Internet Service Providers and Cybersecurity

Device Identification and Security at the Edge

An Operational Practice prepared for SCTE by

Scott Dotto
Senior Product Manager
Charter Communications
6360 S Fiddlers Green Circle
(303) 721-3758
Scott.Dotto@Charter.com

Justinas Bisikirskas, CUJO AI

Kyle Johnson, Charter Communications

Leonardas Marozas, CUJO AI

Tyson Vinson, Charter Communications

Table of Contents

List of Figures

List of Tables

1. Introduction

Cybercrime is a pervasive and increasing risk to businesses and consumers alike. This increasing threat is driven by the expanding influence of digital lives, the growing reliance on technology to deliver essential services and the rise in connected devices, which are projected to reach an estimated 15 billion by the end of 2023. According to a report by Cybersecurity Ventures, the global cost of cybercrime is predicted to reach a staggering $10.5 trillion annually by 2025 (about $1,300 per person on average).[1] In the first half of 2022, an estimated 53 million Americans were impacted by cybercrime, costing US households billions of dollars.[2] Such a massive problem demands effective solutions to safeguard customers' devices, data and financial security.

Internet service providers (ISPs) are in a unique position to improve the cybersecurity landscape. To serve customers, ISPs must know certain traffic characteristics such as IP source and destination. These observations offer ISPs valuable insight into the capabilities of devices on the network and whether traffic from those devices may be suspicious or malicious. Further analysis may uncover vulnerabilities in customer devices and other cybersecurity risks.

The knowledge gained from this analysis may be used to develop new security services and techniques. Sharing deidentified and aggregated information (with a commitment to protecting personal information and restrictions on how that information can be used) with relevant parties—manufacturers of offending devices, other ISPs, or regulatory and standards bodies—can lead to better outcomes in securing customers' data, identities, devices and, consequently, the internet as a whole. This deidentified and aggregated data can be directly used by other parties to make informed decisions to drive industry standards and respond promptly and efficiently to an ever-evolving threat. Additionally, more specific information can be shared with impacted customers so they may take action to protect themselves.

ISPs have a critical role in enhancing cybersecurity and securing the internet. ISPs' access to traffic data empowers them to take proactive steps in protecting their customers and the internet ecosystem at large. By leveraging these insights and collaborating with relevant stakeholders, ISPs can meaningfully contribute to mitigating cybersecurity threats to customers.

2. Cybersecurity and ISPs Landscape

ISPs are a major component in the infrastructure of the internet ecosystem, facilitating the smooth flow of data between end-users and various online resources. Protecting this critical infrastructure, as well as customer security, is standard practice and a high priority. ISPs employ a variety of techniques for security, including but not limited to:

1. **Traffic Filters:** These filters close off commonly abused & attacked services, such as open DNS resolvers and SMTP servers.
2. **Distributed Denial of Service (DDoS) Scrubbing**: DDoS scrubbing helps remove high-volume attack traffic used to impact the availability of internet access.
3. **"Walled Gardens" or Enclosed Network Environments:** Isolates a compromised customer to prevent spreading malware and to provide a call-to-action for the customer to contact the ISP for further assistance.
4. **Endpoint protection software:** Customers can protect their laptops and mobile devices via software provided by the ISP

These techniques are robust and capable; however, ISPs have a responsibility and opportunity to protect customers at all relevant network layers and on all devices. Techniques available at the core network can be reinforced by data and advanced learning models deployed at the edge. These methods enhance the

ability to apply policy to traffic at a more granular level—the device or application. Of particular importance is providing customers with protection for the individual devices they connect to their home WiFi. This enables an ISP to protect multiple households or groups of users and against threats that target individual devices or specific applications within a household.

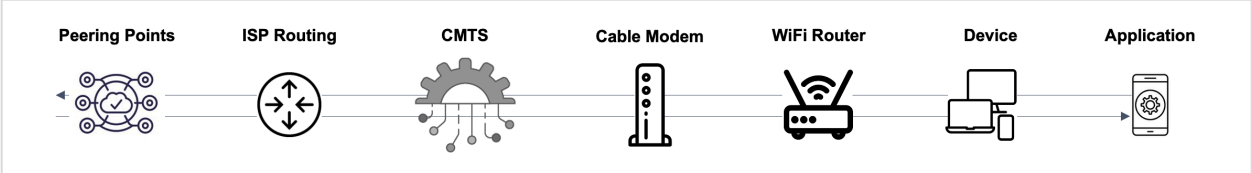

Figure 1: Internet Access Layers

ISPs have a responsibility and the unique capability to protect customers at all relevant points of service delivery. An agent on the WiFi router bolsters cybersecurity for customers beyond the traditional protection at peering and core network.

3. Tools and Techniques to Gather Data

3.1. Connected Device Identification

At the edge of their network, ISPs may deploy capabilities on customer premises equipment. One such example is Charter Communications, which employs a solution developed by CUJO AI, a company focused on cybersecurity and advanced learning models. This solution is integrated onto the WiFi router platform.

By deploying an agent on the WiFi router, it can capture unique device identifiers from network metadata, which is then analyzed by a classification engine to categorize each device by type, brand, model and the device's specific capabilities. For instance, the engine may determine that a device is a streaming device and whether it supports 4K resolution, among other characteristics.

