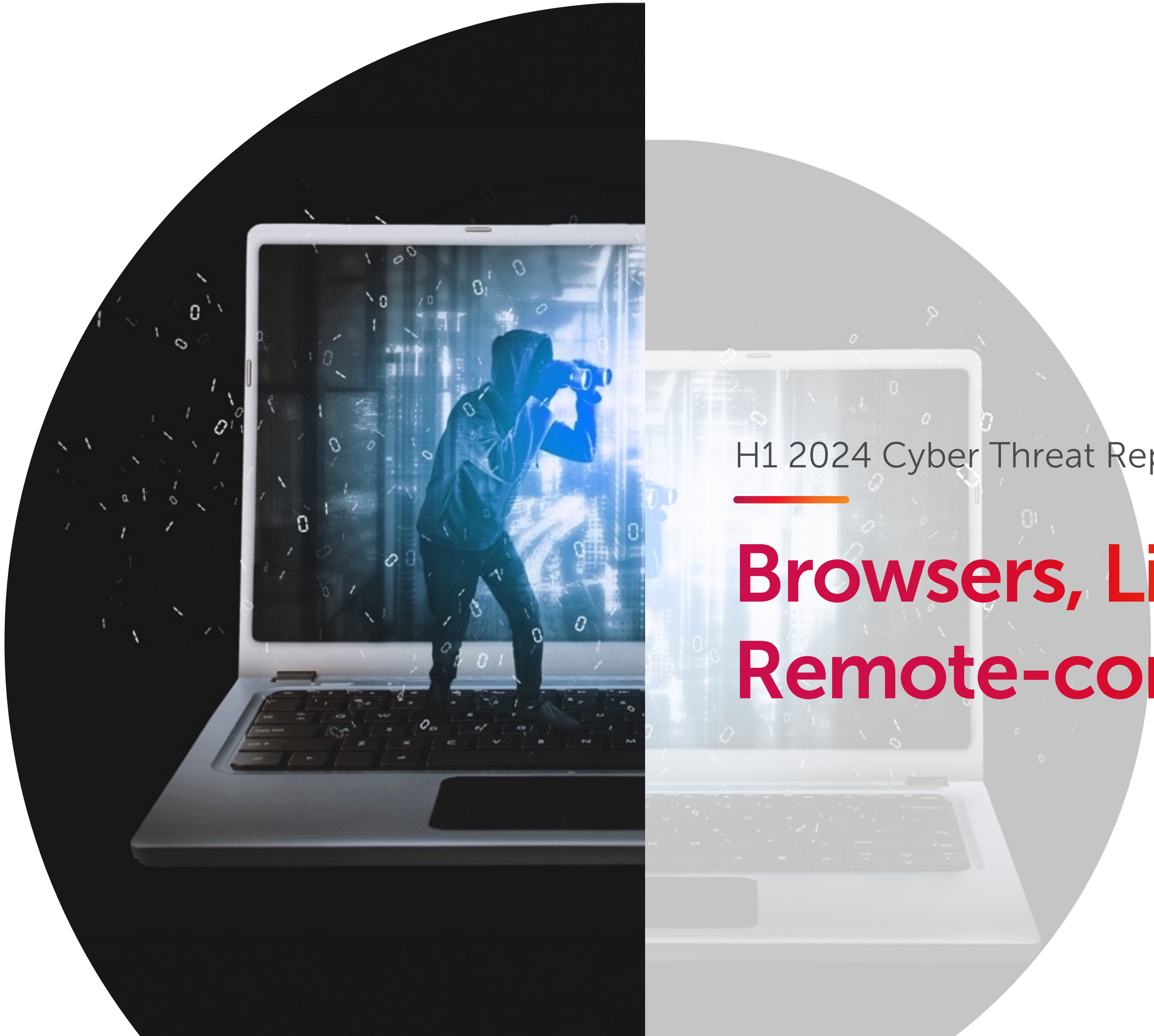
allot

See. Control. Secure.



H1 2024 Cyber Threat Report

# Browsers, Links & Remote-control Threats

# Introduction

This Allot Cyber Threat Report offers a comprehensive overview of the threats that mobile and fixed internet users faced in the first half of 2024 and how Allot, together with its Communication Service Provider (CSP) partners, protects them. This report highlights our analysis of real protection events. We have categorized the threats into three primary types:

- Browser-related threats
- Malicious Links and Sites
- Remote-control threats

Our findings demonstrate the effectiveness of network-native security solutions in mitigating these threats and keeping end users safe.

**Importance of Cybersecurity for Mobile Users**

In today's digital age, mobile devices are integral to our daily lives and hold a wealth of personal and financial information. This makes them attractive targets for cybercriminals. Effective cybersecurity measures are essential to protect end users from these threats and ensure their peace of mind as they navigate the online world. This report emphasizes the critical role of cybersecurity in safeguarding end users' mobile experiences.

**The Role of the CSP in User Protection**

CSPs are at the forefront of protecting users from cyber threats. By integrating advanced cybersecurity solutions directly into their networks, they can provide a robust first line of defense. This proactive approach enhances user safety and reinforces trust in their services. This report showcases how Allot’s security measures intercept threats before they reach CSP’s end users.

# Table of Contents

1

# A Guide to Internet Threats Affecting Everyday Users

To simplify the analysis of threats that regular internet users face, we've categorized them into three main types.

## Browser-related Threats

Cyber threats like Adware, Browser Hijackers, and Spyware Web Trackers can disrupt your browsing experience, push unwanted ads, hijack your browser settings, and track your online behavior. Our network-native service, however, effectively blocks the connections these threats try to establish, invalidating their capacity and keeping subscribers safer online.

## Malicious Links and Sites

This category includes threats like Phishing, Malware, and Malicious Download Pages. These threats lure users to click on dangerous links or visit harmful websites, often leading to the compromise of sensitive information or the download of malicious software. When a subscriber clicks on these risky links, our service takes a proactive stance, interrupting access to these sites and displaying errors or blocking pages.

## Remote Control Threats

Remote Control Threats relate to the connection between infected devices and command and control (C&C) centers. These threats allow cybercriminals to control compromised devices remotely, posing significant user data and privacy risks. Our service halts these connections, ensuring the control attempts are blocked without the user's awareness.

