Decentralized
Cyber Security

WHITEPAPER

July 2018

Written by the
ACESO Team

TABLES

FIGURES

CONTENTS

WHAT IS THE ACESO PROJECT?

The aim of ACESO is to decrease the expenses of protecting a computer from malware to a minimum, where users will no longer have to pay for software, but for a service instead. Additionally, our solution decentralizes the earning centre, and 90% of all earnings are put on a p2p model where a Researcher gets 30% and a Malware analyst – 60% of the computer protection fee.

Currently, getting rid of a computer infection can be quite difficult and infected users are not always given a solution to their malware problems. Depending on their knowledge in the field, the average user would turn towards security programs for malware removal, paying $40 dollars for just one malware removal, which seems illogical. Additional features, like protection against phishing or safe browsing, are also included in the price, that is still a lot of money for resolving one malware problem, or a future situation that might not even happen. So what is the alternative?

ACESO offers a totally different approach to keeping users safe. We aim to create a platform where all could participate in cybersecurity and gain something, whether they are knowledgeable in the field or just someone browsing the Internet. The created platform would allow regular users to fix their malware issues in a much cheaper way, while malware specialists would earn income by providing malware samples/helping others solve their malware problems. It is a win-win situation for everyone.

PROBLEMS

Growing malware market

More than 1 million new malware threats are released every day (Harrison, Pagliery, 2015). With 1.5 million annual cyber-attacks, online crime is a real threat to anyone on the Internet. That number means there are over 4,000 cyber-attacks daily, 170 attacks every hour, or nearly three attacks every minute (These Cybercrime Statistics, 2015). A global study by the UNOCD (2018) finds that digital theft affects between 1 and 17% of the online population, more than 42% of users were targeted by cyber criminals the previous year.

Costs Too Much

Having these numbers in mind, computer users try to protect their computers from possible cyber threats taking over their systems. But they spend huge sums of money on AV programs promising to trace and remove all types of malware, and often are still left with their systems infected. Governments try to cope with the growing number of malware by spending millions of dollars on protection, but it's like an epidemic that spreads no matter what.

Lack of IT Experts

The chances of becoming a victim of a cyber attack only increases due to the shortage of IT Experts. And if you find one, it costs a pretty penny. New malware threats appear every single second and a demand for quick reaction and research is necessary. However, existing antivirus software are too slow and have databases that are too poor to properly react to the new emerging threats. Anti-malware can only cope with the most significant threats, leaving the minor ones, which only fuels the growth of computer threats.

No Real-Time Analysis

Users facing threats need quick real-time analysis, but with lack of proper funding (Limited Coverage) and IT experts, those threats cannot be solved properly. Until all elements are improved, the situation will remain the same.

Problems the cybersecurity industry is facing:

- Growing malware market;
- Costs Too Much;
- Lack of IT Experts;
- Limited Coverage;
- No Real Time Analysis.

Anti-virus programs are often expensive and may not necessarily help. Some bigger AV companies may not detect smaller malware threats, as they tend to focus on more widespread viruses. Users could turn to smaller anti-virus software, which focus on less widespread infections, but a solution is also not guaranteed. Choosing the program that can help also takes a lot of time and effort. If one does not work, you have to search for a different one, etc. In the end, a lot of users turn to forums for help. They describe the problem and cybersecurity experts help for free. They provide detailed instructions on what needs to be done in that specific situation, and this usually results in users being able to clean their computers. The people helping usually do it in their own free time, and for free. Checking through users' logs, identifying the problems and providing solutions can be tough work, but experts still do it for free.

In short, we have a situation where infected users do not get the help they need even after paying for expensive anti-virus, thus turn to forums for help. And in those forums, cybersecurity experts help hundreds of users each day but do not get anything out of it.

SOLUTIONS

ACESO offers a totally new model for user behavior, by changing the cyber security market into advanced innovative solutions – every user can independently control cyber threats.

In simple words, we aim to create a platform which would decrease expenses for users infected with malware and allow malware researchers/analysts to earn money by helping others solve malware problems.

We offer to pay for a service and get it here and now, without any registration or waiting for a cyber-threat to be detected, identified and recognized by AV companies in order to eliminate it. It is completely secure as Analysts will be working with encrypted information.

ACESO would allow users to fix their computers in a much cheaper way, as they would not need to pay for a software. So if their computer was attacked by malware, they would not have to buy expensive security software, they could just pay for that one fix. The payment for that fix would be divided between those who helped fix the issue, aka the Researcher (the one submitting malware samples), the Malware Analyst (the one providing the solution) and ACESO. ACESO is the mediator between the infected user and the Malware Analyst. When a user becomes infected, ACESO performs a scan and checks whether a custom solution is necessary. If it is, the acquired information is stripped of any personal data and then sent to the Analyst. This ensures that infected users' personal information is protected.

Costs Too Much

ACESO suggests an End User to pay an average of one euro/dollar fee for a fix for their computer. Usually, the same infection spreads from the same security holes and in the same geographical location. For example, a hundred users have the same problem. They each put a $1 offer in the ACESO market. Thus, the pot is $100 and the solution for these users is the same. So the Researcher who provides the information for this pot gets $30, the Malware Analyst who identifies the problem gets $60, and ACESO gets $10.

Lack of IT Experts (The cyber crime epidemic is expected to triple the number of open cybersecurity positions to 3.5 million over the next five years.)

ACESO has proof of concept guidelines on how to spot and identify malware. ACESO would prepare step-by-step guidelines and video lessons to help new contributors obtain knowledge required for this field. There are also a lot of users who already have a good grasp in this field. They contribute in various forums for free and help people fix their computers. From now on, they could earn significant money.

Limited Coverage
(70% of threats go undetected)

Big security software vendors are only quick and interested in fixing malware infections that are quite widespread, with a thousand infected users at the very least. ACESO, on the other hand, would help solve even the smaller malware infections in a quick manner.

No Real Time Analysis

Our general information blocks will hold necessary information to detect and distinguish malicious software. The blocks will be held in a decentralized network location and will be updated frequently, thanks to the ACESO market. General information blocks will be constructed on users' machines, placed on a decentralized network, and without the need of expensive anti-malware labs, they will be categorized and activated for all users in moments. In addition, Malware Analysts will be keen on solving the issues as fast as possible because the first person with a solution will earn the most tokens. Thus, malware problems could essentially be solved in real-time.

WE OFFER

ACESO provides service for detection and removal of malicious software via a network, where malicious software is determined as soon as it starts to spread. The spread of malicious software is stopped as soon as researchers put it on the ACESO blockchain, and it is identified as malicious by malware analysts or companies.

This mechanism offers:

- Clients pay for service, not software;
- General researchers earn tokens by providing general blocks of information;
- Malware analysts earn more tokens by identifying malicious blocks.

Unlike other Antivirus/Anti-malware solutions where a company decides what is good and what is bad for the user, ACESO works in a User-To-User environment, with the help of outside malware analysts and companies. There are four main players participating in the platform: the End User, the Researcher, the Malware Analyst and ACESO.

· End user – a user with an infected computer who requests a solution to the malware problem;

· Researcher – a user who provides samples for the malware in question;

· Malware Analyst – a user who analyzes the samples and provides the user with a solution for the malware in question.

· ACESO – the middle man that ensures everything goes as it should.

1. Researcher provides samples. This information is placed in the MARKET.

2a. A malware analyst finds the provided samples and determines whether they are malware or non malware samples. If necessary gives a name.

2b. Malware analyst makes a deal with a particular user for malware investigation. The price is set by the user.

3. End user uses the ACESO service. ACESO compares general information from the user with the samples in the market. If particular general information is marked as malware, the user is informed about the fee and the fix possibility. This fee is divided between the Researcher (30% of the fee), Malware analyst (60% of the fee) and ACESO (10% of the fee) during a fixed period of time, while this information is useful. After the time period has ended, this information goes to the ACESO Malware chain.

4. An AV company wants to buy information about a particular malware. It gives a price on the market. The price is divided to the Researcher (30% of the price) and Malware analyst (60% of the price). Coins are given as soon as the full information is provided. Also, the ACESO database could be sold to AV vendors as packages containing research information about malware from last week/month.

