Zscaler ThreatLabz 2024 Mobile, IoT, & OT Threat Report

Table_of Contents

Executive Summary 3

Top Mobile Threats 4

Key Findings 4

Overview 5

ThreatLabz Research Highlights 6

Android and Windows RATs distributed via online meeting lures 6

Rise of banking malware in the Google Play Store 7

Mobile phishing attacks spike during holiday shopping season 8

Understanding the Copybara mobile malware threat 9

Mobile-focused phishing campaigns targeting Indian banks and postal service 10

QR code scams 11

Banking Malware 12

Banking malware surges despite decline in overall Android threats 12

Accessibility Service abuse remains a popular tactic 12

Banking malware is a trojan-dominated threat 13

Android malware transactions decline 14

Most active malware families based on transaction count 15

Unique blocked transactions 16

Top malware families in the Google Play Store 17

Most malware-infected Google Play Store apps pose as Tools 18

Spyware 19

Geographical Analysis 20

Industry and Sector Analysis 21

Rise in attacks on education and services sectors 22

Top IoT & OT Threats 23

Key Findings 23

Overview 24

IoT Device Categories 25

Routers see the bulk of IoT attacks 26

IoT Malware 27

The U.S. remains the top IoT target 28

Industry and Sector Analysis 29

Manufacturing maintains the widest array of IoT devices 30

Data collection terminals drive business — and the bulk of IoT device traffic 31

The Retail & Wholesale sector is an IoT traffic powerhouse 32

Geographical Analysis 33

IoT Vulnerabilities 34

Challenges in Securing OT Environments 35

Quantifying Security Risks in OT Environments: Legacy Systems, Unauthorized Connections, and High-risk Services 36

Research Highlights 38

2025 Predictions 45

IoT and OT Security Best Practices 47

Mobile Security Best Practices 48

How Zscaler Secures IoT and OT 49

Bringing Zero Trust Inside the Branch and Factory 50

How Zscaler Secures Mobile Access 52

Digital Transformation Requires Zero Trust Connectivity 52

Report Methodology 53

Mobile 53

IoT/OT 53

About ThreatLabz 53

About Zscaler 53

Executive_ Summary

The security domain of the CISO continues to expand. As the number of breaches and cyberattacks like ransomware continue to rise, coupled with US Securities and Exchange Commission (SEC) requirements to disclose material breaches at public organizations, CISOs and corporate boards have greater responsibility than ever over enterprise cybersecurity outcomes.

Among the fastest-moving frontiers in the enterprise cyber footprint are mobile, internet of things (IoT), and operational technology (OT) connectivity. Today, 96.5% of people access the internet with a mobile device, while 59% of internet traffic is generated by mobile devices.[1] Meanwhile, OT and cyber-physical systems, once air-gapped and isolated from the internet, have rapidly become integrated into enterprise networks, where threats can proliferate.

This area is one of the most challenging to protect as the threats that attack these devices, like mobile malware and botnets, are becoming more sophisticated. Mobile and bring your own device (BYOD) connectivity, on both trusted and untrusted devices, has blurred the boundaries between work and personal life, while agentless IoT devices and legacy OT systems present significant gaps for traditional security approaches. Among the largest challenges: each of these categories drives the expansion of a “shadow” attack surface that is invisible to security practitioners and unprotected from attacks.

The Zscaler ThreatLabz 2024 Mobile, IoT, & OT Threat Report offers an overview of this landscape from June 2023 through April 2024, and details the latest trends, targets, threats, and best-practice defense strategies.

ThreatLabz found that mobile threats are becoming more targeted and sophisticated—with 29% and 111% growth in mobile banking malware and mobile spyware attacks, respectively—even as the overall volume of mobile attacks has declined. This trend is epitomized by Android malware families like Vultur, Hydra, and Anatsa, which have successfully proliferated undetected on the Google Play Store. Meanwhile, blocked IoT malware transactions grew by 45% year-over-year as botnets continue to proliferate across IoT devices.

The findings of this report stress the need for organizations to better secure their mobile endpoints, IoT devices, and OT systems.

[1] Forbes, **Internet Usage Statistics In 2024**, March 1, 2024.

Top Mobile_Threats

Key Findings

Financially motivated attacks on the rise with 111% spyware growth.

With **29%** growth in banking malware attacks and a **111%** rise in spyware year-over-year (YoY), it's clear that threat actors are increasingly motivated by the profitability of attacks, either through direct monetary gain or the collection of personalized data and credentials.

MFA bypass and phishing pages are key to financial attacks and fraud.

Most financially motivated malware attacks are highly capable of bypassing multifactor authentication (MFA) and frequently leverage phishing vectors, such as fake login pages for different financial institutions, social media sites, and crypto wallets.

200+ fake applications discovered across the Google Play Store.

Zscaler ThreatLabz has identified more than 200 malicious applications on the Play Store, collectively accumulating nearly 8 million installs.

Anatsa preys on Android users across Europe and Asia.

Anatsa, a known Android banking malware that leverages PDF and QR code readers to distribute malicious code, has targeted banking applications from more than 650 financial institutions worldwide, expanding its reach into countries like Germany, Spain, Finland, South Korea, and Singapore.

Technology is among the most targeted sectors for mobile threats.

The technology (18%), education (18%), and manufacturing (14%) sectors experienced the most mobile malware attacks.

Attacks on education institutions grew by 136%.

The high volumes of personal data education institutions retain have made them attractive targets for cyberattacks, while their large open networks, high diversity of users and devices, and lack of security policies for non-employees make them difficult to defend.

Nearly half of mobile attacks are trojans.

More than 46% of unique blocked transactions are coming from Android trojans.

India is the top target.

For the first time, India saw the largest proportion (28%) of mobile attacks, followed by the United States (27%) and Canada (27%).

Overview_

The mobile threat landscape is more expansive and dynamic than ever as we increasingly rely on mobile devices for work and everyday life. Today, 96.5% of people access the internet with a mobile device, and 59% of internet traffic is generated by mobile devices. In addition, Android is the leading mobile operating system, dominating 70% of the market.[2,3]

This immense volume highlights the fact that, for many users, mobile platforms have become the primary way to engage in a wide range of activities in both the home and the workplace.

At the enterprise level, mobile security has become vital. Organizations must not only secure fleets of managed devices, but contend with the widespread adoption of BYOD culture across various sectors. As these technologies continue to reshape the way we work, securing mobile devices has become even more crucial to protecting sensitive data and networks.

[2] Forbes, **Internet Usage Statistics In 2024,** March 1, 2024.
[3] Similarweb, **Mobile vs. Desktop vs. Tablet Traffic Market Share,** August 2024.

ThreatLabz Research_Highlights

In 2023 and 2024, ThreatLabz researchers utilized Zscaler's mobile telemetry dataset to track malicious activity, identify new mobile malware, and provide actionable intelligence to the security community. Here are significant discoveries made by our team during this period, including high-profile Android malware campaigns.

Android and Windows RATs distributed via online meeting lures

A technical analysis by ThreatLabz determined that a threat actor has been distributing multiple malware families through fake Skype, Zoom, and Google Meet websites. These campaigns involve the distribution of remote access trojans (RATs), including SpyNote RAT for Android platforms and NjRAT and DCRat for Windows systems. When a user visits one of the fake sites, clicking on the Android button initiates the download of a malicious APK file, while clicking the Windows button triggers the download of a BAT file. Once executed, the BAT file performs additional actions, ultimately leading to the download of a RAT payload.

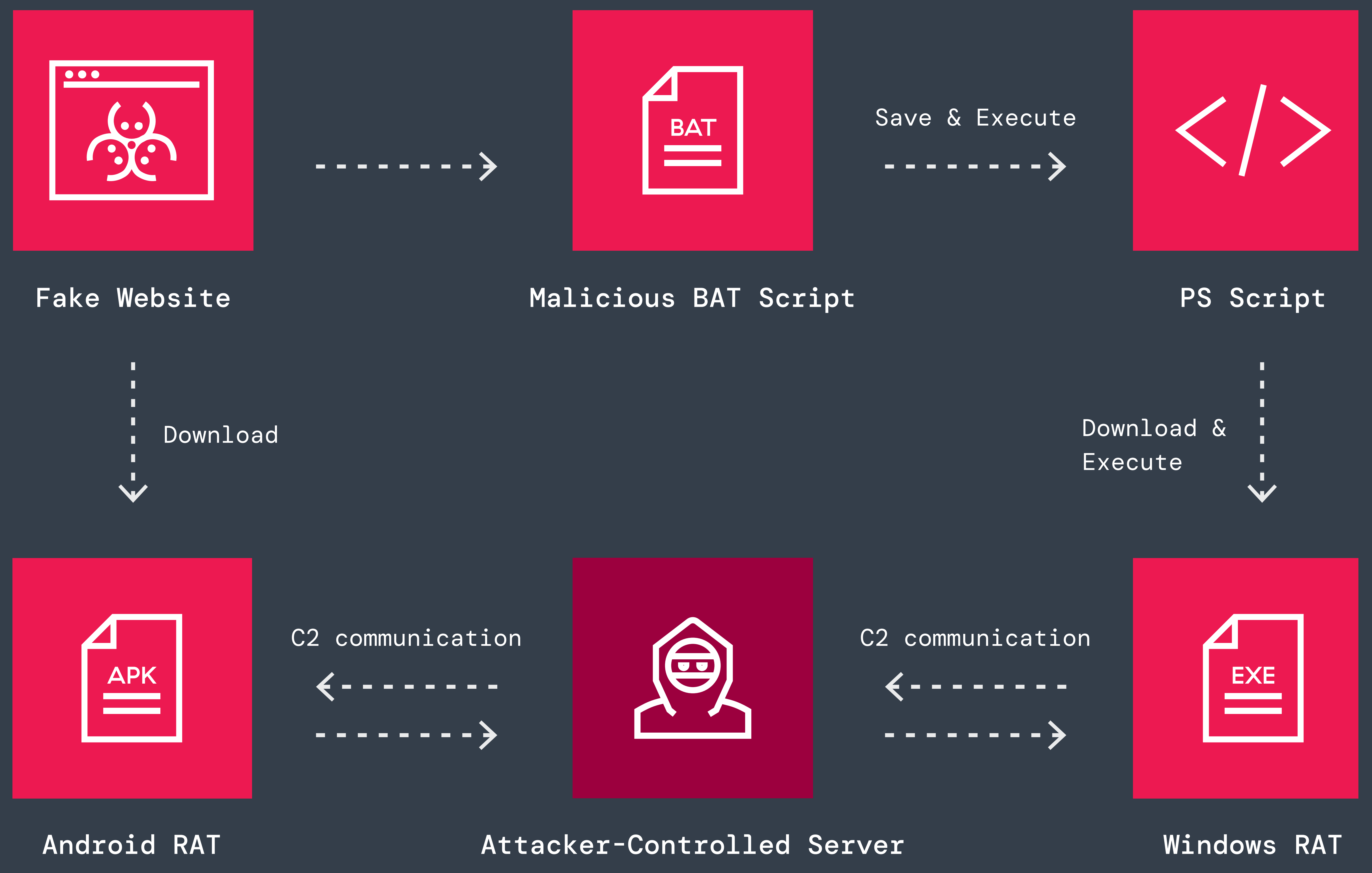


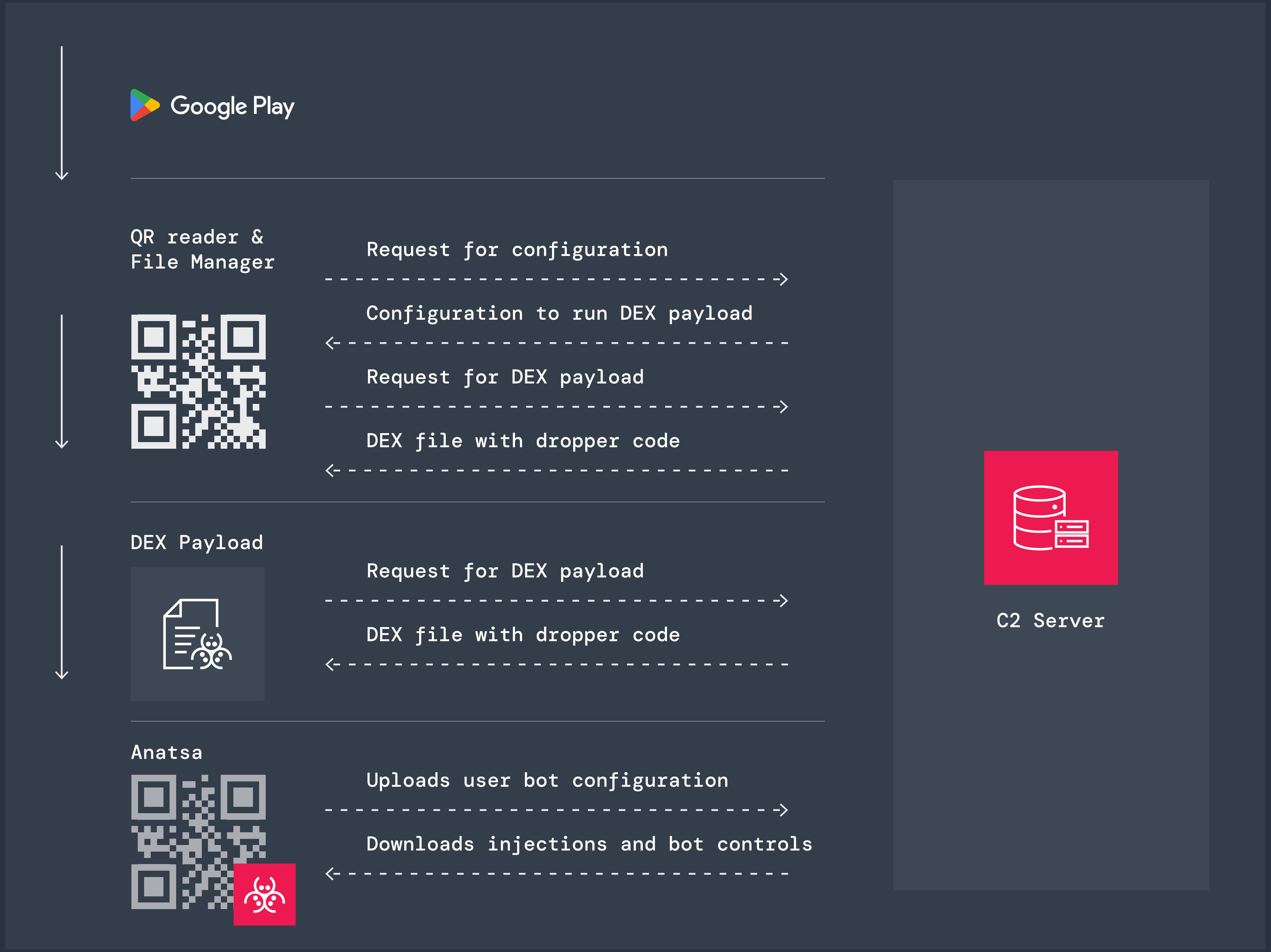
Figure 1: Distribution of Android and Windows RATs

Rise of banking malware in the Google Play Store

ThreatLabz has discovered that threat actors are leveraging decoy applications, such as PDF readers and QR code readers that act as loaders, to deploy the Anatsa (a.k.a. TeaBot) Android malware through the Google Play Store. Many malicious Android applications in the Play Store are disguised as tools such as file managers, editors, or translators.

Anatsa's second stage payload is disguised as a legitimate application update, tricking victims into believing the malware is genuine. The threat actors using Anatsa employ various techniques to evade detection, including checking for virtual environments and emulators as well as purposely corrupting the APK's ZIP headers to hinder static analysis of the malware.

The diagram demonstrates the distribution and execution of Anatsa on the victim's mobile device throughout the campaign:



Google Play
QR reader & File Manager
Request for configuration
Configuration to run DEX payload
Request for DEX payload
DEX file with dropper code
DEX Payload
Request for DEX payload
DEX file with dropper code
Anatsa
Uploads user bot configuration
Downloads injections and bot controls
C2 Server

Figure 2: Distribution and execution of Anatsa on victims' devices

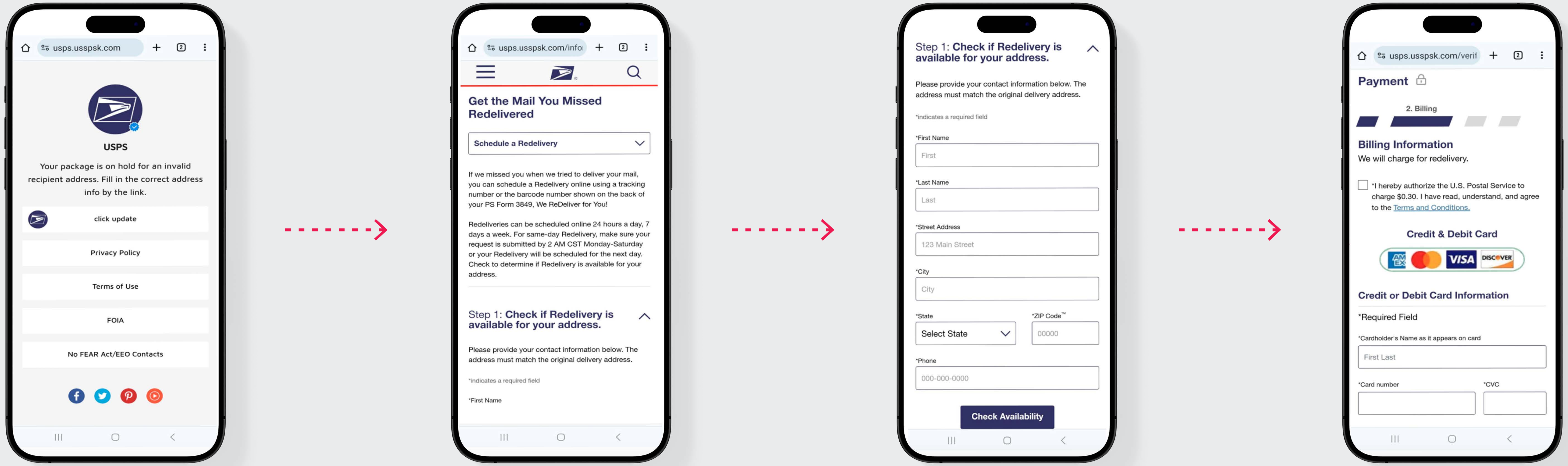
Mobile phishing attacks spike during holiday shopping season

ThreatLabz keeps a close watch on the growing trend of threat actors using popular brands to launch phishing campaigns that target mobile users during holiday shopping seasons, as detailed in this **blog post.**

One recent phishing campaign exploited the United States Postal Service (USPS) brand to deceive individuals into paying for fictitious missing packages. This campaign was specifically designed to target mobile devices, with the malicious USPS page often inaccessible on other devices. When accessing on non-mobile devices, users were redirected to the legitimate USPS website, further obscuring the scam's intent.

On mobile, users were presented with a seemingly legitimate USPS page featuring a "click update" button. This button led to a second fraudulent page that prompted users to enter their address details. After entering this information, users were taken to a payment page and prompted to provide sensitive payment details. Unknown to the victims, any information entered, including payment methods and personally identifiable information (PII), was immediately transmitted to a domain controlled by attackers.

Figure 3: Fraudulent USPS webpages



Your package is on hold for an invalid recipient address. Fill in the correct address info by the link.

Get the Mail You Missed Redelivered

If we missed you when we tried to deliver your mail, you can schedule a Redelivery online using a tracking number or the barcode number shown on the back of your PS Form 3849, We ReDeliver for You!

Redeliveries can be scheduled online 24 hours a day, 7 days a week. For same-day Redelivery, make sure your request is submitted by 2 AM CST Monday-Saturday or your Redelivery will be scheduled for the next day. Check to determine if Redelivery is available for your address.

Step 1: **Check if Redelivery is available for your address.**

Please provide your contact information below. The address must match the original delivery address.

*indicates a required field

*First Name: First

*Last Name: Last

*Street Address: 123 Main Street

*City: City

*State: Select State

*ZIP Code™: 00000

*Phone: 000-000-0000

Billing Information

We will charge for redelivery.

□ *I hereby authorize the U.S. Postal Service to charge $0.30. I have read, understand, and agree to the Terms and Conditions.

Credit or Debit Card Information

*Required Field

*Cardholder's Name as it appears on card: First Last

*Card number

*CVC

Understanding the Copybara mobile malware threat

ThreatLabz published a technical analysis of a new variant of the Android malware Copybara, active since November 2023. This malware spread through voice phishing (vishing) attacks, where victims receive instructions to install the malware on their Android devices.

Once installed, Copybara leverages the Accessibility Service feature to gain extensive control over the device. If the user does not grant this permission, the malware repeatedly prompts the user to enable it. Once granted, Copybara prevents the user from accessing certain settings, making it difficult to uninstall the app.

The infection chain begins with the malware displaying a fake screen requesting the user to enable Accessibility Service. After the permission is granted, Copybara connects to its C2 server using the MQTT protocol. It then downloads phishing pages that mimic well-known financial institutions and cryptocurrency exchanges. These pages are designed to deceive users into entering sensitive information, which is then sent to the attackers.

