Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Krisztina Ágota Gyarmati

Untersuchung der Erkennung von Malware auf Microsoft Systemen

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Krisztina Ágota Gyarmati

Untersuchung der Erkennung von Malware auf Microsoft Systemen

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Angewandte Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter: Prof. Dr.-Ing. Martin Hübner

Eingereicht am: 31.05.2016

Krisztina Ágota Gyarmati

Thema der Arbeit
Untersuchung der Erkennung von Malware auf Microsoft Systemen

Stichworte
Malware, Malwareerkennung, Systemsicherheit, Microsoft, AV-Test, VirusTotal

Kurzzusammenfassung
Thema dieser Arbeit ist eine Analyse der Microsoft Malwareerkennung. Hierfür wird ein genauerer Blick auf die Microsoft Sicherheitstools geworfen. Microsoft hat oftmals bei den Sicherheitstests von AV-Test schlecht abgeschnitten. Diese Testverfahren verwenden Malware Samples. Eine Analyse dieser Samples soll zeigen, warum Microsoft eine schlechte Platzierung erreicht hat. Hierfür werden Malwareinformationen herangezogen, die von VirusTotal zur Verfügung gestellt werden. Daraufhin folgt eine Bewertung der Ergebnisse. Im Anschluss werden Lösungen für die Verbesserung der Malwareerkennung von Microsoft diskutiert.
Krisztina Ágota Gyarmati

Title of the paper
A study about malware detection on Microsoft Systems

Keywords
Malware, malware detection, system security, Microsoft, AV-Test, VirusTotal

Abstract
The purpose of this work is an analysis of the Microsoft malware detection. Therefore a closer look at the Microsoft antimalware products is going to be taken. Microsoft often achieved poor results in security tests performed by AV-Test. These tests use malware samples. The analysis of those samples should indicate why Microsoft achieved a low ranking. For this examination malware information available on VirusTotal.com will be used. Afterwards the results are going to be evaluated. Finally solutions for the improvement of Microsofts malware detection will be discussed.

Inhaltsverzeichnis

Danksagungen

Ich möchte mich an dieser Stelle bei Herrn Maik Morgenstern, Geschäftsführer und technischer Leiter der AV-TEST GmbH, bedanken. Die Bereitstellung der Testinformationen hat die Realisierung einiger Bereiche dieser Bachelorarbeit erst ermöglicht.

Daneben gilt mein Dank Herrn Karl Hiramoto, Technical Account Manager von VirusTotal. Er stellte mir einen kostenlosen VirusTotal Private-API-Key zur Verfügung, um die Funktionalitäten der Privat-API verwenden zu können.

1 Einleitung

Ein Leben ohne Computer und Internet ist heutzutage kaum vorstellbar. Man braucht ständig die aktuellsten Informationen und muss immer auf dem Laufenden sein. Oft geraten die Risiken in den Hintergrund. Die Cyberkriminalitätsrate steigt stetig und die Methoden der Angreifer werden immer komplexer. Doch was ist Cyberkriminalität genau?

Cyberkriminalität ist sehr vielseitig. Ein Trojaner kann ohne das Wissen des Anwenders auf den Computer gelangen und dort weitere Anwendungen, wie Keylogger, installieren. Auch Spam E-Mails leiten Nutzer auf scheinbar harmlose Internetseiten weiter, die getarnte Schadsoftware anbieten. Auf diesen Websites können sich Crimeware-Programme wie Tastenaufzeichner, Viren, Rootkits oder Trojaner verstecken.

Eine weitere und häufig genutzte Hintertür der Angreifer sind Sicherheitslücken und Softwarefehler. Durch solche Lücken, zum Beispiel in einem Browser, können Cyberkriminelle unbemerkt Trojaner oder andere Schadsoftware auf den Rechner des Opfers schmuggeln.

Ein mögliches Szenario ist der Diebstahl und die Manipulation von Daten. Auch Dienste werden durch Hacker bedroht. Zur Cyberkriminalität gehören des Weiteren der Identitätsdiebstahl sowie Bank- oder E-Commerce-Betrug (vgl. norton.com, 2016).

Die Motive der Cyberkriminellen sind fast so breit gefächert wie ihre Methoden. Manche handeln aus Neugier oder aus Langeweile, andere wollen sich mächtig fühlen. Weitere Beweggründe sind politische, religiöse, wirtschaftliche oder destruktive Ziele.

Informationen können einen großen Wert besitzen. Aufgrund dessen geraten immer häufiger große Einrichtungen oder sogar Behörden ins Visier der Cyberkriminellen. Nicht nur der Reputationsverlust durch die Veröffentlichung wichtiger Betriebs- oder Kundeninformationen, sondern auch die Instandsetzung kompromittierter Systeme kostet Zeit und Geld. Hierdurch entstehen enorme Schäden (siehe Abbildung 1.1).

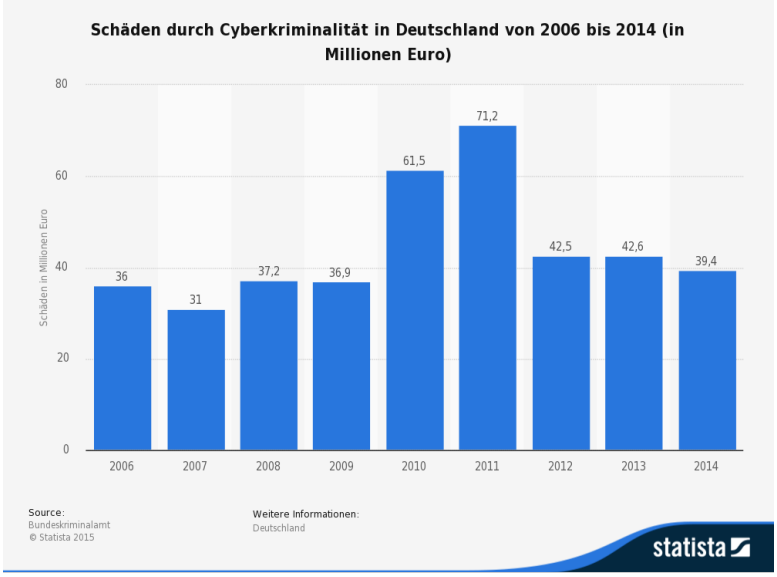

Abbildung 1.1: Cyberkriminalität in Deutschland in den letzten Jahren - Quelle : statista.com (2016)

Angreifer können auch die Kontrolle über industrielle Steueranlagen gewinnen. Die Inbesitznahme der Kontrolle einer Steueranlage stellt nicht unbedingt das primäre Ziel dar und kann unter Umständen als Nebenwirkung eines Angriffs gewertet werden (siehe BSI Lagebericht, 2015, S. 20).

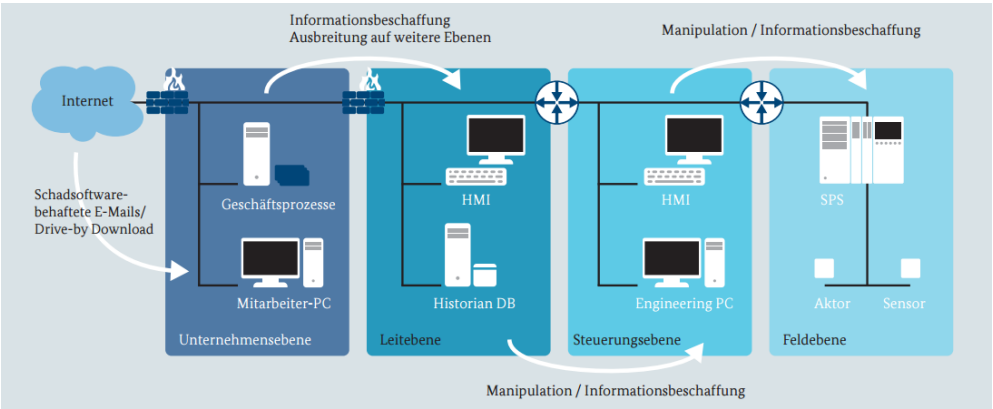

Abbildung 1.2: Ablauf mehrstufiger Angriffe auf eine typische industrielle Steueranlageninfrastruktur - Quelle : BSI Lagebericht (2015)

Am 25. Juli 2015 ist das neue IT-Sicherheitsgesetz in Kraft getreten. Ziel dieses Gesetzes ist die Verbesserung der IT-Sicherheit, um zukünftige Angriffe erfolgreich abwehren zu können.

Zur IT-Sicherheit gehört die Gewährleistung von Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität. Das Gesetz gilt für Unternehmen, die zu den "Kritischen Infrastrukturen", kurz KRITIS, gehören. Auch Dienstleister von KRITIS-Betreibern sind indirekt betroffen.

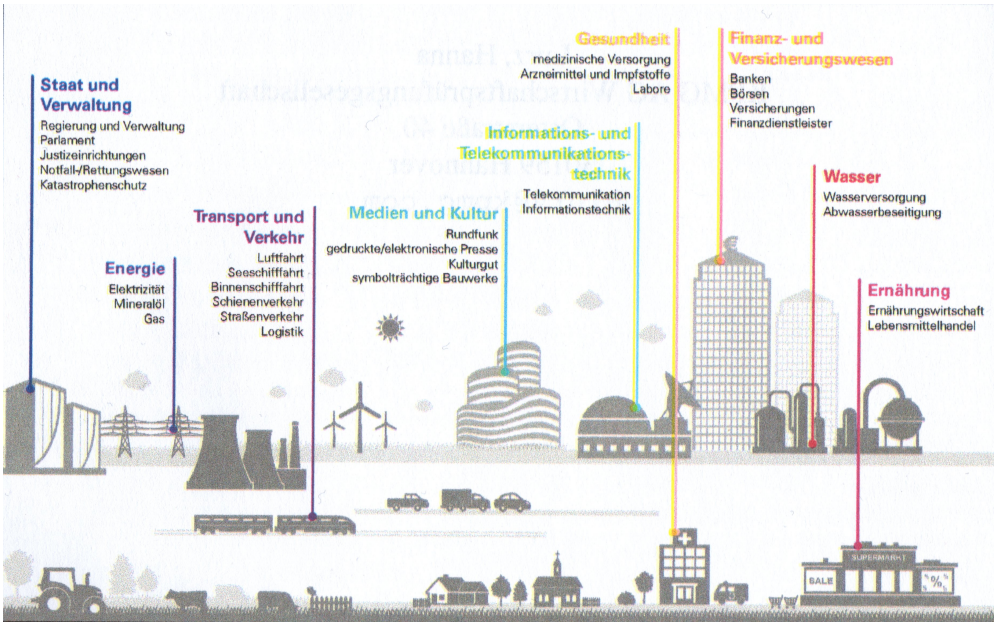

Abbildung 1.3: Sektoren- und Brancheneinteilung kritischer Infrastrukturen - (Quelle: DFN-Konferenz, 2016)

Das IT-Sicherheitsgesetz beinhaltet Verpflichtungen, wie die Einhaltung branchenspezifischer Mindeststandards, regelmäßige Sicherheitsüberprüfungen und die Meldepflicht von Sicherheitsvorfällen (vgl. IT-Sicherheitsgesetzentwurf, 2014, S. 1-2).

In dem neuen Lagebericht vom Bundesamt für Sicherheit in der Informationstechnik steht: “Statt einer reinen Abwehr gegen Angriffe gehört es zum Risikomanagement einer Organisation, sich darauf einzustellen und darauf vorzubereiten, dass ein IT-Sicherheitsvorfall eintritt oder ein Cyber-Angriff erfolgreich ist (Paradigma: Assume the Breach).” (BSI Lagebericht, 2015)

1.1 Problemstellung

Heutzutage existiert eine Vielzahl an Tools und Software, mit denen man sich gegen Cyberangriffe schützen kann. Es gibt unterschiedliche kostenlose oder kostenpflichtige Antivirenprogramme mehrerer Anbieter. Diese Schutzprogramme sind auf Privatpersonen oder Unternehmen unterschiedlicher Größe spezialisiert. Durch das breite Spektrum der angebotenen Produkte ist es wichtig den richtigen Schutz, passend zu den Bedürfnissen des Anwenders, zu finden. Unabhängige Testinstitute vergleichen daher die diversen Sicherheitslösungen anhand verschiedener Kriterien und erleichtern dadurch die Produktauswahl des Anwenders. Die Frage, die sich nun stellt besteht darin, ob ein schlecht bewertetes Sicherheitsprogramm zum Einsatz kommen sollte.

Auch Microsoft bietet eine Sicherheitslösung für kommerzielle Anwender an. Diese wird unter dem Namen *Microsoft System Center Endpoint Protection* vermarktet. Bei einer direkten Gegenüberstellung zu anderen namhaften Herstellern von Sicherheitssoftware schnitt Microsoft mangelhaft ab. Worin bestehen die Ursachen? Bedeutet diese Bewertung eine generelle Distanzierung von Microsofts Sicherheitsprodukten?

1.2 Ziel der Arbeit

Das Ziel dieser Bachelorarbeit besteht darin, die Malwareerkennung von Microsoft zu analysieren. Hierfür werden die Testergebnisse von AV-Test in den Testphasen März/April 2015 und Juli/August 2015 untersucht. Die Grundlagen von Malware, Malwareerkennung und Systemsicherheit werden erläutert. Darauf folgt eine Vorstellung weiterer Microsoft Sicherheitsprodukte.

Anhand der Informationen, der in den Tests verwendeten Malware, werden Rückschlüsse gezogen, welche evaluieren sollen, warum Microsoft eine schlechte Testplatzierung erreicht hat. Abschließend folgt eine Diskussion der gewonnenen Erkenntnisse und mögliche Verbesserungsvorschläge werden formuliert.

1.3 Abgrenzungen

Aufgrund der Vielzahl an Tests und Bewertungen, die man online findet, habe ich mich auf die Analyse der Tests von AV-Test beschränkt. AV-Test ist ein unabhängiges Testinstitut, das über langjährige Erfahrung verfügt und ausschließlich mit selbst gesammelten Daten arbeitet. Diese Faktoren ermöglichen eine objektive Bewertung der Testkandidaten. Eine weitere Abgrenzung besteht darin, dass ausschließlich Testergebnisse von März/April 2015 und Juli/August 2015 für Unternehmen mit Windows 7 Betriebssystem näher betrachtet und analysiert werden.

1.4 Struktur dieser Bachelorarbeit

Die vorgestellten Themen werden in sechs Kapiteln behandelt. Nach diesem Kapitel folgen die Grundlagen zu Malware, Malwareerkennung und Systemsicherheit (Kapitel 2). Die wichtigsten Malwarearten werden präsentiert und die Funktionsweise von Malwareerkennung erklärt. Des Weiteren wird der Begriff Systemsicherheit erläutert.

Darauf folgt die Vorstellung der Sicherheitslösungen von Microsoft (Kapitel 3) und eine Analyse von *System Center Endpoint Protection* anhand der Testdaten von AV-Test (Kapitel 4). Eine Visualisierung der den Tests zugrundeliegenden Malwareinformationen erleichtert die Erkennung möglicher Zusammenhänge und Sicherheitslücken. Im Kapitel 5 werden die Analyseergebnisse bewertet. Am Ende dieser Arbeit (Kapitel 6) wird die Frage beantwortet, ob die Sicherheitsprodukte von Microsoft eine ausreichende Systemsicherheit bieten.

2 Grundlagen

Malwareerkennung ist eines der wichtigsten und kompliziertesten Themen der Informatik. Hacker finden immer wieder neue Wege und Sicherheitslücken, wodurch sie die Sicherheit eines Systems schwächen können. Um die Schwere eines Angriffs einschätzen zu können, müssen wir verstehen, wie Schadsoftware agiert und welche möglichen Konsequenzen aus Cyberangriffen resultieren. Dieses Kapitel beschäftigt sich mit der Erläuterung der Begriffe Malware, Malwareerkennung und Systemsicherheit. Die wichtigsten Malwarearten und deren Funktionsweise werden präsentiert.

2.1 Malware

Malware beschreibt ein Stück Software, dessen Ziel in einer Beschädigung oder Beeinträchtigung der Funktionalität des zu attackierenden Systems liegt. Diese Software agiert ohne Erlaubnis oder Kenntnis des Benutzers. Malware kann Remotezugriffe zu infizierten Systemen ermöglichen, Informationen aufzeichnen und an Dritte senden. Oftmals wird die Kompromittierung des Zielsystems verborgen. Außerdem können bereits aktivierte Sicherheitsmaßnahmen unterbunden werden. Resultierende Effekte sind die Beschädigung des betroffenen Systems, oder die Beeinflussung von Daten- oder Systemintegrität.

Durch die bequeme und einfache Bedienung von Schadsoftware ist eine Automatisierung von Angriffen im größeren Umfang möglich. Kombinationen mit anderen Malwarearten sind hierbei nicht unüblich. Eine Selbstentwicklung des Quellcodes ist nicht notwendig und überschreitet nicht selten die Kompetenz des Angreifers. Deshalb wird Schadsoftware kommerzialisiert. Angriffe werden ermöglicht, die über den Fähigkeiten des Anwenders liegen. Schadsoftwares gefährden nicht nur Computer, sondern auch Smartphones, Server und Netzwerke (vgl. OECD, 2009, S. 21-22).

Durch Social Engineering können Angreifer schnell Vertrauen aufbauen und Computer mit Malware unterwandern.

2.1.1 Malware-Arten

Malwarearten werden oft durch ihre Funktionalität und ihr Verhalten kategorisiert. So entstand die Bezeichnung “Virus” für sich schnell verbreitende Malware. Arten, die sich ohne fremde Hilfe replizieren können, werden “Wurm” genannt. Immer häufiger wird von zwei Kategorien gesprochen: “family” und “variant”. Als Family wird eine eigenständige neue Malwareart bezeichnet. Eine Modifizierung bereits existierender Malware fällt in die Kategorie Variant. Auch neue Versionen bereits bekannter Malware gehören zu dieser Kategorie.

Im Folgenden werden die wichtigsten Formen von Malware präsentiert.

Virus

Analog zu seinem biologischen Namensgeber findet eine Verbreitung durch die Infektion und Modifikation von Programmen oder Dateien statt.

Beim Öffnen eines infizierten Programms oder einer infizierten Datei wird auch das Virus ausgeführt. Eine weitere Fortpflanzung des Schadcodes wird ermöglicht.

Die Idee des selbst replizierenden Automaten wurde schon in 1953 von John von Neumann entwickelt (siehe Neumann, 1966). In der Historie der Viren ist der Creeper-Virus einer der Urväter. Im Laufe der Zeit wurden bösartige Programme immer komplexer und aggressiver. Malware von heute ist nicht mit den Anfängen vergleichbar. Deshalb ist das Verhalten des Creeper-Virus relativ harmlos. Dieses Programm hat sich im ARPANET fortbewegt und sich selbst repliziert. Das betroffene System druckte dann den folgenden Satz: “I’M THE CREEPER: CATCH ME IF YOU CAN”.

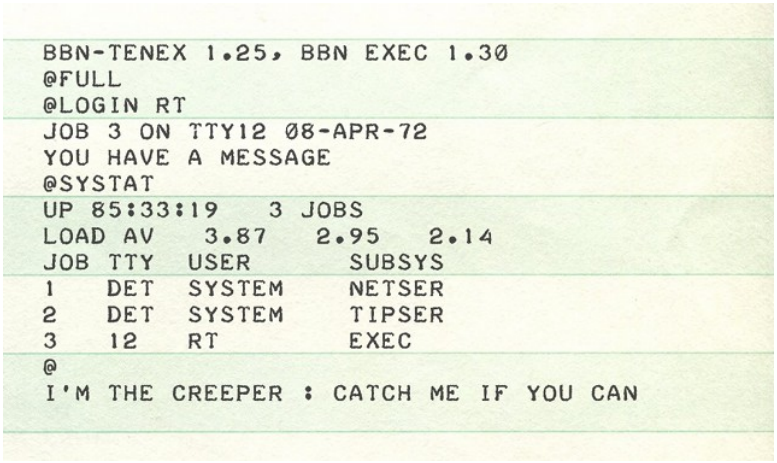

Abbildung 2.1: Die Ausgabe eines vom Creeper-Virus befallenen Rechners - Quelle: core-war.co.uk

Die Wirkung von Viren kann sehr unterschiedlich ausfallen. Die Intention einiger Viren liegt in einer reinen Verbreitung. Andere Viren zerstören gezielt Daten. Dies geschieht manchmal auch unbeabsichtigt durch Fehler in der Programmierung. Durch visuelle Effekte, oder die Ausgabe von Texten auf dem Bildschirm, wollen die Entwickler von Viren zeigen, dass sie erfolgreich in ein System eingedrungen sind.