In addition, ACESO will work a security program, that acts much like an anti-virus. Users will be able to scan their computers with it in order to check whether their computer is infected with malware. Additional AVs will not be necessary as ACESO will have their functionality. Whether the computer is infected with adware or a data-stealing Trojan, the program will notify the user about it.

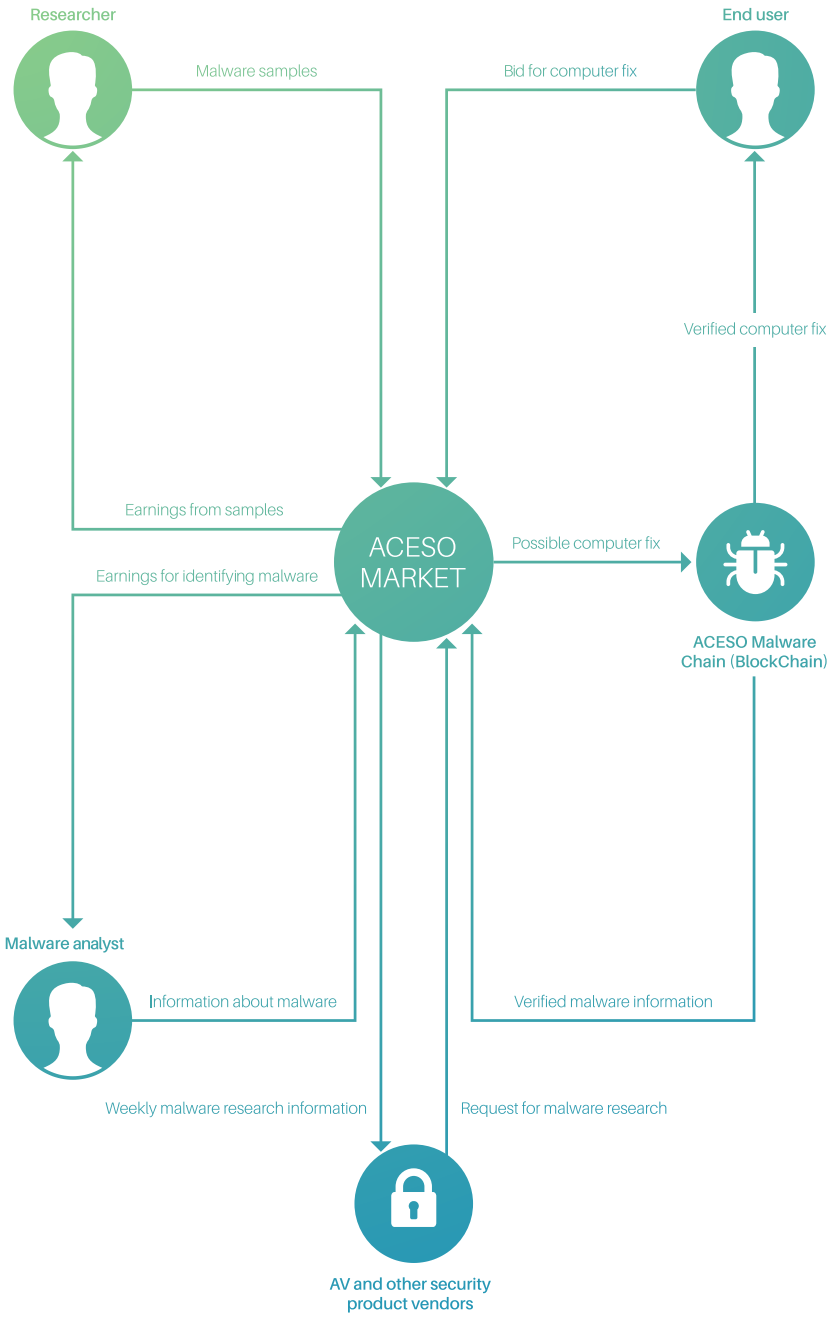

Figure 1. ACESO market

MARKET

Last year, Cybersecurity Ventures predicted that cyber crime would cost the world $6 trillion annually by 2021. Cyberattacks are the fastest growing crime in the US, and they are increasing in size, sophistication, and cost. Cybersecurity Ventures predicts that global spending on cybersecurity products and services will **exceed $1 trillion** cumulatively over the next five years. The cybercrime epidemic is expected to triple the number of open cybersecurity positions to 3.5 million over the next five years.

Top 3 Biggest Cyber Security Companies Revenue (Total 5.4 billion)

- 2017 Kaspersky Revenue – US$698 million
- 2017 AVAST Revenue – US$714 million
- 2017 Symantec GAAP revenue – $4.019 billion

We believe these will be the main compettors, and the companies whose market we will disrupt. We think ACESO could ofer beter protecton for a beter price.

What is the potential?

In today's $8.5 billion anti-virus market, damages from cybercrime are anticipated to reach $6 trillion by 2021. Even 1% of the total market would make ACESO a leading global company. With the recent technological innovations and an experienced team, we are aiming for much more. Assuming that ACESO manages to capture only 1% of the $8.5 Billion a year industry, it's about 85 million in a year.

BUSINESSES MODEL

Around 1 million new threats appear every day. That means that more than 1 million users get hit by malicious software each day. If 1 million users would pay $1 for the removal process of the malicious software, that would be a million dollar market.

The market is divided to malware analyst and researchers in 60% and 30% shares. Convert it to money, and you will get a $600 000 and $300 000 market share just for determining malicious software! ACESO takes 10% from this market for its marketing campaigns, computer resources and further investigations.

