allot
See. Control. Secure.

Cyber Threat Report

Europe Edition, Q3 2020

CONTENTS

INTRODUCTION

Allot is dedicated to protecting networks and their users from all types of attacks including malware, ransomware, Phishing attacks, cryptojacking and more. This report is meant to be a knowledge tool in your arsenal against the cybercriminals whose goal is to disrupt your business and take advantage of your customers.

The data presented in this report is based on malware and other types of attacks that Allot NetworkSecure detected and blocked over the third quarter of the year (Q3 2020). It is notable that all of the events presented in this report were, in fact, stopped by the Allot solutions that are implemented amongst a considerable number of communication service providers in Europe of various sizes from local to multi-national tier one players. In a time when businesses are experiencing radical interruptions resulting from the Coronavirus pandemic, cybercriminals have been ramping up their attacks, targeting people when they are more vulnerable to scams and other crimes. We have added an additional section to this report that describes these new threats.

KEY HIGHLIGHTS

- The average percentage of customers experiencing protection events during this period was 24% of security subscribers across Europe. It started at 23% in July and increased to 26% in September. The time people spend online and working from home contributes to the overall increase in the percentage of customers experiencing protection events.
- Among the main pre-blocked malicious URLs across Europe we observed significant difference between the two most blocked categories (Phishing and Adware Only) and the rest. Phishing ended up this quarter above 58% of the blocks, experiencing a very slight downward correction as mentioned in the previous report but remaining steady after that. Adware Only ended up on a clear decreasing tendency in the last quarter but remained constant for two months. In September Adware Only pre-blocks decreased by 6%.
- In Q3 2020 NetworkSecure pre-blocked 748,199,384 malicious URLs across Europe.
- Adware Only and Infection Only Download Blocks maintained consistent levels during the whole period, continuing the same pattern as during the previous quarter.
- The main Download Block categories during Q3 were Infection Only (47%) and Adware Only (39%).
- As many European countries eased out of the initial Covid lockdown and retured to normal, total blocks decreased from 241M in July to 238M in August. But as soon as the second wave hit Europe, the numbers quickly rose to new peaks, reaching 267M in September.

MAIN TAKE-AWAYS

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

Phishing remains the predominant type of website attack in Europe

- Phishing represented 54% of blocks during Q3; just 1% Below the previous quarter
- Cybercriminals already used Phishing heavily, and the COVID-19 crisis only added additional fuel as they took advantage of the crisis to launch additional attacks that preyed on people's fears.
- The damage from Phishing attacks includes; monetary loss, personal data theft, and compromised account credentials.
- Fake Phishing websites are nearly impossible to detect with the human eye.

The second most important type of threat remained ADWARE, estimated around 30% of total threats being blocked in Europe

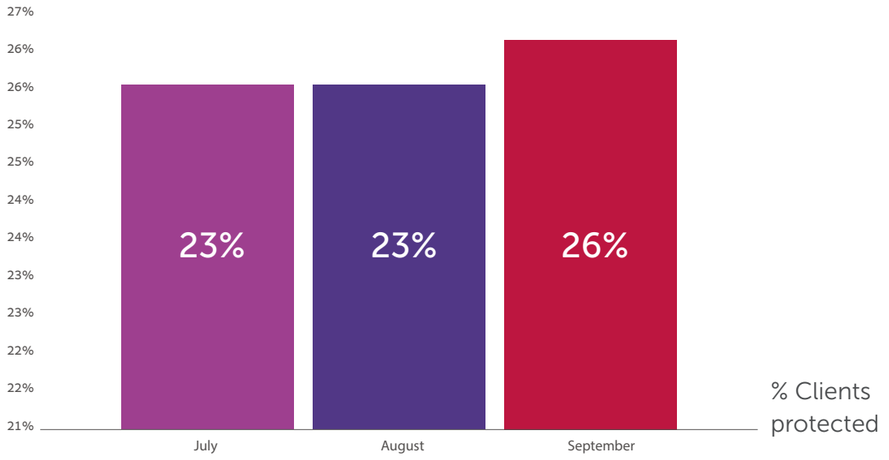
- In addition to the nuisance of increased appearance of online ads and sense of privacy loss, Adware infection can decrease the speed and quality of online experience.
- Adware is more than a mere nuisance and can cause serious damage. Like other malware, Adware can infect user terminals by redirecting to infected pages containing malware of Phishing downloaders.

