



CYBER 2.0

ANALYZER GUIDE

Product description

- Acts as an advanced inventory.
- Displays all the applications and processes from all the network computers (where the agent was installed on).
- It can show you all the applications from a specific computer.
- Or a specific application, on which computers it is installed.
- Furthermore, after the information is analyzed by the central server, the following information is added: it analyzes the number sent to it against various internet data bases and tells you what the Internet thinks of this application or process.
- It shows you the amount of antivirus engines (if any) that scanned it as a malicious program.
- It gives you a link to VirusTotal – displaying the engine that has discovered it as malicious.
- And it tells you if this is something that is entirely unknown to the Internet.

Accessing the web user interface

In order to access the V5 Log reader interface, you should enter the following address: `http://{cyber 2.0 server IP}:9000`

Initial user name: user

Initial Password: Aa123456

The user name and password can be modified on the setting page

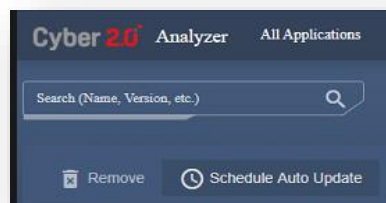
Analyzer tools – these are the tools which help you navigate the app comfortably .

On the main screen there is a table that shows all of the information about the scanned apps.

- Name : the name of the executable.
- Display name : the display name of the app.
- Version : the version of the scanned executable.
- Scan date : the date and time that the system has scanned the app.
- Status : will show the result of the scan . For example it may be suspicious which means some engines have detected it as malicious.
- Positives : will show you how many engines did detect the app as suspicious
- Links : is a link to virus total which shows which engines detected (if they did) as malicious.
- Whitelist : the whitelist status of the app – if its on it or not.
- Auto update : if the app is in auto update you will see the letter “a” as a signal.

Name	Display Name	Version	Scan Date	Status	Positives	Links	Priority	Whitelist	AutoUpdate
------	--------------	---------	-----------	--------	-----------	-------	----------	-----------	------------

Search engine : allows you to search everything in the application table by app name, version, etc. the results will pop up immediately once you start typing the first letter.

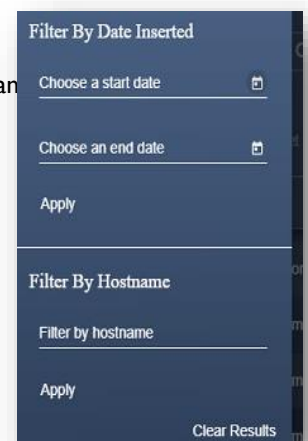
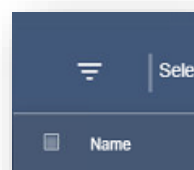


Filter : the filter tool on the left side of main page allows you to filter applications by hostname, date and inbound/outbound.

Hostname- filter results by the name of the computer.

Date- the date that the application was used.

Inbound / outbound -



Analyzer tools – these are the tools which help you navigate the app comfortably .

On the main screen there is a table that shows all of the information about the scanned apps.

- Name : the name of the executable.
- Display name : the display name of the app.
- Version : the version of the scanned executable.
- Scan date : the date and time that the system has scanned the app.
- Status : will show the result of the scan . For example it may be suspicious which means some engines have detected it as malicious.
- Positives : will show you how many engines did detect the app as suspicious
- Links : is a link to virus total which shows which engines detected (if they did) as malicious.
- Whitelist : the whitelist status of the app – if its on it or not.
- Auto update : if the app is in auto update you will see the letter “a” as a signal.

Name	Display Name	Version	Scan Date	Status	Positives	Links	Priority	Whitelist	AutoUpdate
------	--------------	---------	-----------	--------	-----------	-------	----------	-----------	------------

Search engine : allows you to search everything in the application table by app name, version, etc. the results will pop up immediately once you start typing the first letter.

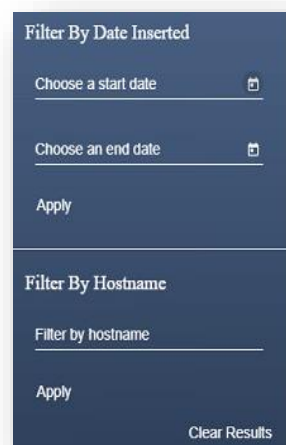
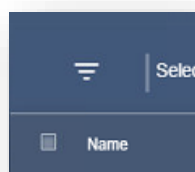


Filter : the filter tool on the left side of main page allows you to filter applications by hostname, date and inbound/outbound.

