HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Cedric Busacker

Eine Analyse: Die Technologien und Methoden moderner Botnetze

Mittweida, 2023

Fakultät CB

BACHELORARBEIT

Eine Analyse: Die Technologien und Methoden moderner Botnetze

Autor:
Herr

Cedric Busacker

Studiengang:
angewandte Informatik

Seminargruppe:
IF19WI2-B

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

Zweitprüfer:
Philipp Engler

Einreichung:
17.07.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty CB

BACHELORTHESIS

An Analysis: The Technologies and Methods of Modern Botnets

author:
Mr.

Cedric Busacker

course of studies:
IT-Security

seminar group:
IF19WI2-B

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

second examiner:
Philipp Engler

submission:
17.07.2023

defence/ evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Busacker, Cedric:
Eine Analyse: Die Technologien und Methoden moderner Botnetze - 2023. – 5, 53, 8 S.
Mittweida, Hochschule Mittweida, Fakultät CB, Bachelorarbeit, 2023

Referat:

In der heutigen digitalen Welt stellen Botnetze eine große Bedrohung für die Informationssicherheit dar. In dieser Bachelorarbeit werden die Funktionsweise moderner Botnetze untersucht. Dabei werden die wichtigsten Technologien und Methoden, die bei der Entwicklung und dem Betrieb von Botnetzen verwendet werden, näher betrachtet. Die Arbeit legt besonderes Augenmerk auf die Herausforderungen, die bei der Bekämpfung von Botnetzen bestehen, und untersucht die Auswirkungen von Botnetzen auf die Informationssicherheit. Das Ziel dieser Arbeit ist es, ein tieferes Verständnis der Funktionsweise moderner Botnetze zu entwickeln, um eine effektivere Verteidigung gegen solche Angriffe zu ermöglichen.

Inhalt

Abbildungsverzeichnis

Abkürzungsverzeichnis

APT	Advanced Persistent Threat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring your own Device
C&C	Command and Control
CC	Cyberkrime
CNN	Convolutional neural network
CPU	Central Processing Unit
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DGM	Domain Generation Algorithm
DNS	Domain Name System
GPU	Graphics Processing Unit
HIDS	Hostbasierte Intrusion Detection Systems
HTTP	Hypertext Transfer Protocol
IDA	Intrusion Detection Agents
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IoT	Internet of Things
IPC	Inter Process Communication
IPS	Intrusion Prevention System
IRC	Internet Relay Chat
ISMS	Informationssicherheits-Management-System
IT	Informationstechnologie
KI	Künstliche Intelligenz
MitM	Man in the Middle

ML	Maschinelles Lernen
NIDS	Netzwerkbasierte Intrusion Detection Systems
NN	Neuronale Netze
RAM	Random Access Memory
RNN	Recurrent neural network
SDE	Signature Detection Engine
StGB	Strafgesetzbuch
TCP	Transport Control Protocol
TTL	Time to Live

1 Einführung

Im Umfeld der Digitalisierung nimmt der Bereich der Informationstechnologie (IT) sowohl im Privaten wie auch in Organisationen einen immer größeren Stellenwert ein. Für den Betrieb von IT kommen Softwarelösungen zum Einsatz, die in der Regel durch eine hohe Fehlerdichte gekennzeichnet sind. So lassen sich in einem durchschnittlichen Betriebssystem rund 3.000 Fehler feststellen und die Tendenz ist steigend. Softwarefehler oder auch „Bugs“ sind nicht nur die Ursache für Abstürze von IT-Systemen oder fehlerhafte Ausführung von Programmen, sie stellen auch Sicherheitslücken dar, durch die potenzielle Angreifer sich Zugang zu IT-Systemen verschaffen und dort Schäden hervorrufen können (Fritzsche; Rust; in: Schulz 2017, S. 310-311; Pohlmann 2022, S. 6f).

1.1 Hintergrund und Bedeutung des Themas

Angreifer von IT-Systemen handeln aus unterschiedlichen Motiven, sie können kriminell, wirtschaftlich oder politisch ausgerichtet sein und ihr Ziel ist es, in fremde Systeme einzudringen und dort Schadsoftware zu installieren. Eine Form von Schadsoftware oder auch Malware stellt das Botnetz dar, das sich dadurch auszeichnet, dass vielfache Ausführungen der gleichen Malware auf diversen, fremden Rechnern installiert und dann vom Angreifer, dem „Bot Herder“ oder Botmaster, remote gesteuert werden. Den Eigentümern der fremden Rechner ist zunächst nicht bekannt, dass sie mit Malware infiziert sind, da die Anwendungen im Hintergrund ausgeführt werden. Die einzelnen Bots, als Teile des Netzwerks, kommunizieren miteinander und können dadurch koordinierte Aktivitäten ausführen. Jeder Bot besitzt auf der technologischen Ebene eine Steuerschnittstelle und ist einer höheren Ebene, dem Mothership, untergeordnet. Botnetze sind keine neue Angriffsform, die ersten Attacken fanden bereits im Jahr 1993 im Internet Relay Chat (IRC) Kommunikationssystem statt. Botnetze werden jedoch nicht ausschließlich für Cyberattacken eingesetzt, es gibt auch gutartige Formen, wie etwa die Webcrawler einer Suchmaschine, die kooperativ agieren und lediglich Informationen für eine Datenbank sammeln (Hattendorf, in: Carle; Schmitt 2009, S. 7).

Sind Botnetze allerdings darauf ausgerichtet, den besetzten Systemen zu schaden, gibt es eine Reihe von Angriffsszenarien. Bekannte Phänomene sind DDOS-Attacken, die den Zugriff auf fremde Server durch Überlastung blockieren; in großen Mengen verschickte SPAM-E-Mails oder Datendiebstahl. Je größer die Anzahl der besetzten Systeme ist, desto wirkungsvoller kann der Botmaster mit seinem Malicious Remote Control Network agieren. Wie in Abb. 1 dargestellt, steuert der Botmaster das Netzwerk von einem zentralen „Command & Control“ Rechner aus und kann auf den infizierten Rechnern über die Bots Befehle ausführen lassen. Während in den ersten Jahren hauptsächlich das ICR-

Kommunikationsprotokoll für die Kommunikation im Botnetz eingesetzt wurde, kommt inzwischen auch das HTTP-Protokoll zum Einsatz. Dabei besitzen die Bots keine dauernde Verbindung zum Botmaster, sondern verbinden sich in Abständen mit diesem und rufen neue Anweisungen ab. Ebenso gibt es Angreifer, die eigene Protokolle entwickeln (Holz 2009a, S. 103).

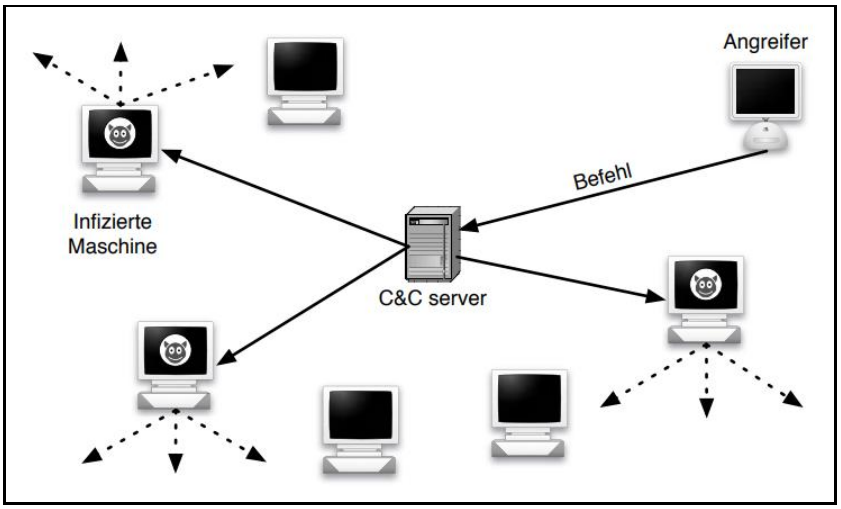

Abb. 1 – Botnetz mit zentralem Server

(Holz 2009a, S. 103)

1.2 Zielsetzung der Arbeit

Als besonders kritisch erweisen sich die Auswirkungen von Botnetz-Angriffen, die auf Unternehmen oder die öffentliche Hand ausgeübt werden, da die Potenziale zur Verursachung schwerwiegender Schäden hier besonders hoch sind. Die vorliegende Untersuchung befasst sich daher mit Botnetz-Attacken, die sich gegen Unternehmen oder den öffentlichen Sektor richten. Es soll eine Analyse der bisher bekannten Technologien und Abwehrmaßnahmen durchgeführt werden. Die Zielsetzung ist es, den aktuellen Entwicklungsstand aufzuzeigen sowie die relevanten Möglichkeiten zur Aufspürung und Entfernung sowie frühzeitigen Abwehr von Botnetzen aufzuzeigen. Als Ergebnis der Analyse sollen die Chancen und Herausforderungen einer frühzeitige Abwehr gegenüber Botnetzen für Unternehmen und öffentliche Einrichtungen ausgearbeitet werden. Es sollen dadurch Empfehlungen zusammengestellt werden, die Unternehmen und öffentlichen Einrichtungen dazu dienen können, eine Sicherheitsstrategie gegenüber Botnetz-Attacken zu entwickeln und sich auf dieser Basis wirkungsvoll dagegen zu schützen.

1.3 Forschungsfragen

Die folgenden Forschungsfragen sollen aus den Ergebnissen der Arbeit beantwortet werden:

1. Wie können Unternehmen und öffentliche Verwaltungsstellen ihre IT-Systeme wirksam gegenüber Botnetz-Attacken schützen?
2. Welche Chancen ergeben sich dadurch für sie?
3. Welche Herausforderungen sind damit verbunden und wie können sie überwunden werden?
4. Welche Empfehlungen können Unternehmen und öffentlichen Stellen gegeben werden, um eine entsprechende Sicherheitsstrategie umzusetzen?

1.4 Methodik

Um zu den angestrebten Ergebnissen zu gelangen, wird eine umfassende Literaturrecherche durchgeführt. Dafür werden zunächst anhand von Stichworten wissenschaftliche Veröffentlichungen in Bibliothekskatalogen und Aufsätze in Journals auf einschlägigen Internet-Plattformen aufgefunden. Anhand der Literaturverzeichnisse werden dann weitere wissenschaftlich fundierte Beiträge gesammelt. Aufgrund der Aktualität des Themas werden außerdem Informationen aus anderen Quellen einbezogen, die sich beispielsweise über das Internet generieren lassen. Dazu gehören Statistiken, Erhebungen, Umfragen, historische Informationen, Rechtsquellen, Grafiken, Angaben auf Unternehmenswebseiten, Standards, Normen, Richtlinien und andere relevante Veröffentlichungen.

1.5 Aufbau der Arbeit

Die Untersuchung gliedert sich in sieben Abschnitte, wobei dieser erste Abschnitt das Forschungsdesign aufzeigt. Im zweiten Abschnitt geht es um die Grundlagen und Definitionen, die für die Darstellung der Thematik von Bedeutung sind. Der dritte Abschnitt stellt detailliert dar, wie Botnetze kommunizieren, agieren und sich vor Erkennung seitens des besetzten Rechners schützen. Im vierten Abschnitt soll dargestellt werden, wie Botnetze wirkungsvoll bekämpft und abgewehrt werden können. In Abschnitt fünf werden die Auswirkungen von Botnetz-Attacken sowie die zukünftigen Optionen in diesem Umfeld betrachtet. Abschnitt sechs zeigt anhand von ausgewählten Fallbeispielen auf, wie sich die Entwicklungen in der Praxis darstellen und welche Empfehlungen an Unternehmen und Behörden gegeben werden können. In Abschnitt sieben werden die Ergebnisse zusammengefasst, einer kritischen Reflexion unterzogen und zur Beantwortung der Forschungsfragen eingesetzt. Die Untersuchung schließt mit einem Ausblick auf künftige Forschungsthemen.

2 Grundlagen und Definitionen

Im Rahmen der Analyse sollen verschiedene Formen und Methoden des Einsatzes von Botnetzen vorgestellt werden, von denen das grundlegende Modell auf der Basis von HTTPS kommuniziert. Daneben sind auch Botnetze auf der Basis von Peer-to-Peer-Kommunikation zu finden, die über keinen zentralen Kontrollserver verfügen. Außerdem werden Fast-Flux-Servicenetzwerke gebildet, die die besetzten Rechner zur Erstellung eines Proxy-Netzwerkes nutzen, über das eine Hosting-Infrastruktur zur Verfügung steht (Holz 2009, S. 4-6). Die verschiedenen Ansätze und deren Eigenschaften sollen im Folgenden näher betrachtet werden.

2.1 Definition von Botnets und besondere Begriffe

Grundsätzlich wird unter der Bezeichnung „Bot“ eine Softwarelösung verstanden, die über eine Fernsteuerung auf einem Computersystem arbeitet. Mit dem Begriff der „Botnetze“ sind miteinander verbundene Bots gemeint, die auf fremden Rechnern installiert werden, um diese zu kompromittieren (Maier; Korolov 2022, o. S.). „Malware“ wird als Oberbegriff für Schadsoftware verwendet, zu denen Viren, Würmer, Trojaner und ähnliche Formen von Applikationen zählen, die verbreitet werden, um auf den angegriffenen Rechnern schädliche Transaktionen auszuführen. Bei der Malware zum Aufbau eines Botnetzes handelt es sich um Software, die sich ohne das Wissen und die Zustimmung des Eigentümers auf Rechnern installiert, um ferngesteuerte Befehle auszuführen (Pohlmann, 2022, S. 7).

Die meisten der heutigen Cyberattacken werden in der Regel systematisch geplant und in aufeinander folgenden Schritten vollzogen, die eine sogenannte „Kill Chain“ bilden (siehe Abb. 2). Sie beginnen mit dem Ausspähen (Reconnaissance), worauf die Auswahl der Waffen folgt (Weaponization), an welche sich der Übergriff anschließt. Sind die Angreifer in das System eingedrungen, beginnen sie, dessen Schwächen zu ermitteln und für sich auszunutzen (Exploitation). Sie verschaffen sich Zugriffsrechte, um sich dann dauerhaft einzunisten (Installation), die Kontrolle zu übernehmen (Command & Control) und das System für ihre Zwecke zu nutzen (Execute) (Fritzsche; Rust; in: Schulz 2017, S. 304-305).

Es gibt verschiedene Akteure, die als Urheber von Angriffen identifiziert werden, sie werden umgangssprachlich als „Hacker“ bezeichnet. So probieren sich etwa die „Skript Kiddies“ nur als Laien aus und agieren von Neugier getrieben, wenn sie Hacker-Tools nutzen, die im Internet frei verfügbar sind. Professionelle Hacker planen ihre Angriffe gezielt und verfügen in der Regel über umfassendes Knowhow sowie eine hochwertige

technologische Ausstattung. Sie setzen ganze Geschäftsmodelle im Umfeld der Cyberkriminalität auf und greifen zu Werkzeugkästen (Exploit Kits), die für kriminelle Attacken im Darknet verfügbar sind. Politisch und wirtschaftlich motivierende Spione gehen am weitesten, denn sie scheuen weder Zeit noch Mittel, um sich wichtige Informationen zu verschaffen, sodass sie nur schwer abgewehrt werden können. Nicht zu vernachlässigen sind außerdem Insider, die Angriffe innerhalb der zu kompromittierenden Organisationen unterstützen, indem sie von innen heraus die „Tore öffnen“, weil sie über die nötigen Berechtigungen verfügen (Fritzsche; Rust; in: Schulz 2017, S. 308-309).

Abb. 2 – Vorgehensweise einer Kill Chain

(Quelle: Fritzsche; Rust; in: Schulz 2017, S. 305)

Die Ziele von groß angelegten Cyberattacken sind Unternehmen und große Organisationen, da sich hier lohnende Beute bietet, sei es in Form von Finanzmitteln oder Reputation. Angreifer, die sensible Bereiche von Organisationen kompromittieren, erlangen eine gewisse Bekanntheit in der kriminellen Szene, die sie auszeichnet. Sie haben unterschiedliche Gesinnungen und ethische Standards, weswegen sie als White-Hat, Grey-Hat oder Black-Hat-Hacker bezeichnet werden – je dunkler, desto skrupelloser (Golem 2023, o. S.).

2.2 Angriffsvektoren und Infektionsmethoden

Als Angriffsvektoren und Infektionsmethoden werden die Wege und Techniken verstanden, mit denen Angriffe auf fremde Computer durchgeführt werden. Die Möglichkeiten, die sich in diesem Bereich bieten, sind vielfältig. Neben der Erzeugung von Botnetzen setzen kriminelle Hacker eine Reihe weiterer Methoden ein, um in Systeme zu gelangen, Informationen auszuspionieren und Geldmittel abzuziehen, mit denen sie ihre Aktivitäten finanzieren. Einige der wesentlichen Angriffsstrategien werden im Folgenden kurz dargestellt:

1. Malware-Webseite und Pishing/ Social Engineering

Die Infiltration eines fremden Rechners mit Malware kann erreicht werden, indem beim Öffnen einer Webseite eine Sicherheitslücke im Browser ausgenutzt wird. Das Öffnen der Webseite wird durch eine Pishing-E-Mail oder Social Engeneering forciert. Dabei werden dem Nutzer vertraute Elemente angezeigt, die ihm vorgaukeln, dass die Webseite bekannt und vertrauenswürdig ist. Tatsächlich erfolgt aber die Öffnung einer infizierten Webseite, wobei sich die Malware automatisch selbst installiert. Pishing-E-Mails sind gefälschte E-Mails, die vorgeben, von vertrauenswürdigen Absendern zu stammen und den Nutzer zur Bekanntgabe seiner Zugangsdaten zu bewegen, die dann gestohlen und für kriminelle Zwecke missbraucht werden. Beim Social Engineering spioniert der Angreifer beispielsweise die sozialen Medien aus und sucht nach Identitäten, die sich manipulieren lassen. Dann nimmt er zu diesen Kontakt auf und verschafft sich durch geschickte Manipulation Zugang zu deren vertraulichen Informationen und finanziellen Mitteln (Fritzsche; Rust; in: Schulz 2017, S. 314-315; Pohlmann 2022, S. 45).

2. Malware in E-Mail-Anhängen

Ähnlich verlaufen Attacken, die Schadsoftware über E-Mail-Anhänge verbreiten, wobei dem Nutzer vertrauenswürdige Absender wie etwa die Hausbank oder ein oft genutzter Online-Shop vorgetäuscht werden. Dies motiviert ihn, den Anhang zu öffnen, der die Malware freisetzt (Fritzsche; Rust; in: Schulz 2017, S. 311; Pohlmann 2022, S. 45-46).

3. Brute-Force-Angriffe

Bei Brute-Force-Angriffen konzentrieren sich kriminelle Hacker darauf, verschlüsselte Informationen zu entschlüsseln, wobei bevorzugt Zugangsdaten, Passwörter, Computerprotokolle, Authentifizierungen, Hash-Funktionen, Webseiten, E-Mail-Accounts, WLAN-Router, Nachrichten oder andere sensible Informationen als Ziel gewählt werden. Es gibt bereits zahlreiche Tools für diese Angriffsarten, wobei die Software anhand von Wörterbüchern und Zeichenfolgen so lange Möglichkeiten ausprobiert, bis die Lösung gefunden ist. Da die Suche automatisiert abläuft, kann sie über Tage, Wochen, Monate oder Jahre fortgesetzt werden, wenn es sich um ein lohnendes Ziel, wie eine Regierungsorganisation oder einen globalen Konzern handelt. Durch die Verbindung von CPU (Central Processing Unit) und GPU (Graphics Processing Unit), das heißt Prozessoren und Grafikprozessoren, kann der Prozess erheblich beschleunigt werden. So lässt sich die Suche nach einem sechsstelligen Passwort, die mit einer leistungsstarken CPU mehr als zwei Jahre dauert, mit GPU auf dreieinhalb Tage reduzieren (Kaspersky 2023, o. S.).

4. Advanced Persistent Threat (APT)

Um Unternehmensnetzwerke zu infiltrieren, kommt die Technik des Advanced Persistent Threat (APT) zur Anwendung. Dabei verschafft sich der Angreifer zunächst über die dargestellten Attacken Zugriff auf das IT-System des Unternehmens. Von dort aus weitet er seinen Angriff aus, indem er sich einen formellen Zugang einrichtet und

Administratorrechte aneignet. Dann kann er sich weitgehend frei im Netzwerk bewegen und in Ruhe dessen Schwachstellen auskundschaften, um einen groß angelegten Angriff vorzubereiten. Dieser gelingt ihm vollumfänglich, da er das System und seine Sicherheitsvorkehrungen bereits kennt. Angriffe dieser Art werden bevorzugt in großen IT-Systemen ausgeführt, wo die Hacker sich über längere Zeiträume unbemerkt verstecken können (Pohlmann 2022, S. 46).

5. **Man in the Middle-Angriffe (MITM)**

Bei einem Man-in-the-Middle-Angriff attackiert der Angreifer einen laufenden Kommunikationsprozess, um die ausgetauschten Daten zu verändern oder zu stehlen. Dadurch kann er Authentifizierungsprozesse umgehen und direkten Zugriff auf sensible Informationen oder das Netzwerk des Opfers erhalten (Fritzsche; Rust; in: Schulz 2017, S. 310; Pohlmann, 2022, S. 46).

6. **Supply-Chain-Angriff**

Ein Angreifer kann sich auch über einen regelmäßig verwendeten Softwaredienst eines Unternehmens Zugriff auf die Systeme verschaffen, indem er ein Softwareupdate manipuliert. Dies kann er tun, wenn er sich unbemerkt Zugang zu einem Hersteller-Update verschafft. Er muss dabei sicherstellen, dass die digitale Signatur der Software nicht beschädigt wird, damit der Empfänger des Updates diese als autorisiert entgegennimmt und ausführt. Hat der Angreifer diese Hürde genommen, kann er einen Angriff auf tausende von Organisationen gleichzeitig umsetzen, die das Softwareupdate aufspielen (Pohlmann 2022, S. 46-47).

7. **DDoS-Angriffe**

DDoS-Angriffe (Distributed Denial of Service) sind Angriffsvektoren, die typischerweise von Botnetzen umgesetzt werden. Dafür werden die Ressourcen des kompromittierten Systems, etwa die Bandbreite, die CPU oder der Arbeitsspeicher, durch eine Vielzahl von Abfragen überbelastet, sodass die von Unternehmen bereitgestellten Dienste für Kunden oder Geschäftspartner nicht mehr zur Verfügung stehen. Dies geschieht, um Konkurrenten auszuschalten oder finanzielle Mittel vom Geschädigten zu erpressen. Sind die Bots einmal platziert, kann der Angreifer schädliche Befehle ausführen lassen und diese noch durch weitere Maßnahmen verstärken. Das Opfer muss das Botnetz identifizieren und sämtliche Bots beseitigen, was eine erhebliche Zeitspanne in Anspruch nehmen kann (Fritzsche; Rust; in: Schulz 2017, S. 309-310; Pohlmann 2022, S. 47).