Warning - devices are not protected off-network!

- Your customers are only protected by NetworkSecure when using your network. If they connect to other networks or public Wi-Fi, they run the risk of downloading a virus.
- Additional malware on the device can cause a high amount of download blocks, especially in the Adware and Trojan-Bitcoin categories.
- Add EndpointSecure for off-network protection.

% OF CUSTOMERS PROTECTED

Before digging into which categories were the most blocked during this period, it is important to understand the percentage of customers protected by our service during the third quarter of 2020.



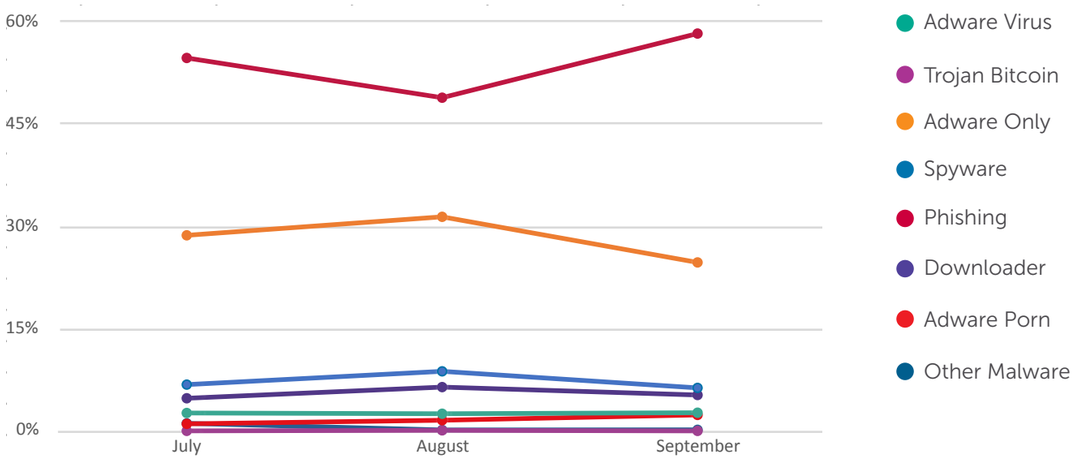
During this period, on average 24% of clients experienced protection events. A 6% decrease compared to Q2 (30%).

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

The last month of the quarter, September, was the most active month for the cybercriminals. Q3 started with a clear decrease as people began going back to the "new normal", but with the second wave of Coronavirus hiting in late August-early September, blocks began to increase once again. As people go back to being more confined, their total time spent online increases, as do cyberattacks.

It is expected that during the next quarter the percentage of customers protected will continue to rise.

