HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Juliane Rehfeld

Kategorisierung der Malware

Mittweida, 2017

Fakultät Angewandte Computer- und
Biowissenschaften

BACHELORARBEIT

Kategorisierung der Malware

Autor:
Frau

Juliane Rehfeld

Studiengang:
Angewandte Informatik (spez. IT-Sicherheit)

Seminargruppe:
IF13wl-B

Erstprüfer:
Prof. Dr. rer. nat. Christian Hummert

Zweitprüfer:
Prof. Dr. rer. pol. Dirk Pawlaszczyk

Einreichung:
Mittweida**, 23.08.2017**

Verteidigung/Bewertung:
Mittweida, 2017

Faculty Applied Computer Sciences & Biosciences

BACHELOR THESIS

Categorization of malware

author:
Ms.

Juliane Rehfeld

course of studies:
Applied Computer Science (IT Security)

seminar group:
IF13wl-B

first examiner:
Prof. Dr. rer. nat. Christian Hummert

second examiner:
Prof. Dr. rer. pol. Dirk Pawlaszczyk

submission:
Mittweida, 23.08.2017

defence/ evaluation:
Mittweida, 2017

Bibliografische Beschreibung

Rehfeld, Juliane: Kategorisierung der Malware (Categorization of Malware), 58 Seiten, 8 Abbildungen und Tabellen, keine Anlagen im Quellenverzeichnis, Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften,

Bachelorarbeit, 2017

Referat

Diese Bachelorarbeit beschäftigt sich mit der Kategorisierung der Malware. Dabei werden verschiedene, vorhandene Konzepte vorgestellt sowie ein Eigenkonzept in Hinblick auf die deutsche Gesetzgebung entwickelt. Die Vorstellung von anderen Kategorisierungsmodellen gibt einen kurzen Einblick in das umfassende Thema der Malware-Kategorisierung. Es gibt viele unterschiedliche Konzepte zur Kategorisierung der Malware, jedoch war der Fokus bisher immer auf spezifische Komponenten der Malware selbst gerichtet. Im vorgestellten Eigenonzept zur Kategorisierung der Malware liegt der Fokus auf dem Payload und der Rückkopplung der einzelnen Malware-Typen. Dieses neu geschaffene Kategorisierungsmodell ermöglicht einen anderen Blickwinkel zum Kategorisieren von Schadsoftware, da sich dieses Modell mit den Wirkprinzipien beschäftigt und dabei rechtliche Aspekte mit einbezieht. Mit allgemeinen Definitionen der einzelnen Typen der Malware kann anhand ihrer speziellen Charakteristiken ein grober Überblick über existierende Computerschädlinge geschaffen werden. Um schließlich einen Bezug zur derzeitigen Gesetzgebung herzustellen, werden relevante Gesetze vorgestellt sowie mögliche rechtliche Lücken aufgezeigt.

Abstract

This bachelor thesis deals with the categorization of malware. Various existing concepts are presented, as well as a proposed concept by the author with regard to German legislation. The presentation of other categorization models gives a brief insight into the comprehensive topic of malware categorization. There are many different concepts for categorizing the malware, but the focus has always been on specific components of the malware itself. The concept of categorization of malware proposed by the author is focused on the payload and the feedback of the individual malware types. This newly created categorization model allows a different viewpoint to categorize malicious software, since this model deals with the operating principles and also incorporates legal aspects. With general definitions of the individual types of malware, a special overview of existing computer pests can be provided by means of their specific characteristics. In order to establish a link with the current legislation, relevant laws are presented, as well as possible legal gaps.

Inhaltsverzeichnis

1. Einleitung – Einführung ins Thema

Im allgemeinen Sprachgebrauch wird der Begriff „Virus“ oft als globale Bezeichnung für Schadsoftware verwendet. Dass es sich dabei jedoch „nur“ um einen ganz speziellen Typ handelt, ist vielen unklar. Vielmehr wird er als Synonym für Schadsoftware bzw. Malware generell angewendet. Der Begriff Malware kommt aus dem englischen Sprachgebrauch, da der Großteil an Entwicklungen und Abhandlungen bezüglich Computertechnik und -software nur auf Englisch zu finden ist. Malware ist eine Komposition aus den Worten 'malicious' (Übersetzung: bösartig) und Software. Dieser zusammengesetzte Begriff bezeichnet alle unerwünschten Programme, deren Funktionen störend oder gar schädlich sind. Schaden kann nicht nur durch unwillkommene Veränderung oder Zerstörung von Daten entstehen. Auch die Überlastung eines Systems sowie Datendiebstahl sind schädlich. Was für den einzelnen Privatnutzer nur ein Problem ist, kann für Firmen eine existentielle Bedrohung darstellen. Folglich wurden entsprechende Gesetze und Normen erlassen, so dass die Entwicklung und Verbreitung von Schadprogrammen strafrechtlich geahndet wird.

Die folgenden Kapitel befassen sich mit der Geschichte von Malware, deren Typisierung nach unterschiedlichen Herangehensweisen und der rechtlichen Einordnung der verschiedenen Malware-Typen aus Sicht der Gesetzgebung.

Im ersten Kapitel wird zunächst die Geschichte der Malware und deren Ursprung betrachtet. Einhergehend mit der Entwicklung der Schadsoftware entstanden schon frühzeitig Betrachtungskonzepte zur Unterteilung der Malware nach unterschiedlichen Kriterien. Einige der Konzepte und deren Kriterien werden ebenfalls in Kapitel 1 betrachtet.

In Kapitel 2 erfolgt der Versuch, auf der Grundlage bestehender Konzepte und dem aktuellen Stand der verschiedensten Malwarevarianten eine globale Betrachtung und Typisierung von Malware zu realisieren. Dabei wird auch die Problemstellung der mittlerweile zahlreichen Hybridvarianten berücksichtigt.

Auf der Basis der in Kapitel 2 aufgezeigten Malwaretypen wird im dritten Kapitel eine Kategorisierung anhand der Wirkungs- und Zielrichtung der Schadsoftware aus Sicht strafrechtlicher Tatbestände nach StGB aufgezeigt.

Das vierte Kapitel beinhaltet den wissenschaftlichen Vergleich mit anderen Konzepten

sowie eine Prognose des Alterns vom Eigenkonzept der Kategorisierung der Malware. Darüber hinaus gibt der Ausblick Aufschluss auf die Anwendbarkeit des Konzepts.

1.1 Geschichte der Malware

Wie eingangs erwähnt, wird die Bezeichnung Virus im umgangssprachlichen Gebrauch als Synonym für Malware verwendet. Über die Entstehung dieses Irrglauben kann nur spekuliert werden. Die ersten theoretischen Ansätze für Computerviren sind schon im Jahre 1949 zu finden, wo John von Neumann grundlegende Theorien zur Selbstreplikation von Automaten entwickelte. [GDATA-URL]

Der Begriff Virus im Bezug auf Computertechnik tauchte jedoch erst gut zwanzig Jahre später auf, erstmals in der Kurzgeschichte 'The Scarred Man' von Gregory Benford. [CH-2017-B]

Anfang der 80er wurden die ersten funktionsfähigen Viren und Würmer programmiert, darunter auch ein UNIX Virus von Fred Cohen, einer der Pioniere der Virentechnologie und ein wichtiger Repräsentant der Computerforensik. [Wiki-URL, Fred Cohen]

Cohen hat nicht nur einen Vertreter der ersten Viren entwickelt, sondern auch den Begriff selbst erstmals geprägt. Zu Beginn der Entwicklung von Malware gab es Joke-Programme, um Bekannte zu necken oder kleine Computer-Streiche, die wie digitale Mückenstiche wirkten. Wo solche Software anfangs zum Spaß entwickelt wurde, um den Nutzer mit eher harmlosen Methoden zu belästigen, kamen Mitte der 80er Jahre die ersten bösartigen Schadprogramme zum Vorschein. Trojaner tauchten auf, die sich als angeblich nützlich ausgaben und dann Dateien löschten. Ab Jahr 1987 infizierten immer mehr Viren (auch .COM Dateien) fremde Systeme. Während „Lehigh“ als erster speicherresidenter Virus gesehen werden kann, weil er die „command.com“ infizierte, war „Stoned“ der erste seiner Art, der den Bootsektor befiel.

In den folgenden Jahren steigerte sich die Entwicklung der Malware rasant, sodass immer komplexere Schadprogramme auftauchten und 1989 das erste Virus Kit erschien. Dies ermöglichte es auch jenen mit weniger Kenntnissen Viren zu erstellen. Der erste Cluster-Virus wurde im Jahr 1991 entdeckt. [GDATA-URL]

Michelangelo tauchte kurze Zeit später auf; der erste Virus, der Schlagzeilen machte. Durch die große mediale Aufmerksamkeit, die ihm zuteil wurde, konnte der Schaden

eingegrenzt werden und Virenscanner wurden populärer. [DB-2017-MZ]

Nachdem nun auch die Antiviren-Software immer weiterentwickelt wurde, ließen sich die Programmierer neue Methoden einfallen, um ihre Viren vor Entdeckung zu schützen. So gab es die ersten polymorphen Viren sowie Stealth- und verschlüsselte Viren. Seit 1993 gab es die erste Wildlist, in der kursierende Schadprogramme aufgelistet wurden. Virus Hoaxes wurden verbreitet, deren Falschinformationen als vermeintliche Sondermeldung getarnt waren. Bald darauf, im Jahr 1995, gab es die ersten Makro-Viren, deren Verbreitung unglaublich rasant vonstatten ging. Es wurde immer mehr Malware für spezielle Ziele entwickelt und für illegale Aktivitäten angewendet. [GDATA-URL]

Seit 2004 gibt es auch Malware für andere technischen Geräte als Computer [NB-2014-URL]. So kann heute verschiedenste Technik mit Malware manipuliert, beeinträchtigt und ausgenutzt werden.

1.2 Konzept nach John Aycock

Dieses Kapitel bezieht sich auf die Einteilung der Schadsoftware nach dem von John Aycock geschriebenen Buch „Computer Viruses and Malware“. Der Autor erklärt und definiert die verschiedenen Typen der Malware. Dabei weist er ihnen jeweils drei Eigenschaften bezüglich Selbstreplikation, Populationswachstum und parasitärem Verhalten zu.
Selbstreplikation beinhaltet die selbstständige Verbreitungsweise der einzelnen Malware-Typen. Während Viren, Würmer und Rabbits Kopien von sich selbst erzeugen, um sich so im Netz zu verbreiten, werden Trojaner, Spyware und Co. durch Computernutzer heruntergeladen. Das Populationswachstum ist abhängig von der Selbstreplikation. Verbreitet sich die Malware nicht von selbst, so ist das Populationswachstum gleich null, da die Zahl der Kopien nicht ohne das Zutun eines Anwenders wächst. Jedoch ist es möglich, dass selbstreplizierende Malware ebenfalls ein Populationswachstum von null vorweist. Die dritte Kategorie zur Einteilung bestimmt das parasitäre Verhalten. Wenn ein Schadprogramm als parasitär klassifiziert wird, bedeutet dies, dass diese Malware abhängig von einem anderen Programm, Skript, Datei oder anderen ausführbaren Daten auf einem Computersystem ist. Es wird ein Wirt benötigt. Es gibt Typen, bei denen ein parasitäres Verhalten möglich ist, jedoch nicht zwingen bestehen muss. Das sind unter anderem Logic Bombs und Backdoors. [JA-2006-B; S. 24ff]

Zu jedem einzelnen Malware-Typ, den der Autor vorstellt, gibt er an, wie die bestimmten Eigenschaften auf den Typ zutreffen. Dabei beschreibt er die reine Grundform der ausgewählten Malware. Folgende Übersicht beinhaltet diese Typen:

Name	Beschreibung	Selbst-replikation	Populations-wachstum	Parasit
Logic Bomb	Besteht aus Payload und Trigger	nein	nein	evtl.
Trojaner	Gibt vor, gutartig zu sein, hat jedoch bösartige Hintergrundfunktion(en)	nein	nein	ja
Back Door	Mechanismen, die ermöglichen normale Sicherheitskontrollen (z.B.: Passwort) zu umgehen Spezialfall: RAT	nein	nein	evtl.
Virus	Verbreitet sich durch Infektion anderer Programme	ja	ja	ja
Wurm	Braucht keinen Wirt, verbreitet sich im Netzwerk	ja	ja	nein
Rabbit	Zwei Typen: → (Bacteria) verbreitet sich rasend schnell, um Ressourcen zu verschwenden → (Subtyp Wurm) verbreitet sich als einzelne Kopie	ja	nein	nein
Spyware	Sammelt Informationen und verschickt sie	nein	nein	nein
Adware	Blendet personalisierte Werbung ein, mithilfe gesammelter Informationen	nein	nein	nein

Tabelle 1: Eigenschaften einzelner Malware Typen [E]

Weiterhin werden Dropper, Blended Thread und Zombies erwähnt, jedoch nicht mit den drei Hauptkategorien in Verbindung gebracht.

Aufgrund der vielfältigen Freiheit des Programmierens entstehen sehr leicht Hybride, die mit mehreren Kategorien identifiziert werden können. Das macht eine eindeutige Klassifikation nahezu unmöglich.

Neben der allgemeineren Klassifikation spezialisiert sich der Autor auf den Malware-Typ Virus. Was sie alle gemeinsam haben ist der Aufbau, bestehend aus Infektionsroutine,

Trigger und Payload. Es werden verschiedene Ziele und Verschleierungstaktiken von Viren vorgestellt. Als Ziele sind dabei nicht die Funktionen gemeint, sondern der Ort der Infektion. So infiziert ein BSI (Boot-Sector Infector) den Boot-Sektor wenn der Computer startet und ein File Infector verseucht Executables während der Laufzeit des Geräts. Executables sind Programme und Dateien, die ausgeführt werden können. Sie unterscheiden sich von Data Files in der Hinsicht, dass letzteres keinen ausführbaren Programmcodes darstellt. Sie werden nicht gestartet und haben auch keine eigenhändige Funktionen. Stattdessen enthalten sie Informationen, die von anderen Programmen interpretiert bzw. gelesen werden. Die dritte Virenkategorie, die unter anderem Makros infiziert, wird entsprechend als Makro-Virus bezeichnet. Dazu gehören beispielsweise die Macro-Dateien von den Microsoft Office Programmen. Jedoch infiziert diese Art Virus nicht nur Makros, sondern auch die genannten Data Files. Das Kapitel, das Verschleierungstaktiken behandelt, zeigt auf, welche Methoden Schadprogramme nutzen, um sich vor normalen Computernutzern und Antiviren-Software zu verstecken.