The classification engine also assigns a unique device identity, ensuring consistency in measuring data over time for many essential use cases, including quality of experience (QoE) metrics, improved customer support and security performance over the device's lifespan. Recent privacy measures, such as private MAC and random MAC, may obfuscate the data to uniquely identify traffic overtime.

Improvements in privacy for online activities also do not necessarily equate to an improved security profile for devices. While many innovative solutions have been introduced to support consumer privacy, they must also aim to ensure that consumers remain protected while online. Appropriate security measures play a vital role in safeguarding devices from potential threats and attacks.

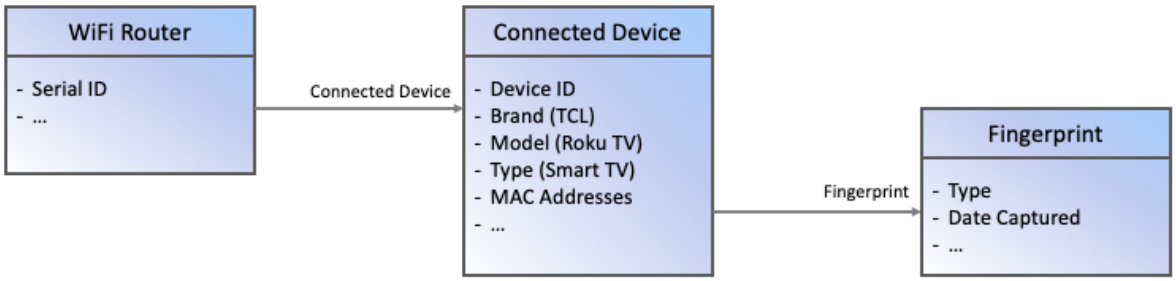

Figure 2: Device Identification

Device identification solution gives both details on the type of device and unique fingerprints.

3.2. Connected Device Security

Each device, depending on its profile, communicates differently on the network making it impractical to have a single cybersecurity solution that fits all. For instance, devices which support web browsing, like smartphones, require safe-browsing security to protect consumers from rogue websites or malicious URLs. On the other hand, IoT devices necessitate a different type of protection, such as blocking unauthorized access from malicious IP addresses and detecting malicious device behavior. Security solutions deployed at the edge should be multi-layered, tailoring appropriate security services specifically to each device based on its profile.

To ensure security for all connected devices, real-time network metadata is captured for processing by a low latency AI engine. This engine investigates and categorizes cybersecurity events into four distinct categories: secure traffic, secure browsing, outbound denial of service (DoS) prevention and smart device protection (remote access threats).

This paper focuses on secure traffic cybersecurity events, which are the most common threats to single-purpose devices such as smart home IoT devices (*single-purpose device* implies a device that lacks a browser and typically requires minimal interaction with the user to perform its purpose). Unlike secure browsing threats, secure traffic better reflects the devices that pose a higher risk to cybersecurity, as it factors out threats blocked due to user behavior (e.g., clicking on an insecure link through a browser on a mobile phone). By focusing on secure traffic for single-purpose devices, the analysis excludes the cybersecurity events stemming from an individual's unsafe browsing behavior and allows for a better comparison of the devices themselves.

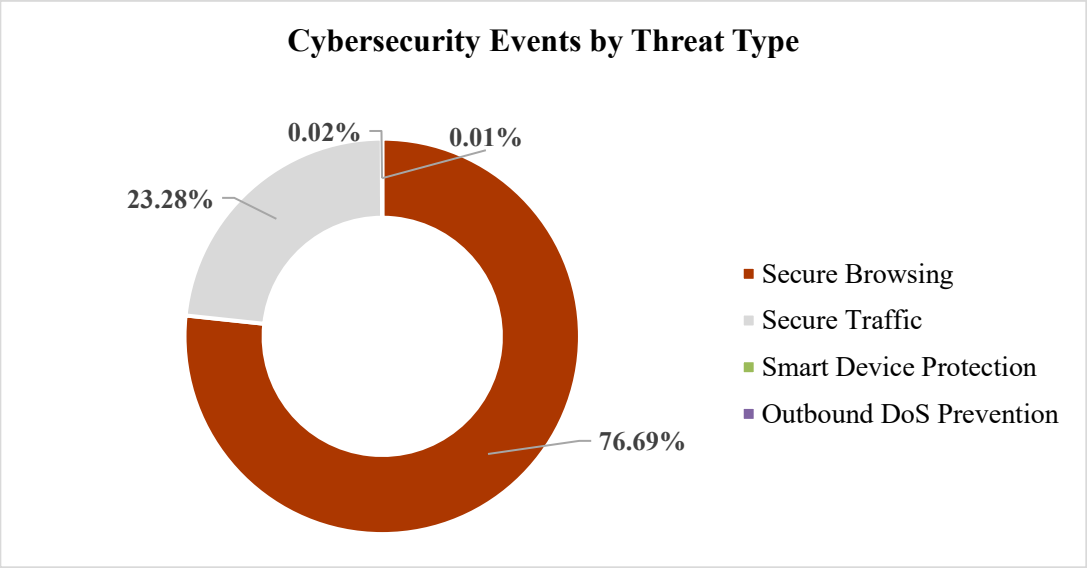
Cybersecurity Events by Threat Type
0.02%
0.01%
23.28%
76.69%
Secure Browsing
Secure Traffic
Smart Device Protection
Outbound DoS Prevention

Figure 3: Cybersecurity Threats by Type

Secure browsing and secure traffic account for the vast majority of cybersecurity events (99.97%)[3].

