# The State of **Consumer Cybersecurity** 2023

By ReasonLabs

January **2023**

# Table of Contents

01

# Summary

In today's digital world, home users from all around the globe are spending increasing amounts of time online. Whether it be for online shopping, gaming, working from home, attending online classes, streaming content, or any other reason, **home users face a seemingly endless barrage of cyber threats.**

Some cyber threats, such as phishing scams or Trojanized files, have been around for a long time. Other threats are new, born out of emerging technologies such as virtual or mixed reality. One commonality that unites most individuals or home users, no matter where they are in the world or what their socioeconomic status might be, is a **lack of adequate cybersecurity with the capabilities of protecting their devices and home networks from next-generation threats.** Many legacy consumer-focused antivirus providers have antiquated engines and users of their systems must replace them with next-generation antivirus solutions.

In this report, researchers from **ReasonLabs' Threat Intelligence Center (TIC)** detail the most common threats that consumers encountered in 2022. While comparing year-over-year metrics from 2021, they are able to provide much-needed context around the growth of certain threats. TIC researchers also describe where these threats have succeeded the most and what their damage possibility was, or where it could be in the future.

Alongside their research, **ReasonLabs' TIC members provide recommendations on how home users can protect themselves** by using various endpoint security tools and safety controls for each family member. Based on this knowledge and the trends detected, **ReasonLabs researchers then offer predictions of the challenges we will face** in the forthcoming year, and how consumers can overcome them.

## Methodology

**The State of Consumer Cybersecurity 2023** report features data sets collected from intelligence gathered by ReasonLabs' security researchers at its Threat Intelligence Center. The data presented ranges from January 1, 2022, through December 31, 2022.

All data detected is derived from Reason Labs users, who are located in over 180 countries around the world. The data is reduced to only real-time detections from users with free-to-use and premium accounts. Utilizing real-time detections from both account levels helps to ensure that outlier data that may alter trends are not accounted for.

# 02 Key Takeaways

**1**

**Malicious web extensions** are becoming more and more prevalent, especially in the United States. 15% of malicious extensions we detected throughout 2022 came from users in the U.S. Home users must be made aware of the threats certain malicious web extensions bring, such as new tab takeovers and search hijacking.

**2**

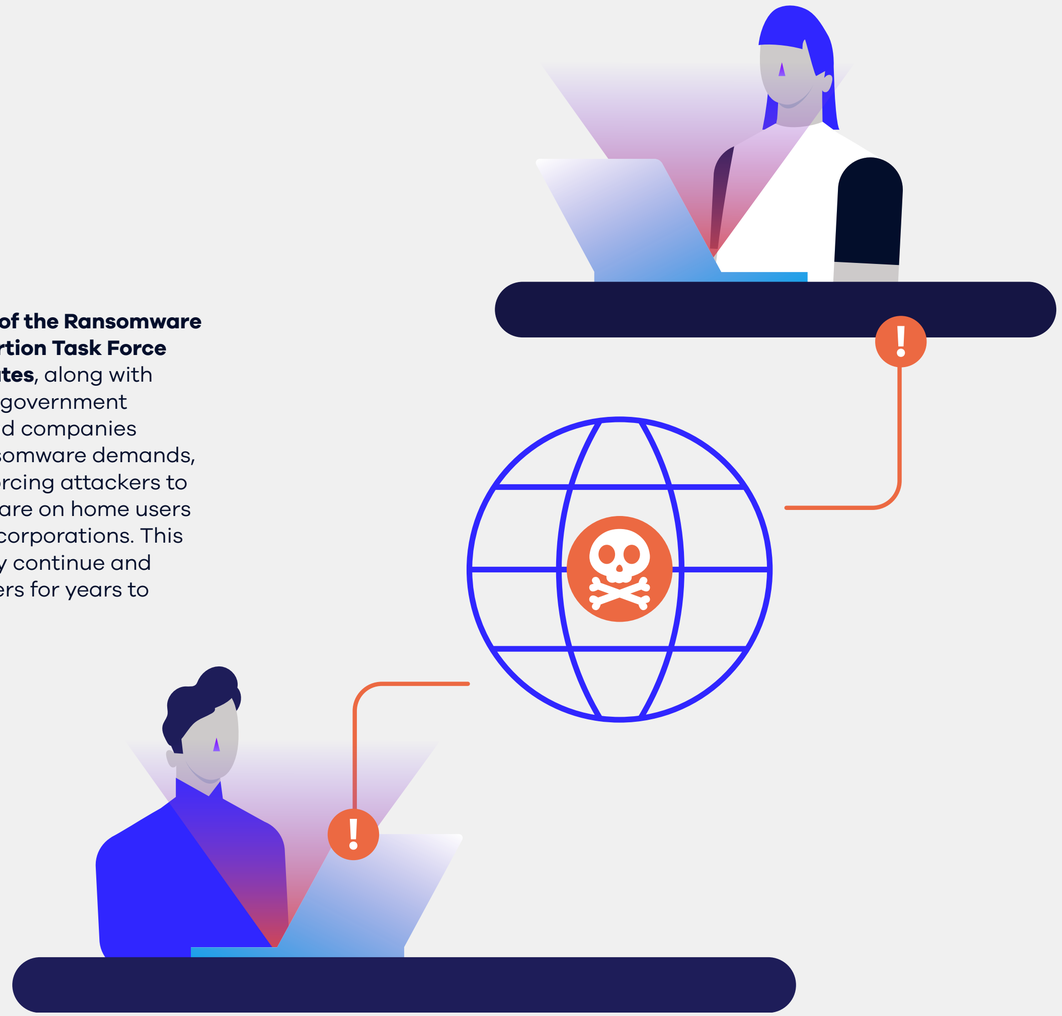
**The rise in HackUtilities** detections from 4% in 2021 to over 20% in 2022, as well as recent outside research, shows that online piracy is either at or near an all-time high. Home users are resorting more and more to the use of pirated or cracked software and applications, no matter where they are in the world.

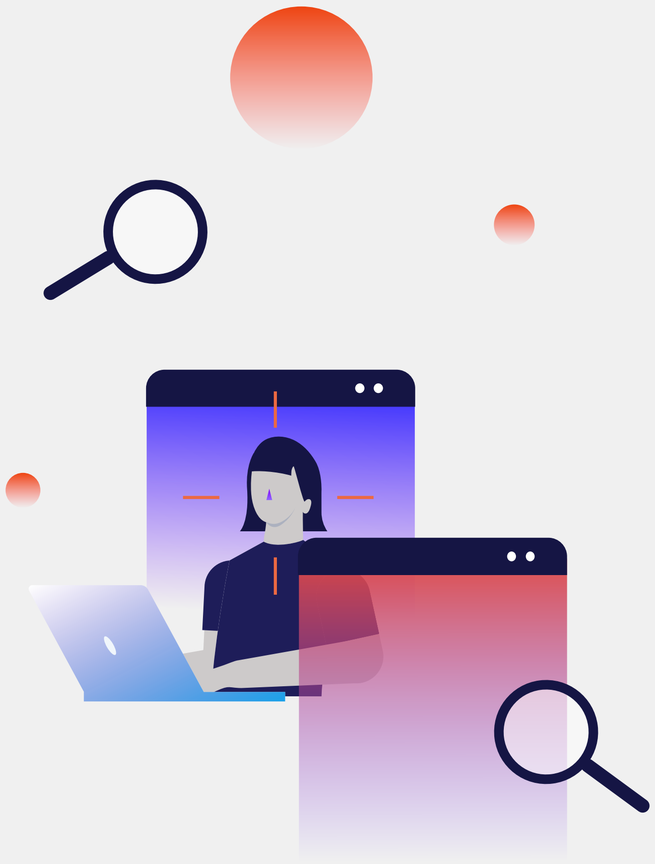
**3**

**As businesses improve their cybersecurity practices and adopt next-generation technology**, attackers are switching their focus to the home user. This improvement from businesses makes them harder to attack, so home users are seen as weaker, easier targets. The continuation of work-from-home has also given attackers a new entry point into the corporate network - often home networks are far less secure and are proving to be a viable new window into corporate networks.

**4**

**The 2021 launch of the Ransomware and Digital Extortion Task Force in the United States**, along with newly promoted government legislation around companies engaging in ransomware demands, is increasingly forcing attackers to deploy ransomware on home users instead of large corporations. This trend should only continue and plague home users for years to come.





## 5

**Technologies such as the Metaverse, IoT devices, and more were once thought of as science fiction.** Those technologies are here now and alongside have come next-generation cyber threats, such as the Metaverse attack vector identified by our researchers earlier this year. Home users must be educated on next-generation threats surrounding these technologies, and antivirus providers must update their systems to include protection against them.

## 6

**Crimeware-as-a-Service or Cybercrime-as-a-Service (CaaS) refers to the practice of providing cyber products and services to other criminals to facilitate large-scale attacks.** This ecosystem is on the rise and more CaaS products are emerging daily. These products and services are typically focused on delivering ransomware, malware, phishing threats, and more. Many are extremely easy to use and are being deployed against home users worldwide.

## 7

**Phishing remains the leading malware distribution method affecting home users and remote employees.** Phishing attacks stayed just as prevalent as they were in 2021, and show no sign of slowing down. Whether the delivery method is via email, SMS, or the weaponization of Office Documents, phishing threats continue to torture home users. Phishing education must be brought into the spotlight so home users can better decipher what is a legitimate message or request, and what is a phishing attempt.

## 8

**Cyberwarfare is a key issue affecting home users today.** Cyberwarfare is generally thought of as a nation-state attacking a nation-state. However, the consequences often trickle down to average citizens who do not usually engage in war. There have also been increasing reports of the direct targeting of citizens and civilians in cyberwarfare campaigns by nation-states in recent years, including in the United States, Ukraine, and other countries.