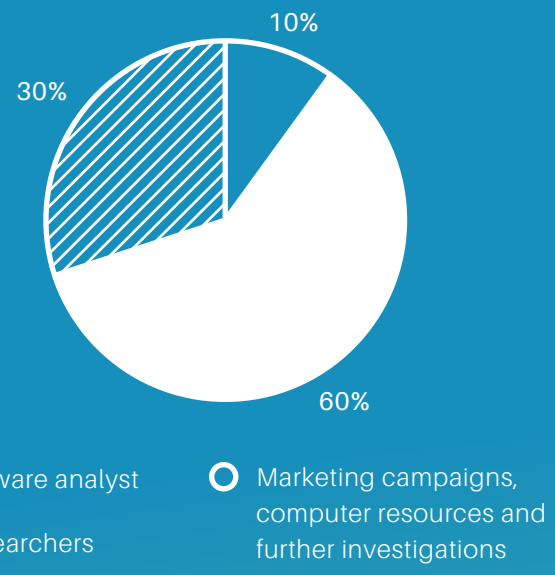

Figure 2. The market parts

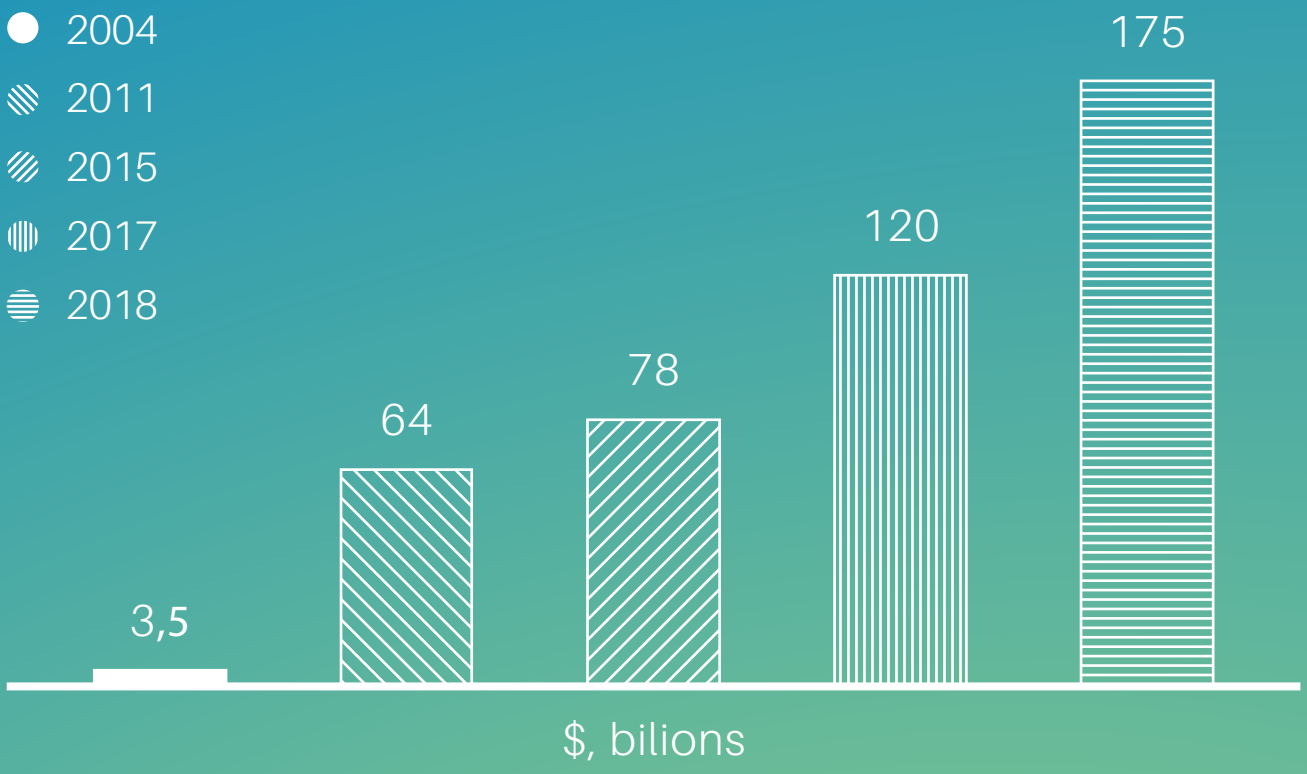

Figure 3. The global cybersecurity market evaluation (2004 - 2017, and expectations in 2018)

BUSINESSES MODEL CANVAS

End User – A lot of users worldwide are complaining about the high prices of antivirus software.

Even after a user pays a big sum of money, often a big AV vendor cannot help the user. In addition, AVs are slow and cannot always identify the problem.

ACESO offers End User to pay an average of one euro/dollar fee for a fix for their computer. Usually, the same infection spreads from the same security holes and in the same geographical location. For example, a hundred users have the same problem. They each put a $1 offer on the ACESO market. The pot is $100 and the solution for these users is the same.

ACESO is also working in ransomware prevention using artificial intelligence. This function will be offered to all users for free. Users will be protected from ransomware infections, such as the famous WannaCry, which locked more than 1 million computers worldwide.

Researcher – People who have free time and want additional income from anywhere in the world. They do not need to have any special skills. ACESO will create a special platform where people could just submit various files or make system screenshots. They just surf the internet and put information on our system. As we have mentioned before, today's market or possible income for researches is $300 000 a day.

Malware analyst – ACESO has proof of concept guidelines on how to spot and identify malware. ACESO would prepare step-by-step guidelines and video lessons to help new contributors obtain knowledge in this field. There are also a lot of users who already have a good grasp in this field. They contribute in various forums for free and help people fix their computers. From now on, they could earn significant money. Malware analysts could be from all around the world. All they need to have is an Internet connection. Malware analysts will work with encrypted information with no personal data, thus everything will be secure. As previously stated, today's market or possible income for Malware analyst is $600 000 a day.

ACESO – We will take a small fee from all transactions in our market between the User and the Malware analyst. For this fee, ACESO guarantees reliability and security for the End User. Another benefit for ACESO is a fast growing database. We believe that a person to person concept is more efficient, faster growing and more reliable. That database could be sold to AV vendors as packages containing research information about last week/month malware.

WHY ACESO NEEDS TOKENS

Everything is done in tokens, thus the ACESO token is crucial to ACESO. It is a critical component in our effort to improve protection to our users. It will be a secure way for users to pay for a malware solution and for malware researchers/analysts to get their rewards.

We will create a tokens market where two users exchange knowledge (computer fix) to tokens. Though we are running the main engine of malware protection the blockchain, we are only taking part as observers. User-to-user communication will be the main core of the process, while we will ensure the quality of the service and personal data protection. Importantly, Tokens are more secure when a user is forced to use a malware infected computer (identity remains totally safe and unknown, no bank account or credit card information is revealed), as the user will have already purchased them. So that users don't end up having to use an infected computer, they will always be recommended to have ACESO tokens. We ensure the fast completion of the process – no bank or time restrictions will make an impact.

The most important reason why ACESO Tokens are necessary is to create a community. We hope that participants in our ICO will be active members, who will not only be able to earn extra tokens but also use them to fix their computers when a problem arises.

TOKEN MODEL

In order to ask for real-time protection or a malware fix, a user needs to purchase tokens first. The purchased tokens will be reserved and only used while getting a malware solution. Purchasing them will also provide certain computer protection features, such as real-time file guard, network traffic control, parental control and ad blocker. The tokens will only be used when a user requests a fix for malware or faces an ongoing threat. Once the malware solution has been delivered to the user, those tokens will then be distributed to the three parties involved, the Researcher, the Analyst and ACESO. The tokens earned by Researchers and Malware Analysts could then be exchanged in exchange services.

Receiving ACESO tokens

- When providing malware samples for a malware whose solution has been requested. If a user's (Researcher's) provided sample is used, he/she gets tokens;
- When providing a correct solution to a malware problem. If the solution solves the malware problem, the user (Malware Analyst) gets tokens.

Spending ACESO tokens

- Protecting a computer;
- Fixing a computer;
- Submitting any file for deeper analysis;
- Getting additonal features.

When users purchase tokens and put them on the ACESO platform, they automatically get additional features, which include:

- File guard;
- Network traffic control;
- Parental control;
- Ad blocker.

Those features will be active as long as the user has tokens. The tokens will only be used when a user requests a malware solution.

BLOCKCHAIN EMPLOYMENT IN ACESO

We need to use the blockchain for our anti-malware Data Base. It is a decentralized data structure that is capable of storing infinite amounts of data. Our blockchain will be capable of working separately and individually from any other blockchain. We need this as we want our software to run on environments, where strict rules apply for data migration (government institutions, enterprises, army). Currently we have about 300mln unique generic information blocks. Our goal is to grow the unique generic blocks up to 100x times and push everything on the blockchain.

EXECUTIVE SUMMARY

The team that is developing ACESO is the same team behind WiperSoft, an anti-spyware program, giving them three years of experience in the malware field. WiperSoft is primarily a scanner that scans and removes malicious software, including rogue security software, adware, and spyware. The company has more than 1 million users in more than 100 countries.

ACESO's malware track engine has already been developed. In addition, ACESO has created the proof of concept method, which will help to identify and track malware as soon as it starts spreading. Our goal is to expand it to the extent that it will become a blockchain principle service and will be accessible to every user, every day. We want to remove the limit, where malware identification and removal is defined with a profit margin by major companies.

TIMELINE

When it was first launched in 2015, WiperSoft was free for home users. In the same year, it was downloaded more than 5 thousand times, with 1 thousand users registered on our system, who were able to use WiperSoft to its full functionality. Over the next year, the program's detection and removal functionalities were improved, the scan engine was re-created and it was launched with a new design. Coming back with a modern look and an improved user interface in 2016 October, WiperSoft became a paid a version for home users.

2016 saw a huge increase in WiperSoft downloads. Compared to 2015, the program's download rate increased by 4600%, with more than 230 thousand downloads. 850 users worldwide purchased the license in that year. In 2017, the numbers continued to go up, with over 1.1 million downloads and 8 thousand sold licenses. While the program was used in more than 100 countries in 2017, the majority of downloads, 60%, were made by users residing in Europe, 9% were made in the US, and 20% in Brazil. We are expecting a similar growth in users in 2018.

We have more than 20 thousand active users on a daily basis, 4,5 thousand of which are scanning their computers. Since WiperSoft was launched in 2015, its threat database has grown very quickly, and users are now protected from 16 thousand threats. Every month, WiperSoft detects more than 18 millions infected items (files, registries, browsers extensions, etc.) on users' personal computers. Overall, since its launch, WiperSoft has removed more than 200 million infected items from users' computers.

1 million Users

WiperSoft has been downloaded 1.1 million times and its sales have grown 950% in 2017. We have more than 20 thousand active users on a daily basis.

1,1M
Downloads

950%
Sales growth

20K+
Active daily users

100 Countries

WiperSoft is used in more than 100 countries, the majority of downloads, 60%, were made by users residing in Europe, 9% were made in the US, and 20% in Brazil.