Table 1: Cybersecurity Event Type Definition

Secure Browsing protects users from accessing websites that are known to be malicious or suspicious
Secure Traffic monitors network traffic at the IP layer; if traffic (inbound or outbound) is detected from a known, malicious IP residing in the reputation database, the connection is blocked
Outbound DoS Prevention prevents customers' devices from participating in a DoS attack; attack traffic to the victim IP address is blocked, while other traffic is allowed
Smart Device Protection detects and blocks IoT communication that deviates from normal communication patterns

When a cybersecurity event is detected, the specific malicious traffic to or from the device is automatically blocked in real time, preventing any negative impact to the customer and their devices. Furthermore, cybersecurity events are recorded for further analysis.

The device identification dataset can be combined with the cybersecurity threat dataset. This integration allows for in-depth exploration of the types of devices, brands, and models that over-index on cybersecurity events—devices that tend to attract unwanted attention from cybercriminals. Identifying these devices constitutes the first step toward better protecting internet customers.

4. Data Analysis

4.1. Connected Device Overview

Unsurprisingly, the most prevalent devices in customers' homes are phones and computers. While many of these devices are subject to cybersecurity threats, most of these threats are from either insecure browsing behavior or exposing ports to the internet, rather than other threat categories to which all devices are susceptible. In fact, most threats (approximately 80%)[3] are related to unsafe browsing and infections directing users to insecure and malicious content. Since cybersecurity events may arise from either user behavior or characteristics of the device, when analyzing the security of a device it is critical to control for user behavior. For devices with multiple, divergent use cases and especially those with brower support (such as phones and computes), it may be difficult to draw strong conclusions about the device.

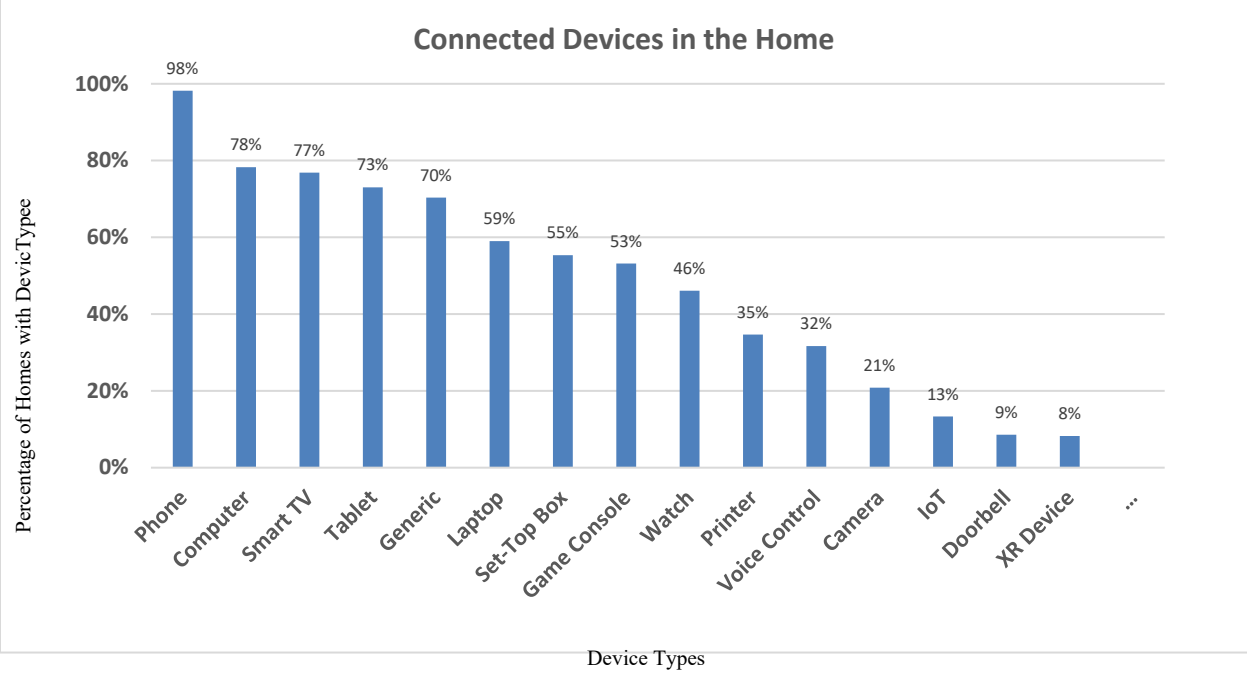

Figure 4: Device Penetration by Category in Charter Homes

Almost all homes have mobile phones (98% of homes), computers (78%) and smart TVs (73%). The prevalence of IoT devices such as security cameras, doorbells, thermostats, smart lights or plugs is also increasing. This chart omits less prevalent device types[3].