- *Viren ohne jegliche Tarnung* sind zwar verhältnismäßig einfach zu schreiben, aber da sie keine zusätzlichen, komplizierten Schutzmechanismen beinhalten, werden sie sehr schnell entdeckt.
- Deshalb werden sogenannte *verschlüsselte Viren* mit einer Verschlüsselung versehen. Dazu zählen sowohl Viren, die ihren eigentlichen Code durch Verschleierung verbergen und damit die Entdeckung erschweren, als auch Viren, die ihren Code durch kryptografische Verschlüsselung unkenntlich machen. Die Methoden reichen von simplen Veränderungen, wie der Verwendung des logischen NOT oder XOR, über einfache Schlüssel bis hin zu komplexen Chiffren.
- Im Gegensatz dazu wird bei *Stealth-Viren* nicht darauf geachtet, wie gut der Code des Virus verborgen wird, sondern wie seine Existenz selbst bestmöglich zu verbergen ist. Dabei werden beispielsweise Zeitstempel, die durch die Infektion aktualisiert wurden, auf einen Zeitpunkt vor der Infektion zurückgesetzt.
- *Verschlüsselte Viren* sind nicht direkt ausführbar. Zur Ausführung kommt zunächst nur der Teil, der die Entschlüsselung des eigentlichen Codes des Virus vornimmt. Dieser sogenannte Decryptor ist deshalb eine Schwachstelle, da sein unverschlüsselter Code von Virenscannern erkannt werden kann.
- *Oligomorphische Viren* sind verschlüsselte Viren, deren Decryptor sich in jeder neuen Generation verändert und somit eine Detektion erschwert. Eine simple Methode dabei ist

eine sich wechselnde Auswahl aus mehreren Decryptions-Routinen.

- Wenn die Anzahl der Decryptor-Variationen so groß ist, dass sie unter praktischen Aspekten als unbegrenzt betrachtet werden kann, spricht man von *Polymorphen Viren.*

- *Metamorphe Viren* sind unverschlüsselt. Der Schutz vor Entdeckung basiert auf der Generierung jeweils modifizierter (mutierter) Varianten. Diese Mutationen machen den Virus unberechenbar. Nicht nur dadurch, dass völlig neue Variationen entstehen, sondern auch unerwartete Wirkungen. Wirtsprogramme können dabei erheblichen Schaden davontragen.

- Inzwischen existieren auch sogenannte *Virus Kits*. Das sind von erfahrenen Programmierern entwickelte Viren-Baukästen, die es gegen Bezahlung auch unerfahrenen Programmierern ermöglichen, komplexe Viren zu generieren. Diese Programme erstellen automatisch Programmcode für ein vollständiges Virus bzw. Teile davon auf Grundlage vorgegebener Einstellungen, die der Anwender vorgenommen hat.

[JA-2006-B]

1.3 Konzept nach Christian Hummert

Das folgende Kapitel bezieht sich auf Kapitel 7 des Buches „Malware Forensics“ von Christian Hummert. Hier wird eine andere Art der Einteilung der Malware beschrieben. Signifikant für dieses Konzept ist eine zweigeteilte Kategorisierung. Zum einen wird die Malware differenziert durch ihre Verbreitungsfunktion und zum Zweiten nach dem Payload. Wortwörtlich aus dem Englischen übersetzt heißt 'payload' Nutzlast oder Fracht. Damit ist der Teil des Schadprogramms gemeint, der die eigentlichen Zielstellungen der Malware beherbergt. Damit ist also unter anderem der Schadcode gemeint.

Nach Hummert gibt es vier verschiedene Verbreitungstypen: Virus, Wurm, Trojaner und Rabbit.

Die Vermehrung eines *Virus* findet durch Infektion statt. Wie bei den biologischen Namensvettern brauchen auch die Computerviren einen Wirt, um sich zu verbreiten. Dabei ist es möglich, dass diese ihre Wirtsprogramme verändern oder gar schädigen. Es gibt verschiedene Methoden, wie sich ein Virus an ein Programm anhängen kann. So kann es beispielsweise das infizierte Programm überschreiben und durch den eigenen Code ersetzen, oder aber mithilfe von Sprungbefehlen vom Wirtsprogramm zum Virus-Code wechseln.

Während ein Virus sich mithilfe anderer Dateien und Programme reproduziert, ist der

Wurm selbstständig unterwegs. Würmer verändern keine fremden Dateien, um sich zu verbreiten, sondern verschicken Kopien von sich selbst.

Der Subtyp *Rabbit* ist eine Art Wurm, die sich, statt viele Kopien seiner selbst zu erzeugen, nur als einziges Exemplar verbreitet. Dabei erstellt das Original eine Kopie und verschickt diese, um sich dann selbst zu löschen bzw. von der Kopie gelöscht zu werden. Dieses Spiel wiederholt sich dann immer weiter und lässt so den Rabbit von System zu System springen.

Trojaner sind Programme, die sich als nützliche Anwendung tarnen, jedoch im Hintergrund schädliche Zusatzfunktionen ausführen. Sie verbreiten sich nicht selbst, sondern werden von Nutzern verteilt. Ihre Hauptfunktion ist vor allem das Verschleiern der eigenen Schadfunktion, damit der Trojaner freiwillig auf das eigene System geladen wird. Schließlich will keiner ein Programm benutzen, von dem er weiß, dass es Malware ist.

Teil zwei der Einteilung ist das Kategorisieren nach der Wirkung des Programms. Es werden neun verschiedene Wirkungs-Typen vorgestellt, die mit den Verbreitungsarten verbunden werden.

Logic Bombs sind Programme, deren Payload erst durch einen sogenannten Trigger aktiviert wird. Das kann beispielsweise ein Datum sein, oder auch das Starten eines bestimmten Programms.

Eine *Backdoor* (übersetzt: Hintertür) funktioniert ihrem Namen entsprechend. Diese Art Malware ermöglicht den unautorisierten Zugriff auf ein fremdes System. Mit diesem Computerprogramm können Schutz- und Sicherheitsmechanismen, unter anderem auch Firewalls, umgangen werden.

Die sogenannte *Bakterie* (engl. Bacteria) ist ein Programm, dass schadet, indem es Ressourcen verbraucht. Dabei wird eine enorme Anzahl an Exemplaren oder Instanzen seiner selbst gestartet. Diese Mengen an unnötig laufenden Prozessen beeinträchtigen damit andere wichtige Prozesse bzw. die Performance des Gerätes. Aber auch andere Systemressourcen können dadurch beeinträchtigt werden, wie beispielsweise der Festplattenspeicher.

Als *Spyware* werden Programme bezeichnet, die heimlich gegen die Interessen des Anwenders persönliche Informationen an Dritte übermitteln. Das können unter anderem Bankdaten (PIN, TAN, etc.) oder Passwörter sein.

Ähnliche Programme gibt es auch, die persönliche Daten auswerten und entsprechend

unerwünschte Werbung einblenden. Diese Malware wird *Adware* genannt.
Sogenannte *Ransomware* kann einzelne Daten oder ein gesamtes Computersystem beschränkt nutzbar oder unzugänglich für den Benutzer machen. Eine weit verbreitete Methode ist dabei das kryptografische Verfahren der Verschlüsselung.
Bots sind Programme, die Rechner infizieren und sich unbemerkt mit anderen Computern vernetzen. Das gebildete Netz verwendet die Ressourcen der gekaperten Rechner, um beispielsweise Spam in Massen zu versenden, DDoS-Attacken durchzuführen oder mittels Bitcoin Mining Gewinne zu erzeugen.
Neben der üblichen Malware, die die Software eines Systems angreift, gibt es auch *Hardware Damaging Malware*. Diese greift Hardwarekomponenten an, indem sie unter anderem Einstellungen ändert und Hardware- Schutzmechanismen deaktiviert, direkt oder durch Betrieb in unzulässigen Zuständen indirekt deaktiviert oder zerstört. (z.B. durch Überlastung von Festplatten).
Dropper sind Programme, die andere Schadprogramme herunterladen und ausführen.
[CH-2017-B]

1.4 Konzept nach Peter Szor

Im Konzept des Buchs „The Art of Computer Virus Research and Defense“ von Peter Szor werden verschiedene Malware-Typen vorgestellt und definiert. Der Begriff Virus wird dabei besonders ausführlich erklärt. Nach Dr. Cohens Auffassung ist ein Virus „ein Programm, das andere Programme durch Modifikation infizieren kann, sodass diese eine eventuell weiterentwickelte Kopie seiner selbst einschließen“[1] [PS-2005-B; Zitat von Fred Cohen; Seite 18]. Jedoch beinhaltet diese Definition keine Companion Viren, da diese den Programmcodes eines anderen Programms nicht modifizieren müssen, um sich zu verbreiten, sondern in deren Umgebung eingreifen. Um diese Art Virus ebenfalls in der Definition zu berücksichtigen, verändert der Autor Cohens Definition dahingehend, dass ein Virus sich selbst in rekursiver Form kopiert, um etwaig weiterentwickelte Kopien zu erstellen. Dabei muss der Virus also nicht unbedingt von einem Wirtsprogramm eingeschlossen werden.
Weitere Malware-Typen werden unterschieden:
Würmer sind Viren, die sich über Netzwerke verbreiten. Sie können sich sowohl ohne das Zutun eines Nutzers als auch über beispielsweise Emails verbreiten. Ein Virus, dessen

1 Freie Übersetzung

Hauptfunktion bezüglich der Verbreitung darin besteht, Netzwerke zu infiltrieren, sollte hiermit als Wurm gelten.

Mailer und *Mass-Mailer-Würmer* sind Untertypen des Wurms. Ihre Verbreitung geschieht durch Email-Verkehr. Sie hängen sich an eine Email und verschicken sich so selbst. Der Unterschied zwischen einem Mailer und einem Mass-Mailer-Wurm ist die Menge der versendeten Emails. Ein bekanntes Beispiel für diese Art Malware ist der Loveletter.

Der *Octopus* stellt ebenfalls einen Untertypen des Wurms dar. Dabei gibt es mehrere Programmteile, die sich auf verschiedenen Computern befinden und miteinander kommunizieren. Mit der Verbindung können die Teile des Octopus eine gemeinsame Funktion erfüllen.

Als *Rabbit* werden Würmer bezeichnet, die nur eine einzelne Kopie von sich erzeugen und das Original dann löschen. Des Weiteren gilt diese Bezeichnung auch für Malware, die sich auf einem einzelnen System vermehrt, um die Performance des Rechners negativ zu beeinflussen.

Eine *Logic Bomb* ist eine Fehlfunktion, die absichtlich in ein bestimmtes Programm eingefügt wurde. Ein bekannter Vertreter dieser Malware war in dem Spiel „Mosquitos“ zu finden, das auf Nokias der Serie 60 installiert war. Aktiviert hat sich die Schadfunktion, als das Spiel gestartet wurde. Dabei wurde eine SMS an eine teure Nummer versandt., sodass dem Nutzer ein finanzieller Schaden entstand.

Trojanische Pferde sollen den Nutzer mit ihren scheinbar nützlichen Funktionen ansprechen, sodass dieser sie freiwillig startet. Ferner gibt es auch echte Tools, die zusätzlich mit schadhaften Funktionen ausgestattet sind.

Eine Backdoor (Trapdoor) ermöglicht dem Angreifer Fernzugriff auf ein fremdes System.

Password-stealing Trojans sind Untertypen des Trojanischen Pferds. Ihre Funktion besteht darin, Passwörter zu stehlen, um sie dem Entwickler zukommen zu lassen, sodass dieser die Passwörter missbrauchen kann.

Germs (übersetzt: Keime) sind Viren in ihrer Ursprungsform. Anders als die Folgegenerationen hat diese erste Generation nicht dieselbe Infektionsroutine und im Normalfall keinen Wirt. Im Allgemeinen sind Germs von Polymorphen oder Verschlüsselten Viren in Klartext-Form zu finden.

Sogenannte *Exploits* sind auf eine bestimmte Schwachstelle spezialisiert. Mithilfe eines solchen Exploits kann der Angreifer durch bestimmte Sicherheitslücken in ein fremdes System eindringen und sich dort Zugriff auf die Daten verschaffen. Neben den

unrechtmäßigen Einbrüchen in fremde Computersysteme, gibt es auch das gewünschte Ausnutzen von Exploits. Diese werden Penetrationstests genannt und haben den Nutzen, dass Schwachstellen entdeckt und geschlossen werden können.

Mit einem *Downloader* wird weitere Malware heruntergeladen sowie installiert und gestartet.

Dialer dienen dazu, um eine kostenpflichtige Verbindung zwischen Opfersystem und einer Premium-Telefonnummer herzustellen. Mit diesem Vorgehen will sich der Angreifer ohne das Wissen des Opfer finanziell bereichern. Neben Telefonverbindungen funktioniert diese Methode unter anderem auch im Internet mit kostenpflichtigen Seiten und Diensten, die unbemerkt in Anspruch genommen werden.

Als *Dropper* werden Programme bezeichnet, die einen inaktiven Virus zum ersten mal installieren und starten.

Ein spezieller Typ des Droppers ist der *Injector*. Diese Sonderform installiert den Virus insbesondere im Computerspeicher.

Auto-Rooter sind Tools, deren Funktion darin besteht, sich root-Rechte zu beschaffen und dem Angreifer entsprechend administrative Rechte zu verleihen.

Mit sogenannten *Kits (Virus Generators)* kann ein Virus per Mausklick erschaffen werden.

Spammer- Programme werden dazu verwendet, um Spam zu verbreiten. Dabei können diese Spam-Nachrichten als unerwünschte Werbung dienen, damit Nutzer bestimmte Webseiten besuchen, aber auch um Phishing zu betreiben.

