

# The State of **Consumer Cybersecurity** 2022

By  Reason Labs

February 2022



# Table of Contents

## **01. Executive Summary**

Methodology

## **02. Key Takeaways**

## **03. Top Detections Affecting Consumers**

Viruses

Adware

Search and New Tab Takeover

Trojans

Behavioral Detections

Living off The Land (LOL)

Macros

## **04. Phishing**

Email Threats

COVID-19

## **05. Top 10 Most Attacked Countries**

Highlighting Russia & The United States

## **06. Common Malware**

Ramnit

Infostealing

## **07. Consumer Ransomware**

## **08. Top Malware Distribution Methods**

Cracked Software

Gaming Malware

Pirated Movie Downloads

## **09. Malvertising & Redirection Campaigns**

## **10. 2022 Predictions**

## **11. Conclusion**

Contributors



## 01

# Executive Summary

**There are more connected devices now than ever before, and people all over the world are spending tremendous amounts of time online** - whether it's for school, work, play, or to remain connected with friends and family. The COVID-19 crisis pushed forward years of digital adoption in a matter of just a few months.

As attack surfaces have expanded, enterprises have begun to shift their cybersecurity practices from reactive to proactive. This transformation has made it harder for bad actors to carry out successful attacks against large institutions. However, it has forced them to turn their attention to the 'low hanging fruit' - average consumers.

The following report will identify and analyze the **biggest threats that consumers faced in 2021**, as detected by ReasonLabs' industry-leading research arm, the Threat Intelligence Center (TIC).

TIC researchers will detail the most common threats found, where they have succeeded the most, and what their damage potential was or could be. Based on this information and the trends witnessed, TIC researchers will offer predictions to the challenges we will face in the coming years, and how we plan to overcome them.

## Methodology



**The State of Consumer Cybersecurity 2022 report features data sets collected from intelligence gathered by ReasonLabs' security researchers at its Threat Intelligence Center.** The data presented ranges from January 1 2021 through to December 31, 2021.

All detection data is derived from **ReasonLabs 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 2021 was the year of the miner.** The number of crypto miners distributed throughout 2021 was enormous and was found virtually everywhere on the consumer's endpoints. While there are users that choose to willingly download legitimate mining programs to their computers, we've determined that these users make up only 1% of legitimate mining activity. The other 99% of mining activity is done maliciously on hosts where users downloaded bundled programs with cryptojackers.
- 2 Phishing via documents and email was still a highly popular way of distributing malware in 2021.** Other vectors of note used by malware to reach hosts include communication websites such as Discord, Telegram, Twitch, and others. For example, we noticed a trend in Discord where users would send each other "joke viruses" - small scripts that would trigger pop-up messages or change the color of the terminal. In these cases, there's a high probability of downloading and running a real virus.
- 3 The top 5 countries in order of average detection per user** were:
  1. Russia
  2. Indonesia
  3. Egypt
  4. China
  5. Poland
- 4 We saw a decrease in the number of threats leveraging 'COVID-19' as 2021 progressed,** no matter the type of attack vector. However, threats related to COVID-19 that came from phishing documents still found their way to users, most of them occurring in Microsoft Office documents with macros. COVID-19 has, of course, not yet left us and may continue to affect us for years to come. As such, we expect specific phishing attacks leveraging COVID-19 will persist.

**6** **Infostealers played a major role in the 2021 threat landscape.** Traditional infostealers used to harvest banking credentials, but now we see a huge shift to harvesting crypto credentials and even stealing crypto funds directly. Even 2FA/MFA is not enough for some advanced infostealers.

**6** **Living Off the Land (LOL) has been a growing category for a couple of years** now and in the past year specifically, we've witnessed a clear rise in the number of detections related to LOLBins.

**7** **For 2022, we expect a general shift in hackers' focus away from enterprises, and back to consumers.** Compared to enterprises, consumers are less secure, have fewer resources, and are sometimes neglected by major AV providers. Most pertinently, we predict the targeting of the most unsecured consumers, such as tweens/teens who are highly connected and starting to use crypto and other digital assets, to come into the mainstream.



## 03

# Top Detections Affecting Consumers

**Consumers all over the world are facing a seemingly endless list of attacks through many vectors.** Our investigations have found that Trojan viruses are at the top of the list. A Trojan virus is a malware that comes in the shape of a legitimate-looking program - but instead of (or in addition to) installing the legitimate program, the user will execute a malicious program.

The malware can be of many types, such as ransomware, cryptominers, RATs, etc. **Many of the Trojans arrive through phishing emails, cracked software and games, and questionable websites.** Recently, ransomware has played a starring role as the most talked-about global threat, and for good reason.