Conversely, for single-purpose devices lacking a browser, the volume of cybersecurity incidents may lead to clear insights on which devices tend to have more vulnerabilities or invite more attacks. Certain IoT device types (e.g., IP cameras, DVRs and doorbells) and network attached storage (NAS) devices tend to over-index on cybersecurity threats—these device types, when controlling for the number of devices represented within each category, consistently have more cybersecurity attempted actions per device. For these devices, the most common blocked security threat is secure traffic, a connection attempt from known, malicious IP addresses.

Over 99% of connection attempts arise from recognized, malicious IP addresses, while less than 1% of threats originate from the infected device, initiating communication with known botnet command and control centers or other malicious IPs. Known, malicious scanners can quickly identify new assets with open ports on the Internet, catalog them and attempt exploitation within seconds.

As Figure 5 below illustrates, IP cameras account for an outsized percentage of all threats observed while only constituting a small percentage of the devices (0.66% of total device count). IP cameras are a distinct category and differentiated from other cameras by sending digital data to be stored in the network. Similarly, NAS devices also over-index relative to other device types in cybersecurity events, accounting for 36% of Secure Traffic events while only accounting for 0.03% of all devices[3].

NAS devices and IP cameras are enticing targets for several reasons:

1. **Weak or Absent Security Features:** Many IoT devices, including NAS devices and IP cameras, lack essential built-in security features, making them an easy target.
2. **Lack of Regular Updates:** Despite the regular appearance of new vulnerabilities and subsequent exploits of NAS devices and IP cameras, they are not consistently updated. Both vendors and users share responsibility—vendors to deliver updates to patch known vulnerabilities and users to ensure devices are operating with the latest firmware.
3. **Value of Data or Function:** Devices that store valuable data, such as NAS devices (or cryptocurrency miners), or perform certain functions, such as IP cameras, are attractive targets due to potential gains for attackers in terms of data or information.
4. **Increasing Interconnectivity:** Many NAS devices and IP cameras expose ports to the internet, either via UpnP or by asking the user to manually configure forwarding on their routers.
5. **High Data Rates:** NAS devices and IP cameras, as opposed to many other IoT devices, transmit high-bandwidth data, enabling obfuscation of DDoS traffic by interspersing with higher-volume legimate traffic.