Trojaner

Trojaner zeigen nicht ihre Absichten. Der erste Blick verrät nicht, dass es sich um eine bösartige Software handelt. Dadurch kann ein Trojaner Sicherheitsmaßnahmen einfacher umgehen und Schäden produzieren. Im Gegensatz zu einem Virus braucht ein Trojaner keinen Wirt, um sich weiter verbreiten zu können. Durch das Unwissen des Anwenders findet eine Verbreitung über Datenträger oder E-Mails statt. Auch durch einen Drive-by-Download kann ein Trojaner auf Rechner gelangen.

Der erste Trojaner hat sich als ein Spiel (“Pervading Animal”) getarnt. Sein Ziel war das Spiel in jedes Verzeichnis zu kopieren, auf das der Spieler Zugriff hatte. Verzeichnisse auf die mehrere Benutzer Zugriff hatten ermöglichten eine Verbreitung von “Pervading Animal”. Dieser Trojaner war nicht bösartig und hat keine schweren Schäden erzeugt.

Ein Trojaner erhält beim Programmstart automatisch alle Nutzerberechtigungen des jeweiligen Anwenders. Dies kann die Fernsteuerung oder Überwachung des Rechners, das Kopieren von Dateien und Daten (wie zB. Passwörter), das Herunterladen weiterer Schadsoftware oder das Deaktivieren von Sicherheitsprogrammen ermöglichen.

Backdoor

Als Backdoor (dt. Hintertür) wird ein Programm bezeichnet, das eine Netzwerkverbindung öffnet, um vom Hacker Remote-Anweisungen annehmen zu können. Auch die Infizierung mit anderer Malware wird hierdurch ermöglicht.

Eines der gefährlichsten Backdoor Programme ist “Beast”. In der Form eines Trojaners gelangt es auf Computer und pflanzt sich beim Programmstart mittels Replikation fort. Durch eine Reverse Connection können Firewalls ausgehebelt werden. Da Firewalls eingehende Verbindungen blockieren, baut die Malware eine Verbindung von dem Infizierten System zum Hacker auf. Hierdurch erlangt der Hacker einen vollständigen Zugriff auf das Zielsystem.

Abbildung 2.2: Der Beast-Client - Quelle: Wikipedia Beast

Die individuellen Schäden, die durch Backdoor Software verursacht werden, hängen ausschließlich von den Intentionen des Hackers ab. Diese bestehen zum Beispiel in der Spionage, Hard- und Softwaremanipulation oder der Datenänderung oder -vernichtung.

Wurm

Ein Wurm ist eine Malware, die sich ohne Wirtprogramm und menschliche Interaktion vermehren kann. Meistens werden Würmer durch den Anhang einer E-Mail verbreitet. Der Empfänger sieht, dass die E-Mail eine Datei mit dem Namen “urlaubsfoto.jpg” enthält, die in Wirklichkeit eine ausführbare Datei namens “urlaubsfoto.jpg.exe” ist. Da Dateiendungen oftmals ausgeblendet werden, denkt der Empfänger, dass es sich um eine Bilddatei handeln muss. Eine andere Tarnungsmöglichkeit für Würmer ist ein langer Dateiname, der nicht vollständig angezeigt werden kann. Dadurch bleibt die Dateierweiterung verborgen und die E-Mail erscheint harmlos.

Würmer können größere Schäden als Viren anrichten, da sie nicht nur Dateien löschen, sondern auch komplette Netzwerke durch Überlastung lahmlegen können.

Keylogger

Ein Keylogger ist ein Programm, das versteckt im Hintergrund läuft und den Tastaturpuffer des infizierten Rechners ausspäht. So können über das Internet sensible Informationen wie Passwörter weitergeleitet werden. Zu softwarebasierten Keyloggern existieren Alternativen. Eine weitere Möglichkeit der Spionage sind Hardwarelösungen in Form von Adaptern zwischen Computer und Tastatur.

Spyware

Spyware nimmt unterschiedliche Benutzereingaben (Mausbewegung oder das Tippen auf der Tastatur) auf. Auch das Auslesen des Bildschirminhaltes oder Zellen des Arbeitsspeichers ist möglich. Das Ziel besteht, wie der Name auch sagt, in einer totalen Spionage des Benutzers.

Adware

Adware ist eine Software, die zusätzlich zu ihrer angebotenen Funktionalität Werbung anzeigt. Meistens ist Adware nervig und recht harmlos. Dennoch kann auch Code enthalten sein, der den Benutzer ausspioniert.

Ransomware

Malware, die die Nutzung des Rechners voll oder teilweise einschränkt und Daten verschlüsselt, ist unter dem Namen Ransomware bekannt. Um den Computer wieder nutzen zu können, fordert der Angreifer eine Geldsumme. Eine etwaige Zahlung garantiert nicht die Freigabe der Daten und Behebung weiterer entstandener Schäden. Durch den Versuch eines seriösen Auftretens wird der Anschein geweckt, es handele sich beispielsweise um Erpressungen der Bundespolizei oder vom FBI.

Abbildung 2.3: Der “Bundestrojaner” - Quelle: giga.de

Rogueware

Rogueware täuscht vor, eine Sicherheitssoftware zu sein und behauptet, dass der Rechner infiziert wurde. Ohne ein sofortiges Handeln könnten entdeckte Schäden nicht repariert werden. Der gutgläubige Benutzer installiert die angebliche Antivirensoftware. Nach dem Herunterladen, was auch durch einen Drive-By Download passieren kann, installiert Rogueware oft weitere Schadsoftware. Es ist üblich, dass die Entwickler von Rogueware Geld des Benutzers fordern, um diese angebliche Antivirussoftware zu erwerben.

Rootkit

Ein Rootkit ist eine Sammlung von Programmen, die verbergen, dass der Rechner kompromittiert wurde. Dadurch kann der Angreifer weitere Programme installieren und dauerhaften Zugriff auf das Zielsystem erlangen. Rootkits sind tief im Betriebssystem versteckt. Funktionen des Betriebssystems werden modifiziert. Eine Antivirensoftware nutzt zum Beispiel die Funktion des Betriebssystems die Ordnerinhalte auflistet. Wurde diese Funktion durch ein Rootkit modifiziert, wird eine Erkennung durch Antivirenprogramme erschwert. Zwei Forscher, Corey Kallenberg und Xeno Kovah haben ein spezielles Rootkit entwickelt, dessen Persistenz sogar nach einem Festplattentausch erhalten bleibt. Nur durch ein BIOS-Update kann es entfernt werden (siehe Kallenberg und Kovah).

Botnetz

Ein Botnetz ist ein Netzwerk von Computern, deren Besitzer wider Willen die Infrastruktur des Botnetz anbieten. Der Besitzer des Botnetzes sendet Befehle in das wachsende verteilte System. Diese sind oftmals der Auftrag für Denial of Service Attacken. Hierbei etablieren alle Teilnehmer eine Netzwerkverbindung zu einem gemeinsamen Zielsystem, dessen Verfügbarkeit durch die Attacke ausfällt. Auch das versenden von Spam E-Mails fällt in den Aufgabenbereich von Botnetzen. Diese Möglichkeiten werden kommerzialisiert.

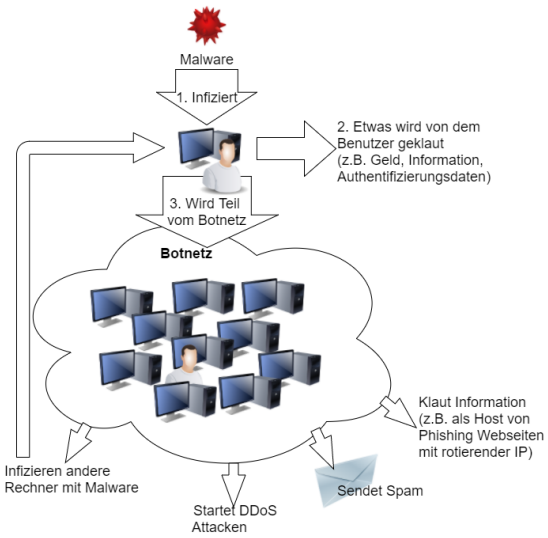

Abbildung 2.4: Botnetz Lebenszyklus

2.2 Malwareerkennung

Eine hundertprozentige Erkennungsrate ist praktisch unmöglich, da immer wieder neue Malware auftaucht. Laut Symantec gab es in 2015 54 Zero-Day-Exploits, also statistisch gesehen jede Woche eine neue Schwachstelle.

Eine Wiedererkennung bereits bekannter Schadsoftware ist deshalb nicht ausreichend. Antivirensoftware muss entscheiden können, ob eine verdächtige Datei eine mögliche Gefährdung darstellt.

2.2.1 Signaturbasierte Erkennung

Bei der signaturbasierten Erkennung wird geprüft, ob die Signatur eines Programms Übereinstimmungen mit einer Signatur in der Malwaredefinitionsbibliothek aufweist. Ist dies der Fall, handelt es sich um eine Malware. Der Erstellungsaufwand einer Signatur ist gering, deshalb kann etwaige Malware schnell determiniert werden.

Verfahren, die Bibliotheken verwenden, scheitern bei fehlenden Signatureinträgen. Unbekannte neue Malware und Programme der Kategorie Variant werden deshalb nicht detektiert.

Eine umgehende Signaturerstellung und Aktualisierung der Datenbank ist unabdingbar. Die Nutzung der neuesten Antivirendatenbank ist deshalb sehr wichtig.

Datenbankupdates entfallen durch die Möglichkeit Signaturen in der “Cloud” zugänglich zu machen. Ohne Internetverbindung ist eine Malwareerkennung des Antivirenprogramms deshalb nicht oder nur beschränkt verfügbar.

2.2.2 Heuristische Erkennung

Sobald das Wissen über ein System unzureichend ist, kommen Heuristiken zum Einsatz. Heuristische Erkennung von Malware werden auch verhaltensbasierte Erkennung genannt. Bei dieser Erkennungsmethode wird versucht Merkmale zu finden, die darauf hinweisen, dass eine Software bösartig sein könnte. Diese Methode erhöht die Wahrscheinlichkeit, dass eine unbekannte Schadsoftware oder ein Malware-Variant trotz fehlender Signatur erkannt wird. Nachteil dieser Methode sind häufige Fehleinstufungen analysierter Dateien. Harmlose Software wird eventuell als bösartig eingestuft.

Heuristische Scanner verwenden statische und dynamische Erkennungsverfahren.

Statische Scanner

Statische Scanner analysieren den Code der Software und versuchen bestimmte Muster oder Merkmale zu finden. Diese Erkennungsmethode funktioniert bei komprimierter, verschlüsselter oder selbst-modifizierender Malware nicht.

Dynamische Scanner

Bei der dynamischen Erkennung wird die Schadsoftware in einer Sandbox-Umgebung isoliert und kontrolliert ausgeführt. Die Sandbox trennt das Testsystem von den Auswirkungen der zu testenden Software. Das Verhalten nach Ausführungsbeginn der zu analysierenden Software wird beobachtet. Malware schützt sich unter Umständen vor dieser Analyse. Erkennt Malware, dass ihre Ausführungsumgebung eine Sandbox ist, legt sie ihr Verhalten ab und kann nicht von heuristischen Scannern erkannt werden.

Verfahren dynamischer Scans sind Ressourcen- und Zeitintensiv. Die maßgebliche Verwendung dieser Verfahren liegt bei den Herstellern von Antivirensoftware. Wurde eine Datei als schädlich klassifiziert, kann eine Signatur für den statischen Scan des Endkunden erstellt werden.

2.3 Systemsicherheit

In der Informationstechnik bedeutet Systemsicherheit den Schutz von Informationssystemen gegen Angriffe und unerwünschte Eingriffe. Die Grundpfeiler der Systemsicherheit sind die Authentizität, Vertraulichkeit, Integrität, Verfügbarkeit, Datenschutz und Verbindlichkeit.

Authentizität

Authentizität stellt sicher, dass Daten echt und glaubwürdig sind. Diese Daten stammen nachweisbar von dem korrekten Absender oder Hersteller.

Vertraulichkeit

Vertraulichkeit gewährleistet, dass unbefugte Personen Daten nicht einsehen, kopieren oder interpretieren können.

Integrität

Die Integrität eines Systems kann durch die Beschädigung oder das Zerstören von kritischen Ressourcen verletzt werden. Des Weiteren induziert das Verfälschen oder die Manipulation von Daten einen Integritätsverlust.

Verfügbarkeit

Verfügbarkeit beschreibt den uneingeschränkten Zugang zu Daten, Programmen, Ressourcen oder Geräten eines Systems. Denial of Service Angriffe durch Botnetze stellen zum Beispiel eine Verletzung der Verfügbarkeit dar.

Datenschutz

Datenschutz wird durch den Schutz personenbezogener Daten realisiert. Geräte die sensible Daten speichern müssen geschützt werden. Datenschutz ist Ländersache und der Begriff kann unterschiedlich ausgelegt werden.

Verbindlichkeit

Verbindlichkeit stellt sicher, dass die Durchführung einer Aktion (z.B. das Senden und Empfangen einer Nachricht) nachweisbar ist und die beteiligten Personen zugeordnet werden können.

IT-Sicherheit behandelt auch den Schutz bestimmter Güter. Zu diesen Gütern gehören sowohl Gegenstände als auch Personen oder der Ruf eines Unternehmens. Mögliche Schwachstellen können Güter angreifbar machen. Jede Schwachstelle erhöht das Risiko ein Ziel darzustellen.

$$Risiko = mögliche\,Schadenshöhe * Eintrittswahrscheinlichkeit \tag{2.1}$$

Um die Sicherheitsgrundwerte einzuhalten, werden Sicherheitsanforderungen formuliert. Dabei werden die Schutzziele festgelegt, die sich aus bestimmten Risiken und Schwachstellen ergeben. Aus diesen Anforderungen werden Sicherheitsmaßnahmen abgeleitet, die vor einer Bedrohung schützen sollen.

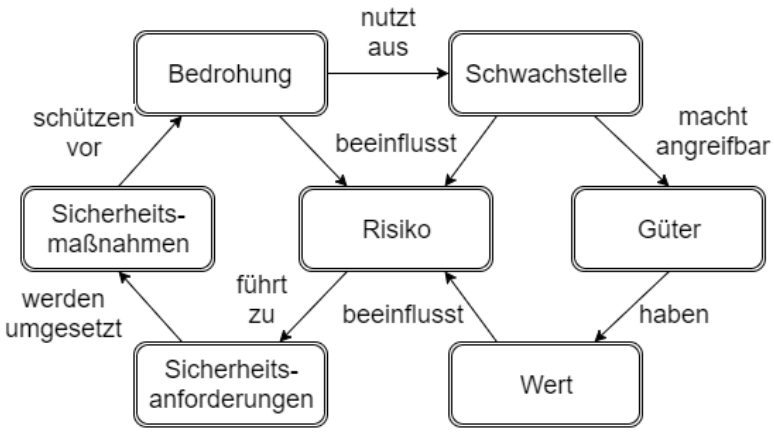

Abbildung 2.5: Zusammenhänge in der IT-Sicherheit - Quelle: Kossakowski (2016)

Die folgenden Sicherheitsmechanismen erhöhen die Grundsicherheit eines Informationssystems.

Authentisierung

Authentisierung sichert die Identität der Akteure (z.B Sender und Empfänger einer Nachricht, oder die Identität des Benutzers eines Rechners).

Zugriffsschutz

Zugriffsschutz stellt sicher, dass nur befugte Personen oder Prozesse auf Ressourcen zugreifen können.

Informationsflusskontrolle

Informationsflusskontrolle ist die Überwachung des Informationsflusses kommunizierender Instanzen. Bei Auffälligkeiten müssen die Akteure dieser Vorgänge identifiziert werden können.

Verschlüsselung

Verschlüsselung dient zur Geheimhaltung des Inhalts von Nachrichten oder Informationen.

Verbergen

Daten werden mit Hilfe von Steganographie in anderen Daten eingebettet und damit verborgen.

Inferenzkontrolle

Inferenzkontrolle bezweckt das Verhindern einer Deanonymisierung. Auch die Verschleierung von Kontexten zwischen Daten ist eines der Ziele.

Protokollierung

Um die Nachvollziehbarkeit sicherheitsrelevanter Abläufe zu gewährleisten, werden alle notwendigen Informationen, die der Klärung von Auffälligkeiten dienen, festgehalten und dokumentiert.

Einbruchsentdeckung

Es ist wichtig, Angriffe frühzeitig zu erkennen. Die Schädigung eines Systems kann so begrenzt werden. Durch das Aufdecken von Sicherheitslücken können Sicherheitslücken umgehend geschlossen werden.

Eine der kritischsten Schwachstellen ist der Mensch. Diese Schwachstelle wird durch das Social Engineering (auch Social Hacking) ausgenutzt. Hierbei werden Menschen so beeinflusst, dass sie Sicherheitsvorkehrungen umgehen und sensible Informationen preisgeben.

Menschen sind einfach zu manipulieren, da schnell eine Vertrauensbasis aufgebaut oder vorgetäuscht werden kann. Gegen Social Engineering kann keine Sicherheitssoftware helfen. Diese Gefahr kann nur durch das Training der Mitarbeiter eingedämmt werden.

3 Unterstützung der Malwareerkennung durch Microsoft

Die Vorgänger der heutigen Antivirenlösungen von Microsoft sind *Windows Live OneCare* und *Microsoft Forefront*.

Windows Live OneCare war eine kostenpflichtige Software zur Absicherung und Optimierung von Windows Betriebssystemen. Die Veröffentlichung von *Windows Live OneCare 2.5* fand am 3. Juli 2008 statt. Circa ein Jahr später wurde der Verkauf eingestellt und seit April 2011 gibt es keinen weiteren Support für die Software (vgl. WinOneCare, 2015)

Microsoft Forefront war eine Sicherheitslösung für Rechnernetzwerke, Server und Endgeräte von Unternehmen. Am 12. September 2012 wurden alle *Forefront* Produkte vom Markt genommen. *Forefront Identity Manager* ist weiterhin erhältlich.

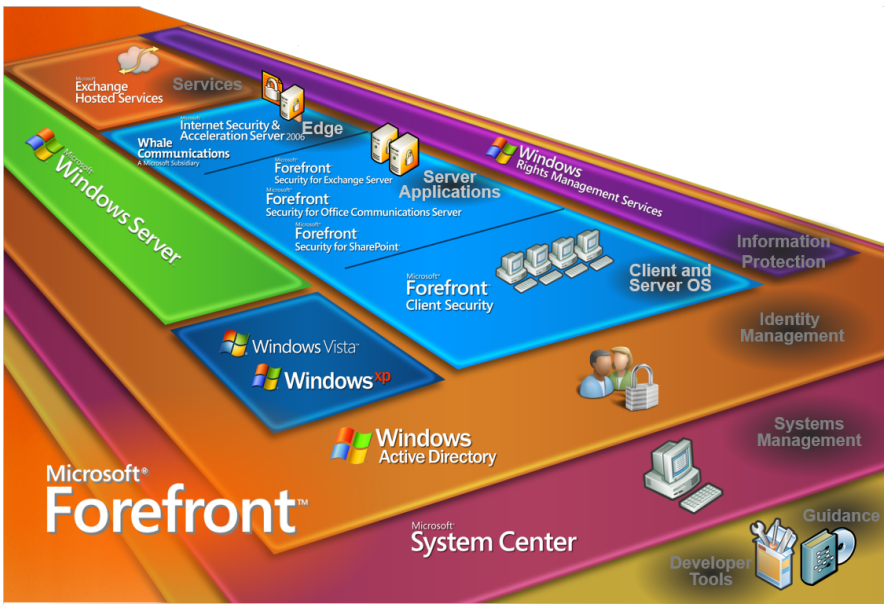

Abbildung 3.1: Microsoft Forefront Security - Quelle: Stix (2008)

Forefront Endpoint Protection, *Forefront Client Security* und *Client Protection* werden durch *System Center Endpoint Protection* abgelöst (vgl. TechNet Forefront, 2012).

Seit 2009 stellt Microsoft unterschiedliche kostenlose Tools für Malwareerkennung zur Verfügung. Dieses Kapitel stellt diese Produkte vor. Nicht für alle Windows Versionen existiert ein äquivalenter Schutz vor bösartigen Angriffen. Die Güte des Schutzes, verschiedener Windows Betriebssysteme durch Microsoft Produkte, können wir aus der Tabelle 3.1 entnehmen.