100+
Counties

200M Total detections

WiperSoft detects more than 18 million infected items (files, registries, drowsers extensions, etc.) on users' personal computers. Overall, since its launch, WiperSoft has removed more than 200 million infected items from users' computers.

17K
Investigated threats

0.8M
Daily detected threats' elements

200M+
Total detected threats' elements

2015

WiperSoft was developed in 2015. The software was free for home users.

2016

In 2016, a new redesigned version was released with improved detection and removal functionalities. In 2016 October WiperSoft became a paid version for home users.

2017

In 2017, WiperSoft reached more than 1.1 million downloads and software was used in more than 100 countries.

2018

In 2018, ACESO, along with technical documents and the whole structure started being developed.

2019

In 2019, when ACESO is released, WiperSoft will become part of it.

Figure 4. Highlights of WiperSoft Historical Facts and Numbers

EXECUTIVE SUMMARY

COMPONENTS

ACESO proof of concept method is made of the following 4 components:

Distributed Malicious detection

We provide an abstraction for a network of professionals, capable of distinguishing between malicious/non malicious software by accessing prepared (depersonalized) information blocks. Furthermore, we provide a service to minimize false positives in detection while we merge professionals' judgments.

The market

we store malware detection and distinguished information in separate decentralized markets supervised by ACESO or an independent company. Markets ensure that payments are made when a service has been correctly and completely provided. Supervision ensures that malicious software is not ignored, no personal information is leaked in the network and no false positive (harmful) actions are made upon service requester.

The method

we developed this method from scratch and have been providing this service for 2 years. We want to release it to the public, where people can share their worries about possibly infected computers with people who had similar symptoms and have knowledge (wisdom) how to completely fix the problem. Out method does not require powerful computers for wasteful computation to mine blocks, instead, we just need time to create and store general information in the network.

General information

each blockchain block contains general information about malicious or non-malicious software. The information helps to detect and destroy malicious software, as well as helps to prevent false positive situations. This information is useless, unless it is needed in action. ACESO supervises the information flow.

PROTOCOL

Distributed malware detection is built on top of blockchain technology and with native token. Clients spend tokens for malware detection; researchers and malware analysts earn tokens by expanding general information blockchain and distinguishing malicious blocks.

- ACESO handles detection and distinguishes requests respectively via supervised markets. Clients and malware analysts set the prices for the services requested and offered, and submit their order to the markets.
- The markets are operated by ACESO which supervises the information flow with its proof of concept method. It ensures that researchers have correctly stored general information, malware analysts have correctly identified malicious software and clients received proper service.
- Finally, researchers can participate in the creation of new blocks for the general information blockchain. They will be able to submit files to ACESO and earn tokens by doing so.

THE SKETCH

The ACESO system works with 3 target groups: client cycle: put – get, researcher cycle: put – get, malware analyst cycle: put – get (see Figure 5).

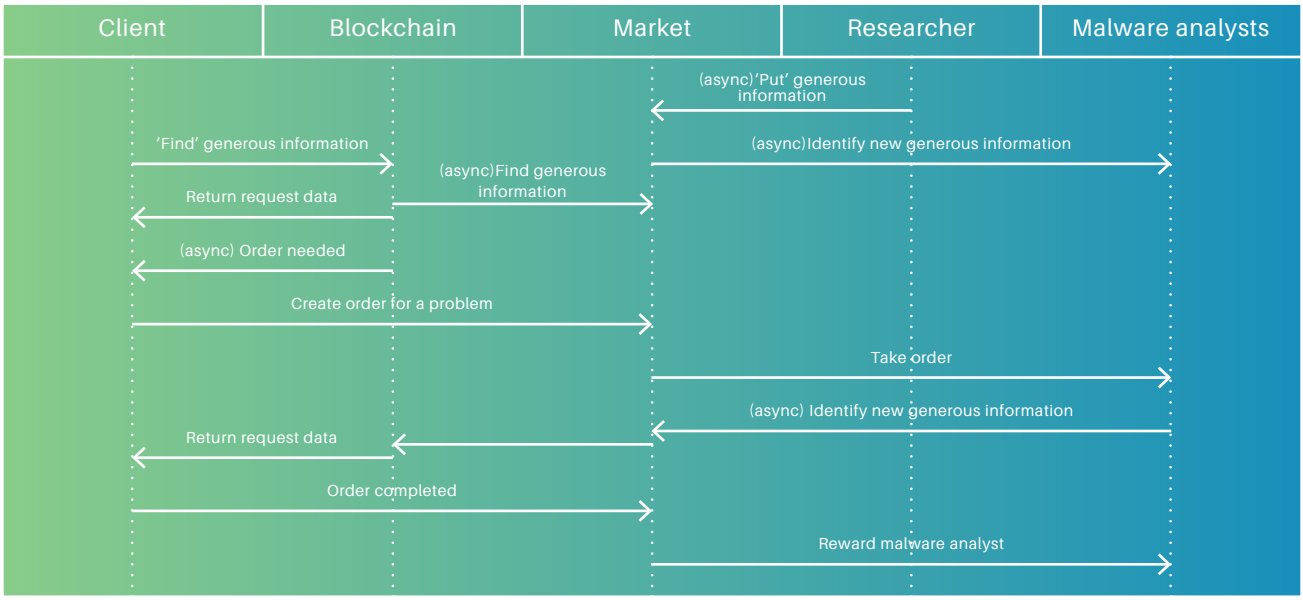

Figure 5. The sketch of ACESO system

RESEARCHER

At any time submits new general information via `Put` method:

- generates general information via software;
- extends general information block, specifying more details;
- sets a price for this general information withing specific limits.

MALWARE ANALYST:

At any time

Identifies new general information:

- confirms general information contents;
- distinguishes general information, claims price.

Takes an order:

- accepts price from a client;
- distinguishes new general information blocks without an additional fee;
- gets a reward for their actions.

THE CLIENT

At any time

Checks for matching general information between computer and blockchain:
· gets matching information OR;
· gets suggestion to make an order in the market.

Creates an order in the market to identify general information blocks;

Signs an order with a Malware Analyst;

Gets information from a Malware Analyst about general information blocks;

Closes the order.

THE MARKET

At any time

Gets 'Put' requests for new general information block with a pre-calculated price;

Gets 'Find' requests for general information blocks;

'Accepts' a general information block and pushes it to the ACESO blockchain;

Creates an order and monitors its state.

BLOCKCHAIN

For each new block:

- checks if the block is in a valid format;
- checks if the block contains all the necessary general information;
- checks if the block contains unique information;
- checks if the block is supervised;
- checks if all transactions are valid;
- checks if all orders are valid;
- discards a block if any of the above fail.

DISTRIBUTED MALICIOUS DETECTION

We introduce the notion of distributed malicious detection (DMD) scheme. DMD aggregates detection offered by multiple independent cyber security professionals and companies. DMD is decentralized, but is supervised by the ACESO Company, which already has experience in this field. There are several strategies offered for detection. Sometimes, a simple hash algorithm is more than enough to detect malicious items, but sometimes one needs to employ several algorithms or even intuition. That is where distributed malicious detection comes in place (see Figure 6):

- **Find (data) ->**

Client executes 'find general information' to receive information about the existence of malicious software;

- **Put (data) ->**

Researcher executes 'put general information' to put information about software and earn coins;

- **Accept (data) ->**

Malware analyst confirms general information being good/bad;

- **Manage ->**

ACESO manages its network of participants via Manage protocol. The Manage protocol helps to audit and supervise participants' actions and data integrity.

This scheme must guarantee general information integrity, confidentiality of personal information, early false positive prevention and equitable reward.

