CUJOAI®

Cybersecurity Report 2024

PHISHING THREATS TO CONSUMERS ON HOME NETWORKS

Table of Contents

02
Executive Summary

04
Introduction
Glossary

07
General Threat Data Overview

IP Reputation Threats

IP Reputation Threat Breakdown

Safe Browsing Threats

Safe Browsing Threat Breakdown

13
Stopping Visits to Phishing Websites with AI

Types of Sites Spoofed by Phishing Campaigns

Phishing Tactics

Challenges

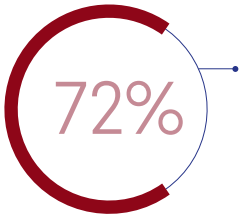
17
Conclusion

Executive Summary

02

Executive Summary

In the six months between April and October of this year, CUJO AI Sentry stopped over 3.23 billion threats, or 12,473 threats per minute, to consumer home networks. Two thirds (67.5%) of home networks were exposed to at least one cyber threat every month:

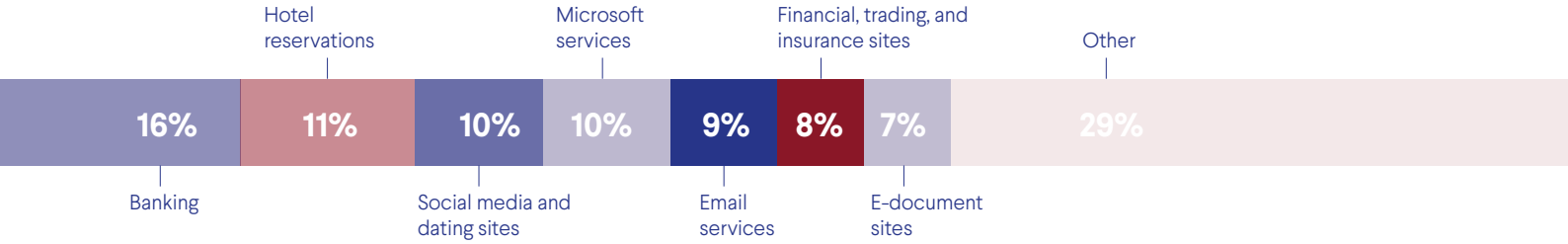


of threats to consumer devices were Safe Browsing threats, or visits to malicious websites. Of these visits:

76% were to sites that distribute or propagate malware infections.

19% were to phishing and scam sites.

Phishing campaigns spoof a wide variety of sites. Our analysis shows that the most popular types were:



IP Reputation threats, or malicious connections to or from disreputable IP addresses, made up 28% of all threats and primarily targeted NAS storage devices, IP cameras, and DVR devices, which often suffer from poor default configurations.

IP Reputation threats:

44% Primarily distribute malware and attempt to infect devices.

26% Participate in and control spam campaigns or known botnets.

23% Scan networks and devices for open ports or other vulnerabilities and attempt to brute force them.

5% Are related to phishing campaigns.

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. 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

04

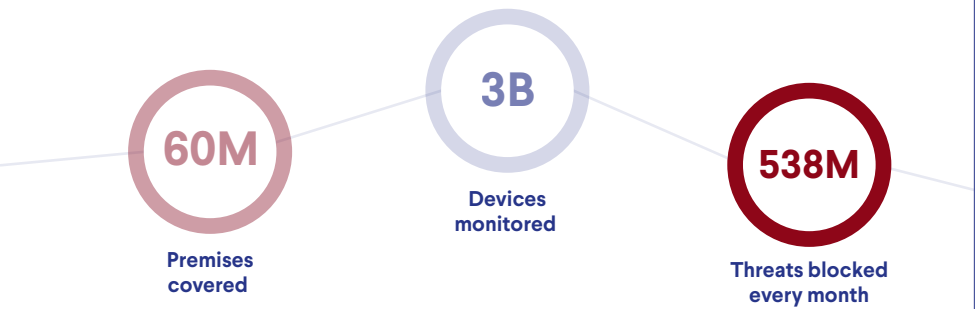
Introduction

This annual report presents threat data captured from deployments of CUJO AI Sentry, a multi-layer cybersecurity solution for network service providers that runs on the consumer's home router and protects every device connected to the network. Our multi-layer cybersecurity solution stopped 3,233,135,426 threats in 180 days between April and October of this year. CUJO AI is currently deployed on more than 60 million home networks in North America and Europe.