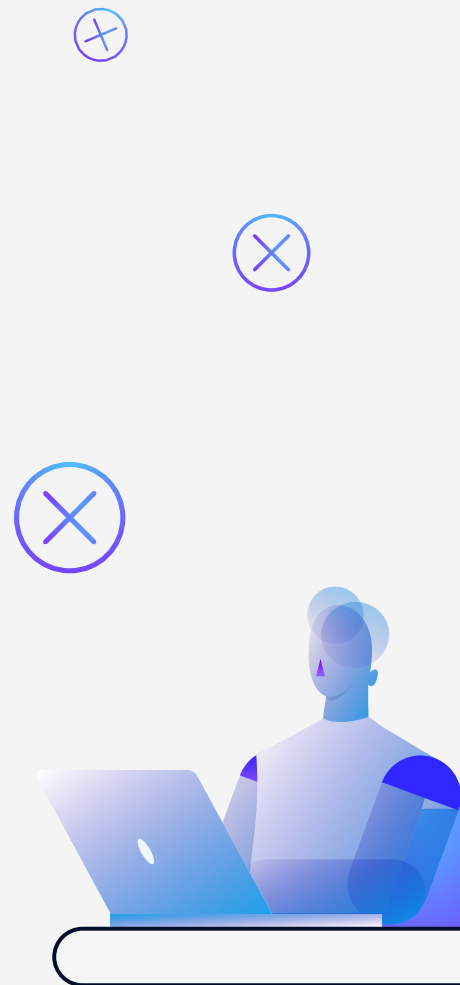
That said, throughout 2021, we observed a sharp rise in cryptojacking and infostealing, catapulting them near the top of the charts. The reason for this may come from the fact that it's relatively tricky to convince the common user to carry out complicated actions such as opening a crypto wallet and buying bitcoin. It's far easier to simply begin mining and reaping the profits from the unsuspecting user.

There are two main cases where a user is infected with a virus:

- 1. When it reaches the user via social engineering techniques, such as phishing.**
- 2. When a user brings the virus upon himself, for example, by downloading the wrong movie torrent or a software crack.**

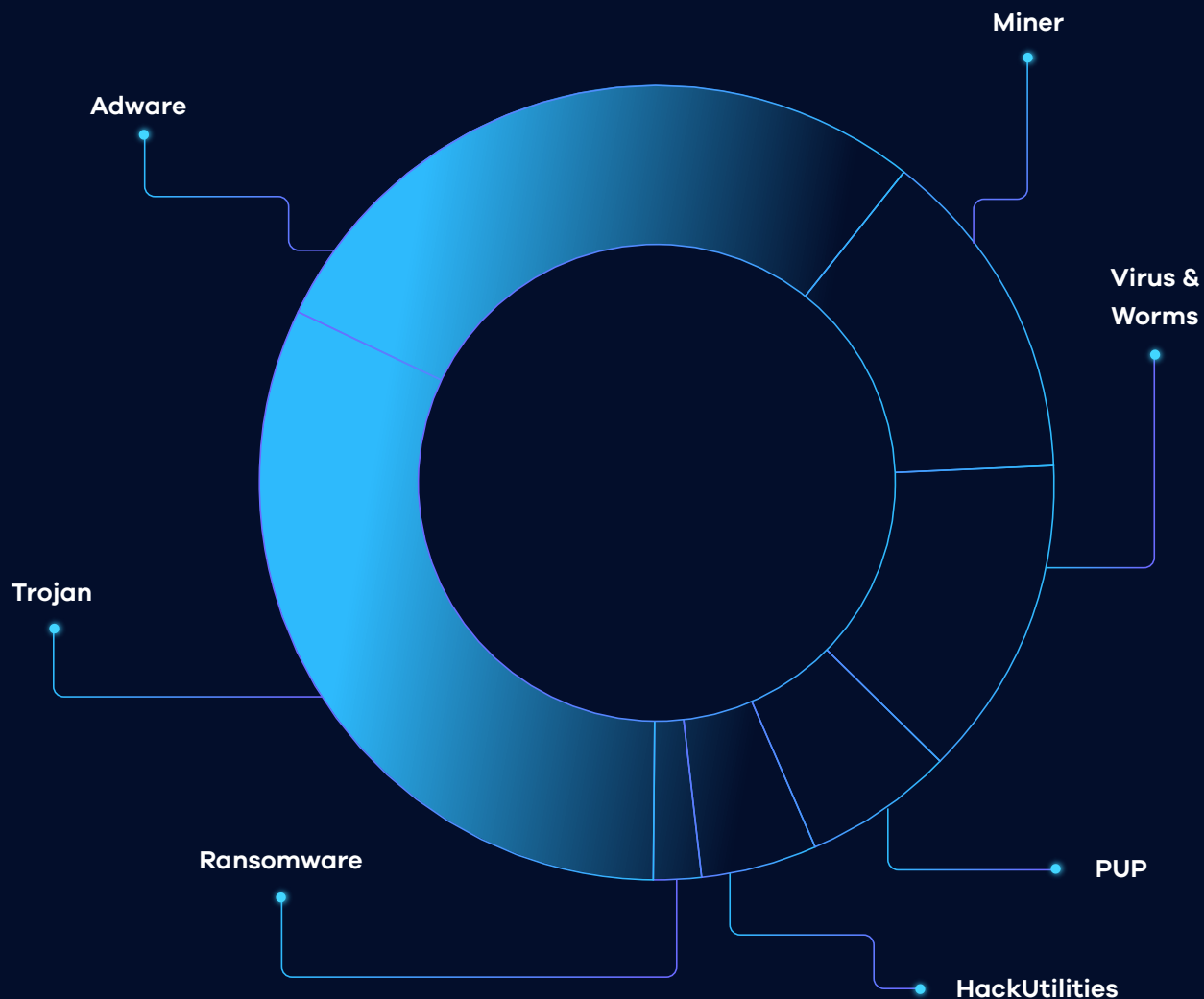
Regarding the first case, phishing via documents/email is still highly popular, as we witnessed far too many detections on malicious documents. Other vectors for malware to reach hosts are from communication websites such as Discord, Telegram, Twitch, and more. We noticed a trend in Discord where users send each other "joke viruses" - small scripts that pop messages or change the color of the terminal. In these instances, there's a higher probability of downloading and running a real virus.