## 9

**The bypassing of Two-Factor Authentication (2FA) continues to rise and is expected to be exploited more and more in the coming years.** In fact, getting around 2FA is becoming so prevalent that we predict an upcoming shift in the industry to include three or even four-factor authentication, instead of just two. Home users must be made aware of these threats and implement as many factors of authentication as they can.

## 10

**Trojanized software continues to be a top threat to home users and remote employees.** In 2022, Trojans accounted for 31% of all detections affecting home users. Trojans such as coin miners, backdoors, infostealers, RATS, and spyware round out the top 5 Trojan family detections from this year.
AV providers must always be updating their systems to recognize attacks stemming from Trojans and stop them in their tracks.

# 03 Top 7 General Detections Affecting Home Users

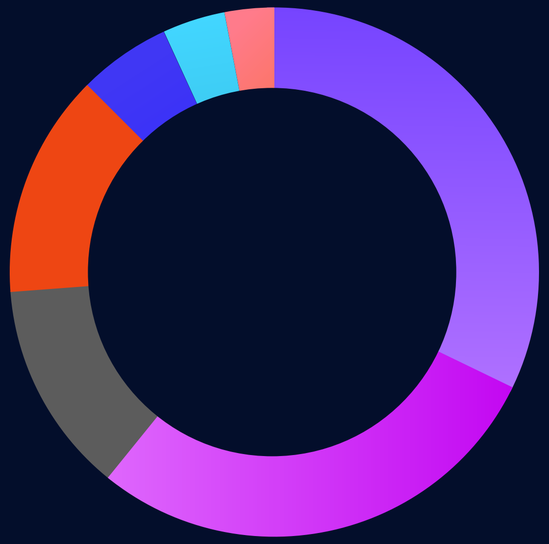
This year's investigation found that **Trojan Viruses, which held the top spot last year, continue to plague home users and were the top detection once again at 31%.** Trojans, consisting of malicious docs, backdoors, RATs, infostealers, etc., are well known, and while some have been around for decades, others are novel threats. This year's investigations also found that Potentially Unwanted Programs (PUPs) rose up the General Detections list, with 30% of all threats registering in that category.

2022 saw a drop in the detection of Miners to 4% vs. 14% in 2021. This drop might seem surprising at first, but given the fall of the crypto markets throughout the year, it's reasonable to expect some sort of decrease. We also found a drop in Adware detections in 2022 compared to 2021, and an increase in HackUtilities in 2022 compared to 2021. HackUtilities are defined as cheats, trainers, licensed software hacks, hacking tools, etc.

**Let's take a look at the numbers**

## Top Detections By General Categories

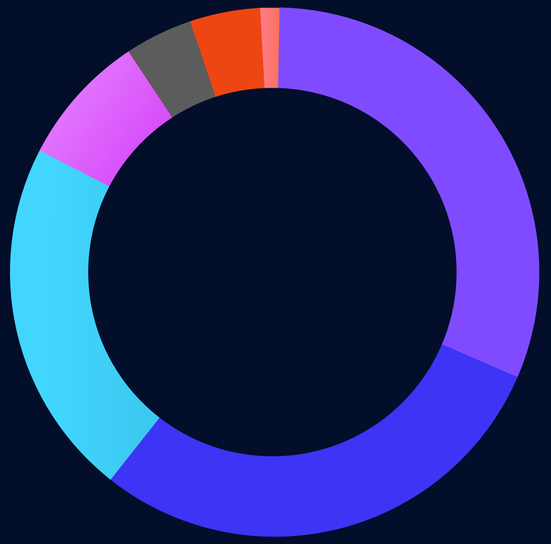
2021



- **32% Trojans** (Malicious docs, backdoors, RATs, infostealers, etc.)
- **29% Adware**
- **14% Miners**
- **13% Viruses & Worms**
- **6% PUPs** (Potentially Unwanted Programs)
- **4% HackUtilities** (Cheats, trainers, license software hacks, hacking tools, etc.)
- **2% Ransomware**

## Top Detections By General Categories

2022



- **31% Trojans** (Malicious docs, backdoors, RATs, infostealers, etc.)
- **30% PUPs** (Potentially Unwanted Programs)
- **22% HackUtilities** (Cheats, trainers, license software hacks, hacking tools, etc.)
- **8% Adware**
- **4% Miners**
- **4% Viruses & Worms**
- **1% Ransomware**

# Trojans

Despite the Trojan family of malware having existed for decades, new varieties of Trojans are being deployed almost daily. The Trojan family encompasses a wide variety of disparate malware types; however, they all have one thing in common, and that is to mask the true purpose of the malware's intent and to evade detection. Within our Trojan families, we include everything from coin and cryptominers to backdoors, spyware, infostealers, and many more threats, all of which are designed to either steal data and resources or cause damage and disruption.

## Droppers

**2022 saw a sizeable increase in Droppers detected. We assume this increase is derived from the need for cyber attackers to evade AV products and security researchers.** The Droppers themselves are not performing malicious actions, except perhaps for dropping a file or downloading it from the internet, which by themselves are not always enough to be registered as malicious.

This activity allows bad actors to reach a higher number of users without gaining a bad reputation. From this point, it is easier to distribute Droppers in higher numbers. Some of the Droppers also perform evasion techniques to make sure they arrived inside a real device of a real user.

## Infostealers

An infostealer is a **type of malware that is designed to collect information from an infected computer about a user.** Most of the time, it will exist as a module within a piece of malware. It often looks for usernames and passwords, credit card numbers saved on the browser, emails, documents, keystrokes, and any other type of personal data. After hijacking the data, it sends the information back to the attacker.

This type of malware has become a **very common threat to home users and remote employees this year.** One reason for such an increase in this type of malware in the past years is due to the fact that infostealers are commonly sold as Malware-as-a-Service (MaaS) on dark web forums and communication platforms, such as Telegram channels. A variety of these malware services exist, with many types of capabilities. They are often extremely easy to use and almost anyone can buy them. The Eternity Stealer is a good example of such malware.

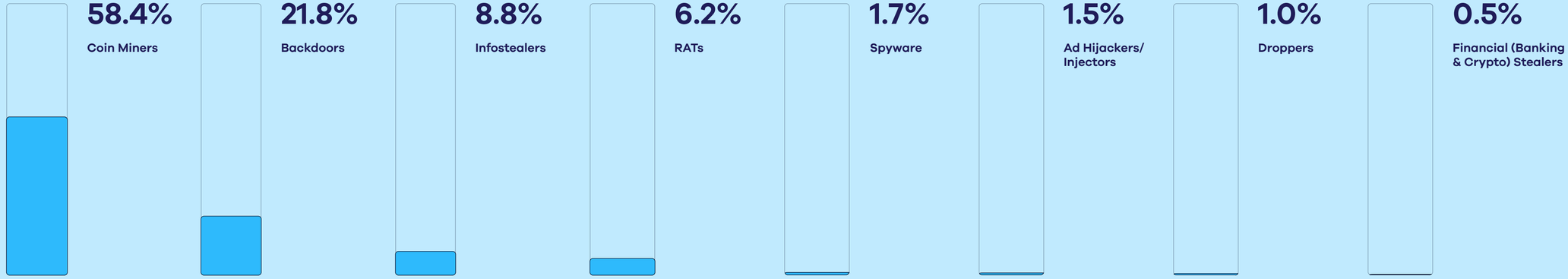
The Eternity Stealer was first seen in 2022 and with high volumes. It has the capability to steal information from well-known apps and allows its "customers" to steal passwords, cookies, credit cards, and crypto-wallets from targets, which can later be sent directly through a Telegram bot so as to not create suspicious network activity. It can be easily configured and built by a Telegram Q&A bot that lets you select features such as AntiVM or select the payload type such as .exe, .scr, etc., and modify other characteristics that help evade detection.

**The ease of buying and using this malware is causing it to become more popular, making it one of the most common attacks we saw for 2022.**

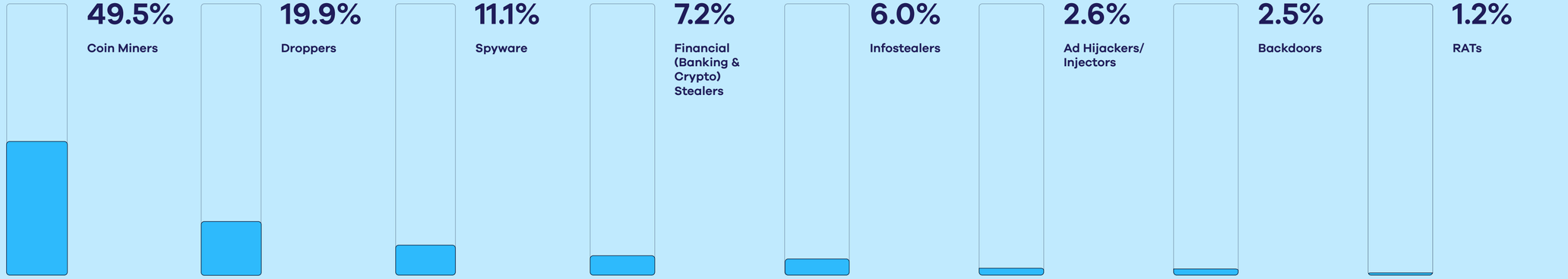
**Let's compare the Trojan detections from 2021 to 2022**

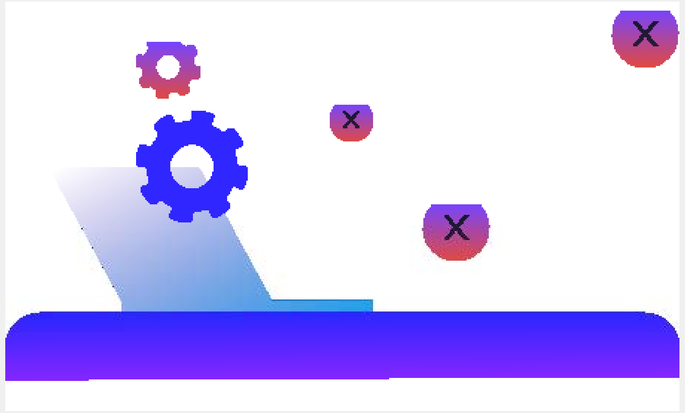
## Trojan Breakdown

### 2021




### 2022





## PUPs (Potentially Unwanted Programs)

PUPs, sometimes referred to as Potentially Unwanted Applications (PUAs) are essentially software that may consume unjustified computer resources, integrate intrusive ads and notifications outside of the product, slow the device functionality, modify system or other software settings without proper user consent and any activity which does not pose a significant risk but still may be unwanted by the end user.

