

Bachelorarbeit

zur Erlangung des akademischen Grades
Bachelor

Technische Hochschule Wildau

Fachbereich Wirtschaft, Informatik, Recht

Studiengang Verwaltungsinformatik Brandenburg (B.Sc.)

Thema (deutsch): Malware-Analyse - Wie Forensik-Tools helfen die Funktionsweise von Cyberangriffen zu verstehen

Thema (englisch): Malware-Analysis - How to enhance the understanding of cyberattacks using forensic-tools

Autor/in: Patrick Lucas Büdke

Seminargruppe: VIB1/19

Betreuer/in: Dr. Frank Seeliger

Zweitgutachter/in: Herr Falko Benthin

Inhaltsverzeichnis

| | |
|---|-------------|
| Zusammenfassung | III |
| Abstract | IV |
| Abbildungsverzeichnis | V |
| Tabellenverzeichnis | VI |
| Abkürzungsverzeichnis | VII |
| Glossar | VIII |
| 1 Einleitung | 1 |
| 1.1 Fragestellung | 1 |
| 1.2 Forschungsstand | 1 |
| 1.3 Aufbau der Arbeit | 1 |
| 2 Theoretische Grundlagen | 2 |
| 2.1 Terraform | 2 |
| 2.1.1 Funktionsweise | 2 |
| 2.1.2 Vorteile | 4 |
| 2.2 Cloud Computing | 5 |
| 2.2.1 Die Arten von Cloud-Diensten | 5 |
| 2.3 Virtuelle Maschinen | 7 |
| 2.3.1 Was ist eine virtuelle Maschine? | 7 |
| 2.3.2 Erstellen einer virtuellen Maschine | 7 |
| 2.3.3 Absicherung einer virtuellen Maschine | 8 |
| 2.4 Malware | 9 |
| 2.4.1 Was ist Malware und wie funktioniert sie? | 9 |
| 2.4.2 Arten von Malware | 9 |
| 2.4.2.1 Viren | 10 |
| 2.4.2.2 Trojaner | 10 |
| 2.4.2.3 Würmer | 11 |
| 2.4.2.4 Spyware/Adware | 11 |
| 2.4.2.5 Scareware | 12 |
| 2.4.2.6 Ransomware | 12 |
| 2.4.2.7 Root kit | 13 |
| 2.4.2.8 Backdoors | 14 |
| 2.5 Malware-Analyse | 15 |
| 2.5.1 Statische Analyse | 15 |
| 2.5.2 Dynamische Analyse | 16 |

| | | |
|----------|--|-----------|
| 3 | Methodik | 17 |
| 3.1 | Terraform | 17 |
| 3.2 | Virtuelle Umgebung | 17 |
| 3.3 | Tools | 18 |
| 3.4 | Malware | 18 |
| 4 | Ergebnisse | 19 |
| 5 | Bewertung des Ergebnisses | 20 |
| 5.1 | Vorteile der Vorgehensweise | 20 |
| 5.2 | Nachteile der Vorgehensweise | 20 |
| 6 | Diskurs | 21 |
| 6.1 | Schlussbetrachtung | 21 |
| 6.2 | Ausblick | 21 |
| 7 | Literatur- und Quellenverzeichnis | 22 |
| | Literatur- und Quellenverzeichnis | 22 |
| 8 | Anhang | 23 |
| A | Anhang A | 23 |

Zusammenfassung

Diese Arbeit untersucht die automatisierte Bereitstellung einer virtuellen und abgesicherten Umgebung, mit welcher schädliche Software analysiert werden kann. Diese Umgebung läuft auf virtuellen Maschinen (VMs), die in kurzer Zeit mit dem Infrastructure-as-Code-Tool (IaC-Tool) Terraform von HashiCorp erzeugt werden. In dieser Umgebung kann Malware beobachtet und analysiert werden, ohne dass es Folgen nach sich zieht. Hier sind zudem, für die Malware-Analyse nützliche Tools installiert.

Abstract

Abbildungsverzeichnis

| | | |
|---|-------------------------------------|---|
| 1 | Terraform - Argument | 2 |
| 2 | Terraform - Block | 3 |
| 3 | Terraform - Planungsphase | 3 |

Tabellenverzeichnis

Abkürzungsverzeichnis

VM Virtuelle Maschine

SSH Secure Shell

DNS Domain Name System

IaaS Infrastructure as a Service

PaaS Platform as a Service

SaaS Software as a Service

OS-Image Operating System-Image

SSD Solid State Drive

Glossar

App - ist eine Anwendung

Cloud - ist in der IT die Abkürzung für Cloud Computing und wird auch als Rechnerwolke oder Datenwolke bezeichnet

Cloud Server - ist ein virtueller Server. Dieser bezieht seine Hardwarekomponenten von externen Dienstleistern und wird über das Internet angeboten.

Firewall - ist ein Sicherungssystem um Netzwerke und Computer vor unerwünschten Zugriffen zu schützen

Open-Source-Software - ist Software deren Quellcode der Öffentlichkeit zugänglich ist. Die Benutzung des Codes steht dem Benutzer selbst offen.

OS-Images - ist eine komprimierte Sammlung von Referenzdateien und Ordnern, die zum Installieren und Konfigurieren eines neuen Betriebssystems auf einem Computer verwendet werden

Workflow - die Abwicklung arbeitsteiliger Vorgänge

Cloud Provider - Anbieter für Cloud Computing

1 Einleitung

-

1.1 Fragestellung

-am ende entscheiden ob der punkt drin bleibt oder nicht

1.2 Forschungsstand

-nennung von Messen wie bspw. defcon
-publikationen aus exposé-quellen einbeziehen

1.3 Aufbau der Arbeit

-von welchem Thema gehe ich zu welchem thema um roten faden darzulegen

2 Theoretische Grundlagen


2.1 Terraform

2.1.1 Funktionsweise

Terraform ist eine *Open-Source-Software*, welche die Vorbereitung von *Cloud Servern* einfacher macht. Sie wurde von HashiCorp dazu entwickelt, Infrastrukturen vorzubereiten und zu verwalten.¹ Mit Infrastrukturen sind hier *virtuelle Maschinen* verschiedenster Anbieter gemeint.² Terraform hat lizenzierte Partner für die seine Dienste anwendbar sind.³ Durch die hohe Konnektivität dieser Software sind die Einsatzorte sehr vielseitig. Das macht die Software in der Entwicklung und im Betrieb von Unternehmen sehr attraktiv.