*	Firewall	Automatische Updates	Antivirus Technologie	Antispyware Technologie
Windows 8	Ja, sie ist automatisch eingeschaltet.	Ja, automatisch eingeschaltet.	Ja, durch Windows Defender	Ja, durch Windows Defender für Windows 8.
Windows 7	Ja, sie ist automatisch eingeschaltet.	Ja, automatisch eingeschaltet.	Nein, man kann aber Microsoft Security Essentials herunterladen.	Ja, durch Windows Defender für Windows 7.
Windows Vista Service Pack 2	Ja, sie ist automatisch eingeschaltet.	Ja, automatisch eingeschaltet.	Nein, man kann aber Microsoft Security Essentials herunterladen.	Nein, man kann aber Microsoft Security Essentials herunterladen.
Windows XP Service Pack 3	Ja, sie ist automatisch eingeschaltet.	Die Unterstützung ist eingestellt.	Nein.	Nein.
Windows Vista ohne Service Pack	Ja, sie ist automatisch eingeschaltet.	Die Unterstützung ist eingestellt. Ein kostenloses Upgrade auf Windows Vista SP2 ist möglich.	Nein, man kann aber Microsoft Security Essentials herunterladen.	Nein, man kann aber Microsoft Security Essentials herunterladen.
Windows XP ohne Service Pack	Ja, sie ist aber nicht automatisch eingeschaltet.	Die Unterstützung ist eingestellt.	Nein.	Nein.

Tabelle 3.1: Malwareschutz wichtiger Windows Betriebssysteme - Quelle: Microsoft Safety & Security Center

Um eine höhere Sicherheit zu erreichen empfiehlt Microsoft die kontinuierliche Benutzung einer Firewall und das regelmäßige Herunterladen und Installieren der neusten Updates.

Auch die Benutzung eines Antivirenprogramms und eines Antispywareprogramms sollte Anwendung finden.

3.1 Malwareerkennung von Microsoft

Microsoft Antimalware-Produkte verwenden eine Malwaredefinitionsbibliothek. Diese Bibliothek wird durch eine Datenbank realisiert, die Informationen über bösartige Dateien und deren Eigenschaften enthält. Regelmäßige Aktualisierungen durch Malwaredefinitionen erweitern ihren Informationsgehalt.

Neu entdeckte oder durch Benutzer gemeldete bösartige Dateien werden von Forschern bei Microsoft überprüft und nach Schweregrad und Typ kategorisiert. Welche Definitionen für Dateien in die Malwaredefinitionsbibliothek aufgenommen werden, entscheiden die Forscher durch die Auswertung folgender Kriterien (vgl. Malware Protection Center, a).

Unerwünschtes Verhalten

Wenn nicht eindeutig erkennbar ist, welche Funktion ein Programm besitzt, oder ob das Programm aktuell ausgeführt wird, ist die Kontrolle über das Programm beschränkt. Diese Eigenschaften können genutzt werden, um Malware zu erkennen. Andere Erkennungsmerkmale sind das Löschen oder Installieren anderer Software ohne Erlaubnis des Benutzers, oder die Unterdrückung der Dialoge von Systemkomponenten. Malware behauptet oftmals selbst ein Microsoft-Produkt zu sein.

Auch die Kontrolle des Nutzers kann eingeschränkt werden. Der Benutzer muss immer in der Lage sein den Lebenszyklus eines Programms zu kontrollieren und zugeteilte Berechtigungen zu ändern.

Bei Kontrollverlust über Programme, oder einem Entzug der Änderungsmöglichkeiten von Softwareeinstellungen, ist eine Kompromittierung des Computers höchst wahrscheinlich. Sollten Routing Entscheidungen bei der Netzwerkkommunikation, oder eine Reinterpretation von Website-Inhalten stattfinden, ist ein weiteres Indiz der Infektion gegeben.

Auch ein ungewolltes Installations- und Deinstallationsverhalten kann nach Systeminfektionen beobachtet werden. Programme sollen einen klaren Installationsvorgang durchlaufen, der von dem Benutzer gestartet und genehmigt werden muss. Die Entscheidung Programme zu entfernen oder zu ändern muss getroffen werden dürfen. Falls diese Vorgänge nicht möglich sind, geht ein hohes Gefährdungspotential von dem Programm aus.

Die Rechenleistung eines Computers kann durch Malware negativ beeinflusst werden. Schadsoftware behauptet nicht selten, eine Erhöhung der Rechenleistung mit sich zu bringen. Das Gegenteil ist weitaus wahrscheinlicher.

Werbung

Freie Software kann und darf Werbung anzeigen. Es gibt Faktoren, die eine Malware von gutartiger freier Software abgrenzt. Malware Programme versuchen den Benutzer durch Werbung auf infizierende Webseiten zu leiten. Programme, die solche Anzeigen schalten, müssen deinstalliert werden können. Die Werbung muss durch den Nutzer geschlossen werden dürfen. Eine eindeutige Inhaberschaft der Werbung muss erkennbar sein. Des Weiteren sollte Werbung keine Downloads starten.

Privatsphäre

Es ist wichtig, dass jederzeit bestimmt werden kann, welche Informationen wie verwendet werden. Eine Protokollierung des Nutzerverhaltens durch ein Programm erhärtet den Verdacht einer Malwarezugehörigkeit. Diese Protokollierung ist in einigen Fällen erwünscht. Kinderschutz-Software benutzt zum Beispiel ähnliche Methodiken wie Keylogger.

Meinung der Kunden

Microsoft legt großen Wert auf die Stimme von Kunden. An Microsoft gemeldete mögliche Gefährdungspotenziale werden sorgfältig analysiert. Nach dieser Analyse wird darüber entschieden, ob die Malwaredefinitionsbibliothek verfeinert wird.

3.2 Microsoft Security Essentials

Microsoft Security Essentials bietet kostenlosen Schutz vor Schadsoftware. Die Leistung des Rechners wird hierdurch nicht stark beeinflusst.

Dieses Tool wurde für Privatbenutzer und kleinere Unternehmen konzipiert. *Microsoft Security Essentials* bietet Echtzeitschutz gegen Malware und scannt den Rechner standardmäßig wöchentlich an einem Zeitpunkt der geringsten Benutzung des Computers. Programme und Treiber können erkannt werden, die Rootkits auf dem Computer installieren wollen. Die Entfernung dieser wird ermöglicht.

Mit einer dynamischen Signatur wird geprüft, ob ein Programm für den Rechner schädlich sein könnte. Indem *Microsoft Security Essentials* eine Ausführung des Programms simuliert,

wird eine Signatur erzeugt. Ein Abgleich mit Signaturen der Datenbank gibt Auskunft über den Gefährdungsgrad. Eine verhaltensbasierte Kontrolle laufender Programme soll für weitere Sicherheit sorgen. Schädliche Aktionen können unterbunden werden. Falls keine Firewall aktiv ist, empfiehlt Microsoft die standard Windows-Firewall zu verwenden (vgl. Microsoft Security Essentials).

Mögliche Bedrohungen werden in unterschiedliche Kategorien gefasst. Weit verbreitete und sehr schädliche Programme werden als "schwerwiegend" eingestuft. Zu den Kategorien "hoch" und "mittel" gehören Programme, die eine Verletzung der Privatsphäre des Benutzers nach sich ziehen, persönliche Informationen sammeln, den Computer beschädigen oder Systemeinstellungen ändern können. "Schwerwiegend" und "hoch" eingestufte Bedrohungen werden automatisch entfernt. Bei den Kategorien "mittel" und "niedrig" geben die Warnungsdetails Informationen darüber, warum das in Konflikt stehende Programm als potenziell unerwünscht eingeordnet wurde. Falls der Softwareanbieter bekannt ist, können diese Warnungen ignoriert werden (siehe Security Essentials Warnstufen).

Als Vorteil kann man die einfache Bedienbarkeit und die unauffällige Arbeit des Tools nennen. Zudem ist es kostenlos und wird täglich aktualisiert. Es hilft dabei einen Grundschutz für den Computer zu etablieren.

3.3 Windows Defender

Im Beta-Stadium wurde *Windows Defender Offline* vorgestellt. Der ursprüngliche Name war *Microsoft Windows AntiSpyware*. Dieses Tool hilft dabei schwierig erkennbare Schadprogramme aufzuspüren und zu entfernen. Die statische Suche verwendet hierfür Malwaredefinitionen. Malwaredefinitionen sind Dateien, die Informationen über schädliche Programme enthalten (vgl. Windows Defender Offline).

Die Benutzung des Tools ist simpel. *Windows Defender Offline* wird nach dem herunterladen auf einer CD, DVD oder USB Stick gespeichert. Dieser Schritt sollte auf einem nicht infiziertem Rechner erfolgen. Nach dem Bootvorgang des Mediums sucht *Windows Defender Offline* nach Schadprogrammen und entfernt die Gefahren.

Das Tool ist also kein Ersatz für ein Antivirenprogramm. Es stellt mehr die letzte Rettung dar, sollte die Bootfähigkeit des infizierten Rechners beeinträchtigt worden sein.

Seit Windows 8 ist *Microsoft Security Essentials* in *Windows Defender* integriert und bietet Echtzeitschutz und Scanoptionen (siehe Wikipedia).

3.4 Malicious Software Removal Tool

Das *Malicious Software Removal Tool* wurde am 13. Januar 2005 veröffentlicht. Es erkennt und entfernt aktuelle und verbreitete Viren, Würmer und Trojaner. Das Ziel der Spyware-Erkennung wird nicht verfolgt, hierfür soll laut Microsoft die Software *Security Essentials* verwendet werden. Das *Malicious Software Removal Tool* bietet eine hohe Kompatibilität zu verschiedenen Windows Versionen. Wenn automatische Updates eingeschaltet sind, wird das Tool am zweiten Dienstag jedes Monats automatisch aktualisiert.

Malicious Software Removal Tool ist kein wirklicher Ersatz für Antivirenprogramme. Es wird nur bekannte und weit verbreitete Malware erkannt, die aktuell auf dem Rechner ausgeführt wird. Es hilft dabei, einen bereits infizierten Rechner zu bereinigen. Ein präventiver Schutz gehört nicht zum Funktionsumfang.

Wenn keine Infektion vorhanden ist, bleibt das Tool im Hintergrund. Bei der Erkennung einer bösartigen Software informiert das *Malicious Software Removal Tool* den Benutzer, sollte er sich als Administrator des Systems angemeldet haben. Nach der Entfernung einer Infektion ist es empfehlenswert einen vollständigen Systemscan durchzuführen.

Infizierungsinformationen über den Befund werden an Microsoft weitergeleitet und analysiert. In der Knowledge Base (siehe Microsoft Support, 2016) stehen die Softwarefamilien, die von der aktuellen Version des *Malicious Software Removal Tools* erkannt werden.

Die Verwendung eines zusätzlichen Antivirenprogramms wird empfohlen, da *Malicious Software Removal Tool* nur Malware erkennen kann, wenn diese während der Analyse ausgeführt wird (siehe Microsoft Support, 2016).

3.5 Microsoft Safety Scanner

Microsoft Safety Scanner ist ein weiteres kostenloses Tool, das den Rechner nach Malware durchsucht und bereinigt. Es ist der Nachfolger von *Windows Live OneCare Safety Scanner*. Zehn Tage nach dem Download ist der *Safety Scanner* nicht mehr aktuell und sollte erneut heruntergeladen werden, um einen Scan mit den neusten Antimalware-Definitionen ausführen zu können. Die Software läuft ohne Installation und ist einfach in der Bedienung. Das Tool liefert unterschiedliche Scanmöglichkeiten und kann auch zum Einsatz kommen, während andere Antivirensoftware läuft (vgl. Microsoft Safety Scanner, 2011).

Wie bei dem *Malicious Software Removal Tool*, ist die Verwendung einer unterstützenden Antivirensoftware sehr empfehlenswert, um einen erhöhten Schutz vor Malware zu erreichen.

3.6 Enhanced Mitigation Experience Toolkit

Das *Enhanced Mitigation Experience Toolkit* hilft, mögliche Sicherheitslücken von Software zu schließen, noch bevor ein Patch bereitgestellt wird. Die neuste Version ist EMET 5.5, die auch Windows 10 unterstützt. EMET ist sowohl für Privatanwender als auch für Unternehmen geeignet. Die wichtigsten Sicherheitsfunktionen dieses Tools sind:

Datenausführungsverhinderung (Data Execution Prevention): Stellt zum Beispiel sicher, dass die Programme den Systemspeicher nur sicher und auf zulässige Weise verwenden.

Speicherverwürfelung (Mandatory Address Space Layout Randomization): hilft Angriffe abzuwehren, die einen Buffer Overflow ausnutzen.

Anti rücksprungsorientierte Programmierung (Anti Return Oriented Programming): EMET kann Angriffe verhindern, die mithilfe von rücksprungorientierter Programmierung, die Datenausfühungsverhinderung umgehen.

Whitelist für Zertifikate: Dies hilft zum Beispiel Man-in-the-middle-Angriffe abzuwehren. Zertifikataussteller für Domänen können hinterlegt werden.

Die vorgeschlagenen Einstellungen sind optimal, dennoch können leichte Anpassungen getroffen werden. Starke Änderungen in den Einstellungen können zu Problemen führen. Grund hierfür ist, dass das *Enhanced Mitigation Experience Toolkit* einige Operationen der Software als bösartig einstufen könnte und damit die Applikation blockiert.

Dieses Tool kann auch Angriffe durch noch unbekannte Malware erkennen und abwehren. Ein Nachteil des *Enhanced Mitigation Experience Toolkit* besteht darin, dass Privatanwender eine erhöhte Kenntnis über die Einstellungsmöglichkeiten haben müssen, um eine Grenze zwischen Fehlalarmen und wirklichen Angriffen ziehen zu können. Änderungen der Standardeinstellungen sind diffizil.

Die nachfolgende Abbildung 3.2 listet den Funktionsumfang von *Enhanced Mitigation Experience Toolkit* auf.

EMET Security Mitigations	Included
Attack Surface Reduction (ASR) Mitigation	✓
Export Address Table Filtering (EAF+) Security Mitigation	✓
Data Execution Prevention (DEP) Security Mitigation	✓
Structured Execution Handling Overwrite Protection (SEHOP) Security Mitigation	✓
NullPage Security Mitigation	✓
Heapspray Allocation Security Mitigation	✓
Export Address Table Filtering (EAF) Security Mitigation	✓
Mandatory Address Space Layout Randomization (ASLR) Security Mitigation	✓
Bottom Up ASLR Security Mitigation	✓
Load Library Check – Return Oriented Programming (ROP) Security Mitigation	✓
Memory Protection Check – Return Oriented Programming (ROP) Security Mitigation	✓
Caller Checks – Return Oriented Programming (ROP) Security Mitigation*	✓
Simulate Execution Flow – Return Oriented Programming (ROP) Security Mitigation*	✓
Stack Pivot – Return Oriented Programming (ROP) Security Mitigation	✓
Windows 10 untrusted fonts***	✓

** Available and applicable only to 32-bit processes*
**** Available on EMET 5.5 Beta, and available only for Windows 10*

Abbildung 3.2: Sicherheitsfunktionen des Enhanced Mitigation Experience Toolkit - Quelle: TechNet EMET

3.7 System Center 2012 Endpoint Protection

System Center 2012 Endpoint Protection von Microsoft wurde für die Verwaltung der Client-Sicherheit von Unternehmen konzipiert. Es bietet komplexe Überwachungsmöglichkeiten durch die *System Center 2012 Configuration Manager* Konsole. Der *Configuration Manager* steht *Endpoint Protection* zur Seite und erleichtert das Herunterladen der neusten Antimalware-Definitionen. Für unterschiedliche Benutzergruppen können verschiedene Antimalware Richtlinien und Windows-Firewall Einstellungen festgelegt werden.

Microsoft Endpoint Protection ist auf Schadsoftware-, Spyware- und Rootkiterkennung sowie die Systemwiederherstellung spezialisiert. Sicherheitsrisiken werden bewertet und Sicherheitslücken durch das Netzwerkinspektionssystem erkannt (vgl. TechNet System Center).

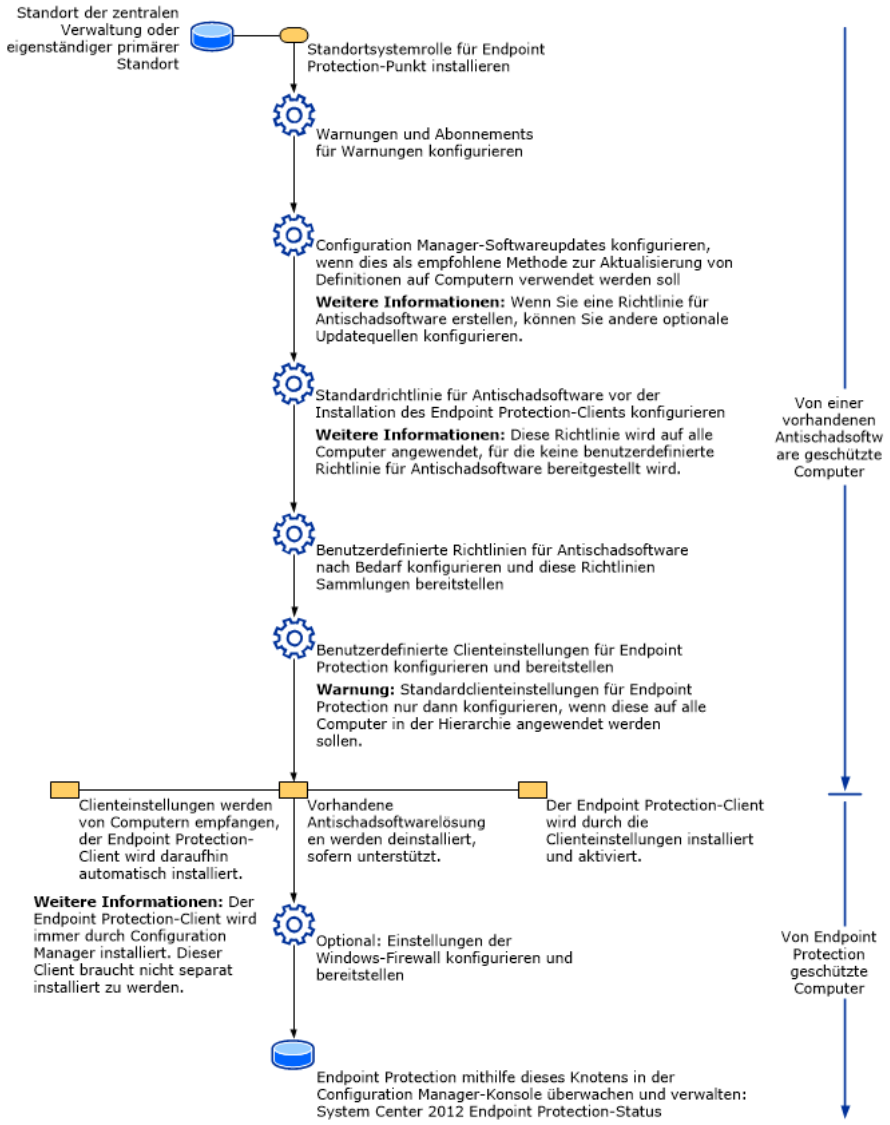

Abbildung 3.3: *Endpoint Protection*-Workflow - Quelle: System Center Endpoint Protection Einführung

Für die Verwendung von *System Center Endpoint Protection* wird ein Lizenz benötigt.

4 Analyse von Microsoft System Center Endpoint Protection

Dieses Kapitel stellt das Testverfahren von AV-Test vor. Darauf folgt die Analyse und die Visualisierung der Eigenschaften der Malwarearten, die von AV-Test verwendet wurden. Die gewonnenen Erkenntnisse werden diskutiert.

4.1 AV-Test

AV-Test ist ein unabhängiges Antiviren-Testlabor. Es ist weltweit führend in den Bereichen der IT-Sicherheit und der Antiviren-Forschung. Das Forschungsziel ist die schnelle Erkundung und ausführliche Analyse neuer Schadsoftware.

AV-Test bietet des Weiteren unterschiedliche Produkte zur Ermittlung, Kategorisierung und Analyse von Malwaredaten an.

Abbildung 4.1: Die AV-Test Produkte - Quelle: av-test.org Produkte

Sunshine ermöglicht das Ausführen potenziell schädlicher Dateien. Beobachtete Änderungen während der Laufzeit von Schadsoftware und die Netzwerkkommunikation des Testsystems werden für die weitere Verarbeitung analysiert und klassifiziert.

