S. remote-capable jobs now hybrid, employees are splitting their time between home and office, often leaning heavily on their mobile devices for communication, productivity, and access to corporate resources. Additionally, 28% of remote-capable roles are now exclusively remote, further reinforcing the critical role of mobile devices as essential tools for the workforce.

The widespread adoption of Bring Your Own Device (BYOD) policies has heightened the importance of securing mobile endpoints. While these policies enhance employee flexibility and reduce hardware costs for organizations, they also expand the attack surface for cyberthreats. Employee-owned devices are often used to access sensitive corporate data, connect to enterprise networks, and utilize productivity applications, creating potential vulnerabilities, particularly in unsecured environments.

Given the growing reliance on mobile devices, this report outlines how threat actors are leveraging and constantly enhancing tactics to target these endpoints. This includes the continuous evolution of Anatsa malware, the development of Android-specific Remote Access Trojans (RATs), the use of mishing (SMS-based phishing), and the strategic targeting of the Tools category in the Google Play Store, knowing that some users depend on these apps for work-related productivity. Understanding these threats is critical for staying ahead of attackers in today's mobile-first world.

ThreatLabz Mobile Research Highlights

During 2024 and 2025, ThreatLabz researchers leveraged Zscaler's mobile telemetry dataset to monitor malicious activities, uncover emerging mobile threats, and deliver valuable intelligence to the security community. This effort led to several notable discoveries, including prominent Android malware campaigns.

ANDROID MALWARE USES SCARE TACTICS TO TARGET USERS IN INDIA

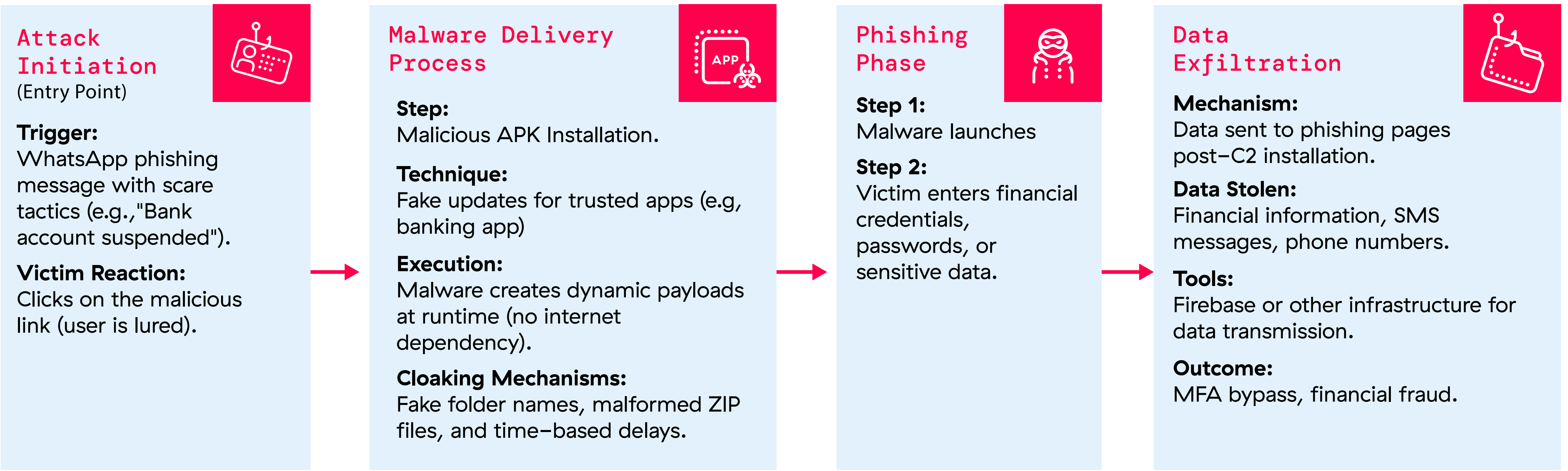
Android phishing malware campaigns targeting Indian users are growing more advanced, using fear-based scenarios to trick victims into divulging sensitive information. These campaigns are distributed through WhatsApp messages designed to scare victims with warnings like bank account suspensions or traffic violations, compelling them to take actions that leave their personal and financial information exposed.

Once installed through a victim's inadvertent click on a WhatsApp message link, the malware embeds itself in installer applications to avoid detection. Rather than downloading malicious files from the internet, the malware generates the files dynamically during runtime using encrypted files already embedded in the parent application. Techniques such as fake folder names, malformed ZIP files, and time-based delays further enable the malware to bypass detection mechanisms effectively.

After installation, the malware prompts the victim to approve seemingly legitimate banking app updates that, upon approval, launch phishing pages that capture the victim's sensitive information such as financial credentials, personal data, and SMS messages, sometimes even bypassing MFA. This data is then sent to the threat (C2) servers, enabling criminal activity.

The malware uses encryption and obfuscation tools that make its payload challenging to analyze. The encrypted files, stored in the app's asset folder, take on different roles, such as managing split APK payload configurations, running session binaries, or delivering phishing APKs disguised as legit updates, like Yono_SBI_v22.0.

Layers of execution work together to complete the attack, with some campaigns even leveraging the same servers for malware deployment and data exfiltration. Threat actors use tools like Firebase databases to exfiltrate data, with some setups leaving stolen data exposed due to misconfigurations.



Attack Initiation
(Entry Point)

Trigger:
WhatsApp phishing message with scare tactics (e.g.,"Bank account suspended").

Victim Reaction:
Clicks on the malicious link (user is lured).

→

Malware Delivery Process

Step:
Malicious APK Installation.

Technique:
Fake updates for trusted apps (e.g, banking app)

Execution:
Malware creates dynamic payloads at runtime (no internet dependency).

Cloaking Mechanisms:
Fake folder names, malformed ZIP files, and time-based delays.

→

Phishing Phase

Step 1:
Malware launches

Step 2:
Victim enters financial credentials, passwords, or sensitive data.

→

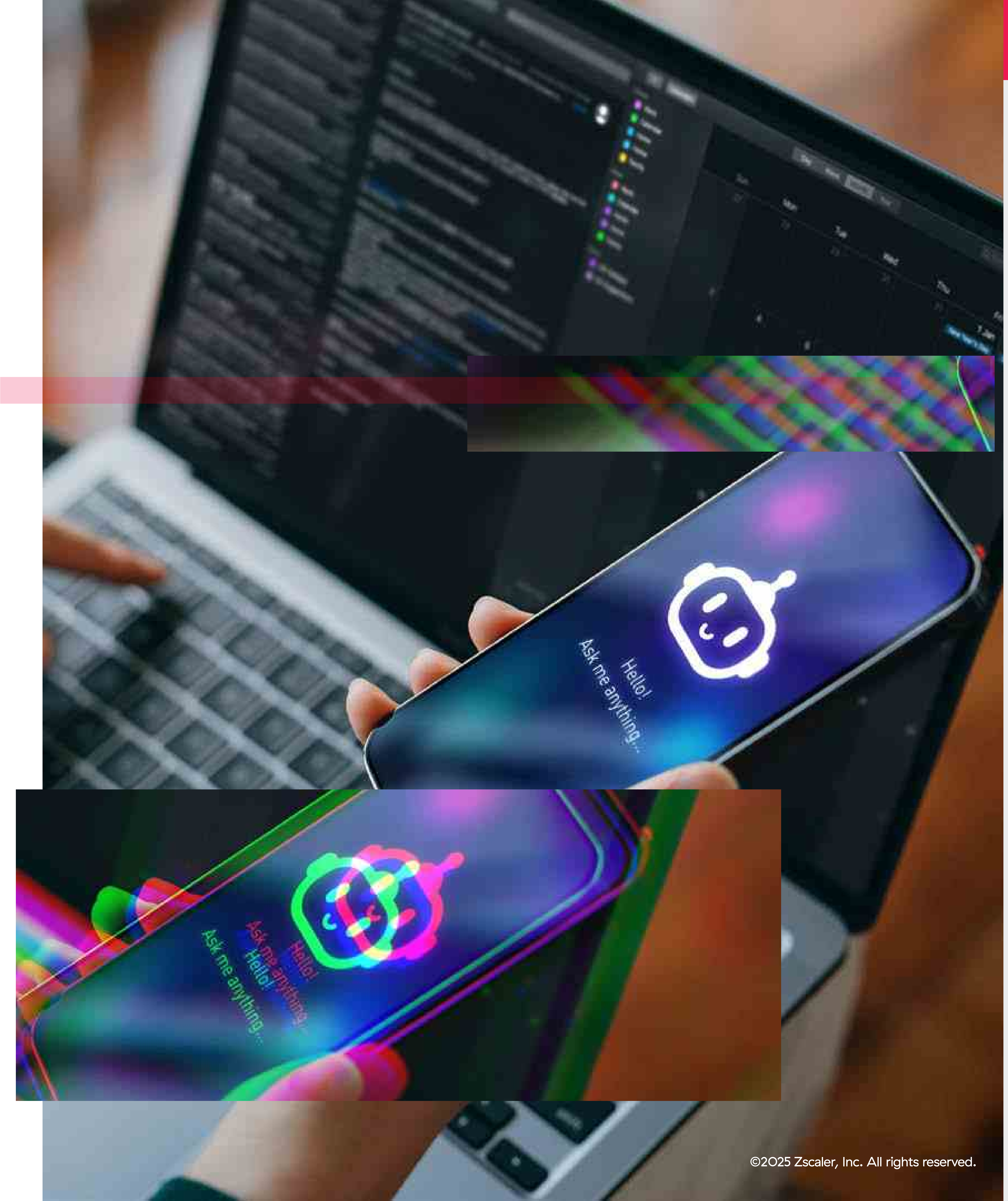
Data Exfiltration

Mechanism:
Data sent to phishing pages post-C2 installation.

Data Stolen:
Financial information, SMS messages, phone numbers.

Tools:
Firebase or other infrastructure for data transmission.

Outcome:
MFA bypass, financial fraud.



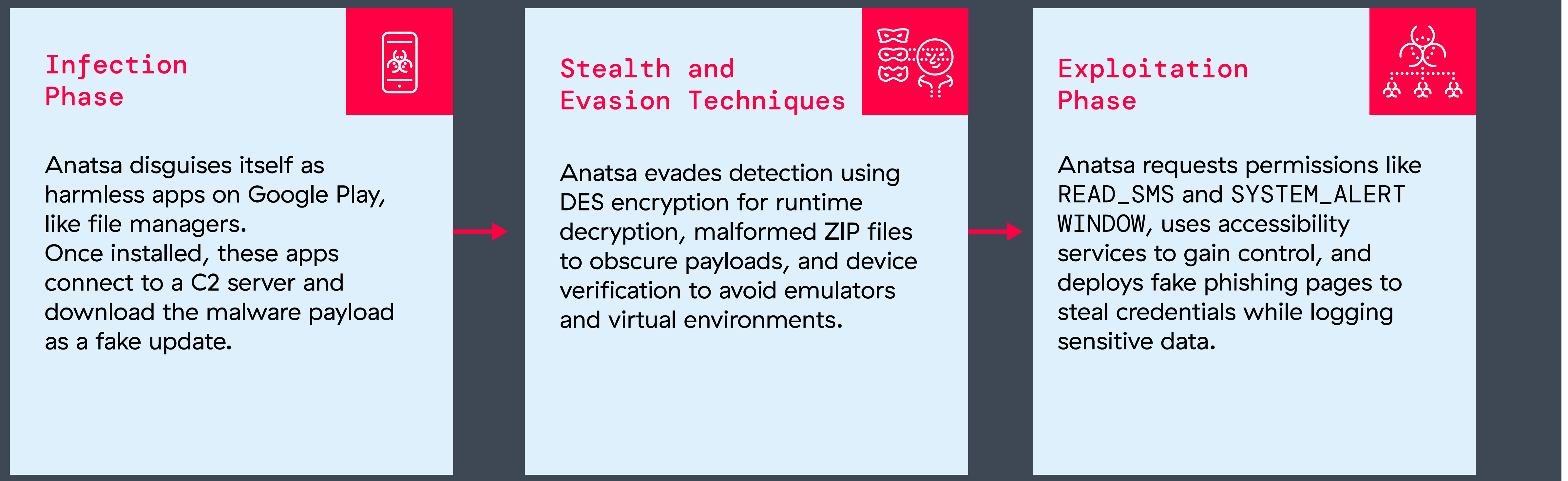
ANATSA IS STILL MAKING THE ROUNDS ON THE GOOGLE PLAY STORE

The ThreatLabz team published another **technical analysis** of Anatsa, an Android banking trojan capable of credential theft, keystroke logging, and facilitating fraudulent transactions. First discovered in 2020, Anatsa initially targeted financial institutions in regions like Europe, the US, and UK. More recently, Anatsa has broadened its focus to over 831 financial organizations globally, including cryptocurrency platforms and regions such as Germany and South Korea, marking its rapid expansion.

Anatsa spreads through the Google Play Store using decoy apps like file managers and document readers that appear harmless. Once installed, these apps contact a command-and-control (C2) server and download the malware payload disguised as an update. The installer employs DES encryption to decrypt strings dynamically during runtime, while malformed ZIP archives conceal payloads, making them hard to detect with static analysis tools. Further, the malware verifies devices, avoiding virtual environments or emulators to ensure it targets genuine user devices.

Once operational, Anatsa requests permissions like READ_SMS and SYSTEM_ALERT_WINDOW, and employs accessibility services to gain full control of the device. Anatsa deploys tailored fake banking login pages from the C2 server that mimic financial apps detected on the victim's device, effectively tricking victims into believing they are using their legitimate banking app and inadvertently providing sensitive details to Anatsa. With a built-in keylogger, Anatsa harvests that sensitive login information. Then, Anatsa uses encrypted communication with its C2 server to execute commands such as hiding SMS notifications, automating payments, and stealing financial data.

ThreatLabz recently reported 77 malicious apps, including Anatsa, to Google, covering a staggering 19 million installs. The evolving malware tactics, including Anatsa's expansion and integration with cryptocurrency platforms, highlight the growing risk of sophisticated mobile malware to users and financial institutions worldwide.



Infection Phase

Anatsa disguises itself as harmless apps on Google Play, like file managers.
Once installed, these apps connect to a C2 server and download the malware payload as a fake update.

Stealth and Evasion Techniques

Anatsa evades detection using DES encryption for runtime decryption, malformed ZIP files to obscure payloads, and device verification to avoid emulators and virtual environments.

Exploitation Phase

Anatsa requests permissions like READ_SMS and SYSTEM_ALERT WINDOW, uses accessibility services to gain control, and deploys fake phishing pages to steal credentials while logging sensitive data.

THREATLABZ DISCOVERS NEW RAT CALLED XNOTICE

The Xnotice Remote Access Trojan (RAT) is a campaign targeting job seekers in the oil and gas industry, particularly in Iran and the Arabic region. Advertised as legitimate job application or exam registration apps, Xnotice deceives users into sharing sensitive data and paying fake exam fees. This aligns with the sharp 387% rise in cyberattacks reported in the energy, oil, and gas sector, reinforcing the notion that cybercriminals are increasingly focusing on high-value, essential industries like energy and manufacturing.

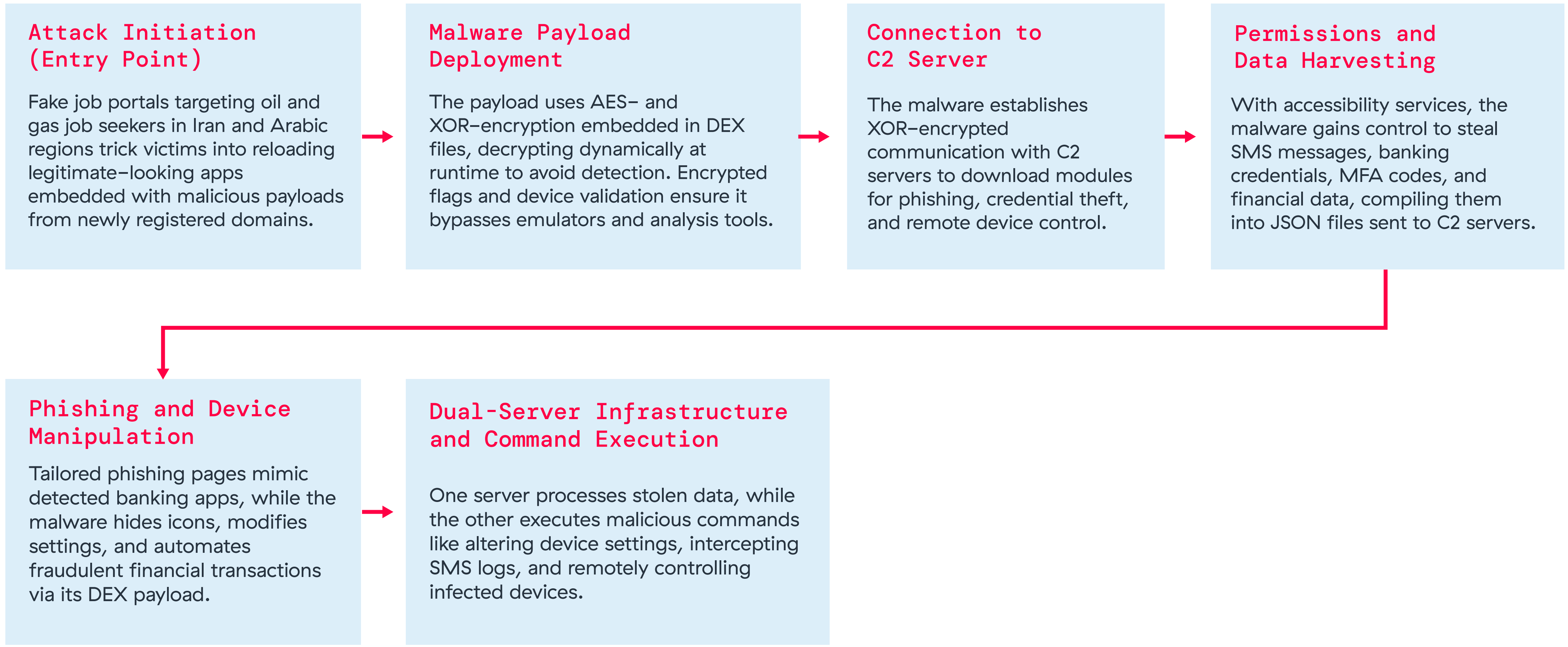
The attack begins with fake job portals hosted on newly registered domains and lures victims with seemingly legitimate opportunities. Visitors are prompted to download applications that appear harmless but conceal AES and XOR-encrypted payloads embedded directly into the APK's DEX files. Unlike traditional malware storing payloads in asset folders, Xnotice injects them into DEX files, decrypting and executing them dynamically during runtime.

Once installed, Xnotice connects to its command-and-control (C2) server to download modules for phishing, credential theft, and remote access onto the victim's device

Xnotice delivers tailored phishing pages matching banking apps detected on the victim's device, capturing login credentials, MFA codes, and financial data. Leveraging accessibility permissions, which is the most common way threat actors gain full control of infected devices, Xnotice can even steal SMS messages and screenshots. In addition, Xnotice extends its reach by utilizing its DEX payload to modify app behaviors, such as hiding icons, altering device settings, and executing unauthorized financial transactions.

