Detektion von Ransomware in der IT-Systemlandschaft bei Betreibern Kritischer Infrastruktur

Abschlussarbeit

zur Erlangung des akademischen Grades
Master of Science (M.Sc.)

an der

Technischen Hochschule Brandenburg
Fachbereich Informatik und Medien
Studiengang Informatik

1. Prüfer:	Prof. Dr. Michael Pilgermann (Technische Hochschule Brandenburg)
2. Prüfer:	Dr. Tino Schonert (Stadtwerke Brandenburg an der Havel GmbH)

Eingereicht von:	Bjarne Jungclaus
Matrikelnummer:	20151304
Datum der Abgabe:	28.01.2023

Abstract

Ransomware-Angriffe auf Kritische Infrastrukturen, wie Energie- oder Wasserversorgung, treten immer häufiger auf und stellen eine große Bedrohung für die Betreiber und die Bevölkerung dar. Eine verlässliche und frühzeitige Erkennung dieser Angriffe ist somit ein wichtiger Bestandteil von IT-Sicherheitskonzepten.
Ziel dieser Arbeit ist die Klärung der Fragen, welche Methoden zur Erkennung von Ransomware eingesetzt werden und welche Indikatoren für Ransomware-Angriffe mithilfe eines Angriffserkennungssystems in einer nachgebildeten IT-KRITIS-Infrastruktur erkannt werden können.
Es wurden Methoden zur Detektion von Malware und Ransomware genauer betrachtet. In einem Experiment wurde die Erkennung von Ransomware mithilfe eines Angriffserkennungssystems (Elastic Stack) untersucht. Das Ergebnis dieser Arbeit zeigt, dass die Erkennung sowohl mit allgemeinen Detektionsansätzen als auch mit auf Ransomware spezialisierten Methoden erfolgen kann.
Aus dem Experiment geht hervor, dass die Detektion von Ransomware-Angriffen mithilfe eines Angriffserkennungssystems in der Praxis erfolgreich ist. Indikatoren für Ransomware-Angriffe werden sowohl auf Systemebene (Prozesse, Dateioperationen, Registry-Änderungen etc.) als auch auf Netzwerkebene (C2-Kommunikation, auffällige DNS-Anfragen, IP-Adressen etc.) erkannt.

Inhaltsverzeichnis

Kapitel 1

Einleitung

Mit dem Voranschreiten des 21. Jahrhunderts macht vor allem eine Kategorie von Malware immer größere Schlagzeilen. Die Rede ist von der so genannten Ransomware. Opfern eines Ransomware-Angriffes wird der Zugriff auf ihre Daten oder sogar das gesamte System verwehrt, bis das geforderte Lösegeld bezahlt wurde.
Heutzutage geraten auch vermehrt größere Unternehmen und Organisationen ins Visier von Cyberkriminellen. Ein Beispiel hierfür ist die Ransomware-Attacke auf *Colonial Pipeline* im Mai 2021. [BK21] Als Betreiber von einer der größten Kraftstoffpipelines in den USA, ist Colonial für die Verteilung von Kraftstoff an viele verschiedene Abnehmer verantwortlich. Um den Schaden im eigenen Netzwerk sowie Missbrauch der kompromittierten Pipelinesteuerung zu verhindern, entschloss sich das Unternehmen, sämtlichen Betrieb einzustellen. Der eingestellte Betrieb führte zu Kraftstoffmangel an Tankstellen und sukzessiven Panikkäufen von Verbrauchern. Obwohl das Unternehmen bereits kurze Zeit nach der Lösegeldforderung von 75 Bitcoin (zu dem Zeitpunkt ca. 4,4 Millionen USD) diese auch zahlte und von den Angreifern mit einem Entschlüsselungswerkzeug versorgt wurde, dauerte die Wiederherstellung und Prüfung der Sicherheit der Systeme an. [TRJ21; CNN22] Insgesamt war der Betrieb der Pipeline sechs Tage, vom 6. bis zum 12. Mai, eingeschränkt.
Damit genau solche Ausfälle von Kritischer Infrastruktur verhindert werden können, sollte die frühzeitige Detektion von Ransomware (und anderer Malware) ein wichtiger Bestandteil von IT-Sicherheitskonzepten sein. Die deutsche Rechtsprechung hat daher die Angriffserkennung zu einem festen Bestandteil für Unternehmen und Organisationen der Kritischen Infrastruktur (KRITIS) gemacht. Ab dem 01. Mai 2023 sind alle Betreiber von KRITIS

dazu verpflichtet, Systeme zur Angriffserkennung zu verwenden.[BMJb; BMJa]
Auch die Stadtwerke Brandenburg an der Havel GmbH (StWB), welche diese Arbeit mit wertvollen Informationen und Ansprechpartnern zum Thema Kritische Infrastruktur unterstützt, sind von dieser Regelung betroffen. Neben der allgemeinen Angriffsdetektion besteht, auch von Seiten der StWB, ein besonderes Interesse an der Detektion von Ransomware-Angriffen, da diese eine der größten Bedrohungen für Unternehmen darstellen.[BSI22b; BSI22e]
Vor diesem Hintergrund soll diese Arbeit klären, welche Methoden zur Detektion von Ransomware genutzt werden und welche Indikatoren von Ransomware-Angriffen mithilfe eines Angriffserkennungssystems in einer nachgebauten IT-KRITIS-Infrastruktur erkannt werden können. Das Ziel ist dabei eine Übersicht über bereits vorhandene Methoden und Vorgehen zu gewinnen und nicht die Entwicklung/Entdeckung von neuen Detektionsmethoden. Der Bereich der OT (Betriebstechnik, engl. Operational Technology) wird explizit nicht näher betrachtet.

Das erste Kapitel dieser Arbeit befasst sich mit den notwendigen theoretischen Grundlagen. Dazu zählt der rechtliche Hintergrund für die Informationssicherheit von Kritischen Infrastrukturen und die Definition des Begriffs Ransomware. Zusätzlich wird eine Taxonomie von Ransomware vorgestellt und die historische Entwicklung von Ransomware genauer betrachtet. Abschließend werden der Lebenszyklus sowie Maßnahmen gegen Ransomware vorgestellt.
Das nächste Kapitel befasst sich mit der Detektion von Malware und Ransomware. Dabei werden neben der Begriffsklärung auch die Herausforderungen des Gebiets betrachtet. Anschließend werden allgemeine Detektionsansätze sowie die explizite Detektion von Ransomware behandelt. Zuletzt werden verschiedene Arten von Angriffserkennungssystemen vorgestellt.
In Zusammenarbeit mit den StWB wird im Kapitel Experiment ein Versuchsaufbau zur Erkennung von Ransomware mittels eines Angriffserkennungssystems erarbeitet. Das Kapitel ist in den Aufbau, die Durchführung, die Beobachtungen und die Auswertung unterteilt. Zuletzt werden die Ergebnisse dieser Arbeit in einem Fazit zusammengefasst und ein Ausblick auf zukünftige Forschungsthemen gegeben.

Kapitel 2

Theoretische Grundlagen

Dieses Kapitel beschäftigt sich mit den notwendigen theoretischen Grundlagen für die Detektion von Ransomware im Kontext der Kritischen Infrastruktur. Zunächst werden die Begriffe *Kritische Infrastruktur* und *Ransomware* erklärt. Daraufhin wird Ransomware genauer unter den Aspekten der Taxonomie, historischen Entwicklung, dem Lebenszyklus sowie Gegenmaßnahmen betrachtet.

2.1 Kritische Infrastrukturen und Informationssicherheit

Kritische Infrastrukturen (KRITIS) werden von den Bundesressorts allgemein als „[...] Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."[BMI09] definiert. Sie sind (Stand 2022) in zehn verschiede Sektoren unterteilt: *Energie*, *Informationstechnik und Telekommunikation*, *Transport und Verkehr*, *Gesundheit*, *Medien und Kultur*, *Wasser*, *Ernährung*, *Finanz- und Versicherungswesen*, *Siedlungsabfallentsorgung* und *Staat und Verwaltung*.
Unter dem Begriff Informationssicherheit versteht man allgemein die Gewährleistung der drei primären Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit für Informationen von technischen und nicht-technischen Systemen. Je nach Kontext können weitere

Schutzziele wie Authentizität, Nichtabstreitbarkeit, Verbindlichkeit und Zuverlässigkeit zusätzlich relevant sein.[BSI22c]
Vertraulichkeit stellt sicher, dass nur berechtigte Personen Zugriff zu den Informationen erhalten. Die Unverfälschtheit und Korrektheit von Informationen werden durch das Schutzziel Integrität gewährleistet. Das Schutzziel Verfügbarkeit garantiert, dass die Informationen einer berechtigten Person zu jeder gewünschten Zeit an definierter Stelle zur Verfügung stehen.

Die Informationssicherheit von Kritischen Infrastrukturen wird in Deutschland erstmals durch das IT-Sicherheitsgesetz (IT-SiG) aus dem Jahr 2015 durch den Gesetzgeber betrachtet. Das Grundziel dieses Gesetzes ist die allgemeine Verbesserung der Sicherheit von IT-Systemen und digitaler Infrastruktur in Deutschland. Zu diesem Zweck wurden die Kompetenzen und Aufgabenbereiche des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erweitert und konkrete Regulierungen für Kritische Infrastrukturen verfasst. Die Aufgaben des BSI werden durch das BSI-Gesetz (BSIG) geregelt, welches durch das IT-SiG geändert und ergänzt wird. Mit dem Inkrafttreten des IT-SiG wurde dem BSIG z.B. der § 8a hinzugefügt, welcher den Aufgabenbereich des BSI, hauptsächlich von Bundesstellen, auch auf die Sicherheit von Informationstechnik Kritischer Infrastrukturen erweitert. Der Paragraf verpflichtet Betreiber von KRITIS u.a. „[...] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.“[Gmb15] Mit § 8b wird das BSI als zentrale Meldestelle für Sicherheitsangelegenheiten etabliert und eine Meldepflicht für sicherheitsrelevante Ereignisse (Störungen, Ausfälle, Cyber-Angriffe, etc.) eingeführt. Der § 8d kann die Verpflichtungen von § 8a aufheben, wenn ein KRITIS-Betreiber andere Rechtsvorschriften einhält, die mit den Anforderungen des Paragrafen vergleichbar oder weitergehend sind.[BMJc]
Ein Beispiel für eine solche Ausnahme sind Energieversorger, die durch das Energiewirtschaftsgesetz (EnWG) reguliert werden, welches ähnliche Anpassungen im Rahmen des IT-SiG erfahren hat. Nach § 11 Absatz 1a muss auch bei Energieversorgern ein angemessener Schutz vor IT-Vorfällen/Angriffen gewährleistet werden. Die Anforderungen werden allerdings durch die regulierende Behörde und nur in Beratung mit dem BSI in einem öffentlichen Sicherheitskatalog definiert. Wenn der Betrieb jedoch durch das BSIG als

KRITIS identifiziert wird, werden zusätzliche Fristen für die Umsetzung fällig, und die Einhaltung kann durch die Bundesnetzagentur überprüft werden. Zusätzlich müssen dann alle sicherheitsrelevanten Ereignisse an das BSI gemeldet werden.

Ob ein Betrieb als KRITIS im Sinne des BSIG gilt, wird durch § 10 Absatz 1 des BSIG, sowie der *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)* geregelt. Letztere stellt eine Reihe von Kriterien und Schwellenwerten (z.B. 500.000 versorgte Personen) auf, welche von einem Betrieb erfüllt oder überschritten sein müssen, um als KRITIS im Sinne des BSIG zu gelten.

Im Jahr 2021 trat das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0), mit dem Ziel das BSI als Cybersicherheits-Behörde weiter zu stärken und Systeme für die Detektion und Abwehr von Cyberangriffen zu etablieren, in Kraft.[Gmb15] Das BSIG wurde in diesem Zuge um § 8a Absatz 1a erweitert, welcher Betreiber von KRITIS ab dem 01.05.2023 dazu verpflichtet, Systeme zur Angriffserkennung einzusetzen.[BMJb] Eine vergleichbare Änderung wurde auch im EnWG vorgenommen (§ 11 Absatz 1d). Die grundlegenden Bestandteile von Angriffserkennungssystemen sind Prozesse aus den Bereichen Protokollierung, Detektion und Reaktion. Sie umfassen somit auch die Detektion von Ransomware. Für KRITIS-Betreiber nach BSI-KritisV werden verbindliche Vorgaben zur Planung, Umsetzung und deren Nachweis festgelegt. Dazu hat das BSI die *Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung* veröffentlicht.[BSI22a]

Zukünftig werden weitere Änderungen/Erweiterungen der IT-Sicherheitsgesetze besonders im Rahmen europäischer Rechtlegungen, wie der Network and Information Security-Richtlinie (EU NIS2) oder Directive on the resilience of critical entities (EU RCE) notwendig werden.[Wei22]

2.2 Definition Ransomware

Ransomware setzt sich aus dem englischen Wort „Ransom“ (dt. Lösegeld) und dem Suffix „-ware“ zusammen und beschreibt eine Unterkategorie von Malware. Im Deutschen ist Ransomware auch unter Namen wie *Verschlüsselungstrojaner*, *Erpressungstrojaner* oder *Erpressungssoftware* bekannt.
Diese Art von Malware schränkt den Zugriff auf Daten und Systeme ein oder verhindert

ihn vollständig. Um erneut Zugriff auf die Daten bzw. Systeme zu erhalten, muss das namensgebende Lösegeld (engl. Ransom) an den Erpresser/Angreifer bezahlt werden.

2.3 Taxonomie von Ransomware

Die tatsächlichen Implementationen von Ransomware fallen jedoch sehr unterschiedlich aus, sodass eine Taxonomie notwendig ist, um eine gute Übersicht über die verschiedenen Charakteristiken von Ransomware zu erhalten. Für diese Arbeit wurde eine Taxonomie auf der Basis von „A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions“ [Oz22] und „Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions“ [AMS18] erstellt.
Die Abbildung 2.1 stellt die Taxonomie in Form einer grafischen Übersicht dar. Ihr ist zu entnehmen, dass die Klassifizierung von Ransomware grundsätzlich nach den vier Aspekten *Ziel*, *Infektion*, *Kommunikation* und *Bösartige Aktion* vorgenommen wird. In den folgenden Abschnitten werden die einzelnen Aspekte sowie ihre Unterpunkte genauer betrachtet und ihre Bedeutung erklärt.

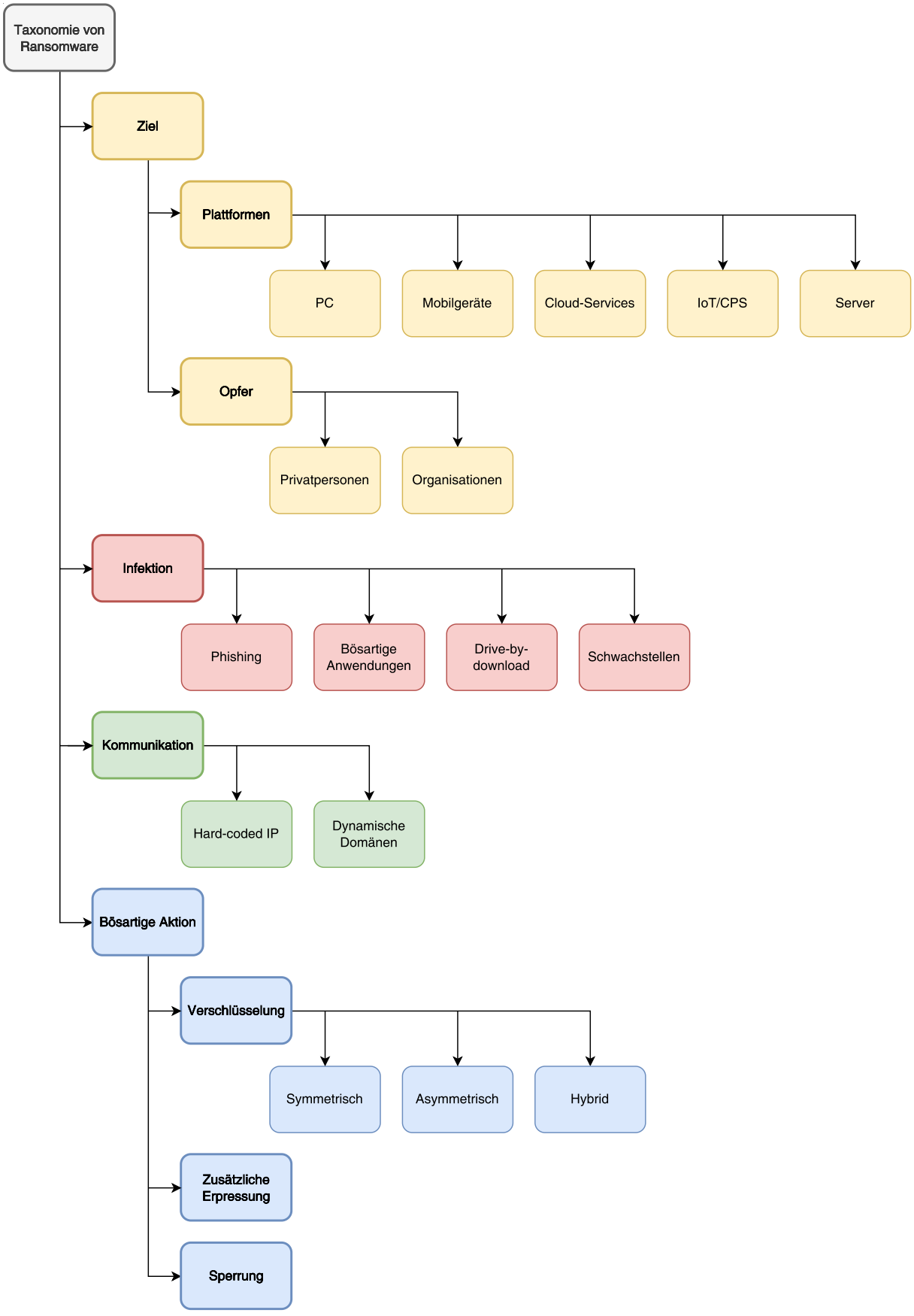


Abbildung 2.1: Ransomware Taxonomie

2.3.1 Klassifizierung über das Ziel

Das (Angriffs-)Ziel wird bei Ransomware in zwei unterschiedliche Ebenen unterteilt, die angegriffene Plattform und die Art des Opfers.

Für die Art des Opfers wird zwischen Privatpersonen und Organisationen unterschieden.

Als **Privatpersonen** wird in diesem Kontext eine Person verstanden, die einen Computer mit Internetzugang besitzt. Besonders anfällig sind diejenigen, die nur ein geringes technisches Wissen sowie minimales Verständnis über Sicherheit im Internet besitzen. Diese Personen sehen oft keinen anderen Ausweg, als das Lösegeld zu bezahlen.[SCL15]
Eine der einfachsten Methoden zur Wiederherstellung von betroffenen Geräten ist das Erstellen von Backups. Nach einer Studie aus dem Jahr 2016 [KMD16] erstellen allerdings ca. 20% aller Privatpersonen keine Backups für ihre Computer. Des Weiteren geht aus den Daten der Umfrage hervor, dass 25% aller wichtigen Dateien und 33% aller wichtigen Ordner (Ansammlung von vielen unspezifischen Dateien) nicht (vollständig) wiederhergestellt werden konnten.
Andere Umfragen von Acronis [Kos19; Mou17] oder The Harris Poll im Auftrag von Backblaze [Bau19] zeigen einen fallenden Trend für nicht gesicherte Geräte, von ~35% in 2008 auf ~17% in 2019. Betrachtet man die Frequenz mit der die Backups erstellt werden (siehe Anhang A.1), so zeigt sich, dass im Jahr 2019 41% Backups einmal pro Jahr oder in noch längeren Zeitabständen gemacht wurden.[Bau19] Für Daten, die ständig aktualisiert werden, ist diese Frequenz viel zu niedrig und kann daher, je nach verstrichener Zeit, zwischen Backup und Ransomware-Angriff, trotz einer Wiederherstellung, als Datenverlust angesehen werden. Zusammen mit 20% gar nicht gesicherten Geräten ergibt sich somit eine potentielle auszubeutende Angriffsmenge von 61% der genutzten Computer.
Im Vergleich zu Organisationen befindet sich das geforderte Lösegeld meist nur im mittleren dreistelligen Bereich (300 - 700 USD). Dies reicht für die Profitabilität der Angriffe aus, da einzelne Ransomware ohne Anpassungen gegen eine breite Masse von Verbrauchersystemen eingesetzt werden kann.[SCL15]

Organisationen sind in diesem Fall als Gegenteil von Privatpersonen anzusehen. Sie umschließen eine Vielzahl von Personen und technischen Geräten. Außerdem obliegt der Betrieb von IT-Infrastruktur geschultem Fachpersonal und gesetzlichen Regelungen, sodass sie bereits ein hohes Maß an IT-Grundsicherheit vorweisen.

Cyberkriminelle können ihre Zielorganisation sorgfältig im Vorfeld auswählen und versuchen eine größtmögliche Unterbrechung der Dienste zu erreichen, um die Chancen zu erhöhen, ein hohes Lösegeld zu erhalten.[OBr17] Das Erpressen von Organisationen ist besonders lukrativ, da Lösegeldforderungen 2021 im Durchschnitt bei 170.404 USD lagen, wobei es eine Spanne von ca. 10.000 USD am unteren und 3,2 Millionen USD am oberen Ende gab. Wie hoch das geforderte Lösegeld ausfällt, hängt laut eines Sophos-Whitepapers [SOP] von den drei Faktoren *Unternehmensgröße*, *Art des Angriffs* und dem *Standort* ab. Grundlegend kann gesagt werden, dass ein Lösegeld höher ausfällt, wenn die Organisation mehr als 1000 Mitarbeiter hat, das spezifisch ausgewählte Ziel des Angriffs ist und der Standort in einem westlichen Industriestaat liegt. Der Druck Lösegelder zu zahlen ist insbesondere dann sehr hoch, wenn Einrichtungen der Kritischen Infrastruktur (z.B. Energie, Gesundheit, Verwaltung, Finanzwesen) betroffen sind, da der Ausfall von Dienstleistungen erhebliche Einschränkungen und Schäden für die Öffentlichkeit mit sich bringt.
Eine weitere Möglichkeit das Lösegeld und den Druck zu erhöhen, ist die Drohung zuvor exfiltrierte sensible Dokumente zu veröffentlichen.

Die Art der angegriffenen Plattform ist ein relevanter Teil der Taxonomie, da die meisten Ransomware-Familien nur auf eine Plattform spezialisiert sind. Dies resultiert aus der Tatsache, dass Ransomware fast immer auf systemspezifische Programmbibliotheken und API-Aufrufe für die Durchführung ihrer Angriffe zurückgreift.

Die Plattform **PC** hat 2021 einen Marktanteil von ca. 43% [sta22b] und ist die Hauptplattform für das Ausführen von Arbeit und somit auch das Hauptangriffsziel von Ransomware. Dieses Angriffsziel kann auf der Ebene der Betriebssysteme weiter aufgeteilt werden. Die Wahrscheinlichkeit eines Ransomware-Angriffs lässt sich ungefähr mit dem Marktanteil des jeweiligen Betriebssystems korrelieren.[Arc18] In 2021 sind daher PCs mit dem Betriebssystem *Windows* (Marktanteil: ~73% [sta21b]) das häufigste Ziel von Ransomware-Angriffen. Andere Betriebssysteme wie *macOS* oder *Linux*, mit ihren Marktanteilen von ~15% und ~2% [sta21b], sind seltener das Ziel von Ransomware.

Die Plattform **Mobilgeräte** besteht aus Smartphones und Tablets, aber auch Wearables (z.B. Smartwatches) und anderen Smart Appliances. Nach einer Schätzung aus dem Jahr 2021 befinden sich im selben Jahr weltweit ca. 15 Milliarden Mobilgeräte, verteilt auf ca. 7,1 Milliarden Nutzer, im Umlauf.[The21] Zusammen mit einem stetigen Wachstum des Marktanteils (2015: ~37%, 2021: ~57% [sta22b]), lässt sich das wachsende Interesse von

Cyberkriminellen und Ransomware-Autoren für diese Plattform erklären. Dies geht auch aus einer Statistik von Ransomware-Angriffen auf Mobilgeräte über den Zeitraum 2020 bis 2021 mit einem Anstieg von 13,26% hervor (siehe A.2).
Ransomware-Angriffe haben selten spezielle Gerätetypen als Ziel, sondern orientieren sich eher am jeweils verwendeten Betriebssystem, da dieses eine konstante Angriffsfläche über eine große Menge an verschiedenen Geräten bietet. Die relevanten Betriebssysteme für Mobilgeräte sind *Android* und *iOS* mit Marktanteilen von ~72% und ~27%.[sta21a]
Neben dem Marktanteil spielt auch die Verfügbarkeit vom öffentlichen Quellcode der Betriebssysteme eine Rolle. Während das von Google veröffentlichte Android ein für jedermann zugängliches Open Source-Projekt ist, wird der Quellcode von Apples Mobilbetriebssystem iOS nicht veröffentlicht. Dies führt dazu, dass das Finden von Exploits und Schwachstellen in iOS mit erheblich mehr Aufwand verbunden ist als bei Android.[SCL15]
Eine von Kaspersky veröffentlichte Statistik [SK22] für den Zeitraum 2020-2021 zeigt, dass alle der Top 10 verwendeten Ransomware-Familien das Betriebssystem Android als Ziel hatten.
Besonders Smartphones speichern, dank ihrer Vielzahl von Einsatzmöglichkeiten (Fotografie, Banking, Social Media, Email, etc.), immer mehr sensible Daten, welche zum Ziel von Cyberkriminellen werden können.

Cloud-Services, wie z.B. Dropbox, Microsoft 365, Google Drive, etc. sind, gerade zu Zeiten des Homeoffices, immer stärker ins Visier von Cyberkriminellen geraten. Gerade Unternehmen haben zur Zeit der Corona-Pandemie einen Wechsel von traditioneller- zu Cloud-IT vorgenommen und waren dabei stärker mit der Aufrüstung ihrer Infrastruktur, als mit dem Schutz dieser beschäftigt.[WW21] Durch Arbeit von Zuhause und der damit einhergehenden Nutzung von Cloud-Services werden Unternehmensnetzwerke nun um die Heimnetze ihrer Angestellten erweitert. Die führt dazu, dass die IT-Sicherheit angepasst werden muss, um möglichen Angriffen oder Schwachstellen zuvorzukommen.
McAfee schätzt, dass Malware gegen Cloud-Services in den kommenden Jahren zu einem entweder „mechanisiert und weit verbreiteten“ oder „gezielt und präzise handgefertigten“ Phänomen bzw. Problem werden wird.[McA21]
Ransomware-Angriffe auf Cloud-Services haben meist den Speicher der Services als Ziel, wo sie versuchen, sämtliche Daten zu verschlüsseln. Gerade Cloud-Storage mit automatisierter Daten-Synchronisation, wird von Ransomware für die schnelle Ausbreitung auf weitere Systeme verwendet.

Geräte der Plattformen Internet of Things (**IoT**) und Cyber Physical System (**CPS**) lassen sich zu einer Kategorie zusammenfassen, da sie in der Regel keine von Benutzern erstellten Dateien und Dokumente enthalten, aber mithilfe von Sensoren, Aktuatoren und Software die Steuerung bzw. das Management von Smart-Infrastrukturen unterschiedlichster Arten (Smart Home, Smart Health, Smart Factories, ...) übernehmen.[Gro15] Mit der Transformation zu Industrie 4.0 werden diese Geräte immer häufiger genutzt, um Maschinen und Abläufe intelligent zu vernetzen und zu automatisieren.[BMW19]
Während das Ziel von Ransomware meist das Geiselhalten von für den Benutzer wichtigen Dateien ist, zielt Ransomware für IoT auf das Blockieren von Funktionen und böswilligen Aktionen (Herunterfahren des Gerätes, Abschalten von gesteuerten Geräten etc.) ab. Dies ist besonders gefährlich, wenn diese Geräte in KRITIS oder in enger Verbundenheit mit Menschen (Herzschrittmacher, Insulinpumpe, Smart-Cars, etc.) eingesetzt und erfolgreich angegriffen werden.[Dic16]

Server sind Geräte, die spezielle Services (z.B. Datenbanken, Web-Server etc.) anbieten. Ein einzelner Server kann dabei, je nach Art, einen bis mehrere Services bereitstellen. Eine Besonderheit ist, dass Server Daten erst nach Anfrage übertragen und Benutzer eines Services nie direkt auf einem Server arbeiten, sondern nur Anfragen stellen können.
Ransomware kann gegen einen Server auf zwei Arten eingesetzt werden. Zum einen besteht die Möglichkeit, auf dem Server vorhandene Daten (besonders bei Datenbanken) zu verschlüsseln und gegen Lösegeld wieder frei zu geben. Dies ist besonders lukrativ, wenn die Daten personenbezogen und sensibel sind. Die andere Art ist, einen Denial of Service-Angriff durchzuführen, bis das Lösegeld bezahlt wurde. Da Server auch Teil von IoT oder CPS sein können, besteht auch hier die Gefahr, dass Menschen oder Sachgegenstände zu Schaden kommen können. Aber auch indirektere Schäden, durch die nicht-Verfügbarkeit von Services/Servern, können die Wahrscheinlichkeit erhöhen, dass Lösegelder bezahlt werden.[BK21; CNN22; TRJ21]

2.3.2 Klassifizierung über die Infektion

Ein System gilt in der Cyber-Sicherheit als infiziert, sobald sich darauf Malware befindet. Auch Ransomware muss zuallererst ein System infiziert haben, damit es seine Wirkung entfalten kann. Besonders der Bereich Prävention kann von den Erkenntnissen dieser

Klassifizierung profitieren. Die Infektionsmethoden für Ransomware lassen sich in vier Bereiche einteilen: Phishing, Bösartige Anwendungen, Drive-by-downloads und Schwachstellen.[Oz22]

Phishing wird vom Oxford Wörterbuch als „the activity of tricking people by getting them to give their identity, bank account numbers, etc. over the internet or by email, and then using these to steal money from them“ definiert.[Oxf22] Etwas allgemeiner kann man Phishing als eine Art Betrug bezeichnen, bei dem Benutzer elektronisch verleitet werden, bestimmte Handlungen vorzunehmen und dabei sensible Informationen preisgeben.[JS11] Ransomware nutzt diese Infektionsmethode sowohl zum Erlangen von Zugangsdaten zu einem System, als auch um Benutzer auf präparierte Seiten zu locken und dann zur Installation von bösartigen Anwendungen zu verleiten oder einen Drive-by-download zu starten. Phishing ist eines der häufigsten Einfallstore für Ransomware.[CIS17]

Bösartige Anwendungen sind Anwendungen, die von Ransomware-/Malwareentwicklern selbst entwickelt werden und Malware enthalten, sich gegenüber von Benutzern jedoch als harmlose und nützliche Software präsentieren. Ihre Installation wird zumeist durch Phishing eingeleitet oder ohne Wissen des Benutzers durch Drive-by-download-Angriffe durchgeführt.

Drive-by-download beschreibt eine Form von Cyber-Angriff, bei welchem bösartige Anwendungen ohne die Zustimmung des Benutzers installiert werden. Dieser Angriff kann sich Anwendungen, das Betriebssystem oder Webbrowser zunutze machen, die aufgrund fehlender Aktualisierungen Sicherheitslücken aufweisen. Es wird kein aktives Handeln durch den Benutzer benötigt, sodass dieser oftmals nicht erkennt, dass ein Angriff stattgefunden hat.[Kas22a]

Schwachstellen (engl. Vulnerabilities) oder auch Sicherheitslücken sind Fehler in z.B. Software, Firmware oder Hardware, die durch Cyberkriminelle ausgenutzt werden können, um ein System zu infizieren. Sicherheitslücken entstehen durch Bugs in Soft- und Firmware und können meist durch Patches von Herstellern geschlossen werden. Oftmals setzt dies jedoch das aktive Installieren der Patches oder Nutzung von Workarounds durch den Benutzer voraus. Wenn Updates fehlschlagen oder nicht installiert werden, können die theoretisch bereits geschlossen Sicherheitslücken weiterhin von Angreifern ausgenutzt werden.
Schwachstellen, die von Cyberkriminellen gefunden und ausgenutzt werden bevor sie

den Herstellern bekannt sind, werden als Zero-Day-Vulnerabilities bezeichnet. Zero-Day-Angriffe sind eher selten, haben jedoch eine besonders hohe Erfolgsquote, da oftmals noch keine Methode zur Verteidigung vorhanden ist.[Kas22b]

2.3.3 Klassifizierung über die Kommunikation

Ein weiteres Merkmal zum Klassifizieren ist die Kommunikation der Ransomware mit den Angreifern. Wenn Kommunikation stattfindet, wird sie durch sogenannte Command-and-Control-Server (C&C-Server) durchgeführt. Diese sind Teil der Domäne des Angreifers und werden im Allgemeinen eingesetzt, um Befehle an Malware auf bereits kompromittierte Systeme zu senden oder Daten von diesen abzugreifen.[JR08]
Im Falle von Ransomware werden sie hauptsächlich genutzt, um Encryption-Keys zwischen Angreifer und infiziertem System auszutauschen. Die Kommunikation zwischen C&C-Server und infiziertem System findet vorrangig über HTTP (Port: 80) und HTTPS (Port: 443) statt.[SOP20] Da die meisten Ransomware-Familien C&C-Server als Kommunikationsmittel verwenden, liegt der Fokus auf der Art des initialen Verbindungsaufbaus. Unterschieden wird hier zwischen Hard-coded IP und dynamischen Domänen.

Hard-coded IP beschreibt jene Ransomware-Familien, die ihre Kommunikation zu ihrem C&C-Server durch fest vorprogrammierte (engl. Hard-coded) IP-Adressen oder Domänen aufbauen. Durch ihre feste Integration ändern sich die Adressen/Domänen nicht und bieten dem Angreifer einen zuverlässigen Kommunikationsaufbau. Gleichzeitig können diese statischen Adressen/Domänen auch von Verteidigern verwendet werden, um Signaturen für die Detektion der Ransomware zu generieren.[Oz22]

Dynamische Domänen ermöglichen die Kommunikation über dynamisch generierte Domänen. Zu diesem Zweck werden sog. Domain Generation Alogrithms (DGA) eingesetzt, die für jeden Verbindungsaufbau einzigartige Domänennamen zur Verfügung stellen.[Sal18] Ständig wechselnde Domänennamen erschweren zwar die Erstellung von Signaturen und Firewall-Regeln [Sal18], jedoch ist die Vorausetzung für eine erfolgreiche Kommunikation, dass die generierten Domänennamen auch vom Angreifer kontrolliert werden. Im Vergleich zum „Hard-Coded IP“-Ansatz benötigt diese Methode erheblichem Mehraufwand durch den Angreifer.

2.3.4 Klassifizierung über die bösartige Aktion

Ransomware hat immer das Ziel Lösegeld von ihren Opfern zu erpressen. Allerdings werden je nach Ransomware-Familie unterschiedliche Strategien angewendet, um dieses Ziel zu erreichen. Die von Ransomware angewendeten bösartigen Aktionen lassen sich in Verschlüsselung und Sperrung sowie die zusätzliche Erpessung gruppieren.

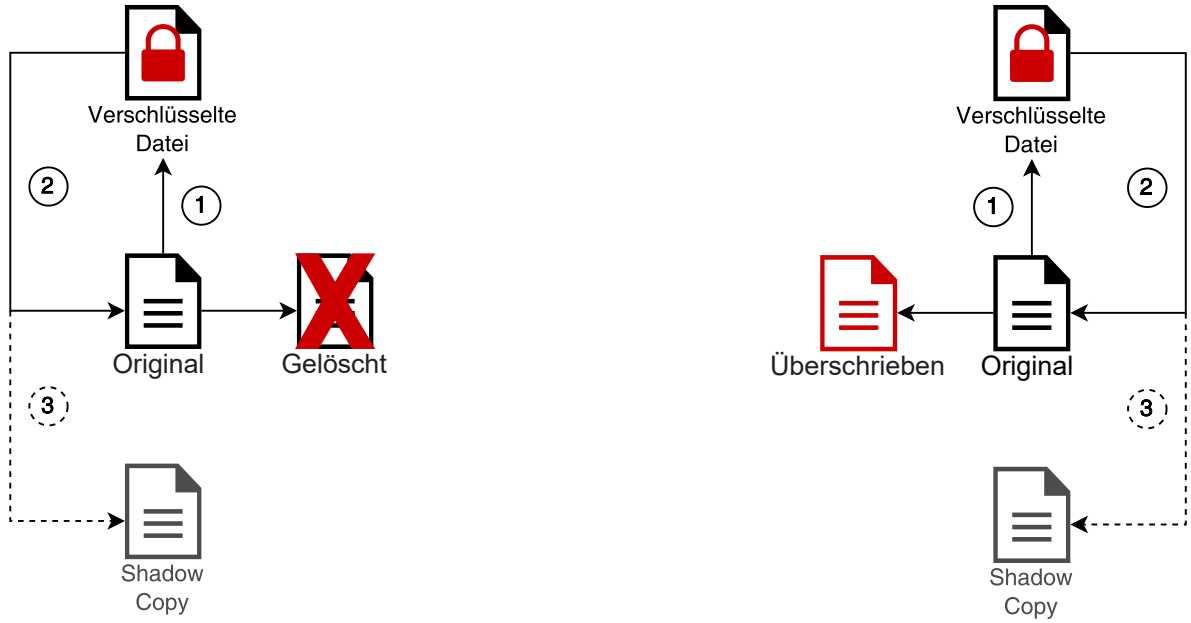
Ransomware-Familien, die durch die Verwendung von **Verschlüsselung** ihre Opfer erpressen, werden auch Crypto-Ransomware genannt. Die Verschlüsselung kann sowohl mit nativen APIs als auch über in der Ransomware selbst enthaltene Verschlüsselungsalgorithmen erfolgen.[SY18] Des Weiteren wird bei der Art der Verschlüsselung zwischen symmetrisch, asymmetrisch und hybrid unterschieden.

Symmetrische Verschlüsselung: Bei dieser Form der Verschlüsselung wird für das Ver- und Entschlüsseln ein einziger Encryption-Key eingesetzt.[Poh19] Dies hat den Vorteil, dass der Vorgang im Vergleich zu anderen Verschlüsselungsarten schneller ist, da weniger Ressourcen (kurze Schlüssellänge) für das Verschlüsseln großer Datenmengen benötigt werden. Gleichzeitig ist die Verwendung eines einzigen Keys auch eine Schwachstelle, da die Sicherheit dieser Verschlüsselung nur gegeben ist, solange der Key geheim bleibt. Wird dieser Key öffentlich bekannt, können Betroffene ihre Daten leicht selbst entschlüsseln.[SCL15] Die Übergabe des Keys vom infizierten System zum Angreifer findet mithilfe von C&C-Servern statt.
Der am häufigsten, von verschiedenen Ransomware-Familien, verwendete symmetrische Verschlüsselungsalgorithmus ist Advanced Encryption Standard (AES).[Oz22] Er gilt als der De-facto-Standard von fast allen modernen Anwendungen. In der Theorie existieren verschiedene Angriffe, die das Verfahren brechen könnten, jedoch nur unter mit heutiger Rechenstärke, unrealistisch hohem Zeitaufwand.[TW15; BKN09; BKR11] Beispiele für Ransomware-Familien mit symmetrischer Verschlüsselung sind: *Chimera*[Isl21], *TeslaCrypt* [LS18], *Petya*[AVA17].

