CUJOAI

CYBERSECURITY REPORT 2023

CONSUMER DEVICES UNDER THREAT

Table of Contents

INTRODUCTION

03

The Scale of Home Network Security Threats Cannot Be Ignored

CUJO AI is the leading provider of AI-driven cybersecurity for network service providers. Our algorithms protect the entire end-user network and every device on it. They help bridge major gaps in device cybersecurity and protect all devices, even those that are not powerful enough to run security software, as well as mobile devices across all networks.

Protecting hundreds of millions of devices every day, CUJO AI Sentry allows network service providers to reduce botnet activities, the prevalence of DDoS attacks, and improve the connected experience thanks to reduced malicious activities on the networks. During the last 12 months, CUJO AI blocked more than 4.2 billion threats.

During the six month period (May 1 – November 1, 2022) covered in this report, Sentry prevented 2,102,990,310 threats. In October alone, it stopped 362,754,105 threats, or over 8,000 threats every minute. Our data shows that over 67% of home networks experience at least a single online threat every month. Social engineering, fraud and phishing websites are a major threat to consumers, with 56% of end-users attempting to access them at least once every month. In total, 66,801,679 phishing attempts were prevented by CUJO AI Sentry in October.

CUJO AI Labs use fully anonymized threat data to discover new vulnerabilities and threats. Network service providers use these new insights to protect consumers from online threats. Over the last several years, our researchers have published in-depth analyses of malware threats, newly discovered malware strains, broad analyses of the evolution of malware, as well as overviews of botnet trends.

Between May 1 and November 1, 2022, we stopped 2,102,990,310 threats, or over 8,113 threats every minute.

This report is the largest general overview of our real-world threat data, with a focus on several key device types and models that are affected by significantly more threats. With this report we aim to bring more awareness of the necessity to precisely classify device types, vendors, and models to prevent widespread cybersecurity issues across large telecommunications networks.

The data in this report covers a six-month period between May 1 and November 1, 2022, and includes threat data from CUJO AI Sentry and device intelligence data from CUJO AI Explorer, the stand-alone service that enables network service providers to precisely identify device types and models.

> Our data shows that over 67% of home networks experience at least a single online threat every month.

Our solution categorizes threats into 4 distinct categories: IP reputation, web reputation, DoS participation, and remote access threats. Two of these threat types make up most of the attacks we prevent:

- **IP reputation threats** are inbound and outbound connections to and from IP addresses that have a low reputation (e.g., are used to command and control botnets). These are the **most common threats to unattended devices**, such as IoT devices, which are mostly automated and do not require user interaction.

- **Web reputation threats** encompass various malicious URLs that can be accessed by users, their email clients or other software. These types of threats are the **most prevalent for attended devices**, such as smartphones, laptop and desktop computers, which are actively used by their owners.

The threat index is used in most sections of this report to represent 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 than average threats, respectively. For example, a device model with a threat index of 400 experiences 10 times more threats on average than a device with a threat index of 40.

The Cybersecurity Landscape in 2022

“

As we examine the tens of millions of threats targeting consumer devices, our security researchers see three distinct trends in today's home cybersecurity landscape:

1. The **spread of adware is growing**, and we have seen extremely large spikes in activity over the past year. Most adware operates like a business – when an owner of an adware network receives an order, devices infected with potentially unwanted programs start getting ad pop-ups. Major spikes in adware activity (up to 400%) usually happen on weekends, when people spend more time online. It may also be the case that ads shown at those times are more effective.

2. The number of end-of-life, **unsupported or outdated devices** is increasing, creating more risk to home networks. IoT device lifetimes often exceed vendor support times, and unprotected devices which have poor configurations (or known unpatched vulnerabilities) are very likely to be hacked. It's a numbers game: both residential and enterprise networks are being scanned for IoT devices by automated scripts and then attacked, which means that a vulnerable device is a sitting duck for automated malicious activities.

3. Phishing is a major cybersecurity issue. Every month, end-users in **around 56% of homes attempt to open at least a single phishing link**. This is extremely worrying due to the major negative impact that a successful phishing attack can have on private data, finances, as well as business and infrastructure security.

While these trends target different attack surfaces (types of devices, vulnerabilities, and behaviors), they are not isolated. For instance, the growth of vulnerable IoT devices feeds into the prevalence of botnets and DDoS attacks. As the cybersecurity landscape continues to evolve, we clearly see the need and value of our comprehensive, multi-layered security solution to protect tens of millions of households.

Leonardas Marozas

Security Lab Manager
CUJO AI

66,801,679
phishing attempts were prevented by CUJO AI Sentry in October, 2022

67%
of homes experience at least one online threat every month

56%
of homes attempt to open phishing links

BRANDS UNDER ATTACK

07

Brands Under Attack

Device manufacturers and vendors are facing increased scrutiny for the security of the devices they produce and sell. As device security regulation ramps up in the EU, UK, and US, we should expect at least some of these brands to improve their record.

25 Brands Targeted by the Most Online Threats

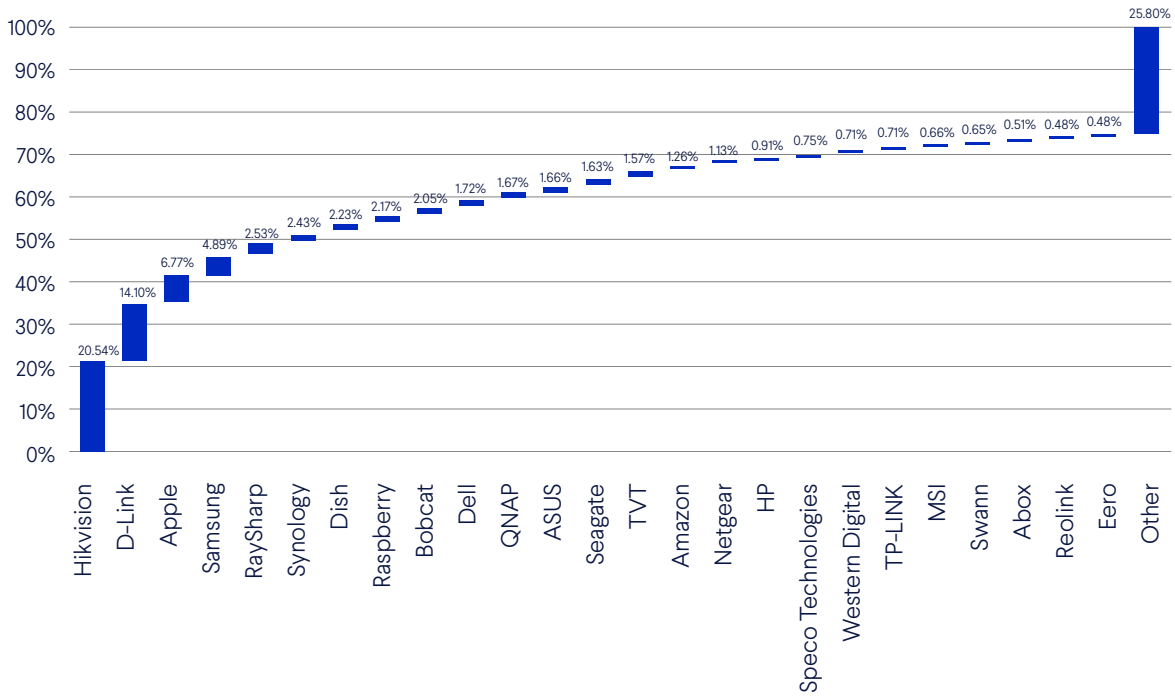
Out of more than 4,359 device brands, 25 are being targeted by over 70% of all digital threats to consumer devices.

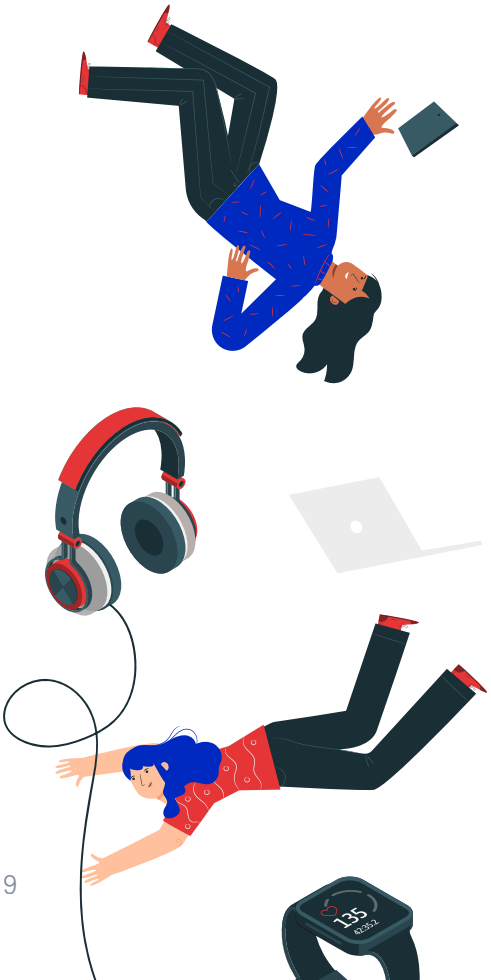
25 DEVICE BRANDS TARGETED BY MOST ONLINE THREATS

1. Hikvision	2. D-Link	3. Apple
4. Samsung	5. RaySharp	6. Synology
7. Dish	8. Raspberry	9. Bobcat
10. Dell	11. QNAP	12. ASUS
13. Seagate	14. TVT	15. Amazon
16. Netgear	17. HP	18. Speco Technologies
19. Western Digital	20. TP-LINK	21. MSI
22. Swann	23. Abox	24. Reolink
25. Eero		

