Factsheet Ransomware

Ransomware (also known as encryption Trojans or blackmail Trojans) are a specific family of malware which encrypts data on the victim's computer and on network shares, thereby making the data unusable for the victim. The ransomware subsequently displays a "locked screen" to the victim requesting that the victim pay a specific sum in the form of bitcoins (internet currency) to the attackers so that the data can be decrypted. The ransomware scene is continually expanding and the current versions are potentially much more damaging than the initial versions, which just blocked the screen without damaging data. The gateway for encryption Trojans such as these are contaminated e-mails and hacked websites.

Effects and risks

- Rendering data unusable on the computer
- Financial loss in the event of payment of the ransom

Preventive measures

- **Regularly make a backup of your data:** The backup should be stored offline, i.e. on an external medium such as an external hard disk. Thus make sure that the medium where the backup is saved is disconnected from the computer after the back-up procedure is complete. Otherwise data on the back-up medium might be encrypted and rendered unusable in the event of a ransomware attack.
- **Make sure that installed software is up-to-date:** Operating systems as well as all applications installed on the computer (e.g. Adobe Reader, Adobe Flash, Sun Java, etc.) must be updated consistently, and preferably with the automatic update function if available.
- **Be careful with suspicious email:** Always be careful with suspicious emails, emails which you receive unexpectedly or which come from unknown senders. Do not follow the instructions in the text, do not open any attachments and do not click on any links.
- **Always keep your virus protection up to date:** If you use virus protection which is subject to a charge, always ensure that the subscription is renewed for an additional year. Otherwise the virus protection will expire and be of no use.
- **A personal firewall must be installed and kept up to date.**

Measures to be taken after a successful attack

- In the event of an infection, we recommend that you immediately disconnect the computer from all networks. It is essential that the system should be reinstalled following this and that all passwords should be changed.
- After cleaning the computer, the back-up data (if available) can then be restored. If no data backup is available, it is advisable to retain the encrypted data and to save it so that it could possibly be decrypted at some later date in case a solution is found.
- In all cases, MELANI recommends bringing the incident to the attention of the Cybercrime Coordination Unit Switzerland (CYCO) and reporting the case to the local police.
- Refrain from paying a ransom because this will only strengthen the criminal infrastructure and thereby allow criminals to blackmail other victims. In addition, there is no guarantee that the key for decryption will be provided.

Measures for companies

For companies MELANI recommends the following in addition to the measures outlined above:

- You can obtain additional protection against malware (such as ransomware) for your IT infrastructure by using the Windows AppLocker. By using the Windows AppLocker[1], you can specify which programmes can be run on the computers in your company.
- By using the Microsoft Enhanced Mitigation Experience Toolkit (EMET)[2] you can prevent known and unknown vulnerabilities in software used in your company from being exploited and used for installing malware for example.
- Block the receipt of dangerous email attachments at your email gateway. These include among others:

.js (JavaScript)
.jar (Java)
.bat (Batch file
.exe (Windows executable
.cpl (Control Panel)
.scr (Screensaver)
.com (COM file)
.pif (Program Information File)
.vbs (Visual Basic Script)
.ps1 (Windows PowerShell)

- Make sure that dangerous email attachments such as these are also blocked if they are sent to recipients in your company in archive files such as ZIP, RAR or even in encrypted archive files (e.g. in a password-protected ZIP file).
- In addition, all email attachments containing macros (e.g. Word, Excel or PowerPoint attachments which contain macros) should be blocked.

[1] https://technet.microsoft.com/en-us/library/dd759117.aspx
[2] https://support.microsoft.com/en-us/kb/2458544

Consult the MELANI factsheet on ICT security for SMEs (not available in English) and the ten-point programme to increase ICT security on the Confederation's portal for SMEs (not available in English).

MELANI factsheet on ICT security for SMEs:
https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

Security precautions for the IT infrastructure of SMEs:
https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/infrastruktur-und-it/fachgerechte-it-infrastruktur/it-sicherheit.html

You can also find this Factsheet online on our website:
https://www.melani.admin.ch/ransomware