In this year's edition, our focus is on the most financially damaging cybersecurity threats to consumers – the scale and breadth of phishing threats. To explore the threat vectors malicious actors use against consumers and their devices, see our 2023 cybersecurity report.

CUJO AI uses in-house machine learning algorithms and internal threat intelligence in combination with industry-leading data providers to identify, classify and stop threats to protect over 3 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 attempt to connect to malicious IP addresses, including attempts to exploit a device's vulnerability, brute force attacks, malicious remote access attempts, as well as coordinated botnet activities, such as distributed denial-of-service (DDoS) attacks.



CUJO AI is used on dozens of millions of networks across two continents. Our scale not only provides us with the highest quality threat intelligence data to train and improve machine learning security, it also allows us detect new threats and stop their spread among every device protected by Sentry.

Santeri Kangas,
CTO

The threat landscape continues to evolve, and our researchers always have many complex and interesting challenges to solve. Currently, online fraud brings in the highest returns for malicious actors. Since these campaigns spread quickly and don't last long, the significance of accurate and fast-acting machine learning solutions in cybersecurity is growing.

Kimmo Kasslin,
SVP Protection Services

Glossary

A **threat** is defined as a single event where an action taken by a malicious actor or dangerous behavior of a device or its user would affect the security of 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 is the category of threats that are encountered when browsing the web or when a compromised device sends a web request. This category of threats includes malware distribution, phishing, spam, and other malicious websites.

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

An **outgoing IP Reputation** threat is an attempt to connect to a malicious IP address.

An **incoming IP Reputation** threat is an attempt to connect from a malicious IP address to a device on the protected network.

Device Intelligence is CUJO AI's industry-leading device detection and identification solution for network service providers that identifies all devices connected to a network and helps determine whether they're affected by a particular threat.

General Threat Data Overview

07

General Threat Data Overview

CUJO AI stops hundreds of millions of threats every month. Our data shows that over 67% of all households were affected by at least one threat per month during the period between April and October 2024.

These threats were grouped into the following categories:

Safe Browsing | **Incoming IP Reputation** | **Outgoing IP Reputation**

THREATS STOPPED ON CONSUMER HOME NETWORKS

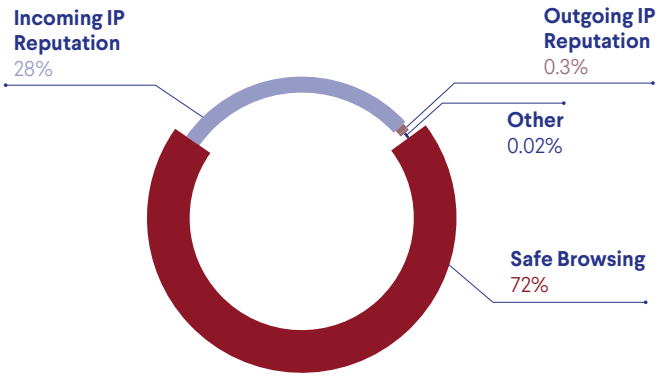


Figure 1 – Threats stopped by CUJO AI Sentry between April 26 and October 23, 2024.

CUJO AI Sentry employs behavioral pattern recognition mechanisms to detect and block compromised devices that are participating in denial-of-service (DOS) attacks. Devices exhibiting these patterns were relatively rare, with occurrences making up just about 0.02% of all threats seen on consumer home networks.

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

A consumer's network can have dozens of different devices from flagship smartphones to simple IoT sensors. Every one of them has a different set of vulnerabilities and security threats. Modern security needs an entire network approach, which is why we combine the strengths of different cybersecurity technologies to protect every device from a wide range of threats.

Sami Visti,
Senior Product Manager

IP Reputation threats most often affect vulnerable, poorly configured, or outdated IoT devices. When malicious actors exploit a device, they can use it in a botnet or further compromise an unprotected network. Exploited IoT devices can go undetected for a long time, since they are not powerful enough to run security applications, while consumers rarely check up on them and assume they are operating normally.