The latter case is also a huge problem as in recent years, more and more aspects of our lives have become digitized, especially since the start of the COVID-19 pandemic, when we found ourselves spending much more time at home.



## Top Detections By General Categories

Threats	Detections
<b>Trojan</b> (malicious docs, backdoor, RATs, infostealers, etc.)	<b>31.95%</b>
<b>Adware</b>	<b>28.60%</b>
<b>Miner</b>	<b>13.63%</b>
<b>Virus &amp; Worms</b>	<b>13.14%</b>
<b>PUP</b> (Potentially Unwanted Program)	<b>6.18%</b>
<b>HackUtilities</b> (cheats, trainers, license software hacks, hacking tools, etc.)	<b>4.76%</b>
<b>Ransomware</b>	<b>1.73%</b>



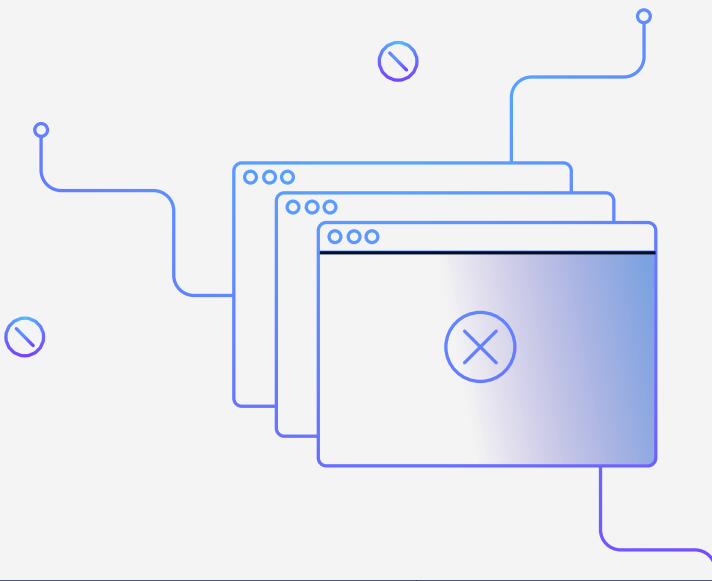
## A More Specific Breakdown

Threats	Detections
Trojans	21.40%
Droppers	20.50%
Adware browser modifiers	17.80%
HackUtilities	13.60%
Coin miners	9.90%
Malicious scripts	7.90%
Malicious macros	7.80%
File infector viruses	5.90%
Legacy viruses	4.60%
PUP	4.30%
Adware	2.10%
Qot Trojan	1.50%
Ransomware	1.20%
Infostealer	0.10%



## Viruses

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, that when run carries 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.



## Virus Breakdown

Ramnit	34.00%
Floxif	19.00%
Neshta	11.00%
Sality	9.00%
Chir	8.00%
Ground	8.00%
Wapomi	6.00%
Jeefo	4.00%
Expiro	2.00%

## Adware Breakdown

Adware Browser Modifiers	65.46%
Bundlers	16.24%
Ad popup scripts	14.85%
Stagers	2.44%
Installers	0.99%

## Adware

The **adware family consists of malware that is generally designed to inject some form of advertising into an unsuspected victim's computer**, programs, or browser. Adware can fall into two distinct categories: advertising-supported software, which is typically non-malicious and designed to show ads, and more nefarious adware that injects unwanted ads, hijacks computer settings such as search behavior, and shows **potentially dangerous ads which can spread to other forms of malware.** Unlike most malware, adware is typically bundled in free software (freeware and shareware) or browser extensions.

## Search & New Tab Takeovers

One of the most prevalent detections is the “Adware Browser Modifiers” category. **Browser modifiers are adware that hijacks the browser’s search settings, new tabs and also, in many cases, can modify the expected behavior of your browsing activity by injecting advertisements.**

This activity is not malicious at its core but can be bothersome at best or prone to abuse at worst. The activity is considered potentially unwanted, due to the fact that the user usually won’t want to change his search provider or ‘new tab’ page intentionally. A ‘new tab’ page takeover involves replacing the page

that opens when one clicks on ‘new tab’ in the browser, or when first launching the browser.

For example, the default page on Chrome is the regular Google Search page. There are extensions in the Chrome Web Store that offer various backgrounds or themes. These extensions replace the default page with a more colorful background and even features.

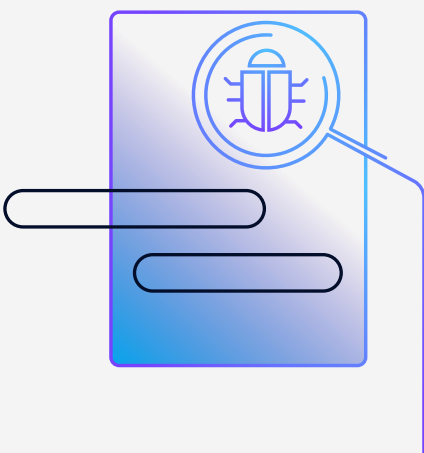
The disadvantage of these extensions is that **they may contain malicious code that can gain access to browser assets.** This includes changing the search provider, access

to browsing history, access to surfing activity, ability to change page contents, redirection to malicious sites, mining crypto coins without user consent, and more.

Chrome has made great efforts to keep malicious extensions out of the Chrome Web Store, so the number of malicious extensions has dropped significantly in recent years. However, holes in security will always be possible to find.

## Trojans

The Trojan family of malware 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.