Asymmetrische Verschlüsselung: Diese Art der Verschlüsselung verwendet ein Schlüsselpaar aus Private-Key und Public-Key. Der Public-Key ist dabei öffentlich verfügbar und wird für die Verschlüsselung genutzt. Die Entschlüsselung ist nur mit dem dazugehörigen Private-Key möglich, der geheim gehalten werden muss.[Poh19]
Aufgrund von längeren Schlüssellängen und komplexeren Verschlüsselungsberechnungen

nimmt die Verschlüsselung von großen Datenmengen deutlich mehr Zeit in Anspruch, als bei symmetrischer Verschlüsselung.[Dan21]
Da der Public-Key öffentlich bekannt sein darf, kann er von Angreifern bereits in die Binärdatei der Ransomware integriert werden. Auf diese Weise kann mit der Verschlüsselung begonnen werden, bevor die Kommunikation mit einem C&C-Server aufgenommen werden muss. Je nach Familie wird der Public-Key allerdings auch erst mit der Kontaktaufnahme zum C&C-Server übergeben. Entsprechend kann erst nach erfolgreicher Übergabe mit der Verschlüsselung begonnen werden.
Damit Opfer, welche das Lösegeld gezahlt haben, ihren erhaltenen Private-Key nicht an andere weitergeben, haben manche Ransomware-Familien Methoden entwickelt, um für jeden Angriff einzigartige Schlüsselpaare zu generieren.[SCL15]
Der große Vorteil gegenüber symmetrischer Verschlüsselung ist, dass der Private-Key, bis zur Zahlung des Lösegelds, dem Opfer völlig unbekannt bleibt und eine Entschlüsselung daher nahezu unmöglich ist.[Arg22] Der für asymmetrische Verschlüsselung am häufigsten verwendete Algorithmus ist Rivest–Shamir–Adleman (RSA).[Oz22] Beispiele für Ransomware-Familien, die asymmetrische Verschlüsselung verwenden, sind: *CryptoLocker*[Jar13], *SamSam*[Jar13], *CryptoWall*[Has19].

Hybride Verschlüsselung: Dieser Ansatz vereint die Vorteile der vorherigen beiden Verschlüsselungsmethoden. Die Dateien des Betroffenen werden schnell durch einen symmetrischen Algorithmus verschlüsselt und der verwendete Key wird daraufhin robust mit einem asymmetrischen Verfahren verschlüsselt und an den C&C-Server gesendet.
In den meisten Fällen wird der Public-Key in die Binärdatei eingebettet und der Angriff unabhängig von einer C&C-Server-Verbindung durchgeführt. Das Opfer wird einfach aufgefordert, den verschlüsselten symmetrischen Key bei der Lösegeldzahlung zu übergeben, und der Angreifer kann diesen daraufhin entschlüsseln und an das Opfer zurücksenden.
Eine häufige Kombination ist die Mischung aus AES & RSA.[Oz22] Bekannte Vertreter für Ransomware-Familien mit hybrider Verschlüsselung sind: *WannaCry*[Has19], *Ryuk*[Has19], *Corona*[Wan21].



(a) Löschen

(b) Überschreiben

Abbildung 2.2: Zerstörungsverhalten von Ransomware

Abbildung 2.2 zeigt die beiden Ausprägungen des **Zerstörungsverhaltens** von Ransomware. Unabhängig von der Art der Verschlüsselung werden die Originaldaten durch die Ransomware *zerstört*, damit sie nur schwer oder gar nicht wiederherstellbar sind. Im Wesentlichen wird zwischen Löschen (siehe Abb. 2.2a) und Überschreiben (siehe Abb. 2.2b) der Originaldatei unterschieden.

Der **1.** Schritt ist in beiden Fällen die Erstellung einer verschlüsselten Version (Kopie) der Originaldatei. Schritt **2** unterscheidet sich dadurch, dass die Originaldatei entweder gelöscht oder überschrieben wird. Wenn die Originaldatei nur gelöscht wird, besteht im vielen Fällen die Möglichkeit, dass sie durch Recovery-Anwendungen (z.B. Photorec, Recuva), ohne das Vorhandensein des Encryption-Keys, wiederhergestellt werden können.[ZWS18] Wird das Original jedoch mit Zufallsdaten oder der verschlüsselten Version überschrieben, sind es auch diese Versionen, die durch die Recovery-Anwendungen wiederhergestellt würden. Die (wiederhergestellte) Originaldatei ist somit unbrauchbar. Beide Formen können beispielsweise durch die Manipulation der Master File Table erreicht werden.[Die14]

Der **3.** Schritt ist optional und umschließt das Löschen von eventuell vorhandenen Shadow Copies. Der Volume Shadow Copy Service (VSS) ist eine von Microsoft entwickelte Tech-

nologie, die es dem Betriebssystem Windows erlaubt, Backups von Dateien und ganzen Volumes (Datenträger) zur Laufzeit zu erstellen.[Doc21] Die daraus resultierende Versionshistorie ist eine der einfachsten Möglichkeiten (unter Windows), um korrumpierte oder gelöschte Daten wiederherzustellen. Entsprechend besitzen viele Ransomware-Familien Mechanismen, um Shadow Copies zu löschen.[Wec16]

Ransomware-Familien, die **Sperrung** von Systemen nutzen, um Lösegeld zu erpressen, werden auch Locker-Ransomware genannt und lassen sich in zwei Unterkategorien einteilen: Screen-Locking und Master Boot Record (MBR)-Locking.

Als **Screen-Locking** werden Ransomware-Familien bezeichnet, die Zugriff auf das Grafische User Interface (GUI) eines Systems unterbinden und Lösegeld fordern, um den Zugriff wiederherzustellen.
Das Sperren (engl. locking) kann durch verschiedene Methoden, z.B. das Erstellen und Persistieren von neuen Desktops durch Betriebssystem-Befehle, ausgeführt werden.[Die14] Besonders Mobilgeräte sind von dieser Form der Ransomware betroffen, da das Entfernen dort erheblich aufwändiger ist, als bei z.B. PCs.[Kas19]

MBR-Locking-Ransomware-Familien sperren den Master Boot Record (MBR) eines Systems. Dieser enthält alle notwendigen Informationen zum Starten (engl. boot) des Betriebssystems. Wenn er durch Cyberkriminelle verschlüsselt oder ersetzt wird, kann das System nicht korrekt hochfahren. In diesem Zustand fordern die Angreifer Lösegeld für eine Anleitung zum Wiederherstellen des Systems.

Zusätzliche Erpressung beschreibt Vorgänge mit denen zusätzliche Lösegelder erpresst und der Zahlungsprozesse beschleunigt werden sollen.
Double Extortion (dt. doppelte Erpressung) beschreibt die Fähigkeit von Ransomware, sensible Nutzerdaten (z.B. Unternehmensunterlagen, Kreditkarteninformationen, persönliche Dateien etc.) vom System der Betroffenen zu extrahieren. Diese Exfiltration ist nur ein Nebenziel und wird genutzt, um weiteres Lösegeld erpressen zu können, indem mit der Veröffentlichung der gestohlenen Daten gedroht wird.[zsc21]
Darauf aufbauend gibt es auch Fälle von sogenannter *Triple Extortion*, bei welcher die Opfer zusätzlich mit weiteren Mitteln, z.B. Distributed Denial of Service (DDoS)-Angriffe oder belästigende Telefonanrufe (Cold Calling), erneut oder zusätzlich unter Druck gesetzt werden.[Nik21; ENI21]

Der Vorteil dieser Taktiken ist, dass Betroffene auch dann zur Zahlung eines Lösegelds gedrängt werden, wenn sie ihre Systeme eigenständig wiederherstellen könnten.

2.4 Historische Entwicklung von Ransomware

Ein weiterer Bestandteil für das Verständnis von Ransomware ist die historische Entwicklung. Abbildung 2.3 zeigt eine zeitliche Übersicht mit einigen der bekanntesten/berüchtigtsten Ransomware-Familien in einem Zeitraum von 1989 bis heute (2022). Die Familien werden anhand des Jahres ihres ersten Auftretens in der Übersicht eingeordnet. Je nach Quelle kann es dabei zu kleinen Abweichungen (wenige Monate) kommen. In dieser Abbildung wurde jenes Jahr verwendet, welches von den meisten betrachteten Quellen als Jahr des Erstauftretens deklariert wurde.

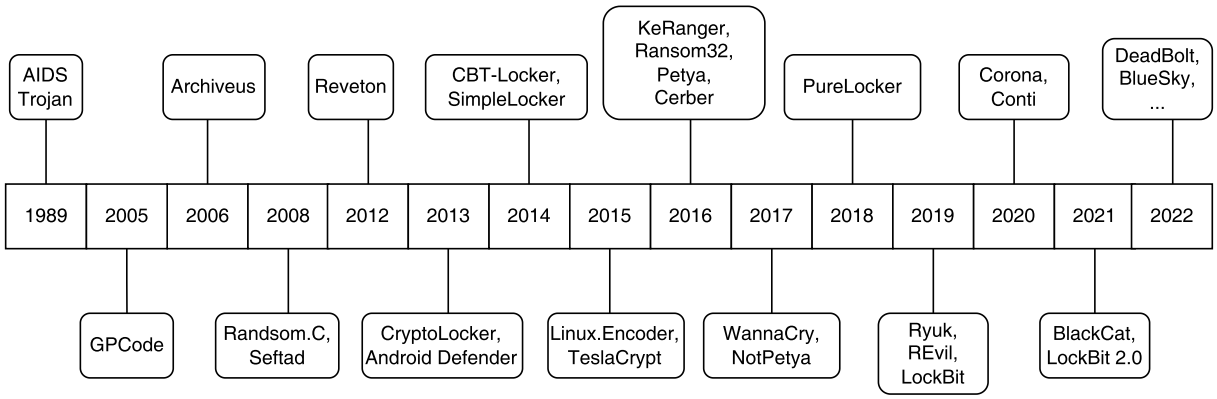


Abbildung 2.3: Zeitliche Übersicht zur Entwicklung von Ransomware

2.4.1 Anfänge

Die erste, als Ransomware deklarierte, Malware war der *AIDS Trojan* (auch als *PC Cyborg virus* bekannt) aus dem Jahr 1989. mithilfe von gestohlenen Adressenlisten der World Health Organization AIDS Conference und des „PC Business World"-Magazins schickte Dr. Joseph L. Popp infizierte Disketten an ca. 20.000 verschiedene Personen und Einrichtungen. Die Ransomware infizierte das C:\-Laufwerk und überschrieb die AUTOEXEC.BAT, welche zu jedem Start des Windows-Betriebssystems ausgeführt wurde. Nach einer zufälligen

Anzahl von Starts verschlüsselte die Ransomware sämtliche Dateinamen auf dem Laufwerk mithilfe von symmetrischer Verschlüsselung. Die Dateiinhalte blieben unberührt, die verschlüsselten Dateinamen und Endungen verhinderten jedoch das Ausführen der Dateien und machten den Computer so großteilig unbenutzbar. Daraufhin wurde der Benutzer aufgefordert eine angeblich ausgelaufene Softwarelizenz, für heute ca. 400 USD (für ein Jahr) bzw. ~800 USD (Lebenslang), zu erneuern. Der Nutzer wurde wiederholt mit der Lösegeldforderung konfrontiert und die geänderte AUTOEXEC.BAT sorgte dafür, dass die Nachricht bei jedem Neustart angezeigt wurde.[Wil90; Les20]

Im Jahr 1996 wurde das Konzept der Krypto-Virologie von Wissenschaftlern in einem Beitrag zu einem IEEE-Symposium vorgestellt. Das Konzept beschreibt einen Krypto-Virus als einen Denial-of-Service-Angriff unter der Verwendung eines öffentlichen Schlüssels und kommt somit der Definition von Ransomware bereits recht nahe.[YY96]

2.4.2 Die ersten Jahre

Im Jahr 2005 überstieg das globale Internet, welches sich bis dahin hauptsächlich im Aufbau befand, eine Milliarde Benutzer.[sta22c] Mit der steigenden Popularität und Verbreitung des Internets tauchte auch Ransomware wieder auf der Bildfläche auf. So erschien 2005 die erste moderne Crypto-Ransomware *GPCode*. Betroffene Geräte wurden mithilfe von Phishing-Emails infiziert und Dateien daraufhin symmetrisch verschlüsselt. Jedoch wurde der verwendete Schlüssel in der Windows-Registry gespeichert, so dass *GPCode* anfangs nur eine geringe Erfolgsquote besaß.[fsec] Die Entwickler der Ransomware kamen zu dem Entschluss, dass ihre erste Version nicht den gewünschten Effekt erzielt hatte und fingen an, Verbesserungen vorzunehmen. [Nik16] Neuere Versionen (2010) verwendeten hybride Verschlüsselung und waren somit fast unmöglich zu brechen.[Kam10]
Die erste Ransomware-Familie, die asymmetrische Verschlüsselung verwendete, war *Archiveus* und hatte 2006 ihr Debüt. Sie verschlüsselte alle Dateien innerhalb des „Meine Dokumente“-Ordners und benötigte ein 30 Zeichen langes Passwort zur Entschlüsselung.[Dra22]

2008 tauchte die erste Locker-Ransomware auf, welche vorgab Teil des Windows-Security-Centers zu sein und Opfer dazu aufforderte, eine gebührenpflichtige Hotline anzurufen, um den Computer wieder freizugeben.[SCL15]

Etwa zur gleichen Zeit erschien *Seftad*, eine Ransomware, die es speziell auf den Master Boot Record (MBR) des Systems abgesehen hat. Sie überschreibt den MBR des Systems und fordert ein Lösegeld zur Freigabe. Die Lösegeldforderung gibt vor, dass alle Festplatten verschlüsselt wurden. Dies ist nur ein Vorwand, um den Druck auf das Opfer zu erhöhen. Tatsächlich ließ sich der MBR durch Eingabe eines korrekten Passworts wiederherstellen, wodurch eine Zahlung des Lösegeld hinfällig wurde.[Fis10]
Einer der größten Flaschenhälse für Ransomware-Angriffe ist die Bezahlung des Lösegelds. Damit Cyberkriminelle nicht direkt nach der Zahlung identifiziert und verhaftet werden, nutzen sie vorrangig Zahlungsmethoden, die ihre Identität schützen oder anonyme Transaktionen erlauben. Da diese Zahlungsmethoden jedoch nicht überall auf der Welt verfügbar und deren Anbieter an lokale Gesetze zur Strafverfolgung gebunden sind, ist die Gruppe der zahlenden Betroffenen und damit der Erfolg der Ransomware begrenzt.[Hua18]
Die Veröffentlichung der Kryptowährung Bitcoin im Jahr 2009 ermöglicht Cyberkriminellen Zugang zu einem dezentral organisierten und weitestgehend unregulierten Zahlungsmittel. Zwar sind alle getätigten Transaktionen öffentlich über die Blockchain persistiert und einsehbar, jedoch sind sie irreversibel und alle Transaktionsparteien hinter pseudo-anonymen Identitäten (Bitcoin-Adressen) versteckt. Forschern und strafverfolgende Institutionen können somit den Fluss des Geldes einsehen und zurückverfolgen, die eindeutige Identifizierung von Kriminellen ist jedoch mit erheblichem Ermittlungsaufwand verbunden.[Mei16] Dies, sowie die geografisch unabhängige Verfügbarkeit von Kryptowährungen, führte dazu, dass sich diese zum Hauptzahlungsmittel für Ransomware-Lösegelder entwickelte.

Im Jahr 2012 wurde die Locker-Ransomware *Reveton* veröffentlicht. Neben dem Aussperren den Nutzers aus seinem System, versuchte *Reveton* die Betroffenen einzuschüchtern, um an das Lösegeld zu kommen. Dies bewerkstelligte die Ransomware, indem sie vorgab von einer Strafverfolgungsbehörde zu sein und die betroffene Person eines Verbrechens beschuldigte (Kinderpornografie, Internetpiraterie, etc.). Des Weiteren übernahm die Ransomware die Webcams seiner Opfer und suggerierte, dass die Aufnahmen durch die Behörde aufgezeichnet würden, wodurch die Glaubwürdigkeit der Erpressernachricht erhöht werden sollte. Spätere Versionen waren mit zusätzlicher Malware (PonyStealer) ausgestattet, um Passwörter zu stehlen.[Kno19b]

2013 trat die *CryptoLocker*-Ransomware-Familie in zwei Aspekten als Pionier auf. Zum einen verwendete sie den hybriden Verschlüsselungsansatz (256-Bit AES für Dateien, 2048-Bit RSA für private Key), zum anderen nutze sie neben typischen Verteilungsmethoden

auch ein Botnet (Gameover Zeus), um sich zu verbreiten.[Dra22; OSC18]
Etwa zu gleichen Zeit wurde die erste Android-spezifische Ransomware *Android Defender* veröffentlicht. Die App gab vor, eine legitime Antivirus-Software zu sein und versucht den Nutzer zunächst mit falschen Sicherheitshinweisen zum Kauf einer Vollversion zu bewegen. Ignorierte der Nutzer diese Hinweise, sperrte die App, ca. sechs Stunden nach dem ersten Ausführen, den Bildschirm des Gerätes, bis die Vollversion gekauft wurde.[LŠB16]
CBT-Locker (Curve-Tor-Bitcoin-Locker) verschlüsselte 2014 Systeme mithilfe von Elliptic Curve Cryptography (ECC).[Kno19a] Der Rest des Namens beschreibt die Währung des Lösegelds, Bitcoin, sowie die Plattform zur Abwicklung des Bezahlvorgangs, TOR-Netzwerk. ECC wird als die nächste Generation von Public-Key-Verschlüsselungsverfahren geführt und bietet, im Vergleich zu RSA, bereits bei kurzen Schlüssellängen hohe Sicherheit.[Sul13]
Im gleichen Jahr trat die erste verschlüsselnde Ransomware für Android *SimpleLocker* auf. Mithilfe von AES wurden sämtliche auf dem Gerät befindliche Dateien in kurzer Zeit verschlüsselt. Da der Encryption-Key als Klartext im Quellcode zu finden war, wurde die Entschlüsselung, besonders im Vergleich zu PC-Ransomware, als trivial angesehen.[LŠB16]

Erste Ransomware, die es innerhalb der Plattform PC nicht auf Windows-Systeme abgesehen hat, trat ab 2015 auf. *Linux.Encoder* war die erste Ransomware, welche explizit für den Einsatz auf Linux-Geräten entwickelt wurde.[DrW15; Bis15]
TeslaCrypt sorgte besonders in der Gaming-Community für Aufruhr, da die Ransomware es besonders auf typische Gaming-Dateien (Spielstände, Nutzerprofile, etc.) abgesehen hatte. Sie verschlüsselte jedoch nur Daten, die kleiner als 268 MB waren.[Kas21a] Anfang 2016 veröffentlichten die Entwickler, auf die Nachfrage eines ESET Forschers, freiwillig den Master-Decryption-Key, da der Support für *TeslaCrypt* eingestellt werden sollte und die meisten Entwickler sich bereits anderen „Projekten“ widmeten.[Abr16]

2.4.3 Ransomware als Geschäftsmodell

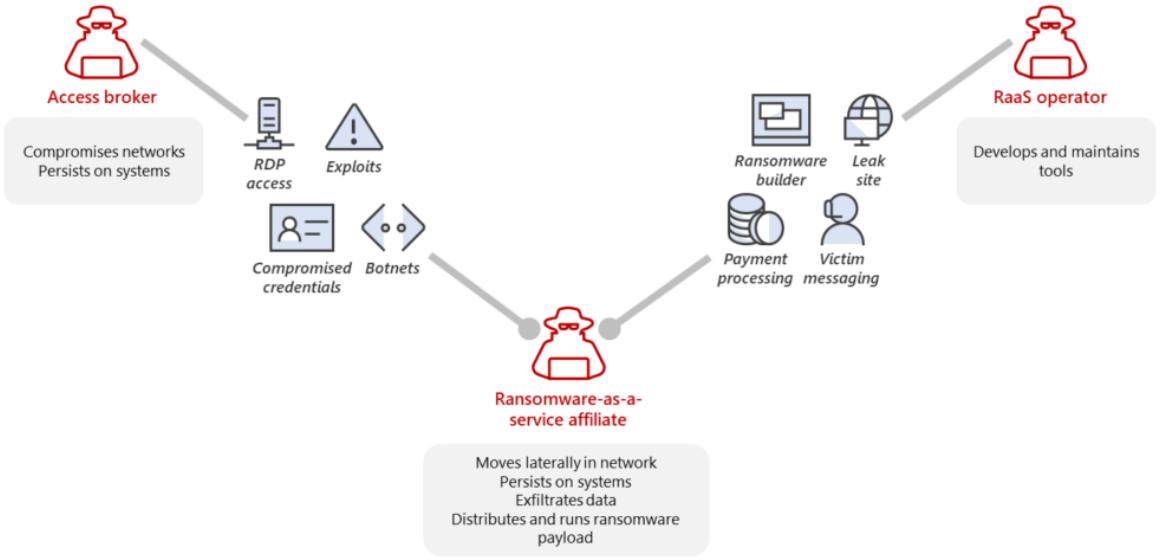


Abbildung 2.4: Funktionsweise des RaaS-Modells anhand von „human-operated ransomware“ aus [MST22]

Im Jahr 2016 wurde Ransomware erstmalig im Rahmen des Ransomware-as-a-Service (RaaS) -Modells verbreitet. Im selben Jahr erreichte die Anzahl von Ransomware-Angriffen einen Höhepunkt[Son22], was sich auch auf das Auftreten von RaaS-Angeboten zurückführen lässt.[Dra22; Kei20] Die Käufer dieser Dienstleistung mieten dabei den Zugang zu Tools, anstelle diese selbst zu entwickeln. Je nach Modell verlangen die Betreiber solcher Services einen Anteil am Lösegeld, einen monatlichen Pauschalpreis oder einmalige Lizenzgebühren.[Clo21]

Abbildung 2.4 zeigt die Funktionsweise dieses Modells am Beispiel von menschengesteuerter Ransomware (engl. human-operated). Der Begriff „menschengesteuerte Ransomware“ wurde vom Microsoft Threat Intelligence Center geprägt, um zu verdeutlichen, dass diese Bedrohungen von Menschen gesteuert werden, die in jeder Phase ihrer Angriffe Entscheidungen auf der Grundlage dessen treffen, was sie im Netzwerk ihres Ziels vorfinden.[MST22] Die Alternative dazu ist Ransomware, die möglichst vollautomatisch versucht in ein System einzudringen und es zu infizieren.
Der steuernde Mensch ist im Falle der Abbildung 2.4 der *Ransomware-as-a-service affiliate*,

welcher die Entscheidungen trifft, wann, wo und wie sich die eingekaufte Ransomware im kompromittierten System bewegt, persistiert oder ausgeführt wird.[MST20] Neben der Entwicklung und Wartung der Ransomware kümmert sich der *RaaS operator* auch um Funktionen, wie das Leaken von exfiltrierten Daten (Double Extortion), die Zahlungsabwicklung des Lösegelds und die Kommunikation mit den Betroffenen. Des Weiteren besteht die Möglichkeit, Zugänge zur Zielinfrastruktur von einem *Access broker* zu erhalten. Dies sind Cyberkriminelle, die sich mithilfe von Exploits, Botnets, Phishing, Social Engineering, etc. (dauerhaften) Zugang zu Netzwerken verschaffen und diese weiterverkaufen.
Unabhängig davon, ob ein Angreifer (hier Affiliate) seine, als Service erworbene, Ransomware selbst steuert oder vollautomatisiert laufen lässt, ist die Einstiegshürde für Cyberkriminelle mit RaaS sehr gering. Manche RaaS-Anbieter stellen einfach zu bedienende Web-Oberflächen (maßgeschneiderte Decryption-Tools, Zahlungsübersichten, Ransomware-Builder, etc.) zur Verfügung. Andere bieten einen 24/7-Live-Support, der sowohl bei technischen Problemen, als auch bei der Wahl der richtigen Lösegeldhöhe unterstützt.[SZ21] Dies führt dazu, dass Ransomware einer breiteren Masse an Kriminellen zur Verfügung steht und die Anzahl der Angriffe zunimmt, was wiederum den Gewinn für alle Beteiligten steigert. Gleichzeitig wird es Strafverfolgungsbehörden und Forschern erschwert, die Initiatoren des Angriffs zu ermitteln, da die Spuren oft nur auf die Servicebetreiber, aber nicht auf die eigentlichen Angreifer zurückzuführen sind.[MST22]

Cerber war eine der ersten und erfolgreichsten Ransomware-Familien, die mit diesem Geschäftsmodell vertrieben wurde.[SR17] Diese Ransomware übermittelte ihre Lösegeldforderung neben der typischen Textform auch als Sprachnachricht, weswegen sie von Betroffenen als „gruselig“ empfunden wurde. In späteren Versionen wurde *Cerber* zu einer sog. Mehrfach-Malware ausgebaut, die neben der Ransomware auch Malware ausführte, die die betroffenen Systeme zum Teil eines bösartigen Botnets machte.[Pik16]
Zusätzlich gab es in 2016 zwei Neuheiten für die Ransomware-Entwicklung. Mit *KeRanger* wurde die erste Ransomware speziell für MacOS veröffentlicht [Ars17] und *Ransom32* machte sein Debüt als erste in JavaScript implementierte Ransomware, die zudem ein weiterer Vertreter des RaaS-Geschäftsmodells ist.[Sar16]

Die *Petya*-Ransomware-Familie verzichtete auf das Verschlüsseln von einzelnen Daten und überschrieb stattdessen den Master Boot Record (MBR) mit einem maßgeschneiderten Bootloader, der einen kleinen bösartigen Kernel lud. Dieser Kernel begann dann mit der Verschlüsselung der Master File Table (MFT) der Festplatten, wodurch das

Dateisystem unlesbar und der Zugriff auf die darunterliegenden Dateien unmöglich wurde.[Lab16; Sno16b] Da *Petya* zum Ausführen Administratorenrechte benötigte, konnte eine Infektion verhindert werden, indem diese Rechte nicht gewährt wurden. Um dieses Problem zu umgehen, wurden neuere Versionen zusammen mit der „Backup-Ransomware“ *Mischa* verbreitet, welche keine Administratorenrechte benötigte und Dateien klassisch einzeln verschlüsseln konnte. Abhängig davon, ob das Opfer Administratorenrechte gewährt hat, wurde entweder *Petya* (mit Admin) oder *Mischa* (ohne Admin) ausgeführt.[Sno16a; Lab17]

Das Jahr 2017 wurde maßgeblich durch einen der größten Ransomware-Angriffe (betroffene Systeme) bis dato geprägt.[Swi21] *WannaCry* wurde weltweit verbreitet und hatte bereits innerhalb der ersten Stunde über 7000 Systeme infiziert. Bis die Ransomware durch die Entdeckung eines Killswitch entschärft werden konnte, fielen ihr bis zu 300.000 Systeme zum Opfer, darunter auch viele Krankenhäuser und andere wichtige Sektoren des öffentlichen Lebens.[Reu17; BB17; r117] Den Zugang zu den Systemen der Opfer verschaffte sich *WannaCry* mithilfe eines ursprünglich von der NSA entwickelten Zero-Day-Exploits namens „EternalBlue“, welcher eine Schwachstelle in Microsoft Windows „Server Message Block (SMB) Version 1 (SMBv1)“-Protokoll ausnutzt. Dieser ermöglicht Fernzugang zu Netzwerken und allen sich darin befindlichen Systemen sowie die Ausführung von beliebigem Code auf diesen.[Sch18; MS-19] In modernen Versionen von Windows ist diese Schwachstelle bereits behoben, ältere Versionen sind jedoch nach wie vor anfällig. Die weitere Ausbreitung der Ransomware konnte nur verhindert werden, da Sicherheitsexperten herausfanden, dass *WannaCry* zu Beginn der Laufzeit prüft, ob eine spezielle Domain erreichbar ist. Wenn die Domain auf die Anfrage der Ransomware antwortet, wird die weitere Ausführung abgebrochen, andernfalls fährt die Ransomware fort und das System wird verschlüsselt.[0xZ22; Lin17] Einer der Forscher registrierte die gefundene Domain und aktvierte damit den eingebauten Killswitch der Ransomware. Entschlüsselungstools für *WannaCry* existieren, beruhen jedoch auf der Grundlage, dass die zur Generierung der RSA- Verschlüsselung notwendigen Primzahlen noch im Speicher des betroffenen Systems vorhanden sind.[Kha17]
Auf Basis des gleichen Exploits wurde eine angepasste und verbesserte Version von *Petya*, *NotPetya* verwendet, um Unternehmen weltweit zu erpressen. Im Unterschied zum Vorgänger konnte sich *NotPetya* selbständig in einem Netzwerk verbreiten und verschlüsselte alle Dateien anstelle nur der MFT der Festplatten. Entgegen der Behauptung in der Lösegeld-

forderung (siehe Abb. 2.5) war sie so konzipiert, dass die Daten nicht wieder entschlüsselt werden konnten und effektiv vernichtet wurden.[Clo18] Als eigentliches Ziel des Angriffs wird die Ukraine angenommen, da sich dort die Mehrheit der betroffenen Unternehmen befand. Zudem wird Russland als Drahtzieher hinter der Ransomware vermutet und der Angriff somit als politisch motiviert eingeordnet.[Nak18; Kov18]

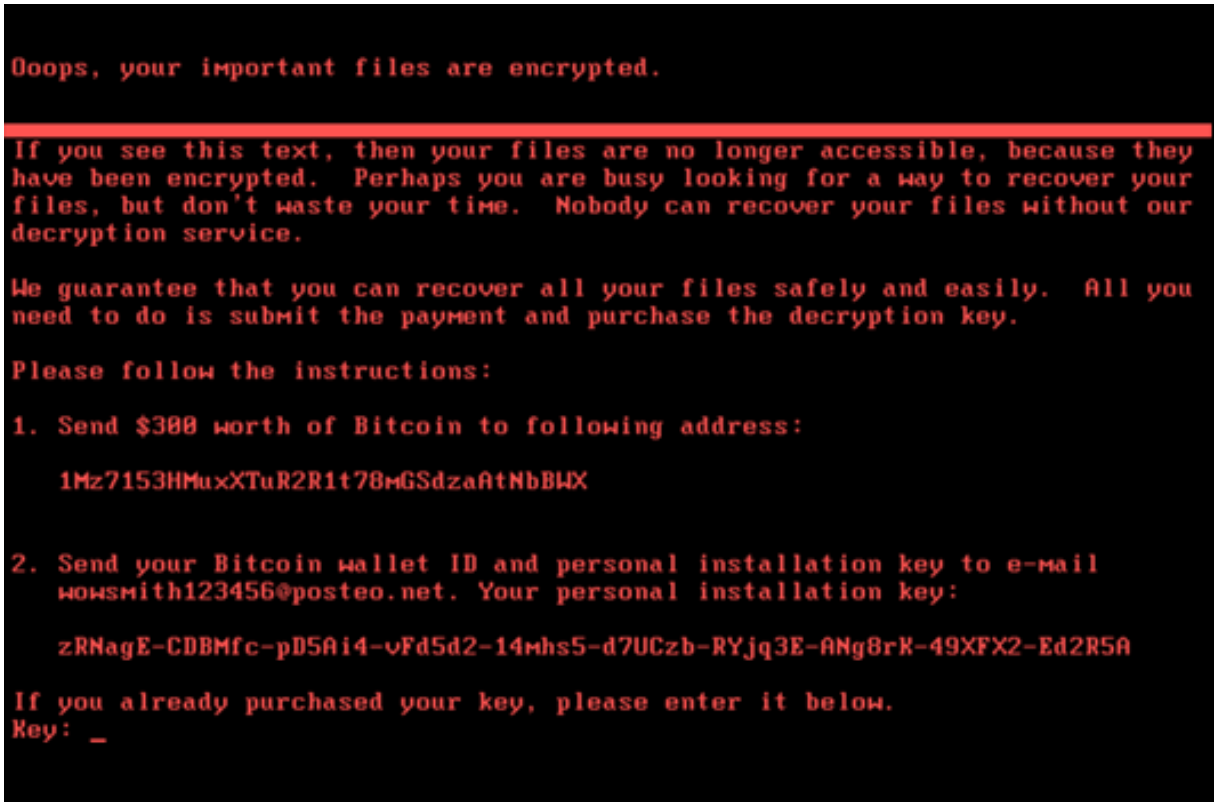


Abbildung 2.5: Screenshot einer Lösegeldforderung von NotPetya aus [Hur17]

2018 trat zum ersten mal die Ransomware *PureLocker*, ein weiteres RaaS-Angebot, auf. Im Unterschied zu vielen anderen Familien ist diese Malware in der Programmiersprache PureBasic geschrieben, welche mehrere Vorteile für die Angreifer bietet. Zum einen haben Anbieter von Antivirensoftware Probleme bei der korrekten Detektion von PureBasic-Binärdateien mittels Signaturen, zum anderen lässt sich der Code leicht in ausführbare Dateien für alle gängigen Plattformen umwandeln. Zusätzlich wurde die Ransomware so entwickelt, dass die bösartigen Funktionen verborgen bleiben, wenn sie nicht mit den korrekten Parametern ausgeführt wird. Laut Sicherheitsforschern werden so die Erfolgschan-

cen erhöht, dass die Ransomware unentdeckt bleibt und dann für gezielte Angriffe genutzt werden kann.[Kaj19]

In 2019 stand der Trend des Big Game Hunting (BGH) im Vordergrund. Das Cybersicherheitsunternehmen Crowdstrike definiert diesen als „[...] a type of cyberattack that usually leverages ransomware to target large, high-value organizations or high-profile entities.“. Die Rede ist von Cyberangriffen, die meist mit Ransomware speziell gegen große und renommierte Unternehmen gerichtet sind.[Cro22] Bei der Auswahl der Opfer ist entscheidend, ob sie zur Zahlung hoher Lösegelder in der Lage sind und dies mit hoher Wahrscheinlichkeit auch tun, um ihren Geschäftsbetrieb wieder aufzunehmen oder Druck aus der Öffentlichkeit zu vermeiden. Beispiele für Ziele von BGH-Angriffen sind: große Unternehmen, Gesundheitseinrichtungen, Behörden, Banken, hochvermögende Privatpersonen (Prominente, Geschäftsführer großer Unternehmen) oder Unternehmen, die mit besonders sensiblen Daten arbeiten.
Als prominenteste Beispiele von für BGH im Jahr 2019 eingesetzte Ransomware gelten *Ryuk*, *REvil* (auch bekannt unter *Sodinokibi*) und *LockBit*. Während *Ryuk* von seinen Betreibern selbst eingesetzt wird [Cro19], werden die als RaaS angebotenen *REvil* und *Lockbit* von Dritten eingekauft, um BGH zu betreiben.[Cro22] Die Webseite ransomwhere.re sammelt mittels Crowdsourcing Daten zu Ransomware Lösegeldzahlungen und zeigt, dass *Ryuk* und *REvil* bis September 2022 7,2 Mio. und 12,1 Mio. USD erpressen konnten.[Cab22]

Das Jahr 2020 wird nicht nur durch die Corona-Pandemie selbst, sondern auch durch Ransomware, die die Not der Menschen ausnutzt, geprägt. Ein Beispiel dafür ist *Corona-Virus*, welche neben der Verschlüsselung von Daten auch versucht, Benutzernamen und Passwörter zu stehlen.[Wue20] Double Extortion Ransomware-Angriffe gegen Gesundheitseinrichtung sind besonders effektiv, da Patientendaten nicht nur besonders schützenswert im Sinne der Datenschutz-Grundverordnung (DSGVO) sind, sondern auch wichtige Informationen für die Behandlung eines Patienten enthalten können.
Des Weiteren beginnt eine vermutlich in Russland ansässige Cybercrime-Gruppe mit dem Einsatz und dem Vertrieb von *Conti* als RaaS. Die Conti-Gruppe wird von Microsoft als DEV-0193 (TrickBot LLC) und als einer der einflussreichsten Akteure der cyberkriminellen Welt geführt. Laut Unit 42 war Conti in 2021 mit über 500 Opfern für rund 15.5% aller Ransomware-Vorfälle verantwortlich.[uni22] Microsofts (und anderen) Forschungen zufolge ist die Gruppe für Entwicklung, Vertrieb und Management von verschiedenen Malware-

Payloads (z.B. TrickBot, Bazaloader, AnchorDNS, etc.) sowie die RaaS-Angebote *Ryuk* (Betrieb seit 2020 eingestellt), *Conti* und *Diavol* verantwortlich.[Tea22] Durch seine großflächige Verbreitung über das RaaS-Modell zählt *Conti* mit ca. 17,4 Mio. USD (Stand 09.2022, siehe Anhang A.3) erbeutetem Lösegeld zu der erfolgreichsten Ransomware überhaupt.[Cab22]

Mitte 2021 wird zum ersten Mal eine verbesserte Version von *LockBit*, *LockBit 2.0* detektiert. Die neue Version wird ebenso wie der Vorgänger als RaaS angeboten und ist nun in der Lage Shadow-Copies zu löschen, sich selbständig weiter zu verbreiten und die Lösegeldforderung auf im Netzwerk detektierten Druckern auszudrucken. Da *LockBit 2.0* Dateien nur partiell (erste 4 Bytes) verschlüsselt und einen Multithreading-Ansatz nutzt, können ca. 25 Tsd. Dateien pro Minute verschlüsselt werden. Damit ist sie die am schnellsten verschlüsselnde Ransomware auf dem Markt (in 2021).[SOC22; Don22]
Zum Ende des Jahres wird die Ransomware *BlackCat* (auch bekannt als *ALPHV* oder *Noberus*) als RaaS angeboten. Die Ransomware ist in Rust geschrieben und wird, plattformunabhängig, vor allem gegen Windows, Linux und im VMware ESXi-Kontext eingesetzt.[Hil22] Des Weiteren bedient sich *BlackCat* der Triple Extortion-Methode. Zum einen drohen die Angreifer mit der Veröffentlichung von vor der Verschlüsselung kopierten Daten auf einer Leak-Site, zum anderen werden DDoS-Angriffe angedroht, sollte das Lösegeld nicht (rechtzeitig) gezahlt werden.[uni22; HTS22]