2

# Browser-related Threats

# Internet Browser, a Hotspot for Cyber Threats

## Let's review some numbers.

The time we spend using the internet increased significantly during COVID-19 and has since stabilized at about 6.4 hours a day1. While most of this time is spent using various applications, around 8% is dedicated to browsing (around 30 minutes a day)[2].

Searching for information remains the primary reason for going online, with over 80% of internet users utilizing some type of browser each month[1].

Given the high likelihood of encountering potential victims, it's not surprising that cybercriminals focus their strategies on internet browsers.

Among the most common and insidious threats are Adware, Browser Hijackers, and Web Trackers. While these malicious entities each operate differently, they share a common goal: to infect internet browsers and take advantage of our online activities for their gain.

Adware bombards us with relentless advertisements, Browser Hijackers seize control of our browser settings, and Web Trackers secretly monitor our every move online. Despite their distinct methods, these threats converge in their potential to invade our privacy, disrupt our browsing experience, and compromise sensitive information.

How does protection with the Network-native service work? If you have online protection, the actions of these malicious mechanisms are blocked. Even if the browser is infected, the ads adware tries to display won't be visible, browser hijackers won't be able to change search engine results or redirect you to unwanted sites, and web trackers won't be able to monitor or collect your browsing activity.

# Understanding Adware

Adware is one of the most common and persistent threats internet users face today. Its primary function is to display advertisements, but its impact goes far beyond simple annoyance.

## Infection method. How do they reach you?

Adware infiltrates your browser through seemingly innocent means. It often bundles with free software or embeds on malicious websites. During the last year, we found many cases where the simple option to allow notifications or even a Captcha button serves as a disguise for Adware to access your browser.

## Impact and risks

If you notice an unusual change in your browsing experience, it might be the first sign that Adware has infected your browser. You suddenly experience an inundation of pop-up ads, banners, and even new browser tabs opening with advertisements. This can slow down your browser, making everyday tasks frustrating.

But the inconvenience of slowed browsing is just the tip of the iceberg. Adware often monitors your browsing history, search queries, and other behaviors. This collected data is then used to target you with even more advertisements or sold to third parties, raising significant privacy concerns.

In some cases, the presence of Adware can expose you to more serious malware threats, further compromising your personal information and online safety.

From a criminal perspective, it is important to understand that the driving force behind Adware is purely financial. Adware creators profit from displaying advertisements to users and collecting data that can be sold or used for targeted marketing. Sometimes, Adware also serves as a gateway for more malicious software, escalating the threat to users' financial and personal data.

## The protection experience

Every day, CSP subscribers with network-native cybersecurity protection solutions from Allot remain safe from Adware attempts. Depending on the website's design, the evidence of unwanted ads being blocked can be more explicit. However, we usually pay attention when intrusive banners and ads crowd our navigation, not the other way around, so the protection experience might go unnoticed.

# Browser Hijackers.
# A Closer Look

While Adware bombards you with ads, Browser Hijackers take a more manipulative approach by changing your browser settings without permission. They often alter your homepage, default search engine, and other configurations to redirect you to specific sites, generating revenue through increased traffic.

Unlike Adware, which primarily annoys, Browser Hijackers pose significant privacy risks by capturing your search queries, browsing history, and even login credentials. This data can lead to identity theft and financial loss, making these threats more insidious.

Browser Hijackers spread through freeware or shareware downloads, bundled with legitimate software, or through malicious websites. Once installed, they cause persistent redirects and unwanted changes that can frustrate users and reduce productivity.

The financial motive behind Browser Hijackers is clear: they profit from redirects and selling your data, unlike Adware, which focuses on displaying ads.

In summary, while Adware disrupts with ads, Browser Hijackers invade privacy and manipulate your online experience for profit.

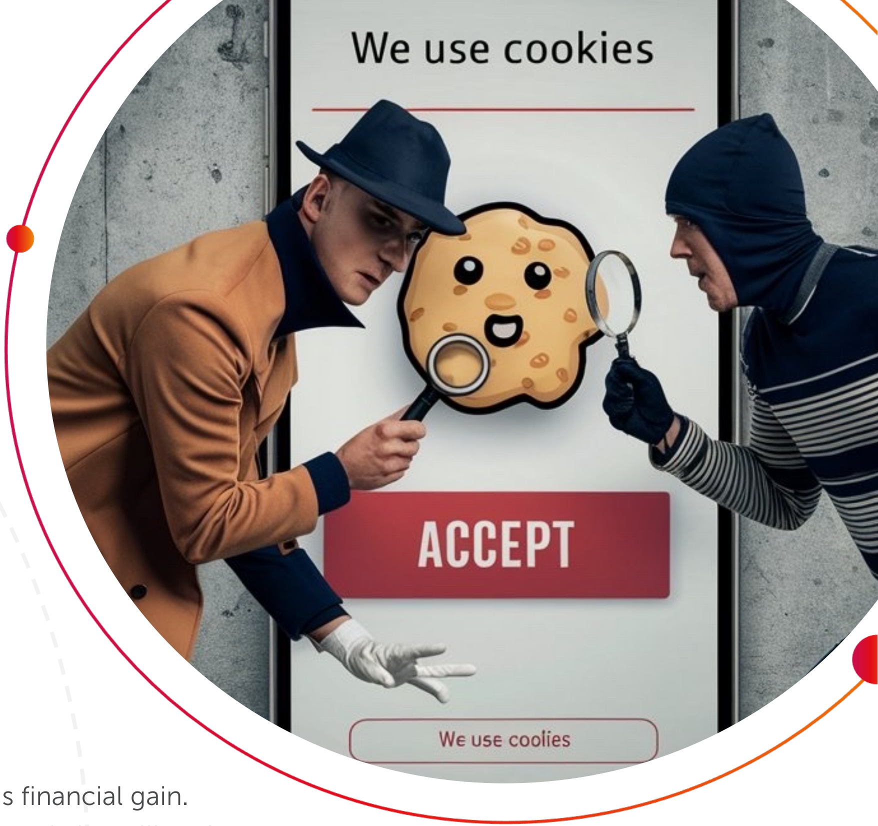
# Web Trackers.
# The Invisible Threat

Spyware Web Trackers are a subtle yet pervasive threat that operates as you browse the internet. Unlike Adware, which bombards you with ads, and Browser Hijackers, which manipulate your browser settings, Web Trackers work quietly in the background, collecting data on your browsing habits.