8. **High-Level-Pishing**

Diese Form des Angriffes kann ein Eindringling vornehmen, indem er sich zunächst Zugriff auf den E-Mail-Account des Geschädigten durch einen Keystroke-Logger verschafft. Keystroke-Logger sind Hard- oder Softwareapplikationen, die sich an die Tastatur eines Gerätes heften und jeden Tastenschlag aufzeichnen, sodass diese vom Angreifer

eingesehen werden können (Lotta 2023, o. S.). Anschließend kann der Angreifer den E-Mail-Verkehr des Angriffsziels verfolgen und Gelegenheiten wahrnehmen, diesen zu manipulieren, um Vorteile daraus zu ziehen. So kann er beispielsweise in den Schriftverkehr bezüglich der Ausgangsrechnungen eines Unternehmens eingreifen und die Finanzströme an seine Bankverbindung umleiten. Da er dafür sorgt, dass ihm genügend Zeit verbleibt, um seine Spuren zu verwischen, entdecken die Opfer solcher Attacken den Schaden meist erst nach Wochen und der Urheber des Pishings kann kaum noch verfolgt werden. Als Variante dieses Angriffsvektors können auch gefälschte Unternehmens-Webseiten erstellt werden, über die der Angreifer anstelle des Unternehmens agieren und hohe Schäden verursachen kann (Fritzsche; Rust; in: Schulz 2017, S. 311; Pohlmann 2022, S. 47-48).

9. Ransom-Attacken

Bei der Umsetzung von Ransom-Attacken durchbrechen kriminelle Angreifer die Sicherheitsbarrieren der Opfer und verschlüsseln deren Daten, die sie erst nach der Auszahlung eines Lösegeldes wieder freigeben. Dies ist im Bereich kritischer Infrastrukturen, wie im medizinischen Bereich, bei Energie- oder Wasserversorgern oder in der Produktion, besonders brisant, da die Opfer sich nicht leisten können, lange auf die Freigabe zu warten und in der Regel bezahlen. Die Informationen zu solchen Attacken werden meist von den Opfern selbst geheim gehalten, um keine Reputationsverluste zu erleiden, dennoch sind diese Formen der Cybererpressung inzwischen weit verbreitet. Hier hängt der Schaden davon ab, ob der Angegriffene über vollständige Backups der Systeme verfügt (Fritzsche; Rust; in: Schulz 2017, S. 307).

Alle dargestellten Angriffsformen können zudem von kriminellen Hackern noch durch KI-Anwendungen ausgefeilt werden. So lässt sich durch Deepfake-Technologien beispielsweise Voice Cloning umsetzen, wobei Angreifer die Stimmen von Führungskräften täuschend echt simulieren, um dann die Mitarbeiter zu Transaktionen zu bewegen, durch die sich der Angreifer bereichert, etwa die Auszahlung von finanziellen Mitteln. Deep Fakes werden ebenso im Bereich der Video-Technik eingesetzt, wo bereits vorhandenes Videomaterial mit neuer Sprache hinterlegt wird. Auf diese Weise können Hacker kreativ werden und alle denkbaren Informationsfälschungen sowie Manipulationen vornehmen, um politische oder wirtschaftliche Szenarien zu kontrollieren. Besonders kritisch ist dabei, dass die Cyberkriminellen in der Regel mit den neusten technologischen Standards arbeiten, wohingegen die attackierten Unternehmen und Behörden sich bei der Umsetzung ihrer Sicherheitsmaßnahmen erst im Frühstadium befinden. Dies wird noch vorangetrieben, wenn Technologieunternehmen wie Microsoft neue Softwarelösungen in diesem Bereich, wie VALL-E und ChatGPT kostenlos und zur freien Verfügung im Internet bereitstellen. Das Fälschen von E-Mails und anderer Kommunikation, die Generierung von Malware sowie die Ausschaltung üblicher Sicherheitsmechanismen wird damit für jedermann ohne großen Aufwand möglich. Zukünftig dürfte sich auch die Fälschung und das Stehlen biometrischer Daten für Kriminelle immer einfacher gestalten. Hier sind Unternehmen gefordert, ihre Technologienutzung und Cybersicherheitssysteme sowie die internen

Kompetenzen nach dem State-of-the-Art auszurichten, um sich nicht durch eigene Nachlässigkeit zu gefährden (Sosafe 2023, S. 5-6). Auch geopolitische Krisen, wie die jüngst grassierende Corona-Pandemie und der im Frühjahr 2022 entfachte Angriffskrieg Russlands auf die Ukraine, die für Unsicherheit in der Bevölkerung sorgen, machen sich Cyberkriminelle zu Nutze. Sie boten dafür etwa während der Corona-Pandemie benötigte Hilfsgüter günstig online an, die gar nicht existierten. Durch groß angelegte Pishing-Mail-Aktionen können sie so sensible Zugangsdaten für den Zahlungsverkehr abfragen und sich damit bereichern. Ebenso werden seit dem Ausbruch des Ukraine-Krieges militärische Einrichtungen verstärkt zum Ziel von Aktivisten, die versuchen, unbemerkt Daten zu stehlen oder Malware zu verbreiten. Die Ereignisse führten in den letzten Jahren zu einer wachsenden Gegenbewegung der Globalisierung: Einer Deglobalisierung, bei der sich besorgte Unternehmen von globalen Engagements zurückziehen und dadurch künstliche Krisen erzeugen. Ausläufer solcher Aktivitäten sind aktuell instabile Lieferketten, steigende Inflation sowie Lebensmittel- und Energiekrisen (Sosafe 2023, S. 12-13).

Wesentliche Akteure im Bereich der Bekämpfung von Cyberkriminalität sind die Mitarbeiter von Organisationen, da sich hier auch unbeabsichtigt Schwachstellen ergeben können. Daher gehört die Schaffung einer „Awareness“ in der Belegschaft zu den grundlegenden Maßnahmen in Bezug auf Cybersicherheit (Sosafe 2023, S. 17).

2.3 Architektur und Struktur von Botnetzen

Es lassen sich eine Reihe unterschiedlicher Architekturen und Topologien unterscheiden, mit denen Botnetze abhängig vom verfolgten Angriffsziel gestaltet werden. Dabei bestimmt die Architektur die erforderlichen, technologischen Komponenten und die Topologie zeigt die Kommunikation und die Formation des Angriffes. Die wesentlichen von ihnen werden nun kurz erläutert.

1. Zentralisierte Architekturen

Bei der Gestaltung eines zentralisierten Botnetzes kompromittiert der Botmaster die Server des Opfers und verbreitet von dort aus die Bots auf den angebundenen Rechnern. Dies kann in einer Stern-Architektur, als Multi-Server-Ansatz oder hierarchisch erfolgen, (siehe Abb. 3; Laass 2011, S. 3-4).

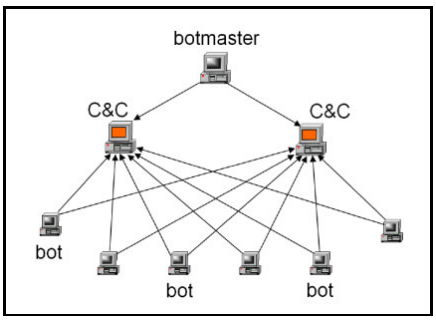

Abb. 3 – Command- & Control-Architektur eines Botnetzes

(Quelle: Dhinnesh/Sundareswaran 2018, S. 422)

Der Angriff erfolgt in mehreren Schritten (Dhinnesh/Sundareswaran 2018, S. 423, siehe Abb. 4):

1. Der Botmaster infiziert ein Opfer mit der Botnet-Malware, wodurch sich ein Bot auf dem System installiert.
2. Wenn das Opfer sich mit dem C&C-Server verbindet, erhält auch der Bot Zugang zum Server.
3. Der Botmaster kann anschließend über den C&C-Server durch den Bot Befehle ausführen lassen, wobei es sich um eine zentrale Steuerung handelt.
4. Der Botmaster infiziert ein weiteres Opfer mit der Malware und die Schritte wiederholen sich so lange, bis er ein ausreichend großes Netzwerk an Bots aufgebaut hat, um seinen Angriff auszuführen.

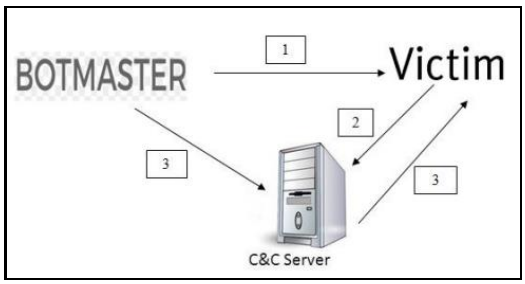

Abb. 4 – Botmaster Setup

(Quelle: Dhinnesh/Sundareswaran 2018, S. 423)

2. Dezentrale Botnetze

Botnetze mit zentraler Steuerung haben einen Single Point of Failure, das heißt, einen zentralen Server, wird dieser eliminiert, funktioniert das gesamte Netz nicht mehr. Um diese Schwäche zu beheben, werden fortgeschrittene Entwicklungen dezentral betrieben. Hier sind im Wesentlichen zwei Formen zu unterscheiden, Peer-to-Peer und Fast-Flux Botnetze, die im Folgenden kurz dargestellt werden.

a. Peer-to-Peer Botnetze

Peer-to-Peer Botnetze verwenden für die Kommunikation Peer-to-Peer-basierte Kommunikationsprotokolle, wobei alle Knoten gleichberechtigt sind. Das heißt, jeder infizierte Rechner ist ein Peer und kann Nachrichten weiterleiten sowie als Client und Server fungieren. Wenn ein Knoten ausfällt, kann er unmittelbar durch einen anderen ersetzt werden. Daher sind Peer-to-Peer Botnetze robust aufgestellt und es bereitet größeren Aufwand, sie einzudämmen (Laass 2011, S. 8).

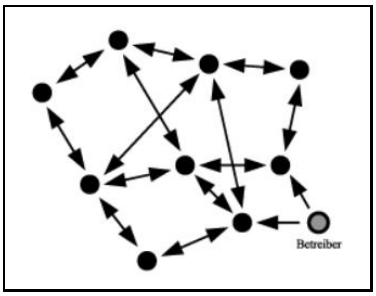

Abb. 5 – Peer-to-Peer Botnetz

(Quelle: Laass 2011, S. 8)

b. Fast-Flux-Service Botnetze

Bei Fast-Flux-Service Botnetzen zielen die Betreiber darauf ab, die Domain zu verschleiern, auf der sie ihre Malware oder Pishing-Webseiten hosten. Damit ihre Webseiten nicht erkannt werden, nutzen sie DNS (Domain Name System) Fast-Fluxing Technologien, wobei eine Vielzahl von IP-Adressen mit einer Domain verbunden sind, die außerdem ständig ausgetauscht werden. Daher lassen sich die IP-Adressen der Domain nicht ermitteln und somit auch nicht blockieren. Dafür setzen die Angreifer eine Form des Load Balancing ein, die als Round Robin DNS bezeichnet wird, und jeder IP-Adresse wird nur eine kurze Lebensdauer, Time to Live (TTL), eingeräumt. Zudem nutzen sie kompromittierte Host als Proxys, um anonym zu bleiben. Um das Botnetz auszuschalten, müsste die Domain eliminiert werden, was ein zeitaufwändiger Prozess ist, der von den Betreibern nicht unbedingt unterstützt wird. Eine andere Art, das Botnetz zu deaktivieren wäre, das Mutterschiff vom Internet zu trennen und auch das lässt sich nicht ohne weiteres umsetzen, weil dahingehende Beschwerden meist unbeantwortet bleiben (Nazario; Holz 2008, S. 24; Silva et al. 2013, S. 394).

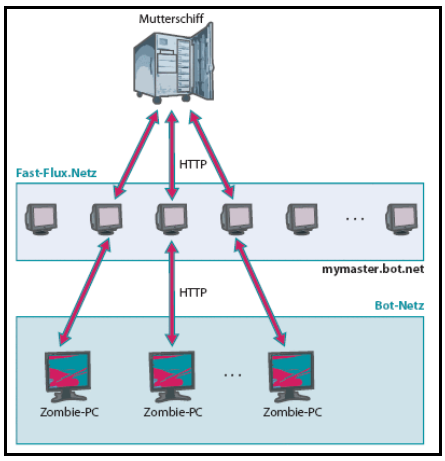

Abb. 6 – DNS Fast Flux Botnetze

(Quelle: Schmidt 2007, S. 2)

2.4 Botnetz-Topologien und ihre Funktionen

Die Topologien von Botnets bestimmen deren Kommunikations- und Angriffsmöglichkeiten wie folgt:

1. **X:1-Topologie (X-Angreifer / ein Opfer)**

Bei einer X:1-Topologie verteilt der Angreifer seine Bots auf einer Vielzahl von Rechnern, die dann als „Zombies“ bezeichnet werden. Er steuert die Bots von einer zentralen Position aus und lässt diese den geplanten Angriff ausführen (siehe Abb. 7).

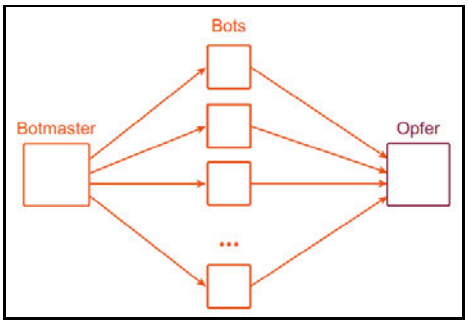

Abb. 7 – X:1-Topologie

(Quelle: Pohlmann 2022, S. 311)

Typische Angriffe, die mit dieser Topologie ausgeführt werden, sind DDoS-Attacken, bei denen die Angreifer die Systeme des Opfers durch Erschöpfung seiner IT-Ressourcen, wie CPU, RAM (Random Access Memory) oder Transmission Bandwith (Übertragungsbandbreite), blockieren (siehe Abb. 4; Pohlmann 2022, S. 311-312).

2. X:Y-Topologie – (X Angreifer / Y Opfer)

Eine weitere Topologie ist die Konstellation von beliebig vielen Angreifern und ebenso beliebig vielen Opfern, bei der ein Botmaster die zentrale Steuerung vornimmt (siehe Abb. 8).

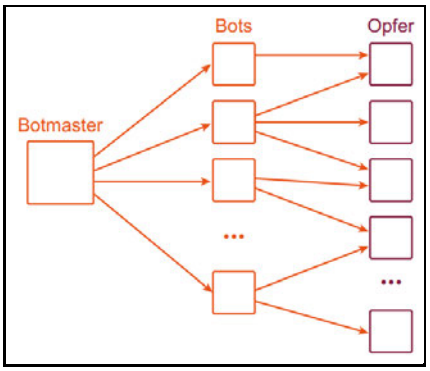

Abb. 8 – X:Y-Topologie

(Quelle: Pohlmann 2022, S. 313)

Mit dieser Topologie können Massenangriffe ausgeführt werden, wenn die Angreifer beispielsweise E-Mail-Spam verbreiten oder Click-Fraud durchführen wollen. Beim Click-Fraud geht es darum, kommerzielle Werbung durch automatisiertes Anklicken zu kompromittieren und die dahinterliegenden Zahlungsdaten zu stehlen (Pohlmann 2022, S. 312-313).

3. 1:Y-Topologie (ein Angreifer / beliebig viele Opfer)

Die Topologie 1:Y lässt sich für das Ausspionieren von Sicherheitslücken nutzen. Dabei eruiert der Angreifer zunächst durch einen Ping-Scan die erreichbaren Systeme eines Ziel Netzwerkes. Dann ermittelt er mit einem Port-Scan, mit welchen Systemen er Verbindung aufnehmen kann, und führt auf den verbundenen Rechnern einen Vulnerabilitätstest durch, der ihm verrät, welche Sicherheitslücken bestehen. Diese Lücken nutzt er dann gezielt für den eigentlichen Angriff, den er zentral steuert (siehe Abb. 9) und bei dem er Ransomware, Keylogger, Trojanische Pferde oder Adware installiert. Trojanische Pferde werden für das Auslesen von gespeicherten Daten auf den Systemen verwendet. Adware dient dazu, dem Nutzer ungewünschte Werbeinhalte anzuzeigen und Daten an die Betreiber des Werbenetzwerkes zu übertragen (Pohlmann 2022, S. 315-316).

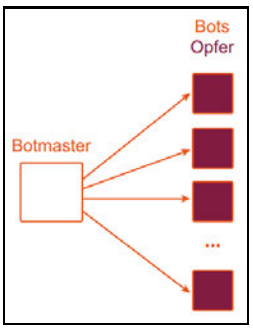

Abb. 9 – 1:Y-Topologie

(Quelle: Pohlmann 2022, S. 315-316)

4. 1:1-Topologie – (ein Angreifer / ein Opfer)

Bei der 1:1-Topologie gibt es einen Angreifer und ein Opfer, wobei der Angreifer sich darauf konzentriert, das System des Opfers vollständig zu kontrollieren (siehe Abb. 10).

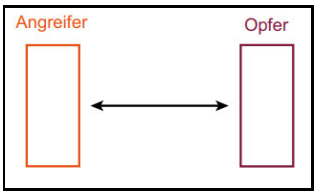

Abb. 10 – 1:1-Topologie

(Quelle: Pohlmann 2022, S. 316-317)

Die Angriffsmethoden in dieser Konstellation sind beispielsweise Advanced Persistent Threat (APT) oder Social Engineering, das durch gezieltes Pishing agiert. Während Pishing grundsätzlich nur dazu dient, eine gewünschten Handlung zu forcieren, richtet sich Spear-Pishing darauf, eine bestimmte Person zu einer gewünschten Handlung zu bewegen. Beim Whaling werden gezielt Führungskräfte oder einflussreiche Personen, die sich in der Öffentlichkeit bewegen, forciert, bestimmte Handlungen durchzuführen (siehe Abb. 11; Lutkevich et al. 2021, o. S.; Seth; Damle; 2022, S. 371 und zum Pishing i. E. siehe Sonowal 2022, S. 25-30).

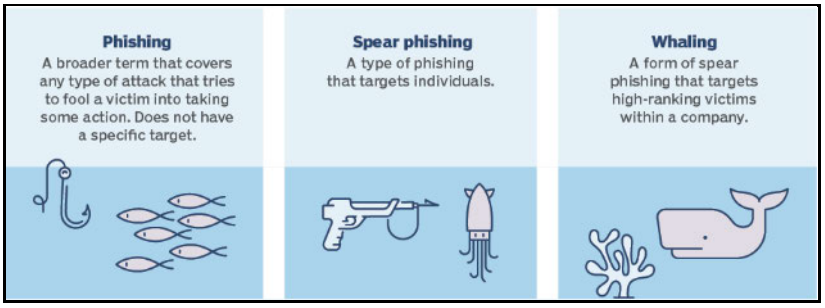

Abb. 11 – Pishing, Spear-Pishing und Whaling

(Quelle: Lutkevich et al. 2021, o. S.)

3 Technologien und Methoden von Botnetzen

In diesem Abschnitt der Untersuchung sollen die Technologien und Methoden, die für den Einsatz von Botnetzen verwendet werden, einer näheren Betrachtung unterzogen werden. Dazu gehören die Kommunikationsprotokolle, die Steuerungselemente, die Verschlüsselung und Tarnung sowie die Infrastruktur und Verbreitung.

3.1 Kommunikationsprotokolle von Botnetzen

Die Kommunikation zwischen den einzelnen Einheiten der Botnetze ist unverzichtbar, da die Steuerung aus Ferne erfolgen muss. Grundsätzlich werden die drei folgenden Steuerungs-Topologien vorgefunden: Zentrale C&C-Steuerung, P2P-Steuerung und hybride Steuerung. Die C&C-Steuerung kann sich auf einem, mehreren oder auf allen infizierten Hosts befinden. Die hybride Steuerung weist eine Proxy-Zwischenschicht auf, die P2P-gesteuert wird und arbeitet auf der ausführenden Ebene mit einer gemischten Steuerung (siehe Abb. 12; Vormayr et al. 2017, S. 2772).

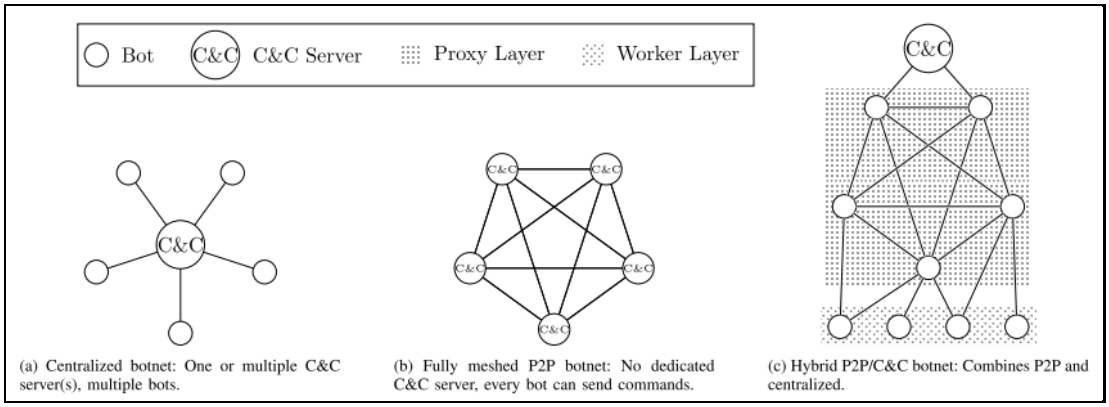

Abb. 12 – Kommunikations-Topologien

(Quelle: Vormayr et al 2017, S. 2772)

3.1.1 Vor- und Nachteile der Topologien

Zunächst sollen die einzelnen Topologien nochmals hinsichtlich ihrer Vor- und Nachteile betrachtet werden.