DoS-Attacken werden durch sogenannte *Flooder* ermöglicht. DoS bedeutet Denial of Service (übersetzt: Verweigerung des Dienstes). Wenn eine Vielzahl an Anfragen bei einem Server eingeht, so kann es passieren, dass der Server irgendwann überlastet und der Dienst blockiert wird. Kommt diese übermäßige Menge an Anfragen von mehreren infizierten Systemen, sogenannten Zombies, spricht man von DDoS (Distributed Denial of Service).

Keylogger werden unter anderem dazu verwendet, um Identitätsdiebstahl zu begehen. Dabei werden Tastatureingaben aufgezeichnet, sodass dadurch Passwörter und persönliche Daten aufgegriffen werden können.

Rootkits bezeichnen Hacker Tools, die ein Angreifer auf einem fremden System installiert, nachdem er dort Root-Rechte erlangt hat. Es werden zwei Typen unterschieden, Rootkis im User-Mode und im Kernel-Mode. Während Rootkits im User-

Mode sich selten vor Antiviren-Software in Kernel-Mode schützen kann, da sie nur User-Mode-Applikationen nutzen können, können sich Rootkits der zweiten Variante sich effektiv verbergen. Entsprechend sind sie gefährlicher.

Abschließend werden weitere Schädlinge aufgelistet, die nach Szor nicht zwingend unter den Begriff Malware fallen: *Joke Programme*, *Hoaxes* (Chain Letters), *Adware* und *Spyware*.

Bevor der Autor die Klassifikation vornimmt, zeigt er auf, wie und wo Malware agiert, um ein grundlegendes Verständnis zu schaffen. Die Abhängigkeiten von verschiedenen Parametern sind ausschlaggebend für die Verbreitung und Funktionstüchtigkeit eines Schadprogramms. So kann sich beispielsweise ein Virus, dass in den 90er Jahren entstanden ist, heute kaum mehr verbreiten, weil die Technik viel zu sehr vorangeschritten ist. Es würde wahrscheinlich sogar überhaupt nicht mehr funktionieren. Bestimmte Anwendungsprogramme (wie Treiber) oder System Files, die früher von Malware infiziert wurden, wurden heute möglicherweise durch andere Programme und Systemkomponenten ersetzt, sodass die entsprechenden Schädlinge gar nicht mehr aktiviert werden können. So, wie sich Sprachen mit der Zeit ändern, verändern sich auch Programmiersprachen und ihre Compiler, sodass Code, der früher einwandfrei lief, heute nicht mehr ohne Fehlermeldungen ausgeführt wird. Auch spielen Betriebs- und Dateisysteme eine große Rolle in der Funktionalität von Malware.

Mit dem Verständnis, von welchen Umgebungen und Abhängigkeiten die Lauffähigkeit der Malware abhängt, wird im Folgekapitel des Buchs erläutert, welche Ziele überhaupt in Angriff genommen werden.

Bootviren gehören zu den ältesten Viren, die durch ihren „Erfolg“ bekannt geworden sind. Sie können einen Computer unabhängig vom Betriebssystem infizieren.

Neben der Infektion des Boot-Sektors, gibt es File Infection Techniken, bei denen der Virus Dateien angreift.

Weiterhin gibt es Methoden für Malware, um resident im Speicher zu bleiben. Diese beschriebenen In-Memory-Strategien beinhalten unter anderem die Manipulation von Interrupts, Hook Routinen das aktive Verstecken sowie das Ausnutzen von Programmen zum Verschleiern und weitere.

Nachdem letztlich Selbstschutzmechanismen, wie Verschlüsselung, Manipulation von Checksummen und Antidebugging-Techniken, ausführlich beschrieben und erklärt werden, kommt es zur Klassifizierung der Malware nach Payload. Dabei werden folgende

Typen unterschieden:

No-Payload bedeutet, dass der Virus keine wirkliche Schadensfunktion beinhaltet. Dazu zählen unter anderem Viren, die allein durch ihre Replikation gewissen Ärger verursachen.

Mit Accidentally Destructive Payload sind Viren gemeint, die durch ihre Verbreitung mehr Schaden anrichten, als geplant. So hat beispielsweise Stoned den Originalen Boot-Sektor an einer anderen Stelle gespeichert, bevor es sich selbst dort hineingeschrieben hat. Ein unerwarteter Mehrschaden entstand, wenn das Root-Verzeichnis der infizierten Diskette zu viele Verzeichniseinträge besaß. Der Grund dafür war, dass Stoned den Boot-Sektor am Ende von root speichert und dabei durch Platzmangel einfach andere Verzeichnisse überschreibt.

Zur Zeit, als das Buch geschrieben wurde, zählten knapp die Hälfte aller Viren zur Kategorie *Nondestructive Payload*. Der Grund, dass eine so erhebliche Menge aus dieser Kategorie kursierte, liegt daran, dass damals die Programmierer mehr politisch orientiert waren und ihre Meinung kundtun wollten.

Somewhat Destructive Payload beinhaltet „milde“ Angriffe durch Viren. Diese Angriffe sind zwar lästig, aber behebbar. Selbst wenn „nur“ die Antiviren-Software angegriffen wird, sind persönliche Daten relativ sicher.

Zu der Kategorie *Highly Destructive Payload* zählen Viren, die andere Daten überschreiben, verschlüsseln und gar zerstören. Weiter gehören dazu auch Viren, die Hardware zerstören und sogenannte Data Diddlers. Der Begriff „Data Diddler“ wurde von Yisrael Radai geprägt und beschreibt Malware, die ein System langsam korrumpiert. Durch den langsamen Prozess der Zerstörung, wird diese Art recht spät entdeckt, sodass selbst zeitige Backups schon verseucht sein können.

Unter der Überschrift DoS Attacks stehen Malware-Vertreter, deren Funktion darin besteht, DoS-Angriffe durchzuführen.

Mit den *Data Stealers* wird auf die finanzielle Bereicherung abgezielt. Dabei werden persönliche Daten, wie PIN und Bankdaten, beschafft und missbraucht, um unrechtmäßig an Geld zu kommen. Dazu gehören unter anderem Phishing Attacken und Backdoors.

[PS-2005-B]

2. Methoden – Malware und ihre Besonderheiten

Im folgenden Kapitel werden die einzelnen Typen der Malware und ihre charakteristischen Merkmale vorgestellt. Dabei werden unter anderem Beispiele zur Veranschaulichung hinzugezogen.

2.1 Virus

Fast alle Quellen stimmen darin überein, dass ein Virus Wirtsprogramme infiziert und dabei eine Kopie von sich selbst erzeugt [JH&JS-1997-URL], [FC-1984-URL]. Viren beinhalten einen Schadensteil (Payload), eine Infektionsroutine und einen Auslöser (Trigger). Durch den Trigger wird der eigentliche Payload, dessen Inhalt die Schadfunktion des Virus' bestimmt, erst aktiviert. Mit der Infektionsroutine stellt der Virus sicher, dass er sich immer weiter verbreiten kann. Es ist denkbar, dass es auch Viren gibt, die einzig und allein eine Vermehrungsfunktion besitzen.

Es gibt verschiedenste Arten von Viren und deren Verbreitungsmethoden. Folgend werden die wichtigsten Vertreter aufgelistet und beschrieben.

Bootviren befallen den Bootsektor verschiedenster Medien, wie Festplatten, USB-Sticks oder bootfähige Disketten, können aber auch auf CDs und DVDs enthalten sein. [FS-URL] Noch bevor das Betriebssystem gestartet wird, wird der Bootvirus aktiv.

Ein *Linkvirus* infiziert auf dem Opfer-System laufende Programme, um deren Startroutine zu verändern. Damit kann der Virus sicherstellen, dass er beim nächsten Programmstart ebenfalls gestartet wird. Zu solchen Wirtsprogrammen gehören auch Treiber und Anwendungssoftware. [SDUG-URL, Linkviren]

Persistente Daten können von sogenannten *Dateiviren* befallen werden. Dabei wird der Virus zum Bestandteil der befallenen Programmdateien und wird dadurch bei jeder Ausführung des Programms aktiviert. Im Regelfall versuchen derartige Viren den Schaden am Wirt zu minimieren, um die Entdeckungsgefahr (z.B.: durch verursachte Programmfehler) zu verringern. [SDUG-URL, Dateiviren]

Makroviren verhalten sich wie Makros und werden daher nur von Programmen ausgeführt, die Makros verwenden. Ein Makro ist ein Unterprogramm oder eine Befehlssequenz, die eine bestimmte, wiederkehrende Funktion beinhaltet. Sie ist nicht

direkt im Hauptteil des Programmcodes eines Programms integriert, sondern wird als separater Programmstreifen von ebendiesem aufgerufen. Dadurch können Anweisungen variabel durchgeführt und so auch entsprechende Viren verbreitet werden. [SDUG-URL, Makroviren]

Ein *Script-Virus* beschreibt einen Computervirus, der sich über Scripte verbreitet. Das sind vor allem HTML-Seiten, aber auch Anwendungen, die in Java Script geschrieben sind. Prinzipiell kann man hier alle Arten von Interpretern betrachten, die in Textform vorliegende Befehle in Programmcode umsetzen. So sind unter anderem Script-Viren in Basic-, Batch-, oder WSH-Dateien (Windows Scripting Host) denkbar. [SDUG-URL, Script-Viren]

Neben Dateien und Programmen, können auch Verzeichnisse infiziert werden. Besonders bei UNIX-basieren Betriebssystemen sind Verzeichnisse ein vertrautes Ziel, da sich diese ähnlich der üblichen Dateien verhalten. Viren mit einem solchen Angriffsziel werden *Verzeichnis-Viren* oder *DIR-Viren* genannt. [SDUG-URL, Verzeichnis-Viren]

Die betagten *Slack-Viren*, die schon in den 80er Jahren um sich griffen, infizierten damals, wie heute, den Slack. So wird der freie Speicherplatz in einem Datenblock (auch Cluster) auf Datenträgern genannt. Nicht zu verwechseln mit dem Stack von Programmen, der einen Speicherbereich im Hauptspeicher darstellt. [SDUG-URL; Slack-Viren]

Durch die vielfältigen Komponenten eines Rechnersystems, sind die Möglichkeiten der Infektion schier unendlich. Dementsprechend gibt es unzählige Varianten von Viren und deren Infektionsroutinen.

Bekannte Vertreter von Viren sind unter anderem Elk Cloner, der erste bekannte Computervirus, sowie Melissa und Loveletter, zwei bekannte Makroviren. [GDATA-URL, Geschichte]

2.2 Trojaner

Signifikant für Trojaner oder auch Trojanische Pferde ist deren Methode, sich durch Täuschung zu verbreiten; ihrem Namensgeber entsprechend. In der griechischen Mythologie war das Trojanische Pferd eine Kriegslist von Odysseus, damit die Griechen die Stadt Troja einnehmen konnten. Dabei bauten sie ein großes, hölzernes Pferd, um es den Trojanern als vermeintliches Geschenk zu übergeben. Jedoch versteckten sich in

dessen Inneren Soldaten, die dann in der Nacht die Stadttore öffneten und Troja somit der griechischen Armee auslieferten. [SS-URL]

Ein Trojaner, bezogen auf die Computertechnik, ist also ein Programm, dass vorgibt, ein nützliches oder harmloses Programm zu sein, jedoch im Hintergrund unerwünschten Payload ausführt. [SM-2016-URL]

2.3 Dropper

Da sich Viren nicht selbstständig verbreiten können, brauchen sie ein Wirtsprogramm. Dropper sind Programme, die einem (noch) inaktiven Virus als Übertragungswirt dienen und ihn aktivieren. [SM-2016-URL]

In weiterer Definition haben Dropper auch die Funktion, weitere (zum Teil zahlreiche, verschiedene) Viren und Malware herunterzuladen [CH-2017-B].

Sasser gilt zwar als Wurm, jedoch zeigt seine Funktionsweise das Verhalten eines Droppers nach weiterer Definition. So nutzt Sasser eine Sicherheitslücke im Windows-System, baut jedoch erst eine Verbindung zu einem Server auf, um den eigentlichen Schadcode herunterzuladen und den Rechner zu infizieren.

2.4 Ransomware

Der Begriff 'ransom' als Übersetzung für Lösegeld deutet schon an, um was für ein Typ Malware es sich handelt. Ransomware ist Schadsoftware, die durch Verschlüsselung, Verwürfelung oder anderweitig die Daten auf dem Rechner des Opfers unzugänglich für den Nutzer macht. Der Nutzer des Computers wird dazu veranlasst, einen Geldbetrag zu überweisen, um die Daten in den ursprünglichen Zustand zu versetzen. Jedoch ist selbst das Überweisen des geforderten Betrags keine Garantie, dass der infizierte Rechner wieder freigegeben wird. [SM-2016-URL]

Unter anderem wird Ransomware auch als Erpressungstrojaner bezeichnet, da Ransomware wohl zumeist auf die Verbreitungsmethode eines Trojaners zurückgreift.

Goldeneye, Petya und Mischa sind Begriffe, die man nicht unbedingt zuerst mit Erpressungstrojanern verbindet. Vielmehr scheinen die Namensgeber ihre Inspiration in James-Bond-Filmen gefunden zu haben. Angelehnt an den 17. Teil („Goldeneye“) der James-Bond-Reihe wurden diese Erpressungstrojaner scheinbar nach den zwei Satelliten

Mischa und Petya benannt, die zu dem russischen Waffensystem „GoldenEye“ gehören. [JB_Wiki-URL, Goldeneye]

Alle drei Begriffe bezeichnen Ransomware, die 2016 ihr Unwesen trieb. Durch die Ähnlichkeit untereinander konnte man schon damals vermuten, dass sie wohl von den selben Entwicklern erschaffen wurden. Mittlerweile wurde ein Entschlüsselung-Key veröffentlicht, sodass die Opfer dieser drei Schädlinge wieder auf ihre Computer und Festplatten zugreifen können. [DS-2017-URL]

2.5 Wurm

Würmer sind Computerprogramme, die sich selbst in einem Netz verbreiten können. Dazu benötigt ein Wurm keine Wirtsprogramme, sondern verwendet Sicherheitslücken und schreibt sich in Systemroutinen. [PS-2005-B]

Eine Unterart ist der *Rabbit*, der sich „springend“ fortbewegt, indem er wiederholend eine Kopie von sich selbst erstellt und das vorherige Original löscht.

