allot
See. Control. Secure.

2020 Cyber Threat Report

European Edition

allot
See. Control. Secure.

CONTENTS

INTRODUCTION

2020 was a year that will be remembered first and foremost as the year the Covid-19 virus spread across the world. In addition to the grave public health catastrophe, the world suffered several secondary coronavirus crises; economic, social, educational, and cyber.

In 2020 Phishing attacks increased an average of 718% from the prior year

Cyber-Covid was characterized by a sharp increase in all types of online threats, particularly Phishing. Cybercriminals moved quickly to take advantage of customers' panicked state-of-mind to launch even more Phishing attacks. In January 2020, Phishing accounted for roughly 5% of all Allot Secure blocks (blocked cyberthreats) in Europe. By April, at the peak of the first wave of Covid-19, Phishing rose to 56% of all blocks.

In June 2020, Mobile users in Spain were hit by a clever banker Trojan that exploited fears of the coronavirus with a spoofed message claiming to have specific information about infected people nearby. The message looked just like a legitimate Android map app, but when users clicked, they were led to a malicious 'Coronavirus Finder' app containing the GINP Banker Trojan.

As Europe and the world are experiencing the beginning of a third destructive wave of Coronavirus infection, so too the online sphere is expected to be hit with a third wave of all types of cybercrime; some of which will be specifically targeted to play on pandemic fears and excitement about vaccinations.

Allot is dedicated to protecting networks and their users from all types of attacks including malware, ransomware, Phishing, cryptojacking and more. This 2020 Cyber Threat Report shows how European communication service providers that partner with Allot Secure were able to block all types of cyberthreats and keep their subscribers safe all year long.

KEY HIGHLIGHTS

- Allot NetworkSecure blocked 2,230,146,650 cyberthreats from harming European Internet users in 2020.
- The average percentage of customers experiencing protection events during 2020 was 23% of security subscribers across Europe. It started at 16% in January and peaked at 41% in April, during the height of the first Coronavirus wave. Rates then stabilized at a high "new normal" of around 24%, showing the long-term negative impact of the pandemic on cybersecurity.
- In 2020, 99% of NetworkSecure protections were via pre-blocking visits to malicious websites.
- Among the main pre-blocked malicious URLs across Europe, we observed significant difference between the three most blocked threat categories (Phishing, Adware and Malicious Download) and the rest. Phishing started the year around 5% and soared to dominance, now constituting 50% of the blocks. Adware made a slow, steady climb from 20% to 28%. Finally, Malicious downloads started the year at 20% but dropped proportionally to 8% of all pre-blocks by year end.
- In Download Blocks, the top two, Adware and Trojans, together consistently accounted for 90% of total download blocks.
- 2020 started with normal numbers, which rose sharply in parallel to the global Covid-19 crisis. At the end of the year, we see the 'new normal' has risen considerably. Unfortunately, 2021 has started off with a third wave of Coronavirus infection that is expected to lead to yet another rise in cyber threats that NetworkSecure will block.

MAIN TAKE-AWAYS

WHAT ARE THE KEY MESSAGES THAT CAN BE COMMUNICATED TO CUSTOMERS?

Phishing remains the predominant threat to European users

- Triggered 51% of all blocks in 2020.
- Already a favored attack method among cybercriminals, they took advantage of the global health crisis by dramatically increasing phishing activity.
- Phishing victims suffer monetary loss, in addition to having their personal data and account credentials stolen. Since we know most users cannot identify phishing sites on their own, a high-quality anti-phishing solution is the only effective way to avoid phishing.