1. **Kritische Aspekte bei zentralen C&C-Servern**

Bei zentralisierten Topologien besteht eine geringe Latenz und hohe Skalierbarkeit, da die Befehle 1:1 vom C&C-Server an jeden einzelnen Host übertragen werden (siehe Abb. 12,

links). Die Topologie ist einfach in der Umsetzung, aber durch den zentralen Server als einzige Steuerungseinheit leicht aufzulösen. Diesen Nachteil könnte das P2P-Netzwerk ausgleichen, es ist jedoch dahingehend durch Aufdeckung gefährdet, als dass die IP-Adressen der C&C-Server in das Botnetz zu kodieren sind. Werden diese entschlüsselt, kann das Netz ebenfalls leicht aufgedeckt werden. Dazu kommt, dass C&C-Server durch die Beobachtung des Netzverkehrs leicht erkannt werden können. Dieses Problem lässt sich durch einen Domain Generation Algorithm (DGM) beheben, der im Zeitablauf die Domainnamen der C&C-Server fortlaufend wechselt. Erkennt ein Detektor jedoch den Algorithmus, kann das Botnetz einfach übernommen werden, indem ein zukünftiger Domainname reserviert wird. Als Alternative dazu lässt sich das bereits dargestellte Fast-Flux-Netzwerk benennen (Vormayr et al. 2017, S. 2772-2773).

2. Kritische Aspekte bei P2P-Steuerung

Wird eine P2P-Topologie eingesetzt, kann jeder Bot Befehle weiterleiten und als C&C-Server fungieren (siehe Abb. 12, Mitte). Dabei lässt sich eine hohe Robustheit erreichen, da ein vollständig verbundenes Botnetz nicht durch die Zerstörung einzelner Bots in seiner Funktion beeinträchtigt wird. Es wird jedoch eine große Zahl an Netzwerkverbindungen benötigt, und da die Zahl der TCP-Sockets (Transport Control Protocol) eines Betriebssystems begrenzt wird, ist ein solches Netzwerk nicht skalierbar. Das TCP ist das Transportprotokoll für die Datenströme, das zum Informationsaustausch zwischen den Bots benötigt wird. Durch die zahlreichen Netzwerkverbindungen kann das Botnetz leichter entdeckt werden und das erforderliche Einfügen neuer sowie das Entfernen vorhandener Bots führt zu umfassenden Nachrichtenverkehr. Daher ist die vollständige Verbindung aller Bots in P2P-Netzwerke in der Regel nicht realisierbar. Das macht es wiederum schwierig, Implementierungen in einem P2P-Netzwerk vorzunehmen, denn es müssen stets die ersten Peers aufgefunden und dann zuverlässige Befehlsketten erstellt werden, um alle Bots zu erreichen. Um das Auffinden der anfänglichen Peers zu erleichtern, werden bekannte Peers als Liste in die ausführbare Bot-Datei codiert oder in Cache-Servern von P2P-Netzwerken gespeichert. Diese Vorgehensweise führt jedoch im Ergebnis dazu, dass wieder ein Single Point of Failure in Form der Peer-Liste entsteht. Die Alternative besteht darin, eine Internetsuche von Peers auf der Basis einer Stichprobe durchzuführen (Vormayr 2017, S. 2773). Wenn Computersysteme nicht über das Internet erreicht werden können, weil sie durch Firewalls oder NAT (Network Address Translation) geschützt werden, arbeiten Botnetze mit Superknoten und NAT-Knoten. Die Superknoten werden für die C&C-Kommunikation und die NAT-Knoten für die Ausführung der Malware eingesetzt (Wang et al. 2010, S. 117-119; Vormayr 2017, S. 2773-2774). Bekannte Botnetze, die mit einer P2P-Topologie arbeiten sind Zeus und Sality. Zeus setzt fest codierte Peer-Listen ein und falls kein Peer verfügbar ist, erfolgt die Umstellung auf eine zentralisierte Topologie. Das Phatbot-Netz agiert über Cache-Server auf einer Filesharing-Plattform, um die Liste der ersten Peers verfügbar zu halten. Sinit und Conficker Botnetze nutzen die zufällige Suche im Internet. Ein Botnetz mit Superknoten und NAT-Knoten ist Zeroacces (Vormayr 2017, S. 2774).

3. Vorteile einer hybriden Steuerung

Bei einem hybriden Steuerungsansatz können die positiven Aspekte beider Ansätze verbunden werden. Dabei werden mehrere verteilte Netze gebildet, die jeweils über einen C&C-Server zu steuern sind. Werden dann Teile des Netzes eliminiert, können die Aktivitäten immer noch über die übrigen Teile fortgesetzt werden. Diese Vorgehensweise wurde beispielsweise vom Waledac-Botnetz verwendet, welches im Jahr 2008 bekannt wurde und im Jahr 2010 eliminiert werden konnte (Zipperle 2014, S. 19).

Modernere Topologien setzen Proxy-Schichten vor die C&C-Server und in vorderster Front eine Schicht aus Worker-Bots, die die Befehle ausführen (siehe Abb.12, rechts). Es sind auch weitere Schichten möglich, um einen besseren Schutz des Servers zu erreichen, was jedoch zu Lasten der Latenz geht. Eine andere Möglichkeit besteht darin, nach Bedarf partiell zentral gesteuerte Elemente und in anderen Bereichen P2P-Elemente einzusetzen. Auch können die Aufgaben separiert werden, indem die Befehle über P2P ausgetauscht und Daten über eine zentrale Topologie übertragen werden. Letztlich bleibt für die Bereiche mit zentraler Steuerung jedoch immer das Risiko des Single Point of Failure bestehen. Hybride Steuerung wurde bei den späten Versionen des Zeus-Botnetzes und dem Miner-Botnetz genutzt (Vormayr et al. 2017, S. 2774).

3.1.2 Kommunikationsprotokolle

Es können verschiedene Kommunikationsprotokolle genutzt werden, um innerhalb des Netzes Informationen auszutauschen. Die Protokolle können auch für die Abschirmung eines Botnetzes von Bedeutung sein, indem etwa ein regulärer Datenverkehr imitiert wird oder Protokolle wiederverwendet werden. Um den Implementierungsaufwand zu reduzieren, werden bereits erstellte Implementierungen mehrfach genutzt. Neoterische Protokolle werden nach dem jeweiligen Bedarf für ein neues Botnetz geschrieben. Neben den C&C-Protokollen sind außerdem weitere Protokolle zu erstellen, abhängig von den gesetzten Zielen des Netzwerks (Vormayr et al. 2017, S. 2774; Zipperle 2014, S. 19).

1. Internet Relay Chat (IRC)

Bei den frühen Botnetzen wurde meist das Internet Relay Chat Protokoll (IRC) eingesetzt, das für große Chat-Räume im Internet entwickelt wurde. Es wird auch heute noch verwendet, weil es eine zentrale Topologie nutzt, einfach implementiert werden kann, eine geringe Latenz hat und allgemein bekannt ist. Es hat die Nachteile, dass es von üblichen Sicherheitssystemen mit Firewalls leicht abzublocken ist und von Unternehmensnetzwerken häufig gar nicht zugelassen wird. Es funktioniert textbasiert und erlaubt die Kommunikation zwischen Clients und Server. Es können auch ganze Kanäle für Gruppen von Clients genutzt und über Passwörter geschützt werden. Außerdem können Daten sowie Binär- und Konfigurationsdateien und Updates übertragen werden. Eines der ersten Botnetze, das als PrettyPark bekannt wurde, setzte IRC als Kommunikationsprotokoll ein (siehe

Abb. 14; Vormayr et al. 2017, S. 2774; Zipperle 2014, S. 19; Khattak et al. 2014, S. 900-901).

2. Hypertext Transfer Protocol (HTTP)

Ein weiteres Protokollformat stellt HTTP dar, das für das Aufrufen von Webseiten über Browser entwickelt wurde. Daher verfügt es auch nicht über Gruppenfunktionen, sondern umfasst nur die Anfrage an einen und Antwort vom einem Server. Jeder Bot muss sich bei diesem Format mit dem Server verbinden, um seine Befehle abzurufen. HTTP kann relativ einfach implementiert werden, da dafür Open-Source-Lösungen vorhanden sind. HTTP ist grundsätzlich für eine zentrale Topologie vorgesehen, kann aber dann für P2P-Topologien eingesetzt werden, wenn jedem Bot ein Server und ein Client implementiert wird. Dabei besteht jedoch die Problematik, dass Kommunikationsschleifen entstehen können und es ist darauf zu achten, dass tatsächlich jeder Bot eine verteilte Nachricht empfangen kann. Sicherzustellen ist außerdem, dass alle Bots im System aufgefunden werden können. Um diese Probleme zu lösen, muss für die P2P-Anforderungen eine zusätzliche Zwischenschicht sowie eine Routing-Schicht für die direkte Kommunikation mit einem spezifischen Bot eingerichtet werden. Vorteilhaft bei der HTTP-Kommunikation ist es, dass die Strukturen den üblichen Kommunikationsmustern im Internet entsprechen und daher nicht leicht zu erkennen sind. Bekannte P2P-Botnetze mit HTTP-Protokollen sind beispielsweise Blackenergy, Miner und Regin. Auf HTTP basierende Botnetze lassen sich nur schwer abschalten, da hier Internet-Betreiber involviert sind, die nicht unbedingt ein Interesse an einer rechtlichen Intervention oder Kooperation zeigen (siehe Abb. 13 und 14 Mitte; Vormayr et al., 2017, S. 2775; Zipperle 2014, S. 19; Khattak et al. 2014, S. 901).

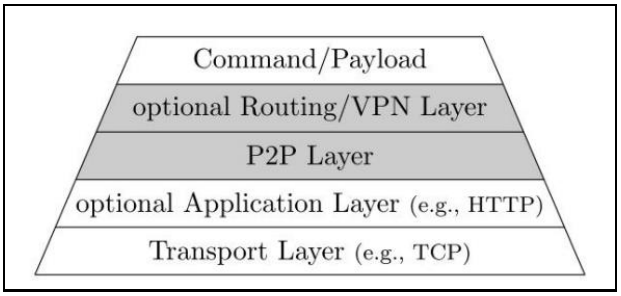

Abb. 13 – Zusätzliche Schichten für P2P und Routing

(Quelle: Vormayr et al., 2017, S. 2775)

3. Server Message Block (SMB)

Ähnlich zum HTTP-Protokoll ist das SMB-Protokoll, das gleichfalls eine Request-Response-Funktion ausführt, also Nachrichten zwischen Client und Server austauscht, wofür eine Authentifizierung erforderlich ist. Anschließend kann der Client entsprechend seiner Berechtigungen verfügbare Dateien und Dienste abrufen und Zugriff auf Drucker erhalten. Über SMB lässt sich außerdem IPC (Inter Process Communication) im

gesamten Netzwerk implementieren, was für den Nachrichtenaustausch oder den Aufruf spezifischer Funktionen von Bedeutung ist. Typisch ist die Infektion anderer Hosts durch ein SMB-Protokoll, indem Dateien weitergeleitet werden, die mit Schadcode versehen sind. Infiziert wird der Host, indem er die Datei öffnet. Sicherheitssysteme können SMB-Protokolle bereits beim Internetzugriff blockieren, die Infektion über lokale Netzwerke ist jedoch häufig möglich. Der Vorteil des SMB-Protokolls liegt darin, dass sich das Format nicht von der typischen Internetkommunikation unterscheiden lässt. Bekannte Botnetze mit SMB-Protokoll sind Regin, Duqu und Phatbot (siehe Abb. 14 Mitte; Vormayr et al. 2017, S. 2775; Xing et al. 2021, S. 4).

4. P2P-Protokolle

Bereits existierende P2P-Protokolle können innerhalb einer P2P-Topologie eingesetzt werden, um ein eigenständiges P2P-Netz zu bilden oder sich in einem bestehenden Netzwerk zu tarnen. Bekannte bestehende Protokolle sind Waste und Kademila, wobei Waste von Phatbot genutzt wird. P2P-Versionen von Zeus setzen Kademila ein (siehe Abb. 14 Mitte; Vormayr et al. 2017, S. 2775-2776; Zipperle 2014, S. 19; Khattak et al. 2014 Mitte, S. 901).

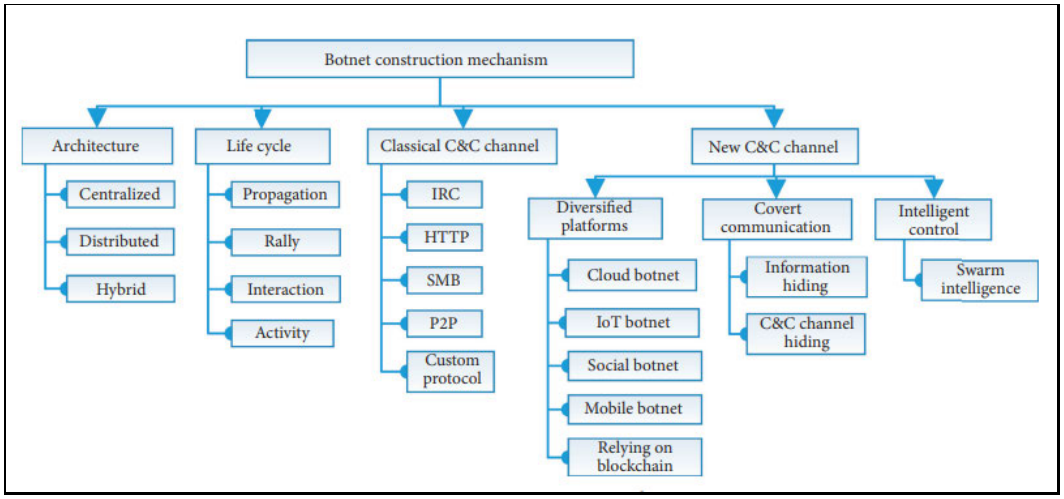

Abb. 14 – Botnet Konstruktionsebenen

(Quelle: Xing et al., 2021, S. 4)

5. Neoterische Protokolle

Botnets können auch selbst entwickelte Protokolle nutzen, um die C&C-Kommunikation zu ermöglichen. Dies kann jedoch dazu führen, dass sich die Kommunikation deutlich von den üblichen Protokollstrukturen unterscheidet und so leichter erkannt werden kann. Um einen Einblick in solche benutzerdefinierten Protokolle zu erlangen, kann Automated-Protocol-Reverse-Engineering eingesetzt werden. Ebenso werden Anwendungen, die für andere Zwecke gedacht sind, für die C&C-Kommunikation herangezogen. Insbesondere sind die sozialen Medien für Botnetze ideal, um über gefälschte Accounts bei Facebook,

Twitter oder anderen Portalen C&C-Server zu generieren. Sind die Accounts überzeugend umgesetzt, können die Befehle über reguläre Funktionen weitergeleitet werden und die Botnetze können sich auf diese Weise etablieren. Die Accounts können für unterschiedliche Zwecke genutzt werden, so etwa die Domain-Generierung, Verbreitung von Malware oder das Umleiten von Befehlen. Bekannte Netze, die Social Media für ihre Zwecke einsetzten, sind Whitewell, das über Facebook agierte, und Torpic, das die Domain-Generierung über Twitter-Suchtrends vollzog. Snif nutzte Twitter für die Verbreitung von Spionage-Malware. Allerdings können diese Social-Media-basierten Botnetze leicht ausgeschaltet werden, da ein Single Point of Failure des C&C besteht (siehe Abb. 14 Mitte, „Custom Protocol“; Khattak et al. 2014, S. 901).

3.2 Command-and-Control-Server und ihre Funktionen

Wie aus den Überlegungen im vorhergehenden Abschnitt deutlich wird, ist der „Command and Control-Server“ das, was Botnetze von anderweitiger Malware unterscheidet. Er ermöglicht es dem Botmaster, und damit den dahinterstehenden, in der Regel kriminellen, Organisationen, spezifische Malware-Aktivitäten auf tausenden von Rechnern auf dem gesamten Globus gezielt umzusetzen. Obwohl die Erkennungsmöglichkeiten sich im Laufe der Entwicklung verbessert haben, lernen auch die Urheber der Botnetze stetig dazu und werden versierter darin, sich vor Entdeckung zu schützen. Die Weiterentwicklung der zentralisierten zu den P2P-Topologien hat dazu geführt, dass sie nicht mehr über eine einzige Schwachstelle, den zentralen C&C-Server, auszuschalten sind. P2P- und hybride Botnetze bieten eine Vielzahl an Gestaltungsmöglichkeiten für potenzielle Angriffe. Die wesentlichen Aktivitäten, die über den C&C-Server umgesetzt werden sind die folgenden (Zeidanloo/Manaf 2009, S. 564):

- Suchen nach anfälligen, nicht abgeschirmten Computern, die als Angriffsziele dienen können
- Verbreiten des Bot-Codes auf diesen Rechnern, um sie zu Bots zu machen
- Anmeldung der Bots auf dem C&C-Server, um eine Verbindung herzustellen und Befehle zu empfangen.

Dazu kommen schädliche Funktionen, die ausgeübt werden, wie etwa das Sammeln von Informationen über die Opfer, das Blockieren von Diensten oder das Kopieren der Daten des Opfers. Auch werden Daten gelöscht, um die Entdeckung der Malware zu verhindern, und die Bots nutzen die infizierten Systeme als Proxy, um zu kommunizieren und ihre Identität zu verbergen. Bots suchen stetig nach neuen Schwachstellen in Systemen, um sich weiterzuverbreiten, verschlüsseln die Daten der Opfer, um Lösegelder zu erpressen, oder erstellen Berichte über die System-Ressourcen. Auch werden Spam und Pishing-Nachrichten versendet und illegale Inhalte auf den Zombie-Systemen gespeichert (Wendzel 2021, S. 103-105; Steffens 2018, S. 57-58).

Wie in Abschnitt 2.2 Nr. 4 dargestellt, sind es vor allem durchorganisierte, professionelle Hacker-Angriffe, die APTs, durch die schwerwiegende Schäden verursacht werden. Sie agieren mit tausenden von Domainnamen und müssen dementsprechende Infrastrukturen an Hardware und Manpower bereitstellen. Kriminelle Cyber-Organisationen verfügen über spezielle Mitarbeiter-Gruppen, die für die Kontrollserver-Infrastruktur verantwortlich sind. Die Kontrollserver spielen eine erhebliche Rolle, denn sie stellen den Zugriff auf die Zombies sicher und errichten einen Schutzwall durch eine oder mehrfache Anonymisierungsschichten, um von Sicherheitssystemen nicht kompromittiert zu werden. Es gibt eine Reihe von Angriffsstrategien, die vom C&C-Server ausgehen, derer sich APTs bedienen (Steffens 2018, S. 57-58):

- Sie nutzen sogenannte Watering-Hole-Webseiten, die vom Opfer häufig besucht werden müssen, um dort Exploits, kleine Schadprogramme zu verlinken, mit denen sich der Nutzer beim Besuch infiziert.
- Sie verschicken Angriffs-E-Mails vom C&C-Server aus.
- C&C-Server werden als Plattform für das Scannen nach vulnerablen Rechnern genutzt.
- Sogenannte Dropper werden für das Nachladen von Malware vom C&C-Server eingesetzt.
- C&C-Server werden für das Speichern von gestohlenen Daten verwendet.
- Auch Befehle an Backdoors können von C&C-Servern gesendet werden. Backdoors sind von Entwicklern oder den Hackern selbst eingebaute Zugänge zum System, durch die übliche Sicherheitsmechanismen umgangen werden können (siehe Abb. 15; Luber/Schmitz 2018, o. S.).

Bezüglich der IT-Kapazitäten gibt es zwei grundlegende Wege, C&C-Server bereitzustellen: Entweder werden Server von externen Dritten gekapert und zum C&C-Sever gemacht, oder die Angreifer kaufen bzw. mieten sich die benötigten Ressourcen. Für das Besetzen fremder Rechner kommen vor allem kleine Unternehmen oder öffentliche Organisationen in Betracht, bei denen die Sicherheitssysteme eine leichte Übernahme erlauben. Da Hacker inzwischen anonymisierende Dienste, wie den Tor-Browser (Torproject, 2023, o. S.) nutzen, um ihre Identität zu verschleiern, laufen die Ermittlungen oft lange Zeit ins Leere. Dennoch sind die Möglichkeiten, auf fremden Rechnern im Hintergrund zu agieren, begrenzt, denn alle Aktivitäten müssen getarnt werden und können jederzeit von den rechtmäßigen Eigentümern beendet werden. Bei der heutigen Professionalisierung der Cyberkriminalität, setzen die Akteure daher vielfach Root-Server ein, über die sie frei verfügen können, arbeiten mit virtuellen Rechnern oder nutzen Shared Hosting. Dann melden sie eine Domain bei einem offiziellen Registrar an, wobei sie ihre Identität weitgehend verdecken können, und bezahlen mit Kryptowährungen (Steffens 2018, S. 59-60).

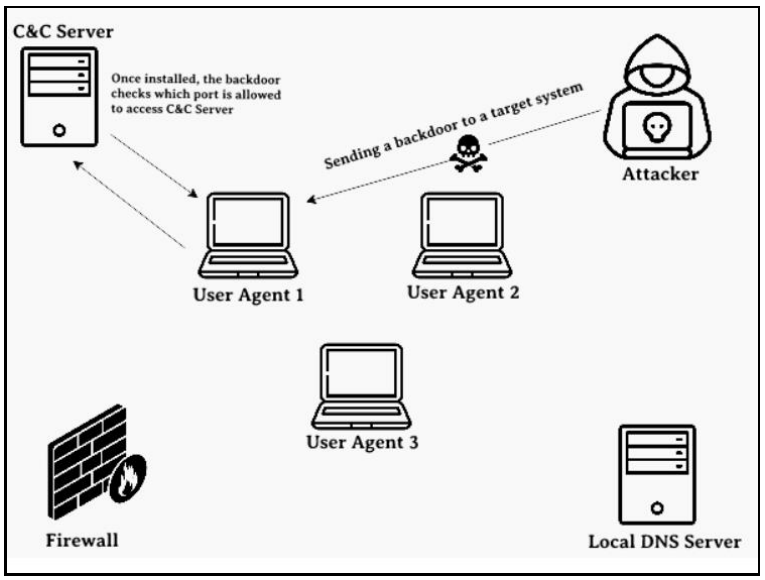

Abb. 15 – Backdoor Attacke

(Quelle: GeeksforGeeks 2022, o. S.)

3.3 Verschlüsselung und Tarnung von Botnetzen

Herausfordernd bei der Verbreitung von Botnetzen ist es, dass die Urheber eine Vielzahl an Malware, Technologien und Strategien kombinieren und immer wieder variieren oder erneuern, um sich erfolgreich einer Entdeckung zu entziehen. Meist profitieren sie dabei finanziell in erheblichem Ausmaß: Die kriminellen Engagements sind so lohnend, dass im Darknet bereits Geschäftsmodelle mit „Cybercrime-as-a-Service“ betrieben werden. Dadurch erhalten auch weniger versierte Hacker Zugang zu ausgefeilten Ressourcen, was die gesamte Botnet-Branche noch befeuert, während die Ermittler in ihren Bemühungen immer einen Schritt zurückzuliegen scheinen. Botnets können inzwischen als komplette Infrastrukturen oder auch Dienste gekauft oder gemietet werden (Georgoulias et al. 2023, S. 219:1-219:2).