CATEGORIES IN PRE-BLOCKED URLs



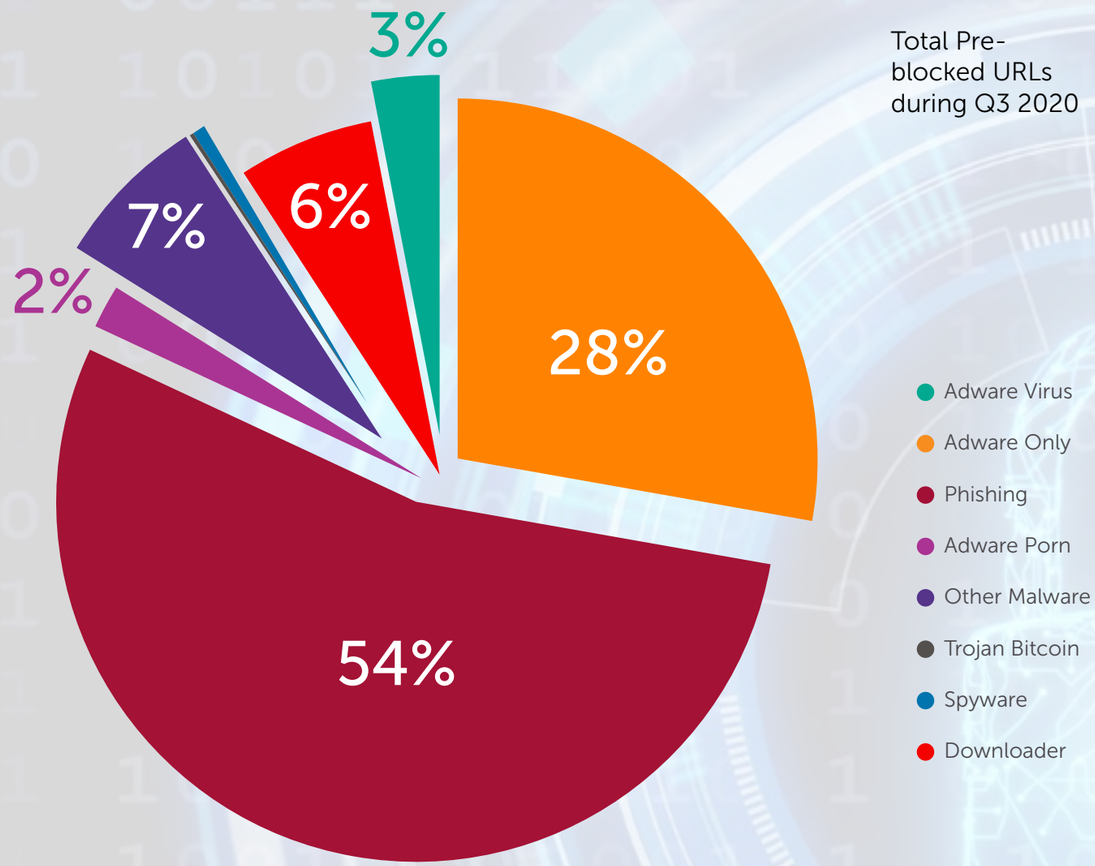
"Pre-blocks" is the name assigned to the blocks that occur before a customer loads a malicious website.

Based on our European data, the distribution per pre-block category (in percentage terms) during the third quarter of 2020 was as follows:

In the previous quarterly report Allot saw that Phishing accounted for approximately 60% of pre-blocked URLs and this percentage remained stable during this quarter; mostly due to a single URL (trk.appittech.com) that appeared dominantly across all our customers.

The other main category during this quarter was Adware Only, which had similar percentages to the previous report (29%).

These threats experienced a spike in the beginning of the Coronavirus and continue to remain at high levels. This tells us that cybercriminals keep pushing these type of threats due to being the most effortless and profitable for them.
The rest of the categories are between 1% and 10%.



Phishing was the most blocked category among our European clients. It represents 54% of total blocks during the Q3. It remained at similar levels to the previous quarter.

Adware Only is the second most blocked category with a 28% of total blocks.

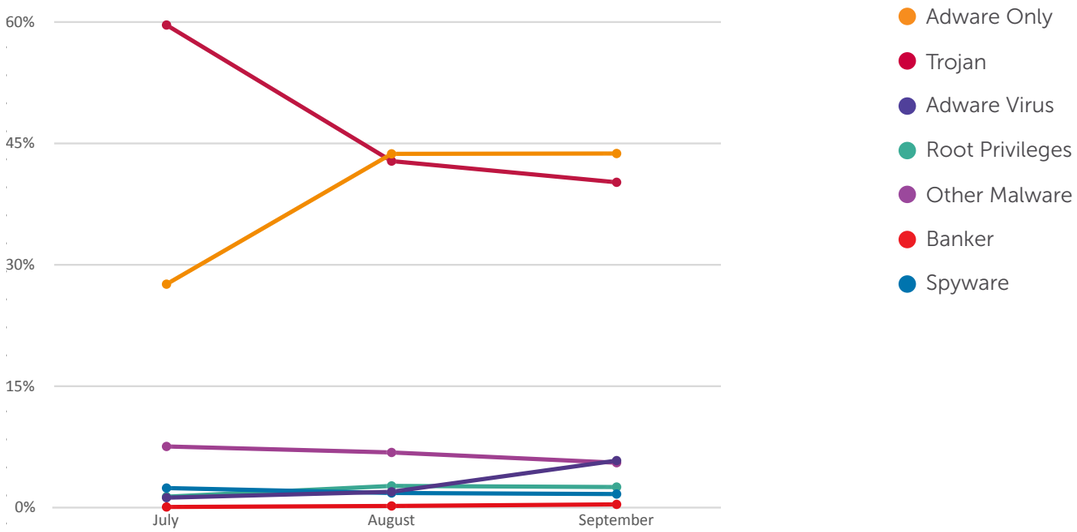
Even though during this quarter some European countries were able to go back to the "new normal", people still spend more time at home and online, causing them to also be exposed to more threats. The percentages of prevalence show that cybercriminals prefer Phishing and Adware Only because they are the least risky and most profitable type of threat.