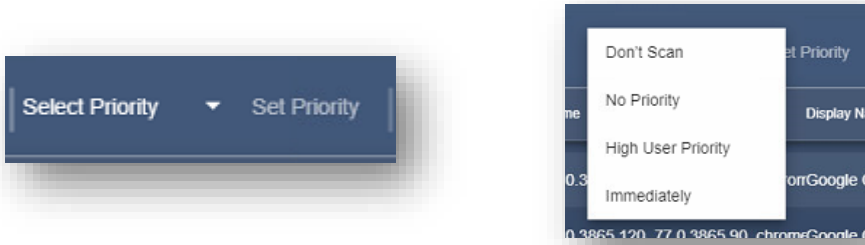
Hostname- filter results by the name of the computer.

Date- the date that the application was used.

Inbound / outbound -



Priority : as a user you can decide which apps are important for you to scan in higher priority or not at all.
 Don't scan – apps which you don't want the system to scan at all .
 No priority – the default scan rate.
 High user priority – apps which are very high priority, scanned before the no priority apps.
 Immediately – apps defined as most urgent and will be scanned immediately.

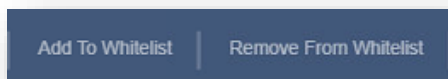





Whitelist details

The whitelist contains every authorized application.
 There is a window that allows you to see the whitelist details.
Time created : the last time someone changed / updated something in the whitelist .
Whitelist number : the number of times an app or multiple apps were uploaded to the whitelist, number of actions.
Application count : the number of apps on the whitelist.
Creator : the user that created the list.
Name : whitelist name
Description :



- Remove from whitelist- an option that lets you remove an authorized application from the whitelist.
- Add to whitelist- an option that lets you add and authorize an application to the whitelist.



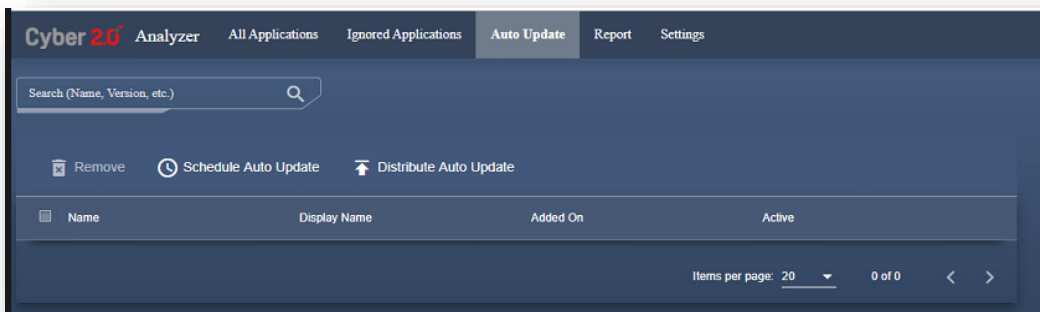
An app that is marked with an  is not in the whitelist and will be blocked once the organization is in defense mode.
 An app which is marked with a  is in the whitelist. To make sure that new versions of the app will be authorized in the white list you can mark the app and press add to auto update. Once it is in the auto update you will see the letter  next to the

Auto update

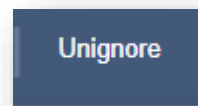
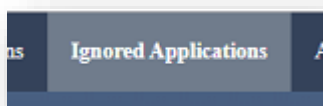
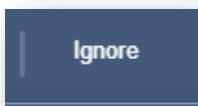
On this page you will see every application that was set to auto update new versions to the whitelist. This is a comfortable way to manage the auto updated apps.

Options:

- In this section you can choose when the applications are being updated by choosing the "schedule auto update" option and defining the time
- You can remove apps from auto updates
- activate the update by selecting the "distribute auto update" option. You can define this in the "all applications" tab.
- A search box is available also in this tab.



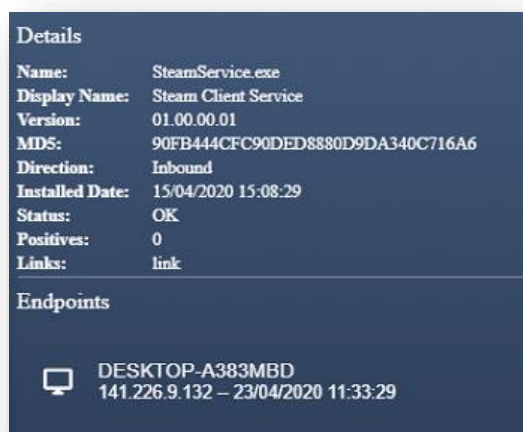
- Ignored applications
- In the ignored apps tab you will see and toggle the apps that you set to "ignore" on the main page.
- It has the same features as the main screen like add to whitelist / auto update and a search box.
- Another feature is "unignore" which brings the app back to the main screen.