VTEST ist ein Multi-Virenscanner-System, das aus 40 unabhängigen Virenscannern besteht. Das Tool gleicht mehrere Millionen Dateien mit bekannten bösartigen Mustern ab. *VTEST*-Systeme arbeiten weltweit verteilt vollautomatisch und zeiteffizient.

FLARE ist ein Service, den AV-Test zur Fehlalarm-Prävention entwickelt hat. Firmenintern verwendet AV-Test *FLARE* für die Registrierung und Analyse von Fehlalarmen.

Die Forschungsumgebung enthält drei Serverräume und mehrere Labore. Der seit über 15 Jahren gesammelte Datenbestand umfasst 150 Millionen nicht schädliche und 330 Millionen

bösartige Testdaten. Dieser Bestand wächst täglich um circa 400.000 neue Einträge (vgl. av-test.org Laborausstattung).

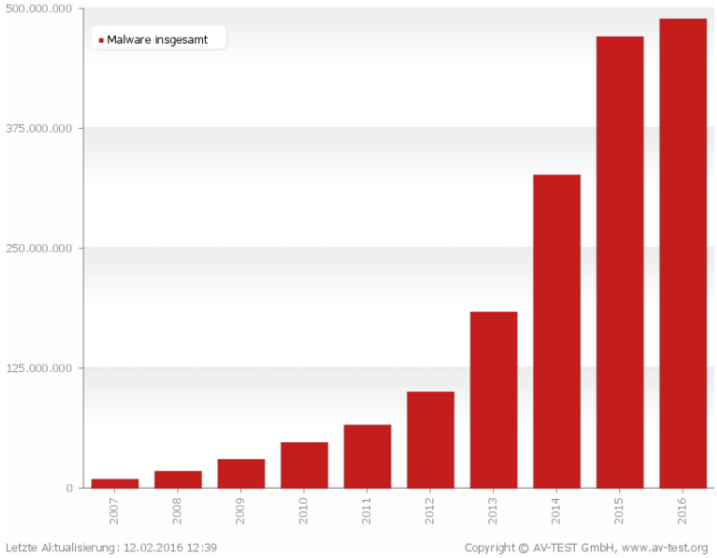

Abbildung 4.2: Anzahl der registrierten Malware der letzten 10 Jahre - Quelle: av-test.org Malware

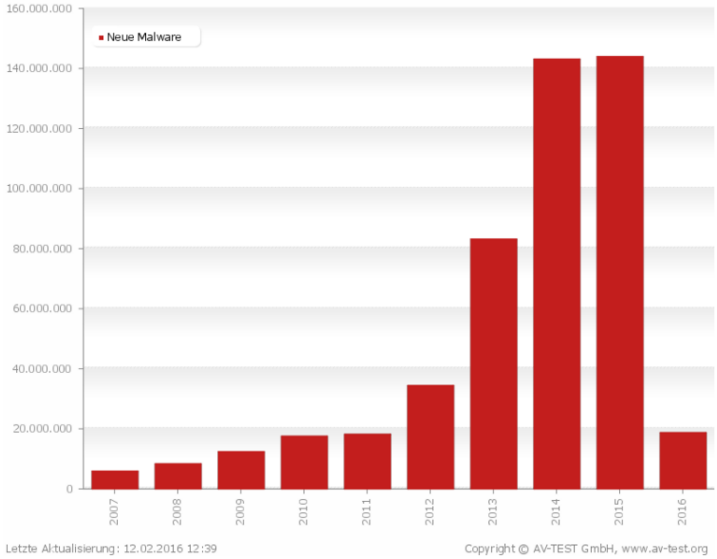

Abbildung 4.3: Anzahl der neu entdeckten Malware der letzten 10 Jahre - Quelle: av-test.org Malware

Auf Abbildung 4.2 kann man eine positive Wachstumstendenz entdeckter Malware seit 2012 erkennen.

Abbildung 4.3 zeigt, dass zwischen 2011 und 2014 die Menge neu entdeckter Malware nahezu exponentiell gestiegen ist.

In den spezialisierten Testlaboren werden mehr als 4500 individuelle Szenarien pro Jahr examiniert. Diese Tests finden auf realer Hardware statt. Als Laufzeitumgebung eine virtuelle Maschine zu wählen, könnte die Ergebnisse verfälschen. Durch selbst entwickelte Tools und den umfangreichen eigenen Datenbestand, kann AV-Test eine Unabhängigkeit, Testintensität und Qualität der Testergebnisse gewährleisten. Auf av-test.org Testverfahren steht: “Alle Analysen basieren auf eigenen, von AV-TEST ermittelten, analysierten und verarbeiteten Testsamples - zusammengetragen in einer der weltweit umfangreichsten Datenkollektionen”.

4.1.1 Testmodule

AV-Test vergibt Qualitätssiegel an getestete IT-Sicherheitsprodukte, die dem Sicherheitslevel des Zertifizierungsstandards zum Testzeitpunkt genügt haben. Das *AV-TEST CERTIFIED* Qualitätssiegel wird an Sicherheitsprodukte für Privatanwender vergeben. Das *AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION* Qualitätssiegel erhalten Produkte, die auf den Endpoint-Schutz im Unternehmen spezialisiert sind. Siegel werden vergeben, wenn Produkte mindestens einen Punkt jeder Kategorie und zehn Punkte der erreichbaren 18 Punkte verdienen.

Die Dauer des Zertifizierungsverfahrens beträgt zwei Monate. Kandidaten des Zertifizierungsverfahrens sind relevante Sicherheitsprodukte, die einem weiten Einsatz in der Praxis unterliegen (siehe av-test.org Zertifizierung).

Schutzwirkung

Bei Tests bezüglich der Schutzwirkung wird ermittelt, wie das Sicherheitsprodukt auf verschiedene Angriffsszenarien reagiert.

Der Test läuft (wie unter av-test.org Schutzwirkung beschrieben) folgendermaßen ab:
Die Produkte werden mit ihren Standardeinstellungen installiert und *Sunshine* erstellt ein Systemabbild. Das Verhalten des Sicherheitsprodukts wird anschließend dokumentiert, während bösartige Webseiten und E-Mails aufgerufen werden. Die ausgeführten Schritte werden dauerhaft von *Sunshine* überwacht. Hieraus geht hervor, ob Bedrohungen komplett oder nur teilweise blockiert wurden. Anhand der dokumentierten Informationen wird das Testergebnis evaluiert.

Jeder Testfall wird für alle Sicherheitslösungen gleichzeitig ausgeführt, um äquivalente Bedingungen zu gewährleisten. Die Komplexität der Tests ist immens. Deshalb wird lediglich mit

einer Teilmenge der zur Verfügung stehenden Bedrohungen gearbeitet. Die Aussagekraft des Testergebnisses ist dennoch realistisch, da getestete Bedrohungen oftmals eine Malwarefamilie bilden und die eingesetzten Bedrohungen aktuell sind.

Eine weitere Methode für die Bestimmung des Schutzes kommt zum Einsatz. Bei diesem Testverfahren wird die signaturbasierte Erkennung, Heuristiken und In-the-Cloud Abfragen der Schutzprogramme angesprochen. Der Test ist zweistufig. Für den Test wird Malware benutzt, die innerhalb der letzten vier Wochen vor Testbeginn durch AV-Test erkannt wurde. Zuerst werden die Schutzprogramme circa 10.000 bis 15.000 bösartigen Dateien ausgesetzt. Anschließend wird weit verbreitete Malware dieser Gruppe verwendet. Diese Menge enthält etwa 1.000 - 1.500 Malware Samples.

Geschwindigkeit

In diesem Testmodul wird die Systembelastung durch Herunterladen und Kopieren von Dateien, Installieren von Programmen sowie das Ausführen und Benutzen von Programmen getestet. Möglicherweise störende Funktionen, wie automatische Updates, werden für den Testzeitraum deaktiviert, sodass diese die Testergebnisse nicht verfälschen.

Diese Tests werden auf Computern mit gleicher Hardwarekonfiguration sieben mal durchgeführt. Der Mittelwert der Ausführungsdauer wird berechnet. Ein Testlauf mit einer hohen Abweichung der Ausführungsdauer wird wiederholt. Im Anschluss wird das Ergebnis mit den Werten eines Referenzsystems verglichen und die Differenz ergibt das Maß der Verlangsamung des Systems (vgl. av-test.org Geschwindigkeit).

Benutzbarkeit

Die Usability von Sicherheitssoftware spielt neben der Qualität der Erkennung eine wichtige Rolle. Bei dem Usabilitytest wird die Anzahl von Warnmeldungen und Fehlerkennungen untersucht, die durch nicht bösartige Software entsteht.

Weit verbreitete gutartige Programme werden heruntergeladen und installiert. Dabei wird beobachtet, ob falsche Warnungen durch das Sicherheitsprogramm entstehen, oder ob es den Benutzer um Zulassung bestimmter Aktionen bittet. Das Programm *Sunshine* überwacht den Installationsvorgang und prüft, ob die Ausführung des gutartigen Programms unterbunden wurde. Das Testresultat ergibt sich aus der Anzahl der Warnmeldungen und Blockierungen. Aufgrund der Komplexität des Tests wird nur mit einer Auswahl von Testprogrammen gearbeitet.

Um das Sicherheitsprogramm auf weitere False Positive Meldungen zu testen, wird eine Testmenge an Programmen aus dem AV-Test *FLARE* Archiv gescannt. Warnmeldungen

durch Programme, bei denen eine eindeutige Klassifizierung schwer ist, wie Remoteverwaltungssoftware und kommerzielle Keylogger, werden nicht berücksichtigt (vgl. av-test.org Benutzbarkeit).

Reparaturleistung

Im Bereich der Reparaturleistung wird die Fähigkeit zur Entfernung laufender Malware und die Erkennung versteckter Malware untersucht. Diese Tests werden mittlerweile in einem separaten Testbericht veröffentlicht. Neben Antiviren-Software werden auch Rettungsmedien und Reinigungsprogramme getestet.

Bei den Tests werden die Testsysteme mit relevanten Schädlingen infiziert. Die Aufgabe der getesteten Software besteht in der vollständigen Identifikation und Entfernung dieser Schädlinge. Eine der schwersten Herausforderung liegt darin, Schädlinge mit Rootkit-Funktionen zu erkennen, da diese sich sehr geschickt verstecken können. Die Testszenarien sind bei allen Sicherheitsprodukten exakt gleich (vgl. av-test.org Reparaturleistung).

4.1.2 Die Testergebnisse

AV-Test testet seit 2011 Sicherheitssoftware für Privatanwender und Unternehmen. Microsoft wurde bei jedem Testlauf vertreten. Zwischen 2011 und 2012 wurde *Microsoft Forefront Endpoint Protection 2010* und ab 2013 wurde der Nachfolger *Microsoft System Center Endpoint Protection* getestet.

Bis Juni 2012 hat das Microsoft Sicherheitsprodukt die Sicherheitsstandards von AV-Test eingehalten und das Zertifikatssiegel erhalten. Nach diesem Zeitpunkt hat Microsoft keine weiteren Zertifikatssiegel erhalten können.

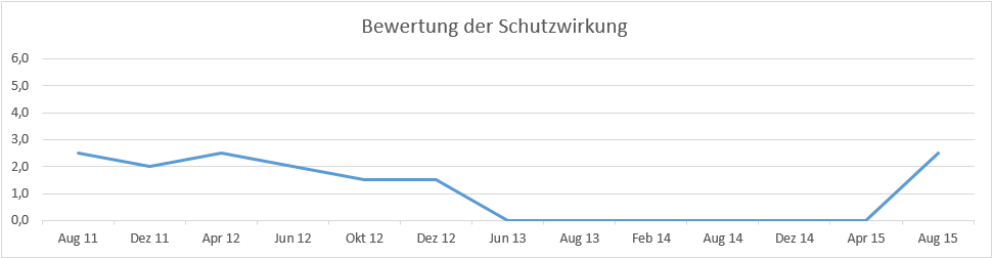

Abbildung 4.4: Bewertung der Schutzwirkung von Microsoft Sicherheitsprodukten für Unternehmen

Zunächst werden die Ergebnisse des Moduls für die Bewertung der Schutzwirkung analysiert. Diese Tests findet man unter av-test.org Testergebnisse.

Microsoft Forefront Endpoint Protection Testergebnisse

Microsoft Forefront Endpoint Protection konnte anfangs mit konkurrierender Sicherheitssoftware mithalten. Allerdings lagen die Ergebnisse in dem Testmodul der Schutzwirkung immer unter dem Industriedurchschnitt.

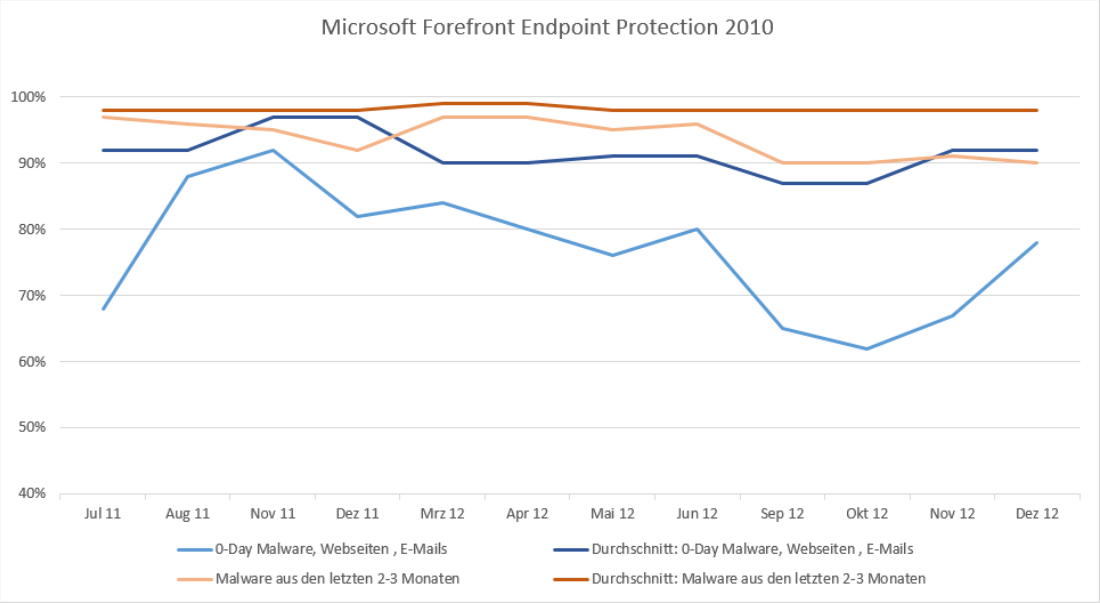

Abbildung 4.5: Die Testergebnisse von *Microsoft Forefront Endpoint Protection 2010*

Wie Abbildung 4.5 zeigt, gab es zwischen Juli und November des Jahres 2011 eine Verbesserung in der Erkennung von Zero-Day Malware, bösartiger Webseiten und E-Mails. Einen Tiefpunkt erreichte die Bewertung dieser Tests im Oktober 2012. Dieser Fall könnte mit der Einstellung der *Forefront* Produkte im September 2012 in Bezug stehen. Des Weiteren ist zu erkennen, dass die Bewertungen von *Forefront Endpoint Protection* den Schwankungen der Durchschnittsbewertung unterliegt.

Die Bewertung der Erkennung von Malware der letzten zwei bist drei Monate, vor der jeweiligen Testphase, weist eine geringere Abweichung von dem Industriedurchschnitt auf. Generell kann die Aussage getroffen werden, dass die Konkurrenz von Microsoft bessere Produkte als *Forefront Endpoint Protection* entwickelt hat. Dies geht aus der durchschnittlichen Erkennungsrate hervor.

Die Schwankungen der Bewertungen der zwei Testmengen aus Abbildung 4.5 sind bei dem Microsoft Sicherheitsprodukt sehr ähnlich.

Microsoft System Center Endpoint Protection Testergebnisse

Seit der Einstellung von *Microsoft Forefront* Produkten wurde *Microsoft System Center Endpoint Protection* getestet. Februar 2014 bildet eine Ausnahme. In diesem Monat wurde *Microsoft Security Essentials 4.4* unter die Lupe genommen.

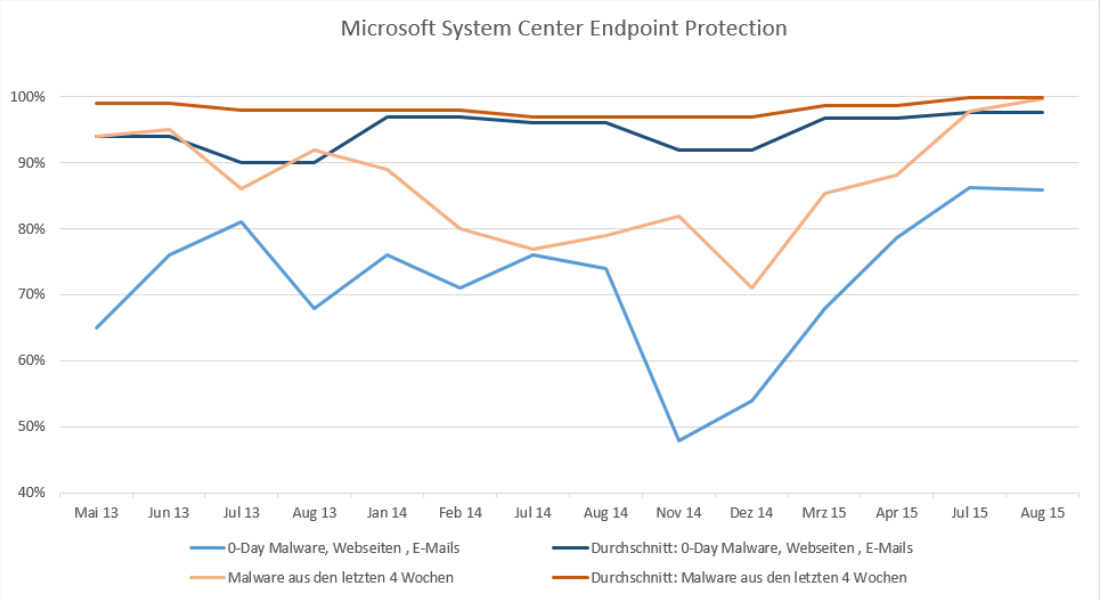

Abbildung 4.6: Die Testergebnisse von *Microsoft System Center Endpoint Protection*

Auf Abbildung 4.6 ist ersichtlich, dass die Schutzleistung von *Microsoft System Center Endpoint Protection* variiert. In der Testmenge von Zero-Day Malware, Webseiten und E-Mails waren die Ergebnisse von Microsoft durchaus unterdurchschnittlich. Der Tiefpunkt von Microsoft lag im November 2014. Bei einer Erkennungsrate von 48% kann nicht mehr von einer ausreichenden Schutzleistung die Rede sein. Zu betonen ist, dass der Durchschnitt zu dieser Zeit bei 92% lag. Seitdem haben sich die Ergebnisse von *System Center Endpoint Protection* stets verbessert. Im Juli und August 2015 wurde der aktuellste Testlauf zu dem Zeitpunkt dieser Arbeit durchgeführt. Hierbei hat Microsoft mit 86% abgeschlossen und rückte somit näher an den Durchschnitt von 98%. Es ist dennoch eine deutliche Differenz erkennbar.

Bei der Erkennung der Malware-Testmenge aus den letzten vier Wochen vor der jeweiligen Testphase, fiel die Schutzleistung von *System Center Endpoint Protection* unterschiedlich aus. Die Ergebnisse waren meist schlechter, als die von *Forefront Endpoint Protection*. Bei dieser Testmenge gab es seit Dezember 2014 eine monotone Steigerung. Im August 2015 konnte Microsoft ein fast durchschnittliches Testergebnis erzielen.

4.1.3 Erkenntnisse

Abbildung 4.7 zeigt den Vergleich der Erkennungsrate zweier Testmonaten innerhalb einer Testphase. Ein positiver Prozentsatz deutet darauf hin, dass im zweiten Testmonat eine höhere Erkennungsrate als im ersten Testmonat erreicht wurde. Eine sinkende Tendenz wird durch einen negativen Prozentsatz dargestellt.