Like silent spies, these trackers monitor your browsing history and search queries, gathering detailed information about your online behavior. Those behind the trackers use this data to build comprehensive profiles of your interests and activities and then sell it to third parties or use it for targeted advertising.

Web Trackers typically infiltrate your system through cookies, scripts, and embedded trackers on websites. They are often hidden within the legitimate elements of the sites you visit, making them difficult to detect and avoid.

The impact on victims is significant, even though it might not be immediately apparent. The constant collection of browsing data erodes your privacy, as your online actions are monitored and analyzed. Eventually, as a victim, you will observe more targeted ads, making you feel watched and manipulated.



Once again, the primary goal is financial gain. Web trackers can profit significantly by selling the detailed user data collected to advertisers and other interested parties. This data is invaluable for creating highly targeted advertising campaigns more likely to result in sales.

### The real risk

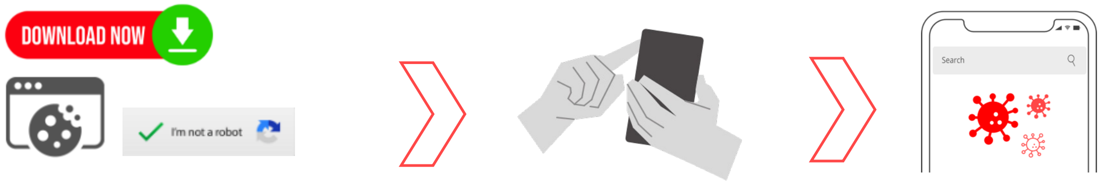
Furthermore, web trackers often serve as part of a bigger malware infrastructure. Cybercriminals usually utilize the knowledge collected from the tracker to tailor-design further attacks on those spied on. With the perfect context on the user's online steps, users are much more vulnerable to being disguised into engaging with malicious messages, ads, and websites.

# Browser-Based Threats Summary

| | ADWARE | BROWSER HIJACKERS | WEB TRACKERS |
|---|---|---|---|
| SHORT DEFINITION | Displays advertisements | Changes browser settings | Tracks browsing habits |
| BROWSER BEHAVIOR | Shows ads, pop-ups, slows browser | Changes homepage/search engine, redirects | Collects browsing data invisibly |
| COMPROMISED INFORMATION | Browsing history, search queries, | Search queries, browsing history, credentials | Browsing history, search queries |
| INFECTION METHOD | Bundled with free software, malicious sites | Freeware/shareware, malicious sites | Cookies, scripts, embedded trackers |
| IMPACT ON VICTIMS | Annoyance, privacy invasion, slow browsing, exposure to more serious malware. | Identity theft, financial loss, disruption, exposure to more serious malware. | Privacy erosion, targeted ads, data exploitation, exposure to more serious malware. |
| CRIMINAL GAIN | Advertising revenue, potential data sales, further malware exposure | Financial gain through redirects, further malware installation | Selling user data to third parties, building user profiles for targeted advertising |

# Browser-Based Threats Summary

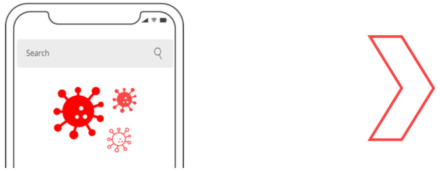
USERS' BROWSERS GET INFECTED



ENTRY POINT · ALLOW ACCESS · BROWSER INFECTED

Usually, access comes from bundled software, allow-type buttons on malicious and compromised sites

BROWSER-BASED THREATS IN ACTION



INFECTED BROWSER

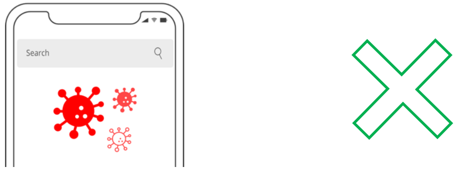
ADWARE: Displays ads

HIJACKER: Redirects navigation

WEB TRACKER: Tracks browser activity

Once the browser is infected, the threats are active every time it is in use.
Signs of abnormal browser experience might be evident.

NETWORK PROTECTION IN ACTION



INFECTED BROWSER

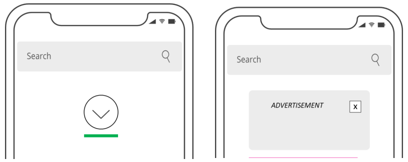
ADWARE: Can't display ads

HIJACKER: Can't redirect navigation

WEB TRACKERS: Can't track browser activity

For protected customers, even if the browser gets infected, the malicious connections are blocked, preventing potential harm.