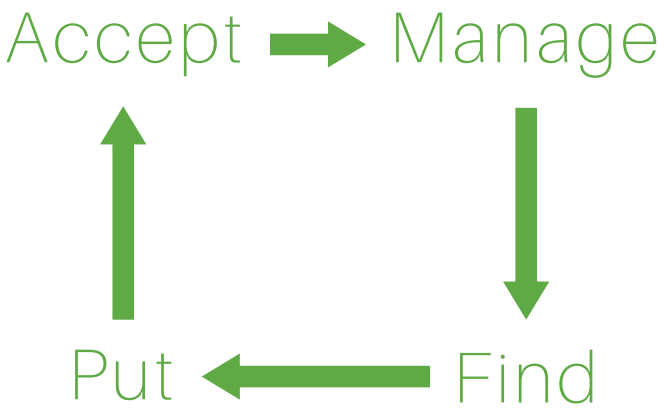

Figure 6. Summary of DMD scheme for clients, Malware analyst and ACESO

EARLY DETECTION

There are two types of malicious software: 0-day and forgotten clone. Our proposed solution in DMD works for both types. Imagine, 0-day malicious software has just started spreading. Millions of users have been infected, however, the main AV companies have just started investigating where this software came from, what it does and how to stop it. Yes, 0-day malicious software becomes ONLY malicious software, and if it is not aggressive, it becomes a low-priority research object. Unless there is interest on the internet, the main AV companies will include it into malicious software in a few days or weeks. Or not include it at all. This way malicious software will become a forgotten clone.

This is where we step in and start working!

We will find out prior to the users about the emergence of something new that might become 0-day malicious software. We will even know the region that it is targeting.

How does it work?

Thousands of researchers will generate and submit information blocks to our monitoring systems. When there is a new block or a group of blocks with similar characteristics, we can already suspect that new malicious software, capable of causing cyber threats, has emerged.

In addition, thousands of professional cyber experts will get a chance to earn tokens by analyzing new information, which we possess about the spread of malicious software. By the time we inform users about the threat of a cyber attack on their systems, we have already solved the problem. The user receives thorough information, a report: where the cyber threat came from, when it started and what damage it has done.

This way other users are protected as well, and simultaneously, help is provided to those users who have suffered damage. All this is possible due to our innovative User-To-User system.

A question may occur about what happens to the forgotten clone? Forgotten clones are just as dangerous as 0-day malicious software. Thousands of other malicious software versions emerge every day. Some of them successfully carry out destructive actions and succeed in infecting millions of computers. Some of forgotten clones "hibernate" and wait for the time to start activity. Thanks to blockchain technologies, not a single malicious software is forgotten. Its general information block is in our memory and when it restarts, we detect it again. A forgotten clone can revive with new details but even a modified version retains its nucleus and principles of activity. This way we identify it and sort of rediscover. In this case, we reward a researcher and malware analyst.

FALSE POSITIVES

By using this system, we maximally reduce error probability. The ACESO system will allow to not only take care of a devices security, but to also earn tokens by submitting (via 'Put' method) and by recognizing (via 'Accept' method) general information blocks. If Put–Accept method is used by one user, probability that his/her solution may be wrong is 50/50. However, if we assess solutions made by 1000 users for the single general information block, our probability to err is maximally reduced.

Thanks to our market, we can rate professionals. A malware specialist who has made multiple errors virtually loses voting, while the one who has made justified decisions many times, increases his/her value. This way, by rating and varying, we decrease a possibility to err to a minimum.

General information contains very important data that helps to automatize the process and, in addition, helps determine the main features, allowing to selectively distinguish if this is malicious software or not. By using the Naïve Bayes algorithm and employing data from general information blocks, we can determine the character of information placed in blockchain in real–time. However, if there are doubts, we use the help of malware analysts. We classify information contained in general information block (see Table 1).

Class	Malicious?	Safe?		
Network	3	1	=4/12	0,33
Hash	5	0	=5/12	0,42
Substrings	2	1	=3/12	0,25
Total	10	2		
	=10/12	=2/12		
	0,83	0,17		

Table 1. Likelihood table

This table does not reflect how many malware analysts voted for a particular general information block. In only shows that not all agreed with the given data pointing to malicious software. This is an OK situation. Later on, we can calculate the whole probability and decide who is going to be rewarded, and who is going to get penalties:

$$P(Malicious|Network,Hash,Substrings)=$$
$$P(Network/Malicious)*P(Hash/Malicious)*P(Substrings/Malicious)*P(Malicious)$$
$$P(Network)*P(Hash)*P(Substring)$$

With the table above, we can predict that there is a 0.72 chance that this general block contains malicious software information.

Our present partners use this formula to avoid false positives as much as possible. However, in the future, when we expand our limits and grant the voting right to a large number of clients (malware analysts), the formula will be changed accordingly. We can offer solutions to those challenges as well.

MARKET

Market plays a significant role for the user who wants to access the service and also for users who want to earn. For the sake of simplicity, we can split the market into four segments: Client market, Put market, Pro market, and Supervisor market. All regular users, depending on what they are trying to achieve, can simply join/use the first 3 market segments. The last segment of market is for closed networks that want to get access to information, approve it and use it in their own services (see Figure 7).

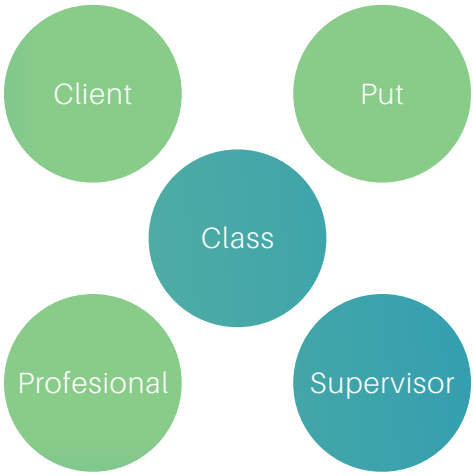

Figure 7. Users' roles of the market system

CLIENT MARKET

The program we present is 'pay for the service, not for the software' type. A user who suspects that his/her computer could have been a victim of cyber attack can acquire a short-term service that eliminates malicious software. Even if there is 0-day malicious software in his/her computer, the service we provide will help him/her by using the support of malware analysts' community. But we recommend our users to purchase service tokens before a cyber attack takes place. In addition, our client has a possibility to purchase tokens from the devices s/he uses (cell phones, tablets, and other computers).

There are situations when a user gets infected with malicious software that has not spread widely yet. In such cases, it is more difficult to get help. Thus, we offer to make a bid on the market, which would help solve the problem faster than usual. A client pays with a ACESO token, which can be bought on our sales, or on the market.

Ps is the price that the client pays for a service. There are two types of services: one-time service, just to find and fix problems, and continuous protection service.

Pm is the price that the client is willing to pay to a malware analyst to identify his/her computer problem.

The formula how to determine a price is the following:

$$M\ min <= Pm <= Mmax$$

M defines market price, meaning, a user cannot underpay and overpay for a service.

PUT MARKET

Certain users could be assigned to a higher risk malicious software group (aka those who are more prone to getting infected), and they can make use of that increased risk. It is just sufficient for them to browse, install unknown software and place general information blocks generated by our market. Later, those blocks are identified and if there is a demand, rewards are paid to users who placed them. We do not encourage users to infect their computers on purpose, however.

There are two periods: – 30 days. ΔT7- 7 days and ΔT30 – 30 days. This means that if the general information block is used within the first 7 days, a researcher will receive 30 % of income, if in 30 days – 20 %.

The formula how to calculate income:

$$PM_{put} = \sum$$

Notes: Ps is a price that a client pays for a service; Gb is general information blocks used for this service.

Now, we just divide it equally to all professionals PMput / Σ M, and each professional receives 30% or 20% depending on their block put time. This market does not require good knowledge about computer processes or the cyber security industry at all. You just run a program, which monitors your computer state and generates general information blocks for the ACESO network. And for this, you earn tokens.

PRO MARKET

This is a higher level of users group. It includes users knowledgeable about the cyber security market and who can earn tokens from how they can recognize information in a general information block. One does not need to infect computers on purpose, it is sufficient to identify and find similarities.

Cyber security professionals will earn rates for their work. The higher the rate, the higher the trust. Additionally, professionals will earn tokens for their work: they will get 60% for general information block identification and 90% for a service paid by a user.

We calculate the 60% of income based on this formula:

$$PPaccept = \Sigma \frac{Ps}{Gb}$$

It is very similar to the Put marker formula, except that we define the number, how much identifications we need for a general information block. We model this number by calculating prediction, described in 4.2 False positives section. We also define that this is always true:

$$PMput < PPaccept * 1.6.$$

This means, that the pro market will always receive the same quantity of income as the put market.

