CUJOAI

CYBERSECURITY REPORT

2023

Table of Contents

EXECUTIVE SUMMARY

Executive Summary

Latest data from CUJO AI Labs shows that, every month, more than 62% of households in North America and Europe are exposed to threats that can be prevented by their Network Service Providers. Of the households affected, 59% have more than one device exposed to a cybersecurity threat.

In just six months between April and October 2023, CUJO AI Sentry stopped close to 2 billion threats across tens of millions of home networks in North America and Europe. The scale of CUJO AI's deployments gives us a unique view of the consumer threat landscape, which includes botnet activities, malware, as well as adware or phishing campaigns.

Cybersecurity threats impacting consumers and their devices fall into two primary categories:

- **IP Reputation**, or connections to and from known malicious IP addresses, representing 47% of all threats.
- **Safe Browsing**, or attempts to access malicious websites, accounting for 53% of all threats.

Over 62% of all households attempted to visit malicious websites at least once every month. In July, this number reached a peak at 79%. In contrast, IP Reputation threats, which make up 47% of all threats, affected just 6% of home networks.

Attended devices, such as smartphones and computers, are more often (88% of threats) affected by Safe Browsing threats, while unattended devices (e.g., IoT devices) are mostly (87% of threats) affected by IP Reputation threats.

Unattended device security depends on their configuration, such as open ports.

Attended device security heavily depends on their usage patterns, digital literacy and hygiene.

Mobile devices (smartphones and tablets) are overwhelmingly (97% of threats) affected by Safe Browsing threats, which include malware distribution (55%), scams and phishing (31%), adware or spyware (6%), and other malicious websites. Some very prolific and widespread campaigns are using malvertising, adware, and other techniques to run their malicious activities as a business.

Network-attached storage devices are affected by over 150 times more threats than an average device. DVRs are attacked over 30 times more often than an average device. Our data shows that ports associated with HTTP/S are targeted frequently. These ports are often opened to access and manage the device. Disreputable IP addresses targeting consumer devices are often related to malware distribution (38%) and malicious scanning (28%).

CUJO AI Sentry is a multi-layer cybersecurity solution that Network Service Providers can deploy to protect every device on their end-users' networks.

INTRODUCTION

05

Introduction

This report covers threat data from real-life deployments of CUJO AI Sentry, a multi-layer cybersecurity solution for network service providers that runs on the end-user's home router and protects every device connected to the network.

The data used in this report shows that attended devices, such as smartphones and computers, and unattended Internet of Things (IoT) devices face different types of threats, as well as the categories of the threats to expose the targets and tactics used by malicious actors against consumers. The report further delineates the categories of these threats, shedding light on the specific strategies and tactics employed by malicious entities targeting consumers.

Unlike our latest IoT botnet report or the previous cybersecurity report, which delved deep into device types and brands under threat, this report focuses more on the variety of threat vectors that impact Internet users: adware campaigns, targeted ports, malicious websites, and botnets in our customers' networks between April 10 and October 10, 2023.

CUJO AI is currently deployed on more than 50 million networks across North America and Europe. It uses in-house machine learning algorithms in combination with industry-leading threat intelligence sources to identify, classify, and protect over 2 billion devices.

CUJO AI Sentry prevents a range of threats, including Safe Browsing events, where devices attempt to access malicious websites, and IP Reputation, where devices are probed by or attempting to connect to disreputable IP addresses, which includes malicious remote access attempts as well as participation in denial-of-service (DOS) attacks.

50 million
premises covered

2 billion
devices monitored

325 million
threats blocked every month

Glossary

A threat – a single event where an action by a malicious actor or dangerous behavior by the device or its user would affect a single device. Visiting a phishing website is a threat, as is getting a device probed for open ports from a known malicious IP address.

Safe Browsing threats – a category of threats that are encountered when browsing the web. This includes malware distribution, phishing, spam, and other malicious websites.

IP Reputation – a category of threats for attempted connections to and from IP addresses that are known for malicious behavior. This includes scanners, botnet command & control centers, malware-related addresses, among dozens of other categories.

OUTGOING
IP REPUTATION THREAT

an attempt to **connect to** a malicious IP address.

INCOMING
IP REPUTATION THREAT

an attempt to **connect from** a malicious IP address to a device on the protected network.

Threat index – a metric used in this report that combines threat data with precise device intelligence data from CUJO AI Explorer to expose which types of devices are affected by cybersecurity threats more (or less) often, on average.

Device intelligence – the industry-leading device detection and identification solution for network service providers that shows them precisely which devices are connected to a network and are affected by a particular threat.

CYBERSECURITY THREATS IN THE HOME

Cybersecurity Threats in the Home

CUJO AI stops hundreds of millions of threats every month. Our data shows that over 65% of all households were affected by at least a single threat each month in the period between April and October 2023. In July, this number peaked at 79% of all homes.

Most of these threats can be grouped into these major categories:

CUJO AI also prevents other types of threats, including participation in Denial-of-Service (DOS) attacks and compromised IoT devices, based on their behavior patterns. However, these make up just 0.03% of all threats stopped across millions of home networks protected by CUJO AI Sentry.

Safe Browsing and incoming IP reputation threats make up an overwhelming majority (over 99%) of all threats to consumer devices.

Our data shows that over 62% of households were affected by at least a single Safe Browsing threat in September. In the same period, only 5.51% of homes were exposed to at least one IP Reputation threat.

The following sections show how significant those numbers are, as relatively few consumers are impacted by close to half of all online threats! These end-users are a key demographic for network service providers, as they are most likely early adopters of smart home devices and IoT gadgets. On the other hand, the widespread exposure to malicious websites is symptomatic of a digital environment where consumers lose billions of dollars to scams every year.

Thanks to advanced cybersecurity solutions like CUJO AI Sentry, network service providers have the opportunity to create much safer and more efficient online experiences for their customers.

A Breakdown of All Threats Stopped by CUJO AI Sentry

The chart below includes all devices protected by CUJO AI Sentry, nevertheless, the types of threats that impact a particular device often depend on the device's type.