PROTECTED SUBSCRIBERS' USER EXPERIENCE

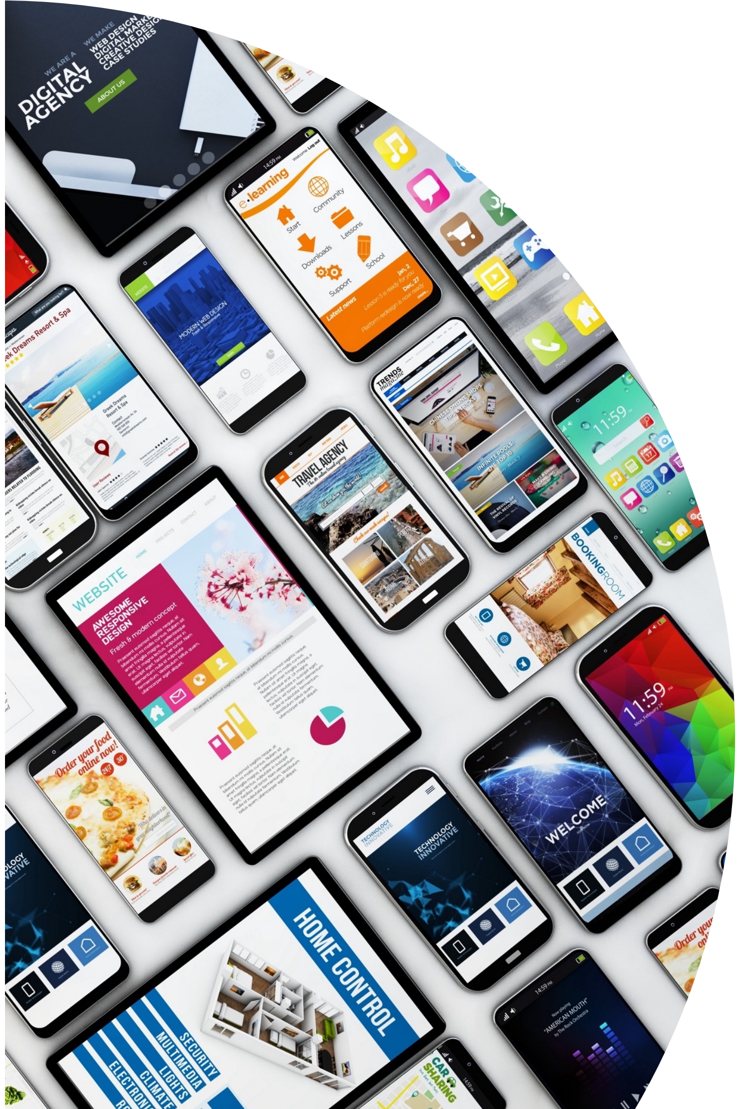


PROTECTED BROWSER EXPERIENCE

Protected customers can enjoy a smooth browsing experience.
The malicious connections are blocked at the browser level with almost no visibility for the user.

2

# Malicious Links & Sites



# Malicious Threats.
# The ABC of Cyberthreats

When people think about online threats, this category often comes to mind. We all know that not everything we see online is legitimate, and cybercriminals can hide behind websites or links in texts and emails. The most common threats associated with these sites are phishing, malicious downloads, malware, and compromised websites.

Phishing sites masquerade as legitimate websites and deceive users into divulging personal information. Malicious download sites trick users into downloading harmful software that can steal data or damage systems. Malware sites host software designed to infiltrate and harm computers without consent. Compromised websites, although initially legitimate, are hijacked by cybercriminals to deliver malware or phishing schemes.

What do these threats have in common? They exploit human vulnerability, requiring user interaction to work. These malicious sites are highly persuasive and use high-quality design to enhance their credibility and effectiveness.

Cybercriminals have two main allies: social engineering and top-notch AI design tools. Social engineering exploits human psychology to manipulate individuals into compromising security by establishing trust, manipulating emotions, and exploiting curiosity and temptation. This makes phishing schemes more convincing and increases the likelihood of downloading malicious files.

Top-notch design tools enable attackers to create compelling and visually appealing content. They can craft emails and websites that closely mimic legitimate ones, making it harder for users to detect fraud. Malicious downloads can be disguised as attractive applications or files, luring users into downloading them. Malware can be embedded in visually appealing software or documents, increasing the chances of execution.
Together, these techniques make cyber threats more pervasive and harder to detect, necessitating advanced cybersecurity measures.

**The protection experience**
When a protected user clicks on a link to a malicious site, the connection is interrupted, showing an error message or a blocking page. In terms of protection perception, this group of cyber threats provides an immediate visual reaction as the user witnesses the blocked connections.
In the following pages, we will see examples of sites that were blocked for protected customers due to the risks they posed online.

# Malicious Downloads

Interacting with online PDFs and QR codes has become second nature in our digital lives. Whether you're downloading a document for work, accessing study materials, or scanning a QR code for a quick restaurant menu, these actions are part of our everyday online routine.

But did you know these seemingly harmless tasks sometimes have hidden risks?

In these two cases, as in many others, Malicious Downloads are often disguised as legitimate PDFs or embedded in QR codes. Scanning or downloading these can inadvertently install malware on your device, putting your personal information and security at risk. It's a stark reminder that even our most routine online interactions can be a gateway for cyber threats.

# Malware

Looking for the latest release of the series you love? Can't you miss the football match that was not included in your TV package?

While the allure of free content is strong, free content sites often hide a dangerous secret. Malicious websites can automatically download and install malware on your device without you even realizing it.

These sites exploit security gaps in your browser or operating system, starting a download as soon as you visit. The malware then sneaks onto your device, allowing cybercriminals to steal your personal information, spy on your online activities, or even take control of your device.

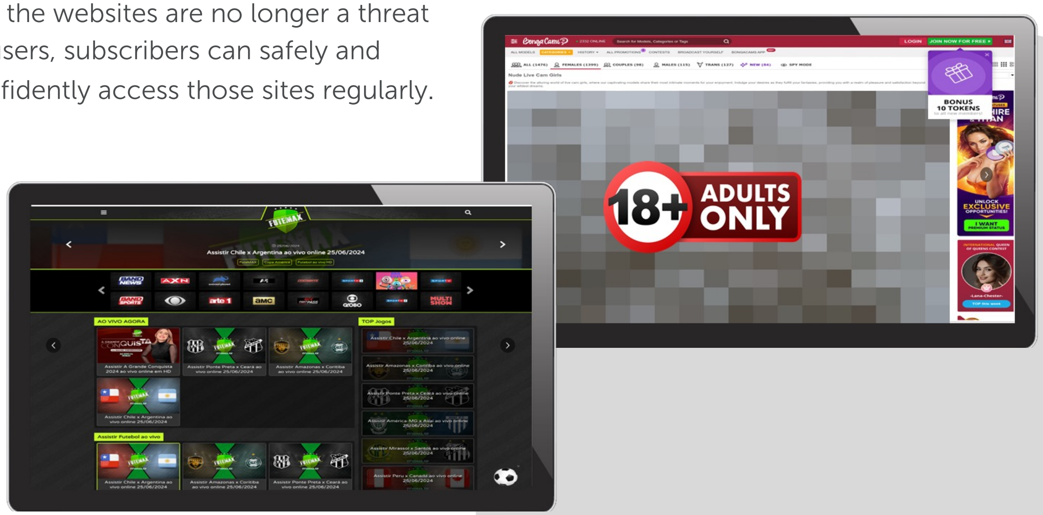
# Compromised Sites

Compromised websites can secretly inject harmful scripts, redirect visitors to fraudulent pages, or distribute malware, leading to identity theft, financial loss, and damaged trust.

