Malware Infection – What to Do?
Checklist for Technicians of Attacked Companies

General Supporting Processes

As a damaged party, when considering the following technical-tactical measures your company should bear in mind that if necessary, business and relationship managers, among others, must be informed in such a way that they are able to communicate for their part. To relieve your own workload, it is recommended that you get corporate communications involved; they can also identify further stakeholders and suggest a prioritisation.

1. Contact your Cantonal Police Corps and MELANI – and Define the Further Procedure Together.

> Inform your cantonal police corps and MELANI – and discuss whether the malware should just be monitored for the time being, or if countermeasures must be taken. The decision regarding further procedure depends largely (but not exclusively) on whether the damaged party is in contact with the perpetrator/s, and whether the perpetrator/s is/are expecting a reply from the damaged party. Police will advise on further procedure, particularly regarding communication with and behaviour towards the perpetrator/s.
> Discuss whether an immediate police deployment for support is practical.

2. Take Countermeasures in the Company Network

> Detect the URL and IP addresses of the perpetrator/s, and the extent of infection.
  > Links to the perpetrator/s (URL and IP addresses) must be detected and immediately blocked on the internal proxy server, or on the firewall. This prevents unwanted communica-tion with the server of the perpetrator/s.
  > In case of infection by e-mail, certain links to the perpetrator/s (URL and IP addresses) may be relatively easy to retrieve, either directly in the e-mail (hyperlink) or in an attachment.
  > Using the logs of e-mail servers, proxy servers and firewall as well as any further security software within the damaged company's network, the extent of the infection may be deter-mined, and the URL and IP addresses of the perpetrator/s detected.
> Block the URL and IP addresses of the perpetrator/s on the internal proxy server, or the firewall.
> Affected devices and computers must be separated from the network as soon as possible. Caution: As long as the malware has not yet been analysed by the cantonal law enforcement authorities and MELANI or the damaged party, infected computers and devices should not be turned off by the damaged party, but instead be left on and stored.

3. Secure the Relevant Data

> Secure the log data, and transfer them to the law enforcement authorities for investigating the perpetrator/s, along with the following relevant data:
  > Logs from the proxy server or the firewall with URL and IP addresses of the perpetrator/s may be sent to law enforcement as e-mail attachments.
  > If the malware reached the damaged party by e-mail, the e-mail including attachments must be compressed into a ZIP file, and then sent to law enforcement as an e-mail attachment.
  > If the malware infection occurred by “drive-by download”, the malware should be isolated by the damaged party if possible, compressed into a ZIP file, and then sent to law enforcement as an e-mail attachment.
  > If the malware infection occurred by USB data carrier, then that carrier must be made - available to law enforcement (sent by registered mail or handed over personally).
  > Any malware analyses carried out by the damaged party themselves may be forwarded to the law enforcement authorities as e-mail attachment.

NEDIK in cooperation with MELANI and Swiss Cyber Experts