THREATS STOPPED BY CUJO AI

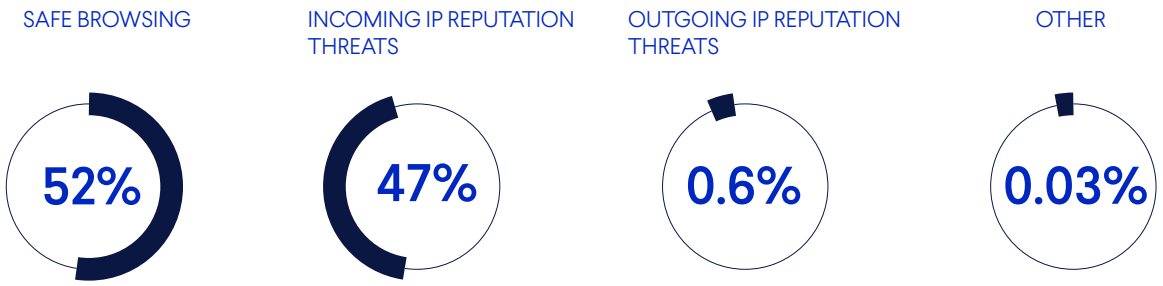


Figure 1 – Threats stopped by CUJO AI Sentry between April 11 and October 10, 2023.

Threats to Attended and Unattended Devices

We can group devices by the way their users interact with them:

> **Attended devices** are devices that have a screen and an easily accessible user interface. People actively use them to access various parts of the Internet. Users might notice when something is out of the ordinary (e.g., a device is compromised) sooner thanks to their familiarity with an attended device.

> **Unattended devices** are IoT devices that are usually set-it-and-forget-it. Most of these devices do not have large connectivity requirements for bandwidth or latency. Many have predetermined behavior patterns (e.g., some should only connect to a single server) and do not require the owner to get involved.

Thanks to CUJO AI Explorer, we can combine our threat data with device intelligence data to categorize billions of devices into dozens of distinct device types and expose the distribution of threats to those devices.

THREATS TO ATTENDED DEVICES

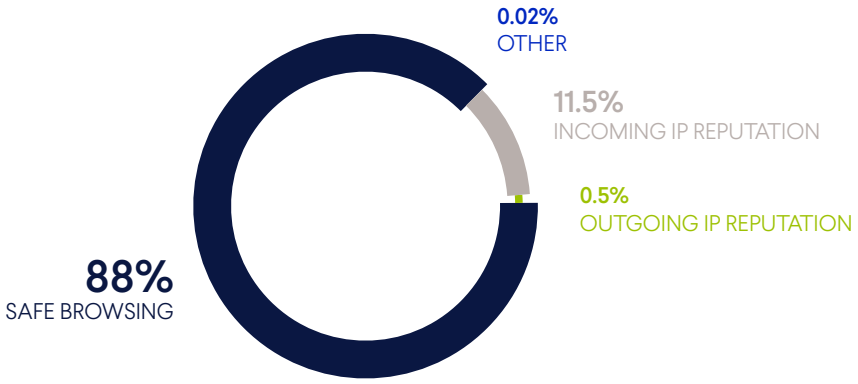


Figure 2 – Threats to attended devices stopped by CUJO AI Sentry between April 11 and October 10, 2023.

Threats affecting attended devices are overwhelmingly related to malicious websites. This is expected, as consumers use these devices to access the web. This is even more evident when we look at the types of threats affecting mobile devices. For more details on the threats to mobile devices, please refer to the "Mobile Device Threats" section.

Note: Figure 2 encompasses data for the following attended devices: laptops, desktop computers, smartphones, tablets, smartwatches, game consoles, and smart TVs.

THREATS TO UNATTENDED DEVICES

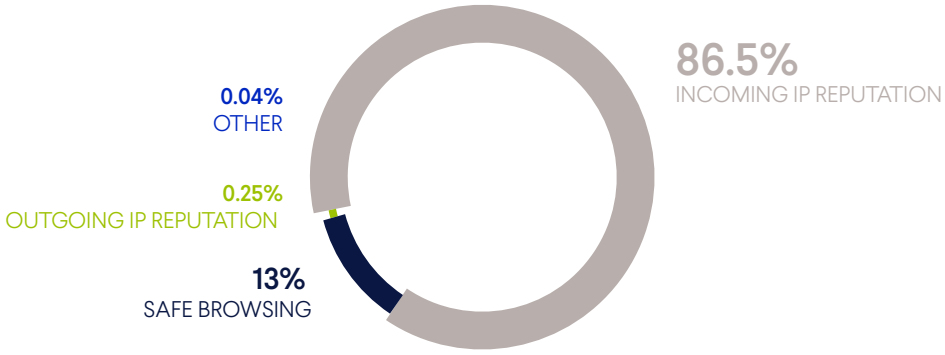


Figure 3 – Threats to unattended devices stopped by CUJO AI Sentry between April 11 and October 10, 2023.

Unattended devices mainly face threats from malicious IP addresses trying to connect to them. It's important to know that these threats can be things like network scans that might not necessarily harm the device. However, it's evident that IP Reputation threats, which make up 47% of all threats (as shown in Figure 1), predominantly target unattended devices.

Safe Browsing threats to unattended devices are likely an indication of compromised devices that are used as proxies by malicious actors to access websites.

For more details on the types of IP Reputation threats, please refer to the "IP Reputation Threats" section.

Mobile Device Threats

Mobile devices (smartphones and tablets) make up around half (49.8%) of all connected devices, according to CUJO AI's device intelligence data. Protecting these devices is especially important when we consider that their owners are likely to connect to multiple, potentially unsecured networks when outside the home.