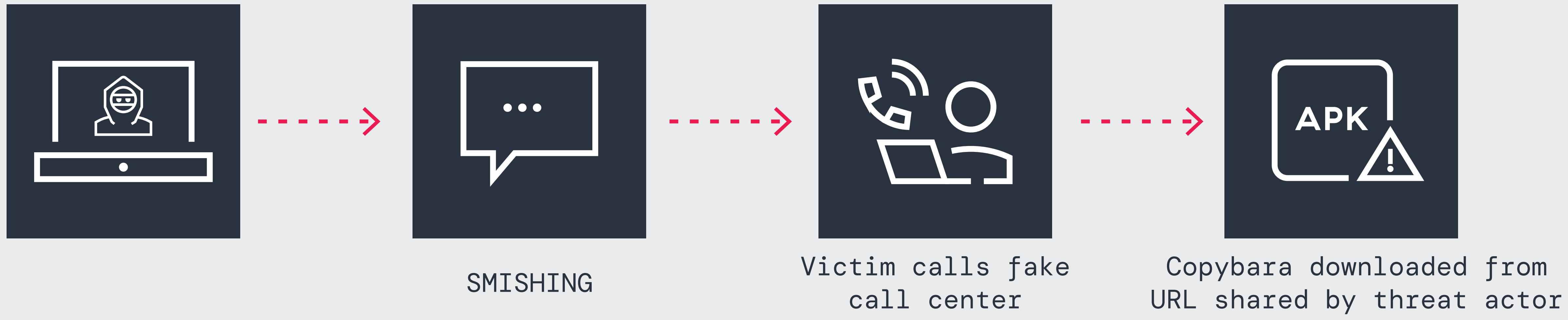
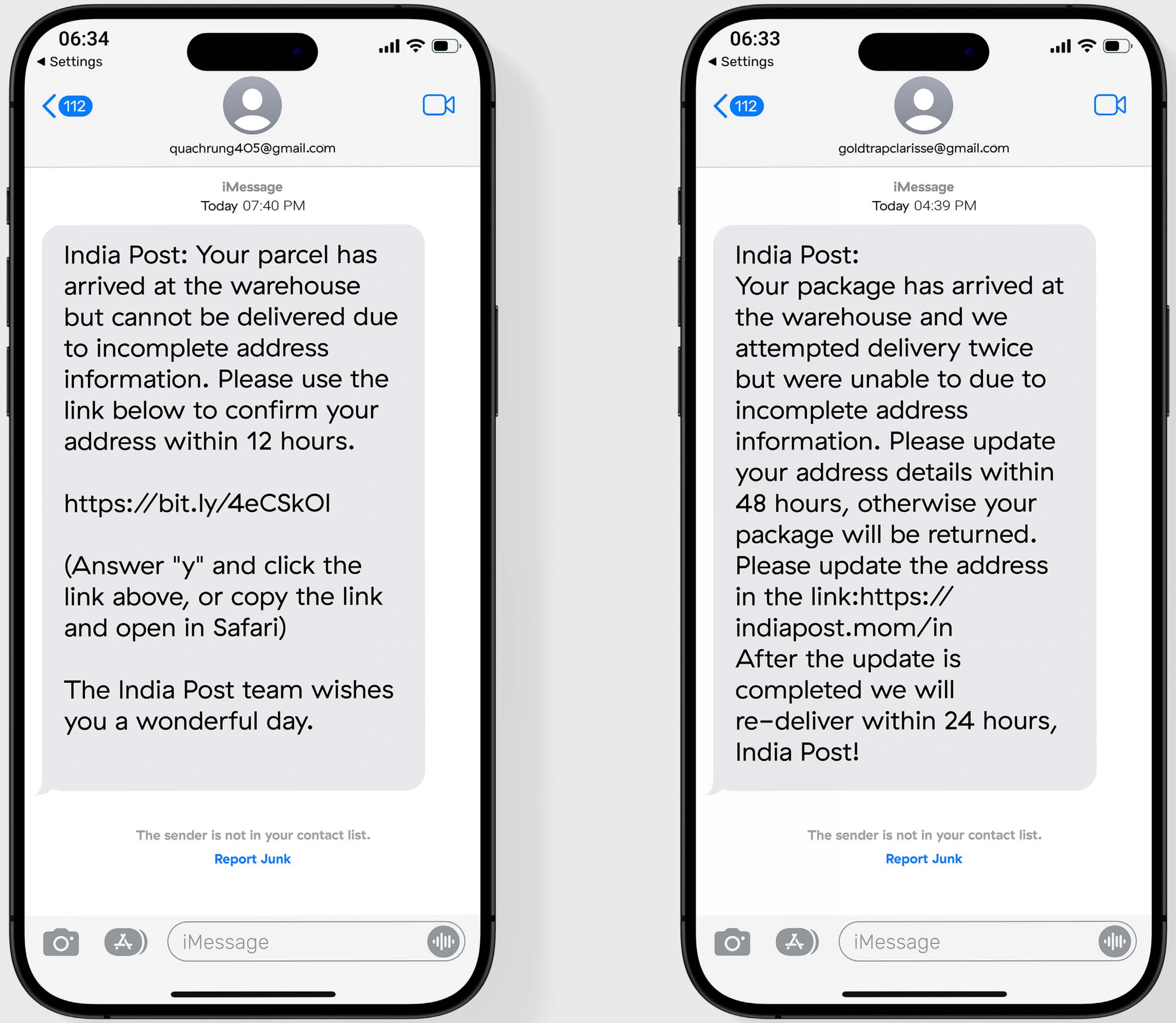

SMISHING
Victim calls fake call center
APK
Copybara downloaded from URL shared by threat actor

Figure 4: Copybara attack chain used to infect a mobile device



quachrung405@gmail.com

Today 07:40 PM

India Post: Your parcel has arrived at the warehouse but cannot be delivered due to incomplete address information. Please use the link below to confirm your address within 12 hours.

https://bit.ly/4eCSkOI

(Answer "y" and click the link above, or copy the link and open in Safari)

The India Post team wishes you a wonderful day.

goldtrapclarisse@gmail.com

Today 04:39 PM

India Post:
Your package has arrived at the warehouse and we attempted delivery twice but were unable to due to incomplete address information. Please update your address details within 48 hours, otherwise your package will be returned. Please update the address in the link:https://indiapost.mom/in
After the update is completed we will re-deliver within 24 hours, India Post!

Figure 5: SMS texts targeting India Post customers

Mobile-focused phishing campaigns targeting Indian banks and postal service

ThreatLabz researchers have detected a rise in phishing campaigns targeting mobile users of major Indian banks, including HDFC, ICICI, and Axis banks. These sophisticated attacks use fake banking sites designed to closely resemble the legitimate ones, tricking mobile users into divulging sensitive bank information. Previously, similar tactics were used to spread Android-based phishing malware through fake card update sites, leading to widespread financial fraud.

Attackers have also turned their attention to the Indian postal service. Using SMS messages, they directed mobile users to phishing sites that prompt them to input credit card details. These fraudulent schemes often exploit common scenarios like missing packages and incomplete delivery addresses, capitalizing on the urgency created by such messages.

QR code scams

In QR scams, threat actors trick victims into using their mobile devices to scan QR codes that lead to malicious links. These scams employ various delivery methods, including malicious redirection, email attachments (such as PDF or DOC files), and other forms of digital communication. Threat actors' most common method is to email a PDF containing a QR code image, which then redirects mobile users to a phishing page.

Unusual URLs

Identifying a QR code scam necessitates examining the associated URL. Legitimate URLs are typically error-free, without misspellings or unusual phrases in their domain name or URL path. Figure 6 shows an unusual pairing, with "gard-ner" next to the usually legitimate "Toyota".

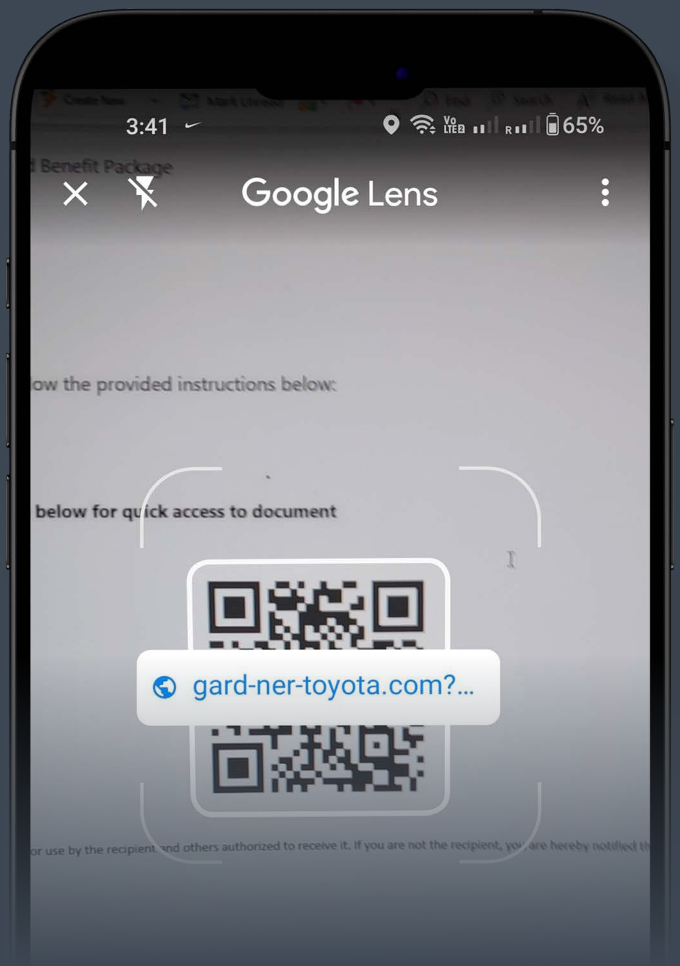
Fake CAPTCHA process

Scam websites that employ QR codes as a CAPTCHA, such as in figure 7, present a deceptive twist to the typical CAPTCHA verification process. Instead of the usual image- or text-based challenge, these sites prompt users to scan a QR code with their mobile device. Then, scammers redirect users to fraudulent websites or extract sensitive information.

Fake security updates

Phishing emails incorporating QR codes, particularly when disguised as security updates (as seen in figure 8), introduce a new level of deception to exploit unsuspecting recipients. These emails often appear to come from reputable sources, such as well-known companies or service providers, claiming to offer important security updates or account verification.

Figure 6: An example of a malicious URL associated with a QR code

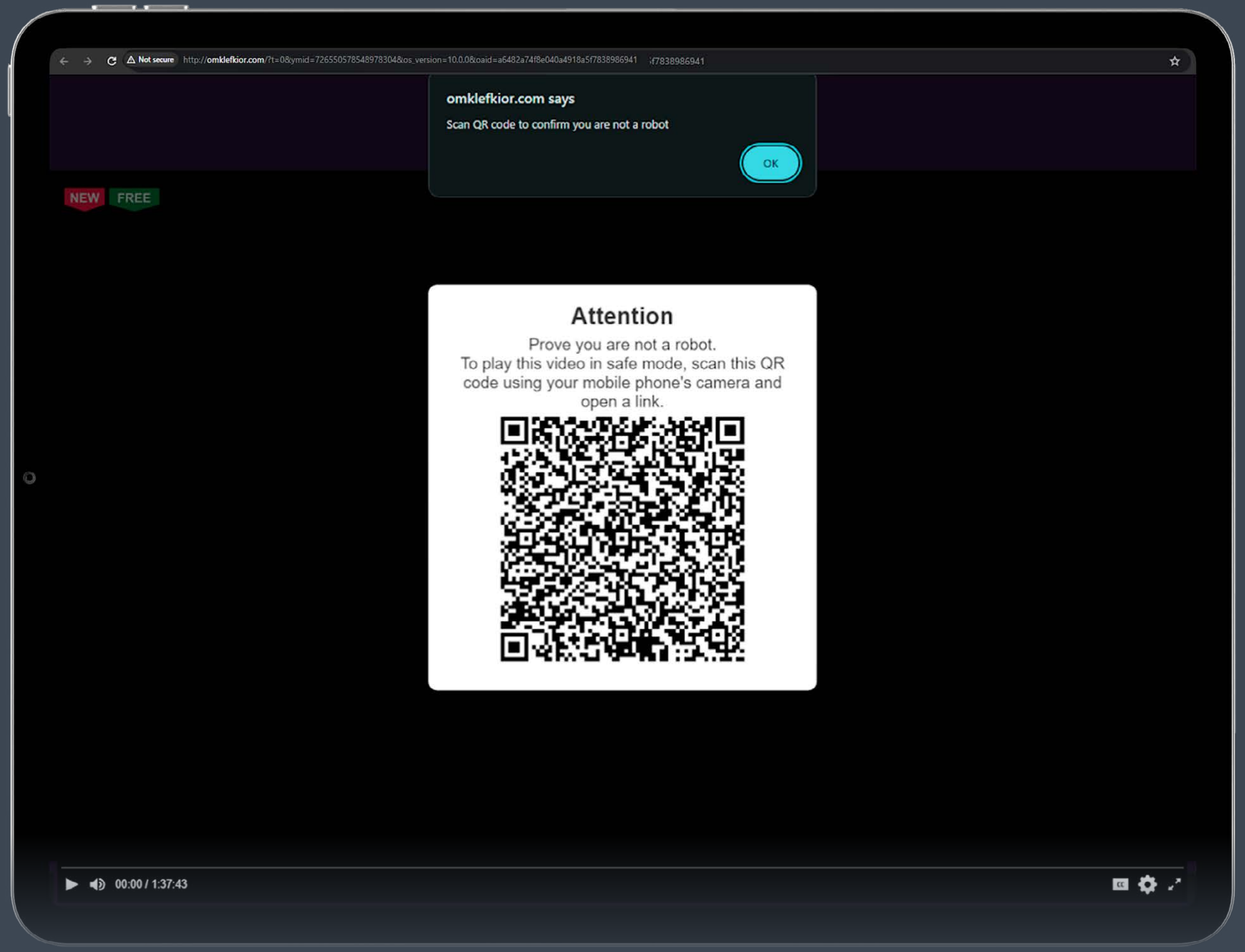


ow the provided instructions below:

below for qu ick access to document

gard-ner-toyota.com?...

Figure 7: A scam website using a QR code as a CAPTCHA verification methodas a CAPTCHA verification method



http://omklefkior.com/?t=0&ymid=7265505785489783048os_version=10.0.0&oaid=a6482a74f8e040a4918a5f7838986941

omklefkior.com says

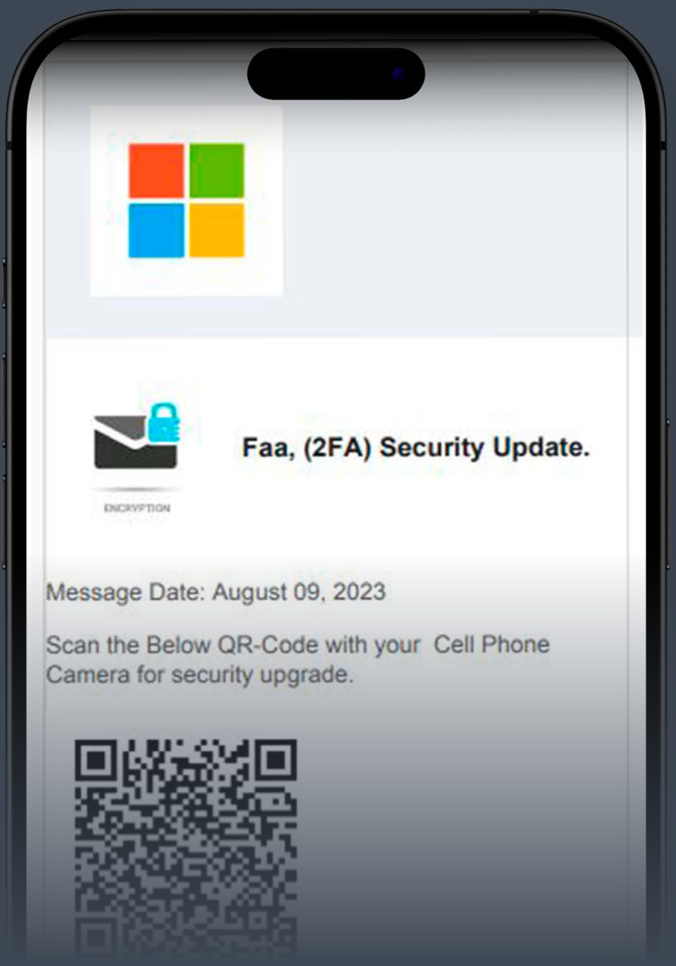
Scan QR code to confirm you are not a robot

OK

Attention

Prove you are not a robot.
To play this video in safe mode, scan this QR code using your mobile phone's camera and open a link.

Figure 8: A phishing email using a QR code to trick users into a fraudulent security update



Faa, (2FA) Security Update.

Message Date: August 09, 2023

Scan the Below QR-Code with your Cell Phone Camera for security upgrade.

Banking_ Malware

Banking malware surges despite decline in overall Android threats

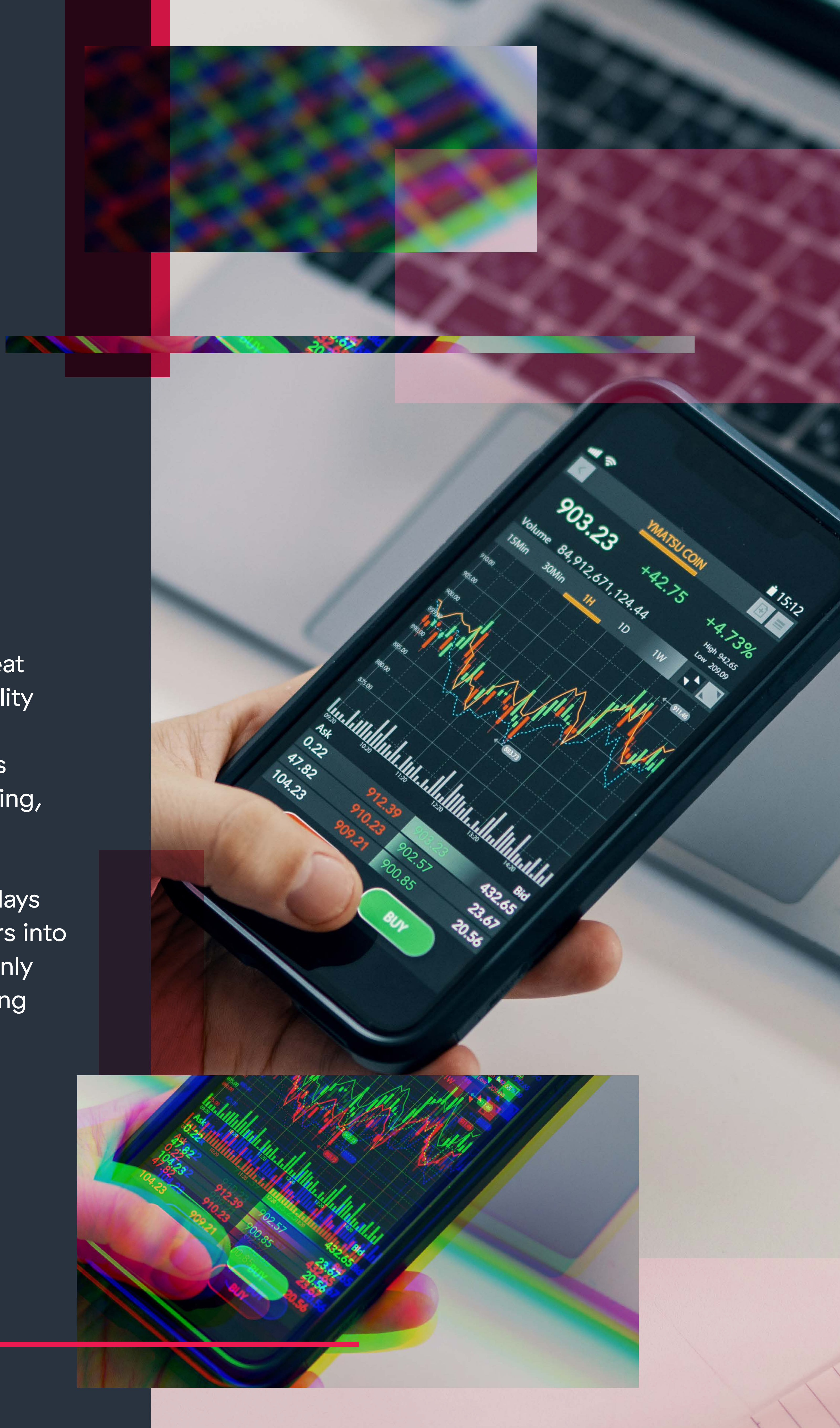
While Android threats have generally decreased, the prevalence of banking mobile malware has surged significantly. ThreatLabz analysis revealed 3.6 million blocks associated with banking malware, encompassing both payload deliveries and botnet transactions. This represents a 29% increase over the previous year.

Despite the overall downward trend in Android threats, banking malware has become more prominent, now constituting 20% of the total Android threat landscape.

Accessibility Service abuse remains a popular tactic

Accessibility Service abuse continues to be a go-to strategy for threat actors aiming to gain control over infected devices. While Accessibility Services are intended to aid users with disabilities, when misused, they can grant attackers granular control over the device. This allows them to monitor user interface events, enabling actions like keylogging, unauthorized permissions escalation, and overlay attacks.

In these overlay attacks, the malware monitors active apps and displays convincing phishing pages over legitimate app screens, tricking users into entering sensitive information like login credentials. This tactic not only compromises user security but also serves as a key tool for exfiltrating sensitive data, making it a critical threat in mobile banking.



Banking malware is a trojan-dominated threat

Banking malware is predominantly made up of trojans, with these malicious programs playing a central role in the threat landscape. An analysis of unique payloads revealed that 43% of all payloads were delivered by various Android trojans, making them the largest contributor to the distribution of malicious software in this banking malware.

Potentially unwanted applications (PUAs) followed, accounting for approximately 35% of the payloads, while adware made up about 11% of the total.

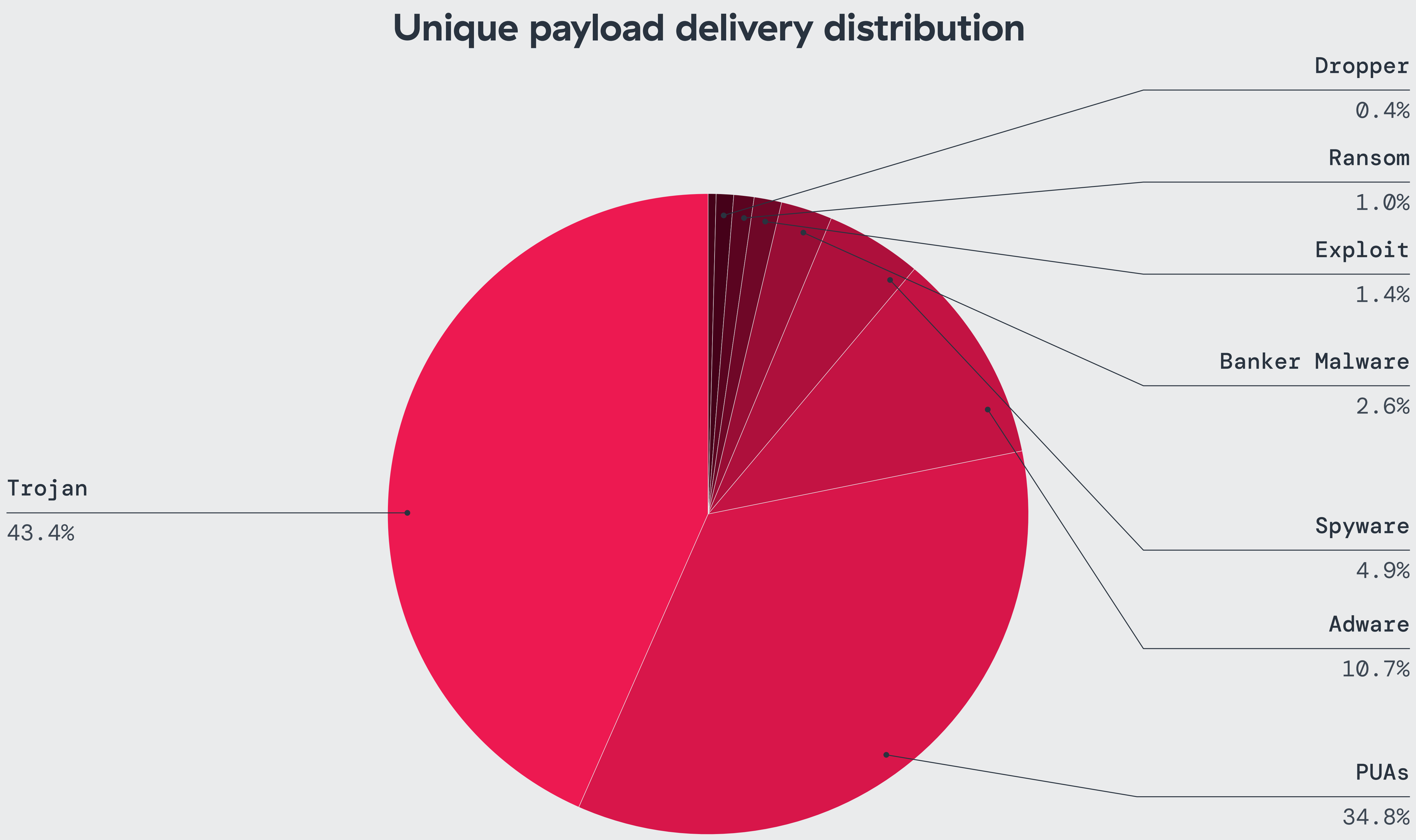


Figure 9: Distribution of unique payloads across different categories within banking malware

Android malware transactions decline

Android malware transactions have seen an overall decline. In 2023 and 2024, ThreatLabz recorded an average of 1.7 million Android malware blocks per month, culminating in a substantial 20 million blocks throughout the year.