Zu Beginn des Jahres 2022 nutzt die Ransomware *Deadbolt* eine Schwachstelle in QNAP-NAS-Geräten, um Zugriff zu erlangen und die vorhandenen Daten zu verschlüsseln. Neben der Tatsache, dass die Ransomware ausschließlich NAS-Geräte befällt, ist auch die Lösegeldforderung (siehe Abb. 2.6) eine Besonderheit. Die Angreifer bieten sowohl den direkt Betroffenen, als auch dem Betreiber der NAS-Firmware (QNAP) die Möglichkeit, Lösegeld zu zahlen. Im Falle der Betreiber werden 5 BTC (ca. 184 Tsd. USD) für die Übergabe von Details zur verwendeten Schwachstelle oder 50 BTC (ca. 1,85 Mio. USD) für den Erhalt des Master-Encryption-Key und die Details zu Schwachstelle, gefordert.[Abr22] Jedoch zeigen spätere Analysen, dass ein solcher Master-Encryption-Key nicht existiert haben kann.[Mic22]
Im Juni tritt zum ersten Mal die Ransomware *BlueSky* auf. Analysen zeigen, dass *BlueSky* explizit für schnelle Verschlüsselung via Multithreading und Lateral Movement in Active Directory (AD)-Umgebungen entwickelt wurde. Teile des Codes haben hohe Übereinstimmungen mit dem Code aus *Conti* und *Babuk*-Ransomware.[Ji22] Obwohl bis August nur

wenige Infektionen gemeldet wurden, gehen Analysten aufgrund der modernen und sorgfältig entwickelten Fähigkeiten der Ransomware davon aus, dass die Anzahl der Fälle noch steigen wird.[Wal22]

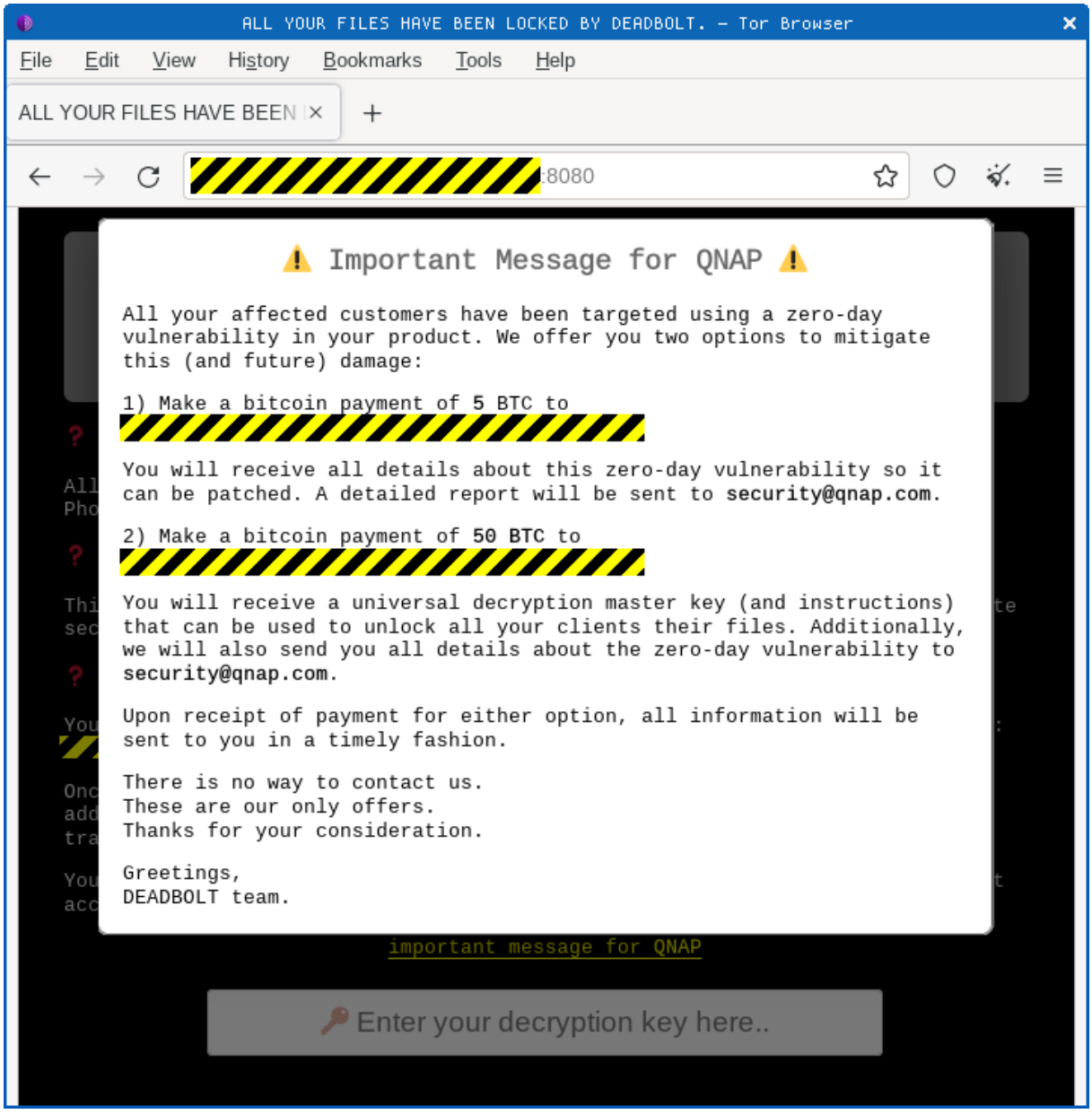
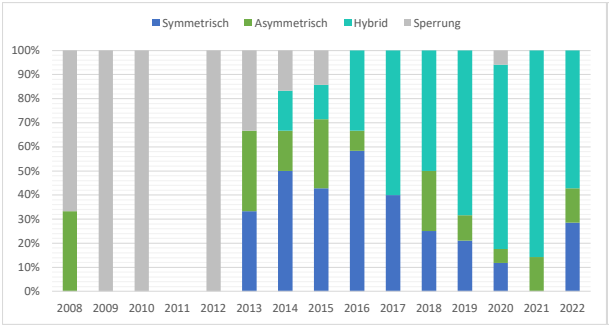
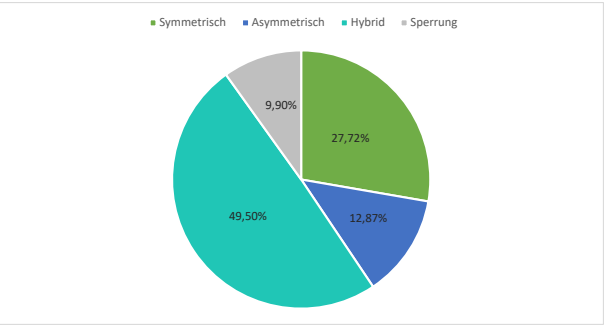


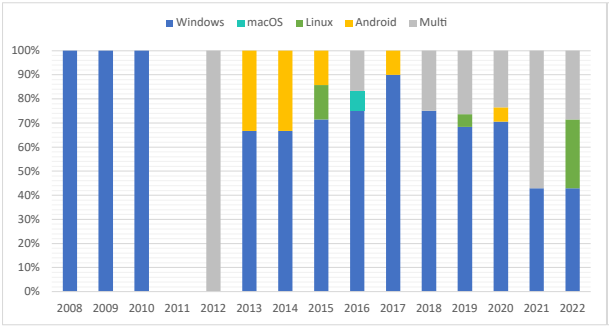
Abbildung 2.6: Screenshot einer Lösegeldforderung von Deadbolt [SOP22]



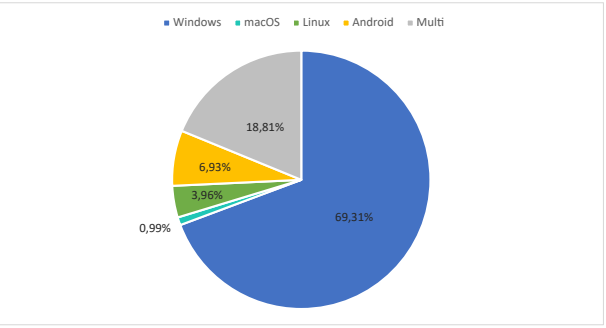
(a) Verteilung der Verschlüsselungsarten pro Jahr



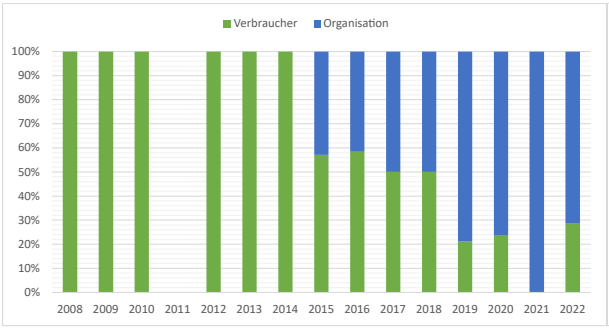
(b) Verteilung der Verschlüsselungsarten gesamt



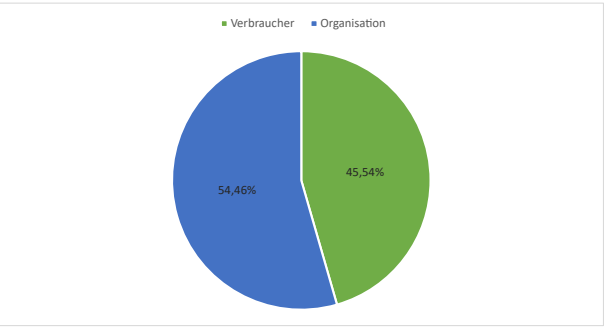
(c) Verteilung der Plattformen pro Jahr



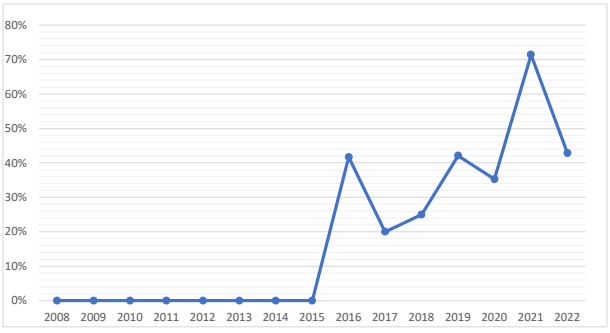
(d) Verteilung der Plattformen gesamt



(e) Verteilung der Opferarten pro Jahr



(f) Verteilung der Opferarten gesamt



(g) Prozentualer Anteil von RaaS pro Jahr

Abbildung 2.7: Historische Verteilung verschiedener Ransomware-Eigenschaften

Neben den in Abbildung 2.3 aufgeführten Ransomware-Familien wurde im Rahmen dieser Arbeit auch eine Liste mit weiteren Familien und ihren Eigenschaften erstellt (siehe Anhang A.1), deren Auswertung (Tabelle: Anh. A.2, Diagramme: Abb. 2.7) im Folgenden genutzt wird, um Trends in der historischen Entwicklung von Ransomware zu erkennen. Die Liste wurde auf der Grundlage einer ähnlichen Tabelle von [Oz22] erstellt und in Eigenarbeit erweitert. Sie umfasst 101 verschiedene Ransomware-Familien in einem Zeitraum von 2008 bis (Mitte) 2022. Die Auswertung ist ausschließlich auf die Daten der Tabelle beschränkt und somit nicht repräsentativ für die Gesamtheit aller Ransomware-Familien. Bis ca. 2013/14 ist die Abdeckung der Berichterstattung über Ransomware-Angriffe und die dazugehörigen Ransomware-Familien, abgesehen von wenigen prominenten Beispielen, so schwach, dass sich kaum verifizierbare Aussagen über Ransomware in diesem Zeitraum treffen lassen. Dies erklärt auch das Fehlen von Daten für das Jahr 2011.
Die Auswahl der Ransomware-Familien für ein jeweiliges Jahr fand zufällig statt und stellt keinen akkuraten Querschnitt für das Jahr dar. Da die Anzahl der pro Jahr gelisteten Familien stark variiert, ist der Vergleich von zwei unterschiedlichen Jahren mit Vorsicht zu betrachten. Dennoch lassen sich gewisse Trends und Entwicklungen feststellen.
Die Diagramme 2.7a und 2.7b zeigen die Verteilung der in der Taxonomie vorgestellten Verschlüsselungsarten (und Sperrung). Allgemein nutzen ca. 50% aller Ransomware-Familien den hybriden Verschlüsselungsansatz. Die Verteilung über die Jahre zeigt, dass dies ein Trend ist, der sich seit ca. 2016 zunehmend durchsetzt.
In Bezug auf die Plattformen ist zu erkennen, dass ca. zwei Drittel der Ransomware-Familien das Betriebssystem Windows zum Ziel haben (siehe Abb. 2.7d). Dazu zählt sowohl Windows für Benutzer (Windows XP, Windows 7, etc.), als auch Windows Server. Der Trend von Multi-Betriebssystem-Ransomware zeigt sich ab ca. 2018 (siehe Abb. 2.7c). In diese Kategorie fallen alle Familien, die z.B. sowohl Linux, als auch Windows-Systeme angreifen. Das Betriebssystem Linux als alleiniges Ziel-OS ist selten vertreten, bietet jedoch eine besonders hohe Diversität von Angriffszielen (QNAP, ESXi, Linux-Server, etc.).
Die Auswertung der Opferarten im Gesamtbild (Abb. 2.7f) ist eher ausgeglichen und bietet nur einen geringen Erkenntniswert. Aufschlussreicher ist die Verteilung pro Jahr (Abb. 2.7e), welche einen ab ca. 2015 stetig steigenden Anteil an auf Organisationen fokussierter Ransomware zeigt. Das gezielte Angreifen von einzelnen Verbrauchern, anstelle von Unternehmen oder Einrichtungen, macht ab 2019 nur noch ca. ein Fünftel der Angriffe aus.
Das Diagramm 2.7g zeigt, dass sich die Häufigkeit von Ransomware-as-a-Service (RaaS)

seit 2016 in einem aufsteigenden Trend befindet. Lässt man die Jahre 2008 bis 2015 außen vor, wird ca. die Hälfte aller Ransomware als Service zum Kauf angeboten.

2.5 Lebenszyklus von Ransomware

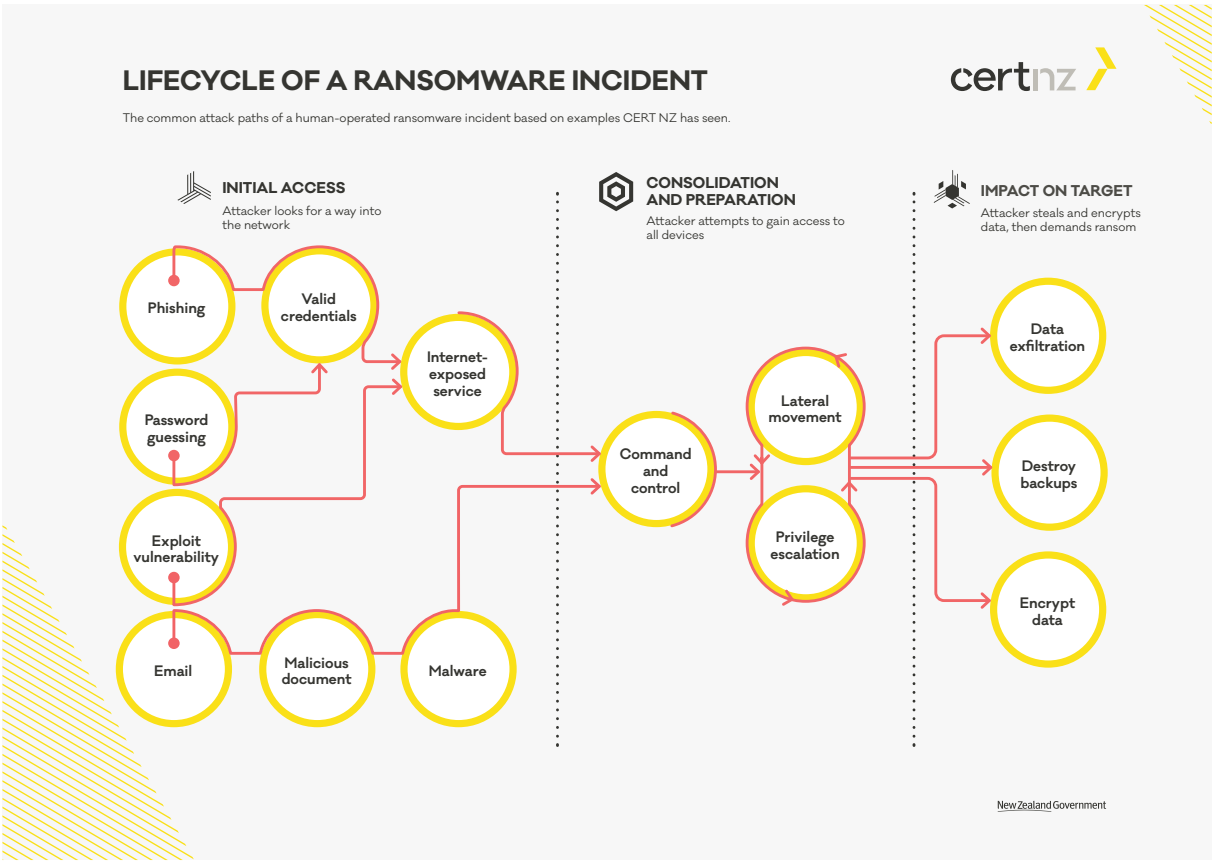


Abbildung 2.8: Lebenszyklus von Ransomware aus [NZa]

Ein weiterer wichtiger Schritt für das Verständnis von Ransomware ist der Lebenszyklus mit seinen Angriffsphasen und Angriffstechniken. Das neuseeländische Computer Emergency Response Team (CERT) *CERT NZ* hat zu diesem Zweck eine Übersicht für den Ablauf eines von Menschen gesteuerten Ransomware-Angriffs erstellt (siehe Abb. 2.8).[NZa] Die Übersicht ist eine Zusammenfassung von mehreren durch das CERT NZ beobachteten Angriffsabläufen und ist somit keine 1:1 Anleitung für jeden Ransomware-Angriff, bietet jedoch eine gute Übersicht und ermöglicht die Grundstrukturen dieser Art von Angriffen

zu erkennen. Zusätzlich werden die Techniken und Taktiken des ATT&CK-Frameworks eingebunden, sodass Vergleiche zu anderen Angriffen leicht möglich sind und konkrete Angriffe schnell um weitere Taktiken/Techniken erweitert werden können.
Das ATT&CK-Framework von MITRE ist eine globale für jeden öffentlich zugängliche Wissensdatenbank. Es beschreibt das Verhalten sowie die verwendeten Techniken, Taktiken und Tools von Cyberkriminellen und ermöglicht damit Rückschlüsse auf die Sicherheit und Risiken in der eigenen Infrastruktur.[MIT]
Wie Abbildung 2.8 zeigt, lässt sich der Lebenszyklus von Ransomware in die drei Phasen *Initial Access*, *Consolidation and Preparation* und *Impact on Target* einteilen. Diese Phasen besitzen auch für automatisierte Ransomware-Angriffe Gültigkeit, sind aber häufig unterschiedlich stark ausgeprägt.

2.5.1 Initial Access

Die erste Phase eines Ransomware-Angriffs ist *Initial Access*, das erste Eindringen in das anvisierte Netzwerk, und wird in den meisten Fällen auf einem von drei Wegen bewerkstelligt. Der erste Weg ist das Eindringen mithilfe von kompromittierten Zugangsdaten für aus dem Internet erreichbare Services (z.B. VPN oder RDP). Die Zugangsdaten erhalten die Kriminellen dabei durch z.B. Phishing- oder Brute-Force-Angriffe.
Der zweite Weg ist die Ausnutzung von Schwachstellen oder Exploits. Je mehr Geräte von solchen Betroffen sind, desto höher ist die Wahrscheinlichkeit, dass Cyberkriminelle sich auf diesem Weg Zugang verschaffen können.
Der dritte Weg ist das Verschicken von Emails, die mit Malware infiziert sind. Die Infizierung erfolgt meist über präparierte Dateien oder Links auf welche der Betroffene klicken muss, damit die Malware im System Fuß fassen kann. Für diesen Weg häufig genutzte Malware sind z.B. Qakbot, Bazar oder TrickBot.[NZd]
Die verwendeten MITRE ATT&CK Techniken sowie Kurzbeschreibungen können Tabelle A.3 entnommen werden.

2.5.2 Consolidation and Preparation

In der zweiten Lebensphase eines Ransomware-Angriffs beginnt der Angreifer seine Kontrolle über das frisch kompromittierte Netzwerk auszuweiten und trifft Vorbereitungen für die letzte Phase. Ziel ist es, Zugang zu allen relevanten Geräten des Netzwerks (Server und Clients), Domain-Administratorenrechten sowie Backup-, Sicherheits- und Virtualisierungssystemen zu erhalten.
Zu diesem Zweck wird als Erstes das sog. Command and Control (C2) eingerichtet. In den meisten Fällen wird dazu ein fertiges Werkzeug, wie z.B. CobaltStrike, eingesetzt, welches genutzt wird, um das Netzwerk zu erkunden und weitere Tools (z.B. Mimikatz oder BloodHound) für die nächsten Schritte bereitzustellen.
Nachdem C2 etabliert wurde, beginnt der Angreifer mit den Schritten Lateral Movement und Privilege Escalation. Diese laufen häufig nebenläufig ab und ergänzen sich gegenseitig. Lateral Movement beschreibt die schrittweise Bewegung durch die Systeme des Netzwerks auf der Suche nach nützlichen Informationen (sensible Daten, Passwörter, etc.). Damit die Suche möglichst unauffällig stattfinden kann, versuchen Angreifer zuerst native Tools des jeweiligen Betriebssystems zu nutzen, bevor sie eigene Tools verwenden. Gleichzeitig versucht der Angreifer durch das Ausnutzen von Schwachstellen im Betriebssystem oder in anderen Anwendungen erhöhte Zugriffsrechte (z.B. Administratorenrechte) zu erlangen. Von C2 bereitgestellte Tools wie Mimikatz können zusätzlich genutzt werden, um weitere Zugangsdaten zu erhalten. Mit diesen Zugangsdaten können neue Pfade/Geräte im Netzwerk erschlossen werden, die wiederum durchsucht und genutzt werden, um weitere Zugangsdaten zu entdecken. Dieser Zyklus findet in der Regel so lange statt, bis dem Angreifer alle relevanten Systeme und Zugangsdaten bekannt sind.[NZb]
Die verwendeten MITRE ATT&CK Techniken und Tools sowie Kurzbeschreibungen können Tabelle A.5 entnommen werden.

2.5.3 Impact on Target

In der dritten und letzten Phase hat der Angreifer bereits Zugriff auf alle für ihn relevanten Daten, Systeme sowie Accounts und kann nun die eigentlichen bösartigen Aktionen (siehe Abschnitt Klassifizierung über die bösartige Aktion) durchführen.

Dabei beginnt der Angreifer, wenn gewollt, mit der Exfiltration von Daten aus dem Zielnetzwerk. Damit dieser Prozess möglichst lange unentdeckt bleibt, können verschiedene Maßnahmen (z.B. Verschlüsselung des Datenverkehrs, Komprimierung der Daten, zeitlich gestaffelte Downloads) getroffen werden. Die Einsatz dieser Maßnahmen erhöht jedoch den zeitlichen Aufwand.
Sind alle gewünschten Daten exfiltriert, versucht der Angreifer alle Arten von Backups zu zerstören, um eine Wiederherstellung ohne Lösegeldzahlung zu verhindern.
Als letzter Schritt werden alle kompromittierten Systeme verschlüsselt und entsprechende Lösegeldforderungen gestellt.[NZc; BSI22b]
Die verwendeten MITRE ATT&CK Techniken sowie Kurzbeschreibungen können Tabelle A.6 entnommen werden.

2.6 Maßnahmen gegen Ransomware

Die Schutzmaßnahmen gegen Malware- sowie Ransomware-Angriffe lassen sich in die drei Bereiche *Prävention*, *Detektion* und *Reaktion* einteilen.[Hop14] Diese Bereiche werden im Folgenden genauer betrachtet.

2.6.1 Prävention

Bei Prävention spricht man von Schutzmaßnahmen, die ergriffen werden sollten, bevor eine Infektion mit Malware stattfinden kann. Beispiele für präventive Maßnahmen, speziell gegen Ransomware, können dem vom BSI veröffentlichen *Maßnahmenkatalog Ransomware* [BSI22d] entnommen werden:

- Datensicherungskonzepte (Backups)
- Mitarbeiterschulungen (z.B. gegen Phishing)
- Aktives Schwachstellenmanagement (regelmäßige Scans und Updates)
- Remotezugänge absichern (z.B. VPN mit Multi-Faktor-Authentifizierung (MFA), Lockout-Policy)

- Sicherer Umgang mit Administrator Accounts (z.B. MFA, Need-To-Know-Prinzip)
- Zugriffe auf Ransomware-C2 Server überwachen/blockieren (z.B. abuse.ch)
- Deaktivieren oder Beschränken von Scripting Umgebungen (z.B. Powershell) und Makros (z.B. Microsoft Office-Anwendungen)
- Anwendungskontrolle (z.B. Application Whitelisting, Verzeichnisregeln)
- konsequente Verwendung von Virenschutzsystemen

2.6.2 Detektion

Wenn die Infektion bereits stattgefunden hat und sich ein Angreifer unbekannt im Netzwerk bewegt, werden Maßnahmen zur Detektion genutzt, um diese Bewegungen zu erkennen und Alarm zu schlagen. Die Detektion von Ransomware wird ausführlich im Kapitel 3 „Detektion“ betrachtet.

2.6.3 Reaktion

Die Maßnahmen des Bereiches Reaktion greifen, wenn ein Angriff detektiert wurde. Dabei macht es (im Kontext der Maßnahmen) nur einen geringen Unterschied, ob der Angriff vollendet wurde, oder frühzeitig erkannt wurde. Das BSI rät ruhig zu bleiben und die folgenden Schritte einzuleiten [BSI22f]:

- Strafanzeige erstellen
- Incident Response
  - Schadensbegrenzung (z.B. Trennen betroffener Geräte von Netz)
  - forensische Untersuchung
    - Bestimmung Infektionsvektoren
    - Schließen gefundener Sicherheitslücken
    - Abgleichen mit und ggf. Anpassung der Präventions-/Detektionsmaßnahmen

- Wiederherstellung des Betriebs

Wurde ein Ransomware-Angriff erst nach seiner Vollendung erkannt, besteht außerdem die Möglichkeit Unterstützung bei Seiten oder Organisationen wie *No more ransom* zu suchen. Diese halten Verzeichnisse von Schlüsseln und Entschlüsselungstools vor, welche unentgeltlich genutzt werden, um Dateien von bestimmten Ransomware-Varianten wieder zu entschlüsseln.[nom22]

Kapitel 3

Detektion

Dieses Kapitel befasst sich genauer mit der Detektion von Malware und ihrer Unterkategorie Ransomware. Zuerst wird der Begriff Detektion definiert und die Probleme sowie Ziele vorgestellt. Darauf folgt eine allgemeine Übersicht über die Kategorien der Malwaredetektion und eine Betrachtung von speziell für Ransomware entwickelte Detektionsmechanismen. Abschließend werden Angriffserkennungssysteme sowie deren Nützlichkeit für die Detektion von Ransomware behandelt.

3.1 Definition

Die Detektion von Malware beschreibt den Prozess der Erkennung des Vorhandenseins von Malware auf einem Host-System bzw. der Unterscheidung, ob ein Programm bös- oder gutartig ist.[KKV11] Dieser Prozess wird erst notwendig, wenn ein Angreifer alle Präventionsmaßnahmen überwinden konnte und sich dadurch im internen Netz befindet. Gerade wenn Unternehmen das Ziel der Angreifer sind, reichen Präventionsmaßnahmen häufig nicht aus, um heutige maßgeschneiderte und hochkomplexe Malware-Angriffe abzuwehren. In diesem Fall ist ein gut funktionierender Detektionsprozess notwendig. Denn je früher ein Angriff erkannt werden kann, desto besser kann der Schaden begrenzt werden.[Str21] Detektion von Malware besteht aus den drei Phasen *Malware-Analyse*, *Extraktion von Merkmalen* und *Klassifizierung* (siehe Abb. 3.2). Die Phase der *Malware-Analyse* betrachtet Malware und versucht mithilfe von statischen (Quellcode) und dynamischen (zur Laufzeit) Analysen den Inhalt sowie das Verhalten zu verstehen und zu dokumentieren.

Während der *Extraktion von Merkmalen* werden die Informationen der vorherigen Phase durch Data-Mining-Verfahren verarbeitet und Merkmale (engl. features) der untersuchten Malware generiert. In der Phase der *Klassifizierung* werden diese Merkmale genutzt, um zu entscheiden, ob eine Eingabe gut- oder bösartig ist. Diese Einstufung findet heutzutage oft durch Machine-Learning-Algorithmen, welche auf Basis von statistischen Wahrscheinlichkeiten Entscheidungen trifft, statt.[AS20]

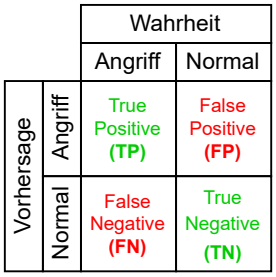


Abbildung 3.1: Konfusionsmatrix

$$\text{Trefferquote} = \frac{TP}{TP + FN} \tag{3.1}$$

$$\text{Wirksamkeit} = \frac{TP}{TP + FP} \tag{3.2}$$

$$\text{Falsch-negativ-Rate} = \frac{FN}{FN + TP} \tag{3.3}$$

$$\text{Falsch-positiv-Rate} = \frac{FP}{FP + TN} \tag{3.4}$$

$$\text{Genauigkeit} = \frac{TP + TN}{TP + TN + FP + FN} \tag{3.5}$$

Die Effektivität eines Detektionsprozesses kann mithilfe einer Konfusionsmatrix (siehe Abb. 3.1) bestimmt werden. Dabei wird die Klassifizierung mit der Wahrheit verglichen. Die getroffenen Entscheidungen werden ausgewertet und in die vier Kategorien *True Positive (TP)*, *True Negative (TN)*, *False Positive (FP)* und *False Negative (FN)* eingeordnet. Ereignisse sind dann *True Positive* bzw. *True Negative*, wenn die Klassifizierung der Wahrheit entspricht. Als *False Positive* wird ein Ereignis eingeordnet, wenn ein Angriff vorhergesagt wurde, es jedoch keiner ist. Umgekehrt wird ein Ereignis, das nicht als Angriff klassifiziert wird, jedoch einer ist, als *False Negative* eingeordnet.
Nachdem die Matrix vollständig befüllt ist, können Qualitätskriterien wie Trefferquote, Wirksamkeit, Falsch-negativ-Rate, etc. durch Formeln (siehe Formeln 3.1, 3.2, 3.3, 3.4, 3.5) bestimmt werden. Die *Trefferquote* beschreibt den Anteil von korrekt als Angriff erkannten Ereignissen aus der Menge der tatsächlichen Angriffe (Spalte „Wahrheit - Angriff“). Der Anteil von korrekt als Angriff erkannten Ereignissen aus der Menge der erkannten Angriffe (Zeile „Vorhersage - Angriff“) wird *Wirksamkeit* genannt. Neben Auswertungen für die Anzahl der richtigen Treffer ist auch die Bestimmung der *Falsch-negativ-Rate* und *Falsch-positiv-Rate* wichtig. Diese geben an, wie viele Ereignisse fälschlich als Normal bzw. als Angriff, aus der Menge der erkannten Normalen (Zeile „Vorhersage - Normal“) bzw.

Angriffe (Zeile „Vorhersage - Angriff“), klassifiziert wurden. *Genauigkeit* gibt den Anteil von korrekt identifizierten Ereignissen aus der Gesamtheit der Ereignisse an.
Das Ziel ist es, höchstmögliche Werte für *Trefferquote*, *Wirksamkeit* und *Genauigkeit* sowie besonders niedrige *Falsch-negativ/postiv-Raten* mit einem gegebenen Detektionsprozess zu erreichen.

3.2 Herausforderungen

Die Erkennung ist eine nicht triviale Aufgabe, da eine große Anzahl von Faktoren/Merkmalen betrachtet werden muss und der Grat zwischen gut- und bösartigen Programmen sehr schmal sein kann. Bereits ab 1987 veröffentlichte Fred Cohen Artikel u.a. über die theoretische Detektion von (Computer-)Viren und postulierte, dass die Detektion ein NP-vollständiges Problem sei.[Coh87; Coh89] Das (wahrscheinliche) Fehlen einer effizienten Lösung für das Detektionsproblem wurde auch nachfolgend in mehreren Veröffentlichungen von z.B. [ZZZ05, Zuo u.a.], [Spi03, Spinellis] oder [CW01, Chess und White] thematisiert und bestärkt.
Neben der theoretischen Komplexität wurden auch praktische Techniken gefunden, um die Detektion von Malware zu erschweren. Diese ändern den Malware-Code so ab, dass er schwerer zu lesen und verstehen ist. Sie werden *Obfuscation-Techniken* (engl. Obfuscation techniques) genannt und sowohl gegen menschliche, als auch automatisierte Analysen eingesetzt. Einige häufig vorkommende Beispiele sind *Verschlüsselung (Encryption)*, *Packing*, *Substitution*, *Metamorphismus*, *Dummy code insertion* und *Anti-Debug/Anti-Temper*.
Durch die **Verschlüsselung** von Codeblöcken oder ganzen Programmen können diese nicht korrekt analysiert werden. Eine Ausprägung dieser Technik ist der *Polymorphismus*. Dabei wird der Binärcode verschlüsselt und erst zur Laufzeit der Malware wieder entschlüsselt. Währenddessen wird eine neue veränderte Version der Malware verschlüsselt, die für den nächsten Durchlauf der Malware verwendet wird. Das Verhalten der Malware bleibt dabei gleich, jedoch hat jede Version ihre eigene Signatur, was die Detektion erschweren soll.[AHT14]
Bei **Packing** wird die Malware nach der Kompilierung komprimiert. Ein komprimiertes Programm nimmt weniger Speicherplatz in Anspruch und wird daher auch von gutartigen Programmen verwendet. Es muss jedoch vor der Ausführung entpackt werden. Cyberkri-

minelle nutzen die Tatsache, dass komprimierte Informationen, ähnlich wie bei Verschlüsselung, bis zum Entpacken unlesbar sind.[AS20; AHT14]
Durch die **Substitution** von Standard-Compiler-Befehlen mit anderen selteneren Alternativen können die Signaturen von Malware leicht verändert werden, ohne dass das Verhalten angepasst werden muss.[Jey22]
Metamorphismus ist eine Obfuscation-Technik, die den dynamischen Binärcode bei jedem Durchlauf der Malware verändert. Damit wird niemals der gleiche Opcode in den Speicher geladen. Manche Malware ist, durch Kommunikation mit dem Internet, in der Lage, neue Funktionen zur Malware hinzuzufügen und sich weiterzuentwickeln (Open-world Malware).[AHT14]
Das Einfügen von zusätzlichem, für die Malware-Logik irrelevanten Code, wird als **Dummy code insertion** bezeichnet und erschwert die Identifizierung des bösartigen Codeanteils.[Lut21]
Von **Transposition** spricht man, wenn die Reihenfolge von Anweisungen, Routinen und Programmabzweigungen verändert wird, ohne dass die Logik beeinträchtig wird. Dies kann, z.B. durch zufälliges Mischen der Anweisungen und das Einfügen von Jump-Befehlen, um die korrekte Abfolge wiederherzustellen, oder der Identifizierung von unabhängigen Code-Blöcken, welche daraufhin neu angeordnet werden, erreicht werden.[Jey22]

Trotz der genannten Herausforderungen werden ständig neue Methoden/Prozesse/Ansätze mit besserer Genauigkeit, niedrigeren Fehlerraten und schnelleren Entscheidungen entwickelt.

3.3 Detektionsansätze

Das Fehlen eines allumfassenden Detektionsansatzes, welcher jede beliebige Malware effizient erkennen kann, führte zur Entwicklung von verschiedenen Ansätzen, die im Folgenden näher betrachtet werden. Die Abbildung 3.2 zeigt, neben den drei Phasen der Detektion, auch eine Übersicht über die Kategorien von Detektionsansätzen. Die Kategorien basieren auf der Doktorarbeit von Alzarooni zum Thema „Malware Variant Detection“ und wurden um die KI-Basierten Ansätze nach [AS20] erweitert.

Signaturbasierte Detektion nutzt statische Merkmale (z.B. Bytesequenzen, Assembler-Anweisungen, Hashes, etc.) um Malware zu erkennen. Dabei werden die Signaturen der zu untersuchenden Eingabe mit denen einer Signatur-Datenbank abgeglichen. Stimmen die Signaturen überein, handelt es sich mit hoher Wahrscheinlichkeit um Malware. Malware, für die es noch keine Signaturen gibt, sowie Malware, die Obfuscation-Techniken verwendet, können nicht erkannt werden.[AS20]
Verhaltensbasierte Detektion macht sich statische und dynamische Merkmale zunutze, die die Funktionsweise einer Malware beschreiben, um sie erkennen. So kann neue unbekannte oder verwandte Malware erkannt werden, wenn sie gleiches oder ähnliches Verhalten aufweist. Die Gewinnung von Verhaltensmerkmalen ist jedoch aufwändig und teilweise mit hohen Fehlerraten behaftet. Dies ergibt sich z.B. durch Verhalten, die sowohl von gut- als auch bösartigen Programmen geteilt werden. Zudem ist es unmöglich jedes potentielle Verhalten von Malware zu spezifizieren. Dennoch hat dieser Ansatz eine hohe Resistenz gegen Obfuscation-Techniken, da diese meist das Verhalten der Malware nicht ausreichend verändern.[AS20]
Der **Heuristik-Basierte** Ansatz verwendet trainierte Erfahrungswerte (Anomalieerkennung), Regeln, kontextfreie Grammatiken (engl. context-free grammar - CFG) und KI-Techniken, um Systeme nach verdächtigen Merkmalen (statisch und dynamisch) zu durchsuchen. Werden hohe Übereinstimmungen bzw. starke Abweichungen vom Normalbetrieb gefunden, wird das auslösende Programm als bösartig eingestuft.[AS20; Alz12] Auf diese Weise können auch Zero-Day-Angriffe erkannt werden. Aufgrund der hohen Komplexität des heuristischen Ansatzes ist das Erstellen der notwendigen Komponenten mit erheblichem Aufwand verbunden.[Kas21b]
Modellbasierte Detektionsansätze beruhen auf Modellen für die Verifizierung der Korrektheit von Systemspezifikationen. Für die Detektion von Malware wurde dieser erstmals durch [SL03] angewendet. Durch manuelle Extraktion von Malware-Verhalten und Kodierung in Lineare temporale Logik (LTL) können diese LTL-Darstellungen gegen das Verhalten von verdächtigen Programmen verglichen werden.[SL03; Alz12] Die Computation tree predicate logic (CTPL), entwickelt durch [Kin05], ist ein weiterer Modellprüfungsalgorithmus, der erfolgreich für die Detektion von Malware eingesetzt und mehrfach weiterentwickelt wurde.[Kin05; HKV07; Kin10] Da nicht alle Verhaltenspfade gefunden und in Modellsprachen übersetzt werden können (Komplexitäts-Problem), bietet auch dieser Ansatz keine Möglichkeit zur allumfänglichen Detektion.
Ansätze die **Semantik-Basiert** sind, betrachten die Bedeutung von Malware-Code.[Alz12]

Dafür werden z.B. sogenannte Malware-Templates erstellt, die auf einer abstrakten Ebene die Bedeutung/Funktionalität eines Code-Abschnitts abbilden. Zusammen mit einer Methode zur abstrakten Darstellung von beliebigen Programmen können die Templates genutzt werden, um Programme erfolgreich zu klassifizieren.[Chr05]

Künstliche Intelligenz-Basierte Ansätze nutzen verschiedene Techniken aus dem Bereich der künstlichen Intelligenz (KI) wie Deep-Learning, Artificial Neural Networks (ANN) oder Deep Belief Networks (DBN). Mithilfe dieser Techniken werden Modelle trainiert, die in der Lage sind, anhand von erlernten Merkmalen, Malware zu erkennen.[AS20] Da das Training über automatisierte Algorithmen ohne aktive menschliche Unterstützung stattfindet, können die Wissensbasen (Modelle) automatisch um neues Wissen erweitert werden. Allerdings könnten Angreifer präparierte „Malware“ benutzen, die der KI falsche Merkmale antrainiert und somit echte Malware unerkannt bleiben lässt.[Kol18; Gro16]

Die genannten Ansätze haben alle gewisse Vor- und Nachteile, sodass in der Praxis häufig mehrere Ansätze kombiniert werden, um eine hohe Genauigkeit und geringe Fehlerquoten zur gewährleisten.