## Trojan Breakdown

Coin miners	58.40%
Backdoors	21.80%
Infostealers	8.80%
RATs	6.20%
Spyware	1.70%
Ad Hijackers	1.50%
Droppers	1.00%
Financial (Banking / Crypto)	0.50%

## Behavioral Detections

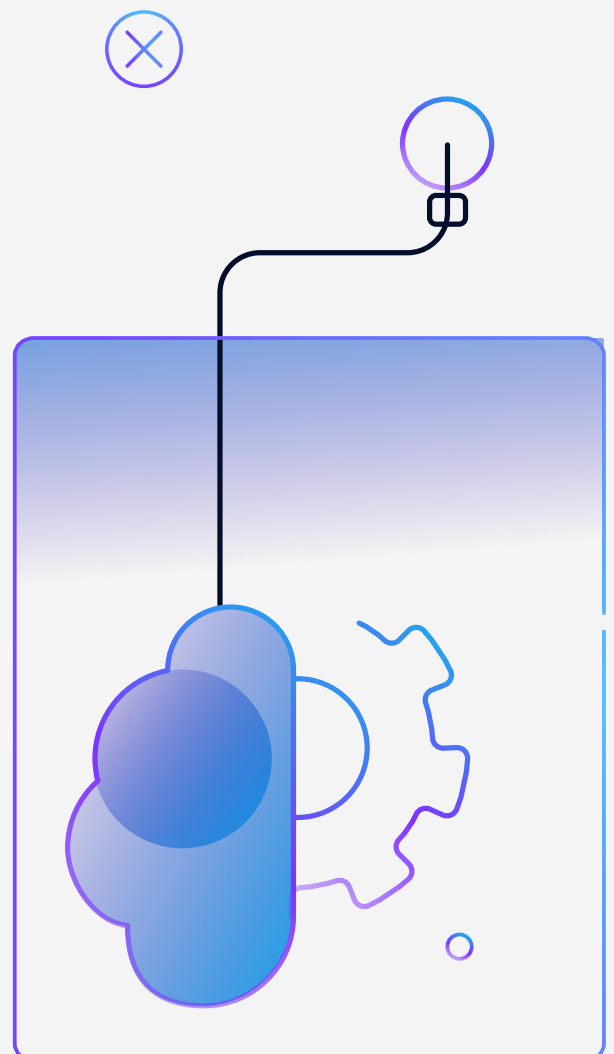
**Behavior-centric detection is a core element of ReasonLabs' multi-layered approach to protection** and has proven to be one of the most efficient ways to protect against advanced malware threats - including zero-day and fileless malware attacks.

By creating tens of thousands of known and assumed playbooks, the very behavior of an attack can be quickly detected and stopped. **Behavior detections are based on heuristic and machine learning models** to find known patterns and anomalies of suspicious actions. With the increase of new and novel attack vectors being seen daily, behavior detections are essentially the next generation of protection.

Types of behavior detections include, but are not limited to: weaponized scripts, office documents, Authenticode hijacking, PE hijacking, sideloading, process injection, ghosting, and a wide range of file attacks that use local operating system files that have been exploited by an attacker - these are known as Living off the Land (LOL or LOLBins, Living off the Land binaries).

### Behavioral Detections Breakdown

Office Documents weaponization	30.00%
Living off the Land (LOL)	20.00%
Scripts (VBS, bat, js, etc.)	13.00%
PowerShell	12.00%
Obfuscation	15.00%
Authenticode hijacking	3.00%
Other	7.00%



## Living off the Land (LOL)

Living off the Land (LOL) has been a growing category for a couple of years now. 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.


**LOLs 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.

## Macros

**Macros are scripts written in Visual Basics that are embedded into office documents.** Using macros, users can enrich their documents with 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.**

During the past year, 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 also witnessed a number of other techniques, which, while effectively having the same behavior as macros, use different technology to weaponize Office documents and include embedded, linked, and remote OLE objects, Excel 4.0 macros and remote templates.

Location	Totals
Indonesia (ID)	22.80%
Brazil (BR)	16.10%
India (IN)	15.90%
Poland (PL)	12.00%
Vietnam (VN)	6.40%
Thailand (TH)	6.00%
China (CN)	5.90%
Turkey (TR)	5.50%
Colombia (CO)	4.90%
France (FR)	4.70%

The distribution of macros across the globe looks like this: 