A good example is Linkbio.co, a tool for creating a personalized link that acts as a menu typically used for the profile description on Instagram, LinkedIn, Facebook, and TikTok. At the beginning of 2024, the site was compromised, and users trying to access any link based on this platform were prevented from reaching the vulnerable site.

Compromised websites are not inherently malicious but originally designed for legitimate purposes. However, attackers can exploit vulnerabilities, transforming these sites into conduits for harmful activities.

Once these security issues are resolved and the websites are no longer a threat to users, subscribers can safely and confidently access those sites regularly.



# Phishing

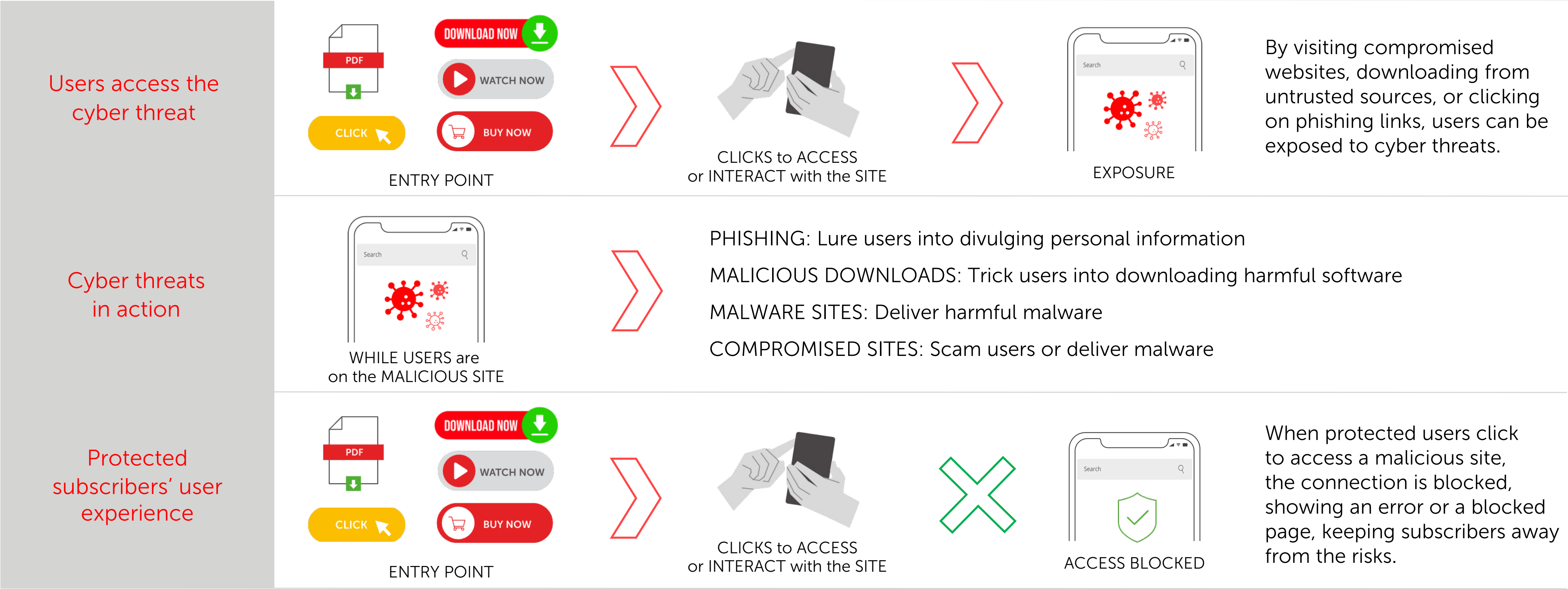
Phishing sites often use favicons (those small icons displayed in a browser's address bar) of legitimate companies to trick users into thinking they are on an authentic website. This tactic boosts visual trust, making users more likely to enter sensitive information. By exploiting brand recognition, scammers exploit familiar websites' established reputation and trust, significantly increasing the chances of successfully obtaining sensitive information from unsuspecting users.

Another typical example of phishing is a fake page that looks just like a regular general interest magazine. Between real notes, it's packed with articles about miraculous medicines and therapies that seem too good to be true—and they are! These convincing articles are part of a phishing scam aimed at getting your personal info or payment details under the guise of promoting health products.

# Threats around Malicious Links & Sites Summary

| | PHISHING | MALICIOUS DOWNLOADS | MALWARE SITES | COMPROMISED WEBSITES |
|---|---|---|---|---|
| SHORT DEFINITION | Impersonation to steal information | Deceptive downloads of infected files | Websites designed to deliver malware | Hacked websites delivering malware |
| COMPROMISED INFORMATION | Login credentials, financial info | Personal files, financial info, system data | Browsing data, personal info, login credentials | Browsing data, personal info, login credentials |
| INFECTION METHOD | Clicking malicious links | Downloading from untrustworthy sources | Visiting compromised sites | Visiting compromised sites |
| IMPACT ON VICTIMS | Data loss, identity theft, financial loss | Data loss, unauthorized access, device damage | Data theft, financial loss, further infections | Data theft, financial loss, further infections |
| CRIMINAL GAIN | Financial access, identity theft, data sales | Device control, data theft, ransom demands | Data harvesting, malware spread, identity theft | Data harvesting, malware spread, identity theft |

# User Experience of Threat Protection for Malicious Links and Sites



Users access the cyber threat

ENTRY POINT

CLICKS to ACCESS or INTERACT with the SITE

EXPOSURE

By visiting compromised websites, downloading from untrusted sources, or clicking on phishing links, users can be exposed to cyber threats.

Cyber threats in action

WHILE USERS are on the MALICIOUS SITE

PHISHING: Lure users into divulging personal information

MALICIOUS DOWNLOADS: Trick users into downloading harmful software

MALWARE SITES: Deliver harmful malware

COMPROMISED SITES: Scam users or deliver malware

Protected subscribers' user experience

ENTRY POINT

CLICKS to ACCESS or INTERACT with the SITE

ACCESS BLOCKED

When protected users click to access a malicious site, the connection is blocked, showing an error or a blocked page, keeping subscribers away from the risks.