Two of the most important URLs related to Phishing were trk.appittech.com (same as previous quarter) and trk.onnur.xyz.

These domains have a "tracking" behavior, meaning that something in the terminal (e.g.: cookies) sends navigation information to these websites. This communication may contain personal information (such as banking details, account credentials, etc.)

The Adware Only category is made up of a large number of well-distributed threats.

CATEGORIES IN DOWNLOAD BLOCKS



- Adware Only
- Trojan
- Adware Virus
- Root Privileges
- Other Malware
- Banker
- Spyware

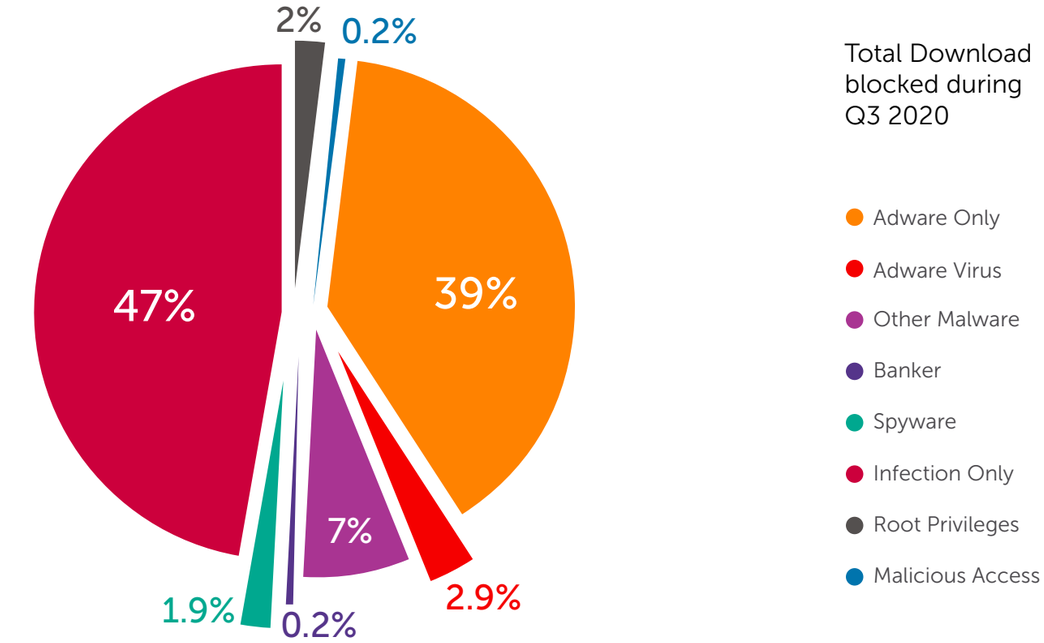
Download blocks are the blocks performed when the victim downloads (intentionally or not) a malicious file. This detection is heuristic and done through different antivirus tools.

The graph above represents (in percentage terms) the most blocked download categories for our European clients during the third quarter of this year. There are two graphs due to the significant difference between the two most blocked categories and the rest.

Also in download blocks, Adware Only was one of the most blocked categories. It started the quarter with a lower rate than Trojan-Bitcoin, but it is important to highlight how these threats evened out around 40% by the end of the quarter.

Trojan-Bitcoin as mentioned above, was also one of the most blocked categories during this period. The fact that these two threats have similar numbers is due to crossover within the groups. Trojans often try to download additional malware onto the device and that secondary infection is usually Adware. Adware viruses cause a nuisance due to high levels of intrusive ads being shown, but can also include redirects that lead the victim to download a Trojan or more Adware.

CATEGORIES IN DOWNLOAD BLOCKS



There is a significant difference between the most blocked categories and the rest. The top two categories are responsible for triggering 86% of categories blocked.