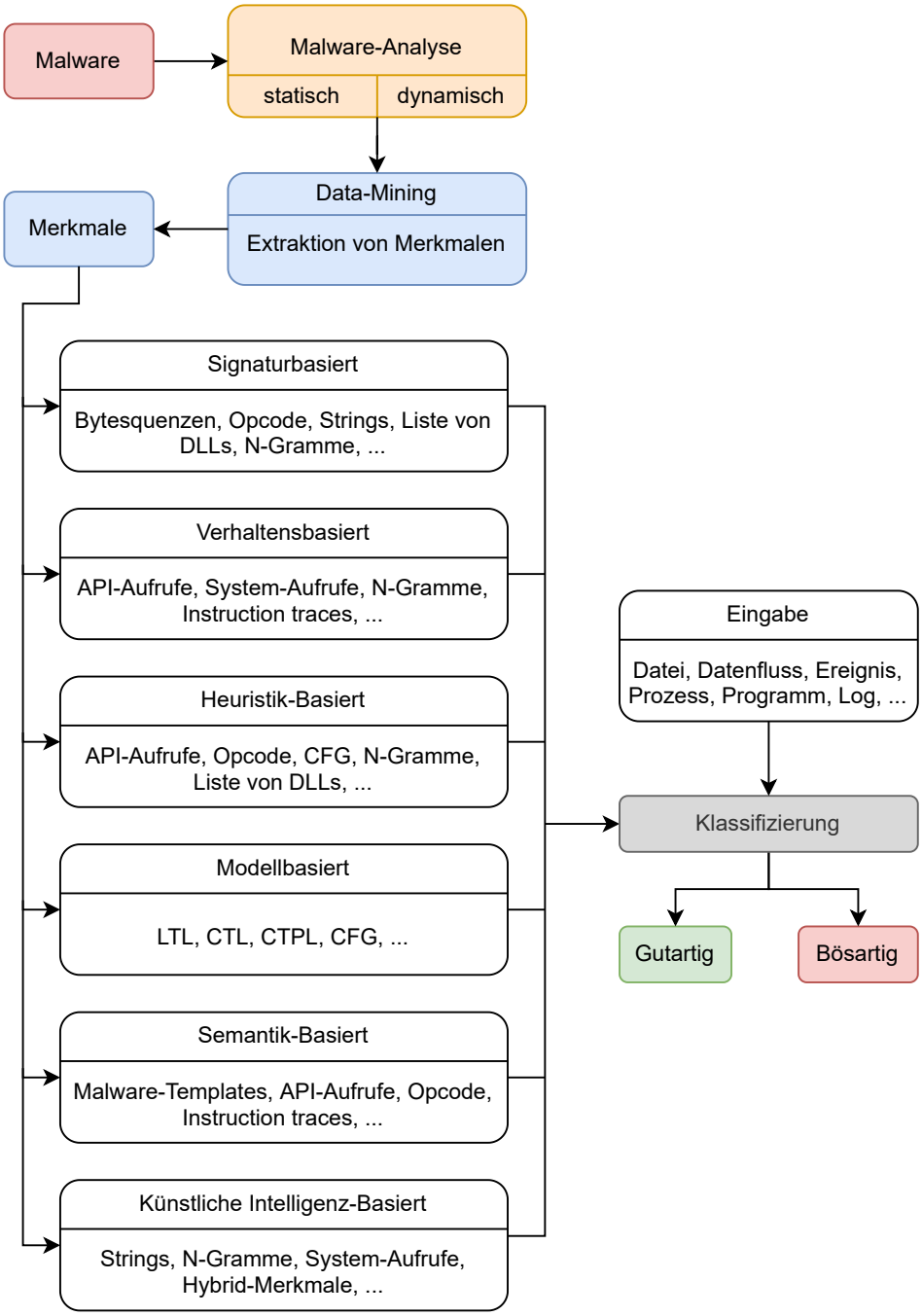


Abbildung 3.2: Übersicht zur Detektion von Malware nach [AS20; Alz12]

3.4 Detektion von Ransomware

Neben den Ansätzen für die allgemeine Erkennung von Malware wurden auch Ansätze primär für die Detektion von Ransomware entwickelt. Diese sind auf Merkmale von Ransomware-Angriffen spezialisiert und haben meist höhere Trefferquoten als allgemeine Ansätze. Im Folgenden werden verschiedene Beispiele für Ansätze zur Erkennung von Ransomware vorgestellt.

Das Konferenzpaper von Kharaz u. a. stellt ein System zur dynamischen und automatischen Erkennung von Ransomware mit dem Namen UNVEIL vor. Dieses nutzt ein verhaltensbasiertes Verfahren, um Ransomware-spezifische Merkmale zu extrahieren. Als Ergebnis zeigte sich, dass erfolgreiche Ransomware-Angriffe immer die Dateien der Benutzer ändern müssen. Auf der Basis dieser Erkenntnis überwacht UNVEIL die Aktivitäten des Dateisystems und erkennt Ransomware-typische Dateioperationen.[Kha16]

Weckstén u. a. untersuchten, wie Ransomware die Backups auf Windows-Systemen nachhaltig löscht und fanden heraus, dass die Angreifer dafür immer auf das windowseigene Tool *vssadmin.exe* zurückgriffen. Durch einfaches Umbenennen dieses Tools waren die untersuchten Ransomwares nicht mehr in der Lage, die Backups zu löschen und verschlüsselte Dateien konnten schnell und einfach wiederhergestellt werden.[Wec16]

Moore testete die Nützlichkeit von Honeypot-Ordnern auf File-Servern für die Ransomware-Erkennung. Ein Honeypot-Ordner ist ein Ordner, der der Ransomware vorgibt, ein echter Ordner mit zu verschlüsselnden Dateien zu sein. In Wirklichkeit wird der Ordner nicht von den Benutzern genutzt oder ist ihnen sogar völlig unbekannt. Jedoch wird der Honeypot-Ordner durch den *File Server Resource Manager* des Windows Servers genaustens überwacht.
Zusammen mit Windows Eventlogs wurde ein System entwickelt, das mit unterschiedlichen Eskalationsstufen gegen die Ransomware vorgehen konnte. Bei einem anfänglichen Verdacht wird der Admin des Netzwerks per E-Mail informiert. Fortwährende Aktivitäten triggern die zweite Stufe, welche den Ursprung des Angriffs einem Benutzerkoto zuweist und dieses deaktiviert. Besteht die Bedrohung weiterhin, wird der Netzwerkzugang des Servers deaktiviert und auf der letzten Stufe schließlich der betroffene Server heruntergefahren.[Moo16]

Das Ransomware-Frühwarnsystem CryptoDrop (CryptoLock and Drop It) wurde durch Scaife u. a. entwickelt. Auch dieses System nutzt Ransomware-Merkmale im Bereich von Dateioperationen, um einen Angriff zu erkennen. Zu diesem Zweck überwacht CryptoDrop z.B. Änderungen von Dateitypen, Entropie von Dateien und führt Ähnlichkeitsvergleiche zwischen Originalen und ihren Kopien durch. Wird anhand dieser und weiteren Merkmalen ein Angriff erkannt, kann das System den Ransomware-Prozess stoppen.[Sca16]

Min u. a. implementierten einen „Ransomware Attack Risk Indicator“ (RARI) für Schreiboperationen auf SSDs, welcher automatisch Backups für Pages durchführt, die einen hohen RARI-Wert erhalten haben. Sollte die Information auf der Page durch einen Ransomware-Angriff verschlüsselt worden sein, kann das Amoeba getaufte System diese automatisch wiederherstellen.[Min18]

Der von Morato u. a. beschriebene Detektionsalgorithmus „REDFISH“ erkennt Ransomware-Angriffe auf geteilte Netzwerklaufwerke, indem der Netzverkehr überwacht und analysiert wird. Eine Kopie des Netzverkehrs wird auf Ransomware-typische Dateioperationen (Lesen, Schreiben, Löschen) untersucht. Auf diese Weise wurden Angriffe in 99% der Fälle nach ca. 10 Dateilöschungen mit einer Fehlalarmrate von 0,00001% erkannt.[Mor18]

Ein weiteres Erkennungssystem auf Basis von Netzwerkaktivitäten wurde von Modi u. a. entwickelt. Dieses System untersucht den verschlüsselten Netzverkehr von Ransomware und nutzt Merkmale von Verbindungen, Verschlüsselungen und Zertifikaten in KI-Ansätzen, um Angriffe zu erkennen. Dadurch kann der für Ransomware typische Netzwerkverkehr erkannt und eine Infektion noch vor Ausführung der Verschlüsselung festgestellt werden.[Mod19] Um Operationen wie Lateral Movement (LM) und Privilege Escalation (PE) zu detektieren, müssen diese über das Netzwerk erfolgen, da lokale Ereignisse nicht erkannt würden.
Der von Mehnaz, Mudgerikar und Bertino entwickelte RWGuard erkennt Angriffe in Echtzeit, indem er Decoy (dt. Köder) verwendet und laufende Prozesse sowie das Dateisystem genau überwacht. Seine Fehlerrate wird durch den Einsatz von KI minimiert, welche das Benutzerverhalten erlernt und somit besser zwischen normalen und bösartigen Aktionen unterscheiden kann.[MMB18]

Chen u. a. entwickelten eine Methode, die API-Aufrufe von einem System im Normalbetrieb in Kontrollflussgraphen abbildet, welche so umgewandelt werden, dass sie von KI genutzt werden können. Die Forscher nutzten vier verschiedene KI-Klassifizierungssysteme und

testeten ihre Effektivität bei der Erkennung von Ransomware. Simple Logistic war mit einer Trefferquote (True-postive-Rate) von 97,6%, Genauigkeit von 98,2% und einer Fehlerrate von 1,2% das beste Klassifizierungssystem.[Che17]

Name/Quelle	**Consolidation and Preparation**			**Impact on Target**		
	C2	**LM**	**PE**	**Ex**	**DBu**	**En**
UNVEIL [Kha16]						x
Wecksten et al. [Wec16]					x	
Moore [Moo16]						x
CryptoDrop [Sca16]						x
Amoeba [Min18]					x	
REDFISH [Mor18]						x
Modi et al. [Mod19]	x	(x)	(x)	x		
RWGuard [MMB18]						x
Chen et al. [Che17]						x

Tabelle 3.1: Erkennung von Phasen des Ransomware-Lebenszyklus durch Ransomware-Detektionsansätzen

Die Tabelle 3.1 listet alle vorgestellten Erkennungsansätze noch einmal auf und zeigt, in welchen Phasen des Ransomware-Lebenszyklus der jeweilige Ansatz einen Angriff erkennen könnte. Es ist zu erkennen, dass die meisten Ansätze erst im Falle der Verschlüsselung einen Ransomware-Angriff detektieren und keiner alle Phasen/Schritte abdeckt.
Besonders in Phase zwei (Consolidation and Preparation) werden oft Werkzeuge verwendet bzw. Ereignisse erzeugt, die nicht typisch/primär Ransomware zuzuordnen sind und somit von Ransomware-spezifischen Ansätzen gar nicht oder nur bedingt erkannt werden. Das System von Modi u. a. hat von allen Betrachteten die besten Chancen einen Ransomware-Angriff noch vor der Verschlüsselung zu erkennen. Gleichzeitig kann möglicher Schaden auch extrem reduziert werden, indem Ansätze wie Amoeba beschädigte Dateien einfach wiederherstellen.
Eine Kombination aus allgemeiner Malware- und Ransomware-Detektion würde es ermöglichen, eine Infektion schon vor der Verschlüsselung zu erkennen. Ransomware-Familien, die der Detektion durch allgemeine Systeme ausweichen, könnten dann von den spezialisierten Systemen früh, innerhalb der Verschlüsselungs-Phase erkannt werden.

3.5 Angriffserkennungssysteme

Das IT-SiG 2.0 definiert Angriffserkennungssysteme als „[...] durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme“.[Gmb21] Diese Systeme sind besonders für Unternehmen/Organisationen relevant, die ein Netzwerk aus verschiedenen Komponenten (Datenbanken, Share-Servern, VPN-Gateways, Clients, etc.) vor Angriffen schützen wollen. Wie bereits aus der Definition zu erkennen ist, geht mit der Verwendung von Angriffserkennungssystemen auch ein organisatorischer und in vielen Fällen auch ein personeller Aufwand einher. Zwar generieren die Systeme automatisiert Alarme, die Überprüfung dieser muss in den meisten Fällen jedoch manuell erfolgen. Damit dies auch effizient möglich ist, ist es wichtig, gute Präventionsmaßnahmen einzusetzen. Diese wehren die meisten „einfachen“ Angriffe ab und reduzieren so die Anzahl der zu überprüfenden Ereignisse drastisch.

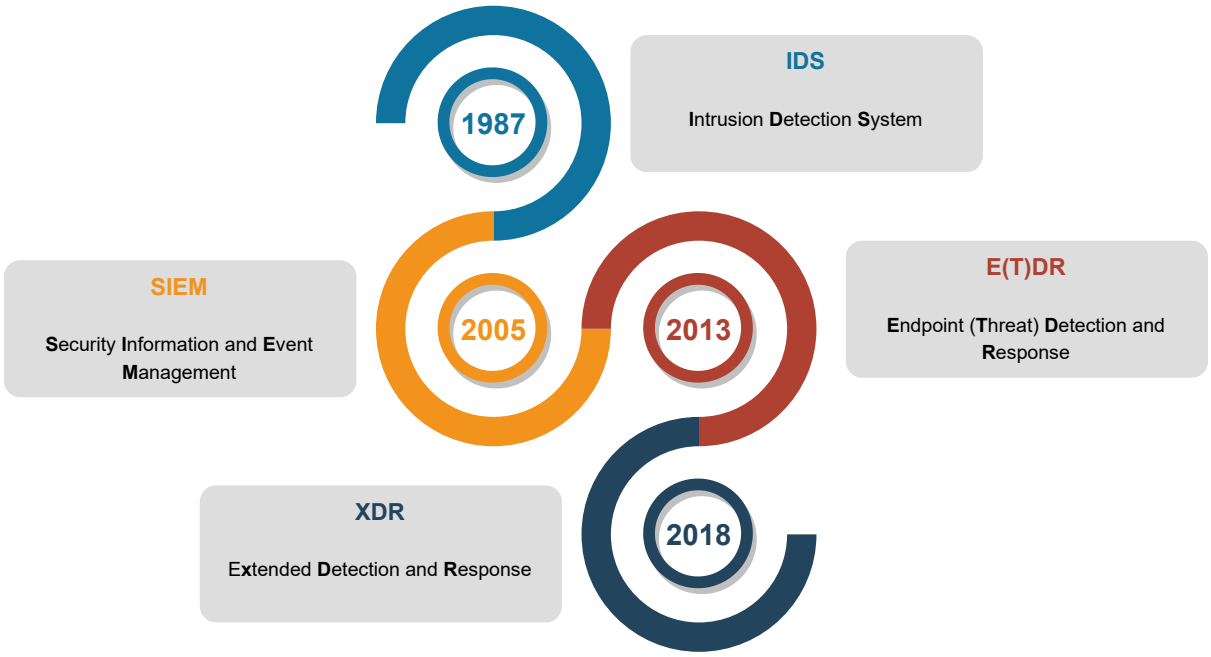


Abbildung 3.3: Historische Entstehung von Angriffserkennungssystemen

Die Entstehungsgeschichte von Angriffserkennungssystemen beginnt in den 1980er Jahren mit der Entwicklung eines Konzeptes für Intrusion Detection Systems IDS (siehe Zeit-

strahl in Abb. 3.3). Die Basis für IDS wurde 1987 von [Den87] gelegt, welche ein Modell für ein Intrusion Detection Expert System (IDES) veröffentlichte. Die ersten IDS basierten jedoch fast ausschließlich auf signaturbasierten Ansätzen sowie der Erkennung von Schwachstellen und sind den heutigen Cyber-Bedrohungen nicht mehr gewachsen.[Ext21] 2005 prägen Williams u. a. vom Marktforschungsunternehmen Gartner Inc. den Begriff Security Information and Event Management (SIEM).[WN05] Diese Systeme sammeln und kategorisieren Daten aus möglichst vielen Quellen innerhalb eines Netzwerks und korrelieren sie anschließend, um Angriffe zu erkennen.[Spl22] Ab 2013 werden die durch [Chu13] geprägten Endpoint Threat Detection and Response (ETDR)-Systeme immer populärer. 2015 findet eine Umbenennung in die bis heute bestehende Form Endpoint Detection and Response (EDR) statt. EDR-Systeme schützen, wie der Name suggeriert, die Endpunkte (PCs, IoT, Mobiltelefone, etc.) eines Netzwerks. Dabei arbeiten sie oft mit sog. Agents, Programmen, die auf den Endgeräten laufen und Informationen zu Verhalten und Ereignissen an eine zentralen Stelle weiterleiten, welche bei Auffälligkeiten Alarm schlägt. Die Weiterentwicklung von EDR ist Extended Detection and Response (XDR) und wurde durch den Sicherheitsforscher Palo Alto Networks Ignite 2018 geprägt. XDR verbindet die Ansätze von SIEM und EDR zu einem und sammelt so viele relevante Informationen wie möglich aus der gesamten IT-Infrastruktur (Endpoints, Server, E-Mail, Cloud-Anwendungen, etc.), um Angriffe zu erkennen.[Pal18] Je nach Anbieter der EDR und XDR-Lösungen sind auch Möglichkeiten zur Bekämpfung von detektierten Angriffen Teil dieser.

3.5.1 Intrusion Detection System

Intrusion Detection Systeme lassen sich in zwei Kategorien und drei Detektionsansätze unterteilen. Je nach dem, ob ein IDS den Netzverkehr oder einzelne Geräte (Hosts) überwacht, werden sie als *NIDS* (Network Intrusion Detection Systems) oder *HIDS* (Host Intrusion Detection Systems) kategorisiert. Des Weiteren lassen sich IDS einem der drei Detektionsansätze *Signaturbasiert*, *Anomaliebasiert* oder *Hybrid* zuordnen.
Signaturbasierte IDS versuchen Signaturen von bereits bekannter Malware zu finden, um einen möglichen Angriff zu entdecken. Da der Großteil des Netzverkehrs heutzutage verschlüsselt stattfindet, haben signaturbasierte NIDS große Probleme, Angriffe korrekt zu erkennen. *Anomaliebasierte* IDS vereinen alle Detektionsansätze (Verhalten, Heuristik,

Modell, etc.), die einen Angriff durch Veränderungen gegenüber einer bekannten Ausgangsbasis erkennen. *Hybride* IDS verwenden sowohl Anomalie- als auch signaturbasierte Techniken zur Angriffserkennung.[Khr19]

Besonders ältere IDS leiden unter hohen Falschalarmraten (False Positives/Negatives), verschlüsseltem Datenverkehr und schlechter Skalierbarkeit, weshalb empfohlen wird, auf neuere oder andere Angriffserkennungssysteme umzusteigen, die diese Probleme nicht haben.[Ext21]
Bekannte Beispiele für IDS sind: Solarwinds, Snort, OSSEC, Suricate oder SecurityOnion.[Hel22]

3.5.2 Security Information and Event Management

Security Information and Event Management (SIEM) ist die Kombination von Ansätzen aus Security Information Management (SIM) und Security Event Management (SEM). SIEM sammelt, analysiert, kategorisiert und korreliert verschiedenste Informationen/Ereignisse von Geräten in einem Netzwerk in Echtzeit.
Die Korrelation von Daten ist ein großer Vorteil von SIEM gegenüber klassischen IDS. Während eine fehlgeschlagene Anmeldung auf einem Geräte durchaus vorkommt, sollten mehrere solcher Versuche auf unterschiedlichen Geräten vom gleichen Benutzer genauer untersucht werden. Zusätzlich zu lokal eingerichteten Regeln und Erkennungstechniken greifen SIEM-Systeme auch auf externe Ressourcen (z.B. Threat Intelligence Feeds verschiedener Anbieter) zu, um potentielle Bedrohungen in einem breiterem Kontext zu betrachten. Wird eine potentielle Bedrohung erkannt, informiert ein SIEM-System automatisch zuständiges Personal, welches die aufbereiteten Informationen überprüfen und weitere Schritte einleiten kann.[Spl22]
Neuere Generationen von SIEM verwenden User and Entity Behavior Analytics (UEBA) und Security Orchestration and Automation (SOAR), um die Effizienz weiter zu steigern. Mit UEBA werden normale und atypische Verhalten von menschlichem Verhalten durch KI-Ansätze erlernt und für die Angriffserkennung eingesetzt. SIEM-Systeme, die SOAR implementierten, erweitern ihre Fertigkeiten um automatische Incident-Response-Systeme, die eine Bedrohung mit festgelegten Maßnahmen bekämpfen können.[Exa]

Die Einrichtung und der Betrieb eines SIEM-Systems ist in den meisten Fällen mit erheblichem Aufwand und Kosten verbunden. Die Aufwendungen setzen sich aus Software-, Hardware und Personalkosten zusammen. Tabelle 3.2 zeigt die Kosten der am häufigsten genutzten SIEM Betriebsarten aus der Sicht eines Unternehmens, welches ein SIEM System neu anschaffen möchte.

SIEM Betriebsart	**Software**	**Hardware**	**Personal**
Self-hosted + Self-managed	€	€€€	€€€
Software as a Service (SaaS)	€€	-	€€
Managed Security Service Provider (MSSP)	€€€	-	-

Tabelle 3.2: Kosten verschiedener SIEM Betriebsarten

Die Softwarekosten ergeben sich aus den Lizenzkosten sowie den ggf. anfallenden Nutzungsgebühren des Anbieters. Diese Kosten sind gering, wenn das Unternehmen die Software eigenständig hosted und verwaltet. Wird Open Source Software eingesetzt, können sie vollständig entfallen. Allerdings gibt es hohe Kosten bei der Anschaffung von Hardware, wie Server, Computer oder Räumlichkeiten für Personal und die Geräte. Zusätzlich müssen sowohl Administratoren für die Wartung der Geräte, als auch Analysten für die Auswertung der Alarme eingestellt und fortlaufend bezahlt werden.
Wird SIEM als Software as a Service (SaaS) betrieben, werden die Software und die dazugehörige IT-Infrastruktur durch den Anbieter bereitgestellt, sodass die Kosten hauptsächlich durch die Nutzungsgebühren des Anbieters sowie die Personalkosten für Analysten entstehen.
Möchte man Kosten für eigene Hardware und eigenes Personal sparen, bietet es sich an, SIEM über einen Managed Security Service Provider (MSSP) einzukaufen. Dieser übernimmt vollständig den Aufbau und den Betrieb des SIEM-Systems, lässt sich dies jedoch in Form von besonders hohen Softwarekosten bezahlen.[Exa]

Bekannte Beispiele für SIEM-Systeme sind Splunk, LogRhythm, QRadar, Trellix oder Elastic (ELK-Stack).[Ins22]

3.5.3 Endpoint Detection and Response

Endpoint Detection and Response (EDR) Angriffserkennungssysteme arbeiten mit auf den Endgeräten installierten Agenten, welche Informationen zu allen Logs, Ereignissen

und Vorgängen an einem zentralen Punkt sammeln (siehe Abb. 3.4). Die gesammelten Informationen werden mit fortlaufend aktualisierten Regeln sowie KI-Methoden auf auffällige Verhaltensmuster untersucht. Der Vorteil von EDR gegenüber SIEM ist die engere Verzahnung des Agenten mit dem Betriebssystemen der Endgeräte. Dies ermöglicht bei der Analyse der Informationen zusätzliche Detailinformationen zu den jeweilig betroffenen Endgeräten mit einzubeziehen und damit einen vollständigeren Gesamtkontext zu erhalten.[Str21] Ein weiterer Vorteil gegenüber SIEM ist, dass EDR auch mit Funktionen für die Reaktion (engl. Response) auf erkannte Angriffe ausgestattet ist. Einfachere EDR-Systeme können automatisch Prozesse beenden und die Netzwerkkommunikation der betroffenen Geräte eindämmen. Fortgeschrittenere Systeme bieten Funktionen zum automatischen Rollback bösartiger Änderungen an Dateisystemen oder der Registry, zur Verwaltung von Backups oder zur Erstellung von Snapshots für spätere forensische Analysen.[Lub21a]
In den seltensten Fällen lassen sich EDR-Systeme als Informationslieferanten für SIEM nutzen, da Hersteller in der Regel keine nativen Schnittstellen anbieten, um die Rohdaten der Agenten auszulesen.[Str21]

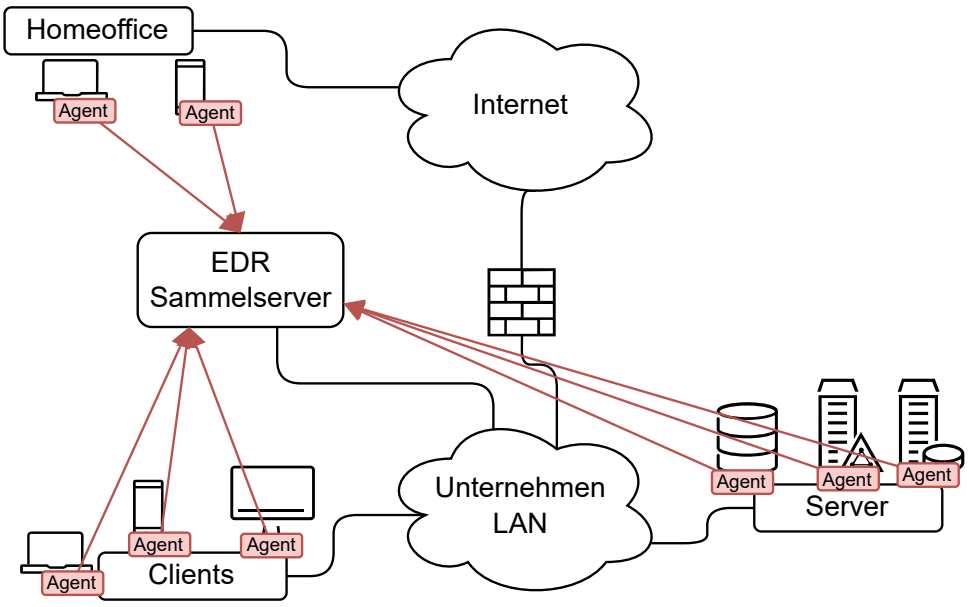


Abbildung 3.4: Beispiel einer IT-Infrastruktur eines Unternehmens mit EDR

Bekannte Beispiele für EDR-Systeme sind Cisco Secure Endpoint, Wazuh, Cynet 360, F-Secure Elements Endpoint Detection and Response oder FortiEDR.[Str21]

3.5.4 Extended Detection and Response

Die Weiterentwicklung von EDR Extended Detection and Response (XDR) verfolgt den gleichen Ansatz wie sein Vorgänger, nutzt aber neben Endpunkten auch noch weitere Informationsquellen, wie Netzwerkkomponenten (Router, Switches, Firewalls), Cloud-Services und sonstige IT-Anwendungen (E-Mail, ERP).[Lub21b] Das Ziel von XDR ist die plattformunabhängige und ganzheitliche Abdeckung einer IT-Infrastruktur, um die größtmögliche Menge an Informationen und Kontext für die Erkennung von Angriffen zur Verfügung zu haben. Die eigentliche Detektion findet, wie bei EDR, mithilfe von aktuellen Regelsätzen und KI-Methoden statt. Anbieter von XDR-Systemen bieten teilweise auch erweiterte Funktionalitäten im Zusammenspiel mit anbietereigener Hardware (Firewalls, Gateways, etc.) an. Zwar bieten diese Symbiosen meist noch effizientere Detektionsquoten, jedoch entsteht auch eine Abhängigkeit zu dem Anbieter. Sollte dieser Insolvenz anmelden oder anderweitig kompromittiert werden, kann eine solche Abhängigkeit schnell selbst zu einer Bedrohung werden. Solche Monokulturen werden daher als problematisch angesehen.[Str21]

Beispiele für bekannte XDR-Systeme sind Heimdal Security, Cynet 360 AutoXDR, Cortex XDR oder CrowdStrike Falcon Insight.[Inc22]

Kapitel 4

Experiment

Im Rahmen dieser Masterarbeit soll ein Experiment entwickelt, aufgebaut, durchgeführt und ausgewertet werden. Ziel ist es, echte Ransomware in einem Netz, welches der IT-Systemlandschaft von KRITIS-Betreibern nachempfunden ist, möglichst zeitnah zu detektieren. Die Detektion soll durch verschiedene Sensoren auf den einzelnen Komponenten im Netz erfolgen.
Die Stadtwerke Brandenburg an der Havel GmbH (StWB) bieten kritische Dienstleistungen aus dem Sektor Energie (Strom-, Gas- und Fernwärmeversorgung) für die Stadt Brandenburg an der Havel, sowie das Umland an. Da sie den Schwellenwert von 500.000 versorgten Personen bisher nicht überschreiten, gelten sie nicht als Kritische Infrastruktur im Sinne des BSIG.[BBK21] Als Energieversorger unterliegen sie jedoch dem Energiewirtschaftsgesetz und müssen so nach §11 Absatz 1b „[...] einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme (...) gewährleisten [...]“[BMJa] und bis zum 01.05.2023 Systeme zur Angriffserkennung einsetzen(§11 Abs. 1e).[BMJa]
Die Stadtwerke betreiben Infrastruktur sowohl im Bereich der Informationstechnologie (IT), als auch im Bereich der operativen Technologie (engl. operational technology, OT). Da sich die Einfallstore für Ransomware jedoch weiterhin auf der Seite der IT-Infrastruktur befinden, fokussiert sich dieses Experiment auf die Detektion in diesem Bereich.[BSI22e]

Dieses Kapitel ist in Abschnitte für die verschiedenen Phasen des Experiments *Aufbau*, *Durchführung*, *Beobachtungen* und *Auswertung* unterteilt.

4.1 Aufbau

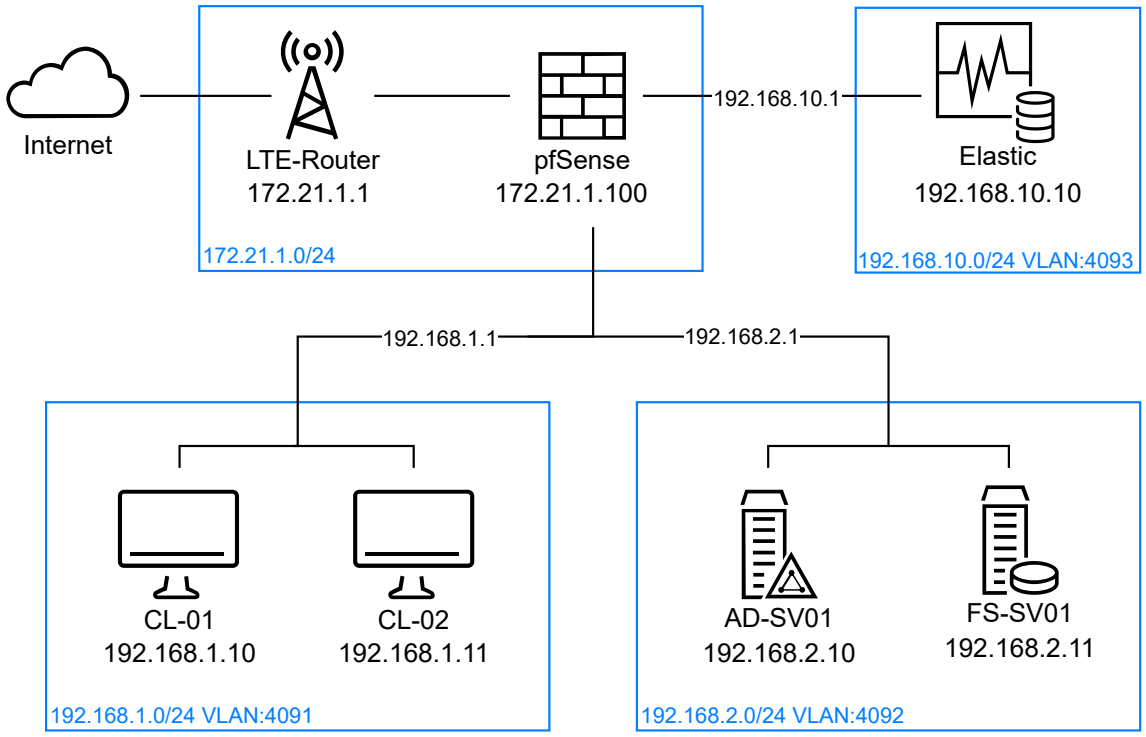


Abbildung 4.1: Netzplan der Testumgebung

In Zusammenarbeit mit den Stadtwerken Brandenburg wurde ein abstrakter Plan für eine beispielhafte Office-IT-Infrastruktur für ein Energie-KRITIS-Unternehmen entwickelt. Auf der Basis dieses wurde eine Testumgebung mit sieben Geräten in einem Labor der Technischen Hochschule Brandenburg aufgebaut. Eine Aufstellung dieser Geräte, sowie ihrer Rollen und der Betriebssysteme, können Tabelle 4.1 entnommen werden. Der Netzplan (Abb. 4.1) gibt eine Übersicht über die verschiedenen Netzsegmente, Kommunikationswege und die Verteilung der Geräte. Der allgemeine Aufbau entspricht dem einer Office-IT-Infrastruktur.

Da Windows den größten Marktanteil für Desktopgeräte besitzt [sta22a] und ein Großteil der Ransomware Windows-basiert ist, wurde sich dafür entschieden, den Versuch mit Windows Betriebssystemen aufzubauen. Um der Office-Struktur eines Unternehmens zu entsprechen, wurde festgelegt, einen Active Directory- sowie einen Fileserver in das

Netzwerk zu integrieren (siehe Abschnitt 4.1.3). Des Weiteren sollen nur die Phasen *Consolidation and Preparation* und *Impact on Target* betrachtet werden. Es wird daher angenommen, dass der *Initial Access* bereits stattgefunden hat und Ransomware, auf einem der Geräte, zur Ausführung bereit ist.

Name	**Gerät**	**Rolle**	**Betriebssystem**
LTE-Router	Archer MR600	Internetzugang	-
pfSense	Netgate 7100	Firewall/Router	pfSense® Plus software 22.05
CL-01	Acer Aspire 5	Client	Microsoft Windows 10 Education 64 Bit 10.0.19044 Build 19044
CL-02	Acer Aspire 5	Client	Microsoft Windows 10 Education 64 Bit 10.0.19044 Build 19044
AD-SV01	Acer Aspire 5	Domaincontroller	Microsoft Windows Server 2019 Standard Evaluation 10.0.17763 Build 17763
FS-SV01	Acer Aspire 5	File-Share-Server	Microsoft Windows Server 2019 Standard Evaluation 10.0.17763 Build 17763
Elastic	Acer Aspire 5	Elastic Stack	Ubuntu 20.04.4 LTS

Tabelle 4.1: Aufstellung verwendeter Geräte

4.1.1 Internetzugang und Routing

In Rücksprache mit den Stadtwerken wurde beschlossen, dass die Testumgebung einen Internetzugang erhalten soll, damit Netzwerkkommunikation zwischen Testumgebung und Angreifer möglichst vollständig nachvollzogen werden kann. Zu diesem Zweck wurde ein LTE-Router verwendet, welcher der pfSense als Internet-Uplink dient. Auf diese Weise kann das Experiment unabhängig vom internen Netz der THB durchgeführt werden und die Möglichkeit einer Infektion dieses ausgeschlossen werden.
Die pfSense fungiert als Router und Firewall und teilt das Netzwerk mithilfe von VLAN in drei Netzsegmente für Clients, Server sowie den Elastic-Server ein (blaue Kästen mit Subnetzmaske und VLAN-ID in Abb. 4.1). Dies verhindert, dass Geräte aus unterschiedlichen Segmenten miteinander kommunizieren, ohne das dies explizit erlaubt wurde. Für die

Kommunikation der Segmente untereinander wurden Firewall-Regeln erstellt, die sämtlichen Verkehr zwischen den Geräten zulassen, ihn jedoch loggen und diese Logs im Rahmen von Netflow-Daten an den Elastic-Sever weiterleiten.

4.1.2 Clientsegment

Das Clientsegment hat die Subnetzmaske 192.168.1.0/24 und die VLAN-ID 4091. Es besteht aus den zwei Windows-Clients CL-01 (192.168.1.10) und CL-02 (192.168.1.11), die Teil der *ad.ransom.local*-Domain sind. CL-01 wird in diesem Experiment vom Benutzer *Teo Tester* und CL-02 von *Nadia Nutzer* verwendet. Unabhängig davon sind beide Systeme identisch eingerichtet.
Mithilfe eines Python-Scripts (siehe Quelltextauszug A.1) wurden Binärdateien mit zufällig generierten Namen und Dateiendungen auf jedem Client erstellt, die später von Ransomware angegriffen werden können. Möglich Dateiendungen sind: *.pdf*, *.txt*, *.png*, *.jpg*, *.xlsx*, *.docx* oder *.exe*. Diese wurden zufällig zugeordnet. Um eine typische Benutzerumgebung zu simulieren, wurden die gängigsten Ordner, *Desktop*, *Dokumente*, *Bilder* und *Downloads*, mit jeweils 25 Dateien á 1-50 MB und drei Dateien á 1 GB befüllt.