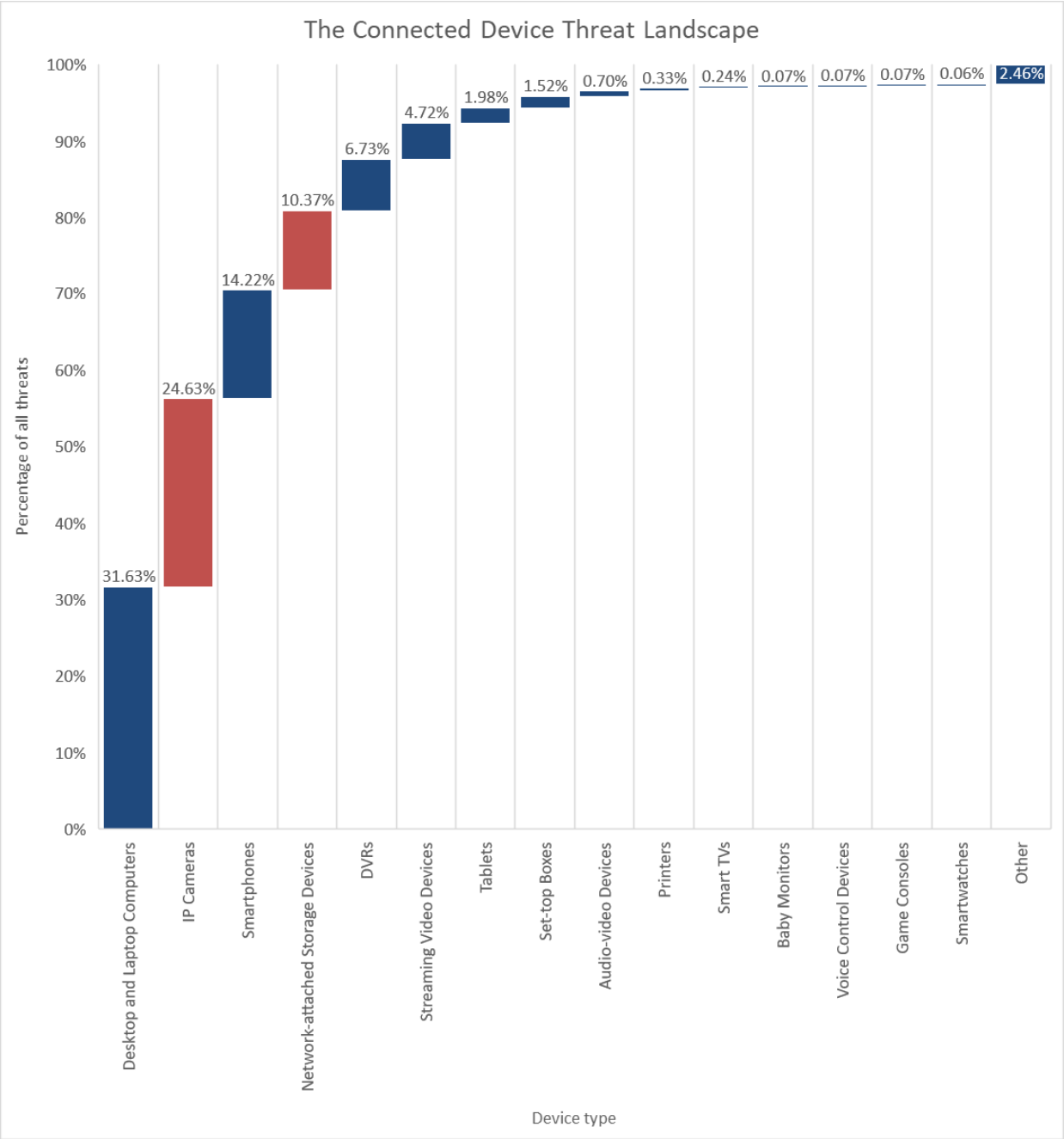

Figure 5: Percentage of Threats by Device Type

A relatively small number of device types account for most cybersecurity threat events[3].

While these device types often carry greater risk, recommending customers completely remove such devices from their homes is not a practical stance. Gaining insight into which specific devices within these categories pose the highest risk can offer more alternatives for effectively mitigating these threats.

4.2. Popular Brands and Models

This analysis can also be extended further to device brands and models. Comparing brands and models within a specific category better illustrates which brands and models over-index in cybersecurity events, given certain device types may just be inherently riskier to provide the services they are designed for. Devices from those over-indexing brands pose a higher risk to customers compared to their peer devices.

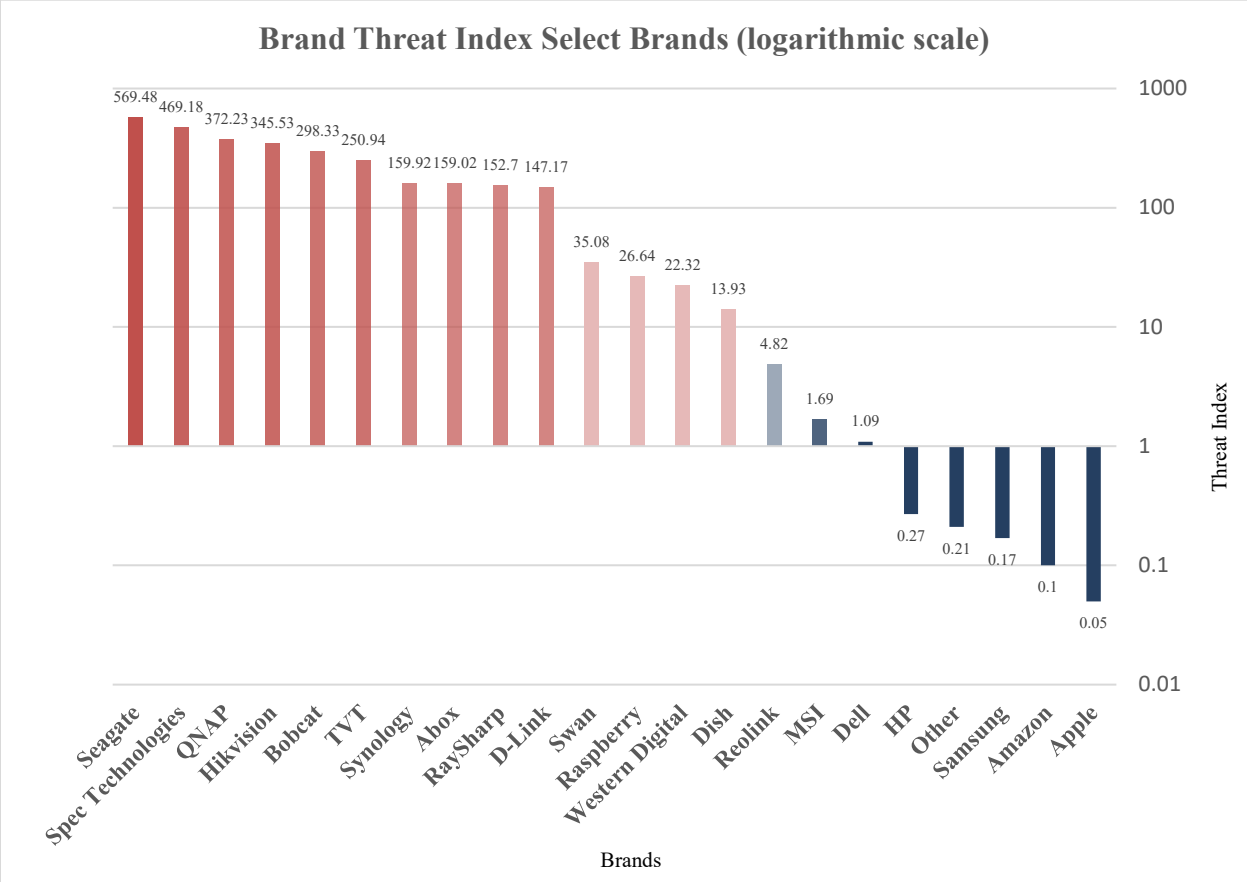

Figure 6: Brand "Threat Index"

The *threat index* represents the ratio of average threats per device in a category. A group of devices with a threat index above or below 1.00 experience 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[3].