## Adware

Adware is typically divided into **two categories: software that pushes ads outside of the software's scope or nefarious adware that causes harm.**

The second of the two categories consist of malware that can inject unwanted ads onto a device, hijack a computer's settings, such as search behavior, and show potentially dangerous ads that can spread into other forms of malware.

**Browser extensions have grown from being a small piece of software into a full-on sub-economy of the Internet industry.** In fact, extensions and malicious extensions have become so impactful, that we will take a closer look at them within the Emerging Threats section of this report. For now, it's important to note that with the rise in the popularity of extensions has also come a rise in malicious extensions.

**Home Tab Takeover**
**32.40%**

**Search Hijackers**
**29.52%**

**Browser Modifiers**
**13.59%**

**New Tab Takeover**
**13.51%**

**Dropper**
**10.98%**

**The most prevalent Adware detection for 2022 was Home Tab Takeovers.** Home Tab Takeovers, together with Search Hijackers, aim to hijack the search of the user. Home Tabs usually change the background image of the Home Tab and add widgets for the user's convenience, like a direct link to Twitter, Amazon, or other websites. Those widgets can also lead to malicious sites, or serve as affiliate links. **Attackers often gain money from serving as the affiliates of a user's searches or even steal all of what the user is searching for and sell the data.**

## HackUtilities

**We saw an increase in HackUtilities detections from just 4% in 2021 to 22% in 2022.** This could be explained for a few different reasons, but first, let's explain what HackUtilities detections encompass. **HackUtilities are defined as cheats, trainers, licensed software hacks, hacking tools, etc. HackUtilities are borderless and detected from virtually every country in the world.**

One reason for this increase in HackUtilities detections could be the increase in online piracy. A MUSO study recently found that the number of visits to online piracy sites has increased by more than 20% compared to last year. While piracy is nothing new, this YoY rise could be a result of the current global economic crisis. Home users might be turning more towards pirating software or the use of cracked applications in order to save money. Another possible reason for the increase in HackUtilities detections from 2021 to 2022 could be the ongoing war in Ukraine. When Russia began its attack on Ukraine, governments from around the world levied economic sanctions and many corporations pulled out from Russia. Microsoft was one of those corporations. They pulled support from Russia in March, meaning people could not purchase Windows operating systems or any other Microsoft-related devices. In June it was reported that Russia-based web searches for pirated Microsoft software surged by as much as 250% and there was a 650% surge in searches for Excel downloads.

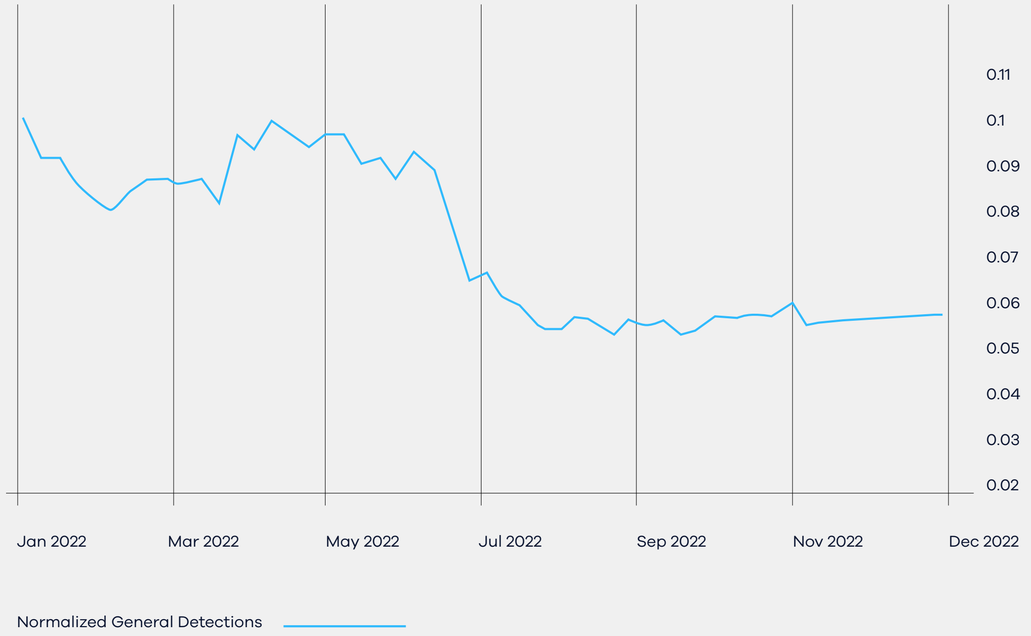
**No matter the reason why, the increase in HackUtilities detections signals that home users are resorting more to pirated or cracked software.**

## Miners

2022 saw a sharp **decrease in the detection of miners compared to 2021, as well as an overall decrease as 2022 progressed.** This drop could be attributed to many different factors, however, we assume **one big reason is due to the overall sentiment shift in the crypto markets.**

Bitcoin's USD value is down over 50% at the time of writing compared to its value on January 1, 2021. Some bad actors might be moving on from crypto, while others could be patiently waiting for the market sentiment to shift positively. Another possible reason for the drop could be attributed to the multiple arrests made throughout 2022 on cyber gangs from Russia.

**Global Crypto Miner Detections Throughout 2022**



## Viruses & Worms

While most people think of malware as being a virus, the term 'virus' typically refers to malware that is designed to self-replicate and infect other files on a victim's computer. It does so by adding its own malicious code to innocent files, such as other programs. When these programs are executed, they then carry out malicious activities defined by the virus. Once believed to be less prevalent as time goes on, it turns out that many legacy viruses of yesteryear are still active in the ecosystem, spreading their payloads.

2021

| 34% | 18% | 11% | 9% | 8% | 8% | 6% | 4% | 2% |
|---|---|---|---|---|---|---|---|---|
| Ramnit | Floxif | Neshta | Sality | Chir | Ground | Wapomi | Jeefo | Expiro |

2022

| 24.75% | 15.04% | 9.40% | 8.63% | 7.94% | 6.06% | 5.21% | 4.11% | 3.71% |
|---|---|---|---|---|---|---|---|---|
| Ramnit | Floxif | Sality | Neshta | Ground | Delf | Chir | Wapomi | Jeefo |

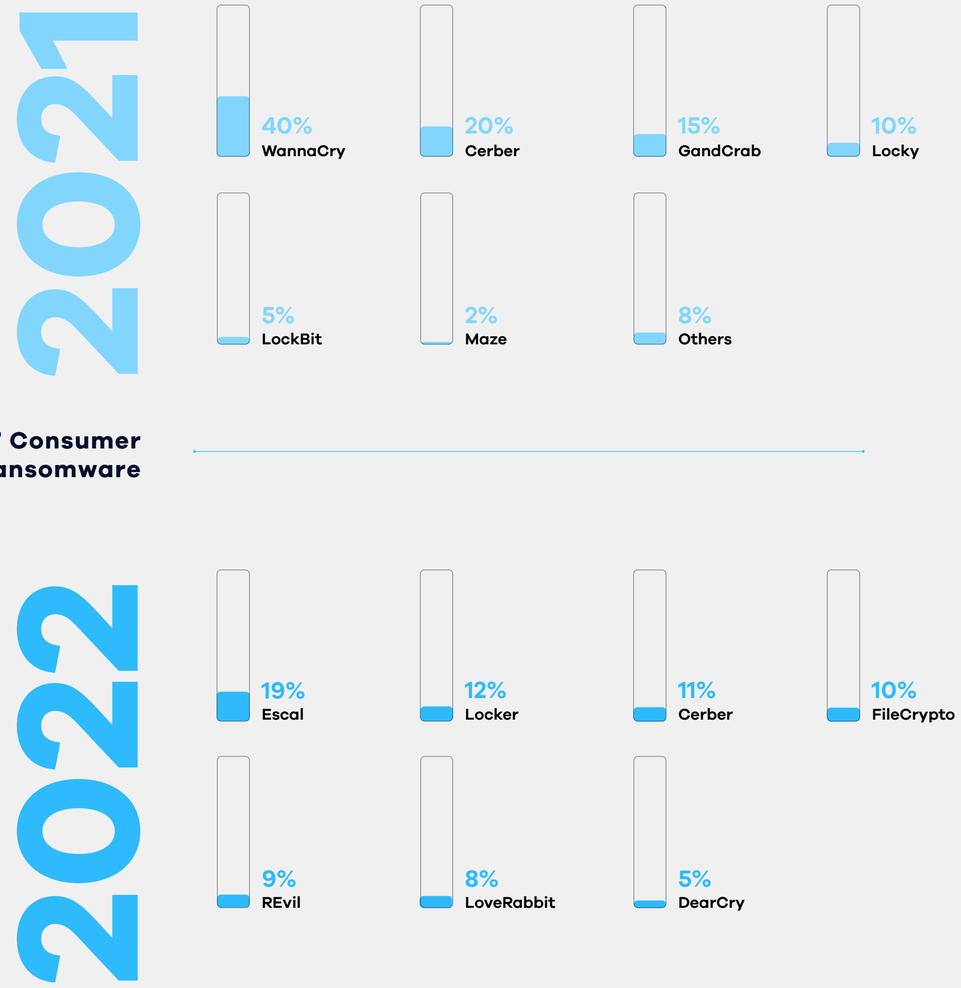
# Ransomware

**Detections of ransomware affecting home users dropped slightly in 2022 compared to 2021**. This decrease could be attributed to a few different factors, including the drop in the global crypto markets, notable arrests of Russian cyber attackers, the closing of REvil, and more.