Xnotice transmits all stolen data via XOR-encrypted communication to the C2 server as JSON files. Xnotice operates through a dual-server infrastructure: one server handles stolen data, while the other manages malicious command execution.

To evade detection, the malware uses encrypted flags in DEX metadata and avoids virtual devices by validating hardware architecture and SIM country codes.



Attack Initiation (Entry Point)

Fake job portals targeting oil and gas job seekers in Iran and Arabic regions trick victims into reloading legitimate-looking apps embedded with malicious payloads from newly registered domains.

Malware Payload Deployment

The payload uses AES- and XOR-encryption embedded in DEX files, decrypting dynamically at runtime to avoid detection. Encrypted flags and device validation ensure it bypasses emulators and analysis tools.

Connection to C2 Server

The malware establishes XOR-encrypted communication with C2 servers to download modules for phishing, credential theft, and remote device control.

Permissions and Data Harvesting

With accessibility services, the malware gains control to steal SMS messages, banking credentials, MFA codes, and financial data, compiling them into JSON files sent to C2 servers.

Phishing and Device Manipulation

Tailored phishing pages mimic detected banking apps, while the malware hides icons, modifies settings, and automates fraudulent financial transactions via its DEX payload.

Dual-Server Infrastructure and Command Execution

One server processes stolen data, while the other executes malicious commands like altering device settings, intercepting SMS logs, and remotely controlling infected devices.

Mobile Threat Trends

ANDROID MALWARE THREATS ARE SHIFTING

In our 2024 report, ThreatLabz identified the Joker malware family as the most prominent, making up about 38% of threats. This year, adware completely usurped Joker, leading with 69% of cases, nearly doubling its impact since last year. Joker dropped to 23%, while the Harly malware family accounted for 5%.

THE TOOLS CATEGORY IS A PRIME TARGET FOR DISTRIBUTING MALWARE IN THE GOOGLE PLAY STORE

The "Tools" category remains the most impersonated and exploited by threat actors on the Google Play Store. This category is frequently used as a disguise for distributing malicious applications, leveraging its association with productivity and workflow apps that users often rely on for work-related tasks. The targeting of the Tools category makes strategic sense, as it allows attackers to capitalize on users' trust in functionality-driven applications, especially in hybrid and remote work environments where mobile devices play a critical role in professional workflows.

THREAT ACTORS ARE ABANDONING CARD-FOCUSED FRAUD IN FAVOR OF MOBILE PAYMENTS

The rapid and worldwide adoption of mobile payment systems has made transactions faster and more convenient. However, this progress has also introduced new vulnerabilities, as threat actors shift their focus from traditional card fraud to mobile payment exploitation because of its accessibility and widespread use.

Several factors drive this shift. Traditional card fraud relied on physical methods like skimming or cloning card data. Skimming required physical interaction with devices like point of sales (PoS) terminals and ATMs, while RAM-scraping malware intercepted data during transactions. Vulnerabilities in card-generation systems allowed attackers to clone EMV cards, but these methods have become less effective due to improved security standards, such as chip-and-PIN technology.

In response to these improved physical security measures, threat actors have increasingly turned their attention to the digital realm, leveraging techniques such as phishing, smishing, SIM swapping, and authorized push payment scams. These strategies, which heavily rely on social engineering, circumvent physical barriers and exploit the trust-based design of mobile payment systems, which makes them particularly vulnerable to manipulation.

To carry out these attacks, cybercriminals deploy phishing trojans and malicious apps designed to steal financial information and login credentials. Weak security practices by app developers and users further magnify these vulnerabilities. Peer-to-peer (P2P) transactions through mobile platforms present another opportunity for exploitation. Since these transactions are irreversible and difficult to trace, they serve as an attractive target for threat actors.

Among these strategies, toll fraud stands out for its capability to deceive users into unintentionally subscribing to unwanted services or incurring charges that are billed through their mobile carriers. Malware targeting NFC scans, such as the NGate variant, exemplifies the sophistication of attacks on mobile payment systems. These malicious tools intercept card data during scanning processes, allowing attackers to clone the information or relay it for unauthorized transactions.

Ghost-tapping attacks further escalate the risk by intercepting one-time passwords (OTPs) and loading stolen card data into mobile wallets, facilitating undetected transactions often conducted via burner phones to bypass fraud detection mechanisms. Another method involves the use of malicious overlays on Android devices. Fraudsters craft these overlays to perfectly mimic legitimate payment screens, enabling them to harvest user credentials and stealthily track activity.

THREAT ACTORS ARE LEVERAGING BANKING AND GOVERNMENT APP LURES TO TARGET SPECIFIC GROUPS

Threat actors are increasingly leveraging app lures themed around banking and government services to target specific user groups. In particular, Indian banking users have become a focal point for malicious actors.

One striking example is the Gigabud malware, which employs government-themed app lures to deceive victims. Masquerading as legitimate applications from government agencies or financial institutions, Gigabud deploys screen-capturing techniques and keylogging mechanisms to harvest credentials and other sensitive information. Additionally, it grants attackers remote access to infected devices, enabling them to bypass authentication procedures, tamper with two-factor verification, replace bank card numbers stored on clipboards, and carry out automated payments, all while evading detection.

These attacks often succeed by exploiting a sense of urgency or users' lack of awareness, making victims more likely to engage.

A SURGE IN MALFORMED AND MODIFIED ZIP TECHNIQUES IN MOBILE MALWARE

This year has seen a notable rise in the use of malformed ZIP parameters in APK files by various malware families. These modifications complicate analysis for both security researchers and traditional detection engines. Banking trojans, like Anatsa, frequently employ these techniques to evade detection and increase their success rate. Below are some key ZIP manipulation techniques used by malware to bypass and/or hinder analysis:

Invalid Compression Methods or File Sizes

Local file headers in APKs are modified with invalid compression methods or incorrect file size values.

Fake "Encrypted" Flags

APKs contain files with dummy "encrypted" flags in the local file headers to mislead and break standard ZIP-parsing utilities.

Malformed ZIP headers and Long Filenames

The use of excessively long filenames or invalid offsets disrupts static analysis tools.

ZIP Bombs

The inclusion of highly compressed files within the APK that expand exponentially when unpacked overwhelm analytical systems.

Malformed Manifest Files

Tampering with the Android manifest structure to conceal the malware's true configuration and behavior.

Invalid Resource Paths

Altered paths in resource sections to obscure the location of critical files like the manifest and DEX payloads.

Additionally, some malware extends this tampering beyond general ZIP Headers issues to manipulate XML files. Techniques include using excessively long XML namespaces, creating inconsistent file structures, and inserting dummy data into XML objects. These tricks further complicate parsing and make the malware harder to dissect.

MISHING AS A KEY ATTACK VECTOR FOR THREAT ACTORS

Mobile-specific phishing, often referred to as "mishing," is a growing cybersecurity threat that exploits the unique vulnerabilities of smartphone usage. This attack method encompasses tactics designed to deceive users and steal sensitive information, including smishing, quishing, and vishing. These strategies take advantage of mobile users' trust, habits, and the urgency created by deceptive communication.

Smishing (SMS Phishing) leverages the prevalence of text messaging to deliver malicious links. Attackers create fraudulent SMS messages that impersonate trusted brands, financial institutions, or government agencies. These messages often include urgent scenarios, such as warnings about compromised accounts or failed package deliveries, to prompt quick action—a tactic commonly employed by threat actors across various scams and attack trends. Victims are directed to phishing websites through embedded URLs, where they unknowingly provide sensitive information such as login credentials or payment details.

Example: A victim receives an SMS text message claiming a delivery has failed and directs the victim to a website to resolve the issue. Once on the site, the victim is prompted to pay a small fee via credit card. By entering their payment details, the victim unknowingly exposes their financial information to threat actors.

Quishing (QR Code Phishing) uses QR codes as a method to distribute malicious links. As QR codes become more mainstream for legitimate purposes, such as accessing menus or processing payments, threat actors are exploiting this familiarity. Scanning a fraudulent QR code can redirect users to phishing websites to steal credentials or even inject malware into their devices. QR codes hide the malicious nature links, as users cannot easily verify the destination before scanning.

Example: Users are presented with a QR code, claiming it will download a PDF file. When scanned, the QR code redirects them to a fake login page designed to capture credentials, ultimately resulting in data theft.

Vishing (Voice Phishing) relies on voice calls to manipulate victims into revealing sensitive information. Attackers may spoof caller IDs to mimic banks, government agencies, or other trusted entities, creating a false sense of legitimacy. Using social engineering techniques, they deceive users into providing login credentials, one-time passcodes (OTPs), or other personal data under the pretext of resolving account issues or verifying identity.

Example: A victim receives a call claiming to be from their bank, stating there is suspicious activity on their account. The caller asks the victim to provide their online banking password or OTP to "resolve the issue," granting the attacker access to their account.

THREAT ACTORS STILL ABUSING ACCESSIBILITY TO GAIN CONTROL

Accessibility abuse continues to be a cornerstone for threat actors, enabling them to use permissions designed to assist users for malicious purposes. This technique allows attackers to perform high-level actions like intercepting sensitive data, stealing financial credentials, manipulating device settings, and executing unauthorized transactions. Its consistent use across malware families and attack trends, including prominent banking malware and campaigns like Xnotice, reflects how threat actors leverage accessibility permissions as a reliable entry point for device compromise.

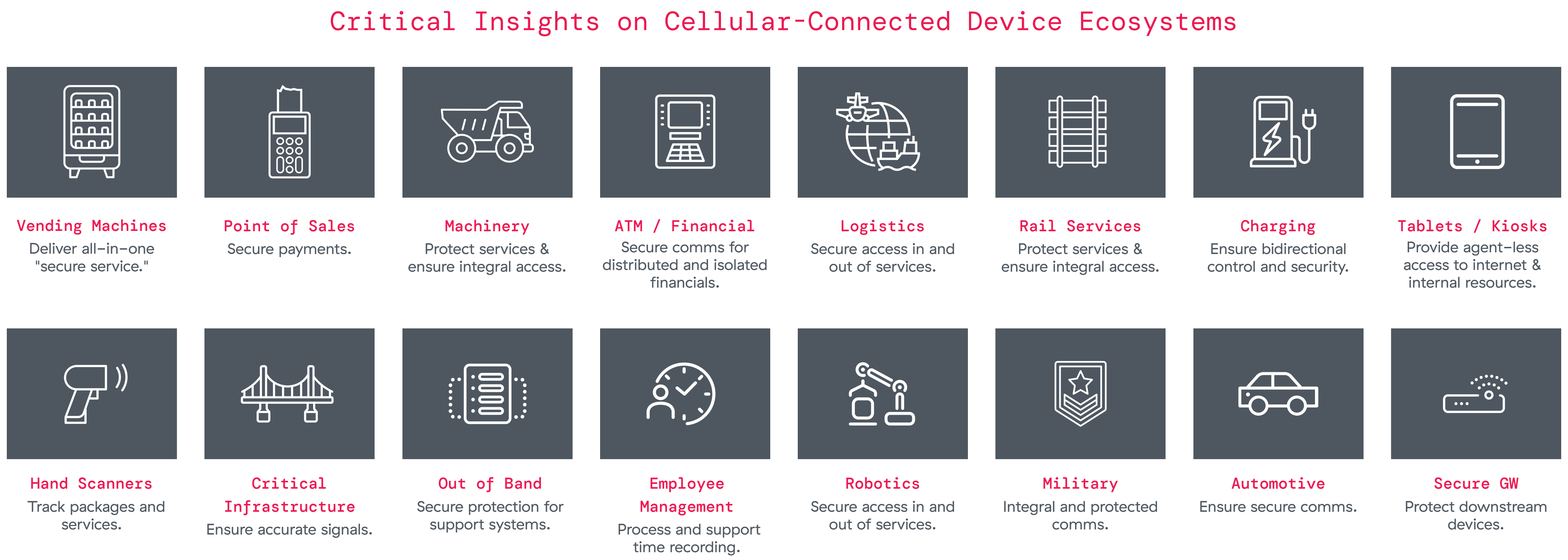

Critical Insights on Cellular-Connected Device Ecosystems
Vending Machines
Deliver all-in-one "secure service."
Point of Sales
Secure payments.
Machinery
Protect services & ensure integral access.
ATM / Financial
Secure comms for distributed and isolated financials.
Logistics
Secure access in and out of services.
Rail Services
Protect services & ensure integral access.
Charging
Ensure bidirectional control and security.
Tablets / Kiosks
Provide agent-less access to internet & internal resources.
Hand Scanners
Track packages and services.
Critical Infrastructure
Ensure accurate signals.
Out of Band
Secure protection for support systems.
Employee Management
Process and support time recording.
Robotics
Secure access in and out of services.
Military
Integral and protected comms.
Automotive
Ensure secure comms.
Secure GW
Protect downstream devices.

Figure 1: The many diverse security use cases needed in the cellular-connected device landscape.

Along with pure-play smartphones and mobile devices, the broader ecosystem of cellular-connected devices represents a growing risk for enterprises. For example, the cellular IoT device ecosystem ecosystem is positioned to be a cornerstone of technological infrastructure as industries undergo rapid digital transformation. With projections of over 4 billion cellular-connected IoT devices by 2030[4], these devices are becoming critical enablers of operational efficiency across key sectors such as manufacturing, logistics, energy, automotive, retail, corrections, and AI-driven smart infrastructure. Cellular IoT devices—ranging from remote sensors to ruggedized equipment—play vital roles in ensuring operational continuity in demanding environments and are integral to the growth of connected systems across industries.

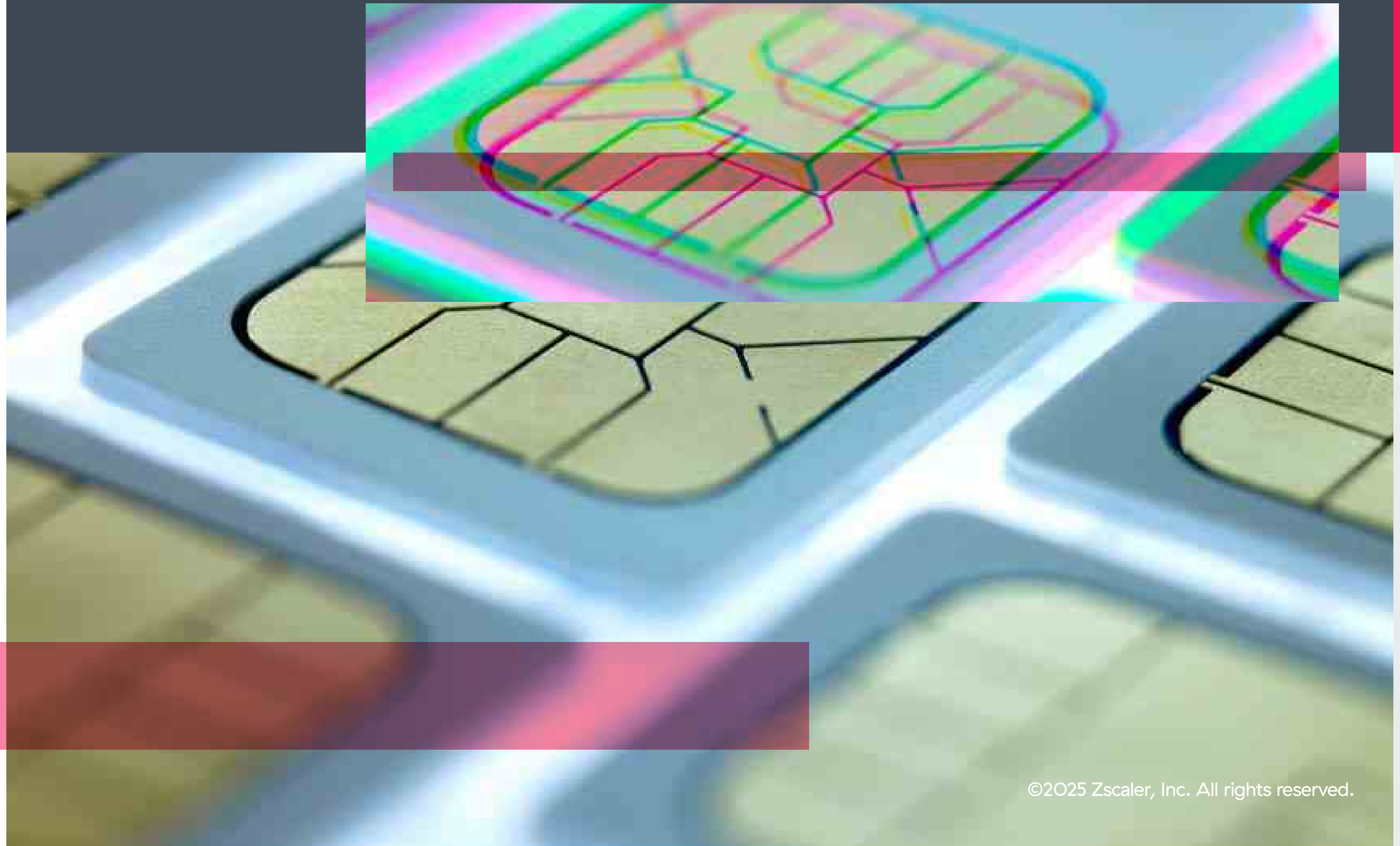
Despite this massive growth, several challenges and vulnerabilities have emerged within the cellular IoT space. Despite the increased reliance on cellular-connected devices, many organizations hold the misconception that once a device connects to a cellular network, it's automatically under control. In reality, active Subscriber Identity Modules (SIMs) can transmit data freely across borders and networks without sufficient visibility or restriction. This false sense of security leaves businesses vulnerable to compliance violations and cyberthreats, especially when location-based or behavioral policy enforcement is necessary.

Although mobile carriers offer network-level protections, these safeguards often lack the granularity required to protect the sensitive data and applications hosted on cellular IoT devices.

Cellular endpoints frequently run diverse software components, generating outbound traffic that traditional tools cannot adequately monitor or manage. Without proper visibility into these devices' behavior and data transmissions, security teams are unable to detect anomalies, enforce policies, or respond effectively to emerging risks. This reliance on implicit trust within mobile connectivity expands the attack surface, increasing operational risks and exposing critical systems to compromise.

Security concerns revolve around SIM misuse, including unauthorized access to internal apps that can breach organizational perimeters, exploitation of unlimited internet plans resulting in "bill shock," and improper use of secure remote access mechanisms, which opens the attack surface. Environmental factors further compound these risks, with issues such as battery consumption, latency increases, and speed reductions affecting device performance in harsh and remote operating conditions.

Advancements such as 5G networks and technologies like REDCAP (Reduced Capability) devices enable low-power, effective communications for cost-sensitive and ruggedized ecosystems[2]. However, gaps remain, with many current 5G networks relying on legacy 4G backends and outdated modems in devices, thus limiting their ability to fully utilize next-gen capabilities[3]. Moving forward, cellular IoT devices and infrastructure will require both modern network architectures and robust security frameworks to maximize scalability, reliability, and protection across industries critical to modern infrastructure.