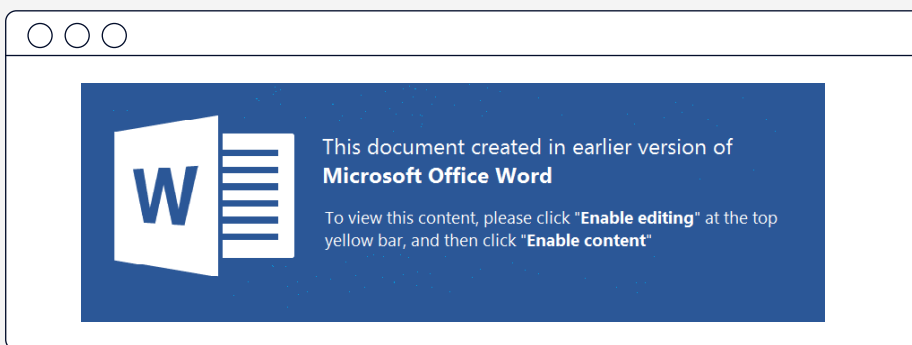
## 04

# Phishing

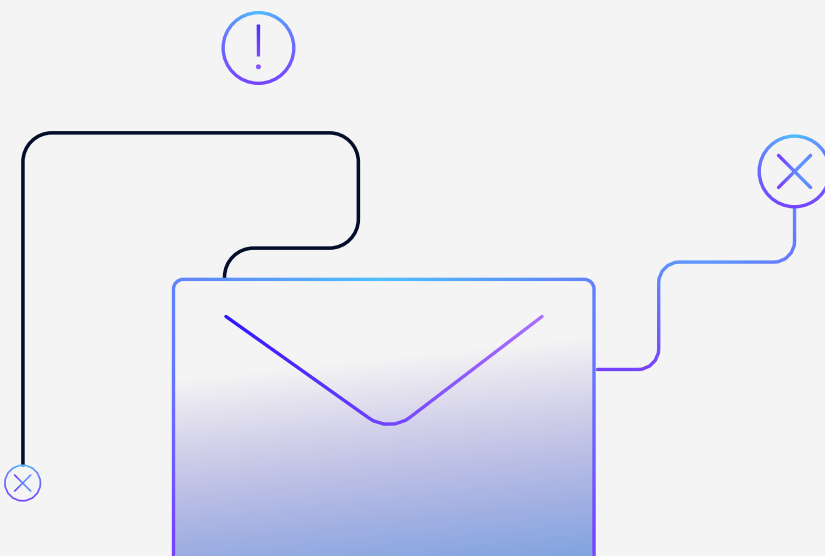
Phishing also played a key role in 2021 and was most certainly a **top threat that affected consumers**. In fact, phishing attacks were so prevalent last year that they deserve a full deep-dive.

As we saw in the previous graph, the amount of documents that contain malicious macros is very high. This means that many users are getting threats from external sources that try to convince them to “enable editing”, which will eventually cause the execution of macros.

The below photo is a phishing example taken from a malicious document found by ReasonLabs.



Besides phishing documents, there are also a lot of malicious script files (.exe or zips) that are downloaded from emails. Grammatical errors in these messages offer hints that these may be phishing attempts but of course, for a non-English speaker, these clues won't help.



## Phishing Email Downloads

.EXE	32.79%
JS	26.28%
MHT	21.99%
VBS	4.92%
DLL	4.17%
BAT	2.54%
CS	1.06%
DOCX	1.01%
XLS	0.72%
REG	0.71%
PS1	0.85%
MSI	0.57%
XLSX	0.55%
DOC	0.50%
JPG	0.45%
PDF	0.31%
ZIP	0.30%
XLSM	0.28%

## 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.** We saw lots of malicious email attachments sent to users all over the world, including one sent to a ReasonLabs user in France with the name of "votre releve fiscal ameli.vbs", which translates to English as "your tax return." The attachment is not a tax return, but an obfuscated vbs script that will execute PowerShell commands and take over the host. This is just one of many examples of phishing emails that we blocked.

## COVID-19 Threats

We saw a decrease in the number of files and documents containing phrases related to COVID-19 as 2021 progressed. 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. 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.

### COVID-19 Phishing Threats By Country

Location	Totals	Location	Totals
Poland (PL)	<b>20.6%</b>	Brazil (BR)	<b>6.1%</b>
Indonesia (ID)	<b>15.8%</b>	Egypt (EG)	<b>5.7%</b>
United States (US)	<b>9.9%</b>	India (IN)	<b>4.5%</b>
Colombia (CO)	<b>9.0%</b>	Turkey (TR)	<b>4.1%</b>
Thailand (TH)	<b>7.0%</b>	Russia (RU)	<b>4.0%</b>

## 05

# Top 10 Most Attacked Countries

In this section, we will compare **detection rates and detection types across different countries.**

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.

## Average Detections Per User



Russia (RU)	6
Indonesia (ID)	3
Egypt (EG)	3
China (CN)	1
Poland (PL)	1
Thailand (TH)	1
United States (US)	1
Turkey (TR)	1
India (IN)	1
Brazil (BR)	1

Let's dig deeper into Russia's numbers as an example:

Threats	Detections
Trojans	<b>21.50%</b>
Adware browser modifiers	<b>19.80%</b>
Virus & Worms	<b>14.00%</b>
Miners	<b>12.80%</b>
PUP	<b>11.60%</b>
Macros	<b>11.50%</b>
Adware	<b>6.10%</b>
HackUtility	<b>1.60%</b>
Ransomware	<b>0.50%</b>





Now let's reveal the data on the United States:

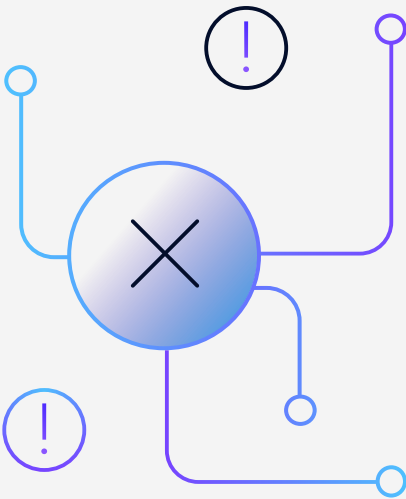
Threats	Detections
<b>PUP</b>	<b>33.40%</b>
<b>Trojan</b>	<b>17.90%</b>
<b>Adware</b>	<b>15.40%</b>
<b>Miner</b>	<b>12.8%</b>
<b>Adware browser modifiers</b>	<b>7.90%</b>
<b>Virus &amp; Worms</b>	<b>12.80%</b>
<b>Malicious scripts</b>	<b>3.90%</b>
<b>Macro</b>	<b>2.00%</b>
<b>HackUtility</b>	<b>1.90%</b>
<b>Ransomware</b>	<b>1.00%</b>

Coin miners are mostly distributed all over the world, but if we examine the different types of threats, we can see that Russia has suffered many more Macro and Trojan threats, as opposed to PUP incidents in the US. The differences noted between these countries, or regions, can be explained by raised awareness, economics, and needs.