In 2021, it was found that nearly 75% of all ransomware revenue goes to Russian-linked hackers. This year's notable arrests might have caused some bad actors to get cold feet. Also, as most ransomware is distributed from Russia, it is possible that the Russian government is using many of these criminals to help attack Ukraine or other fronts. For example, it was recently discovered that Russian hackers have deployed a new strain of ransomware specifically against Ukraine, called Somnia.

Despite the overall drop, **we did find interesting trends around the attackers who do deploy ransomware aimed at home users.** Escal was the top detection of the year, after not being featured in the top seven in 2021. WannaCry ransom detections, which held the top spot last year with 40%, plummeted off the top seven list.

Let's look at the data →




## Magniber Ransomware

During the second half of 2022, we saw a **large increase in distribution attempts of the** Magniber ransomware. Magniber is known for being a very evasive and sophisticated attack group that has, in the past, utilized zero-days and exploits to distribute their ransomware to clients.

Recently, in order to cover more clients, they have disguised the programs they distribute with names of Windows updates, such as "SYSTEM.Security.Database. Upgrade.Win10.0.jse", "win10-11_ system_upgrade_software.msi", "MS. Update.Center.Security.KB[random]" instead of using exploits.
The group's newest distribution method includes an MSI installer file that contains a malicious DLL. The DLL holds a malicious encrypted payload that is decrypted into the process memory upon execution and infects the host. The attack is completely file-less in order to evade as many AVs and EDRs as possible. They target end-users specifically and not organizations.

# 04 Cyberwarfare

The term ‘cyberwarfare’ has reached the mainstream in recent years, defined as the activity of using the internet to attack a country’s computers. This could be done in order to **damage infrastructures such as communication and transport systems, or water and electricity supplies.** Different types of cyberwarfare include espionage, sabotage, propaganda, and economic disruption, among others. They are typically motivated by military actions, hacktivism, monetary gain, not-for-profit research, and more.

Cyberwarfare is generally thought of as a nation-state attacking a nation-state. However, often the consequences trickle down to average citizens who do not usually engage in war. There have also been reports of the direct targeting of citizens and civilians in cyberwarfare campaigns by nation-states in recent years. The most notable examples of this come from the ongoing war in Ukraine.

Researchers from Mandiant recently detailed some of Russia’s evolving cyberwarfare strategies aimed at citizens at the 2022 CYBERWARCON security conference in Arlington, Virginia. They reported that “… the [Russian] GRU has shifted in particular to what they call “living on the edge.” Instead of the phishing attacks that GRU hackers typically used in the past to steal victims’ credentials or plant backdoors on unwitting users’ computers inside target organizations, they’re now targeting “edge” devices like firewalls, routers, and email servers, often exploiting vulnerabilities in those machines that give them more immediate access.”

Another example of the direct targeting of civilians with cyberwarfare is when the Russian government interfered with the 2016 U.S. presidential election. The various attacks were aimed at many U.S. politicians, including Hillary Clinton and former President Donald Trump. However, the effects were felt directly by U.S. citizens.

**Let’s dig into some of our data that shows what’s happening to home users around the world.**

# Top 20 Most Attacked Countries

In this section, we will compare detection rates and detection types across different countries and locations. We will see that threat types may differ between countries, as geography plays a key factor in the type, amount, and prevalence of different versions of cybersecurity attacks.

The top five countries with the most detections per user throughout 2022 are Kazakhstan, Russia, Egypt, Ukraine, and Bolivia respectively. While the list is diverse, over 50% (11/20) of the most attacked countries are in Asia, while only 10% (2/20) are from Europe.


**Avg Detections Per User In 2022**

| | | | |
|---|---|---|---|
| Kazakhstan (KZ) | 23.37 | Argentina (AR) | 8.40 |
| Russia (RU) | 20.26 | China (CN) | 8.28 |
| Egypt (EG) | 13.48 | Arab Emirates (AE) | 8.25 |
| Ukraine (UA) | 10.44 | Philipines (PH) | 7.92 |
| Bolivia (BO) | 10.24 | Thailand (TH) | 7.83 |
| Indonesia (ID) | 10.00 | India (IN) | 7.72 |
| South Africa (ZA) | 9.77 | Hungary (HU) | 7.69 |
| Israel (IL) | 9.68 | Canada (CA) | 7.53 |
| Morocco (MA) | 9.11 | Taiwan (TW) | 7.43 |
| Pakistan (PK) | 8.91 | Peru (PE) | 7.37 |

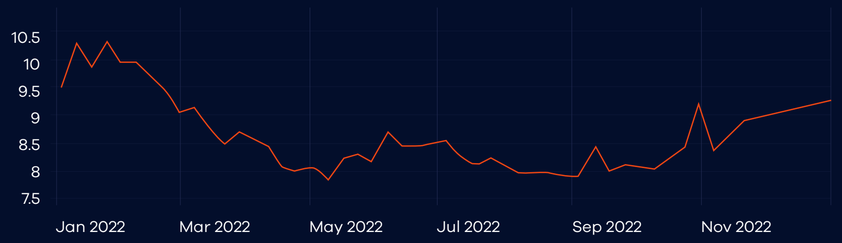
## Russia vs. USA

It's important to compare and contrast the data of certain countries or regions to gain an understanding of what's happening around the world. Let's take one of the most attacked countries based on average detections per user throughout 2022, Russia, and compare the data to the United States.

While the top detections in both countries were quite similar throughout 2022, Trojans were highly prevalent in Russia compared to the U.S. with almost 50% more detections. HackUtilities made up over 10% of detections in Russia while they did not register as a top detection in the U.S. Adware was more prevalent in the U.S. than in Russia, which includes malicious web extensions, which we will touch on more in the Emerging Threats section of the report.

Russia

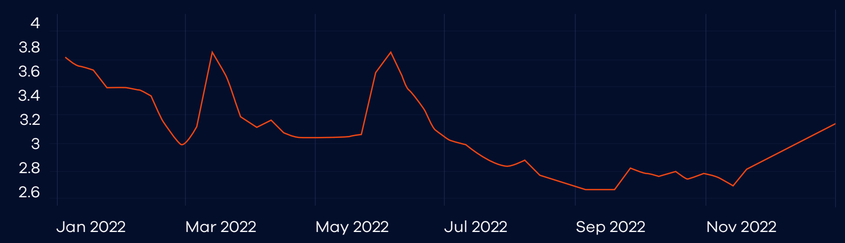
### Detections per week throughout 2022



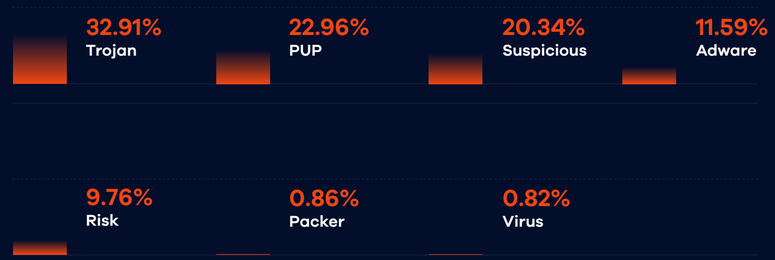

### Top Detections in Russia From 2022


United States

### Detections per week throughout 2022




### Top Detections in the United States From 2022

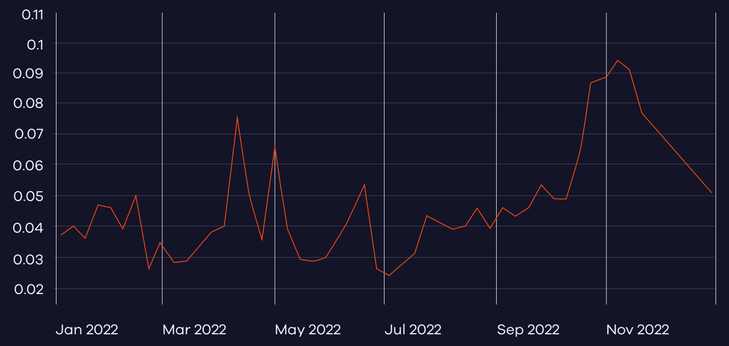



# The War In Ukraine

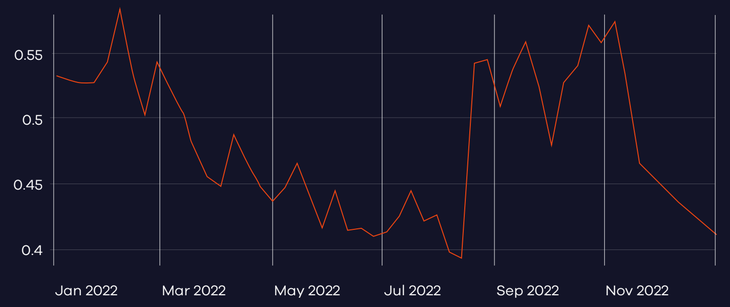
The war in Ukraine, which began on February 24, 2022, is still ongoing at the time of writing this report. It has unfortunately created Europe's largest refugee crisis since World War II and caused tens of thousands of casualties. Civilians in both Ukraine and Russia have faced numerous attacks, both physical and virtual. Cyber attacks in Ukraine specifically started even before February, with the first reported attack taking place in January.