SUPERVISOR MARKET

The last but not the most important market segment is 'supervisor market'. It funds ACESO subsistence and development of activities: improvement and purchase of equipment. This segment of the market solves emerging problems and rates malware analysts. Thus, we create a small market on the market. Users buy services there; market supervisors, who take small shares for maintaining the order, work there; a blockchain, which takes its share for data storage and processing is also there.

THE METHOD

We developed and expanded a method of malicious software detection and prevention that has been successfully used for several years. In general, 'The method' includes distributed malicious software detection, the Market and General information blocks. The innovation of the method we have developed is that it is easily scalable. But it is reduced in such a way that one company can successfully manage it with the resources it has. In addition, there are no clear limits where market participants are and what has to be rated and rewarded. We seek to expand the method to such an extent that we could become just observers, and all the power is focused on technology (general information blockchain) and the user-to-user intellectual capital.

This is how we would scale the method we worked out:

- A client who has a valid token has the option to use the service. It does not matter if s/he needs the service now or will need it in the future; s/he can use the service as long as s/he has a valid token. Depending on the type of selected service, s/he either needs to have the software to access the service, or does not. The system works in a simplified way: there is no need to pay for software, it is provided as an addition. The payment is for a service, just like for electricity or telephone connection.

- A client can supply his/her service program. We will scale this method until independent cyber security providers have a possibility to check/find the general information block and determine which category it belongs to.

- We offer an external market, i.e. User-to-User will identify a general information block. We, as observers, will make the final decision about the inclusion of information into a blockchain. While moving this segment we will try to speed up identification, to prevent situations when unknown malicious software is spreading and one has to wait for many days until the main AVs include it into identification systems.

- The algorithm we have developed has no limits to generate general information blocks. It means that in the future, it will easily integrate or expand to more complex ones, which will be able to accumulate more information, but at the same time, it will outstandingly implement backward compatibility.

PARTICIPANTS

Any user can participate as a Client, researcher and malware analyst.

• Clients pay for a service – malicious software detection and elimination. Service is accessible via `Find` requests. Client can choose what type of service he/she wants to access: continuous or single-use. We also name 'Client' joint networks, who just want to use the 'Find' method to identify their own generated general information blocks by our rules.

• Researchers generate their system general information blocks and provide it to ACESO network via `Put` method. While this operation is not yet key to earning tokens, it is the starting point. General information must contain full descriptive information about malicious software. This information is approved by malware analysts or by the ACESO Company. To receive research rewards, there must be a `Find` request for this particular block by geographically different Clients. The Client willing to pay for this general information block is key to reward the malware analyst.

• Malware analysts can 'accept' requests and get reward (penalty) if this information is (in)correct. They can also earn on the Market, by helping to distinguish general information provided by the Client. Each action gives or takes trust points for this malware analyst. Trust points and price for the service will help Clients to choose a Professional for help on the Market.

GENERAL INFORMATION

General information blocks hold precious piece of data in our blockchain. These blocks are uploaded by researchers, their integrity and correctness are confirmed by malware analysts. ACESO Company carries out only the actions of monitoring to make sure that a blockchain is not damaged while making a decision about the type of general information block. For the sake of simplicity, we can declare, that general information can be of two types: static and dynamic. Static general information can be a hash string for a program or program group, substrings of a file or even a URL address. A dynamic block holds behavior description. It is captured in time, monitoring particular program behavior. Just imagine, there is malicious software in your computer, which activates itself only at midnight and only if the computer is in the idle state for quite some time (just like a regular office computer). It continuously checks for URL generated by a specific algorithm. The requests does not look very suspicious for regular office administrators because the URL does not exist. But for ACESO, this is very suspicious and this is how a general information block is made. ACESO creates behavior information blocks and asks for identification from a malware analyst. Since this block of information came from a user who paid for the service, there is a countable budget for identification. Thus, the sooner a professional identifies this behavior as malicious, the sooner s/he will get reward, increases his/hers rating and the client gets rid of malicious software. General information is placed in a blockchain. We chose this technology because the market of cyber security is expanding and getting more complicated. In our view, vital information cannot be placed in one centralized location because in case of an unforeseen cyber-attack, our users would be left without protection. Blockchain is a decentralized system.

SMART CONTRACTS

ACESO provides three basic primitives to the end users: Find, Put, and Accept. These primitives allow clients to find (merge, compare), put and accept general information to the markets at their preferred price. While the primitives cover the default use cases for ACESO, we enable for more complex operations to be designed on top of Find, Put and Accept by supporting a deployment of smart contracts.

CONTRACTS IN ACESO

Smart Contracts allow ACESO users to expand functionality, they define the use of tokens, expand the possibilities of data use and ensure integrity. Users can interact with smart contracts by sending transactions to the ledger that triggers function calls in the contract. We extend the Smart Contract system to support specific ACESO operations. Accessing supports contracts specific to general information, as well as more generic smart contracts. General Contracts: we allow users to program the conditions for which they are offering general information. There are several examples worth mentioning:

- contracting malware analysts: clients can specify in advance the professionals offering the service without participating in the market;
- payment strategies: clients can design different reward strategies for the malware analysts, for example, a contract can pay the malware analyst increasingly more through time, another contract can set the price of service informed by a trusted oracle;
- ticketing services: a contract could allow a client to deposit tokens and to pay for service on behalf of their users;
- more complex operations: clients can create contracts that allow for general information update.

INTEGRATION WITH OTHER SYSTEMS

We are developing a group of tools that will help to integrate ACESO blockchain among other systems, and – to integrate other systems based on blockchain and to integrate their functionality into the ACESO system.

- ACESO on other platforms: although there are not many other blockchain systems with cyber security functionality, we are planning to develop an interim interface to integrate ACESO functionality and to expand limits. By integrating our system, we will increase competitiveness, availability of services and we will provide a higher degree of freedom to our users.
- Other platforms in ACESO: we are developing an interface for other systems offering their services and working with blockchain technology.

ROADMAP

Here we present preliminary development milestones (see Figure 8):

Technical specification adoption, WiperSoft components integration into Aceso Network.

2018 Q4

ACESO prototype

2019 Q2 This program will be key for using the ACESO service. This initial release will allow us to begin capturing general information blocks and putting them onto the market. This initial release will be accessible only for selected test users and test researchers.

Initial market for researchers

2019 Q3. We open the initial market model. Temporarily, there will be no possibility to do the planned actions, but it will be possible to monitor the status of blocks and demand for general information blocks.

Market for malware analysts

2019 Q4. Professional cyber experts market is opened. Malware specialist can already emerge there, start collecting tokens and carry out ratings for the work done. We will start testing their methods of monitoring and we will look for the right algorithm identifying errors.

We connect the ACESO program into the market

2020 Q1 We will transform the prototype into a fully functional program, connect it to the market and start testing.

We will connect the ACESO program into the market when a user will be able to purchase a service

1 month. Malware analysts get more rights and their market forms.

2018 Q4 Scaling Process

2019 Q2 ACESO prototype

2019 Q3 Initial market for researchers

2019 Q4 Market for malware analyst

2020 Q1 ACESO market

2020 Q2 Monitoring

Figure 8. ACESO project development roadmap

2020 Q2 Monitoring -

a) Monitoring of the whole system integrity and correcting errors.

b) We provide a possibility for other companies to buy parts of the general information block from our network.

FUTURE WORK

Our project milestones reveal plans and pursuits how we intend to expand the distributed malicious software detection method. At present, the technology has been successfully tested for a few years, therefore, we want to share it with the world and expand to a safe user-to-user system. And this is only a starting point for our future research on malicious software detection and prevention methods.

ON-GOING WORK: PROJECT DEVELOPMENT

A specification of the general information in every block:

- Ethereum interface contracts and protocols.
- Blockchain archives, backups.
- Supervision mechanism with minimal intervention in order to deal with the market.
- Depersonalization process for each general information.

OPEN QUESTIONS AND RISKS

There are number of open questions and herewith risks, the answers to which have the potential to substantially improve the project as a whole, despite the fact that none of them have to be solved before the launch.

- New algorithms for detection and prevention of the evolving malicious software world.
- To develop user cooperation on the market, to grant reward points that will increase the trust in user actions.
- To fully automatize the company's monitoring mechanisms by employing AI methods.
- To increase transparency and data availability that allows to check the system integrity and efficiency.
- A possibility to involve already existing cyber security companies and jointly develop data network.
- Not to limit ourselves to the range of serviced devices (cell phones, personal computers), to attract IoT devices.
- To develop the algorithm of network monitoring, able to detect "hot" sources of malicious software spread and to prevent future spread.