Figure 10 illustrates a clear downward trend in Android malware blocks from July 2023 through May 2024. The data shows a significant reduction in blocked transactions over this period, with monthly blocks in May 2024 falling to barely one-third of the volume observed in July 2023.

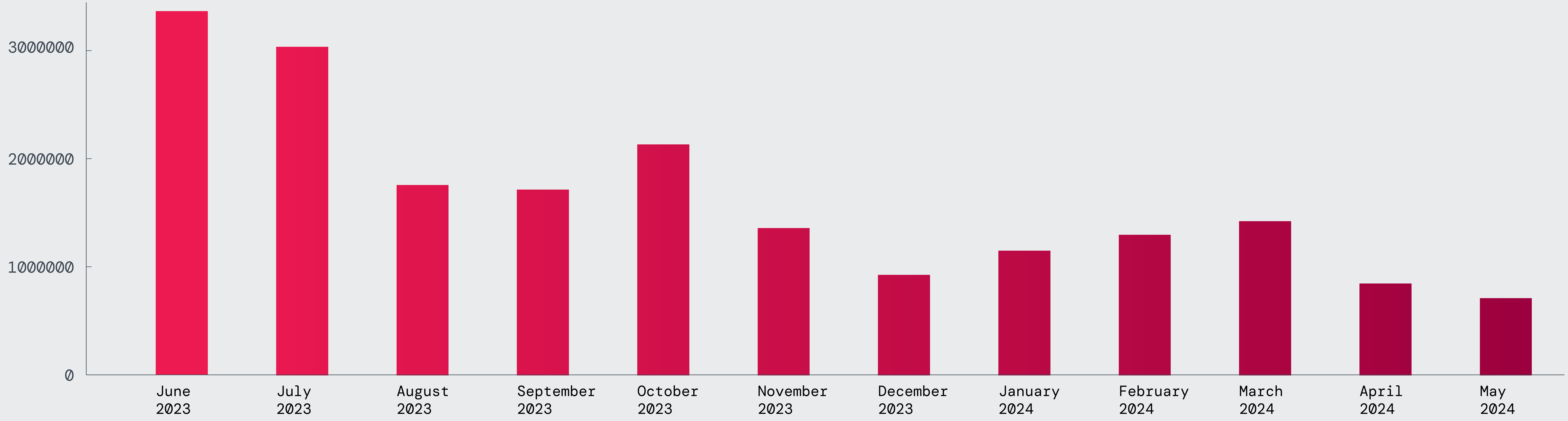


Figure 10: Downward trend in Android malware blocks month over month, July 2023-May 2024

Most active malware families based on transaction count

The following banking malware families are the most active:

1. Vultur

Vultur, discovered in March 2021, is primarily distributed through the Google Play Store, and records keystrokes and captures banking information entered into the victim’s device.

2. Hydra

Hydra, discovered in 2019, is distributed through phishing messages, websites, and malicious Google Play Store apps. Hydra steals banking credentials by obtaining powerful permissions from the user and hijacking their credentials when the user tries to log in to an app.

3. Ermac

Ermac, discovered in August 2021, is typically delivered through fake websites. Derived from Cerberus malware, Ermac steals the following from devices: lists of installed applications, SMS messages, accounts, and seed phrases for cryptocurrency wallets.

4. Anatsa (a.k.a. TeaBot)

Anatsa (a.k.a. TeaBot) emerged in early 2021. Anatsa steals the credentials and SMS messages of its victims. In recent samples, Anatsa is distributed through the Google Play Store in “dropper apps.”

5. Coper (a.k.a. Octo)

Coper (a.k.a. Octo) is a well-known trojan that targets banking apps in Europe, Australia, and South America. Coper is disguised as a legitimate app in the Google Play Store for distribution.

6. Nexus

Nexus targets banking apps and cryptocurrency services and is capable of account takeover (ATO) attacks. The malware is distributed through phishing pages that masquerade as legitimate websites.

Unique blocked transactions

Unique blocked transactions focus on the distinct instances of malware, counting each malware type only once, regardless of how often it has been blocked. This metric is used to understand the distribution of different malware types across the blocked transactions, helping normalize the data and provide insight into the variety of malware threats rather than the frequency. It's very useful for identifying the relative prevalence of different types of malware.

Trojans hold a significan a significant share, accounting for 46% of unique blocked transactions. This reaffirms that trojans dominate in the Android malware ecosystem, as they were the most common type of distinct threat, even though they might have been blocked multiple times.

Mobile adware was another major contributor, representing 24% of unique blocked transactions, while PUAs accounted for 21%.

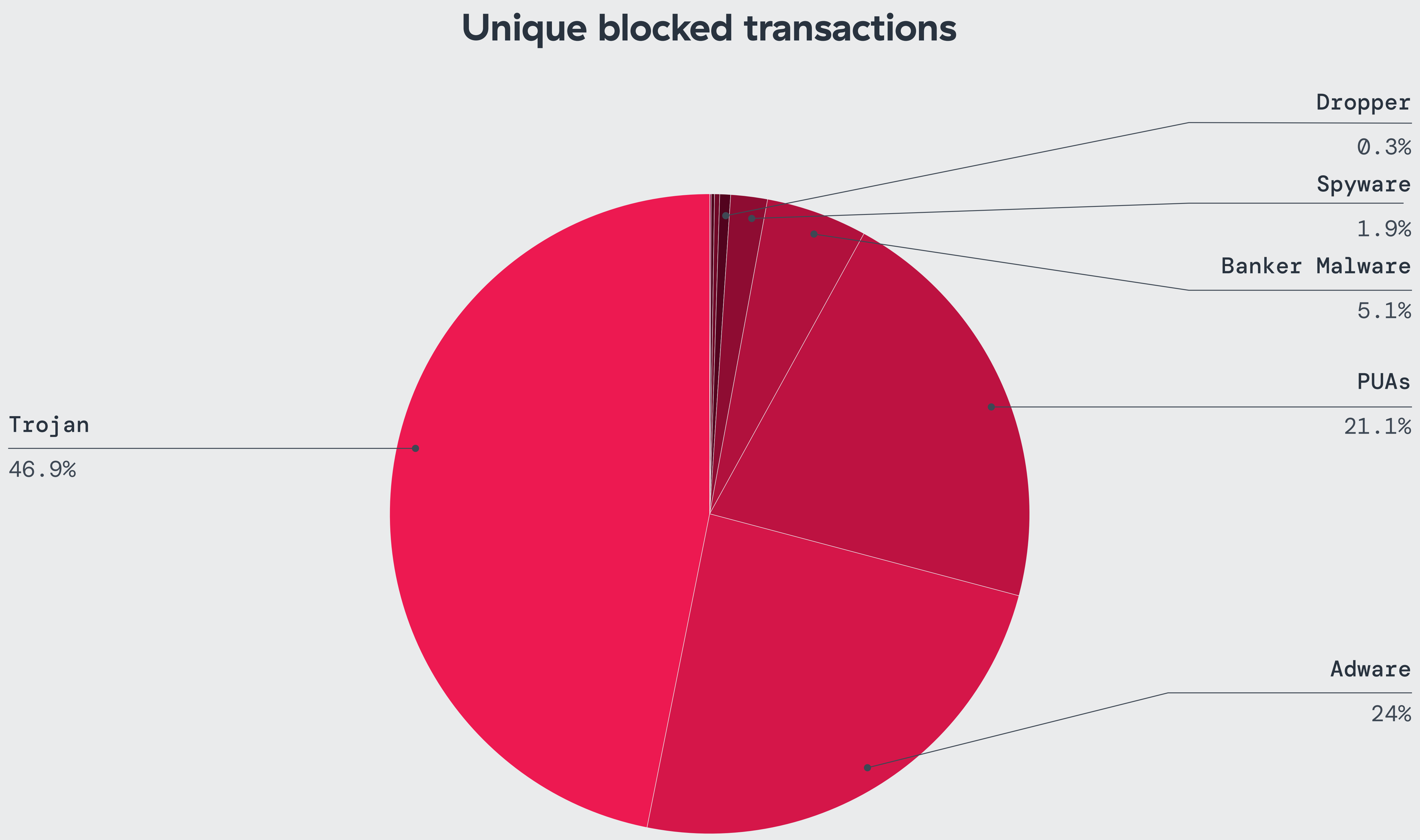


Figure 11: Unique distribution of blocked Android transactions across all malware types

Top malware families in the Google Play Store

ThreatLabz continuously monitors the Google Play Store to identify and analyze malicious apps. Over the past year, we detected more than 200 malicious apps uploaded to the platform, which collectively garnered nearly 8 million installations.

Joker emerged as the most prevalent malware family, accounting for 38% of the malicious apps identified. Joker is notorious for Wireless Application protocol (WAP) fraud, where it silently subscribes users to premium services without their consent, leading to unexpected charges.

Adware was the second most common malware type, making up 35% of observed threats.

The third most prominent malware family was Facestealer, responsible for 14% of the detected malicious apps. Facestealer specializes in stealing Facebook credentials, putting users' social media accounts—and potentially their personal and business data—at risk.

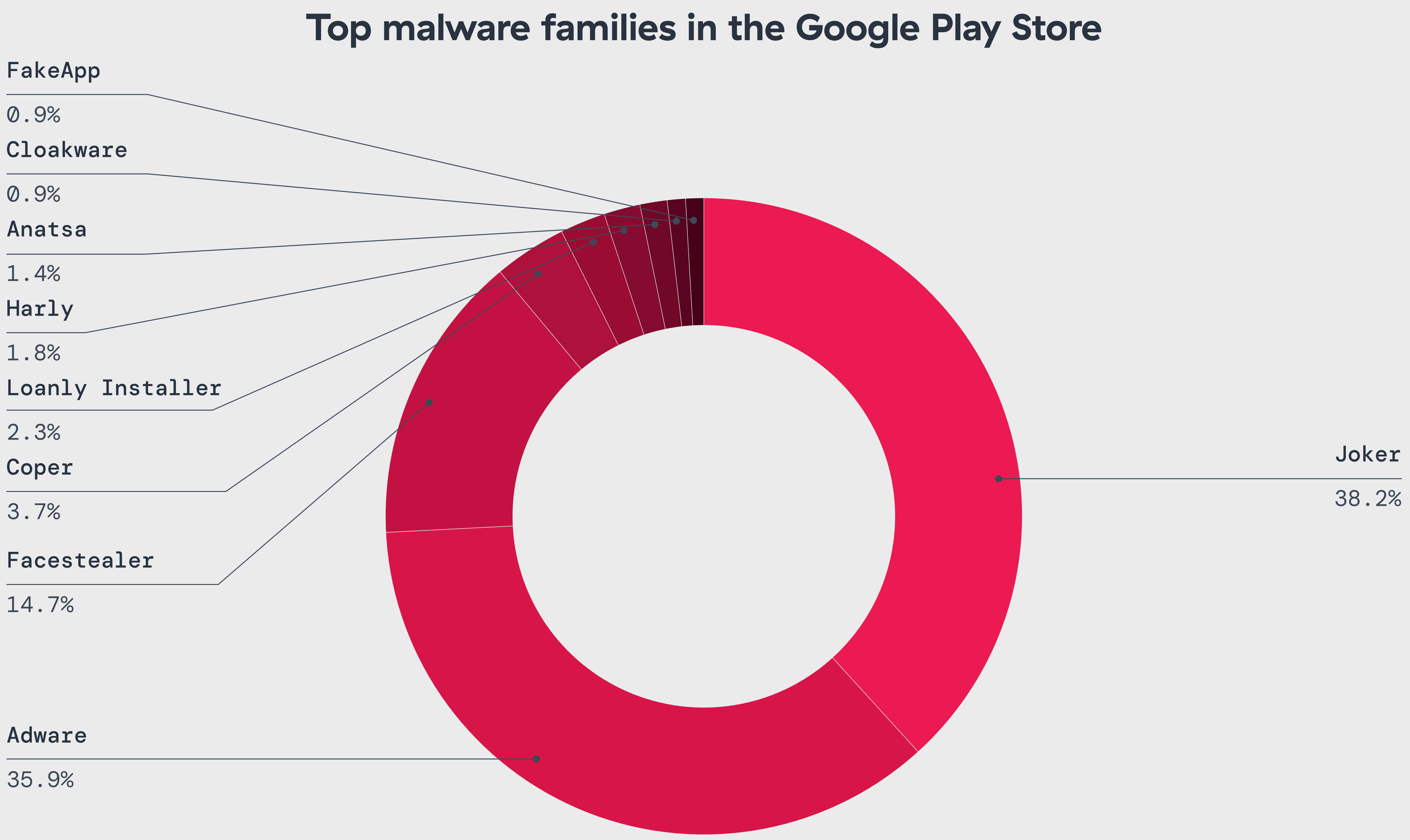


Figure 12: Most common malware families in the Google Play Store

Most malware-infected Google Play Store apps pose as Tools

ThreatLabz analysis reveals that the Tools category is the most abused by threat actors on the Play Store, accounting for nearly 48% of malware–infected apps.

Personalization and photography apps also see significant abuse, making up 15% and 11%, respectively.

Most abused app categories in the Google Play Store

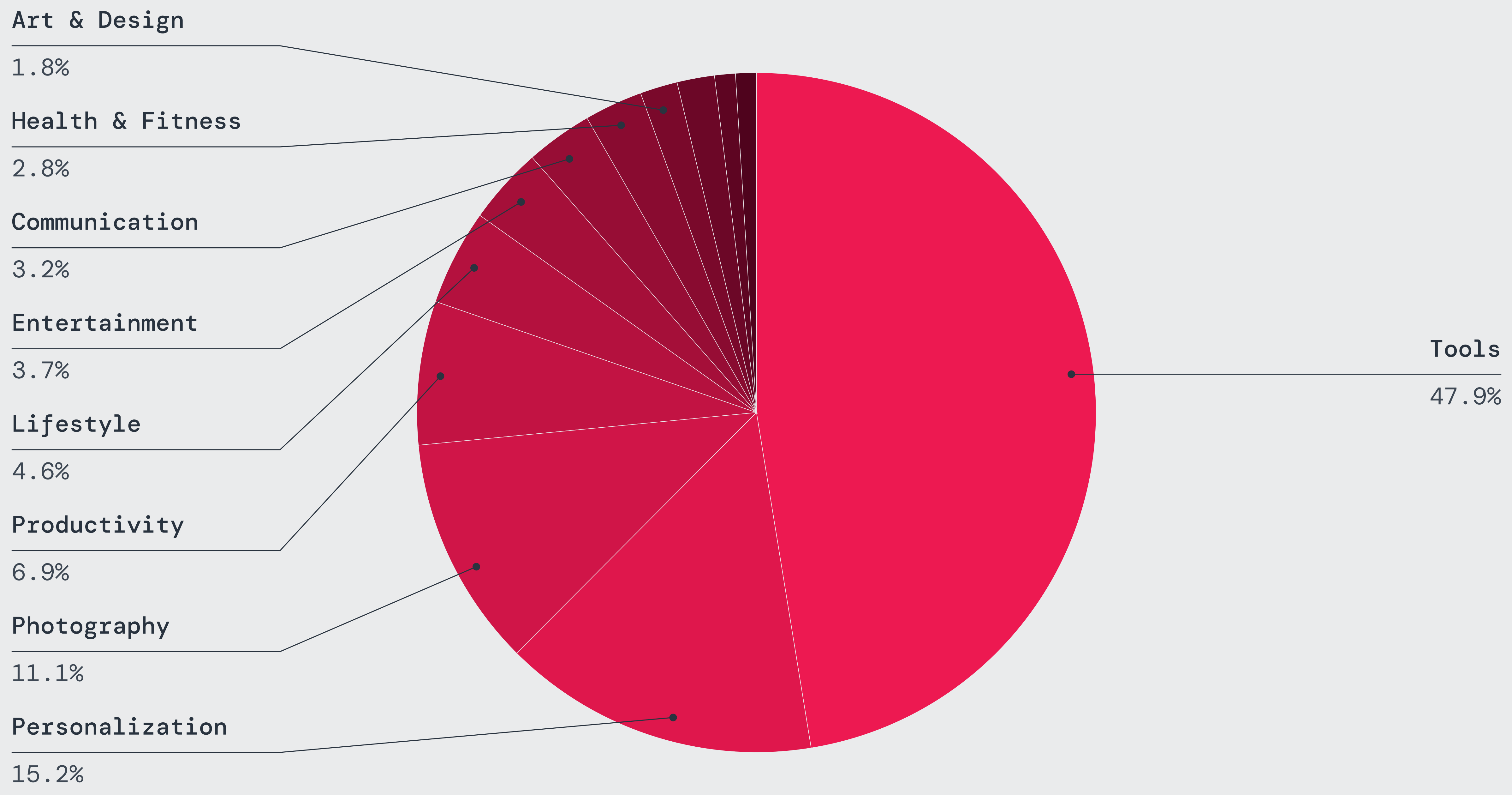


Figure 13: Distribution of app categories most commonly targeted to spread malware

Spyware

In addition to the rise in banking malware, the Android spyware threat also saw a significant increase, with blocked transactions increasing by since 100% over the previous year.

Spyware-related blocks reached 232,000, making up 1% of all blocked transactions. This surge is largely attributed to the growing prevalence of campaigns like SpinOk and SpyNote within the Android spyware families.

Year	Number of spyware transactions
2022-2023	109,889
2023-2024	232,093

The most prominent spyware malware families observed during our analysis were SpyLoan, SpinOk, and SpyNote.

SpyLoan

SpyLoan steals personal data from the device, including a list of all accounts, device information, call logs, installed apps, calendar events, local Wi-Fi network details, and metadata from images.

SpinOk

SpinOk spyware is distributed as a marketing software development kit (SDK) with embedded spyware functionality. It collects sensitive data and files from various locations on an infected device and exfiltrates them to remote servers.

SpyNote (a.k.a. SpyMax, CypherRat)

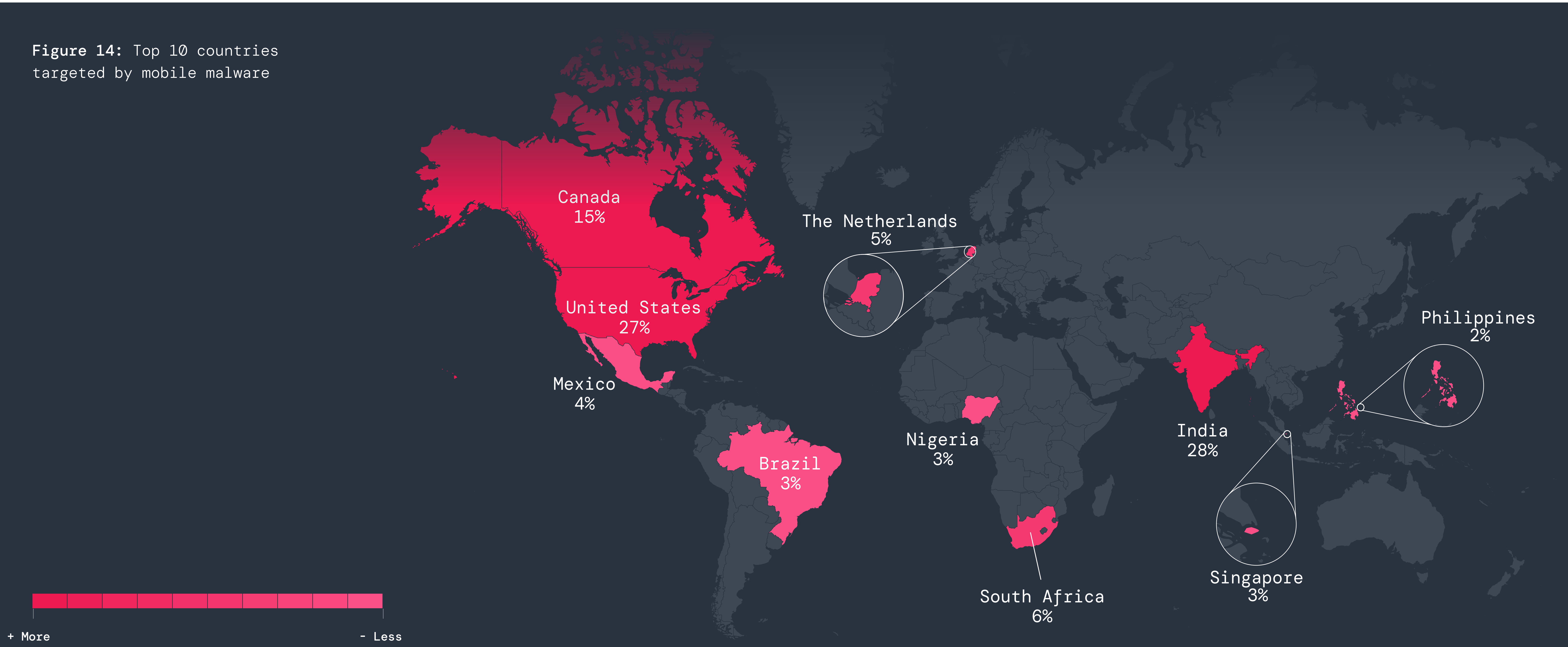
Spynote (a.k.a. SpyMax, CypherRat) is spyware with RAT capabilities. The infection typically begins with a fake SMS message (smishing) containing a link to download a malicious app. It can gather personal information from the infected device without user consent and send it to C2 servers.