Since the war was one of the defining events of 2022, we decided to investigate the data and dig deeper into the cyber detections made in Ukraine. Below we highlight three areas where Ukrainian civilians were highly affected: detections of Phishing Documents, Trojan Viruses, and Exploits.

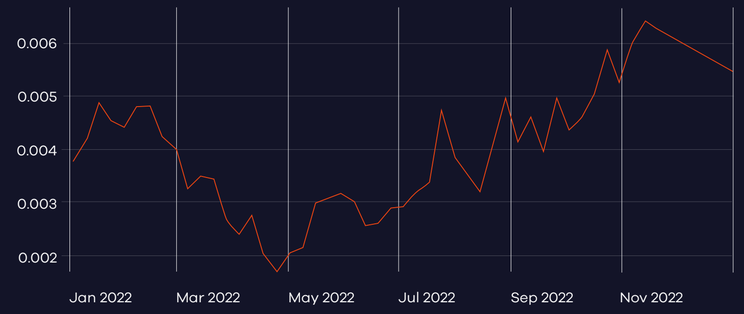
**Phishing Documents**




**Trojans**




**Exploits**



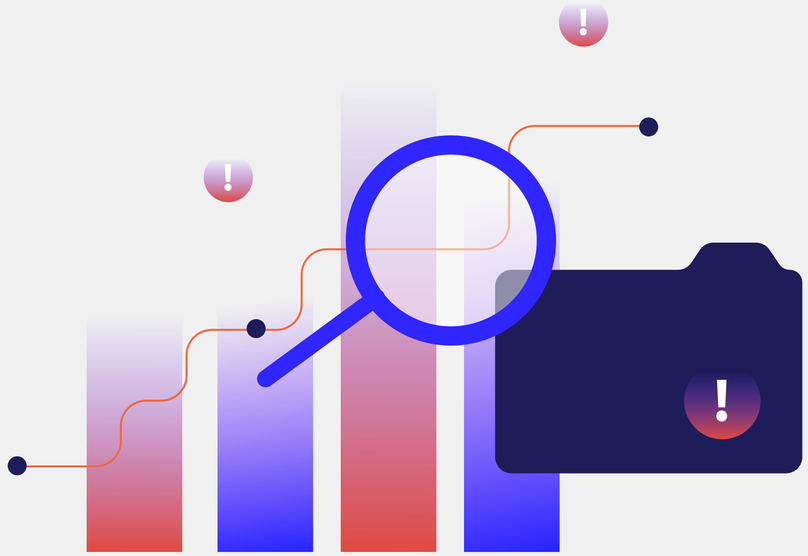

On all three charts, we see an increase in detections in February compared to January, signaling that the Russian invasion of Ukraine was also paired with cyber attacks. Detections then decrease somewhat sharply in March, which we attribute to the possibility of civilians fleeing or hiding the attacks and not using their devices as often. As the year progressed, we saw all three types of attacks pick up strongly.

# Data Breaches

The term 'data breach' typically refers to the exposure of confidential or sensitive user information. Hackers tend to target large institutions such as private enterprises, publicly traded companies, healthcare providers, government agencies, universities, and any other organization with sensitive user data. Many large-scale data breaches are accomplished with the deployment of ransomware, malware, social engineering tactics, Trojans, or sophisticated phishing attacks. Once hackers attain sensitive user data, it can be sold on the dark web or even in easily accessed forums.

Data breaches are not a new phenomenon, however, in 2022 we saw a host of breaches that affected millions of home users worldwide, including:

- **North Korean hacking group Conti pulled off a massive Ransomware attack against Costa Rica**, which crippled parts of the country and affected millions of citizens.
- Medibank Private Ltd, the largest health insurance provider in Australia, **had the sensitive data of over 4 million users stolen in a hack**, which was recently put up for sale on the dark web.
- Two million patients of the Massachusetts-based Shields Health Care Group were affected by a data breach when social security numbers, names, medical records, billing information, and more were stolen.
- FlexBooker, an online booking software provider, suffered a breach in which over 3.7 million users were affected.
- The Russian hacking group Vice Society leaked over 500GBs of data from the Los Angeles Unified School District (LAUSD), the U.S.'s second-largest school district.



It's also worth pointing out the year that the notorious hacking group Lapsus$ had in 2022. They went on an all-out hacking spree that included the successful breaches of large companies like Globant, Microsoft, Nvidia, Okta, Samsung, T-Mobile, and more. While some of these hacks and breaches did not directly affect consumers, they were widely publicized. The group focused on extorting these companies with data theft and seemed to relish in the notoriety. Despite the sophistication of the hacking rampage, it was reported that key group members were in fact teenagers, including the apparent mastermind who was only 16 years old.

# 05 Top Exploits of 2022

## **Follina** (CVE-2022-30190)

'Follina' (CVE-2022-30190) is a Microsoft Office zero-day vulnerability affecting the Microsoft Support Diagnostic Tool (MSDT), which was **brought to light** in May of this year. It's a high-severity vulnerability that leads to remote code execution attacks. 'Follina' is also exploited by the 'XFiles' infostealer malware for dropping its payload on target computers.

This works by exploiting the ability of Microsoft Office document templates to download additional content from a remote server. Many phishing campaigns exploit that vulnerability by sending attachments leveraging Follina. Microsoft has since **released guidance** for the exploit. However, many users do not update their operating system or harden its configuration, thus they are still exposed to it and attackers continue to use this vulnerability.

## **Log4Shell** (CVE-2021-44228)

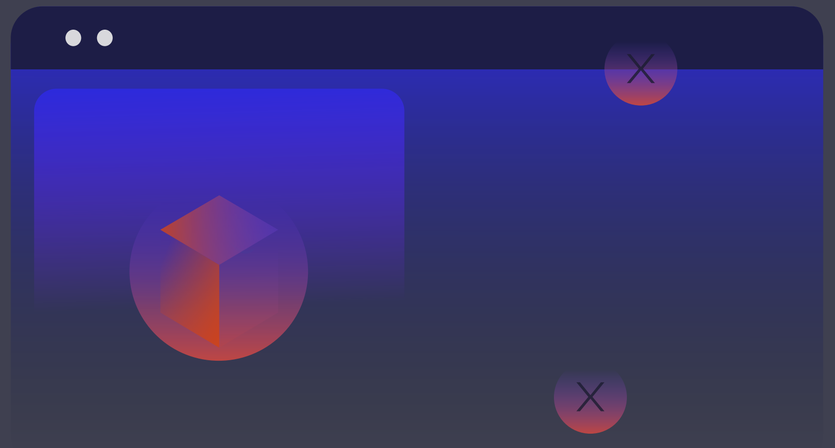
The top exploit of 2022 that affected home users was Log4Shell. Apache Log4j is an open-source Java-based logging utility that is part of the Apache Logging Services. At the close of 2021, a critical flaw that led to remote code execution was found. It is widely exploited due to the prevalence of the Log4j library in web applications and is estimated to affect hundreds of millions of devices of individuals, organizations, governments, etc.

It even exposed an estimated 93 million monthly active users of the famous game **'Minecraft', which uses Log4j.** In this instance, an adversary can exploit a Minecraft server and take control over the players' computers, which makes it a huge entry point for an attacker and can lead them to steal sensitive information from users. This CVE got a score of 10 on the CVSS, which is the highest available score and is considered one of the most severe exploits that have been seen in the past years. Its effects will be felt for years to come.

## Chrome Zero-Days

2022 saw an **abundance of Google Chrome vulnerabilities,** some of them zero-days that were spotted by Google in the wild. While Google abstains from providing the full details of these vulnerabilities, they do make light of them when they are discovered. Some of the zero-day vulnerabilities are far-reaching and affect not only Google Chrome but other browsers as well. For example, vulnerability CVE-2022-1096 **affected Microsoft Edge**, which was forced to quickly release an urgent patch.

Some of the vulnerabilities that were found in 2022 could affect users who simply surf malicious web pages. This would be enough to infect them by remote code execution, which can lead to information stealing or malware installation on their device. It's important to mention that malicious extensions could also hinder the updating mechanism of Chrome, so users might suffer from different vectors due to that occurrence. Updating the web browser regularly is highly important.



## Rootkits

Rootkits are malicious software that allows hackers to remotely control a computer while operating in a hidden fashion, often going unnoticed by the user.

Rootkits can have a number of tools or modules. For example, programs that can track keystrokes, enable hackers to steal passwords or sensitive private information. Rootkits can also give hackers the ability to subvert or disable key parts of a user's system, like anti-malware software, which will make it harder to detect them. We've seen more new rootkits this year and with the rise of vulnerable drivers, we've seen more combinations of the two, such as the **FudModule rootkit**, used by the North Korean hacking group Lazarus, that abuses a Dell hardware driver.

Along with using vulnerable drivers to exploit the kernel, Rootkits have become stealthier by exploiting the firmware and making themself invisible. An example of this that has hurt consumers for a long time is the Unified Extensible Firmware Interface (UEFI) Rootkit called **CosmicStrand**. This rootkit has been used in the wild since 2016 to ensure computers remain infected even if an operating system is reinstalled or a hard drive is completely replaced. The UEFI is a low-level and highly opaque chain of firmware required to boot up almost every computer.