Adware remained the second most pervasive threat type, comprising approximately 28% of all threats blocked in Europe

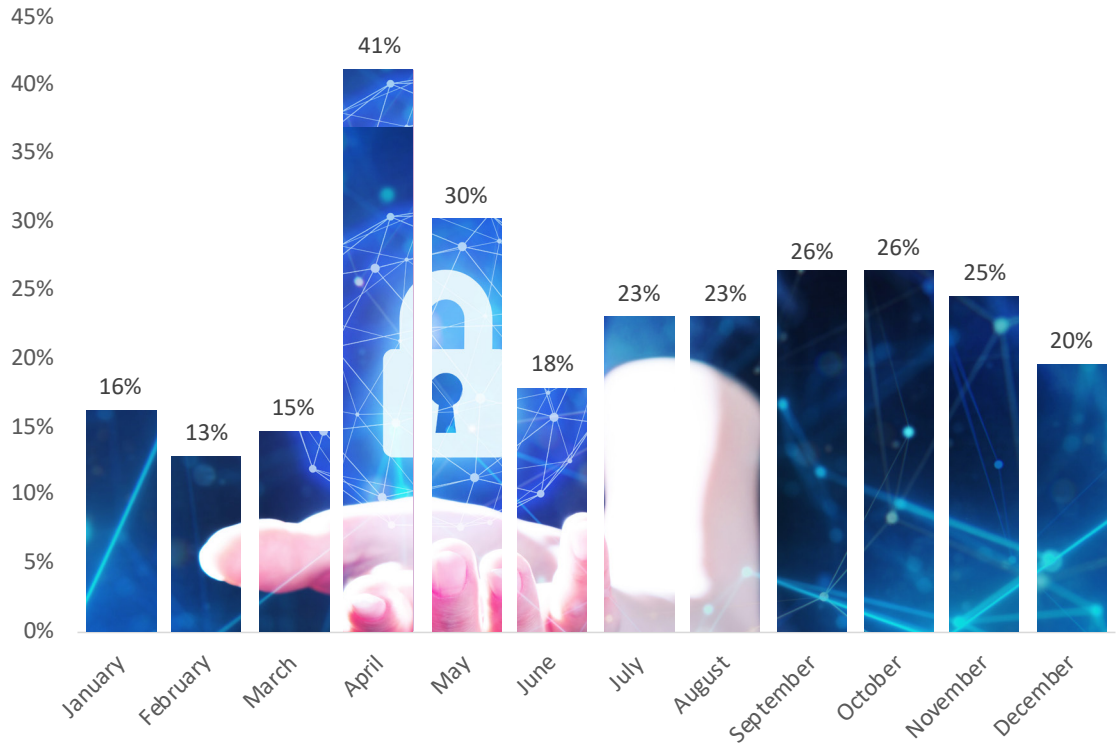
- Adware infection is the cause of bothersome pop-up ads and can also slow browsing speed.
- It can be as dangerous as any other type of malware by redirecting users to infected pages containing malware downloaders or even phishing pages.

The Corona cyber pandemic is not over yet

- Every time a country faced a new wave of Coronavirus, cybercriminals quickly followed with increased and targeted attacks. The world is suffering from Corona fatigue, but as a third wave of infection hits, we cannot let our guard down.
- Vaccination campaigns are beginning throughout Europe. Cybercriminals will use the excitement to manipulate people and try to trick them with promises of important information or access to vaccinations. Users must take care to only read and respond to official sources of health and vaccination information. We discourage opening any unsolicited communication, even if it appears to be from a trusted source. Upon receiving a suspicious communication, people should reach out directly to the organization to verify the communication.

% OF CUSTOMERS PROTECTED

Before digging into which categories were the most blocked during this period it is important to appreciate the percentage of customers who were protected by NetworkSecure blocking events during 2020.



On average, 23% of customers were protected by a blocking event in 2020.