THREATS TO MOBILE DEVICES

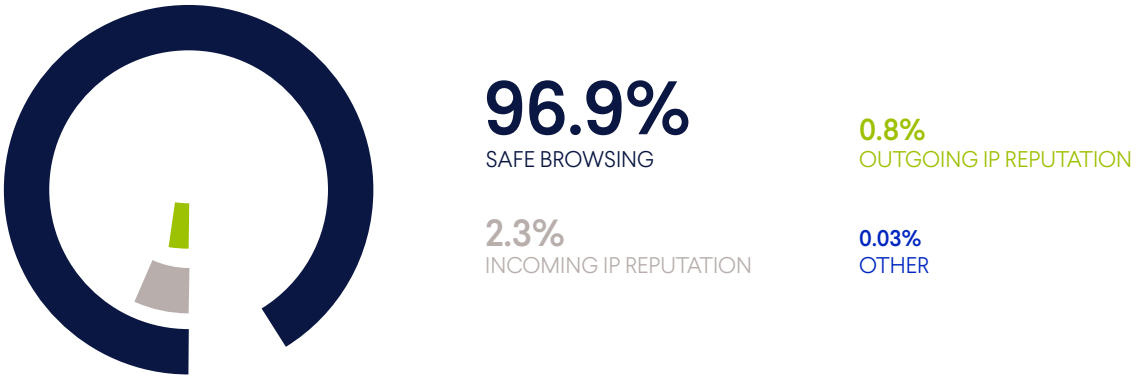


Figure 4 – Threats to mobile devices stopped by CUJO AI Sentry between April 11 and October 10, 2023.

As evidenced by the chart above, mobile devices are most often affected by their users' behavior. Since mobile devices rarely have ports opened to the Internet, they do not get attacked by disreputable IP addresses as often as other types of devices.

Since most threats to mobile devices stem from a user's browsing behavior and their app selection, it is extremely important to provide Safe Browsing protection to mobile devices when they are outside the protected home network. CUJO AI On The Move is a versatile SDK that network service providers can integrate into their native applications and extend CUJO AI's Safe Browsing protection to mobile devices across all networks.

Desktop and Laptop Computer Threats

Computers make up around 17.5% of all connected devices, according to our device intelligence data. These devices are versatile and can run a large variety of operating systems and software. This versatility is also reflected in their threat data.

THREATS TO DESKTOP AND LAPTOP DEVICES

Figure 5 – Threats to computers blocked by CUJO AI Sentry between April 11 and October 10, 2023.

Computers are targeted by incoming IP Reputation threats almost ten times more often than mobile devices. This is because a computer can have a suboptimal configuration, such as particular ports open for online gaming or peer-to-peer file sharing (e.g., for the BitTorrent protocol), which make it vulnerable to malicious actors.

We will discuss what sort of activities IP Reputation threats encompass, which ports are targeted most often, and what Safe Browsing threats consumers are most likely to encounter further in the report.

SAFE BROWSING THREATS

Safe Browsing Threats

As we've noted in the sections on attended devices, web browsing and the use of mobile applications greatly impact consumer cybersecurity. With close to 97% of all threats to mobile devices coming from malicious websites, the impact of browsing threats is significant, especially as it has an outsized impact on the largest segment of connected devices – smartphones.

Malicious websites come in many forms: some distribute malware, while others impersonate legitimate websites to steal the visitor's data, personal information, money, cryptocurrency and other Web3 assets.

Phishing websites are some of the most difficult threat vectors to stop, as they are usually active for only a very short time. In many cases, phishing campaigns have already ended before their domains are flagged by public threat intelligence sources.

CUJO AI Sentry uses machine learning algorithms to analyze previously unseen websites and alert users whenever they attempt to access a suspicious website. This use of artificial intelligence allows us to bridge the cybersecurity gap left by reactive cybersecurity solutions.

Safe Browsing Threat Breakdown

Our data shows that most Safe Browsing threats are related to malware and phishing campaigns. Social engineering, scams, and phishing campaigns are becoming more lucrative and widespread, and the Federal Trade Commission in the US assessed that consumers reported losing nearly $8.8 billion to fraud in 2022, an increase of more than 30 percent over the previous year. The FBI has also stated that Americans had lost even more – over $10 billion – to online scams in 2022.

SAFE BROWSING THREATS

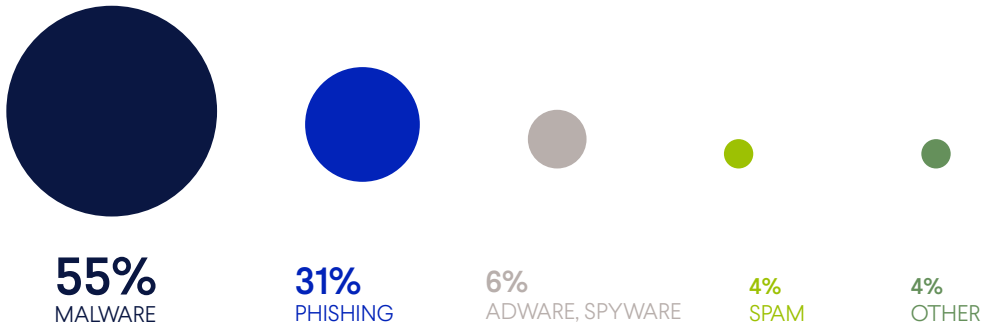


Figure 6 – Safe Browsing threats blocked by CUJO AI Sentry between April 11 and October 10, 2023.

Note: some domains can be flagged for more than one malicious activity.

Consumer protection from online scams and phishing websites is a necessary element in the protection of their digital life, as malicious campaigns become more scalable with the help of generative AI models.

Adware Campaigns

Between April and October 2023, our researchers observed several widespread campaigns that impacted consumers in North America and Europe. These malicious activities likely operate as businesses, selling advertisement views and clicks or guiding traffic to their client's pages.

A common tactic used by some of the most popular campaigns is malvertising, where an advertisement on a legitimate ad network is used to redirect a user multiple times and land them on a different site that often contains explicit adult content.

Several campaigns also use adware – malicious software that displays unwanted advertisements to the user. The software is often installed with free applications, browser toolbars or fake software updates.

While these campaigns use adware to show unwanted ads and websites, they also often promote other similar tools and software, creating an almost circular ecosystem of adware, malvertising, and promotion of unwanted software.

CUJO AI Labs have also observed campaigns that hijacked web browsers to display pop-up advertisements as well as misleading information that was designed to entice the user to share sensitive information for possibly illegal purposes.

WHICH DEVICES ARE ATTACKED MOST OFTEN?

Which Devices Are Attacked Most Often?

Our data shows that over 65% of all home networks are affected by at least a single threat on an average month. Of these, 59% (equivalent to 38% of all home networks) have multiple devices that are targeted by threats within the month. Alarmingly, more than 5% of households had five or more devices targeted or exposed to threats.