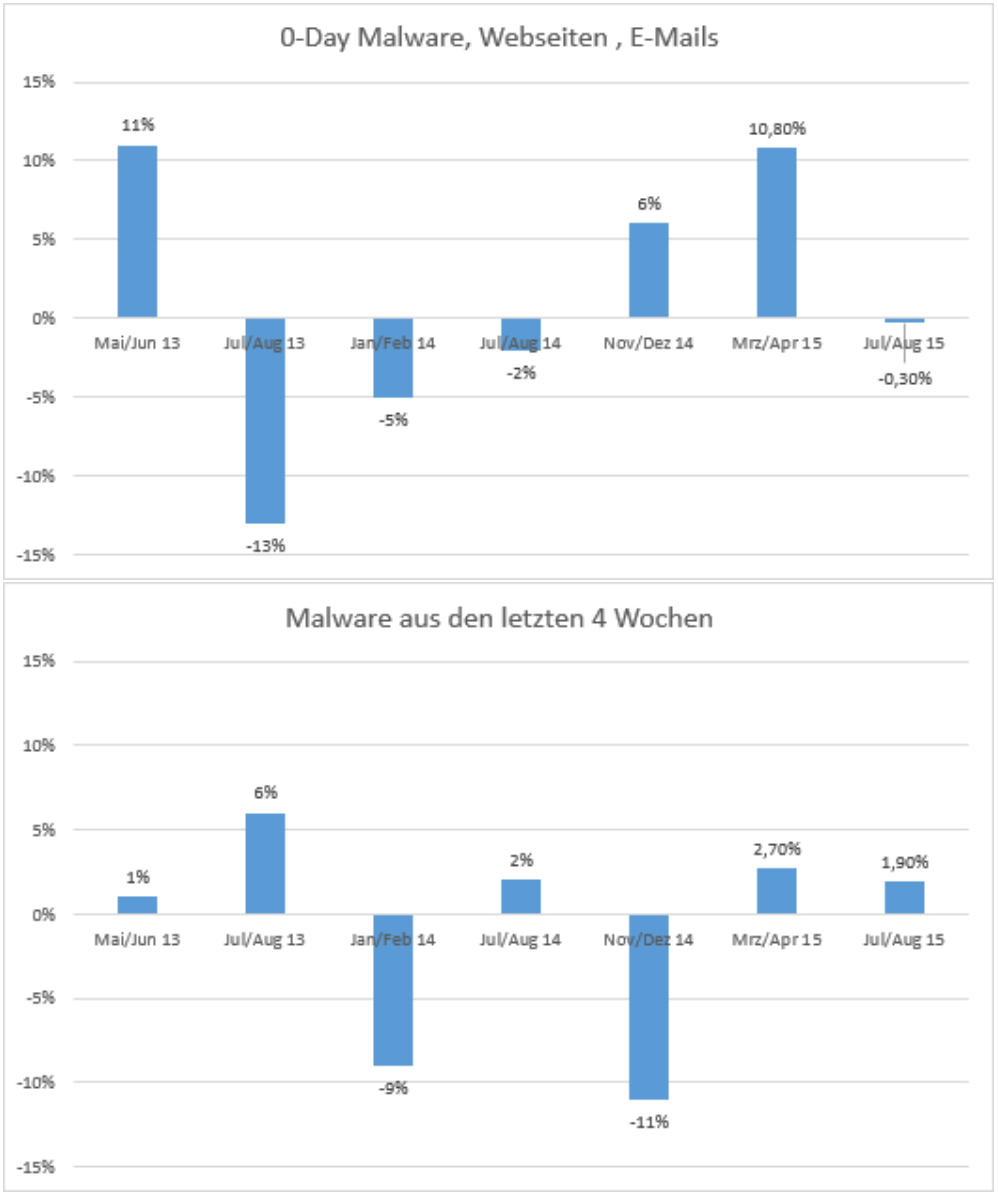

Abbildung 4.7: Vergleich der Änderungen der Erkennungsrate von Malware innerhalb einer Testphase

Die Ergebnisse einer Kombination beider Testmengen aus Abbildung 4.7 zeigt, dass die Testphasen der Monate Mai und Juni 2013 sowie März und April 2015 eine positive Erkennungstendenz erzielten.

Maik Morgenstern, Geschäftsführer und technischer Leiter der AV-TEST GmbH, hat sich zu diesen Ergebnissen, in direktem E-Mail-Verkehr mit mir, wie folgt geäußert: “Dies ist dem Umstand geschuldet, dass Microsoft Erkennungen mit großer Verzögerung einpflegt. Im Test werden diese Dateien also nicht erkannt, ein paar Tage später dann schon.” (Morgenstern, 2015).

Um aus den Tests von AV-Test weitere Informationen zu gewinnen, habe ich die Testergebnisse der Antivirenprogramme für Windows Client Unternehmensanwender mit Windows 7 aus dem Zeitraum März/April 2015 und Juli/August 2015 weiter analysiert. Die detaillierten Testinformationen hat Herr Morgenstern freundlicherweise zur Verfügung gestellt.

Für die Monate März, April, Juli und August 2015 gibt es jeweils zwei Dateien.

Die Datei mit dem Namen prevalent_*_vtest.csv enthält eine Liste über die erfolgten Detektionsergebnisse der getesteten Virenscanner. Der Stern des Dateinamens steht für den jeweiligen Testmonat. Die Testergebnisse sind in einer Tabelle zusammengefasst. Diese enthält verschiedene Hash-Werte von Malware Samples und ob die zu testende Antivirensoftware eine Erkennung gewährleistet hat. Weitere wichtige Informationen, wie das Datum des ersten Vorkommens und die Dateigröße der Schadprogramme, sind auch in der Tabelle enthalten.

H	I	J	K	L	M	N	AE	AF
first_seen	last_seen	last_scanned	scanner_count	scanner_detected_count	scanner_detected_percent	antivir	microsoft	norman
16.02.2015 19:52	27.02.2015 10:43	04.07.2015 11:44	27	21	78	TR/Spy.Agent.331776.18	-	Troj_Generic
08.02.2015 00:27	12.02.2015 11:42	30.08.2015 21:14	27	21	78	TR/Crypt.Xpack.75151	PWS:Win32/Zbot.gen!VM [generic]	-
14.02.2015 00:16	14.02.2015 01:11	21.06.2015 18:56	27	19	70	TR/Agent.433152.75	Trojan:Win32/Gatak!rfn	Kryptik.PDB
17.02.2015 00:14	27.02.2015 10:32	14.06.2015 17:36	27	22	81	-	Backdoor:MSIL/Noancooe.C	Suspicious_C
24.02.2015 00:10	28.02.2015 04:34	25.09.2015 21:07	27	22	81	TR/PSW.MSIL.428	VirTool:MSIL/Injector.FW	Suspicious_C
12.02.2015 00:07	12.02.2015 00:14	23.08.2015 21:20	27	21	78	TR/Spy.Agent.884736	-	Troj_Generic
10.02.2015 00:07	18.05.2015 02:43	12.09.2015 11:48	27	21	78	TR/Crypt.XPACK.Gen	Trojan:Win32/Gatak!dha	Suspicious_C
13.02.2015 00:18	18.02.2015 11:31	18.07.2015 11:49	27	21	78	TR/Spy.Fareit.81920	PWS:Win32/Fareit	Troj_Generic
25.02.2015 05:54	26.02.2015 20:20	14.06.2015 18:09	27	22	81	TR/Crypt.ZPACK.112003	Trojan:Win32/Dynamer!ac	Kryptik.STR
26.02.2015 00:17	09.03.2015 01:49	21.06.2015 19:57	27	18	67	TR/Crypt.ZPACK.Gen4	-	Dridex.L
11.02.2015 00:17	23.02.2015 21:54	14.06.2015 19:04	27	19	70	TR/Kryptik.kjsfg	-	Kryptik.HDR
21.02.2015 04:38	22.03.2015 08:02	14.06.2015 19:05	27	24	89	TR/Crypt.XPACK.Gen7	PWS:Win32/Zbot!rfn	ZBot.XUUG
18.02.2015 03:24	27.02.2015 09:34	14.06.2015 19:26	27	25	93	TR/Patched.Gen	Worm:Win32/Wervik.G	Troj_Generic
25.02.2015 04:48	26.02.2015 17:59	21.06.2015 20:45	27	20	74	TR/Injector.A.293	Trojan:MSIL/Stimilini	Suspicious_C

Abbildung 4.8: Auszug einer der prevalent_*_vtest.csv Tabellen

Um einen besseren Überblick zu erhalten, beschränkt sich prevalent_*_detection.csv auf Hashwerte der Malware und ob Malware durch *Microsoft System Center Endpoint Protection* erkannt wurde. Eine positive Erkennung wird mit einer 1 gekennzeichnet. 0 sagt aus, dass die Erkennung ausblieb (siehe Abbildung 4.9).

d4cffe5a35c8bdfc5a62044c19fcd8f4a197b75a4e0a3cb5ff197a91ec4c03f7	1
d4fc04243fa4e14d1c58f3a7a4204f7b3d1f314b52355bd073ab993397237b0e	1
d5349d0a1242f3020d6f29c1e3b3cc371bdddd770f2ea20c95d0e1503906ee5f	0
d5425a4dfe7fafac8be89a5c843bc5978a2b5c17f86b89ef65a93752fe9759d2	1
d62726fba5bbc2f3c6b1a67032e5c885cb87ec6da6bdb6899b3e38463f09f615	1
d64b45df110497db10e3b19bb59ec5f5e6868b34c4bf34b087c3121bcaa41fe3	1
d67f799a1ce75b3fe9de7334ce8280f99e0be9199848e24af86af1c56db58227	1
d68983d85bb275072078e8faf13f4023ff01f36fb5da5419af0cf419f0457d94	0
d6d67b778ec645761491e6de5ada095a67139060061426adec594efe821aa668	1

Abbildung 4.9: Auszug einer der prevalent_*_detection.csv Tabellen

4.2 VirusTotal

VirusTotal ist ein kostenloser Online-Service, der Dateien und URLs analysiert. *VirusTotal* gibt nach der Analyse Auskunft über eine etwaige Kompromittierung. Intern verwendet der Service hierfür Informationen von Antivirenprogrammen und Website-Scannern. Auch auf Datenbankeinträge bereits bekannter Malware wird zurückgegriffen. Der Anwender kann auf der Website von *VirusTotal* ausführliche Informationen über eine Vielzahl von Malware finden. *VirusTotal.com* ist seit dem 7. September 2012 eine Tochtergesellschaft von *Google*.

VirusTotal bietet eine Public API und eine Private API an. Diese ermöglichen das Hochladen und Scannen von Dateien, das Einsenden und Scannen von URLs sowie den Zugriff auf Berichte bereits durchgeführter Analysen. Die APIs werden mittels einfacher Scripts angesprochen (siehe virustotal.com).

4.2.1 VirusTotal Private API

Die Private API umfasst die Funktionalität der Public API und erweitert diese um fortgeschrittene Analysemöglichkeiten. Die Funktionen sind durch HTTP-Requests erreichbar und liefern Antworten im JSON Format.

Die Public API erlaubt vier Abfragen pro Minute. Für kommerzielle Anwender ist dies zu wenig. Deshalb ermöglicht die Private API ein Kontingent von 10000 Abfragen am Tag.

Eine der Private API Funktionen liefert Informationen über das Verhalten bestimmter Schadprogramme in einer Sandbox-Umgebung.

Bei Sandbox Tests werden schädliche oder verdächtigte Programme, Dateien oder Webseiten in einer virtuellen isolierten Umgebung ausgeführt. Hierdurch wird sicher gestellt, dass die Ausführung der Datei keine Einflüsse der äußeren Umgebung mit sich bringt. Dennoch können wichtige Informationen über das Verhalten und die Vorgehensweise gesammelt werden.

Durch den Service von VirusTotal werden nun solche Informationen, für alle von AV-Test bereitgestellten Malware Hashes, erlangt. Darauf folgt eine Analyse und ein Vergleich der Abfrageergebnisse.

Um die Funktionen der Private API verwenden zu können, benötigt man einen kostenpflichtigen API-Key. Herr Karl Hiramoto, Mitarbeiter des VirusTotal Teams, hat mir für meine Forschungszwecke einen zeitlich begrenzten kostenlosen Private API Key gegeben. Mit dessen Hilfe ist es mir gelungen, interessante Malware-Informationen zu sammeln. Hierfür wurde das Python Skript aus Abbildung 4.10 entwickelt.

behaviour_request.py

```python
import requests
import json
import os

save_path = 'C:/Uni/Bachelorarbeit/VirusTotal/Detected/BehaviourReports_PrevalentJuly/'
if not os.path.exists(save_path):
    os.makedirs(save_path)

with open('prevalent_july_detected_md5.txt', 'r') as f:
    for line in f:
        stripped_hash = line.strip()
        params = {'apikey': '[redacted]', 'hash': stripped_hash}
        response = requests.get('https://www.virustotal.com/vtapi/v2/file/behaviour', params=params)
        json_response = response.json()
        jsonString = str(json_response).replace('\'', '%temp%').replace('\"', '\'').replace('%temp%', '\"')
        filename = stripped_hash + '.json'
        with open(os.path.join(save_path, filename), 'w') as temp_file:
            print(jsonString, file=temp_file)
print('Done')
```

Abbildung 4.10: Python Skript, das Hashwerte aus einer Datei liest, Abfragen über Malware-Hashes tätigt und die Antworten in <Hashwert>.json speichert

Die Informationen über Hashes wurden nach dem Monat, in dem sie als Testmaterial verwendet wurden und nach Erkennungserfolg kategorisiert.

4.2.2 Informationen über Malware

VirusTotal liefert leider nicht für jede Malware detaillierte Informationen. Die folgende Tabelle zeigt die Anzahl der Malware Hashes, über die VirusTotal Auskunft geben konnte.

In Tabelle 4.1 ist erkennbar, dass der Informationsverlust in manchen Fällen bis zu 59,7% beträgt. Entweder war der abgefragte Malware-Hash nicht bekannt, oder es lagen keine Information über eine Ausführung in einer Sandbox-Umgebung vor. Wenn der Verlust zu groß ist, sinkt der Aussagegehalt der Visualisierung. Dennoch stellt die Visualisierung eine gute Möglichkeit dar, die Datenflut besser greifbar zu machen.

Von Microsoft in dem Monat ...	Informationen vorhanden	Keine Informationen	Prozentsatz des Informationsverlusts
März erkannt	7073	4183	37,16%
März nicht erkannt	1088	837	43,48%
April erkannt	5054	7486	59,70%
April nicht erkannt	1145	596	34,23%
Juli erkannt	4618	2229	32,55%
Juli nicht erkannt	130	28	17,72%
August erkannt	7535	4085	35,15%
August nicht erkannt	31	11	26,19%

Tabelle 4.1: Ergebnis der GET /vtapi/v2/file/behaviour Abfrage bei VirusTotal

Abbildung 4.11 zeigt ein Beispielergebnis der GET Abfrage /vtapi/v2/file/behaviour.

Die Inhalte der Abfragen wurden weiter gefiltert, um nur für die Analyse relevante Daten zu veranschaulichen. Ein Teil der Daten war meiner Meinung nach wenig aussagekräftig. Das Ausführungsdatum, die Ausführungsdauer und weitere Attribute der Malware können bei der Visualisierung vernachlässigt werden. Einige Einträge waren mit den Mitteln der Visualisierung schlecht darstellbar. Ein Beispiel hierfür ist der *Process Tree*.

Rot markierte Bereiche der Abbildung 4.11 sind von größerem Interesse. Durch Malware aufgerufene Windows Schnittstellenfunktionen, die Parametrierung dieser Aufrufe, die Kategorie der Schnittstellenfunktion und die während der Ausführung verwendeten Mutexe wurden so markiert. Eine nähere Beschreibung des Begriffes Mutex folgt später in diesem Kapitel. Die Visualisierung beinhaltet die Aufbereitung der folgenden Netzwerkinformationen:

- DNS Hostname
- IP-Adresse
- Host-Name
- Pfad des Verbindungsaufrufs
- Methodenname
- Verwendeter Port für HTTP Requests
- TCP/UDP Quell- und Zieladresse
- TCP/UDP Quell- und Zielport

```
{"behavior": {"processes": [{"calls": [{"api": "CreateMutexW",
                                        "arguments": [{"name": "lpName",
                                                       "value": "W3iCoreLogger"}],
                                        "category": "synchronization",
                                        "repeated": 0,
                                        "return": "0x00000028",
                                        "status": "SUCCESS",
                                        "timestamp": "20120826150207.734"}],
                                "first_seen": "20120826150207.734",
                                "parent_id": "1856",
                                "process_id": "484",
                                "process_name":
"82a4d0467f93e3ddec3b51a66dbd55cfce3f6c5725d2759850fb4b3b37c28304"},
                                .....],
                    "processtree": [{"children": [],
                                     "name":
"82a4d0467f93e3ddec3b51a66dbd55cfce3f6c5725d2759850fb4b3b37c28304",
                                     "pid": 484}],
                    "summary": {"files": ["\\\\.\\PIPE\\lsarpc",
                                          "C:\\82a4d0467f93e3ddec3b51a66dbd55cfce3f6c5725d2759850fb4b3b37c28304",
                                          "C:\\DOCUME~1\\<USER>~1\\LOCALS~1\\Temp\\pkg_f272e80\\stub.log"],
                                "keys": ["HKEY_LOCAL_MACHINE\\\\Software\\Microsoft\\Rpc\\PagedBuffers",
                                         "HKEY_LOCAL_MACHINE\\\\Software\\Microsoft\\Rpc"],
                                "mutexes": ["W3iCoreLogger",
                                            "W3iPackageManager",
                                            "FreezeWrap_Preload_Mutex"]}},
 "info": {"duration": "76 seconds",
          "ended": "2012-08-26 17:03:10",
          "started": "2012-08-26 17:01:53",
          "version": "v0.1"},
 "network": {"dns": [{"hostname": "dl.installiq.com", "ip": "66.77.96.107"},
                     {"hostname": "dl6.iq7download.com","ip": 93.184.220.20"},
                     {"hostname": "liveupdate.symanteclive update.com",
                      "ip": "23.14.93.17"}],
             "hosts": ["0.0.0.0",
                       "255.255.255.255",
                       "10.0.2.2"],
             "http": [{"body": "",
                       "data": "GET"
 "/api/detectionrequest.aspx?keyid=1&shortname=videosaver&langid=0x0409 "
                                "HTTP/1.1\r\n"
                                "User-Agent: Mozilla/4.0 (compatible; MSIE 7.0;"
                                "Windows NT 5.1)\r\n"
                                "Host: dl.installiq.com\r\n"
                                "Cache-Control: no-cache\r\n"
                                "\r\n",
                       "host": "dl.installiq.com",
                       "method": "GET",
                       "path":
"/api/detectionrequest.aspx?keyid=1&shortname=videosaver&langid=0x0409",
                       "port": 80,
                       "uri":
"http://dl.installiq.com/api/detectionrequest.aspx?keyid=1&shortname=videosav
er&langid=0x0409",
                       "user-agent": "Mozilla/4.0 (compatible; MSIE 7.0; "
                                     "Windows NT 5.1)",
                       "version": "1.1"}],
             "tcp": [{"dport": 80,
                      "dst": "66.77.96.107",
                      "sport": 1045,
                      "src": "10.0.2.15"}],
             "udp": [{"dport": 67,
                      "dst": "255.255.255.255",
                      "sport": 68,
                      "src": "0.0.0.0"}]}}
```


Abbildung 4.11: JSON Beispiel

Falls bei VirusTotal keine Verhaltensinformationen zu einem Hash gefunden werden können, wird folgende JSON-Nachricht zurückgegeben:

```
1 {"response_code": 0, "verbose_msg": "No behavioural report for this file", "hash": "
      ffdcd072c327e9c379d99c71ed9745136f596b205fefb5f6c503d227bdfc11d2"}
```

4.2.3 Visualisierung der Ergebnisse

Das Ziel der Visualisierung besteht darin, Ähnlichkeiten zwischen nicht erkannter Schadsoftware herzustellen und damit mögliche Sicherheitslücken zu entdecken.

Für die Visualisierung der Malwareinformationen von *VirusTotal* wurde eine Kombination aus Kibana und Elasticsearch verwendet. Elasticsearch ist eine graphenbasierte Suchmaschine für größere Datenmengen. Kibana ist ein beliebtes Visualisierungsplugin für Elasticsearch. Beide Tools sind Open Source Produkte. Die Daten werden als JSON-Dokumente an Elasticsearch übergeben und gespeichert.