# 06 Phishing: The Leading Malware Distribution Method Affecting Home Users

**Phishing threats have continued to play a major role in our society** at large and specifically the cybersecurity landscape throughout 2022. Phishing attacks remained just as prevalent as they were in 2021, so let's take a quick deep dive into the subject.

Phishing attacks can be deployed in many ways, however, **the most common attacks are done via email, SMS messages, Microsoft Document weaponization, and malicious script files.** Several tactics are used in phishing campaigns to trick users into opening links or visiting harmful sites, including using timely trends, copying private information, leveraging personal data, and more. Oftentimes there are telltale signs of phishing attempts, such as the misspelling of words, the incorrect use of URLs, completely irrelevant messaging, and more.

In addition, **we have witnessed a significant rise in the amount of Unitrix file names, which is a great method for phishing to work on users, even the technical ones.** We've witnessed, for example, a wave of Redline infostealers distributing its files using this method. ReasonLabs researchers detailed Unitrix threats earlier in the year, which you can read here.

**Below we will examine phishing Office Documents weaponization, email downloads, and threats leveraging COVID-19, that all targeted home users in 2022.**

## Office Documents Weaponization

Macros are scripts written in Visual Basics that are embedded into Office Documents. Using macros, users can enrich their documents with the automation of repetitive tasks, and improve productivity. However, once attackers realized it is possible to distribute Office Documents with malicious scripts inside them, this attack vector grew to be one of the most common ways to lure users into a trap. The macros can be used to do anything on the machine, beginning with downloading more malware, executing it, and sending back data.

Over the years, we've witnessed an increase in the usage of macros in Office Documents. And it's not just macros being used to attack victims - we've witnessed a number of other technologies which, while effectively having the same behavior as macros, use different techniques to weaponize Office Documents and include embedded, linked, and remote OLE objects, Excel 4.0 macros and remote templates.

**The distribution of macros across the globe in 2022**

| | |
|---|---|
| Japan (JP) **12.09%** | Indonesia (ID) **9.93%** |
| Bolivia (BO) **11.75%** | Colombia (CO) **9.77%** |
| Peru (PE) **10.60%** | Ecuador (EC) **8.77%** |
| Morocco (MA) **10.10%** | Brazil (BR) **8.44%** |
| South Africa (ZA) **10.10%** | Vietnam (VN) **8.44%** |

## Email Threats

Office Documents that hide macro code are still very common, and many files were sent as phishing documents to lure users to run the malicious code in emails. Out of all the malicious files detected via phishing emails, here are the countries that were most affected throughout 2022:

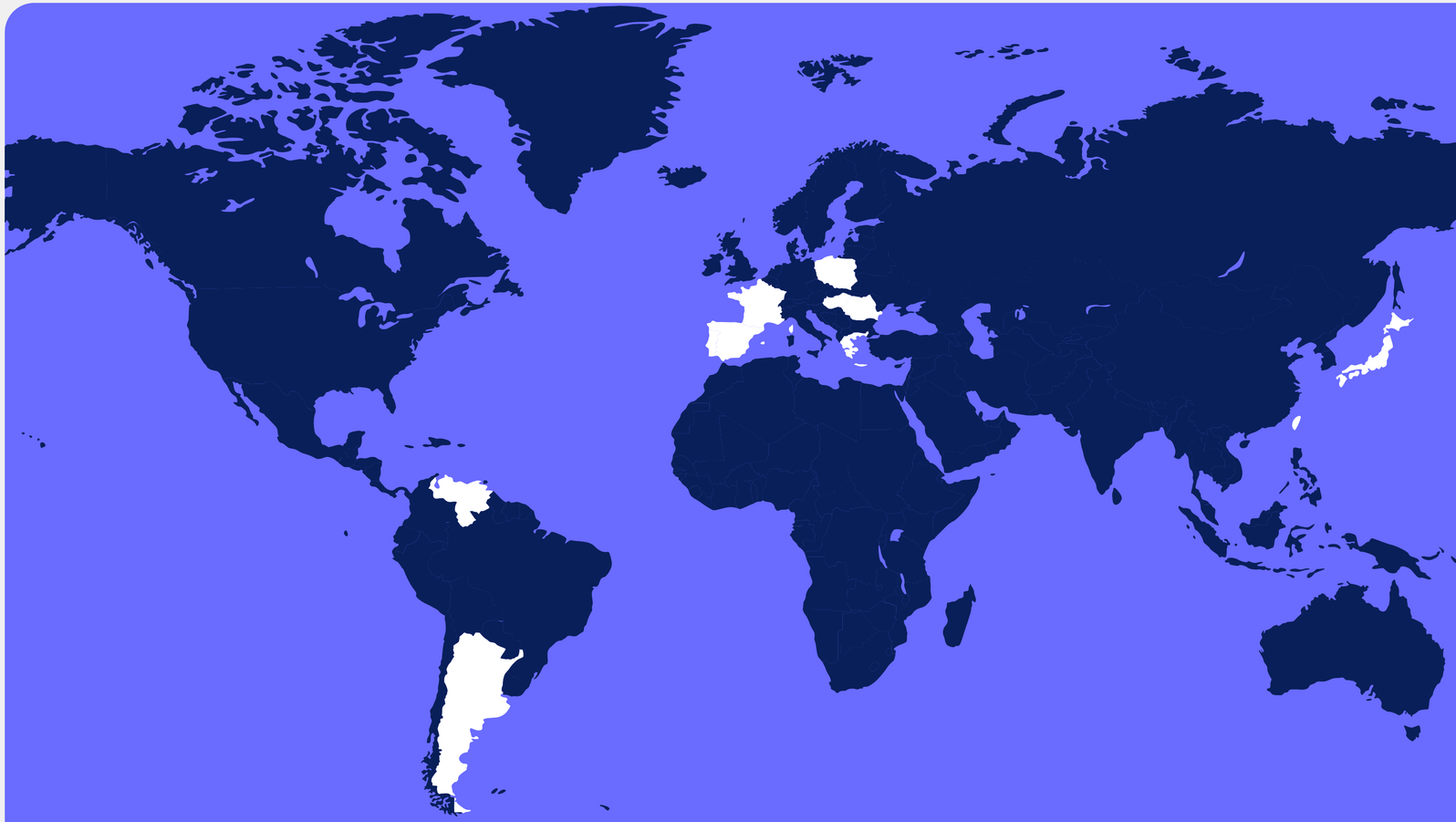
## COVID-19 Threats

2021 saw a decrease in the number of files and documents containing phrases related to COVID-19, compared to 2020. Nevertheless, threats coming from phishing documents related to COVID-19 still found their way to users, most of them occurring in Microsoft Office documents with macros.

2022 was no different, as COVID-19 has of course not yet left us and may continue to affect us for years to come. As such, we expect phishing attacks leveraging COVID-19 will persist. Let's take a look at which countries were affected the most by COVID-19-related phishing threats throughout 2022.

**COVID-19 Phishing Threats By Country In**

# 2022



| | | | | |
|---|---|---|---|---|
| **Japan (JP)** 7.0% | **Taiwan (TW)** 6.0% | **Argentina (AR)** 5.6% | **Poland (PL)** 5.5% | **Hungary (HU)** 5.1% |
| **Spain (ES)** 6.7% | **Portugal (PT)** 5.6% | **France (FR)** 5.5% | **Greece (GR)** 5.4% | **Venezuela (VE)** 4.9% |

# 07 Emerging Threats

## Metaverse Security Threats

The Metaverse, including **Virtual Reality (VR) and Mixed Reality (MR)**, is firmly being established in the mainstream of our society. What used to be considered science fiction is now being brought to life, with over 170 million people worldwide using some form of VR today.

While the market is large and filled with different providers and manufacturers, many users are utilizing Android-powered devices such as Meta's Oculus and HTC's Vive. In fact, according to IDC, Meta's Quest 2 product has nearly 15 million users and its VR sales grew 242% in Q1 '22.

Many home users of VR devices have been pirating games and software in recent years. To install these apps, devices must be switched into Developer Mode. Favored ways for installing free games on VR devices include popular platforms such as Steam, SideQuest, and other piracy sites.

Earlier in the year, ReasonLabs researchers identified an attack vector that can connect remotely to Android-based VR devices, set to Developer Mode, and record the headset screen. We will no doubt see more threats like this in the near future, and AV providers must be ready to take on these threats.

Home users must also be wary of using pirated games or software on their devices.

## Steganography

Steganography derives from the ancient art of hiding information in plain sight, in objects that do not cause suspicion. In the digital era, the usage of such a technique has been successfully adapted by malware authors, usually using PNGs or digital images. A recent example of this was brought to light in November of 2022 when it was discovered that Worok hackers hid new malware in PNGs using steganography.

The usage of steganography in malware is carried out by dividing a whole program into bytes and scattering those bytes inside the information of the picture. In more detail, pictures are represented by pixels, where each pixel is defined by 24 bits, in which each octet represents the amount of one of the RGB colors. Each representation results in a color. There are a couple of ways to hide information using the pixels, the most common being to change the least significant bit of the pixel - that way the change in color is undetectable, while information was added to it.

It's important to note that the picture itself cannot execute the hidden code; it needs another program that knows exactly where and how the information was hidden in order to extract and execute it. It's equally important to note that steganography is not exclusive to image files, and can be used on any other object.

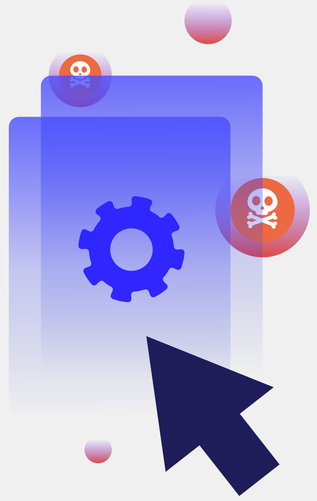
The usage of steganography in malware is carried out by dividing a whole program into bytes and scattering those bytes inside the information of the picture. In more detail, pictures are represented by pixels, where each pixel is defined by 24 bits, in which each octet represents the amount of one of the RGB colors. Each representation results in a color. There are a couple of ways to hide information using the pixels, the most common being to change the least significant bit of the pixel - that way the change in color is undetectable, while information was added to it.

