Week 7: Supposed order confirmation delivers malware and new variants in fake extortion emails

By Federal Department of Defence, Civil Protection and Sport DDPS

Archived: 2026-04-06 00:30:23 UTC

Week 7: Supposed order confirmation delivers malware and new variants in fake extortion emails

22.02.2022 - Last week, the NCSC received a persistently high number of reports. Hackers are attempting to distribute remote access malware by means of bogus order notifications. In addition, there has been an increase in the spread of fake extortion emails being sent in the name of prosecution authorities, and they are now written in German as well.

Bogus order confirmations contain remote access malware

The way people shop has changed since 2019, with a shift towards online shopping. Fraudsters are taking advantage of this trend by sending bogus parcel notifications. In most cases, the emails sent involve credit card phishing or ask the recipient to purchase paysafecards and provide the codes.

A suspicious email was forwarded to the NCSC last week, and an analysis of it revealed a new modus operandi: The email contained a notification that an order had been received and that it was now being processed. Intentionally, the fraudsters did not include any references to any seller or items purchased; only a meaningless order number was listed.

The attachment is an HTML file with a cryptic name. When this file is executed, the download of an additional ISO file must be permitted. This is when all alarm bells should be ringing, at the very latest.

ISO files are treated by computers like executable CDs and DVDs, and often contain installation media for games or office programmes, for example.

In this case, the program contained malware called AsyncRAT. RAT stands for "remote access tool", which allows an attacker to access the infected computer remotely.

Remote access to the computer gives an attacker the opportunity to steal data stored on it and also to upload and install other malware in order to be able to intercept passwords when they are entered, for example.

- **Be wary all unsolicited email notifications you receive.**
- **Be especially suspicious if you are asked to open or download a file.**
- **Never allow your computer to execute files obtained in this way.**
- **Report such cyberincidents to the NCSC and, if possible, send us the email in question.** NCSC-Reporting form

Fake extortion emails in the name of various police authorities are now also being sent in German

In recent weeks, thousands of fake extortion emails written in French in the name of almost a dozen different law enforcement agencies were found in the email inboxes and spam folders of Swiss citizens. In France, this form of fraud has been known for years. At the end of last year, the fraudsters began to focus on the French-speaking part of Switzerland and now more and more emails of this type are appearing in Ticino (with Italian authority logos) and in German-speaking Switzerland (with German authority logos).

The emails make drastic accusations against the recipients in the name of randomly composed prosecution authorities. The aim is to get the recipients to reply to the email address mentioned in the letter. If someone contacts the fraudsters, they promise to drop the alleged "accusations" against payment of a high four-digit sum of money. However, this is not the end of the story for people who do pay the amount requested. In these cases, the fraudsters keep coming back with new demands for money until the victim finally realises the fraud and stops paying. The resulting loss can be very considerable.

Since the email addresses used by the fraudsters are crucial for communicating with the victims and sending such messages en masse, the NCSC reports the email addresses used by the attackers to the corresponding email providers. Currently, these are mostly student email accounts at various universities. In some cases, the NCSC's rapid intervention stopped further emails from being sent, thus averting potential loss.

- **Do not allow yourself to be put under pressure and do not react to such threats.**
- **Ignore such messages and mark them as spam.**

Current statistics

Last week's reports by category:

Current figures