4.1.3 Serversegment

Das Serversegment erhält die Subnetzmaske 192.168.2.0/24 sowie die VLAN-ID 4092. Es besteht aus einem Domaincontroller (AD-SV01) und einem Windows-Fileserver (FS-SV01). Beide nutzen Windows Server 2019 als Betriebssystem.
Der AD-SV01 wird als Windows Active Directory-Server eingerichtet und als Domaincontroller für die neu erstellte *ad.ransom.local*-Domain konfiguriert. Er ist über die IP 192.168.2.10 erreichbar.
Für die Domain werden zwei Benutzer, *Teo Tester* und *Nadia Nutzer*, angelegt. Teos Benutzerkonto hat volle Domainadministratorrechte und Nadias nur Standardbenutzerrechte. Zusätzlich wurden Group Policy Objects (GPO) zum Deaktivieren des automatischen Windows Updates, der Windows Firewall und des Windows Defenders erstellt. Mit diesen Policies soll sichergestellt werden, dass die Clients sich nicht automatisch updaten und über die Dauer des Experiments eine konsistente Version nutzen. Gleichzeitig soll die

Ransomware eine bestmögliche Ausgangslage auf den Clients haben, sodass sie bei ihrer Ausführung nicht eingeschränkt ist und sich somit ein vollständiges Verhaltensbild für die Analyse ergibt.
Der Fileserver ist als solcher an der Domain registriert und stellt ein Netzwerklaufwerk bereit, welches durch ein GPO als *Drive map* für die gesamte Domain, unter dem Laufwerksbuchstaben *S:*, zur Verfügung gestellt wird. FS-SV01 ist unter der IP-Adresse 192.168.2.11 zu erreichen.
Für beide Server und das Netzwerklaufwerk wurden Dummy-Dateien mithilfe des Python-Scripts (siehe A.1) generiert.

4.1.4 Elastic Stack

Das Segment des Elastic Stacks erhält die Subnetzmaske 192.168.10.0/24 und die VLAN-ID 4093. Es besteht nur aus einem Laptop mit Ubuntu 20.04.4 LTS, der über die IP 192.168.10.10 zu erreichen ist und auf dem ein Elastic Stack eingerichtet ist. Die Komponenten des Stacks sind Elasticsearch, Kibana und Filebeat in der Version 8.4.1. Elasticsearch ist eine verteilte JSON-basierte Suchmaschine und Analytics-Engine. Kibana dient als Benutzeroberfläche zur Visualisierung und Suche der Elasticsearch-Einträge. Mit Filebeat können weitere Logs und Logformate an Elasticsearch weitergeleitet werden.[Ela]
In diesem Experiment wird Filebeat genutzt, um die Netflow-Daten der pfSense einzusammeln.
Der Elastic Stack wird in diesem Experiment als Angriffserkennungssystem eingesetzt, da es frei verfügbar ist und individuell, ohne großen Overhead, eingerichtet werden kann.

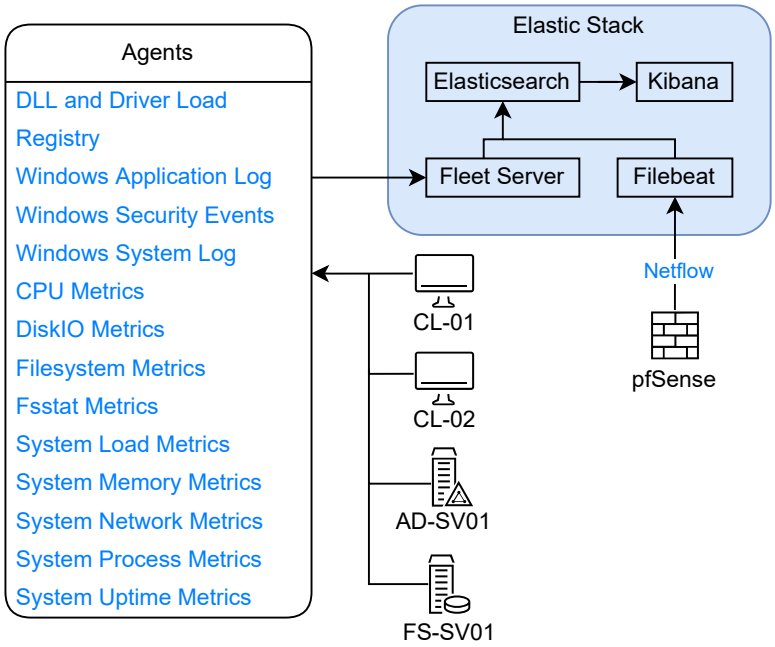


Abbildung 4.2: Übersicht Elastic Datenquellen

Daten von Clients und Servern werden durch sogenannte Agenten, die von einem Elastic Fleet Server verwaltet werden, gesammelt (Abb. 4.3). Welche Daten von den Agenten gesammelt werden, wird über die Agent policy bestimmt. Für dieses Experiment besteht die Agent policy aus den zwei Integrationen, *System* und *Endpoint and Cloud Security*. Eine Zusammenfassung welche Datenquellen von welcher Komponente des Stacks gesammelt werden, kann Abbildung 4.2 entnommen werden. Die dort blau geschriebenen Texte sind die konkreten Daten und Metriken, welche später für die Analyse verwendet werden.

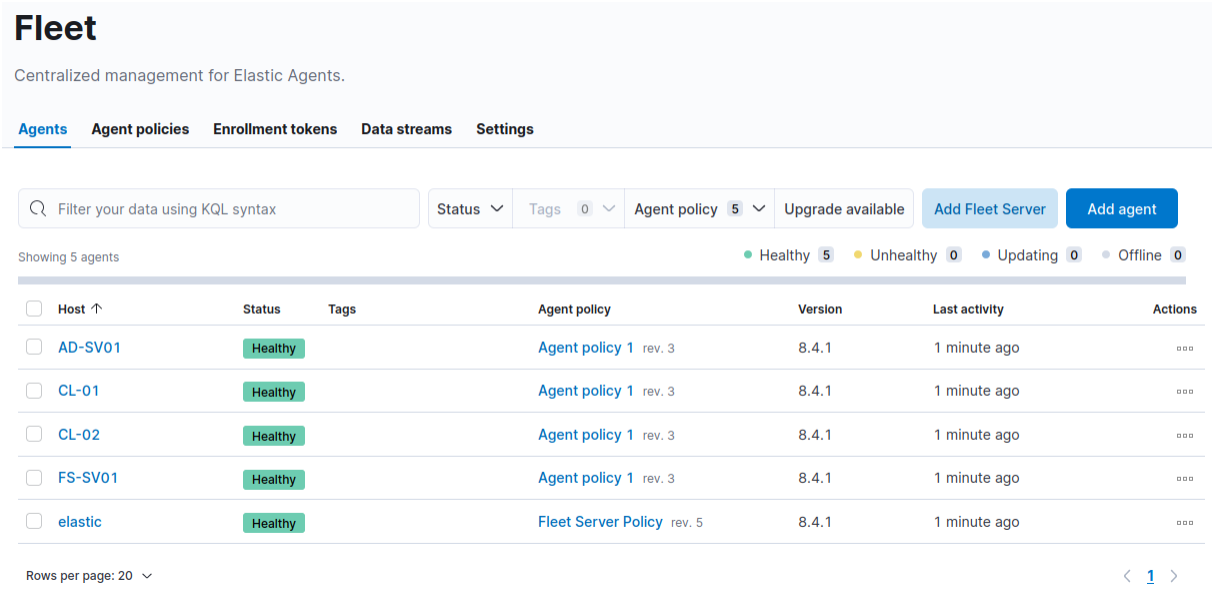


Abbildung 4.3: Übersicht Elastic Fleet mit Agenten

4.1.5 Backupmanagement

Damit mehrere Durchläufe des Experiments möglich sind, wird eine Backupstrategie benötigt, die von Ransomware betroffene Geräte schnell wieder betriebsfähig machen kann. Um Angriffe auf die Backups auszuschließen, wurde entschieden auf externe Speichermedien zurückzugreifen. Zu diesem Zweck wurden zwei USB3.2 2 TB externe SSDs angeschafft. Mithilfe von Clonezilla wurden Abbilder der Partitionen erstellt. Damit das Wiederherstellen der Partitionen möglichst schnell ist, wurden die Partitionsgrößen der Geräte auf 250 GB beschränkt. Mit dieser Beschränkung kann eine Partition in ca 2 min wiederhergestellt werden (Dauer des Kopiervorgangs). Tabelle 4.2 stellt die Namen intern und auf der SSD sowie die Größe der Partition übersichtlich dar. Zur Absicherung wird die zweite SSD als Backup der ersten genutzt.

Name	**Name SSD**	**Part. Größe GB**
CL-01	sda1	250
CL-02	sda2	250
AD-SV01	sda3	250
FS-SV01	sda5	250
FS-SHARE	sda6	79,9

Tabelle 4.2: Übersicht Partitionen

4.2 Durchführung

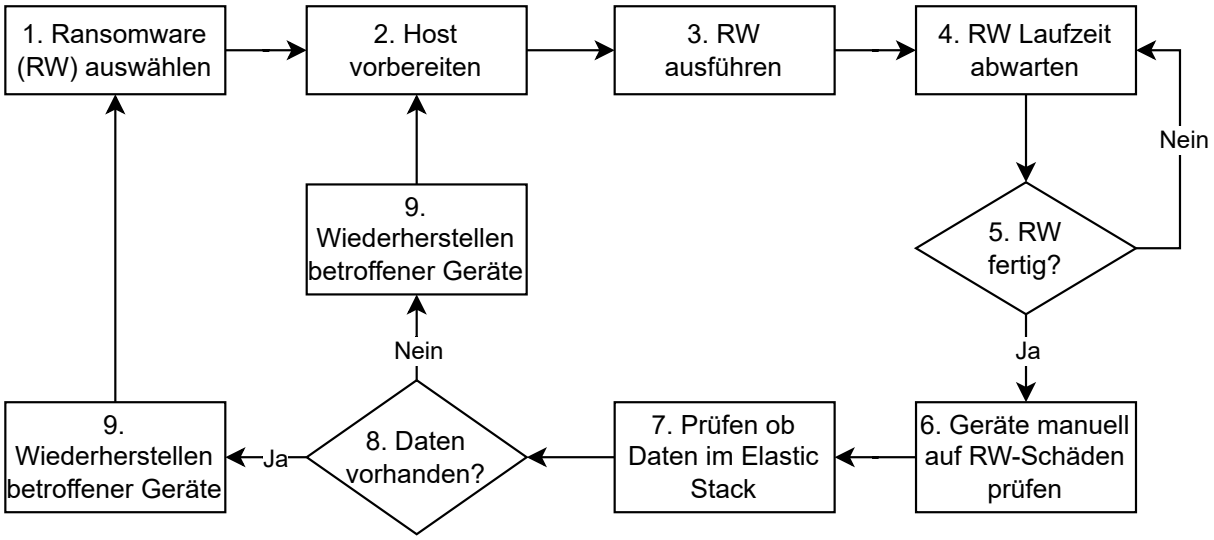


Abbildung 4.4: Ablauf des Experiments

Der Ablauf des Experiments lässt sich grob in neun Schritte einteilen, welche in Abbildung 4.4 visuell dargestellt werden. Der **erste Schritt** ist die Auswahl einer geeigneten Ransomware, die für den jeweiligen Durchlauf verwendet werden soll. Dafür wurden verschiedene Repositories mit Ransomware-Samples ([Jin22; kh422; UIM23]) nach Kandidaten für dieses Experiment durchsucht. Die Kandidaten sollten aktuell sein (Aufgetreten nach 2019) und nach Möglichkeit Fähigkeiten zur Privilege Escalation (PE), Lateral Movement (LM) oder Datenexfiltration (Ex) haben. Je neuer die Ransomware, desto besser stehen die

Chancen, dass Schwachstellen und Exploits für PE und LE noch nicht gepatched wurden und auch diese Prozesse beobachtet werden können.
Das Experiment wird mit den sechs verschiedenen Ransomwares aus Tabelle 4.3 durchgeführt. Für den Wert „Jahr“ wurde das erstmalige Entdeckungsjahr der im Experiment verwendeten Version der Ransomware mithilfe von VirusTotal ermittelt. Weitere Informationen zu den jeweiligen Ransomwares sind weiter unten zu finden.

Name	**Jahr**	**PE**	**LM**	**Ex**
TeslaCrypt	2015			
Lockbit	2020	x	x	
REvil	2021	x	x	x
BlueSky	2022	x	x	
Lilith	2022			x
Moisha	2022		x	

Tabelle 4.3: Übersicht verwendeter Ransomware

Im **zweiten Schritt** wird das Hostsystem, von welchem aus die Ransomware starten soll, vorbereitet. Es wird z.B. überprüft, ob der Elastic-Agent korrekt Daten übermittelt, das System mit dem Internet verbunden ist und ob die Dummy-Dateien vorhanden sind.
Mit dem **dritten Schritt** wird die Ransomware ausgeführt. Während der **Schritte vier** und **fünf** wird gewartet bis der Ransomware-Prozess beendet wurde. Dies lässt sich mithilfe in den Daten des Elastic Stacks durch das Event „process end“ermitteln. Ist dieses Ereignis eingetreten werden im **sechsten Schritt** die Clients und Server manuell auf Schäden durch die Ransomware untersucht. In den **Schritten sieben** und **acht** wird überprüft, ob die Daten korrekt an den Elastic Stack übermittelt wurden. In beiden Fällen werden die betroffenen Geräte, im **neunten Schritt**, mithilfe der Backups wiederhergestellt. Jedoch wird nur bei erfolgreicher Übermittlung eine neue Ransomware für den nächsten Durchlauf ausgewählt. Andernfalls werden die Konfigurationen geprüft und das Hostsystem für einen erneuten Versuch vorbereitet.

Mit den in Tabelle 4.3 aufgezählten Ransomwares werden insgesamt acht Durchläufe absolviert:

1. **TeslaCrypt** (VirusTotal Link)
   Hostsystem: CL-01
   Dateiname: 3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370.exe
   SHA-256: 3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370

2. **REvil** (VirusTotal Link)
   Hostsystem: CL-01
   Dateiname:12d8bfa1aeb557c146b98f069f3456cc8392863a2f4ad938722cd7ca1a773b39.exe
   SHA-256: 12d8bfa1aeb557c146b98f069f3456cc8392863a2f4ad938722cd7ca1a773b39

3. **REvil** (VirusTotal Link)
   Hostsystem: CL-02
   Dateiname: 12d8bfa1aeb557c146b98f069f3456cc8392863a2f4ad938722cd7ca1a773b39.exe
   SHA-256: 12d8bfa1aeb557c146b98f069f3456cc8392863a2f4ad938722cd7ca1a773b39

4. **Lockbit** (VirusTotal Link)
   Hostsystem: CL-01
   Dateiname: 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe
   SHA-256: 2280898cb29faf1785e782596d8029cb471537ec38352e5c17cc263f1f52b8ef

5. **BlueSky** (VirusTotal Link)
   Hostsystem: CL-01
   Dateiname: bscy_22808.exe
   SHA-256: 2280898cb29faf1785e782596d8029cb471537ec38352e5c17cc263f1f52b8ef

6. **BlueSky** (VirusTotal Link)
   Hostsystem: AD-SV01
   Dateiname: bscy_22808.exe
   SHA-256: 2280898cb29faf1785e782596d8029cb471537ec38352e5c17cc263f1f52b8ef

7. **Lilith** (VirusTotal Link)
   Hostsystem: CL-01
   Dateiname: lilith.exe
   SHA-256: f3caa040efb298878b99f883a898f76d92554e07a8958e90ff70e7ff3cfabdf5

8. **Moisha** (VirusTotal Link)
   Hostsystem: CL-01

Dateiname: b3ebc327773f5f846deeb1255475644a630c4d0d3b4eda3bbf995a36599c07cf.exe
SHA-256: b3ebc327773f5f846deeb1255475644a630c4d0d3b4eda3bbf995a36599c07cf

Neben der Detektion der einzelnen Ransomware-Familien soll mit *REvil* und *BlueSky* auch untersucht werden, wie sich unterschiedliche Benutzerrechte/Hostsysteme auf den Verlauf des Angriffs auswirken. *REvil* wird daher einmal auf CL-01 mit den Rechten von *Teo Tester* und einmal auf CL-02 mit den Rechten von*Nadia Nutzer* ausgeführt. Für *BlueSky* wird beide Male der gleiche Benutzer (*Teo Tester*) verwendet, jedoch wird die Ransomware einmal von CL-01 und einmal von AD-SV01 aus gestartet.
Unter der Prämisse, dass eine Ransomware sich besser ausbreiten kann, wenn sie mit Administratorrechten ausgeführt wird, werden die Ransomwares voranging auf CL-01 mit dem Konto von *Teo Tester* gestartet.

4.3 Beobachtungen

In diesem Abschnitt werden die Beobachtungen zu den im vorherigen Abschnitt vorgestellten Durchläufen festgehalten. Allgemein wurde beobachtet, dass jede Ransomware nur Millisekunden nach ihrem Start durch den Elastic-Agenten erkannt wurde (Beispiel Lockbit Abb. 4.5).

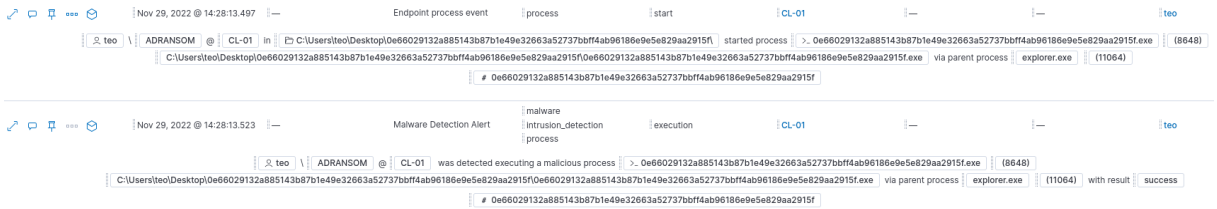


Abbildung 4.5: Ausschnitt Security-Dashboard von Lockbit

Für die Beobachtungen wurden die Daten auf dem Elastic Stack sowohl manuell über das Analytics-Discover-Dashboard (Abb. 4.6), als auch Security-Timelines (Abb. 4.7) betrachtet.

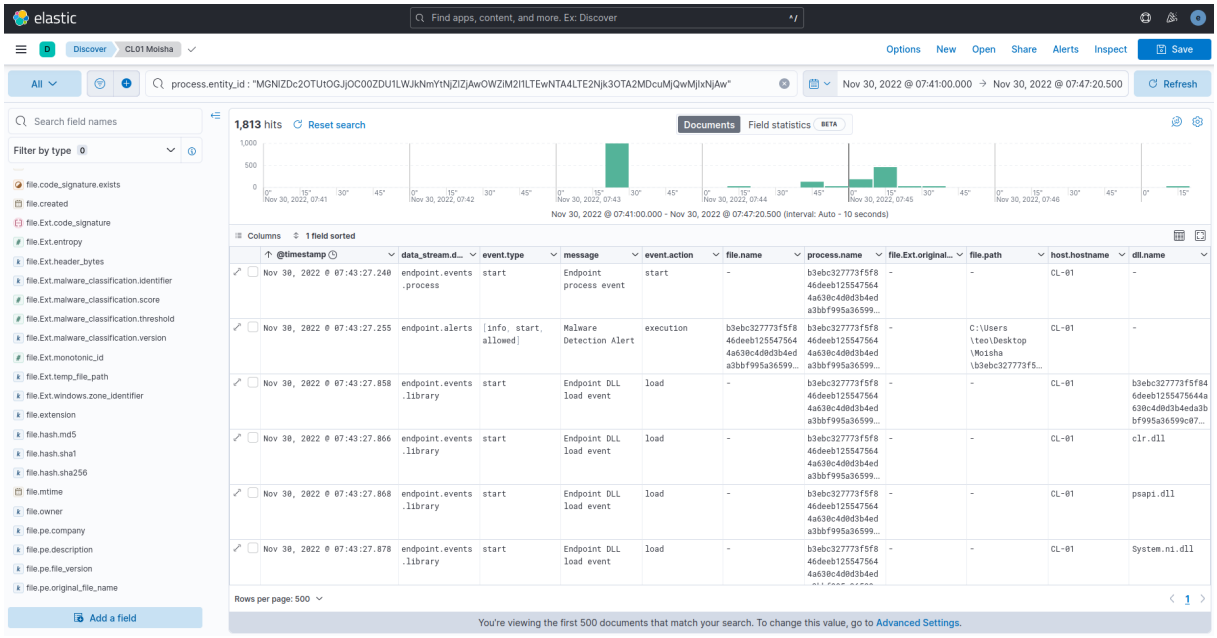


Abbildung 4.6: Analytics-Discover-Dashboard

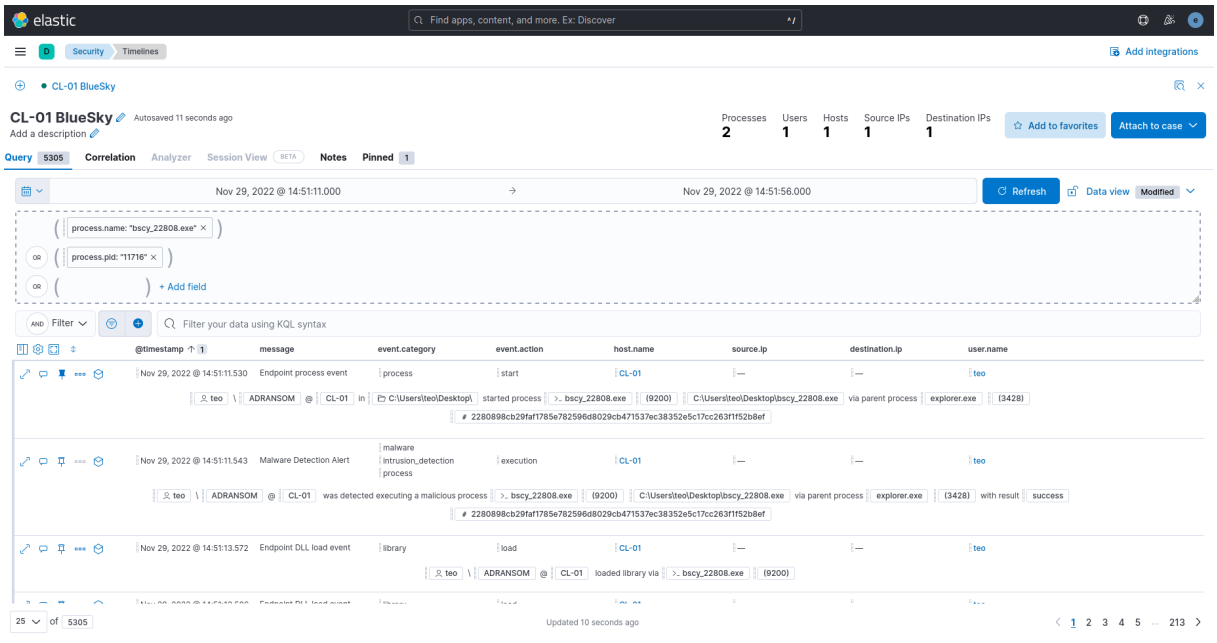


Abbildung 4.7: Security-Timelines von Lockbit

4.3.1 TeslaCrypt CL-01

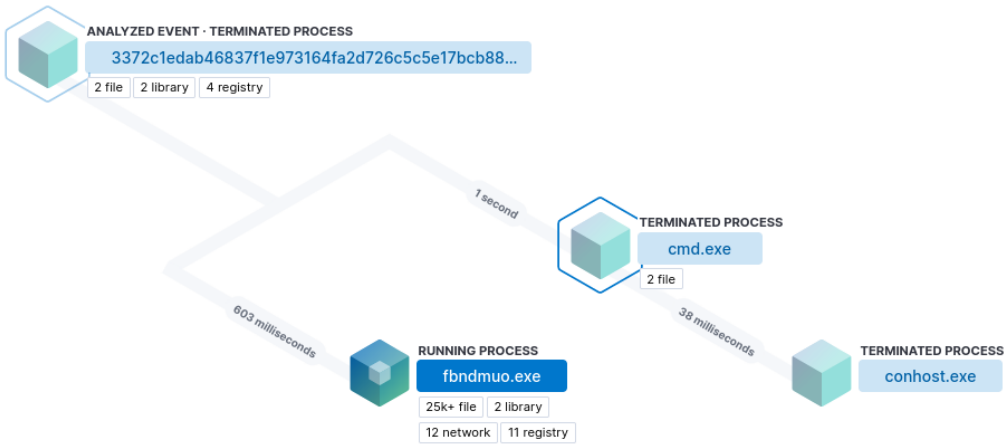


Abbildung 4.8: Übersicht TeslaCrypt Prozesse

- Start: 11:35:20.224 Uhr
- Ende: 11:37:59.015 Uhr
- Dauer: 02:38.791 min

Die *TeslaCrypt* Ransomware wurde in Form der *3372c1eda[...]4a370.exe* um 11:35:20.224 Uhr gestartet. Die Abbildung 4.8 zeigt eine Übersicht der entstandenen Prozesse und welche bzw. wie viele Ereignisse jedem Prozess zugeordnet wurden. Insgesamt wurden zwei verschiedene Libraries geladen und elf Registry-Einträge (siehe Tabelle A.7) angepasst. Als Libraries wurde die Ransomware-eigene und die Prozessstatus-Library *psapi.dll* geladen. Nachdem der Ursprungsprozess die Libraries geladen hat, erstellt er die *fbndmuo.exe* in *C:/Users/teo/AppData/Roaming/*, befüllt diese mit Inhalt und führt sie anschließend direkt aus. Daraufhin löscht sich die ausgeführte Datei durch einen *cmd.exe*-Aufruf selbst. Der Konsolenfenster-Host *conhost.exe* wird unter Windows 10 automatisch beim Start von Befehlszeilentools (cmd, powershell, etc.) gestartet und ist hauptsächlich für die korrekte Darstellung des Fensters verantwortlich. Die eigentlichen Befehle werden weiterhin über

das jeweilige Befehlszeilentool verarbeitet.[Gle22] Daher kann *conhost.exe* in den meisten Fällen bei der weiteren Betrachtung ignoriert werden.
Unmittelbar nach dem Start beginnt *fbndmuo.exe* mit der Erstellung einer *key.dat*-Datei und der Verschlüsselung der Daten. Die Originaldaten werden beim Verschlüsseln überschrieben und erhalten die Dateiendung *.ecc*. Insgesamt werden 25.027 Verschlüsselungsereignisse durch den Elastic-Agenten registriert. Auch eine manuelle Stichprobe zeigt nur verschlüsselte Dateien. Dateien auf dem Netzwerklaufwerk bleiben unverändert.
Nach der vollständigen Verschlüsselung erstellt die Ransomware nun die Lösegeldforderung *HELP_TO_DECRYPT_YOUR_FILES.txt* auf dem Desktop des Benutzers. Gleichzeitig wird die Lösegeldforderung mithilfe von Registry-Änderungen als Hintergrundbild eingerichtet. Während der Verschlüsselung versucht die Ransomware folgende Adressen zu erreichen:

- 7tno4hib47vlep5o.tor2web.fi
- 7tno4hib47vlep5o.tor2web.org
- 7tno4hib47vlep5o.tor2web.blutmagie.de
- 103.198.0.111

Um 11:37:59.015 Uhr wird das letzte Event, welches der Ransomware zugeordnet ist, registriert. Damit beträgt die gesamte Laufzeit ungefähr 2 min und 39 s.

4.3.2 REvil CL-01

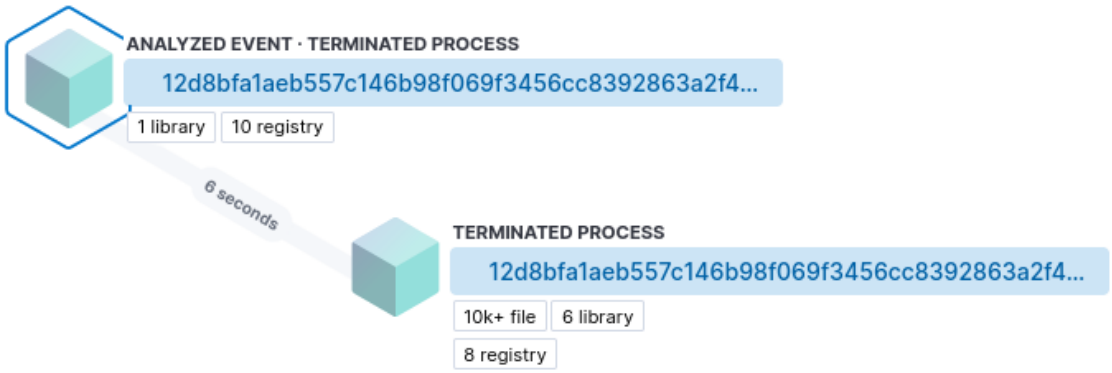


Abbildung 4.9: Übersicht REvil Prozesse (CL-01)

- Start: 14:42:48.275 Uhr
- Ende: 14:43:47.139 Uhr
- Dauer: 58.864 s

Um 14:42:48.275 Uhr wird die Ransomware *REvil* auf dem Client CL-01 über die *12d8bf[...]cd7ca1a773b39.exe* gestartet. Nachdem die Ransomware ihre eigene Library geladen hat, ändert sie verschiedene, den lokalen Benutzer betreffende (*HKEY_USERS/...*), Registry-Einträge (siehe Tabelle A.8), startet eine weitere Instanz der Ransomware und terminiert anschließend.
Die neue Instanz ist mit *Token-Elevation-Level = full* und *Token-Integrity-Level = high* gestartet worden und besitzt somit mehr Rechte und Zugriff auf Ressourcen, als der Ursprungsprozess.[Hac22; Sec22] Die Registry-Änderungen dieser Instanz betreffen daher auch Einträge, die für alle Benutzer gelten (*HKLM/...*)[Del22]. Zusätzlich werden neben der Ransomware-Library noch *wbemprox.dll*, *wbemcomn.dll*, *wbemsvc.dll*, *fastprox.dll* und *symamsi.dll* geladen.
Die Ransomware führt zur Laufzeit 10.905 Dateioperationen durch, welche sich auf die Aktionen Create, Delete und Rename aufteilen. Etwa die Hälfte aller Operationen (5.449) entfällt auf das Löschen sämtlichen Inhalts des *$Recycle.Bin*-Ordners. Nach dem Löschen

beginnt *REvil* mit dem Verschlüsseln der restlichen Dateien (4.869) und erstellt für jeden durchsuchten Ordner eine Lösegeldforderung mit dem Namen *4wrl8m4m6-readme.txt* (587 mal). Zu den verschlüsselten Dateien, denen die Endung *.4wrl8m4m6* angehängt wird, zählen auch die des Netzwerklaufwerks. Bevor die Ransomware um 14:43:47.139 Uhr nach einer Laufzeit von ca. 59 s terminiert, erstellt sie die Bilddatei *tgr767.bmp*, welche als Bildschirmhintergrund gesetzt wird und die Lösegeldforderung in Bildform repräsentiert. Es wurden keine auffälligen Netzwerkkommunikationen detektiert.

4.3.3 REvil CL-02

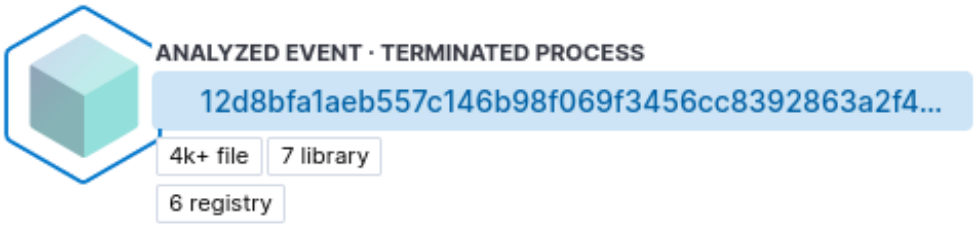


Abbildung 4.10: Übersicht REvil Prozesse (CL-02)

- Start: 12:05:35.587 Uhr
- Ende: 12:06:13.284 Uhr
- Dauer: 37.697 s

Die zweite Ausführung von *REvil* wird mit der gleichen Datei um 12:05:35.587 Uhr auf CL-02 gestartet. Nach ihrem Start beginnt die Ransomware mit dem Laden von Libraries und dem Ändern von Registry-Einträgen (siehe Tab. A.9). Zusätzlich zu den Libraries, die auch im Durchlauf auf CL-01 genutzt wurden, lädt die Ransomware die *UMEngx86.dll*. In diesem Durchlauf beginnt der Prozess direkt nach seiner Initiierung mit der Verschlüsselung der Daten. Von den 4.323 registrierten Datei-Ereignissen sind 3.878 der Verschlüsselung zuzuordnen. Die restlichen Dateioperationen sind auf die Erstellung der Lösegeldforderungen mit dem Namen *d3936-readme.txt* zurückzuführen. Analog erhalten

verschlüsselte Dateien die Endung *.d3936*. In diesem Durchlauf werden nur Dateien auf dem Netzwerklaufwerk verschlüsselt, auf die der Account von *Nadia Nutzer* auch Zugriff hat. Nach ca. 38 s terminiert die Ransomware um 12:06:13.284 Uhr mit der Erstellung der Lösegeldforderung als Bild (*fez6xxy.bmp*) und der Einrichtung dieses als Hintergrundbild. In diesem Durchlauf wurden keine auffälligen Netzwerkkommunikationen erkannt.

4.3.4 Lockbit CL-01

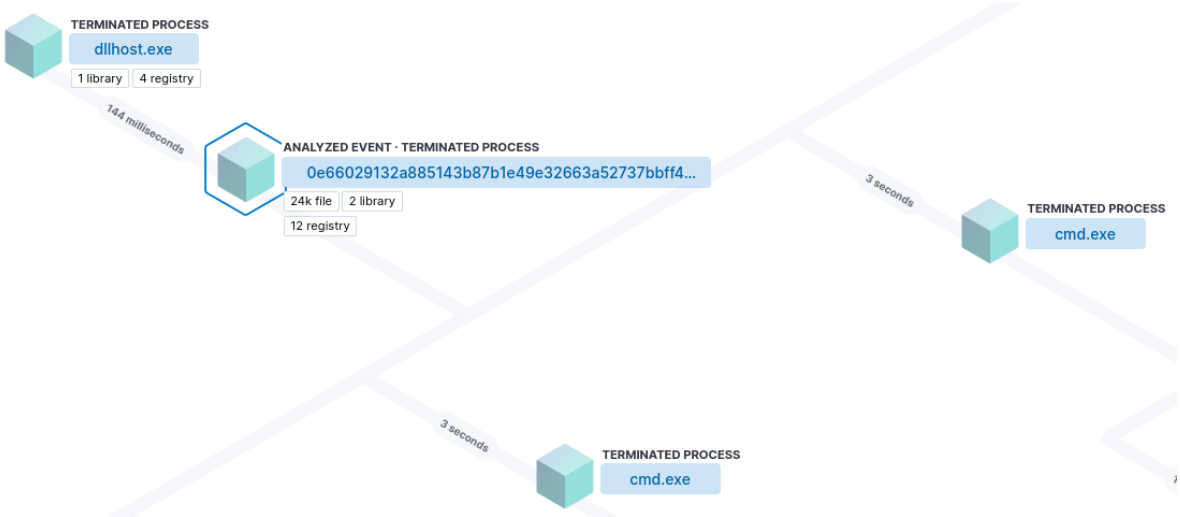


Abbildung 4.11: Übersicht Lockbit Prozesse

- Start: 14:28:13.497 Uhr
- Ende: 14:31:53.013 Uhr
- Dauer: 03:39.516 min

Um 14:28:13.497 wird auf CL-01 die Ransomware *Lockbit* über die *12d8bfa1[...]a773b39.exe* gestartet. Dieser Prozess startet umgehend, nachdem seine Ransomware-Library geladen wurde, einen *dllhost.exe*-Prozess, welcher eine neue Instanz der Ransomware mit erhöhten Rechten (Token-Elevation = full und Integrity-Level = high) startet (siehe Abb.4.11) und erste Änderungen, bezüglich der Interneteinstellungen, an der Registry vornimmt (siehe Tab. A.10). Zusätzlich zur Ransomware-Library wird an dieser Stelle auch die *bcrypt.dll* geladen.

Die nun mit erhöhten Rechten operierende Ransomware-Instanz löscht alle Dateien in *$Recycle.Bin* (5.449) und beginnt mit der Verschlüsselung der restlichen Dateien. Alle 16.918 verschlüsselten Dateien, einschließlich der des Netzwerklaufwerks, bekommen die Endung *.lockbit*. Pro abgeschlossenem Ordner wird eine Lösegeldforderung in Form einer *Restore-My-Files.txt* erstellt (1.576 mal).
Mit wenigen Sekunden Verzögerung startet die Ransomware mehrere Kommandozeilenprozesse (*cmd.exe*) mit unterschiedlichen Parametern, teilweise auch doppelt oder dreifach. Insgesamt werden 28 Zusatzprozesse gestartet. Eine Übersicht dieser kann Tabelle 4.4 entnommen werden.

cmd.exe
/c wevtutil cl system
/c wevtutil cl security
/c wevtutil cl application
/c wbadmin DELETE SYSTEMSTATEBACKUP
/c wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
/c wmic SHADOWCOPY /nointeractive
/c vssadmin Delete Shadows /All /Quiet
/c bcdedit /set default bootsatuspolicy ignoreallfailures
/c bcdedit /set default recoveryenabled no
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet

Tabelle 4.4: Von Lockbit gestartete Zusatzprozesse

Nach einer Laufzeit von ca. 3 min und 40 s terminiert sich der Ransomware-Prozess eigenständig um 14:31:53.013 Uhr, ohne dass auffällige Netzwerkaktivitäten detektiert wurden.