[2] https://www.ericsson.com/en/reports-and-papers/white-papers/redcap-expanding-the-5g-device-ecosystem-for-consumers-and-industries

[3] https://www.bloomberg.com/explainers/why-5g-is-an-expensive-flop

[4] https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook

Android Threat Landscape

Zscaler ThreatLabz recorded nearly 34 million blocks for various Android malware, marking a 67% increase compared to last year's data. The growth was primarily driven by trojans (64%), followed by Adware (22%) and potentially unwanted applications (PUAs) (7%).

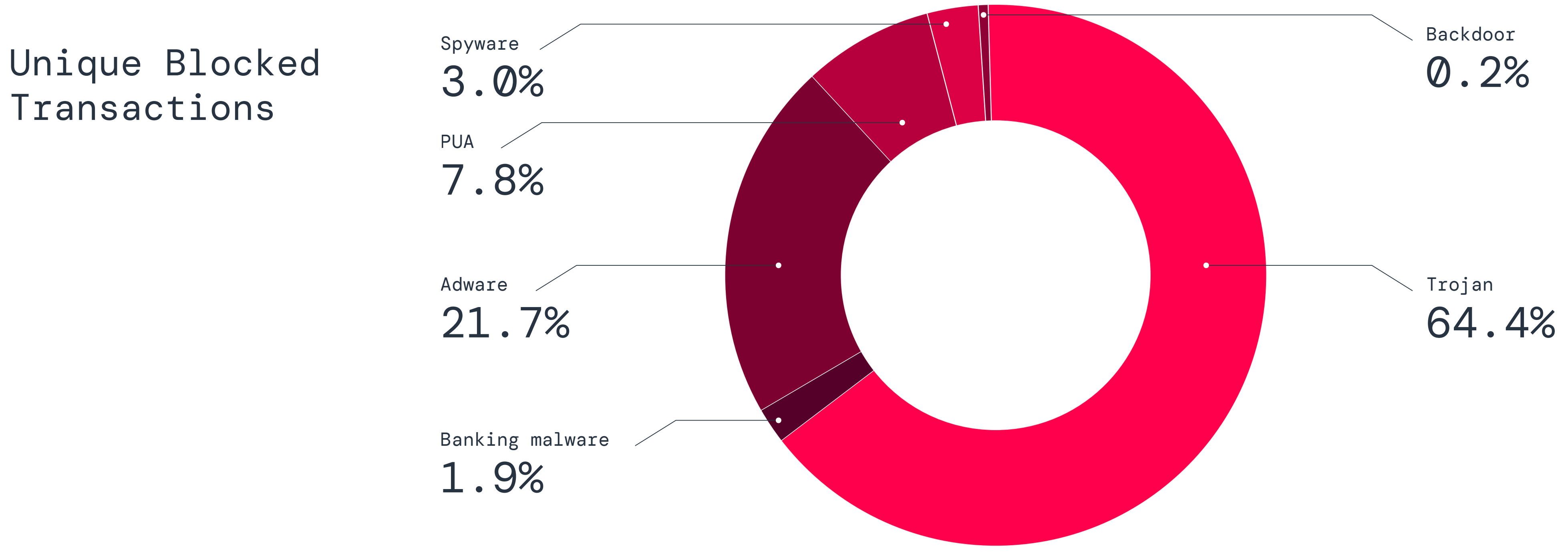


Figure 2: Shows unique blocked transactions for Android malware.

Comparing month-over-month data, ThreatLabz observed an average of 2.8 million blocks, with a significant spike in March due to Android Void malware specifically targeting Android TVs.

Android Void (usually spelled Vo1d) malware was first observed in September 2024, and functions as a backdoor, allowing threat actors to download and install third-party software unbeknownst to the owner of the infected device. As of February 2025, Android Void is **known** to have infected at least 1.6 million Android TVs. Android Void specifically targets streaming boxes running old Android versions using the **Android Open Source Project**. Between June 2024 and May 2025, ThreatLabz successfully blocked 17,696,808 transactions associated with Android Void.

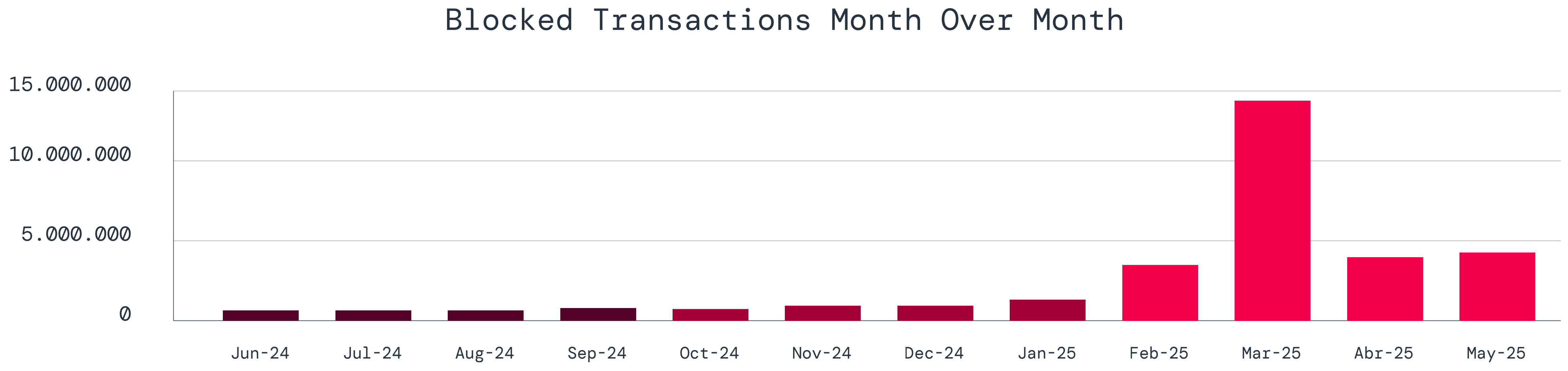
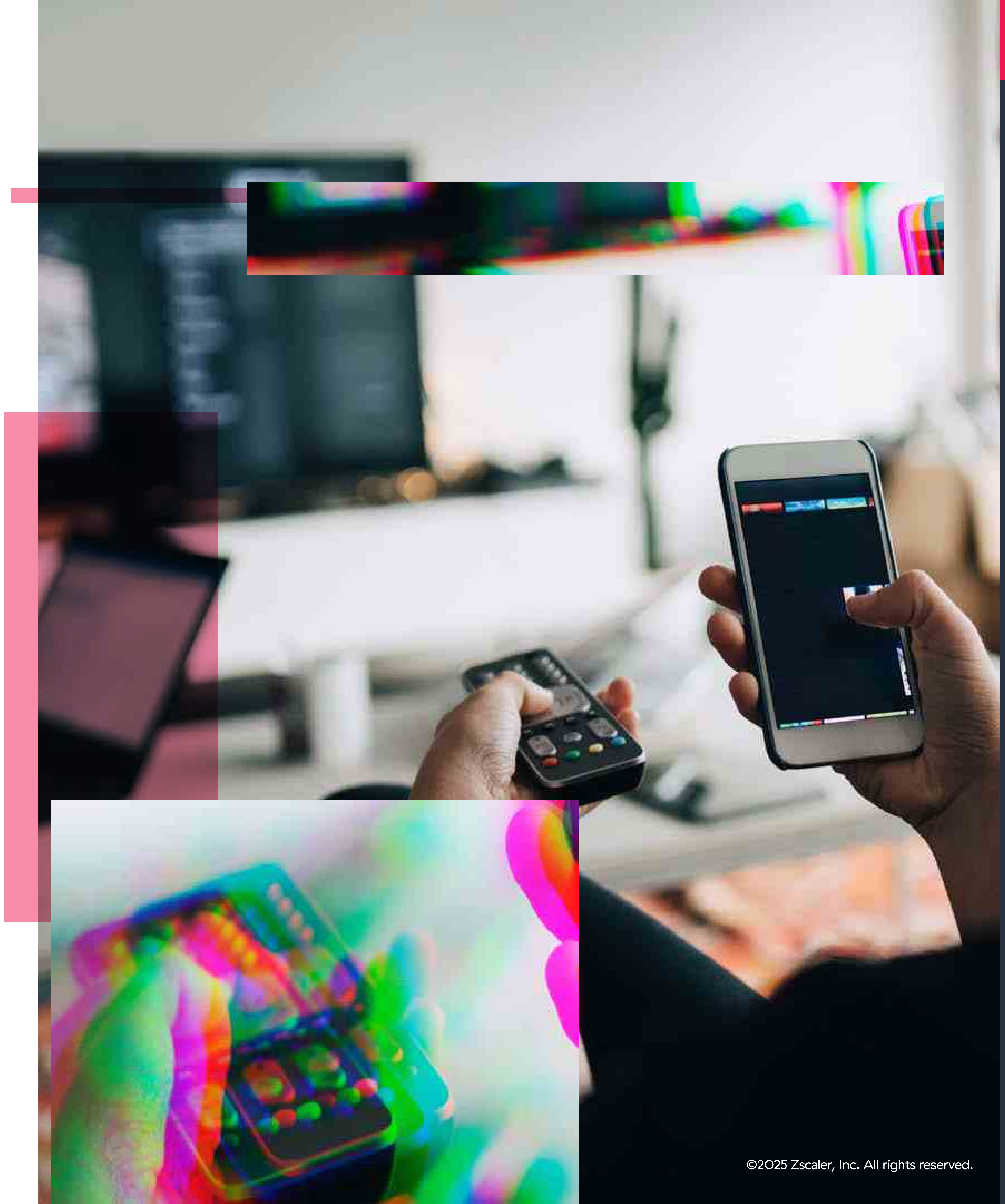


Figure 3: Shows blocked Android transactions month over month.



Banking Malware

Banking malware remains consistent, demonstrating steady growth over the past three years. During 2022–2023, banking malware transactions totaled 3.68 million, increasing significantly to 4.76 million in 2023–2024, a 29% year-over-year rise. The trend continued into 2024–2025, reaching 4.89 million transactions, though the growth rate slowed to 3%.

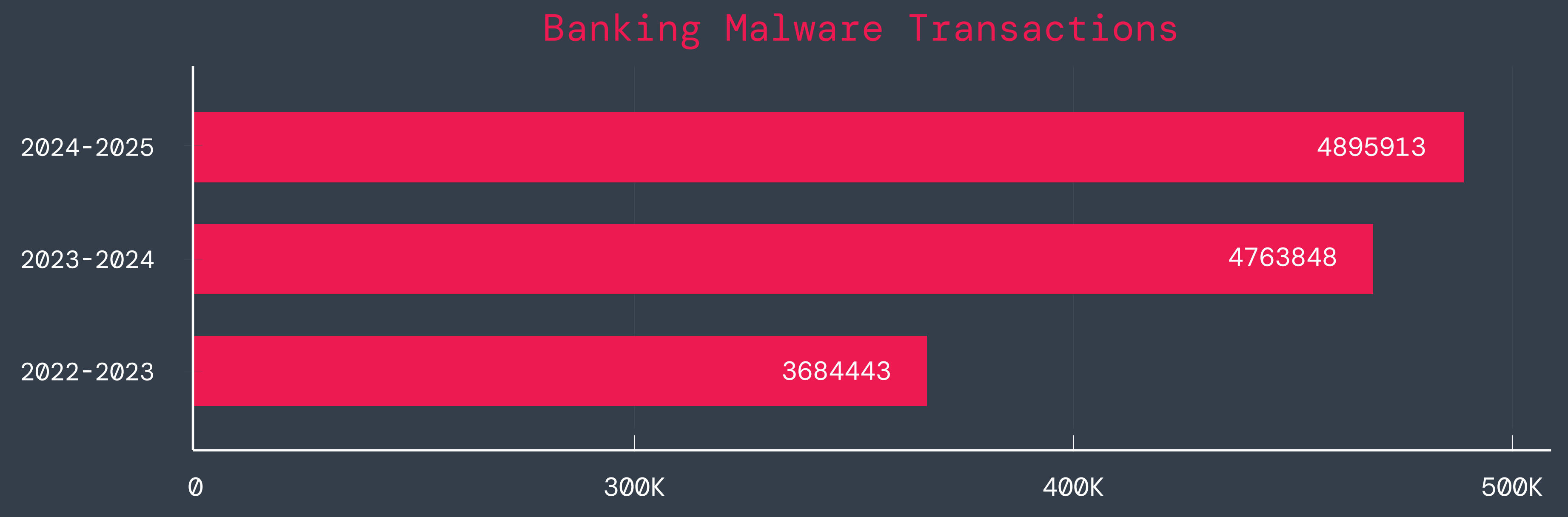


Figure 4: Banking malware transactions by year

The most active banking malware families, based on transaction count, include:

Trickmo: is an Android banking trojan developed in 2020 as companion malware to TrickBot. In 2021, it became a standalone trojan with overlay attack capabilities, and in 2024 gained remote control features for on-device fraud.

Ermac: is an Android banking trojan based on Cerberus malware, first identified in 2021. It targets banking apps to steal credentials, intercept SMS messages, and bypass MFA. It uses overlay attacks to collect sensitive information and is distributed via fraudulent apps posing as legitimate.

Anatsa: is a well-known Android banking trojan targeting financial apps, now affecting over 831 banking apps. It recently expanded operations into regions like Germany and South Korea and is distributed via dropper apps, including through the Google Play Store.

Cerberus: is an Android banking trojan that steals login credentials, two-factor authentication codes, and personal data. It overlays fake login screens on banking apps or collects data directly from infected devices.

Coper: is an Android banking trojan linked to ExoBotCompat, derived from Exobot malware. Discovered in July 2021 targeting users in Colombia, it has spread to Europe, Australia, and South America. It is disguised as legitimate apps on the Google Play Store and uses a modular design and multi-stage infection to avoid detection and removal.

THE FOLLOWING ARE KEY FEATURES OF ANDROID BANKING MALWARE:

Overlay-Based Phishing
Uses fake login screens or pop-ups over legitimate apps to steal credentials in real time. Captured credentials are sent to attackers.

Accessibility Service Abuse
Exploits Android's Accessibility Service to gain device control," read screen content, perform clicks, auto-grant permissions, disable security features, and steal sensitive data.

SMS and Notification Hijacking
Intercepts SMS messages, including two-factor authentication (2FA) codes, and uses notification hijacking to suppress OTP alerts while stealing the codes.

Keylogging and Screen Capture
Records user interactions with financial apps by logging keystrokes, capturing taps, taking screenshots, or recording videos to steal sensitive data.

Remote Control & Command-and-Control (C2)
Includes RAT functionality, enabling attackers to remotely control infected devices and execute commands covertly.

Clipboard Hijacking (Cryptotheft)
Targets cryptocurrency users by replacing wallet addresses in clipboard data or stealing private keys to enable unauthorized access to funds.

Persistence and Self-Defense
Conceals app icons to evade detection and prevent removal; employs tactics to block device reboots or interfere with uninstallation processes.

Anti-Analysis and Evasion
Uses anti-emulation, anti-debugging, code obfuscation, and encryption techniques to avoid detection by security tools and make malware analysis more difficult.

Geofencing and Targeted Attacks
Targets specific countries or financial apps, activating only under certain criteria to enhance effectiveness and avoid raising suspicion.

Data Harvesting and Profiling
Collects personal data, such as contacts, browser history, device location, and installed apps, for use in further attacks, social engineering, or selling on the dark web.

Spyware

Spyware activity increased by 220% year over year, driven by malware families like TrickMo, Ermac, SpyLoan, and SpyNote. Designed to monitor and collect user activity without consent, spyware captures call logs, messages, contacts, location data, browsing history, and even real-time audio and video. Attackers use this data for identity theft, blackmail, and targeted cyberattacks.

Based on transaction count, the top three spyware families include:

SpyNote (a.k.a. SpyMax) is spyware with RAT capabilities, typically delivered via smishing attacks. Users are tricked into downloading malicious apps disguised as legitimate software. Once installed, SpyNote allows attackers to access the device remotely, stealing personal data, intercepting SMS messages, recording calls, capturing screenshots, activating cameras and microphones, and manipulating files.

SpyLoan is Android malware that disguises itself as loan apps, targeting regions where payday and personal loans are popular. These apps promise quick loans but instead collect sensitive data like contacts, messages, and device details. The information is used for harassment, blackmail, or extortion related to predatory loan practices.

BadBazaar is Android malware designed for surveillance and data theft, targeting specific regions or communities. It masquerades as legitimate apps like communication or utility tools. Once installed, it gathers call logs, SMS messages, location data, and device details while enabling remote monitoring.

Timeframe	Number of Spyware Transactions
2022—2023	109,889
2023—2024	232,093
2024–2025	743,806

Geographical Analysis

A worldwide surge in mobile threat attacks has been observed, with numerous countries among the top 10 by attack volume witnessing a substantial increase compared to the previous year. The majority of these attacks were concentrated in three key regions: India, accounting for 26% of all mobile attacks, followed by the United States at 15%, and Canada at 14%. This concentration suggests a focus by threat actors on regions with high mobile device penetration and potentially broader attack surfaces.

India, in particular, experienced a significant 38% increase in mobile threat attacks compared to the previous year. This alarming rise aligns with multiple advisories issued by the Government of India concerning a surge in Android malware attacks. The prevalence of Android devices in the Indian market, coupled with evolving threat actor tactics, likely contributes to this elevated risk. The nature of these attacks in India often involves sophisticated social engineering techniques, phishing scams, and malicious applications designed to compromise user data and device integrity. This necessitates robust user education campaigns and advanced mobile security solutions capable of detecting and mitigating complex threats.

While India, the USA, and Canada represent the largest volumes of attacks, two other regions, Italy and Israel, have shown a dramatic increase in blocked transactions compared to last year's report. Although these regions currently contribute less to the overall volume of attacks, their exponential growth warrants close monitoring. Italy experienced an astonishing increase of over 800% in blocked transactions, while Israel witnessed an even more staggering surge of approximately 4000% compared to the previous year. This dramatic escalation is likely attributable to a combination of targeted attacks and the volatile geopolitical unrest prevalent in the region. Threat actors often exploit periods of instability and heightened digital activity to launch sophisticated cyber campaigns. These attacks could range from espionage and data exfiltration to financially motivated schemes, adapted to the specific sociopolitical context of these nations.