## 06

# Common Malware

## Ramnit



**Ramnit virus has accompanied us since 2010 and is our most commonly found malware family.** In 2015, Europol's European Cybercrime Center (EC3) coordinated a joint international operation to take down the Ramnit botnet. Despite this effort seven years ago, **Ramnit still causes users great pain on their devices today.**

The first variants were viruses that infected .EXE, DLL, and HTML files. **Over the years, Ramnit evolved from being a simple file infector to becoming a botnet, or banking malware.** The file infection is executed by adding extra code to the end of other executables of HTML files. Ramnit variants are usually distributed from other infected Ramnit files, removable devices, or as part of a payload from other malware.

This is a great example of a type of malware that can still effortlessly cause damage, despite it being 'old'. Due to its spreading capabilities, older devices that were infected with it in the past can still spread the malware to new, clean devices. Throughout 2021, we encountered a number of new alerts, most of them in removable devices or drives.

## Infostealing



Another rising threat that we saw this past year was infostealing. Two examples of common infostealers are RedLine and Racoon. The RedLine infostealer surged at the beginning of COVID-19, where it spread itself by using COVID-19 terms. Racoon has accompanied us since at least 2020 and is still very much alive.

**Both of these infostealers steal login information, credentials, FTP & VPN configurations, credit card info, crypto wallets, gaming data, and instant messaging data,** and are a threat to the user's privacy and sensitive data.

## 07

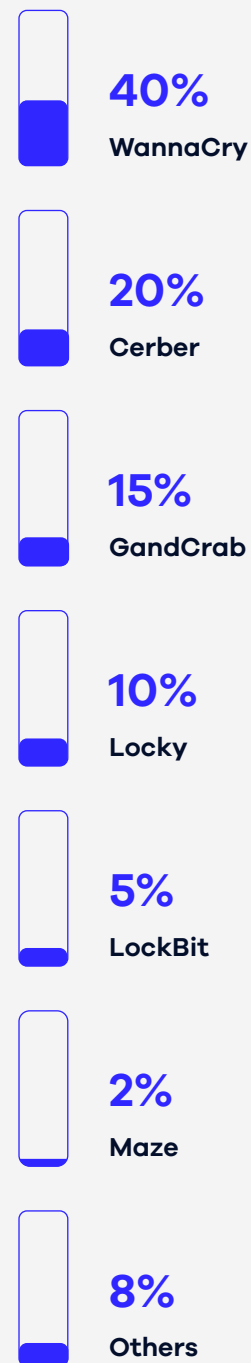
# Consumer Ransomware

2021 was one of the first years in the past decade that actually saw a reduction in overall ransomware infections that targeted the consumer market. This was most likely due to the fact that ransomware gangs put a lot of their effort into targeting enterprises, where ransoms were valued at upwards of 1000 times that of consumers. Where the average consumer would possibly spend less than \$1000 to free their computers, enterprises were likely to spend millions of dollars.

In addition, most enterprises end up paying their ransom, whereas consumers are a lot less likely to. However, this is due to change, as the security posture of larger institutions and their spending on cyber protection has increased significantly these past few years. We expect to see a shift yet again to consumers as targets.

In 2021, the most common ransomware threats still targeting consumers included some familiar faces, with a couple of new ones. Legacy ransomware that still plagues users includes WannaCry, Cerber, GandCrab, LockBit, Maze, and Locky. WannaCry remains the top threat, with Cerber and GandCrab rapidly closing in, by taking advantage of Ransomware as a Service (R-A-S) for quicker and well-organized distribution.

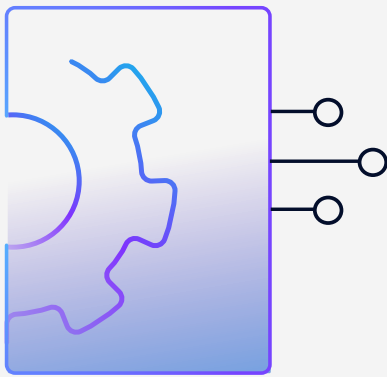
Consumer Ransomware Breakdown →



## 08

# Top Malware Distribution Methods

## Cracked Software



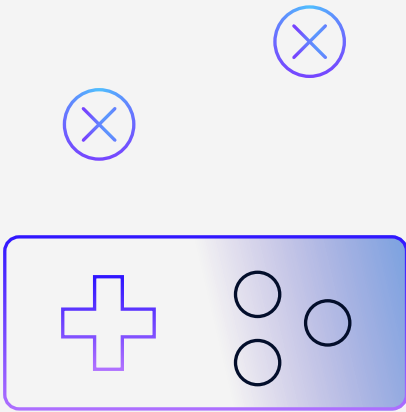
Pirated software may appeal to consumers as they feel they are saving money - yet the common user doesn't know if the source of the download is "legitimate" or credible, making them take a risk for each pirated program they install. Even the most technical user could get lost when trying to figure out how many AVs mark the pirated program, as many of the detections in these cases are "HackUtility," which does not help to understand the type of risk.

A great deal of pirated software includes Trojans delivering malware to a user's system. In some cases, the actual cracked program will be installed, so the user won't suspect that something untoward is happening. In some cases, users will never receive the expected software, only the malware.