Die in Kibana getätigten Abfragen für die Visualisierung erfolgen in der Lucene Query Syntax. Kibana bietet unterschiedliche Möglichkeiten zur Veranschaulichung der Daten. Dashboards sind die Container für verschieden grafische Elemente. In der hier demonstrierten Anwendung enthält das Dashboard Tabellen, Diagramme und mehrere geographische Karten. Durch eine parallele Darstellung kann man Datenmengen auf einen Blick vergleichen.

Aufgrund der einfachen Bedienbarkeit und früheren Erfahrungen mit Kibana und Elasticsearch habe ich mich für diese Tools entschieden. Diese wurden, wie auf der Homepage https://www.elastic.co/ beschrieben, installiert.

Um die Daten in Elasticsearch bzw. Kibana einzupflegen wurde ein Java Programm geschrieben, das die Informationen der *.json Dateien deserialisiert und die gefilterten Eigenschaften und Informationen in serialisierter Form an den lokalen Elasticsearch Server schickt.

Das Programm benötigt zwei Argumente. Das erste Argument ist der Pfad zu dem Verzeichnis das die JSON Dateien enthält. Das zweite Argument ist die Kategorie der Information. Die Bezeichnungen der Kategorien haben folgende Form: <Erkennung>_<Monat> . Als Beispiel dienen die nicht erkannten Malware-Samples vom März 2015. Die Kategorienbenennung hierfür ist *missed_march*. Die Kategorie für Samples, die im März 2015 erkannt wurden, lautet *detected_march*. Die so aufbereiteten Daten können im Anschluss von Kibana abgefragt und visualisiert werden.

Abbildung 4.12 zeigt, wie die Informationen der Malware-Hashes in eine Visualisierung überführt werden.

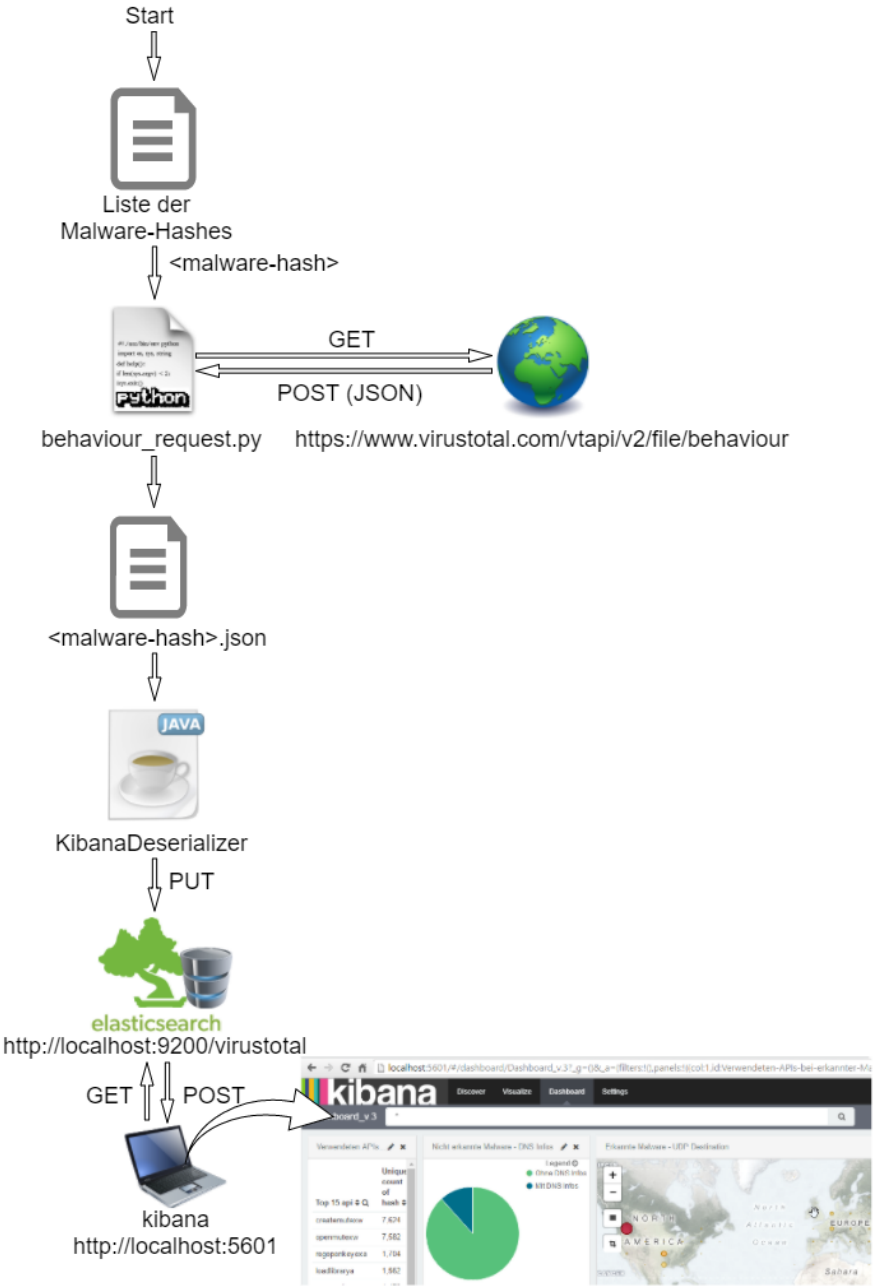

Abbildung 4.12: Datenfluss

Für die Visualisierung der IP-Adressen wandelt das Java Programm die IP-Adressen in geographische Koordinaten um. Dies geschieht mithilfe der *Maxmind GeoIP2* Datenbank und deren OpenSource Java API.

```
private void dns(String hash, DnsInfos dns) {
    String url = kibanaUrl + idZaehler.toString();
    ArrayList<Double> coords = new ArrayList<>();

    String ip = dns.getIp();
    String host = dns.getHostname();

    String body = "{\"hash\" : \"" + hash + "\" , \"ip\" : \"" + ip + "\" , \"hostname
        \" : \"" + host + "\"}";
    try {

        coords.addAll(geo.getLocation(ip));
        Double lat = coords.get(0);
        Double lon = coords.get(1);

        if (lat != null && lon != null) {
            body = "{\"hash\" : \"" + hash + "\" , \"ip\" : \"" + ip + "\" , \"
                hostname\" : \"" + host + "\" , \"coordinates\" : { \"lat\" : " + lat.
                toString() + ", \"lon\" : " + lon.toString()   + "}}";
        }
    } catch (GeoIp2Exception e) {
        e.printStackTrace();
    }

    try {
        HttpResponse<JsonNode> jsonResponse = Unirest.post(url).body(body).asJson();
    } catch (UnirestException e) {
        e.printStackTrace();
    }

    idZaehler++;
}
```

Listing 4.1: Codebeispiel zum Einlesen der DNS Informationen eines Samples

4.3 Die Ergebnisse der Visualisierung

Wie im vorherigen Abschnitt beschrieben, werden nicht alle Informationen dargestellt, die AV-Test vorhält.

Als erstes werden die erkannten Malwarearten näher inspiziert.

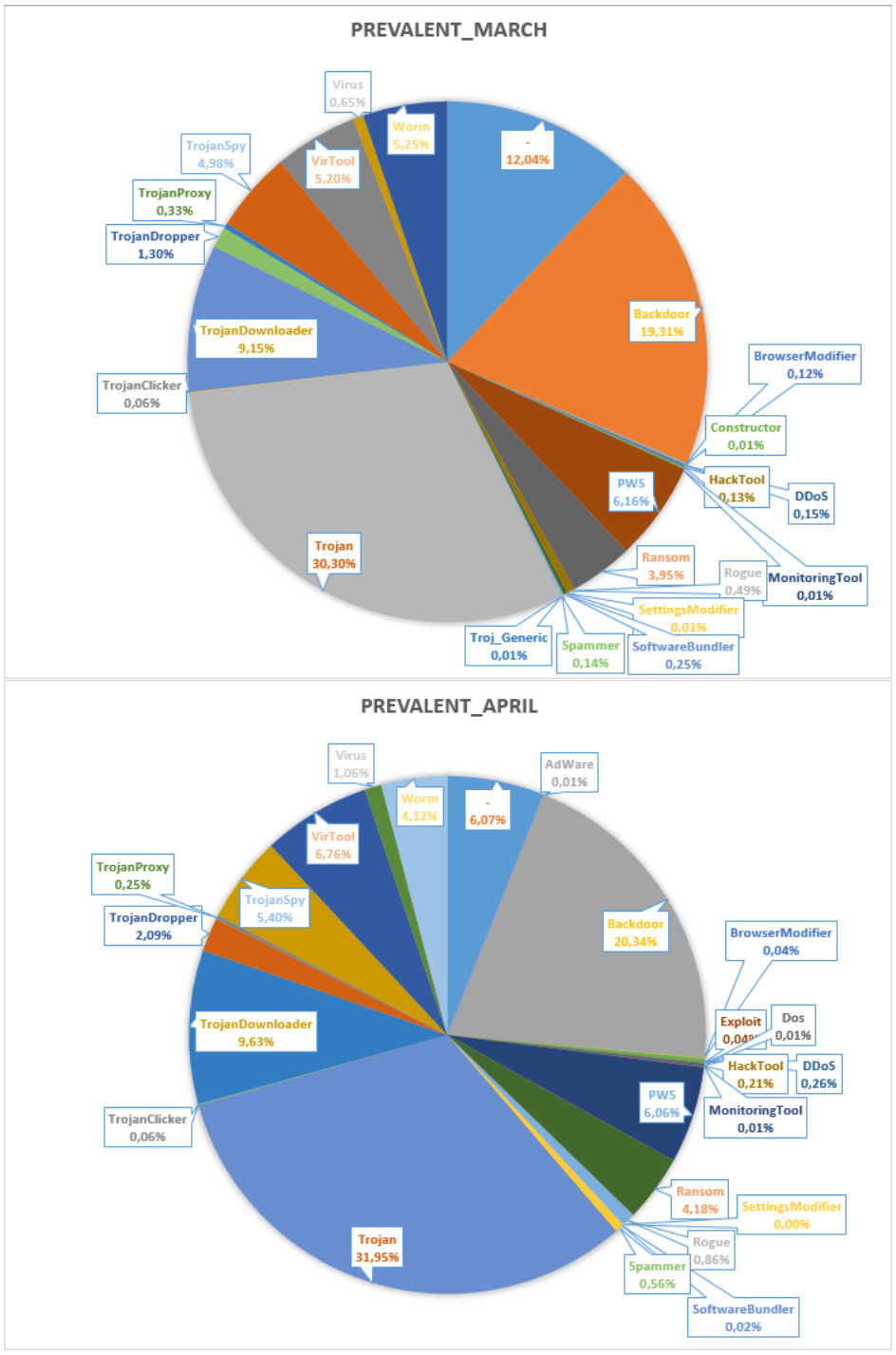

Abbildung 4.13: Erkannte Malwarearten der Testphase März/April 2015

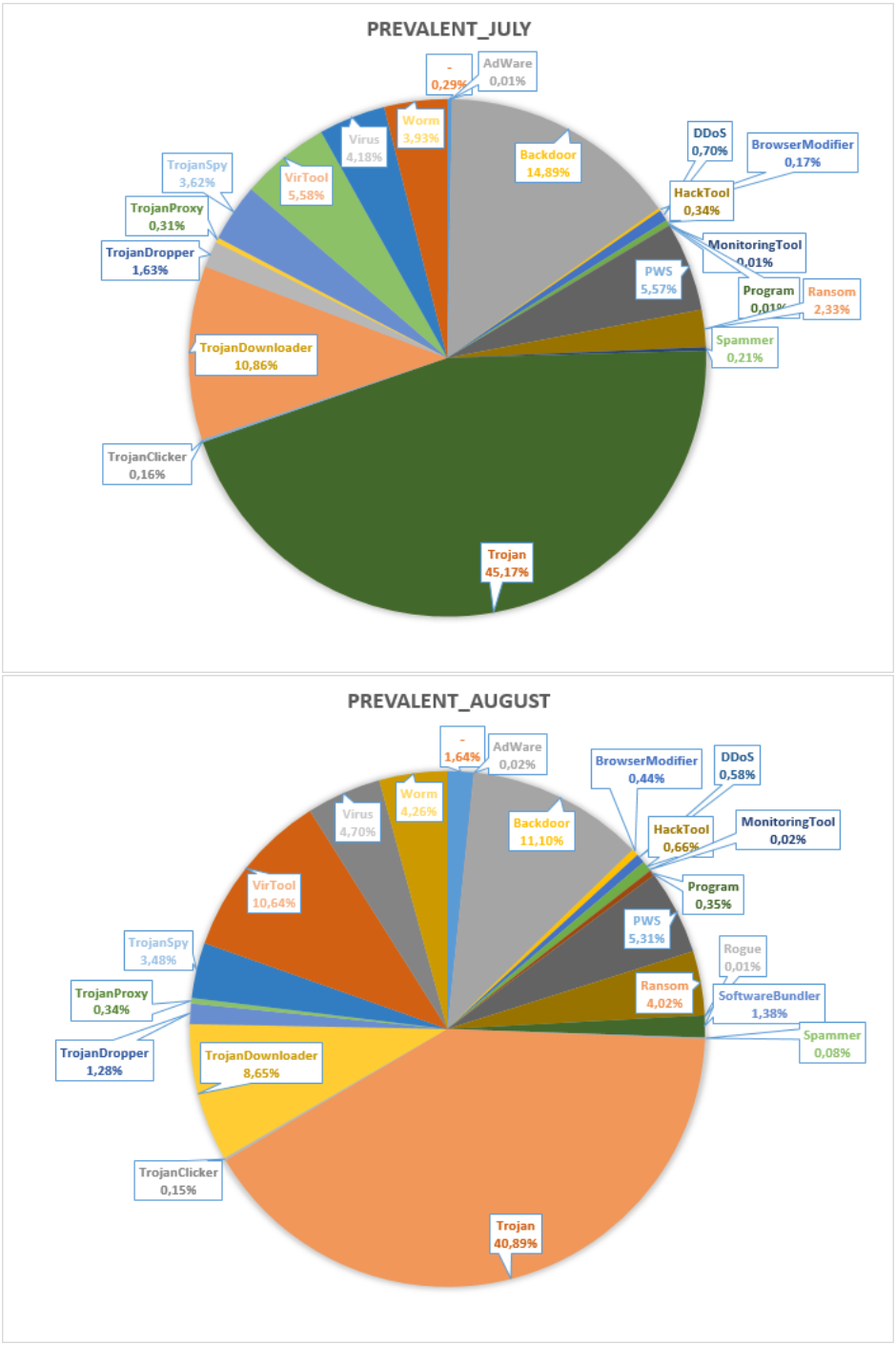

Abbildung 4.14: Erkannte Malwarearten der Testphase Juli/August 2015

Microsoft System Center Endpoint Protection erkennt eine Vielzahl von Malwarearten. Die meisten davon sind Trojaner, Backdoors oder Password Stealer (PWS). Abbildung 4.13 und Abbildung 4.14 zeigen die Malwarearten, die während der Tests erkannt wurden.

Windows API

Zunächst wird die Häufigkeit der verwendeten Windows API Funktionalitäten analysiert.

Abbildung 4.15 zeigt die 15 häufigsten durch Malware verwendeten Funktionen der Windows API. Neben dem Namen der gelisteten Funktionalitäten steht die Anzahl der Malware, die diese verwendet haben. In Abbildung 4.15 erkennt man zwei Tabellen. Die linke Tabelle enthält Windows API Funktionsaufrufe von Malware, die mittels *Microsoft System Center Endpoint Protection* erkannte wurde. Die rechte Tabelle enthält Funktionsaufrufe nicht erkannter Malware.

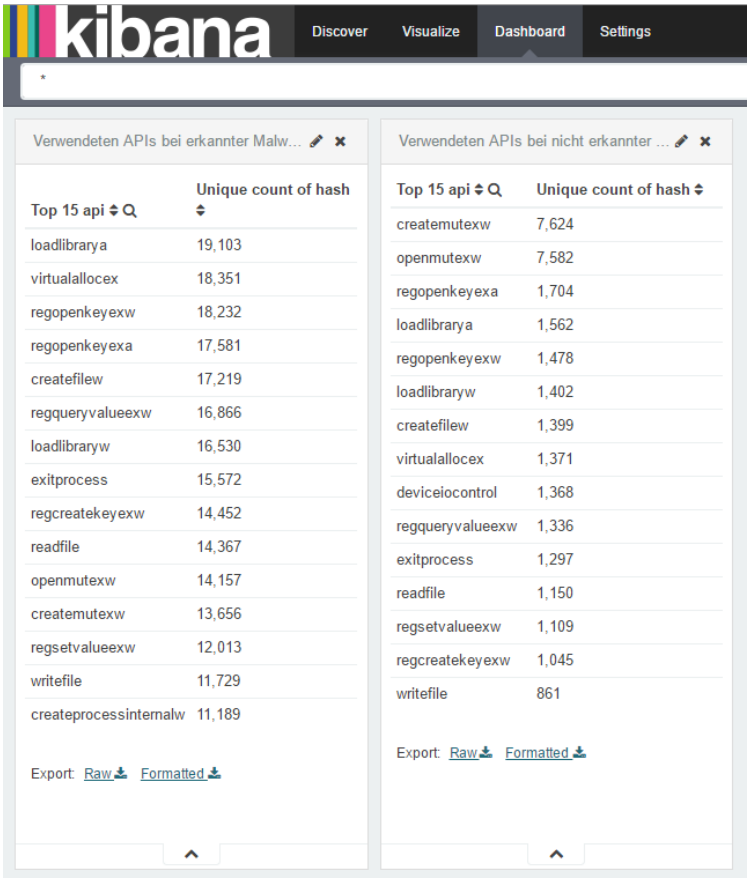

Abbildung 4.15: Die meist verwendeten API Funktionen erkannter und nicht erkannter Malware

Zu erkennen ist, dass beide Tabellen ähnliche Betriebssystemsmechanismen enthalten. Bei den meisten Aufrufen handelt es sich um Schnittstellenfunktionen für Registry-, Mutex- oder Fileoperationen.

Wenn man die verwendeten Funktionen betrachtet, könnte man auf die Absicht der Malware schließen. Die API *GetTickCount* wird beispielsweise häufig von Malware benutzt um festzustellen, ob momentan ein Debugger läuft. Die APIs *AdjustTokenPrivileges* und *LookupPrivilegeValueA* werden für den Zugriff auf Windows Security Tokens verwendet. *RegSetValueExA*, *RegCreateKeyA* und *RegCloseKey* ermöglichen Registryzugriffe oder -änderungen.

Tabelle 4.2 liefert weitere Sequenzen von API Funktionsaufrufen, die häufig von Malware verwendet werden.

Beschreibung des verdächtigen Verhaltens	Sequenzen von API Funktionsaufrufen
Zugriff auf das Systemverzeichnis	GetWindowsDirectory, GetSystemDirectory
Suche nach Dateien, um sie zu infizieren	FindFirstFile, FindNextFile, FindClose
File Mapping erstellen	CreateFileMapping, MapViewOfFile, UnMapViewOfFile
In ein File schreiben	CreateFile, OpenFile, WriteFile, CloseHandle
Änderung der Fileattribute	GetFileAttributes, SetFileAttributes
Zeitstempel von Dateien ändern	GetFileTime, SetFileTime
Verteilung von globalem Speicher	GlobalAlloc, GlobalFree
Verteilung von virtuellem Speicher	VirtualAlloc, VirtualFree
Laden der Registry	RegOpenKey, RegCreateKey, RegSetValue, RegCloseKey

Tabelle 4.2: Beschreibung verdächtiger Verhaltensmuster durch API Sequenzen - Quelle : Wang u. a. (2009)

In der Untersuchung von Wang u. a. (2009) findet man, dass Aufrufe wie *GetWindowsDirectory* und *GetSystemDirectory* häufig in Kombination verwendet werden (siehe Tabelle 4.2). In den mir zur Verfügung gestellten Informationen über Malware konnten diese Sequenzen dennoch nicht gefunden werden. Vereinzelte Funktionsaufrufe liegen vor, aber die expliziten Sequenzen blieben aus.

Mutex

Ein Mutex-Objekt wird als Synchronisationsmechanismus verwendet. Hierdurch kann verhindert werden, dass mehrere Threads gleichzeitig auf die selbe Ressource zugreifen. Wenn ein Thread A auf eine Ressource zugreifen möchte, die gerade von einem anderem Thread B verwendet wird, muss A warten bis B den zugehörigen Mutex freigibt.