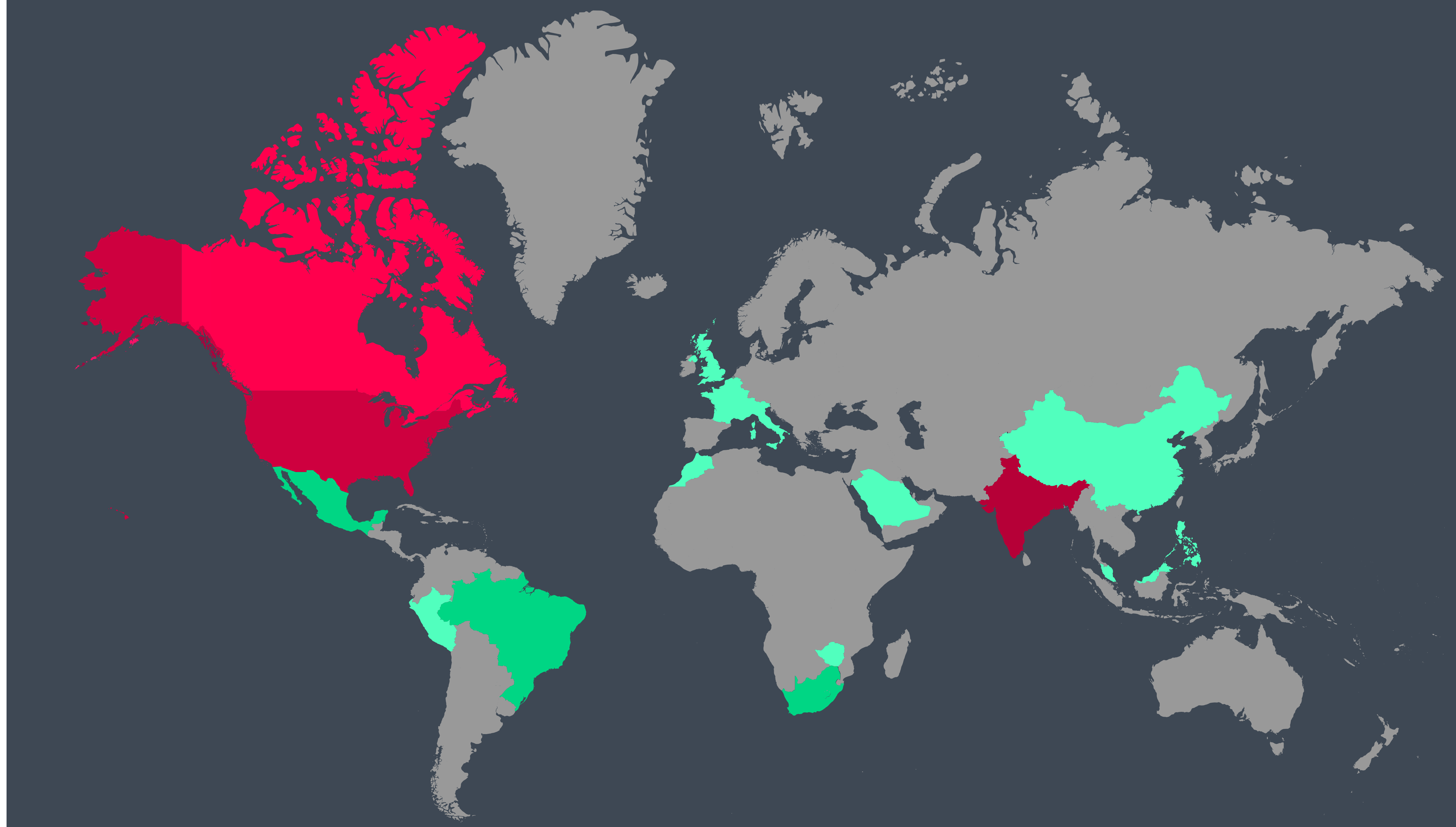


Figure 5: Top 10 Most Targeted Malware by Country

TOP 10 MOST TARGETED COUNTRIES

Most mobile malware targeted the following countries:

- India
- United States
- Canada
- Mexico
- South Africa
- Brazil
- Israel
- United Kingdom
- United Arab Emirates
- Italy

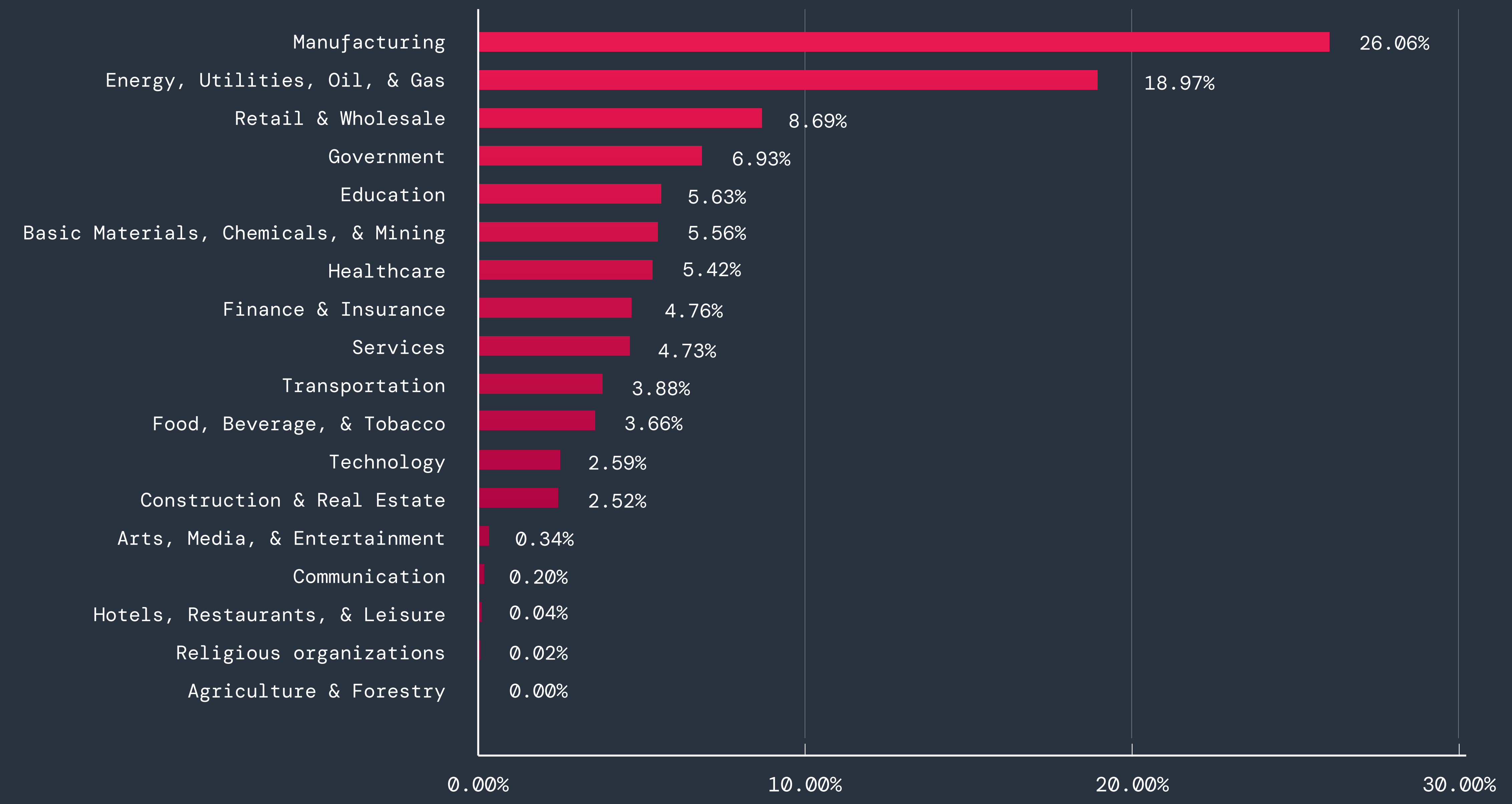
Industry and Sector Analysis

Most targeted verticals

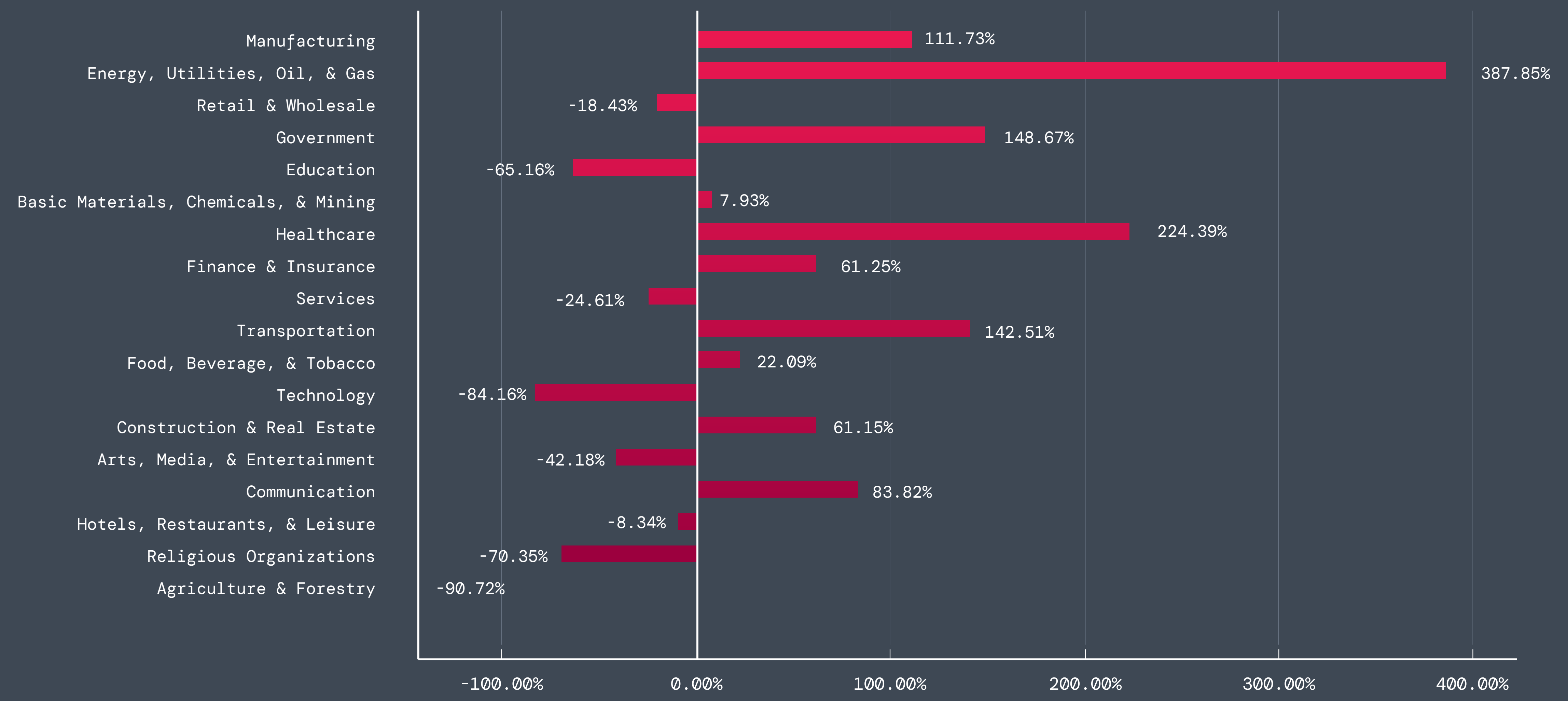
Attackers consistently prioritized industries where mobile demands are growing and use cases are expanding.. This pressure stemmed from several factors: the potential for severe operational disruption, the sensitivity of stolen data leading to significant reputation damage, and heightened regulatory exposure. Analyzing overall Android attack volumes per industry reveals a clear pattern of attacker focus. The Manufacturing and Energy sectors, including critical Oil and Gas industries, alongside Retail and Wholesale, remained the most frequently targeted sectors, representing high stakes environments where successful attacks could yield substantial returns for cybercriminals.

A year-over-year comparison highlights a massive surge in attacks against the Energy and Healthcare sectors. The Healthcare sector experienced a nearly 225% increase in attack volume, reflecting the critical nature of its services and the invaluable, highly sensitive patient data it holds. Similarly, the Energy sector saw an even more dramatic rise, with a 387% increase compared to the previous year's report. This significant escalation underscores the growing threat to critical infrastructure and the increasing exploitation of vulnerabilities within these essential industries. The interconnectedness of these sectors, coupled with their vital role in daily life and national security, makes them prime targets for sophisticated cyber campaigns designed to maximize impact and financial gain.

Industry Verticals



Changes in vertical attacks



Top
IoT & OT Threats

The IoT and OT threat landscape continues to evolve, with attackers increasingly refining their tactics and expanding their focus across industries and regions. Malware families like Mirai, Mozi, and Gafgyt dominate attacks, leveraging vulnerable IoT devices for botnet expansion and malicious payload delivery. Geographic targeting has diversified significantly, with new hotspots emerging in Asia and Europe, challenging the United States' historical prominence as the top target. Industry shifts highlight growing risks in Manufacturing, Transportation, Hospitality, and Arts & Entertainment, all driven by increased IoT adoption. Attackers continue to exploit common vulnerabilities, such as command injection in routers, demonstrating the persistent reliance on weak device security to penetrate networks and disrupt operations.

Overview

As organizations across industries embrace IoT and OT technologies to drive efficiency, productivity, and automation, cyberthreat actors are adapting their approaches to exploit vulnerabilities in these increasingly interconnected systems. Recent projections estimate that the number of IoT devices worldwide will double from 19.8 billion in 2025 to more than 40.6 billion by 2034, highlighting the critical role these devices play in modern infrastructure[4]. From smart sensors optimizing manufacturing processes to connected cameras monitoring remote sites, IoT and OT ecosystems have become foundational to operations in sectors such as logistics, energy, healthcare, and automotive.

The widespread integration of IoT and OT systems into essential workflows significantly raises the stakes for cybersecurity. Many of these devices are embedded in environments with unique challenges, such as ruggedized ecosystems in harsh conditions or legacy systems dependent on outdated protocols. This creates fertile ground for attackers to exploit weaknesses, target unpatched vulnerabilities, and leverage IoT endpoints to breach corporate networks or disrupt operations.

Just as Bring Your Own Device (BYOD) policies have expanded attack surfaces for mobile endpoints, IoT's exponential growth and diverse applications have similarly transformed the threat landscape. With malicious actors employing tactics such as IoT botnets, command injection vulnerabilities, and SIM misuse, this report sheds light on how adversaries are increasingly targeting these systems. Understanding these evolving risks is crucial for organizations to strengthen defenses and protect the critical infrastructure built on IoT and OT technologies.

[4] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Trends

THREAT ACTORS RAMP UP EXPLOITATION OF ROUTER VULNERABILITIES

Year after year, ThreatLabz has observed that routers are a primary target for IoT exploitation. Threat actors use vulnerabilities to execute commands, propagate malware, and expand botnets. Netgear routers are an especially popular target for threat actors with common exploitation methods observed, including command injection via API endpoint URLs and directory traversal techniques to access sensitive subdirectories such as /cgi-bin/. These attacks often exploit unauthenticated remote code execution (RCE) vulnerabilities, such as CVE-2016-10174 and CVE-2018-10561 that allow threat actors to bypass authentication and execute scripts remotely. Payloads like Mirai, the most popular malware targeting IoT devices, are frequently deployed to recruit compromised devices into botnets which then enable network-wide control for Distributed Denial of Service (DDoS) attacks or further propagation. Additional exploits, such as those targeting Parks Fiberlike routers (CVE-2023-33617) and D-Link routers (CVE-2016-20017), also indicate that the ongoing trend of threat actors exploiting routers shows no signs of slowing down.

THREAT ACTORS CONTINUE TO USE IOT WEAKNESSES TO SPREAD BOTNETS

IoT-based botnets, like the aforementioned Mirai, continue to exploit weak router configurations and firmware vulnerabilities to automate their propagation. Threat actors use shell commands to delete files, download malicious payloads with wget or curl, and set permissions with chmod in the /tmp directory. These vulnerabilities are exploited to further recruit more vulnerable devices into the botnet. Infected devices are often observed beaconing to C2 servers or sending out traffic containing exploits to further recruit devices, providing evidence of their activation as botnet nodes.

CASE STUDY: BEACONING ACTIVITY IN A SUSPECTED COMPROMISED ROUTER

In one instance, the Zscaler Threat Hunting team observed a device that exhibited consistent beaconing activity to a suspicious IP address at 26 to 27-second intervals. Each request measured exactly 78 bytes, with the user agent identified as `curl/7.60.0`. The precise and repetitive pattern, with a standard deviation of just 1 second, strongly suggested automated botnet behavior or backdoor exploitation.

Further analysis revealed that the beaconing activity was isolated to a single device which was most likely a compromised router reaching out to a Chinese destination IP address. The device appeared to be a Wavlink model, a widely available router already known for vulnerabilities that allow remote code execution and recruitment into botnets.

Botnets, like Mirai, have a history of exploiting such weaknesses to compromise devices in order to further coordinate attacks, including Distributed Denial of Service (DDoS) campaigns. An infamous example is the 2016 Mirai-driven DDoS attack on Dyn that took down popular platforms such as X.com (formerly Twitter), GitHub, and PayPal.

Once infected, these devices not only participate in attacks but also propagate malware to other vulnerable devices, further expanding the botnet's reach, especially in home environments where security measures are typically weaker.

THREAT ACTORS ARE LEVERAGING USER-AGENT STRINGS TO IDENTIFY COMPROMISED DEVICES

Another trend observed by the Zscaler Threat Hunting team is threat actors leveraging notable User-Agent strings. Many observed user agents are anomalous and conspicuous, such as "`linus-torvalds-loves-you`" or "`r00ts3c-owned-you,`" while others are less obvious, such as "python-requests/2.32.3" or "`curl/7.60.0.`" These modified user agents can be used to identify script-based exploitation attempts and beaconing activity, and create irregular traffic patterns that may signal botnet activity. The use of these conspicuous User-Agent strings often reflects traffic from compromised IoT devices that the Zscaler Threat Hunting team will continue to monitor and report.

IoT Malware

Mirai continues to dominate the IoT malware landscape by a wide margin, maintaining its position as the most prevalent threat. This year, Mozi edges out Gafgyt with a slight lead, taking the second spot. Together, these three families account for the majority of observed activity, showing little change in the broader trend of a few dominant malware strains leading the space.