Da die Botnet-Aktivitäten vor Entdeckung geschützt werden sollen, setzen die Urheber, wie bereits dargestellt, geläufige Protokolle, wie IRC, HTTP/S und DNS ein, damit der Netzwerk-Datenverkehr keine Auffälligkeiten erkennen lässt. Durch kryptografische Verschlüsselung vermeiden sie eine signaturbasierte Erkennung, der sich die potenziellen Opfer zwar durch ein Blockieren von unbekanntem, verschlüsseltem Datenverkehr entziehen könnten. Allerdings leidet darunter die Sicherheit des Netzwerks insgesamt und es können Fehlalarme ausgelöst werden, die zu einem Ausfall von Diensten führen, sodass dies für potenzielle Opfer keine gangbare Lösung darstellt (Zhong et al. 2015, S. 110).

1. Kryptografie

Der Begriff Kryptografie leitet sich aus den beiden griechischen Begriffen „kryptós“ und „gráphein“ ab, was „verborgen“ und „schreiben“ bedeutet. Es geht also darum, Informationen, die im Geheimen ausgetauscht werden, zu verschlüsseln, damit sie von außenstehenden nicht verstanden werden können. In der Informatik gibt es zahlreiche Bereiche, in denen kryptografische Verschlüsselung eingesetzt wird, da sich dadurch Schutz des Eigentums und Anonymität herstellen lässt. Bekannte Beispiele dafür sind E-Mail-Verschlüsselung und Blockchain-Anwendungen. Daher ist die Verschlüsselung nicht grundsätzlich mit unlauteren Absichten verbunden, im Bereich der Botnetze dient sie allerdings dazu, die kriminellen Aktivitäten der Urheber zu verschleiern. Das Prinzip der Kryptografie besteht darin, eine Nachricht zu chiffrieren, also unlesbar zu gestalten, wobei der Empfänger jedoch über einen Schlüssel verfügt, mit dem er den Inhalt dechiffrieren und dann verstehen kann. Für die Chiffrierung werden in der Regel kryptografische Algorithmen eingesetzt, die bekannt sind, das, was geheim zu halten ist, ist der Schlüssel. Verwendet werden symmetrische und asymmetrische Kryptografie, wobei erstere denselben Schlüssel zum ver- und entschlüsseln einsetzt. Letztere setzt zum chiffrieren einen öffentlichen Schlüssel ein und zum Dechiffrieren einen privaten, wodurch das Verfahren als sicherer gilt, aber auch den Prozess verlangsamt (Wendzel 2018, S. 113-118). Botnetze nutzen Kryptografie, um ihre Kommunikation zu verschlüsseln (siehe Abb. 16; Zhing et al. 2015, S. 110).

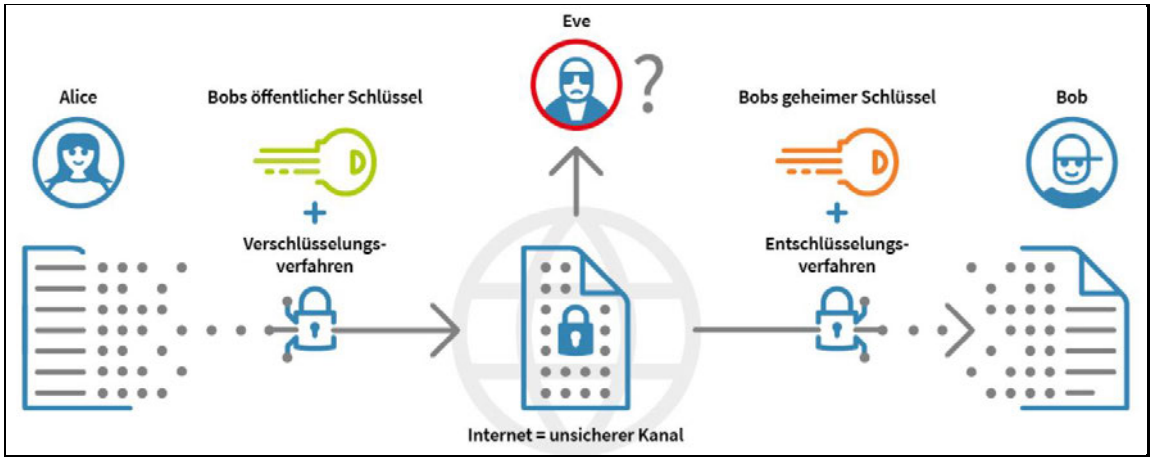

Abb. 16 – Asymmetrische Kryptografie

(Quelle: Plickert, 2023, o. S.)

2. Ausspähen

Botnetze bewegen sich als Netzwerke innerhalb ihrer Opfer-Netzwerke und müssen daher entsprechende Tarnungsstrategien einsetzen, um nicht erkannt zu werden. Sie beginnen ihre Aktivitäten in der Regel, indem sie das anzugreifende Netzwerk scannen, wobei sie herausfinden, welche IP-Adressen ansprechbar sind, welche offenen Ports auf einzelnen Hosts bestehen und welche Software in welchen Versionen installiert ist. Um nach

offenen Netzwerken zu suchen, ist auch das sogenannte Wireless Wardriving üblich, bei dem die Angreifer mit Fahrzeugen durch eine dicht besiedelte Region streifen, um offene WLAN-Netzwerke zu finden. Inzwischen werden auch bevorzugt Geräte aus dem Internet of Things (IoT) aus der Logistik und im Smart Home Bereich aufgespürt. Außerdem können Fahrzeug-Botnetze gebildet werden, um offene IoT-Geräte zu finden und zu besetzen, die wesentlich schlagkräftiger sind, als einzelne Wardriver. Im Ergebnis erstellen sich kriminelle Organisationen daraus Landkarten, in der die gefundenen Netze eingezeichnet sind und die innerhalb der Organisation geteilt werden. Durch Protocol Fuzzing, bei dem die Angreifer für das jeweilige Protokoll unzulässige Daten an die Netzwerksoftware senden, um dann die Reaktion des Systems zu analysieren, verschaffen sie sich weitere Informationen über das Netzwerk. Diese Technik lässt sich auch für Dateiformate und Webseiten-Adressen einsetzen (Wendzel 2018, S. 198-199, Garip et al. 2019, S. 1-2).

3. Kommunikation mitlesen oder abfangen

Aus dem Datenverkehr, den die vorgesehenen Opfer empfangen, können Angreifer weitere wichtige Informationen entnehmen, daher sind sie bestrebt, diesen mitzulesen. Dafür setzen sie Sniffer ein, die auf die Netzwerkschnittstellen zugreifen können. Um auch Nachrichten einzusehen, die nicht für das Opfer, sondern für andere Teilnehmer bestimmt sind, kann der Sniffer die Schnittstelle in den „Promiscous Mode“ versetzen. Wenn die Netzwerkkarten so eingestellt werden, dass sie nur Daten aufnehmen, aber keine Daten versenden, erhalten sie eine Tarnung, durch die sie von außen nicht mehr erkannt werden.

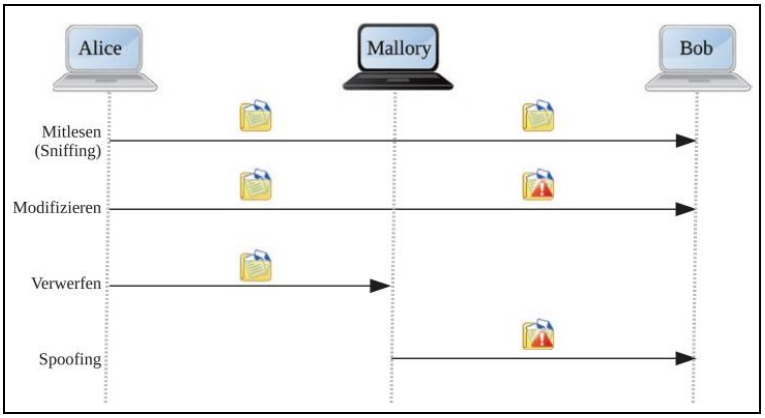

Abb. 17 – “Man-in-the-Middle”-Angriffe (MitM)

(Quelle: Wendzel, 2018, S. 200)

Bei Man-in-the-Middle-Angriffen (MitM) schalten sich die Angreifer gezielt zwischen bestimmte Kommunikationspartner, um zu spezifischen Informationen zu gelangen. Sie lesen den E-Mail-Verkehr mit, modifizieren die geteilten Inhalte, blockieren E-Mails oder fügen neue Daten ein, was als Spoofing bezeichnet wird. Beim Spoofing können sie auch ihre eigene Identität fälschen, indem sie sich als vertrauenswürdiges Gerät anmelden und

dann Falschnachrichten oder, innerhalb eines IoT, Datenpakete oder Malware verbreiten. Bei einem Redirect- oder Rooting-Angriff gibt sich Angreifer als Rooter aus, wofür er Schwachstellen in Routingprotokollen nutzt, und kann dann die Kommunikation mitlesen sowie MitM-Attacken durchführen (siehe Abb. 15; Wendzel 2018, S. 199-200; Misha/Dixit 2018, S. 1-2).

4. Distributed Denial-of-Service (DoS)

Wie bereits erwähnt, zielen Angreifer auch darauf ab, IT-Dienste durch massive Überlastung zum Erliegen zu bringen. Dies kann ein einzelnes Netzwerk betreffen, einen Router oder sich auf eine Reihe von IT-Ressourcen, die über das Internet verbunden sind, also ein IoT richten. Im letzteren Fall ist von Distributed-Denial-of-Service (DDoS) die Rede. Um einen solchen Angriff durchzuführen, müssen die Urheber erhebliche IT-Ressourcen bereitstellen. Diese erhalten sie, indem sie auf die bereits beschrieben Weise Systeme mit Malware infizieren und sie dann als Botnetz steuern. Kritisch können DDos-Attacken etwa dann werden, wenn wichtige Dienste für die Allgemeinheit, wie Krankenhäuser, oder kritische Infrastruktur, wie militärische Einrichtungen oder Versorgungswerke, betroffen sind. Inzwischen nutzen die Urheber außerdem Amplifier, mit denen die Angriffe verstärkt werden, oder Amplifier Networks, als Multiplikatoren, was die Wirkung der Angriffe vervielfältigt. Da sie ihre Absender-Adresse fälschen, können sie nicht zurückverfolgt werden. Permanent-DoS-Angriffe gehen noch weiter, indem sie Sicherheitslücken auf den Zielsystemen nutzen, um Systemschäden hervorzurufen, etwa durch das Löschen grundlegender Daten (Wendzel 2018, S. 201-203; Sujatha et al. 2022, S. 1-2).

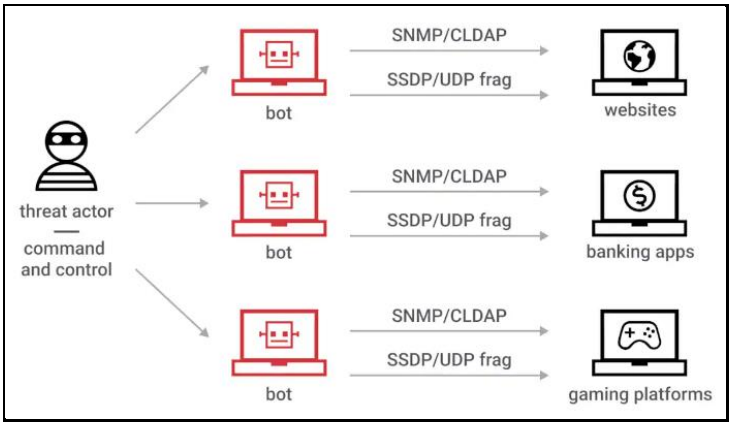

Abb. 18 – Volumetrischer DDoS-Angriff

(Quelle: Akamai 2023, o. S.)

5. Steganografie

Eine wesentliche Rolle bei der Übertragung von Informationen im Zusammenhang mit Botnetzen spielt auch die Steganografie. Dabei geht es darum, unsichtbare Informationen innerhalb sichtbarer Informationen so zu verstecken, dass ihre Existenz nicht zu erkennen ist. Im Gegensatz zur Kryptografie, bei der die Daten sichtbar verschlüsselt sind, nur nicht

gelesen werden können, sollen Instanzen, die auf die Inhalte zugreifen können, nicht einmal von deren Vorhandensein wissen. Das Einbetten und Extrahieren der Stegodaten erfolgt so, dass die Hülldaten unverändert bleiben (siehe Abb. 19; Franz/Pfitzmann 1998, S. 183-184). Im Zusammenhang mit Botnetzen geht es vor allem darum, versteckte Botschaften so in Netzwerkdaten zu integrieren, dass die übertragenen Daten einer regulären Form entsprechen. Dabei sind zwei Arten von Kanälen wesentlich: Verdeckte Kanäle und Seitenkanäle. Verdeckte Kanäle sind irreguläre Kommunikationskanäle, die gegen Sicherheitsrichtlinien verstoßen. Seitenkanäle sind verdeckte Kanäle, die Informationen ohne eine Intention übertragen (Wendzel 2018, S. 293).

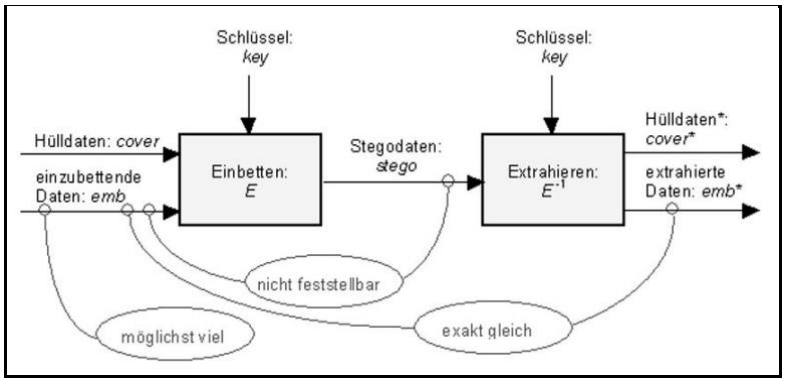

Abb. 19 – Steganografie

(Quelle: Franz/Pfitzmann, 1998, S. 184)

Netzwerk-Steganografie richtet sich auf paketvermittelnde Kommunikation aus, wie sie für das Internet verwendet wird. Das Internet sowie Fest- und Mobilfunknetze, und insbesondere die Kommunikationsprotokolle, eröffnen zahlreiche Möglichkeiten der verdeckten Kommunikation. Dabei werden die folgenden Manipulationen vorgenommen:

1. Einzelne Funktionen der Protokolle werden verändert.
2. Spezifische Fehler und Schwächen werden eruiert und/oder
   die Art des Informationsaustauschs oder die Nachrichtenform werden verändert.
3. Die beobachtbaren Auswirkungen der Veränderungen werden auf ein Minimum reduziert.

Auf Basis dieser Bedingungen lassen sich Netzwerksteganografie-Techniken umsetzen. Auch wenn die erste Bedingung nicht vorliegt, können versteckte Nachrichten übermittelt werden, indem eine von Sender und Empfänger definierte Interpretation der Ergebnisse vereinbart wird. Netzwerksteganografie kann bezüglich ihrer Wirksamkeit nach drei Kriterien beurteilt werden: Steganografische Bandbreite, Resistenz gegen Steganalyse und Robustheit. Im Idealfall zeigt die Methode eine hohe Robustheit, das heißt Widerstandsfähigkeit gegenüber Veränderungen, ist schwer erkennbar und hat dabei eine möglichst

hohe Bandbreite. Mit steigender Bandbreite sinken tendenziell Widerstandsfähigkeit und Robustheit (Lubacz et al. 2014, S. 225-227).

4 Bekämpfung von Botnetzen

Aus den bisherigen Überlegungen lässt sich erkennen, dass Botnetze erhebliche Schäden verursachen und als Ausläufer der organisierten Cyberkriminalität gelten können. Umso wichtiger wird es, im Rahmen der Cybersicherheit Mittel und Wege zu finden, um dem entgegenzutreten. Zu unterscheiden sind dabei zwei Wirkungsgrade: Angriffe können einerseits durch Intrusion Detection Systems (IDS) erkannt, zu Protokoll gebracht und gemeldet oder durch ein Intrusion Prevention System (IPS) gleich beim ersten Kontakt abgewehrt werden (Wendzel 2018, S. 206).

4.1 Botnet Intrusion Detection und Removal

Grundsätzlich lassen sich drei Formen von IDS unterscheiden (Wendzel 2018, S. 206; Mohd Dollah et al. 2018, S. 27):

- HIDS sind hostbasierte IDS für lokale Systeme, die etwa die Konfiguration eines Systems auf verdächtige Aktivitäten scannen.
- NIDS sind netzwerkbasierte IDS, die das Netzwerk auf ungewöhnliche Aktivitäten scannen.
- Hybride IDS, die lokale Systeme und Netzwerke scannen.

Der Lebenszyklus eines Botnetzes kann in die Phasen der Verbreitung, Formation, Interaktion und Umsetzung der schädlichen Aktivitäten bis zum Tod eingeteilt werden (Zipperle 2014, S. 18). In der Inkubationsphase dringen die Bots als eigenständig lauffähige Software über Schwachstellen in Systeme ein und besetzen sie, bis ihr Netzwerk die gewünschte Größe erreicht. Dem folgt die Formation, bei der die Bots sich mit dem C&C-Server verbinden, wobei sie entweder durch eine statische oder durch eine dynamische Adressierung verbunden sind. Bei der statischen Adressierung ist die Verbindung mit den Ressourcen des C&C-Servers unveränderlich gestaltet, bei der dynamischen Adressierung wird sie anhand eines Algorithmus generiert. In der Interaktionsphase nisten sich die Bots im System entsprechend ihren Vorhaben ein, indem sie sich registrieren, Dateien herunterladen, Aufträge erteilen und die Ergebnisse aufzeichnen. In der Angriffsphase wird die Malware aktiviert, um Pishing, DDoS, Spamming und betrügerische Aktivitäten zur Gewinnung finanzieller Mittel auszuführen (Xing et al. 2021, S. 4). Für die Erkennung von Botnetzen ist es wichtig, dass sie bereits in der Inkubationsphase aufgespürt werden, denn die von ihnen ausgehenden Gefahren sind im Vergleich zu anderen Bedrohungen der Netzwerksicherheit als schwerwiegend zu bewerten (Xing et al. 2021, S. 1 und 3).

Potenzielle netzwerkbasierte Angriffe können über die folgenden Ebenen ermittelt werden (Wendzel 2018, S. 206; Xing et al. 2021, S. 2):

- anomaliebasiert
- signaturbasiert
- spezifikationsbasiert
- DNS-basiert
- Mining-basiert

Bei der anomaliebasierten Erkennung geht es darum, Abweichungen von der Norm zu erkennen, was über statistische Modelle oder Heuristik erreicht werden kann. Diese Verfahren bergen jedoch Schwächen, da es schwierig ist, die Grundannahmen exakt zu bestimmen. Daher wurden in der weiteren Entwicklung maschinelles Lernen und Entropieanalysen eingesetzt (Wendzel 2018, S. 207). Signaturbasierte Verfahren haben den Nachteil, dass sie keine neuen Angriffe ermitteln können, wenn die Angriffssignaturen noch unbekannt sind (Mohd Dollah et al. 2018, S. 27). Spezifikationsbasierte Verfahren nutzen eine Vorlage, anhand der die Daten überprüft werden. Weichen die Daten von dieser ab, könnte eine Sicherheitsbedrohung vorliegen, es ist jedoch nicht eindeutig, daher muss die Abweichung weiter untersucht und in Zusammenhang mit dem Kontext gestellt werden (Wendzel 2018, S. 209).

Neben den bereits dargestellten Protokollen (IRC, HTTP, P2P, SMB) nutzen Botnetze inzwischen zahlreiche neue C&C-Kanäle, wie

- diversifizierte Plattformen
- verdeckte Kommunikation
- intelligente Steuerung

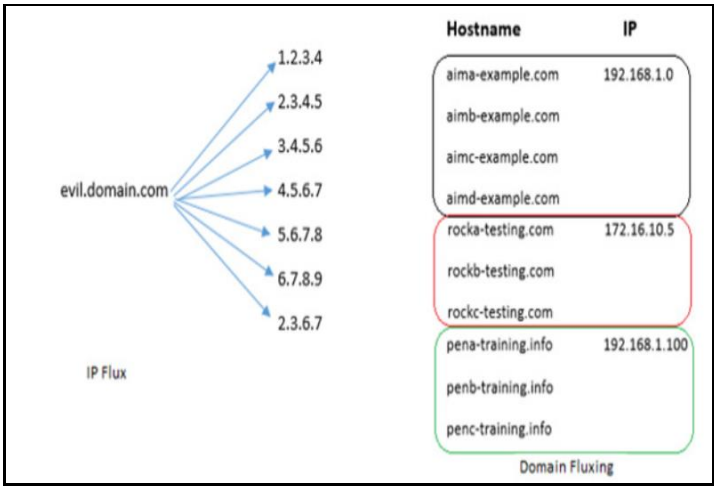

Abb. 20 – Domain-Flux und IP-Flux

(Quelle: Agyepong et al. 2018, S. 17)

Das heißt, sie arbeiten mit gemieteten Clouds, besetzen IoT-Netzwerke, soziale Medien und mobile Netzwerke, wodurch sie insgesamt sehr viel mächtiger werden, da die Wahrscheinlichkeit eines Ausfalls sinkt. Sogar die Blockchain-Technologie wird inzwischen eingesetzt, um Schlagkraft und Lebensdauer von Botnetzen zu erhöhen und finanzielle

Transaktionen mit Kryptowährungen zu vollziehen. Durch Kryptografie, Komprimierung, Verschleierung und Steganografie haben sie immer bessere Möglichkeiten sich zu tarnen. Während bei der Verwendung von Fast-Flux-Netzen über DNS nur eine Verschleierung des Standortes möglich ist, setzen sie Domain- oder IP-Flux ein, um die Domain des C&C-Servers fortlaufend zu wechseln. Dadurch ist eine Entschlüsselung des Domain-Algorithmus erforderlich, um den echten Standort zu ermitteln (siehe Abb. 20; Xing 2021, S. 5; Agyepong et al. 2018, S. 16). Außerdem zeigen sich intelligente Systeme, die durch Selbstorganisation, Robustheit und Anpassungsfähigkeit gekennzeichnet sind, als Grundlage für Architektur und Kommunikationsprotokolle von Botnetzen richtungsweisend. Bei einer solchen Umsetzung könnten intelligente Bots auf Basis spontaner Interaktion auftretende Fehler minimieren und sich dynamisch an die jeweilige Umgebung anpassen (Xing et al. 2021, S. 5).