Terraform ist ein Infrastructure-as-Code-Tool und wird für die Bereitstellung von physischen als auch virtuellen Servern verwendet. Das Tool arbeitet mit Konfigurationsdateien, die in der HashiCorp Configuration Language(HCL) geschrieben werden. Die genannten Dateien sind von Menschen lesbar und gewährleisten dadurch die geringe Komplexität der Sprache. Zudem ist HCL eine deklarative Sprache. Das heißt, dass der Nutzer den Wunschaufbau des Servers in der Terraform-Datei beschreibt. Die einzelnen Schritte um den gewünschten Serverzustand zu erreichen werden von Terraform übernommen.

Die Prozesse in die die Arbeit mit Terraform unterschieden werden kann, sind in drei Schritte aufgeteilt. Der erste Schritt ist `write`. In dieser Phase wird der Code definiert. Dafür werden die benötigten Ressourcen für die jeweiligen Provider definiert. Dafür Terraform-Konfigurations-Dateien mit der Endung `.tf` verwendet. Aus diesen Dateien entnimmt Terraform beispielsweise welcher Cloud-Anbieter verwendet wird. Als Beispiel für einen Anbieter mit dem Terraform funktioniert kann die "Hetzner-Cloud" genannt werden. Zu den Providern findet sich auf der Seite von Terraform eine jeweilige Dokumentation darüber, wie die Ressourcen einzubinden sind. Der Code der Konfigurations-Dateien entscheidet darüber, wie der Server konfiguriert wird, wenn das Skript ausgeführt wird.



```
image_id = "abc123"
```

Abbildung 1: Terraform - Argument

¹Wang, 2022.

²Brikman, 2019

³HashiCorp, 2022.

In der obigen Abbildung ist die allgemeine Syntax eines Argumentes in Terraform dargestellt. Ein Argument ist ein Name dem ein Wert zugewiesen wird. Die Art dieses Wertes ist vom Kontext abhängig in dem das Argument erstellt wird.

```
# Create a server
resource "hcloud_server" "forensics" {
  name          = "forensics"
  image         = "ubuntu-22.04"
  server_type   = "cx11"
  firewall_ids = [hcloud_firewall.saferfw.id]
  ssh_keys     = [hcloud_ssh_key.default.id]
  user_data     = file("user_data.yml")
}
```

Abbildung 2: Terraform - Block

In dieser Abbildung ist der allgemeine Aufbau eines Blocks in Terraform zu erkennen. Ein Block beginnt mit dem `type`. Er legt auch fest welche und wie viele sogenannte Bezeichner folgen müssen. Der Inhalt des Blocks befindet sich in geschweiften Klammern. In diesen Klammern sind zusätzliche Argumente zu finden. Diese bestimmen die Abhängigkeiten und die Zusammenhänge mit anderen Blocks und Argumenten. In diesem Beispiel ist der Typ des Blocks ein Server in der "Hetzner-Cloud". Dieser verlangt als weiteren Bezeichner einen Namen. Innerhalb des Blocks ist zudem die Abhängigkeit von der Firewall zu erkennen.

Wenn der Code verfasst wurde folgt der nächste Schritt im Arbeitsablauf von Terraform. Dieser ist die Planung der vorgenommenen Aktionen. Wird `terraform apply` in der Kommandozeile eingegeben so wird dieser Plan erstellt. Dieser wird im Anschluss daran ausgegeben. Um Fortzufahren muss der Plan, indem jeder Schritt aufgelistet ist, den Terraform durchführen wird, bestätigt werden. Diese einzelnen Schritte können Änderungen, Löschungen oder das Hinzufügen von Dateien sein.

```
terraform apply

Terraform used the selected providers to generate the following execution plan.
Resource actions are indicated with the following symbols:
  + create

Terraform will perform the following actions:
```

Abbildung 3: Terraform - Planungsphase

Die Dritte und letzte Phase im Terraform-*Workflow* ist `apply`. Sie beginnt mit der Bestätigung des Plans. Ab diesem Zeitpunkt beginnt Terraform mit der Bereitstellung des Servers. Welche Systemkomponenten und Sicherheitseinstellungen dieser hat ist von den Konfigurationsdateien abhängig.

2.1.2 Vorteile

Terraform birgt einige nützliche Vorteile. Einer dieser ist die Flexibilität. Terraform ist ein großes Provisioning-Tool und hat viele Partner in Form von Providern. Diese Provider lassen eine Servererstellung mittels Terraform zu. So kann beispielsweise eine Konfiguration für einen Hetzner-Server mit wenigen Änderungen verwendet werden um eine virtuelle Umgebung bei "Oracle " zu erstellen. Diese Flexibilität ist besonders für dieses Projekt interessant, denn so kann die virtuelle Umgebung bei verschiedenen Anbietern identisch konfiguriert und verwendet werden.

Ein weiterer Vorteil der sich daraus ergibt ist, dass Terraform sehr schnell ist. Mit den Befehlen `init` und `apply` wird nach Bestätigung eine virtuelle Umgebung mit den gewünschten Konfigurationen erstellt. Dies ist gegenüber dem manuellen Einrichten einer virtuellen Umgebung sehr zeitsparend.