Geographical Analysis

Most mobile malware targeted the following countries:

1. India (28%)
2. US (27%)
3. Canada (15%)
4. South Africa (6%)
5. The Netherlands (5%)
6. Mexico (4%)
7. Nigeria (3%)
8. Brazil (3%)
9. Singapore (3%)
10. Philippines (2%)

Figure 14: Top 10 countries targeted by mobile malware



Industry and Sector Analysis

The following industries faced the highest concentration of threats:

1. Technology (18%)
2. Education (18%)
3. Manufacturing (14%)
4. Retail and Wholesale (12%)
5. Services (7%)

Most targeted verticals

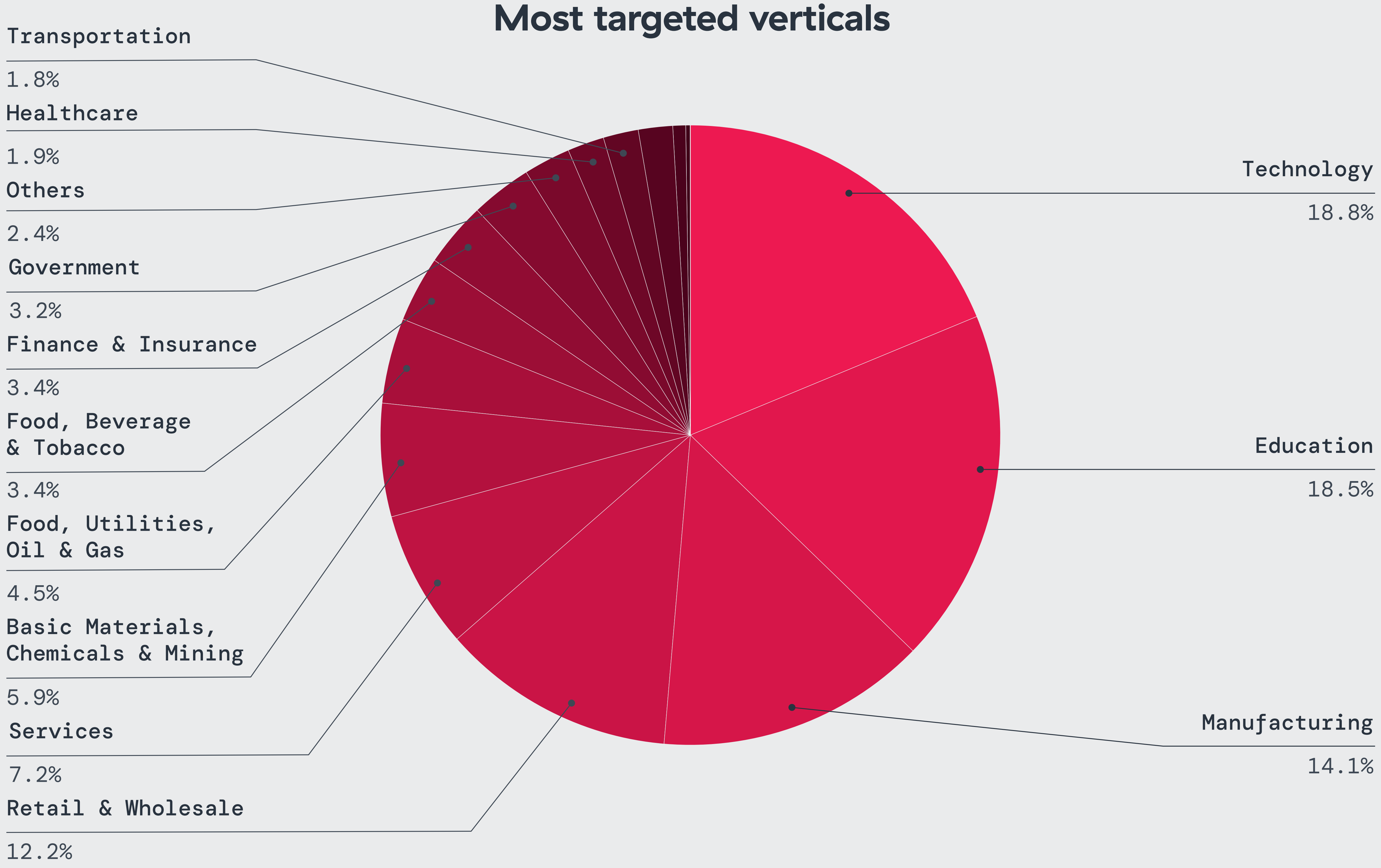


Figure 15: Distribution of attacks across industries

Rise in attacks on education and services sectors

Year over year, most verticals experienced a decline in blocked mobile threats, except for Education and Services.

The Education sector saw a 136% increase in blocked transactions, while the Services sector experienced a 40% rise, marking a significant uptick in targeted attacks compared to the previous year.

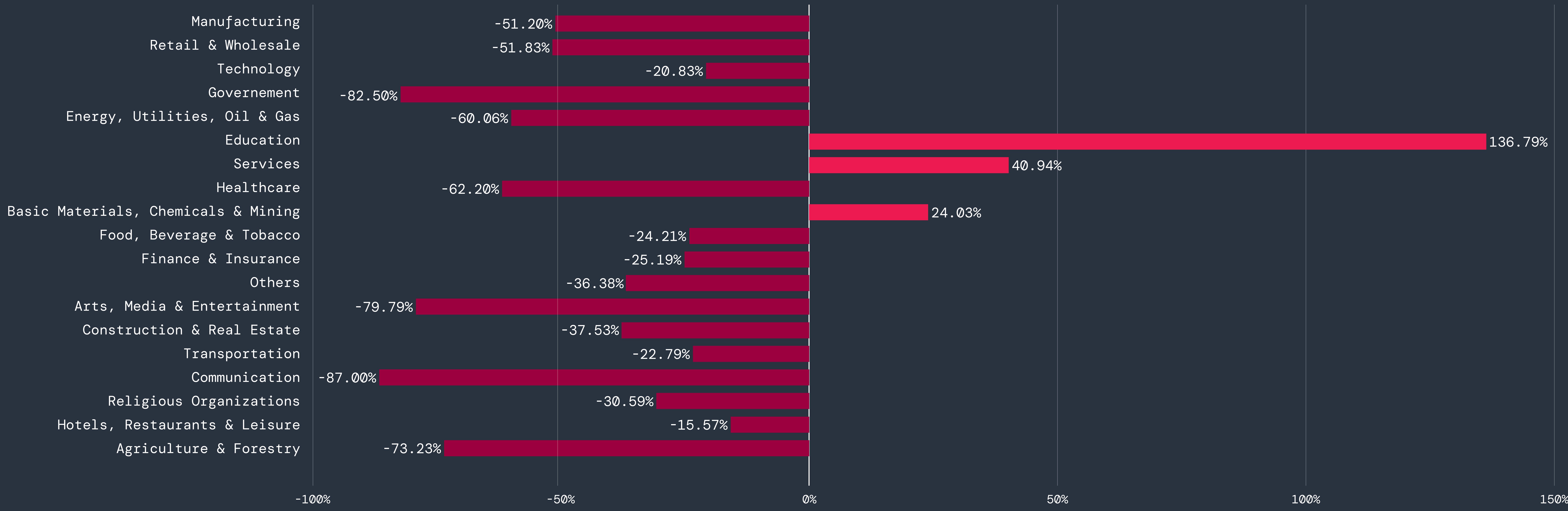


Figure 16: General decline in blocks across most sectors

Top IoT & OT_Threats

Key Findings

IoT malware attacks rose 45%, with increased payload delivery.

Zscaler blocked 45% more IoT malware transactions than the previous year. ThreatLabz also observed a 12% rise in the number of attempts to deliver malware (payload deliveries) to IoT devices.

The Mirai and Gafgyt malware families still dominate.

More than 75% of blocked IoT transactions were linked to the Mirai malware family, which is notorious for creating IoT botnets. Meanwhile, roughly 50% of all malicious payloads originated from the Mirai and Gafgyt malware families, underscoring their continued prevalence in IoT attacks.

The US remains a top target for IoT attacks.

More than 80% of IoT botnet attacks targeted devices in the US, largely due to the proliferation of IoT devices among US industries and consumers, as well as the country's robust digital infrastructure.

Manufacturing experiences the lion's share of attacks.

For the second year in a row, the manufacturing vertical experienced the highest volume of IoT malware attacks, accounting for 36% of all IoT malware blocks observed.

Command injection vulnerabilities make up the bulk of IoT CWEs.

Nearly 75% of exploited common weakness enumerations (CWEs) were related to command injection vulnerabilities, which allow attackers to execute unauthorized commands, often leading to the download and installation of stager scripts or malicious binaries.

OT security risks abound.

In a ThreatLabz analysis of large OT deployments, often **more than 50%** of OT devices are dependent on legacy, end-of-life operating systems, typically with known vulnerabilities. Moreover, high-risk legacy protocols and services often make up more than 20% of internal East-West network connections.

Overview

As IoT and OT environments continue to expand rapidly, they play an integral role in both consumer and industrial settings. Indeed, IoT devices and historically air-gapped OT systems are now connected to core enterprise IT systems. Being business-critical, they are also increasingly the targets of attack across large industries.

From 2023 to 2024, ThreatLabz observed a significant uptick in IoT activity overall. This included more than 9 billion device transactions from over 1,164 unique IoT devices across more than 300 brands. This represents a 37% year-over-year growth in the number of IoT devices interacting with the Zscaler Zero Trust Exchange.

This growth in IoT transactions has also come with a surge in IoT threats. Overall, ThreatLabz tracked a 45% increase in IoT malware attacks over the past year. Meanwhile, in an analysis of large-scale OT deployments, ThreatLabz identified persistent risks. These include the fact that as many as 50% of OT devices in many deployments use legacy, end-of-life operating systems that contain known vulnerabilities. This surge in IoT transactions, combined with increased OT system connectivity and the rising threat landscape, underscores the growing complexity and scale of the IoT/OT ecosystem, making it a critical area of focus for security efforts.

IoT Device Categories

Top device categories interacting with the Zscaler cloud

The IoT devices that interact with the Zscaler cloud, found commonly in both consumer and enterprise environments, reflect the ever-expanding network of connected technology in our daily lives and the critical need for robust security measures to protect the vast amounts of data they generate and transmit.

Leading the pack are set-top boxes (accountable for 17% of total devices), followed closely by smart watches (14%) and smart TVs (10%). Other notable contributors include data collection terminals and media players.

A full spectrum of IoT devices

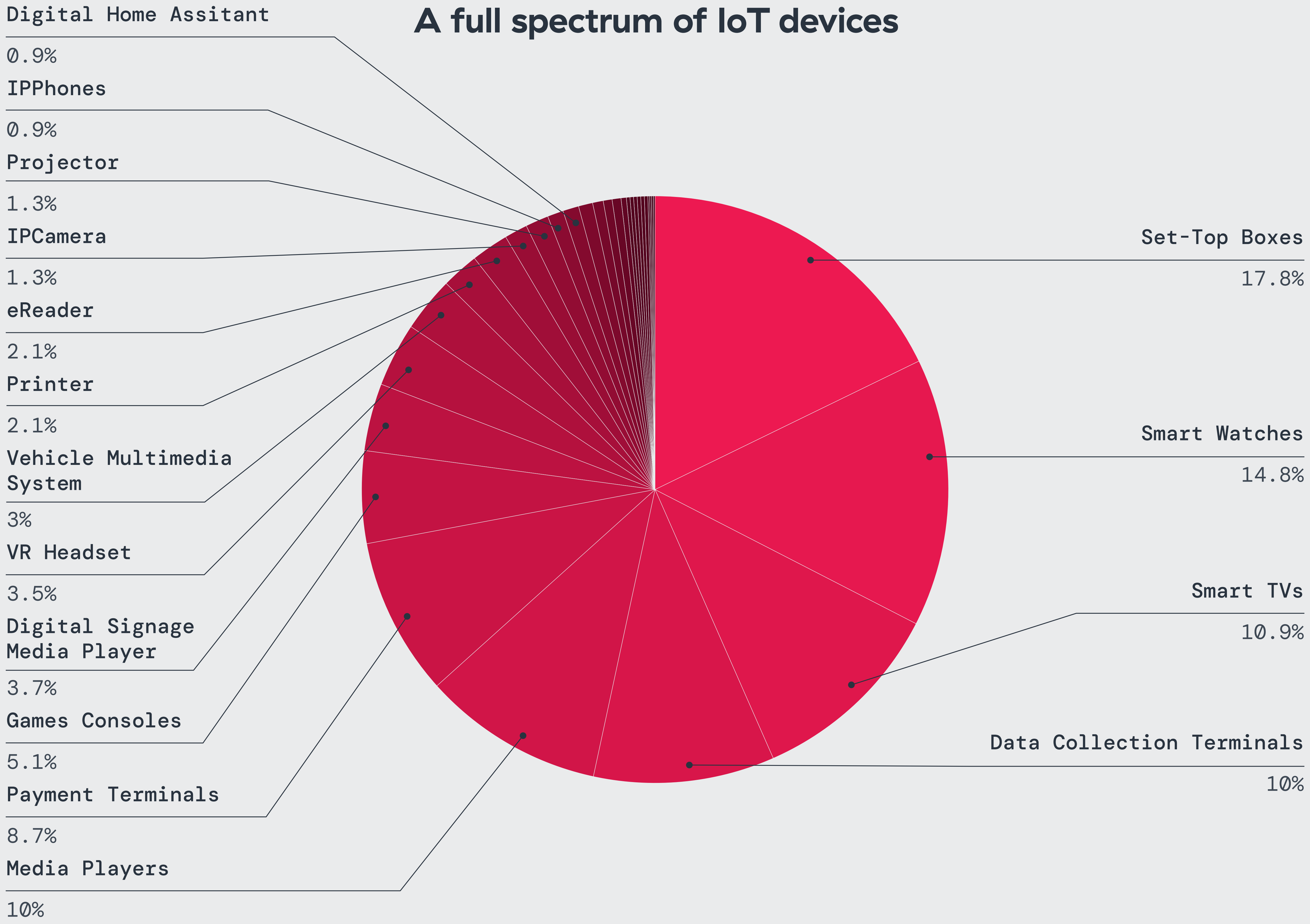


Figure 17: Distribution of IoT device categories in the Zscaler cloud

Routers see the bulk of IoT attacks

Most targeted device type

Similar to the previous year, routers remain the most targeted device type for malware attacks, with **66% of attacks aimed at them.** Not only are routers internet-connected and therefore discoverable by threat actors, they can often have security vulnerabilities that may be exploited.

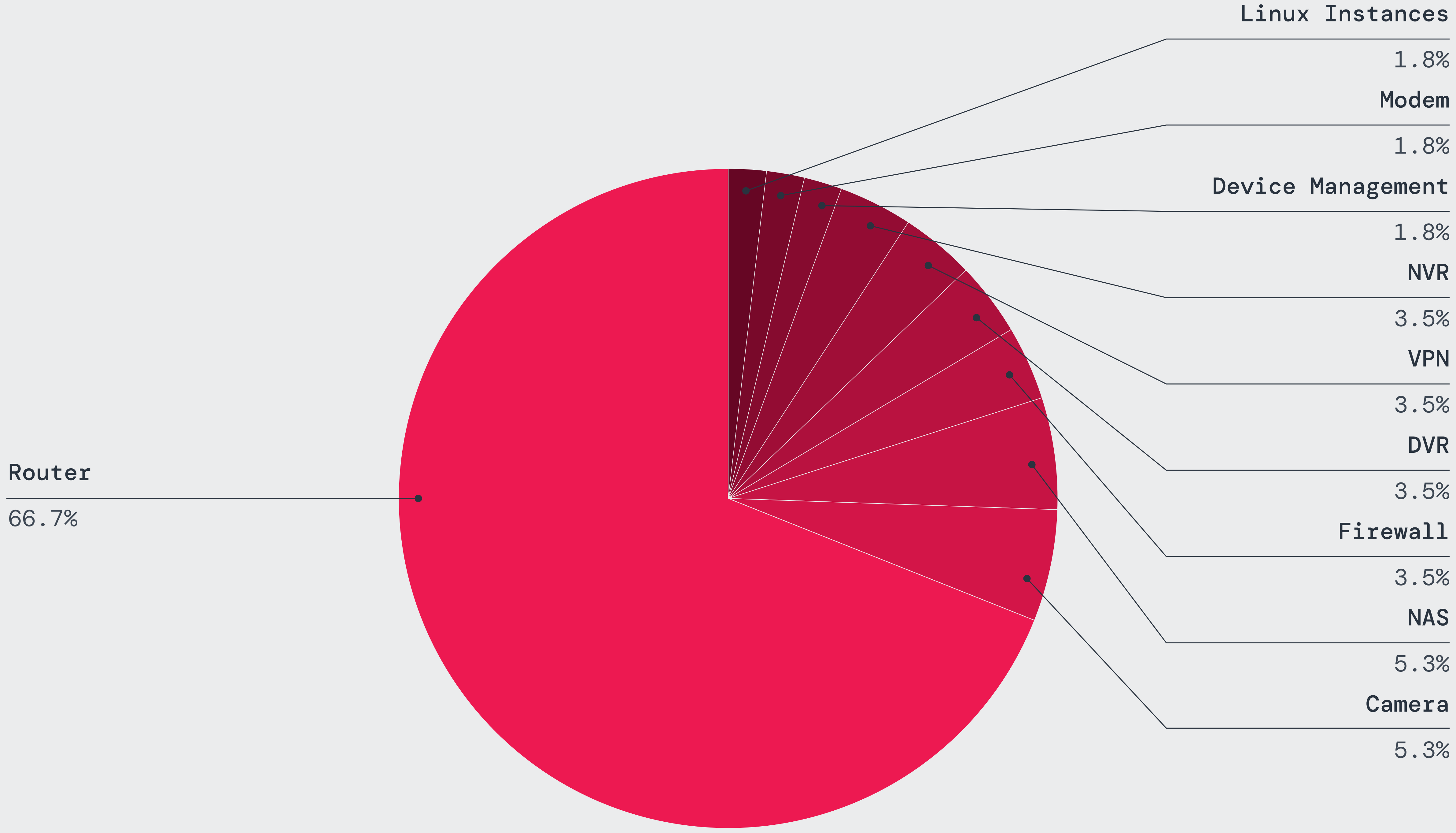


Figure 18: Devices most targeted by malware attacks

IoT Malware

Top IoT malware families

The Mirai and Gafgyt malware families continue to drive most malware attacks, maintaining their status as the most prolific IoT malware threats for another year.

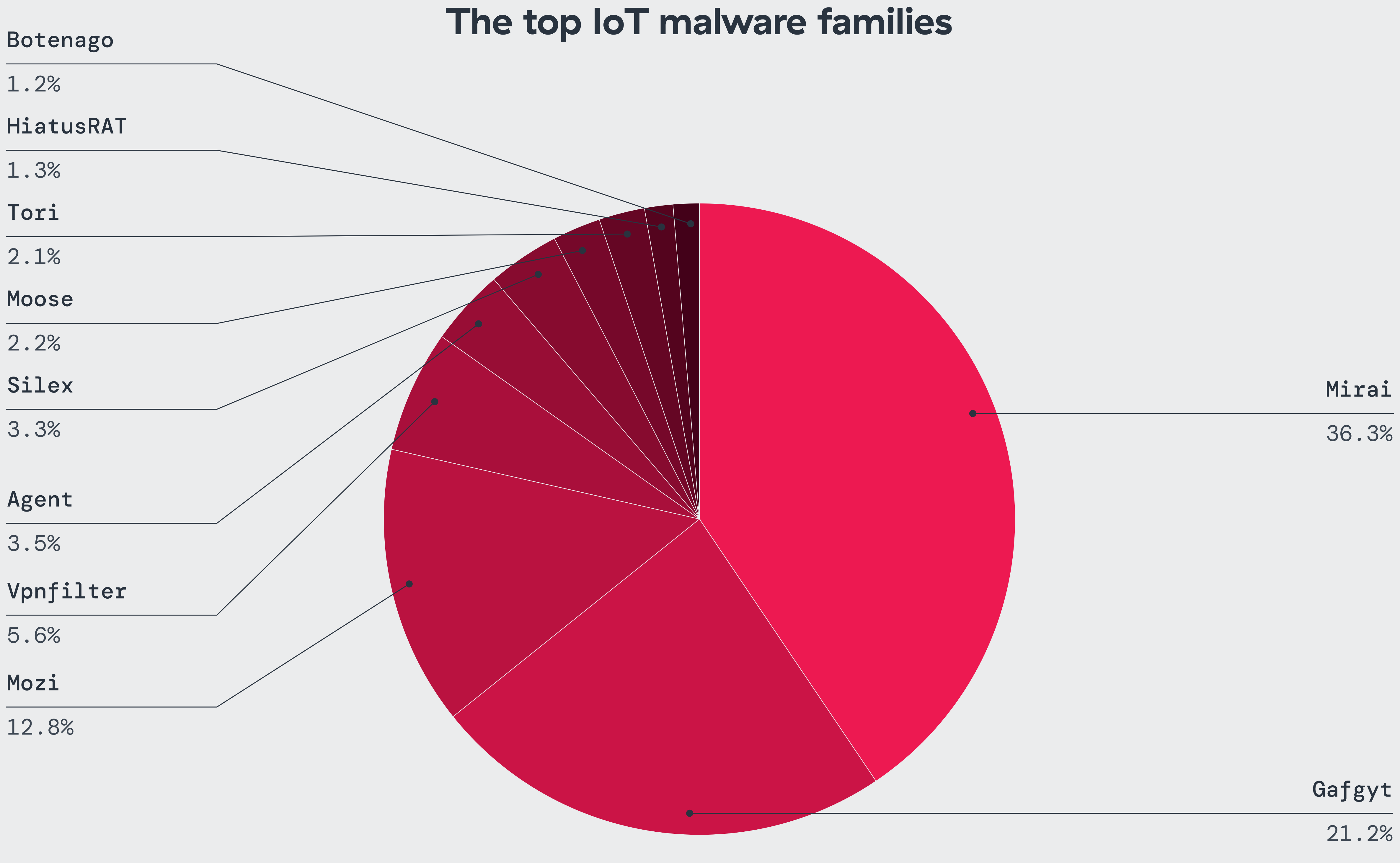


Figure 19: Top IoT malware families observed in the Zscaler cloud

The U.S. remains the top IoT target

Most targeted countries

The US experienced the vast majority of IoT malware transactions, accounting for 81% of all IoT attacks. Singapore and the United Kingdom followed with 5% and 3% of overall blocked transactions, respectively.