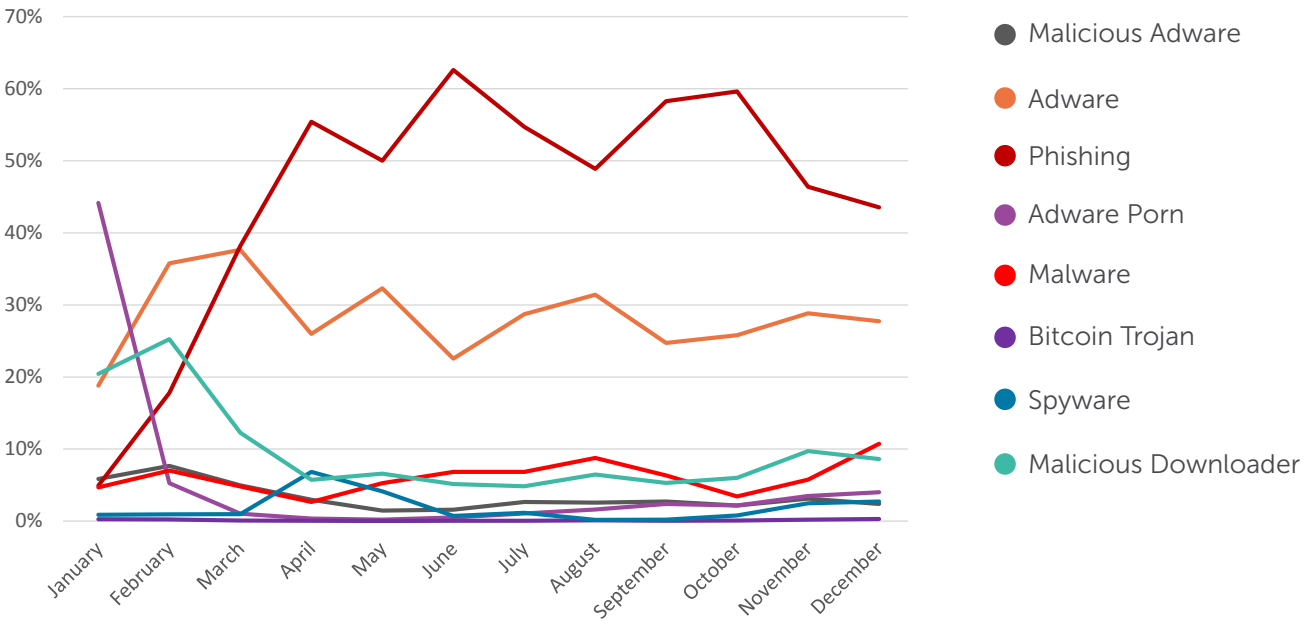
It is important to highlight that this percentage is calculated using the security subscribers and not the entire customer base of the CSPs.

In April 2020 there was a sharp increase in cyber protection events as the Coronavirus crisis hit Europe. This was followed by a correction in the summer months, then another increase as the second coronavirus wave hit in September. The year ended with several months at the newer, higher average of just over 20%.

A surprising effect of the virus-fueled cybercrime cycle is that December, which is usually a peak for online holiday shopping scams, was relatively quiet compared to the months prior.

CATEGORIES IN PRE-BLOCKED URLs

"Pre-blocks" is the name assigned to the blocks that occur before a customer loads a malicious website. Based on our European data, the distribution per pre-block category (in percentage terms) during the year of 2020 was the following:



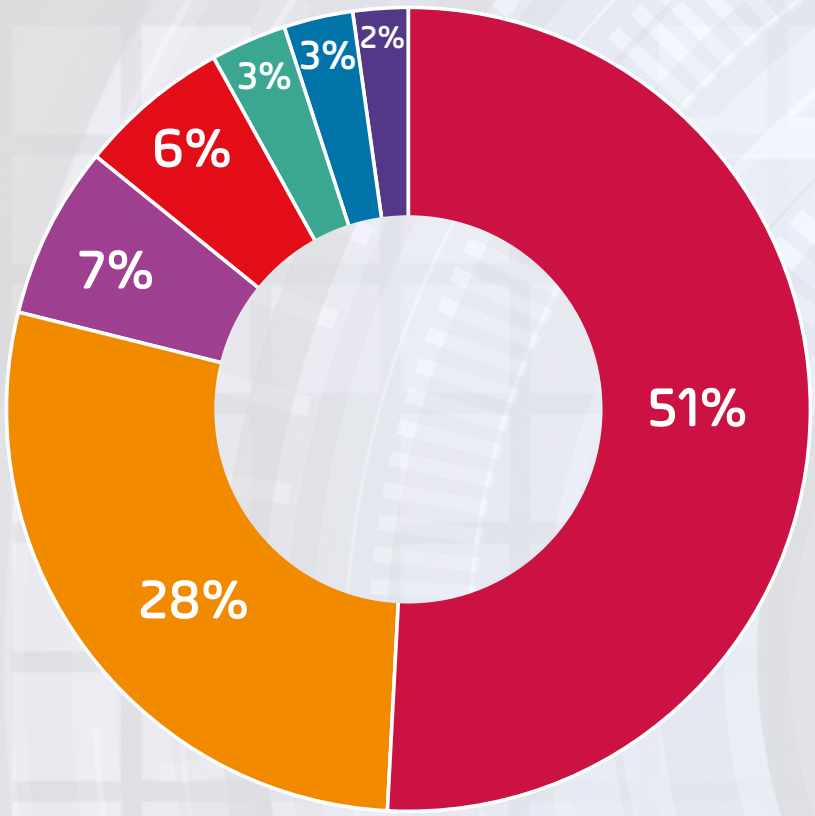
The graph shows the rise in Phishing coincided with the fist Coronavirus outbreak in late February. The Covid-19 crisis fueled huge growth in Phishing attacks. The most prevalent threats in this category are trackers such as **trk.appittech.com or trk.onnur.xyz.**

On average, Adware represented 28% of the blocks during 2020. It is important to highlight that though adware may seem harmless, the pop-ups shown can download additional malware or even redirect the victim to phishing pages.

The third most prevalent category is Malicious Downloader. The main behavior of these pages is to host malware and trick the victim into downloading and installing it. This type of threat is usually spread through Adware.

Adware Porn started 2020 at 45% and dropped to below 10% as the year went on. The rest of the categories are between 1% and 10%.

Total Pre-blocks
in % During 2020



- Phishing
- Adware
- Malicious Downloader
- Malware
- Adware Porn
- Malicious Adware
- Malicious Downloader
- Spyware

2020 was a year of Phishing and adware. Cybercriminals know that these attacks are very profitable and pose almost no risk to the criminal.

Phishing was the most blocked category among European CSPs. It represents 51% of total blocks in 2020.

Adware was the second most blocked category accounting for 28% of total blocks.

There were more than 2,000,000,000 blocking events in Pre-blocks.

Of those, more than 1,000,000,000 belong to Phishing while 623,249,493 belong to Adware.

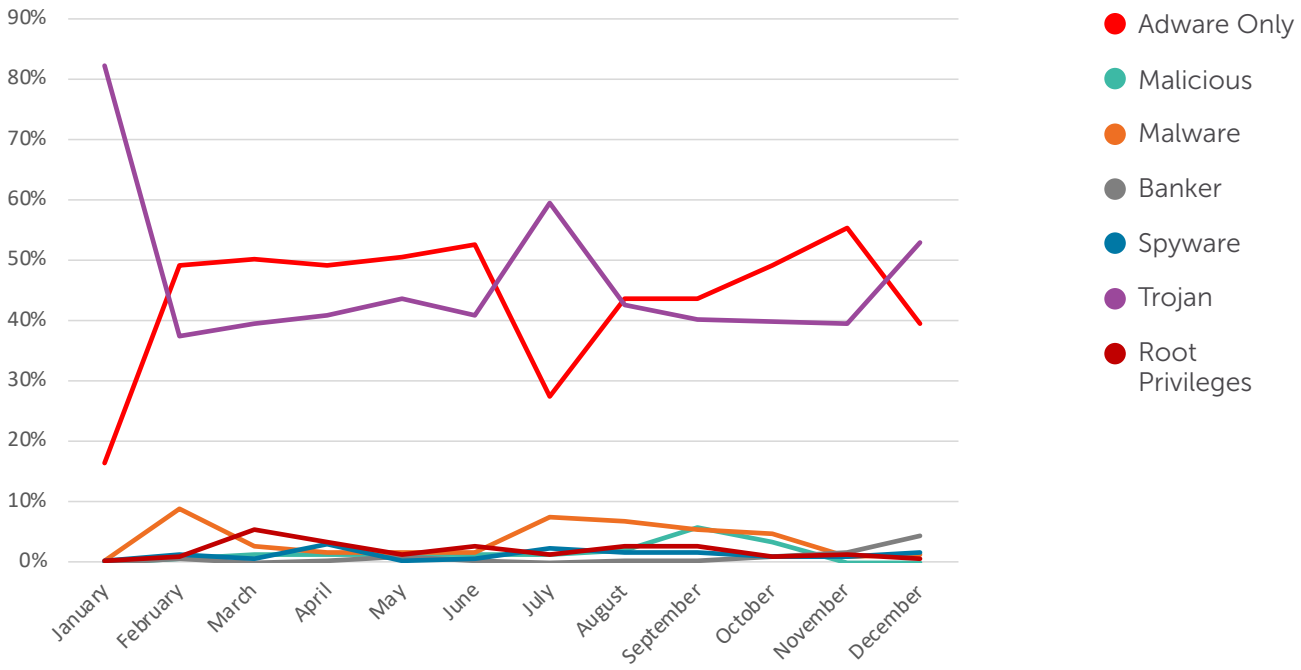
Two of the most important URLs related to Phishing during this year were trk.appittech.com and trk.onnur.xyz.

