Lab 1 – Removing Trojans

Lukas Fuller

IA-301 Introduction to Information Assurance

Prepared for

Professor Elizabeth Tolson

**Abstract**

The student is expected to complete each step then answer the questions in the last section of this lab to reinforce the learning objectives.

**Materials**

Windows based Computer with Microsoft® Windows® Malicious Software Removal Tool

**Methodology**

By using the Windows software removal tool

**Lab**

It didn’t label any screenshots to be included, so for order I decided to leave this here ☺

**Questions:**

1. Define malware? **Malware is a form of software that is programmed to inhibit a systems performance, permanently damage a system, or anything crippling one’s system**
2. Explain how Anti malware software detects malware? **Depending on the type of anti-malware software, or the type of scan, it can vary on how exactly they it detects malware. For example, on-access scanning will check every file you open usually in real-time, whereas a full-system scan will essentially scan the entire system at that moment for any traces of malware software.**
3. What Anti malware software does NIST SP 800-69 recommend to protect USG computers? **–**
4. Network Defender offers two types of scans; what are they? **Quick scan and full system scan**
5. What are the four options available under the “action” tab? **Quick scan, full scan, customized scan, and choose folder**
6. Select a detected malware and Click “View more information about this item online”. Write a paragraph assessing the threat posed by that malware to your computer. **Due to my windows 2003 server not functioning properly (I tried to run the VM but it kept saying it was corrupted), I’m going to write about my experience with removing malware in the past from my mother’s computer. The virus in particular was a form of adware, and it would drastically hinder the performance of her computer whenever she used any web browser. The potential harm I would say after looking into the particular virus (can’t exactly remember the name), would be gathering user data, and most importantly generate loads of ad revenue for the user who infected the file that was downloaded by my mother (of course she blamed me and my videogames for it). Most noticeably, whenever you would open the browser, by default it would display dosearches.com as the home page with loads of ads and a search icon that I wouldn’t dare press, and to check how many ads were being displayed I went onto Youtube and ran ad blocker. To my surprise within the span of 10 minutes it had blocked over 100-200 ads and counting, and I’d imaging it generated a decent amount of money for the amount of time it remained on her computer. However, after a few hours of troubleshooting I was able to remove the adware through the C drive, and manually uninstalling chrome where it appeared it had taken root.**
7. Under what circumstances would you not remove detected malware from your computer? **If it was tied to necessary file to the system’s core performance I suppose, but if you can’t disinfect the virus then you most likely have lost the file anyways.**

**Conclusion**

This lab went over the process of removing malware and viruses like the ever common Trojan horse. However, I had a bit of trouble with the Microsoft 2003 server VM, so from my previous experience I was able to answer the questions regarding the removal of malware. I did learn more about anti-malware software though, which is necessary to any health pc. Lastly, the references listed in the lab were also helpful to learn more about malware.

**Grading Rubric**

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | **Points Allowed** | **Points Actual** | **Comments** |
|  |  |  |  |
| **Title page** | **5** |  |  |
| **Screen shots** | **5** |  |  |
| **Questions** | **10** |  |  |
| **Conclusion** | **5** |  |  |
|  |  |  |  |
| **Extra Credit** |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Total Points** | **25** |  |  |