Threat Distribution by Brand

OVERALL THREAT DISTRIBUTION BY BRAND

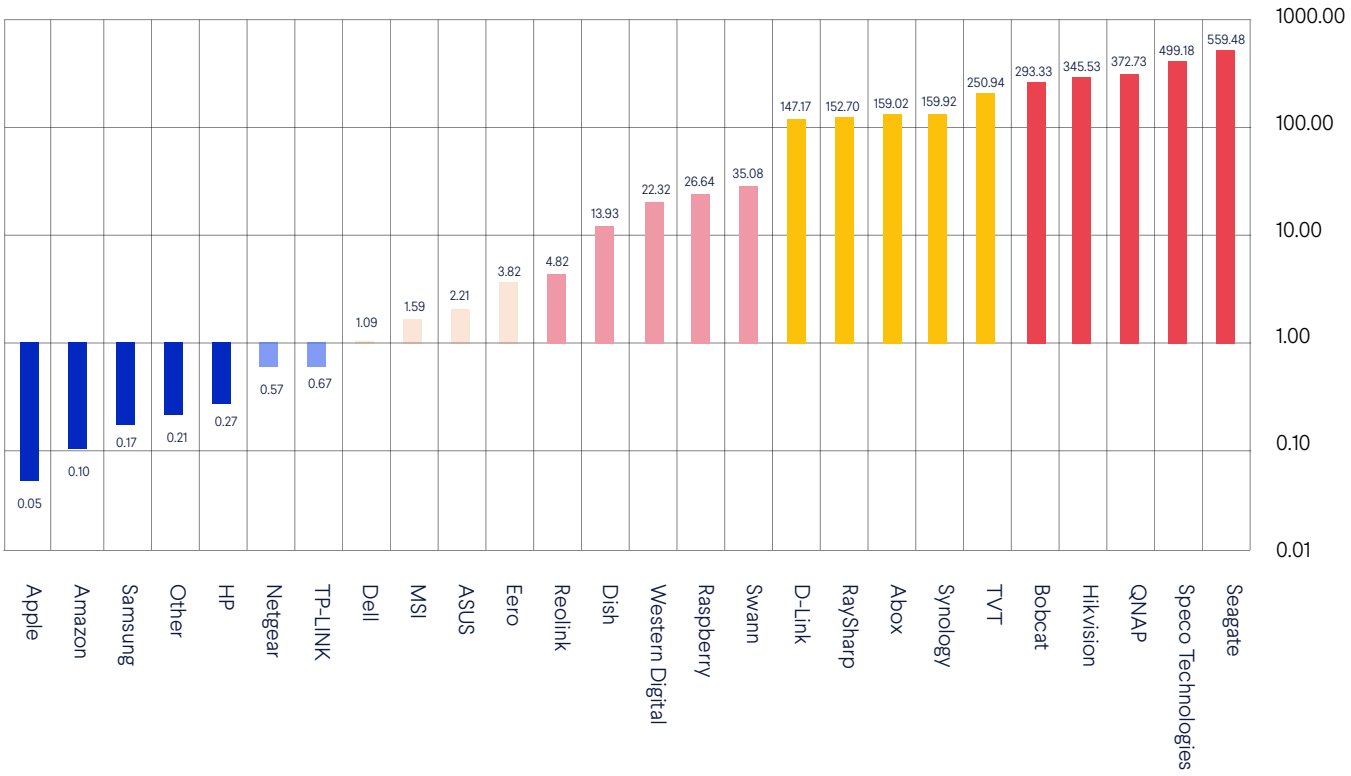




Hikvision (20.54%), D-Link (14.1%), Apple (6.77%), and Samsung (4.89%) are the four most attacked brands by the overall number of threats targeting. Nevertheless, this distribution does take device population into accounts. For example, our latest device intelligence report showed that Apple and Samsung devices were extremely popular, with 89% and 73% of households having at least one, respectively. To add some perspective, we have calculated a threat index, which corresponds to the average threats per device for each brand.

The Most Attacked Brand Threat Index

THE BRAND THREAT INDEX (LOGARITHMIC SCALE)

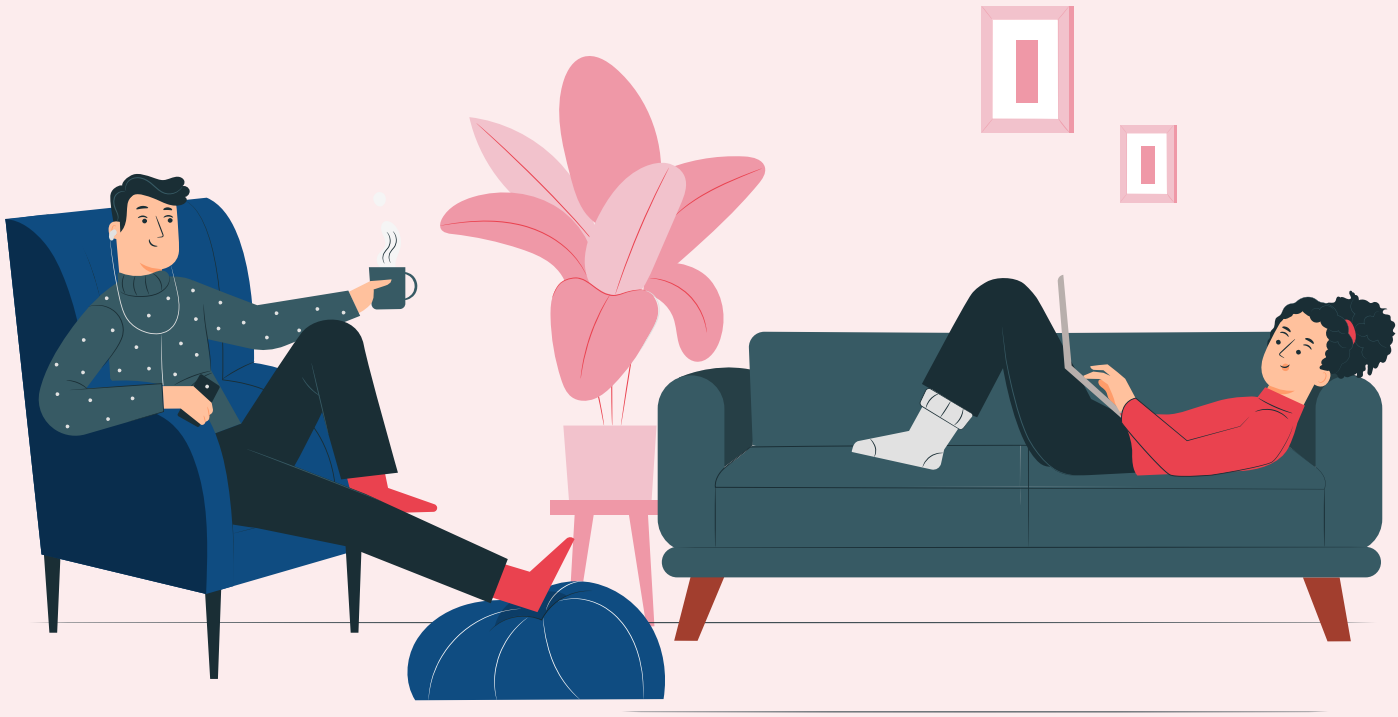


These results are displayed on a logarithmic scale and include only the 25 most attacked brands. Other brands may have higher threat indexes than those displayed, as shown in later sections of the report.

The threat index shows quite a different picture, where Apple and Samsung devices experience orders of magnitude fewer threats on average than Hikvision or D-Link devices. Seagate, Speco Technologies, QNAP, Hikvision, Bobcat, and TVT devices are among the most attacked brands, with the first four drawing in **over 300 times more threats** on average than Dell devices, which are very close to the overall average.

It should be noted that Speco Technologies, which specialize in security cameras, audio, DVR, and CCTV products, have a very small population of devices. These are some of the most targeted device categories, as we discuss in the next section. Bobcat, which produces a cryptocurrency mining hotspot device, has a rather small population of devices, too.

Computers and smartphones also have a very different threat profile from unattended devices. While most IoT devices are attacked from the outside by automated scanners, smartphones are usually targeted when they access malicious websites. Therefore, devices from brands like Apple and Samsung also face different threats than D-Link or Western Digital devices.



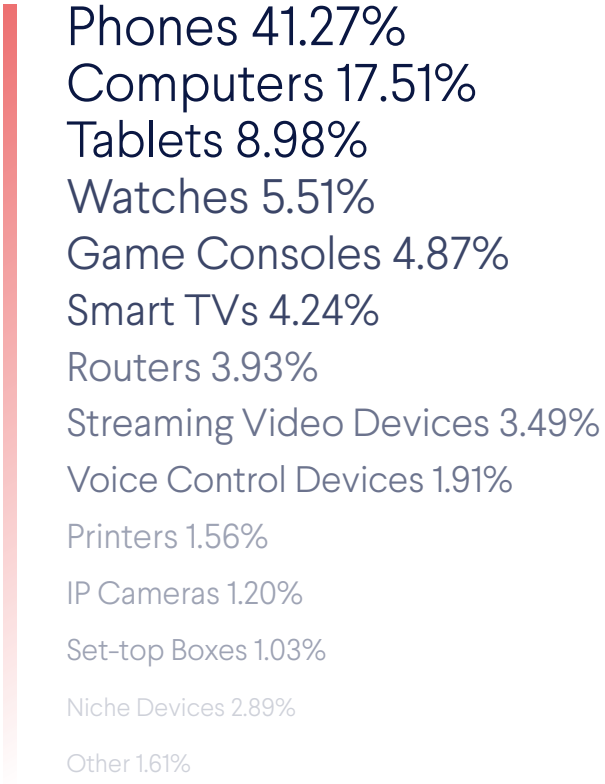
CONSUMER DEVICES UNDER THREAT

12

Consumer Devices Under Threat

Every device model has a different security profile: some have well-known vulnerabilities, others are extremely valuable to attackers, or are easier to attack due to bad configurations. CUJO AI monitors over 1.8 billion connected consumer devices, and, thanks to our device intelligence algorithms, we know what these devices are.

THE MOST POPULAR CONNECTED CONSUMER DEVICES IN 2022



We use device identification data to stop suspicious activities, for example, a thermostat or a smart light bulb connecting to suspicious IP addresses or sending unusual amounts of connection requests.

When we combine the device and threat intelligence data, we can see which device types and models are affected by the most attacks.

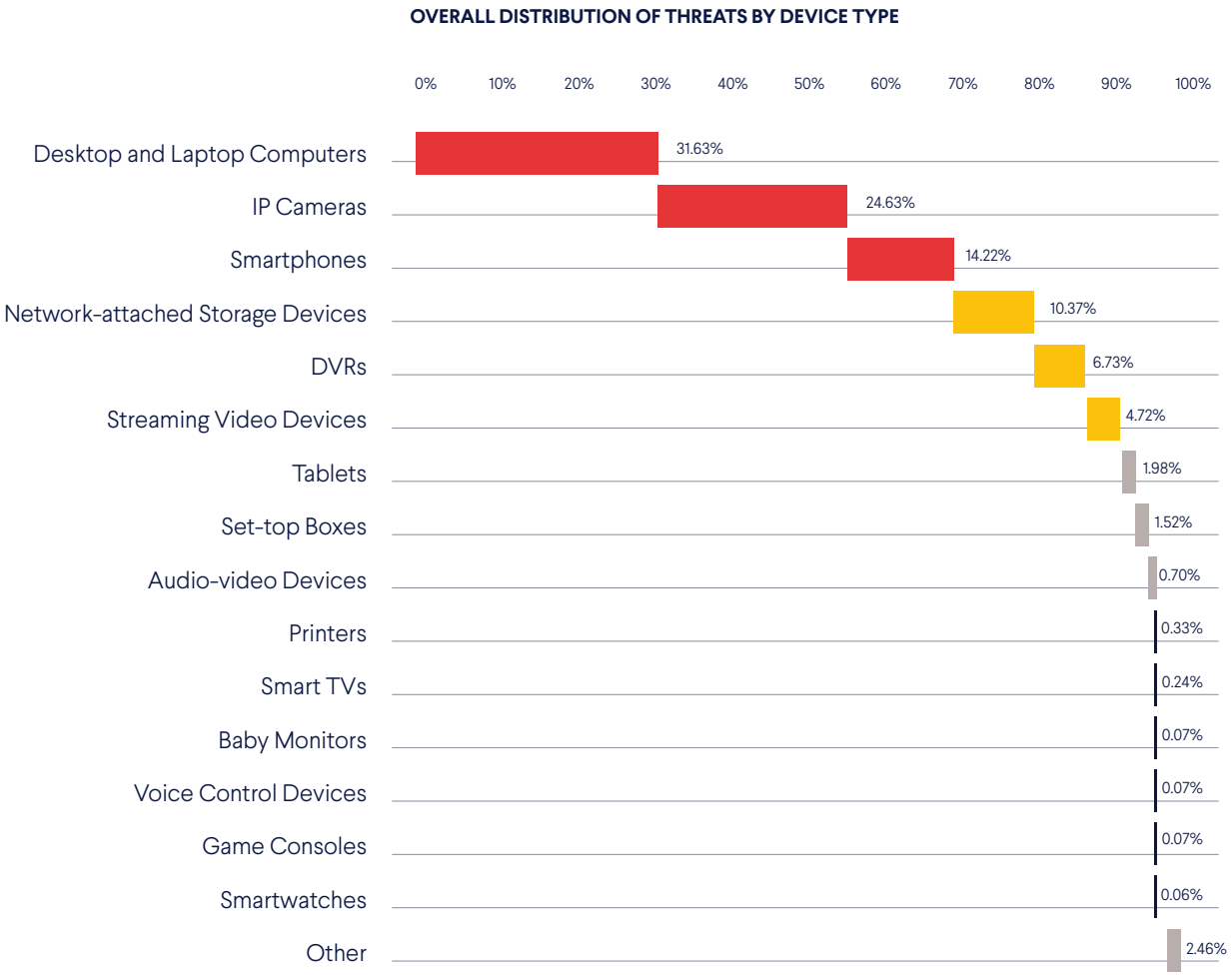
For more information about the consumer device landscape, visit our Device Statistics portal and download our annual device intelligence reports.