To find out which devices are targeted most often, and whether some device types are affected by more threats on average, we combined our AI-driven device intelligence data that precisely identifies and classifies device types, brands, and models, and allows us to observe and analyze threat data across dozens of distinct device types, ranging from smartphones to simple IoT sensors.

OVERALL THREATS TO DEVICES

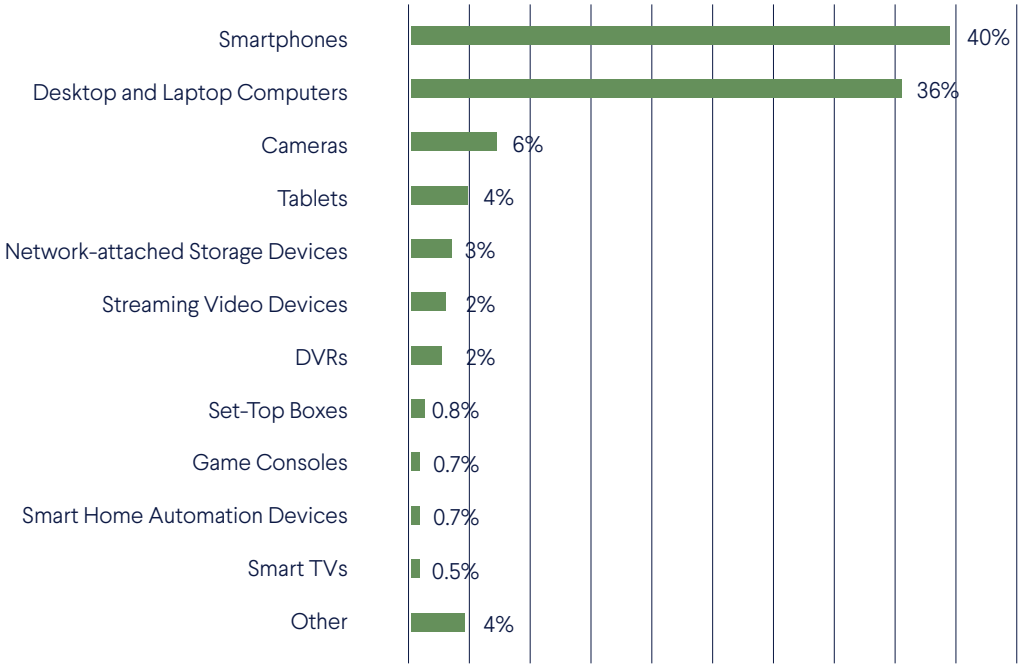


Figure 7 – Overall threats to devices blocked by CUJO AI Sentry between April 11 and October 10, 2023.

If we consider the raw number of threats to particular types of devices, smartphones and computers together are affected by over 75% of all cybersecurity threats. Nevertheless, this does not mean that an average computer or smartphone will be more likely to come under threat, since these devices are very common.

This is why, just as in last year's cybersecurity report, we calculated a device threat index, which allows us to compare the average number of threats affecting devices of a particular type. The threat index is the ratio of average threats per device in a category. A group of devices with a threat index above (or below) 1.00 experiences more (or fewer) threats than an average device in the whole device population. For example, a device model with a threat index of 400 is affected by 10 times more threats on average than a device with a threat index of 40.