These are tracking domains that use browser cookies or other methods to send information about the users' online navigation to these websites. This communication could contain personal information (such as banking details, account credentials, or be used for illegal targeted marketing).

There are a large number of websites that distribute Adware, the two most prominent are: tosnl.com and greatforwarding.com.

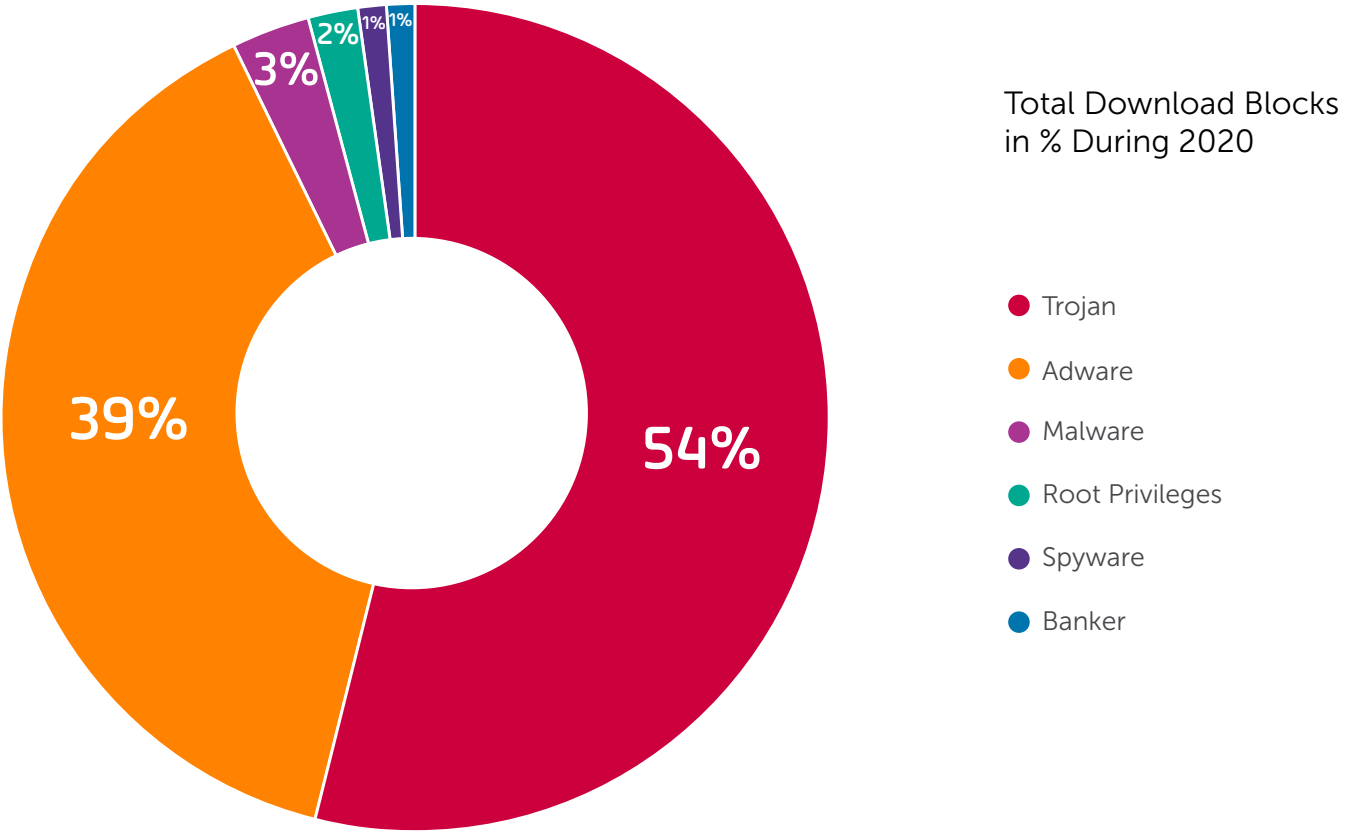
CATEGORIES IN DOWNLOAD BLOCKS

Download blocks are the blocks performed when a user downloads (intentionally or not) a malicious file. The NetworkSecure Antivirus engine detects the malicious files and blocks them from download before they can pose any danger to the user. The majority of download blocks were for Adware and Trojans, shown at the top of the graph. The rest of the categories triggered blocks in the low single digits.