Hinzu kommt, dass Terraform gut zu verstehen ist. Die Sprache in der die Konfigurationsdateien geschrieben ist, ist sehr intuitiv und gut verständlich. Wenn die Syntax einmal begriffen wurde lässt sich aus den Konfigurationsdateien gut auf das Endprodukt schließen. Natürlich sind virtuelle Umgebungen die von Grund auf komplex sind auch in Terraform komplex. Dennoch ist die Verständlichkeit der Sprache eine positive Anmerkung Wert.

Weiterhin ist für IT-Teams die Planungsphase ein gutes Tool um Veränderungen bereits im Vorweg zu sehen und Folgen abschätzen zu können. Dabei können Fehler die zu einem unerwünschten Ergebnis führen frühzeitig erkannt und vermieden werden. Zudem ist die Möglichkeit Server über Terraform zu verwalten sehr attraktiv, um schnelle und bedachte Änderungen an der Umgebung vorzunehmen.

2.2 Cloud Computing

Cloud Computing (*deutsch Rechnerwolke oder Datenwolke*) ist das Bereitstellen von einzelnen Anwendungen bis hin zu Rechenzentren. Die Ressourcen hierfür werden aus der *Cloud* genommen, welche auch als *Internet* bekannt ist. Durch flexible Einstellungsoptionen ist es durch Cloud Computing möglich IT-Systeme bedarfsspezifisch und flexibel anzubieten. Dabei ist auch zu beachten, dass Cloud Computing viele Vorteile mit sich bringt. Darunter fallen beispielsweise die Kosten und die Skalierbarkeit virtueller Systeme.

Cloud Computing wird in drei Arten aufgeteilt: Public (öffentlich), Privat (privat) und Hybrid (Mischung aus öffentlich und privat). Bei der öffentlichen Form besitzt ein Dienstleister die benötigten Ressourcen, welchen man *Cloud Provider* nennt. Dabei werden die den Kosten entsprechenden Komponenten dem Kunden über das Internet zur Verfügung gestellt. Dabei spielen die Kosten als Vorteil eine große Rolle, da die Hardware nicht selbst angeschafft werden muss. Zudem sind Hardware-Wartungen nicht nötig, da diese vom *Cloud Provider* übernommen werden. Durch die Vielzahl an Hardware-Komponenten, die große Anbieter haben, steigt die Skalierbarkeit sehr stark. Die Servermenge ist außerdem ausschlaggebend dafür, dass das Risiko eines Ausfalls minimiert wird.

Die private Form des Cloud Computings unterscheidet sich von der öffentlichen Form. Besonders im Aspekt des Zugriffs auf die Hardware treten Unterschiede auf. Während bei der öffentlichen Form die selbe Hardware von verschiedenen Kunden genutzt wird, wird die Hardware bei privaten Cloud Computing-Lösungen nur einem Kunden zugewiesen. Diese kann hierbei im Besitz des Kunden sein und sich in seiner Organisation befinden. Auch kann sich die Hardware in Räumen von Drittanbietern befinden. Dabei ist sie dennoch nur für einen Käufer der Systemkomponenten bestimmt. So können Unternehmen ihre Netzwerkrichtlinien souverän bestimmen. Zudem gewährleistet die private Nutzung von Hardware mehr Sicherheit.

In der hybriden Form sind die beiden vorangegangenden Modelle vereint. Ziel dabei ist es die Vorteile beider Formen in einer Form zu verschmelzen. Beispielsweise kann die große Flexibilität von öffentlichen Clouds benutzt werden. Währenddessen stellt die private Cloud, durch ihre höhere Sicherheit, eine Zone für vertrauliche Objekte des Netzwerkes da. Aus der Zusammenführung der beiden Modelle ergibt sich eine Form, die die Vorteile vereint. Die Netzwerkkontrolle ist geboten, die Kosteneffizienz ist hoch und es wird ein hohes Maß an Flexibilität geboten.

2.2.1 Die Arten von Cloud-Diensten

Infrastructure as a Service (IaaS) oder zu deutsch: *Infrastruktur als Dienstleistung* stellt die notwendigen Systemkomponenten bereit. Dazu zählen beispielsweise der Arbeitsspeicher, die Festplatte oder der Prozessor. Diese Komponenten können von Drittanbietern oder von der Organisation selbst bereitgestellt werden. In dieser Kategorie sind *Amazon*

Web Services, *Microsoft Azure* oder auch die *Hetzner Cloud* einzuordnen. Diese bieten das digitale bereitstellen von Servern an. Diese Server sind an die Anforderungen angepasst und flexibel erweiterbar. So zahlt der Nutzer nur für das, was er benutzt. Zudem muss er so keine Hardware für die Server selber bereitstellen.

Platform as a service (PaaS) oder zu deutsch: *Plattform als Dienstleistung* stellt die Plattform für Entwicklungen und Anwendungen bereit. Diese wird von der folgenden Dienstleistung *Software as a service (SaaS)* benötigt. Nutzer von PaaS sind zum Beispiel Anwendungsentwickler die in großen Teams zusammen an einem Projekt arbeiten. Als Vertreter von PaaS -Produkten kann *Google App Engine* genannt werden. Hier stehen für den Nutzer verschiedene Entwicklungssprachen zur Verfügung. Der Vorteil ist, dass viele Aufgaben die Entwickler übernehmen müssten um eine skalierbare Software zu schreiben, von Google übernommen werden. Somit werden die Arbeitszeit und Kosten verringert.