What Types of Devices Are Under Most Threat

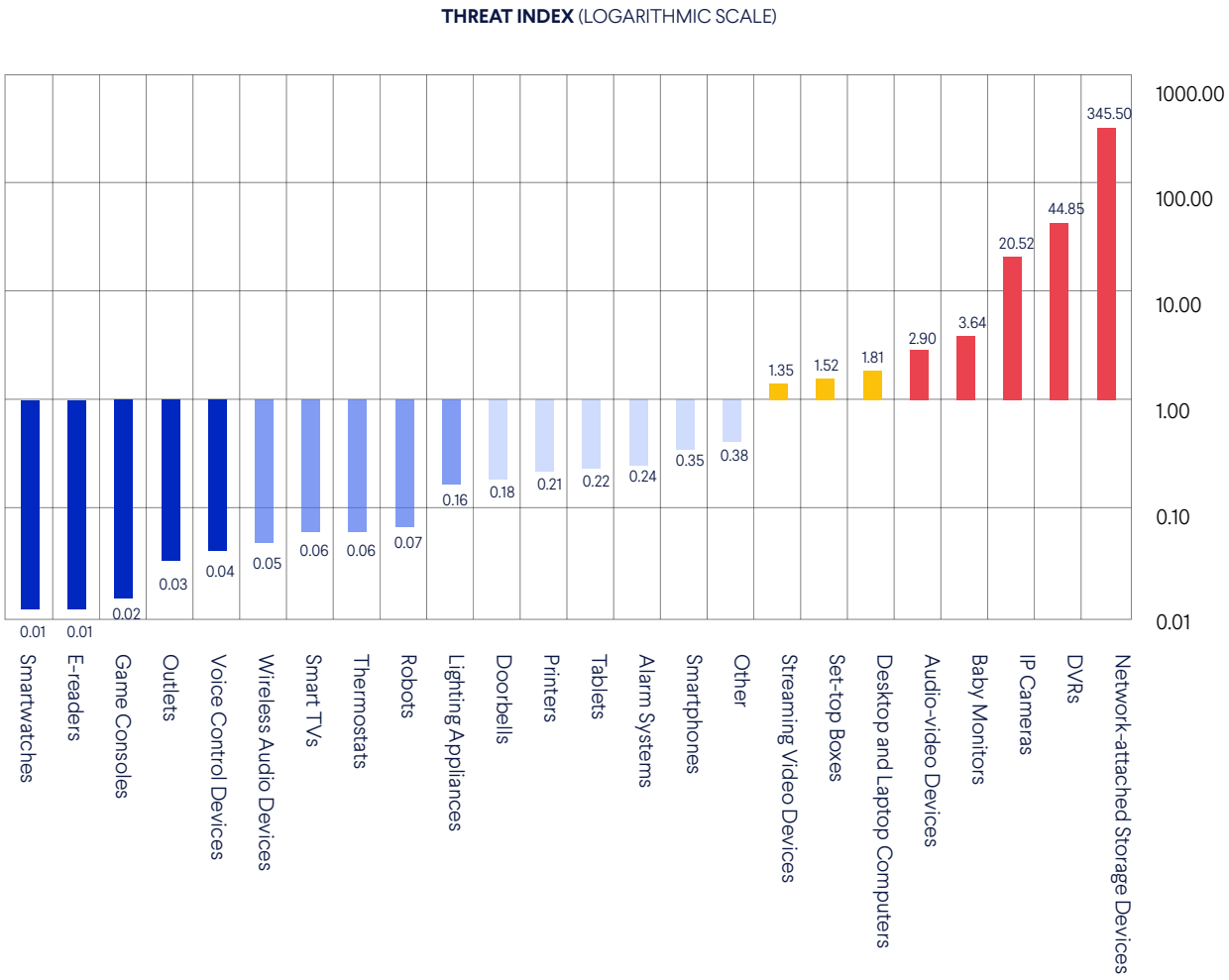
Just 7 device types are targeted by over 90% of all threats. While desktops, laptop computers, and smartphones make up close to 60% of all devices, they are targeted by a significantly lower percentage (45.85%) of threats. IP Cameras, which make up just 1.2% of all devices are targeted by over 24% of malicious activities on consumer networks.

As we've noted in the previous section, attended devices (computers, smartphones) are most often attacked when a device visits a malicious URL, while unattended devices are predominantly attacked from outside the network without the user being aware of the attack.

Even though attended devices can run endpoint protection solutions (e.g., antimalware software), our survey has also shown that only 35-37.5% of consumers in the US, France, and Italy, as well as 54% of consumers in Germany self-reported using security software in 2021. This means that a massive number of attended consumer devices are unprotected.



Device Type Threat Index



An average attended device faces orders of magnitude fewer threats than NAS or DVR devices.

The device type threat index shows that several key categories attract an outstanding number of threats. Network-attached storage (NAS), DVR, IP cameras, baby monitors, and audio-video devices are the **5 most targeted device types**, when we consider the average number of threats to each device type.

Popular devices, such as smartphones, smartwatches, tablets, or computers, face orders of magnitude fewer threats than NAS devices or DVRs, on average.

To dive deeper into the consumer threat landscape, we've examined the 5 most targeted device types.

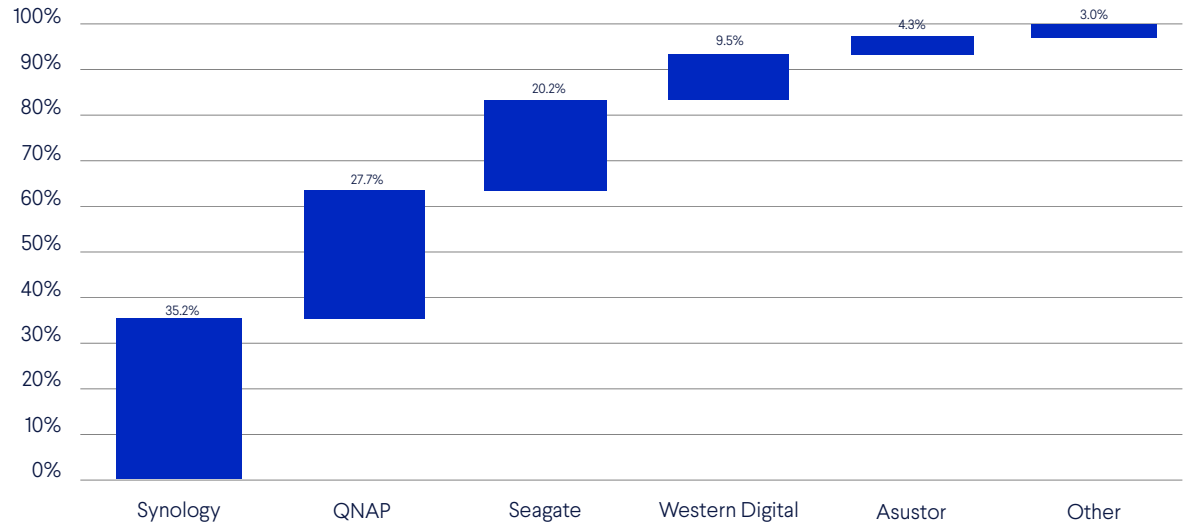
NETWORK-ATTACHED STORAGE (NAS)

16

Network-attached Storage (NAS)

Our data shows that NAS devices are targeted by malicious activities the most often.

DISTRIBUTION OF THREATS TO NAS DEVICES BY BRAND



This section excludes the discontinued Space Monkey devices which are responsible for over 80% of threats to NAS devices. The discontinued devices have known security vulnerabilities and we encourage consumers to stop using these devices.

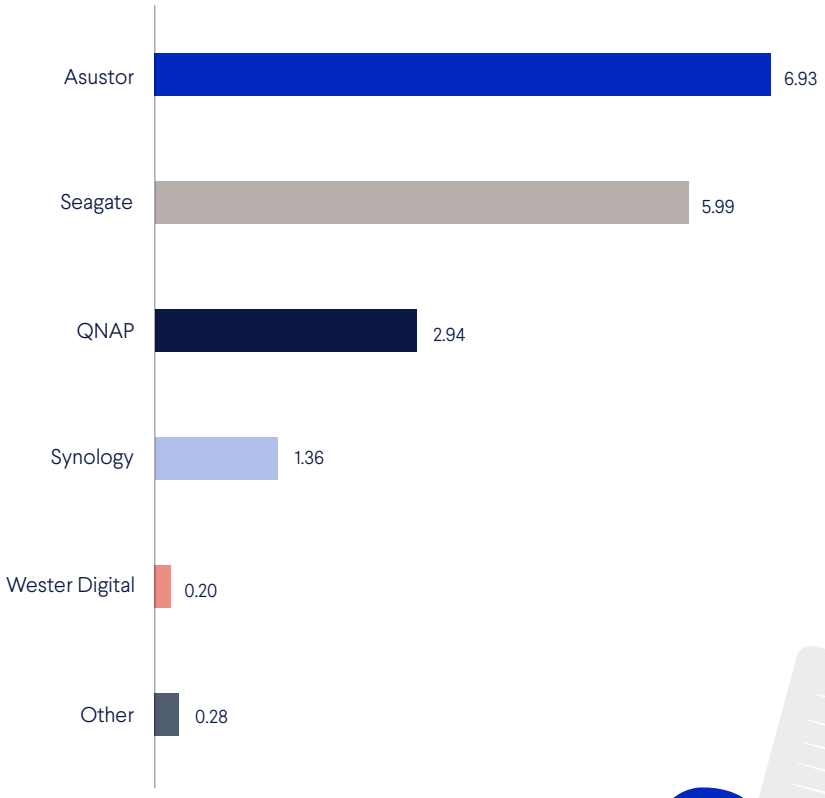
There are several reasons why NAS devices are targeted so often:

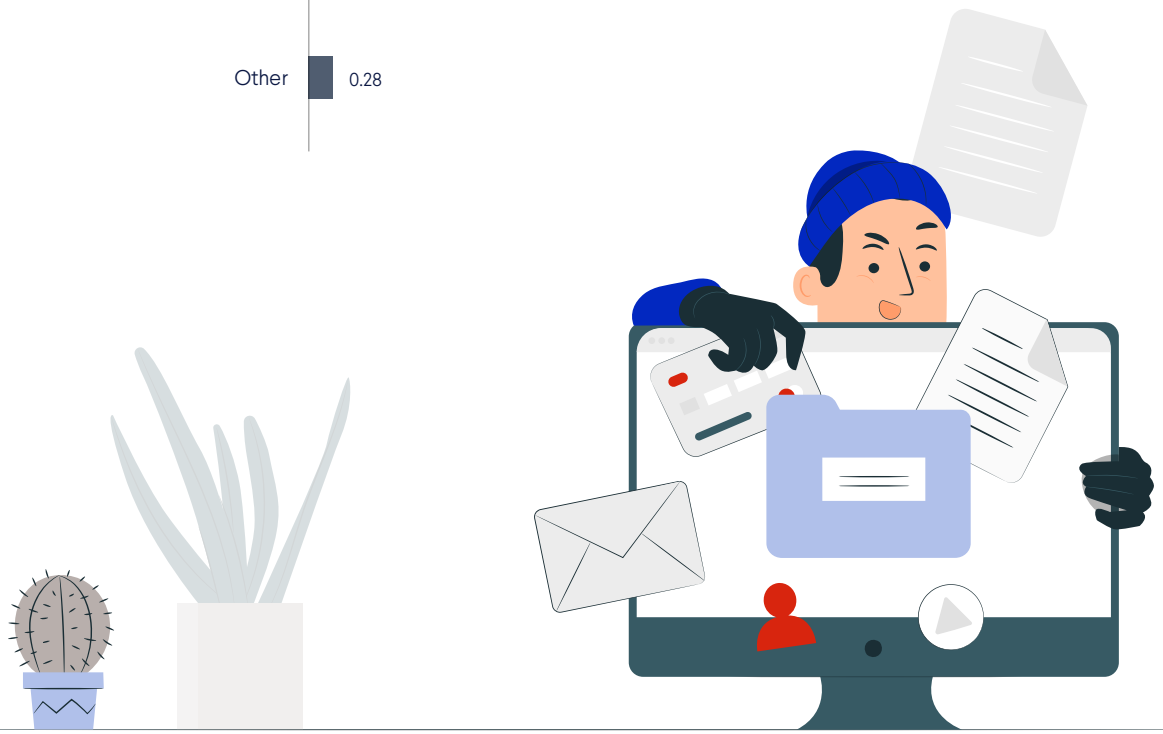
- They are the perfect targets for ransomware due to the valuable data they hold.
- NAS devices are often configured to make them more susceptible to attacks: they need to have ports opened for the owner to access data when away from home. With ports 8080 and 443 open, NAS devices are easily noticed by attackers.
- Users usually have to approve firmware upgrades, which adds significant delays to the patching process.

The NAS Brand Threat Index

Even though Asustor NAS devices have a relatively small share of overall NAS threats, their small number makes them the most targeted devices, on average. Western Digital has the lowest threat index among popular NAS device brands, but the brand's threat index in the overall device population is still quite large (see Brand Threat Index, page 10).

NAS BRAND THREAT INDEX

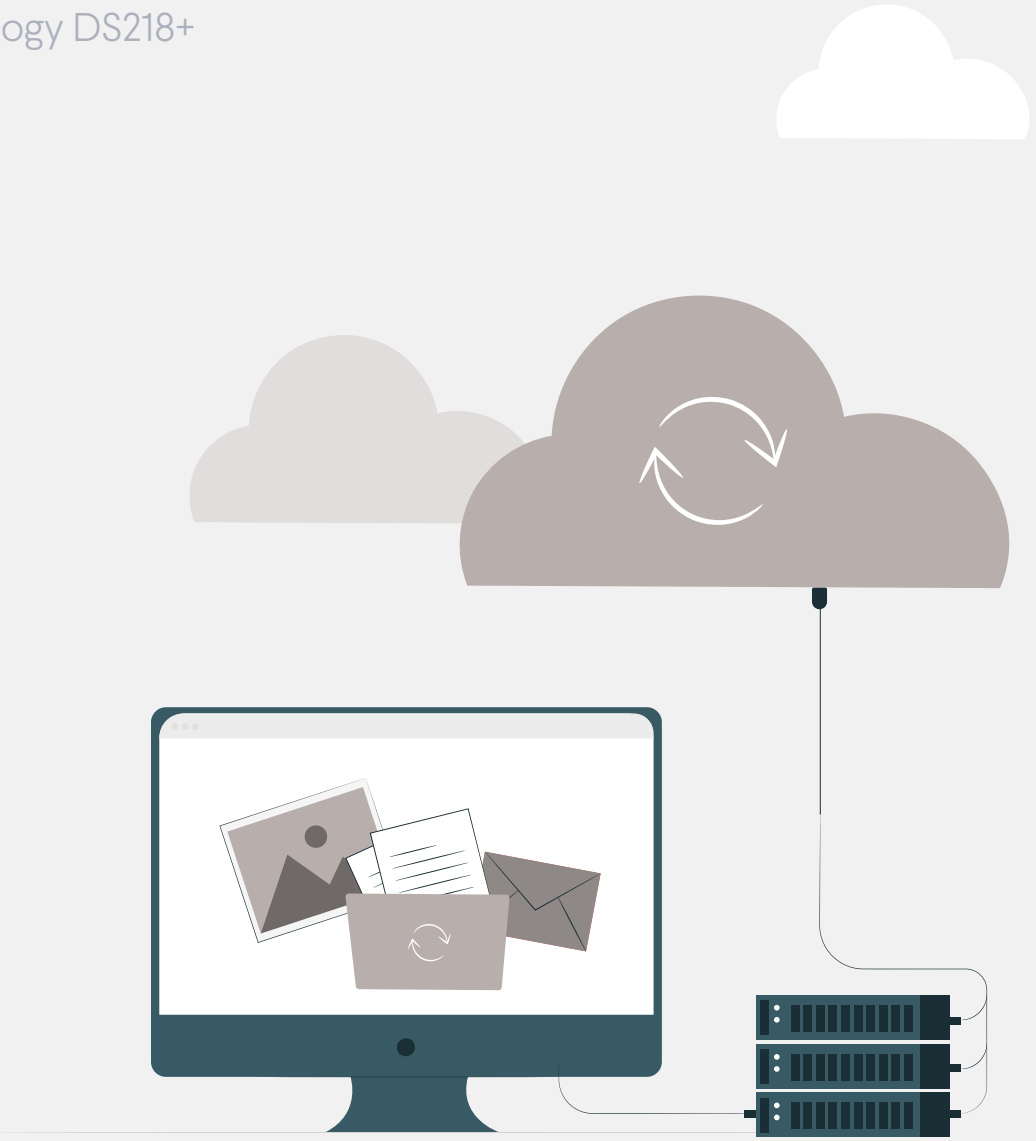




Which NAS Devices Are Attacked the Most

Even though Seagate has discontinued remote access to GoFlex Home since 2019, these devices are still targeted by the most threats.

1. **Seagate GoFlex Home**
2. Western Digital My Cloud
3. Synology DS920+
4. Synology DS218+