4.3.5 BlueSky CL-01

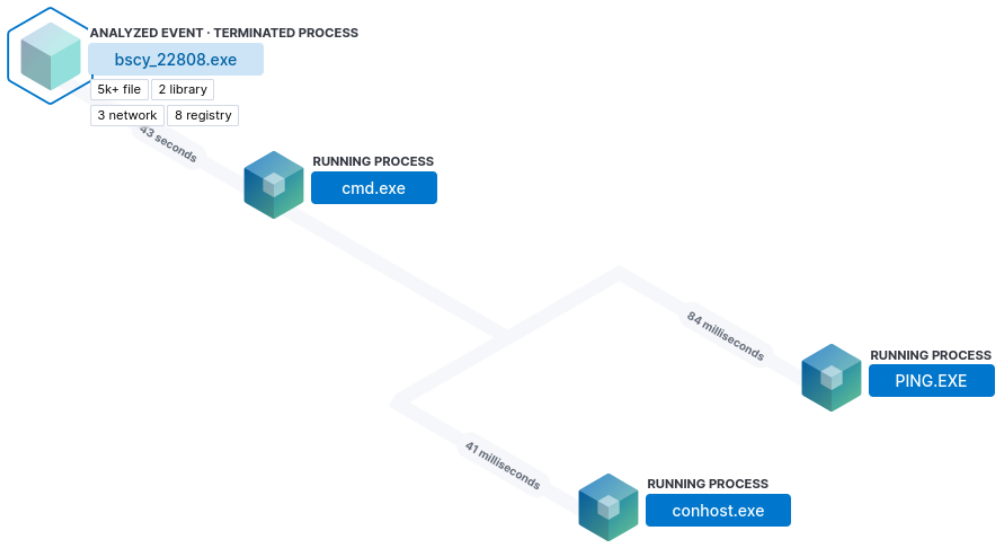


Abbildung 4.12: Übersicht BlueSky Prozesse (CL-01)

- Start: 14:51:11.530 Uhr
- Ende: 14:51:55.137 Uhr
- Dauer: 43.607 s

Die Ransomware *BLueSky* wird um 14:51:11.530 Uhr auf CL-01 durch Ausführen der *bscy_22808.exe* gestartet. Unmittelbar nach dem Start lädt die Ransomware erst ihre eigene Library gefolgt von *bcrypt.dll* und nimmt Änderungen an den Registry-Einträgen aus Tabelle A.11 vor. Danach beginnt sie mit der Verschlüsselung der Dateien (4.393). Die Lösegeldforderung wird immer doppelt als *# DECRPT FILES BLUESKY #.txt* und *# DECRPT FILES BLUESKY #.html* erstellt (je 445; gesamt 890). Die verschlüsselten Dateien erhalten die Endung *.bluesky*. Auch das Netzwerklaufwerk ist durch die Ransomware betroffen.
Während seiner Laufzeit versucht *BlueSky* eine Verbindung zu sich selbst auf Port 445

aufzubauen. Abgesehen davon wurden keine weiteren Auffälligkeiten bei der Netzwerkkommunikation erkannt.
Nachdem die Ransomware die Verschlüsselung abgeschlossen hat (ca. 43 s), ruft sie einen *explorer.exe*-Prozess auf, welcher localhost pingt und im Hintergrund die *bscy_22808.exe* löscht. Somit terminiert die Ransomware um 14:51:55.137 Uhr nach einer Laufzeit von ca. 44 s.

4.3.6 BlueSky AD-SV01

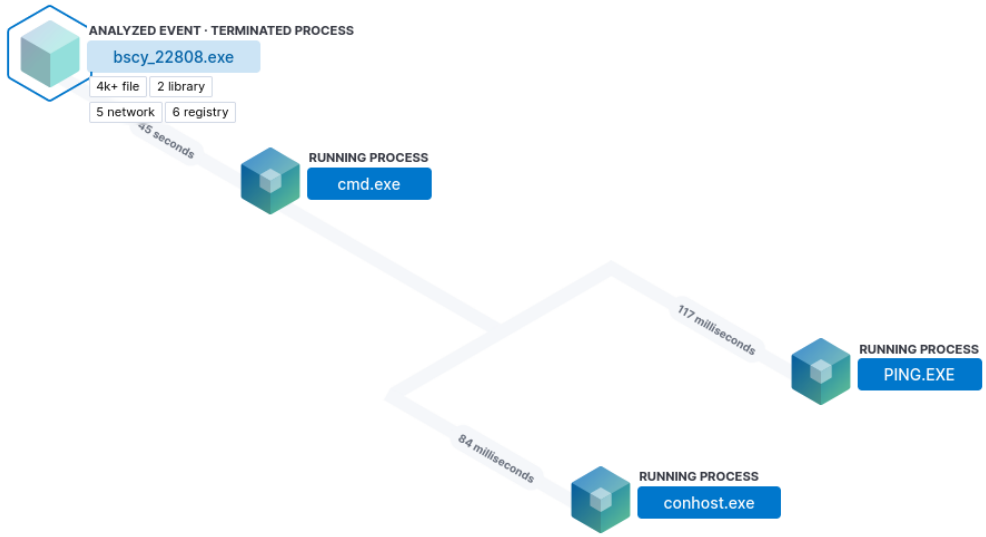


Abbildung 4.13: Übersicht BlueSky Prozesse (AD-SV01)

- Start: 12:12:15.701 Uhr
- Ende: 12:13:01.025 Uhr
- Dauer: 45.324 s

Im zweiten Durchlauf mit *BlueSky* wird die Ransomware durch *bscy_22808.exe* auf AD-SV01 um 12:12.15.701 Uhr gestartet. Analog zum vorherigen Versuch lädt die Ransomware ihre eigene sowie die *bcrypt.dll* Library. Daraufhin werden Änderungen an der Registry

vorgenommen (siehe Tab. A.12). Anschließend beginnt *BlueSky* mit der Verschlüsselung der Daten im lokalen Dateisystem und auf dem Netzwerklaufwerk. Die verschlüsselten Dateien erhalten die Endung *.bluesky*. Die Lösegeldforderung wird doppelt in den Dateien *# DECRPT FILES BLUESKY #.txt* und *# DECRPT FILES BLUESKY #.html* verbreitet.
Um 12:12:45.363 versucht die Ransomware eine Verbindung zu 192.169.2.11 (FS-SV01) auf Port 445 aufzubauen. Kurz nachdem diese Verbindung von FS-SV01 angenommen wird, beginnt *BlueSky* auch auf diesem Gerät die Dateien zu verschlüsseln und Lösegeldforderungen zu erstellen. Die Anzahl der Verschlüsselungen und erstellten Lösegeldforderungen auf den beiden Geräten können Tabelle 4.5 entnommen werden. Insgesamt wurden 6.367 Dateioperationen durch die Ransomware durchgeführt.
Um 12:13:01.025 Uhr löscht sich die Ransomware nach einer Laufzeit von ca. 45 s durch den gleichen Mechanismus wie im vorherigen Versuch.

Host	**Anz. Verschlüsselungen**	**Anz. Lösegeldforderungen**
AD-SV01	3.513	862
FS-SV01	1.030	962
$\sum$	4.543	1.824

Tabelle 4.5: Anzahl von Verschlüsselung und Lösegeldforderungen

4.3.7 Lilith CL-01

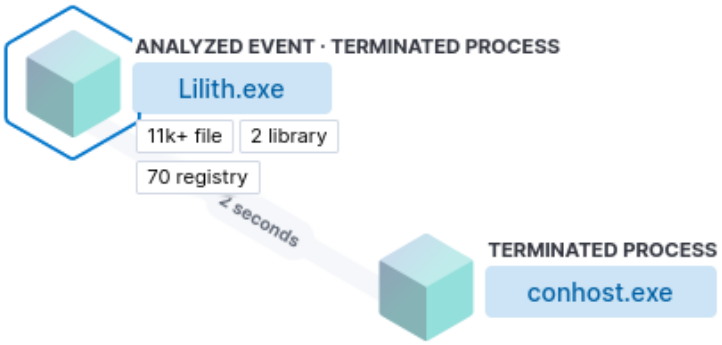


Abbildung 4.14: Übersicht Lilith Prozesse

- Start: 08:07:58.967 Uhr
- Ende: 08:10:16.534 Uhr
- Dauer: 02:17.567 min

Lilith wird um 08:07:58.967 Uhr durch die *lilith.exe* auf CL-01 gestartet. Die Ransomware lädt *bcrypt.dll* sowie ihre eigene Library und modifiziert die Registry an 70 verschiedenen Stellen (siehe Tab. A.13).
Es werden insgesamt 9.044 Verschlüsselungsoperationen durchgeführt und 2.692 Lösegeldforderungen mit dem Namen *Restore_Your_Files.txt* erstellt. Auch das Netzwerklaufwerk ist betroffen. Verschlüsselte Dateien erhalten *.lilith* als Dateiendung. Zwei Sekunden nach dem Start der Ransomware startet diese einen *conhost.exe*-Prozess in der Legacyversion V1. Der Analyzer zeigt, dass jedoch keine weiteren Ereignisse durch diesen Prozess

entstanden sind. Trotz der theoretischen Fähigkeit zur Datenexfiltration wurden keine auffälligen Netzwerkkommunikationen detektiert. Schließlich terminiert sich die Ransomware um 08:10:16.534 Uhr nach einer Laufzeit von ca. 2 min und 18 s selbst.

4.3.8 Moisha CL-01

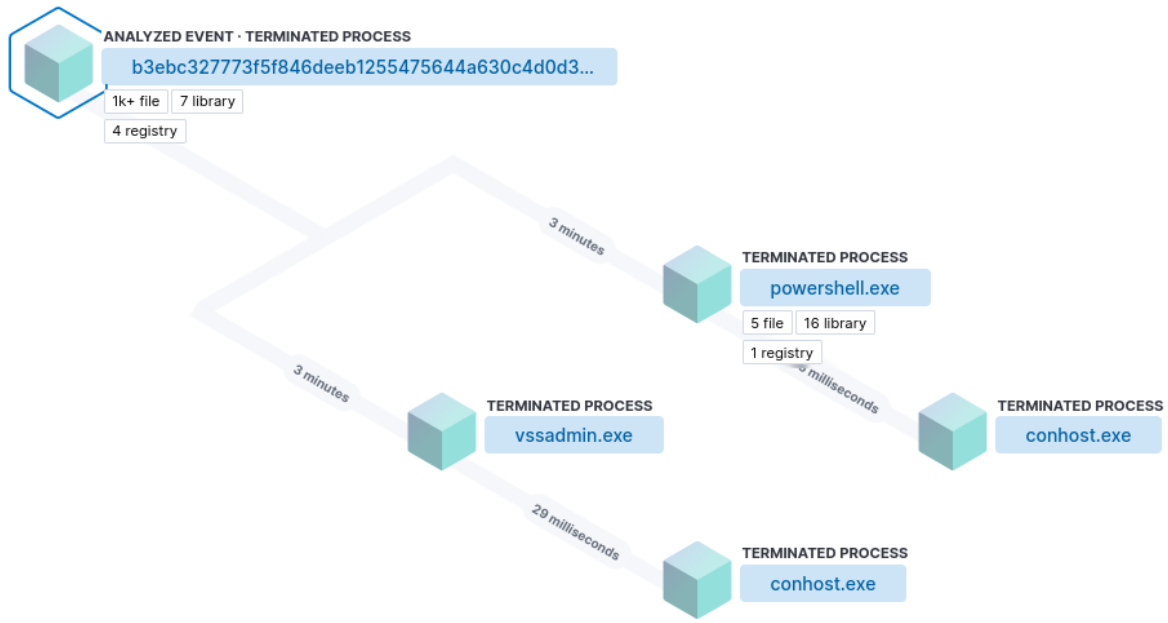


Abbildung 4.15: Übersicht Moisha Prozesse

- Start: 07:43:27.240 Uhr
- Ende: 07:47:18.534 Uhr
- Dauer: 03:51.294 min

Als letzter Durchlauf dieses Experiments wurde *Moisha* mittels der *b3ebc327773[...]99c07cf.exe* um 07:43:27.240 Uhr gestartet. Die Ransomware lädt eine Vielzahl an Libraries, die Tabelle 4.6 entnommen werden können, und ändert die Registry-Einträge aus Tabelle A.14. Anschließend beginnt sie mit der Verschlüsselung von 579 Dateien, wobei z.B. *.exe*-Dateien ausgelassen werden. Die Dateien des Netzwerklaufwerks sind auch von diesem Vorgang

betroffen. Es wird nur der Inhalt verschlüsselt und keine Dateiendung angefügt. Die Lösegeldforderungen werden durch *!!!READ TO RECOVER YOUR DATA!!!.txt*-Dateien verbreitet (396 mal).
Nachdem diese beiden Vorgänge abgeschlossen sind, startet die Ransomware zwei weitere Prozesse. Der *vssadmin.exe*-Prozess startet mit den Argumenten *delete shadows /all /quiet* und löscht alle Windows Shadowcopies. Mit dem *powershell.exe*-Prozess werden mehrere Instanzen eines *PSScriptPolicyTest_.ps1* erstellt und wieder gelöscht sowie mehrere Libraries geladen. Die eigentliche Funktion des Prozesses ist das Löschen der *b3ebc327773[...]99c07cf.exe*-Datei.
Die Laufzeit von *Moisha* endet nach ca. 3 min und 51 s um 07:47:18.534 Uhr. Es wurden keine auffälligen Netzwerkkommunikationen detektiert.

Library	**Beschreibung**
b3ebc327773[...]99c07cf.exe	Ransomware Library
bcrypt.dll	Windows Cryptographic Primitives Library
clr.dll	.NET Runtime Common Language Runtime
System.ni.dll	.NET Framework
System.ServiceProcess.ni.dll	.NET Framework
System.Core.ni.dll	.NET Framework
System.DirectoryServices.ni.dll	.NET Framework
System.Management.ni.dll	.NET Framework
System.Data.ni.dll	.NET Framework Module
System.Configuration.ni.dll	.NET Framework Module
System.Transactions.ni.dll	.NET Framework
System.Configuration.Install.ni.dll	.NET Framework Module
System.Drawing.ni.dll	.NET Module
System.Windows.Forms.ni.dll	.NET Framework module
symamsi.dll	Symantec AMSI provider
psapi.dll	Process Status Helper

Tabelle 4.6: Von Moisha geladene Libraries

4.4 Auswertung

Die Detektion von Ransomware-Angriffen hat in diesem Experiment eine Erfolgsquote von 100%, da alle eingesetzten Ransomwares bereits wenige Millisekunden nach ihrem Start durch die Elastic Agenten erkannt wurden (Bsp. Abb. 4.5). Allerdings muss beachtet werden, dass die Detektion in diesem Fall so erfolgreich war, weil alle verwendeten Samples bereits vorher bekannt waren und somit über Signaturen verfügten. Die Detektion von bisher unbekannter Ransomware wurde nicht überprüft.

RW	**verschl. Dateien**	**Dauer**	**Verschl. pro s**
TeslaCrypt	25.027	158,791 s	157,61
REvil CL-01	4.869	58,864 s	82,72
REvil CL-02	3.878	37,697 s	102,87
Lockbit	16.918	219,516 s	77,07
BlueSky CL-01	4.393	43,607 s	100,74
BlueSky AD-SV01	4.543	45,324 s	100,23
Lilith	9.044	137,567 s	65,74
Moisha	579	231,294 s	2,50
Minimum	579	37,697 s	2,50
Mittelwert	8.656	116,583 s	86
Maximum	25.027	231,294 s	157,61

Tabelle 4.7: Auswertung Beobachtungen

Die Tabelle 4.7 zeigt die Anzahl der verschlüsselten Dateien, die Dauer der Verschlüsselung sowie deren Quotienten (Verschlüsselungen pro Sekunde). Betrachtet man die Anzahl der verschlüsselten Dateien, ist zu erkennen, dass es eine sehr große Differenz zwischen Minimum und Maximum gibt. Auch wenn Ransomware-Entwickler unterschiedliche Ziele und Ausnahmen für bestimmte Ordner oder Dateitypen haben, erscheint die Zahl der detektierten Verschlüsselungsereignisse für *Moisha*, auch im Bezug zur benötigten Zeit, sehr gering.
Durchschnittlich wurden 8.656 Dateien in 116,583 s verschlüsselt, was einer Geschwindigkeit von 86 Verschlüsselungen pro Sekunde entspricht. Im Vergleich mit einem Whitepaper

von Splunk [DS22], die u.a. Verschlüsselungsgeschwindigkeiten von verschiedenen Ransomwares untersucht haben, zeigt sich, dass die ermittelten Werte für Verschlüsselungen pro Sekunde sehr ähnlich sind.
Damit der Schaden von Ransomware begrenzt werden kann, sollte diese also möglichst vor der Verschlüsselung erkannt werden, da bei einer Detektion während des Verschlüsselungsvorgangs nur wenig Zeit bleibt, um eine vollständige Verschlüsselung zu verhindern.
Im Fall von *BlueSky* sind keine nennenswerten Unterschiede zwischen den beiden Durchläufen in der Tabelle erkennbar. Die Verbreitung auf andere Systeme war jedoch nur von AD-SV01 aus erfolgreich, obwohl die selben Rechte zum Ausführen zur Verfügung standen. Würde dieses Muster auch in anderen Experimenten nachgewiesen werden, geht von der Infektion eines Domaincontrollers eine deutlich höhere Gefahr aus, als von den selben Nutzerrechten auf einem Client-Gerät.
Bei *REvil* werden im Durchlauf auf CL-02 ca. 1.000 Dateien weniger verschlüsselt, was auf fehlende Zugriffsrechte hinweisen könnte. Gleichzeitig ist dieser Durchlauf auch fast 20 s schneller und verschlüsselt ca. 20 Dateien pro Sekunde mehr als der mit Administratorrechten ausgeführte Lauf auf CL-01.

Library	**TeslaCrypt**	**REvil**	**Lockbit**	**BlueSky**	**Lilith**	**Moisha**
bcrypt.dll			x	x	x	x
clr.dll						x
fastprox.dll		x				
psapi.dll	x					x
symamsi.dll		x				x
System.Configuration.Install.ni.dll						x
System.Configuration.ni.dll						x
System.Core.ni.dll						x
System.Data.ni.dll						x
System.DirectoryServices.ni.dll						x
System.Drawing.ni.dll						x
System.Management.ni.dll						x
System.ni.dll						x
System.ServiceProcess.ni.dll						x
System.Transactions.ni.dll						x
System.Windows.Forms.ni.dll						x
UMEngx86.dll		x				
wbemcomn.dll		x				
wbemprox.dll		x				
wbemsvc.dll		x				

Tabelle 4.8: Übersicht verwendeter Libraries

Die Tabelle 4.8 zeigt, welche Libraries während der Ransomware-Laufzeiten geladen und subsequent detektiert worden sind. Zur Ermittlung, ob es Überscheidungen zwischen den DLLs gibt, wurden sowohl der Name, als auch die Hashwerte verglichen. Dabei ist zu erkennen, dass es kaum Überscheidungen gibt. Lediglich *bcrypt.dll* und *psapi.dll* wurden

von mehreren Ransomwares geladen. Die „Windows Cryptographic Primitives Library“ *bcrypt.dll* stellt verschiedenste kryptographische Funktionen zur Verfügung, die z.B. verwendet werden können, um Dateien zu verschlüsseln.[stra] Die *psapi.dll* ist eine Library von Prozessstatus-Helfern, die genutzt wird, um den Status von laufenden Prozessen und Treibern abzurufen.[strb] Der Elastic-Agent erkennt nur die Libraries, welche explizit durch die Ransomwares geladen werden. Libraries, die durch die Cyberkriminellen in die Ransomware-eigene fest integriert wurden, werden daher nicht erkannt.

Bei der Betrachtung der detektierten Registry-Änderungen lassen sich zwischen den Ransomwares nur wenige Gemeinsamkeiten erkennen. Mit der Ausnahme von *Lilith* haben jedoch alle, in mind. einem Durchlauf, Änderungen an den Registries *HKEY_USERS/[...] /Internet Settings/ZoneMap/AutoDetect*, *UNCAsIntranet*, *IntranetName* und *ProxyBypass* vorgenommen. Die Tabelle 4.9 zeigt eine Übersicht, in welchen Durchläufen die genannten Registries geändert wurden. Es wird vermutet, dass diese Änderungen gemacht werden, damit die Ransomware auf Netzwerklaufwerke zugreifen kann.[Ant20]

Durchlauf	**/AutoDetect**	**/UNCAsIntranet**	**/IntranetName**	**/ProxyBypass**
TeslaCrypt	x	x	x	x
REvil CL-01	x	x	x	x
REvil CL-02				
Lockbit	x	x	x	x
BlueSky CL-01	x	x	x	x
BlueSky AD-SV01	x	x		
Lilith				
Moisha	x	x	x	x

Tabelle 4.9: Übersicht verwendeter Libraries

Ein weiteres Ergebnis aus den Beobachtungen ist, dass nur bei *BlueSky* und *TeslaCrypt* auffällige Netzwerkkommunikationen erkannt wurden. Entsprechend ihrer Fähigkeiten (Tabelle 4.3) müssten auch bei *Lockbit*, *REvil*, *Lilith* und *Moisha* entsprechende Ereignisse zu detektieren sein.
Dies könnte sich aus dem Aufbau bzw. der Durchführung des Experiments ergeben, da explizit nur die Ransomwares-Samples selbst ausgeführt wurden. Die Samples sind jedoch oftmals nur das Ende einer komplexeren Angriffskette, welche alle drei Phasen eines Ransomware-Angriffs abdeckt. Die Ransomware-Executable wird dabei oft erst in der dritten Phase (Impact on Target) ausgeführt. Vorherige Phasen kümmern sich um das Einschleusen (Initial Access) und Ausbreiten (Consolidation and Preparation) im Zielnetzwerk. Das Command and Control kann einen Kommunikationskanal zwischen der

Ransomware und dem Angreifer bereitstellen. Fehlt dieser Kanal, weil nur die Ransomware-Executable gestartet wird, ist denkbar, dass manche Funktionen der Ransomware nicht korrekt ausgeführt werden und sich deshalb keine Netzwerkkommunikation beobachten lässt.

Kapitel 5

Zusammenfassung und Fazit

5.1 Zusammenfassung

Als Ransomware wird Schadsoftware (engl. Malware) verstanden, die den Zugriff auf Dateien und Systeme einschränkt oder vollständig verhindert. Den erneuten Zugriff geben die Angreifer erst nach der Zahlung von Lösegeld frei.
Um die verschiedenen Implementationen von Ransomware in der Praxis unterscheiden zu können, wurde eine Taxonomie vorgestellt, welche eine Klassifizierung nach den vier Aspekten *Ziel*, *Infektion*, *Kommunikation* und *Bösartige Aktion* vornimmt.
Die historische Entwicklung zeigt, dass sich Ransomware von einer einfachen Erpressermasche gegen hauptsächlich Einzelpersonen zu einem Geschäftsmodell mit einem Fokus auf größtmöglichen Gewinn entwickelt hat. So wird Ransomware seit 2016 vermehrt als Service im Darknet verkauft und das Ziel von Ransomware-Kampagnen richtet sich immer stärker gegen Organisationen und Unternehmen. Trotz der zunehmenden Verbreitung mobiler Geräte sind Windows-basierte Systeme nach wie vor das Hauptziel von Ransomware. Die von der Ransomware ausgeübten *bösartigen Aktionen* entwickeln sich von der vorangingen Sperrung von Systemen hin zu Verschlüsselung mit hybridem Ansatz. Gleichzeitig nutzen Angreifer den Zugriff zu infiltrierten Systemen, um Daten zu extrahieren und drohen dann zusätzlich mit der Veröffentlichung, sollte der Lösegeldforderung nicht Folge geleistet werden.
Im weiteren Verlauf der Arbeit wird der Lebenszyklus von Ransomware, welcher sich in die Phasen *Initial Access*, *Consolidation and Preparation* und *Impact on Target* aufteilt,

betrachtet. Während sich *Initial Access* und *Consolidation and Preparation* mit der Infektion der Zielinfrastruktur und der Ausbreitung in dieser befassen, findet die eigentliche Ransomware-Aktivität, das Exfiltrieren von Daten, Löschen von Backups und die Verschlüsselung erst in der dritten und letzten Phase statt.
Maßnahmen gegen Ransomware werden in die Kategorien *Prävention*, *Detektion* und *Reaktion* eingeteilt. Der Einsatz von präventiven Maßnahmen ist wichtig um die Anzahl der Vorfälle, die detektiert werden müssten, zu reduzieren. Haben Angreifer die präventiv getroffenen Maßnahmen überwinden können, greifen Maßnahmen der *Detektion*, deren Ziel die Erkennung des Angriffs ist. Wurde ein Angriff erfolgreich detektiert, werden Maßnahmen aus dem Bereich der *Reaktion* angewendet, um weiteren Schaden zu verhindern und bereits entstandene Schäden wieder zu reparieren.

Die Detektion von Malware ist der Prozess der Erkennung, ob Malware auf einem Host-System vorhanden bzw. ob ein Programm bös- oder gutartig ist. Dieser Prozess ist in die drei Phasen *Malware-Analyse*, *Extraktion von Merkmalen* und *Klassifizierung* unterteilt. Die Effektivität einer Detektionsmethode kann mithilfe einer Konfusionsmatrix sowie dazugehörigen Auswertungen bestimmt werden. Die Herausforderungen von Detektion sind sowohl theoretischer (NP-Vollständigkeit), als auch praktischer (Obfuscation-Techniken) Natur. Ansätze zur Detektion von Malware lassen sich in die Kategorien *Signaturbasiert*, *Verhaltensbasiert*, *Heuristik-Basiert*, *Modellbasiert*, *Semantik-Basiert* und *Künstliche Intelligenz-Basiert* unterteilen. Es gibt keinen Ansatz, der jede Art von Malware besser erkennen kann als alle anderen, da alle Ansätze Vor- und Nachteile haben. Die Detektion speziell von Ransomware zeigte, dass sich diese Methoden stark auf die Verschlüsselung als Indikator für einen Angriff verlassen. Indikatoren aus anderen Phasen wurden selten oder gar nicht verwendet. Nachfolgend wurde die Entstehungsgeschichte von Angriffserkennungssystemen sowie die Angriffserkennungssystemkategorien *Intrusion Detection System*, *Security Information and Event Management*, *Endpoint Detection and Response* und *Extended Detection and Response* betrachtet.

Das in dieser Arbeit beschriebene Experiment wurde in seinem Aufbau einer IT-Infrastruktur eines KRITIS-Unternehmens nachempfunden. Dafür wurden zwei windowsbasierte Clients, ein Windows Fileserver und ein Windows Active Directory eingerichtet. Zur Detektion wurde ein Elastic Stack auf einem weiteren Gerät konfiguriert, welcher mithilfe von Agenten verschiedene Informationen von den anderen Geräten sammelt und analysiert. Zwecks einer Internetverbindung wurde der pfSense-Firewall, welche für die Konfiguration des

Netzwerks verantwortlich war, ein LTE-Router vorgeschaltet.
Insgesamt wurden acht Durchläufe mit sechs unterschiedlichen Ransomwares durchgeführt. Die verwendeten Ransomwares waren *TeslaCrypt*, *Lockbit*, *REvil*, *BlueSky*, *Lilith* und *Moisha*. Mit der Ausnahme von *TeslaCrypt* wurden diese Ransomwares ausgewählt, da sie potentiell Fähigkeiten zu Privilege Escalation, Lateral Movement oder Datenexfiltration besitzen. *REvil* und *BlueSky* werden doppelt verwendet, um die Unterschiede zwischen verschiedenen Start-Host-Systemen zu erkennen.
Die Auswertung der Beobachtungen zeigte, dass die Infektion des Domaincontrollers ein besseres Ausgangssystem für Ransomware bieten, als ein Client-System, obwohl der derselbe Account zur Ausführung verwendet wurde. Gleichzeitig zeigte sich, dass unterschiedliche Ransomware-Familien unterschiedlich viele Dateien verschlüsseln und dabei auch unterschiedlich schnell sind. Im Durchschnitt wurden 86 Verschlüsselungen pro Sekunde durchgeführt, sodass für eine Reaktion und Schadensbegrenzung nur wenig Zeit bleibt, wenn die Ransomwares erstmal mit der Verschlüsselung begonnen haben. Des Weiteren wurden nur wenige Netzwerkaktivitäten detektiert, obwohl die verwendeten Ransomwares explizit für diese Fähigkeiten ausgewählt wurden.

5.2 Fazit

Die Anzahl von Ransomware-Angriffen auf Kritische Infrastrukturen nimmt immer stärker zu, da Cyberkriminelle Ransomware zu einem Geschäftsmodell entwickelt haben, welches auf bestmöglichen Profit aus ist. Unternehmen und Organisationen (KRITIS und nicht KRITIS) sind ein besonders lukratives Ziel dieses Geschäftsmodells.
Im Rahmen dieser Arbeit wurde gezeigt, dass die Detektion von Ransomware sowohl mit allgemeinen Detektionsansätzen als auch mit auf Ransomware spezialisierten Methoden gelingt. Die Ansätze, die ausschließlich für die Erkennung von Ransomware entwickelt wurden, sind jedoch nicht für alle Phasen des Lebenszyklus von Ransomware geeignet. Fast alle untersuchten Ansätze können einen Angriff erst in der dritten und letzten Phase des Angriffs erkennen. Die Erkennung erfolgt somit sehr spät im Lebenszyklus und lässt nur wenig Zeit für angemessene Reaktionen. Für die Früherkennung eines Ransomware-Angriffs ist die Kombination beider Ansatztypen (allgemein und spezialisiert) besser geeignet.
Das in dieser Arbeit durchgeführte Experiment hat gezeigt, dass die Detektion von

Ransomware mithilfe eines Angriffserkennungssystems in einer KRITIS nachempfundenen IT-Infrastruktur auch in der Praxis möglich ist. Die Indikatoren von Ransomware-Angriffen können dabei sowohl auf der Systemebene (Prozesse, Dateioperationen, Registry-Änderungen, etc.) als auch im Netzwerk (C2-Kommunikation, auffällige DNS-Anfragen, IP-Adressen, etc.) gefunden und erkannt werden. Gleichzeitig hat das Experiment auch gezeigt, dass die verwendeten Ransomware-Samples nur wenige Netzwerkaktivitäten durchgeführt haben, obwohl diese Fähigkeiten erwartet wurden. Dies ist möglicherweise darauf zurückzuführen, dass die Ransomware-Executable nur Teil einer komplexeren Angriffskette ist und die Netzwerkkommunikation normalerweise durch andere Komponenten/Tools übernommen wird, welche in diesem Experiment nicht vorhanden waren.

5.3 Ausblick

In weiteren Arbeiten könnte das Experiment für konkretere Fragestellungen modifiziert werden. Ein Ziel könnte beispielsweise sein, eine Ransomware-Angriffskette mit all ihren Phasen und den verwendeten Tools zu erkennen. Eine weitere Möglichkeit ist der Ausbau des Elastic Stacks. Durch Hinzufügen von weiteren Fleet-Integrationen und Datenquellen kann die Menge erhobener Daten erhöht werden, wodurch Elastic präzisere Bewertungen treffen kann.

Abbildungsverzeichnis

Tabellenverzeichnis

Quelltextverzeichnis

Glossar

ESET ESET ist ein in Bratislava gegründetes Sicherheissoftware-Unternehmen. 21

KRITIS Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Die zehn Sektoren sind: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Medien und Kultur, Wasser, Ernährung, Finanz- und Versicherungswesen, Siedlungsabfallentsorgung und Staat und Verwaltung. [BSI]. 3, 11

Malware Malware – ein Kofferwort aus den englischen Wörtern **mal**icious und Soft**ware** – beschreibt Computersoftware, welche schädliche und vom Opfer ungewollte Funktionen ausführt. 5

Abkürzungsverzeichnis

AD *Active Directory* 27

AES *Advanced Encryption Standard* 14, 15

BGH *Big Game Hunting* 26

BSI *Bundesamt für Sicherheit in der Informationstechnik* 4

BSIG *BSI-Gesetz* 4

C&C-Server *Command-and-Control-Server* 13, 15

CERT *Computer Emergency Response Team* 31

CPS *Cyber Physical System* 11

CTPL *Computation tree predicate logic* 41

DDoS *Distributed Denial of Service* 17

DGA *Domain Generation Alogrithms* 13

DSGVO *Datenschutz-Grundverordnung* 26

ECC *Elliptic Curve Cryptography* 21

EDR *Endpoint Detection and Response* 48, 50

EnWG *Energiewirtschaftsgesetz* 4

ETDR *Endpoint Threat Detection and Response* 48

GPO *Group Policy Object* 56

IDS *Intrusion Detection System* 47

IoT *Internet of Things* 11

IT-SiG *IT-Sicherheitsgesetz* 4

IT-SiG 2.0 *IT-Sicherheitsgesetz 2.0* 5, 47

KI *Künstliche Intelligenz* 42

LTL *Lineare temporale Logik* 41

MBR *Master Boot Record* 17, 20, 23

MFA *Multi-Faktor-Authentifizierung* 34

MFT *Master File Table* 16, 23

MSSP *Managed Security Service Provider* 50

RaaS *Ransomware-as-a-Service* 22, 30

RSA *Rivest–Shamir–Adleman* 15

SaaS *Software as a Service* 50

SIEM *Security Information and Event Management* 48, 49

SOAR *Security Orchestration and Automation* 49

UEBA *User and Entity Behavior Analytics* 49

VSS *Volume Shadow Copy Service* 16

XDR *Extended Detection and Response* 48, 52

Literaturverzeichnis

[0xZ22] 0xZuk0. *Malware Analysis Report WannaCry Ransomware*. 14. März 2022. URL: https://github.com/0xZuk0/rules-of-yaras/blob/0087fed9c7e65fd9fe52bba3ab51dcc6a594e690/reports/Wannacry%20Ransomware%20Report.pdf (besucht am 12. 10. 2022).

[Abr16] Lawrence Abrams. *TeslaCrypt Shuts down and Releases Master Decryption Key*. BleepingComputer. 18. Mai 2016. URL: https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/ (besucht am 06. 10. 2022).

[Abr22] Lawrence Abrams. *New DeadBolt Ransomware Targets QNAP Devices, Asks 50 BTC for Master Key*. BleepingComputer. 25. Jan. 2022. URL: https://www.bleepingcomputer.com/news/security/new-deadbolt-ransomware-targets-qnap-devices-asks-50-btc-for-master-key/ (besucht am 17. 10. 2022).

[AHT14] Shahid Alam, R. Nigel Horspool und Issa Traore. „MARD: A Framework for Metamorphic Malware Analysis and Real-Time Detection“. In: *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*. 2014 IEEE 28th International Conference on Advanced Information Networking and Applications. Mai 2014, S. 480–489. DOI: 10.1109/AINA.2014.59.

[Alz12] K. M. A. Alzarooni. „Malware Variant Detection“. Doctoral. UCL (University College London), 28. Mai 2012, ?–? 212 S. URL: https://discovery.ucl.ac.uk/id/eprint/1347243/ (besucht am 22. 12. 2022).

[AMS18] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof und Syed Zainudeen Mohd Shaid. „Ransomware Threat Success Factors, Taxonomy, and Countermeasures“. In: *Computers and Security* 74.C (1. Mai 2018), S. 144–166. ISSN: 0167-4048. DOI: 10.1016/j.cose.2018.01.001. URL: https://doi.org/10.1016/j.cose.2018.01.001 (besucht am 15. 05. 2022).

[Ant20] Stefano Antenucci. *WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group*. NCC Group Research. 23. Juni 2020. URL: https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/ (besucht am 19. 01. 2023).

[Arc18] Daniel G Arce. „Malware and Market Share“. In: *Journal of Cybersecurity* 4.1 (1. Jan. 2018), tyy010. ISSN: 2057-2085. DOI: 10.1093/cybsec/tyy010. URL: https://doi.org/10.1093/cybsec/tyy010 (besucht am 22. 06. 2022).

[Arg22] Ionut Arghire. *Researchers Devise Method to Decrypt Hive Ransomware-Encrypted Data | SecurityWeek.Com*. 21. Feb. 2022. URL: https://www.securityweek.com/researchers-devise-method-decrypt-hive-ransomware-encrypted-data (besucht am 13. 05. 2022).

[Ars17] Liviu Arsene. *Keranger: The First “in-the-Wild” Ransomware for Macs. But Certainly Not the Last*. Macworld. 25. Okt. 2017. URL: https://www.macworld.com/article/230621/keranger-the-first-in-the-wild-ransomware-for-macs-but-certainly-not-the-last.html (besucht am 11. 10. 2022).

[AS20] Ömer Aslan Aslan und Refik Samet. „A Comprehensive Review on Malware Detection Approaches“. In: *IEEE Access* 8 (2020), S. 6249–6271. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2963724.

[AVA17] Jagmeet Singh Aidan, Harsh Kumar Verma und Lalit Kumar Awasthi. „Comprehensive Survey on Petya Ransomware Attack“. In: *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*. 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS). Dez. 2017, S. 122–125. DOI: 10.1109/ICNGCIS.2017.30.

[Bau19] Roderick Bauer. *Survey Asks: How Often Do People Backup Their Computers?* Backblaze Blog | Cloud Storage & Cloud Backup. 9. Juli 2019. URL:

https://www.backblaze.com/blog/more-people-than-ever-backing-up-according-to-our-survey/ (besucht am 15. 06. 2022).

[BB17] Henry Belot und Stephanie Borys. „WannaCry Attack a Warning Not to Stockpile Tech Threats: Microsoft“. In: *ABC News* (14. Mai 2017). URL: https://www.abc.net.au/news/2017-05-15/ransomware-attack-to-hit-victims-in-australia-government-says/8526346 (besucht am 12. 10. 2022).

[BBK21] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe BBK. „Klärung und Erweiterung des KRITIS-Vokabulars“. In: (Jan. 2021), S. 9.

[Bis15] David Bisson. *Website Files Encrypted by Linux.Encoder.1 Ransomware? There Is Now a Free Fix*. Graham Cluley. 10. Nov. 2015. URL: https://grahamcluley.com/website-files-encrypted-linux-encoder-1-ransomware-free-fix/ (besucht am 05. 10. 2022).

[BK21] Christopher Bing und Stephanie Kelly. „Cyber Attack Shuts down U.S. Fuel Pipeline ‘Jugular,’ Biden Briefed“. In: *Reuters. Technology* (8. Mai 2021). URL: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/ (besucht am 06. 06. 2022).

[BKN09] Alex Biryukov, Dmitry Khovratovich und Ivica Nikolić. „Distinguisher and Related-Key Attack on the Full AES-256“. In: *Advances in Cryptology - CRYPTO 2009*. Hrsg. von Shai Halevi. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009, S. 231–249. ISBN: 978-3-642-03356-8. DOI: 10.1007/978-3-642-03356-8_14.

[BKR11] Andrey Bogdanov, Dmitry Khovratovich und Christian Rechberger. „Biclique Cryptanalysis of the Full AES“. In: *Advances in Cryptology – ASIACRYPT 2011*. Hrsg. von Dong Hoon Lee und Xiaoyun Wang. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2011, S. 344–371. ISBN: 978-3-642-25385-0. DOI: 10.1007/978-3-642-25385-0_19.

[BMI09] Bundesministerium des Inneren und für Heimat BMI. *Nationale Strategie Zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*. 17. Juni 2009. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html (besucht am 28. 10. 2022).

[BMJa] Bundesministerium der Justiz BMJ. *§ 11 EnWG - Einzelnorm*. URL: https://www.gesetze-im-internet.de/enwg_2005/__11.html (besucht am 30. 11. 2022).

[BMJb] Bundesministerium der Justiz BMJ. *§ 8a BSIG - Einzelnorm*. URL: https://www.gesetze-im-internet.de/bsig_2009/__8a.html (besucht am 10. 11. 2022).

[BMJc] Bundesministerium der Justiz BMJ. *§ 8d BSIG - Einzelnorm*. URL: https://www.gesetze-im-internet.de/bsig_2009/__8d.html (besucht am 03. 12. 2022).

[BMW19] Bundesministerium für Wirtschaft und Energie BMWi. *Was ist Industrie 4.0?* Was ist Industrie 4.0? 2019. URL: https://www.plattform-i40.de/IP/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html (besucht am 26. 07. 2022).