Adware and Trojan blocks mirror each other in a symbiotic 'dance' as the two types of infection work together. This is because the two threats are related and work together in tandem. Once a Trojan infects a user's device it usually tries to download additional malware to the terminal. That additional malware is usually Adware. The adware then shows ads that can lead the victim to download yet another Trojan or Adware, continuing the vicious cycle.

The rest of threats are each only single digit percentages for all malicious downloads. In this range, the most blocked threat was Malware and Malicious Adware (Adware that downloads viruses directly from the pop-up, without needing to redirect to another site).



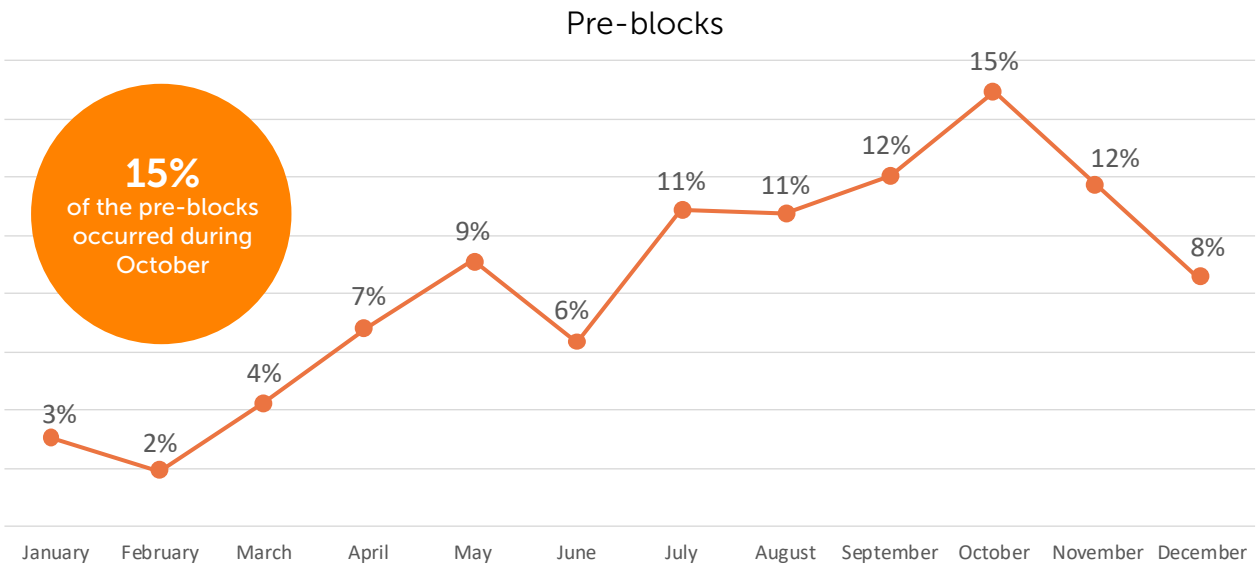
There is a significant gap between the two most blocked categories and the rest. Adware and Trojans together represent 93% of blocked downloads.