For example, the below chart shows Trojanized Adobe Photoshop installations that were detected as miners:

Location	Detection	Location	Detection
Lebanon (LB)	41.90%	Turkey (TR)	2.30%
Brazil (BR)	33.80%	Pakistan (PK)	1.80%
India (IN)	8.10%	South Korea (KR)	1.40%
United States (US)	4.50%	Indonesia (ID)	1.40%
South Africa (ZA)	3.60%	Portugal (PT)	1.40%

## Gaming Malware



Users must be careful when downloading foreign software or following instructions from messages sent to them while playing, either from within forums or through apps like Twitch or Discord. To avoid detection, these actors send messages with terms to search in Google and proceed to download malware from the search results.

There are those who don't want to pay and those who can't pay. Whether it's children or teenagers that cannot afford the cost of a game or simply someone who wants to 'beat the system' and get it for free - either way, **the market is flooded with cracked games, allowing users to acquire virtually any game available.**

Along with the actual game, some users also receive malware with, or completely instead of, their desired game. Throughout 2021, we have seen countless threats that came specifically from supposed games, including **miners, RATs, and infostealers, all delivered in a bundle with the game.** The fact that the game is cracked makes it impossible to appear on legitimate trusted sites, which implies that users must seek them out in risky places. **Doing so means putting their trust in the hands of unknown actors.**

Another issue is game cheating - gaming companies try their best to make it impossible to cheat, so users will not be able to spam, DDOS, or get expensive items with little effort, or indeed for free. **Some bad actors find ways to distribute bots, apply cheats, or steal items from other users to later sell them and earn real money.**

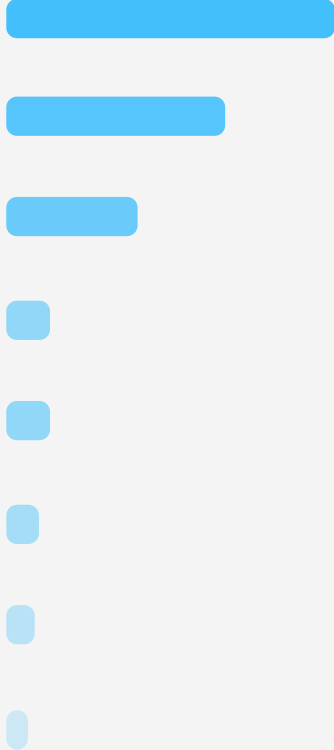
For example, the below chart shows Trojanized *Fifa* installations that were detected as miners:

Location	Detection	Location	Detection
<b>Poland (PL)</b>	<b>21.60%</b>	<b>Brazil (BR)</b>	<b>7.80%</b>
<b>South Africa (ZA)</b>	<b>19.60%</b>	<b>Georgia (GE)</b>	<b>5.90%</b>
<b>Egypt (EG)</b>	<b>11.80%</b>	<b>Serbia (RS)</b>	<b>5.90%</b>
<b>Morocco (MA)</b>	<b>9.80%</b>	<b>Australia (AU)</b>	<b>4.10%</b>
<b>India (IN)</b>	<b>9.80%</b>	<b>Czech Republic (CZ)</b>	<b>4.10%</b>

## Pirated Movie Downloads

Downloading or distributing pirated movies online is nothing new. It's an act that has plagued the global film industry for years and unfortunately, it seems like there is no end in sight. Just like with cracked software or gaming malware, sometimes users who download pirated movies receive the movie itself. However, often users are receiving malware. [Below is the breakdown of threat categories of pirated movie downloads from last year.](#)

Threats	Detections
<b>PUP</b>	<b>38.70%</b>
<b>Virus &amp; Worms</b>	<b>25.80%</b>
<b>Adware</b>	<b>15.50%</b>
<b>Miner</b>	<b>5.20%</b>
<b>Trojan dropper</b>	<b>5.20%</b>
<b>Infostealer</b>	<b>3.90%</b>
<b>Ransomware</b>	<b>3.40%</b>
<b>RAT</b>	<b>2.60%</b>