Software as a service (SaaS) befasst sich mit der Software von Systemen. Eine Software ist eine Anwendung für einen Computer. Der Inhalt der Software legt fest was bei seiner Ausführung auf dem Computer passiert. Der ausführende Teil wird von der Hardware übernommen. Bei Software aus dem Modell *SaaS* werden Anwendungen, die cloud-basiert arbeiten können angeboten. Diese sind in der Regel skalierbar, sodass sie auf Wünsche einzelner Organisationen eingehen können. Darunter fällt beispielsweise das Tool des Softwarekonzerns *SAP Enterprise Resource Planning*. Dieses Tool ist für Unternehmen gedacht und kann Prozesse im Zusammenhang betrachten und beispielsweise analysieren. Hier wird klar, dass die Skalierbarkeit von *SaaS* große Vorteile bringt. So kann Software individuell auf Unternehmen angepasst werden, um den einzelnen Anforderungen gerecht zu werden.

2.3 Virtuelle Maschinen

2.3.1 Was ist eine virtuelle Maschine?

Virtuelle Maschinen bilden mit Infrastructure as a Service (IaaS) eines der drei Servicemodelle des Cloud Computings. Sie beruhen auf der Idee Hardware, Rechenleistung, Speicherplatz und Netzwerkressourcen aus der Cloud bereitzustellen. So soll der Benutzer von virtuellen Maschinen das gleiche Erlebnis wie er es auch bei physischen Geräten haben.

Der Vorteil daran, dass virtuelle Maschinen ein aus dem Internet bereitgestellter Dienst ist ist die Flexibilität. Durch die Verwendung von virtuellen Maschinen können Kosten gespart werden. Das rührt daher, dass der Kunde sein System den Anforderungen entsprechend planen und umsetzen kann. Ist die VM einmal aufgesetzt und soll vergrößert werden, muss nicht die Hardware ausgetauscht werden. Stattdessen wird die Größe der virtuellen Umgebung individuell angepasst. Damit einher geht auch die Änderung der Kosten für das System.

Zudem ist die Unabhängigkeit vom Host-System ein Vorteil. In vielen Unternehmen wird Windows als graphisches Betriebssystem benutzt. Dennoch kann es sein, dass ein Rechner mit einem Linux-System für manche Prozesse besser geeignet ist. Alle Rechner auf Linux umzustellen nur, weil bestimmte Abläufe so besser funktionieren ist aber auch keine Lösung. Auch die Anschaffung eines einzelnen Rechners, um Linux zu benutzen ist nicht effizient und praktisch. Stellvertretend dafür kann Linux auf einer virtuellen Umgebung laufen. Die Kosten dafür sind je nach Gerätekonfiguration weit unter dem Hardwarepreis für ein Gerät mit gleicher Ausstattung. Zudem ist die Verfügbarkeit des Gerätes gewährleistet, da theoretisch von überall wo es freien Internetzugang gibt auf die Cloud zugegriffen werden kann.

2.3.2 Erstellen einer virtuellen Maschine

Eine virtuelle Maschine kann in der Regel bei einem *Cloud Provider* erstellt werden. Bevor jedoch eine VM erstellt wird muss darüber nachgedacht werden zu welchem Zweck die VM ist. Daraus ergeben sich wichtige Konfigurationsmerkmale wie das Betriebssystem oder die Sicherheitskonfigurationen. Nach dieser Planungsphase kommt es zum Erstellen der VM. Hierfür kann die grafische Umgebung der jeweiligen Provider genutzt werden. Das Erstellen eines einfachen Servers ist so schnell und unkompliziert gemacht. Für die Verbildlichung einer solchen Weboberfläche wird in dieser Arbeit die *Hetzner-Cloud* verwendet. Hier wird zuerst über das Feld "NEUES PROJEKT" ein Projekt erstellt. In diesem Projekt kann mithilfe des Buttons "SERVER HINZUFÜGEN" ein Server erstellt werden. Der Server hat die Konfigurationsoptionen:

Standort - bestimmt woher die Serverleistungen kommen sollen

Image - ist in die Reiter *OS-Images* und *Apps* aufgeteilt. Es bietet die Möglichkeit das Betriebssystem und Tools zu installieren.

Typ - hier kann die Rechenleistung, Festplattengröße und das maximale Datenaufkommen festgesetzt werden. Der Preis der jeweiligen Cloudlösung ist mit aufgelistet.

Volume - hier kann SSD-Speicher festgelegt werden

Networking - Festlegen über welche Netze der Server kommunizieren darf

Firewalls - können hinzugefügt werden, nachdem sie in einem anderen Teil der *Hetzner Cloud* erstellt wurden

Zusätzliche Features - Festlegung von Benutzerdaten, Backups und Platzierungsgruppen

SSH-Key - hier kann der SSH-Key hinzugefügt werden

Name - Festlegung des Servernamens

Die virtuelle Maschine kann auch mit Terraform aufgesetzt werden. Durch die Vielzahl an Partnern sind Konfigurationen in Terraform besser an andere Provider anpassbar und werden somit wiederverwendbar. Dafür müssen in den Konfigurationsdateien von Terraform nur wenige Ressourcen geändert werden. Wie eine VM mit Terraform aufgesetzt werden kann, wird in einem späteren Teil der Arbeit an einem Beispiel aufgegriffen(3.1).

2.3.3 Absicherung einer virtuellen Maschine

Die Sicherung der virtuellen Maschine kann je nach Einsatzgebiet eine große Bedeutung haben. Um Sicherheitskonfigurationen einzubinden kann die Firewall bearbeitet werden. Auch dafür bietet Terraform eine Möglichkeit.

-Terraform

2.4 Malware

2.4.1 Was ist Malware und wie funktioniert sie?

Laut Definition ist Malware eine "böswärtige Software" (auf Englisch "malicious software").

Allgemein dient der Begriff Malware als Klassifizierung von Dateien oder Software, die Schäden verursachen, sobald sie sich im System des Benutzers befinden.

Die häufigsten Arten sind:

1. Viren
2. Trojaner
3. Würmer
4. Spyware/Adware
5. Scareware
6. Ransomware
7. Root kit und Backdoors

Dabei können sowohl persönliche Schäden als auch Sachschäden entstehen.