[BSI] Bundesamt für Sicherheit in der Inforamtionstechnik BSI. *Was sind Kritische Infrastrukturen?* Bundesamt für Sicherheit in der Informationstechnik. URL: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis.html?nn=126640 (besucht am 26. 07. 2022).

[BSI22a] Bundesamt für Sicherheit in der Inforamtionstechnik BSI. *BSI - KRITIS Und Regulierte Unternehmen - Orientierungshilfe Zum Einsatz von Systemen Zur Angriffserkennung*. 29. Sep. 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf (besucht am 10. 11. 2022).

[BSI22b] Bundesamt für Sicherheit in der Inforamtionstechnik BSI. *Die Lage der IT-Sicherheit in Deutschland 2022*. Bundesamt für Sicherheit in der Informationstechnik. 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410 (besucht am 04. 12. 2022).

[BSI22c] Bundesamt für Sicherheit in der Inforamtionstechnik BSI. *IT-Grundschutz-Kompendium*. Bundesamt für Sicherheit in der Informationstechnik. 2022. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-

Grundschutz-Kompendium/itgrundschutzKompendium.html?nn=128568 (besucht am 04. 12. 2022).

[BSI22d] Bundesamt für Sicherheit in der Inforamtionstechnik BSI. *Maßnahmenkatalog Ransomware*. Bundesamt für Sicherheit in der Informationstechnik. 23. Feb. 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.html?nn=132646 (besucht am 09. 12. 2022).

[BSI22e] Bundesamt für Sicherheit in der Inforamtionstechnik BSI. *Ransomware: Bedrohungslage 2022*. Bundesamt für Sicherheit in der Informationstechnik. 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html?nn=132646 (besucht am 09. 12. 2022).

[BSI22f] Bundesamt für Sicherheit in der Inforamtionstechnik BSI. *Ransomware: Bedrohungslage, Prävention & Reaktion 2021*. Bundesamt für Sicherheit in der Informationstechnik. 27. Sep. 2022. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Ransomware/Ransomware.html?nn=133710 (besucht am 09. 12. 2022).

[Cab22] Jack Cable. *Ransomwhere: A Crowdsourced Ransomware Payment Dataset*. Version 1.0.0. Zenodo, Mai 2022. DOI: 10.5281/zenodo.6512123. URL: https://doi.org/10.5281/zenodo.6512123.

[Che17] Zhi-Guo Chen u. a. „Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph“. In: *Proceedings of the International Conference on Research in Adaptive and Convergent Systems*. RACS '17. New York, NY, USA: Association for Computing Machinery, 20. Sep. 2017, S. 196–201. ISBN: 978-1-4503-5027-3. DOI: 10.1145/3129676.3129704. URL: https://doi.org/10.1145/3129676.3129704 (besucht am 29. 12. 2022).

[Chr05] Mihai Christodorescu u. a. „Semantics-Aware Malware Detection“. In: Proceedings - IEEE Symposium on Security and Privacy. 8. Juni 2005, S. 32–46. ISBN: 978-0-7695-2339-2. DOI: 10.1109/SP.2005.20.

[Chu13] Anton Chuvakin. *Named: Endpoint Threat Detection & Response*. Anton Chuvakin. 26. Juli 2013. URL: https://blogs.gartner.com/anton-chuvak

in/2013/07/26/named-endpoint-threat-detection-response/ (besucht am 03. 01. 2023).

[CIS17] Center for Internet Security CIS. *Ransomware: Facts, Threats, and Countermeasures*. CIS. 15. Mai 2017. URL: https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/ (besucht am 02. 08. 2022).

[Clo18] Cloudflare. *Was sind Petya und NotPetya? | Ransomware-Angriffe*. Cloudflare. 2018. URL: https://www.cloudflare.com/de-de/learning/security/ransomware/petya-notpetya-ransomware/ (besucht am 12. 10. 2022).

[Clo21] Cloudflare. *Was ist Ransomware-as-a-Service (RaaS)?* Cloudflare. 2021. URL: https://www.cloudflare.com/de-de/learning/security/ransomware/ransomware-as-a-service/ (besucht am 06. 10. 2022).

[CNN22] Evan Perez CNN Zachary Cohen and Alex Marquardt. *First on CNN: US Recovers Millions in Cryptocurrency Paid to Colonial Pipeline Ransomware Hackers*. CNN. 8. Juni 2022. URL: https://www.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html (besucht am 06. 06. 2022).

[Coh87] Fred Cohen. „Computer Viruses: Theory and Experiments“. In: *Computers & Security* 6.1 (1. Feb. 1987), S. 22–35. ISSN: 0167-4048. DOI: 10.1016/0167-4048(87)90122-2. URL: https://www.sciencedirect.com/science/article/pii/0167404887901222 (besucht am 20. 12. 2022).

[Coh89] Fred Cohen. „Computational Aspects of Computer Viruses“. In: *Computers & Security* 8 (1. Juni 1989), S. 297–298. DOI: 10.1016/0167-4048(89)90089-8.

[Cro19] Crowdstrike. *What Is Ryuk Ransomware? The Complete Breakdown*. crowdstrike.com. 10. Jan. 2019. URL: https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/ (besucht am 16. 10. 2022).

[Cro22] Crowdstrike. *What Is Cyber Big Game Hunting? | CrowdStrike*. crowdstrike.com. 20. März 2022. URL: https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/ (besucht am 11. 10. 2022).

[CW01] David Chess und Steve White. „An Undetectable Computer Virus“. In: (19. Okt. 2001).

[Dan21] Brett Daniel. *Symmetric vs. Asymmetric Encryption: What's the Difference?* 4. Mai 2021. URL: https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption (besucht am 08. 08. 2022).

[Del22] Deland-Han u. a. *Windows Registry for Advanced Users - Windows Server.* 4. Juni 2022. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users (besucht am 13. 01. 2023).

[Den87] D.E. Denning. „An Intrusion-Detection Model". In: *IEEE Transactions on Software Engineering* SE-13.2 (Feb. 1987), S. 222–232. ISSN: 1939-3520. DOI: 10.1109/TSE.1987.232894.

[Dic16] Ben Dickson. *What Makes IoT Ransomware a Different and More Dangerous Threat?* TechCrunch. 3. Okt. 2016. URL: https://social.techcrunch.com/2016/10/02/what-makes-iot-ransomware-a-different-and-more-dangerous-threat/ (besucht am 26. 07. 2022).

[Die14] Sven Dietrich. *Detection of Intrusions and Malware, and Vulnerability Assessment.* Juli 2014. URL: https://link.springer.com/book/10.1007/978-3-319-08509-8 (besucht am 14. 08. 2022).

[Doc21] MS Docs. *Volume Shadow Copy Service.* 8. Okt. 2021. URL: https://docs.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service (besucht am 14. 08. 2022).

[Don22] Chuong Dong. *LockBit Ransomware v2.0.* Chuong Dong. 19. März 2022. URL: https://cdong1012.github.io//reverse%20engineering/2022/03/19/LockbitRansomware/ (besucht am 16. 10. 2022).

[Dra22] Veronica Drake. *The History and Evolution of Ransomware Attacks.* Flashpoint. 29. Juli 2022. URL: https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/ (besucht am 23. 08. 2022).

[DrW15] Dr.Web. *Encryption Ransomware Threatens Linux Users.* 6. Nov. 2015. URL: https://news.drweb.com/show?i=9686&c=5&lng=en&p=0 (besucht am 05. 10. 2022).

[DS22] Shannon Davies und Splunk. *An Empirically Comparative Analysis of Ransomware Binaries*. 2022. URL: https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf (besucht am 18. 05. 2022).

[Ela] Elasticsearch. *Elasticsearch: Die offizielle Engine für verteilte Suche und Analytics*. Elastic. URL: https://www.elastic.co/de/elasticsearch (besucht am 06. 01. 2023).

[ENI21] ENISA. *ENISA Threat Landscape 2021*. ENISA. 2021. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (besucht am 16. 06. 2022).

[Exa] Exabeam. *A SIEM Security Primer: Evolution and Next-Gen Capabilities*. Exabeam. URL: https://www.exabeam.com/explainers/siem/a-siem-security-primer/ (besucht am 03. 01. 2023).

[Ext21] ExtraHop. *Next Generatrion Intrusion Detection Systems*. 2021. URL: https://assets.extrahop.com/whitepapers/ng-ids.pdf (besucht am 02. 01. 2023).

[Fis10] Dennis Fisher. *New Seftad Ransomware Attacks Master Boot Record*. 30. Nov. 2010. URL: https://threatpost.com/new-seftad-ransomware-attacks-master-boot-record-113010/74714/ (besucht am 22. 08. 2022).

[fsec] f-secure. *Trojan:W32/Gpcode Description | F-Secure Labs*. URL: https://www.f-secure.com/v-descs/gpcode.shtml (besucht am 22. 08. 2022).

[Gle22] Walter Glenn. *What Is Conhost.Exe and Why Is It Running?* How-To Geek. 22. Dez. 2022. URL: https://www.howtogeek.com/4996/what-is-conhost.exe-and-why-is-it-running/ (besucht am 12. 01. 2023).

[Gmb15] „Gesetz Zur Erhöhung Der Sicherheit Informationstechnischer Systeme (IT-Sicherheitsgesetz)“. In: *Bundesgesetzblatt Teil I* 31 (24. Juli 2015). Hrsg. von Bundesanzeiger Verlag GmbH, S. 1324. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf (besucht am 08. 11. 2022).

[Gmb21] „Zweites Gesetz Zur Erhöhung Der Sicherheit Informationstechnischer Systeme“. In: *Bundesgesetzblatt Teil I* 25 (27. Mai 2021). Hrsg. von Bundesanzeiger Verlag GmbH, S. 1122. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf (besucht am 08. 11. 2022).

[Gro15] Somayya Madakam$IT Applications Group u. a. „Internet of Things (IoT): A Literature Review“. In: *Journal of Computer and Communications* 03.05 (05 2015), S. 164. DOI: 10.4236/jcc.2015.35021. URL: http://www.scirp.org/journal/PaperInformation.aspx?PaperID=56616&#abstract (besucht am 26. 07. 2022).

[Gro16] Kathrin Grosse u. a. *Adversarial Perturbations Against Deep Neural Networks for Malware Classification*. 16. Juni 2016. DOI: 10.48550/arXiv.1606.04435. arXiv: 1606.04435 [cs]. URL: http://arxiv.org/abs/1606.04435 (besucht am 22. 12. 2022).

[Hac22] Hacktricks. *Integrity Levels*. 2022. URL: https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/integrity-levels (besucht am 13. 01. 2023).

[Has19] Nihad A. Hassan. „Ransomware Families“. In: *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks*. Hrsg. von Nihad A. Hassan. Berkeley, CA: Apress, 2019. ISBN: 978-1-4842-4255-1. DOI: 10.1007/978-1-4842-4255-1_3. URL: https://doi.org/10.1007/978-1-4842-4255-1_3 (besucht am 08. 08. 2022).

[Hel22] Software Testing Help. *Top 10 BEST Intrusion Detection Systems (IDS) [2023 Rankings]*. Software Testing Help. 28. Dez. 2022. URL: https://www.softwaretestinghelp.com/intrusion-detection-systems/ (besucht am 03. 01. 2023).

[Hil22] Jason Hill. *BlackCat Ransomware (ALPHV) | Varonis*. 26. Feb. 2022. URL: https://www.varonis.com/blog/blackcat-ransomware (besucht am 16. 10. 2022).

[HKV07] Andreas Holzer, Johannes Kinder und Helmut Veith. „Using Verification Technology to Specify and Detect Malware“. In: *Computer Aided Systems Theory – EUROCAST 2007*. Hrsg. von Roberto Moreno Díaz, Franz Pichler

und Alexis Quesada Arencibia. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2007, S. 497–504. ISBN: 978-3-540-75867-9. DOI: 10.1007/978-3-540-75867-9_63.

[Hop14] Tobias Hoppe. „Prävention, Detektion und Reaktion gegen drei Ausprägungsformen automotiver Malware: eine methodische Analyse im Spektrum von Manipulationen und Schutzkonzepten“. Magdeburg: Universitätsbibliothek, 2014.

[HTS22] Alex Hinchliffe, Amanda Tanner und Doel Santos. *Threat Assessment: BlackCat Ransomware*. Unit 42. 27. Jan. 2022. URL: https://unit42.paloaltonetworks.com/blackcat-ransomware/ (besucht am 16. 10. 2022).

[Hua18] Danny Yuxing Huang u. a. „Tracking Ransomware End-to-end“. In: *2018 IEEE Symposium on Security and Privacy (SP)*. 2018 IEEE Symposium on Security and Privacy (SP). Mai 2018, S. 618–631. DOI: 10.1109/SP.2018.00047.

[Hur17] Karan Sood and Shaun Hurley. *NotPetya Ransomware Attack [Technical Analysis]*. crowdstrike.com. 29. Juni 2017. URL: https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ (besucht am 22. 01. 2023).

[Inc22] Gartner Inc. *Top Cortex XDR Competitors & Alternatives 2023 | Gartner Peer Insights*. Gartner. 2022. URL: https://www.gartner.com/market/endpoint-detection-and-response-solutions/vendor/palo-alto-networks/product/cortex-xdr/alternatives (besucht am 04. 01. 2023).

[Ins22] Gartner Peer Insights. *Security Information and Event Management (SIEM) Reviews 2023 | Gartner Peer Insights*. 2022. URL: https://www.gartner.com/reviews/market/security-information-event-management (besucht am 04. 01. 2023).

[Isl21] Md Mazharul Islam u. a. „CHIMERA: Autonomous Planning and Orchestration for Malware Deception“. In: *2021 IEEE Conference on Communications and Network Security (CNS)*. 2021 IEEE Conference on Communications and Network Security (CNS). Okt. 2021, S. 173–181. DOI: 10.1109/CNS53000.2021.9705030.

[Jar13] Keith Jarvis. *CryptoLocker Ransomware*. 18. Dez. 2013. URL: https://papers.vx-underground.org/papers/Malware%20Defense/Malware%20Analysis/2013-12-18%20-%20CryptoLocker%20Ransomware.pdf (besucht am 08. 08. 2022).

[Jey22] Anusthika Jeyashankar. *Most Common Malware Obfuscation Techniques - Security Investigation*. 2. Feb. 2022. URL: https://www.socinvestigation.com/most-common-malware-obfuscation-techniques/ (besucht am 20. 12. 2022).

[Ji22] Yang Ji u. a. *BlueSky Ransomware: Fast Encryption via Multithreading*. Unit 42. 10. Aug. 2022. URL: https://unit42.paloaltonetworks.com/bluesky-ransomware/ (besucht am 17. 10. 2022).

[Jin22] Jinni. *Download Malware Samples*. Tutorial Jinni. 2022. URL: https://www.tutorialjinni.com/download-free-malware-samples.htm (besucht am 09. 01. 2023).

[JR08] Markus Jakobsson und Zulfikar Ramzan. „Crimeware : Understanding New Attacks and Defenses / M. Jakobsson, Z. Ramzan.“ In: (1. Jan. 2008).

[JS11] K. Jansson und Rossouw Solms. „Phishing for Phishing Awareness“. In: *Behaviour & Information Technology - Behaviour & IT* 32 (1. Jan. 2011), S. 1–10. DOI: 10.1080/0144929X.2011.632650.

[Kaj19] Michael Kajiloti. *PureLocker: New RaaS Being Used Against Enterprise Servers*. Intezer. 12. Nov. 2019. URL: https://www.intezer.com/blog/malware-analysis/purelocker-ransomware-being-used-in-targeted-attacks-against-servers/ (besucht am 14. 10. 2022).

[Kam10] Vitaly Kamluk. *GpCode-like Ransomware Is Back*. 29. Nov. 2010. URL: https://securelist.com/gpcode-like-ransomware-is-back/29633/ (besucht am 22. 08. 2022).

[Kas19] Kaspersky. *Mobile Ransomware: Major Threats and Best Means of Protection*. Juni 2019. URL: https://www.kaspersky.com/blog/mobile-ransomware-2016/12491/ (besucht am 14. 08. 2022).

[Kas21a] Kaspersky. *TeslaCrypt Ransomware Attacks*. www.kaspersky.com. 13. Jan. 2021. URL: https://www.kaspersky.com/resource-center/threats/teslacrypt (besucht am 06. 10. 2022).

[Kas21b] Kaspersky. *Was ist die heuristische Analyse?* www.kaspersky.de. 13. Jan. 2021. URL: https://www.kaspersky.de/resource-center/definitions/heuristic-analysis (besucht am 22. 12. 2022).

[Kas22a] Kaspersky. *What Is a Drive by Download.* www.kaspersky.com. 9. Feb. 2022. URL: https://www.kaspersky.com/resource-center/definitions/drive-by-download (besucht am 02. 08. 2022).

[Kas22b] Kaspersky. *What Is a Zero-day Attack? - Definition and Explanation.* 9. Feb. 2022. URL: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit (besucht am 02. 08. 2022).

[Kei20] N. Keijzer. *The New Generation of Ransomware : An in Depth Study of Ransomware-as-a-Service.* 25. Juni 2020. URL: http://essay.utwente.nl/81595/ (besucht am 10. 10. 2022).

[kh422] kh4sh3i. *Ransomware-Samples.* 21. Dez. 2022. URL: https://github.com/kh4sh3i/Ransomware-Samples (besucht am 09. 01. 2023).

[Kha16] Amin Kharaz u. a. „{UNVEIL}: A {Large-Scale}, Automated Approach to Detecting Ransomware“. In: 25th USENIX Security Symposium (USENIX Security 16). 2016, S. 757–772. ISBN: 978-1-931971-32-4. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kharaz (besucht am 18. 05. 2022).

[Kha17] Swati Khandelwal. *WannaCry Ransomware Decryption Tool Released; Unlock Files Without Paying Ransom.* The Hacker News. 19. Mai 2017. URL: https://thehackernews.com/2017/05/wannacry-ransomware-decryption-tool.html (besucht am 12. 10. 2022).

[Khr19] Ansam Khraisat u. a. „Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges“. In: *Cybersecurity* 2 (1. Dez. 2019). DOI: 10.1186/s42400-019-0038-7.

[Kin05] Johannes Kinder u. a. „Detecting Malicious Code by Model Checking“. In: *Detection of Intrusions and Malware, and Vulnerability Assessment.* Hrsg. von Klaus Julisch und Christopher Kruegel. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2005, S. 174–187. ISBN: 978-3-540-31645-9. DOI: 10.1007/11506881_11.

[Kin10] Johannes Kinder u. a. „Proactive Detection of Computer Worms Using Model Checking“. In: *IEEE Transactions on Dependable and Secure Computing* 7.4 (Okt. 2010), S. 424–438. ISSN: 1941-0018. DOI: 10.1109/TDSC.2008.74.

[KKV11] Stefan Katzenbeisser, Johannes Kinder und Helmut Veith. „Malware Detection“. In: *Encyclopedia of Cryptography and Security*. Hrsg. von Henk C. A. van Tilborg und Sushil Jajodia. Boston, MA: Springer US, 2011, S. 752–755. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_838. URL: https://doi.org/10.1007/978-1-4419-5906-5_838 (besucht am 15. 12. 2022).

[KMD16] Matjaž Kljun, John Mariani und Alan Dix. „Toward Understanding Short-Term Personal Information Preservation: A Study of Backup Strategies of End Users“. In: *Journal of the Association for Information Science and Technology* 67.12 (Dez. 2016), S. 2947–2963. ISSN: 23301635. DOI: 10.1002/asi.23526. URL: https://onlinelibrary.wiley.com/doi/10.1002/asi.23526 (besucht am 15. 06. 2022).

[Kno19a] KnowBe4. *CTB-Locker Ransomware | KnowBe4*. 2019. URL: https://www.knowbe4.com/curve-tor-bitcoin-locker (besucht am 05. 10. 2022).

[Kno19b] KnowBe4. *Reveton Worm Ransomware | KnowBe4*. 2019. URL: https://www.knowbe4.com/reveton-worm (besucht am 04. 10. 2022).

[Kol18] Bojan Kolosnjaji u. a. *Adversarial Malware Binaries: Evading Deep Learning for Malware Detection in Executables*. 12. März 2018. DOI: 10.48550/arXiv.1803.04173. arXiv: 1803.04173 [cs]. URL: http://arxiv.org/abs/1803.04173 (besucht am 22. 12. 2022).

[Kos19] Dave Kostos. *World Backup Day: 2019 Survey Results*. Acronis. 26. März 2019. URL: https://www.acronis.com/en-us/blog/posts/world-backup-day-2019-survey-results/ (besucht am 15. 06. 2022).

[Kov18] Eduard Kovacs. *U.S., Canada, Australia Attribute NotPetya Attack to Russia | SecurityWeek.Com*. 16. Feb. 2018. URL: https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia (besucht am 12. 10. 2022).

[Lab16] Malwarebytes Labs. *Petya - Taking Ransomware To The Low Level | Malwarebytes Labs*. Malwarebytes. 1. Apr. 2016. URL: https://www.malwarebytes.com/blog/news/2016/04/petya-ransomware (besucht am 11. 10. 2022).

[Lab17] Malwarebytes Labs. *Keeping up with the Petyas: Demystifying the Malware Family | Malwarebytes Labs*. Malwarebytes. 14. Juli 2017. URL: https://www.malwarebytes.com/blog/news/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family (besucht am 11. 10. 2022).

[Les20] Marlese Lessing. *Case Study: AIDS Trojan Ransomware*. SDxCentral. 3. Juni 2020. URL: https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-aids-trojan-ransomware/ (besucht am 22. 08. 2022).

[Lin17] Michael Link. *Ransomware WannaCry: Sicherheitsexperte findet "Kill-Switch"– durch Zufall*. heise online. 13. Mai 2017. URL: https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-Sicherheitsexperte-findet-Kill-Switch-durch-Zufall-3713420.html (besucht am 12. 10. 2022).

[LS18] Yassine Lemmou und El Mamoun Souidi. „Infection, Self-reproduction and Overinfection in Ransomware: The Case of TeslaCrypt“. In: *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). Juni 2018, S. 1–8. DOI: 10.1109/CyberSecPODS.2018.8560670.

[LŠB16] Robert Lipovský, Lukáš Štefanko und Gabriel Braniša. *Rise of Android Ransomware*. Feb. 2016. URL: https://www.welivesecurity.com/wp-content/uploads/2016/02/Rise_of_Android_Ransomware.pdf (besucht am 21. 08. 2022).

[Lub21a] Stefan Luber. *Was ist Endpoint Detection and Response (EDR)?* 5. Mai 2021. URL: https://www.security-insider.de/was-ist-endpoint-detection-and-response-edr-a-1044268/ (besucht am 04. 01. 2023).

[Lub21b] Stefan Luber. *Was Ist XDR?* 19. Apr. 2021. URL: https://www.security-insider.de/was-ist-xdr-a-1021710/ (besucht am 04. 01. 2023).

[Lut21] Ben Lutkevich. *What Is Obfuscation and How Does It Work?* Security. Apr. 2021. URL: https://www.techtarget.com/searchsecurity/definition/obfuscation (besucht am 20. 12. 2022).

[McA21] McAfee. *2021 Threat Predictions Report*. McAfee Blog. 13. Jan. 2021. URL: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report/ (besucht am 06. 07. 2022).

[Mei16] Sarah Meiklejohn u. a. „A Fistful of Bitcoins: Characterizing Payments among Men with No Names“. In: *Communications of the ACM* 59.4 (23. März 2016), S. 86–93. ISSN: 0001-0782. DOI: 10.1145/2896384. URL: https://doi.org/10.1145/2896384 (besucht am 30. 08. 2022).

[Mic22] Trend Micro. *Closing the Door DeadBolt Ransomware Locks Out Vendors With Multitiered Extortion Scheme*. Trend Micro. 6. Juni 2022. URL: https://www.trendmicro.com/en_us/research/22/f/closing-the-door-deadbolt-ransomware-locks-out-vendors-with-mult.html (besucht am 17. 10. 2022).

[Min18] Donghyun Min u. a. „Amoeba: An Autonomous Backup and Recovery SSD for Ransomware Attack Defense“. In: *IEEE Computer Architecture Letters* 17.2 (Juli 2018), S. 245–248. ISSN: 1556-6064. DOI: 10.1109/LCA.2018.2883431.

[MIT] MITRE. *FAQ | MITRE ATT&CK®*. URL: https://attack.mitre.org/resources/faq/ (besucht am 05. 12. 2022).

[MIT21a] ATT&CK MITRE. *Account Discovery, Technique T1087 - Enterprise | MITRE ATT&CK®*. 13. Okt. 2021. URL: https://attack.mitre.org/techniques/T1087/ (besucht am 08. 12. 2022).

[MIT21b] ATT&CK MITRE. *Encrypted Channel, Technique T1573 - Enterprise | MITRE ATT&CK®*. 20. Apr. 2021. URL: https://attack.mitre.org/techniques/T1573/ (besucht am 08. 12. 2022).

[MIT21c] ATT&CK MITRE. *Permission Groups Discovery, Technique T1069 - Enterprise | MITRE ATT&CK®*. 15. Okt. 2021. URL: https://attack.mitre.org/techniques/T1069/ (besucht am 08. 12. 2022).

[MIT22a] ATT&CK MITRE. *Archive Collected Data, Technique T1560 - Enterprise | MITRE ATT&CK®*. 4. Jan. 2022. URL: https://attack.mitre.org/techniques/T1560/ (besucht am 08. 12. 2022).

[MIT22b] ATT&CK MITRE. *BloodHound, Software S0521 | MITRE ATT&CK®*. 27. Sep. 2022. URL: https://attack.mitre.org/software/S0521/ (besucht am 08. 12. 2022).

[MIT22c] ATT&CK MITRE. *Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®*. 19. Apr. 2022. URL: https://attack.mitre.org/techniques/T1110/ (besucht am 08. 12. 2022).

[MIT22d] ATT&CK MITRE. *Cobalt Strike, Software S0154 | MITRE ATT&CK®*. 12. Okt. 2022. URL: https://attack.mitre.org/software/S0154/ (besucht am 08. 12. 2022).

[MIT22e] ATT&CK MITRE. *Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®*. 16. Juni 2022. URL: https://attack.mitre.org/techniques/T1486/ (besucht am 08. 12. 2022).

[MIT22f] ATT&CK MITRE. *Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®*. 19. Okt. 2022. URL: https://attack.mitre.org/techniques/T1005/ (besucht am 08. 12. 2022).

[MIT22g] ATT&CK MITRE. *Data from Network Shared Drive, Technique T1039 - Enterprise | MITRE ATT&CK®*. 16. Juni 2022. URL: https://attack.mitre.org/techniques/T1039/ (besucht am 08. 12. 2022).

[MIT22h] ATT&CK MITRE. *Domain Trust Discovery, Technique T1482 - Enterprise | MITRE ATT&CK®*. 16. Juni 2022. URL: https://attack.mitre.org/techniques/T1482/ (besucht am 08. 12. 2022).

[MIT22i] ATT&CK MITRE. *Exfiltration Over Web Service, Technique T1567 - Enterprise | MITRE ATT&CK®*. 19. Okt. 2022. URL: https://attack.mitre.org/techniques/T1567/ (besucht am 08. 12. 2022).

[MIT22j] ATT&CK MITRE. *Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®*. 19. Apr. 2022. URL: https://attack.mitre.org/techniques/T1190/ (besucht am 08. 12. 2022).

[MIT22k] ATT&CK MITRE. *Exploitation for Privilege Escalation, Technique T1068 - Enterprise | MITRE ATT&CK®*. 16. Juni 2022. URL: https://attack.mitre.org/techniques/T1068/ (besucht am 08. 12. 2022).

[MIT22l] ATT&CK MITRE. *External Remote Services, Technique T1133 - Enterprise | MITRE ATT&CK®*. 16. Juni 2022. URL: https://attack.mitre.org/techniques/T1133/ (besucht am 08. 12. 2022).

[MIT22m] ATT&CK MITRE. *Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®*. 19. Apr. 2022. URL: https://attack.mitre.org/techniques/T1490/ (besucht am 08. 12. 2022).

[MIT22n] ATT&CK MITRE. *Lateral Tool Transfer, Technique T1570 - Enterprise | MITRE ATT&CK®*. 19. Apr. 2022. URL: https://attack.mitre.org/techniques/T1570/ (besucht am 08. 12. 2022).

[MIT22o] ATT&CK MITRE. *Mimikatz, Software S0002 | MITRE ATT&CK®*. 3. Aug. 2022. URL: https://attack.mitre.org/software/S0002/ (besucht am 08. 12. 2022).

[MIT22p] ATT&CK MITRE. *Network Service Discovery, Technique T1046 - Enterprise | MITRE ATT&CK®*. 20. Apr. 2022. URL: https://attack.mitre.org/techniques/T1046/ (besucht am 08. 12. 2022).

[MIT22q] ATT&CK MITRE. *OS Credential Dumping, Technique T1003 - Enterprise | MITRE ATT&CK®*. 8. März 2022. URL: https://attack.mitre.org/techniques/T1003/ (besucht am 08. 12. 2022).

[MIT22r] ATT&CK MITRE. *Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®*. 4. Jan. 2022. URL: https://attack.mitre.org/techniques/T1566/ (besucht am 08. 12. 2022).

[MIT22s] ATT&CK MITRE. *Remote Services, Technique T1021 - Enterprise | MITRE ATT&CK®*. 28. März 2022. URL: https://attack.mitre.org/techniques/T1021/ (besucht am 08. 12. 2022).

[MIT22t] ATT&CK MITRE. *Remote System Discovery, Technique T1018 - Enterprise | MITRE ATT&CK®*. 6. Sep. 2022. URL: https://attack.mitre.org/techniques/T1018/ (besucht am 08. 12. 2022).

[MIT22u] ATT&CK MITRE. *Transfer Data to Cloud Account, Technique T1537 - Enterprise | MITRE ATT&CK®*. 16. Juni 2022. URL: https://attack.mitre.org/techniques/T1537/ (besucht am 08. 12. 2022).

[MIT22v] ATT&CK MITRE. *Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®*. 19. Okt. 2022. URL: https://attack.mitre.org/techniques/T1078/ (besucht am 08. 12. 2022).

[MMB18] Shagufta Mehnaz, Anand Mudgerikar und Elisa Bertino. „RWGuard: A Real-Time Detection System Against Cryptographic Ransomware: 21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12, 2018, Proceedings“. In: 7. Sep. 2018, S. 114–136. ISBN: 978-3-030-00469-9. DOI: 10.1007/978-3-030-00470-5_6.

[Mod19] Jaimin Modi u. a. „Detecting Ransomware in Encrypted Web Traffic“. In: *Foundations and Practice of Security: 12th International Symposium, FPS 2019, Toulouse, France, November 5–7, 2019, Revised Selected Papers*. Berlin, Heidelberg: Springer-Verlag, 5. Nov. 2019, S. 345–353. ISBN: 978-3-030-45370-1. DOI: 10.1007/978-3-030-45371-8_22. URL: https://doi.org/10.1007/978-3-030-45371-8_22 (besucht am 29. 12. 2022).

[Moo16] Chris Moore. „Detecting Ransomware with Honeypot Techniques“. In: 1. Aug. 2016, S. 77–81. DOI: 10.1109/CCC.2016.14.

[Mor18] Daniel Morato u. a. „Ransomware Early Detection by the Analysis of File Sharing Traffic“. In: *Journal of Network and Computer Applications* 124 (15. Dez. 2018), S. 14–32. ISSN: 1084-8045. DOI: 10.1016/j.jnca.2018.09.013. URL: https://www.sciencedirect.com/science/article/pii/S108480451830300X (besucht am 29. 12. 2022).

[Mou17] Guennadi Moukine. *Acronis World Backup Day Survey Results*. Acronis. 29. März 2017. URL: https://www.acronis.com/en-us/blog/posts/acronis-world-backup-day-survey-results/ (besucht am 15. 06. 2022).

[MS-19] MS-ISAC. *Security-Primer-EternalBlue.Pdf*. Jan. 2019. URL: https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf (besucht am 12. 10. 2022).

[MST20] Microsoft Threat Intelligence Center MSTIC. *Human-Operated Ransomware Attacks: A Preventable Disaster*. Microsoft Security Blog. 5. März 2020. URL: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (besucht am 11. 05. 2022).

[MST22] Microsoft Threat Intelligence Center MSTIC. *Ransomware-as-a-Service: Understanding the Cybercrime Gig Economy and How to Protect Yourself*. Microsoft Security Blog. 9. Mai 2022. URL: https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/ (besucht am 11. 05. 2022).

[Nak18] Nakashima. „Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes". In: *Washington Post* (12. Jan. 2018). ISSN: 0190-8286. URL: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html (besucht am 12. 10. 2022).

[Nik16] Nikolai. *Ransomware Brief - Evolution and The Future*. 3583 BYTES FREE, READY? 27. Jan. 2016. URL: https://3583bytesready.net/2016/01/27/ransomware_evolution_introduction/ (besucht am 22. 08. 2022).

[Nik21] Sean Nikkel. *Triple Extortion | 3 Varianten von Ransomware*. 19. Juli 2021. URL: https://www.digitalshadows.com/de/blog-and-research/das-geschaeft-mit-der-erpressung-drei-varianten-von-ransomware/ (besucht am 14. 08. 2022).

[nom22] nomoreransom. *Home*. The No More Ransom Project. 2022. URL: https://www.nomoreransom.org/de/index.html (besucht am 20. 01. 2023).

[NZa] CERT NZ. *How Ransomware Happens and How to Stop It*. CERT NZ. URL: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/ (besucht am 29. 04. 2022).

[NZb] CERT NZ. *Lifecycle of a Ransomware Attack: Consolidation and Preparation | CERT NZ*. URL: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/lifecycle-of-a-ransomware-attack-consolidation-and-preparation/ (besucht am 08. 12. 2022).

[NZc] CERT NZ. *Lifecycle of a Ransomware Attack: Impact on Target*. CERT NZ. URL: https://www.cert.govt.nz/it-specialists/guides/how-rans

omware-happens-and-how-to-stop-it/lifecycle-of-a-ransomware-attack-impact-on-target/ (besucht am 08. 12. 2022).

[NZd] CERT NZ. *Lifecycle of a Ransomware Attack: Initial Access*. CERT NZ. URL: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/initial-access/ (besucht am 06. 12. 2022).

[OBr17] Dick O'Brien. *ISTR Ransomware Special Report*. Juli 2017. URL: https://docs.broadcom.com/doc/istr-ransomware-2017-en (besucht am 16. 06. 2022).

[OSC18] Philip O'Kane, Sakir Sezer und Domhnall Carlin. „Evolution of Ransomware". In: *IET Networks* 7.5 (2018), S. 321–327. ISSN: 2047-4962. DOI: 10.1049/iet-net.2017.0207. URL: https://onlinelibrary.wiley.com/doi/abs/10.1049/iet-net.2017.0207 (besucht am 15. 05. 2022).

[Oxf22] OxfordDictionary. *Phishing Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.Com*. 2022. URL: https://www.oxfordlearnersdictionaries.com/definition/english/phishing (besucht am 02. 08. 2022).

[Oz22] Harun Oz u. a. „A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions". In: *ACM Computing Surveys* (18. Feb. 2022), S. 3514229. ISSN: 0360-0300, 1557-7341. DOI: 10.1145/3514229. arXiv: 2102.06249 [cs]. URL: http://arxiv.org/abs/2102.06249 (besucht am 18. 05. 2022).

[Pal18] Palo Alto Networks Ignite, director. *Ignite USA '18 Keynote - Nir Zuk (Featuring Keren Elazari)*. 4. Juni 2018. URL: https://www.youtube.com/watch?v=c71uPTimW_A (besucht am 03. 01. 2023).

[Pik16] Sarah Pike. *Cerber ist mehr als nur eine gewöhnliche Ransomware*. 27. Mai 2016. URL: https://www.kaspersky.de/blog/cerber-multipurpose-malware/7851/ (besucht am 11. 10. 2022).

[Poh19] Norbert Pohlmann. *Cyber-Sicherheit*. 2019. ISBN: 978-3-658-36243-0. URL: https://link.springer.com/book/10.1007/978-3-658-36243-0 (besucht am 26. 07. 2022).

[r117] rain-1. *Wannacrypt0r-FACTSHEET.Md*. Gist. 23. Mai 2017. URL: https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168 (besucht am 12. 10. 2022).

[Reu17] Reuters. *Shadow Brokers Threaten to Release Windows 10 Hacking Tools*. The Express Tribune. 31. Mai 2017. URL: https://tribune.com.pk/story/1423609/shadow-brokers-threaten-release-windows-10-hacking-tools (besucht am 12. 10. 2022).

[Sal18] Saeid Salehi u. a. „A Novel Approach for Detecting DGA-based Ransomwares". In: *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*. 2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC). Aug. 2018, S. 1–7. DOI: 10.1109/ISCISC.2018.8546941.

[Sar16] Sarah. *Die erste Ransomware in JavaScript: Ransom32*. Emsisoft | Sicherheitsblog. 1. Jan. 2016. URL: https://blog.emsisoft.com/de/21077/meet-ransom32-the-first-javascript-ransomware/ (besucht am 10. 10. 2022).

[Sca16] Nolen Scaife u. a. „CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data". In: *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS). Juni 2016, S. 303–312. DOI: 10.1109/ICDCS.2016.46.

[Sch18] Fabian Scherschel. *EternalBlue: Hunderttausende Rechner über alte NSA-Schwachstelle infizierbar*. Security. 19. Sep. 2018. URL: https://www.heise.de/security/meldung/EternalBlue-Hunderttausende-Rechner-ueber-alte-NSA-Schwachstelle-infizierbar-4167918.html (besucht am 12. 10. 2022).

[SCL15] Kevin Savage, Peter Coogan und Hon Lau. „The Evolution of Ransomware". In: (6. Aug. 2015), S. 57.

[Sec22] Ultimate IT Security. *Windows Security Log Event ID 4688 - A New Process Has Been Created*. 2022. URL: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4688 (besucht am 13. 01. 2023).

[SK22] Tatyana Shishkova und Anton Kivva. *Mobile Malware Evolution 2021*. 21. Feb. 2022. URL: https://securelist.com/mobile-malware-evolution-2021/105876/ (besucht am 05. 07. 2022).

[SL03] P.K. Singh und A. Lakhotia. „Static Verification of Worm and Virus Behavior in Binary Executables Using Model Checking“. In: *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.* IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003. Juni 2003, S. 298–300. DOI: 10.1109/SMCSIA.2003.1232440.

[Sno16a] John Snow. *Petya arbeitet jetzt mit Ransomware Mischa zusammen.* 18. Mai 2016. URL: https://www.kaspersky.de/blog/mischa-ransomware/7703/ (besucht am 11. 10. 2022).

[Sno16b] John Snow. *Ransomware Petya verschlüsselt Festplatten.* 30. März 2016. URL: https://www.kaspersky.de/blog/petya-ransomware/7375/ (besucht am 11. 10. 2022).