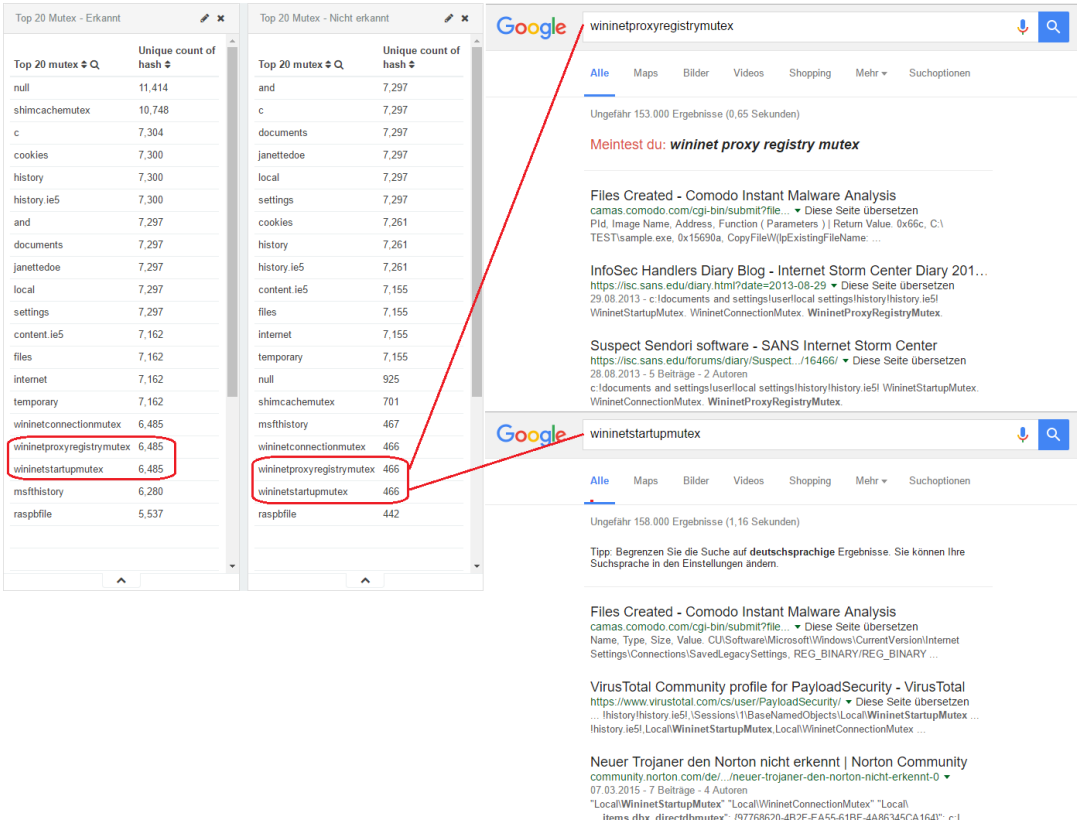

Abbildung 4.16: Die meist verwendeten Mutexe von erkannter und nicht erkannter Malware

Es ist schwierig herauszufinden, ob ein Mutex durch Malware dazu missbraucht wird eine Ressource zu blockieren. In Abbildung 4.16 sind zwei Tabellen (links) zu erkennen. Diese zeigen die 20 am häufigsten durch Malware verwendeten Mutexnamen. Die linke Tabelle beschränkt sich auf die Ergebnisse erkannter Malware, die rechte Tabelle zeigt die Ergebnisse nicht erkannter Malware.

Als Beispiel habe ich die Mutexnamen *wininetproxyregistrymutex* und *wininetstartupmutex* näher betrachtet. Durch eine Google-Sucheanfrage stellte sich heraus, dass diese Mutexe möglicherweise von einer Malware erstellt wurden.

Eine Differenzierung der gutartigen und schadhaften Nutzung von Mutexen ist nicht immer möglich. Es gibt dennoch einige Erkennungsmerkmale die indizieren, ob ein Mutex durch eine Malware erstellt wurde. Die Länge, die Formatierung sowie die Verwendung und Verteilung von Sonderzeichen innerhalb des Namens können Hinweise liefern.

Im Internet existieren Listen über verdächtige Mutexnamen. Tools wie LockPick sind darauf spezialisiert ungewöhnliche Mutexnamen zu erkennen.

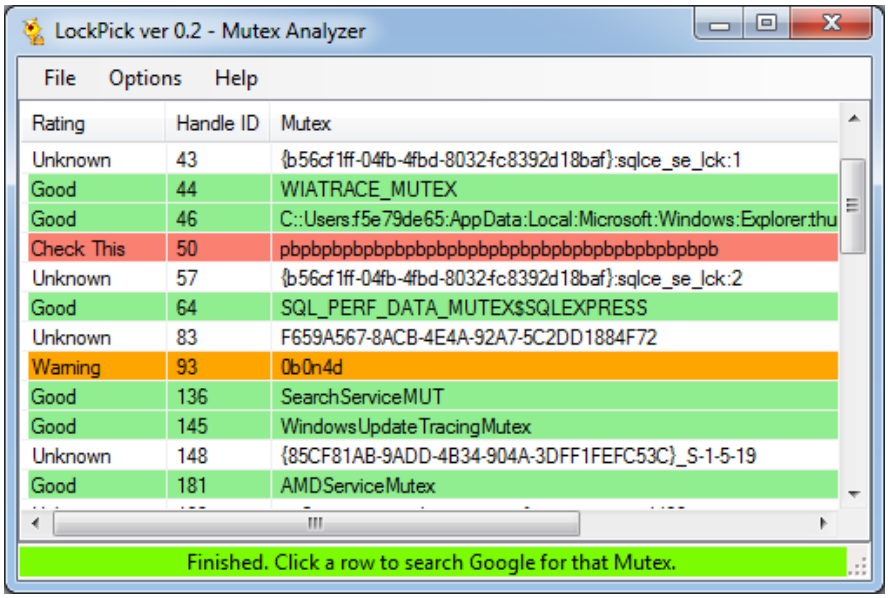

Abbildung 4.17: LockPick - Mutex Analyzer - Quelle: Infosec

Netzwerkinformationen

Die folgenden Abbildungen liefern Informationen über den Netzwerkverkehr, der während einer Infektion durch Malware entstanden ist.

In Abbildung 4.18 und Abbildung 4.19 wird über Netzwerke kommunizierende Malware blau gekennzeichnet. In grün wird Schadsoftware dargestellt, die entweder kein kommunikatives Verhalten besitzt, oder bei der keine Aufzeichnungen darüber vorliegen. Die Kreisdiagramme sollen lediglich das Verhältnis beider Gruppen veranschaulichen.

Ein Eintrag in den Feldern “hostname” oder “ip” unter “dns” der Netzwerkinformationen von VirusTotal weist darauf hin, dass die Malware versucht hat eine Verbindung zu einem Host aufzubauen.

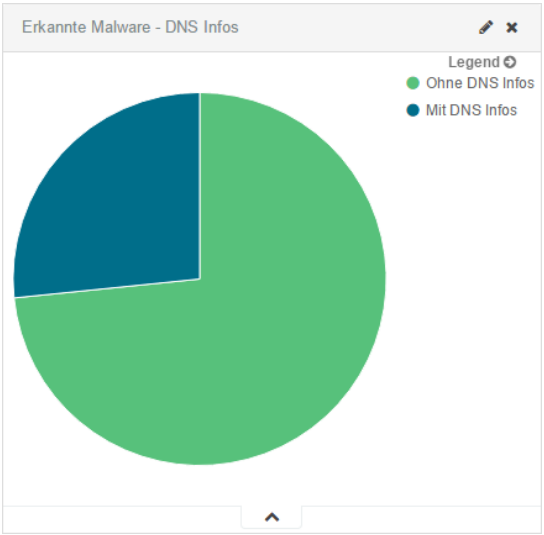

Abbildung 4.18: Erkannte Malware mit Verbindungsinformationen

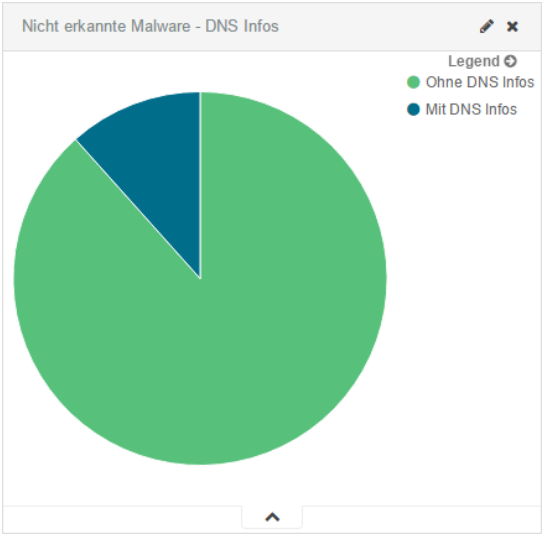

Abbildung 4.19: Nicht erkannte Malware mit Verbindungsinformationen

Erkannte Malware Programme (siehe Abbildung 4.18) versuchten in ca. 73% aller Fälle einen Verbindungsaufbau. Bei den nicht erkannten Samples (siehe Abbildung 4.19) liegt dieser Prozentsatz bei 88%.

Die Abbildungen 4.20 und 4.21 zeigen die Verhältnisse der verwendeten HTTP Request-Methoden.

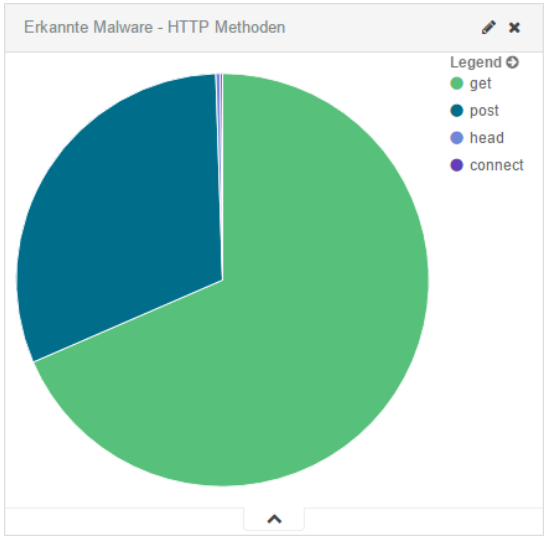

Abbildung 4.20: Erkannte Malware - HTTP Request-Methoden

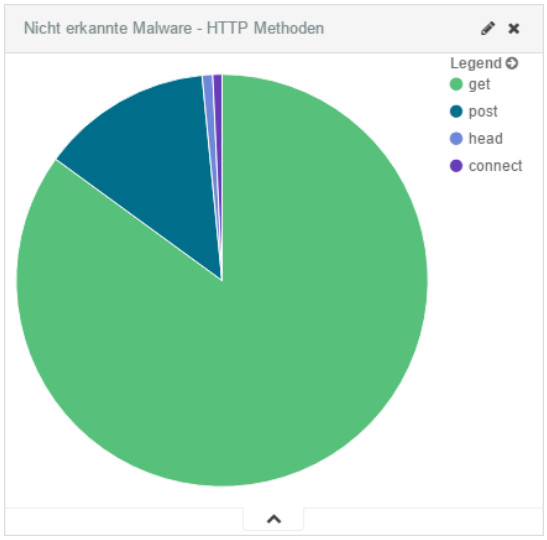

Abbildung 4.21: Nicht erkannte Malware - HTTP Request-Methoden

Die Lokalisierung von IP-Adressen ausgehender TCP und UDP Verbindungen erfolgte mithilfe der *Maxmind GeoIP2* Datenbank. Die IP-Adressen wurden in geographische Koordinaten überführt und Visualisiert. Es existieren einige IP-Adressen, für die keine entsprechenden Koordinaten in der Datenbank vorlagen.

Abbildung 4.22: Erkannte Malware mit Koordinaten zu ausgehenden TCP Verbindungen

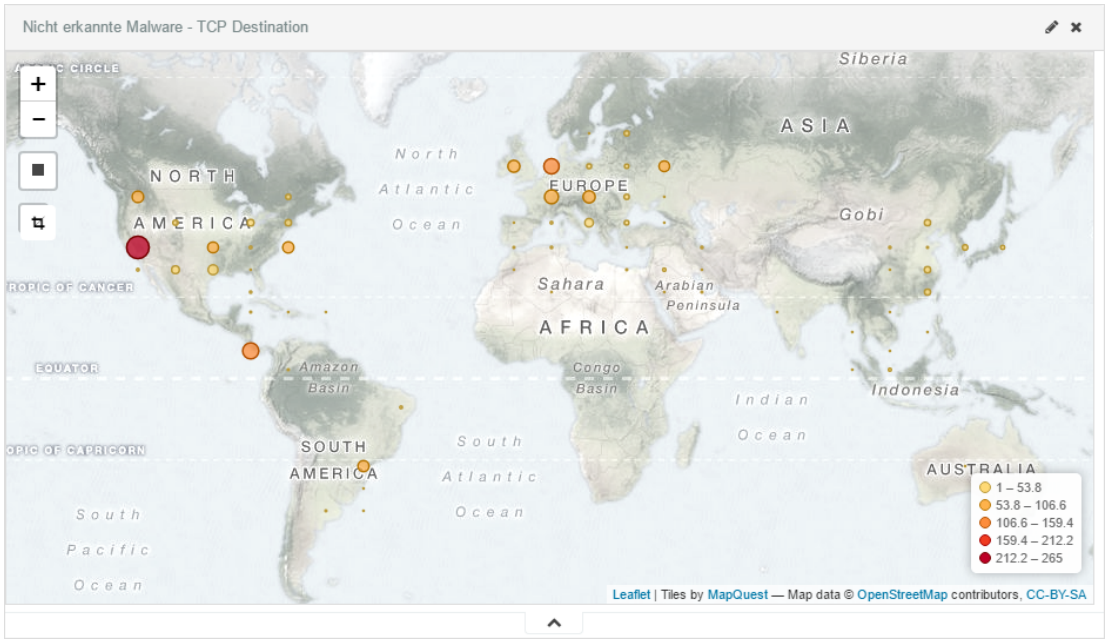

Abbildung 4.23: Nicht erkannte Malware mit Koordinaten zu ausgehenden TCP Verbindungen

Abbildung 4.24: Erkannte Malware mit Koordinaten zu ausgehenden UDP Verbindungen

Abbildung 4.25: Nicht erkannte Malware mit Koordinaten zu ausgehenden UDP Verbindungen

Die Karten zeigen, dass die Anzahl der Verbindungen in stark entwickelten Regionen, wie Nordamerika oder Zentraleuropa, gehäuft ist.

Auf der Website von *Kaspersky Lab* findet man eine Karte der Cyberkriminalität, die in Echtzeit aktualisiert wird. Diese Karte diente für einen rein visuellen Vergleich meiner Ergebnisse. Die Ballungszentren des Netzwerkverkehrs sind weitestgehend kongruent.

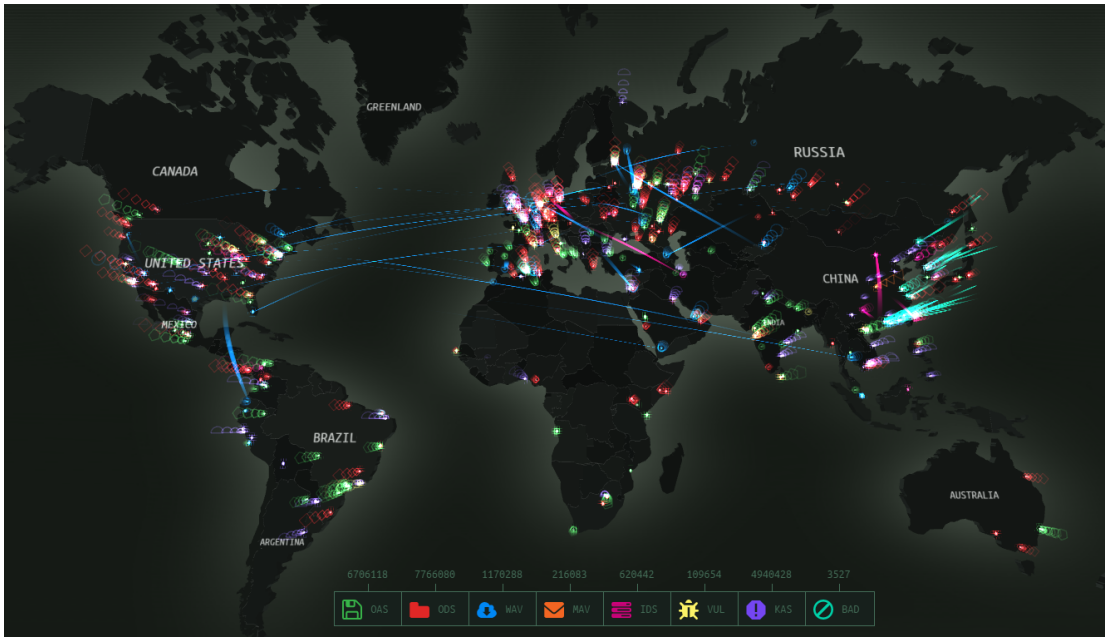

Abbildung 4.26: Kaspersky - Cyberthreat Real-Time Map - Quelle: cybermap.kaspersky.com

5 Bewertung

In diesem Kapitel werden die Ergebnisse der Visualisierung und Malwarestatistiken diskutiert. Darauf folgt die Bewertung der Antimalware Tools von Microsoft anhand der Ergebnisse aus Kapitel 3 und Kapitel 4.

5.1 Evaluation der Visualisierungen

Eine textuelle Repräsentation von Daten bietet sich nur eingeschränkt für die menschliche Interpretation an. Mit dieser Problematik haben sich auch Bollier und Firestone beschäftigt: "Perhaps one of the best tools for identifying meaningful correlations and exploring them as a way to develop new models and theories, is computer-aided visualization of data." (Bollier und Firestone, 2010, S. 9). Die Visualisierungen haben dabei geholfen, die immense Datenflut von VirusTotal zu veranschaulichen. Erst hierdurch konnte ein Überblick der Daten geschaffen werden. Nicht für alle Malware Samples existieren Informationen auf VirusTotal. Dieser Umstand kann die Ergebnisse der Visualisierung negativ beeinflussen.

Meine Erwartung, dass die Vergleiche zwischen erkannten und nicht erkannten Malware-Samples einen größeren und klar erkennbaren Unterschied aufweisen, wurde leider nicht erfüllt.

Die Untersuchung der verwendeten Mutexnamen in Kapitel 4 unter Abschnitt 4.3 indiziert, dass einige Malwareangriffe möglicherweise zu verhindern gewesen wären.

Bei Malware, die Mutex-Objekte verwendet, sind die Mutexnamen, in den meisten Fällen, feste Bestandteile des Quellcodes und ändern sich nicht. Eine Liste mit verdächtigen Mutexnamen und der zugehörigen Malware findet man Beispielsweise auf hexacorn.com. Mit Kibana wurden alle Mutexnamen gesammelt, die von nicht erkannter Malware stammen. Das Ergebnis des Vergleichs dieser Listen kann aus Abbildung 5.1 entnommen werden.

	A	B	C	D	E	F
1	Top 9999 mutex	Unique count of hash	Malware		Malware	Mutexname
3	c	7,297	W32.IRCBot		Adware.ADH	FFEEFERURLWUp
18	wininetconnectionmutex	466	Trojan.Spyeye		Adware.Clkpotato	Global_setup_ap
19	wininetproxyregistrymutex	466	Infostealer.Bankash.E		Adware.Clkpotato	Global\Setup_028
20	wininetstartupmutex	466	Trojan.Spyeye		Adware.Clkpotato	SAIBackupFileWri
23	1	110	Backdoor.Trojan		Adware.CommonN	winnet
44	1003	51	Trojan.Gen		Adware.Gen	IE Update
142	exe	2	Backdoor.Trojan		Adware.WinFavori	Bridge1
186	123	1	W32.Spybot.Worm		Backdoor.Akak	J&srl!hsl^AHSgh
289	b	1	Backdoor.Trojan		Backdoor.Cycbot!g	{0ECE180F-6E9E-4
294	ba4c12bee3027d94da5c81db2d196bfd	1	Backdoor.Trojan		Backdoor.Cycbot!g	{5D92BB9F-9A66-4
400	mutex	1	Trojan.Gen		Backdoor.Hitcap	ThirdReich10rv3
464					Backdoor.Papi	)!VoqA.I4
465					Backdoor.Paproxy	AVUPSCHED13912
466					Backdoor.Pcclient	Global\Minserver

Abbildung 5.1: Vergleich der Mutexnamen

Abbildung 5.1 zeigt, dass elf Mutexnamen, die durch nicht erkannte Malware verwendet wurden, in der Liste von hexacorn.com wiedergefunden werden konnten. Diese Liste lag bereits im Dezember 2014 und somit vor den Testläufe von AV-Test vor. Die Abbildung zeigt auch die Anzahl der einzelnen Hashwerte, die diese Mutexnamen verwendet haben.