It's important to note that the picture itself cannot execute the hidden code; it needs another program that knows exactly where and how the information was hidden in order to extract and execute it. It's equally important to note that steganography is not exclusive to image files, and can be used on any other object.

### Living Off the Land (LOL) Attacks

Living Off the Land (LOL) has been a growing category for a couple of years now. Steganography is not considered a Living off the Land method but comes hand-in-hand with the general idea of camouflaging and staying out of sight from AVs and researchers.

Malware adversaries want to stay undetected for as long as possible. General threats produce different IOCs once they run on the machine, and those IOCs are used to mark them once researchers and AV companies find them.



LOL attacks use techniques that do not produce IOCs - for example, they avoid creating files and instead use programs that already exist on the machine, such as PowerShell or WMI. They use these programs to add exceptions to the local firewall, add exclusions to Windows Defender, add persistence mechanisms, alter shortcuts, and so forth. In the past year, we've witnessed a steady rise in the number of detections related to LOLbins.

In the past year, we've seen 15 new LOL binaries and scripts that enable attackers to download and execute malicious code. At the time of writing this report, there are 175 published LOLs divided into binaries, scripts, libraries, and other binaries from Microsoft, such as Visual Studio's binaries for example. The entire repository of LOLs makes it possible for attackers to execute and compile code, as well as to carry out file operations such as downloading, uploading, and copying. It can give them persistence, an option to side-load DLLs, and more. Such a toolset that can evade many AVs is essential for attackers, which is why it makes it so popular among their malware.

## Vulnerable Drivers (B.Y.O.V.D)

Vulnerable drivers have been a very hot topic in the last year and are important to detail. Simply put, vulnerable drivers make it easy for malware adversaries to bypass Windows kernel protections. An adversary merely installs the legitimate signed third-party driver that contains a memory corruption vulnerability or other serious flaws and then exploits them in order to escalate their privileges.

As opposed to malicious drivers and rootkits, vulnerable drivers are legitimate drivers that are usually used for their original purposes. This slight difference makes it harder for traditional AVs to detect such an attack and therefore this method has become more common, especially through the past year. Many known threat groups have used this technique in the wild, and continue to do so. For example:

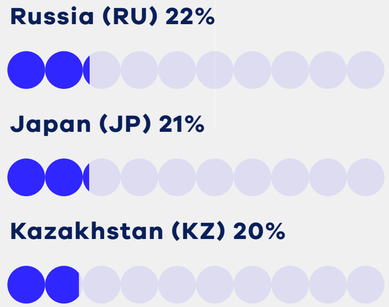
- North Korean hacking group 'Lazarus' abused a Dell hardware driver in September of 2022.
- 'BlackByte' ransomware group recently exploited a driver signed by MSI.
- Turla exploited the signed VirtualBox driver to deactivate DSE and load its unsigned payload drivers afterward.
- 'Remsec' has a plugin to drop and execute vulnerable Outpost Sandbox or Avast Virtualization drivers in order to gain kernel mode privileges.

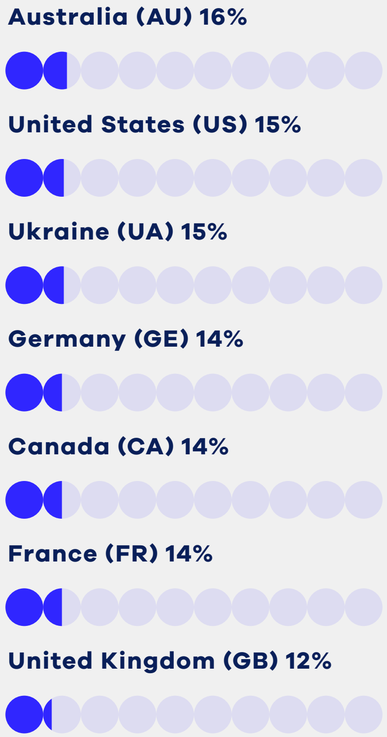
Usage of vulnerable drivers has been spotted even with Office Documents that exploit them to gain privilege escalation. With the existence of such drivers and the ongoing process of discovering similar new drivers, we've witnessed a rise in the number of detections related to vulnerable drivers.

## Malicious Web Extensions

Web browser extensions have grown from being just a niche piece of software into a full-on sub-economy of the Internet industry. Extensions are supported on most browsers, including Google Chrome, the world's most popular web browser, which offers over 100,000 extensions in its Chrome Web Store. With the rise in the popularity of extensions has come a rise in malicious extensions built by bad actors who have pinpointed this relatively new attack vector.

Here we will examine where the majority of the malicious web detections found in 2022 originated from



**Extensions & Browser Modifier Breakdown From 2022**

**Home Tab Takeover**

28.22

**Search Hijackers**

21.23%

**Risk Extensions**

18.50%

**Toolbar**

12.08%

**Browser Modifiers**

9.97%

**Dropper**

7.07%

**New Tab Takeover**

2.94%





## CDNs of Unintended Malicious Use on the Rise

Attackers always manage to find new interesting techniques to use for the operation of their malware. Often they try to imitate normal, expected traffic to avoid detection so they can communicate with systems under their control. To do so, attackers abuse Content Delivery Networks (CDNs) to mask malware command and control (C2) traffic over platforms that many users use on a daily basis.

Communication platforms such as Discord, Telegram, Signal, WhatsApp, and more have been abused to command and control intruded systems and to spread their malware. Besides the above, there are more methods that are sometimes used for C2. In even more sophisticated attacks, adversaries would use steganography methods to hide their malware in media files, which makes the attack even less detectable. We have even encountered a C2 channel using the audio streaming platform Spotify.

Every year there are new unusual methods for C2 channels and it gets harder to detect them. Moreover, there are many open-source codes that implement it, which makes it easier for every malware to use it.

# 08 How Home Users Can Protect Themselves

There are many tools available that home users and remote employees can utilize to shore up their at-home cybersecurity. These tools not only include physical and digital products but also include general education and cybersecurity awareness.

## Education & Awareness

The continued push for cyber education and cyber awareness is paramount in order to reduce the vulnerability of home users and remote employees, and the overall success of next-generation attacks.

As phishing continues to be the leading malware distribution method affecting consumers, education surrounding this form of cyber attack is vital. Individuals must learn to recognize the signs of phishing. Common methods such as phishing emails and SMSes are often only successful through social engineering. Simple things like not opening suspicious emails, clicking on suspicious links, or downloading from suspicious sites, can all avert the risk of a phishing attack.

Education from a young age is also crucial. Connected devices are being used by increasingly younger ages, so we need to raise awareness of cyber safety, as well as implement defenses such as parental control apps, to prevent young users from getting harmed. Raised awareness surrounding the importance of fully protecting, and how to enable this protection, for all devices should also be prioritized.

Tools such as DNS, VPN, EDR for the home, and more must be utilized by individuals, not just large corporations.

**Let's dig into some of these much-needed tools below.**

## Endpoint Protection with Next-Gen Antivirus (NGAV)

Home users' best chances of fighting off modern cyber threats lies with the use of endpoint protection, otherwise referred to as endpoint security. Simply put, an endpoint is a device that shares information and communicates with other devices and end users over a network i.e. desktops, laptops, and mobile devices.

Endpoints are often used as entry points by hackers, targeted merely because they are perceived as vulnerable. Endpoint protection systems are needed to protect the endpoints themselves from cybersecurity threats that can then infiltrate further across networks. This is especially relevant for employees who work from home. If a malicious actor can gain entry into your home network, he can potentially then gain access to your corporate network.