3

# Remote Control Threats

# The Secret Weapon of Network-native Protection

In this challenging scenario, where it seems inevitable that some devices will become infected with viruses, Allot's network-native protection is crucial in keeping customers safe. How? By detecting and stopping the communication from the virus installed on the infected devices to its Command and Control (C&C) center.

## Main reasons cybercriminals use Command and Control in their designs:

⚠ **Remote Control Capabilities**
Attackers can manage and execute commands on infected devices from afar.

⚠ **Real-Time Data Exfiltration**
Sensitive information can be stolen and transmitted in real time.

⚠ **Coordinated Attacks**
Multiple infected devices can be used to launch large-scale attacks.

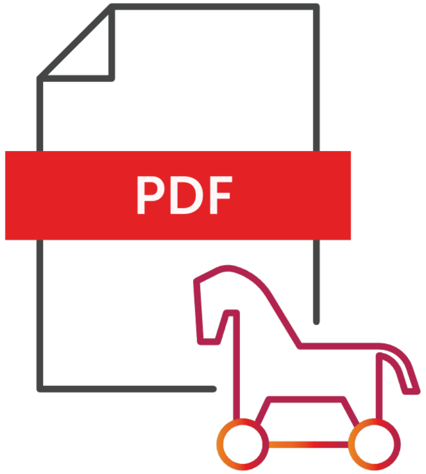
⚠ **Persistent Operations**
Viruses can maintain their presence on your device, even after attempts to remove them.

⚠ **Resilience Against Countermeasures**
C&C techniques help viruses adapt and continue operating despite security defenses.

In the next few pages, we will dive into the most common Viruses using C&C blocked by Allot during the first half of 2024.

# TROJAN PDFPHISH

Have you ever received an email with an attached PDF that seemed like legitimate business communication? Beware, it could be carrying a nasty surprise called PDFPHISH, a TROJAN designed to steal your credentials.



## What is PDFPHISH?

PDFPHISH is a sneaky TROJAN that uses malicious PDF files to carry out phishing attacks. These deceptive emails often mimic invoices, delivery notes, or other work-related documents to trick you into opening the attachment.

## How Does it Work?

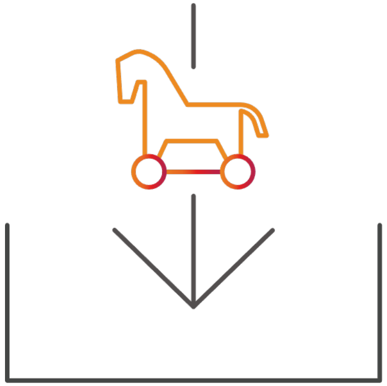
Once you open the malicious PDF, it contains a malformed hyperlink leading to a phishing websites. These sites might show fake login pages that capture your enterprise domain credentials. If you interact with these links and enter your details, cybercriminals can gain access to sensitive corporate information.

## Why is it Dangerous?

PDFPHISH files are crafted to look legitimate and might display an authentic-looking document as a decoy. Meanwhile, harmful code is either installed directly on your device or downloads additional malware from a remote site. Some variants constantly change their file names, making them hard to delete manually.

# TROJAN Downloader Unruy

Unruy is a sneaky TROJAN downloader that poses a significant risk to your device's security and personal privacy. Although it primarily targets Windows systems, mobile users should be aware of the potential risks.



## What is  Unruy?

Unruy is a downloader, meaning its primary job is to download and install additional malicious software on infected devices. This can lead to a cascade of harmful programs infiltrating your mobile phone.

## How Does It Behave?

Once Unruy finds its way onto your device, it communicates with the remote host to silently download and install other malicious programs without the user's consent or knowledge. Additionally, it starts displaying out-of-context advertisements and performing ad-clicking to generate revenue for its controllers.

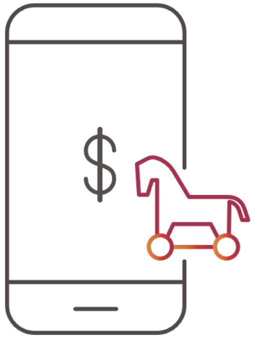
## Why is it Dangerous?

As a TROJAN downloader, Unruy can bring in more malware, leading to multiple infections that can seriously compromise your device's security and your personal information.

# Banking TROJAN BankBot

## What is BankBot?

BankBot an advanced banking TROJAN designed to steal your financial information by mimicking legitimate banking apps and using several malicious behaviors.
It masquerades as legitimate apps, such as video players or weather apps, to trick users into downloading it.



## How Does it Work?

**Phishing Overlays:** BankBot creates fake login screens that look like those of legitimate banking apps to steal your credentials and payment card details.

**Targeting Multiple Apps:** It can target hundreds of banking and financial apps, with some variants affecting over 400 apps on Google Play.

**SMS Interception:** It can intercept SMS to capture one-time passwords and transaction verification codes, bypassing two-factor authentication.

**Keylogging:** The TROJAN captures keystrokes, including sensitive data entered into banking apps.

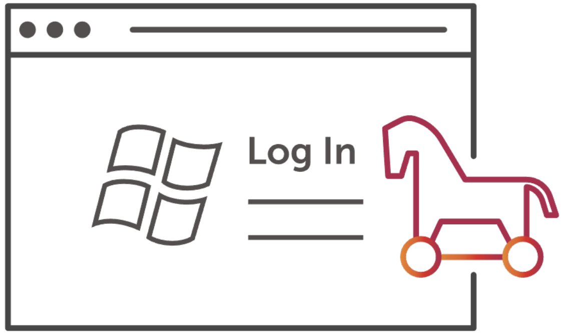
Among other capabilities, it can drop additional malware, propagate as a worm, and exploit Android's accessibility services to control the device functions and manipulate app interfaces.

## Why is it Dangerous?

BankBot is highly dangerous because it can steal login credentials and payment details, facilitating unauthorized transactions and financial loss. It bypasses security measures like two-factor authentication through SMS interception and phishing overlays, granting attackers access to your accounts. Additionally, its C&C capabilities allow attackers to execute commands and further exploit the device. Its self-replication and stealth techniques make it difficult to detect and remove, potentially spreading to other devices and causing widespread harm.