DEVICE TYPE THREAT INDEX

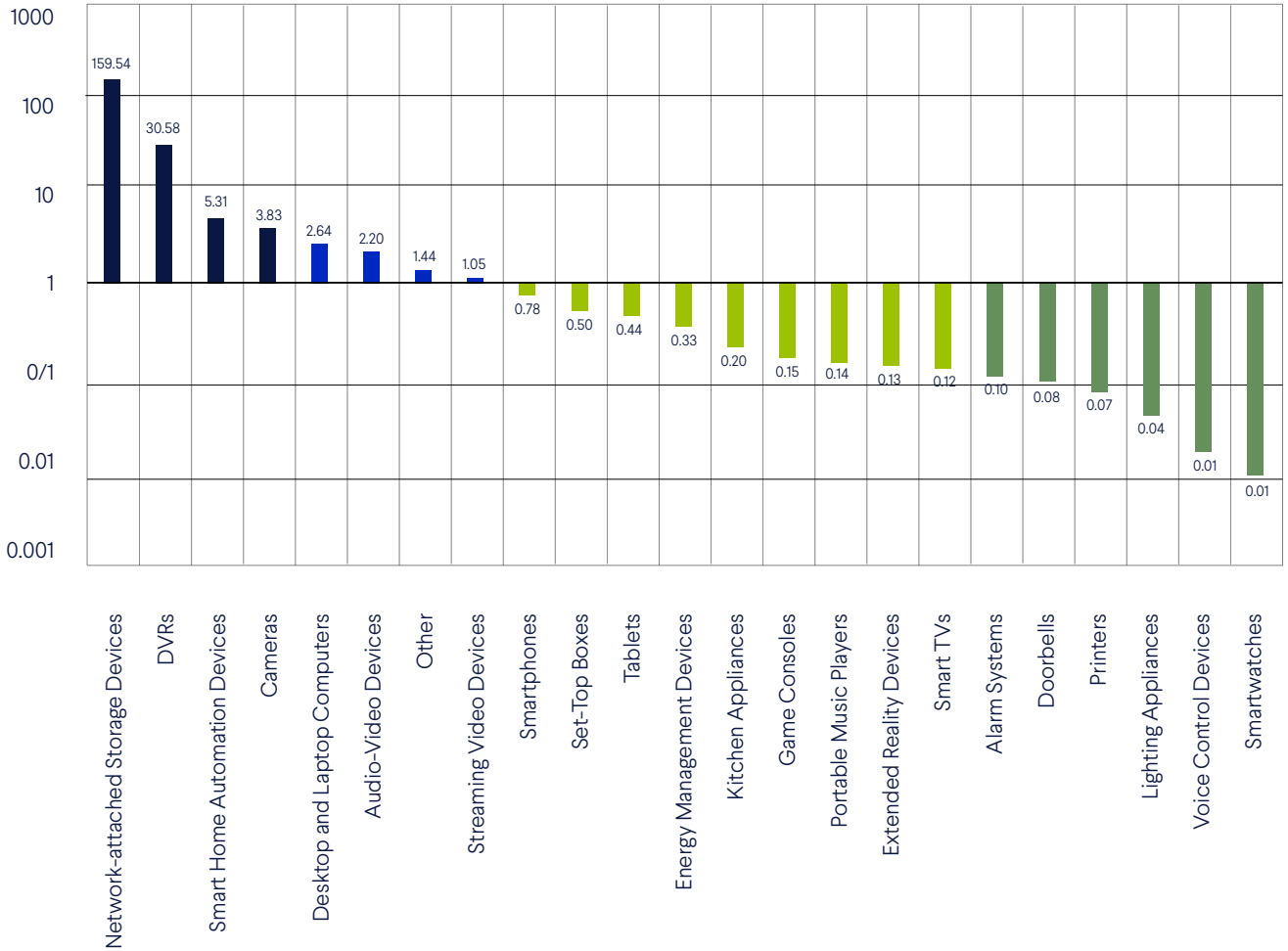


Figure 8 – The device threat index shows which devices are affected by cybersecurity threats more often, on average. Data from the period between April 11 and October 10, 2023.

5 DEVICES TYPES WITH THE HIGHEST THREAT INDEX

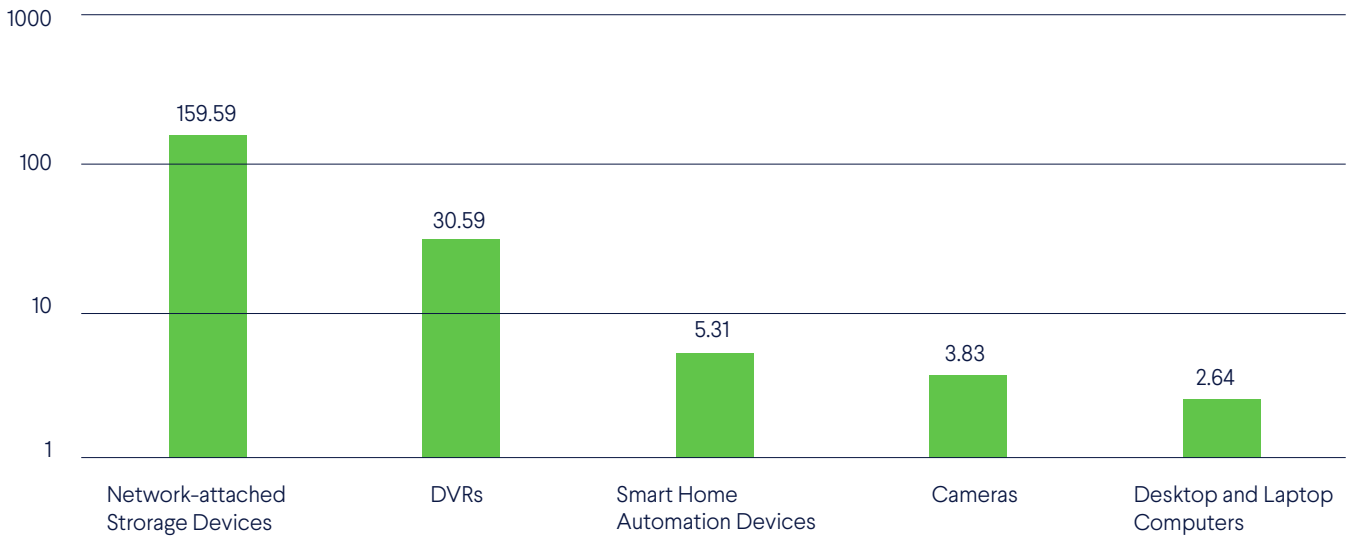


Figure 9 – On average, these five types of devices were affected by cybersecurity threats most often during the period between April 11 and October 10, 2023.

The device threat index shows us that network-attached storage (NAS) devices remain the most-attacked devices on average by a wide margin. These devices, just like DVRs, are large data storage devices that are meant to be accessed remotely.

Many NAS devices, DVRs, as well as other devices in the top 5 list, have poor default configurations, such as default usernames and passwords, port forwards configured for remote access, unprotected debug interfaces, or outdated and vulnerable software components.

Most Frequently Targeted Ports

Many connected devices have open ports for various communications protocols. Some ports allow the owner to remotely access data or a video stream on the device, while others enable peer-to-peer communication and file sharing, online gaming, software updates, or other use cases.

Ports can be opened automatically through protocols like Universal Plug and Play (UPnP) or by configuring router settings manually. Automation simplifies the setup of a device and enables various services, but it can pose security risks by exposing the network to external threats.

Malicious actors frequently scan and probe networks to find and target ports that might be left open; therefore, implementing proper security measures is crucial for home network security. CUJO AI Sentry blocks such attempts from known malicious sources, protecting the devices, and allowing their owners to continue using them without obstructions.

As noted in our recent IoT Botnet Report, some ports are targeted by botnet malware to compromise devices with known vulnerabilities.

Overall, data from our deployments show that several ports are targeted most often:

- **TCP 80, 8080, 443,** and **8443** ports are often collectively considered web-related ports, used for HTTP and HTTPS traffic. However, it's essential to note that these ports can be used for services beyond web protocols. Because HTTP and HTTPS are commonly allowed through perimeter routers, these ports are frequently open, making them attractive targets for unauthorized access.

- **TCP 22** port is typically used to access devices remotely by using the Secure Shell (SSH) protocol.

- **TCP 9000** port is often opened for various services and development tasks, including debugging. Its flexibility in usage makes it another point of interest for attackers.