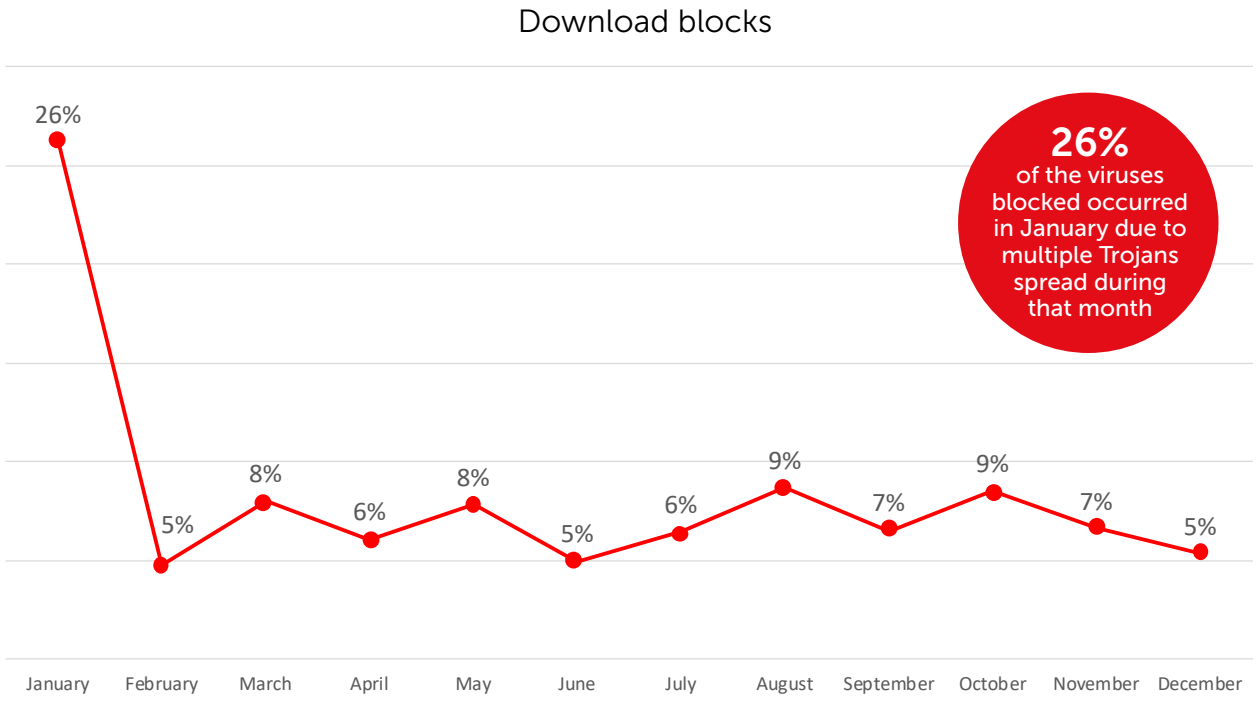
Trojans were the most blocked download category during 2020, triggering 54% of download blocking protection events in Europe. This comes as no surprise, as most Trojans remain undetected and continue to download additional malware, mostly Adware and Trojans, which in turn trigger more and more blocks for each additional attempt.

The second most blocked category is Adware, representing 39% of the download blocks during this year.

In 2020, NetworkSecure protected European Internet users 3,917,905 times from downloading malicious files. This number is much smaller than the pre-blocks, but the potential damage from each infected file is much greater, and many malicious files are pre-blocked before the download even begins and are therefore counted as pre-block events.