Top IoT Malware Families

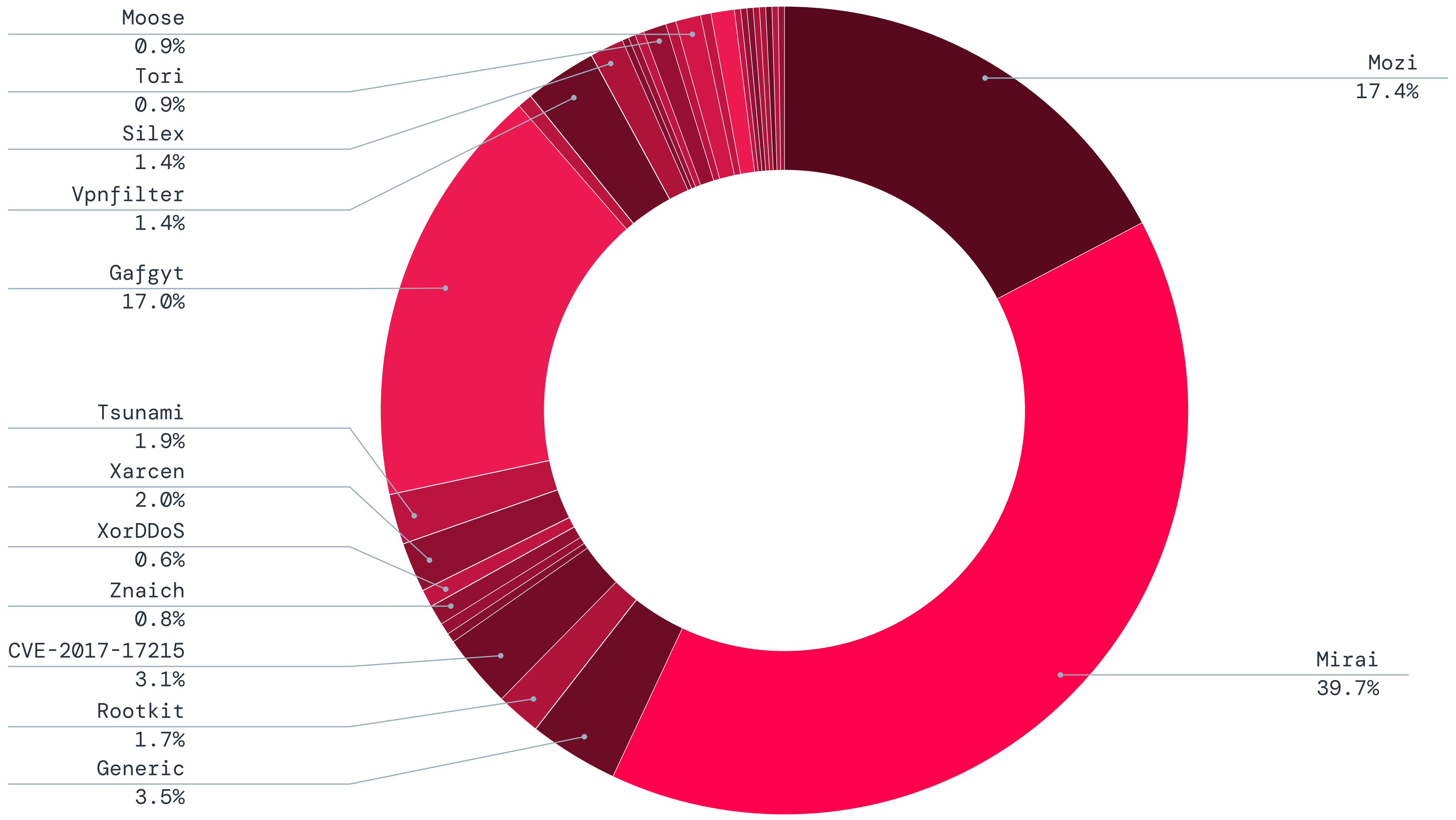


Figure 6: Top IoT malware families observed in the Zscaler cloud

ROUTERS REMAIN THE PRIMARY FOCUS OF IOT ATTACKS

Routers continue to be the primary target for IoT malware, making up 76.2% of all attacks. This trend reflects their central role in IoT networks and the consistent focus of attackers on exploiting them, likely due to their position as the gateway for connected devices and data flows.

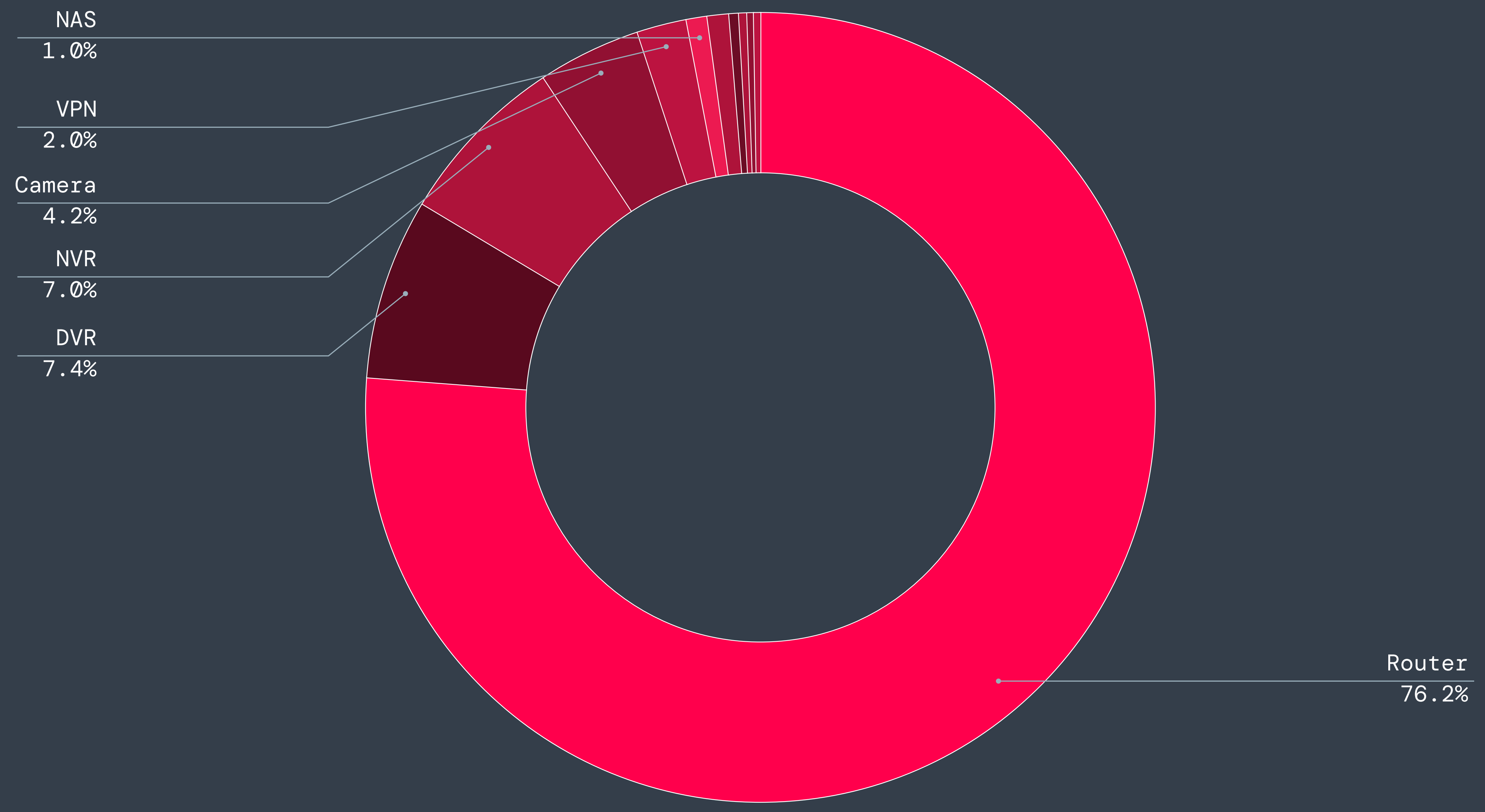


Figure 7: Devices most targeted by malware attacks

IoT Device Categories

Benign IoT devices and their traffic:

TOP DEVICE CATEGORIES INTERACTING WITH THE ZSCALER CLOUD

The IoT devices connecting to the Zscaler cloud, encompassing both consumer and enterprise environments, underscore the exponential growth of connected technologies in our daily lives. This trend highlights the importance of implementing robust security solutions to safeguard the significant volume of data generated and transmitted by these devices.

The latest IoT device distribution data reveals evolving trends in cloud-connected technologies. Leading the chart are set-top boxes (13.8%) and data collection terminals (13.6%), emphasizing their prevalence in entertainment and logistics sectors. Close behind are payment terminals (12.2%) and smartwatches (11.9%), reflecting their prominence in secure transactions and wearable technology.

IoT Device Distribution

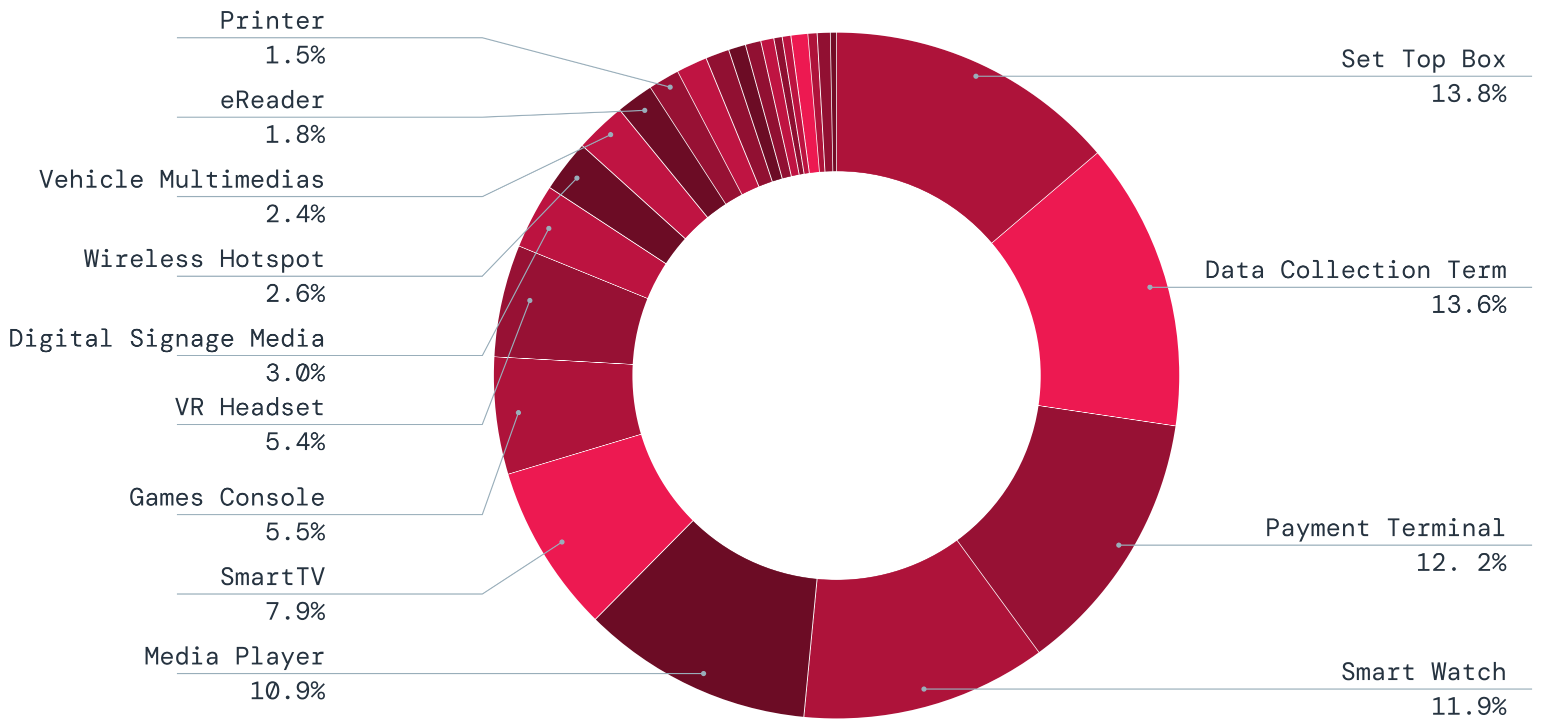


Figure 8: Distribution of IoT device categories in the Zscaler cloud

Data Collection Terminals remain the backbone of IoT traffic, accounting for a substantial 78.7% of the total. These devices are pivotal across industries like manufacturing, logistics, and warehousing, enabling efficient data aggregation and operational optimization. Printers (7.1%), digital signage media players (6.3%), and set-top boxes (6.2%) contribute significantly, showcasing the diverse applications of IoT devices. Medical devices, while representing 0.6%, highlight the growing niche for IoT in healthcare. This distribution underscores the integral role IoT devices play in driving data-centric workflows and innovation in interconnected systems.

IoT Device Transaction Distribution

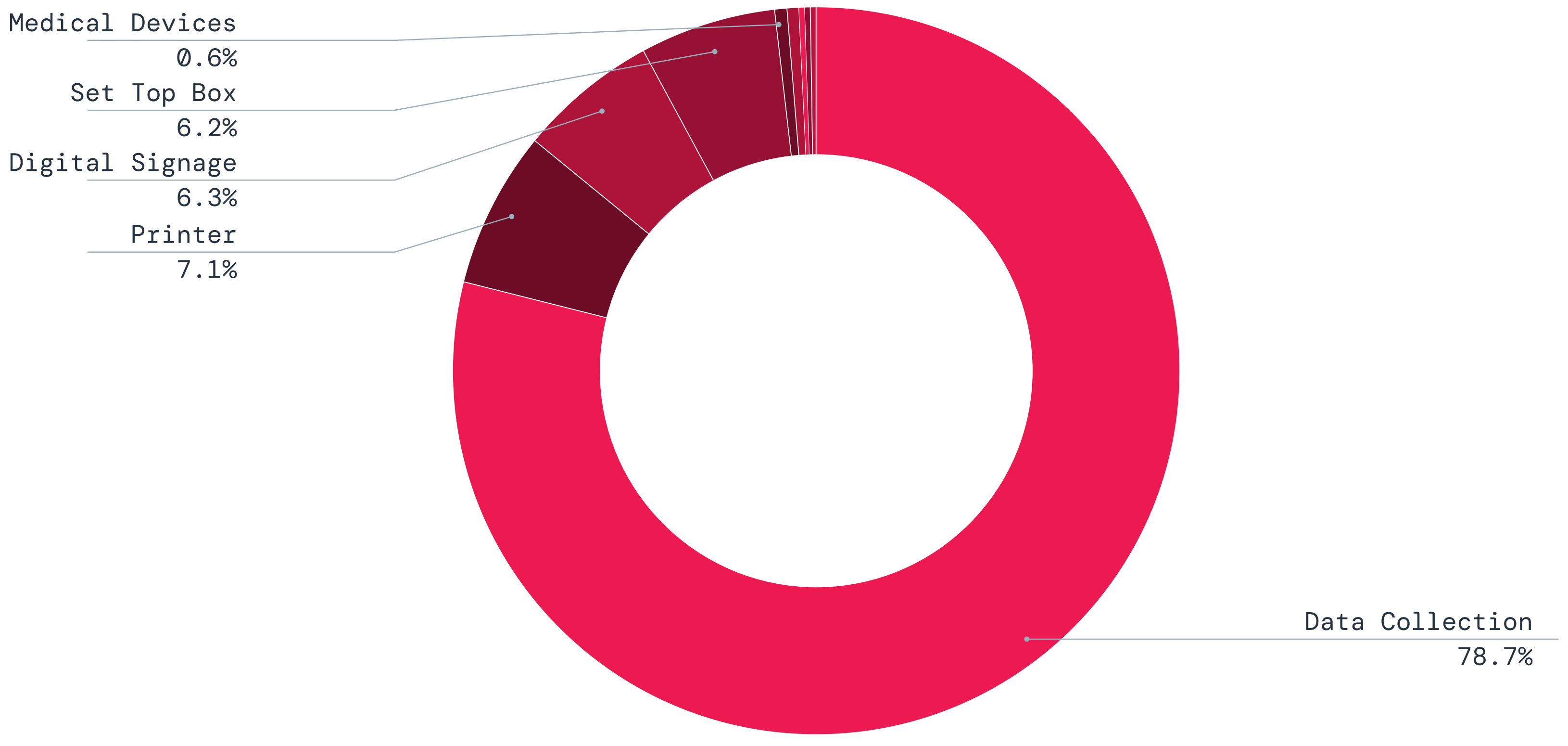


Figure 9: IoT devices generating the most traffic

THE RETAIL & WHOLESALE SECTOR REMAINS A LEADING IOT TRAFFIC GENERATOR

The Retail & Wholesale vertical continues to dominate IoT traffic, accounting for 52.7% this year. While still the largest contributor, this marks a notable decrease from last year's figure of 68%, indicating a shift in IoT traffic distribution across industries. This decline may reflect the diversification of IoT applications in other sectors like Transportation, which grew to 19.3%, and Manufacturing, which now stands at 6.8%. Despite the decrease, data collection terminal devices remain integral to Retail & Wholesale operations, driving a significant portion of its IoT traffic and underscoring their critical role in supply chain management and point-of-sale activities.

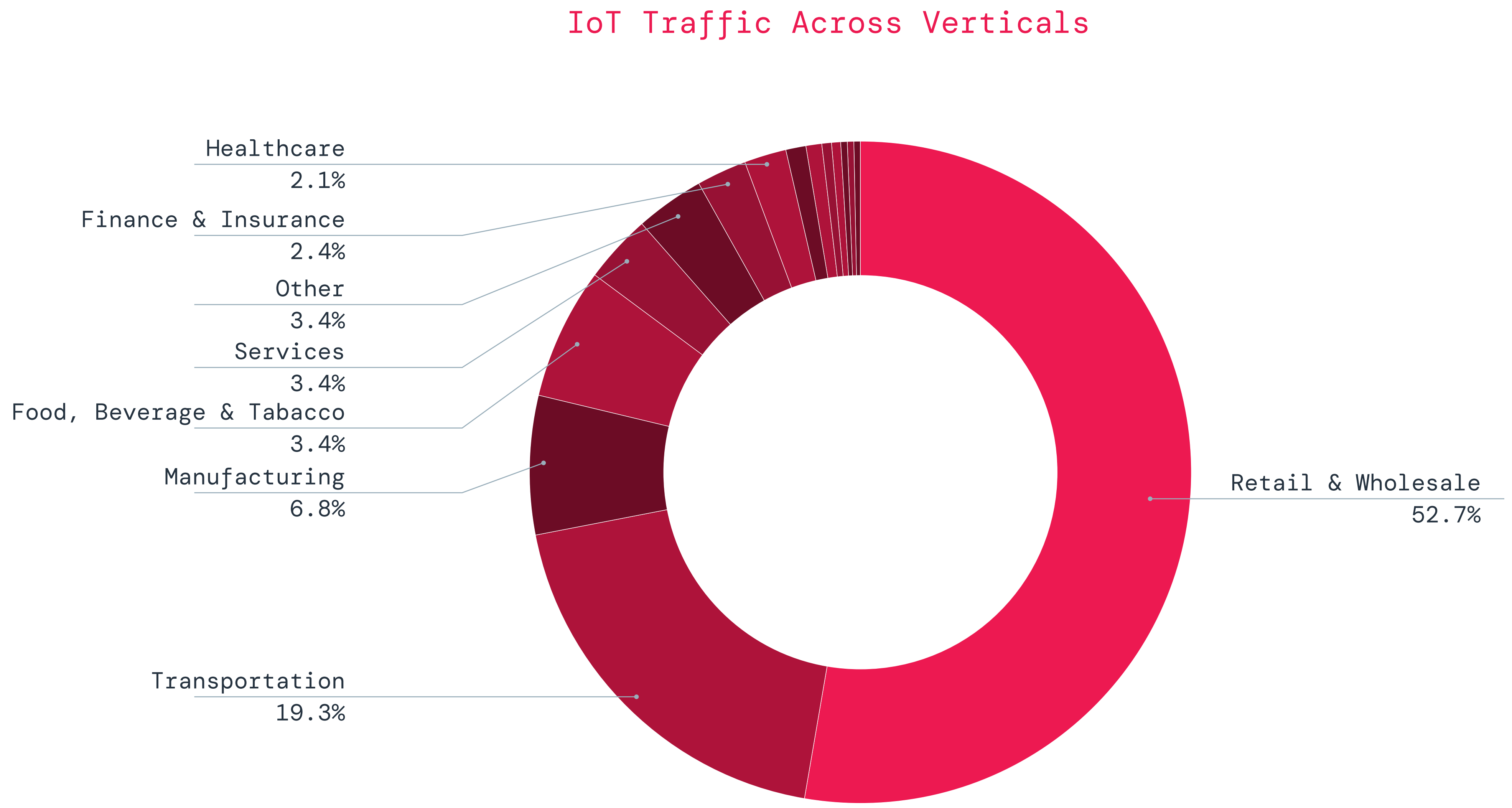


Figure 10: Industries that generated the most IoT traffic

MANUFACTURING LEADS IOT ADOPTION ACROSS VERTICALS

The Manufacturing sector continues to lead with the highest count of unique IoT devices among all verticals, showcasing its extensive use of connected technologies. This dominance is driven by the versatile applications of IoT in manufacturing, including automation, quality control, process optimization, and supply chain management. Other key verticals such as Services, Finance & Insurance, and Retail & Wholesale also demonstrate significant IoT adoption, reflecting the growing reliance on connected solutions in diverse industries.