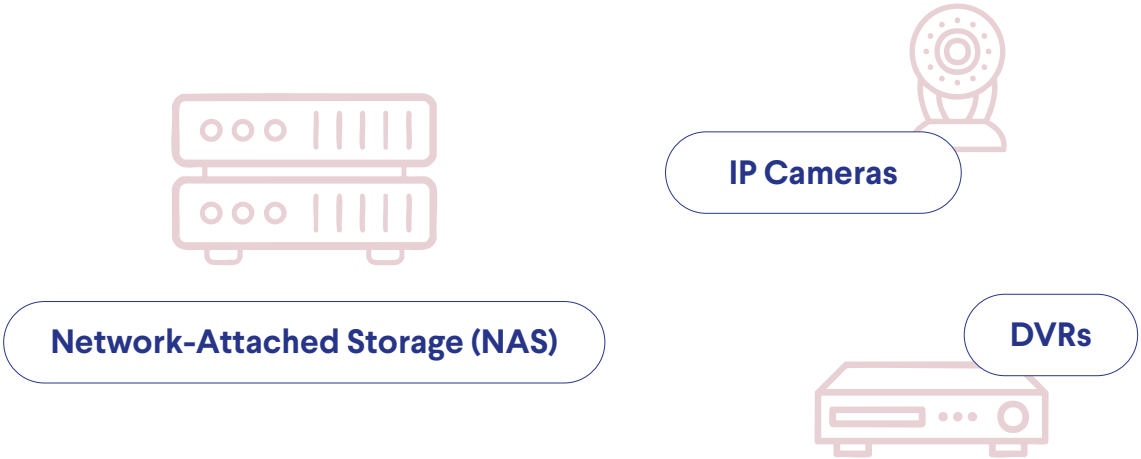
Leonardas Marozas,
Senior Lab Manager

IP Reputation Threats

As noted in our 2023 annual cybersecurity report, IP Reputation threats – attempts to connect to or from known malicious IP addresses – primarily target unattended IoT devices. Our most recent data shows that three types of connected devices are targeted by these threats a lot more often.

These types of devices are often configured to be remotely accessible from the Internet by default (e.g., through open ports), which make them easily detectable to even the most primitive scanners. Poor configurations, such as default usernames and passwords, unprotected debug interfaces, and outdated and vulnerable software components make devices prime targets for malicious actors.

TOP 3 DEVICES TARGETED BY IP REPUTATION THREATS



Network-attached storage devices remain the most-attacked devices by a significant margin. Some NAS vendors do not properly secure their products and have had alarming numbers of security vulnerabilities disclosed in recent years.

It should be noted that some network service providers rely solely on DNS-based security, which offers no protection against IP Reputation threats. CUJO AI Sentry fills this gap by preventing malicious actors from remotely accessing valuable consumer data on mass storage devices or their cameras and violating their privacy.

IP Reputation Threat Breakdown

Our data shows that most of the disreputable IP addresses targeting consumer devices were associated with malware distribution (44%), scanning and brute force attacks (23%), and spam (21%).

While 5% of all IP Reputation threats can be attributed to known botnets, it should be noted that botnets use masking techniques, such as residential proxies, to target device vulnerabilities, carry out scanning, brute force attacks, and distribute malware, all of which have their own categories. Therefore, actual botnet activity is significantly higher.

A single IP address can engage in multiple types of malicious activity, so these percentages provide only an estimated view of the actual distribution of all IP Reputation threats.