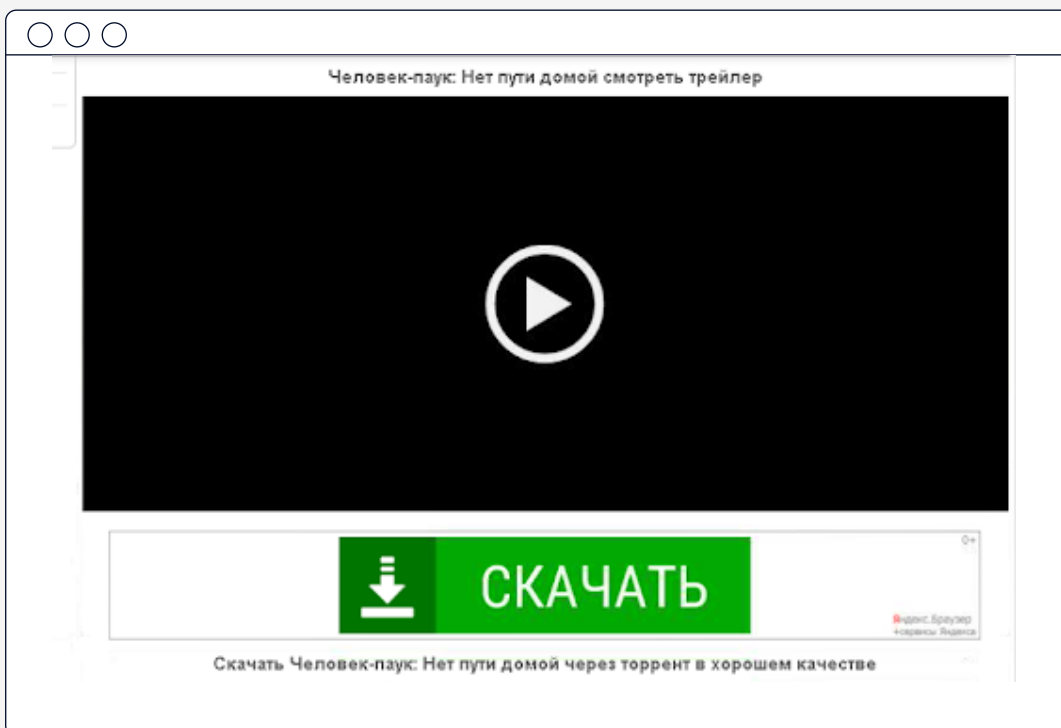
## 09

# Malvertising & Redirect Campaigns

Malvertising and redirect campaigns have played an important role in the global consumer threat category throughout 2021. **We define malvertising as ‘malicious software advertising,’ which is mainly used to spread malware through ads online.**

Usually, these malware-ridden advertisements are placed onto **real networks or real products**, tricking users into thinking that it’s a real ad. Some of the world’s most prominent news sites such as *The New York Times*, *The Atlantic*, and *The London Stock Exchange* have fallen prey to malvertising in the past.

Below is an example that was taken from a malicious website found by ReasonLabs. The green “ad” is actually malware overlaid onto a real advertisement.



# 2022 Predictions

2022 has only just begun but we have already witnessed recurring and novel threats affecting consumers worldwide.

Here are three predictions for what we can expect throughout the industry in 2022 →

# 1

A general shift from enterprises back to consumers - consumers are less secure, enterprises are making significant investments in security, and AVs are chasing the enterprise dollars.  
**Consumers are now the easiest target.**

# 2

**More 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.

# 3

As apps are connecting to digital financial assets, **the surface area for attackers is becoming much larger**. Scams and bundled malware in cracks, games, cheats, etc. are increasing significantly, and **young consumers are most at risk**.



Here is a breakdown of the top three threats we expect to be carried out for 2022: —————>

## Infostealers

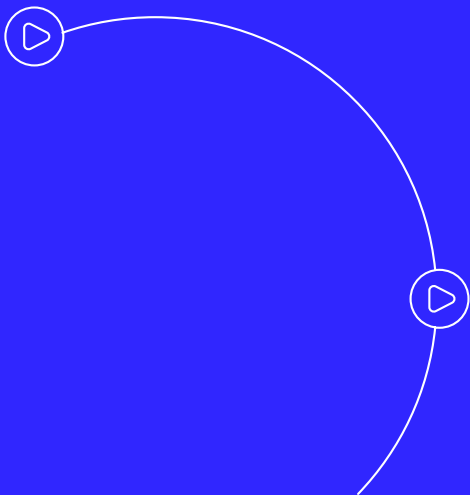
We predict a **massive growth in infostealers specifically targeting crypto**. Since many more apps are connected to crypto wallets, from games to the metaverse, and due to the fact that consumers are unaware of their security posture, attackers are sure to take advantage of this.

## Coin miners & Cryptojackers

2021 was the year of the miner and as such, bad actors will continue to utilize them. Due to their ability to operate silently and go virtually undetected, **cryptojacking will continue to increase significantly in the coming years**, no matter where a user is located.

## Ransomware

Consumer protection has changed little against ransomware, and these attackers aren't dissipating any time soon. They will shift their **focus to unprotected consumers, with the number of attacks drastically increasing** to cover the pay gap.



## 11

# Conclusion

With 2021 being the first full year of our COVID-19 new normal, consumers around the world have only just begun to adjust to being connected virtually 24/7 for a host of different reasons.

With people spending more time online, education around the different types of commonly found cyber threats and overall best cybersecurity practices are paramount. There will always be some basic ways in which consumers can protect themselves, as well as more technical ways to pre-empt threats.

There are certain products available for consumers such as next-generation antivirus (NGAV) solutions like RAV Antivirus, virtual private networks (VPN) such as RAV VPN, and domain name systems (DNS) like Saferweb. They are all highly recommended components in order to fully protect a consumer's endpoints - whether it be a laptop, desktop, tablet, or other handheld devices.

Now, more than ever before, the importance of staying cyber-safe is critical.

**reasonlabs.com**  
**support@reasonlabs.com**

ReasonLabs is a leading cybersecurity company providing enterprise-grade protection for all users around the globe. Led by a team of cyber experts and visionaries, including former Microsoft Lead Security Program Manager, Andrew Newman, ReasonLabs has developed unique, cutting-edge technology to combat all emerging cyber threats at the earliest possible stage. ReasonLabs' innovative engine scans over 2 billion files in 180 countries a day, delivering fast, comprehensive data while providing 24/7 real-time threat detection. Please visit [reasonlabs.com](https://reasonlabs.com) for more information.

Copyright © 2022 Reason Cybersecurity Ltd. All rights reserved.

## Contributors



**Abi Djanogly**

Content Manager, ReasonLabs



**Yaniv Dudu**

VP Security, ReasonLabs



**Andrew Newman**

Founder and CTO, ReasonLabs



**Eric Wolkstein**

Marketing Communications Manager, ReasonLabs



**Dana Yosifovich**

Security Researcher, ReasonLabs