2.6 Bakterie

Ähnlich der Vermehrung einer biologischen Bakterie brauchen auch *Computerbakterien* keinen Wirt für ihre Verbreitung. Entsprechend ihres Namensgebers vermehren sie sich exponentiell, indem jede Instanz weitere Instanzen oder Kopien von sich selbst erzeugt. Grundsätzlich kann man die Bakterie mit Würmern vergleichen, da sie sich ebenfalls selbst repliziert. Jedoch liegt der Unterschied hier in den Auswirkungen. Während der Wurm das Ziel der möglichst weiten Verbreitung im Netz beabsichtigt, verbreitet sich die Bakterie auf einem einzelnen System, um diesem wichtige Ressourcen und Speicherplatz zu entziehen. Dabei sind unter anderem auch nur lokale Instanzen der Bakterie nötig, während der Wurm Kopien seiner selbst auf anderen Systemen erstellt. [CH-2017-B]

Die Bakterie wird wegen vergleichbarer Reproduktionsraten oftmals auch als *Rabbit* (übersetzt: Kaninchen) bezeichnet. Man muss hier jedoch die abweichende Bedeutung zum gleichnamigen Spezialfall des Wurms beachten. Im UNIX-Bereich findet auch der Begriff *Fork-Bomb* Anwendung. [Wiki-URL; Forkbomb]

2.7 Backdoor

Es gibt viele Sicherheitslücken, deren Entstehung nicht beabsichtigt ist oder die übersehen wurden. Jedoch gibt es auch Softwareentwickler, die absichtlich versteckte Zugänge in ein System einbauen. Diese Sicherheitslücken werden Backdoors genannt. Der Begriff Backdoor kommt aus dem englischen Sprachgebrauch und bedeutet übersetzt Hintertür. Dadurch können andere Schadprogramme in das System eindringen, wobei Passwörter sowie Firewalls und andere Zugangssicherungen umgangen werden können. [SM-2016-URL]

2.8 Rootkit

Rootkits sind Werkzeuge zum Verschleiern von unerwünschten Prozessen und Dateien, insbesondere das Verstecken anderer Malware, sodass ein Antivirenprogramm diese nicht entdeckt. Diese Schadsoftware kommt von außen ins System und installiert sich selbst auf dem Rechner (oder wird installiert). Der Begriff Rootkit bezieht sich auf die administrativen Rechte eines Root-Kontos bzw. des Hauptverzeichnisses (/root) eines Unix-basierten Systems. Root-Rechte werden auch als Administratorrechte bezeichnet, da der Besitzer entsprechend auf alles Zugriff hat. Nachdem ein Computersystem mit einem Rootkit infiziert wurde, kann der Angreifer ohne Probleme darauf zugreifen, da das Programm ihm diese Rechte freigibt. [SM-2016-URL]

2.9 Bot

Botnetze (oder Botnets) entstehen durch den Zusammenschluss von vielen einzelnen Computern, ohne das Zutun der eigentlichen Nutzer. Diese missbrauchten Rechner wurden von sogenannten Bots (Abk. für 'Robot') infiziert, die dem Netz dann Ressourcen und den Zugriff auf das infiltrierte System freigeben. [GDATA-URL, Botnet] Der Urheber dahinter, der die gekaperten Rechner letztendlich missbraucht, heißt Botmaster.

Anders bekannt ist diese Art Malware auch unter dem Namen Zombie. Es ist jedoch hierbei zu beachten, dass diese Bezeichnung auf die gekaperten Rechner zutrifft, nicht auf das Programm, das dies verursacht.

Man kann den nach Szor definierten Begriff des Octopus auch als Bot bezeichnen, da Bots ebenfalls über ein Netz kommunizieren und gemeinsame Funktionen erfüllen.

Mit bestimmten Bots ist es unter anderem möglich, Bitcoins zu generieren, da dies mit Rechenarbeit verbunden ist. Je mehr Rechenleistung ein sogenannter Bitcoin-Miner zur Verfügung hat, umso schneller kann er mithilfe dieser Kapazitäten erforderliche Rechnungen lösen, um zur Belohnung Bitcoins zu erhalten. Ausgenutzt haben dieses Verfahren zwei deutsche Männer indem sie mit einem modifizierten Trojaner fremde Computer infiziert und so ein Botnetz erschaffen haben. Durch diesen Zusammenschluss von vielen Rechnern konnte entsprechend eine hohe Summe an Bitcoins generiert werden. Letztendlich wurden die beiden erwischt und verhaftet. [TB-2013-URL]

2.10 Spyware

Unter dem Begriff Spyware versteckt sich jegliche Malware, die zum Ausspionieren von persönlichen Daten genutzt wird. Dazu zählen auch Keylogger, deren Funktion es ist, Tastatureingaben aufzuzeichnen. [SM-2016-URL]

Anzumerken ist, dass Keylogger dabei nicht nur als Softwarevariante existieren, sondern auch in Form von Hardware, wie USB-Sticks, zu finden sind.

2.11 Adware

Oftmals dringt Adware unbemerkt in das System, wenn andere, meist nützliche Programme heruntergeladen und installiert werden. Adware wird neben der unerfreulichen Malware auch als legitime Werbung betrachtet, die mit einer gekauften Software oder Freeware zusammen auf das System gelangt. Auch der Begriff „Adware“ ist ein zusammengesetztes Wort aus dem englischen Sprachraum, bestehend aus 'ad' von 'advertisement' („Werbung“) und Software. Die definierende Funktion dieser Malware ist es, Werbung in Form von Pop-Up Fenstern oder anderen Werbemethoden einzublenden. [SM-2016-URL]

Neben dieser offensichtlichen Funktion, kann Adware aber auch eine Form von Spyware sein. Um personalisierte Werbung einblenden zu können, werden vorher die persönlichen Daten und/oder das Nutzerverhalten auf dem Rechner ausgelesen und ausgewertet. Das System wird also ausspioniert, um die Reklamen benutzerspezifisch anzupassen.

2.12 Hardware Damaging Malware

Wie der Name schon sagt, greift diese Art der Malware die Hardware an. Hardwarekomponenten werden also durch schädliche Software beschädigt oder zerstört. Das kann sich beispielsweise in Form einer Überhitzung durch Manipulation der Lüfter zeigen oder Beeinträchtigungen am BIOS hervorrufen [PS-2005-B, Seite 305]. Die Auswirkungen eines solchen Hardware-Schädlings kann man nicht außer Acht lassen, da ein solcher Angriff dem Nutzer nicht nur finanziell schaden kann, sondern auch auf körperlicher Ebene. Ein einzelner Funken kann einen Brand auslösen, wenn er nicht bemerkt wird. Natürlich sind hauptsächlich Hardware-Probleme die Ursache, aber solange die Möglichkeit solcher Auswirkungen besteht, ist Hardware Damaging Malware ein sehr gefährlicher Vertreter der Malware.

Ein sehr bekanntes Beispiel für diese Art ist CIH (auch Chernobyl), geschrieben von dem Studenten Chen Ing-Hau aus Taiwan [UG-2011-URL]. Diese Malware überschrieb das BIOS und machte damit das System unbrauchbar. Der Payload aktivierte sich am 26. April, dem Jahrestag von der Nuklearkatastrophe von Chernobyl [DJ-2015-URL]. Zwar ist dies ein Zeichen für das Verhalten von Logic Bombs, weil die Aktivierung des Payloads zu einen bestimmten Zeitpunkt passiert, bleibt jedoch bei der Definition von Hardware Damaging Malware unerheblich. Schließlich geht es bei dieser Definition um die Schadenswirkung auf Hardwareebene.

2.13 Logic Bomb

Als Logic Bomb werden Schadprogramme bezeichnet, die eine bestimmte Funktion zu einem bestimmten Zeitpunkt oder durch eine spezifische Aktion aktivieren. So könnten sich Logic Bombs über Jahre hinweg inaktiv auf einem Rechner befinden, ohne bemerkt zu werden oder Schaden anzurichten. Erst wenn der Trigger, das auslösende Ereignis, eintrifft, wird der Payload dieser Malware initiiert.

Die Definition nach Peter Szor unterscheidet sich ein wenig von der allgemeinen Definition. Dabei gilt sie nicht als einzelnes Programm, sondern vielmehr als eine eingebaute Schadfunktion. [PS-2005-B; Seite 30]

Je nach Funktionsweise, kann die Logic Bomb nach Szor auch als Teil eines Tojaners oder Dialers bezeichnet werden.

2.14 Wiper

Seit Kurzem hat sich ein neuer Begriff in der Malware-Welt herauskristallisiert; der sogenannte Wiper (übersetzt: Wischer). Das Wort „wiping“ bedeutet im Zusammenhang mit Computertechnik das Löschen von Daten. Entsprechend dazu ist die Funktion eines Wipers eindeutig: Datenvernichtung.

Angelehnt an den Ransomware-Vertreter Petya ist NotPetya sehr ähnlich aufgebaut. Man kann davon ausgehen, dass Petya als Grundlage gedient hat, da beide in ähnlicher Vorgehensweise den MBR manipulieren und so die Daten unbrauchbar machen. Doch anstatt so, wie die Petya-Autoren, sich mit Erpressung zu bereichern, ist NotPetya scheinbar nicht darauf aus. Die Schäden der Malware sind irreparabel. Selbst wenn ein entsprechender Key zur Entschlüsselung eingegeben wird, bleibt das System beschädigt. [JS-2017-URL]

2.15 Dialer

Ein *Dialer* hat in der damaligen Zeit unbemerkt eine Internetverbindung aufgebaut und dem Nutzer dahingehend geschadet, dass zusätzliche Kosten durch die Verbindung entstanden. Heute sind Dialer unter anderem durch DSL-Verbindungen kaum noch in der Computertechnik zu finden, viel mehr aber bei Mobiltelefonen. [SM-2016-URL]

2.16 Blended Threat

Ein *Blended Threat* (übersetzt: gemischte Bedrohung) ist ein Software-Exploit, der sich mehrere Schwachstellen zunutze machen kann. Dabei kann er unter anderem auf mehrere Verbreitungsroutinen zurückgreifen und sich somit beispielsweise über Emails verbreiten und sich gleichzeitig durch HTML-Seiten auf andere Systeme herunterladen. Der Aufbau hängt von der Zielsetzung des Autors ab. Bekannte Beispiele sind Nimba, CodeRed, Bugbear und Conficker. [TT-2015-URL]

2.17 Spammer-Programme

Spammer-Programme verschicken Spam-Nachrichten. Der Begriff Spam leitet sich von einer bekannten Dosenfleisch-Marke ab, die es in Großbritannien an jeder Ecke zu kaufen gab. Durch diese starke Präsenz griff man dies in einer Comedy-Serie auf und prägte

somit den Begriff als etwas, das unnötig oft wiederholt wird. Später wurde Spam dann in der Kommunikation verwendet. [Wiki-URL; Spam]

Ein Spammer-Programm kann einen Untertypen eines Bots darstellen, muss jedoch nicht zwingend einer sein, da sich die Definition auf die primäre Funktion des Verschickens von Spam beschränkt.

2.18 Weitere Bedrohungen

Folgende virtuelle Bedrohungen sind nicht zwingend Malware und werden nur der Vollständigkeit halber erwähnt.

Sogenannte *Exploits* (exploit = ausnutzen) sind Methoden zur systematischen Ausnutzung von Sicherheitslücken. Exploit ist ein sehr weitläufiger Begriff, der eine Bezeichnung für Computerprogramme sein kann, aber auch nur Codefragmente darstellen kann. Man kann Exploits als Machbarkeitsstudien für die Analyse von Schwachstellen betrachten. Mangels Schadwirkung kann man hier nicht unbedingt von Malware sprechen, da erst der Einsatz als Bestandteil von Malware eine Schädlichkeit begründet. [HS-URL]

Bloatware bezeichnet im eigentlichen Sinne keine Malware, sondern Programme, deren übermäßige Anzahl an Funktionen das System überlastet. [SM-2016-URL]

Joke-Programme sind zwar lästig, sollen aber eher zur Belustigung dienen und keinen ernsthaften Schaden anrichten. Ob das Opfer diese Scherz-Programme amüsant findet, ist jedoch fraglich.
Unter dem Begriff *Hoax* versteht man eine Falschmeldung, deren Inhalt nichts weiter als ein Gerücht ist. Ziel dieser Nachrichten ist es oft, einen Computernutzer dazu zu verleiten, unnötige Aktionen durchzuführen und dabei eventuell wichtige Systemdateien zu löschen. Hoax ist nicht nur auf die Computertechnik beschränkt. So können „wichtige“ Sondermeldungen über bestimmte Dinge völlig absurd und frei erfunden sein. [SM-2016-URL]

Ähnlich zum Hoax funktioniert auch *Scareware* bzw. *Rougeware*. Jedoch werden dem Nutzer nicht nur Falschinformationen gegeben, sondern sollen diese Informationen ihm regelrecht Angst bereiten. Diese veranlassen ihn dazu, auf dem eigenen System vermeintlich entdeckte Malware gegen Bezahlung entfernen zu lassen. Scareware kann in der Form von angeblich seriöser Antiviren-Software oder anderen

Sicherheitsprogrammen erscheinen, aber auch ein Link kann ursächlich für die Infektion mit Scareware sein. [SM-2016-URL]

Mit *Phishing* versucht ein Angreifer, den Nutzer hauptsächlich über Emails auf falsche Websiten zu leiten, um ihn dort persönliche Daten zu stehlen. Dabei wird dem User eine echte Webseite vorgegaukelt, sodass dieser seine Daten eingibt, die dann vom Angreifer missbraucht werden können. [SM-2016-URL]

3. Eigenmodell – Kategorisierung der Malware

Gesetze sind darauf ausgelegt, in einer Gesellschaft für Ordnung zu sorgen und jene zu bestrafen, die anderen schaden. Malware ist heutzutage ein bekanntes digitales Risiko. Sie kann in vielerlei Hinsicht einem Menschen Schaden zufügen, beginnend bei Belästigung bis hin zu Erpressung und Diebstahl. In diesem Kapitel folgt eine Art der Kategorisierung von Malware, die im Zusammenhang mit gesetzlichen Normen steht, besonders im Hinblick auf das deutsche Strafgesetzbuch. Zuerst wird eine Reihe von möglichen Straftaten aufgelistet, die durch die verschiedenen Malware-Typen begangen werden sowie deren Vertreter. Um daraus eine Kategorisierung zu entwickeln, wird die Malware in drei Hauptarten unterteilt: Malware, deren primäre Schadfunktion auf ein einzelnes Ziel ausgerichtet ist; Malware, die durch die Rückkopplung mit dem Urheber, mehrere Absichten beinhalten kann und dabei sogar weitere Straftaten ermöglicht und Malware, deren Funktionen erst durch weitere Einflüsse Schaden bewirken. Die erste Hauptkategorie wird im Folgenden als „Unilaterale Malware“ bezeichnet. Sie beinhaltet unter anderem sofortigen Schaden, wie Zerstörung von Daten, aber auch Erpressung und Betrug. Dabei wird ein ganz bestimmtes Ziel verfolgt. Die Malware der zweiten Hauptkategorie (im Folgenden „Multilaterale Malware“) wurde geschrieben, um vom Angreifer ausgewertet bzw. ausgenutzt zu werden. Dazu zählt unter anderem Spyware. Die Dritte und letzte Kategorie beinhaltet nicht nur Malware ohne primäre Schadfunktion, sondern auch Internetbedrohungen, wie Phishing und Hoaxes. Während also Unilaterale Malware eher als eine Einzelaktion betrachtet werden kann, kann Multilaterale Malware als Paket angesehen werden und Nonlaterale Malware etwa als Hilfssmittel oder Belästigung.