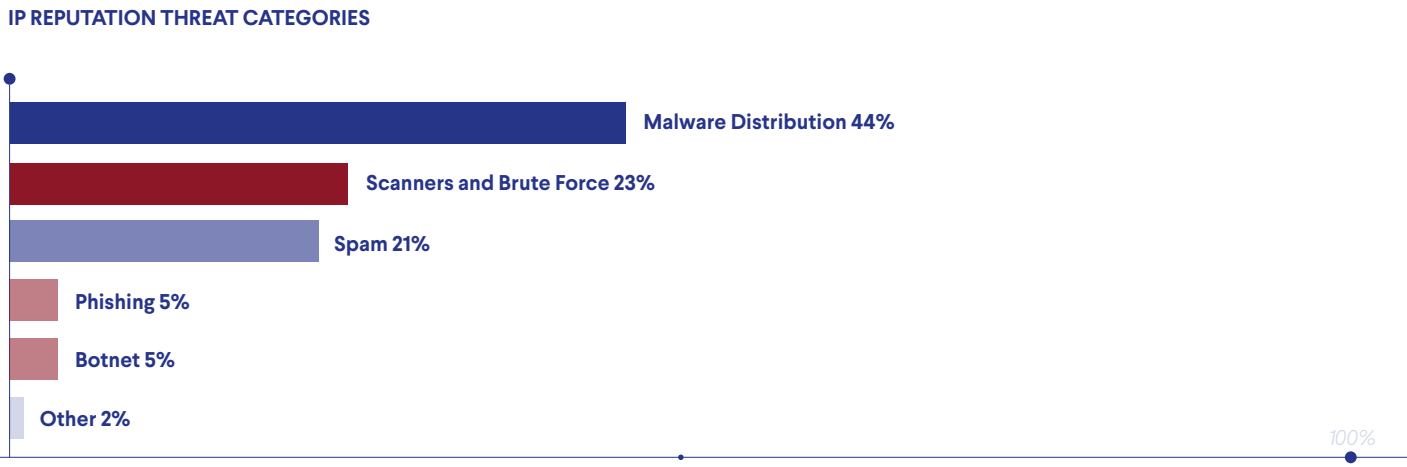


Figure 2 – Categories of IP Reputation threats stopped by CUJO AI Sentry between April 26 and October 23, 2024.
Note: a single threat source can participate in and be attributed to several categories.

Network service operators can 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 – smart home and IoT adopters – since IP Reputation threats primarily affect unattended devices.

We saw a significant increase in the number of IP Reputation threats related to phishing campaigns. Since these threats are primarily related to user behavior and *Safe Browsing* practices, we will expand on phishing threats in subsequent sections of this report.

Safe Browsing Threats

Web browsing and mobile applications greatly impact consumer cybersecurity. We have previously observed that close to 97% of all threats to mobile devices came from malicious websites.

Malicious websites come in many forms. Some distribute malware. Others impersonate legitimate websites to steal the visitor's data, personal information, financial data, cryptocurrency and other Web3 assets.

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.

Millions of people visit suspicious websites and download compromised software, including mobile applications, every day. Dangerous user behavior is one of the most important cybersecurity factors for devices that otherwise have good security configurations.

Dorka Palotay,
Senior Researcher

Safe Browsing Threat Breakdown

Our data shows that most Safe Browsing threats are related to malware (76%) and phishing campaigns (19%).

Figure 3 – Safe Browsing threats blocked by CUJO AI Sentry between April 26 and October 23, 2024.

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.

Fraud, scams and other social engineering attacks can be extremely financially damaging to consumers. Detecting and stopping these threats is essential to any modern cybersecurity solution.