Um einen solchen Malware Angriff zu tätigen, benötigt man einen Schadcode. Mithilfe dessen verschaffen sich Cyberkriminelle Zugriff auf das System des Opfers und klauen Passwörter oder andere sensible Daten. Um den Datendiebstahl durchzuführen, muss ein Cyberkrimineller dafür sorgen, dass der Schadcode auf dem Zielsystem ausgeführt wird. Damit das klappt, betten diese den schädlichen Code in eine Datei ein, die das Opfer öffnen soll. Nach der Durchführung erfüllt der Schadcode seinen Zweck und installiert zum Beispiel eine Backdoor oder startet einen Key-Logger. Key Logger können unter anderem die Eingabe von Passwörtern protokollieren.

2.4.2 Arten von Malware

Neue Schadprogramm Varianten entstehen, wenn die Funktionsweise der neuen Malware grundlegend von bereits vorhandenen Schadprogrammen abweicht. Wichtig ist hierbei, dass der Hashwert einzigartig ist, aber ein neuer Hashwert nicht mit einer neuen Malware gleichzusetzen ist. Das Ergebnis einer Hashfunktion unterscheidet sich bereits bei geringfügigen Veränderungen im Programmcode. Das heißt, dass ein neuer Hashwert nicht eine neue Malware bedeutet, da die Funktionsweise des Schadcodes teilweise die selbe bleibt.

Während für bekannte Schadprogramm-Varianten teilweise Detektionsmethoden existieren, sind neue Varianten unmittelbar nach ihrem Auftreten unter Umständen noch nicht als Schadprogramme erkennbar und daher besonders bedrohlich.

Zudem kann zwischen den Arten nicht sonderlich stark differenziert werden, da sie ineinander übergehen und ähnliche Methodiken und Ziele verfolgen.

2.4.2.1 Viren

Viren, die Programme befallen, bestehen wie ausführbare Programme aus Code. Der spezifische Code ist stark von der jeweiligen Hardwareplattform und auch dem verwendeten Betriebssystem abhängig. Das ergibt sich mitunter daraus, dass Programme grundsätzlich einige Funktionen des Rechners nicht direkt ansprechen und durch System Calls bewilligt werden müssen.

Da sich der Virencode in den Programmcode einbetten muss, ist ein Virus meistens auf eine bestimmte Plattform und Betriebssystem als Wirt festgelegt und kann Systeme mit anderer Plattform oder anderem Betriebssystem nicht infizieren.

Der ausführbare Code des Virus wird im Code des ursprünglichen Programms platziert und das Programm so modifiziert, dass beim Start zuerst der Virus aufgerufen wird.

Um länger unbemerkt zu bleiben, transferieren viele Viren danach die Kontrolle zurück an das ursprüngliche Programm, so dass dessen Funktion durch den Virus scheinbar nicht beeinträchtigt wird. Gelangt das Virus zur Ausführung, kann es weitere Programmdateien auf dem Rechner infizieren und gegebenenfalls weiteren Schadcode ausführen.

Viren müssen nicht unbedingt nur ausführbare Programme infizieren. Einige Viren nisten sich im Hauptspeicher des Rechners ein und bleiben dort durchgehend aktiv. Solche Viren werden als "speicherresistente" Viren bezeichnet.

In bestimmten Fällen können sich Viren auch über Dokumente, also eigentlich nicht ausführbare Daten, verbreiten. Dies ist unter anderem möglich, wenn die Anwendungsprogramme, welche die Dokumente aufrufen, Schwachstellen aufweisen, welche die Ausführung des injizierten Codes ermöglicht.

2.4.2.2 Trojaner

Trojaner sind Schadsoftware-Varianten, über die meist destruktive oder datenstehlende Malware auf ein System geschleust wird. Anders als Viren und Würmer, sind Trojaner nicht in der Lage, sich selbstständig zu replizieren oder Dateien zu infizieren. Sie tarnen ihre Malware als nützliches Programm und hoffen darauf, dass arglose Nutzerinnen und Nutzer sie eigenhändig installieren. Täuschung ist hierbei ihre Verbreitungsstrategie. Häufig kommen Trojaner in fingierter Software vor, die von Cyber-Kriminellen manipuliert wurde. Diese Software ist zumeist als Download in unseriösen Quellen verfügbar.

In den meisten Fällen bestehen Trojaner aus zwei eigenständigen Programmen, die auf verschiedene Weise miteinander verknüpft sein können. Sogenannte Linker heften das Schadprogramm an eine ausführbare Wirtssoftware. Wird das vermeintlich nützliche Programm ausgeführt, startet gleichzeitig auch der Schadcode im Hintergrund.

Eine zweite Möglichkeit ist der Einsatz eines Droppers, der beim Start des Wirtsprogramms heimlich die Schadsoftware auf dem System ablegt. Während die Ausführung des schädlichen Programms im ersten Fall vom Wirt abhängig ist, kann es bei Einsatz

des Droppers völlig unabhängig vom Trojanischen Pferd agieren.

Die dritte Möglichkeit ist die Integration des geheimen Codes in eine Wirtssoftware, wie es zum Beispiel bei vielen Browser-Plugins der Fall ist. Auch hier ist die Ausführung des schädlichen Programms an die Wirtssoftware gebunden. Wird diese beendet oder gelöscht, stehen auch die geheimen Funktionen nicht mehr zur Verfügung.

Weil der Trojaner in der Regel durch den Anwender selbst gestartet wird, hat er die gleichen Rechte wie der angemeldete Benutzer. Folglich kann er alle Aktionen ausführen, die auch der Nutzer ausführen könnte.