Eine wesentliche Rolle im Bereich der Botnet-Detektion spielen außerdem sogenannte Honeypots und Honeynets. Diese werden beim Honeytrapping potenziellen Angreifern als lohnende Beute präsentiert, um sie einerseits von echten Systemen abzulenken und andererseits die Vorgehensweise und Ressourcen der Botnetze auszuspähen. Hier ergeben sich besondere Vorteile in Bezug auf die Entdeckung von Zero-Day-Exploits, Schadsoftware, die bisher noch unbekannt ist, und deren Aufzeichnung (siehe Abb. 21; Wendzel 2018, S. 209-210; Li et al. 2021, S. 59).

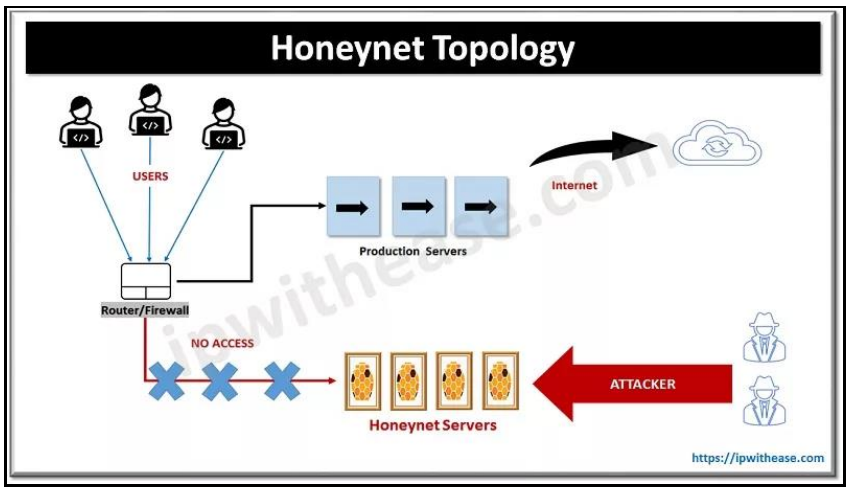

Abb. 21 – Honeypot und Honeynet

(Quelle: Bhardwaj, 2022, o. S)

Für die Arbeit mit Honeynets gibt es spezielle Software (beispielsweise Snort; Snort, 2023, o. S.), die umfassende Netzwerke auf einem Rechner simuliert, ohne dafür erhebliche Ressourcen zu benötigen. Dabei kann allerdings die täuschend echte Simulation von Industriesteueranlagen eine Ausnahme darstellen, diese kann durchaus zusätzliche Hardware erfordern. Honeypots können als virtuelle Systeme oder separat aufgestellte Rechner eingesetzt und sowohl mit Low-Interaction (LI) oder High-Interaction (HI) betrieben werden, wobei die HI-Systeme mehr Wartungsaufwand benötigen, im Gegenzug aber

auch tiefere Einblicke in die Ressourcen der Angreifer ermöglichen (Wendzel 2018, S. 209-211). Beim Einsatz von Honeypots/-nets gibt es jedoch Schwächen, da sie verschlüsselten Datenverkehr und unbekannte Angriffe nicht identifizieren können (Xing et al. 2021, S. 6). Außerdem ist eine effiziente Umsetzung mit hohen Kosten verbunden und sie zeigen wenig Flexibilität in der Gestaltung (Li et al. 2021, S. 59).

Erfolgreich arbeiten Methoden zur anomaliebasierten Bot-Erkennung, die mit Deep Learning, einer fortgeschrittenen Form des Maschinellen Lernens, oder Neuronalen Netzen arbeiten. Sie können basierend auf räumlichen Merkmalen (CNN, Convolutional Neural Network), Zeitreihen (RNN, Recurrent Neural Network), einer Kombination von CNN und RNN, Fast-Flux-Erkennung, Domänennamen (DNN, Domain Neural Network) und anderen Möglichkeiten entwickelt werden. Eine weitere Form stellt das Reinforcement Learning (Verstärkungslernen) dar, bei dem ein Algorithmus eingesetzt wird, um sequenzielle Entscheidungsprobleme zu lösen. Dadurch kann die Lösung den Katalog von bekannten Merkmalen stetig erweitern sowie verteilte KI-Detektoren einsetzen, die intelligente Entscheidungen treffen (Xing et al. 2021, S. 6-8). Eine Zusammenstellung der möglichen Varianten solcher auf Deep Learning beruhenden Lösungen findet sich bei Xing et al. (Xing et al. 2021, S. 9-10). In jedem Fall gehört das Sammeln und Analysieren von Informationen über Angreifer und Attacken sowie der Einsatz dieses Wissens zur Prävention, die sogenannte Threat Intelligence, zu den wesentlichen Maßnahmen der Netzwerksicherung. Um Social Engineering abzuwehren, können Netzwerke durch verschärfte Zugriffskontrollen gehärtet sowie spezifische Detektoren und Reaktionstools eingesetzt werden (Wendzel 2018, S. 212-213).

4.2 Botnet Intrusion Prevention und Schutzmaßnahmen

Ein IDS kann letztlich auch der Vorsorge gegenüber Botnetzen dienen, wenn es als IPS konfiguriert wird. Am Beispiel von Snort (Snort 2023, o. S.), das sowohl als IDS wie auch als IPS (Wendzel 2018, S. 206), also als IDPS genutzt werden kann, soll dies nun praktisch aufgezeigt werden. Bei einem Angriff auf Anwendungen oder Hardware eines Netzwerkes wird dem Administrator zunächst ein Regelverstoß gemeldet und dieser wird innerhalb eines Schutzdaten- und Ereigniskontrollsystems erfasst. Das Intrusion-Monitoring eines IDS überwacht den eingehenden Datenverkehrsfluss und muss zunächst feststellen, wie der reguläre Datenverkehrsfluss sich darstellt. Die Regelverstöße werden dann durch die folgenden Klassen von Angriffserkennung unterschieden (Sharma et al. 2022, S. 473-475):

- Network IDS
- Host IDS
- Protokollbasierte Intrusion Detection Systems (PIDS)
- Anwendungs-Protokoll-basierte Intrusion Detection Systems (APIDS)
- Hybride IDS

Verstöße können beispielsweise gegen Computer-Sicherheitsgesetze, Fair-Use-Regeln oder Standardsicherheits-Praktiken erkannt werden. Das IDS übt die Funktionen Überwachung, Erkennung, Warnung aus. Ein IPS prüft, erkennt, klassifiziert und wehrt den Angriff so weit wie möglich ab. Mit Applikationen wie Snort werden Anomalien, Regelverletzungen und Verhaltensweisen des Netzwerks beobachtet, Sicherheitsrisiken werden erkannt und sofortige Maßnahmen zur Verhinderung der Gefahren werden umgesetzt. Das IPS nutzt dann die gesammelten Daten aus dem IDS, um mithilfe von Künstlicher Intelligenz (KI) und Maschinellem Lernen (ML) durch Algorithmen eigenständige Erkennungsmechanismen zu entwickeln. Dafür wird sowohl überwachtes, wie auch unüberwachtes Lernen benutzt. Im ersten Fall werden gezielt Trainingsdaten für den Lernprozess eingesetzt, im zweiten Fall wendet der Algorithmus die gesammelten Informationen auf unbekannte Datensätze an und entwickelt dadurch die Fähigkeit, Bedrohungen eigenständig zu erkennen und mit entsprechenden Maßnahmen darauf zu reagieren (Sharma et al. 2022, S. 477-479).

Die Funktionen, die eine Open-Source-Software wie Snort bieten, sind Echtzeit-Verkehrsüberwachung, IP-Netzwerk-Paket-Protokollierung sowie Überprüfung und Anpassung der Prozesse. Darüber hinaus können die Bedarfe des individuellen Netzwerkes durch den Nutzer in Form von eigenen Regeln integriert werden. Die Erkennung erfolgt hauptsächlich auf der Basis der Identitäten, signaturbasiert, anomaliebasiert und über eine vollständige Protokollanalyse. Es können beispielsweise „Internet Control Message“-Protokolle (ICMP) oder „File Transfer“-Protokolle (FTP) abgefangen und analysiert werden, wobei die Software in Versuchen eine erfolgreiche Abwehr zu 98,89 % umsetzen konnte. Eine IPS-Software sollte parallel zu anderen Sicherheitsmaßnahmen, wie der Verwendung von Anti-Viren-Software, Firewalls und Netzwerksegmentierungen eingesetzt werden, um die Systeme optimal zu sichern. Firewalls schirmen ein Netzwerk von außen ab, Netzwerksegmentierung teilt ein physisches Netzwerk in virtuelle Bereiche auf, die durch unterschiedliche Sicherheitsvorkehrungen geschützt werden, um ein Durchqueren des Netzes von Angreifern zu erschweren. Wesentlich für den Erfolg ist jedoch eine korrekte Konfiguration der Software in Abstimmung mit den vorhandenen Netzwerk-Rahmenbedingungen (Sharma et al. 2022, S. 482-484).

4.3 Juristische Aspekte von Botnetzen

Nach dem Bericht des Bundeskriminalamtes waren im Jahr 2021 rund 146.363 Straftaten im Bereich Cyberkriminalität zu verzeichnen (siehe Abb.2). Insgesamt wurden dabei im Jahr 2022 hochgerechnet Schäden in Höhe von rund 202,7 Milliarden Euro verursacht (Statista, 2022a). Botnetze tragen einen erheblichen Anteil an diesen kriminellen Aktivitäten, es stellt sich die Frage, inwieweit sie auf rechtlicher Ebene zur Rechenschaft gezogen werden können.

Die Verbreitung und der Einsatz von Botnetzen zu kriminellen Zwecken berührt grundsätzlich zwei Vorschriften des Strafgesetzbuches (StGB) (Stam 2017, S. 547 und 550):

- § 202 a StGB

„Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter der Überwindung der Zugangssicherung verschafft“ macht sich strafbar.

- § 303 StGB

„Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert“ macht sich strafbar.

In der Rechtsprechungspraxis ist es jedoch keineswegs einfach, den Kriminellen Straftaten zur Last zu legen. Im Fall des § 202 a StGB scheitert eine Verurteilung durch den Begriff der „besonderen Zugangssicherung“, der vom Oper der Attacke nachgewiesen werden muss. Nur wenn ein Geschädigter aufzeigen kann, dass er nach dem Kauf eines Rechners einen zusätzlichen Schutz, wie etwa ein Anti-Virenprogramm, installiert hat und dieses auch aktiv war, gilt der Tatbestand der besonderen Zugangssicherung als gegeben (Stam 2017, S. 548-550). Im Gegensatz dazu greift § 303 StGB jedoch in der Regel, da bei Installation eines Botnetzes auf einem Rechner Daten verändert werden, indem beispielsweise bewirkt wird, dass die Bot-Software beim Starten des PCs ausgeführt wird. Das Strafmaß beträgt bis zu zwei Jahren Freiheitsstrafe (Stam 2017, S. 550-551).

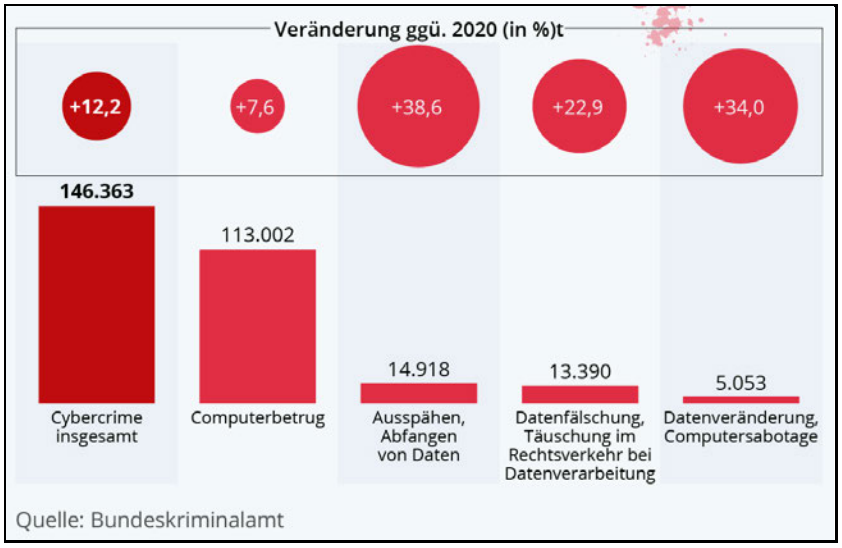

Abb. 22 – Anzahl der Cybercrime-Delikte in Deutschland 2021

(Quelle: Statista 2022, o. S.)

Der Begriff der Cyberkriminalität im engeren Sinne bezieht sich auf IT-Aktivitäten und schließt den Handel mit verbotenen Gegenständen über das Inter-/Darknet aus, er zeigt sich auf sehr vielfältige Weise. Die Verbreitung sowie der Missbrauch von Botnetzen berühren im Grunde eine ganze Reihe von Straftatbeständen, je nachdem wie sie gelagert sind. Dazu zählen Attacken im Bereich Ransomware, Malware, Pishing, DDoS sowie das unbefugte Eindringen in fremde IT-Ressourcen. Die Verfolgung ist jedoch in der Regel mit

langwierigen Verfahren verbunden, in denen die Ermittler genauestens aufklären müssen, wie sich das Verbrechen gestaltete und welche Straftatbestände davon berührt werden (Peters 2022, S. 8-10). Besonders drastisch lässt sich anhand eines im Jahr 2020 zugetragenen Falls erkennen, wie komplex Fälle von Cyberkriminalität sich zeigen und wie schwierig es letztlich, die Sachverhalte aufzuklären, nachzuweisen und zu ahnden. Das Universitätsklinikum Düsseldorf wurde Opfer einer Ransomeware-Attacke, wodurch die Systeme des Krankenhauses ausfielen und in der Folge ein Mensch verstarb. Es entstand außerdem ein erheblicher Sachschaden und es dauerte mehrere Wochen, bis das Krankenhaus wieder vollständig einsatzfähig war. Straftatbestände ergeben sich aus dem Einsatz einer Verschlüsselungssoftware, der Forderung eines Lösegelds und dem Tod eines Patienten. Berührt werden dabei die bereist genannten §§ 202 a und 303 StGB und weitere Paragrafen. Es lassen sich Verletzung des Geheimbereichs (§§ 201-210 StGB), Sachbeschädigung (§§303-305a StGB), Computersabotage (§ 3030 b STGB), Erpressung (§ 253) und ggf. Mord oder Totschlag (§§ 211 und 212 StGB) als Straftatbestände annehmen. Schließlich stellte sich aber anhand der Untersuchungen heraus, dass der Angriff ein Versehen war, da eigentlich die Universität selbst das Ziel des Angriffs war. Die Lösegeldforderung wurde daraufhin zurückgezogen. Außerdem konnte nach Obduktion der verstorbenen Patientin festgestellt werden, dass diese auch ohne den Angriff nicht hätte überleben können. Im Ergebnis sind die Ermittlungen immer noch nicht abgeschlossen, es konnte niemand zur Rechenschaft gezogen werden und die Spur der Angreifer verläuft sich in Richtung Russland (Peters 2022, S. 11-20). Das Beispiel zeigt, dass auch die Umsetzung eines Rechtsverfahrens gegen Cybercrime-Attentäter nicht unbedingt zu adäquater Bestrafung führt, dass die Verfahren langwierig sind, die Beweislage schwierig sei kann und letztlich immense Schäden entstehen, für die unter Umständen niemand aufkommt. Im Endeffekt erscheinen umfassende, vorbeugende Schutzmaßnahmen vor potenziellen Attacken empfehlenswerter, als Risiken in dieser Hinsicht einzugehen.

5 Botnetze und Informationssicherheit

Kriminelle Botnetze werden initiiert, um Institutionen, Unternehmen oder Personen zu schädigen und finanzielle Mittel zu erbeuten. Die zunehmende Verbreitung der Angriffe zeigt Folgen in Wirtschaft, Gesellschaft und Politik. Einige der aktuellen Entwicklungen sollen nun aufgezeigt werden.

5.1 Wirtschaftliche Schäden und Risiken von Botnetzen

Im Jahr 2022 wurden weltweit bei rund 108,9 Millionen Accounts Datenschutzverletzungen gemeldet, was einem Anstieg um 70 % gegenüber dem Vorjahr entsprach. Die Hacker-Gruppe „Lapsus$“ konnte im März 2022 nachweisen, dass sie in der Lage war, eine Reihe von Microsoft-Produkten zu attackieren. Das Unternehmen wehrte den Angriff nach eigenen Angaben ohne Datenschutzverletzungen ab. Dennoch zeigt dies, dass selbst einer der weltweit führenden IT-Player nicht vor Angriffen sicher ist. Beim Unternehmen Cash App wurden im April 2022 durch einen ehemaligen Mitarbeiter Kundendaten gestohlen, mutmaßlich blieb es jedoch bei personenbezogenen Daten, ohne dass Kontodaten kompromittiert wurden. Auch das Internationale Komitee des Roten Kreuzes wurde im Jahr 2022 gehackt, Daten von etwa einer halben Million Menschen waren in Gefahr. Als Folge wurden die Server vom Internet getrennt und bis heute ist es unklar, wer hinter dem Angriff steht. Die weltweiten Schäden werden für 2025 auf 10,5 Billionen US-Dollar geschätzt, was einem Anstieg gegenüber 2015 um 300 % entspricht (Etheridge 2022, S. 5-7).

Im Juni 2022 wurde das russische Botnetz RSOCKS in Zusammenarbeit von Behörden aus den USA, Deutschland, den Niederlanden und Großbritannien abgeschaltet. Das Netzwerk hatte sich auf Millionen von Rechnern und Geräten installiert, ohne dass es den Eigentümern bekannt war, vor allem im Internet of Things sowie auf Android-Geräten und PCs. Über eine eigene Webseite wurden die so verfügbaren Rechner-Kapazitäten zu Preisen zwischen 30 und 200 Dollar pro Tag vermietet, wobei die Anzahl der Geräte, auf die Kunden Zugriff nehmen konnten, zwischen 2.000 und 90.000 lag. Verblüffend ist dabei, dass auch größere Institutionen, wie ein Hotel, eine Universität und ein Fernsehstudio unbemerkt besetzt werden konnten. Die Bots wurden genutzt, um Malware zu verbreiten, Standorte zu verschleiern, Zugriff auf Webseiten zu nehmen, Pishing-Mails zu versenden und unerkannt Social-Media-Accounts zu nutzen. Zugang erhielten die Angreifer durch Brute-Force-Attacken, das automatisierte Ausprobieren von Passwörtern. Fünf Jahre haben die Ermittlungen angedauert, während dieser Zeit waren die Beamten des FBI damit beschäftigt, das Geschehen auszuspähen. Die Informationen zur Aufdeckung des Falls wurden über die Nachrichtenagentur Reuters veröffentlicht (Spiegel Netzwelt 2022, o. S.)

Aus den Beispielen ist ersichtlich, dass Cyberkriminalität sowohl in der Häufigkeit wie auch in der Höhe der verursachenden Schäden wächst und damit auch Botnetz-Angriffe. Da sich die Hacker-Szene stetig weiterentwickelt, müssen die Schutzvorrichtungen diesem Grad an Professionalisierung gerecht werden.

5.2 Soziale und politische Konsequenzen von Botnetzen

Die Corona-Pandemie hat in den Jahren 2020 bis 2022 dafür gesorgt, dass Menschen auf globaler Ebene zu Hause arbeiten mussten, wodurch die Digitalisierung der Gesellschaft einen starken Schub erhielt. Für viele Mitarbeiter ist daraus ein Arbeitsplatz mit Homeoffice-Anteil geworden und es werden häufig auch private Geräte, wie Handy oder Tablet, bei der mobilen Arbeit genutzt. Daraus können sich für Unternehmen erhebliche Sicherheitslücken eröffnen, etwa wenn die Mitarbeiter den Sicherheitsstatus ihrer Geräte nicht auf dem aktuellen Stand halten. Von Hackern werden diese Geräte gerne genutzt, um ihre Botnetze zu erweitern, wodurch sich indirekt auch ein Zugriff auf die Unternehmen selbst ergeben könnte. Daher wird Unternehmen von Sicherheits-Experten empfohlen, eine BYOD- (Bring your own Device) Richtlinie zu erstellen, mit der ein Umgang mit privaten Geräten an die Sicherheitsstandards angepasst wird (Etheridge 2023, S. 8). An diesen Entwicklungen wird deutlich, dass im Zuge der fortschreitenden Digitalisierung die Grenzen zwischen unternehmerischer und privater Informationstechnologie schwinden. Dies wird durch die Etablierung der Social Media als moderne Form der technologischen Kommunikation noch verstärkt.

Auf der politischen Ebene wurde in Deutschland bereits im Jahr 1991 das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingerichtet, das heute Dienstsitze in Bonn, Freital und Saarbrücken unterhält. Es sieht seine wesentliche Aufgabe darin, den sicheren Einsatz der Informations- und Kommunikationstechnik von Staat, Wirtschaft und Gesellschaft in Deutschland zu gewährleisten. Dazu gehört es auch, Tatbestände zu Risiken der Informationstechnik und mögliche Schutzmaßnahmen zur Aufklärung zu sammeln und offenzulegen. Das BSI entwickelte die Coordinated Vulnerability Disclosure (CVD)-Richtlinie, die ein Meldeverfahren für Sicherheitsvorfälle von Bund und Unternehmen regelt. Zudem veröffentlichte das BSI das BSI-Grundschutz-Kompendium, einen Standard, der es Institutionen erleichtern soll, ein Informationssicherheits-Management-System (ISMS) zu etablieren. Auch erarbeitete das BSI einen Standard zum Risikomanagement bei der Erstellung eines ISMS. Auf der Basis des IT-Grundschutzes können Institutionen eine Zertifizierung nach dem internationalen Standard ISO/IEC 27001 erwerben, um ein effizientes ISMS umzusetzen (BSI 2023, o. S., „Auftrag“).