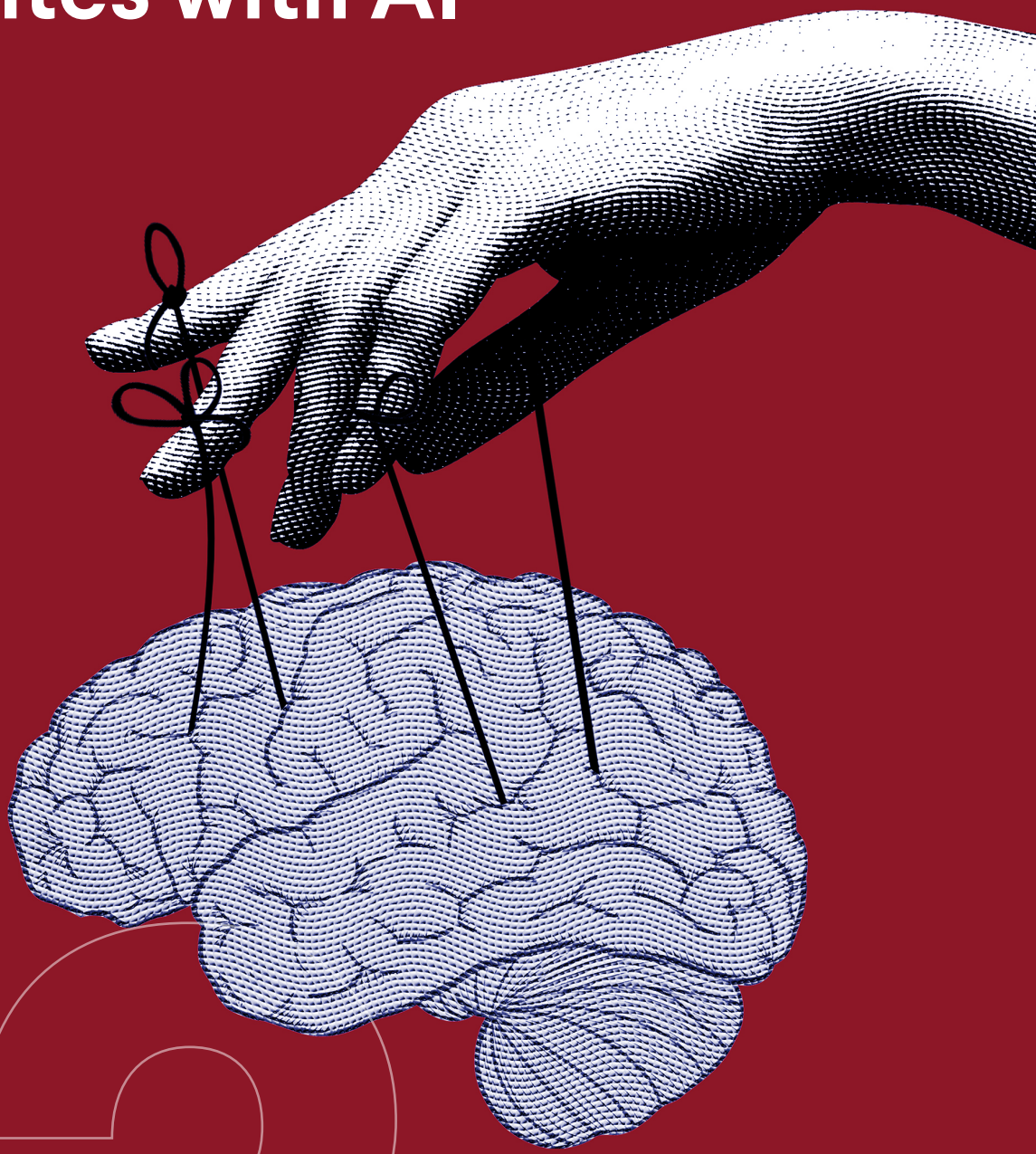
In the malware category, we have been seeing a wider use of domain generation algorithms (DGAs) – malicious automation techniques that generate new domain names and IP addresses. Due to how quickly DGAs scale, they significantly inflate the relative size of the malware category.

ViperSoftX has recently emerged as a significant malware threat. To read a detailed analysis of ViperSoftX, visit our blog.

ViperSoftX employed a multi-stage C2 system designed to avoid detection and maintain persistence on infected machines. It's DGA, fake DNS and HTTP queries pose a challenge for traditional, static security solutions. The malware infected devices through pirated software and cracks, as well as through malicious phishing email campaigns. Malicious actors behind ViperSoftX gather a lot of data about the infected system, which allows them to prioritize high-value targets, such as cryptocurrency wallets or valuable data.

Aurelio Picon,
Senior Researcher

Stopping Visits to Phishing Websites with AI



13

Stopping Visits to Phishing Websites with AI

CUJO AI Sentry uses a combination of technologies to counter short-lived and extremely damaging phishing campaigns, including:

1. Real-time real-world threat intelligence from the millions of networks already protected by CUJO AI.
2. Machine learning-driven real-time analysis of previously unseen websites.
3. Industry-standard threat intelligence sources, combined and enhanced by our algorithms.

Whenever we detect a previously unknown website, our machine learning algorithms set out to automatically analyze it. CUJO AI's extensive coverage of consumer networks allows us to protect the entire end-user base after a single visit to the site alerts our system. It should be noted that, in most cases, simply visiting a fraudulent page does not compromise the visitor's security. A more important aspect of phishing protection is preventing them from subsequently submitting their data to the suspicious website.

As noted in the preceding sections of this report, 19% of Safe Browsing threats and 5% of IP Reputation threats are associated with phishing campaigns. This section of the report details some high-level aspects of phishing threats.

Types of Sites Spoofed by Phishing Campaigns

We analyzed the distribution of targets that phishing pages in our dataset attempted to fake. As expected, finance and private data were the primary choice for these campaigns.