Application details

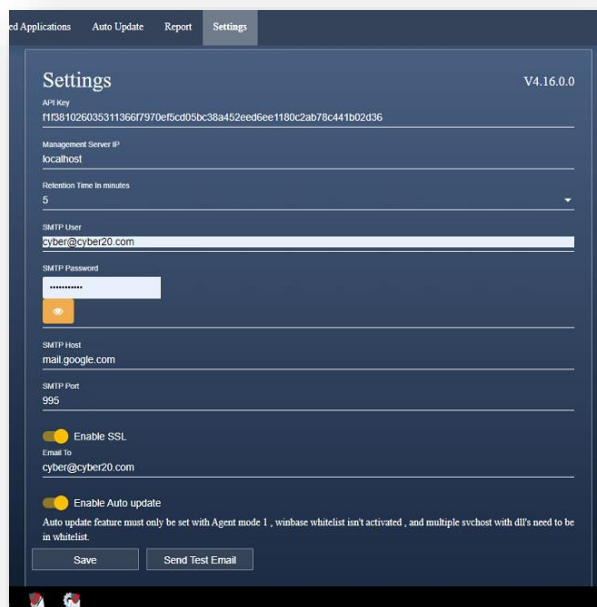
When you select an application, the app's details will show up on the right side of the screen. It also shows you the endpoint users of every app.

- Name : the name of the executable.
- Display name : the display name of the app.
- Version : the version of the scanned executable.
- MD5 : the file's hash.
- Direction :
- Installed date : the date that our system detected the installation.
- Status : will show the result of the scan . For example it may be suspicious which means some engines have detected it as malicious.
- Positives : will show you how many engines did detect the app as suspicious
- Links : is a link to virus total which shows which engines detected it (if they did) as malicious.
- Endpoints : the computers which the app was installed on .



Settings

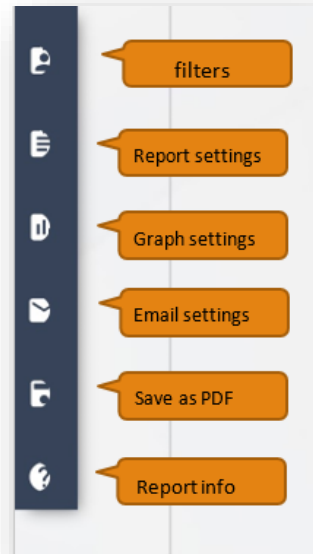
- API key- a unique key that is given by Cyber 2.0 which allows to scan all the files.
- Management server IP- management server address.
- Retention time in minutes- configure how often (in minutes) there's an update of data from the data base
- SMTP user, SMTP password, SMTP host, SMTP port- mail settings.
- "enable auto update"- the switch that allows auto update. Without it on you will not be able to use the auto update option.



Report page

The report is a tool for the user to see the systems statistics in an organized structure.

- filter - with this option you can filter computers by hostnames or groups.
- report settings
- graph settings - allows you to choose which shape of graph is more comfortable for you.
- E-mail settings - choose the frequency of the report that's being sent to your E-mail account.
- save file as pdf - saves a pdf file of your report.
- report info - with this category you can learn more about how the report is built, and how to read the scanned application status



Critical- the applications which will appear in this section are categorized as critical because they were recognized by more than five engines.

Moderate- these apps were recognized by 1-3 engines.

"Unknown" applications- apps that no information was found about them on the web or applications with version 1.0.0

Infected computers – computers with at least one malicious application.

- Every malicious app that appears on the report has a link to virustotal.
- When you select one of the malicious applications a description will appear in which you can even see an infected file or more.

<i>Critical:</i>	
No.	Application name
<hr/>	
<i>Moderate:</i>	
No.	Application name
1	war3.exe
2	WmiApSrv.exe
3	TeamViewer.exe
4	MicrosoftEdgeSH.exe
5	lpremove.exe
6	wermgr.exe
7	TeamViewer.exe
8	GoogleUpdateOnDemand.exe
9	GoogleUpdateOnDemand.exe

<i>Unknown:</i>	
No.	Application name
1	StartSuService.exe
2	OUTLOOK.EXE