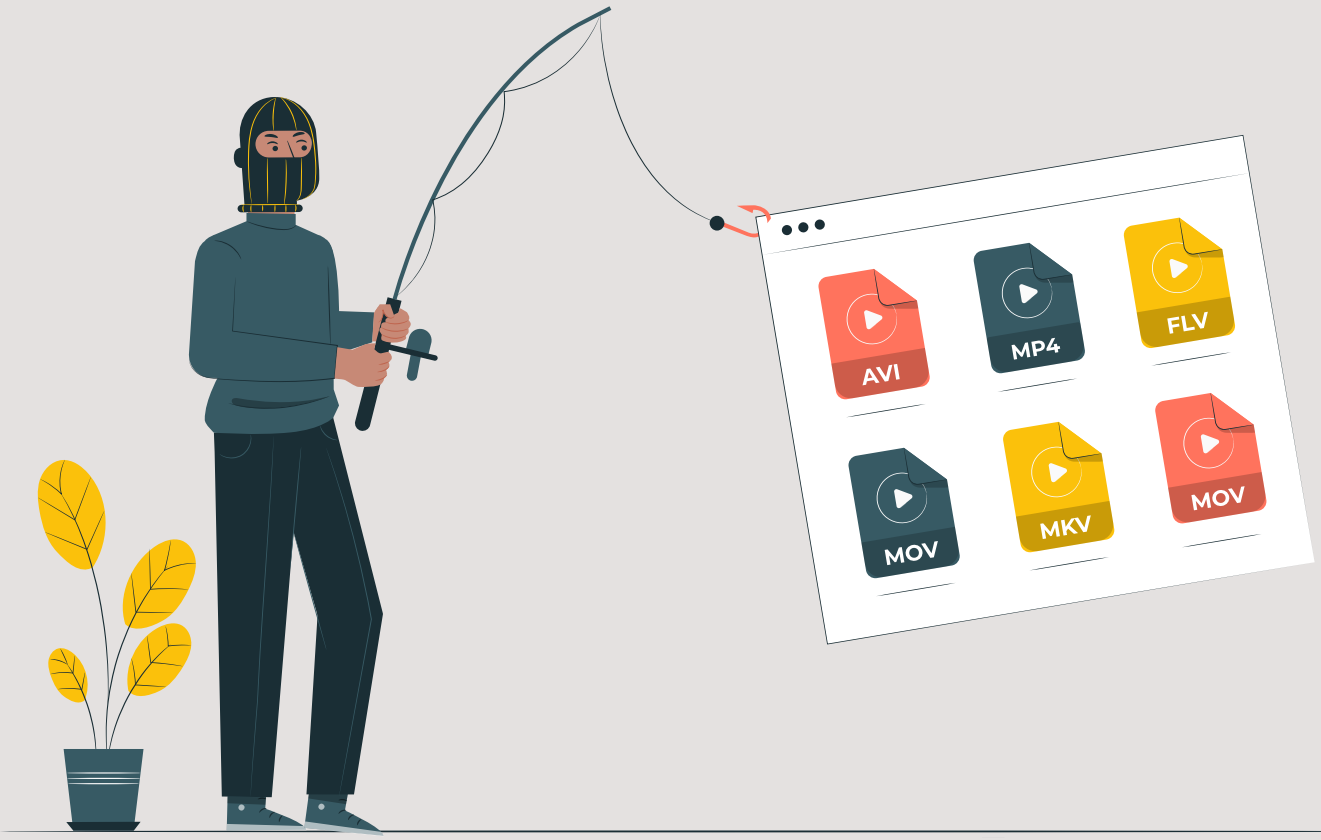
DVR DEVICES

20

DVR Devices

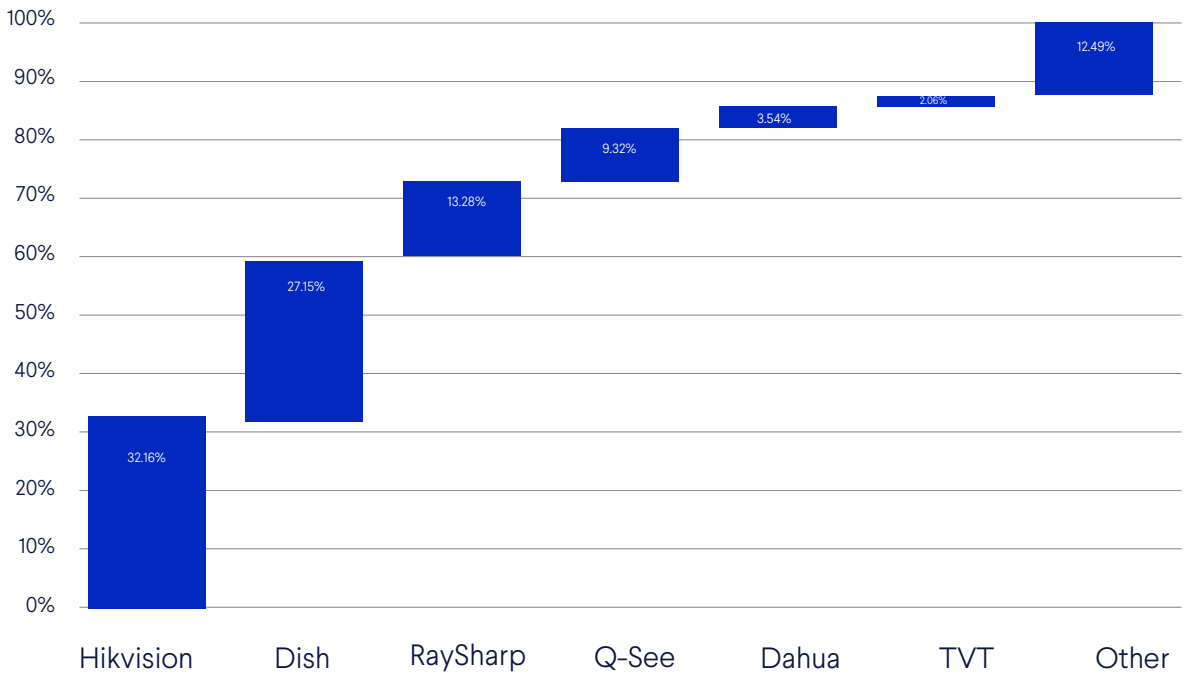
Digital video recorders (DVR) are used to record digital video from IP cameras and other sources to disk drives, USB flash drives, SD memory cards or mass storage devices. Some DVR vendors sell poorly configured devices with open ports that allow access from outside the home network. Also, many DVR vendors autoconfigure the home router via UPnP to open its ports to the Internet. Here, the data shows that a handful of vendors are targeted by the vast majority of threats.

While a compromised DVR may not seem as dangerous as a compromised laptop or NAS device, it can be used as a *stepping stone* to compromise the home network laterally or as a proxy for external attacks.



Which DVR Brands Are Attacked the Most

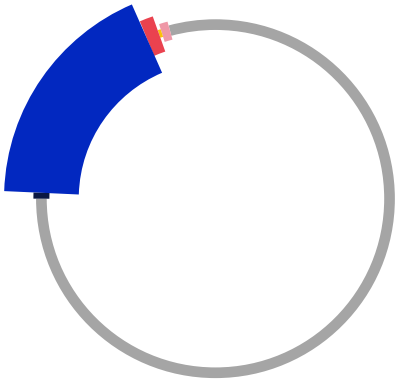
6 BRANDS ARE TARGETED BY 87% OF THREATS TO DVRs



Hikvision, Dish, RaySharp, Q-See, Dahua, and TVT are targeted by close to 90% of all threats to DVR devices. When we consider the device population, the impact of these brands seems even more substantial, as they make up less than a quarter of all DVR devices.

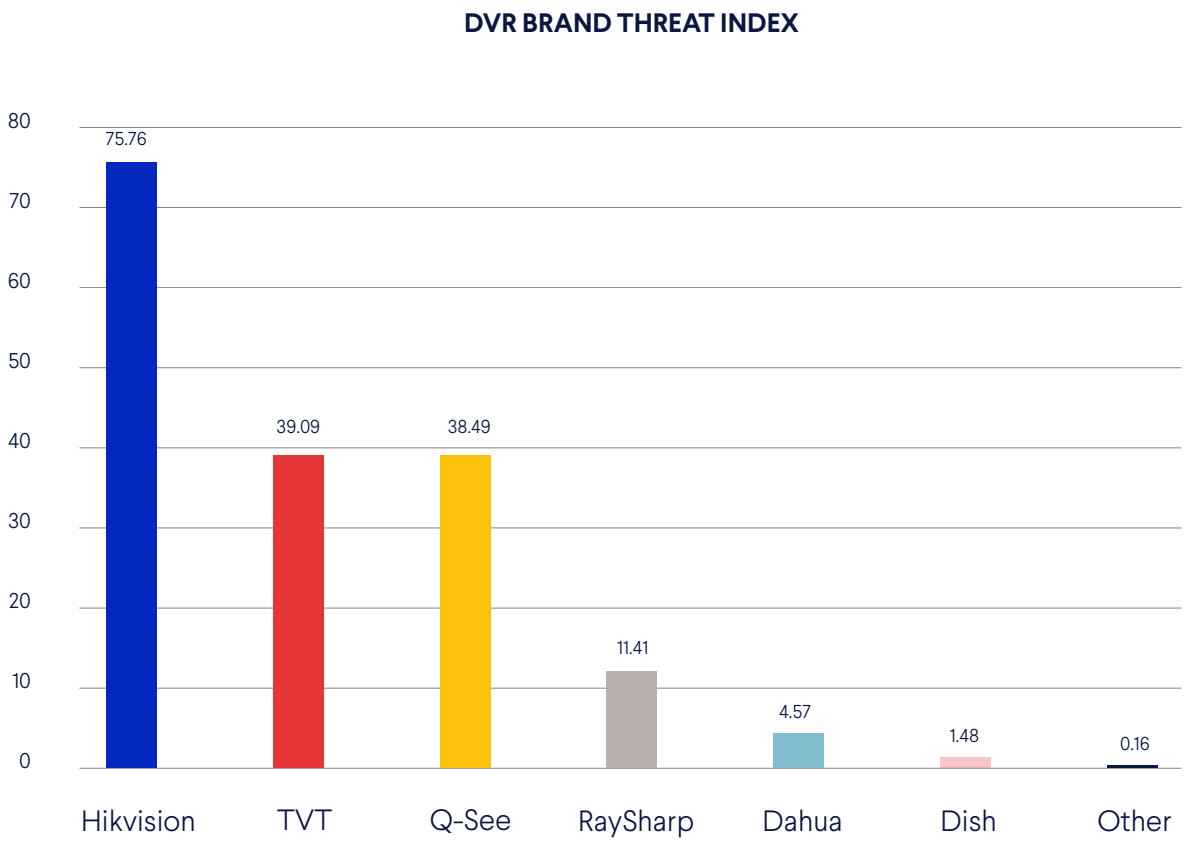
THOSE 6 BRANDS MAKE UP 21% OF ALL DVRs

Evidently, only Dish has a truly sizeable DVR device population, therefore its threat index is much smaller than that of the other 5 most targeted brands.



- Dish 18.34%
- RaySharp 1.16%
- Dahua 0.42%
- Hikvision 0.42%
- Q-See 0.24%
- TVT 0.05%
- Other 79.00%

DVR Brand Threat Index



Hikvision, Q-See, TVT, and RaySharp have substantially outsized threat indexes among DVR devices. We see that beyond the 6 most attacked brands, the threat index of all other DVR devices is much smaller. This is a good example of how a few bad apples can create a bad name for the whole category of devices.

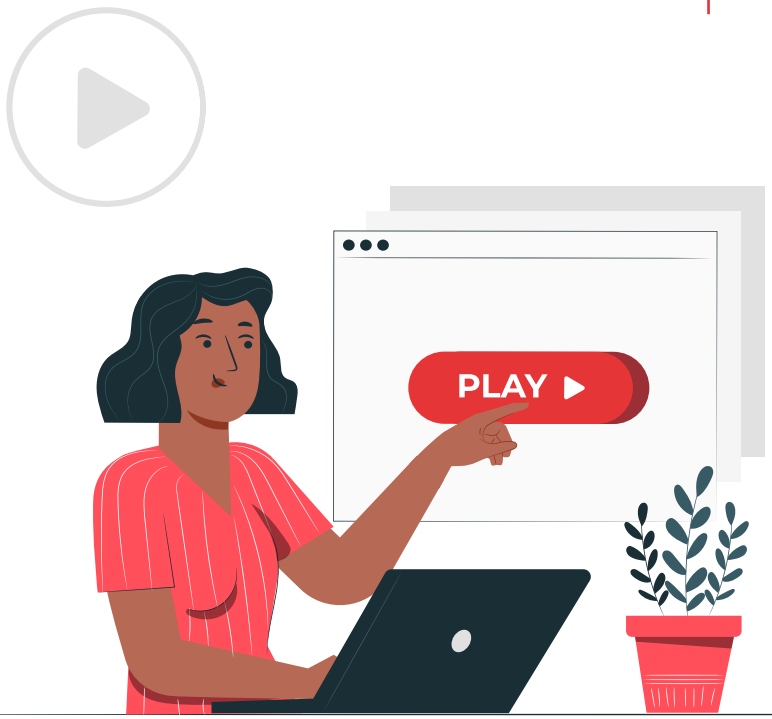
IP CAMERAS

24

IP Cameras

IP cameras are famous for having poor security. They are being hacked not only to spy on people, but also to participate in coordinated DDoS attacks. Infected IP cameras also often become part of botnets. Many IP cameras have poor configurations, such as publicly known hard-coded administrator credentials, which make them easy targets for brute-force attacks. Since, like NAS devices, IP cameras are accessed remotely by their users, they are often exposed to the Internet. Like DVRs, many IP cameras autoconfigure the home router via UPnP to open ports to the Internet.