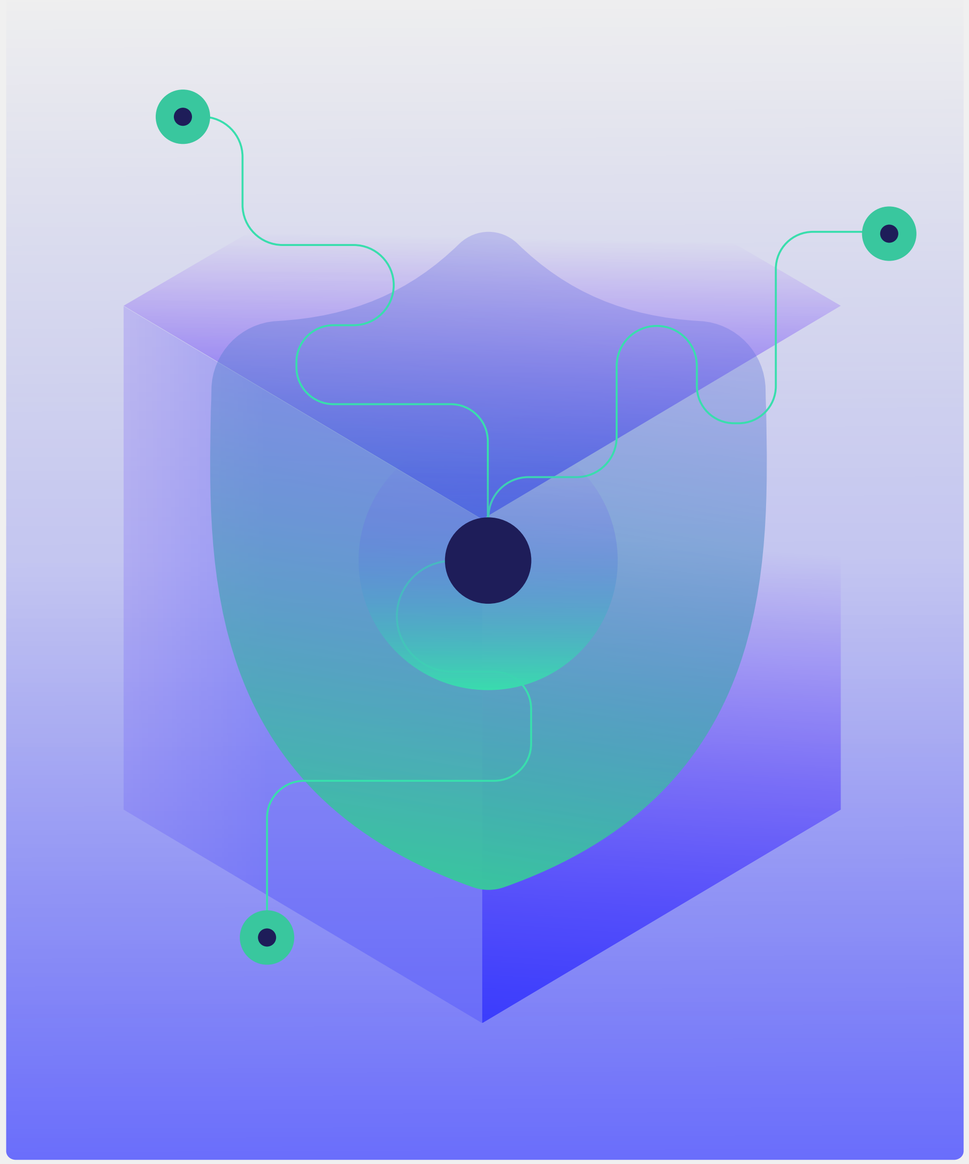
Typically thought of as an enterprise-only resource, ReasonLabs is bringing endpoint protection into the homes of millions across the globe. ReasonLabs is the first endpoint protection provider with a multilayered machine-learning engine designed specifically for home users. Its full suite of security products, beginning with **RAV Endpoint Protection**, complement each other to provide the widest array of protection possible.

## Virtual Private Network (VPN)

Whether you're browsing the internet at home or using a public Wi-Fi network, your activity is visible to the Internet service provider (ISP), search engines, government agencies, social media sites, and other websites you may visit. Even when using private mode on browsers, your device's IP address will still remain visible, which in turn provides your approximate geolocation. The only way to truly protect your anonymity online and increase your privacy is with the use of a Virtual Private Network (VPN).

A VPN will conceal your online identity, using encryption technology to secure your device's connection. Even though your ISP will know you're using a VPN, it cannot see or track your activity while you are using it. Another advantage of a VPN includes the ability to bypass geo-blocks and access content or software from other parts of the world.

**ReasonLabs's RAV VPN** provides a secure, effortless, and confidential browsing experience that meets enterprise-level operating standards. RAV VPN is simple to install and easy to use, enabling a user's device to connect quickly to the Internet. All transferred data is 100% encrypted using the latest security protocols and ReasonLabs maintains an ironclad no-logs policy - meaning no activity is ever shared with anyone.



## Domain Name System (DNS) Filtering

The Domain Name System (DNS) is the naming system used to classify services, computers, and other assets reachable through Internet Protocol (IP) networks. The DNS translates a website's domain name into an IP address that computers can then use to load a webpage. It effectively serves as the phonebook to the Internet.

Home users can utilize a DNS filter, such as ReasonLabs' **Safer Web**, to ensure a safe browsing experience and block all unwanted ads. A good DNS filter can also be used to limit the access of explicit content on a wide variety of commonly used websites and apps. From a security view, a DNS filter can block suspicious URLs, and prevent hackers or malicious software from monitoring activity, recording actions, or attacking any personal assets online.

## Parental Control Software

Parental control software is a great tool that parents can leverage to protect their children, as well as various endpoints used throughout their homes. Even though our kids are being brought up in a digital-first environment, many are overly confident in their skills. According to a **recent study**, people under the age of 20 lost over $100 million to online scams in 2021.

While parental control software is important to use on desktop computers and laptops, it's equally as important to use on mobile devices. Apps such as ReasonLabs' **FamilyKeeper** parental control app serve as a tool to help parents raise their children in the digital world. The dual app provides state-of-the-art security and protection powered by artificial intelligence. It also delivers much-needed insights into the trials and tribulations of digital parenting.

# 09 2023 Predictions

2023 is only just beginning, but **the trends and recurring threats we have witnessed over 2022 show no signs of slowing down.** Here are five predictions for what we can expect throughout the cybersecurity industry in 2023:

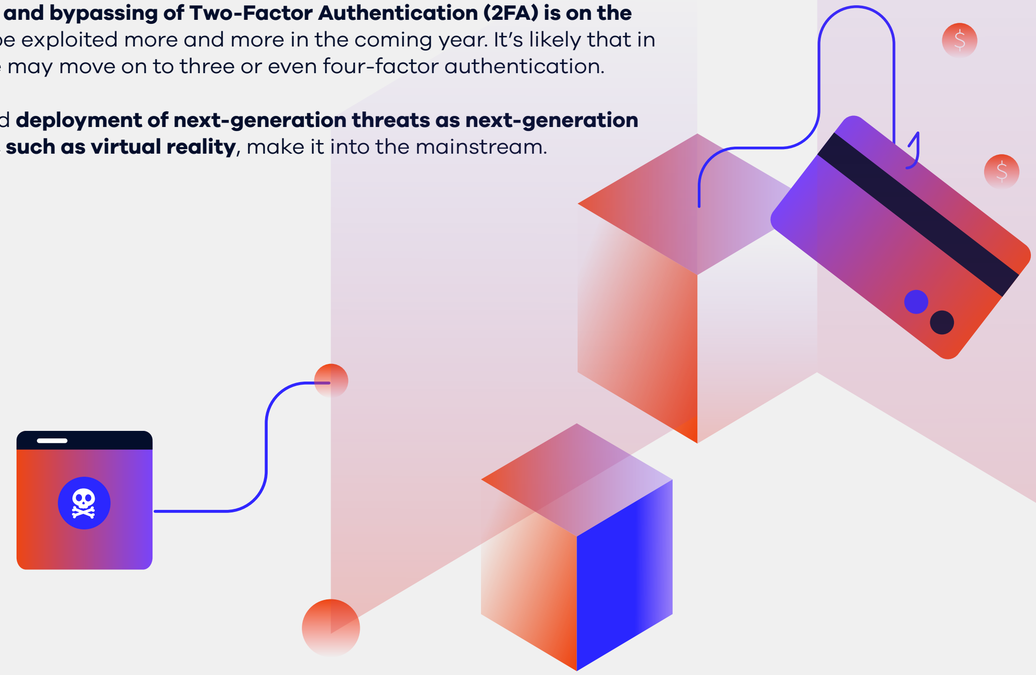
1. **Phishing and social engineering becoming more and more sophisticated** as home users become more aware of common tactics. Home users remain the easiest targets as AV providers are focused on securing enterprise dollars for their services.

2. **We will see more Phishing-as-a-Service (PaaS) and overall Cybercrime-as-a-Service (CaaS),** which refers to the practice in the cybercriminal ecosystem to provide products and services to other cybercriminals.

3. The continued **targeting of unsecured consumers such as tweens and teens, who are highly connected and starting to use crypto,** buying into the Metaverse and other digital assets.

4. The **cracking and bypassing of Two-Factor Authentication (2FA) is on the rise** and will be exploited more and more in the coming year. It's likely that in the future, we may move on to three or even four-factor authentication.

5. The continued **deployment of next-generation threats as next-generation technologies, such as virtual reality**, make it into the mainstream.



# 10 Conclusion

Cybersecurity protection will only grow more important as time goes on. We have seen some trends that have continued on the same path, as well as new technologies creating further opportunities for criminal activity.

To that end, **home users and remote employees are at greater cyber risk than ever before.** The use of connected devices is only growing, no matter what the reason. **Much time and money are now being spent by large corporations to protect their network security. The same level of cybersecurity must be afforded to individual home users as well.** Home users must be made aware of next-generation threats and be educated on the best cybersecurity practices.

**ReasonLabs' mission is to bring the need for education into the spotlight and ensure that every home user around the world is protected against all cyber threats.** We hope this report will bring awareness to the current threats, vulnerabilities, signs of attack attempts, and needs of other antivirus providers, as well as to consumers in general.

## Contributors



**Dana Yosifovich**
Security Researcher, ReasonLabs


**Daniel Moshe**
Security Researcher, ReasonLabs


**Andrew Newman**
Founder and CTO, ReasonLabs


**Yaniv Dudu**
VP Security, ReasonLabs


**Eric Wolkstein**
Marketing Communications Manager, ReasonLabs


**Abi Djanogly**
Content Manager, ReasonLabs


## Contact us


**www.reasonlabs.com**
**support@reasonlabs.com**
**press@reasonlabs.com**


**ReasonLabs is a cybersecurity pioneer equipping tens of millions of families and individuals worldwide with the same level of cyber protection enjoyed by Fortune 500 companies.**

**Its AI-powered, next-generation antivirus engine scans billions of files around the world to predict and prevent cyberattacks in real-time, 24/7. Its full product suite—including its flagship endpoint security solution, RAV Endpoint Protection—forms a multilayered line of defense that safeguards home users against next-generation threats. Co-founded in 2016 by seasoned cybersecurity expert Andrew Newman—an architect of Microsoft's native cybersecurity program, Microsoft Defender—ReasonLabs is based in New York and Tel Aviv. For more information visit reasonlabs.com.**