[SOC22] SOCRadar. *Lockbit 3.0: Another Upgrade to World's Most Active Ransomware.* SOCRadar® Cyber Intelligence Inc. 6. Apr. 2022. URL: https://socradar.io/lockbit-3-another-upgrade-to-worlds-most-active-ransomware/ (besucht am 16. 10. 2022).

[Son22] SonicWall. *Number of Ransomware Attacks per Year 2022.* Statista. Juni 2022. URL: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ (besucht am 06. 10. 2022).

[SOP] SOPHOS. *Ransomware-Report 2021.* SOPHOS. URL: https://www.sophos.com/de-de/content/state-of-ransomware (besucht am 29. 04. 2022).

[SOP20] SOPHOS. *Ransomware: How an Attack Works.* 13. Mai 2020. URL: https://support.sophos.com/support/s/article/KB-000036277?language=en_US (besucht am 06. 08. 2022).

[SOP22] SOPHOS. *DEADBOLT Ransomware Rears Its Head Again, Attacks QNAP Devices.* Naked Security. 7. Sep. 2022. URL: https://nakedsecurity.sophos.com/2022/09/07/deadbolt-ransomware-rears-its-head-again-attacks-qnap-devices/ (besucht am 22. 01. 2023).

[Spi03] D. Spinellis. „Reliable Identification of Bounded-Length Viruses Is NP-complete“. In: *IEEE Transactions on Information Theory* 49.1 (Jan. 2003), S. 280–284. ISSN: 1557-9654. DOI: 10.1109/TIT.2002.806137.

[Spl22] Splunk. *Was ist ein SIEM?* Splunk. 1. Aug. 2022. URL: https://www.splunk.com/de_de/data-insider/what-is-siem.html (besucht am 02. 01. 2023).

[SR17] Stanislav Skuratovich und Neomi Rona. *Virus Bulletin :: VB2017 Paper: Nine Circles of Cerber*. 2017. URL: https://www.virusbulletin.com/virusbulletin/2017/12/vb2017-paper-nine-circles-cerber/ (besucht am 11. 10. 2022).

[sta21a] statcounter. *Mobile Operating System Market Share Worldwide*. StatCounter Global Stats. 2021. URL: https://gs.statcounter.com/os-market-share/mobile/worldwide/ (besucht am 04. 07. 2022).

[sta21b] statista. *Desktop OS Market Share*. Statista. 2021. URL: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/ (besucht am 22. 06. 2022).

[sta22a] statcounter. *Desktop Operating System Market Share Worldwide*. StatCounter Global Stats. 2022. URL: https://gs.statcounter.com/os-market-share/desktop/worldwide/ (besucht am 17. 01. 2023).

[sta22b] statcounter. *Desktop vs Mobile Market Share Worldwide*. StatCounter Global Stats. 2022. URL: https://gs.statcounter.com/platform-market-share/desktop-mobile/worldwide/#yearly-2009-2022 (besucht am 22. 06. 2022).

[sta22c] statista. *Number of Internet Users 2021*. Statista. 2022. URL: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ (besucht am 22. 08. 2022).

[stra] strontic. *Bcrypt.Dll | Windows Cryptographic Primitives Library*. STRONTIC. URL: https://strontic.github.io/xcyclopedia/library/bcrypt.dll-001E4599898EF88078E0AA8A5F0EC1A1.html (besucht am 19. 01. 2023).

[strb] strontic. *Psapi.Dll | Process Status Helper*. STRONTIC. URL: https://strontic.github.io/xcyclopedia/library/psapi.dll-39FDC69FB223A2CE7ECD1BEACDB46B6A.html (besucht am 19. 01. 2023).

[Str21] Stefan Strobel u. a. „Auf dem Radar: Endpoint Detection and Response: Gefahren schnell erkennen und reagieren“. In: *iX* 2021.11 (20. Okt. 2021), S. 52–67. ISSN: 0935-9680. URL: https://www.heise.de/select/ix/2021/11/2124214395927300312 (besucht am 23. 12. 2022).

[Sul13] Nick Sullivan. *A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography*. The Cloudflare Blog. 24. Okt. 2013. URL: http://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/ (besucht am 05. 10. 2022).

[Swi21] Swiss Cyber Institute. *5 Biggest Ransomware Attacks in History*. 27. Sep. 2021. URL: https://swisscyberinstitute.com/blog/5-biggest-ransomware-attacks-in-history/ (besucht am 12. 10. 2022).

[SY18] Shina Sheen und Ashwitha Yadav. „Ransomware Detection by Mining API Call Usage“. In: *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). Sep. 2018, S. 983–987. DOI: 10.1109/ICACCI.2018.8554938.

[SZ21] Dmitry Shestakov und Andrey Zhdanov. *Inside the Hive*. Group-IB. 9. Dez. 2021. URL: https://blog.group-ib.com/hive (besucht am 22. 10. 2022).

[Tea22] Microsoft 365 Defender Threat Intelligence Team. *Ransomware as a Service: Understanding the Cybercrime Gig Economy and How to Protect Yourself*. Microsoft Security Blog. 9. Mai 2022. URL: https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/ (besucht am 16. 10. 2022).

[The21] Inc The Radicati Group. *Mobile Statistics Report, 2021-2025 Executive Summary*. Jan. 2021. URL: https://www.radicati.com/wp/wp-content/uploads/2021/Mobile_Statistics_Report,_2021-2025_Executive_Summary.pdf (besucht am 04. 07. 2022).

[TRJ21] William Turton, Michael Riley und Jennfier Jacobs. *Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom - Bloomberg*. 13. Mai 2021. URL: https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom#xj4y7vzkg (besucht am 06. 06. 2022).

[TW15] Biaoshuai Tao und Hongjun Wu. „Improving the Biclique Cryptanalysis of AES“. In: *Information Security and Privacy*. Hrsg. von Ernest Foo und Douglas Stebila. Lecture Notes in Computer Science. Cham: Springer International

Publishing, 2015, S. 39–56. ISBN: 978-3-319-19962-7. DOI: 10.1007/978-3-319-19962-7_3.

[UIM23] UIM-SEC. *Ransomware Samples*. UIM-SEC, 3. Jan. 2023. URL: https://github.com/UIM-SEC/ransomware-samples (besucht am 09. 01. 2023).

[uni22] unit42. *2022 Unit 42 Ransomware Threat Report*. Palo Alto Networks. 24. März 2022. URL: https://www.paloaltonetworks.com/resources/research/2022-unit-42-ransomware-threat-report (besucht am 16. 10. 2022).

[Wal22] Jim Walter. *BlueSky Ransomware | AD Lateral Movement, Evasion and Fast Encryption Put Threat on the Radar*. SentinelOne. 25. Aug. 2022. URL: https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/ (besucht am 10. 10. 2022).

[Wan21] Liu Wang u. a. *Beyond the Virus: A First Look at Coronavirus-themed Mobile Malware*. 18. Apr. 2021. DOI: 10.48550/arXiv.2005.14619. arXiv: 2005.14619 [cs]. URL: http://arxiv.org/abs/2005.14619 (besucht am 08. 08. 2022).

[Wec16] Mattias Weckstén u. a. „A Novel Method for Recovery from Crypto Ransomware Infections“. In: *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*. 2016 2nd IEEE International Conference on Computer and Communications (ICCC). Okt. 2016, S. 1354–1358. DOI: 10.1109/CompComm.2016.7924925.

[Wei22] Paul Weissmann. *EU-Regulierung für Cyber Security in Kritischen Infrastrukturen*. 2022. URL: https://www.openkritis.de/it-sicherheitsgesetz/eu-kritis-europa.html (besucht am 03. 12. 2022).

[Wil90] Edward Wilding. „Virus Bulletin, January 1990“. In: (1990), S. 20.

[WN05] Amrit T. Williams und Mark Nicolett. *Improve IT Security With Vulnerability Management*. Gartner. Mai 2005. URL: https://www.gartner.com/en/documents/480703 (besucht am 03. 01. 2023).

[Wue20] Candid Wuest. *Digital CoronaVirus: Yet Another Ransomware Combined with Infostealer*. Acronis. 28. Apr. 2020. URL: https://www.acronis.com/en-us/blog/posts/digital-coronavirus-yet-another-ransomware-combined-infostealer/ (besucht am 14. 10. 2022).

[WW21] Eric Waltert und Elke Witmer-Goßner. *Ransomware bedroht die Cloud*. 11. Nov. 2021. URL: https://www.cloudcomputing-insider.de/ransomware-bedroht-die-cloud-a-1073291/ (besucht am 06. 07. 2022).

[YY96] A. Young und Moti Yung. „Cryptovirology: Extortion-Based Security Threats and Countermeasures“. In: *Proceedings 1996 IEEE Symposium on Security and Privacy*. Proceedings 1996 IEEE Symposium on Security and Privacy. Mai 1996, S. 129–140. DOI: 10.1109/SECPRI.1996.502676.

[zsc21] zscaler. *What Is Double Extortion Ransomware?* Zscaler. 2021. URL: https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware (besucht am 14. 08. 2022).

[ZWS18] Aaron Zimba, Zhaoshun Wang und Luckson Simukonda. „Towards Data Resilience: The Analytical Case of Crypto Ransomware Data Recovery Techniques“. In: *International Journal of Information Technology and Computer Science* 10 (8. Jan. 2018), S. 40–51. DOI: 10.5815/ijitcs.2018.01.05.

[ZZZ05] Zhi-hong Zuo, Qing-xin Zhu und Ming-tian Zhou. „On the Time Complexity of Computer Viruses“. In: *IEEE Transactions on Information Theory* 51.8 (Aug. 2005), S. 2962–2966. ISSN: 1557-9654. DOI: 10.1109/TIT.2005.851780.

Anhang A

A.1 Diagramme

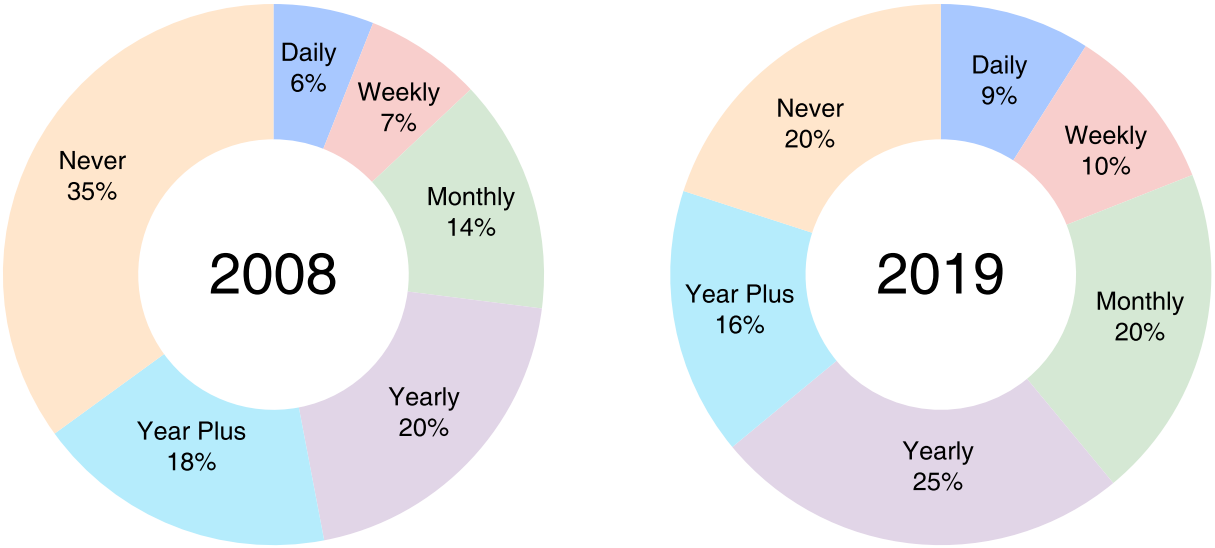
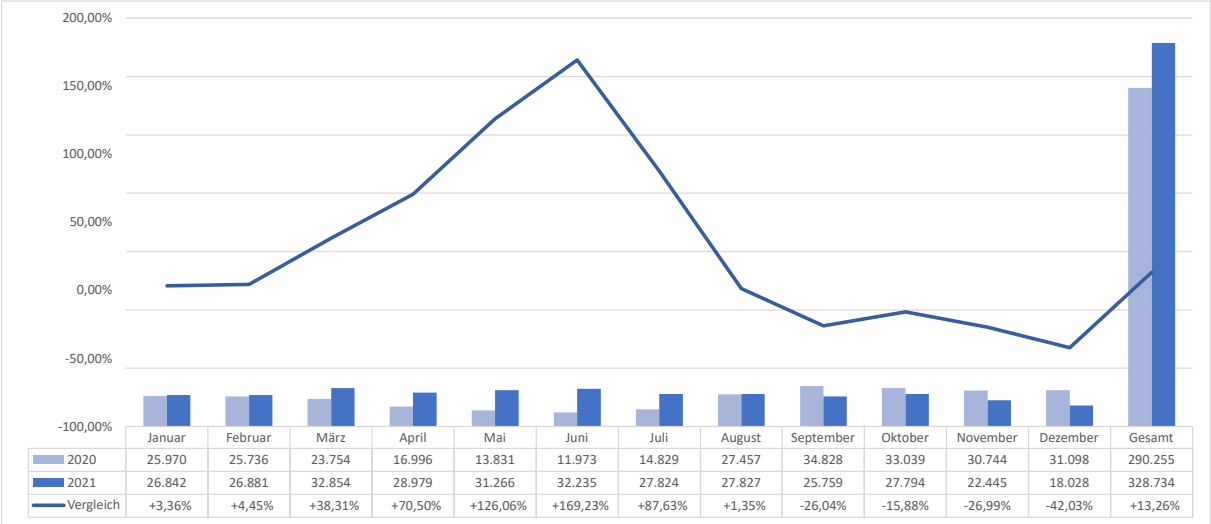


Abbildung A.1: Backup-Frequenzen in den Jahren 2008 und 2019 nach [Bau19]



	Januar	Februar	März	April	Mai	Juni	Juli	August	September	Oktober	November	Dezember	Gesamt
2020	25.970	25.736	23.754	16.996	13.831	11.973	14.829	27.457	34.828	33.039	30.744	31.098	290.255
2021	26.842	26.881	32.854	28.979	31.266	32.235	27.824	27.827	25.759	27.794	22.445	18.028	328.734
Vergleich	+3,36%	+4,45%	+38,31%	+70,50%	+126,06%	+169,23%	+87,63%	+1,35%	-26,04%	-15,88%	-26,99%	-42,03%	+13,26%

Abbildung A.2: Angriffe mit Mobilgeräte-Ransomware in 2020 und 2021 nach [SK22]

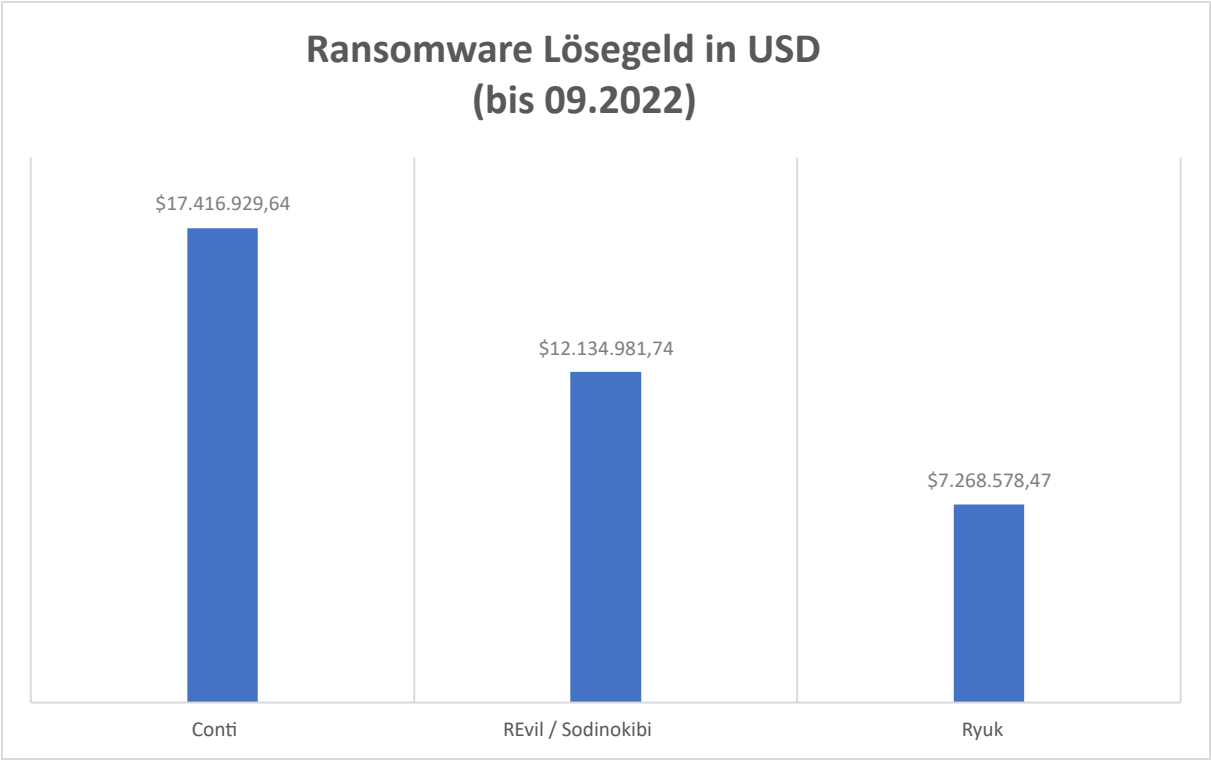


Abbildung A.3: Lösegeld für BGH Ransomware (Stand 09.2022) nach [Cab22]

A.2 Tabellen

Jahr	Name	Verschlüsselung	Opfer	RaaS	Plattform
2008	Randsom.C	Sperrung	Verbraucher		Windows
2008	Seftad	Sperrung	Verbraucher		Windows
2008	Krotten	Asymmetrisch	Verbraucher		Windows
2009	Urausy	Sperrung	Verbraucher		Windows
2010	Winlock	Sperrung	Verbraucher		Windows
2012	Reveton	Sperrung	Verbraucher		Multi
2013	CryptoLocker	Asymmetrisch	Verbraucher		Windows
2013	CryptoWall	Asymmetrisch	Verbraucher		Windows
2013	FakeDefender	Sperrung	Verbraucher		Android
2013	DirtyDecrypt	Symmetrisch	Verbraucher		Windows
2013	AndroidDefender	Sperrung	Verbraucher		Android
2013	Rakhni	Symmetrisch	Verbraucher		Windows
2014	Lockdroid	Sperrung	Verbraucher		Android
2014	SimpleLocker	Symmetrisch	Verbraucher		Android
2014	TorrentLocker	Hybrid	Verbraucher		Windows
2014	TrolDesh	Symmetrisch	Verbraucher		Windows
2014	CryptoDefense	Asymmetrisch	Verbraucher		Windows
2014	FileCoder	Symmetrisch	Verbraucher		Windows
2015	CBTLocker	Asymmetrisch	Organisation		Windows
2015	TeslaCrypt	Symmetrisch	Verbraucher		Windows
2015	Fusob	Sperrung	Verbraucher		Android
2015	Chimera	Symmetrisch	Organisation		Windows
2015	LinuxEncoder	Hybrid	Verbraucher		Linux
2015	HiddenFear	Symmetrisch	Verbraucher		Windows
2015	AlphaCrypt	Asymmetrisch	Organisation		Windows
2016	Ransom32	Symmetrisch	Verbraucher	x	Multi
2016	Dharma	Symmetrisch	Organisation		Windows
2016	Locky	Hybrid	Organisation		Windows
2016	Cerber	Symmetrisch	Verbraucher	x	Windows
2016	Jigsaw	Hybrid	Verbraucher		Windows

2016	KeRanger	Hybrid	Verbraucher		macOS
2016	Petya	Symmetrisch	Organisation	x	Windows
2016	DMALocker	Symmetrisch	Verbraucher		Multi
2016	Mischa	Hybrid	Organisation	x	Windows
2016	Zcryptor	Asymmetrisch	Verbraucher		Windows
2016	Enigma	Symmetrisch	Verbraucher		Windows
2016	Xorist	Symmetrisch	Organisation	x	Windows
2017	Sage	Hybrid	Verbraucher		Windows
2017	BadRabbit	Hybrid	Organisation		Windows
2017	WannaCry	Hybrid	Organisation	x	Windows
2017	GoldenEye	Symmetrisch	Organisation	x	Windows
2017	NotPetya	Symmetrisch	Organisation		Windows
2017	BitPaymer	Hybrid	Organisation		Windows
2017	Atlas	Hybrid	Verbraucher		Windows
2017	Spora	Hybrid	Verbraucher		Windows
2017	LokiBot	Symmetrisch	Verbraucher		Android
2017	RedBoot	Symmetrisch	Verbraucher		Windows
2018	SamSam	Asymmetrisch	Organisation		Windows
2018	GrandCrab	Symmetrisch	Organisation	x	Multi
2018	Katyusha	Hybrid	Verbraucher		Windows
2018	Scarab	Hybrid	Verbraucher		Windows
2019	REvil	Hybrid	Organisation	x	Windows
2019	Robbinhood	Hybrid	Verbraucher		Windows
2019	Maze	Hybrid	Organisation		Multi
2019	Ryuk	Hybrid	Organisation	x	Multi
2019	MegaCortex	Symmetrisch	Organisation	x	Multi
2019	LockerGaga	Hybrid	Organisation	x	Windows
2019	Ekans	Hybrid	Organisation		Linux
2019	Phobos	Hybrid	Organisation		Windows
2019	Netwalker	Symmetrisch	Organisation	x	Windows
2019	MedusaLocker	Hybrid	Organisation		Windows
2019	LockBit 1.0	Hybrid	Organisation	x	Multi

2019	PewCrypt	Hybrid	Verbraucher		Windows
2019	Nemty	Hybrid	Verbraucher		Windows
2019	Mira	Symmetrisch	Verbraucher		Windows
2019	Hackbit	Symmetrisch	Organisation		Windows
2019	SunCrypt	Hybrid	Organisation	x	Windows
2019	Pysa	Asymmetrisch	Organisation		Windows
2019	Clop	Asymmetrisch	Organisation		Windows
2019	Snatch	Hybrid	Organisation	x	Multi
2020	PureLocker	Symmetrisch	Organisation		Multi
2020	Tycoon	Symmetrisch	Organisation		Windows
2020	CovidLock	Sperrung	Verbraucher		Android
2020	Corona	Hybrid	Organisation		Windows
2020	Conti	Hybrid	Organisation	x	Multi
2020	DarkSide	Hybrid	Organisation	x	Multi
2020	WastedLocker	Hybrid	Organisation	x	Windows
2020	Hades	Hybrid	Organisation	x	Windows
2020	DoppelPaymer	Hybrid	Organisation	x	Windows
2020	Nefilim	Hybrid	Organisation		Windows
2020	Makop Ransomware	Hybrid	Organisation		Windows
2020	PonyFinal	Asymmetrisch	Verbraucher		Windows
2020	MountLocker	Hybrid	Organisation	x	Windows
2020	Exorcist	Hybrid	Verbraucher		Windows
2020	HelloKitty	Hybrid	Organisation		Multi
2020	Avaddon	Hybrid	Organisation		Windows
2020	Corona-Lock	Hybrid	Verbraucher		Windows
2021	BlackCat	Hybrid	Organisation	x	Multi
2021	LockBit 2.0	Hybrid	Organisation	x	Multi
2021	Phoenix Locker	Hybrid	Organisation	x	Windows
2021	PayloadBIN	Hybrid	Organisation	x	Windows
2021	Babuk	Hybrid	Organisation		Multi
2021	Cring	Hybrid	Organisation		Windows
2021	Hive	Asymmetrisch	Organisation	x	Multi

2022	Deadbolt	Symmetrisch	Verbraucher		Linux
2022	BlueSky	Symmetrisch	Organisation	x	Windows
2022	LockBit 3.0	Hybrid	Organisation	x	Multi
2022	Cheerscrypt	Hybrid	Organisation		Linux
2022	Black Basta	Hybrid	Organisation	x	Multi
2022	Lillith	Asymmetrisch	Organisation		Windows
2022	Moisha	Hybrid	Verbraucher		Windows

Tabelle A.1: Zusammenfassung verschiedener Ransomware-Familien von 2008 bis 2022

Jahr	**Anz.**	**Verschlüsselung**				**Opfer**		**RaaS**	**RaaS%**	**Plattform**				
		Sym.	**Asym.**	**Hybrid**	**Sperr.**	**Verbr.**	**Org.**			**Windows**	**macOS**	**Linux**	**Android**	**Multi**
2008	3	0	1	0	2	3	0	0	0,00%	3	0	0	0	0
2009	1	0	0	0	1	1	0	0	0,00%	1	0	0	0	0
2010	1	0	0	0	1	1	0	0	0,00%	1	0	0	0	0
2011	0	0	0	0	0	0	0	0	0,00%	0	0	0	0	0
2012	1	0	0	0	1	1	0	0	0,00%	0	0	0	0	1
2013	6	2	2	0	2	6	0	0	0,00%	4	0	0	2	0
2014	6	3	1	1	1	6	0	0	0,00%	4	0	0	2	0
2015	7	3	2	1	1	4	3	0	0,00%	5	0	1	1	0
2016	12	7	1	4	0	7	5	5	41,67%	9	1	0	0	2
2017	10	4	0	6	0	5	5	2	20,00%	9	0	0	1	0
2018	4	1	1	2	0	2	2	1	25,00%	3	0	0	0	1
2019	19	4	2	13	0	4	15	8	42,11%	13	0	1	0	5
2020	17	2	1	13	1	4	13	6	35,29%	12	0	0	1	4
2021	7	0	1	6	0	0	7	5	71,43%	3	0	0	0	4
2022	7	2	1	4	0	2	5	3	42,86%	3	0	2	0	2
Gesamt	101	28	13	50	10	46	55	30	-	70	1	4	7	19
Mittelwert	6,73	1,87	0,87	3,33	0,67	3,07	3,67	2,00	18,56%	4,67	0,07	0,27	0,47	1,27
Prozent	100%	27,72%	12,87%	49,50%	9,90%	45,54%	54,46%	29,70%	-	69,31%	0,99%	3,96%	6,93%	18,81%

Tabelle A.2: Auswertung von Tab. A.1

ATT&CK Technik	**Kurzbeschreibung**
T1133 External Remote Services [MIT22l]	Angreifer verwenden externe Schnittstellen (z.B. VPN, RDP), die Zugang zu einem internen Netzwerk ermöglichen.
T1078 Valid Accounts [MIT22v]	Angreifer verwenden Zugangsdaten von bereits bestehenden Konten, um Zugangskontrollen zum und im Zielnetzwerk zu umgehen.
T1110 Brute Force [MIT22c]	Angreifer nutzen Brute-Force-Methoden, um Passwörter zu bestehenden Konten (Valid Accounts) zu erhalten.
T1190 Exploit Public-Facing Application [MIT22j]	Angreifer versuchen Schwachstellen von dem Internet zugänglichen Geräten oder Programmen auszunutzen, um Zugriff zu erhalten. Häufige Ziele sind dabei Webseiten, Datenbanken, Standarddienste (SMB, SSH) und Verwaltungsprotokolle (SNMP).
T1566 Phishing [MIT22r]	Angreifer nutzen Social-Engineering-Methoden, um Opfer dazu zu verleiten freiwillig ihre Zugangsdaten preiszugeben oder getarnte Malware zu installieren.

Tabelle A.3: MITRE ATT&CK Techniken für die Initial Access-Phase nach [NZd]

ATT&CK Technik	**Kurzbeschreibung**
T1573 Encrypted Channel [MIT21b]	Angreifer versuchen den durch C2 generierten Internet-Traffic mithilfe von verschlüsselten Kommunikationskanälen zu verstecken.
T1078 Account Discovery [MIT21a]	Angreifer versuchen eine Auflistung der Accounts eines Systems oder Netzwerks zu erhalten.
T1018 Remote System Discovery [MIT22t]	Angreifer versuchen ein Auflistung von anderen Systemen (IP-Adresse, Hostname, etc.) zu erhalten.
T1046 Network Service Scanning [MIT22p]	Angreifer versuchen eine Auflistung von auf anderen Systemen laufenden Services zu erhalten, die Schwachstellen für weitere Angriffe bieten.
T1582 Domain Trust Discovery [MIT22h]	Angreifer suchen nach Vertrauensbeziehungen zwischen (Windows-)Domänen.
T1069 Permission Groups Discovery [MIT21c]	Angreifer suchen nach Gruppen und Berechtigungseinstellungen.
T1003 OS Credential dumping [MIT22q]	Angreifer versuchen Anmeldedaten aus dem Betriebssystem und Software herauszulösen (dumpen). Das Ergebnis sind zumeist Klartext oder Hashes von Passwörtern.
T1068 Exploitation for Privilege Escalation [MIT22k]	Angreifer versuchen Schwachstellen in der Software auszunutzen, um ihre Rechte zu erhöhen.
T1078 Valid Accounts [MIT22v]	Angreifer verwenden Zugangsdaten von bereits bestehenden Konten, um Zugangskontrollen zum und im Zielnetzwerk zu umgehen.
T1021 Remote Services [MIT22s]	Angreifer versuchen sich mithilfe von Valid Accounts bei Services anzumelden, die für den Remotezugriff auf Systeme genutzt werden (z.B. SSH, telnet, VNC).
T1570 Lateral Tool Transfer [MIT22n]	Angreifer übertragen Tools und andere Dateien (z.B. Malwaremodule, Payloads, etc.) zwischen Systemen in der kompromittierten Umgebung.

Tabelle A.4: MITRE ATT&CK Techniken für die Consolidation and Preparation-Phase nach [NZb]

Werkzeug nach ATT&CK	**Kurzbeschreibung**
S0154 CobaltStrike [MIT22d]	CobaltStrike ist eine Anwendung für die Simulation von Cyberangriffen und Pentesting. Sie wird auch oft von bösartigen Akteuren verwendet, um echte Angriffe durchzuführen.
S0002 mimikatz [MIT22o]	Mimikatz ist ein Credential Dumper, der u.a. Windows-Anmeldedaten als Klartext auslesen kann.
S0521 BloodHound [MIT22b]	BloodHound ist ein Werkzeug zum Finden von versteckten Beziehungen und Angriffswegen in Active Directory Umgebungen.

Tabelle A.5: Werkzeuge nach ATT&CK-Kennung für die Consolidation and Preparation-Phase nach [NZb]

ATT&CK Technik	**Kurzbeschreibung**
T1005 Data from Local System [MIT22f]	Angreifer durchsuchen lokale Systeme (z.B. Dateisysteme, Konfigurationsdateien, Datenbanken, etc.) nach nützlichen oder sensiblen Informationen.
T1039 Data from Network Shared Drive [MIT22g]	Angreifer durchsuchen freigegebene Netzwerklaufwerke, auf kompromittierten Geräten, nach nützlichen oder sensiblen Informationen.
T1560 Archive Collected Data [MIT22a]	Angreifer komprimieren und/oder verschlüsseln gesammelte Daten vor der Exfiltration, um die Entdeckungschancen der Exfiltration zu minimieren.
T1567 Exfiltration over Web Service [MIT22i]	Angreifer verwenden legitime Webdienste, anstelle ihres C2-Kanals, um Daten zu exfiltrieren.
T1537 Transfer Data to Cloud Account [MIT22u]	Angreifer exfiltrieren Daten zu einem anderen Account des gleichen Cloud-Dienstes, um typische Dateiübertragungen/Downloads und netzwerkbasierte Exfiltrationserkennung zu umgehen.
T1490 Inhibit System Recovery [MIT22m]	Angreifer löschen Betriebssystemdaten oder deaktivieren Dienste, die bei der Wiederherstellung von beschädigten Systemen verwendet werden, um die Wiederherstellung zu erschweren oder ganz zu verhindern.
T1486 Encrypt Data for Impact [MIT22e]	Angreifer verschlüsseln Daten, um deren Verfügbarkeit zu unterbrechen. Dies geschieht entweder um Lösegeld zur Wiederherstellung der Verfügbarkeit zu erpressen, oder Daten dauerhaft unzugänglich zu machen.

Tabelle A.6: MITRE ATT&CK Techniken für die Impact on Target-Phase nach [NZc]

Registry
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/UNCAsIntranet
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/IntranetName
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/AutoDetect
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/ProxyBypass
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/5.0/Cache/Cookies/CachePrefix
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/5.0/Cache/History/CachePrefix
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/5.0/Cache/Content/CachePrefix
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.html/OpenWithProgids/htmlfile
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/crypto13
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/Control Panel/Desktop/TileWallpaper
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/Control Panel/Desktop/WallpaperStyle

Tabelle A.7: Registry-Änderungen von TeslaCrypt

Registry
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/54k
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/aOwO
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/hq0G6X
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/Krdfp
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/x4WHjRs
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/XFx41h1r
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/UNCAsIntranet
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/IntranetName
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/AutoDetect
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/ProxyBypass
HKLM/SOFTWARE/WOW6432Node/BlackLivesMatter/aOwO
HKLM/SOFTWARE/WOW6432Node/BlackLivesMatter/Krdfp
HKLM/SOFTWARE/WOW6432Node/BlackLivesMatter/54k
HKLM/SOFTWARE/WOW6432Node/BlackLivesMatter/hq0G6X
HKLM/SOFTWARE/WOW6432Node/BlackLivesMatter/x4WHjRs
HKLM/SOFTWARE/WOW6432Node/BlackLivesMatter/XFx41h1r
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/CLSID/{645FF040-5081-101B-9F08-00AA002F954E}/DefaultIcon/
HKLM/SYSTEM/ControlSet001/Control/Session Manager/PendingFileRenameOperations

Tabelle A.8: Registry-Änderungen von REvil auf CL-01

Registry
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/54k
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/aOwO
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/hq0G6X
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/Krdfp
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/x4WHjRs
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/VirtualStore/MACHINE/SOFTWARE/WOW6432Node/BlackLivesMatter/XFx41h1r

Tabelle A.9: Registry-Änderungen von REvil auf CL-02

Registry
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/UNCAsIntranet
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/IntranetName
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/AutoDetect
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/ProxyBypass
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/XO1XADpO01
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/LockBit/full
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/LockBit/Public
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/BitBucket/Volume/{ddecd258-eea6-4dcc-bf38-a16da221a66d}/MaxCapacity
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/BitBucket/Volume/{ddecd258-eea6-4dcc-bf38-a16da221a66d}/NukeOnDelete
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/BitBucket/Volume/{6444f976-8135-4e0b-be7b-40c624f19008}/MaxCapacity
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/BitBucket/Volume/{6444f976-8135-4e0b-be7b-40c624f19008}/NukeOnDelete
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/CLSID/{645FF040-5081-101B-9F08-00AA002F954E}/DefaultIcon/

Tabelle A.10: Registry-Änderungen von Lockbit

Registry
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/DE2B238178ACBC7EE17705487DA2E8ED/ RECOVERY-BLOB
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/DE2B238178ACBC7EE17705487DA2E8ED/x25519_public
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/DE2B238178ACBC7EE17705487DA2E8ED/ completed
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ SlowContextMenuEntries
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/ProxyBypass
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/IntranetName
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/UNCAsIntranet
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/AutoDetect

Tabelle A.11: Registry-Änderungen von BlueSky auf CL-01

Registry
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/Software/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/AutoDetect
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/Software/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/UNCAsIntranet
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106_Classes/Local Settings/MuiCache/3/52C64B7E/LanguageList
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/Software/BBDBC225E21436DABA0A33A981AA592E/RECOVERYBLOB
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/Software/BBDBC225E21436DABA0A33A981AA592E/x25519_public
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/Software/BBDBC225E21436DABA0A33A981AA592E/completed

Tabelle A.12: Registry-Änderungen von BlueSky auf AD-SV01

Registry
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0000/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0000/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0000/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0000/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0000/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0001/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0001/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0001/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0001/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0002/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0002/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0002/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0002/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0002/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0003/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0003/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0003/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0003/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0003/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0004/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0004/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0004/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0004/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0004/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0005/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0005/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0005/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0005/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0005/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0006/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0006/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0006/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0006/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0006/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0007/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0007/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0007/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0007/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0007/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0008/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0008/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0008/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0008/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0008/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0009/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0009/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0009/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0009/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0009/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0010/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0010/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0010/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0010/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0010/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0011/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0011/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0011/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0011/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0011/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0012/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0012/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0012/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0012/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0012/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0012/SessionHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0013/Owner
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0013/RegFiles0000
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0013/RegFilesHash
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0013/Sequence
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/RestartManager/Session0013/SessionHash

Tabelle A.13: Registry-Änderungen von Lilith

Registry
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/AutoDetect
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/UNCAsIntranet
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/IntranetName
HKEY_USERS/S-1-5-21-2455417735-1121996341-945197012-1106/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap/ProxyBypass

Tabelle A.14: Registry-Änderungen von Moisha

A.3 Codeauszüge

Codeauszug A.1: Python-Script zum Generieren von Testdateien

```
1  import os
2  import random
3  import words
4  from pathlib import Path
5
6  def createFile(name, size):
7      with open(name, 'wb') as fout:
8          fout.write(os.urandom(size))
9      fout.close()
10
11 def createFilename():
12     ext = [".pdf", ".txt", ".png", ".jpg", ".xlsx", ".docx", ".exe"]
13     rin = random.randint(0, len(words.nouns)-1)
14     ria = random.randint(0, len(words.adj)-1)
15     riv = random.randint(0, len(words.verbs)-1)
16     rie = random.randint(0,len(ext)-1)
17
18     fname = words.verbs[riv].capitalize() + words.adj[ria].capitalize() + ↩
           words.nouns[rin].capitalize() + ext[rie]
19     return fname
20
21 abspath = os.path.abspath(__file__)
22 dname = os.path.dirname(abspath)+"/out"
23 Path(dname).mkdir(exist_ok=True)
```

```
24 os.chdir(dname)
25
26 # 1-50 MB
27 for i in range(1,25):
28     createFile(createFilename(),random.randint(1,50)*1024*1024)
29 # 1 GB
30 for i in range(1,3):
31     createFile(createFilename(),1024*1024*1024)
```

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die Prüfungsaufgaben selbstständig und ohne jede unerlaubte Hilfe bearbeitet habe und keine anderen als die erlaubten Hilfsmittel benutzt sowie eigene Textbausteine keiner anderen Person zur Verfügung gestellt habe.
Ich willige ein, dass meine Antworten mittels einer Plagiatssoftware überprüft werden können und dass zu diesem Zweck elektronische Kopien (in anonymisierter Form) gefertigt und gespeichert werden können.
Mir ist bekannt, dass ein Plagiat gemäß §11 Abs. 3 der Rahmenordnung (RO-THB 2021, RO-THB 2018 und RO-FHB 2015) geahndet wird und eine Bewertung der Prüfungsleistung mit der Note 5,0 (nicht ausreichend) nach sich zieht.

Brandenburg an der Havel, den 28.01.2023

Bjarne Jungclaus
Matrikel-Nummer: 20151304