The most blocked category during the third quarter of this year was “Infection Only”, representing 47% of protection events registered across Europe during that period. This differs from how the previous quarter ended, when Adware Only was the most blocked.

The fact that the Trojans are one of the most blocked threats during this quarter is no surprise. Most of the trojans, apart from once installed remaining disguised from the human eye, will try to download additional malware (mostly Adware or other Trojans) causing an increase of blocks in these categories.

The second most blocked category was Adware Only, representing 39% of the download blocks during this quarter.

CATEGORIES IN SMB

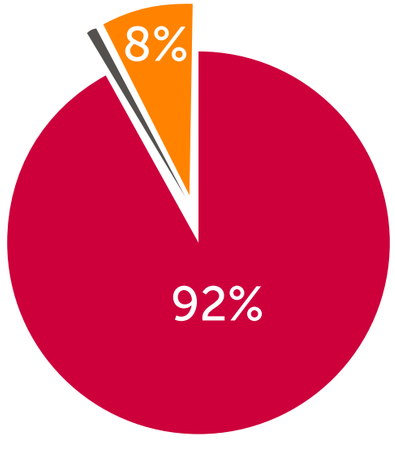
For our SMB customers we can see a difference (especially in the pre-blocks) between the categories blocked for SMBs and consumers.

Phishing was the most blocked category in Pre-block, representing 92% of the blocks, followed by Adware Only with 8%.

The type of online navigation is completely different for SMB users that from private users. This is reflected in the type of threats blocked for SMBs. The Phishing blocks are due to redirections or sites disguised as tools (such as the email or different Microsoft pages) that are used in a working environment.

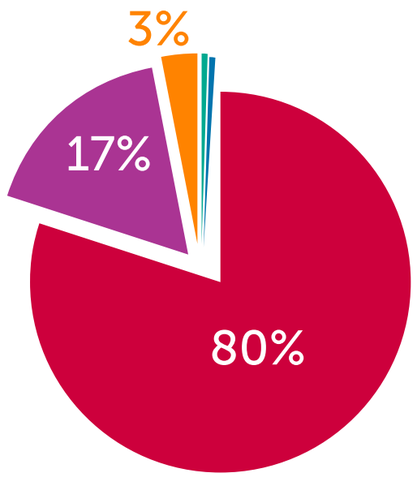
As workplace Internet use is more focused on legitimate websites, Phishing blocks are a lower percentage of all pre-blocked URLs for SMBs.

The top download blocks were similar to what was previously seen for private consumers, at least in terms of most blocked threats (Infection Only and Adware Only). As Trojans are disguised as legitimate programs, the blocking of these threats comes from the victim initially trying to download a program for work.



Total Pre-blocks during Q3 2020 (SMB)

- Adware Only
- Phishing
- Downloader



Total Download blocks during Q3 2020

- Other Malware
- Infection Only
- Adware Only
- Ransomware
- Spyware

IMPORTANT BLOCKS

Atrimunte.com appeared for the first time during the Coronavirus crisis. By July 2020 it escalated to the top 5 most blocked threats in Pre-blocks. According to the information available, it mainly targeted victims in Germany but had a significant impact also in Spain.

It was the main threat during this quarter of the Adware Only category. Atriminte.com is a perfect example of why we must not underestimate the threat of Adware.

By definition, this threat category only shows intrusive advertisement to the victims, but those ads can include redirects to malicious websites. When we tested these in a test environment some of the advertisement led to a Vhishing page (Voice Phishing calls) or even a Phishing page disguised as Amazon.

In the example shown we can see the Vhishing page. Once the victim establishes a connection to that website, the terminal will be blocked, and a red pop-up shows saying that the PC or Mobile phone has been blocked due to an infection. In order to fix it, the user is instructed to call what looks like an official Microsoft help phone number, but is actually a VoIP number. When the user calls the Phishing part of the attack takes place and a human agent will attempt to defraud the user of their personal bank account information.

In a time when businesses are experiencing radical interruptions resulting from the Coronavirus pandemic, cybercriminals have been ramping up their attacks, targeting people when they are more vulnerable to scams and other crimes.

Barry Spielman,
Product Marketing Director, Allot Secure

For more cyber security intelligence, click here »

November 2020