Die angewandten Begriffe „unilateral“ und „multilateral“ haben ihren Ursprung aus der Politik, bekommen jedoch im Folgenden eine andere Konnotation. Die gemeinsame Endung „lateral“ kommt von dem lateinischen Wort „latus“, was übersetzt „Seite“ bedeutet. Während „uni-“ dabei den Begriff zu einem sinngemäßen „einseitig“ vervollständigt, ergibt sich der entsprechende Gegensatz „vielseitig“ aus dem Präfix „multi“ (von „multus“). In politischer Sichtweise beziehen sich die Begriffe auf das Zusammenspiel von Staaten. Multilaterale Länder handeln diplomatisch und nehmen Rücksicht auf die Interessen anderer Länder, während unilateral das genaue Gegenteil

bedeutet: diese Länder kümmern sich nur um eigene Interessen. [Wiki-URL; Unilateralität, Multilateralität]

Nonlateral hat keine spezifische Bedeutung in der Politik, da ein „keinseitig“ kaum einer passenden Logik entspricht. Jedoch ist der Begriff im Folgenden ein wichtiger Bestandteil der Kategorisierung.

3.1 Computergesetze

Im folgenden Abschnitt werden einzelne Gesetze aufgegriffen, die Relevanz in der Cyberkriminalität haben. Dabei werden unter anderem verschiedene Malware-Typen sowie Vertreter beispielhaft aufgeführt. [2]

3.1.1 Datenmanipulation

Die Tatbestände Computersabotage und Datenveränderung sind womöglich die Hauptanklagepunkte im Falle Schadsoftware, da Malware im weitesten Sinne immer ein System verändert. Wenn Malware auf ein fremdes System gelangt, kann man von Datenveränderung sprechen, da kein Programm ohne Spuren auf einem System existieren kann und sobald Spuren entstehen, wurde etwas verändert.

3.1.1.1 Datenveränderung

Gemäß §303a StGB ist die unrechtmäßige Veränderung, Löschung, Unterdrückung und das Herbeiführen einer Unbrauchbarkeit von Daten strafbar. Dabei ist nicht nur die Aktion selbst rechtswidrig, sondern auch die Vorbereitung derer.

Dieser Sachverhalt trifft insbesondere auf Viren zu, da sie ihren Wirt so verändern, dass bei dessen Aufruf auch der Virus aufgerufen wird. Jedoch nicht nur Viren verändern etwas auf dem Computersystem. Im Allgemeinen verändern Malware-Programme Daten und hinterlassen dabei Spuren, sodass die Datenveränderung nach §303a StGB der größte Anhaltspunkt in der Rechtsprechung gegen Malware sein dürfte.

3.1.1.2 Computersabotage

Der Folgeparagraph (§303b StGB) umfasst Straftaten, deren Folgen eine starke Beeinflussung eines Computersystems nach sich ziehen. Darunter zählt sowohl die

2 Kapitel 3.1 bezieht sich auf Paragraphen des StGB, BGB und UWG.

Zerstörung, Veränderung und Beseitigung von Datenträgern, aber auch die Eingabe und Übermittlung von Daten am missbrauchten System, wenn dadurch einem anderen ein Nachteil zugefügt wird.

3.1.2 Unzumutbare Belästigung

Der wahrscheinlich lästigste Malware-Typ ist Adware, da sich diese durch meist unerwünschte Werbung bemerkbar macht. Im §7 des UWG (Gesetz gegen den unlauteren Wettbewerb) ist der zivilrechtliche Tatbestand Unzumutbare Belästigungen zu verzeichnen [UWG-2016-URL, Kap. 1]. Adware weist augenscheinlich einen Verstoß gegen diesen Paragraphen auf, da sie ohne das freiwillige Zutun eines Nutzers eingeblendet wird. Auch wenn der User keine Werbemitteilungen wünscht, kann Adware-Werbung nicht ohne Weiteres entfernt werden, da trotz Schließen der Werbe-Fenster immer wieder neue Reklame erscheint.

2006 wurde die amerikanische Softwarefirma Zango durch die FTC (Federal Trade Commission), eine Behörde US-Amerikas zum Verbraucherschutz, zu drei Millionen Dollar Strafe verpflichtet. Zango war einer der größten Adware-Anbieter weltweit, deren Adware unter anderem durch kostenlose Programme auf den Rechnern von Kunden gelangte. Diese Software sei nach der FTC ohne das Wissen der Nutzer installiert worden. Die Deinstallation wurde dahingehend erschwert, da unter anderem die Herkunft der Ads verschleiert wurde. Zwischen FTC und Zango gab es letztendlich eine außergerichtliche Einigung, dass der Anbieter die Summe bezahlen sowie dem Kunden eine freiwillige Installations- und Deinstallationsmöglichkeit anbieten würde. [FTC-2006-URL]

Zwar ist dies kein deutscher Fall, aber kann entsprechend ähnlich ablaufen, da das UWG das deutsche Wettbewerbsrecht regelt, das einen Teil im Verbraucherschutzes abdeckt und die FTC zuständig für den Verbraucherschutz in Amerika ist. Trotz des offensichtlichen Verstoßes gegen die Gesetzgebung scheint die Verfolgung eher rar. Zum einen wohl durch die seltene Anzeige der Fälle, aber auch dadurch, dass sich der Ursprung im Ausland befindet, lohnt sich eine intensive Ermittlung wenig.

3.1.3 Ausspähen von Daten

Wenn die Funktionen der Adware darüber hinausgehen, nur Werbung einzublenden, sondern auch die Daten auf einem fremden Rechner auszuwerten, kann man auch von

Spyware sprechen. Nach §202a StGB ist das Ausspähen von Daten untersagt und wird bei Zuwiderhandlung mit einer Geldstrafe bzw. Freiheitsstrafe geahndet [StGB-2012-B]. Spyware ist Software, die gezielt dazu verwendet wird, sich fremder Daten ohne Zustimmung des Besitzers zu bemächtigen. Mit den gesammelten Daten können dann weitere Straftaten, wie beispielsweise Identitätsdiebstahl, unrechtmäßige Bereicherung und Erpressung, durchgeführt werden.

3.1.4 Erpressung

Auf Ransomware trifft der Sachverhalt Erpressung (§253 StGB) zu. Der Angreifer nötigt sein Opfer dazu, einen bestimmten Geldbetrag zu überweisen, damit das blockierte System wieder freigegeben wird. Somit entsteht der genötigten Person ein Vermögensschaden, während der Angreifer sich damit bereichert. In den Fällen, wo selbst nach einer Überweisung keine Freigabe folgt, spricht man zusätzlich von Betrug gemäß §263 StGB.

3.1.5 Computerbetrug

Paragraph 263a des deutschen Strafgesetzbuchs erläutert speziell den Computerbetrug. Dort steht geschrieben, dass es strafbar ist, wenn eine Person sich oder anderen durch Betrug über Informationstechnik einen unrechtmäßigen Vermögensvorteil verschafft und dabei einem anderen finanziell schadet. Es ist hierbei darauf zu achten, dass sich Betrug ausschließlich auf Täuschungen bezieht, die das Vermögen angreifen. Trojaner spielen hierbei eine große Rolle, da ihre Funktion, sich als nützliches Programm auszugeben, einen unbedarften Nutzer in die Irre führt und ihn dann zumeist finanziell schadet.

3.1.6 Täuschung

Nicht alle Trojaner sind darauf ausgelegt, einem Opfer finanziell zu schaden. Wenn ein Trojaner nicht das Vermögen angreift (das heißt unter anderem, dass das Opfer keinen Betrag für die scheinbar gutartige Software bezahlt hat), kann Betrug hierbei nicht unbedingt in Betracht gezogen werden. Stattdessen entspricht dies am ehesten dem Sachverhalt der Arglistigen Täuschung nach §22 aus dem BGB. Wenn aber kein Vertrag abgeschlossen wurde, ist dieser Sachverhalt ebenfalls nicht adäquat. Entsteht dem Betrogenen ein Imageschaden, ist fraglich, wie der Angreifer belangt werden kann.

3.1.7 Gesetzliche Grenzen

Das Programmieren von Malware selbst ist eine Straftat, da dies die Vorbereitung zur Datenveränderung nach §303a StGB aufweist. Da jedes Programm auf einem Computersystem Daten verändert, trifft der Sachverhalt Datenveränderung auf alle Malware-Typen zu. Jedoch ist es fraglich, ob neben dieser grundlegenden Straftat alle durch Malware verursachte Tatbestände in der Gesetzgebung abgedeckt werden. Besonders bei Imageschäden gestaltet sich die Anklage schwierig, da hierbei kein Vermögen oder ähnliches angegriffen wird. Es ist kompliziert, einen solchen Schaden überhaupt nachzuweisen, geschweige denn, die Höhe des Schadens zu beziffern.

Innerhalb Deutschlands können Entwickler von Malware nach deutschem Recht belangt werden. Doch sobald die Schadprogramme aus einem anderen Ursprungsland kommen, sieht es mit der strafrechtlichen Verfolgung schlecht aus. Ebenso ist es schwierig den Urheber von Malware, die im Ausland „erfolgreich“ ist, hier in Deutschland zur Rechenschaft zu ziehen. [TH-2013-URL]

3.2 Abgrenzung der Malware

Zur Abgrenzung der einzelnen Typen werden drei Hauptkategorien ausgearbeitet. Neben Multilateraler und Unilateraler Malware sollen auch Computerschädlinge beachtet werden, die zwar keine richtige Malware darstellen, aber unter der Überschrift Cyberkriminalität erwähnt werden.

Im Folgenden wird die Zielsetzung von Malware anhand der primären Schadfunktion betrachtet. Generell sind Verbreitungsfunktionen und Ähnliches bereits direkt oder indirekt mit Schäden oder zumindest Veränderungen an Computersystemen verbunden, die hier aber als sekundär betrachtet werden. Ausnahme bildet Malware, deren Verbreitungsmechanismus zugleich die Hauptschadfunktion darstellt (Bakterie).

Folgend ist zu beachten, dass genannte Tatbestände zwar augenscheinlich eintreten und wohl Hauptanklagepunkte darstellen, jedoch nicht weitere Tatbestände ausschließen.

3.2.1 Unilaterale Malware

Als uniliterale Malware wird Malware bezeichnet, deren primäre Schadfunktion bzw. deren Payload die Hauptfunktion und integraler Teil der Malware ist. Die Schadsoftware

ist rückkopplungsfrei und benötigt nach ihrer primären Verbreitung keine Verbindung zum Entwickler, um die primäre Schadfunktion auszuführen. Dies ist rechtlich insoweit relevant, da hierbei im Regelfall Vorsatz anzunehmen wäre.

Folgende Vertreter sind hierbei aufzuzeigen:

- **Virus**: Ein reiner Virus verbreitet sich durch Infektion anderer Programme. Sobald der Virus freigesetzt wurde, ist er selbstständig, sodass der Entwickler keine weitere Maßnahmen erbringen muss, damit das Programm seinen Zweck erfüllt. Da ein Virus schon allein mit seiner Verbreitungsmethode Daten verändert, ist eindeutig ein Verstoß gegen §303a StGB zu verzeichnen. Je nach Payload kommen weitere Tatbestände hinzu.

  → Tatbestand: Datenveränderung (§303a StGB)

- **Wurm**: Ein Wurm kann sich nach Freisetzung ebenfalls völlig allein bewegen, sogar ohne dabei ein Wirtsprogramm zu brauchen. Dabei nutzt ein Wurm Systemfunktionen, um in ein System zu gelangen. Da ein Wurm schon allein mit seiner Existenz Spuren auf einem System hinterlässt, besteht hier ebenfalls der Tatbestand Datenveränderung.

  → Tatbestand: Datenveränderung (§303a StGB)

- - **Trojaner**: Trojaner verbreiten sich nicht selbstständig, aber sind dennoch nicht auf ihren Entwickler angewiesen. Sie werden von ahnungslosen Computernutzern heruntergeladen und können so dessen System verseuchen.

  → Tatbestand: Arglistige Täuschung (§22 BGB)

- **Ransomware**: Mit Ransomware versucht der Angreifer durch das Sperren eines Opfersystems eine finanzielle Bereicherung zu erzwingen. Aufgrund der Tatsache, dass der Schaden bereits entstanden ist und die Malware keine direkte Rückkopplung realisiert, gehört die Ransomware zur unilateralen Malware. Die mögliche Verbindung des Opfers zum Erpresser herstellt, ist hierbei nicht maßgebend, da sie nicht Teil der Software ist.