MOST TARGETED PORTS BY NUMBER OF ATTACKS

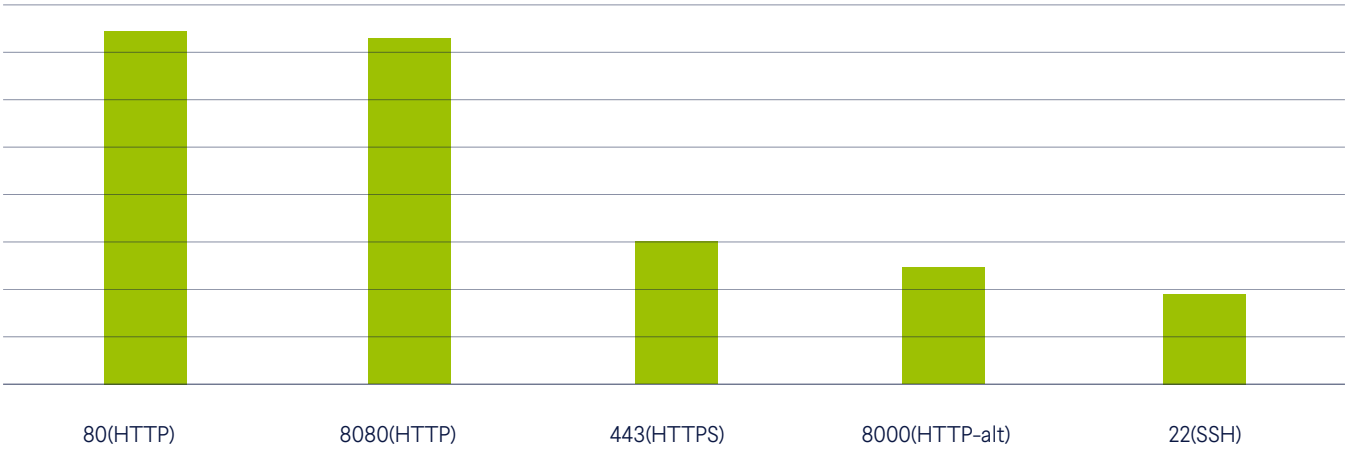


Figure 10 – HTTP/S and SSH ports are targeted by malicious actors most often. CUJO AI Labs data from June 2023.

Ports 80 and 8080 are targeted by the largest number of attacks, but our data shows that these attacks affect a much smaller number of households and devices than attacks on port 443, which are the most distributed.

DISTRIBUTION OF ATTACKS TARGETING PORTS

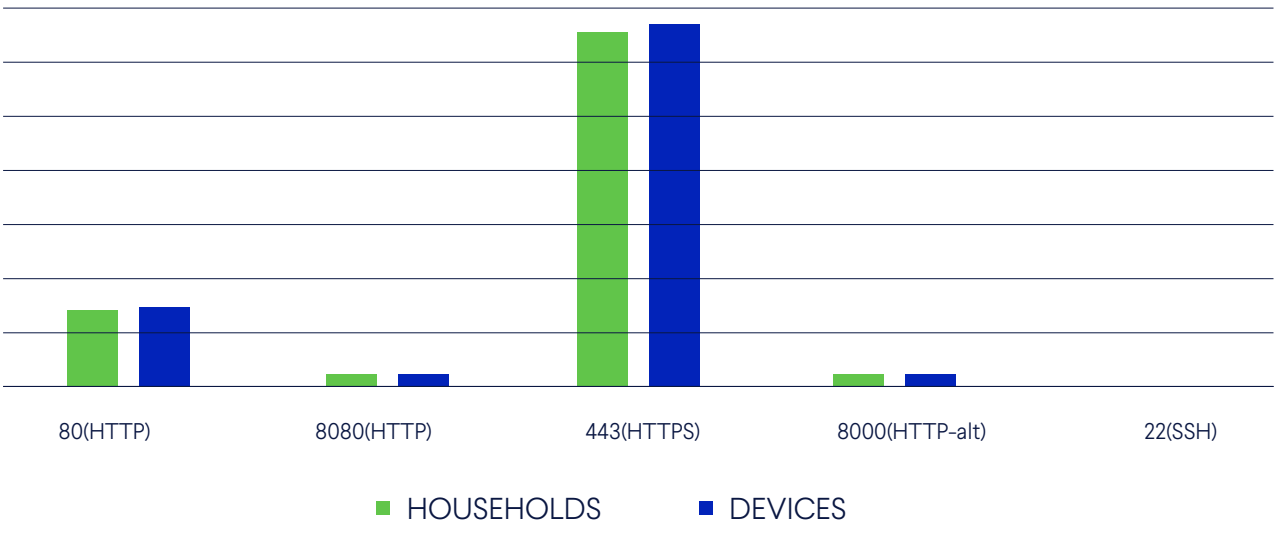


Figure 11 – Attacks targeting port 443 have, by far, the widest distribution across home networks and devices by far. CUJO AI Labs data from June 2023.

Malicious actors can target home devices for various reasons. While it is commonly believed that most attackers want to create botnets, our data on incoming IP Reputation threats shows a different picture.

IP REPUTATION THREATS

23

IP Reputation Threats

Connections to and from known malicious IP addresses predominantly impact unattended IoT devices. While these threats make up almost half (over 46%) of all malicious activities stopped by CUJO AI Sentry, their targets are not as numerous as one might suspect.

Our data shows that in an average month, all IP Reputation threats affect relatively few home networks (5.51%). Of these, over 78%, or 4.33% of all households, are affected by fewer than 20 threats. This means that a relatively minuscule number of end-users are targeted by many IP Reputation threats.

Network service operators have an opportunity to reduce malicious activities related to malware, network scanning, spam, and other threats on their networks by improving the security of a key segment of their user base.

IP Reputation Threat Breakdown

Our data shows that most disreputable IPs targeting consumer devices were related to malware distribution (38%), scanning and brute force attacks (28%), and spam (24%). While only 5% of all IP Reputation threats can be definitively attributed to specific botnets, it should be noted that botnets use techniques such as scanning, brute force, and malware distribution, which we attribute to their own categories, therefore the actual botnet activity is likely more significant.

Note: a single threat source (IP address) can be flagged for multiple malicious activities; therefore, these percentages show only an approximation of the true distribution of IP Reputation threats.

IP REPUTATION THREAT SOURCES

Figure 12 – Incoming IP Reputation threat categories according to CUJO AI Sentry data from the period between April 11 and October 10, 2023. Note: a single threat source can be attributed to several categories.

BOTNETS

25

Botnets

Due to the scale of CUJO AI's deployments at the leading service providers' networks, we have a unique view of the botnet activity on home networks. Our data shows that several botnets were active on these networks in 2023.

Qakbot

In August, the most active botnet, Qakbot, was taken over by the US Federal Bureau of Investigation (FBI) and its international partners, severing its control of the compromised devices. Our botnet data clearly shows how Qakbot ceased its activities after August 24.

