HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

BACHELORARBEIT

Herr
Kim Rikard Nordqvist

Erstellung von Erkennungs-mustern für Ransomware-gruppen mithilfe von Threat Intelligence

Mittweida, 2023

Fakultät Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Erstellung von Erkennungsmustern für Ransomwaregruppen mithilfe von Threat Intelligence

Autor:
Herr

Kim Rikard Nordqvist

Studiengang:
IT-Sicherheit

Seminargruppe:
IF19wl2-B

Erstprüfer:
Herr Prof. Dr.-Ing. Christian Roschke

Zweitprüfer:
Herr M. Sc. Bruno Oliveira

Einreichung:
Würzburg, 05.02.2023

Verteidigung/Bewertung:
Würzburg, 2023

Faculty Angewandte Computer- und Biowissenschaften

BACHELOR THESIS

Creation of detectionrules for ransomware groups with help of Threat Intelligence

author:
Mr. Kim Rikard Nordqvist

course of studies:
IT-Security

seminar group:
IF19wl2-B

first examiner:
Mr. Prof. Dr.-Ing. Christian Roschke

second examiner:
Mr. M. Sc. Bruno Oliveira

submission:
Würzburg, 05.02.2023

defence/ evaluation:
Würzburg, 2023

Bibliografische Beschreibung:

Nordqvist, Kim Rikard:
Erstellung von Erkennungsmustern für Ransomwaregruppen mithilfe von Threat Intelligence. - 2023 – Inhalt: 57 Seiten, Anhänge: 20 Seiten
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2023

Referat:

Diese Bachelorarbeit befasst sich mit der Frage wie man sich gegen die zurzeit aktiven Ransomware-Gruppen schützen kann. Dabei wird das Ziel gesetzt, den Nutzen von IT-Sicherheit zu verdeutlichen sowie Erkennungsregeln für unterschiedliche Taktiken und Techniken zu erstellen. Um dies zu erreichen werden, wird mit Threat Intelligence und der Methodik des Intelligence Cycles, öffentlich zugängliche Informationen zu den bereits angegriffenen Unternehmen, dessen Standorten und Branche gesammelt und ausgewertet. Für die Beschaffung der Daten wird das Webscraping mittels Python und Selenium sowie vorhandene Open Source Projekte, die bereits von Ransomware-Gruppen überwachen, genutzt. Durch die vorhandenen Informationen ist es möglich für eine gewählte geografische Lokation die aktivsten Gruppen zu bestimmen, was jedoch nicht für alle Unternehmen gelingt. Als Umfang wurde sich hier auf Europa konzentriert. Es werden die aktivsten Gruppen priorisiert und basierend auf deren vergangenen angriffen genauer betrachtet und verglichen. Es wird sich auf die Techniken und Taktiken konzentriert, welche von mehreren Gruppen genutzt werden. So ist es möglich die Erkennungsregeln so zu erstellen, dass die Angriffe der Gruppen mit wenigen Regeln erkannt werden können.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
C2 / C&C	Command and Control
DNS	Domain Name System
EDR	Endpoint Detection and Response
HTTP(S)	Hypertext Transfer Protocol (Secure)
IOC	Indicator of Compromise
KRITIS	Kritische Infrastruktur
OSINT	Open Source Intelligence
RaaS	Ransomware-as-a-Service
RAT	Remote Access Tool
SIEM	Security Information and Event Management
SOC	Security Operations Center
TCP	Transmission Control Protocol
TTP	Tactics, Techniques and Procedures
UNBÖFI	Unternehmen von besonderem öffentlichem Interesse
WEC	Windows Event Collector
WEF	Windows Event Forwarding
XDR	Extended Detection and Response

1 Einführung und Motivation

In der heutigen Zeit werden IT-Systeme in unserer Gesellschaft immer relevanter [Soni22, S. 1]. Dazu gehören nicht nur die Geräte, welche privat genutzt werden. Sie werden in allen Bereichen der Welt genutzt, ob in Krankenhäusern, in der Fertigung oder beim lokalen Bäcker. Dabei sind Unternehmen dauerhaft von Cyberangriffen betroffen [Soni22, S. 1], welche dazu führen können, dass Systeme für kurze Zeit ausfallen, bis hin zu Datendiebstahl oder sogar eine komplette Zerstörung aller Daten und Infrastruktur, wodurch ein Betrieb auf unbestimmte Zeit, unmöglich ist. Um diese Gefahren zu minimieren und im besten Fall verhindern zu können, müssen Unternehmen ihre Systeme überwachen und Prozesse entwickeln, wie bei Angriffen reagiert werden soll, um den Betrieb der Systeme, welche für das Unternehmen existenzkritisch sind, sicherstellen zu können.

Jeder Angriff verfolgt dabei ein bestimmtes Ziel wie beispielsweise die Verschlüsselung von Daten. Diese Art von Angriff wird mithilfe sogenannter Ransomware durchgeführt. Die Anzahl der Angriffe ist in den letzten Jahren sehr stark angestiegen [Soni22, S. 14], da sich mittlerweile durch den Durchbruch von Kryptowährungen viele Angreifer sich einen finanziellen Vorteil durch die Angriffe verschaffen können. Oft wird bei den Angriffen mit der Angst der Unternehmen Geld verdient, da diese sonst riskieren ihre Daten zu verlieren.