In Deutschland sind verschiedene Gesetze und Richtlinien erlassen worden, wie das „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ aus dem Jahr 2009. Dieses räumte dem BSI verschiedene Befugnisse im Zusammenhang mit der Meldung und Offenlegung von IT-Sicherheitsvorfällen ein. Es wurde im Jahr 2015 zum ersten IT-Sicherheitsgesetz, wobei ein besonderer Bezug zur Cybersicherheit kritischer

Infrastrukturen (KRITIS), für industrielle Anlagen und humanitäre Versorgungseinrichtungen hergestellt worden ist. Im Jahr 2021 ist es weiter novelliert worden, um Detektion und Abwehr von Cyberangriffen, mobile Cybersicherheit, Cybersicherheit von Unternehmen und Cybersicherheits-Zertifizierungen in den Fokus zu stellen. In diesem Rahmen hat der BSI nach dem Cybersecurity Act der Europäischen Union, EU 2019/881, die Aufgabe, die Zertifizierungen zu beaufsichtigen und durchzuführen (BSI 2023, o. S., „Kritis“ und „IT-Sicherheitsgesetz 2.0“).

Mit der strafrechtlichen Verfolgung von Cyberkriminalität befasst sich die Abteilung CC (Cybercrime) des Bundeskriminalamtes, die im Jahr 2020 eingerichtet wurde. Zu ihren Aufgaben gehört es, gegen Cyberkriminelle zu ermitteln, Daten auszuwerten, Lagebewertungen vorzunehmen, Informationen zu sammeln, Bundeseinrichtungen und kritische Infrastrukturen zu schützen, rechtlich zu beraten und zentraler Ansprechpartner für alle Anliegen bei der Verfolgung von Cyberkriminalität zu sein (BKA 2023, o. S.).

5.3 Zukünftige Entwicklungen und Trends von Botnetzen

In den letzten Jahren zeigt sich ein deutlicher, neuer Trend im Bereich der Cyberkriminalität: Botnetze werden im IoT integriert. Dazu gehören Geräte wie industrielle Sensoren und Aktoren, Überwachungskameras, digitale Videorecorder, Wearables, Mobilfunkgeräte, Smart Home Technologien u. v. a.. Dies ist vor allem dadurch bedingt, dass die Sicherheitsvorkehrungen aufgrund der kleineren Rechenkapazitäten einzelner Geräte im IoT geringer ausfallen und tendenziell auch die Überwachung durch die Nutzer nachlässiger erfolgt, als es bei großen Rechnersystemen der Fall ist. Ein Beispiel dafür ist das im Jahr 2016 bekannt gewordene Botnetz Mirai, das aufgrund einer Authentifizierungs-Lücke 600.000 IoT-Geräte kaperte, hauptsächlich Geräte zur Videoüberwachung sowie Drucker, und diese für DDoS-Attacken gegen große Institutionen einsetzte. Die Hacker machen es sich dabei zunutze, dass die Anzahl der mit dem Internet vernetzten Geräte in den nächsten Jahren auf rund 50 Milliarden ansteigen wird (Nasir et al. 2022, S. 1-2).

Insgesamt gewinnt die organisierte Cyberkriminalität auch dahingehend an Bedeutung, als dass sie immer stärker mit dem klassischen organisierten Verbrechen verflochten ist, etwa dem Handel mit Menschen, Waffen und Drogen, mit terroristischen Organisationen und politischem Extremismus. Die Angriffe der Botnetze gewinnen an Komplexität und Professionalität, wobei es, trotz bestehender Abkommen und Rechtshilfe, immer noch an Möglichkeiten mangelt, schnell auf Angriffe zu reagieren und international zusammenzuarbeiten. Der Grund dafür liegt einerseits darin, dass die Geschäfte solche Gewinne abwerfen, wie sie sonst nur im Vertrieb illegaler Güter und Dienstleistungen der Fall ist. Andererseits verbreiten sich Informations- und Kommunikationstechnologien so schnell und weitreichend, dass bereits eine immense Abhängigkeit sowohl vonseiten des Staates wie auch von Wirtschaft und Gesellschaft besteht. Für die Strafverfolgungsbehörden erweist es sich zudem als verfahrenstechnische und kriminalistische Herausforderung, die Aktivitäten der Netzwerke nachzuvollziehen und handfeste Beweise für eine strafrechtliche

Belangung der Beteiligten vorzulegen, was eine Verurteilung erschwert (Puchkov 2022, S. 27-28).

Ein Trend in der H von Hackern lässt sich inzwischen deutlich erkennen: Tatsächlich sind es nur wenige, elitäre Spezialisten, die ausgefeilte Kenntnisse im Bereich von Informatik und Mathematik einsetzen, um komplexe Betrugstechnologien zu entwickeln. Die Ergebnisse werden dann zusammen mit Gebrauchsanweisung in großem Stil und zu hohen Summen von professionellen Händlern im Darknet verkauft. Ein großer Teil der Cyberkriminellen nutzt die angebotenen, benutzerfreundlichen Technologien lediglich, um damit geschäftsmäßig und über Jahre hinweg finanzielle Mittel zu erbeuten. Das heißt, Cyberkriminalität wird heute als Produkt und Dienstleistung auf illegalen Marktplätzen angeboten. Durch Angriffe auf die IT-Systeme für polizeiliche Ermittlungen und Gerichtsverfahren können die Kriminellen sich zudem Vorteile in der Strafverfolgung verschaffen. Durch die wachsende Digitalisierung dürften zukünftig auch Smart City, Smart Factory, Systeme des Autonomen Fahrens, Flugsicherungssysteme, Heimrouter, Monitore, medizinische Hilfsgeräte und viele weitere Geräte Ziele von Botnetz-Attacken werden (Puchkov 2022, S. 29-32).

6 Fallstudien und Praxisbeispiele

Botnetze haben inzwischen Geschichte geschrieben, da dazu viele Beiträge in den Medien veröffentlicht wurden. Zwei bekannte Formen sollen nun vorgestellt werden. Außerdem werden Maßnahmen zur erfolgreichen Bekämpfung und Empfehlungen für die Eindämmung kurz zusammengefasst.

6.1 Analyse der bekannten Botnetze Zeus und Emotet

Das Zeus-Botnetz, auch Zbot oder ZeuS: genannt, wurde im Jahr 2007 erstmals gesichtet und für kriminelle Finanztransaktionen eingesetzt. Ursprünglich war es für Microsoft Windows programmiert, inzwischen ist es auch auf Android-Mobilgeräten zu finden. Obwohl im Jahr 2010 bekannt wurde, dass der ursprüngliche Initiator des Botnetzes das Projekt nicht weiterverfolgte, konnten sich durch die Veröffentlichung des Quellcodes im Jahr 2011 zahlreiche, neue Varianten verbreiten. Zeus war zunächst zentralisiert und ist später als Peer-to Peer-Lösung entwickelt worden, die zentralisiert wird, wenn kein Peer erreicht werden kann. Spätere Varianten kommen auch als Hybrid-Versionen vor. Zeus tritt durch einen Trojaner in Erscheinung, das heißt, er kommt mithilfe von Spam-Nachrichten oder Downloads, in denen Malware versteckt ist. Er versteckt sich auch in Online-Werbung oder auf Webseiten und wird beim Öffnen aktiviert. Das Exploit richtet zunächst ein Botnetz ein und dann geht es um das Abfangen von Anmeldedaten für die Nutzung von Online-Banking. Ermöglicht wird dies durch Keylogging und Überwachung von Webseiten. Die Malware ist in der Lage, zu erkennen, wenn ein Nutzer sich auf einer Webseite für Online-Banking einloggt und kann die Zugangsdaten mitlesen. Wenn die Malware sich auf Android-Geräten installiert hat, kann sie die Zwei-Faktor-Authentifizierung umgehen, die für das Anmelden beim Online-Banking einen Code auf ein Mobilgerät sendet. Die Attacken werden auch durch Social-Media-Kampagnen verbreitet, bei denen die Weiterleitung zu einer Webseite führt, die Malware installiert. Dabei können auch die Anmeldedaten für die genutzten Accounts kopiert werden, um von dort aus dann gefälschte Nachrichten zu verschicken. Das Zeus-Botnetz ist bis heute aktiv, um sich zu schützen, wird die Nutzung einer Anti-Virensoftware empfohlen. Mit dem Snort-IPS konnten in einer Simulation auf einem Rechner vorhandene Zeus-Botnetze erkannt werden (Belcic 2023, o. S.; BSI 2023, „Zeus“; Vormayr et al. 2017, S. 2782, Hasan; Sani 2022, S. 1-3).

Emotet ist ein Botnetz, das im Jahr 2014 erstmals entdeckt wurde und sich in IoT-Netzen verbreitet. Es wurde bekannt durch Angriffe auf die US-Präsidentschaftswahlen und Saudi Aramco, den größten, globalen Öl-Konzern, sein mutmaßliches Herkunftsland ist Russland. Es beherrscht verschiedene Arten von Angriffen, wobei es sich zunächst als Botnetz aufstellt und dann Bank-Zugangsdaten stiehlt, DDoS-Angriffe ausführt und Ransomware-

Erpressung betreibt. Die Angriffe beginnen über E-Mails, die Excel oder Word-Dateien im Anhang mitführen und beim Herunterladen das Öffnen von Makros fordern, wodurch sich die Power-Shell-Malware öffnet. Diese sorgt für eine schnelle Übernahme des gekaperten Netzwerks und die Steuerung über den C&C-Server (siehe Abb. 23; Garg et al. 2023, S. 912).

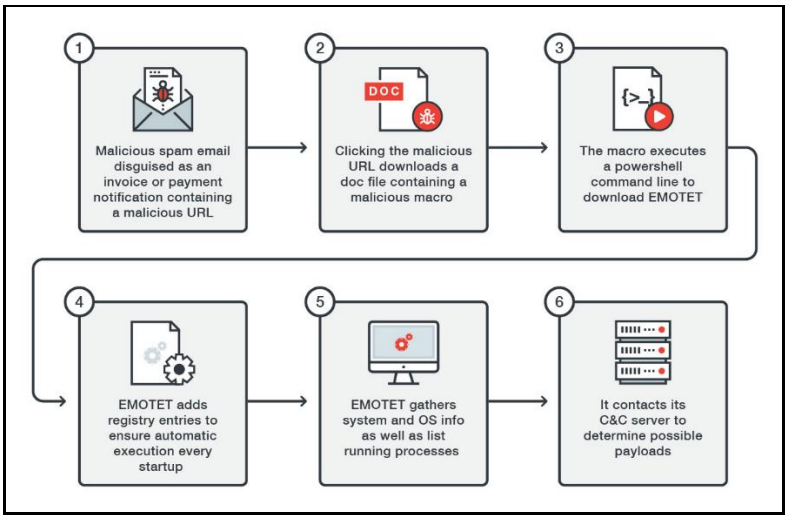

Abb. 23 – Emotet Botnet

(Quelle: Ladores 2017, o. S.)

Obwohl das Botnetz Emotet bereits mehrfach als stillgelegt betrachtet wurde, ist es inzwischen wieder aktiv. Durch spezielle Malware-Analysen können so komplexe Botnetze wie Emotet hinsichtlich ihres Aufbaus und der vorhandenen Informationen untersucht werden. Bei einer statischen Analyse von Emotet erfolgt zunächst eine Klassifizierung nach Merkmalen bereits analysierter Malware. Durch die Untersuchung der ausführbaren Dateien können Einblicke in die Funktionalitäten und die Urheber gewonnen werden. Mit dem Tool HxD, einem Hex-Editor, kann der PE-Header, also der Kopf-Bereich einer ausführbaren Windows-Datei angezeigt werden, wobei die Datei-Signatur sichtbar wird. Es ist beispielsweise erkennbar, dass der PE-Header als .exe- oder.dll-Format vorliegt. Durch eine String-Analyse können die lesbaren Zeichen und Wörter aus der Malware betrachtet werden. Anhand der IP-Adresse lassen sich URLs, Domänenbezeichnung und Registrierungsschlüssel erkennen, die Informationen können Aufschluss darüber geben, inwieweit die Datei schädlich ist. Das String-Befehlszeilen-Dienstprogramm zeigt auf, über welche Handlungsoptionen eine Malware verfügt. Cyberkriminelle können jedoch auch mit Absicht gefälschte Zeichenfolgen in den Code einfügen, um das Analysieren zu erschweren (Garg et al. 2023, S. 912).

Der Analyst kann außerdem prüfen, ob das Hostsystem mit dem Befehlszeilen-Dienstprogramm kompatibel ist. Die Funktionen der Malware können innerhalb der PowerShell eingesehen werden. Mit dem Tool Exeinfo PE lässt sich überprüfen, ob die Datei gepackt ist, was meist einen Hinweis auf das Vorliegen von Malware gibt. Eine Malware ist typischerweise in zwei Abschnitte unterteilt, den PE-Header und die Sections (siehe Abb. 24, links

blau). Der PE-Header besteht wiederum aus sechs Abschnitten (siehe Abb. 24, Mitte orange). Sie kann etwa einen DOS-Header haben, die sie als Binärdatei identifiziert. Der DOS-Stub gibt Aufschluss über die Kompatibilität des Betriebssystems. Besonders wichtig ist der optionale Header, da er die Einzelheiten der Subsysteme und die Einstiegspunkte aufzeigt. Aus dem PE-Header lassen sich im Ergebnis die Bibliotheken, Funktionsimporte, Subsysteme sowie Datum und Uhrzeit der Kompilierung entnehmen. Der Analyst lässt die Datei dann über einen Hash-Algorithmus laufen und erzeugt damit einen Fingerabdruck, durch den die Malware eindeutig identifizierbar ist und der auf einer Online-Datenbank hinterlegt werden kann, um so Informationen für andere Analysten bereitzustellen. Der Hash-Wert stellt sich auf jedem System gleich dar und ist konstant sowie unabhängig von der jeweiligen Architektur (Garg et al. 2023, S. 912-913). Durch die Analyse von Malware, die in Botnetzen wie Emotet verwendet wird, können also wertvolle Einblicke in die Vorgehensweise von Cyberkriminellen gewonnen werden, die das Auffinden und Abwehren von Angreifern und Attacken leichter machen (Garg et al. 2023, S. 914).

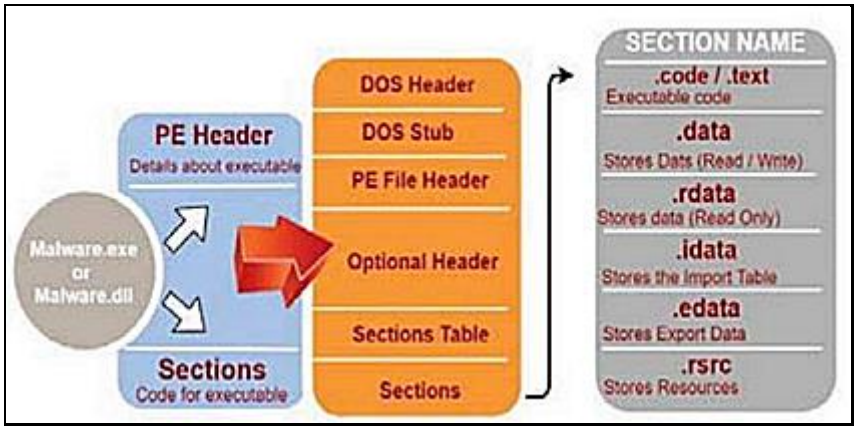

Abb. 24 – Aufbau einer Malware-Datei

(Quelle: Garg et al. 2023, S. 913)

6.2 Erfolgreiche Bekämpfungsmaßnahmen von Botnetzen

Bei der Erkennung und Abwehr von Botnetzen werden inzwischen gezielt digitale Technologien eingesetzt und von der Forschung sind bereits viele Modelle dazu vorgestellt worden. Ein IDS wird so eingerichtet, dass bei Verstößen gegen die Sicherheitsregeln und dem Erkennen böswilliger Aktivitäten Meldungen generiert und Protokolle erzeugt werden, im besten Fall werden diese gleich an einen Security-Analysten weitergeleitet, der die Tatbestände genauer untersucht. Dann erfolgt eine Klassifizierung der Aktivität, zum Beispiel als NIDS oder HIDS und die Feststellung, nach welcher Methode der Angriff erkannt wurde, etwa Anomalie basiert, signaturbasiert, spezifikationsbasiert, DNS-basiert oder Mining-basiert. Für diese Erkennung können Algorithmen und maschinelles Lernen eingesetzt werden. Werden Botnetze über IoT-Angriffe verbreitet, kommt die kollaborative Intrusion Detection zum Einsatz, wobei eine Reihe von Intrusion Detection Agents (IDAs) über

das Netzwerk verteilt arbeiten, denn die Geräte verfügen nur über wenig Speicherplatz für Sicherheitssoftware. Damit die Überwachung sich effizienter gestaltet, werden die Agents mit mehr Kapazitäten ausgestattet und im ganzen Netz verteilt (Nasir et al. 2023, S. 6).

Die Blockchain-Technologie besitzt die Eigenschaften der Unveränderlichkeit, Dezentralisierung, Transparenz, Sicherheit vor Manipulationen, Automatisierungen durch Smart Contracts und die Verwendung von Konsensmechanismen. Sie kann vor allem die signaturbasierte Erkennung optimieren und die Integration eines Trust Management Systems (TMS) ermöglichen. Dafür wird eine private Blockchain eingesetzt, zu der externe Angreifer keinen Zugang haben. Das Trust Management System schafft die Basis für die sichere Zusammenarbeit der zahlreichen Geräte. Dabei werden für jeden Knoten automatische Vertrauensbewertungen durchgeführt, basierend auf einer Anfangseinschätzung, dem individuellen Verhalten, dem Laufzeit-Feedback und dem lokalen Vertrauen sowie Einschätzungen, die von einzelnen Peers abgegeben werden. Auf der Grundlage der Gesamtbewertungen kann eine Vertrauensmatrix gebildet werden, die die Möglichkeiten zur Interaktion der einzelnen Knoten bestimmt. Um das IDS mit möglichen Angreifern vertraut zu machen, wird maschinelles Lernen mit öffentlichen Botnetz-Datensätzen eingesetzt, beispielsweise ISOT oder BOT IOT (Nasir et al. 2023, S. 6-7).

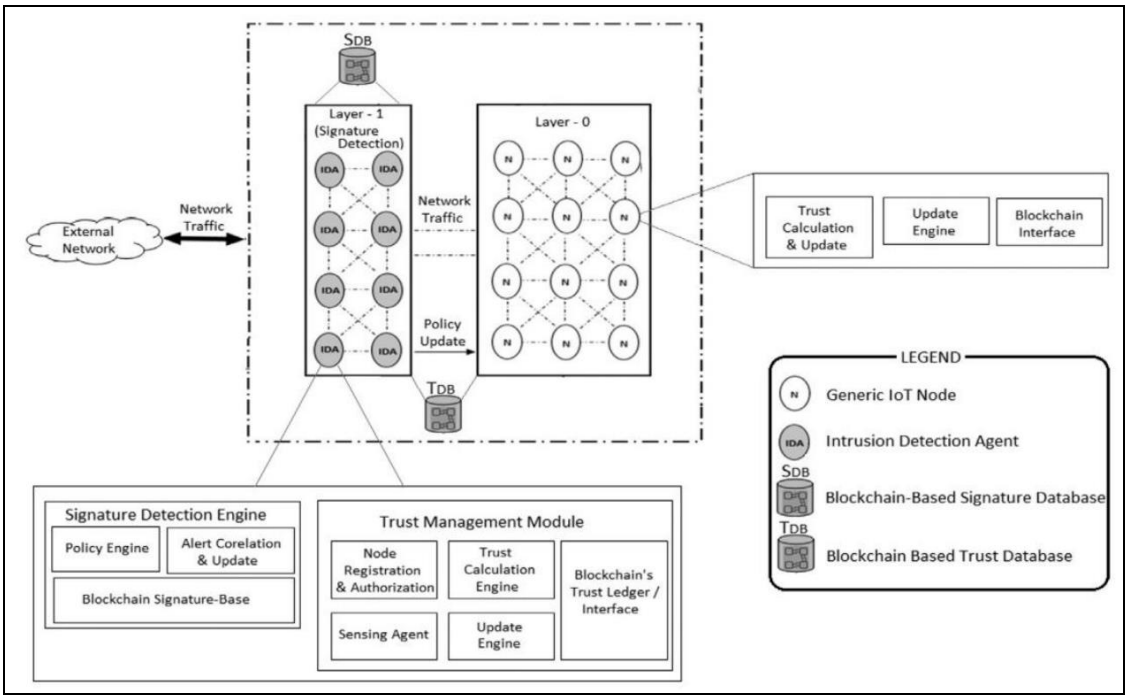

Abb. 25 – Framework zur Botnetz-Erkennung auf Geräteebene

(Quelle: Nasir et al., 2023, S. 11)

Nasir et al. (2023) haben ein Framework zur Botnet-Erkennung auf Geräteebene vorgestellt, das kollaborative Knoten einsetzt, um eine signaturbasierte Identifikation zu ermöglichen (siehe Abb. 25). Die kollaborative Umsetzung zeigt sich besonders wirksam bei IoT-Botnetzen, wie sie in den letzten Jahren zunehmend verbreitet werden, da es aufgrund

der begrenzten Kapazitäten der Geräte nicht ausreicht, die Sicherheitsmaßnahmen nur auf einem Gerät durchzuführen. Das Framework zeigt die generischen IoT-Knoten des Netzwerks, die Daten senden und empfangen können (Abb. 25, Layer 0), und mit Modulen für Trust Calculation, Blockchain Interface und Update-Erstellung ausgestattet sind (siehe Abb. 25, rechts oben). Die vorgeschalteten Intrusion Detection Agents (IDA; Abb. 25, Layer 1) verfügen über eine Signature Detection Engine (SDE) und die Trust Management Module (siehe Abb. 25, unten, links und Mitte). Sie bilden einen Schutzschild zwischen dem IoT und dem Datenverkehr mit externen Quellen. Die Agents verfügen im Gegensatz zu den anderen Geräten über genügend Speicherplatz, eine Signatur-Erkennungs-Software auszuführen. Sie sind auch für die Steuerung und Verwaltung des dezentralen Trust Management Moduls sowie die Registrierung und Autorisierung der Knoten zuständig. Sie nehmen zudem an der Ermittlung und Aktualisierung des Vertrauensstatus der Geräte teil, verwalten die Signaturdatenbank, die auf Basis einer Blockchain arbeitet, und verwalten die globale Bewertung der Knoten (Nasir et al., 2023, S. 10).

