Technische Hochschule Ingolstadt

Seminararbeit/Whitepaper

Analyse der Malware

angefertigt von

Name:	Dominik Gunther Florian Schlecht
Matrikelnummer:	00032209

Betreuer:

Technische Hochschule Ingolstadt:	Prof. Hahndel

Ingolstadt, 28. Mai 2015

Inhaltsverzeichnis

1. Einleitung **0**

2. Verwendete Tools und Infrastruktur **0**
2.1. Physikalisches Betriebssystem . . . 0
2.2. Virtualisierungslösung . . . 0
2.3. Virtuelles Betriebssystem . . . 0
2.4. Disassembler . . . 0
2.5. Weitere Tools . . . 1
2.5.1. RegShot . . . 1
2.5.2. Resoucehacker . . . 1
2.5.3. PEView . . . 1
2.6. Webseitn . . . 1
2.6.1. Virustotal . . . 1
2.6.2. Malwr . . . 1

3. Infektionsweg **1**

4. Dynamische Analyse **1**

5. Statische Analyse **1**

6. Fazit **1**

A. Appendix **1**

B. Quellcode **1**

C. Ergänzende Grafiken **1**

D. Quellcode Grafiken **1**

1. Einleitung

Im Rahmen dieser Seminararbeit werden asasd

2. Verwendete Tools und Infrastruktur

2.1. Physikalisches Betriebssystem

Als Grundsystem wurde ein Linux verwendet. Dies hat den Vorteil, dass ein Großteil der sich derzeit im Umlauf befindlichen Malware für Windows konzipiert ist. (Ebenso steigt der Anteil der Malware für mobile Betriebssysteme stetig, diese werden hier jedoch nicht behandelt.) Als unkompliziertes, wandelbares und trotzdem hoch modifizierbares System wurde Debian 8 gewählt. Versuche mit z.B. Gentoo zeigten Probleme mit der verwendeten Virtualisierungslösung.

2.2. Virtualisierungslösung

Es gibt viele Vorteile für die Nutzung einer Virtualisierungslösung bei der Malwareanalyse, jedoch auch Nachteile. Vorteilhaft ist vor allem das erstellen von sogenanneten Snapshots, welche einen bestimmten Zustand eines Systems aufzeichnen und es möglich machen, diesen später wieder herzustellen. Zudem wird das Host-System vor der Malware geschützt. Ein Nachteil ist, dass moderne Malware immer häufiger überprüft, ob sie in einer virtuellen Umgebung ausgeführt wird. Falls ja, werden oft andere Funktionen ausgeführt, um die ursprüngliche Funktion zu verschleiern. Insgesammt überwiegen aber die Vorteile den Nachteil. Falls die Malware auf die virtuelle Umgebung prüft, muss geprüft werden, ob über Prüffunktion über den Disassembler deaktiviert oder umgangen werden kann.
Als Virtualisierungslösung wurde VMWare Workstation 11 genutzt. Diese bietet gerade im Bereich der Netzwerkmodifikation weitere Möglichkeiten gegenüber der kostenlosen Variante Virtualbox von Oracle. Die Workstation kann von der offiziellen Webseite heruntergeladen und für 30 Tage kostenlos getestet werden.

2.3. Virtuelles Betriebssystem

Als virtuelles Betriebssystem wurde Windows 7 Pro verwendet. Dies ergibt sich einfach daraus, dass Windows 7 derzeit mit eines der meistverbreiteten Betriebssysteme ist und Malware meistens für Windows konzipiert ist.
Zudem wurde 32-bit als Architektur gewählt, um die Komapatibilät mit Tools wie Cukoo siche zu stellen. Außedem wurden sowohl das UAC, Updates sowie die Firewall deaktiviert, um der Malware eine Möglichst einfache Umgebung zu bieten. Die VMWare-Tools wuden absichtlich nicht installiert, da dies einer Malware eine sehr einfache Möglichkeit bieten würde, die Umgebung zu erkennen.
Diese Konfiguraton wird als Grundimage verwendet.

2.4. Disassembler

Als Disassembler wurde IDA PRO Free (Version 5.0) verwendet. Diese Version reicht für grundliegende Analysen, jedoch sind die möglichen Anwendungen auf 32-bit begrenzt. Da

Malware jedoch so konzipiert ist, dass ein möglichst breites Spektrum an Geräten angegriffen werden kann, ist diese zumeist ebenfalls 32-bit. Um mit IDA PRO Free 64-bit Malware zu analysieren, ist eine kostenpflichtige Version notewendig. Als Alternative zu IDA PRO Free kann Hopper in Betracht gezogen werden. Hopper gibt es ebenfalls in einer kostenfreien Version, die Stärke liegt jedoch in der kostenpflichtigen Lizenz, welche ähnliche Features bietet wie IDA PRO, jedoch wesentlich billiger und somit auch für Privatpersonen erschwinglich ist. Zudem bietet Hopper den Vorteil, dass es vorgefertige Versionen für Windows, OS X und Linux gibt. IDA Pro (Free) liegt nur für Windows vor, ist jedoch über Wine relativ einfach auf Linux installierbar.

2.5. Weitere Tools

2.5.1. RegShot

2.5.2. Resoucehacker

2.5.3. PEView

2.6. Webseitn

2.6.1. Virustotal

2.6.2. Malwr

3. Infektionsweg

4. Dynamische Analyse

5. Statische Analyse

6. Fazit

A. Appendix

B. Quellcode

C. Ergänzende Grafiken

D. Quellcode Grafiken