The data indicates that well-recognized brands generally exhibit strong performance in terms of the number of threats per device. A significant portion of the brands that over-index in security threats are those with a smaller presence in the market. Notably, these brands also tend to correspond to devices within the categories previously identified as having a higher incidence of cybersecurity events, including NAS devices, IP cameras, doorbells (mainly equipped with cameras) and cryptocurrency miners.

Additionally, the data shows that a large preponderance of cybersecurity events come from a small number of device brands. Small, targeted efforts to correct issues with a few brands or models could potentially yield large reductions in cybersecurity events for customers.

Exploring more deeply how specific brands or models perform within their respective device type categories reveals more clearly which devices tend to pose the highest risks. Further investigation may provide insights into the underlying reasons for this trend. When factoring in the number of devices represented by each brand or model, a select few become more prominent.

5. Case Studies (Examples)

5.1. Hikvision IP Cameras & DVRs

As mentioned earlier, IP cameras generally have a higher incidence of cybersecurity events relative to other device types when controlling for number of devices represented. When examining specific brands within the IP camera device category, the disparity becomes even more pronounced. Despite constituting only 3.7% of the IP camera market share, Hikvision devices contribute to 58% of the documented cybersecurity threats[3]. Although another brand, ClareVision, fares even worse when factoring in the device count, their limited presence in the market mitigates the substantial threat to customers.

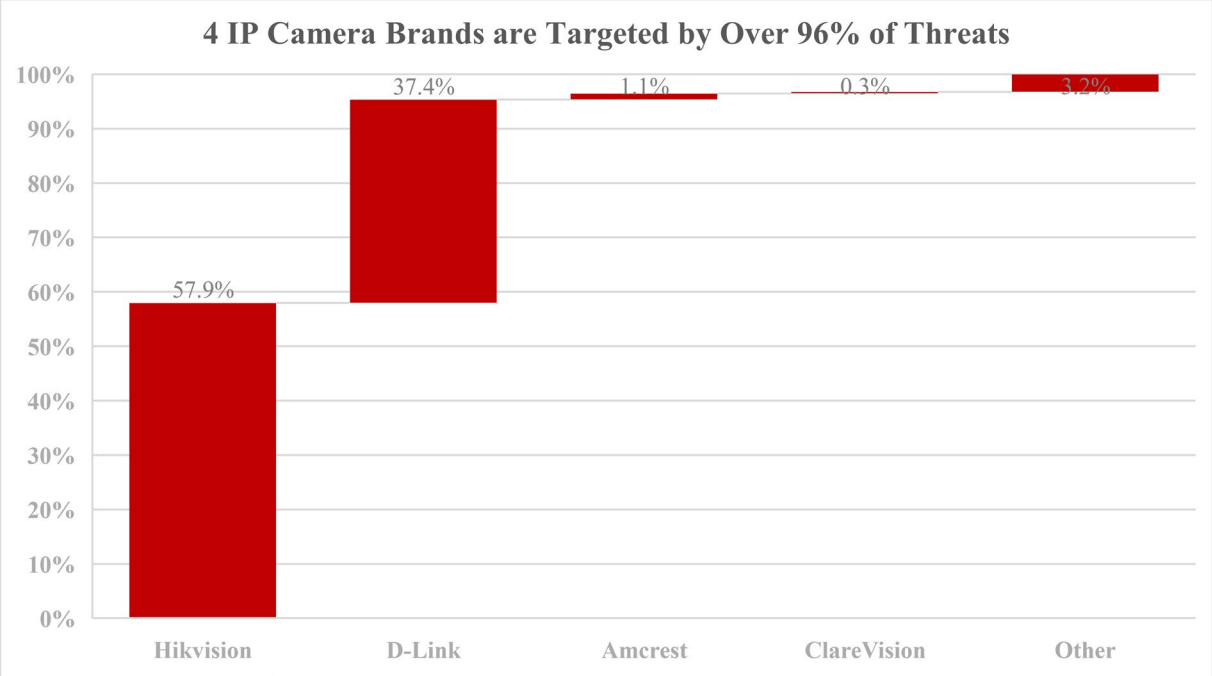

Figure 7: Percentage of Threats by IP Camera Brand

Hikvision accounts for over half of the threats against IP cameras, with D-Link accounting for another 37%. Combined they account for 95% of threats[3].

The notable prominence of Hikvision is even more intriguing in light of its ban by the Federal Communications Commission (FCC) in November 2022 due to its "unacceptable risk to national security."[4] Specifically, the ban blocks import and sale of new video surveillance and telecommunications equipment from Hikvision in the US "for the purpose of public safety, security of government facilities,

physical security surveillance of critical infrastructure, and other national security purposes."[4] This ban is not enforceable for all consumer-grade equipment, which may still find its way to customers in the US market. Hikvision devices potentially introduce an undisclosed risk to the consumers who possess them, originating from a company deemed a national security risk by the US government.