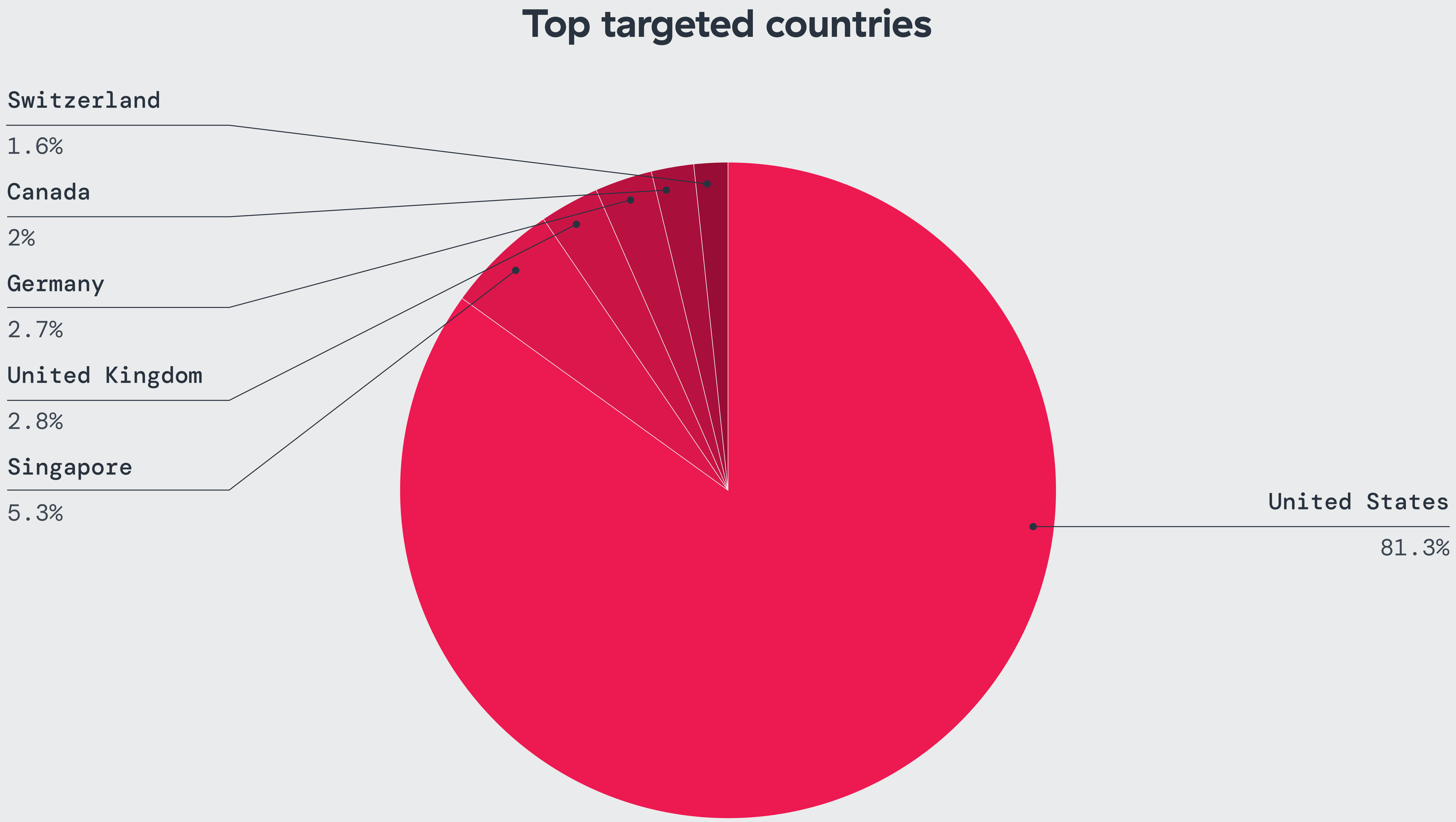


Figure 20: Most targeted countries for IoT malware attacks

Industry and Sector Analysis

Most targeted verticals

The manufacturing, transportation, and food & beverage sectors were the primary targets of IoT attacks. These industries remain prime targets due to their extensive reliance on IoT devices, which are often vulnerable to cyberattacks.

Manufacturing was hit the hardest, accounting for 36% of all IoT malware blocks observed. The transportation sector followed with 14%, while food & beverage saw 11% of total blocks.

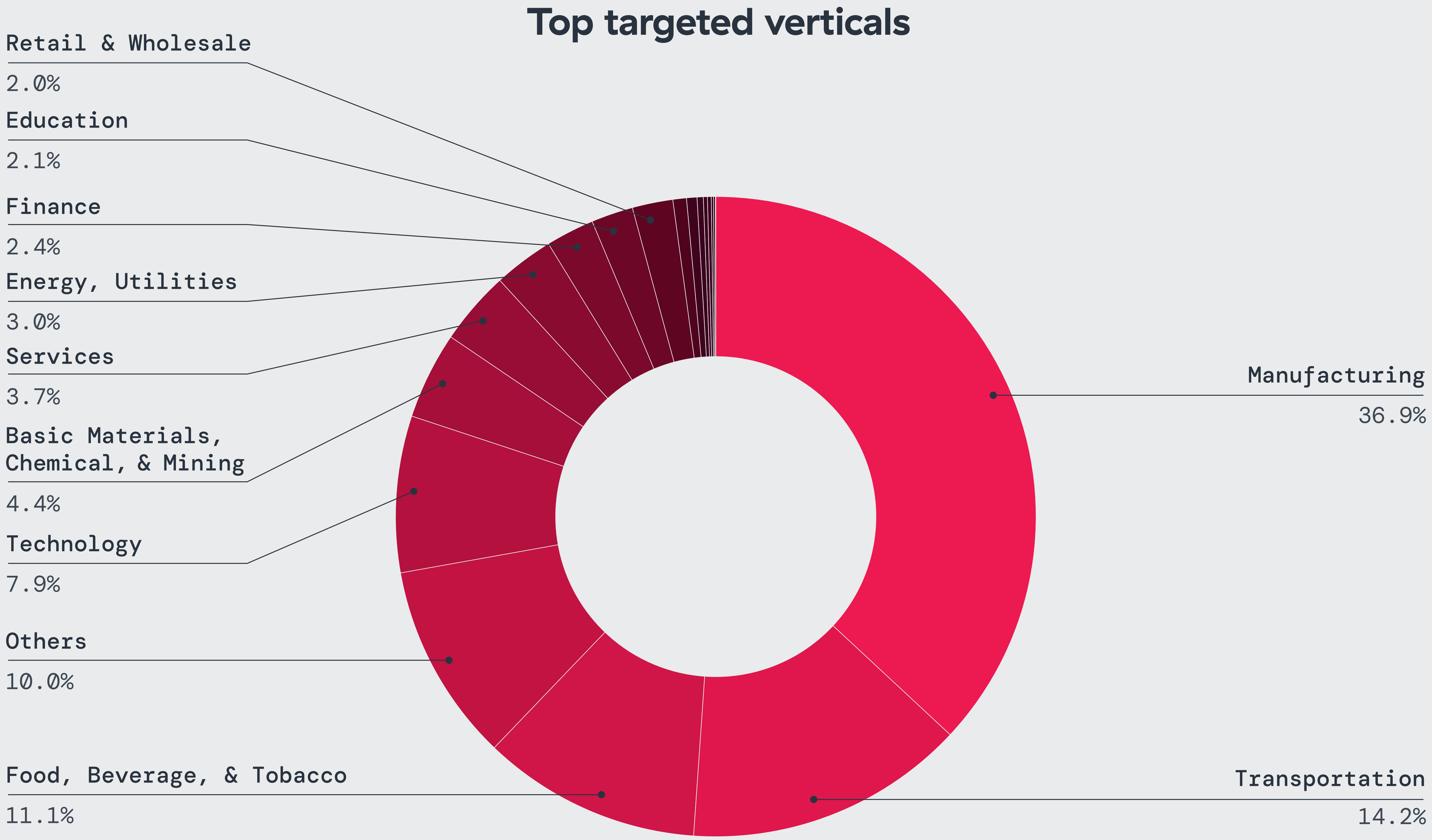


Figure 21: Distribution of the most targeted industries

Manufacturing maintains the widest array of IoT devices

Most unique devices per vertical

When analyzing unique devices across different verticals, the Manufacturing sector stands out with the highest implementation of IoT devices. This is largely due to the extensive range of applications IoT technology supports within manufacturing, from automation and process monitoring to supply chain management.

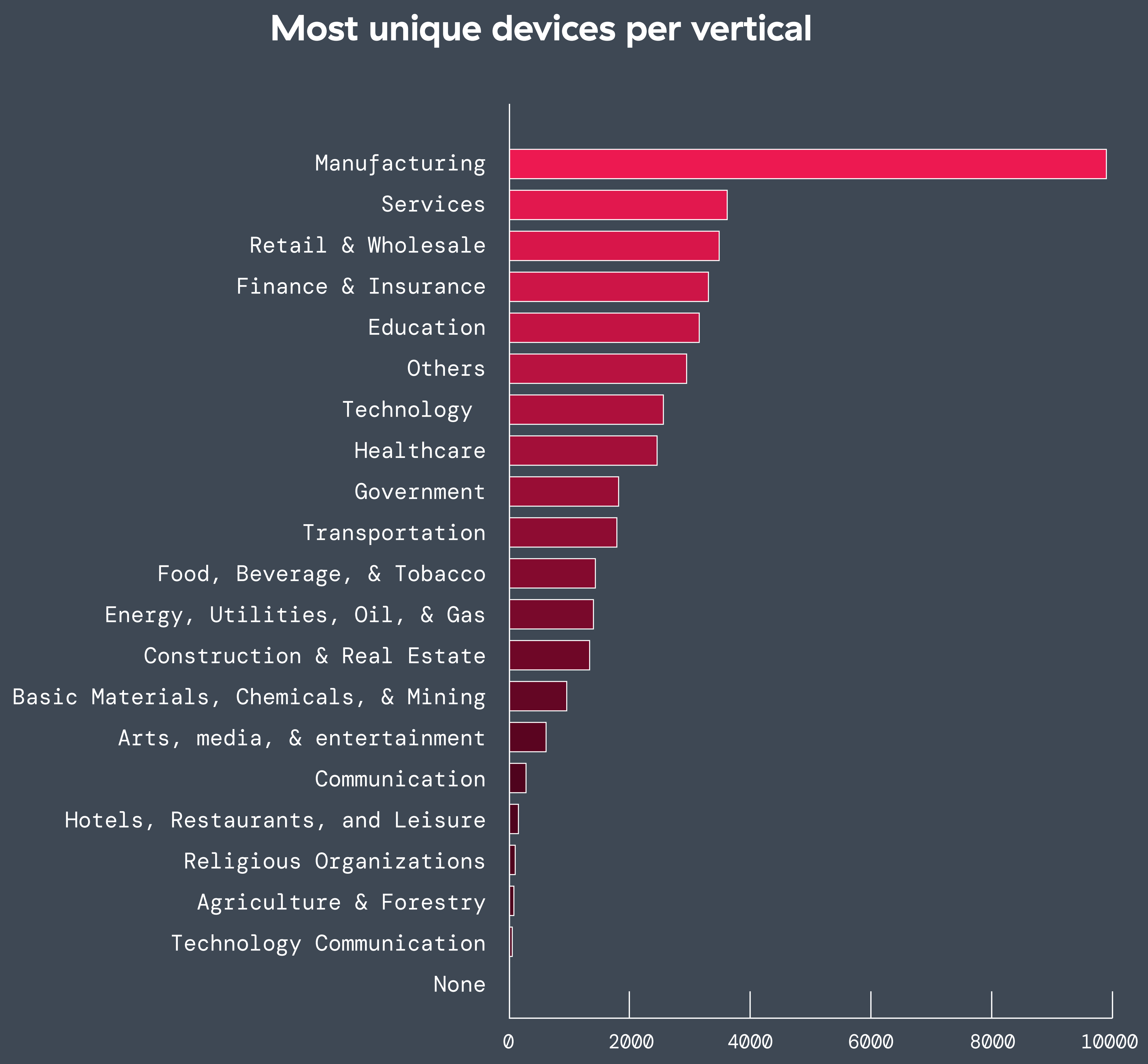


Figure 22: Unique device count by vertical

Data collection terminals drive business — and the bulk of IoT device traffic

Top IoT devices by traffic generated

A significant portion of IoT device traffic is driven by business transactions, with data collection terminals (wireless barcode readers used in manufacturing, engineering, logistics, and warehousing applications) leading the way at 79%—underscoring their critical role in business operations.

Printers generate 9% of traffic, while media players add 5%, reflecting the diverse range of devices that facilitate business processes and operations in the IoT landscape.

Top IoT devices by traffic generated

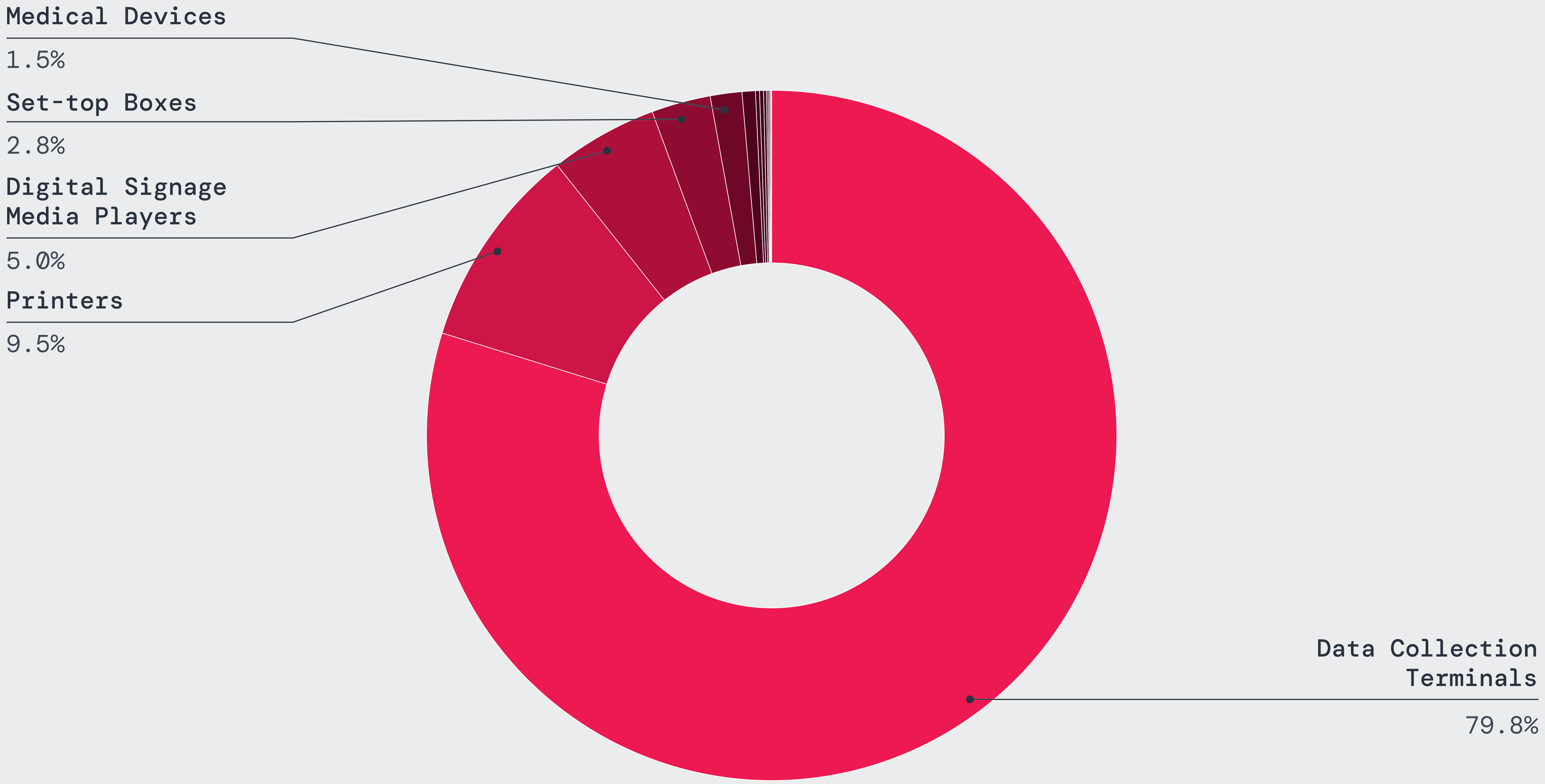


Figure 23: IoT devices generating the most traffic

The Retail & Wholesale sector is an IoT traffic powerhouse

Top verticals driving IoT traffic

The Retail & Wholesale vertical generates most IoT traffic (68%), largely driven by the extensive use of data collection terminal devices. These terminals play a crucial role in daily operations, contributing significantly to the overall traffic of these industries.

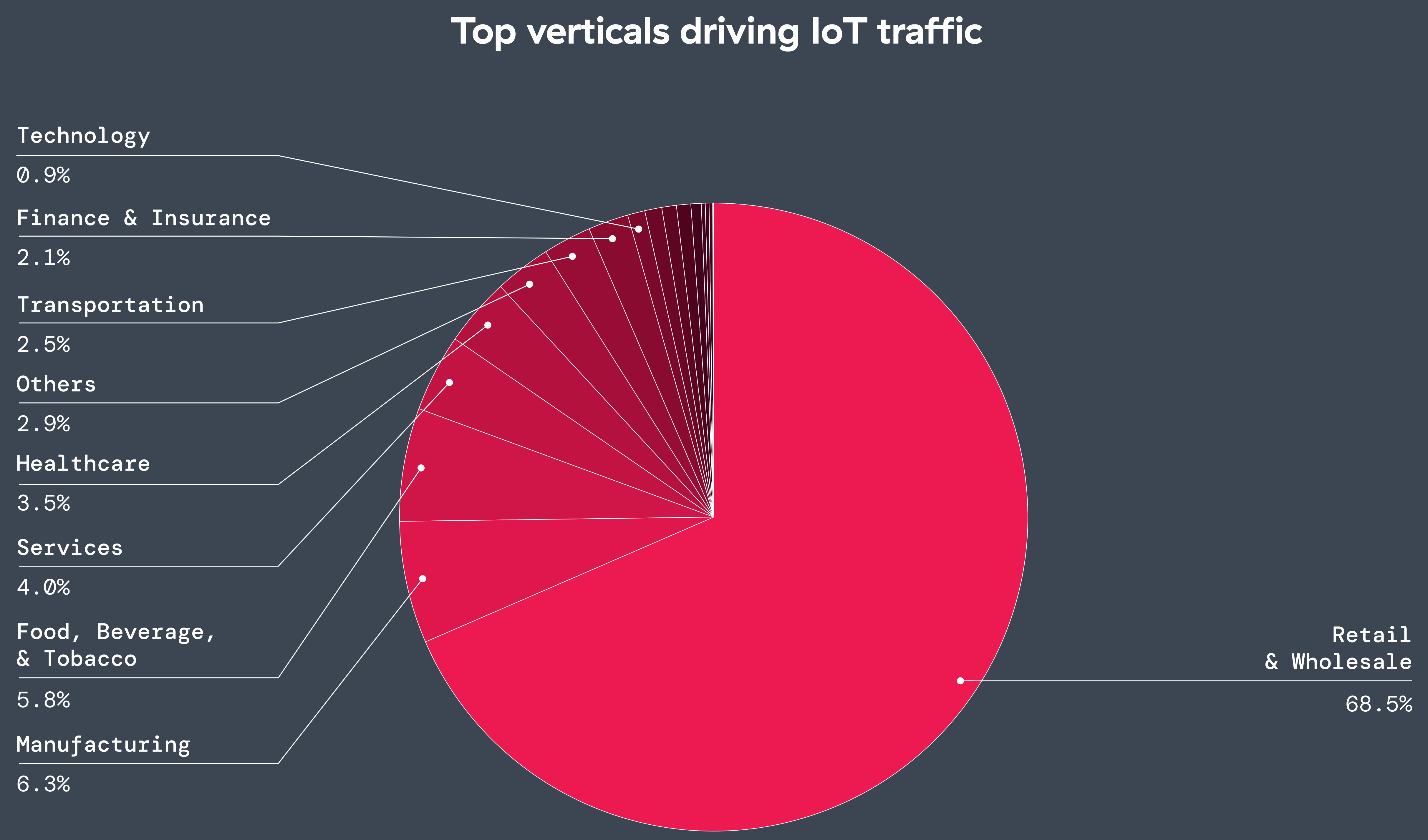


Figure 24: Industries that generated the most IoT traffic

Geographical Analysis

Top destinations based on unique devices

The US stands out as the primary destination for IoT device traffic, with 87% of overall IoT–generated traffic directed at the US. This highlights the country's central role in global communication and data processes, but also explains why the US attracts the majority of IoT malware attacks.

The following countries receive the most IoT traffic:

1. United States
2. Japan
3. China
4. Singapore
5. Germany
6. Hong Kong
7. France
8. United Kingdom
9. The Netherlands

Entertainment and home automation devices continue to route to China and Russia

Entertainment and home automation devices continue to route a significant portion of their traffic to China and Russia. Smart TVs are the primary contributors to this traffic, accounting for 86%.

While much of this traffic is legitimate and benign, these destinations are flagged as suspicious by ThreatLabz due to concerns over potential government surveillance and other data vulnerabilities.

Top devices sending traffic deemed "suspicious"

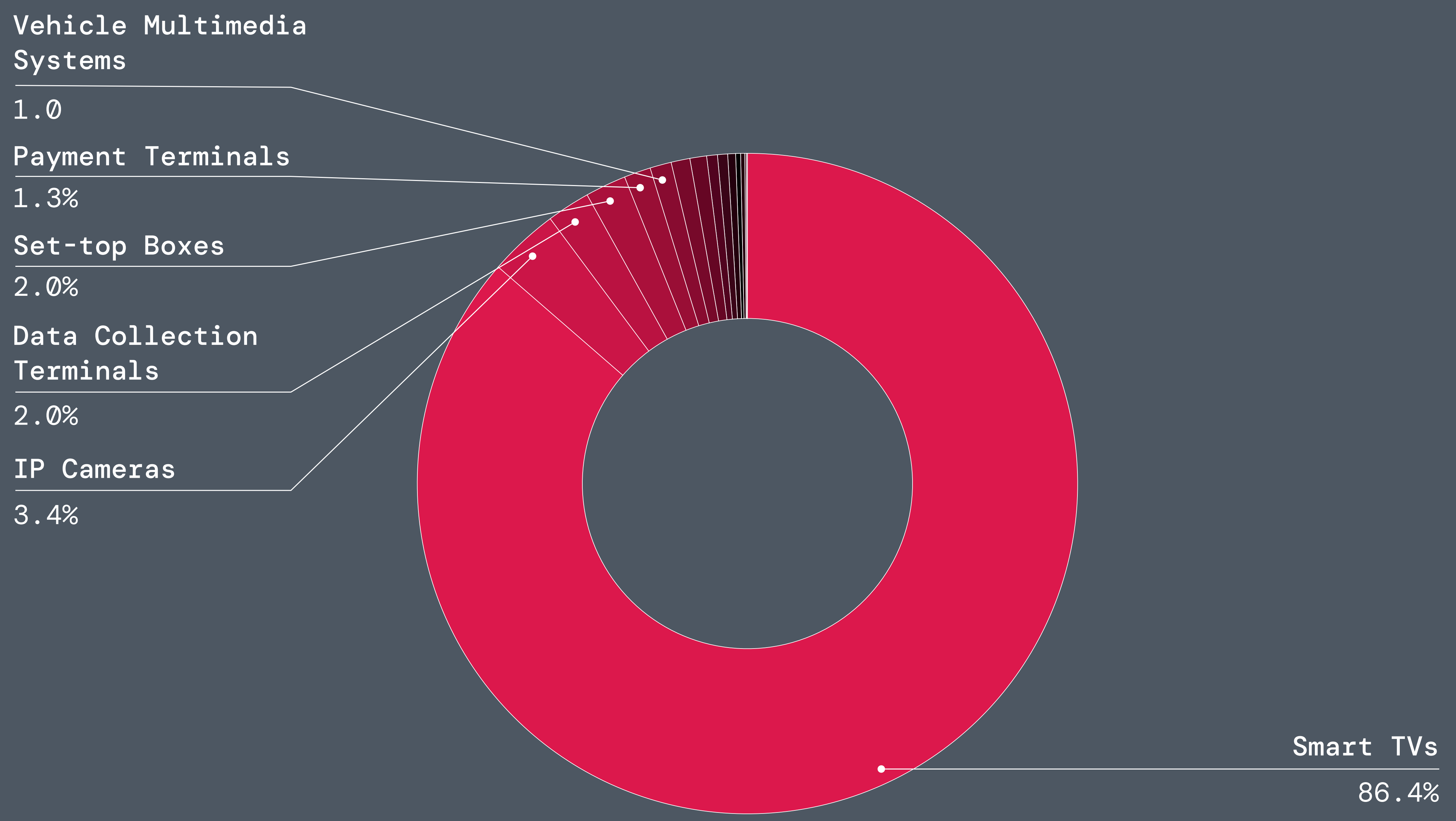


Figure 25: Distribution of devices across traffic deemed "suspicious"

IoT Vulnerabilities

Most popular exploits

IoT malware is known for weaponizing different known exploits in IoT devices to carry out attacks on those devices. By analyzing the vulnerabilities in observed payloads, we saw 75% of exploits were command injection attacks, wherein an unauthorized executable inputs commands, which are often used to download and execute stager scripts or malicious binaries.