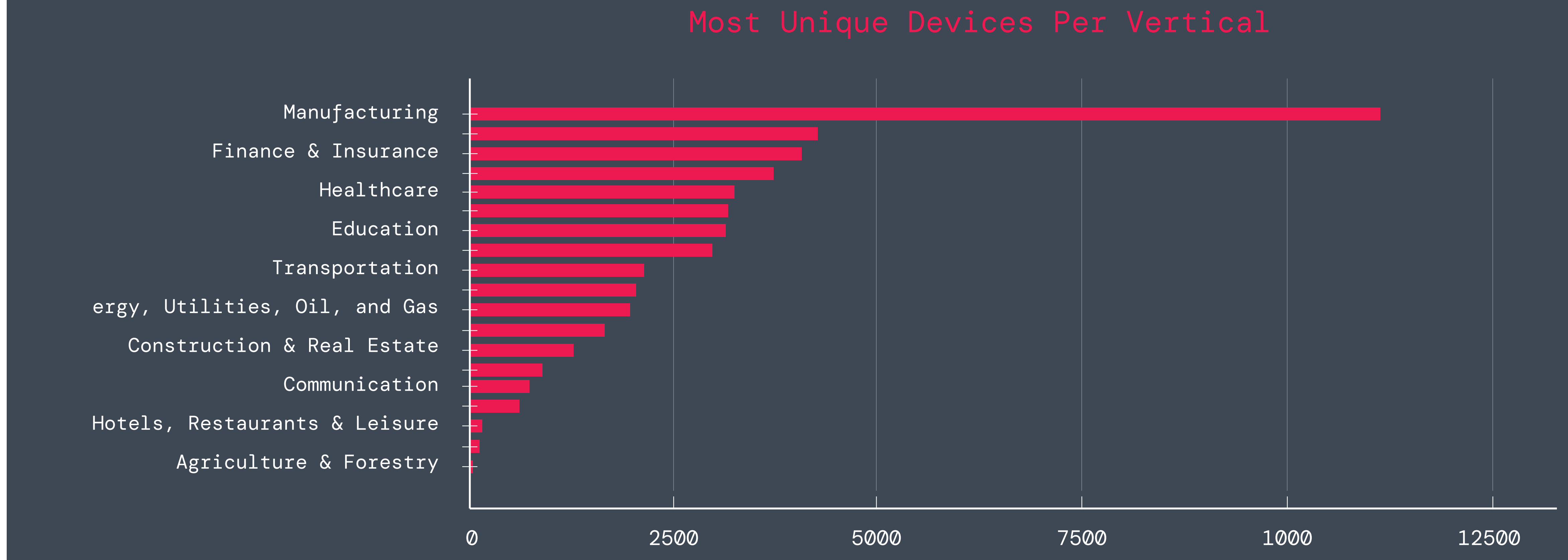
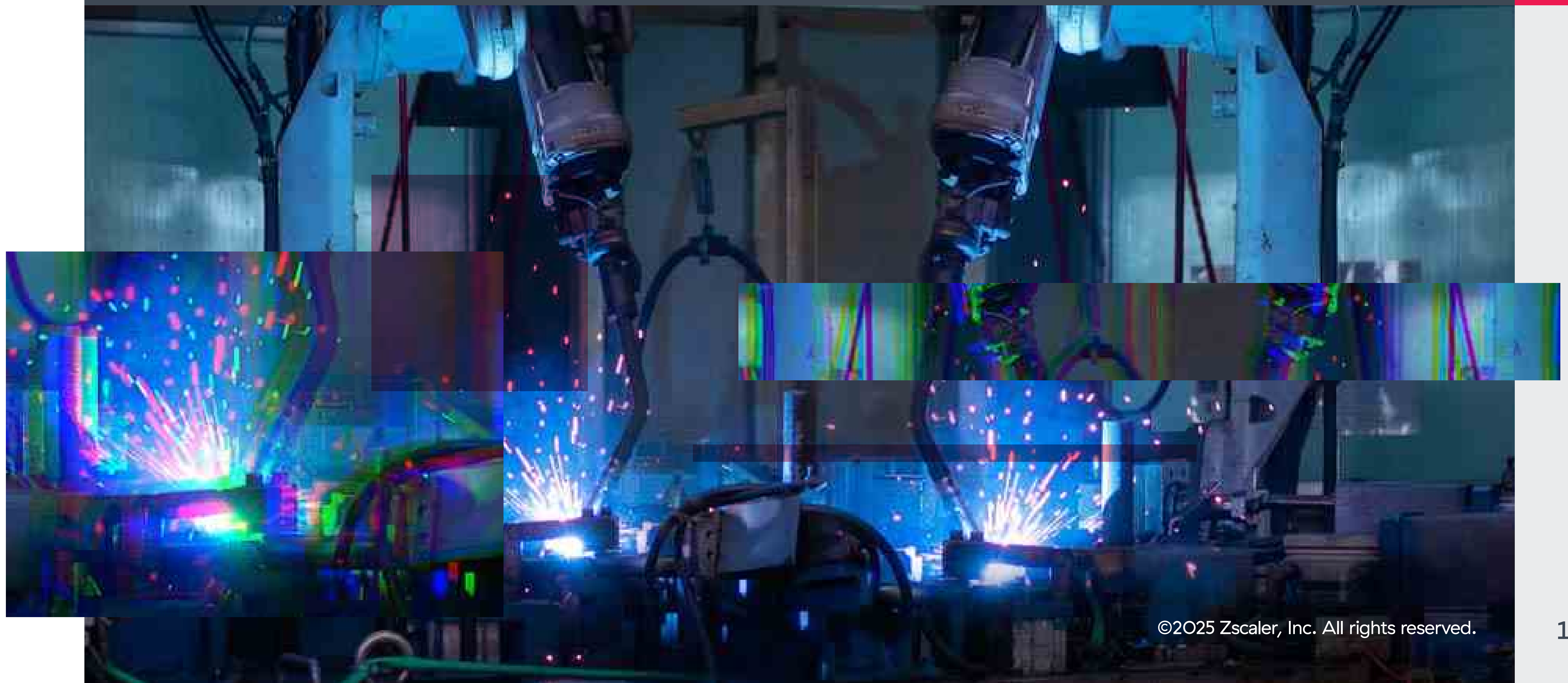


Figure 11: Unique device count by vertical



Industry and Sector Analysis

The Manufacturing and Transportation sectors continued to top the list of most-targeted verticals. This year, both sectors accounted for an equal 20.2% of all observed IoT malware attacks, jointly making up over 40% of total incidents. This represents a shift from 2024, when Manufacturing alone bore the brunt with 36%, followed by Transportation at 14% and Food & Beverage at 11%. The current distribution suggests that while Manufacturing remains a critical target, threat actors are increasingly spreading their efforts across other high-dependency IoT industries.

Notably, attacks surged in the Arts, Media & Entertainment sector, which now represents 8.8% of attacks—surpassing Finance & Insurance (6.9%), and closely followed by Services (8.6%). The Hospitality sector (Hotels, Restaurants, and Leisure) also saw increased activity, receiving 3.0% of attacks. These trends point to a widening threat landscape as IoT adoption grows beyond industrial domains, making a broader range of sectors vulnerable to malware-based disruptions.

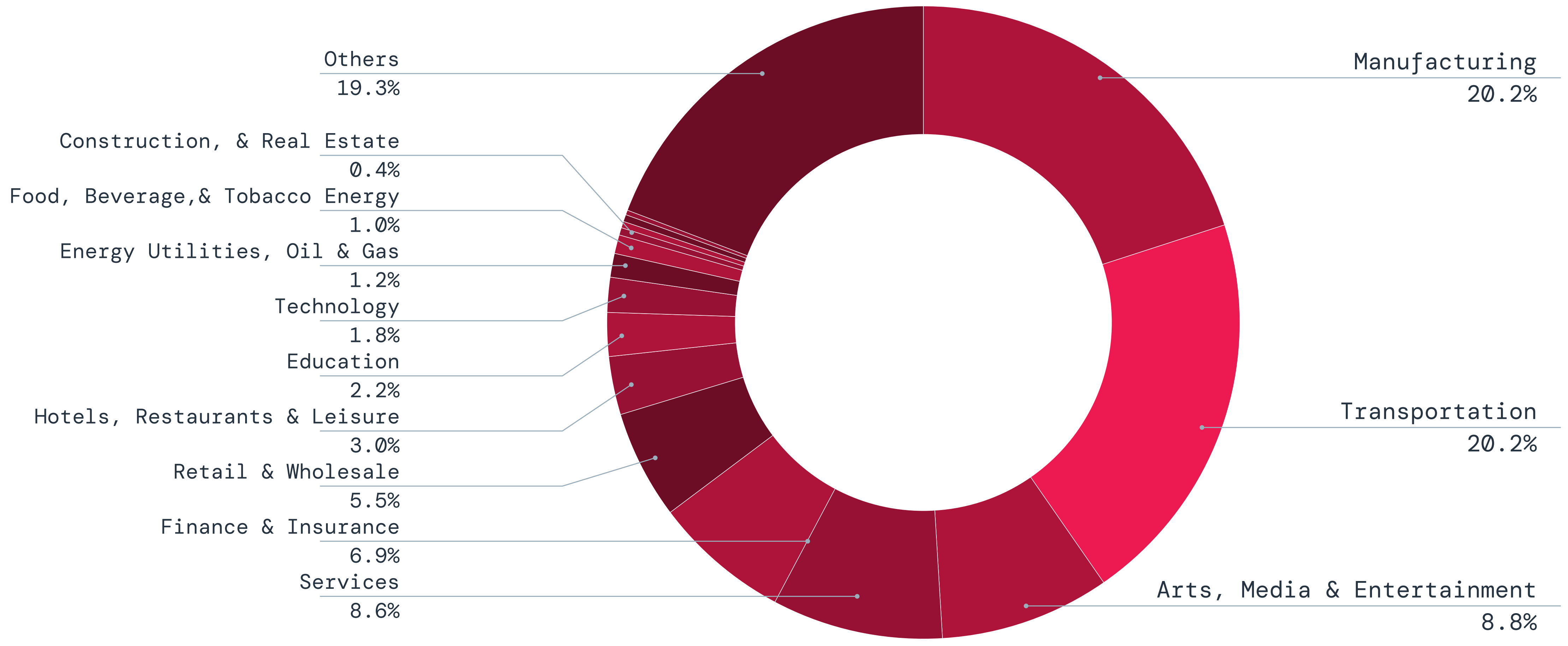


Figure 12: Distribution of the most targeted industries

Industries experiencing explosive YoY growth in attacks

Arts, Media, & Entertainment: This sector experienced a significant surge of 1,862% in IoT malware transactions. The widespread adoption of smart devices in entertainment venues, production studios, and home media consumption likely created new entry points for attackers seeking to disrupt operations, steal intellectual property, or leverage compromised devices for other malicious activities.

Education: The Education sector witnessed an alarming 861% increase in IoT malware activity, emerging as a significant target for cybercriminals. The surge can be attributed to the widespread adoption of IoT-connected technologies in schools, universities, and training facilities. From smart classroom devices and connected learning tools to campus security systems, these advancements have inadvertently created an expansive attack surface. Threat actors may be motivated by the potential to disrupt learning, steal sensitive student and faculty data, or conduct ransomware campaigns targeting understaffed IT systems in schools. With typically limited budgets for cybersecurity and expansive networks of devices, educational institutions face challenges in securing their increasingly interconnected infrastructure, making them prime targets for exploitation.

Finance & Insurance: This traditionally high-value target saw a substantial 702% growth. While often well-defended, the increasing integration of IoT devices for smart offices, security systems, and remote monitoring within financial institutions still presents opportunities for attackers, perhaps for initial compromise leading to more sophisticated attacks.

Energy, Utilities, and Oil & Gas: With a 459% YoY increase in IoT attacks, the Energy, Utilities, and Oil & Gas sector has become a critical target for malware campaigns. The ongoing digital transformation in this industry—such as the implementation of connected equipment, SCADA systems, and automated monitoring—has increased operational efficiencies but also exposed vital infrastructure to attackers. Motivations may range from espionage and intellectual property theft to operational disruption or sabotage, such as impairing energy grids, disrupting oil production, or tampering with natural gas pipelines. Given the essential role this sector plays in national security and economy, cybercriminals and even nation-state actors have shown a clear interest in exploiting these vulnerabilities. This growth serves as a reminder of the urgent need to secure IoT systems across critical energy infrastructure

Industries with Substantial Increases:

Several other sectors also demonstrated notable increases in IoT malware activity, indicating a broader expansion of attacker focus beyond the most dramatic surges:

Construction & Real Estate: This sector experienced a 410% rise, likely driven by the increasing use of smart building technologies, connected construction equipment, and IoT sensors for monitoring and automation in modern infrastructure projects.

Transportation: The Transportation sector saw a significant 382% increase in IoT malware attacks, highlighting the growing vulnerability of this critical industry. The rise in IoT adoption in transportation—such as connected vehicles, smart traffic management systems, fleet tracking technologies, and infrastructure sensors—has transformed operations but introduced considerable security challenges. Cybercriminals may seek to exploit IoT vulnerabilities to disrupt logistics and operations, compromise vehicle safety systems, or steal proprietary data. Additionally, the interconnected nature of transportation systems could allow attackers to launch cascading attacks that ripple across the supply chain. This alarming surge underscores the need for heightened security measures across transportation networks.

Government: The Government sector saw a concerning 370% increase in IoT malware activity, a testament to attackers increasingly targeting critical public infrastructure. IoT adoption by government agencies for resource monitoring, security, surveillance systems, and smart city initiatives has introduced new vulnerabilities into national and local infrastructure. Threat actors may exploit these systems to gain unauthorized access to sensitive government data or disrupt vital services such as traffic systems, emergency alerts, or public utilities. Given the sector's role in managing critical services, any successful compromise could lead to far-reaching consequences, impacting citizens directly. This rise highlights the necessity for governments to invest in robust IoT cybersecurity strategies to safeguard public trust and operational functionality.

Hotels, Restaurants, and Leisure: With 228% growth in attacks, this industry sector has become an increasing focus for IoT malware attacks. The proliferation of smart hospitality systems, connected appliances, and guest-facing IoT devices in hotels, resorts, and restaurants presents a vast attack surface. The motivation here could range from data theft (customer information, payment details) to operational disruption or even ransomware campaigns impacting critical services.

Services: With a 104% increase, the broad "Services" sector, encompassing a range of business and personal services, indicates a generalized expansion of IoT-related threats. This could be due to the adoption of IoT for efficiency and automation in diverse service industries and an increasingly attack surface.

MANUFACTURING: DEEPER DIVE

Despite a notable drop in the proportion of IoT malware attacks focused on Manufacturing—from 36% in 2024 to 20.2% in 2025—the sector remains the most-attacked industry, with 41% year-over-year growth. This is primarily due to the sheer volume and criticality of IoT implementations within Manufacturing. IoT devices play a central role in modern manufacturing operations, ranging from automation and process monitoring to predictive maintenance and supply chain management. These technologies drive efficiency and productivity but also create a vast attack surface for cybercriminals to exploit.

Manufacturing's reliance on IoT devices makes it uniquely vulnerable, as these devices are often interconnected with sensitive operational technology (OT). A compromise in one point of the network can ripple across systems, leading to production delays, financial losses, and potential safety hazards. Furthermore, the industry's critical role within global supply chains makes it an attractive target for attackers aiming to disrupt entire economies or extort organizations based on their dependency on seamless operations.

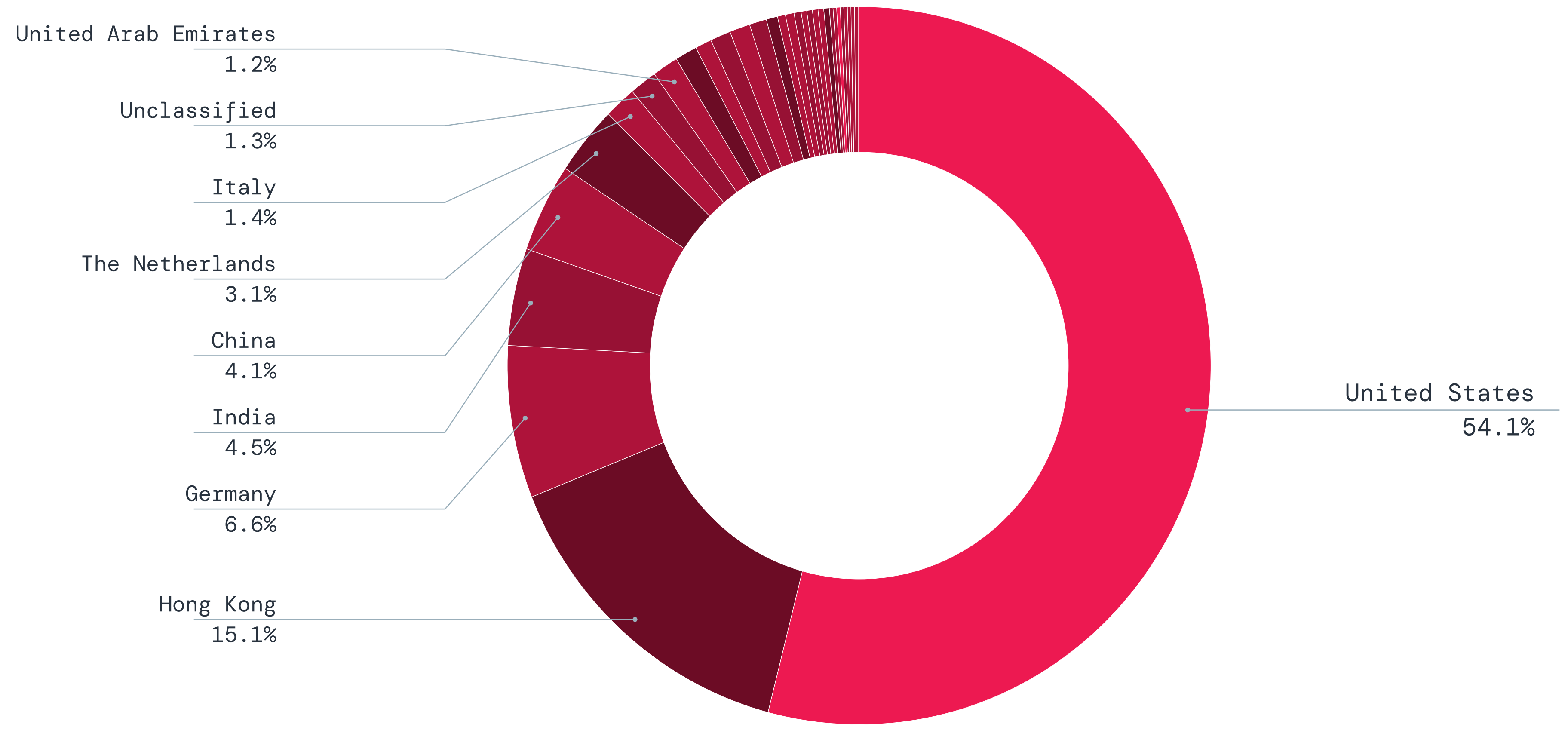
The diversification of threat activity across other IoT-heavy sectors, such as Transportation and Food & Beverage, highlights evolving adversary strategies. However, Manufacturing remains a prime target due to its vast attack surface, high-value processes, and deeply integrated IoT systems, which collectively make it a lucrative industry for cybercriminals. This reinforces the need for robust cybersecurity measures tailored to IoT vulnerabilities and heightened efforts in securing critical production environments.