QAKBOT ACTIVITY IN AUGUST

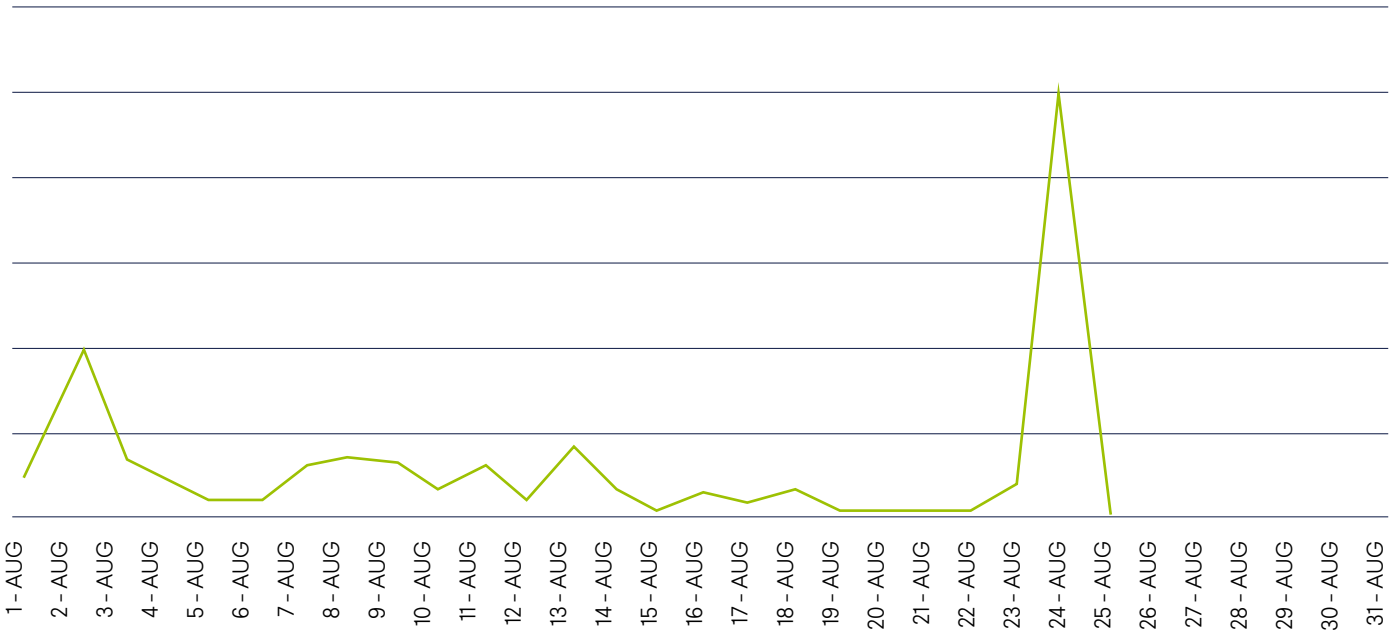


Figure 14 – Qakbot activity data on networks protected by CUJO AI in August 2023, showing how the botnet was no longer active after FBI and its international partners took it over on August 24-25.

The spike we observed in the last days of the active botnet is likely due to the FBI and other organizations reporting additional malicious IP addresses used in the botnet. If we look at the daily number of IP addresses that are used and related to Qakbot, we see a four-fold increase in the number of active unique IP addresses.

UNIQUE IP ADDRESSES RELATED TO QAKBOT

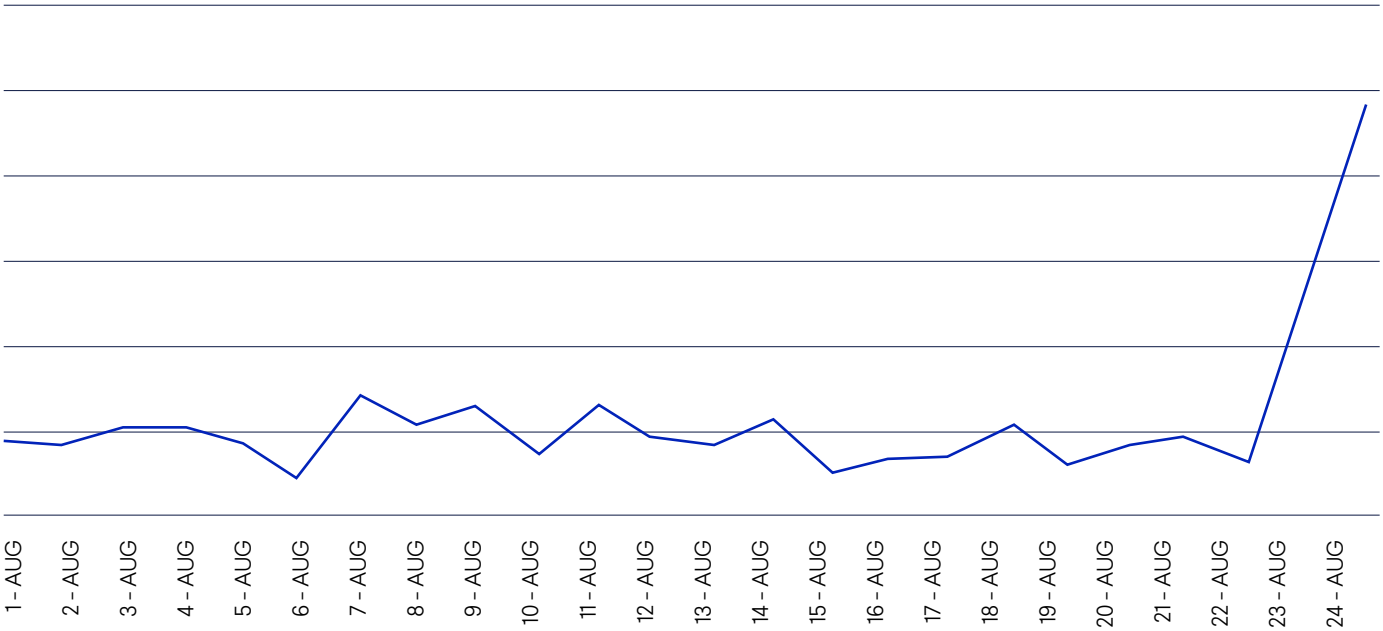


Figure 15 – Unique IP addresses related to Qakbot in August 2023, likely indicating that a large number of new IP addresses were flagged days before the botnet was taken down.