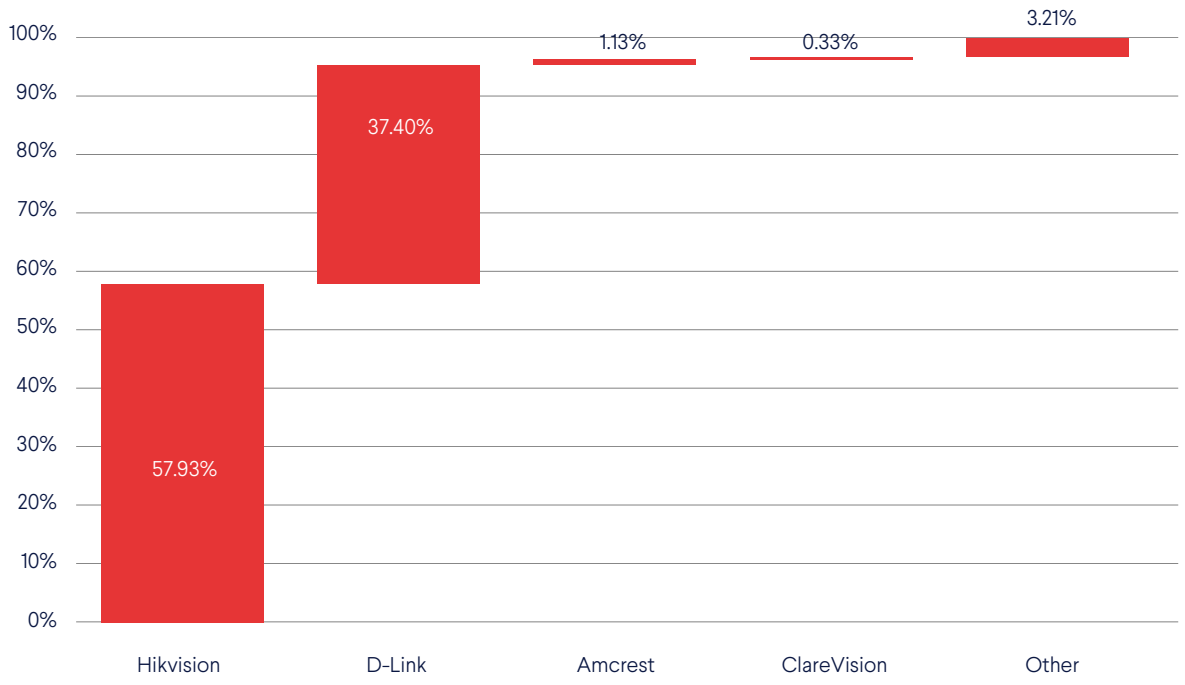
Of the top 30 most attacked IoT devices, all are IP cameras from various vendors.



Which IP Camera Brands Are Attacked the Most

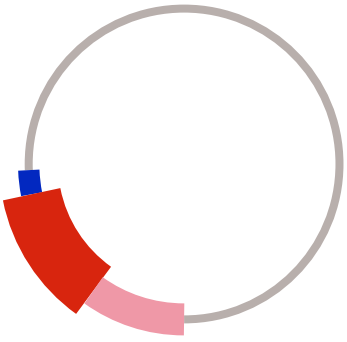
Much like with DVR devices, a handful of brands attract the bulk of threats. Just 4 brands get attacked by more than 96% of attacks. Hikvision and D-Link devices have substantially outsized threat footprints with over 95% of threats, while Amcrest and ClareVision are targeted by just 1.13% and 0.33% of threats, respectively.

4 IP CAMERA BRANDS ARE TARGETED BY OVER 96% OF THREATS



When we take IP camera population numbers into account, the distribution of threats becomes even more staggering: none of the most attacked brands make up more than 12% of all IP cameras. Interestingly, there are hundreds of different IP camera vendors and brands out there and identifying some of them can be a challenge when the only difference is the sticker on the camera.

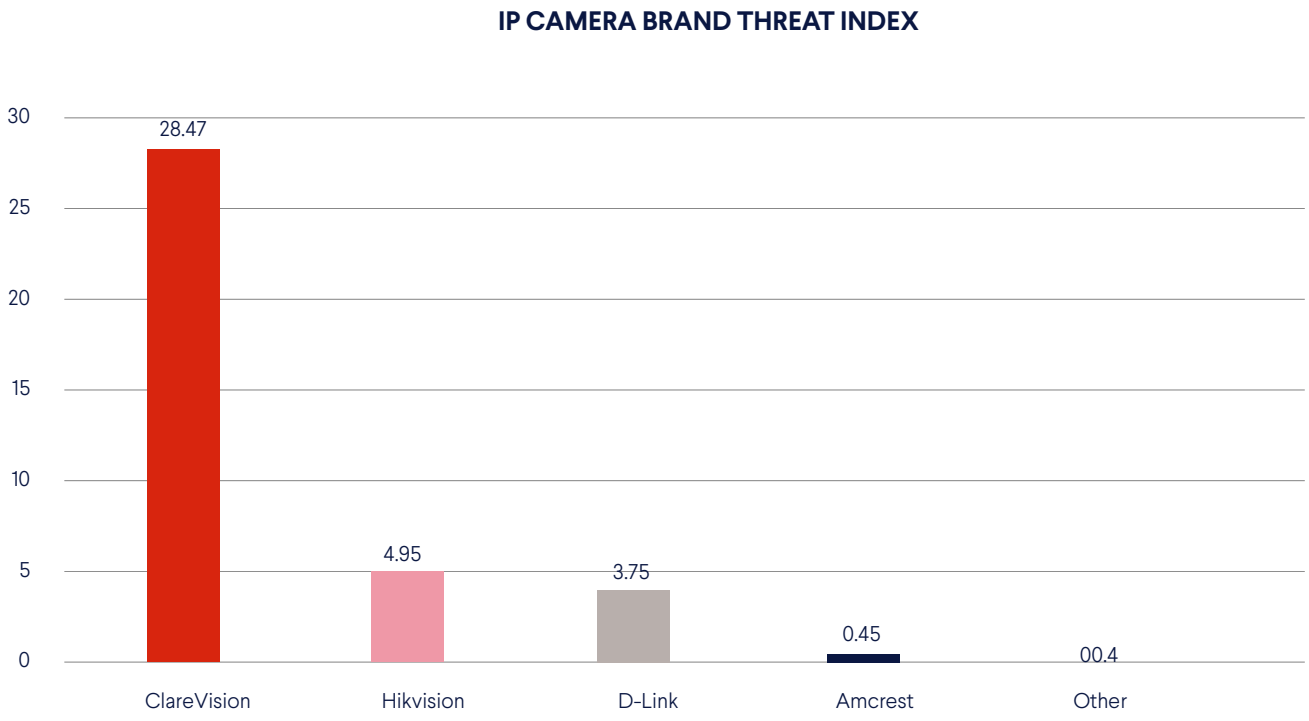
THOSE 4 BRANDS MAKE UP JUST OVER 24% OF ALL IP CAMERAS



- Hikvision 11.71%
- D-Link 9.97%
- Amcrest 2.53%
- ClareVision 0.01%
- Other 75.77%

IP Camera Brand Threat Index

Even though Hikvision and D-Link devices are targeted extremely often, they do not have the highest threat index among IP cameras, as ClareVision devices are attacked almost six times as often! Other brands have a negligible threat index, when compared to the 4 most attacked brands.



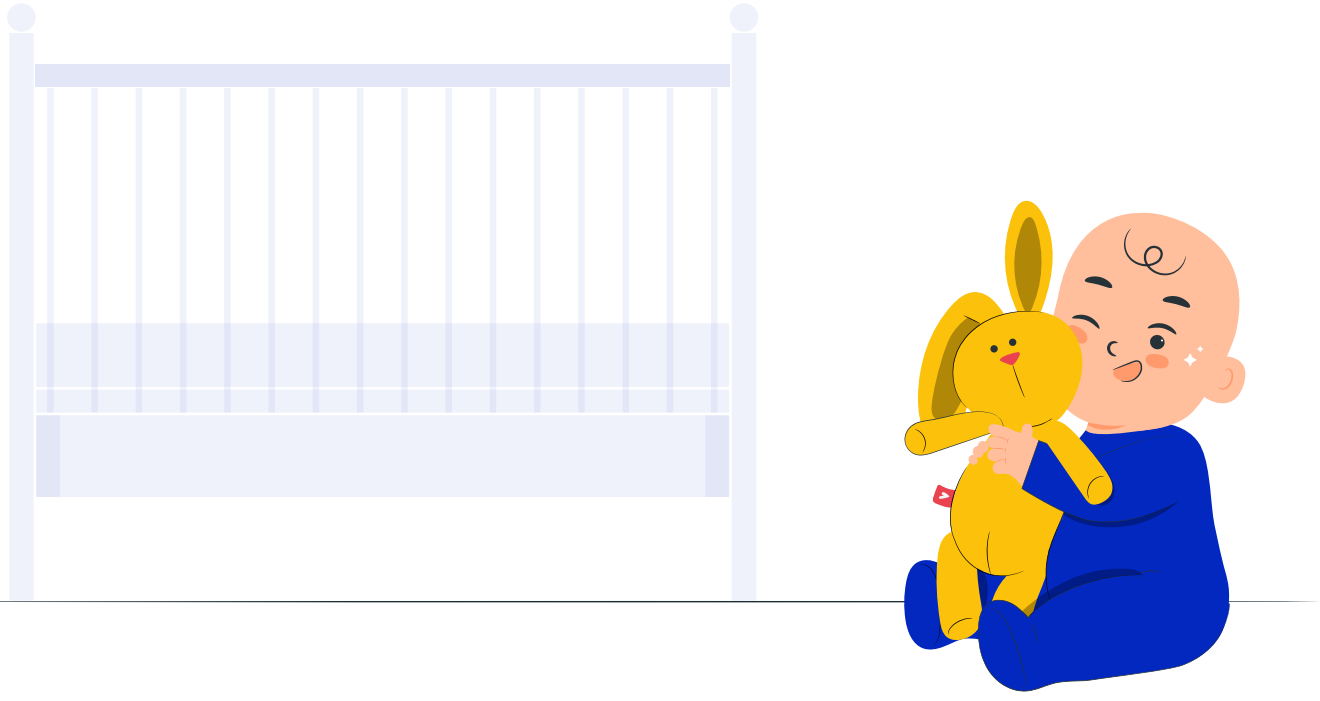
BABY MONITORS

28

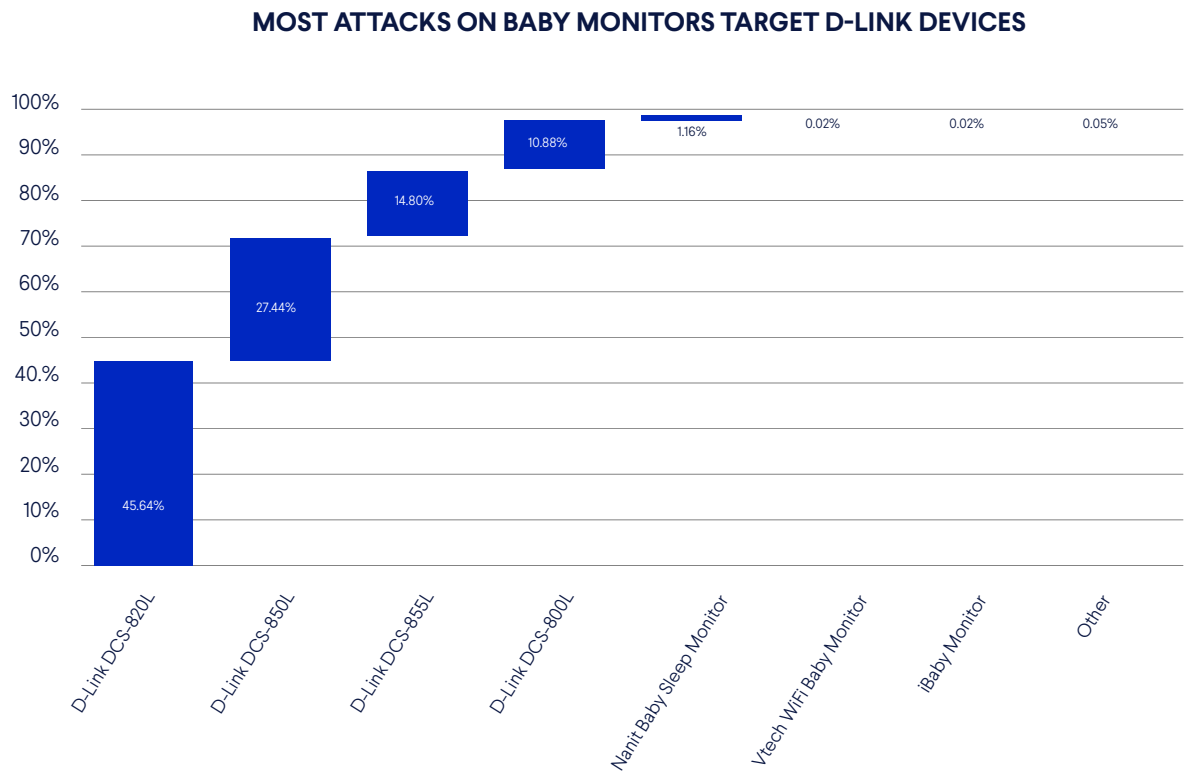
Baby Monitors

Large hacks of baby monitors are often portrayed in the media and resonate within society, since these devices are placed in very private settings. Our data shows that baby monitors are indeed attacked very often, albeit not as often as NAS devices or IP cameras. Most of the time, baby cameras are running the same software and have the same vulnerabilities as IP cameras. Baby monitors with cloud-only interfaces are safer from these types of threats, but can be still vulnerable to other attack vectors, like password reuse.