  → Tatbestand: Erpressung (§253 StGB) / Computerbetrug (§263a StGB)

- **Bakterie**: Diese Art Malware dient zur Beeinflussung eines Systems durch das Überfüllen von Arbeits- bzw. Hauptspeicher. Folgen einer solchen Beeinflussung

sind entsprechend die Beeinträchtigung eines Computersystems.

→ Tatbestand: Computersabotage (§303b StGB)

- **Logic Bomb**: Der Trigger ist im Code einprogrammiert, sodass die Logic Bomb keinen „Fernzünder“ benötigt, um ihren Payload zu aktivieren. Da Malware prinzipiell Spuren auf einem System hinterlässt, trifft Datenveränderung in jedem Fall zu. Je nach Payload kommen weitere Tatbestände hinzu.

  → Tatbestand: Datenveränderung (§303a StGB)

- **Hardware Damaging Malware (HDS)**: Das Ziel dieser Art Malware ist die physikalische Zerstörung von Computertechnik. Bräuchte sie hierfür ihren Entwickler, könnte dieser genauso gut die IT mit einem Hammer unschädlich machen.

  → Tatbestand: Computersabotage (§303b StGB)

- **Dialer**: Dialer nehmen zwar Verbindung zu einem Netzwerk auf, jedoch nicht, um dem Urheber Daten zuzusenden, sondern, um dem Nutzer des infizierten Geräts finanziell zu schaden.

  → Tatbestand: Computerbetrug (§263a StGB) / Untreue (§266 StGB)

- **Wiper**: Die Hauptfunktion dieser Art Malware ist das Zerstören von Daten.

  → Tatbestand: Datenveränderung, Computersabotage (§303a,b StGB)

- **Blended Threat**: Da diese Art an sich schon mehrere Verbreitungsfunktionen besitzt, ist die Interaktion mit dem Urheber überflüssig. Eine Rückkopplung besteht nicht.

  → Tatbestand: Datenveränderung (§303a StGB)

3.2.2 Multilaterale Malware

Multilaterale Malware zeichnet sich generell durch eine Rückkopplungsfunktion aus. Diese Funktion kann in der Steuerbarkeit der Malware (Bot), der Rückmeldung von Daten (Spyware), dem Nachladen unabhängiger Schadfunktionen oder zusätzlicher unilateraler Malware (Dropper) zu finden sein. Aufgrund der stetigen Verbindung zum Angreifer, ist es wahrscheinlicher, dass der Ursprung des Schadprogramms

herausgefunden werden kann. Mit Multilateraler Malware macht sich der Entwickler nicht nur für den Schadcode strafbar sondern unter anderem auch für die Vorbereitung weiterer Straftaten. Dabei schafft er sich andere Möglichkeiten, das infizierte System selbst oder Inhalte darauf zu missbrauchen. Mit Multilateraler Malware ist organisierte Kriminalität möglich.

Zu Multilateraler Malware zählen folgende Vertreter:

- **Bot:** Durch einen Bot wird der verseuchte Rechner an ein Botnetz gekoppelt. Mit diesem Netz kann der Botmaster die Computer fernsteuern und illegale Aktivitäten, wie beispielsweise DDoS-Angriffe, durchführen. Bots haben auch andere Anwendungsmöglichkeiten. Darunter zählt Bitcoin-Mining, Massenspam und andere Aktionen, bei denen eine große Menge an Ressourcen eine Rolle spielt.

  → Tatbestand: Computersabotage (§303b StGB)

- **Spammer-Programme**: Hier hängt die Kategorisierung von der Implementierung ab. Greift ein Spammer-Programm auf bestimmte Ressourcen zurück, die bereitgestellt wurden, zählt es zur multilateralen Malware. Wenn es ohne Rückkopplung Spam verteilt, so gilt es als unilateral.

  → Tatbestand: Unzumutbare Belästigung (§7 UWG)

- **Spyware:** Mithilfe von Spyware kann der Angreifer persönliche Daten, wie Bankdaten, Passwörter sowie private Bilder und Dateien, ermitteln. Dies lässt sich unter anderem durch Abfangen von Tastatureingaben und das Hacken von Webcams bewerkstelligen. Die unrechtmäßig gesammelten Daten werden dann dem Urheber gesandt, sodass dieser weitere unrechtmäßige Aktivitäten durchführen kann. Durch die erlangten Daten können weitere Straftaten durchgeführt werden. Die Möglichkeiten sind je nach gesammelter Information sehr vielfältig. Persönliche Bilder geben Potential zur Erpressung, Passwörter ermöglichen Identitätsdiebstahl und wenn Bankdaten erspäht wurden, ist das Vermögen ebenfalls nicht mehr sicher.

  → Tatbestand: Ausspähen von Daten (§202a StGB)

- **Dropper:** Dropper sind dazu da, um Malware initial zu aktivieren. Zusätzlich

dazu können sie auch als Verbreitungsorgan dienen, indem sie andere Malware auf das System herunterladen. Mit einem Dropper werden nicht nur Straftaten vorbereitet, sondern auch Beihilfe bei der Verbreitung geleistet.

→ Tatbestand: Vorbereitung von Computersabotage, Ausspähen von Daten (§303b Abs. 5, §202c StGB)

3.2.3 Nonlaterale Malware

Zu dieser Kategorie zählt Malware, die keine primäre Schadfunktion besitzt sowie keine Rückkopplung zum Urheber nötig ist. Ebenso werden hier auch andere Computerschädlinge eingeordnet, die nicht als Malware per se bezeichnet werden können (Hoax, Phishing, usw.).

- **Adware**: Adware wird dazu verwendet, um einer dritten Person unerwünschte Werbung einzublenden. Da dies weder strafrechtlich geahndet wird, noch eine Rückkopplung besteht, gehört diese Art Malware zur nonlateralen Malware. Der Fall, dass Daten für personalisierte Werbung ausgespäht werden, wird als Spyware betrachtet.

  → Tatbestand: Unzumutbare Belästigung (§7 UWG)

- **Backdoor**: Durch eine Backdoor kann der Angreifer auf ein fremdes System zugreifen und dort entsprechend illegale Aktivitäten durchführen. Jedoch muss der Entwickler einer Backdoor nicht zwingend damit interagieren. Des Weiteren schadet die Funktion einer Backdoor nicht, bevor sie von anderen für illegale Zwecke ausgenutzt wird.

  → Tatbestand: Vorbereiten des Ausspähens und Abfangens von Daten (§202c StGB)

- **Rootkit**: Ein Rootkit verleiht dem Angreifer Root-Rechte, sodass dieser, wie bei einer Backdoor, ohne das Zutun des Computerbesitzers auf das System zugreifen kann. Ähnlich der Backdoor ist die Verbindung zum Entwickler nicht nötig, damit das Rootkit nach Wunsch funktioniert. Jedoch ist auch hier die primäre Schadfunktion nicht ohne äußere Einflüsse schadend, da eine Verschleierung nichts bringt, wenn es nichts zu verschleiern gibt.

  → Tatbestand: Vorbereiten des Ausspähens und Abfangens von Daten

(§202c StGB)

- **Weitere Bedrohungen (Hoax und Co.):** Da diese Art der Cyberkriminalität keine Malware darstellt, werden die Einzeltypen nicht näher betrachtet.

3.2.4 Übersicht der einzelnen Kategorien

Malware	Unilateral	Multilateral	Nonlateral
Virus	x		
Trojaner	x		
Wurm	x		
Dropper		x	
Ransomware	x		
Bakterie	x		
Backdoor			x
Rootkit			x
Bot		x	
Spyware		x	
Adware			x
HDS	x		
Logic Bomb	x		
Wiper	x		
Blended Threat	x		
Spammer-Programm	(x)	x	

Tabelle 2: Eigenkonzept zur Einteilung der Malware [E]

4. Diskussion – Verschiedene Konzepte

In den vorangegangenen Kapiteln wurden mehrere Konzepte und Modelle zur Differenzierung und Unterteilung von Schadsoftware vorgestellt und im Einzelnen betrachtet. In diesem Kapitel sollen nun die Unterschiede, die Vor- und Nachteile der Konzepte direkt miteinander verglichen werden. Die Funktionsfähigkeit und insbesondere die zukünftige Nutzbarkeit stehen hier im Mittelpunkt der Betrachtung.

Im Konzept von John Aycock sind drei Kriterien für die Einstufung von Schadsoftware zu berücksichtigen: Selbstreplikation, Populationswachstum und das parasitäre Verhalten. Basierend auf den ursprünglichen reinen Typen, wie sie insbesondere aus den Anfängen der Malwareentwicklung bekannt sind, ist diese Einteilung für eine funktionale und globale Kategorisierung sehr passend und bietet eine eindeutige Zuordnung.

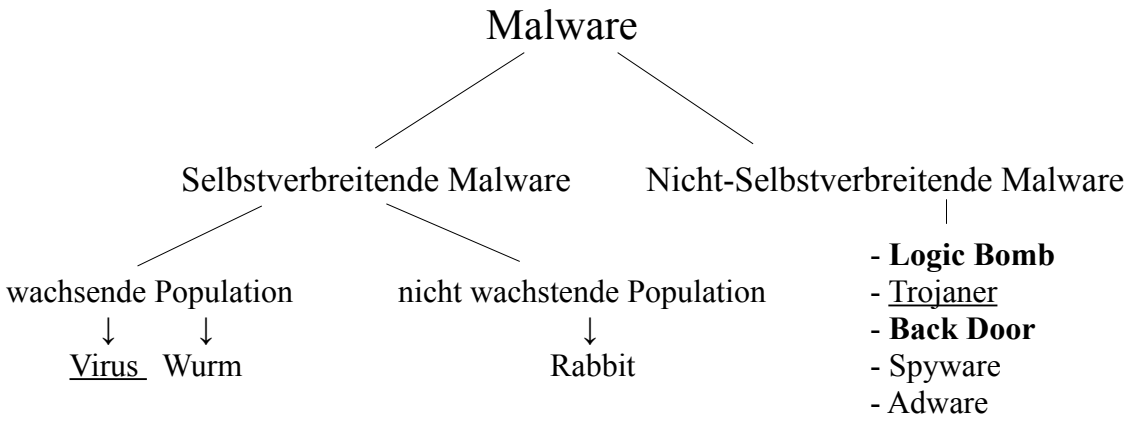


Abbildung 1: Visuelle Interpretation des Kategorisierungsmodells nach Aycock [E]

Problematisch sind jedoch die partiellen Abhängigkeiten und Überschneidungen zwischen den Hauptkategorien. Während die ersten beiden Kategorien (Selbstreplikation und Populationswachstum) untereinander abhängig sind, (ohne Replikation gibt es kein Wachstum), ist das dritte Kriterium (parasitäres Verhalten) davon komplett unabhängig. Damit wird eine zuverlässige Differenzierung der verschiedenen Malwareformen in aktuellen Erscheinungsformen schwierig. Die Zuordnung der vielen, mittlerweile

existierenden Hybride kann damit kaum eindeutig vorgenommen werden. Betrachtet man die Entwicklung der Schadsoftware allgemein, so treten immer mehr Mischformen auf und die Kategorisierung nach Aycock kann dem in Zukunft nur schwer gerecht werden. Sie ist also weniger geeignet.

[JA-2006-B]

Die Klassifizierung nach Hummert ist ein duales Verfahren zur Kategorisierung von Schadsoftware. In der ersten Stufe wird nach der Verbreitungsmethode klassifiziert und im zweiten Teil nach dem Payload. Dieses Konzept ist sehr unkompliziert und verständlich gehalten. Objektiv differenzierbare und eindeutige Kriterien machen die Klassifizierung geeignet für den allgemeinen Gebrauch.

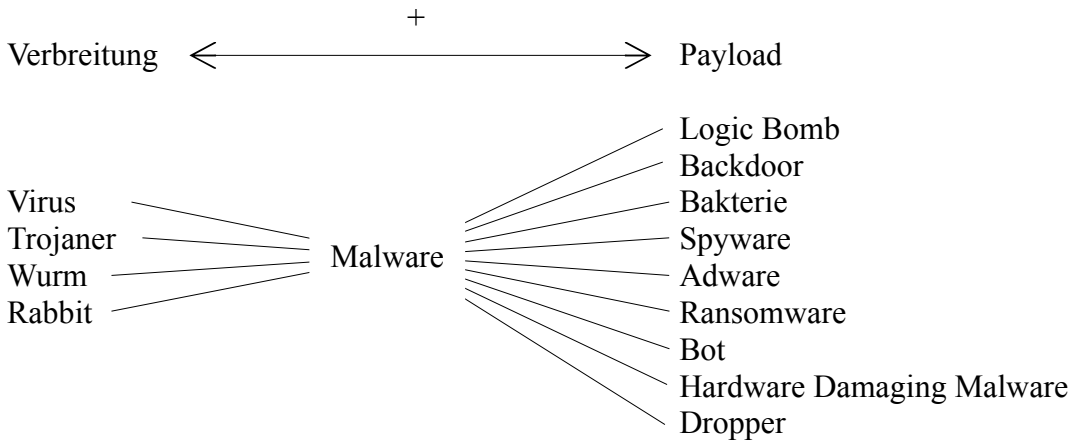


Abbildung 2: Kategorisierungsmodell nach Hummert [E]

Aktuelle Schadsoftware ist inzwischen vielfach nach dem Baukastenprinzip aufgebaut. Die Tendenz geht dabei immer mehr zu Verbreitungsvarianten, die einerseits geringen Aufwand seitens des Entwicklers aufweisen und andererseits eine größtmögliche Verbreitung sicherstellen sollen. Die Folge sind entsprechend eine zunehmende Verbreitung von Methoden, die unter anderem per Social Engineering den Nutzer zur Verbreitung einbeziehen (Phishing, Verbreitung per Mail, infizierte Webseiten, etc.). Diese Vorgehensweisen stellen geringere Ansprüche an die Schadsoftware selber, da die Überwindung von Sicherheitsmechanismen in den Hintergrund rückt. Der reduzierte

Aufwand ermöglicht damit aber gleichzeitig auch die Verwendung verschiedener Verbreitungsmethoden parallel oder als sequentielle Variante. Dadurch kann Malware beispielsweise als Trojaner in ein System vordringen, um sich dort dann viral oder als Wurm (z.B. durch Nutzung von Sicherheitslücken in Netzwerkprotokollen) innerhalb lokaler Netzwerke zu verbreiten.