We found that 10% of exploits were based on improper input validation type vulnerabilities, where input received on IoT devices doesn't get properly checked or validated.

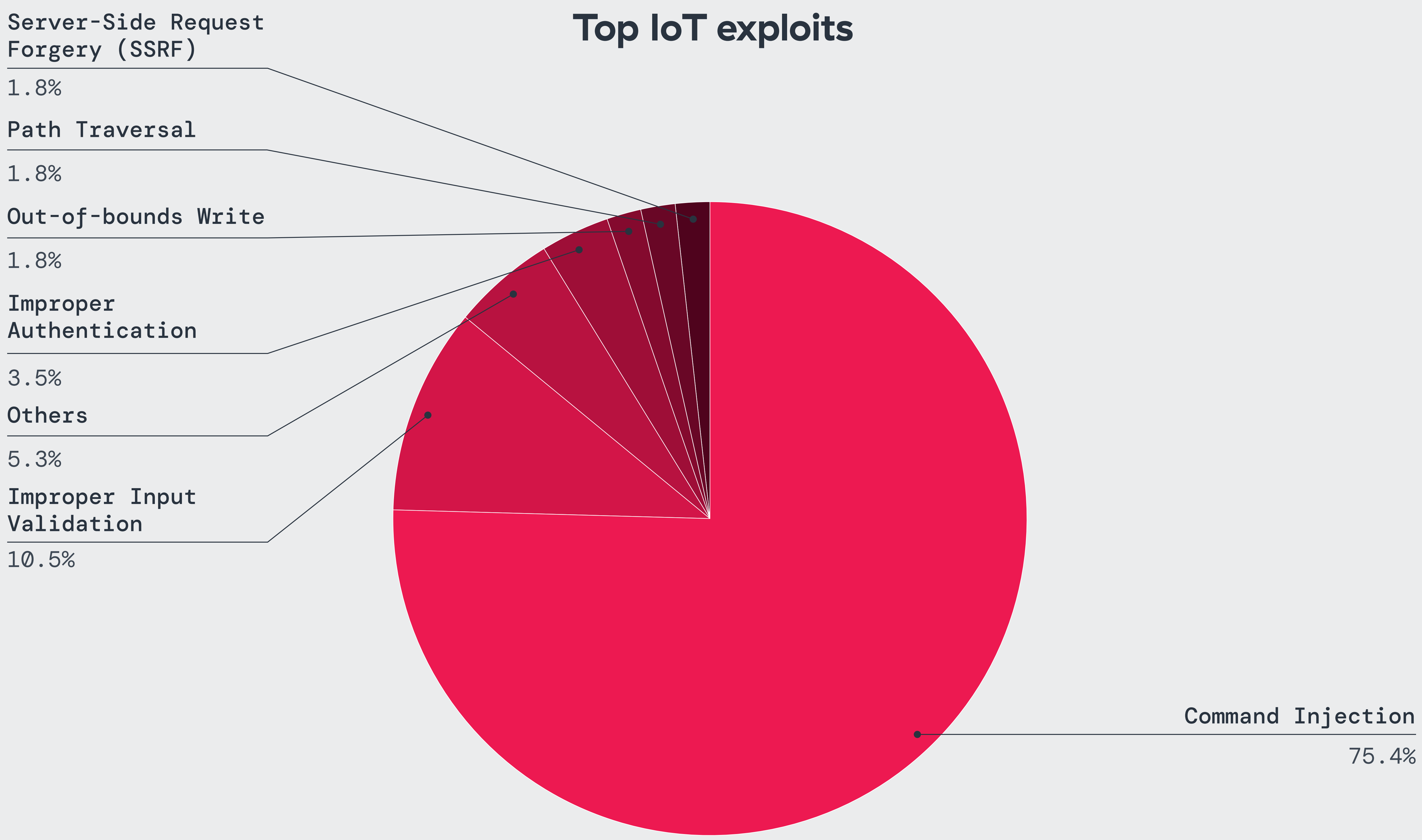


Figure 26: Distribution of IoT/OT-related vulnerabilities observed in the Zscaler cloud

Challenges in Securing OT Environments

Recently, there has been a surge in alerts and warnings concerning cyberattacks from state-sponsored threat actors on US critical infrastructure. On February 7, 2024, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), along with the National Security Agency (NSA), issued an advisory warning to governmental organizations regarding cyber actors poised to disrupt critical infrastructure, such as water treatment plants, electric grids, oil and natural gas pipelines, and transportation systems.

In addition, the US Department of Energy (DOE) has released the Cybersecurity Baseline, and the North American Electric Reliability Corporation (NERC) has nearly finalized the update to CIP-015-1. The Transportation Security Administration (TSA) has also issued an alert for airports and aircraft operators that mirrors earlier alerts for railways. The core compliance requirement: “Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised, and vice versa.”[4]

Real-world critical infrastructure networks, such as manufacturing, hospitals, transportation, and energy networks, have always been difficult to secure. Filled with unprotected identities and OT/IoT endpoints that cannot host security agents, these verticals remain a primary cyberattack target. This threat is not isolated to initial breaches by threat actors, but rather to their ability to move laterally across OT and connected IT networks before embedding ransomware and prepping malicious payloads. Highlighting this urgency, the CISA has reported a massive surge in real-time surveillance of SCADA devices by threat groups, targeting unprotected sensors, headless devices, and legacy controllers.

Experts including industry analysts, insurers, and standards agencies, such as NIST, are pushing hard for segmentation as a critical defense strategy. Gartner highlights this broader trend, noting, "The increasing interest in zero trust architectures drives requirements to reduce flat networks into increasingly smaller trust zones where workloads are positively identified, and only allowed connections between workloads exist.”[5] Unfortunately, traditional segmentation is difficult to implement in practice. While advocating segmentation as a core security principle, Gartner also notes, “The failure rate for network segmentation projects is high, and most projects last longer than the average tenure of a CISO.”

Segmentation has long been a staple in networking, with tools like access control lists (ACLs) and firewalls managing north-south (client-to-server) traffic. However, OT microsegmentation and device segmentation shifts the focus to the more vulnerable east-west traffic, which flows laterally between devices and workloads. On shared VLANs, devices can see and communicate with all others, creating a rich environment for malware to spread. However, agent-based solutions pioneered in the WAN are unable to segment the legacy and headless or agentless machines common in OT environments, while ACL-based approaches remain so overcomplicated that they are ineffective in practice.

[4] TSA, **TSA issues new cybersecurity requirements for airport and aircraft operators**, March 7, 2023.
[5] Gartner, **The 6 Principles of Successful Network Segmentation Strategies**, Jeremy D’Hoinne, Andrew Lerner, November 19, 2022.

Quantifying Security Risks in OT Environments: Legacy Systems, Unauthorized Connections, and High-risk Services

ThreatLabz surveyed large-scale OT environments in the manufacturing and healthcare industries, with the goal of quantifying the internal attack surface and understating its key risks. In general, OT devices are business-critical, carry high capital and operational costs, and typically rely on legacy operating systems. Moreover, OT networks often generate as many internal (east-west) connections across services and devices as they do to the public internet. Many of these connections can be unauthorized; meanwhile, numerous internal protocols and services can create additional risk. All of this contributes to a large OT attack surface that threat actors can more easily navigate and exploit.

LEGACY SYSTEMS IN OT

A substantial number of OT environments rely on outdated **legacy Windows systems** that often have known vulnerabilities, with most physical sites depending on over **500 unique OT devices.** This creates a significant security vulnerability: if one device is compromised, the remaining **499 are also at risk of infection.**

UNAUTHORIZED CONNECTIONS

Enterprise OT networks are often rife with unauthorized connections. In one large OT deployment representing tens of thousands of OT devices, **67% of connections** with the network are classified as **unwanted** or **unauthorized**, highlighting the significant volume of unnecessary traffic. Out of the 8.6 million data flows observed, **5.8 million were tied to drop policies,** emphasizing the prevalence of connections that violate security policies and need to be blocked. This underscores the importance of enabling stronger access controls, particularly with individual device segmentation, and continuous monitoring to minimize unauthorized activity and enhance network security.

NETWORK TRAFFIC

Manufacturing organizations are experiencing **nearly equal levels** of internal (east-west) and external (internet-facing) network traffic, underscoring the growing complexity of modern network environments. Yet enterprises typically have difficulty gaining east-west visibility and segmenting east-west traffic. Indeed, lack of focus on internal security could expose manufacturing organizations to lateral threat movement, making east-west traffic a critical area for monitoring and protection.

HIGH-RISK SERVICES

Manufacturing organizations face significant security risks due to the prevalence of **legacy services** like **Server Message Block (SMB), Windows Management Instrumentation (WMI), Telnet, Network Basic Input/Output System (NetBIOS), and Remote Desktop Protocol (RDP),** which remain among common high-risk services. For example, in one large-scale OT deployment, high-risk services including SMB, WMI, and Telnet represented 23% of their network connections. In another deployment, SMB, WMI, RDP, and NetBios accounted for over 26% of connections. These protocols, often integral to daily operations, are notorious for their vulnerabilities, making them prime targets for exploitation by attackers. Without proper segmentation and monitoring, the use of these services can provide easy entry points for lateral movement within networks.

Case study: Large-scale OT manufacturing environment

In the manufacturing sector, OT deployments can involve thousands of connected OT devices spread across dozens of sites. This creates a substantial attack surface that is vulnerable to external threats, such as those that exploit known or zero-day vulnerabilities in internet-connected systems. Just as importantly, this also creates a large internal attack surface between internal (east-west) OT traffic that increases the risk of lateral movement and the potential blast radius of a successful attack.

To demonstrate these risks, ThreatLabz analyzed the OT environment of a large-scale manufacturing organization. This deployment involved more than 17,000 connected OT devices across more than 40 locations. On average, each site contains more than 500 OT devices with end-of-life Windows operating systems (OS), many with known vulnerabilities. This is a significant attack vector, as any single compromised device means that the 499 other devices are at risk of infection.

Meanwhile, this environment carries substantial network risks due to the use of numerous high-risk protocols and services.

Risky services and protocols in East-West traffic

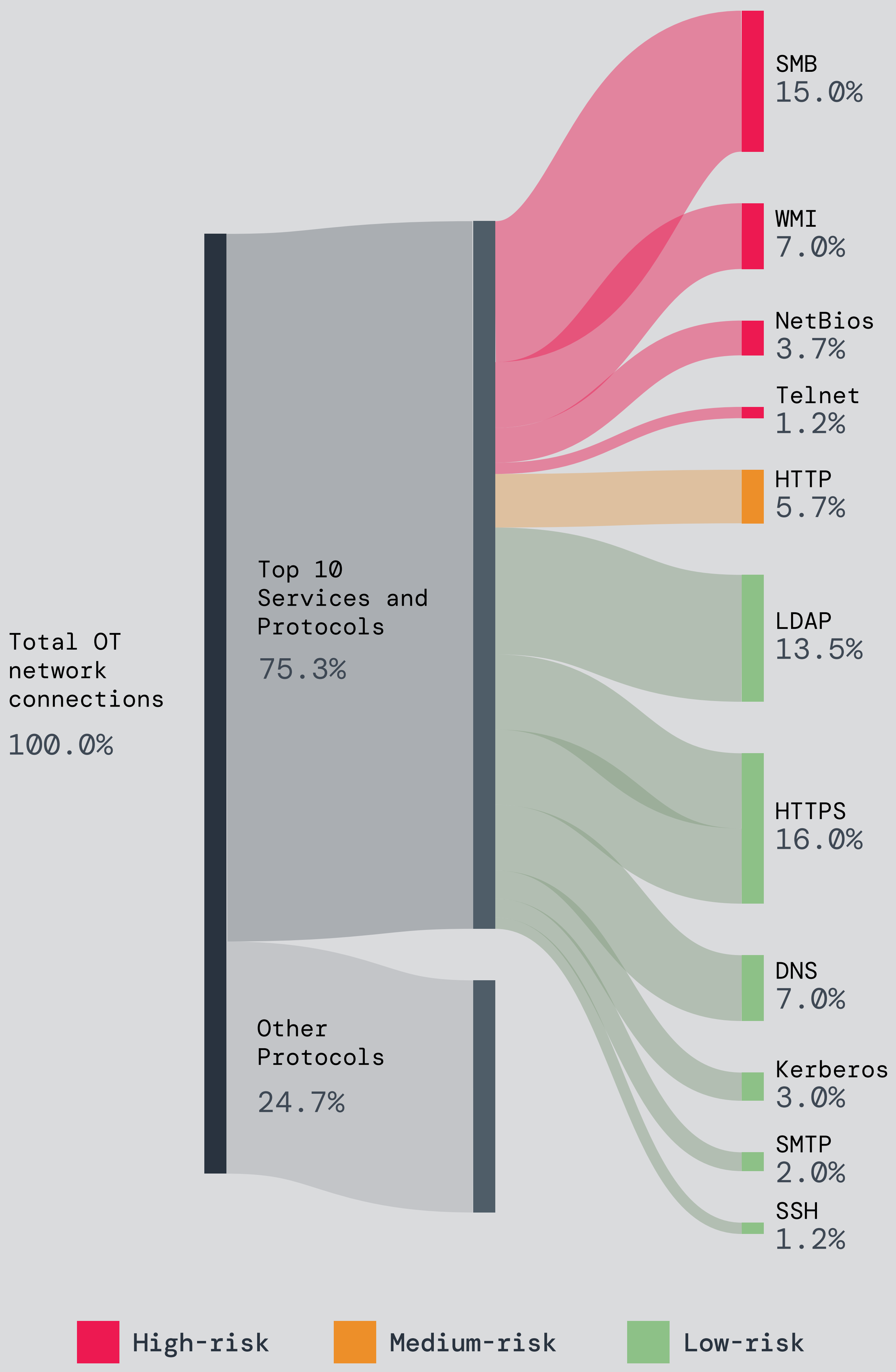
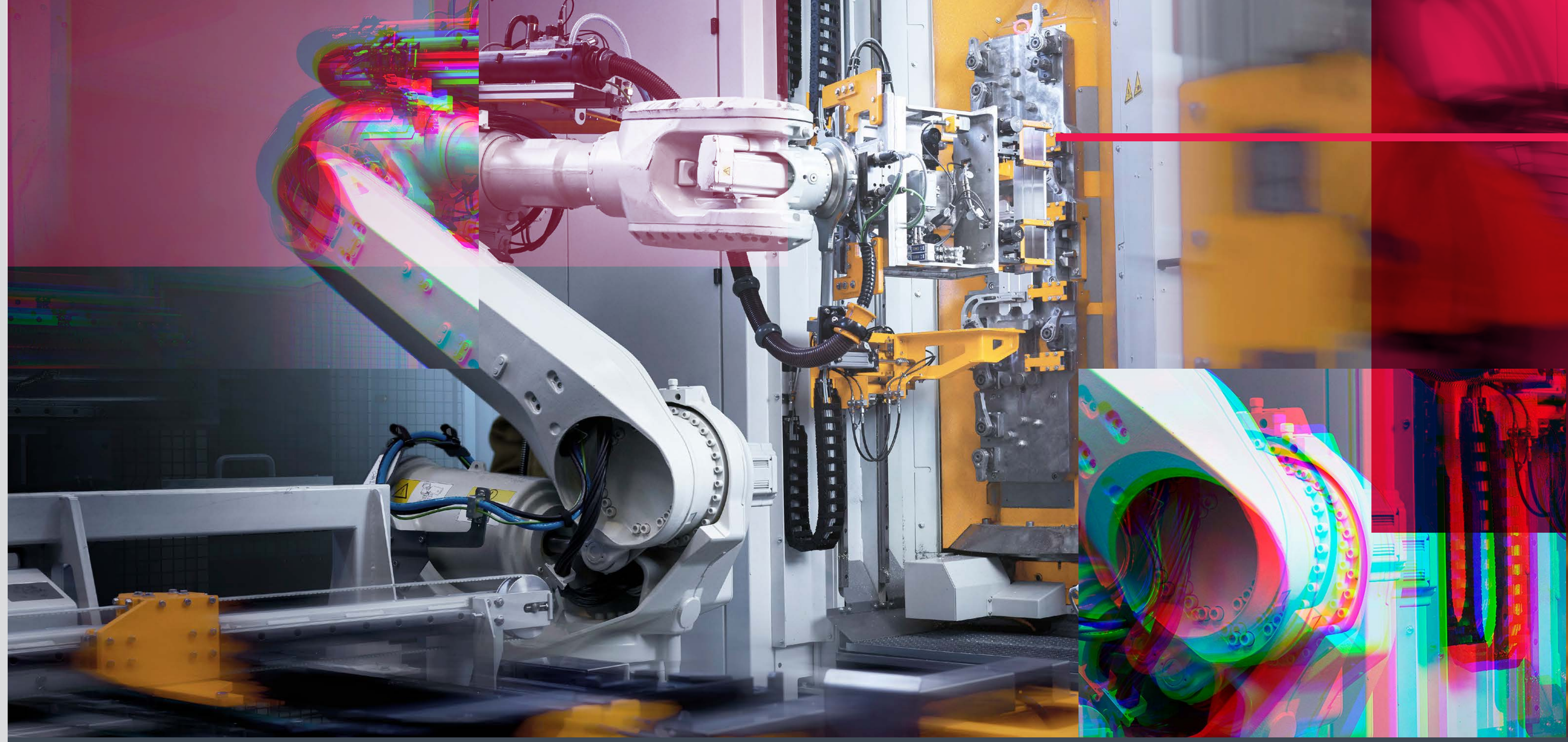


Figure 27: Risky services and protocols in a manufacturing OT environment



Risk snapshot of real-world OT deployment

Industry: Manufacturing

Total OT devices: **17,000+**

Total sites: **40+**

Devices per site with end-of-life (EOL) Windows OS: **500+ typically with known vulnerabilities**

Unauthorized/blocked network connections: **67% of total**

Size of internal attack surface (East-West): **equal to external, internet-facing attack surface**

Proportion of high-risk connections (risky services and protocols): **23.2%**

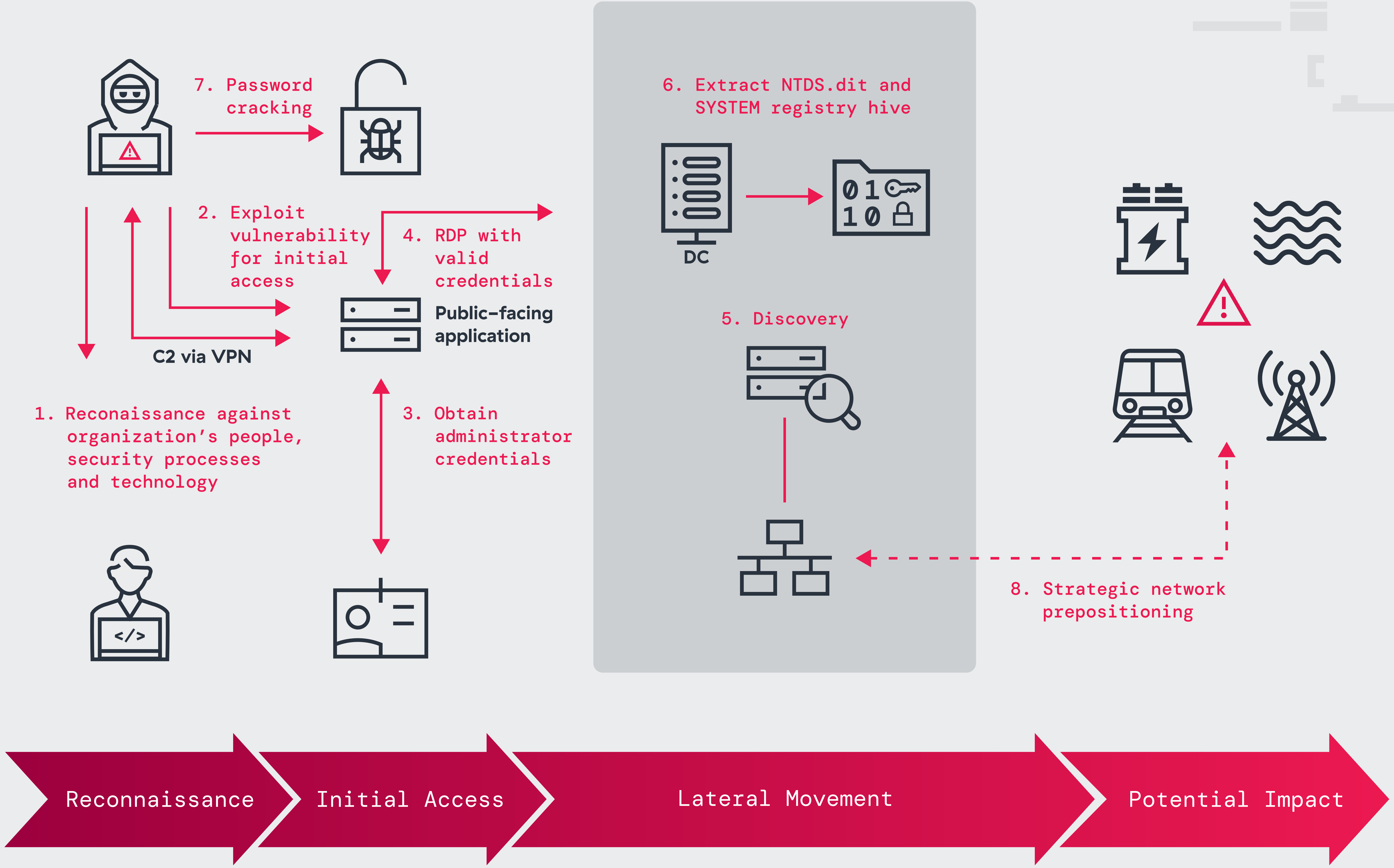
Research Highlights

Volt Typhoon infiltrates routers and positions itself to potentially disrupt infrastructure

Targeted device: Routers

Malware: Volt Typhoon

Volt Typhoon is a state-sponsored cyber campaign attributed to the People's Republic of China (PRC). Active since at least May 2023, it has been targeting US critical infrastructure with the potential for significant disruption.[6] The impact of this activity, ongoing through August 2024, could be severe, as these intrusions are not merely about espionage but are believed to be pre-positioned for potential destructive cyberattacks, especially during geopolitical tensions or conflicts. Such disruptions could lead to failures in critical infrastructure systems, causing widespread harm to both public safety and national security.