5.2. Space Monkey NAS Devices

Space Monkey was a brand of NAS devices offering a unique solution that combined the concepts of cloud storage and an in-home device. This approach provided a distributed and decentralized storage solution. Customers' data was not exclusively stored on their NAS device at home but was duplicated over Space Monkey's extensive device footprint. Frequently used files were locally cached for quick access[5].

In 2014, Vivint acquired Space Monkey but later chose to discontinue support for that business line[5] and the devices no longer receive firmware updates. These devices are now susceptible to cybercrime through known vulnerabilities, making them an appealing target.

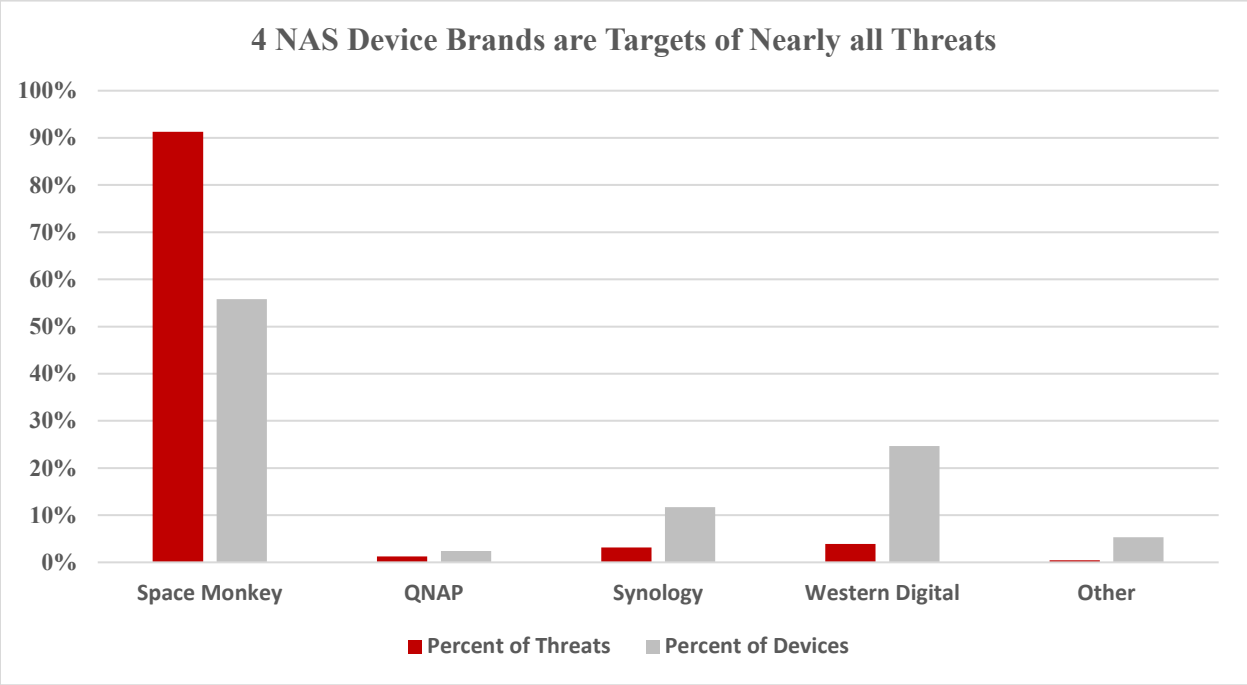

Figure 8: Percent of Cybersecurity Events and Number of Devices by Brand Among NAS Devices

Space Monkey devices account for over 90% of cybersecurity events observed across all NAS devices, while accounting for 56% of NAS devices observed in market[3].

6. What Actions Can ISPs Take?

As the above examples illustrate, a large percentage of the threats can be attributed to relatively few brands. That is helpful in considering a response strategy given a small, specific action may yield great results. Better securing a few devices may drastically reduce the number of cybersecurity events on an ISP's network.

This data provides insights into various measures to enhance network and customer security. First, for devices that might pose significant risks or are plagued by difficult-to-address vulnerabilities (such as those arising from limited or absent firmware support, as seen in the case of discontinued brands), the ISP could share this information with the customer. Often, customers may not be aware of the risks associated with using certain devices. In situations where devices are well supported and established, sharing deidentified and aggregated information directly with the brand/manufacturer could provide them with valuable insights to mitigate specific security risks and enhance their product line.

In the cases of both Hikvision and Space Monkey, notifying customers may be the most effective strategy for mitigating ongoing cybersecurity threats. Hikvision might not have the incentive to patch devices in a market that bans their products, and Space Monkey is no longer a supported device, thus lacking available updates. In other scenarios, conveying these insights to device manufacturers directly might equip them with the necessary information to rectify vulnerabilities, allowing their devices to perform more closely with industry peers.

This deidentified and aggregated information could also be reinforced by sharing it with other ISPs possessing similar capabilities. By exchanging additional data, ISPs could potentially verify or dismiss specific concerns. Cumulatively, there might be ample data and coverage to facilitate broader dissemination, reaching standards bodies, regulatory entities or open-source cybersecurity threat-sharing initiatives like Malware Information Sharing Platform (MISP) Threat Sharing. This data could contribute to aiding other organizations by offering information on emerging threats.