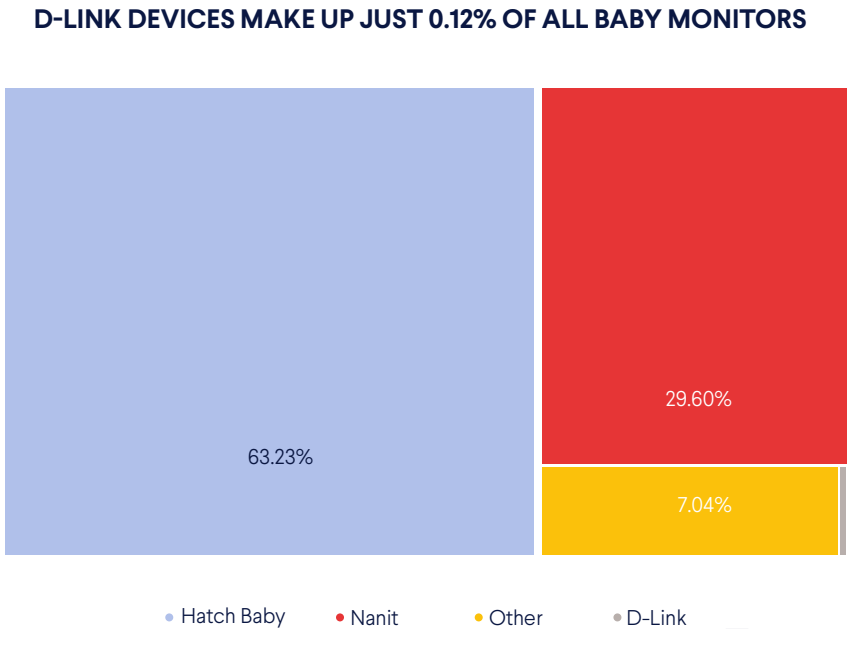
The threat landscape of baby monitors looks rather surprising, as our data clearly shows that just a few D-Link devices are being targeted by almost all (98%) of all threats to baby monitors.



Which Baby Monitor Models Are Attacked the Most



D-Link devices have an outsized threat profile with a tiny percentage of all baby monitors in use.



AUDIO-VIDEO DEVICES

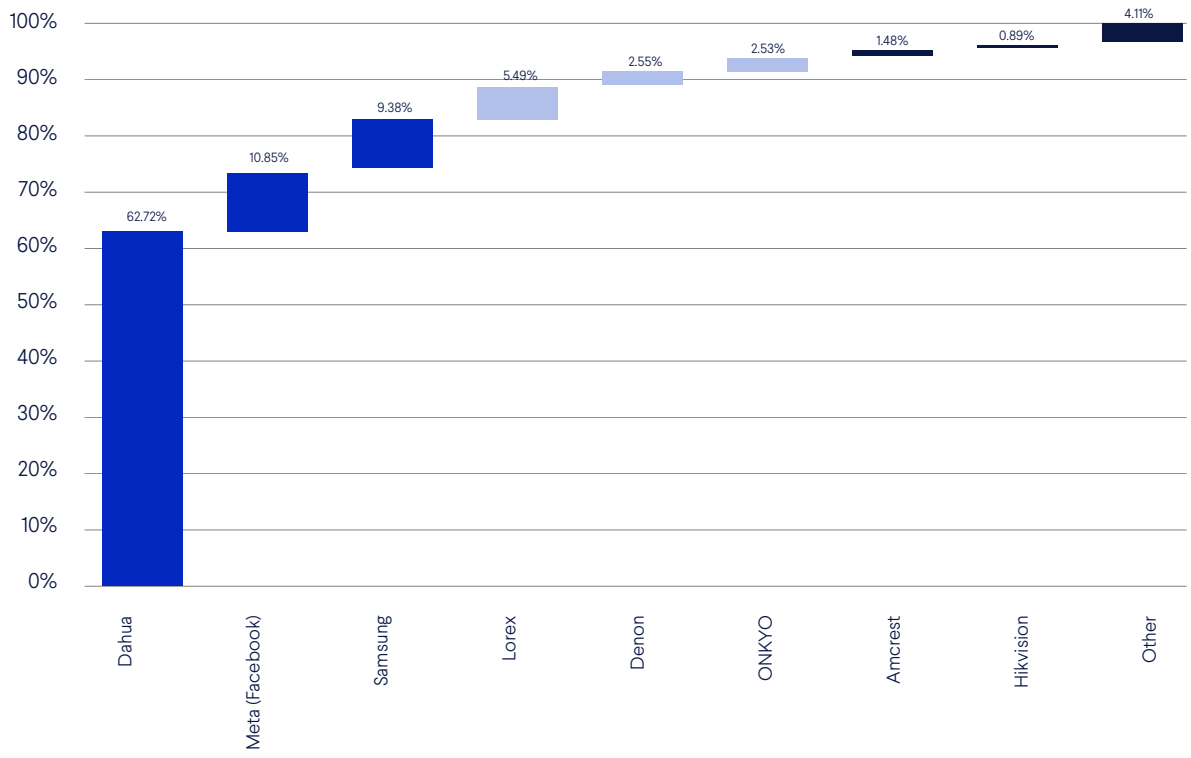
31

Audio-video Devices

The audio-video device category combines a variety of devices that perform video conferencing, audio, video streaming. Quite a few brands are targeted by threats in this category.

Which Audio-video Device Brands Are Attacked the Most

DISTRIBUTION OF THREATS TO AUDIO-VIDEO DEVICES BY BRAND

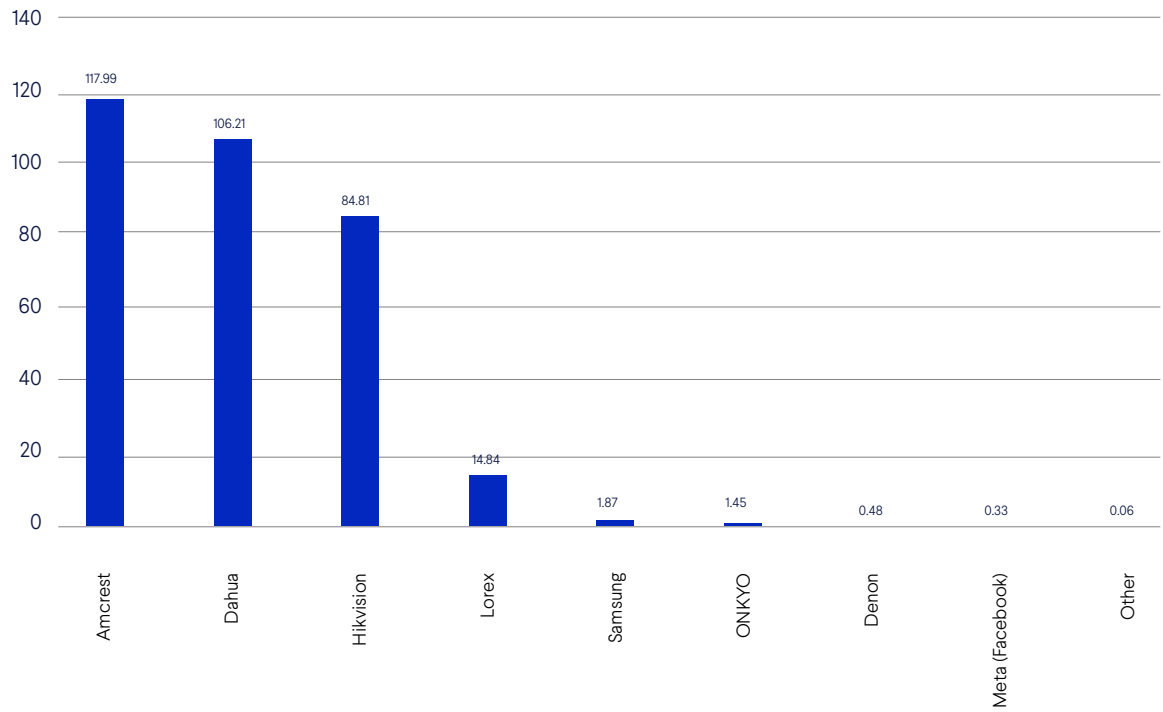


Dahua devices attract almost two-thirds of all threats, followed by Meta and Samsung, which are targeted around 10% of the time.

Audio-video Device Brand Threat Index

When we look at the audio-video device threat index, Amcrest, Dahua, and Hikvision emerge as the most attacked device brands on average.