7. Password cracking
2. Exploit vulnerability for initial access
4. RDP with valid credentials
Public-facing application
C2 via VPN
1. Reconaissance against organization's people, security processes and technology
3. Obtain administrator credentials
6. Extract NTDS.dit and SYSTEM registry hive
DC
01
10
5. Discovery
8. Strategic network prepositioning
Reconaissance
Initial Access
Lateral Movement
Potential Impact

Figure 28: How a Volt Typhoon attack works

[6] CISA, Joint Cybersecurity Advisory, February 7, 2024.

How it works

1. **Initial reconnaissance:** Volt Typhoon actors conduct extensive reconnaissance to understand the target organization's network architecture, operational protocols, and security measures, as well as identify key IT staff to customize their attacks.

2. **Initial access:** The actors gain access to the target's IT network by exploiting known or zero-day vulnerabilities in public-facing network appliances such as routers, VPNs, and firewalls. Once they gain initial access, the threat actors will typically connect to the target network via VPN to carry out privilege escalation and beyond.

3. **Privilege escalation:** The threat actors focus on obtaining administrator credentials within the network. This is often achieved by exploiting privilege escalation vulnerabilities in the operating system or network services. In some cases, credentials are obtained from insecurely stored data on compromised public-facing network appliances.

4. **Lateral movement:** Using compromised administrator credentials, the actors move laterally across the network, targeting the domain controller (DC) and other critical devices using remote access services like Remote Desktop Protocol (RDP). The threat actors perform extensive discovery within the network using "living off the land" tactics, such as using legitimate tools like PowerShell to remain undetected.

5. **Data exfiltration and persistence:** Volt Typhoon actors often extract the Active Directory database (NTDS.dit) from the DC using command-line utilities like vssadmin to create shadow copies of the volume hosting the NTDS.dit file. They likely use offline password cracking techniques to decrypt the hashes found in the NTDS.dit file, enabling them to gain elevated access.

6. **Identifying targets:** Volt Typhoon actors focus on identifying and accessing OT assets critical for infrastructure, such as HVAC and energy controls. They test access using default or compromised credentials to prepare for potential disruptions.

Real-life harmful impact

- **Infiltration of OT systems and potential physical manipulation:** In at least one confirmed case, Volt Typhoon actors moved laterally within the network to gain access to OT systems, where they are positioned to disrupt control systems. This capability could allow them to:
  - Manipulate critical infrastructure operations like energy distribution, transportation systems, and water treatment processes
  - Access and manipulate HVAC systems in server rooms, which could lead to overheating and hardware failures
  - Access camera surveillance systems

- **Compromise of smaller critical service providers:** Many victims of this campaign include smaller organizations that have limited cybersecurity resources, yet provide essential services to larger organizations or key geographic areas. The compromise of these smaller providers could have a cascading effect, disrupting services on a much broader scale.

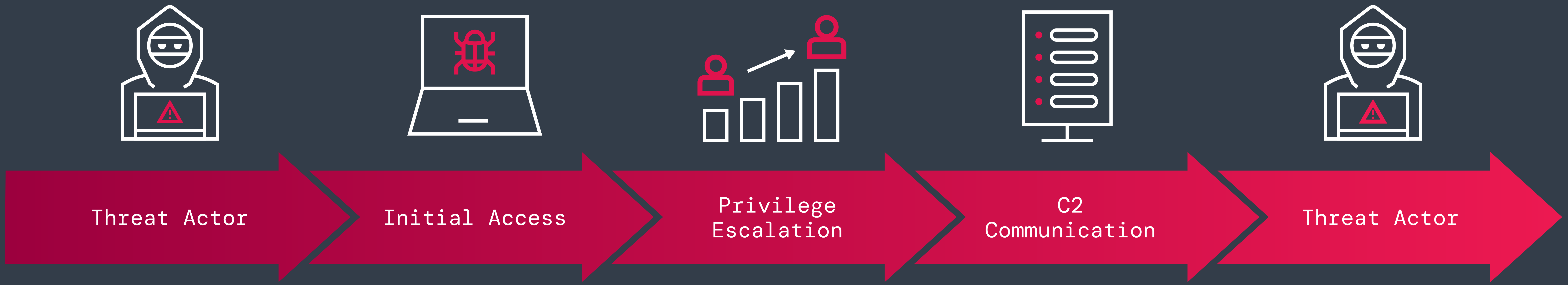
- **Long-term persistent threat:** The ongoing nature of this campaign means the threat is persistent, with the actors maintaining access over extended periods. This allows them to conduct long-term surveillance, gather intelligence, and potentially time their attacks to maximize impact, particularly during periods of heightened vulnerability, such as natural disasters or geopolitical tensions.

Pandora hijacks set-top boxes for cyberattacks

Targeted device: Set-top boxes
Malware: Mirai

Pandora, a variant of the notorious Mirai botnet, has been identified as a significant threat targeting inexpensive Android-based TV sets and TV boxes.[7] This is a considerable threat as set-top boxes generate the largest share (17%) of traffic in the Zscaler cloud. This malware has been observed leveraging set-top boxes to execute distributed denial-of-service (DDoS) attacks. The Pandora botnet infiltrates devices through malicious firmware update or pirated video streaming applications, exploiting vulnerabilities in Android TV devices like Tanix TX6, MX10 Pro 6K, and H96 MAX X3.

[7] The Hacker News, **Mirai Botnet Variant 'Pandora' Hijacks Android TVs for Cyberattacks**, September 7, 2023.



Threat Actor

Attacker publishes malicious firmware updates to website.

Initial Access

The attacker gains initial access to the system via a malicious firmware update/pirated video application

Privilege Escalation

Once in the system, the attacker gains higher level permissions and replaces host files with rogue variant.

C2 Communication

The malware makes contact with the attacker-controlled c2 server to mount attacks.

Threat Actor

Attacker uses devices under control to launch large scale DDOS attacks.

Figure 29: How a Pandora attack works

How it works

1. **Initial access:** Pandora gains access to Android-based TV sets primarily through malicious firmware updates and pirated streaming applications. Malicious firmware updates, distributed from websites using publicly available Android Open Source Project test keys, install the malware's backdoor during the firmware installation process. Pirated streaming apps like Latino VOD, Tele Latino, UniTV, and YouCine TV are used to trick users into installing malware under the guise of providing free content.

2. **Privilege escalation:** Once installed, Pandora's components are activated. For firmware-based infections, Pandora embeds itself in the boot image, ensuring it persists through system restarts. For app-based infections, the installed app launches a background service called GoMediaService, which then installs Pandora with elevated privileges, allowing it to operate with increased control over the device.

3. **Command-and-control (C2):** Pandora establishes a connection to a remote server, modifies the device's hosts file to redirect traffic, and receives commands to execute distributed DDoS attacks using TCP and UDP protocols. The malware also opens a reverse shell, enabling further control over the compromised device. This setup allows Pandora to leverage infected TV boxes to perform large-scale DDoS attacks, impacting online services and potentially causing disruptions.

Real-life harmful impact

- **Widespread disruption:** Pandora's use of TV set-top boxes, a very common and inexpensive device type, for DDoS attacks positions it to cause significant downtime and service loss for a large number of users.

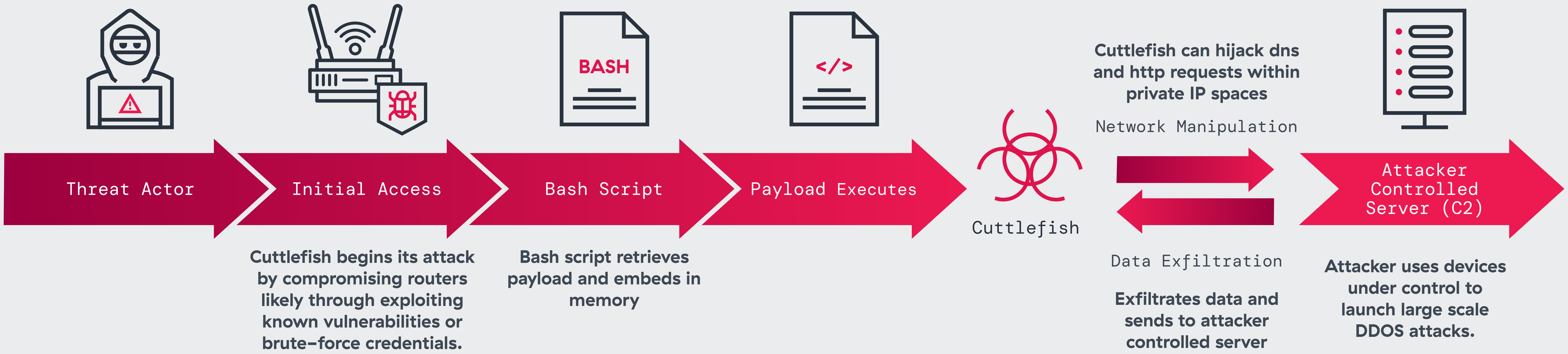
- **Extensive impact on users:** The abuse of common low-cost devices by Pandora can result in widespread user impact, including potential data breaches and security compromises.

New Cuttlefish malware infects routers to monitor traffic for credentials

Targeted device: Router
Malware: Cuttlefish

Cuttlefish malware targets enterprise-grade and small office/home office (SOHO) routers.[8] Believed to be active since July 2023, this malware infiltrates routers to monitor and steal authentication information by setting up a proxy or VPN tunnel.

[8] Bleeping Computer, New Cuttlefish malware infects routers to monitor traffic for credentials, May 1, 2024.



Cuttlefish begins its attack by compromising routers likely through exploiting known vulnerabilities or brute-force credentials.

Bash script retrieves payload and embeds in memory

Cuttlefish can hijack dns and http requests within private IP spaces

Exfiltrates data and sends to attacker controlled server

Attacker uses devices under control to launch large scale DDOS attacks.

Figure 30: How a Cuttlefish attack works

How it works

1. **Initial access:** Cuttlefish begins by compromising routers, likely through exploiting known vulnerabilities or brute-force credentials. Once the router is breached, a bash script is deployed to gather important system data such as directing listings, running process, and active connections. The primary Cuttlefish payload is then downloaded and loaded directly into memory, which allows it to evade detection as the original file is deleted from the system.

2. **Data and credential exfiltration:** Cuttlefish operates by monitoring all network traffic passing through the compromised router. It uses a packet filter to sniff out specific credentials and tokens, particularly those tied to public cloud services like AWS and CloudFlare. Once these credentials are captured, they are logged and exfiltrated to the threat actor's C2 server using a VPN or proxy tunnel.

3. **Network manipulation:** Beyond credential exfiltration, Cuttlefish can hijack DNS and HTTP requests within private IP spaces. This allows the malware to redirect traffic to threat actor-controlled infrastructure, manipulating internal communications and introducing additional malicious payloads. This hijacking can also grant attackers access to secured resources within private networks that are not otherwise reachable through the public internet.

Real-life harmful impact

- **Data breaches and network disruption:** Cuttlefish's ability to steal credentials from routers, particularly those linked to cloud services, poses a serious risk of data breaches and unauthorized access to sensitive resources like:

  - Confidential data—customer records, PII, intellectual property, and trade secrets
  - Cloud resources—services and applications hosted on platforms like AWS, AliCloud, and Digital Ocean
  - Internal network systems—routers, servers, and communication systems

- **Long-term persistent threat:** By evading detection through memory-resident payloads and manipulating traffic, Cuttlefish can maintain a long-term presence within compromised networks. This persistent threat can lead to ongoing security risks, including continuous data exfiltration and the potential for further exploitation of the compromised systems.

2025_ Predictions

1. IoT and OT devices will remain primary threat vectors

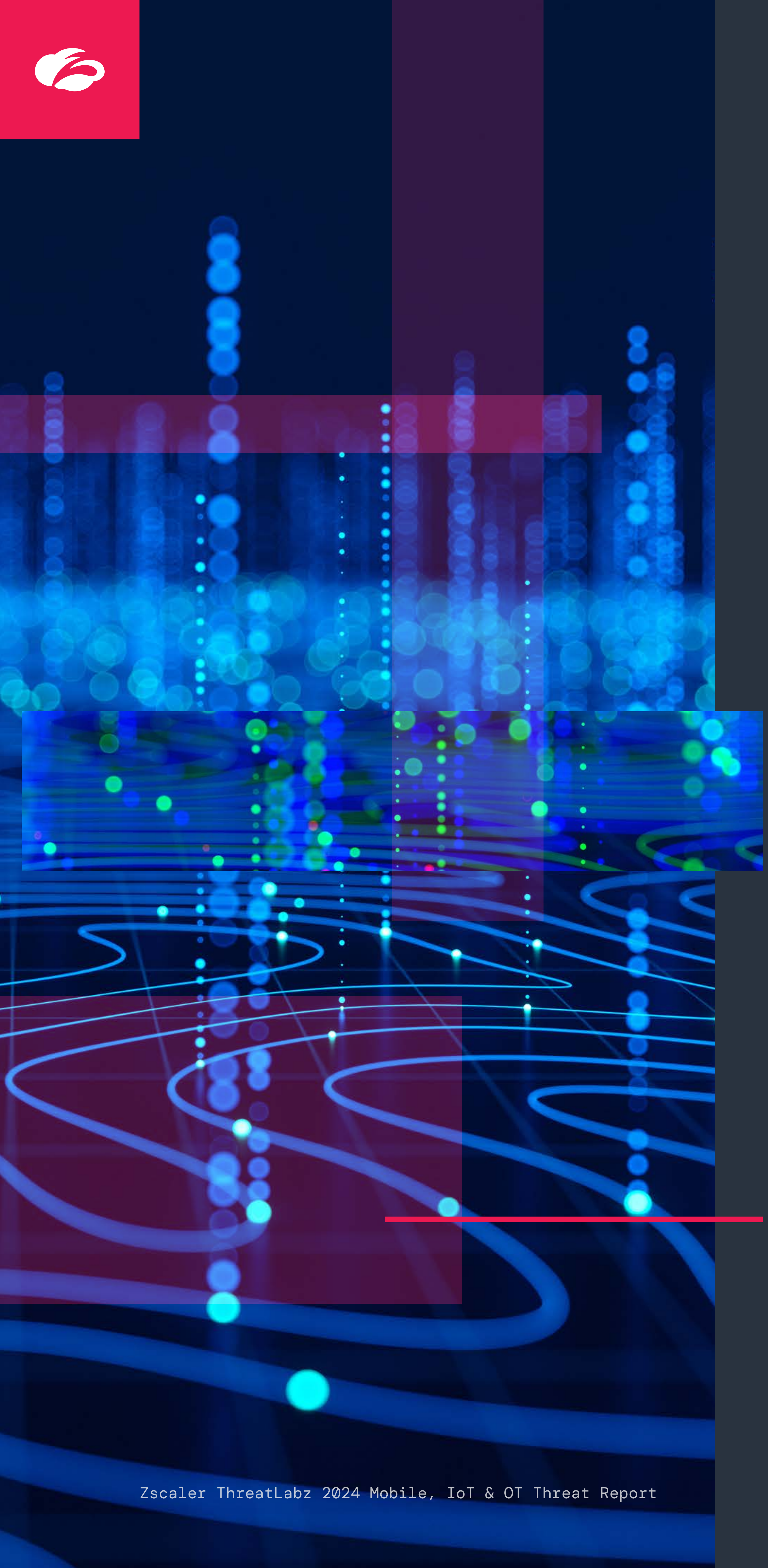
With a significant 45% increase in IoT malware and a series of successful attacks targeting IoT assets, it's clear that these devices remain a favored entry point for cybercriminals. A single infected IoT device can compromise the entire routable enterprise network—and IoT devices typically lack inbuilt security controls. In response, enterprises will intensify efforts to minimize the attack surface of internet-connected IoT and OT devices. This includes improving security measures that control how these devices connect to larger organizational networks, including by segmenting every device and authorizing every transaction.

2. Manufacturing will remain a top target for IoT attacks, including ransomware

For the second consecutive year, the manufacturing sector has emerged as the industry most vulnerable to IoT attacks, while also being highly targeted by mobile attacks, where it ranks third. The persistent targeting is likely due to the critical nature of interconnected environments in manufacturing operations, which continue to expand—growing the attack surface and making it lucrative to disrupt these companies through ransomware and other malicious exploits.

3. AI will increasingly be used to create believable phishing campaigns targeting mobile users

AI already contributes to building convincing phishing campaigns aimed at mobile users, making already difficult-to-detect phishing attacks indistinguishable from legitimate sites. This will expand to a broad range of phishing attacks, including the creation of simple QR code attacks, fake apps and landing pages, as well as AI-generated smishing and vishing attacks to create additional legitimacy among users. Users will need to be trained on how AI can be used in mobile attacks, and organizations will need to ensure users are accessing only legitimate applications on their devices.



4. Zero trust device segmentation will become a top security priority for IoT and OT systems, starting with critical infrastructure

As threats evolve, so must enterprise approaches to network security. Given that unsecured and agentless IoT/OT devices can be easily compromised, enterprises will work to bring zero trust microsegmentation to these networks. Here, enterprises will work to isolate and segment every IoT and OT device into networks of one. This strategy is essential for securing agentless devices and legacy servers, while preventing lateral movement and giving enterprises east-west security and control. Given that IoT/OT threats are only poised to grow, this approach will gain significant momentum in the coming year.

6. Private 5G ecosystems with zero trust will become a key strategy for IoT and OT connectivity

Enterprises have already begun to adopt private 5G and edge ecosystems to improve connectivity in IoT, OT, and mobile environments. However, these networks can be attractive targets because a single infected IoT device can compromise the entire routable enterprise network—and IoT devices typically lack inbuilt security controls. As a result, enterprises will work to minimize this risk by deploying zero trust solutions in the 5G core. This approach will enable device connectivity while minimizing the attack surface, authorizing every device connection, and ensuring that IoT/OT and mobile devices are not on the same routable network as enterprise applications in the data center, cloud, or the edge.

5. AI will play a critical role for IoT and OT defenders

AI tools will transform how IoT and OT security is managed. Overcoming the hype, AI will help defenders automate critical functions, such as discovering IoT and OT assets in complex environments and enabling IoT/OT segmentation and control at scale. AI will also enable enterprises to better align and adopt IoT/OT security policies to real-time risks, such as the threat of ransomware or malware. This will allow defenders to take back control over IoT and OT environments and better prioritize their efforts to drive greater security impact.

7. The trend of security platform consolidation will extend to IoT and OT environments

As organizations seek to streamline security operations and reduce complexity, the trend toward security platform consolidation will extend to the realm of IoT and OT. This shift will lead to the integration of numerous security tools and functions into unified platforms that can drive zero trust security, device segmentation, and comprehensive visibility and control across diverse and distributed IoT and OT environments. Such consolidation will make it easier to manage IoT/OT security and enforce consistent security policies across the entire enterprise digital footprint—from private applications in the cloud to mobile devices on the factory floor.

IoT and OT Security Best Practices

With state-sponsored actors actively targeting OT systems and critical infrastructure, alongside the rapid 45% YoY growth in IoT malware, organizations should adopt recommended practices to keep their devices and networks safe from exploitation and lateral movement.

Zscaler ThreaLabz has created a set of best-practice guidance that enterprises and public organizations can follow to mitigate cyberthreats and improve their IoT/OT security posture.

- □ **Work to discover, classify, and inventory IoT and OT assets.** Prioritize gaining holistic visibility into the IoT and OT attack surface—which includes discovering, classifying, and inventorying both managed and unmanaged or "shadow" devices. This allows defenders to better understand and defend against IoT/OT threats while prioritizing remediation.
- □ **Collect and monitor network logs for user access, application, and system event activity.** Continuously monitor network logs for key indicators that should be investigated, particularly given that threat actors like Volt Typhoon can have significant dwell time inside organizational systems.
- □ **Enable phishing-resistant multifactor authentication (MFA).** Change default passwords and protect administrative credentials while enabling phishing-resistant forms of MFA, such as FIDO2 or biometric-based authentication.
- □ **Maintain vigilant patching for critical vulnerabilities and internet-facing systems.** Unpatched, internet-connected assets are the most vulnerable to threat actors. Enable automated updates and quickly patch IoT and OT assets to minimize the risk that new vulnerabilities may present. Use AI-driven threat intelligence platforms to prioritize and manage security patches effectively.
- □ **Enforce zero trust device segmentation for IoT and OT assets.** Deploy granular device-to-application, user-to-application and application-to-application segmentation, brokering access via least-privileged access controls to eliminate lateral movement, minimize data exposure, and enhance your overall security posture.
- □ **Enable privileged remote access to OT systems.** As previously air-gapped OT systems become connected to the internet and converge with traditional enterprise IT networks and services, it's important to secure third-party vendor and remote access to OT systems. Critically, avoid the use of VPNs, which can cause friction and are easier for threat actors to exploit. Instead, enable zero trust, outbound-only connectivity that leverages fully isolated RDP and SSH sessions between users and the OT system.
- □ **Inspect encrypted traffic.** Attacks commonly use encrypted channels, which often are not inspected, making it easy for even moderately sophisticated attackers to bypass security controls. It's essential to inspect all encrypted traffic to prevent attackers from compromising systems.
- □ **Follow Zscaler ThreatLabz research feeds.** Get regular insights on the latest cyberthreats and developments, including published indicators of compromise (IOCs) and MITRE ATT&CK mappings. This information can be used to train employees, improve security posture, and help prevent IoT attacks.

  X (formerly Twitter) @ThreatLabz | ThreatLabz security research blog

Mobile Security Best Practices

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 cyber threats. 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 connectivity.** 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.