TOKEN SALE

WHY PARTICIPATE IN CROWDSALE?

More Than Just a Cryptocurrency

The ACESO Token will be a token with a significant difference to most other cryptocurrencies that have been issued before. Use ACESO tokens for yourself, protect your system and privacy from hackers in a much cheaper way.

INNOVATIONS is in our DNA

ACESO is leading the way into the future by being the first to create the market where demand and supply chain takes place with two users exchanging knowledge (computer fix) to tokens.

Proven Business Model and an experienced team

ACESO's team already has 3 years of experience in the malware field, having created anti-spyware. Because the team has successfully developed WiperSoft, ACESO already has a framework. It will just be on a much bigger scale. Our goal is to expand ACESO to the extent that it will become the principle blockchain service Team.

Tokens will be locked for 2 years

Our goals are long term. To prove this, Team tokens will be locked for 2 years. (Crowdsale tokens will not be locked. Only Team Members').

Concrete Expansion Plans

We have concrete plans and a team ready to begin. Our plan is to conquer all the top and most promising markets.

Demand for the Token

ACESO token demand is driven by the growth of the users' community and the use of the token on the market. The malware market is growing every day; we believe that the demand for ACESO tokens will grow in the same way.

Tokens Exchange

The token will be listed on some Digital Asset Exchanges. Tokens will be accessible to people who did not get them during the Token Sale, as well as to those who need them to fix their computers.

Pre-ICO

Before the public ICO, a presentation will be prepared for partners wishing to purchase ACESO coins.

Pre-ICO will be in August.

1 ETH = 14000 tokens

Only 28,672,000 Aceso tokens will be issued at a special price for a limited number of participants.

At present, we have a sufficient amount of funds needed for our functioning. However, this initial support phase would help us to achieve our aims faster. Scaling of the method requires a significant workload, in particular human resources and time input. Pre-ICO will help expand the team of developers and will significantly increase the speed of coding.

Pre-ICO will be based on the "first come, first served" principle, therefore, we cannot guarantee the availability of the tokens for all interested.

ICO

Public sale will be held for 3 months. Several payment methods are available for ACESO tokens:

Ethereum (ETH) – Preferred currency;

Bitcoin (BTC);

PayPal.

Hard Cap – 32 768 ETH.

Soft Cap – 2048 ETH.

USE OF FUNDS

35% – Development team

5% – Bonus to developers

20% – Sales and marketing team

20% – Research and development team

5% – Legal support

15% – Operating expenses

TOKEN ALLOCATION

60% – Token Holders (not locked)

15% – Team (2 year lockup)

10% – Private sale

6% – Advisors, Legal Counsel, third – party services

5% – Future developments

4% – Strategic partnerships & mergers

BONUSES AND DISCOUNTS FOR ICO STAGE

ICO discounts will be issued in 5 stages. There will be a fixed amount of ETH for each stage. When a certain ETH amount is reached, another stage will start. The earlier the funding starts, the higher the discount will be received. (See Figure 10).

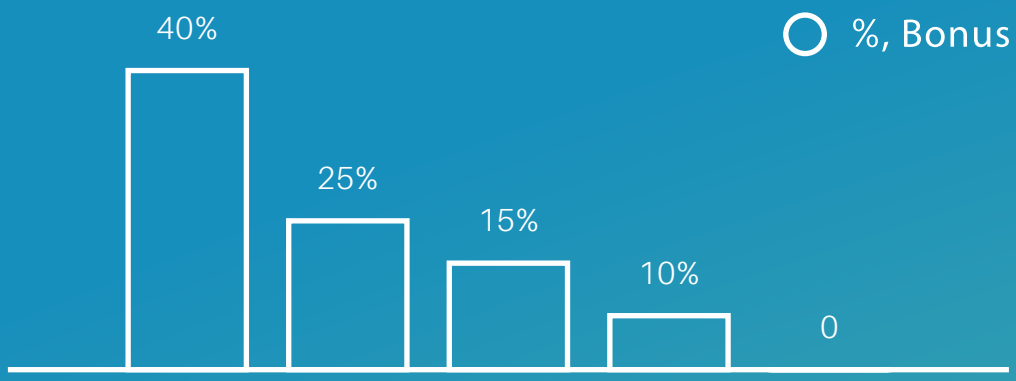

Figure 9. Discounts for ICO stage

Public ASO tokens Sale				
Bonus, %	ETH count	ETH interval	1ETH=xxx ASO tokens	ASO tokens count
40,00 %	2048	0–2048	14000	28672000
25,00 %	8192	2049–10240	12500	102400000
15,00 %	12288	10241–22528	11500	141312000
10,00 %	7168	22529–29696	11000	78848000
0	3072	29697–32768	10000	30720000
Total, ETH:	32768		Total public, ASO:	381952000

Figure 10. Public ASO tokens Sale

ASO tokens distribution	Share	ASO tokens count
Public ASO tokens	60,00 %	381952000
Team, advisors share	30,00 %	190976000
Private investors	10,00 %	63658667
Total ASO tokens	100,00 %	636586667

Figure 11. ASO tokens distribution

BUDGET AND HUMAN RESOURCES

The budget lines of the system we are developing have been distributed by the principle of human resources and system support (See Figure 8).

20% – to the research and development team. The development of new detection methods, AI integration, software adaptation for foreign devices; 20% – to the sales and marketing team. It will cover marketing expenses, media content, attracting new users, malware analysts and companies. 35% – to the development team to complete research team products and prepare it for real world scenarios; to develop for a mobile platform, web platform and desktop applications. 15% – for the operating expenses. General costs for the office, network and servers. 5% – to the legal support, 5% – for the bonuses of developers.

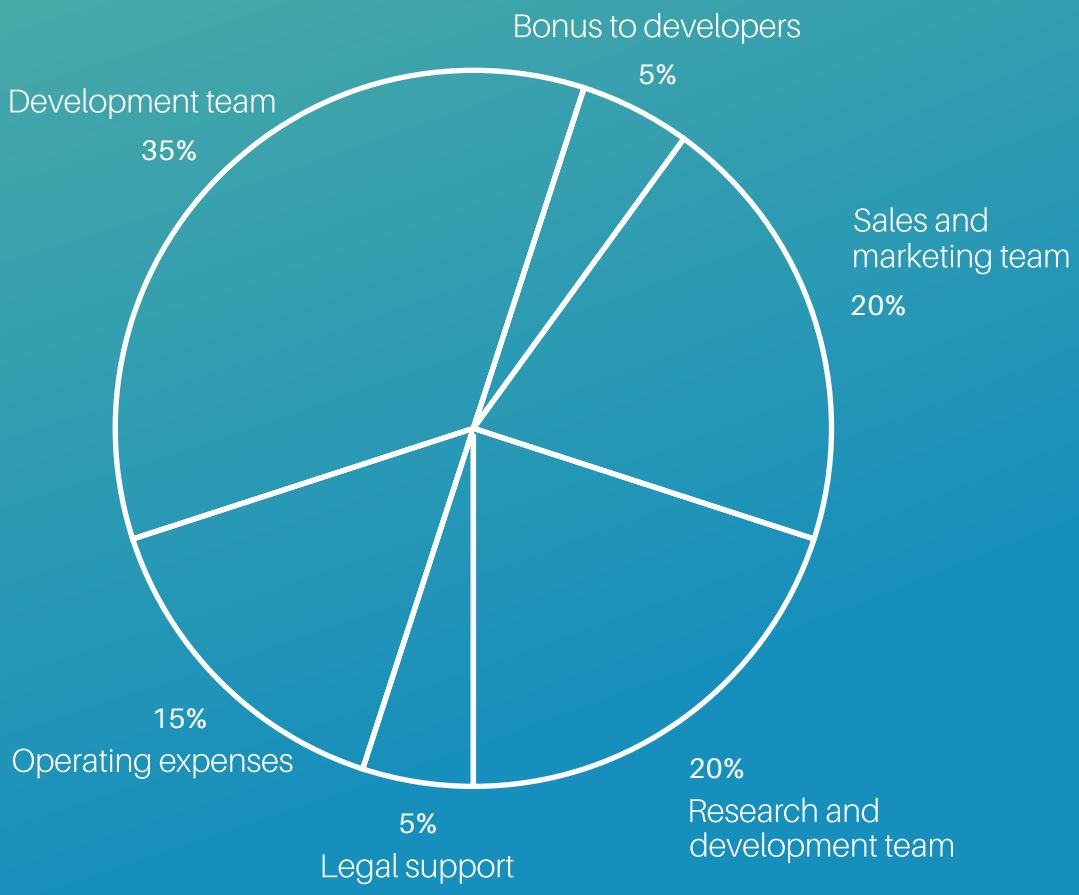

Figure 12. Budget lines

TEAM

ACESO has assembled an expert management team with a diverse range of skills. Cumulatively they have experience in: software development, IT project management, business development, ecommerce, apps, internet marketing and economics.