Up to that point, Qakbot was the most active botnet on the networks protected by CUJO AI. Two other active botnets (Emotet and Dridex) had also been disrupted by security agencies in the past but have been successfully resurrected since. For example, Emotet used the infrastructure of TrickBot to re-establish itself in late 2021 and has since become more prevalent and active than TrickBot in the networks that we monitor. This is why we should always be cautious when considering the future possibilities of these malicious actors.

Botnet Activity

Botnets usually operate by first deploying a stager shell script, which downloads and starts executing malware binaries.

Most of the malware observed in the IoT landscape are variants of the infamous Mirai or Gafgyt botnets, but malware written in Go is becoming more common. Some prime examples of malware written in Go are Zerobot and Sysrv, which is not very active at the moment.

TWO MAIN VECTORS FOR THE SPREAD OF BOTNETS

- Brute-forcing weak login credentials
- Exploiting known software vulnerabilities

In general, the first one is the more common method, as noted in our 2021 IoT botnet report, and the problem remains prevalent today.

"Poor quality IoT devices often come with hard-coded, default passwords that are not changed by the user or, when a password change is enforced, changed to an easy to remember (and therefore quickly brute-forceable) password".

Detecting and Analyzing Malware Activity

At the beginning of October 2022, our analysts observed a peculiar behavior pattern that allowed us to uncover a malware instance spreading in our customers' networks.

Due to a significant spike in traffic, we discovered several devices that were sending connection requests to dynamically generated URLs. Their connectivity followed a similar pattern: devices would ramp up their connection requests into the thousands within a day. One device that we observed had connected to around 5 thousand unique IP addresses and 167 unique ASNs.

Only a handful of those addresses were used for malicious communication. Among the most used IPv4 addresses, we saw an address associated with the vipersoftx malware, as well as an address that is associated with the Nivdort malware family, which is known for dynamically generating domains to mask C2 activity. These few IP addresses generated a massive amount of traffic, which helped us connect the activity to a particular malicious actor.

Studying the pattern of this malware has allowed us to adjust our security solutions to safeguard end-user devices against the malware's behavior. It also showed that two malware families shared a trait, showcasing how malware continues to evolve.

For more in-depth analysis of IoT botnet malware discovered on networks protected by CUJO AI, read our latest IoT Botnet Report.

CONCLUSION

Conclusion

The landscape of threats to consumers continues to shift as malicious actors prioritize easy targets and seek the highest return for their effort.

Our research highlights that phishing and other malicious websites pose significant risks to consumers. This concern amplifies when considering the surging consumer financial losses due to online scams. In our experience, leveraging AI to proactively combat emerging phishing campaigns emerges as a potent strategy to counteract these malicious endeavors.

This report highlights the tactics employed to target consumer devices within home networks. It reveals that certain device types are targeted more frequently than others because of their configuration, or lack thereof. Additionally, consumer preferences, such as desiring a web interface for device management, influence their vulnerability to attacks.

Malicious advertisement networks and malware are spreading across continents. Additionally, social engineers are targeting consumers even on devices considered relatively safe. Network service providers have a pivotal role here. They can not only enhance their own security and efficiency by preventing these malicious activities but also differentiate themselves from competitors by offering a safer connected experience for their end-users.

The evolving threat landscape requires network operators to be proactive and take advantage of leading multi-layer security solutions that are geared towards stopping the threats of tomorrow.

CUJO AI Sentry

CUJO AI Sentry is a multi-layered machine learning network security solution that network service providers can offer to their end-users. It detects and blocks threats directed at any device connected to the network, while respecting the privacy of the end-users.

Once deployed on any broadband router, CUJO AI Sentry requires no additional software to secure any and all computers, phones or IoT devices in the home. Sentry can also be deployed on the carrier's native app to provide full protection to mobile devices outside the home network.

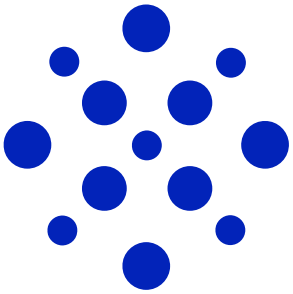
Sentry is a proven solution that already protects tens of millions of homes around the world.

CUJO AI Explorer

CUJO AI Explorer is a stand-alone device intelligence solution for network service providers, which uses machine learning to identify device types, manufacturers, models, OS versions, and hardware capabilities. The largest network service providers in the world use Explorer to future-proof and optimize their core services and networks.

CUJO AI On The Move

On The Move is a versatile SDK for Android and iOS devices that extends CUJO AI Digital Life Protection services outside the home network. With On The Move network service providers can give end-users the same peace of mind and proactive security wherever they go online.



About CUJO AI Labs

CUJO AI Labs is an advanced research department of CUJO AI specializing in IoT threat research and NSP customer cybersecurity. Labs researchers use the largest scale real-world device behavior database of over 2 billion anonymized consumer devices to empower advanced machine learning technologies that protect tens of millions of households around the globe. Every year, CUJO AI Labs publishes in-depth data-based reports, such as this one, on the IoT ecosystem and cybersecurity.

About CUJO AI

CUJO AI provides advanced multilayered cybersecurity and device intelligence as a product for Internet Service Providers, which allow them to protect end users' devices and home networks.

Major mobile and broadband providers partner with CUJO AI to offer security as a value-added service to their clients.

As the only platform of its type deployed to in tens of millions of homes and covering over 2 billion connected devices, CUJO AI offers advanced AI algorithms to help its clients uncover previously unavailable insights and raise the bar on customer experience & retention with new value propositions and superior operational services.

Fully compliant with all privacy regulations, CUJO AI services are trusted by the largest broadband operators worldwide, including Comcast, Charter Communications, TELUS, Sky Italia, Rogers, Cox, Shaw, and Videotron.

More information: **connect@cujo.com**

Media inquiries: **press@cujo.com**

cujo.com