Geographical Analysis

In an analysis of global IoT threats, the United States emerged as the primary target, absorbing a striking 54% of all detected IoT attacks. This substantial figure underscores the critical vulnerability of US-based IoT infrastructure. Following the US, Hong Kong experienced a notable 15% of these attacks, highlighting its position as a secondary, yet still significant, target for malicious IoT actors. Along with that, China, India and Germany saw IoT malware activities as well.

The United States remains the leading destination for IoT device traffic, handling 62.97% of overall transactions, reaffirming its critical role in global IoT infrastructure and communications. This dominant position highlights the US as both a hub for IoT activity and a primary target for malware attacks. The United Kingdom follows at 9.60%, with Australia (6.99%) and France (6.87%) contributing notable shares. While countries like Thailand (0.99%), Germany (0.92%), and Switzerland (0.91%) account for smaller portions, their presence underscores the growing geographical distribution of IoT activity. This diversification reflects an expanding IoT ecosystem worldwide, presenting both opportunities and risks across global markets.

Most Targeted Countries



Smart TVs and Data Collection Terminals Lead IoT Traffic Directed to China and Russia

Business Operations and Entertainment devices route a substantial share of their traffic to China and Russia with Data Collection Terminals emerging as the primary contributor, accounting for 53.7% of the total traffic.

Although a significant portion of this traffic is legitimate and harmless, ThreatLabz identifies these destinations as suspicious, raising concerns about potential government surveillance and data security vulnerabilities.

IoT Traffic Headed To Suspicious Destinations

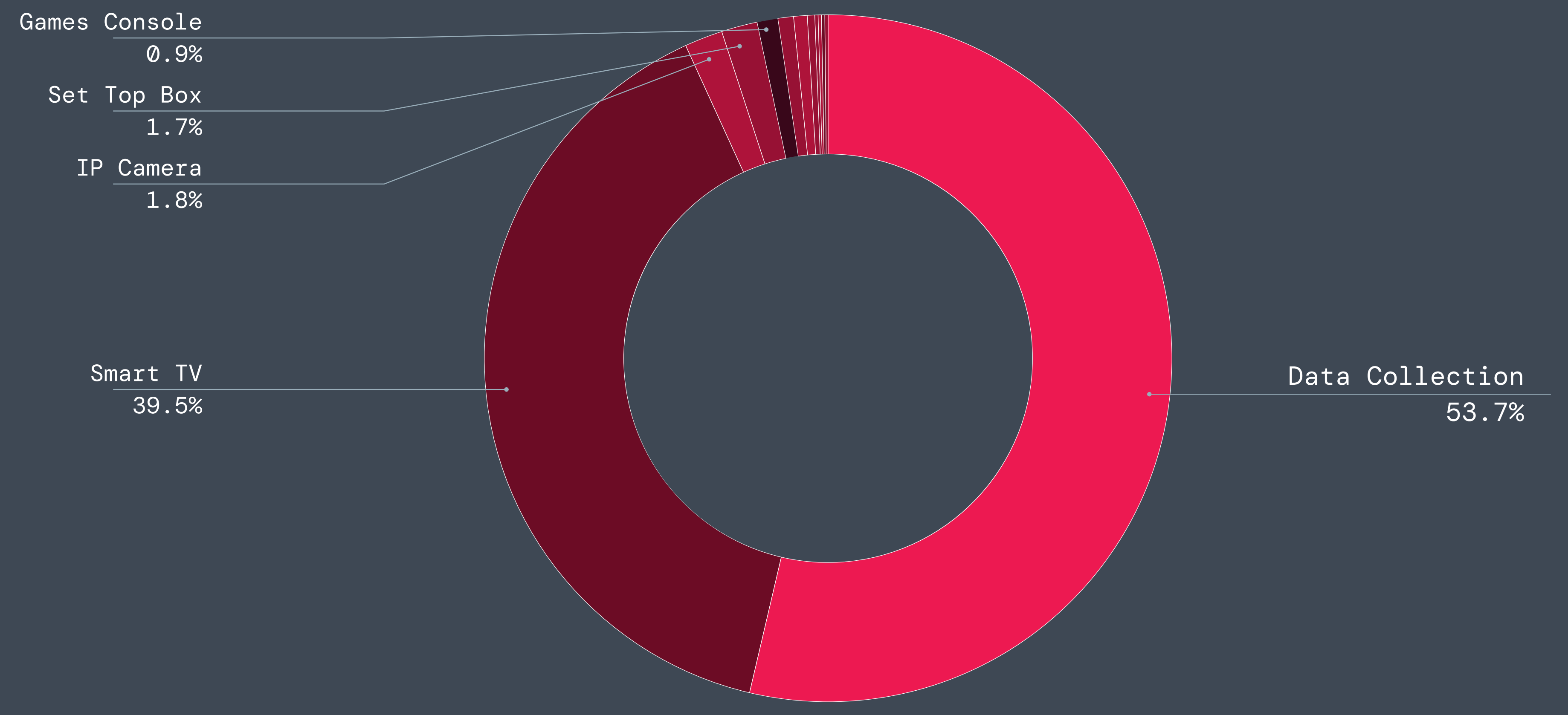


Figure 12: Distribution of devices across traffic deemed "suspicious"

Top Countries

United States

Hong Kong

Germany

India

China

The Netherlands

Italy

United Arab Emirates

Singapore

France

Public Sector: Defending Mobile, IoT, and OT Threats

Federal agencies and the public sector face mounting cybersecurity challenges as interconnected mobile, IoT, and OT systems become critical to delivering essential services. Overall, the Goverment sector saw a significant 370% rise in IoT malware attacks, together with a 147% growth in mobile-related attacks, the latter driven primarily by the proliferation of Android malware targeting devices critical to public operations. Meanwhile, the Energy sector experienced an unprecedented 387% increase in attack volume, underscoring the relentless targeting of critical infrastructure, while Healthcare, another vital industry, saw a nearly 225% increase in mobile attacks—driven by the value of highly sensitive patient data and the necessity of uninterrupted services for public health.

Legacy IoT and OT systems often lack modern security controls, making them prime targets for ransomware and state-sponsored threats. Nation-state actors such as Volt Typhoon deploy stealthy techniques to infiltrate government networks and maintain persistence, while Salt Typhoon uses weaponized IoT devices, including public routers and cellular-connected sensors, to gain access and facilitate lateral movement through critical infrastructures. In parallel, botnet families like Mirai, Mozi, and Gafgyt exploit IoT vulnerabilities, amplifying risks across increasingly integrated systems. Meanwhile, attacks targeting critical infrastructure sectors—including water treatment facilities, energy grids, and transportation networks—highlight the need for securing ruggedized IoT and cellular-connected devices to ensure continuity even in situations.

Supply chain vulnerabilities further complicate the security landscape, as compromised hardware, firmware, or third-party dependencies introduce new entry points for attackers. Securing cellular-connected devices with SIM-level traffic inspection mitigates unauthorized access and reduces the attack surface associated with insecure IoT adoption. Mobile endpoints, widely used in government applications, face escalating risks from phishing, smishing, and exploitation of telecom stacks. Enforcing zero trust policies for device connections and applying anomaly detection for network traffic are critical steps to manage these risks.

To address these challenges, federal agencies must apply zero trust architectures, advanced segmentation for IoT/OT devices, and proactive monitoring to counter rising threats. Embedding security across cellular networks, legacy systems, and public-facing devices is essential to securing sensitive information, maintaining operational resilience, and ensuring compliance with federal cybersecurity standards.

ACTIONABLE RECOMMENDATIONS

Zero Trust Implementation for Critical Networks

Federal agencies should adopt zero trust architectures to secure cellular IoT connections, isolate unmanaged OT systems into "networks of one," and prevent lateral movement by enforcing strict device segmentation.

Protect IoT and Cellular Gateways

Harden IoT and cellular gateways through continuous monitoring, anomaly detection, and firmware-level protections to counter supply chain risks and botnet recruitment vulnerabilities.

Enhance Supply Chain Risk Management

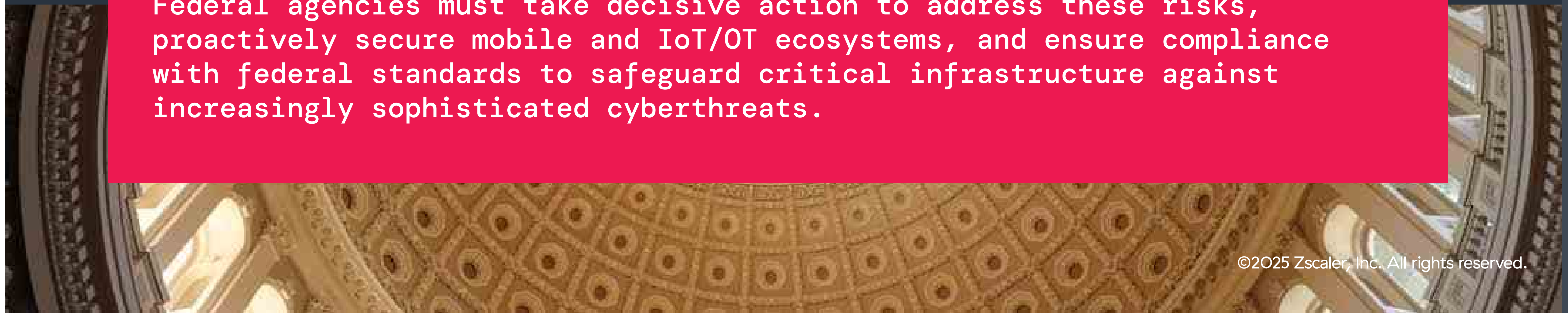
Create robust policies for IoT device procurement, ensuring all hardware and software meets established security standards (e.g., encryption, secure firmware updates). Collaborate with vendors consistent with CISA guidelines to address weak configurations before deployment.

Strengthen Endpoint Security Measures

Deploy advanced protections for mobile endpoints, including anomaly detection for SIM-level traffic, active phishing defenses, and strict enforcement of application control policies to prevent exploitation of telecom stacks by threat actors.

Collaborative Threat Intelligence

Partner with cross-agency initiatives and industry stakeholders to proactively share threat intelligence on nation-state campaigns, botnet activity, and vulnerabilities across public-facing IoT systems.



Federal agencies must take decisive action to address these risks, proactively secure mobile and IoT/OT ecosystems, and ensure compliance with federal standards to safeguard critical infrastructure against increasingly sophisticated cyberthreats.

2026 Predictions

1. **Ai-driven exploits will continue to expand.** AI tools will accelerate the creation of hyper-targeted phishing campaigns. Smishing and vishing attacks will leverage AI models to mimic real people and trusted brands to compromise mobile devices. Enterprises will need AI-driven defenses to identify these highly advanced threats.

2. **Public and private 5G networks will be vulnerable without strong zero trust models.** Cellular IoT and mobile networks will grow but will require zero trust frameworks to protect these ecosystems at the core. Security must be embedded at the SIM or eSIM level, enabling precise, context-aware controls based on identity, location, behavior, or risk. For example, SIMs can be restricted to operate only within specific countries or regions, preventing unauthorized roaming or data exfiltration. Anomaly detection can flag or block suspicious activity such as attempts to access disallowed resources or connect from unexpected locations, ensuring consistent protection across the globe without operational overhead.

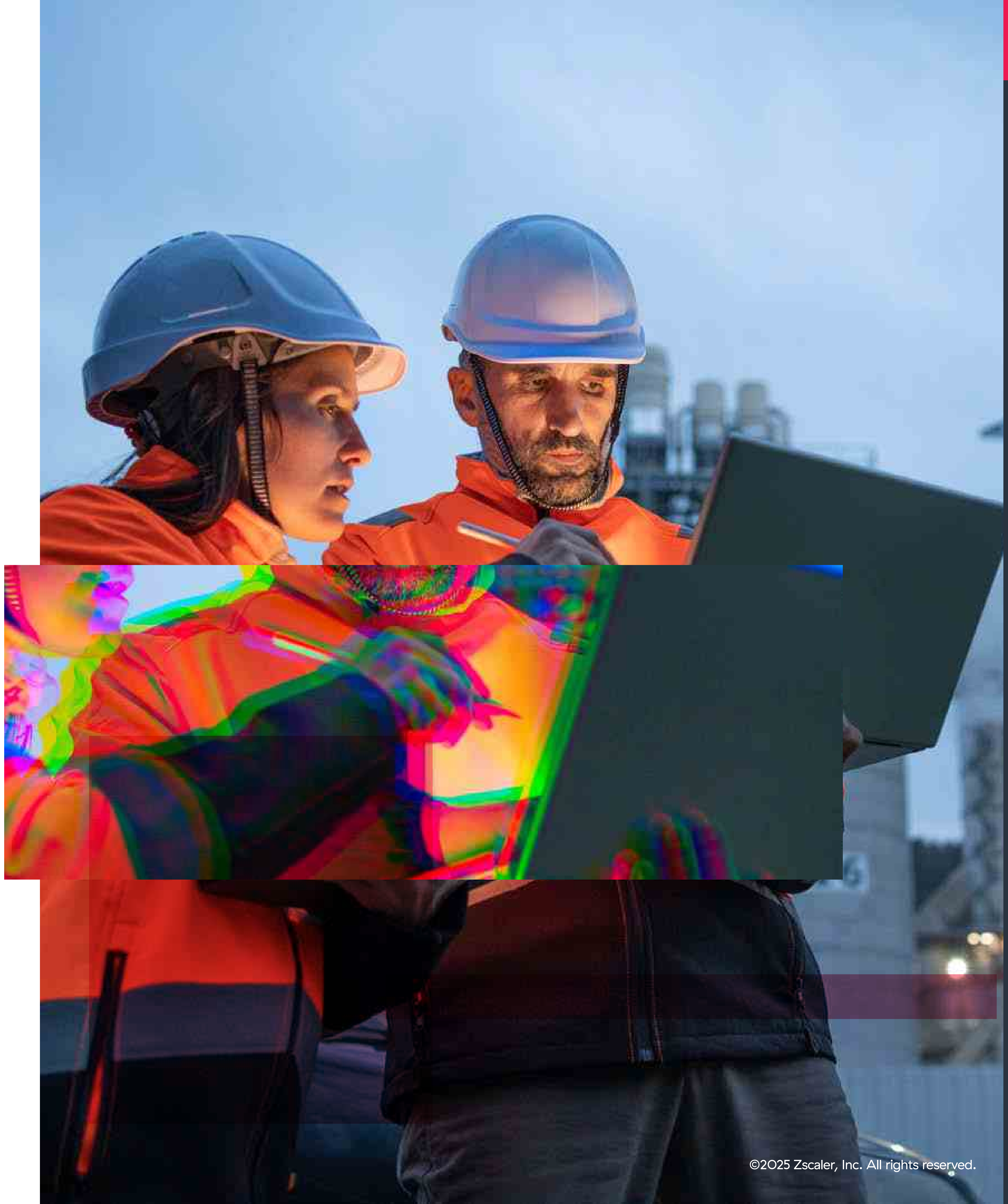
3. **Mobile applications will increasingly be supply chain attack vectors.** Attackers will increasingly compromise third-party mobile app development pipelines to inject malicious code into widely trusted apps. Continuous analysis of all app permissions and behavior will become a security standard.

4. **Sustained IoT and ot ransomware attacks targeting critical sectors.** Industries heavily reliant on IoT/OT environments (manufacturing, energy, healthcare) will remain high-priority targets for ransomware campaigns, with evolving tactics to exploit network interdependencies and disrupt critical services.

5. **Zero Trust Segmentation will be increasingly integrated into IoT/OT environments.** Enterprises will isolate IoT/OT devices into granular layers using zero trust frameworks. Each device (or group of devices) will have its own validation requirements, helping to block lateral movement when devices are compromised while ensuring continuous compliance.

6. **Consolidation of IoT/OT and mobile security systems.** Enterprises will increasingly consolidate IoT, OT, and mobile device security into unified platforms. These platforms will offer end-to-end zero trust enforcement, device microsegmentation, AI-based anomaly detection, and game-changing visibility across edge, cloud, and 5G networks.

7. **Expanded adoption of zero trust frameworks for routers and edge devices.** Organizations will increasingly deploy zero trust principles on public-facing devices, such as routers, to prevent botnet propagation and defend against constant attacks. Routers and gateways will be segmented into isolated zones of operation and authenticated before any communication with broader enterprise networks, using continuous behavioral analysis for validation.



IoT and Security
Best practices

PERFORM ENHANCED DISCOVERY, CLASSIFICATION, AND INVENTORY OF IOT AND OT DEVICES

Develop a unified strategy to achieve complete visibility into your IoT and OT ecosystem, including the discovery and inventory of all devices—managed, unmanaged, and "shadow" systems. Leverage AI-driven tools for dynamic classification across device types, operational environments, and risk levels. This ensures defenders can better assess vulnerabilities, prioritize remediation, and adapt security to an ever-expanding network of devices.

CONTINUOUSLY MONITOR AND CORRELATE NETWORK TRAFFIC

Enable advanced telemetry and real-time monitoring for all IoT and OT device communications. Collect detailed logs of user access, application events, and system activity to identify anomalies indicative of compromised systems or dwell time from advanced persistent threats (APTs). Utilize predictive analytics to correlate patterns and detect hidden threats like those associated with nation-state actor campaigns.

ENABLE ADVANCED MULTIFACTOR AUTHENTICATION (MFA)

Push beyond traditional MFA approaches by securing administrative credentials and enforcing phishing-resistant MFA, such as FIDO2 cryptographic authentication or biometric-based systems. These modern frameworks reduce the effectiveness of credential-stealing techniques, particularly under sophisticated attack methods frequently targeting IoT and OT environments

PRIORITIZE AUTOMATED PATCHING WITH AI INTEGRATION

IoT and OT devices remain disproportionately vulnerable to unpatched or outdated systems. Deploy automated update systems that respond dynamically to new threats, with vulnerability prioritization driven by AI analytics. Focus on fast patching for critical internet-connected systems to protect against the exploitation of zero day vulnerabilities, while limiting downtime for essential systems.