# TROJAN Windows Expiro

Expiro is a crafty and persistent malware family that has been causing trouble for over a decade. Although it primarily targets Windows systems, mobile users should be aware of the potential risks.



## What is Expiro?

Expiro is a file-infecting virus that traditionally targets executable files on Windows systems. However, its ability to steal sensitive information and credentials can indirectly affect mobile users if those credentials are used across devices.

## How Does it Work?

Expiro's main job is to steal user credentials and sensitive information, like credit card data. It can also grant cybercriminals backdoor access and remote control, allowing them to compromise other connected devices, including mobile phones. Additionally, it lowers security settings, installs unwanted extensions, and changes configurations to avoid detection.

## Why is it Dangerous?

Expiro makes lasting changes to your device's configuration, making removing and restoring your device to its original state difficult. It continuously evolves, with numerous variants like Expiro.AA, Expiro.AB, and Expiro.Y. These updates often introduce new infection routines, making it a persistent threat.

# FormBook Credential Stealer

FormBook is a sophisticated piece of malware primarily targeting Windows systems, but it can indirectly affect mobile users by compromising their data and accounts.

## What is FormBook?

FormBook is a credential and information stealer that targets over 90 different applications, including web browsers, email clients, and messaging apps. It captures data from keystrokes, browser autofill, and clipboards, and extracts information from website HTML forms, such as credit card numbers and authentication tokens.

## How Does it Work?

**Data Theft:** it steals credentials and sensitive information from various applications, capturing data from keystrokes, autofill features, and clipboards. It can also extract information directly from website forms.

Delivered through email campaigns with malicious attachments or links, FormBook copies itself to specific directories and sets up persistence via autorun registry keys or scheduled tasks.

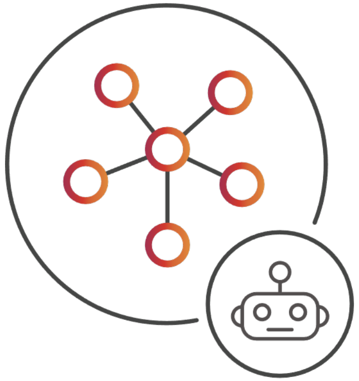
## Why is it Dangerous?

**Indirect Impact:** While FormBook primarily targets Windows systems, mobile users can be affected if they access compromised accounts or data on their devices.

**Credential Theft:** Stolen credentials from desktop systems can be used to gain unauthorized access to mobile accounts and applications, posing significant security risks.

# Mirai Botnet

Mirai is a notorious malware that primarily targets IoT devices, but its impact can extend to mobile users in significant ways.



## What is Mirai?

Mirai is a type of malware that infects Internet of Things (IoT) devices such as routers, security cameras, and DVRs. It takes advantage of default usernames and passwords to gain access and control over these devices.

## How Does it Work?

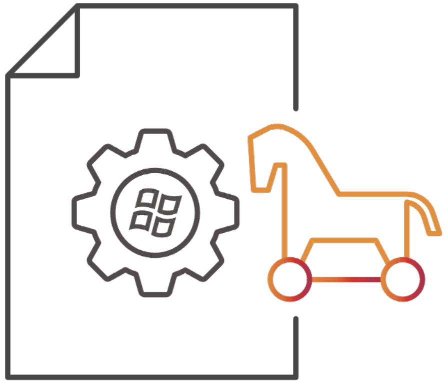
**Infection Method:** Mirai scans the internet for vulnerable IoT devices and can infect Android devices through the Android Debug Bridge, if it's enabled.
**Post-Infection Activity:** Infected devices often function normally but may become sluggish and consume more bandwidth. Mirai also blocks remote administration ports and removes competing malware.
**Propagation:** The malware continuously scans for and infects other vulnerable devices, making it highly persistent. It can reinfect devices quickly if passwords are not changed.

## Why is it Dangerous?

**Network Performance:** Mobile users may experience slower internet speeds due to the increased network traffic generated by Mirai-infected devices.
**Botnet Formation:** Infected devices become part of a botnet used for large-scale Distributed Denial of Service (DDoS) attacks, which can disrupt online services.
**Data Security:** Compromised IoT devices pose a risk to personal data and overall network security.
**Broader Implications:** The botnet can be used for various malicious activities, including click fraud, which can increase costs for businesses and consumers.

# Windows TROJAN Pasta

The Windows TROJAN Pasta is a significant malware threat that primarily targets Windows systems. However, mobile users should also be aware of its potential risks due to indirect impacts.



## What is Windows TROJAN Pasta?

The Windows TROJAN Pasta is malicious software designed to infect Windows systems. It modifies system settings and ensures its persistence, allowing it to facilitate further malicious activities.

## How Does it Work?

**System Modifications**: Pasta alters various registry entries on Windows systems to ensure it starts automatically and drops copies of itself in critical directories.

**Remote Control**: Some variants can download additional malware from remote hosts, potentially leading to further infections and malicious activities.

**Botnet Involvement**: This TROJAN can become part of a botnet, enabling cybercriminals to use the infected system for spam, DDoS attacks, and more.

## Why is it Dangerous?

**Shared Networks**: Infected Windows systems on shared networks can become a launchpad for attacks on other devices, including mobile phones.

**Data Synchronization**: Syncing data between PCs and mobile devices can expose mobile devices to risks if the PC is compromised.

**Increased Phishing**: The botnet activities can lead to more phishing attempts, targeting mobile users to steal sensitive information.