Das Trust Management Module aggregiert und interpretiert die globalen Vertrauenswerte und verfügt über die Engine, die für die Registrierung und Autorisierung der Knoten zuständig ist. Darüber hinaus verteilt sie die anfänglichen Vertrauenswerte, die neuen Knoten zugeschrieben werden. Ein Sensing-Agent-Submodul ist für die Steuerung des Trust Ledger Interface der Blockchain zuständig. Die Trust Calculation Engine erstellt die globale Reputation der Knoten und eine Update-Engine nimmt Aktualisierungen vor. Die wesentlichen Informationen des Netzwerks werden im Ledger-Speicher der Blockchain aufbewahrt, der die Funktionen von Reputationsmanagement und Erkennung von schädlichen Signaturen ausübt. Wenn es Knoten an Vertrauenswürdigkeit mangelt, kann das Sensing Agent Modul die Zusammenarbeit ablehnen. Das Ledger hat zwei wesentliche Funktionen: Es bewahrt die Trust Informationen zur Vertrauensbildung im Netzwerk auf und hält auch die Informationen über potenziell schädliche Signaturen bereit, auf deren Basis die Detektoren unter anderem Malware erkennen. Dafür werden die jeweiligen Hashs der Datenbanken ermittelt. Zusätzlich ist noch eine Policy Engine in den SDEs enthalten, sowie ein Alarmsystem, das die Meldung, Alarmaggregation, Normalisierung und Analyse von Ereignissen ausführt (Nasir et al. 2023, S. 10-11). Insgesamt lässt sich am Konzept von Nasir et al. (2023) erkennen, dass inzwischen durch innovative, digitale Technologien, wie maschinelles Lernen, KI und Blockchain, durchaus wirkungsvolle Systeme zur Botnetz-Abwehr bereitgestellt werden können, die neben der Verarbeitung und Analyse von Sicherheits-Ereignissen auch präventiven Schutz bieten. Dazu kommt der Vorteil, dass sich durch kollaborative Signature Detection Agents die wachsenden Bedrohungen für IoT-Netzwerke eindämmen lassen.

6.3 Empfehlungen für Unternehmen und Behörden

Die in dieser Untersuchung aufgezeigten Risiken durch Botnetz-Angriffe sind für Unternehmen und Behörden gleichermaßen alarmierend, die Beseitigung der Folgen kann mit

hohen Kosten, erheblichem Arbeitsaufwand und Reputationsverlusten einhergehen. Da auch für die Erkennung eines fortgeschrittenen Advanced Persistent Threat schon Expertise erforderlich ist, sollten Unternehmen und Behörden ein systematisches Cybersicherheits-Management betreiben. Dies beginnt mit einer allgemeinen Grundlage, wie etwa dem IT-Grundschutz nach dem Vorgehensmodell des BSI, für den eine Zertifizierung erworben werden kann. Darauf aufbauend kann der Standard der ISO 27001 zur IT-Sicherheit umgesetzt werden, der ebenfalls zertifizierbar ist (BSI 2020, o. S.).

Auch das US-amerikanische Cybersicherheits-Institut NIST hat ein Sicherheitskonzept entwickelt, das Cybersecurity Framework. Es umfasst die folgenden Schritte (NIST 2018, o. S.):

1. Identifizieren

Zum Identifizieren gehört zunächst die Identifikation kritischer Unternehmensprozesse und Vermögenswerte. Außerdem sind die Informationsflüsse zu dokumentieren und es sollten Richtlinien, Rollen und Verantwortlichkeiten festgelegt werden. Dann werden Bedrohungen, Schwachstellen und Risiken hinsichtlich der Vermögenswerte ermittelt (NIST 2018, S. 7).

2. Schützen

Der Bereich des Schützens umfasst die Einrichtung einer Zugriffsverwaltung, der Schutz sensibler Daten, die Durchführung von Backups, die Installation von hostbasierten Firewalls und die Nutzung von Sicherheitssoftware. Software ist regelmäßig zu aktualisieren und erkennbare Schwachstellen sollten beseitigt werden. Wichtig ist es auch, die Mitarbeiter zu schulen, damit sie ein Sicherheitsbewusstsein entwickeln und Verantwortung dafür tragen (NIST 2018, S. 7).

3. Erkennen

Zum Erkennen zählt es, Einheiten und Transaktionen im System aufzuspüren, die nicht autorisiert sind. Protokolle sollten gepflegt und im Hinblick auf Muster und Anomalien überwacht werden. Die regulären Datenströme des Unternehmens sollten bekannt sein, damit nicht-reguläre Datenflüsse bemerkt werden. Cybersicherheits-Ereignisse sollten erkannt, gemeldet, so weit wie möglich behoben und dann analysiert werden. Die Erfahrungen sollten als Lessons Learned für das künftige Sicherheits-Management ausgewertet und durch neue Maßnahmen etabliert werden (NIST 2018, S. 7).

4. Antworten

Zum Antworten ist es wichtig, dass die eingesetzten Reaktionspläne getestet und regelmäßig aktualisiert werden. Auch sollte eine Koordination der Pläne mit internen und externen Stakeholdern zur Verbesserung der Planung erfolgen (NIST 2018, S. 8).

5. Genesen

Zum Genesungsprozess nach einem Sicherheitsereignis sollte eine effektive Kommunikation mit den Stakeholdern betrieben werden. Auch sind Wiederherstellungs-Pläne anzulegen, wobei die Zugriffsrechte der einzelnen Teilnehmer auf spezifische Informationen zu verwalten sind. Die Öffentlichkeitsarbeit kann dazu beitragen, die Reputation einer Organisation zu erneuern, indem ein verantwortungsvoller Informationsaustausch erfolgt (NIST 2018, S. 8).

Wenn ein grundlegendes Sicherheitskonzept installiert wurde, kann ein individuell auf die Organisation zugeschnittenes Botnetz Intrusion Detection und Prävention System (IDPS) konzipiert werden, wie es beispielsweise das von Nasir et al. (2023) vorgestellt Konzept ist. Dabei werden zum einen Methoden des maschinellen Lernens und KI eingesetzt, um die Intrusion Detection Agents zu trainieren. Zum anderen kann zusätzlich eine Blockchain mit einem Trust Management System implementiert werden, um die wesentlichen Informationen sicher zu speichern und abzurufen. Dies bietet insbesondere hinsichtlich der in Organisationen stark wachsenden Anteile an IoT-Assets Vorteile. Da das Trust Management die Geräte aufgrund ihrer Datenlage einschätzen kann, wird das Betreiben schädlicher Aktivitäten im Netzwerk erschwert und der Sicherheitsstatus erhöht.

7 Zusammenfassung und Fazit

In diesem Abschnitt sollen die Ergebnisse der Untersuchung zusammengefasst und ausgewertet sowie die Forschungsfragen beantwortet werden.

7.1 Zusammenfassung und Reflexion der Ergebnisse

Die durchgeführte Untersuchung befasst sich mit einer speziellen Form von Cyberkriminalität: Den Botnetzen, die durch ein Netzwerk funktionaler, auf fremden Rechnern illegal eingenisteter Software-Roboter gekennzeichnet sind. Sie sorgen seit den 1990er Jahren durch ihre Aktivitäten für Schlagzeilen und haben seither schwerwiegende Schäden bei diversen Organisationen verursacht. Dafür wird insgeheim eine Schadsoftware auf die Rechner übertragen, woraufhin sich die Bots automatisch installieren. Das Ziel solcher Angriffe ist es, die ferngesteuerten Bots als Netzwerk zu steuern, über das dann umfassende Cybercrime-Aktivitäten ausgeübt werden.

Die Cyberattacken werden inzwischen von versierten IT-Spezialisten durchgeführt, die einen hohen Grad an Professionalität erreicht haben. Nicht selten werden sie dabei von internen oder ehemaligen Mitarbeitern der Organisationen unterstützt, die über Zugangsparameter zum Unternehmensnetzwerk verfügen. Die Angriffe folgen einer Kill-Chain, vom Ausspähen über das Bewaffnen, bis zum Einnisten auf den fremden Systemen und schließlich stellen sich die Botnetze auf hunderten oder gar tausenden von Rechnern oder Geräten auf und können so komplexe Attacken ausführen. Viele der inzwischen bekannt gewordenen Botnetze konnten ihre Aktivitäten jahrelang vor den Augen der betroffenen Organisationen und der Kriminal-Ermittler verbergen, bis es endlich gelang, sie stillzulegen. Meist fahren die Aktivisten dabei zweigleisig, indem sie einerseits mit den von ihnen kontrollierten Mengen von Bots schädliche Transaktionen gegen ihre Feinde ausführen, was ihnen enorme Schlagkraft verleiht. Andererseits ziehen sie durch das Ausspähen von Bankdaten finanzielle Mittel ab, mit denen sie ihre technologisch aufwendigen Attacken finanzieren.

Es lassen sich verschiedene Formationen von Botnetzen unterscheiden, bei denen unterschiedlich viele Angreifer und Zielobjekte einbezogen werden. Die Attacken von Botnetzen erfolgen verdeckt, eine häufig gewählte Form ist das Infizieren einer Webseite, über die beim Öffnen eine Malware auf dem System installiert wird. Um den Nutzer dazu zu bringen, die schädliche Webseite zu öffnen werden Methoden wie Social Engineering und Pishing eingesetzt. Dabei wird dem Nutzer Vertrauenswürdigkeit vorgetäuscht, indem bekannte Elemente der echten Webseite angezeigt werden, hinter denen sich die Malware verbirgt. Gerne werden auch E-Mail-Anhänge oder Anhänge in Social-Media-

Kommunikation mit der Malware versehen, die sich, wenn der Nutzer die Anhänge öffnet, automatisch herunterlädt und auf dem Rechner installiert. Für das Knacken von Zugangsdaten, wie Passwörtern, werden Brute-Force-Angriffe ausgeführt, bei denen ein automatisiertes Ausprobieren nach einem Wörterbuch erfolgt. Dies lässt sich durch Grafikprozessoren inzwischen erheblich beschleunigen. Besonders schwerwiegend sind Advanced-Persistent-Threat-Angriffe (APT), wobei die Initiatoren zunächst die Ressourcen, offenen Ports und Schwachstellen des Systems auskundschaften. Dann greifen sie an, indem sie sich auf dem Rechner installieren, integrieren und verstecken, um von dort aus verdeckt, über lange Zeiträume hinweg ihre Aktivitäten ausüben zu können. Die Besitzer der Netzwerke bemerken häufig gar nicht oder erst spät, dass ihr System kompromittiert wurde. Weitere mögliche Angriffsformen sind Man-in-the-Middle-Attacken, bei denen die Kommunikation abgefangen wird und Supply-Chain-Angriffe, wobei Softwareupdates abgefangen und infiziert werden. Der typische Botnetz-Angriffsvektor ist die DDoS-Attacke, bei der die Systeme des Opfers durch eine Flut von Anfragen überlastet werden und dadurch Dienste zum Erliegen kommen. Bei Ransom-Attacken werden die Systeme durch Verschlüsselung gesperrt und erst gegen die Entrichtung eines Lösegeldes wieder freigegeben. Insgesamt gesehen können Botnetze also erheblichen Schäden in materieller Hinsicht und bei der Reputation ihrer Opfern verursachen, sodass sich gefährdete Organisationen mit diesem Risiko befassen und Gegenmaßnahmen ergreifen sollten.

Um den Cyberkriminellen aber auf die Schliche zu kommen, ist es zunächst wichtig, sich Informationen über die Architekturen und Strukturen solcher Netzwerke zu verschaffen. Die frühen Formen von Botnetzen aus der Mitte der 1990er Jahre verwendeten meist eine zentrale Architektur, das heißt, es gab einen einzelnen C&C-Server und eine Menge von Bots, die von ihm gesteuert wurden. Da sich ein solches Netz durch die Eliminierung des C&C-Servers mit einem Schlag ausgeschaltet werden kann, kamen die Peer-to-Peer-Netze auf, bei denen jeder Bot als Sender und Empfänger dienen kann, was das Ausschalten erschwert. P2P-Botnetze haben jedoch den Nachteil, dass viele Netzwerkverbindungen herzustellen sind, die sich leicht erkennen lassen und durch die Anzahl der TCP-Sockets begrenzt werden. Wenn jedoch die Funktionalitäten eingeschränkt werden und nicht alle Bots direkt erreichbar sind, müssen Implementierungen anhand von Peer-Listen erfolgen, die wiederum Angriffsfläche bieten. NAT-Knoten und Superknoten können dann eingesetzt werden, wenn das Ziel des Angriffs sich durch eine Firewall oder NAT schützt. Einige der bekannten Netze besitzen hybride Strukturen, nutzen also zentrale und Peer-to-Peer-Steuerung. Eine besonders schwer auszuschaltende Variante sind Fast-Flux-Botnetze, sie nutzen Technologien zur Verschleierung ihrer IP-Adressen und Domainnamen.

Ein wichtiges Instrument, das dabei behilflich sein kann, Botnetze zu verstehen und auszuschalten, ist ihre Kommunikation. Es können verschiedene Kommunikationsprotokolle verwendet werden, beispielsweise IRC, HTTP, SMB, P2P oder auch individuelle Formen. In jedem Fall ist die Analyse der Protokolle für die Erkennung von Botnetzen aufschlussreich: Wenn Protokolle innerhalb des Netzwerks sich stark von den regulären Protokollen unterscheiden, kann dies ein Hinweis auf Botnetz-Aktivitäten sein. Schwer erkennbar ist

es hingegen, wenn die übliche Internetkommunikation oder Social Media Accounts eingesetzt werden, da sich dann keine Auffälligkeiten erkennen lassen. Bei APT-Angriffen ziehen die Angreifer alle Register, indem sie Webseiten infizieren, die von ihren Opfern besucht werden müssen, das Botnetz aufbauen und dann verschiedene Formen von Malware für ihre diversen Ziele einsetzen. Heutige Botnetze verfügen über zahlreiche Ressourcen: Sie nutzen eigene Rechner, gemietete und gekaperte IT, Clouds, Shared Hosting, Cybercrime-as-a-Service, Social Media Accounts, IoT-Geräte und mehr, wodurch sich ihnen ein erheblicher Aktionsspielraum bietet. Viele der neueren Versionen setzen diversifizierte Plattformen und intelligente Steuerung ein und nutzen auch mobile Netzwerke. Außerdem kombinieren sie verschiedene Formen von Malware, Strategien und Betrugsmodellen, was ihre Widerstandfähigkeit und Schlagkraft erhöht.

Um sich in fremden Ressourcen zu bewegen und außerhalb zu agieren, setzen Botnetze Verschleierungs-Taktiken ein. Sie arbeiten mit Verschlüsselungen, wie Kryptografie und Hash-Werten, spähen ihre Opfer durch Wardriving aus, fangen Kommunikation ab, verändern Daten und blockieren gezielt die Kapazitäten des Angriffsziels. Mit Domain und IP-Flux können sie ihren Standort und die Domain verschleiern und nutzen zunehmend auch Verfahren des maschinelles Lernen (ML), Künstliche Intelligenz (KI) und Blockchain-Technologien, um sich zu tarnen, sowie Kryptowährungen für Finanztransaktionen. Durch Steganografie verstecken sie Botschaften in den Datensätzen der Opfer, um miteinander zu kommunizieren und Informationen zu hinterlegen.

Damit Organisationen den raffinierten Strategien von Botnetzen etwas entgegensetzen können, wurden Intrusion-Detection- und Intrusion Prevention-Systeme (IDS/IPS) entwickelt. Diese sind zunächst darauf ausgerichtet, Hosts und Netzwerke zu scannen, um dort frühzeitig die Spuren der Angreifer zu entdecken und sie bereits in der frühen Inkubationsphase unschädlich zu machen. Sie suchen nach Anomalien, bekannten Signaturen oder Spezifikationen und können die Systeme auch auf der Basis von DNS oder Mining prüfen. Durch den Einsatz von Honeypots und Honeynets werden für potenzielle Angreifer Köder ausgeworfen, die von den eigentlichen Systemen ablenken und über die sich Ressourcen der kriminellen Akteure ausspionieren lassen, um direkten Einblick in ihre Machenschaften zu erhalten. Dies geschieht auf der Basis von Software-Simulationen und kann in vielen Fällen schon mit geringen Ressourcen umgesetzt werden.

Um die Botnetz-Erkennung zu optimieren, werden inzwischen Deep Learning als Form des ML und Neuronale Netze eingesetzt. Damit ist die gezielte Erkennung von bekannten Botnetzen möglich, indem die Detektoren mit dazugehörigen Datensätzen trainiert werden. Aus dem IDS lässt sich dann ein IPS entwickeln, indem der Datenverkehr analysiert wird, und Anomalien, Regelverletzungen und Verhaltensweisen untersucht werden. Durch KI und ML werden die Sicherheitslösungen stetig weiterentwickelt und können dann auf der Basis ihres gesammelten Wissens auch neue Datensätze im Hinblick auf schädliche Aktivitäten überprüfen. Anhand der beispielhaft vorgestellten IDS/IPS-Lösung Snort kann gezeigt werden, dass sich damit ein erheblicher Anteil von Angriffen präventiv erkennen

lässt. Allerdings erfordert dies eine sorgfältige Konfiguration der Software und des zugehörigen Netzwerks.

Auf juristischer Ebene lässt sich feststellen, dass Botnetz-Kriminalität massiv fortschreitet, große Schäden verursacht und nur selten tatsächlich geahndet werden kann. Die Gründe dafür liegen in den fortgeschrittenen Technologien, die Angreifer nutzen, dem relativ starren Rechtssystem und der Schwierigkeit, rechtskräftige Beweise zu erbringen. Die Kreise der Cyberkriminalität ziehen sich inzwischen bis in die Kommunikationssysteme von Privatpersonen, was durch die Corona-Pandemie und die Arbeit im Homeoffice noch befeuert wurde. Empfohlen werden kann daher die Einrichtung von systematisch arbeitenden Sicherheits-Lösungen und die Ausrichtung an Standards, wie dem BSI-Grundschutz und der ISO 27001. Für große Organisationen empfiehlt sich die Anwendung eines Cyber-Security-Frameworks, wie es vom US-amerikanischen Institut NIST vorgestellt wurde. Auch das Melden und der Informationsaustausch von IT-Sicherheitsvorfällen spielt eine wichtige Rolle bei der Botnetz-Bekämpfung.

Als Trend lässt sich eine zunehmende Verbreitung von Botnetzen über IoT-Geräte erkennen, für die besondere Sicherheitsmaßnahmen erforderlich sind. Auch kann die Dienstleistung „Cyberkriminalität“ im Darknet verzeichnet werden, die es selbst technologisch unerfahrenen Hackern ermöglicht, sich ein Botnetz zu mieten oder zu kaufen und damit kriminelle Aktivitäten auszuüben. Bekannte Botnetze, wie Zeus und Emotet, haben gezeigt, wie beharrlich, versiert und resistent die Aktivitäten von Botnetzen umgesetzt werden, wobei es in den meisten Fällen darum geht, sich materiell bzw. finanziell zu bereichern. Durch gezielte Analysen von Botnetz-Software können aufschlussreiche Erkenntnisse hinsichtlich der Art, Qualität und Herkunft gewonnen. Ein aktuelles Modell für die Gestaltung eines IDS/IPS-Systems zeigt beispielhaft, wie durch die Verbindung moderner digitaler Entwicklungen, etwa maschinelles Lernen, KI und Blockchain in Verbindung mit einem Trust-Management für IoT-Geräte, ein wirkungsvolles und schlagkräftiges IDPS entwickelt und eingesetzt werden kann.

Die vorliegende Untersuchung bringt insgesamt nahe, dass Botnetz-Kriminalität auf dem Vormarsch ist und dass Organisationen ihre Ressourcen schützen müssen, um diesen Aktivitäten nicht zum Opfer zu fallen. In diesem Umfeld ist Detektion und Prävention die bessere Wahl, denn die Akteure werden nur selten gefasst uns können noch seltener zur Rechenschaft gezogen werden. Selbst wenn es zu einer Verurteilung kommt, wird der verursachte Schaden den betroffenen Organisationen kaum ersetzt werden, da solche Risiken in der Regel bisher kaum versichert werden können.

Umso erfreulicher erscheint es, dass inzwischen die Sicherheitslösungen in diesem Bereich beachtliche Fortschritte gemacht haben. Moderne IDPS-Systeme bieten eine Verbindung von ML und KI, die auf Basis von bekannter Malware trainiert und dann weiterentwickelt werden, bis sie ihre Funktionalität auch auf neue Datensätze anwenden können. Das Ausspionieren der Angreifer mit Honeypots und Honeynets eignet sich dazu, möglichst viele Informationen über die Gegner zu sammeln. Die daraus gewonnenen

Erkenntnisse werden unmittelbar für das Trainieren der IDPS-Algorithmen eingesetzt, wodurch die Möglichkeiten der Prävention sich stetig erweitern. Ebenso ist eine frühzeitige Alarmierung und das unmittelbare Ergreifen von Abwehrmaßnahmen von Bedeutung, um Schadenbegrenzung zu betreiben. Sicherheitsorganisationen wie das BSI tragen dazu bei, dass Angriffe gemeldet und Informationen über Schadsoftware veröffentlicht werden. So können die Sicherheitsstandards kontinuierlich vorangetrieben werden, was die allgemeine Sicherheit erhöht.

7.2 Beantwortung der Forschungsfragen

Die im ersten Abschnitt gestellten Forschungsfragen sollen nun beantwortet werden.

1. Wie können Unternehmen und öffentliche Verwaltungsstellen ihre IT-Systeme wirksam gegenüber Botnetz-Attacken schützen?

Die Organisationen sollten ein systematisches Sicherheitssystem aufbauen, wie es beispielsweise durch den BSI-Grundschutz oder die ISO 27001 aufgezeigt wird. Das komplexe Framework des NIST kann ebenfalls dazu dienen, die schrittweise Entwicklung eines umfassenden Sicherheitskonzeptes vorzunehmen. Für die spezielle Abwehr von Botnetzen kann auf dieser Basis ein IDS/IPS-System wie es beispielsweise Snort bietet, eingesetzt werden. Mit einer zielgerichteten Netzwerkkonfiguration und der Abstimmung des IDPS auf diese kann ein weitreichender Schutz gegenüber Botnetzen erreicht werden.

2. Welche Chancen ergeben sich dadurch für sie?

Organisationen, die ihr Sicherheitssystem effektiv aufgestellt haben, können die wirtschaftlich schwerwiegenden Folgen von Cyberattacken präventiv abwehren und sich somit ganz auf ihre strategischen Ziele konzentrieren sowie ihre Wertschöpfungskette optimieren. Sie können digitale Technologien nutzen und von einer umfassend aufgestellten IT-Organisation profitieren, ohne dabei befürchten zu müssen, dass ihre Systeme kompromittiert werden. Damit sind auch Organisationsgeheimnisse, sensible Informationen und Knowhow vor unberechtigtem Zugriff geschützt.

