

Forum:[Hack Forums](#)

Thread: [WOLFEEY KEYLOGGER, A SUGGESTION FOR ANYBODY THAT NEEDS TO MONITOR A COMPUTER](#)

edurne - October 5, 2018, 8:47 am

Today we tested a brand new keylogger called Wolfeye Keylogger. We found the monitoring program very interesting as it is the newest of the developer group Security Software Solutions, which are well known for the latest developments in PC surveillance.

You can use Wolfeye Keylogger despite Antivirus Software:

In our view, Wolfeye Keylogger belongs to the best PC Monitoring Tools out there: the software is only 270 kb in size and uses very few resources. The program makes it possible to turn your own computer into a private investigator.

Like a detective, the keylogger secretly stores all keystrokes in the background without the user noticing. The software allows access to passwords, chat conversations, Facebook, email, visited websites and more. The logged information sends the program to the email address of the supervisor and thus allows complete monitoring of the computer in question – even remotely.

Wolfeye Keylogger can be used to control employees or monitor the Internet behavior of their own children. Illegal, however, is the use of third-party computers, as this would constitute a serious violation of the privacy sphere.

The following are the 3 steps to ensure a trusted and secure download and enable successful operation despite the use of Antivirus Software:

1. Creating an inconspicuous folder:

First, you should create a folder in which the application Wolfeye Keylogger is copied into it. The program remains in the folder and only stores information and files there. For example, in My Documents, create a folder named winupdate.

2. Set the inconspicuous folder in the antivirus program exceptions:

If you are using Norton Antivirus follow this:

Wolfeye Keylogger is a monitoring software and works like a hacking tool. As a keylogger, it is understandable that anti-virus programs classify the program as suspicious since it is a spy tool.

For this reason, it is necessary to add the created folder “winupdate” in the antivirus settings to the exceptions. This will remove the folder from the antivirus scans and the program will work fine.

It is sufficient to set only this folder in the antivirus settings to the exceptions. Because as already mentioned, Wolfeye Keylogger does not copy anything outside of this folder but only works in it. The anti-virus program can continue to scan all other files and folders as usual.

Trusted Download:

It is important that the downloaded application is trusted and does not contain any virus. To ensure a secure and trustworthy download, it is important that Wolfeye Keylogger is downloaded from the manufacturer site or from trusted websites such as Chip or CNET:

You can download from their official site: <https://www.windows-keylogger.com/en>

Or from CNET: https://download.cnet.com/Wolfeye-Keylogger/3000-2162_4-75755660.html

Or from Chip Online: https://www.chip.de/downloads/Wolfeye-Keylogger_72070578.html

Trial period: 3 days

Testing the Keystroke logging:

The software can be tested completely free of charge. You will be convinced and if not, the program can very easily be removed from the computer via the “uninstall” button.

When testing the keylogger, it is important to be structured and to test the individual monitoring components separately.

After opening the application, check the box only for “Capture Keystrokes”. Then press the “Start” button and close the application via the red Windows “X”. Now you can type things into the keyboard, enter texts, log in to Facebook.

To check if the keylogger has successfully logged the keystrokes, restart the application and press the “Stop” button to stop recording. Then press the “Open Keystrokes” button to open the log file with the recorded keystrokes.

In order to delete the keystrokes or the log file, simply press the “Delete Keystrokes” button.

Testing the Screenshot Feature:

After opening the application, check the box only for “Capture Screenshots every ...”. To test, select a 1 as an interval. In this way, screenshots are taken every minute. This is of course only for the test, you would normally choose a higher interval such as 10.

Then press the “Start” button and close the application via the red Windows “X”. Now you have to wait 1-2 minutes until the first screenshots are taken.

To check if the keylogger has successfully recorded the recording, restart the application after 1-2 minutes and press the “Stop” button to stop the recording. Then press the “Open Screenshots” button to see the screen captures.

To delete the screenshots, simply click on the button “Delete Screenshots”. If that worked, you can continue with the third step in the next post. Otherwise, please write us an email, we will reply within a few minutes.

Testing the Email Feature:

Next, enter the correct values for the “SMTP Server” and “Port” fields, which can be looked up here depending on the email account: [r/http://www.patshaping.de/hilfen_ta/pop3_smtp.htm](http://www.patshaping.de/hilfen_ta/pop3_smtp.htm)

Example Gmail:

SMTP server: smtp.gmail.com

Port number: 25 or 465 or 587

It is necessary to also make an additional adjustment in the email account:

Example Gmail:

Google Account settings: Log into the Google Account, and after you are logged, visit this page and select “Activate”: <https://www.google.com/settings/security/lesssecureapps>

After the correct settings are set, the email function can be checked by pressing the button “Test Email”. If the email settings are correct and the test email has been sent successfully, you will receive a message about the successful mailing.

Download Now:

<https://www.windows-keylogger.com/en.html>