AUDIO-VIDEO DEVICE BRAND THREAT INDEX



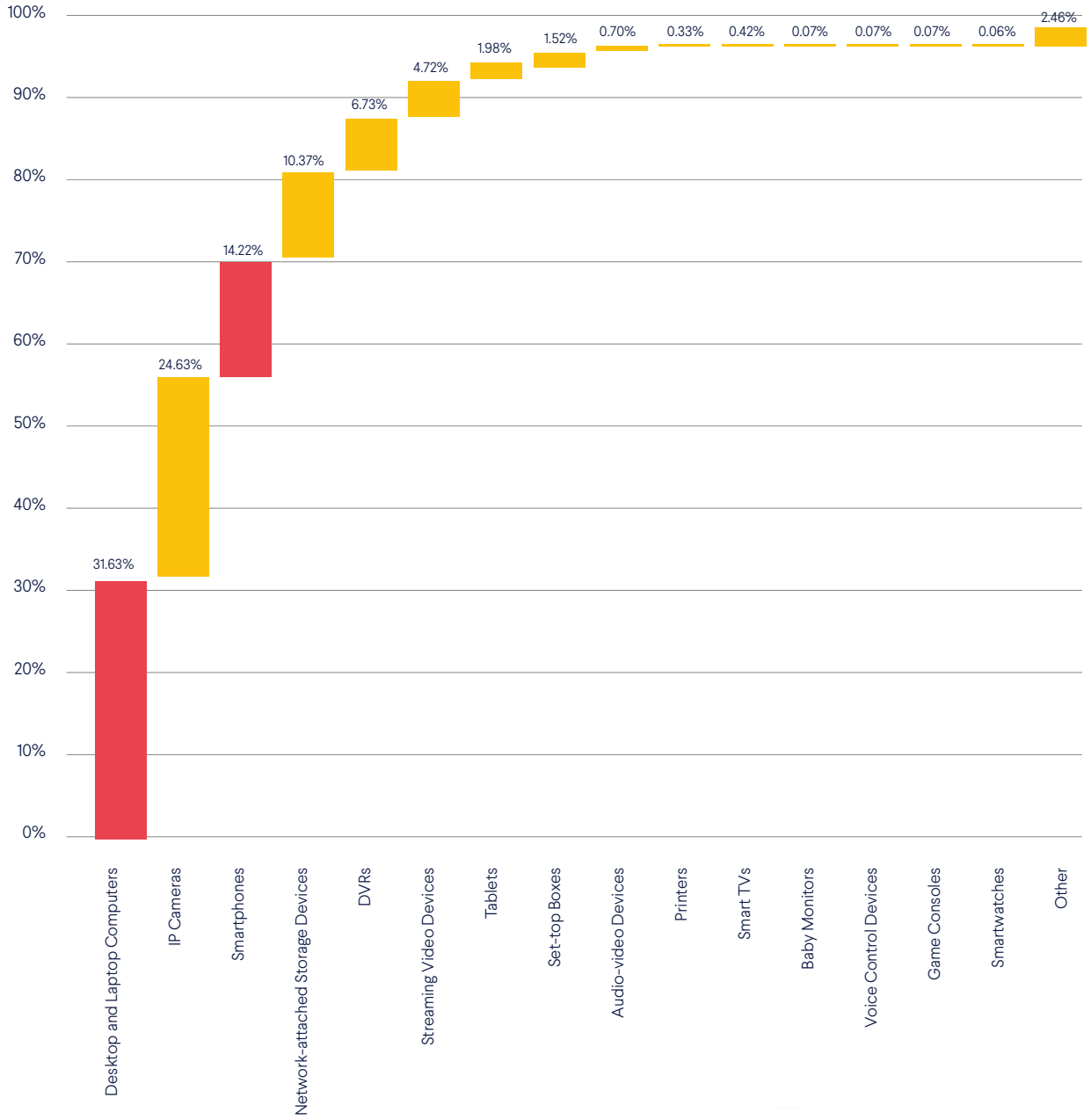
THREATS TO ATTENDED DEVICES

34

Threats to the Most Popular Devices

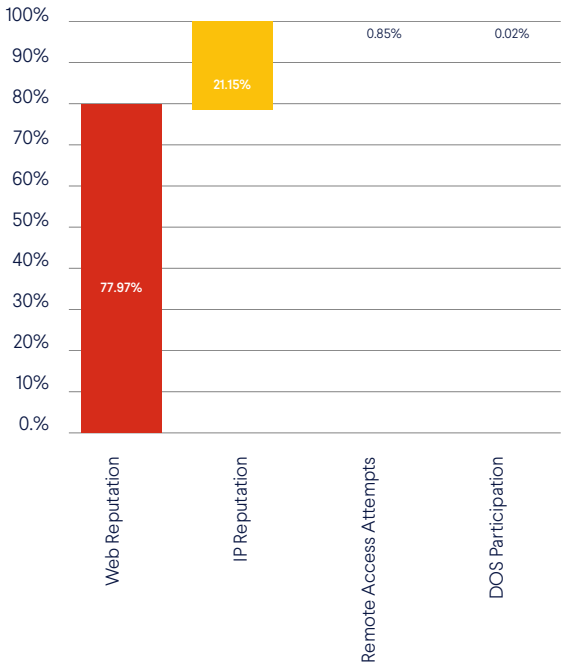
Smartphones and computers make up around 60% of all connected devices. Even though the threat indexes of these devices are not extremely large, these two categories still attract around 45% of all threats that are stopped by our web and IP reputation solutions.

THE CONNECTED DEVICE THREAT LANDSCAPE 2022

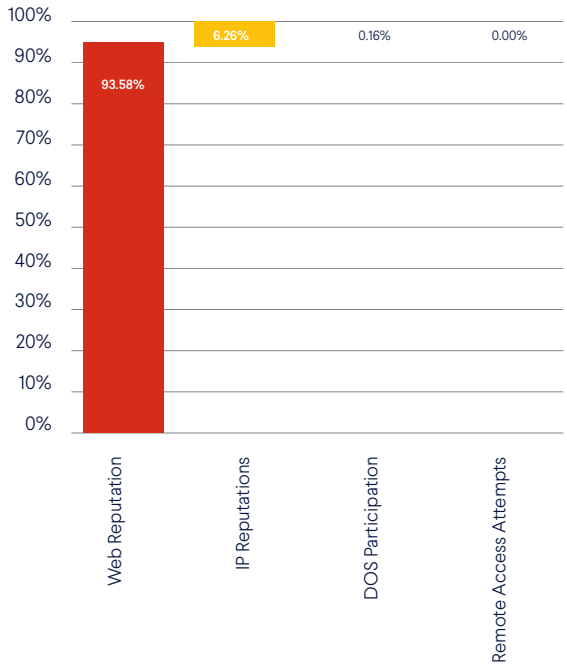


Computers and smartphones also have a different threat type profile – while most IoT and background devices get IP reputation threats from outside the home network, attended devices have more secure configurations. Instead, web reputation threats are a key factor in the safety of smartphones and computers.

THREATS TO COMPUTERS



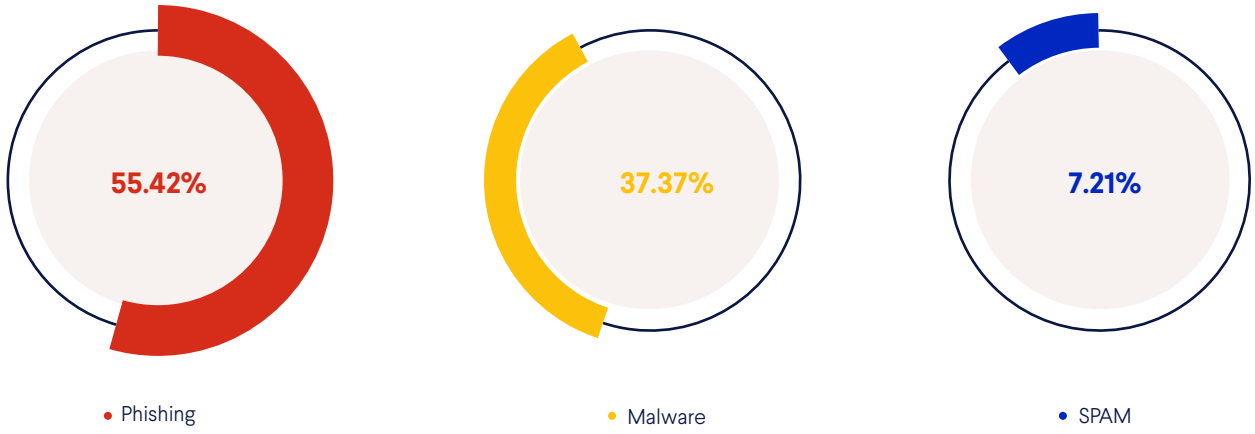
THREATS TO SMARTPHONES



Web reputation threats are a key vector in end-user security. Our data shows how the majority of threats to smartphones and computers come from attempts to access malicious URLs: fraudulent (phishing) websites, spam or malware distribution sites.

Web Reputation Threats

WEB REPUTATION THREATS



Online phishing accounts for more than 55% of all web reputation threats. As noted in the introduction of this report, every month, end-users in 56% of homes attempt to access phishing websites. These phishing threats range from fake bank websites to fraudulent charities and beyond.

As our algorithms identify and block millions of phishing websites, machine learning helps bridge the gap between when these sites appear and when they are added to industry blocklists. The short-lived nature and novelty of these sites makes them hard to detect at scale without using advanced machine learning algorithms.

Having the advantage of protecting tens of millions of households, CUJO AI has the best real-life datasets to prevent phishing threats.

Adware

Adware campaigns have grown significantly in 2022. An analysis of the last 12 months of Web Reputation data shows that several adware distributors had a 300% larger footprint in the second half of the year.

Adyourexchange[.]com, omnatuor[.]com were some of the fastest growing adware campaigns.

Web3 Scams

“

Web3 is a term used to describe “a new iteration of the World Wide Web”, based on decentralization and blockchain technologies. Cryptocurrencies, non-fungible tokens (NFTs), and other token-based economies are a major part of the Web3 movement.

The transaction technologies used in Web3 applications are most often irreversible, making them a good environment for scammers – once a user is fooled into making a transaction, there is very little they can do to get their tokens back.

There is an entire shadow economy of Web3 scams, where scammers can buy or rent everything needed to run a scam. CUJO AI Labs have recently published an analysis of one such NFT scam as a service that was distributed for free and used to scam the scammers themselves, too.

To get a better idea of how widespread Web3 scams are, we analyzed a recent sample of our data that showed at least 0.5% (20 out of a sample of 3,500) of new, previously unknown phishing threats were related to Web3 scams.

The CUJO AI Labs team expects Web3 scam numbers to grow significantly in the near future, as the number of Web3 scam websites discovered daily is slowly growing, according to our data.

Kimmo Kasslin

VP of Research Laboratories
CUJO AI

CONCLUSION

39

Conclusion

The cybersecurity landscape is extremely complex and has a lot of depth. This year's report looks at it through the lens of device types and models to provide *a new way* of approaching the problem, as some device types clearly face more threats due to their value, accessibility or known vulnerabilities.

There are some outlines we can draw between unattended (mostly IoT) and attended devices (smartphones and computers): the latter face growing phishing threats, while background devices can be targeted en-masse by botnet malware.

While attended device security depends on the user's behavior, unattended device security depends on vendors and device configurations, as well as the time users spend finetuning the security of their devices. In any case, such devices get bombarded by automated scanners and exploitation services constantly.

There is a growing need for security regulation in the connected device space, but it should be noted that no regulation can bridge the gap between when a vulnerability is discovered, and an update is installed. In some cases, we do not expect end-users to update their devices due to technical difficulties, poor notification practices, buggy patches or lack of time and priority.

As evidenced by our data, an average household is threatened every other day. While the number of connected devices continues to grow, we expect IoT security to become an even greater issue. While more consumers should install and use security software on attended devices, they also increasingly need protection for other connected devices on their networks. Perimeter protection with CUJO AI Sentry can help network service providers protect their end-user networks.

To access more reports and research by CUJO AI Labs, visit our blog and the ISP security hub.

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.

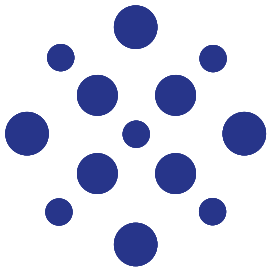
Sentry is a proven solution that already protects tens of millions of homes around the world.

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 1 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 almost 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