Die Klassifizierung nach Hummert deckt in der hier vorliegenden Form nicht alle derzeit möglichen Varianten ab. Multiple Verbreitungsmethoden oder auch multiple Payloads erschweren die Anwendung der Kategorisierung. Es ist durchaus denkbar bzw. wurde auch schon in der Realität beobachtet, dass zum Beispiel Viren, die ein System infiziert haben, als Bots fungieren, um mit deren Hilfe (Funktion als Dropper) weitere Viren nachzuladen.

Schadsoftware ohne eine der kategorisierten Verbreitungsmethoden fällt aus der Betrachtung nach diesem Verfahren heraus. Die Verbreitung von Schadsoftware per Mail oder über infizierte Webseiten könnte man zwar im Prinzip auch in die Verbreitungsmethode „Trojaner“ einstufen, das erscheint aber nicht wirklich als geeignet.

[CH-2017-B]

Die Definitionen einzelner Malware-Typen von Peter Szor unterscheiden sich an einigen Stellen signifikant von anderen Definitionen (beispielsweise Logic Bomb). Die zugrundeliegende Betrachtungsweise folgt einer eigenen Logik, deren Berechtigung nicht abzustreiten ist, jedoch wirken die Definitionen der einzelnen Typen beim Vergleich mit im Netz kursierender aktueller Schadsoftware als nicht mehr zureichend. Das Konzept der Klassifizierung ist jedoch wegen der vereinfachten Charakteristik der Oberkategorien in einfachen Fällen immer noch nutzbar.

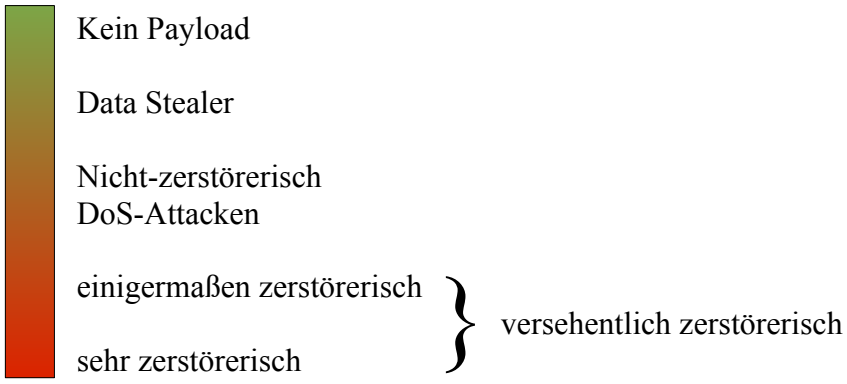


Abbildung 3: Kategorisierungsmodell nach Szor in Bezug auf den Zerstörungsgrad [E]

Für die Nutzung bei Vorliegen spezifischer Malwarekonstruktionen oder bei differenzierter Betrachtung ist jedoch problematisch, dass die Definitionen nicht eindeutig sind. Speziell die Verwendung subjektiver Beurteilungskriterien ist kritisch. Verschiedene Sichtweisen des Nutzers (= subjektive Betrachtung) auf den Zerstörungsgrad führen z.B. dazu, dass eine Person den Virus in die Kategorie „Somewhat Destructive“ (einigermaßen zerstörerisch) steckt, während der Virus für einen anderen doch eher als „Highly Destructive“ (sehr zerstörerisch) entspricht. Für eine fundierte Betrachtung, besonders in Bezug auf rechtliche Aspekte und Straftatbestände, ist dieses Verfahren mehrdeutig und nicht differenziert genug.

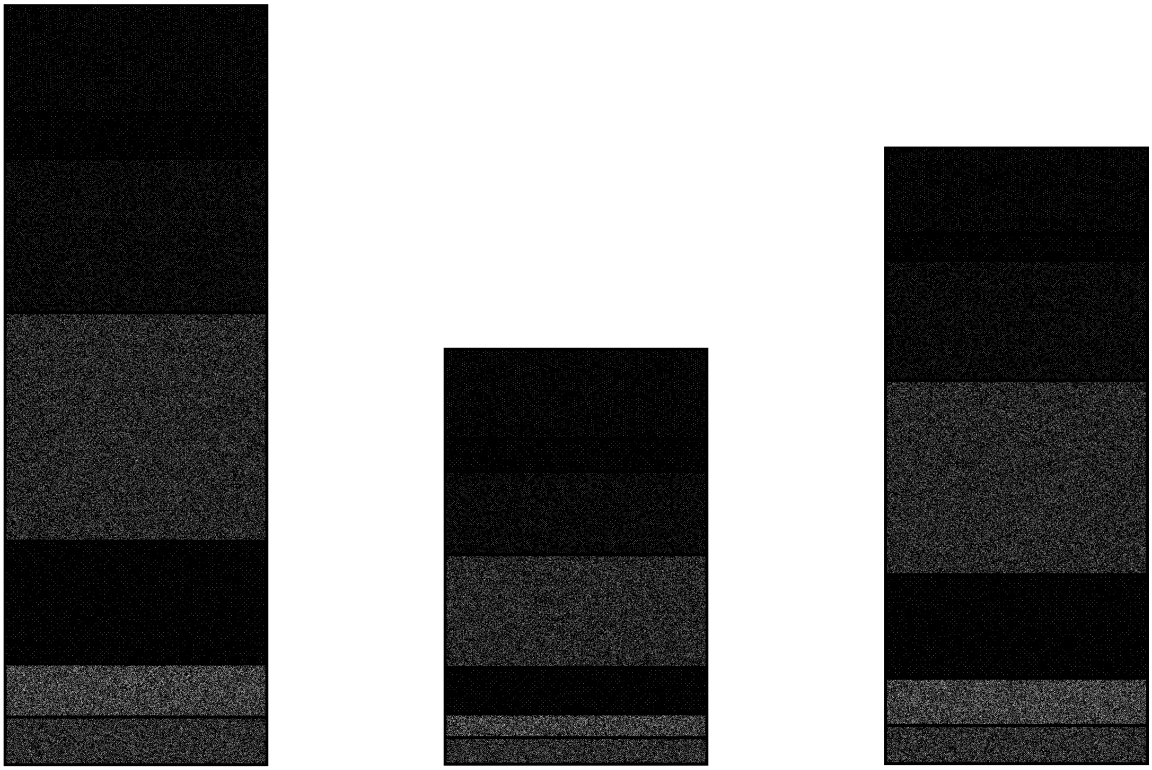
[PS-2005-B]

Im Folgenden werden weitere Methoden zur Kategorisierung von Malware vorgestellt, die nicht in der Einleitung erläutert wurden, aber ebenfalls Einblicke in andere Kategorisierungsansätze ermöglichen und entsprechend Relevanz zum Thema haben. Aufgrund der Vielzahl an verschiedenen Ideen und Ausarbeitungen können nicht alle wissenschaftlichen Arbeiten gewürdigt werden.

Eine interessante Herangehensweise wird im Paper „Malware Images: Visualization and Automatic Classification“ von Lakshamanan Nataraj, Shanmugavadivel Karthikeyan, Grégoire Jacob und B. S. Manjunath vorgestellt. Auf binärer Ebene können Dateien auf einem Computer als Zeichenkette dargestellt werden. Dieses Prinzip wird in dem Konzept

auf Malware-Programme angewandt, sodass die Aneinanderreihung von Nullen und Einsen ein Bild ergibt. Anhand der visuellen Darstellung konnten Ähnlichkeiten zwischen einzelnen Malware-Arten erkannt werden, da diese eine ähnliche Bildstruktur aufweisen. Um den Malware-Code bildlich darzustellen, wird der Binärcode als 8bit-Vektor gelesen und dann in ein 2D-Array umgewandelt. Das entstandene Bild hat eine festgeschriebene Breite, ist aber, je nach Länge des Codes, variierbar lang. Folgende Abbildung zeigt eine beispielhafte Visualisierung von drei fiktiven Malware-Programmen derselben Familie.

[NKJM-2014-URL]



Sample 1 Sample 2 Sample 3

Abbildung 4: Beispielhafte Visualisierung von Malware einer Familie [E]

Um die Textur der visualisierten Malware zu analysieren, nutzen die Autoren eine Methode ähnlich zum „Gabor filtering“, das einen automatisierten Ersatz zum menschlichen visuellen System darstellt, um Muster zu erkennen und zu verarbeiten. Die abschließende Klassifikation wird dann durch das Betrachten der k-nächsten Nachbarn durchgeführt.

Vorteil des Konzepts ist das Potential auf visueller Ebene, besonders durch die große Genauigkeit dieser Methode. Jedoch treten Probleme auf, wenn sich die Komponenten der unterschiedlichen Malware-Typen einer Familie trotz der gemeinsamen Merkmale zu sehr in der Abbildung unterscheiden.

Das folgende Konzept wurde gemeinsam von Chaitanya Yavvari, Arnur Tokhtabayev, Huzefa Rangwala, und Angelos Stavrou entwickelt. Es beruht auf der Betrachtung von spezifischen Komponenten der Malware. Dabei wird eine sogenannte „Behavioral Map“ ausgearbeitet, bei der Verhaltensspuren von Malware-Vertretern verglichen werden. Das entsprechende Behavioral Mapping erfolgt in drei Schritten: Projektion, Soft Clustering und Visualisierung. Im ersten Schritt werden Samples (Spuren-Sequenzen) von Malware auf einem bestimmten Referenz-Sample abgebildet. Die Projektion der Sequenzen besteht dabei aus binären Merkmalsvektoren, wobei deren Länge der Länge der Referenzsequenzen entspricht. Beim Soft Clustering werden diese Sequenzen anhand der Ähnlichkeit der Projektionen gruppiert. Im dritten und letzten Schritt werden die ähnlichen Sequenzen visuell dargestellt. In jeder Zeile werden die Gemeinsakeiten der Samples mit der Referenz markiert. Alle grauen Balken werden nach dem Clustering als ähnlich zu der Referenz angegeben. Das heißt Referenz und Sample haben ähnliches Verhalten. Wie man in Abbildung 5 sieht, haben manche an gewissen Stellen das gleiche Verhalten, manche nicht. Daraus lässt sich schließen, dass dort möglicherweise eine andere Komponente benutzt wird. Demnach kann man diese Malware zusammen gruppieren.

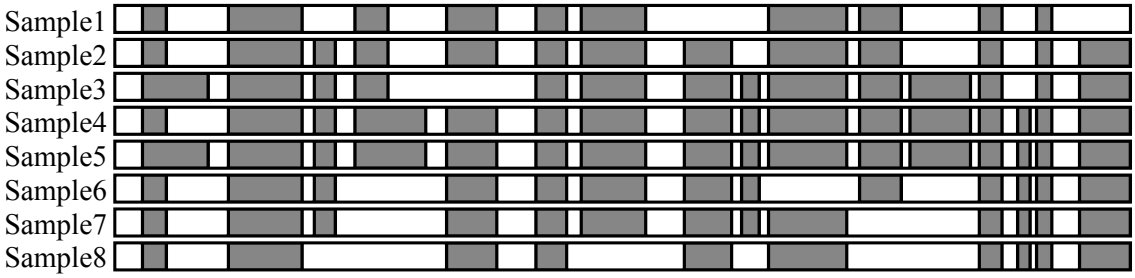


Abbildung 5: Behavior Map verschiedener Malware-Samples [E]

Um eine umfassende Analyse zu erreichen, bei der auch Verhaltensspuren beachtet werden, die mit der Referenz keine Gemeinsamkeiten haben, wird das Behavioral

Mapping iterativ angewandt. Das bedeutet, die Vergleichs-Referenz wird zufällig aus den vorhandenen Samples ausgewählt und zur Projektion verwendet. Mithilfe dieser Methode können die einzelnen Malware-Vertreter durch ihre signifikanten Ähnlichkeiten in eine gemeinsame Kategorie eingeordnet werden.

Durch die entsprechende Betrachtung von einzelnen Komponenten ist es möglich, das Verständnis für Malware zu verbessern, um damit heuristische Analysen zu verfeinern.

[YTRS-URL]

Abschließend wird noch einmal das Hauptkonzept dieser Arbeit kurz analysiert. Das im Kapitel 3 vorgestellte Eigenmodell versucht die Differenzierung von Schadsoftware nicht über spezifische Methoden der Software darzustellen, sondern basiert auf grundlegenden Wirkprinzipien bzw. der Wirkungsrichtung. Zusätzlich wird quasi ein Wirkungsgrad betrachtet, da die Einteilung in Stufen gesehen werden kann. Hier besteht Ähnlichkeit zum Zerstörungsgrad bei Peter Szor.

Durch die Einteilung nach primärer Schadfunktion und Rückkopplung, kann das Problem der Einstufung besonders bei Hybrid-Malware effektiv gelöst werden. Da bei hybriden Formen die jeweils höchste erreichte Einstufung entscheidend ist, wird die Schadsoftware in ihrer Gesamtheit berücksichtigt, so dass weniger relevante Eigenschaften nicht überbewertet werden. Dennoch bleibt auch die „reinrassige“ Malware nicht unberücksichtigt.

