# A Few Clarifications Concerning
# a Keylogger
# Installed in My Computer

**A Few Clarifications Concerning a Keylogger Installed in My Computer**

Recently, as I[1] was reading the report on the hearings[2] of the trial that we are facing following the Turin investigation "Scripta Manent"[3], staged by prosecutor Roberto Sparagna, I noticed an explanation regarding the keylogger (or Agent Elena[5], as the miserable Naples ROS[6] called it).

A text that appears in some sites says that a keylogger was allegedly used to intercept off-line comments during RadioAzione live recordings.

That would be nice, but unfortunately the reality is different.

The keylogger was a proper bug, sent to my PC via Internet through a virus, and it was capable of intercepting everything around my computer.

It was sufficient for the computer to be connected to the Internet and the miserable ones were able to hear all audio nearby (no video because the webcam has always been blocked out).

So, because I have my PC in my bedroom they listened not only to radio off-line comments but even more… everything in fact!

Moreover it was used to capture screenshots of my computer while I was writing texts or translating those of other comrades, texts that were were subsequently published to the RadioAzione website.

All this for six years in a row, in spite of the fact that I formatted my PC on a number of occasions[7].

---

[1] *No Trace Project (N.T.P.) note:* The author of this text was a member of the Italian anarchist radio station *RadioAzione*. As part of an investigation into the radio station, malware (called "keylogger" in this text) was installed on the author's computer.

[2] https://anarhija.info/library/italy-april-july-2018-reports-on-the-scripta-manent-trial-it

[3] *N.T.P. note:* You can find more information about the Italian repressive operation "Scripta Manent" here[4].

[4] https://notrace.how/threat-library/repressive-operations/scripta-manent.html

[5] *N.T.P. note:* The malware was a software called "Enhanced Law Enforcement Neotronic Agent" (ELANA), marketed by the italian company Neotronic.

[6] *N.T.P. note:* The *Raggruppamento Operativo Speciale* (ROS) is an Italian law enforcement agency.

[7] *N.T.P. note:* Another text[8] provides more details on the malware:

> "The operating system of the infected computer was Windows. The software was installed remotely through Internet. It stayed on the computer for four years. When the computer was re-installed/formatted, the surveillance software was installed again remotely through

I really wanted to make this clarification because the way it was described in the text in the trial report it could be misunderstood. We could all have a keylogger in our PC (even if it costs them 120 euros per day… unless they inflated the invoices contained in the investigation papers) and so it's better to know how it works.

Therefore my advice to those who think they could have one of those installed in their computer is to switch it off when they are not using it, and avoid talking in the area where it is connected.

Erroneously I had linked an external microphone to a mixer, as I thought that if it was on "Mute" it wouldn't intercept the audio, but it was pointless. Through the keylogger they activated the microphone inside the computer.

Remember to disconnect the Internet before you write a text or translate one[9].

---

Internet. Apparently, the software needed a constant Internet connection to spy and send the collected informations. It wasn't capable of saving the data locally to send them later. The software was able to record the text typed on the keyboard, to take periodic screenshots, and, depending on the security measures on the computer, to record communications sent and received (visited web pages, etc). The presence of the software was discovered thanks to investigation files."

[8]https://earsandeyes.noblogs.org/post/2019/01/27/more-precisions-keylogger-italy

[9]*N.T.P. note:* This is not good advice, because some malware can record data locally while Internet is disabled, and transmit the recorded data when Internet is enabled again. To mitigate the risk of malware, we recommend following digital best practices[10].

[10]https://notrace.how/threat-library/mitigations/digital-best-practices.html

The keylogger was a proper bug, sent to my PC via Internet through a virus, and it was capable of intercepting everything around my computer. It was sufficient for the computer to be connected to the Internet and the miserable ones were able to hear all audio nearby (no video because the webcam has always been blocked out). So, because I have my PC in my bedroom they listened not only to radio off-line comments but even more… everything in fact!