Ransomware (encryption Trojans)

Criminals use various strategies to steal money from their unsuspecting victims. One popular approach is to encrypt users' files, to only grant them access again once a "ransom" has been paid – well, just maybe grant them access...!

How to protect yourself against ransomware:

- **Regularly create a back-up copy of your data.**
  Make sure to disconnect the medium used to hold your back-up copy from your computer once the back-up process has finished. Otherwise, it is possible for data on the back-up medium to become encrypted in case of a "ransomware" infection, too.
- **Always keep all software and plug-ins installed up-to-date.**
  Ensure that all installed software, apps as well as web browser plug-ins are always up to date. Whenever possible, always use the automatic update feature of your respective software programs.
- **Be careful with suspicious e-mails.**
  Caution is called for with any e-mails you receive out of the blue, even if these seem to originate from senders you know. Don't follow any instructions in the text, don't open any attachments, and don't follow any links.
- **Use antivirus software.**
  Your antivirus software must be kept continuously updated with the help of automatic updates. Otherwise there is a risk that newly developed malware is not recognized.

Operating principle

It can happen quite quickly: Simply opening a malicious e-mail attachment or an infected website might just possibly be enough for an encryption Trojan to worm its way into your system and to inexorably render your data useless by deleting or encrypting them.

Once files on a computer have been encrypted by this ransomware, victims are shown a "blocking screen". This asks victims to pay a certain sum of money in the shape of a crypto-currency to the attackers, for them to release encrypted files so they can be used again (ransom). Due to the use of an Internet currency, it becomes more difficult to trace authorship of the attack.

When spreading their ransomware, cyber-criminals particularly attack companies since they have large volumes of business-critical data and are more prepared to pay high sums of ransom money to avert data losses which would threaten their existence. Yet private users can be hit by an encryption Trojan and by ensuing data loss just as well.

How to proceed in case of damage

The most important measure must be taken before any damage occurs: The regular creation of back-up copies of your data! Of course, any potential infection of your system will be troublesome and associated with some effort (reinstallation). But what really counts is that your personal data can be rescued – from other threats, too! Further information on this topic can be found in "Step 1: Back up your data (https://www.ebas.ch/en/1-backing-up-data/)".

We actively discourage anyone from actually paying a ransom! There is absolutely no guarantee that victims will be provided access to their encrypted files again. In addition, such payments will finance the criminals' business model and allow them to continue their ransomware attacks and harm further victims.

How to proceed in case of damage:

- **Switch off your device completely.**

If you notice any irregularities on your system or suspect that ransomware or another type of malware generally is on the loose, switch off your device completely! This means disconnecting your device from its power supply – please make sure to pull the power plug, or push your device power switch for at least 5 seconds. This is the only way to salvage as many of your data as possible. It is not that easy to disconnect a smartphone or tablet from its power supply though, and you should shut them down as "usual".

- **Use a live system to clean your device.**
  If possible and feasible for you, restart your device using a live system, for instance "Desinfec't (https://www.heise.de/download/product/desinfect-71642) " by "c't". You can use this to scan, clean and establish another back-up of your data in a secure manner. Otherwise, take your device to a specialist, so they can do this for you.
- **If known, use decryption routines.**
  You can establish whether a certain type of ransomware is already known on such websites as www.nomoreransom.org (https://www.nomoreransom.org/en/index.html) . From there, you can also download and run decryption routines.
- **Change all your passwords.**
  Further information on this topic can be found in "Step 4: Protecting online access (https://www.ebas.ch/en/4-protecting-online-access/) ".
- **Report this to the authorities.**
  Let the Nationale Zentrum für Cybersicherheit (NCSC) know using their report form (https://www.report.ncsc.admin.ch/en/) , and also report this to your local police station.

Breachstortion

So-called "breachstortion" is a new strategy of attack very similar toransomware, and frequently used in combination with it. This does not primarily involve the encryption of data, but threats to publish sensitive information, which could damage a victim's (usually a company's) reputation. To protect their reputation, victims receive a demand to remit a certain sum of money to the attackers.

This strategy plays on victims' fears, and is meant to reinforce an attacker's ransom demand even further – if a victim is not prepared to remit the amount of money demanded for decrypting data.

Ransomware is a certain family of malware. This usually spreads via malicious e-mail attachments or infected websites. Once installed, ransomware will encrypt files on its victims' computers and on any network drives and storage media connected to them (for instance USB sticks). Victims are then unable to use these encrypted files again.