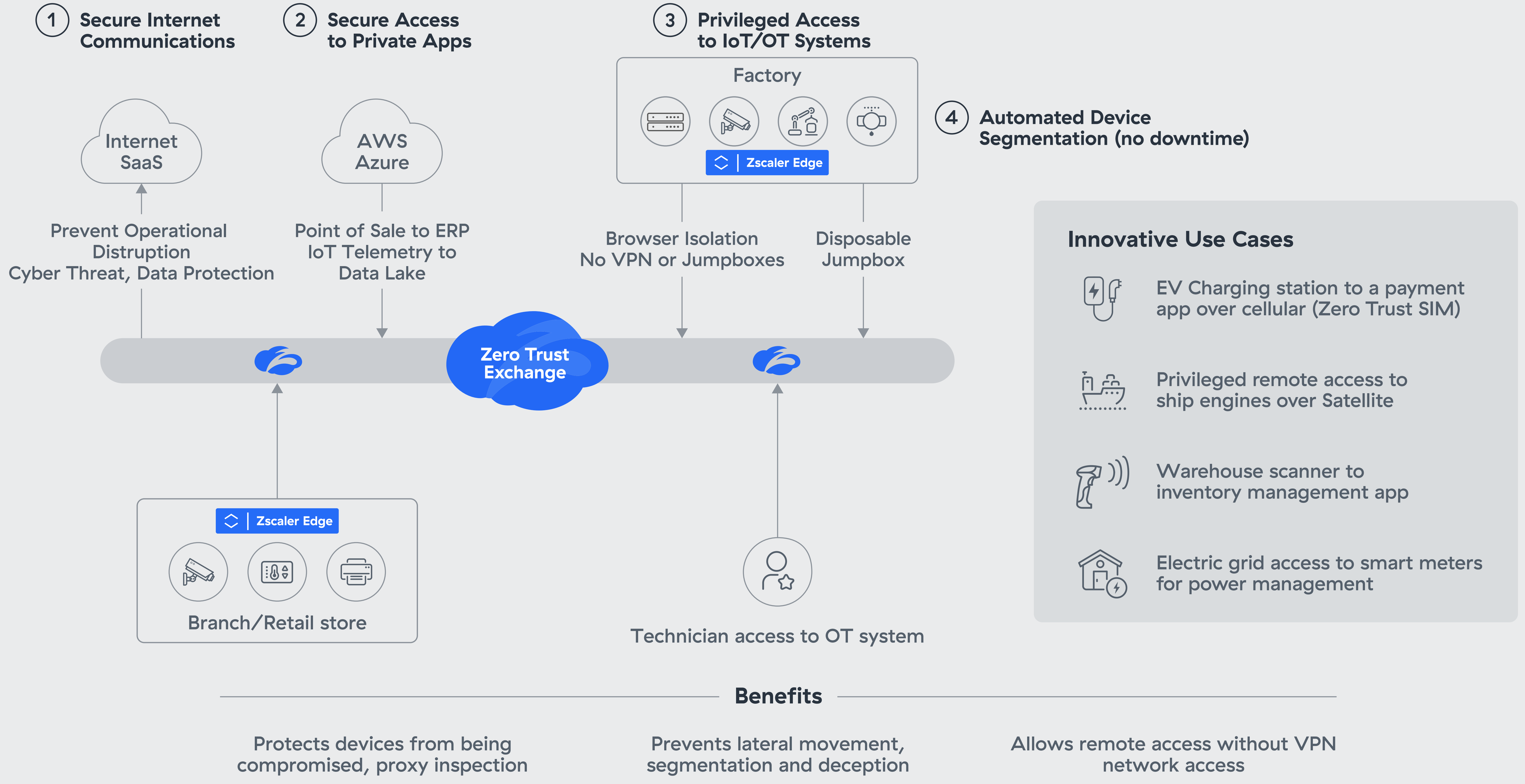
How Zscaler Secures IoT and OT

As enterprises connect to a rapidly growing set of IoT devices and critical OT systems, they must prioritize secure connectivity and access to them. Despite being business-critical in offices, factories, and branch or retail locations, these devices represent a vast and growing attack surface for cybercriminals to exploit. Indeed, threat actors frequently move laterally from these devices to traverse enterprise networks, deploy malware and ransomware, or other compromise critical OT systems. Yet these devices and networks are rarely designed with security in mind, and enterprises typically lack visibility into this known and unknown attack surface—much less achieve zero trust segmentation between devices. In reality, this is impossible using yesterday's security and networking technologies.

With IoT attacks up 45% year over year, protecting valuable IoT and OT assets is an imperative to secure the enterprise.

Zscaler IoT Device Visibility

Zscaler IoT Device Visibility provides a complete view of all IoT devices, servers, and unmanaged user devices across your organization. Automated discovery of IoT devices, continuous monitoring, and AI/ML classification eliminate blind spots to provide a complete picture of your IoT landscape and reduce administrative burden. It enables organizations to implement IoT across the business to increase productivity and business agility with the confidence that their devices are secure. Zscaler customers can run an IoT Discovery Report through the Analytics dashboard in Zscaler Internet Access.



1 Secure Internet Communications

2 Secure Access to Private Apps

3 Privileged Access to IoT/OT Systems

4 Automated Device Segmentation (no downtime)

Factory

Zscaler Edge

Internet SaaS

AWS Azure

Prevent Operational Distruption
Cyber Threat, Data Protection

Point of Sale to ERP
IoT Telemetry to Data Lake

Browser Isolation
No VPN or Jumpboxes

Disposable Jumpbox

Zero Trust Exchange

Zscaler Edge

Branch/Retail store

Technician access to OT system

Innovative Use Cases

- EV Charging station to a payment app over cellular (Zero Trust SIM)
- Privileged remote access to ship engines over Satellite
- Warehouse scanner to inventory management app
- Electric grid access to smart meters for power management

Benefits

Protects devices from being compromised, proxy inspection

Prevents lateral movement, segmentation and deception

Allows remote access without VPN network access

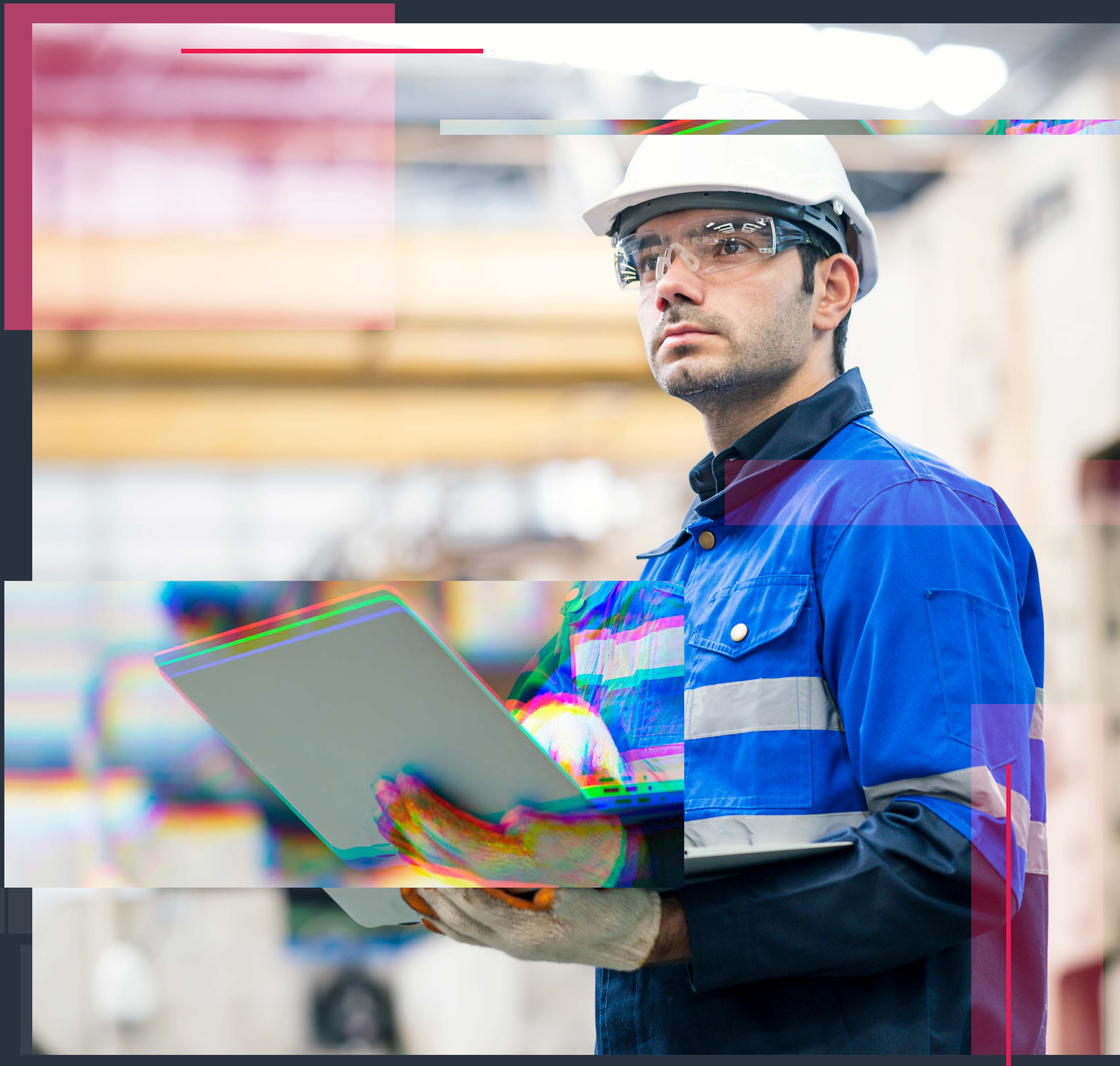
Figure 31: Zscaler for IoT and OT offers four areas of functionality to improve security, productivity, and digital experience

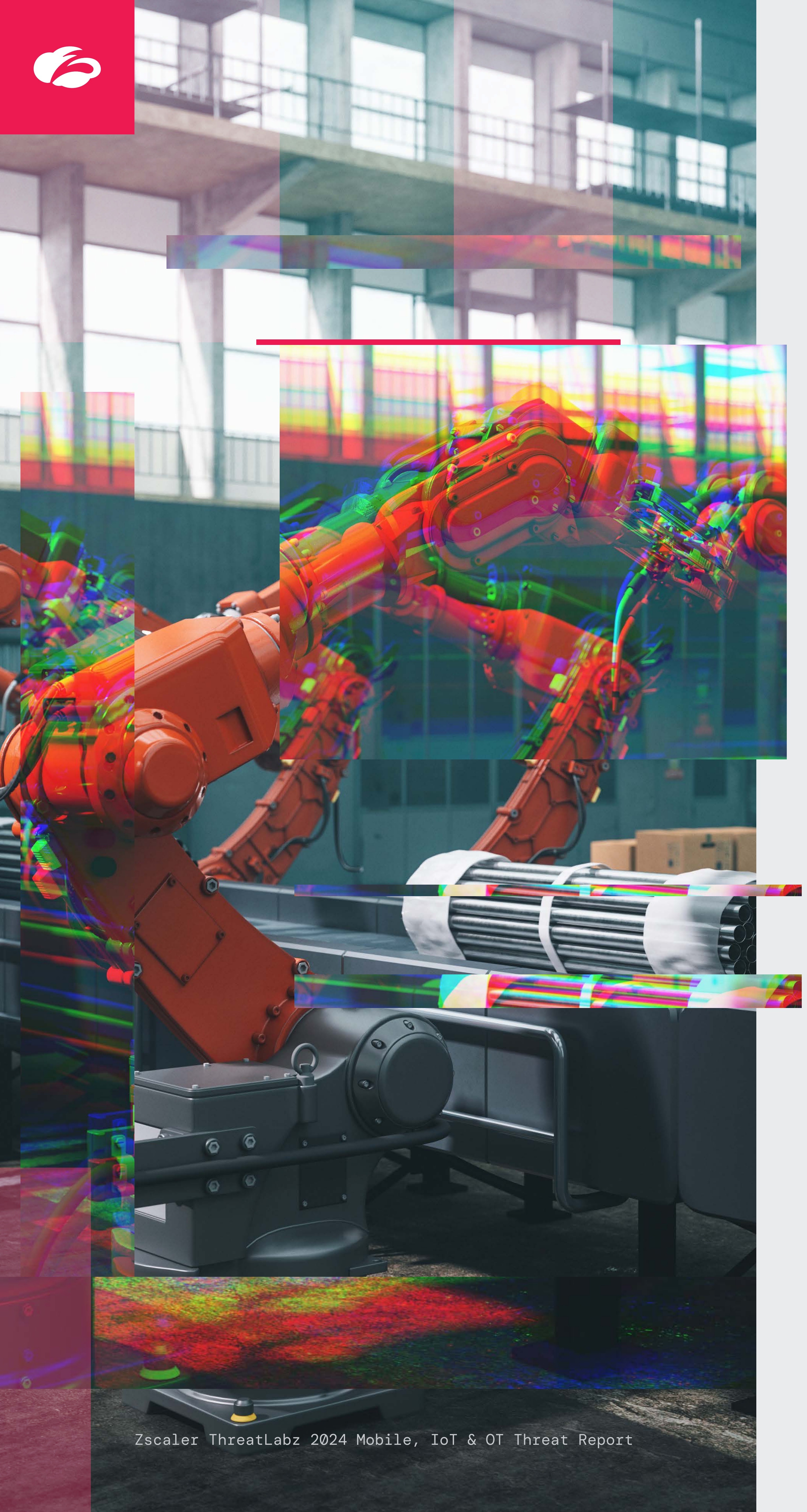
Bringing Zero Trust Inside the Branch and Factory

Zscaler for IoT and OT enables enterprises to reduce cyber risk while embracing IoT and OT connectivity to drive business agility and increase productivity. Powered by the Zscaler Zero Trust Exchange™, these capabilities protect IoT devices against compromise and prevent lateral movement with device segmentation and deception, all while allowing for remote access to OT systems without risky VPN connectivity.

Zscaler for IoT and OT provides automatic discovery, classification, and inventory of IoT devices with continuous east-west traffic visibility, while delivering security across four critical areas:

1. **Secure internet communications:** Secure IoT and OT connectivity between the internet and SaaS applications and branch or retail locations. Enable inline, proxy-based cyberthreat and data protection while preventing any operational disruption.
2. **Secure access to private apps:** Secure private application access with inside-out IoT connectivity to your private applications, such as point of sale (PoS) devices to ERP systems, or warehouse scanners to inventory management applications.
3. **Privileged access to IoT/OT systems:** Enable privileged, zero trust remote access for technicians and third-parties to critical systems using browser isolation or a disposable jumpbox, with no need for VPN or traditional jumpboxes.
4. **Automated device segmentation:** Enforce zero trust and eliminate lateral movement without the need for endpoint agents. With Zero Trust Device Segmentation, isolate and fully segment agentless IoT/OT devices into a secure "network of one", including legacy servers and headless machines—without business disruption or any software, east-west firewalls, or NAC required.

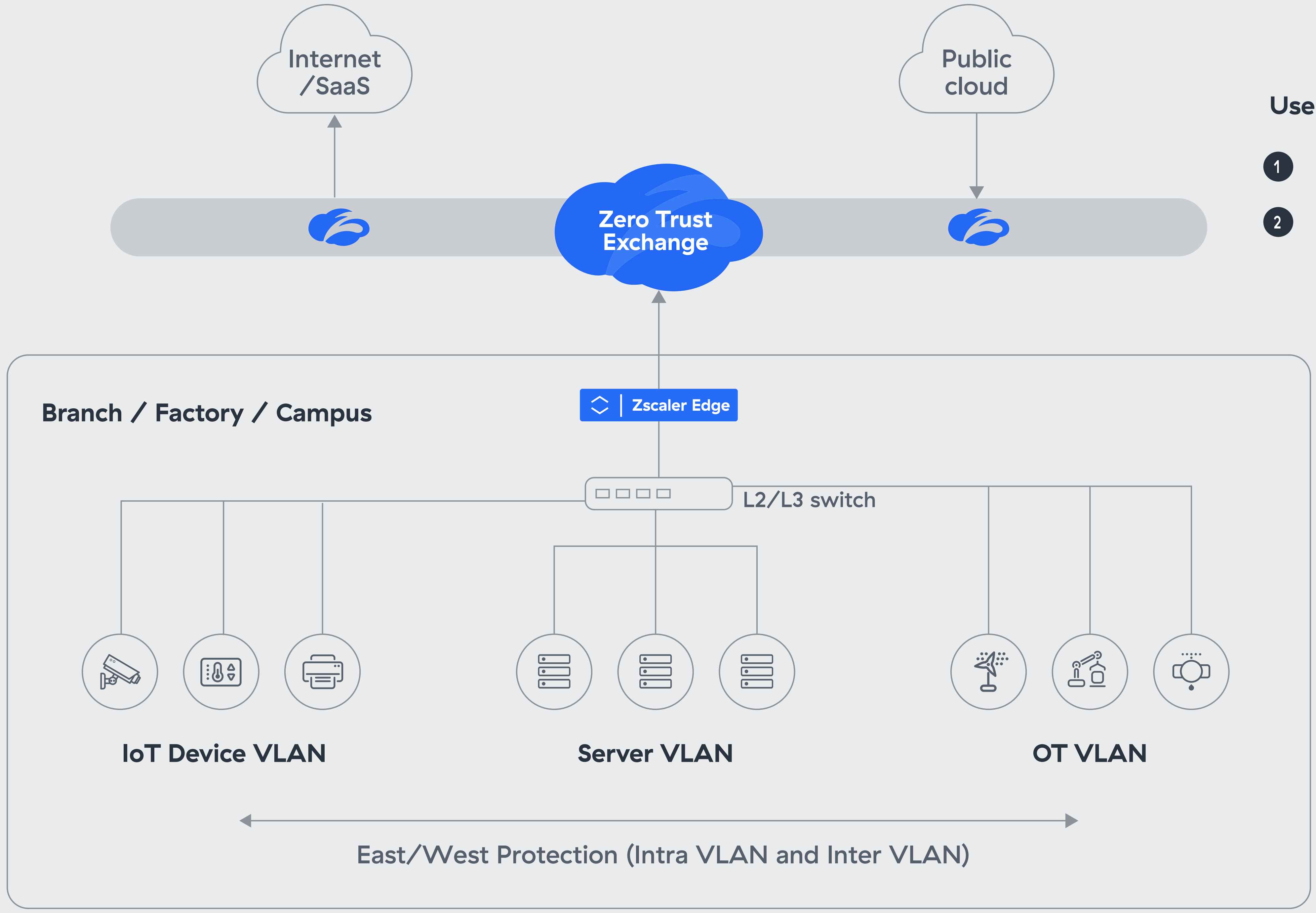




Zero Trust Device Segmentation

Zscaler Edge

- ✓ L3 Gateway & DHCP Proxy
- ✓ Automated device discovery and clasification
- ✓ Zero Trust Device Segmentation (NAC & East West Firewall Replacement)



Use Cases

1. IoT/OT segmentation
2. IT segmentation without firewalls/NAC/ACL

Benefits

- ✓ Prevents lateral threat movement
- ✓ No agents, no VLAN changes
- ✓ Deployable in hours

What gets eliminated ✗ East/West Firewalls ✗ NAC ✗ Branch DHCP ✗ Expensive Switches

Figure 32: Zscaler Device Segmentation enables enterprises to eliminate lateral movement with no need for endpoint agents

How Zscaler Secures Mobile Access

Users can now work from anywhere, with mobile access to the internet, SaaS apps, and private applications, whether in the cloud or the data center. To enable secure hybrid work and provide seamless access to any application, enterprises need to retire network-centric approaches that slow productivity and leave organizations vulnerable to lateral movement. Instead, they must embrace zero trust transformation that enables secure remote access from any user device to any application, from any location.

Digital Transformation Requires Zero Trust Connectivity

Zscaler Client Connector™ is a lightweight agent that enables fast, seamless zero trust connectivity for user endpoints to the internet, SaaS, and private enterprise applications. Securing smartphones, laptops, and tablets, Client Connector encrypts and forwards mobile traffic to the Zero Trust Exchange, helping secure access for endpoints while enabling the same zero trust policies to follow users regardless of their device, location, or the application accessed.

Client Connector delivers comprehensive zero trust security

SECURITY FOR ANY ACCESS

Client Connector facilitates seamless zero trust connectivity to the internet, SaaS applications, and private apps in the cloud and the data center.

SECURITY FOR ANY USER DEVICE

Client Connector supports laptops, smartphones, and tablets, and runs on Windows, macOS, iOS, Android, Linux, and ChromeOS.

PROTECTION FOR ENDPOINT DATA

Zscaler Endpoint DLP uses Client Connector to stop data loss via leakage channels such as removable storage, printing, and personal cloud storage.

USER EXPERIENCE MONITORING

Zscaler Digital Experience™ (ZDX) leverages Client Connector to gain valuable insight into app, network, and device performance, accelerating issue resolution.

CYBERCRIMINAL DECEPTION

Zscaler Deception uses Client Connector to deploy decoy passwords, cookies, sessions, and app bookmarks on endpoints, luring attackers.

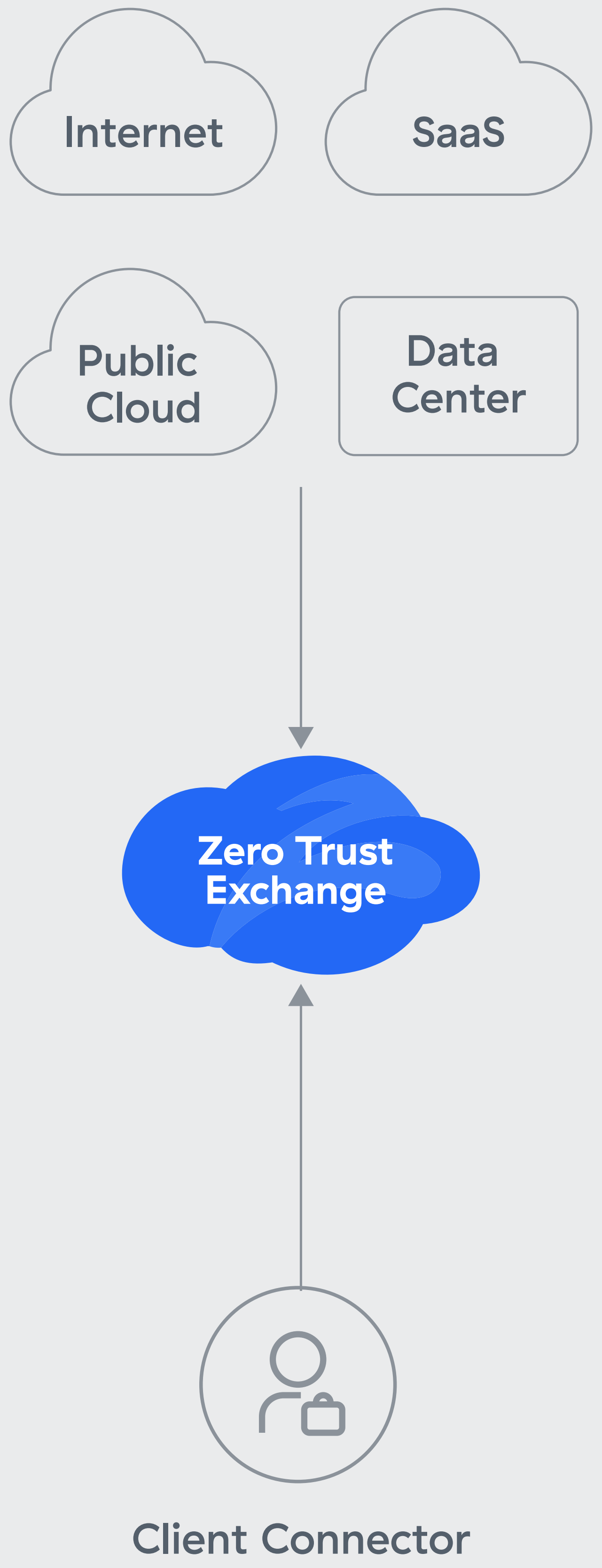


Figure 33: Zscaler Client Connector enables seamless zero trust connectivity from user endpoints to the internet, SaaS applications, and private applications in the cloud or data center

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 2023 and May 2024. 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 2024 to May 2024 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 2023 to May 2024 included

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

About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, **research.zscaler.com**.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ 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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit **www.zscaler.com.**

zscaler™ | Experience your world, secured.™