Attack against Czech Hospital

FOR INTERNAL USE ONLY / TLP AMBER

Date: 17 March 2020

Author: NCSC/GovCERT.ch
Contact: outreach@govcert.ch

Distribution: Healthcare sector MELANI, H+, HIN

We received some information about a ransomware attack against a Czech hospital (see: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/).

Indicators of compromise (IOCs) are listed below:

IP: 162.216.240[.]7

Domain involved: syvansoft[.]com

Malware used: Cobalt Strike*

Other IPs involved:

142.202.188[.]233

142.202.188[.]223

*Cobalt Strike is a post-exploitation tool deployed after another malware already infected a machine. Please stay vigilant and investigate any malware detection to determine its root cause.

We classify this attack as being a targeted ransomware attack most likely done by a criminal actor with the goal of extorting money. It is important to understand that these attacks are having multiple stages and that the attackers are using various tools in order to gain enough privileges to encrypt large parts of a network. This includes in most cases gaining high privileges in Active Directory.

For all questions reach out to: outreach@govcert.ch