2.4.2.3 Würmer

Bei einem Computerwurm handelt es sich um eine Malware, die sich selbstständig reproduziert und sich über Netzwerkverbindungen verbreitet. Der Computerwurm infiziert dabei normalerweise keine Computerdateien, sondern einen anderen Computer im Netzwerk. Dies geschieht, in dem sich der Wurm repliziert. Diese Fähigkeit gibt der Wurm seinem Replikat weiter, wodurch auch dieser auf die gleiche Art und Weise andere Systeme infizieren kann.

An der Stelle zeigt sich auch der Unterschied zwischen Computerwürmern und -viren. Computerwürmer sind eigenständige Programme, die sich selbst replizieren und im Hintergrund laufen, während Viren eine Host-Datei benötigen, die sie infizieren können. Aus diesem Grund kommt es häufig vor, dass ein Computerwurm erst bemerkt wird, wenn das Programm Systemressourcen verbraucht, wodurch andere Aufgaben verlangsamt oder angehalten werden.

2.4.2.4 Spyware/Adware

Bei Spyware handelt es sich um eine Software, die ohne Wissen des Anwenders Aktivitäten auf dem Rechner oder im Internet ausspioniert und aufzeichnet. Dabei werden Informationen weitergeleitet und durch verschiedene Methoden die Daten gesichert. Häufig wird hierbei das Keylogging verwendet um Benutzernamen, Passwörter und Bankdaten herauszufinden. Aufzeichnungen von Audio- und Videodaten sind ebenso wie das Erfassen von Inhalten aus E-Mail-, Messaging- und sozialen Apps keine Seltenheit. Jede Tätigkeit, die auf dem Rechner ausgeführt wird, ist nachvollziehbar. Spyware kann nicht nur gefährlich sondern auch aufdringlich werden. Adware installiert sich selbst ebenso heimlich auf dem Rechner und spioniert den Browserverlauf aus um mit passenden Anzeigen den User zu belästigen. Auch in der Gaming-Szene spielt Spyware eine immer größer einhergehende Rolle. Viele Programmierer lassen in der Installationkonsole eine Red-Shell-Spyware mitinstallieren mit der die Online-Aktivität des Spielers verfolgt werden soll, um in Zukunft bessere Spiele zu veröffentlichen, die angepasster an den Verbraucher sind. Der Verbraucher wurde weder in Kenntnis davon gesetzt, noch hat dieser der Installation zugestimmt. Es handelt sich also demnach um

Spyware.

2.4.2.5 Scareware

Scareware ist eine Art von Malware, die einen Virus oder ein anderes Problem auf einem Gerät zu erkennen vorgibt. Die Benutzer sollen zur Behebung des Problems schädliche Software downloaden oder kaufen. Üblicherweise ist Scareware die Vorstufe für einen Cyberangriff und nicht ein Angriff an sich.

Scareware-Angriffe beginnen häufig mit einer Pop-up-Werbung, die den Eindruck erweckt, sie stamme von einer Sicherheitssoftware oder vom Betriebssystem des Rechners. Klicken die Benutzer darauf, werden sie auf eine infizierte Webseite geleitet. Auf dieser sollen Sie weitere Anweisungen zur Behebung ihres angeblichen Problems erhalten. Das umfasst beispielsweise die Installation eines neuen Tools oder Programms, einen Scan des Rechners, die Eingabe von Anmeldedaten, um mehr Informationen zu erhalten, oder das Hochladen von Kreditkartendaten für den Wiederherstellungsprozess. Häufig führt das dazu, dass Benutzer unwissentlich schädliche Programme wie bereits erwähnte Malware-Arten auf das Gerät herunterladen.

Scareware-Angriffe können auch über E-Mail erfolgen. Bei dieser Angriffsart verschicken die Angreifer E-Mails mit hoher Priorität oder Dringlichkeit, die Benutzer zum sofortigen Handeln auffordern. Die Links in der E-Mail täuschen den Benutzern vor, mit ihnen würden die Bedrohung behoben oder das System gescannt. Ein Klick darauf führt zum Download und zur Installation von infizierten Dateien, schädlichem Code oder Schadprogrammen.

Ebenso wie viele andere Arten von Malware sind Scareware-Angriffe sehr problematisch, weil die Betrüger Zugang zu den Konto- oder Kreditkartendaten der Benutzer erlangen können, was Identitätsdiebstahl oder andere Betrugsarten ermöglicht.

2.4.2.6 Ransomware

Ransomware ist eine Art von Schadsoftware. "ransom " bedeutet übersetzt Lösegeld, was schon eine Aussage über die Funktionalität der Malware trifft. Beispielsweise spricht man von Ransomware, wenn der Schadcode darauf programmiert ist, Daten eines vermeintlichen Opfers so zu codieren, dass diese nicht wieder hergestellt werden können. Somit hat der Angreifer ein großes Druckmittel in der Hand mit dem das Opfer zur Zahlung von Lösegeld aufgefordert werden kann. Bemerkbar macht sich Ransomware durch Erpresserbriefe oder einen blockierten Bildschirm, welcher erst wieder freigegeben wird, wenn die eingeforderte Summe gezahlt wird. So können mitunter große Unternehmen zu sehr hohen Zahlungen aufgefordert werden, da hier eine Codierung der Daten sehr schädigend für das Unternehmen werden kann. Die Zahlung garantiert jedoch nicht, dass der Computer und die Daten wieder freigegeben werden. Als Schutz vor Datenverlust gelten regelmäßige Backups der Daten und Updates der Sicherheitssysteme.

2.4.2.7 Root kit

Bei einem Rootkit handelt es sich nicht um eine einzelne Malware sondern um eine Sammlung verschiedener Schadprogramme, die sich über eine Sicherheitslücke in einen Computer einnistet und Angreifern den dauerhaften ferngesteuerten Zugriff (Remote-Access) auf diesen erlaubt. Wesentliches Merkmal von Rootkits ist, dass sie sich vor Virenscoannern und Sicherheitslösungen verstecken können, sodass der Benutzer nichts von ihrer Existenz mitbekommt.