Another instance of such interorganizational collaborations could involve consortiums of incident response teams, such as Forum of Incident Response and Security Team (FIRST[6]). These platforms would enable partners and other organizations to collectively engage in threat research, enhancing their incident response capabilities. Furthermore, they could provide highly-valuable data for Special Interest Group (SIG) chapters, which could then elevate compliance and standards pertaining to data handling and protection based on the gathered data. Additionally, sharing information with Information Sharing and Analysis Centers (ISAC) or Information Sharing Analysis Orgranizations(ISAO), such as the Comm-ISAC may provide another path to explore threat information and best practices through exisiting entities. Many ISPs are already members of Comm-ISAC, and increased membership and participation may aid in collective goals regarding cybersecurity.

Collaboration with standards bodies or academic institutions with this data who could perform more extensive research would benefit internet security. The National Institute for Standards and Technology (NIST), for example, publishes device standards for consumer-grade IoT products, which may benefit from these insights. In addition to end devices, this data may guide other initiatives aimed at securing gateways and the traffic they route such as the “Gateway Device Security Best Common Practices” published by CableLabs[7].

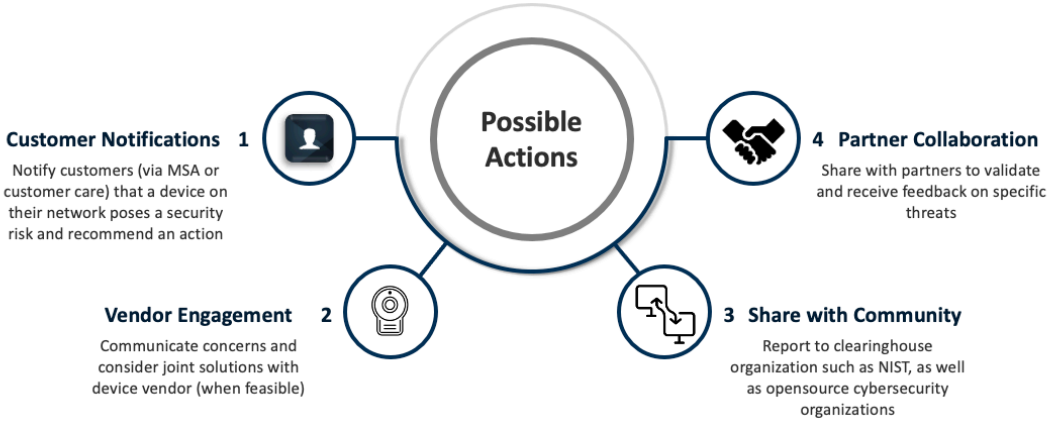

Figure 9: ISP Opportunities

7. Conclusion

The escalating threat of cybercrime poses a widespread and growing danger to everyone, and this challenge necessitates effective solutions to safeguard customers' devices, information and financial assets. ISPs have a distinct opportunity to play a pivotal role in bolstering the cybersecurity landscape.

ISPs should be building and deploying capabilities to profile single-purpose devices on their networks with respect to cybersecurity. And when armed with that information, ISPs should engage in discourse with all relevant parties to determine how best to fix uncovered vulnerabilities in end devices.

ISPs wield a critical function in elevating cybersecurity and safeguarding the integrity of the internet. Their access to traffic data empowers them to take proactive measures in shielding their customers and the broader online ecosystem. By harnessing these insights and collaborating closely with stakeholders, ISPs stand poised to make substantial strides in protecting customers from the ever-changing landscape of cybersecurity threats.

Abbreviations

AI	artificial intelligence
CMTS	Cable Modem Termination System
DoS	Denial of Service
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FCC	Federal Communications Commission
FIRST	Forum of Incident Response and Security Team
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IP	Internet Protocol
IR	internal report
ISP	Internet Service Provider
MAC	Media Access Control
MISP	Malware Information Sharing Platform and Threat Sharing
NAS	network attached storage
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
SIG	Special Interest Group
SMTP	Simple Mail Transfer Protocol
SSDP	Simple Service Discovery Protocol
Tbps	terabits per second
TCP	Transmission Control Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator

Bibliography & References

1. Forbes, “10.5 Trillion Reasons Why We Need a United Response to Cyber Risk”; https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=3b14abce3b0c
2. AAG, “The Latest 2023 Cyber Crime Statistics (updated July 2023)”; https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Headline%20Cyber%20Crime%20Statistics&text=1%20in%202%20American%20internet,the%20first%20half%20of%202022.
3. Charter Advanced WiFi Platform Data, June 2023
4. FCC, “FCC Bans Authorizations for Devices That Pose National Security Threat”; https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat
5. Wikipedia, “Space Monkey (company); https://en.wikipedia.org/wiki/Space_Monkey_(company)
6. https://www.first.org/
7. CableLabs, ““Gateway Device Security Best Common Practices”; https://www.cablelabs.com/specifications/CL-GL-GDS-BCP