IMPLEMENT ADVANCED ZERO TRUST NETWORK SEGMENTATION

Refine zero trust principles across IoT and OT systems with highly granular device-to-application, user-to-application, and application-to-application segmentation. Enforce least-privileged access controls to prevent lateral movement, minimize data exposure, and isolate vulnerabilities. Emphasize event-driven segmentation strategies that dynamically zone devices and apps based on shifts in risk or operational demands.

SECURE PRIVILEGED REMOTE ACCESS TO OT SYSTEMS

As OT systems become increasingly internet-facing, move beyond traditional VPN-based access to avoid friction and exposure to exploitation. Deploy zero trust privileged access solutions, featuring outbound-only connectivity with fully isolated RDP and SSH sessions. Prioritize identity-centric access controls and vendor-specific tools to reduce risks from third-party access and ensure integrity in connected OT environments.

INSPECT AND ANALYZE ALL ENCRYPTED TRAFFIC

Threat actors frequently exploit encrypted channels to bypass security controls. Adopt advanced SSL/TLS traffic inspection tools to ensure all encrypted traffic—including IoT and OT device communication—is analyzed without compromising performance. Use AI-powered threat intelligence platforms to identify attack patterns within encrypted data streams.

ENHANCE SECURITY FOR CELLULAR IOT DEVICES

As cellular IoT adoption accelerates across industries like manufacturing, energy, logistics, and smart infrastructure, organizations must proactively secure these devices to prevent misuse and ensure operational continuity.

- **Gain network visibility:** Leverage platforms that provide end-to-end visibility into cellular IoT connections, enabling real-time understanding of device behavior, application usage, and traffic patterns.
- **Implement zero trust network access:** Enforce controls that broker access based on device and application requirements, ensuring cellular IoT devices are protected without expanding the attack surface.
- **Prevent device misuse:** Secure SIM cards and cellular endpoints to prevent unauthorized access to internal applications or abuse of unlimited data plans, which could lead to perimeter breaches or costly "bill shock."
- **Optimize device-control policies:** Deploy solutions that manage app permissions, block unwanted activity, and ensure secure communications for cellular-connected devices, especially in ruggedized or remote environments.
- **Protect cellular IoT traffic:** Apply encrypted traffic inspection and enforce outbound-only device connectivity, minimizing exposure while ensuring seamless communication across cellular networks.

Mobile Security
Best prectices

Enterprises must adapt their approach to securing hybrid work in a mobile-first world, where users can access any SaaS or private application, whether in the cloud or the data center, from any location. Given the continuing rise of threats like mobile malware and spyware, enterprises should adopt security best practices that include zero trust connectivity for the remote workforce—keeping users productive and the business secure.

ADOPT BEST-OF-BREED ENDPOINT SECURITY AND IDENTITY MANAGEMENT FROM INDEPENDENT PROVIDERS

Zero trust security begins with identity and endpoint security. Enterprises should seek to integrate best-of-breed identity management and endpoint security solutions that allow them to authenticate remote users and protect endpoints against malicious cyberthreats. Enterprises should not rely on any single cloud company or security provider—akin to putting all your eggs in one basket—but instead adopt a layered approach from multiple independent security organizations.

ENABLE ZERO TRUST ACCESS

Coupled with identity management and endpoint security, enterprises should adopt an industry-leading zero trust access solution. This solution should provide zero trust, adaptive access based on the real-time security and posture of user devices—harnessing identity intelligence, user risk factors, and device telemetry to make per-session access decisions. Moreover, this approach should leverage a zero trust architecture, enabling direct connectivity between endpoints and applications—never to the underlying network.

PROTECT ENDPOINT DATA

Enterprises should prevent sensitive enterprise data from leaking or being exfiltrated from user endpoints—which can include channels like printing, removable storage, or personal cloud storage. As such, defenders should adopt comprehensive data loss prevention (DLP) solutions for endpoints that alert and block sensitive data from leaving the enterprise.

ENFORCE CONSISTENT, ZERO TRUST SECURITY POLICIES

Given that users can access the internet, SaaS, and private applications from anywhere, enterprises should strive to enforce the same zero trust access policies, whether users are located at HQ, the branch, or accessing applications remotely.

Zero Trust Branch:
How Zscaler Secures Mobile, IoT, and OT

The Zscaler Zero Trust Branch delivers comprehensive security and operational efficiency for branch offices, remote sites, and distributed networks that rely heavily on mobile, IoT, cellular IoT, and OT technologies. Leveraging a cloud native, AI-driven Zero Trust architecture, Zscaler ensures that every user, device, and application—whether inside or outside the traditional network perimeter—remains protected through real-time verification and robust policy enforcement.

Zscaler OT/IoT Segmentation provides an agentless alternative to firewalls, NAC, and manual VLANs, allowing for complete device isolation without the need for agents, upgrades, or downtime. This solution ensures the safety and operational integrity of legacy machines and headless systems. Automated policies deliver simple, seamless security that integrates smoothly with production, avoiding any slowdowns.

NO ENDPOINT AGENTS

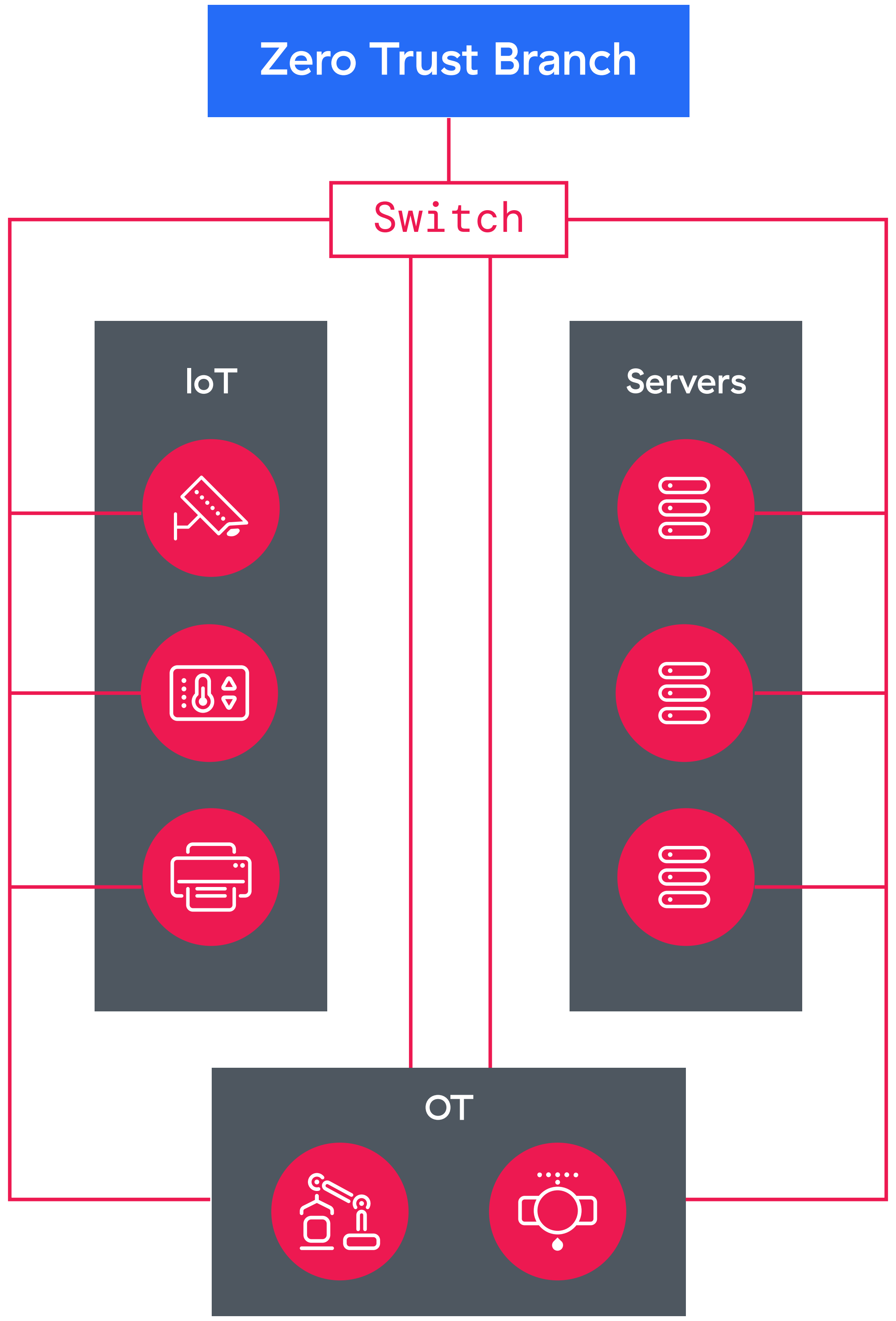
Fully segment legacy servers, headless machines, and IoT/IoMT devices that can't accept agents.

A UNIFIED SOLUTION

Seamlessly deploy integrated OT/IoT Segmentation, Zero Trust SD-WAN, and Privileged Remote Access (PRA).

MAXIMUM UPTIME

Deploy quickly and with no hardware upgrades or VLAN readdressing. Extend the life of legacy equipment.



Automated IoT / OT Segmentation
Segment of 'one' for every device

Zscaler Cellular: Securing Mobile and Cellular

Zscaler Cellular delivers secure, scalable, and efficient connectivity as a service for cellular-connected IoT and mobile devices. Powered by the Zscaler Zero Trust Exchange™ platform, it enforces granular policies, ensures centralized visibility, and eliminates attack surfaces for cellular traffic. Through seamless integration with your existing telecom infrastructure, it simplifies management while enabling global connectivity over any protocol.

KEY COMPONENTS

Zscaler SIM:

- A zero trust-based SIM card enabling secure connectivity for IoT devices across cellular networks (such as 4G/5G).
- Routes traffic through Zscaler Cellular Edge for inspection and application of security policies.

Zscaler Cellular Edge:

- Acts as the bridge between telecom networks and Zscaler Zero Trust Exchange.
- Inspects cellular traffic and enforces granular control for activities such as anomaly detection and telemetry monitoring.

FEATURES

Secure and Simplified Connectivity:

- Uniform protection without requiring client-side software or hardware installation.
- Eliminates lateral movement risks by enforcing zero trust principles.

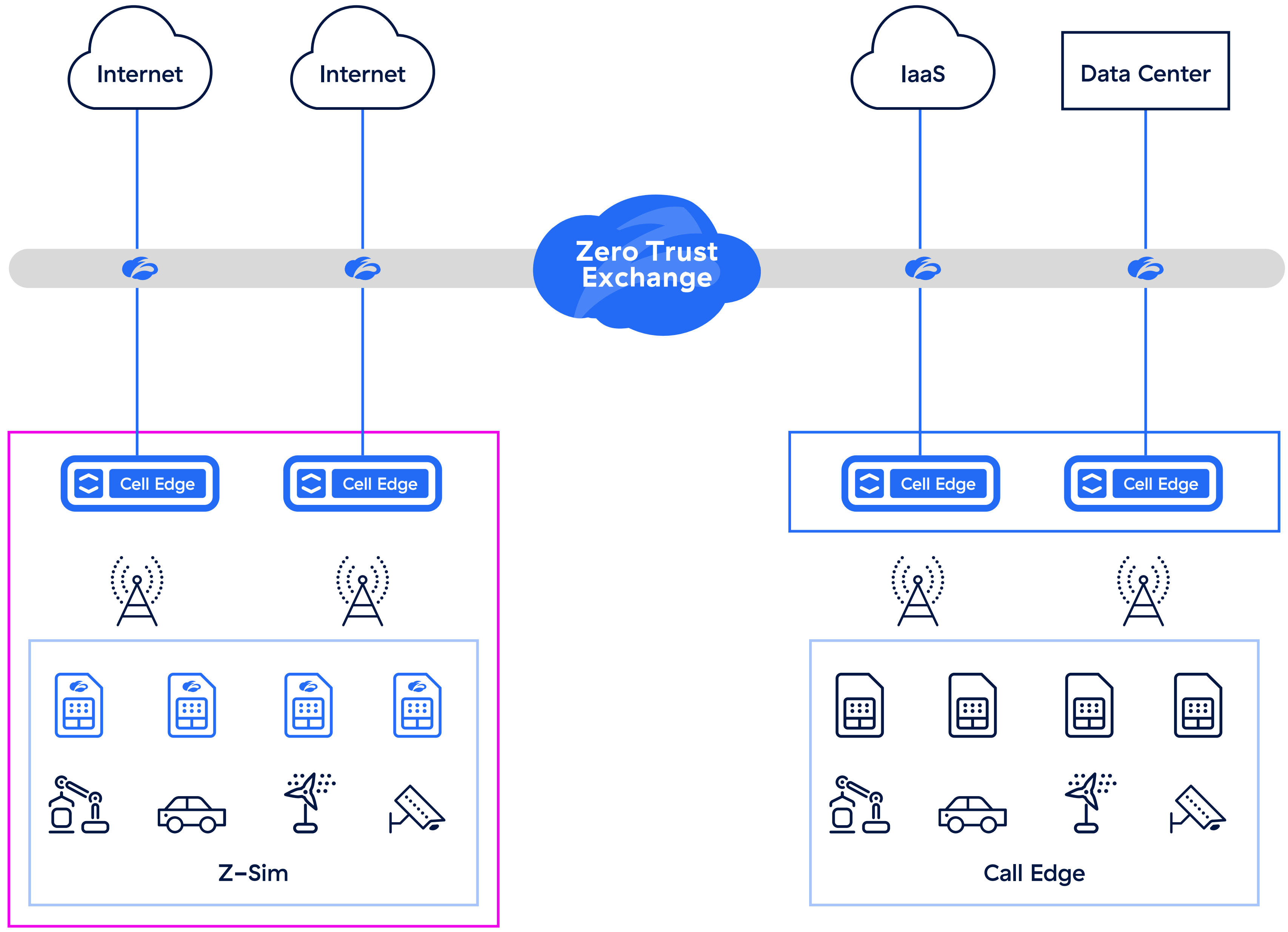
Comprehensive Traffic Visibility:

- Real-time logging and centralized dashboards provide actionable insights, including SIM activity and traffic anomalies.

Zero Attack Surface:

- By ensuring all traffic passes through ZTE, the architecture removes exposed infrastructure and limits the attack surface effectively.

Zscaler Cellular provides unified control over cellular traffic for superior, secure operations and scalable connectivity in any environment.



Report Methodology

MOBILE

The research methodology for this report includes analysis of mobile transactions and associated cyberthreats based on data collected from the Zscaler cloud between June 2024 and May 2025. The dataset comprises more than 20 million threat-related mobile transactions.

This report focuses on identifying patterns, trends, and emerging threats specifically within the Android ecosystem.

IOT/OT

The research methodology for this report includes analysis of device logs from a multitude of sources and industry verticals.

The report uses data derived from customer deployments that connect to the Zscaler global security cloud, which processes more than 500 trillion daily signals, blocks more than 9 billion threats and policy violations per day, and delivers more than 250,000 daily security updates to Zscaler customers.

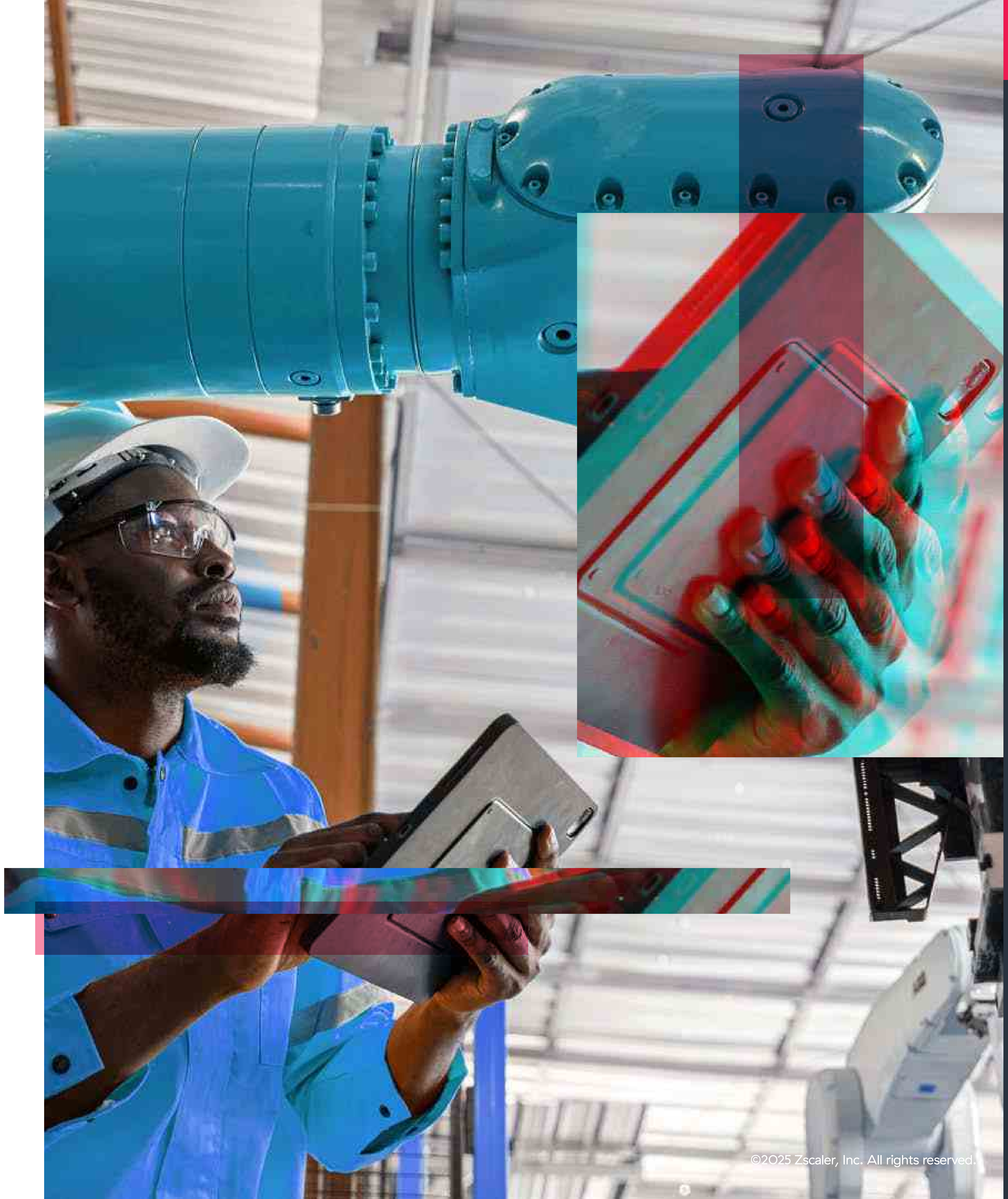
The team focused their research on understanding the distinct attributes and activity of IoT devices via device fingerprinting (DFP) and analyzing the IoT malware threat landscape.

Device fingerprinting data from March 2025 to May 2025 included:

- A complete inventory of devices, including device types and manufacturers
- The volume and source of IoT device transactions
- The industries and geographies contributing to IoT traffic

IoT malware threat data from June 2024 to May 2025 included:

- The most active malware families
- The industries and geographies most targeted by IoT attacks
- The top attacked devices



zscaler™ | Zero Trust Everywhere

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**