Cyber-Security and Risk Exposition at Hospitals during the Extraordinary Situation

FOR INTERNAL USE ONLY

Date: March 20, 2020
Author: NCSC / GovCERT.ch
Contact: outreach@govcert.ch
Distribution: Healthcare sector MELANI, H+, HIN

Baseline

Attackers can try to gain access to hospitals by sending fake emails with malicious attachments. Up to this point, mainly non-targeted attacks distributing information stealers have been seen, as for example “Hawkeye” and “AgentTesla”. However, more target attacks using the same methods could appear in the near future. The probability of mistakes in the IT area is increased because of the high work load in hospitals, and the consequences become more serious. Additional measures are hard to implement in the current situation and need to be well balanced because of potential disturbances during implementation. Moreover, additional use of work from home changes the attack surface: devices such as notebooks used at home are not protected as well and are monitored less tightly by the IT-security team of the organizations. The use of remote access gateways (RAS) significantly increases the risk for successful phishing and password stealing, like dictionary[1], password spraying[2], and brute force[3] attacks, notably if no second factor for authentication is applied. (two factor authentication).

[1] https://en.wikipedia.org/wiki/Dictionary_attack
[2] https://www.triaxiomsecurity.com/2018/11/08/password-spraying-attack/
[3] https://attack.mitre.org/techniques/T1110/

The aim of this document is to show some central aspects for protection against phishing, malware, and lateral movement in a condensed form. A lot of additional information and publications by MELANI were made available at healthcare workshops, on MELANI-NET (closed customer group only), on the MELANI homepage, and the NCSC/GovCERT.ch blog; additional organizations like the German Federal Office for Information Security are listing further measures.

Prevention

Technical

At this moment, it is hard to recommend and implement generic preventive, technical measures. Some are worth to be considered nevertheless:

- Checking mail server preferences in respect to dangerous files. Attachments of incoming mails with potential dangerous files should generally be blocked[4]
- Validating the backup strategy: are there offline copies of highly critical data, notably regarding the current COVID-19 situation?
    - Is it possible to write highly critical data on WORM media (write once, read many)?
    - Is it possible to keep a copy of current patient data on a second system completely separated from the internet?
- Work from home:
    - Is a two factor authentication implemented (e.g. SMS, Authenticator, RSA token)?
    - If no: Is it possible to implement GeoIP restriction to only allow access from Swiss IP addresses?
    - Are logs checked, specially a sequence of login failures followed by a successful login?
    - Enforced tunnelling is recommended on devices like notebooks and tablets, such that all traffic from and to these devices are directed through protection- and detection infrastructure of the organization. This is very important due to the assumed increase of phishing attacks caused by more frequently use of work from home.
- Critical infrastructures are recommended to discuss with their ISP the possibility to implement Emotet/Trickbot and MELBL (MELANI botnet list) BGP feeds. Non-critical

[4] https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/assets/blocked-filetypes.txt

infrastructures can contact incidents@govcert.ch to obtain information how to implement these block lists.

- If block lists on proxies are already present and can be adapted without too much effort:
    - MELBL (contact incidents@govcert.ch)
    - URLHaus block list: https://urlhaus.abuse.ch/api/
    - Feodo tracker block list: https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.txt
    - Spamhaus Don't Route Or Peer List (DROP): https://www.spamhaus.org/drop/
    - Optional: block TLDs with low reputation: https://www.spamhaus.org/statistics/tlds/
- Blocking of websites not yet classified or categorized by your proxy service. This measure will cause additional work, but is also very efficient.

Besides, all recommendations made during our critical infrastructure workshops remain valid:

Blog «Severe Ransomware Attacks Against Swiss SMEs»:
https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/

Beware: Ransomware continues to pose a significant security risk for SMEs:
https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/sicherheitsrisiko-durch-ransomware.html

Information security checklist for SMEs:
https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/merkblatt-it-sicherheit-fuer-kmus.html

Organizational

The focus on the organizational level is:

- Suspend any current phishing awareness campaigns until the situation normalizes
- Most organizations already implement COVID-19 awareness campaigns. These can be complemented with the following supplement (e.g. PostIT or poster):

Criminal and state sponsored actors are trying to abuse the attention caused by COVID-19 in their interest by distributing malware in the name of health care organizations. Please be very careful when opening documents received by E-Mail, SMS, or any messenger services.

Never activate Macros contained in such documents. In case of doubt, contact your help desk or IT security team.

Detection

Technical

If block lists supplied by NCSC/GovCERT.ch and other source can't be implemented as prevention measure, it might still be possible to include these into your log monitoring. While this can't prevent an initial infection, it might allow to stop lateral movement if reacted upon in time. Moreover, a lightweight intrusion detection system (IDS), e.g. passiveDNS offered by NCSC/GovCERT.ch or Suricata, is suggested.

On end user devices like notebooks and PCs, the application of sysmon (contained in Microsofts's Sysinternals suite) should be considered; However, be aware of the implementation risk if applied during a crisis.

Suspicious E-mails, file attachments, or links can be forwarded to incidents@govcert.ch for analysis at any time.

Organizational

Staff members are among the most important sensors at all. They should always report suspicious activities like E-mails. Ideally, a spam reporting button (Outlook) can be used to make it easy for staff members to forward suspicious mails to a central point.

Reaction

Technical

In case of an infection, it has to be checked if a dropper known for delayed lateral movement at specific targets was used, e.g. Emotet/Trickbot, OSTAP, or Get2/SDBBot. In such cases, a deeper analysis is required to check if such a lateral movement already happened. If so, NCSC/GovCERT.ch can be contacted for support. If a damage already happened, e.g. by attacking the active directory or data encryption, NCSC/GovCERT.ch should also be contacted as soon as possible.

Organizational

It is highly recommendable to inform your staff internally in an open way about successful attacks and apply a communication concept for external communication as openly and transparently as possible to avoid rumours. The operational incident response process must be directed by a protection approach and designed such that evidence can be preserved to support a later criminal charge. Generally, we recommend to press criminal charges after lateral movement or actual damage happened.

Contact

In case of an IT security incidents, suspicious email, questions, etc :

E-Mail: outreach@govcert.ch

On-call team: +41 79 152 20 80 (**Emergencies only!**)