Fighting bushfires with Preparation: Prevention of Malware spread using Security-Configuration Guidelines

Bachelor's Thesis

Supervisor: Prof. Dr. Alexander Pretschner
Advisor: Patrick Stöckle
Email: {alexander.pretschner, patrick.stoeckle}@tum.de
Phone: +49 (89) 289 - 17314

Starting date: immediately

Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17314
https://www4.in.tum.de

Context

Currently, the most dangerous malware is probably Emotet. [1] In the past few months, we have seen several serious attacks in which Emotet or variants of it have been used. Two notable examples here are the attack on the Kammergericht Berlin, the highest state court of Berlin, and the attack on the University of Gießen. In Gießen, the attack forced the university to deactivate thousands of computers because they might be infected and to reset 38,000 passwords because the might be known to the attackers. The fact that a major German university could be a victim of such a severe attack sheds a dark shadow over the security of German institutions. One main problem is that Emotet does not impose sophisticated attacks using unknown vulnerabilities, but known weaknesses in often-used programs to infect the victims' computers. Most of the weaknesses should be well known to the people responsible for the security of these networks as they are tackled by security-configuration guidelines published by the Center for Internet Security (CIS) [2]. During this thesis, we want to investigate if guidelines were applied but did not block the attacks, if the guidelines were not strict enough and left the systems in an insecure state, or if there were no guidelines at all.

Goal

The goal of this thesis is to answer the following research questions.

- What kind of weaknesses have been used to infect and destroy the systems in the case of Emotet? Here, we want to try to collect as much information as possible from the different incidents which happened in the last few months.
- Were security guidelines applied when the attacked happened? If so, why could the attack still be completed? Did the attackers use other weaknesses to infiltrate the system under attack?
- How can we improve existing security-configuration guidelines to make Emotet infections harder or impossible? This could be evaluated using two test systems: One system in the state where the attack was successful and one hardened using the new guideline. If we can infect system one, but not system two, the new guideline might be useful.

Working Plan

1. Gather information about Emotet and known attacks
2. Analyze which weaknesses and vulnerabilities have been used to infect to systems and to destroy data
3. Define additional rules for the security configuration guideline to block Emotet attacks
4. Evaluate result on different test systems

References

[1] https://en.wikipedia.org/wiki/Emotet
[2] https://www.cisecurity.org/