Romualdas Cukuras

Co-Founder / CTO

Co-Founder of ACESO, already created 4 malware/spyware removal software. 10+ years of experience in software development and apps. CEO and Core Developer of WiperSoft antispyware. Co-developer on cellular network GSM/3G, network inspection, embeddable scripting language and other projects.

Mindaugas Sinkevičius

CEO

Having worked and consulted for LionBridge and Fortune 50 companies, professional services firms and startups across diverse industries, Mindaugas can boast 8 years of experience in data driven Marketing, Product Management and Market Research.

Giedrius Morkūnas

Head of Growth and Marketing

Co-Founder of Riard. With 13 years of experience working in both start-ups and Fortune 500 companies, he is also involved in the Lithuanian Marketing Association. Board member in Lithuanian Marketing Association (LiMA) and member of LiMA Blockchain Marketing group. SEO and Growth Hacking trainer.

Povilas Jurna

Lead Blockchain Developer

As a specialist in blockchain, Povilas has successfully started ICOs like SpectroCoin, an all-in-one solution for Bitcoin, and Bankera. As a developer, he has strong technical, analytical, architectural and communication skills, and is willing to help the team, as well as share his knowledge.

Jonas Krikštopaitis

Cloud Specialist

Over 10 years of professional IT expierience in local and international companies including Barclays. Jonas took part in major project developing and supporting secure scalable and resiliant platforms for self-service consumption. Provided hosting integration for AWS cloud, VMware, Nutanix, Red Hat Openstack and other internal service hosting solutions. Skilled in IT service management and big-scale projects technical delivery.

Milda Morkūnienė

CFO

With the extensive experience on treasury management as well as cash-flow and investments management for international companies, Milda will look after business and financial planning, cash-flow planning and forecast, financial reporting and treasury management.

Marius Sinkevičius

Lead Database Developer

With experience as division team lead in Technologiju ir inovaciju centras, Marius will serve as the technical lead in database-centric software development projects of moderating-to-high complexity. As team lead, he will also be responsible for hands-on software development and design, as well as creating and updating ACESO project plans and/or task checklists for assigned projects.

Gintarė Edintaitė

Head of Human Resources

Gintare is currently a PHD Lecturer at Kaunas University of Technology. Gintare believes that the team is the most important component of a successful business, and she will ensure this success in ACESO as Head of Human Resources.

Marius Vizbaras

Lead of Technical Support

Marius is currently involved in projects for Evo-soft Ltd, a leading UK Microsoft Gold Enterprise Resource Planning Partner. As Lead of Technical Support in ACESO, Marius brings experience in secure software engineering, vulnerability analysis, digital forensics, and reverse engineering. He is experienced in developing software for a wide range of platforms, from embedded microcontrollers to large distributed systems, as well as in reverse engineering a variety of targets, and performing threat analysis on malware samples.

Tomas Zuklys

Lead Software Engineer

Tomas is Full Stack Java Team Lead at CUJO AI, which offers Internet Security Firewall for home users and a modular package of services for Network Operators. He can boast more than 10 years of experience in developing software for local and international companies, as well as 5+ years on technical leadership with architecture responsibilities. As lead software engineer in ACESO, he will help deliver cutting-edge research using partial homomorphic encryption applied to network signatures, and audit thousands of lines of code for security vulnerabilities. He will also create a variety of custom-designed binary applications, each possessing deliberate vulnerabilities, which will be used to test the efficacy of automated programs analysis tools.

Vaida Kardokaitė

VP of Community Management

While working for a wide range of organizations, both small start-ups and worldwide brands, Vaida has gained valuable experience in working and consulting in digital marketing, community management and content creation.

João Leite

Community manager

Working with several blockchain projects for half a year. Founder and manager of a crypto community. Cybersecurity degree with Cisco CCNA certificate.

ADVISORS

Fabio Cardoni

Blockchain & ICO advisor

Serial entrepreneur, business development strategist. Trading and investing in cryptocurrencies since 2012. Member of the Jur network, advisor for lympo, carVertical and BIT. Previous experiences: Founder & CEO of The Black Douglas Motorcycle Co., Tessier (Founder & CEO), Chilworth Technology.

Shahar Namer

ICO Advisor

Shahar is an early Bitcoin investor and the founder of The ICO Rocket. He co-founded a London based Venture Capital Fund together with the former CEO & Chairman of Warner Music International (sushivp.com). Shahar also built from scratch 3 international startup accelerators in London and in Israel, the "Start-up Nation" including StartupBootcamp.org which currently has 17 startup accelerator programmes across 11 countries.

Paul Cliffe

ICO Strategy Consultant

CEO of Block Venture Project, a company with the primary aim of creating a bridge for traditional investors to gain exposure to crypto-assets through risk managed, diversified funds which help to expand efficient frontiers for their portfolios. Paul's musings on bitcoin and other such crypto-assets have been featured in Yahoo finance and he is a regular contributor to such sites as cryptotelegraph.co.uk and cryptocurrencyhub.io

Lora Yessenova

Head of Investor Relations

Senior Partner at the world's first Underwriter for Initial Coin Offerings at The ICO Rocket The ICO Rocket brings a global wealth of knowledge, experience, and expertise in cryptocurrency issuance, ICO marketing and token presale capital raising.

Vadim Toptunov

Cybersecurity Advisor

A cyber security professional, possess 18+ years of experience in information and cyber security planning, servicing, management and consulting. Advocating crypto economy since 2011, contributing, investing, advising and securing various blockchain related projects.

David Lofts

ICO Strategy Consultant

David is a Brand Architect with a solid background in global consumer marketing with organisations like BAT, Mars, Chrysler JEEP, Lloyds Group, Saudi American Bank & AXA. David now works exclusively in the field of ethical start-up funding for blockchain businesses. He is a founder of crypto & blockchain start-ups Chainstarter and the 21 Million Project.

REFERENCES

1. Harrison, V., Pagliery, J. (2015).

Nearly 1 million new malware threats released every day. @CNNTech, April 14, 2015. Retrieved 10 March, 2018, from: http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html

2. Cybersecurity Businesses Report (2016).

Cybersecurity spending outlook: $1 trillion from 2017 to 2021. Retrieved 2 May, 2018 from: https://www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html

3. Norton UK Blog data (2017).

The 8 Most Famous Computer Viruses of All Time. Retrieved 9 March, 2018, from: https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html

4. The Cybercrime Statistics (2015).

These Cybercrime Statistics Will Make You Think Twice About Your Password: Where's the CSI Cyber team when you need them? CSI: Cyber, March, 2015. Retrieved 9 March, 2018, from: https://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/

5. UNOCD (2018).

A global study by the UNOCD on Cybercrime.

6. Bizz Tech Today (2016).

How well does your Antivirus work? Retrieved 2 May, 2018 from: http://www.bizztechnology.today/2016/04/how-well-does-your-antivirus-work.html

7. Cyber Security Ventures (2017).

Cybersecurity Jobs Report 2018-2021. Retrieved 2 May, 2018 from: https://cybersecurityventures.com/jobs

8. Cyber Security Ventures (2017).

Cybercrime Damages $6 Trillion by 2021. Retrieved 2 May, 2018 from: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

9. CSO (2017).

Is antivirus getting worse? Retrieved 2 May, 2018 from: https://www.csoonline.com/article/3159073/computers/is-antivirus-getting-worse.html

10. CNN Tech (2015).

Nearly 1 million new malware threats released every day. Retrieved 2 May, 2018 from: http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html