BLOCKS OVER TIME





IMPORTANT BLOCKS

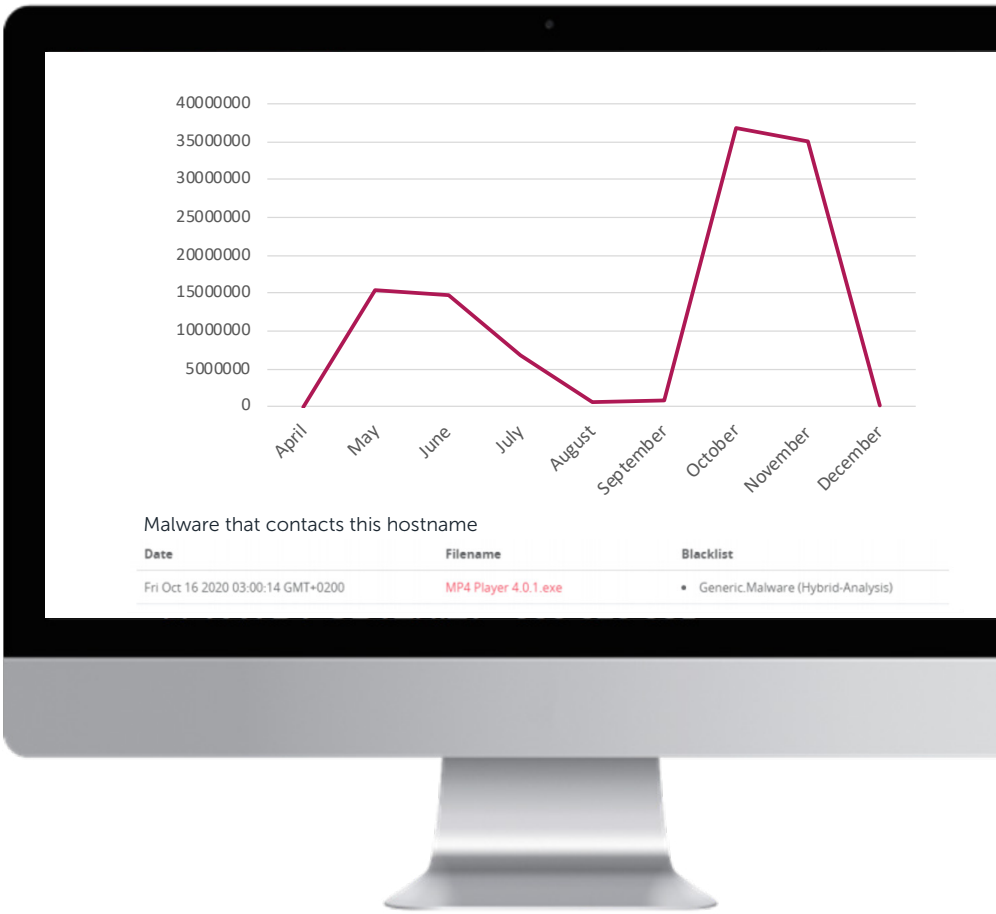
To better understand how malicious domains are used by cybercriminals, let's take a closer look at Brettericharddson.com. This domain alone triggered 119,478,039 blocks during 2020.

In April it started off as a phishing domain and remained active for about three months. Then in July activity dropped and went into a "hibernation" during August and September during which it barely triggered any blocking events.

At the end of September activity suddenly spiked into the tens of millions of blocks. This time Brettericharddson.com was being used as a command and control (C&C) domain for viruses to download instructions for further malicious activities.

In December, the domain again went dormant and did not trigger any blocking events.

It is just a matter of time until brettericharddson.com resumes activity using another method to keep performing its malicious activities.



We are excited to offer a secure and trusted mobile service, while enabling parents to be worry-free about how their children are using their devices."

Rudolf Schrefl CCO, Hutchison Drei

For more cyber security intelligence,
visit Allot CyberHub »

February 2021