Je nachdem, auf welcher Berechtigungsebene sich das Rootkit ausgebreitet hat, kann es dem Angreifer sogar umfassende Administrationsrechte verschaffen (in diesem Fall spricht man von einem Kernel-Mode-Rootkit), wodurch er die uneingeschränkte Kontrolle über den Rechner erhält.

Sie bestanden anfangs zumeist aus modifizierten Versionen standardmäßiger Programme wie „ps“ (ein Unix command, das eine Liste aller aktiven Prozesse aufruft) und „passwd“ (zum Ändern des Benutzerpassworts). Daraus ergibt sich die Bezeichnung "rootkit": Mit „Root“ wird bei Unix der Administrator bezeichnet, der Wortteil „kit“ bedeutet so viel wie „Ausrüstung“ oder „Werkzeugkasten“. Der zusammengesetzte Begriff Rootkit umschreibt somit ein Set von Software-Werkzeugen, das einen Angreifer dazu ermächtigt, Root-Rechte über einen Computer zu erlangen (gemeint sind Kernel-Mode-Rootkits).

Inzwischen existieren allerdings für eine Vielzahl von Betriebssystemen Rootkits. Aber auch für Windows- und andere Betriebssysteme ergibt die Bezeichnung „Rootkit“ durchaus Sinn: Denn einige Rootkits dringen bis in den Kernel, also den innersten Kern und damit die „Wurzel“ (Englisch: „root“) des Systems vor und werden von dort aus aktiv.

Die Infiltration eines Systems durch ein Rootkit lässt sich allgemein in folgende Punkte gliedern:

1. Infektion des Systems
2. Tarnung (Stealth)
3. Einrichtung einer Hintertür (Backdoor)

Infektion des Systems

Zunächst wird das Rootkit durch eine Sicherheitslücke oder einen Drive-By Download in den Computer eingnistet. An Passwörter und Zugangsdaten kommen die Angreifer in der Regel durch Beeinflussung oder bewusste Täuschung. Solche Sicherheitslücken sind demnach meist menschlicher Komponente. Je nach Berechtigungsebene, kann das Rootkit verschiedene Ziele verfolgen, die eher recht oberflächlich sind oder aber auch im direkten Kern agieren (Kernel-Mode-Rootkit).

Tarnung (Stealth)

Sobald das Rootkit im System eingedrungen ist, verschleiert es seine Existenz. Dafür beginnt das Rootkit jene Prozesse zu manipulieren, über die Programme und Systemfunktionen Daten untereinander austauschen. Auf die Art erhält das Virenprogramm beispielsweise gefälschte Informationen, aus denen sämtliche Hinweise auf das Rootkit

herausgefiltert wurden.

Einrichtung einer Hintertür (Backdoor)

Die Backdoor wird im folgenden dann als Mittel zum Zweck genutzt, damit der Angreifer mittels Remote-Access, ausgespähtem Passwort oder Shell in das System gelangt. Das Rootkit verschleiert dabei jegliche Hinweise und ermöglicht dadurch weitere Installationen wie beispielsweise Keylogger.

2.4.2.8 Backdoors

Backdoors oder zu deutsch Hintertüren sind alternative Zugangsmethoden zu Software und/oder Hardware. Diese können bewusst vorhanden sein oder durch eine Lücke im Code entstehen. Außerdem kann eine Backdoor durch eine sich auf dem System befindende Malware installiert werden.

Die Nutzung von Backdoors ist unterschiedlich. Absichtlich gelassenen Backdoors werden dazu verwendet um beispielsweise Adminpasswörter zurückzusetzen. Auch für Reparaturzwecke ist eine Backdoor nützlich. Von Hackern wird eine Backdoor hingegen häufig zum Datenklau oder für die Installation weiterer Malware verwendet.

Die Backdoor gelingt meist über einen Trojaner 2.4.2.2 in das System.

2.5 Malware-Analyse

Malware kann sowohl statisch als auch dynamisch analysiert werden.

2.5.1 Statische Analyse

Bei der statischen Analyse wird das *Sample* der Malware analysiert ohne es auszuführen. Oft ist das auch der erste Schritt bei der Analyse um eine Vorstellung darüber zu haben wie sich die Schadsoftware verhalten könnte. Es gibt hierfür verschiedene Tools und Vorgehensweisen.

Für diese Art der Analyse werden beispielsweise Antivirus-Programme verwendet. Diese können in der Regel bestätigen ob es sich bei dem vorliegenden Programm um Malware handelt. Um aussagekräftige Ergebnisse zu bekommen müssen hier mehrere Antivirus-Programme benutzt werden. Virusscanner können eine Aussage über die Malware treffen indem sie den "Fingerabdruck" der Datei mit den Fingerabdrücken in ihrer Datenbank vergleichen. Ein solcher "Fingerabdruck" ist einzigartig für jedes Programm. Er lässt sich in einem Hashwert abbilden. Um einen Hashwert zu ermitteln stehen verschiedene Hashfunktionen zur Verfügung. Darunter zählen beispielsweise der "Message-Digest-Algorithm 5"(MD5) oder der "Secure Hash Algorithm" (SHA) in verschiedenen Ausführungen. Das Problem an Hashfunktionen ist, dass je nach Inhalt der zu verschlüsselnden Datei ein neuer Wert ermittelt wird. Das heißt, wenn der Programmierer des Schadcodes einen Part des Codes abändert, ist der Hashwert ein anderer. So hat sich an der Malware nichts verändert außer der Hashwert. Dadurch kann es vorkommen, dass Virens Scanner Malware aufgrund minimaler Änderungen nicht mehr erkennen können. Somit erkennt die Antivirusprüfung Malware nicht mit völliger Sicherheit. Um Antivirus-Programme zu täuschen verwenden Hacker beispielsweise *msfvenom*. Dieses Tool hilft bei der Verschlüsselung von Code. So kann die selbe Malware einen anderen Hashwert haben. Unter Umständen ist dieser auch nicht in den Datenbanken der Virens Scanner enthalten, wodurch die schädliche Software unentdeckt bleiben kann.