Eine Heuristik stellt immer nur den Versuch dar ein Problem zu lösen. Verifizierte Informationen, welche Heuristiken Microsoft für die Malwareerkennung verwendet, sind leider nicht zugänglich. Hätte Microsoft beispielsweise die oben aufgelisteten Mutexnamen mit in ihre Heuristiken aufgenommen, hätten eventuell weitere Angriffe blockiert werden können.

Die restlichen Visualisierungen lieferten inkonklusive Ergebnisse, da die Gründe für gescheiterte Erkennungen nicht eindeutig ersichtlich wurden.

5.2 Bewertung der Microsoft Antimalware Tools

Eine mögliche Erklärung für den mangelnden Schutz der Microsoft Sicherheitstools sind die seltenen Updates der Malwaredefinitions Datenbank. Das *Malicious Software Removal Tool* wird nur einmal im Monat aktualisiert. Im schlimmsten Fall lädt man dieses Tool am Tag vor der Aktualisierung herunter. Der Schutz umfasst dann nicht die neuste Malware des letzten Monats. Die *System Center Endpoint Protection* wird mit den Einstellungen der Standardinstallation täglich aktualisiert. Allerdings kann diese Aktualisierung laut Malware Protection Center (b) durch bestimmte Malware deaktiviert werden. So kann der Rechner für einen unbestimmten Zeitraum unbemerkt infiziert sein.

Der Schutz von *Microsoft Security Essentials* ist dank der Heuristiken und dem Cloud-basierten Signaturdienst eine bessere Alternative. Allerdings ist dieses Tool nur durch Privatanwender oder kleine Unternehmen (mit maximal bis zu zehn Endgeräten) optimal einsetzbar.

Vollständige Systemscans werden standardmäßig einmal pro Woche durchgeführt. Die Erhöhung der Scans pro Woche könnte die frühzeitige Erkennung von Schadsoftware verbessern.

Ein weiteres Tool, das Heuristiken verwendet, ist das *Enhanced Mitigation Experience Toolkit*. Es bietet eine zusätzliche Verteidigungslinie gegen Zero-Day-Exploits. Es ist sowohl für Privatanwender als auch für Unternehmen geeignet. Hierbei ist eine kompetente Konfigurierung des Tools entscheidend. Zu strenge Einschränkungen können die Blockierung harmloser Programme hervorrufen.

In den Tests von AV-Test wird die getestete Sicherheitssoftware mit den Standardeinstellungen ausgeführt. *Microsoft System Center Endpoint Protection* ist stark von den vorhandenen Malwaresignaturen abhängig und bietet daher nur einen Basisschutz gegen bekannte Malware. Bei neuer und nicht in der Signaturdatenbank geführter Malware ist der Echtzeitschutz von *System Center Endpoint Protection* gefragt. Dieser sucht ausschließlich nach Verhaltensmustern bekannter Malware. Der dynamischer Signaturendienst ist nur dann aktiviert, wenn auch *Spynet* verwendet wird (vgl. Plue, 2012, S. 18). *Spynet* ist eine online Community, deren Mitglieder Microsoft Sicherheitsprodukte verwenden und Informationen über Malware oder verdächtige Software bereitstellen.

In der Standardinstallation ist *Spynet* deaktiviert und somit auch der dynamische Signaturdienst. Dies schränkt die Erkennungsmöglichkeiten erheblich ein. Zusätzlich zu *System Center Endpoint Protection* könnte auch *Enhanced Mitigation Experience Toolkit* installiert werden. Dies würde den Schutz deutlich erhöhen.

Laut Gartner (2016) gehört *System Center Endpoint Protection* zu den Herausforderern (engl. Challengers). Das bedeutet, dass *System Center Endpoint Protection* zu den Antimalware Produkten zählt, die eine stabile Grundsicherheit aufbauen. Es beinhaltet eine ausreichende Basisfunktionalität und ist für eng definierte Probleme effizient und praktisch einsetzbar. Aber auch hier zeigt sich, dass dieses Microsoft Sicherheitsprodukt nicht zu der Gruppe der führenden Sicherheitslösungen gehört.

Abbildung 5.2: Gartner Quadrant - Quelle: Gartner (2016)

Auf der RSA Conference (2015) wurde in dem Vortrag von Microsoft CTO, Mark Russinovich, zum ersten Mal "Project Sonar" erwähnt. Hinter dem Codenamen "Project Sonar" versteckt sich ein Dienst, der täglich Millionen verdächtiger Dateien in Microsofts *Azure-Cloud* ausführt und analysiert. Dies zeigt auch Microsofts Bestrebungen den Schutz seiner Produkte zu verbessern und so konkurrenzfähig zu bleiben. Dieses Projekt würde es Microsoft ermöglichen ihre Signaturdatenbank schnell durch eine Analyse großer Datenmengen zu erweitern.

Die Tests von AV-Test haben gezeigt, dass eine Standardinstallation von *System Center Endpoint Protection* nur gegen bekannte Malware schützt. Im Fall von Zero-Day Malware ist die Schutzwirkung vor Angriffen geringer. Sowohl *System Center Endpoint Protection*, als auch *Security Essentials* haben die neusten Tests von Januar/Februar 2016 bestanden und das Zertifikatssiegel von AV-Test erhalten.

6 Fazit

In diesem Kapitel erfolgt die abschließende Betrachtung dieser Bachelorarbeit. Die Ergebnisse werden vorgestellt und zusammengefasst. Abschließend werden im Ausblick Weiterentwicklungsmöglichkeiten formuliert.

6.1 Ergebnisse

Eines der Ziele dieser Arbeit bestand darin, einen Überblick der Produktpalette von Microsofts Sicherheitslösungen zu erzeugen.

Um weitere Informationen über Malware Samples von AV-Test zu generieren, wurde ein Python-Skript entwickelt. Dieses Skript kann mit einem Private-API-Key weiterverwendet werden, um Malwareinformationen bei VirusTotal abzufragen und abzuspeichern.

Die (wie oben beschrieben) gewonnenen Informationen können mithilfe des erarbeiteten Java-Programms eingelesen werden. Nach dem Einlesen werden die Informationen an einen lokal eingerichteten Elasticsearch Suchserver weitergegeben. Dieser beinhaltet im Anschluss die Daten der nachfolgenden Visualisierung. Eine Erweiterung oder Anpassung dieses Java-Programms ist schnell möglich. Hierdurch können zu einem späteren Zeitpunkt andere Malwareattribute, die in dieser Arbeit keine Erwähnung finden, verarbeitet werden.

Durch die Visualisierungen sind die Eigenschaften von Malware einfacher zu vergleichen.

Die Testergebnisse von AV-Test deuten darauf hin, dass die Einpflegung neuer Malwareinformationen und -signaturen bei Microsoft zu lange dauert. Darunter leidet sowohl die signaturbasierte als auch die verhaltensbasierte Erkennung von *System Center Endpoint Protection*.

6.2 Zusammenfassung

Um ein Basiswissen zu erzeugen, wurden die Grundlagen zum Thema Malware, Malwareerkennung und Systemsicherheit erläutert. Dieses Wissen ist notwendig, um die Relevanz des Themengebiets der Malwareerkennung zu verstehen und zu betonen. Darauf folgte die Präsentation der wichtigsten Sicherheitssoftware von Microsoft.

Im Kapitel 4 wurde über AV-Test und deren Testverfahren berichtet. Danach erfolgte ein Einblick in die VirusTotal-API und der wichtigsten Funktionen. Zur Visualisierung der Malwareinformationen dient der Elasticsearch Suchserver in Kombination mit Kibana.

Diese Arbeit hat gezeigt, dass Microsoft viele unterschiedliche Tools für Systemsicherheit anbietet. Der Anwender muss gut informiert sein und wissen, welches Tool für den jeweiligen Spezialfall einsetzbar ist. Es macht den Eindruck, dass Microsoft in erster Linie Privatanwender ansprechen möchte. Dennoch können auch Unternehmen den kostenlosen Schutz der Microsoft Sicherheitsprodukte in Anspruch nehmen. Die Ergebnisse von AV-Test haben gezeigt, dass Microsofts Sicherheitslösungen immer konkurrenzfähiger werden.

6.3 Ausblick

Die gewonnenen Malwareinformationen können für weitere Analysen oder Statistiken verwendet werden.

Die detaillierten Testergebnisse geben Aufschluss darüber, welche Sicherheitssoftware einen nahezu vollständigen Schutz in Kooperation mit *System Center Endpoint Protection* erzielen würde. Ein paralleler Einsatz anderer Antivirensoftware neben *System Center Endpoint Protection* ist dennoch leider ausgeschlossen.

Ein Test der Schutzwirkung von *System Center Endpoint Protection* in Kombination mit *Enhanced Mitigation Experience Toolkit* wurde in dieser Arbeit nicht durchgeführt. Ob hiermit eine Verbesserung der Erkennungsrate erreicht werden kann, könnte eine weitere Untersuchung erarbeiten.

Literaturverzeichnis

[av-test.org Benutzbarkeit] AV-Test: *Einfluss auf die Benutzbarkeit.* https://www.av-test.org/de/testverfahren/testmodule/benutzbarkeit/. – Abruf: 2016-04-23

[av-test.org Geschwindigkeit] AV-Test: *Geschwindigkeit (Systembelastung).* https://www.av-test.org/de/testverfahren/testmodule/geschwindigkeit/. – Abruf: 2016-04-23

[av-test.org Laborausstattung] AV-Test: *Mit Hightech, Know-how und Effizienz.* https://www.av-test.org/de/institut/laborausstattung/. – Abruf: 2016-04-23

[av-test.org Malware] AV-Test: *Malware.* https://www.av-test.org/de/statistiken/malware/. – Abruf: 2016-04-23

[av-test.org Produkte] AV-Test: *Produkte aus dem Expertenlabor.* https://www.av-test.org/de/institut/produkte/. – Abruf: 2016-04-23

[av-test.org Reparaturleistung] AV-Test: *Reparaturleistung.* https://www.av-test.org/de/testverfahren/testmodule/reparaturleistung/. – Abruf: 2016-04-23

[av-test.org Schutzwirkung] AV-Test: *Schutzwirkung.* https://www.av-test.org/de/testverfahren/testmodule/schutzwirkung/. – Abruf: 2016-04-23

[av-test.org Testergebnisse] AV-Test: *Die besten Antivirus Programme für Windows Client Unternehmensanwender.* https://www.av-test.org/de/antivirus/unternehmen-windows-client/. – Abruf: 2016-04-23

[av-test.org Testverfahren] AV-Test: *Detaillierte Analysen und umfassende Tests.* https://www.av-test.org/de/testverfahren/. – Abruf: 2016-04-23

[av-test.org Zertifizierung] AV-Test: *Zertifizierte Sicherheit.* https://www.av-test.org/de/testverfahren/zertifizierung/. – Abruf: 2016-04-23

[Bollier und Firestone 2010] Bollier, David ; Firestone, Charles M.: *The promise and peril of big data.* Aspen Institute, Communications and Society Program Washington, DC, 2010

[BSI Lagebericht 2015] Bundesamt für Sicherheit in der Informationstechnik ; Informationstechnik, Bundesamt für Sicherheit in der (Hrsg.): *Die Lage der IT-Sicherheit in Deutschland 2015.* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob=publicationFile&v=4. November 2015

[corewar.co.uk] Core War: *Creeper & Reaper.* http://corewar.co.uk/creeper.htm. – Abruf: 2016-04-24

[cybermap.kaspersky.com] Kaspersky Lab ZAO: *CYBERTHREAT REAL-TIME MAP.* https://cybermap.kaspersky.com/. – Abruf: 2016-05-16

[DFN-Konferenz 2016] Lurz, Hanna ; Dolle, Wilhelm: Sicherheit von kritischen Infrastrukturen in Deutshcland - sind wir mit dem IT-Sicherheitsgesetz auf dem richtigen Weg? In: Paulsen, Dr. C. (Hrsg.): *Sicherheit in vernetzten Systemen : 23. DFN-Konferenz.* DFN-CERT Services GmbH, Sachsenstraße 5, d-20097 Hamburg : BoD - Books on Demand, Februar 2016, S. H–1 – H–13

[Gartner 2016] Gartner: *Magic Quadrant for Endpoint Protection Platforms.* https://www.gartner.com/doc/reprints?id=1-2XXIZ8F&ct=160204&st=sg&mkt_tok=3RkMMJWWfF9wsRonvKjNeu2FhmjTEU5z16OgrW6C1hJl41El3fuXBP2XqjvpVQcNiPb%2FKRw8FHZNpywVWM8TIJdQVt9ZlLwziDmk%3D. Februar 2016. – Abruf: 2016-04-23

[giga.de] Giga: *Bundestrojaner entfernen - und das ganz ohne zu zahlen.* http://www.giga.de/extra/malware/tipps/bundestrojaner-entfernen-und-das-ganz-ohne-zu-zahlen/. – Abruf: 2016-04-24

[hexacorn.com] Hexacorn Ltd: *2014-12-24_santas_bag_of_mutants.* http://hexacorn.com/examples/2014-12-24_santas_bag_of_mutants.txt. – Abruf: 2016-05-19

[Infosec] Golomb, Gary: *Mutexes, part one: The Canary in the Coal Mine and Discovering New Families of Malware*. http://resources.infosecinstitute.com/mutexes-analysis-part-one/. – Abruf: 2016-05-08

[IT-Sicherheitsgesetzentwurf 2014] Bundesministerium des Innern: *Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile. Dezember 2014. – Abruf: 2016-04-22

[Kallenberg und Kovah] Kallenberg, Corey ; Kovah, Xeno: *How Many Million BIOSes Would you Like to Infect?* http://legbacore.com/Research_files/HowManyMillionBIOSWouldYouLikeToInfect_Full.pdf. – Abruf: 2016-04-24

[Kossakowski 2016] Kossakowski, Dr. Klaus-Peter: *IT-Sicherheit: Einleitung*. http://users.informatik.haw-hamburg.de/~kpk/pub/sose2016/it-sicherheit/ITSW-01-Einleitung_v03.pdf. 2016. – Abruf: 2016-05-01

[Malware Protection Center a] Microsoft: *How Microsoft antimalware products identify malware: unwanted software and malicious software*. https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx. – Abruf: 2016-04-25

[Malware Protection Center b] Microsoft: *Updating your Microsoft antimalware and antispyware software*. https://www.microsoft.com/security/portal/definitions/adl.aspx. – Abruf: 2016-05-10

[Microsoft Safety & Security Center] Microsoft Windows: *See if your Windows operating system has protection built in*. https://www.microsoft.com/en-us/security/pc-security/protect-os.aspx. – Abruf: 2016-04-23

[Microsoft Safety Scanner 2011] Microsoft: *Microsoft Safety Scanner: Kostenloser Sicherheitsscan für Ihren Computer*. https://www.microsoft.com/security/scanner/de-de/default.aspx. 2011. – Abruf: 2016-04-23

[Microsoft Security Essentials] Microsoft: *Produktinformationen zu Microsoft Security Essentials*. http://windows.microsoft.com/de-de/windows/

security-essentials-product-information#tabs1=overview. – Abruf: 2016-04-23

[Microsoft Support 2016] Microsoft: *Das Microsoft Windows Tool zum Entfernen von bösartiger Software dient zum Entfernen von spezifischer, weit verbreiteter bösartiger Software von Computern, auf denen unterstützte Versionen von Windows ausgeführt werden.* https://support.microsoft.com/de-de/kb/890830. April 2016. – Abruf: 2016-04-23

[Morgenstern 2015] Morgenstern, Maik: *Fragen zu dem Test von März-April 2015.* E-Mail mmorgen@av-test.de. Oktober 2015

[Neumann 1966] Neumann, John von ; Burks, Arthur W. (Hrsg.): *Theory of Self-Reproducing Automata.* University of Illinois Press, 1966

[norton.com 2016] Norton: *Norton Was ist Cyberkriminalität?* http://de.norton.com/cybercrime-definition. 2016. – Abruf: 2016-04-22

[OECD 2009] Organisation for Economic Co-operation and Development (Hrsg.): *Computer viruses and other malicious software : a threat to the internet economy.* Paris : OECD, 2009

[Plue 2012] Plue, Andrew ; Moss, Stephanie (Hrsg.) ; Sheikh, Azharuddin (Hrsg.) ; Mayekar, Kaustubh S. (Hrsg.): *Microsoft System Center 2012 Endpoint Protection Cookbook.* Livery Place, 35 Livery Street, Birmingham B3 2PB, UK : Packt Publishing Ltd., October 2012

[RSA Conference 2015] Russinovich, Mark: *Malware Hunting with the Sysinternals Tools.* https://www.rsaconference.com/writable/presentations/file_upload/hta-t07r-license-to-kill-malware-hunting-with-the-sysinternals-tools-final.pdf. April 2015. – Abruf: 2016-05-10

[Security Essentials Warnstufen] Microsoft: *Warnstufen in Microsoft Security Essentials.* http://windows.microsoft.com/de-de/windows/understanding-alert-levels. – Abruf: 2016-04-23

[statista.com 2016] Statista: *Schäden durch Cyberkriminalität in Deutschland von 2006 bis 2014 (in Millionen Euro).* http://de.statista.com/statistik/daten/studie/193207/umfrage/

finanzielle-schaeden-durch-cyberkriminalitaet-in-deutschland/. 2016. – Abruf: 2016-04-22

[Stix 2008] Stix, Manuel: *Microsoft Forefront Sicherheit für Unternehmensnetzwerke*. http://slideplayer.org/slide/875464/. 2008. – Abruf: 2016-04-23

[Symantec] Symantec Corporation: *A New Zero-Day Vulnerability Discovered Every Week in 2015*. https://www.symantec.com/content/dam/symantec/docs/infographics/istr-zero-day-en.pdf. – Abruf: 2016-04-25

[System Center Endpoint Protection Einführung] Microsoft: *Einführung in Endpoint Protection in Configuration Manager*. https://technet.microsoft.com/de-de/library/hh508781.aspx. – Abruf: 2016-04-23

[TechNet EMET] Microsoft: *Enhanced Mitigation Experience Toolkit*. https://technet.microsoft.com/de-de/security/jj653751?f=255&MSPPError=-2147217396. – Abruf: 2016-05-06

[TechNet Forefront 2012] Microsoft Forefront: *Important Changes to Forefront Product Roadmaps*. https://blogs.technet.microsoft.com/server-cloud/2012/09/12/important-changes-to-forefront-product-roadmaps/. 2012. – Abruf: 2015-04-22

[TechNet System Center] Microsoft: *System Center 2012 Endpoint Protection*. https://technet.microsoft.com/de-de/systemcenter/hh877806. – Abruf: 2016-04-23

[virustotal.com] VirusTotal: *About VirusTotal*. https://www.virustotal.com/de/about/. – Abruf: 2016-04-23

[Wang u. a. 2009] Wang, Cheng ; Pang, Jianmin ; Zhao, Rongcai ; Fu, Wen ; Liu, Xiaoxian: Malware Detection Based on Suspicious Behavior Identification. In: Hu, Zhengbing (Hrsg.) ; Liu, Qingtang (Hrsg.): *First International Workshop on Education Technology and Computer Science* Bd. 2 The Institute of Electrical and Electronics Engineers, Inc. (Veranst.), IEEE, März 2009, S. 198 – 202

[Wikipedia] Wikipedia: *Windows Defender*. https://de.wikipedia.org/wiki/Windows_Defender. – Abruf: 2016-04-23

[Wikipedia Beast] WIKIPEDIA: *Beast (Trojan horse)*. https://en.wikipedia.org/wiki/Beast_(Trojan_horse). – Abruf: 2016-04-24

[Windows Defender Offline] MICROSOFT: *Was ist Windows Defender Offline?* http://windows.microsoft.com/de-DE/windows/what-is-windows-defender-offline. – Abruf: 2016-04-23

[WinOneCare 2015] WIKIPEDIA: *Windows Live OneCare*. https://de.wikipedia.org/wiki/Windows_Live_OneCare. 2015. – Abruf: 2016-04-22

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 31.05.2016 Krisztina Ágota Gyarmati