3. Welche Herausforderungen sind damit verbunden und wie können sie überwunden werden?

Die Aufstellung eines solchen Sicherheitssystems erfordert Expertise, Mitarbeiterentwicklung und benötigt entsprechende Ressourcen. Es kann auch nur schrittweise aufgebaut werden und ist mit einem weitreichenden Changemanagement zu verbinden. An erster Stelle steht dabei, einen Schutzstatus nach einem Standard oder Framework einer damit befassten Institution, wie dem BSI oder dem NIST, herzustellen. Dafür muss die IT-Organisation auf den State-of-the-Art gebracht werden, die Systeme müssen zentral organisiert, harmonisiert und kontrolliert werden. Veraltete Hard- oder Software, die möglicherweise Sicherheitslücken enthält muss gegen neue Lösungen ausgetauscht werden.

Siloorganisation muss durch Netzwerkorganisation ersetzt werden und eine übergeordnete Netzwerk-Administration ist für die Überwachung und Steuerung der Systeme einzusetzen. Auch müssen die Mitglieder der Organisation geschult werden, um ein Sicherheits-Bewusstsein zu erlangen und verantwortlich zu handeln. Ein Zugriffs- und Rechte-Management, das für Authentifizierung und Autorisierung zuständig ist, muss implementiert werden. Für die Entwicklung eines IDS/IPS ist die Nutzung einer geeigneten Software und die entsprechende Anpassung an das Netzwerk erforderlich, was nur durch qualifizierte IT-Spezialisten umgesetzt werden kann.

4. Welche Empfehlungen können Unternehmen und öffentlichen Stellen gegeben werden, um eine entsprechende Sicherheitsstrategie umzusetzen?

Die erste Empfehlung ist die Einrichtung eines IT-Sicherheitsmanagements nach einem anerkannten Standard, wie ISO 27001 oder NIST-Framework, mit allen bereits genannten Maßnahmen hinsichtlich der Aufstellung der Ressourcen, Changemanagement und Entwicklung der Mitarbeiter.

Die zweite Empfehlung besteht in der Auswahl und Einrichtung einer IDS/IPS-Software, wie sie etwa Snort im Bereich Open Source bietet. Für die Konfiguration des Netzwerks und des IDPS sind versierte IT-Experten einzusetzen. Falls die Organisation nicht über eigene Fachkräfte verfügt, können externe Berater hinzugezogen werden. Dabei kann das Framework für IoT von Nasir et al. (2023) als Vorlage für die Architektur des Abwehrsystems dienen. Es erscheint sinnvoll, das eigentliche Netzwerk durch eine Schicht von Signature Detection Agents (SDEs) zu schützen, die mit einer erhöhten Speicherkapazität ausgestattet sind und so eine umfangreichere Sicherheitssoftware aufnehmen können. Auf Basis einer Blockchain kann dann ein Trust Management System entwickelt werden, was den Teilnehmern des Netzwerks einen Vertrauensstatus zuweist, auf den sich die Genehmigung von Transaktionen im Netzwerk stützt. Das hat den Vorteil, dass auch neuere Formen von Botnetzen, die auf die Besetzung von IoT-Geräten abzielen, von den SDEs wirksam geschützt werden können. Auffällige Elemente des Netzwerks werden durch das Trust Management System erkannt und durch den daraufhin zugeteilten, niedrigen Vertrauenswert von schädlichen Aktivitäten abgehalten.

Die dritte Empfehlung ist die Schulung der gesamten Organisation im Hinblick auf das Verhalten und den Umgang mit IT-Sicherheitsthemen. Mitarbeiter können auch unbeabsichtigt Internet-Kriminellen in die Hände arbeiten, wenn sie nicht sensibilisiert hinsichtlich der Sicherheitsthemen sind.

Die vierte Empfehlung ist das Melden und die Analyse jedes Sicherheitsvorfalls, wobei zu klären ist, wie es dazu gekommen ist, welche Personen verantwortlich sind, welche Schäden sich ergeben, wie der Schaden zu beheben ist und wie ein ähnlicher Vorfall künftig ausgeschlossen werden kann.

Die fünfte Empfehlung ist es, IT-Risiken im Rahmen des organisationalen Risikomanagements zu berücksichtigen, da hier finanzielle Risiken in beträchtlicher Höhe bestehen, für die im Schadensfall möglicherweise niemand haftbar gemacht werden kann.

7.3 Implikationen und Ausblick

Insgesamt konnten in dieser Untersuchung wertvolle Erkenntnisse zur Vorgehensweise, Erkennung und Prävention von Cyberkriminalität durch Botnetze gewonnen werden. Das Thema wurde anhand der bestehenden Fachliteratur recherchiert und es lässt sich feststellen, dass die Quellenlage in diesem Bereich von den 1990er Jahren bis heute gut abgedeckt ist. Auch zum neueren Phänomen der IoT-Botnetze sind aktuelle Forschungsbeiträge vorhanden. Ein Bereich, der von dieser Untersuchung nicht erfasst wird, ist die detaillierte Entwicklung eines Trust Management Systems auf Basis einer Blockchain. Auch könnten Tests mit weiteren IDPS-Systemen, wie Suricata oder SolarWinds, durchgeführt werden. Dies scheint für zukünftige Forschungsansätze zur weiteren Entwicklung des Themas sinnvoll.

8 Literaturverzeichnis

Aathi Oli S. et al. (2018). *Aathi Oli S.; Mohammed Raeesul Irfan; Vijayalakshmi - Title: Review Paper on Phishing Attacks.* Abgerufen am 01. 06 2023 von Engpaper.com: https://www.engpaper.com/download/review-paper-on-phishing-attacks.pdf

Agyepong et al. (2018). *Agyepong, Enoch; Buchanan, William J.; Jones, Kevin - Detection of Algorithmically Generated Malicious Domain.* Abgerufen am 21. 06. 2023 von Researchgate: https://www.researchgate.net/publication/325714929_Detection_of_Algorithmically_Generated_Malicious_Domain

Akamai. (2023). *Akamai - Was ist ein DDoS-Angriff?* Abgerufen am 19. 06. 2023 von akamai.com: https://www.akamai.com/de/glossary/what-is-ddos

Belcic. (2023). *Belcic, Ivan - Was ist der Zeus-Trojaner?* Abgerufen am 10. 07. 2023 von avast.com: https://www.avast.com/de-de/c-zeus

Bhardwaj. (2022). *Bhardwaj, Rashmi - Honeypot vs Honeynet: Complete Guide.* Abgerufen am 21. 06. 2023 von ipwitheas.com: https://ipwithease.com/honeypot-vs-honeynet-complete-guide/

BKA. (2023). *BKA- Bundeskriminalamt Deutschland.* Abgerufen am 08. 07. 2023 von BKA.de: Bka.de

BSI. (2020). *BSI - Bundesamt für Sicherheit in der Informationstechnik - Informationssicherheit mit System - Der IT-Grundschutz des BSI.* Abgerufen am 12. 07. 2023 von BSI Bund.de: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/sonstiges/Informationssicherheit_mit_System.pdf?__blob=publicationFile&v=3

BSI. (2023). *BSI - Deutschland - Digital - Sicher.* Abgerufen am 08. 07. 2023 von BSI.bund.de: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html

Carle/Schmidt. (2009). *Carle, Georg; Schmitt, Corinna -.* Abgerufen am 29. 05. 2023 von net.in.tum.de: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2009-04-1.pdf

Dhinnesh/Sundareswaran. (2018). Dhinnesh, Navin; Sundareswaran, N. - Botnet Life Cycle and Topologies. *International Journal of Pure and Applied Mathematics, Volume 119, No. 17, 2018, S. 421-429*, S. 421-429.

Dreo et al. (2012). *Dreo, Gabi; Golling, Mario; Stelte, Björn - Ausgewählte Themen der IT-Sicherheit.* Abgerufen am 29. 05. 2023 von gbv.de: https://www.gbv.de/dms/tib-ub-hannover/783131534.pdf

Etheridge. (2023). *Etheridge, Emrick - Trends und Prognosen zur Informationssicherheit.* Abgerufen am 07. 07. 2023 von Dataguard.de: https://www.dataguard.de/expert-report-2023-information-security

Franz/Pfitzmann. (1998). Franz, Elke; Pfitzmann, Andreas - Einführung in die Steganographie und Ableitung eines neuen Stegoparadigmas. *Informatik-Spektrum, 21:183-193 (1998)*, S. 183-193.

Garg et al. (2023). *Garg, Umang; Kumar, Santosh; Ghanshala, Mridul - Analysis and Categorization of Emotet IoT Botnet.* Abgerufen am 10. 07. 2023 von eeexplore.ieee.org: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10085302

Garip et al. (2019). *Garip, Mevlut Turker; Reiher, Peter; Gerla, Mario - RIoT: A Rapid Exploit Delivery Mechanism against IoT Devices Using Vehicular Botnets.* Abgerufen am 19. 06. 2023 von ieeexplore.ieee.org: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8891228

Geeksforgeeks. (2022). *Geeksforgeeks - How to Prevent Backdoor Attacks?* Abgerufen am 19. 06. 2023 von Geeksforgeeks: https://www.geeksforgeeks.org/how-to-prevent-backdoor-attacks/

Georgoulias et al. (2023). *Georgoulias, Dimitrios; Pedersen, Jens Myrup; Falch, Morten; Vasilomanolakis, Emmanouil - Botnet Business Models, Takedown Attempts, and the Darkweb Market: A Survey.* Abgerufen am 16. 06. 2023 von ACM Computing Surveys, Vol. 55, No. 11, Article 219. Publication date: February 2023.: https://dl.acm.org/doi/10.1145/3575808

Golem. (2023). *Golem - Hacker.* Abgerufen am 31. 05. 2023 von Golem.de: https://www.golem.de/specials/hacker/

Halang/Fitz. (2018). *Halang, Wolfgang; Fitz, Robert - Nicht hackbare Rechner und nicht brechbare Kryptographie.* Berlin: Springer Vieweg.

Hasan/Sani. (2022). *Hasan, Hanis B. A.; Sani, Razeli Bin -.* Abgerufen am 10. 07. 2023 von Researchgate.net: https://www.researchgate.net/profile/Hanis-Basira-2/publication/365632739_Detection_Of_Zeus_Botnet_Traffic_Using_Snort_In_Simulated_Virtual_Network_Environment/links/637c345c1766b34c54454f0c/Detection-Of-Zeus-Botnet-Traffic-Using-Snort-In-Simulated-Virtua

Holz. (2009). *Holz, Thorsten - Tracking and Mitigation of Malicious Remote Control Networks.* Abgerufen am 29. 05. 2023 von madoc.bib.uni-mannheim.de: https://madoc.bib.uni-mannheim.de/2330/1/dissertation-holz.pdf

Holz. (2009a). *Holz, Thorsten - Verfolgen und Abschwächen von Malicious Remote Control Networks.* Abgerufen am 29. 05. 2023 von dl.gi.de: https://dl.gi.de/handle/20.500.12116/33659

Kaspersky. (2023). *Kaspersky - Was ist ein Brute-Force-Angriff?* Abgerufen am 31. 05. 2023 von Kaspersky.de: https://www.kaspersky.de/resource-center/definitions/brute-force-attack

Khattak et al. (2014). *Khattak, Sheharbano; Ramay, Naurin Rasheed; Khan, Kamran Riaz; Syed, Affan A.; Khayam, Syed Ali - A Taxonomy of Botnet Behavior, Detection, and Defense.* Abgerufen am 15. 06. 2023 von IEEE Communications Surveys & Tutorials, Vol. 16, No. 2 Second Quarter 2014: https://ieeexplore.ieee.org/abstract/document/6616686?casa_token=S1lTOMUXIzYAAAAA:N38GUVGDh3m14rXTSrGp6MLp4XSN-fMcvyJVpe6QBJMOzacHF8st6-2Ba7IzUBA7AeAePVXL3A

Laass. (2011). *Laass, Matthis - Botnetze: Aufbau, Funktion & Anwendung.* Abgerufen am 29. 05. 2023 von Researchgate.net: https://www.researchgate.net/publication/263842949_Botnetze_Aufbau_Funktion_Anwendung

Ladores. (2017). *Ladores, Don Ovid - Emotet Returns, Starts Spreading via Spam Botnet.* Abgerufen am 10. 07. 2023 von Trendmicro.com: https://www.trendmicro.com/de_de/research/17/i/emotet-returns-starts-spreading-via-spam-botnet.html

Latto. (2023). *Latto, Nica - Was ist ein Keylogger?* Abgerufen am 30. 05. 2023 von Avast.com: https://www.avast.com/de-de/c-keylogger

Li et al. (2021). *Li, Ruidong; ; Zheng, Minjiao; Bai, Donglin; Chen, Zhengduo - SDN Based Intelligent Honeynet Network Model Design and Verification.* Abgerufen am 21. 06. 2023 von ieeexplore.ieee.org: https://ieeexplore.ieee.org/document/9611668

Lubacz et al. (2014). *Lubacz, Józef; Mazurczyk, Wojciech; Szczypiorski, Krzystof - Principles and overview of network steganography.* Abgerufen am 19. 06. 2023 von ieeexplore.ieee.org.

Luber/Schmitz. (2018). *Luber, Stefan; Schmitz, Peter - Definition Backdoor - Was ist eine Backdoor?* Abgerufen am 16. 06. 2023 von Security-Insider.de: https://www.security-insider.de/was-ist-eine-backdoor-a-676126/

Lutkevich et al. (2021). *Lutkevich, Ben; Clark, Casey; Shea, Sharon - Definition - whaling attack (whaling phishing).* Abgerufen am 01. 06. 2023 von Techtarget: https://www.techtarget.com/searchsecurity/definition/whaling

Maier/Korolov. (2022). *Maier, Florian; Korolov, Maria - Was ist ein Botnet?* Abgerufen am 30. 05. 2023 von csoonline.com: https://www.csoonline.com/de/a/was-ist-ein-botnet,3673859

Misha/Dixit. (2018). *Misha, Abhishek; Dixit, Abishek - Resolving Threats in IoT: ID Spoofing to DDoS.* Abgerufen am 19. 06. 2023 von ieeexplore.ieee.org: https://ieeexplore.ieee.org/document/8493729

Mohd Dollah et al. (2018). *Mohd Dollah, R. F., M. A., F., Arif, F., Mas'ud, M. Z., & Xin, L. K. - Machine Learning for HTTP Botnet Detection Using Classifier Algorithms.* Abgerufen am 21. 06. 2023 von jtec.utem.edu.my: https://jtec.utem.edu.my/jtec/article/view/3591/2484

Nasir et al. (2022). *Nasir, Muhammad Hassan; Khan, Muhammad Mubashir; Arshad, Junaid - A Quantitative Assessment of Emerging Trends in IoT Botnet Attacks.* Abgerufen am 08. 07. 2023 von ieeexplore.ieee.org: https://ieeexplore.ieee.org/abstract/document/10100587?casa_token=UBUjInbG5PkAAAAA:K2OqF2JcfBanqCFjLpNWRJaIRO_SpiV2aMMnyUNGFAWDkrsuNWd_88k_tbfkNCO3s8rgR-mugg

Nasir et al. (2023). *Nasir, Muhammad Hassan; Arshad, Junaid; Khan, Muhammad Mubashir - Collaborative device-level botnet detection for internet of things.* Abgerufen am 11. 07. 2023 von open-access.bcu.ac.uk: https://www.open-access.bcu.ac.uk/14223/

Nazario/Holz. (2008). *Nazario, Jose; Holz, Thorsten - As the Net Churns: Fast-Flux Botnet Observations.* Abgerufen am 01. 06. 2023 von ieeexplore.ieee.org: https://ieeexplore.ieee.org/abstract/document/4690854?casa_token=cxl-ySv9nYEAAAAA:9VLhLrbOqi_OpedTxEXuJraBvznyMCJzhTiCuy_GWG9zLUhf_ezgW4etfj0a1X2cWwU36nIZ2Q

NIST. (2018). *NIST - Cybersecurity Framework.* Abgerufen am 29. 06. 2023 von NIST.gov: https://www.nist.gov/cyberframework/framework

Peters. (2022). *Peters, Kristina - Cyberkriminalität - Aktuelle Herausforderungen für Polizei, Staatsanwaltschaften, Gerichte und Wissenschaft.* Abgerufen am 07. 07. 2023 von epub.ub.uni-muenchen.de: https://epub.ub.uni-muenchen.de/92172/1/Peters_Cyberkriminalitaet.pdf

Plickert. (2023). *Plickert, Janine - Was ist eigentlich Kryptographie?* Abgerufen am 19. 06. 2023 von Gdata.de: https://www.gdata.de/ratgeber/was-ist-eigentlich-kryptographie

Pohlmann. (2022). *Pohlmann, Norbert - Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung.* Wiesbaden: Springer Vieweg.

Puchkov. (2022). *Puchkov, Denis - Main Trends in the Development of International Crime in the Implementation of Cybertechnologies; Y. Liu et al. (eds.), Cybercrimes and Financial Crimes in the Global Era.* Singapore: Springer Nature Singapore Ltd.

Schmidt. (2007). *Schmidt, Jürgen - Hydra der Moderne - Die neuen Tricks der Spammer und Phisher.* Abgerufen am 01. 06. 2023 von Heise.de: https://www.heise.de/hintergrund/Hydra-der-Moderne-Die-neuen-Tricks-der-Spammer-und-Phisher-270912.html

Seth/Damle. (2022). *Seth, Prerna; Damle, Madhavi - A Comprehensive Study of Classification of Phishing Attacks with its AI/I Detection.* Abgerufen am 01. 06. 2023 von Ieeexplore.ieee.org: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10060305

Sharma et al. (2022). *Proceedings of ICDSM 2021Sharma, Shubham; Nand, Parma; Sharma, Pankaj - Intrusion Detection and Prevention Systems Using Snort - Advances in Data Science and Management - Proceedings of ICDSM 2021.* Singapore: Springer Nature Singapore Pte. Ltd.

Silva et al. (2013). Silva, Sergio S.C.; Silva, Rodrigo M.P.; Pinto, Raquel C.G.; Salles, Ronaldo, M. - Botnets: A Survey. *Computer Networks, 57 (2013)* , S. 378-403.

Snort. (2023). *Snort.org - Snorg 3 is available.* Abgerufen am 06. 07. 2023 von Snort.org: https://www.snort.org/

Sonowal. (2022). *Sonowal, Gunikhan - Phishing and Communication Channels - A Guide to Identifying and Mitigating Phishing Attacks.* Berkley, California: Apress.

Spiegel Netzwelt. (2022). *Spiegel Netzwelt - Millionen gekaperte Geräte Deutsche Ermittler und Partner zerschlagen russisches Botnet.* Abgerufen am 07. 07. 2023 von Spiegel.de: https://www.google.com/search?q=Millionen+gekaperte+Ger%C3%A4te+Deutsche+Ermittler+und+Partner+zerschlagen+russisches+Botnet&oq=Millionen+gekaperte+Ger%C3%A4te+Deutsche+Ermittler+und+Partner+zerschlagen+russisches+Botnet&aqs=edge..69i57&sourceid=chrome&ie

Stam. (2017). Stam, Fabian - Die Strafbarkeit des Aufbaus von Botnetzen. *Zeitschrift für Internationale Strafrechtsdogmatik – www.zis-online.com, 9/2017, 547:552*, S. 547-552.

Statista. (2022). *Statista - Cyberkriminalität.* Von Statista.com: https://de.statista.com/infografik/23077/anzahl-der-straftaten-im-bereich-cybercrime/ abgerufen

Statista. (2022a). *Statista - Schäden durch Cyberkriminalität in Deutschland 2022 - hochgerechnet.* Von Statista.com: https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/ abgerufen

Sujatha et a. (2022). *Sujatha, G.; Kanchal, Yash; Geogen, George - An Advanced Approach for Detection of Distributed Denial of Service (DDoS) Attacks Using Machine Learning Techniques.* Abgerufen am 19. 06. 2023 von ieeexplore.ieee.org: https://ieeexplore.ieee.org/document/9951944

Torproject. (2023). *Torproject - Join the Tor Community.* Abgerufen am 16. 06. 2023 von community.torproject.org: https://community.torproject.org/

Vormayr et al. (2017). *Vormayr, Gernot; Zseby, Tanja; Fabini, Joachim - Botnet Communication Patterns.* Abgerufen am 02. 06. 2023 von ieeexplore.ieee.org: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8026031

Voß. (2022). *Voß, Andy - Emotet ist zurück: Berüchtigtes Botnet spammt wieder.* Abgerufen am 10. 07. 2023 von Computerbild.de: https://www.computerbild.de/artikel/cb-News-Sicherheit-Emotet-ist-zurueck-Beruechtigtes-Botnet-spammt-wieder-34096013.html

Wang et al. (2010). *Wang, Ping; Sparks, Sherri; Zou, Cliff C. - An Advanced Hybrid Peer-to-Peer Botnet.* Abgerufen am 13. 06. 2023 von IEEE Transactions on Dependable and Secure Computing, Vol. 7, No. 2, April-June 2010, 113:127: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4569852

Wendzel. (2021). *Wendzel, Steffen - IT-Sicherheit für TCP/IP- und IoT-Netzwerke Grundlagen, Konzepte, Protokolle, Härtung.* Wiesbaden: Springer Vieweg.

Xing et al. (2021). *Xing, Ying; Shu, Hui; Li, Dannong; Guo, Li - Survey on Botnet Detection Techniques: Classification, Methods and Evaluation.* Abgerufen am 14. 06. 2023 von downloads.hindawi.com: https://downloads.hindawi.com/journals/mpe/2021/6640499.pdf

Zeidanloo/Manaf. (2009). *Zeidanloo, Hossein Rouhani; Manaf, Azizah Abdul - Botnet Command and Control Mechanisms.* Abgerufen am 15. 06. 2023 von

Ieeexplore.ieee.org: https://ieeexplore.ieee.org/abstract/document/5380180?casa_token=bAQyQkgiswYAAAAA:q4Lb9wZRYMvcMPLEcYsNI8EsGLWt-4Da-dHXLnXUC0vQEvi9V0Ltr88B3WujKDt3HKuVlQyT_w

Zhong et al. (2015). *Zhong, Xingsi; Fu, Yu; Yu, Lu; Brooks, Richard; Venayagamoorthy, G. Kumar - Stealthy Malware Traffic – Not as Innocent as It Looks.* Abgerufen am 16. 06. 2023 von IEEExplore.ieee.org: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7413691

Zipperle. (2014). *Zipperle, Florian - Überblick über Botnetz-Erkennungsmethoden.* Abgerufen am 29. 05. 2023 von net.in.tum.de: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2014-08-1/NET-2014-08-1_03.pdf

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

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

Zossen, den 14.07.2023

Cedric Busacker