Overall, fraudulent banking sites made up 16% of all phishing sites analyzed in our dataset. Other categories, including financial, trading, and insurance (8%), hotel reservations (11%), social media and dating (10%), and webmail (9%) were also frequently observed. E-document sites and Microsoft login pages made up 7% and 10% of all phishing pages observed, respectively.

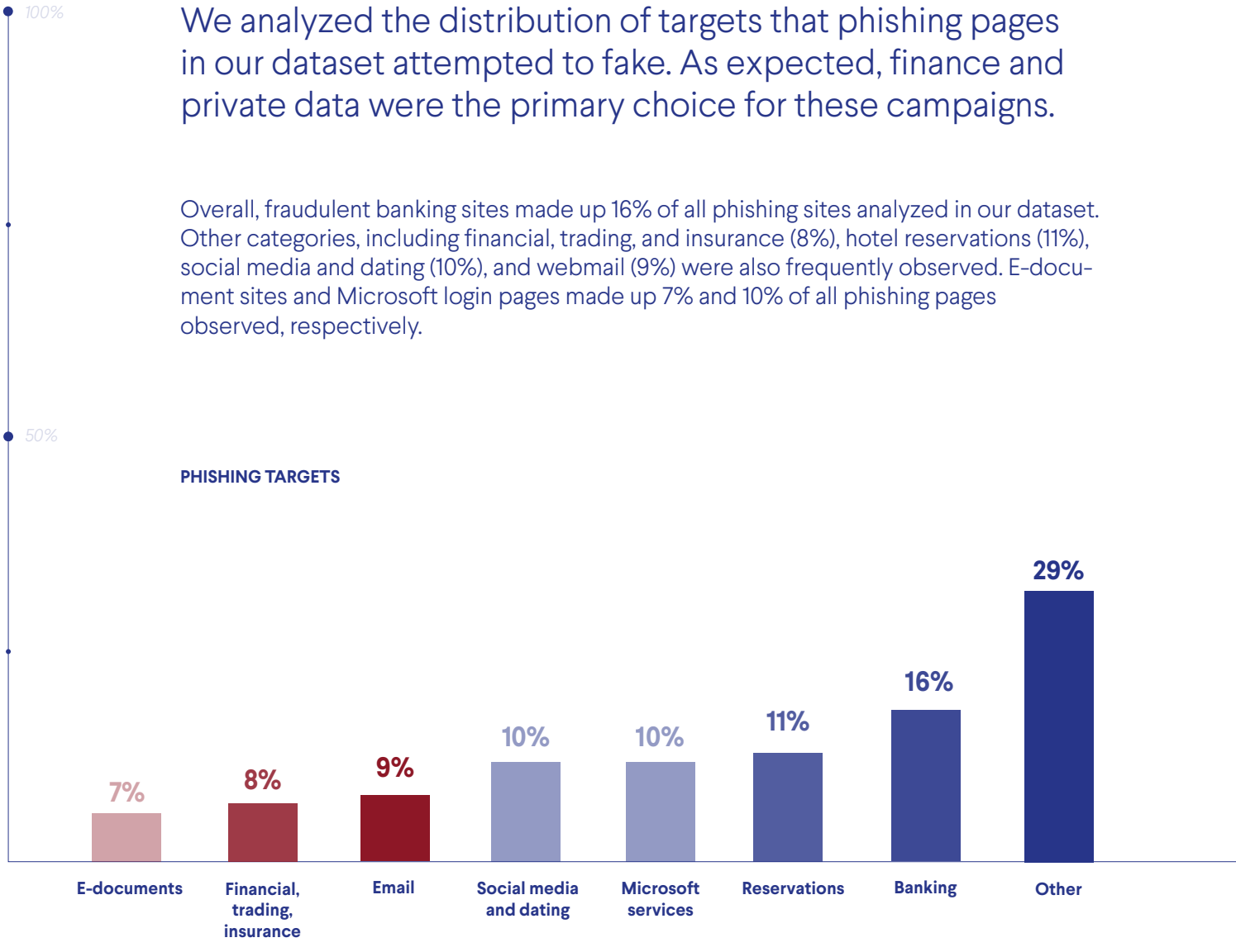


Figure 4 – Safe Browsing phishing threats blocked by CUJO AI Sentry. Distribution by type of site spoofed.