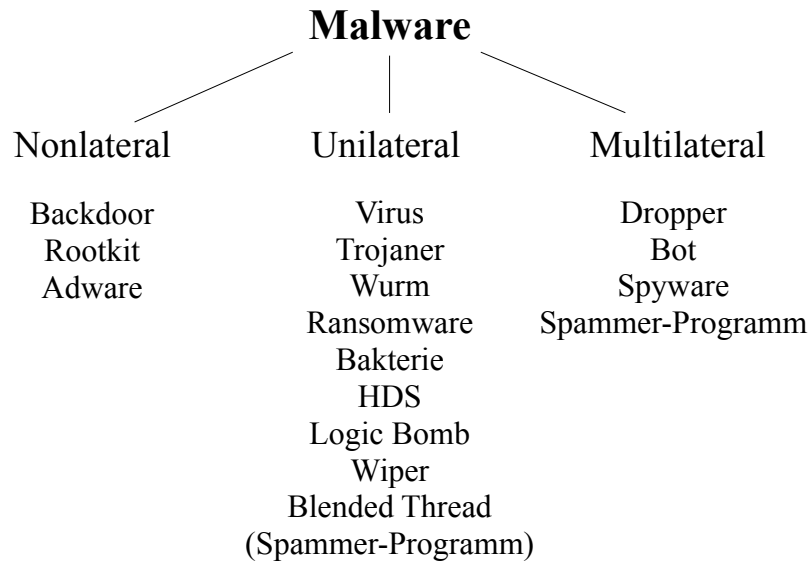


Abbildung 6: Darstellung des Eigenmodells [E]

Vorteil dieser Methode ist die Möglichkeit der eindeutigen Einstufung aller Formen von Schadsoftware. Die Einstufung ermöglicht eine Grundbeurteilung des Gefahrenpotentials und möglicher Maßnahmen zur Reduzierung von Schadenswirkungen (Anwendbarkeit heuristischer Methoden, Blockade der Kommunikation, etc.). Das Beurteilungsverfahren kann als relativ einfach betrachtet werden.

Für spezifische Zwecke, bei denen beispielsweise der Verbreitungsweg (z.B.: für die Beurteilung der Sicherheit eines Systems) in Kombination mit möglichen Eigenschaften der befallenen Systeme entscheidend ist, kann das Verfahren nur bedingt verwendet werden. Die Beschränkung auf wenige Grundkriterien bedingt eine Vereinfachung, die bei spezifischen Fragestellungen unzureichend sein kann.

4.1 Fazit

Es gibt viele verschiedene Konzepte der Kategorisierung der Malware, jedoch war der Fokus bisher immer auf spezifische Komponenten der Malware selbst gerichtet. Das neu geschaffene Kategorisierungsmodell ermöglicht einen anderen Blickwinkel zum Kategorisieren von Schadsoftware, da sich dieses Modell mit den Wirkprinzipien beschäftigt. Zwar ist dies der Einteilung nach Payload recht ähnlich, unterscheidet sich aber signifikant durch den Zusatz der Rückkopplungsfunktion. Durch das weitere Kriterium entsteht ein völlig eigener Ansatz. Da sich das vorgestellte Konzept klarer und

eindeutiger Kriterien zur Einordnung der Malware bedient, ermöglicht es eine objektive Betrachtung. Mit dieser Art der Einteilung ist es außerdem leichter, Anhaltspunkte in der deutschen Gesetzgebung zu finden. Dadurch ist ihre Verwendung noch nützlicher, besonders unter dem Gesichtspunkt der rechtlichen Weiterentwicklung. Folglich können Gesetze und Normen mithilfe dieser Kategorisierung an die immer moderner werdende Internetkriminalität angepasst werden.

4.2 Ausblick

Das vorgestellte Konzept der Kategorisierung der Malware nach uni-, multi- und nonlateraler Malware hat eine Chance, gut zu altern, da der Fokus auf den Wirkprinzipien liegt. Durch das Einteilen nach der Wirkung ist die technische Umsetzung völlig irrelevant. Dementsprechend ist auch der technische Fortschritt keine Problemquelle mehr, da beispielsweise Datenverlust durch Malware unabhängig vom Betriebssystem entstehen kann. Somit wird das Modell der Klassifizierung zeitlos. Besonders in der Rechtsprechung hat das Konzept eine gute Anwendbarkeit und auch im allgemeinen Gebraucht ist es gut anzuwenden, da die Einteilung der einzelnen Typen objektiv und eindeutig vonstatten geht. In Hinblick auf die Weiterentwicklung von Anti-Malware-Strategien ist dieses Konzept jedoch weniger geeignet. Da der Schwerpunkt nicht auf dem „Wie?“ beruht, ist nicht ersichtlich, auf welche Art und Weise Malware schneller entdeckt werden kann oder wie genau sie funktioniert. Somit ist diese Art der Kategorisierung kaum ein Ansatzpunkt für modernere Verteidigungstaktiken.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.
Alle Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 23.08.2017

Juliane Rehfeld

Quellverzeichnis

Abkürzungssystem

[Kürzel - Jahr - Art der Quelle, Unterlink/Kapitel]

B = Buch, E = Eigenwerk, MZ = Magazin, URL = Webseite/Online-Dokument

Quellen

[JA-2006-B]

John Aycock;

„Computer Viruses and Malware“

1. Aufl. Springer US, 2006

[PS-2005-B]

Peter Szor;

„The Art of Virus Research and Defense“

1. Aufl. Hagerstown, Maryland : Semantec Corporation, 2005

[CH-2017-B]

Prof. Dr. rer. nat. Christian Hummert;

„Malware Forensics“,

unveröffentlichte Fassung, Kapitel 7, 2017

[DB-2017-MZ]

Detlef Borchers;

„Und er sah, dass es viral war“

c't Ausgabe 6; 04.03.2017; ISSN: 0724-8679

[NB-2014-URL]

Nota Bene;
„10 years since the first smartphone malware – to the day.“
<https://eugene.kaspersky.com/2014/06/15/10-years-since-the-first-smartphone-malware-to-the-minute/>;
veröffentlicht am 15.06.2014

[VB-2015-URL]

Vladislav Biryukov; <info@kaspersky.de>
„Fakt oder Fiktion: Kann ein Virus die PC-Hardware beschädigen?“,
<https://blog.kaspersky.de/fact-or-fiction-virus-damaging-hardware/6155/>
veröffentlicht am 15.09.2015

[TB-2013-URL]

Timo Brücken; <info@stern.de>
„Die dubiose Masche der Bitcoin-Betrüger“
<http://www.stern.de/digital/online/dreister-betrug-mit-digitaler-waehrung-die-dubiose-masche-der-bitcoin-betrueger-3640722.html>
veröffentlicht am 23.12.2013

[FC-1984-URL]

Fred Cohen;
„Computer Viruses - Theory and Experiments“, 1984
<https://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html>
abgerufen am 23.07.2017

[UG-2011-URL]

Ulrike Garlet; <info@crn.de>
„Chernobyl-Virus aus den 90ern wieder aufgetaucht“
<http://www.crn.de/security/artikel-92039.html>
veröffentlicht am 29.08.2011

[TH-2013-URL]
Thomas Haar;
„Zur Strafe“
<https://www.heise.de/ix/artikel/Zur-Strafe-1892408.html>
veröffentlicht am 11.03.2013

[DJ-2015-URL]
Diana Jensen; <info@de.gbs.com>
„Computerwürmer, Viren und Trojaner der letzten Jahrzehnte“
<https://blog.gbs.com/trends-markt/computerwuermer-viren-und-trojaner-der-letzten-jahrzehnte>
veröffentlicht am 15.08.2015

[SM-2016-URL]
Sebastian Minnich; <webmaster@heise.de>
„Malware, Viren und Trojaner – Das Schädlings-ABC“
<https://www.heise.de/download/blog/Malware-Viren-und-Trojaner-Das-Schaedlings-ABC-3356219>
veröffentlicht am 20.10.2016

[DS-2017-URL]
Dennis Schirrmacher;
„Master-Schlüssel der Erpressungstrojaner GoldenEye, Mischa und Petya veröffentlicht“
<https://www.heise.de/security/meldung/Master-Schluessel-der-Erpressungstrojaner-GoldenEye-Mischa-und-Petya-veroeffentlicht-3767637.html>
veröffentlicht am 09.07.2017

[FS-URL]

Frederick Schiwek; <sites@keyworddomains.com>;
„Bootvirus“
<http://computervirus.de/bootvirus/>;
abgerufen am 23.07.2017

[JS-2017-URL]

Jürgen Schmidt;
„Petya/NotPetya: Kein Erpressungstrojaner, sondern ein "Wiper"
<https://www.heise.de/security/meldung/Petya-NotPetya-Kein-Erpressungstrojaner-sondern-ein-Wiper-3759293.html>;
veröffentlicht am 29.06.2017

[SS-URL]

Sylvia Seelert;
„Der Trojanische Krieg – Der Fall Trojas“
<http://www.mythentor.de/griechen/troja9.htm>
abgerufen am 24.07.2017

[HS-URL]

Prof. (FH) Mag. Dr. Helmut Siller, MSc;
<springerfachmedien-wiesbaden@springer.com>;
„Exploit“
<http://wirtschaftslexikon.gabler.de/Archiv/1408531/exploit-v3.html>
abgerufen am 23.07.2017

[JH&JS-1997-URL]

Jeffrey Horton & Jennifer Seberry; <{jeffh; j.seberry}@cs.uow.edu.au>
„Computer Viruses An Introduction“
<http://www.uow.edu.au/~jennie/WEBPDF/1997_09.pdf>
abgerufen am 23.07.2017

[NKJM-2014-URL]

L. Nataraj, S. Karthikeyan, G. Jacob & B. S. Manjunath
<lakshmanan_nataraj@ece.ucsb.edu>, <karthikeyan@ece.ucsb.edu>,
<gregoire.jacob@gmail.com>, <manj@ece.ucsb.edu>
„Malware Images: Visualization and Automatic Classification“
<https://www.researchgate.net/profile/Shanmugavadivel_Karthikeyan/publication/228811247_Malware_Images_Visualization_and_Automatic_Classification/links/0deec53bee6c992ef1000000/Malware-Images-Visualization-and-Automatic-Classification.pdf>
veröffentlicht 10.07.2014

[YTRS-URL]

Chaitanya Yavvari, Arnur Tokhtabayev, Huzefa Rangwala, and Angelos Stavrou
<cyavvari@gmu.edu>, <atokhtab@gmu.edu>, <astavrou@gmu.edu>,
<rangwala@cs.gmu.edu>
„Malware Characterization using Behavioral Components“
<http://cs.gmu.edu/~astavrou/research/Behavioral_Map.pdf>
abgerufen am 19.08.2017

[FTC-2006-URL]

FTC; <webmaster@ftc.gov>
„Zango, Inc. Settles FTC Charges“
<https://www.ftc.gov/news-events/press-releases/2006/11/zango-inc-settles-ftc-charges>
veröffentlicht am 03.11.2006

[GDATA-URL, Geschichte]

G DATA Software AG; <info@gdata.de>
„Was ist eigentlich die Geschichte der Malware?“
<https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware>,
abgerufen am 23.07.2017

[GDATA-URL, Botnet]
Dr. Ines Maria Eckermann; <info@gdata.de>
„Was ist eigentlich ein Botnet?“
<https://www.gdata.de/ratgeber/was-ist-eigentlich-ein-botnet,>
abgerufen am 23.07.2017

[JB_Wiki-URL; Goldeneye]
James Bond Wiki;
„goldeneye (weapon)“
<http://jamesbond.wikia.com/wiki/GoldenEye_(weapon)>
abgerufen am 23.07.2017

[SDUG-URL]
Sharehouse Digital UG; <info@sharehouse-digital.de>
„Viren“
<http://www.spam-info.de/viren/>
abgerufen am 23.07.2017

[SDUG-URL, Linkviren]
Sharehouse Digital UG;
„Linkviren“
<http://www.spam-info.de/viren/linkviren/>
abgerufen am 23.07.2017

[SDUG-URL, Dateiviren]
Sharehouse Digital UG;
„Dateiviren“
<http://www.spam-info.de/viren/dateiviren/>
abgerufen am 23.07.2017

[SDUG-URL, Makroviren]
Sharehouse Digital UG;
„Makroviren“
<http://www.spam-info.de/viren/makroviren/>
abgerufen am 23.07.2017

[SDUG-URL, Script-Viren]
Sharehouse Digital UG;
„Script-Viren“
<http://www.spam-info.de/viren/script-viren/>
abgerufen am 23.07.2017

[SDUG-URL, Verzeichnis-Viren]
Sharehouse Digital UG;
„Verzeichnis-Viren“
<http://www.spam-info.de/viren/verzeichnis-viren/>
abgerufen am 23.07.2017

[SDUG-URL; Slack-Viren]
Sharehouse Digital UG;
„Slack-Viren“
<http://www.spam-info.de/viren/slack-viren/>
abgerufen am 23.07.2017

[TT-2015-URL]
TechTarget;
„Blended Threat – Gemischte Bedrohung“
<http://www.searchsecurity.de/definition/Blended-Threat-Gemischte-Bedrohung>
Stand Februar 2015

[Wiki-URL, Fred Cohen]
Wikipedia
„Fred Cohen“
<https://en.wikipedia.org/wiki/Fred_Cohen>
abgerufen am 15.08.2017

[Wiki-URL; Forkbomb]
Wikipedia;
„Forkbomb“
<https://de.wikipedia.org/wiki/Forkbomb>;
Stand vom 09.01.2017

[Wiki-URL; Multilateralität]
Wikipedia
„Multilateralität“
https://de.wikipedia.org/wiki/Multilateralit%C3%A4t
Stand: 07.01.2016

[Wiki-URL; Spam]
Wikipedia;
„Spam“
<https://de.wikipedia.org/wiki/Spam>
Stand vom 23.07.2017

[Wiki-URL; Unilateralität]
Wikipedia
„Unilateralität“
https://de.wikipedia.org/wiki/Unilateralit%C3%A4t
Stand 20.02.2017

[BGB-2017-B]

„Bürgerliches Gesetzbuch“

Hrsg.: Deutscher Taschenbuch Verlag

55. Auflage; 2017

[StGB-2012-B]

„Strafgesetzbuch“,

Hrsg.: Deutscher Taschenbuch Verlag

50. Auflage; 2012

[UWG-2016-URL]

„Gesetz gegen den Unlauteren Wettbewerb“

<https://dejure.org/gesetze/UWG>

abgerufen am 22.06.2017

[UWG-2016-URL, Kap. 1]

„Gesetz gegen den Unlauteren Wettbewerb“

§7 Unzumutbare Belästigungen,

<https://dejure.org/gesetze/UWG/7.html>

abgerufen am 22.06.2017