Um in der Analyse weiter voranzukommen und herauszufinden wie sich die Malware verhält gibt die Methode Strings aus dem Code zu lesen und zu deuten. Strings sind in der IT Zeichenketten. Diese sind in bestimmten Fällen im Code von ausführbaren Dateien, beispielsweise als *URLs*, enthalten. Sie können Auskunft über die Funktionsweise der Malware geben und sind somit ein wichtiger Faktor in der Analyse dieser. Um Strings aus Dateien auslesen zu können müssen die entsprechenden Tools installiert sein. Anhand der Menge der gefundenen Strings kann vermutet werden ob ein Programm verschachtelt oder verpackt wurde. Das ist eine Methode die Hacker verwenden um in einer Antivirus-Prüfung nicht aufzufallen. Womit das Programm verpackt wurde kann unter Linux anhand der Software "Detect-It-Easy"] aufgedeckt werden. Solche Programme geben die Art des sogenannten "Packers" aus. So kann die Malware wieder entpackt werden um mehr Strings finden und auszuwerten zu können.

Zur grundlegenden statischen Analyse von Malware gehört auch zu überprüfen ob verlinkte Bibliotheken oder Funktionen vorliegen. Diese Verbindungen zu verschiedenen Bibliotheken können sowohl statisch als auch dynamisch sein. Statisch bedeutet hierbei, dass der gesamte Code der Bibliothek in den Quelltext kopiert wird. Diese Methode wird jedoch selten verwendet. Öfter kommt die dynamische Verlinkung zu Bibliotheken zum Einsatz. Der Begriff "dynamisch " kommt daher, dass die Verbindung erst im laufenden Prozess hergestellt wird. Diese Verlinkungen können weitere Aussagen darüber treffen, wie sich die Malware im laufenden Zustand verhält.

2.5.2 Dynamische Analyse

Die dynamische Analyse von Malware ist die Untersuchung des Schadprogrammes während es ausgeführt wird. Hierbei wird das Verhalten der Malware während der *Laufzeit* beobachtet und analysiert. Außerdem ist die Analyse des Systems nach der Laufzeit ein Teil dieser Methode. Das ist nützlich um den Schadcode einer groben Art von Malware zuzuordnen. Wichtig hierbei ist vorallem die Umgebung auf der das Schadprogramm ausgeführt wird. Es ist wichtig eine Art *forensisches Labor* zu erstellen in der kein Schaden für das Produktionssystem entstehen kann.

Um eine Untersuchung durchzuführen muss das Programm erstmal ausgeführt werden. Wenn die ausführbare Datei nicht im Format ".exe" vorliegt werden hierfür, je nach Betriebssystem, weitere Tools benötigt. Wenn

3 Methodik

3.1 Terraform

Für diese Arbeit wird Terraform als Konfigurationstool für die erstellten Server verwendet. Um eine sichere virtuelle Umgebung zu schaffen werden zwei Server benötigt. Ein Server bearbeitet DNS-Anfragen und der andere Server ist mit Malwareanalyse-Tools ausgestattet. Zudem sind keine Verbindungen zugelassen, außer Port 22. Dieser ist der SSH-Port und bietet hier die Möglichkeit den Server von außen zu beobachten. Ansonsten besteht die Möglichkeit für den Analyseserver, dass er sich mit dem DNS Server verbindet. Das ist daher nötig, da Malware teilweise nur mit Internetverbindung funktioniert. Diese wird über die Verbindung zum DNS Server hergestellt.

Für die Umsetzung dieses Konzeptes bedarf es Terraformdateien, welche die entsprechenden Serverkonfigurationen und Abhängigkeiten festlegen.

- configs zeigen und einzelne befehle erklären: warum mache ich was

3.2 Virtuelle Umgebung

- was habe ich wo und wie gemacht

- mit screenshots dokumentieren und untermauern an passenden stellen

3.3 Tools

- ltrace
- Ghidra
- reverse engineering Tool
- binary analysis cookbook page 202
- flare-fakenet-ng
- Dynamisches Netzwerkanalysetool für die Kommandozeile
- EDB Debugger
- binary analysis cookbook

3.4 Malware

- kurze Erklärung, dass ich Malware hab

4 Ergebnisse

5 Bewertung des Ergebnisses

5.1 Vorteile der Vorgehensweise

5.2 Nachteile der Vorgehensweise

6 Diskurs

6.1 Schlussbetrachtung

6.2 Ausblick

- wiki wird in Zukunft über die VM mit tools etc erstellt

7 Literatur- und Quellenverzeichnis

Literatur

Brikman, Yevgeniy (2019). *Terraform: Up Running: Writing Infrastructure as Code*. Ö'Reilly Media, Inc."

HashiCorp (2022). *Providers*. URL: <https://registry.terraform.io/browse/providers> (besucht am 07.09.2022).

Wang, Kevin (14. Apr. 2022). *What is Terraform?* URL: <https://www.terraform.io/intro> (besucht am 07.09.2022).

aufteilen in internetquellen publications books

8 Anhang

A Anhang A

Eidesstattliche Erklärung

Hiermit versichere ich, die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie die Zitate deutlich kenntlich gemacht zu haben.

Ich erkläre weiterhin, dass die vorliegende Arbeit in gleicher oder ähnlicher Form noch nicht im Rahmen eines anderen Prüfungsverfahrens eingereicht wurde.

Berlin, den 22. September 2022

Patrick Lucas Büdke