# Remote Control Protection Summary

| | PDFPHISH TROJAN | TROJAN DOWNLOADS | CREDENTIAL STEALER |
|---|---|---|---|
| SHORT DEFINITION | A TROJAN that uses malicious PDF files to carry out phishing attacks. | A TROJAN designed to download and install additional malicious software on infected devices. | Malware that steals credentials and sensitive data. |
| COMPROMISED INFORMATION | Targets enterprise domain credentials and sensitive corporate information. | May steal user credentials and system information to facilitate further malware downloads. | Steals credentials from browsers, email clients, etc. |
| IMPACT ON VICTIMS | Victims risk having their credentials stolen, leading to potential data breaches and unauthorized access. | Infected devices may experience multiple malware infections, leading to system slowdowns and data breaches. | Unauthorized access to accounts, data breaches. |
| CRIMINAL GAIN | Access to sensitive enterprise information, potential for corporate espionage. | Generates revenue through ad fraud and by facilitating further malware distribution. | Access to sensitive information for further exploitation. |
| SIGNS OF INFECTION | Malformed hyperlinks in PDFs, unexpected redirects to login pages. | Out-of-context advertisements, system slowdowns, unknown software installations. | Unusual account activity, stolen credentials. |

# User Experience of Threat Protection Against C&C Attacks

## Devices get infected

ENTRY POINT

VIRUS ACCESS THE DEVICE

Viruses are sneaky and have several ways to access and infect devices.

## TROJAN Viruses in action

VIRUS INSTALLED IN THE DEVICE

PDFPHISH: Steals credentials and redirects users to phishing sites

STEALER: Steals credentials and sensitive data from applications.

DOWNLOADER: Downloads and facilitates further infections

## Protected subscribers' user experience

VIRUS INSTALLED IN THE DEVICE

PDFPHISH: Can't steal credentials and redirect users to phishing sites

STEALER : Can't steal credentials and sensitive data from applications.

DOWNLOADER: Can't download and facilitate further infections

Network-native protection blocks the C&C connections, stopping Virus's malicious activity

4

# Takeaways & Conclusion

# Staying Away from the Most Dangerous Threats

By examining the always-evolving cyber landscape, we were able to shed some light on the real motivations behind cyber attacks on everyday users and small businesses.

Given the range of cyberthreats, from the lucrative black market for private user data, to the subtle yet impactful world of digital footprint commodification, there is a critical need to adapt cyber security measures to protect telco subscribers of all sizes.

## What is the role of Allot Protection against Virus Infection?

### Protection by Blocking Virus' Most Common Entry Points

- Blocking Links in Phishing Emails, Instant Messages, and Social Media
- Avoiding Visits to Compromised or Malicious Websites
- Avoiding Visits to Sites Offering Malicious Downloads
- Blocking Malicious Ads (Adware)
- Blocking Backdoor communications to install a virus remotely

### Other Infections Sources out of Network-native Protection

- Removable USB or External Hard Drivers
- Unsecure Network, Public Wi-Fi, or Network Shares
- Software Vulnerabilities, Outdated or Unpatched
- Operating System Vulnerabilities, Outdates or Flaws
- Physical Access

Furthermore, the ever-evolving nature of modern viruses, especially those with polymorphic and metamorphic characteristics, means no guarantee of 100% protection. Some sophisticated malware can evade detection for extended periods, adapt to defensive measures, and even turn off security software.

# Key Takeaways

1 **Proactive Protection**
Allot's network-native cybersecurity solution effectively blocks thousands of cyber threats for CSPs daily, ensuring service subscribers a safer internet.

2 **User Safety**
We emphasize the value and impact of cybersecurity in protecting end users' personal and financial information from cybercriminals.

3 **CSP's Role**
CSPs integrate advanced security solutions directly into their networks, providing a robust first line of defense against evolving cyber threats.

4 **Types of Threats**
We categorize threats into Browser-related Threats, Malicious Links and Sites, and Remote-Control Threats, providing a clear framework for understanding the different types of dangers.

5 **User Awareness**
Increasing user awareness about the types of threats and the value of Allot cybersecurity solutions is essential for enhancing online safety for everyone in the CSP's customer base.

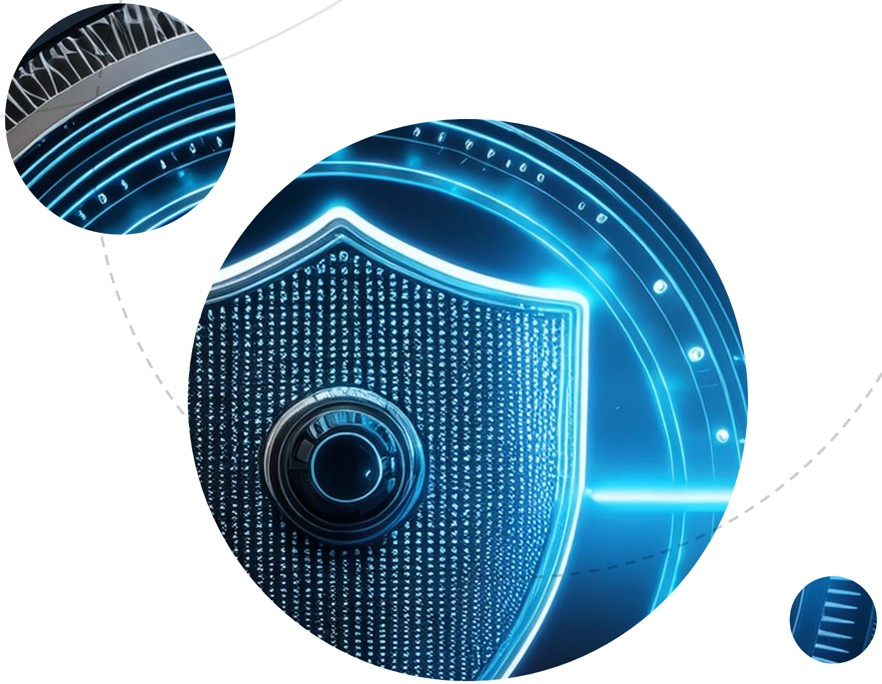
# Conclusions

As we conclude this report, we reflect on the significant strides Allot has made in protecting end users from an array of cyber threats.

The data presented underscores the effectiveness of our network-native cybersecurity solutions in mitigating threats before they can cause harm.

Our commitment to safeguarding personal and financial information remains unwavering, ensuring end users enjoy a secure and seamless online experience.

For more information about how Allot Secure can protect communication service provider's consumer and SMB customers, visit Allot Security Solutions



REFERENCES
1. HTTPS://DATAREPORTAL.COM/REPORTS/DIGITAL-2024-GLOBAL-OVERVIEW-REPORT
2. HTTPS://WWW.STATISTA.COM/STATISTICS/1294586/GLOBAL-TIME-SPENT-BROWSERS-AND-APPS/