Financially motivated phishing attacks included a very diverse set of sites. Hotel reservation phishing sites mostly spoofed booking.com. E-document suites often imitated DocuSign and Adobe Document Cloud. Microsoft's login page was so prevalent that we gave it its own section in the graph. Other login services, such as Apple's, were also spoofed by phishing campaigns.

Phishing Tactics

The phishing campaigns we observed employed a variety of tactics to evade detection and fool victims. We observed varying quality in the fake websites, some of which included almost carbon-copy clones of the entire front-end of the imitated site.

Malicious actors also used website redirects and, at times, employed malware either as an additional vector, or as the end-goal of the fraud campaign.

> Our internal analyses show that Sentry is able to identify both a wide range of phishing categories and locations with diverse languages.
>
> *Balint Bicski,*
> *Junior Researcher*

For more in-depth analyses of particularly notable malicious campaigns we observe, visit our blog.

Challenges

Stopping phishing threats at scale is not an easy task. Automated machine learning-based website analysis systems, while often ideal for large-scale classification of potentially malicious sites, can encounter a variety of problems.

For instance, if a site renders poorly, partially or is 'under construction' or 'down for maintenance' and doesn't return proper server response codes, some analysis mechanisms will be hampered. Thus, automated web analysis solutions must rely on additional data sources, such as lists of known legitimate business IP addresses.

Further challenges in the area of website reputation analysis can arise when legitimate businesses publish suspicious looking advertisements (landing pages) or websites. In other cases, legitimate businesses in one jurisdiction are illegal in others. Gambling websites are a good example of this.

Ultimately what this means is that machine learning security solutions must be context-aware, and able to reduce both false positives and false negatives to a high degree.

12

Conclusion

Conclusion

We observed that roughly two thirds of all Internet users were exposed to cybersecurity threats on a monthly basis. As such, additional security measures designed to protect their online activities and smart home devices are highly recommended.

Phishing threats have continued to evolve year over year. Due to their potential to inflict heavy financial damage, they represent some of the most important threats to detect and block. However, their short-lived nature makes them difficult to defend against.

Phishing campaigns impersonate a broad section of online businesses and services, ranging from financial (banking, investment, insurance) to social media and dating sites. Machine learning-based automated website analysis mechanisms have proven invaluable in the fight against these threats, in combination with insights and data from our extensive deployments across North America and Europe.

We observed many *IP Reputation* threats targeting devices that store valuable data. CUJO AI Sentry enhances the security of these often-misconfigured gadgets by protecting every device on a network. Because our cybersecurity offerings are augmented with *Device Intelligence*, which can accurately identify each and every device on a network, CUJO AI's solutions can apply additional protective measures for specific IoT devices, analyze malicious activity, and expose suspicious device behavior to network service providers and end-users.

The scale of CUJO AI's deployments gives us a unique view into the consumer threat landscape, which includes botnet activities, malware, adware, and phishing campaigns.

About CUJO AI Sentry

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

Once deployed on any broadband router, CUJO AI Sentry requires no additional software, and secures all computers, phones, and 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.

About CUJO AI Labs

CUJO AI Labs is CUJO AI's advanced research department. It specializes in IoT threat research and network service provider customer cybersecurity.

Labs researchers use the largest scale real-world device behaviour database of over 3.1 billion anonymized consumer devices to empower advanced machine learning technologies that protect tens of millions of households around the globe.

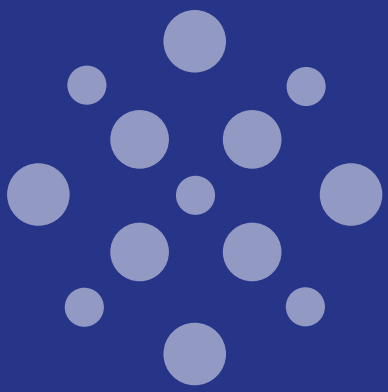
Every year, CUJO AI Labs publishes in-depth data-based reports, such as this one, on the IoT ecosystem and cybersecurity.

About CUJO AI

CUJO AI provides advanced multi-layered 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 tens of millions of homes and covering over 3 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, EE, Sky UK, Sky Italia, TELUS, Rogers, Cox, Shaw, and Videotron.



CUJOAI®

More information: connect@cujo.com
Media inquiries: press@cujo.com

cujo.com