24.02.2023

The “Qbot” e-banking Trojan

Several security companies warn of the “Qbot” malware. This e-banking Trojan for instance is top of Check Point’s “Most Wanted Malware” list.

The Check Point security company publishes a “Most Wanted Malware” list each month. This shows which malware is most widespread in which country. The Swiss list has been topped by the “Qbot” e-banking Trojan since December already.

This Trojan is frequently spread using fake correspondence. Cybercriminals intercept e-mails concerning business matters and manipulate them with the aim to convince recipients to click on a link and open an archive file (zip file).

In addition to our 5 steps for your digital security (https://www.ebas.ch/en/5-steps-for-your-digital-security/) , you should also make sure to take the following measures:

- Use up-to-date antivirus software (https://www.ebas.ch/en/2-monitoring-with-antivirus-software-and-firewall/) .
- Be wary of e-mails referring to past correspondence, in particular if they contain a link asking you to click on it.
- Check the sender address of the e-mail and the Internet address the link points to by hovering over it with your mouse without clicking.
- Never load and open zip files from unknown sources.