Durch die stetig steigende Zahl der Angriffe in den letzten Jahren, werden immer mehr Unternehmen auf die Gefahren aufmerksam und erkennen die Notwendigkeit für IT-Sicherheit im eigenen Betrieb. Da der Aufbau einer IT-Sicherheitsabteilung sehr teuer ist und viel Zeit in Anspruch nimmt, werden Dienstleister für diese Aufgaben eingekauft, da diese bereits das nötige Fachwissen und Erfahrungen mitbringen. Hierzu gehört beispielsweise das nötige Wissen über Angriffe, die mit der oben genannten Ransomware durchgeführt werden.

Da diese Angriffe nicht nur eine Bedrohung für die Industrie darstellen können, sondern auch für die Infrastruktur eines Landes trägt zusätzlich die Gesetzgebung ihren Teil zum Schutz bei. Dafür hat diese im Juli 2015 das so genannte IT-Sicherheitsgesetz erlassen. In diesem Gesetzestext werden bestimmte Bereiche der Infrastruktur in Deutschland angesprochen, die sogenannte kritische Infrastruktur (KRITIS). Ziel ist es die Unternehmen in diesen Bereichen dazu zu verpflichten, die Sicherheit zu erhöhen, da diese Unternehmen für Grundbedürfnisse der Bürger/innen als besonders wichtig eingestuft sind. Zusätzlich wurde im April 2021 eine neue Version dieses Gesetzes verabschiedet, was dazu geführt hat, dass weitere Bereiche der KRITIS zugeordnet und dazu verpflichtet wurden ein Mindestmaß an IT-Sicherheitsmaßnamen einzuführen.

1.1 IT-Sicherheitsgesetz

Da Angriffe nicht nur für Unternehmen verheerend sind, sondern sich diese auch auf die gesamte Wirtschaft und Gesellschaft auswirken können, wurde im Juli 2015 von der Bundesregierung das so genannte IT-Sicherheitsgesetz verabschiedet. Damit möchte die Regierung positiv dazu beitragen, dass IT-Systeme und die digitale Infrastruktur sicherer gemacht werden. Hierbei werden hauptsächlich Unternehmen angesprochen, die im Bereich der Kritischen Infrastruktur (KRITIS) operieren [§2 IT-SiG].

Die KRITIS sind „… Einrichtungen, Anlagen oder Teile davon, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“ [$2 Absatz 2 IT-SiG]

Als Erweiterung für das IT-Sicherheitsgesetz wurde im April 2021 das IT-Sicherheitsgesetz 2.0 verabschiedet, dadurch werden unter anderem die KRITIS durch einige neue Bereiche erweitert. Die Sektoren, die zum Zeitpunkt des Verfassens der KRITIS zugeordnet sind, sind in Abbildung 1 zu sehen:

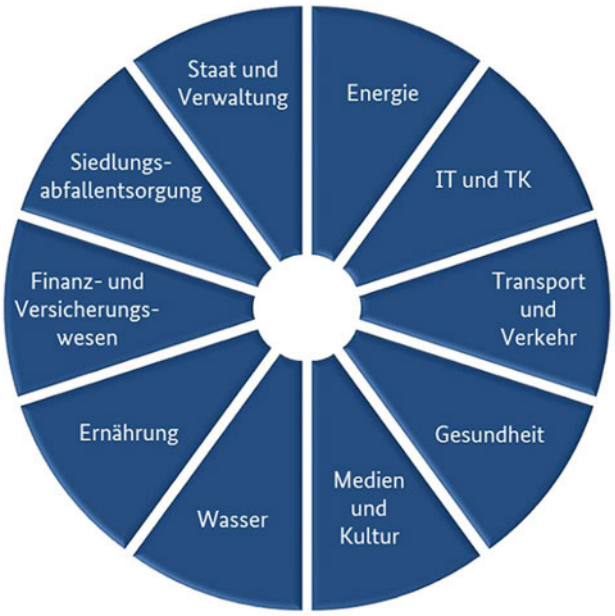


Abbildung 1 – Sektoren der KRITIS [BSI]

Ebenfalls zählen mit der Erweiterung des IT-Sicherheitsgesetzes 2.0 Unternehmen von besonderem öffentlichem Interesse (UNBÖFI) zur KRITIS. Dazu gehören:

- Rüstungshersteller
- Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen
- 100 größten Unternehmen in Deutschland mit erheblicher volkswirtschaftlicher Bedeutung (bewertet nach der Wertschöpfung)
- Betreiber von Betriebsanlagen mit Gefahrstoffen der oberen Klasse

Dadurch wird es einen deutlichen Zuwachs an Unternehmen geben, welche von dem neuen Gesetz betroffen sind. Allerdings muss beachtet werden, dass bei Betrachtung der 100 größten Unternehmen, nicht das gesamte Unternehmen, dem Gesetz unterliegt, sondern nur die Teile des Unternehmens als KRITIS betrachtet werden, wo die Anlagen zu finden sind, die der KRITIS zugeordnet sind [§2 Absatz 14 Satz 1 BSIG].

Sobald ein Unternehmen sich als Bestandteil der KRITIS identifiziert hat, muss dieses Unternehmen sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als solche, mit einer Kontaktstelle im Unternehmen, registrieren. Zusätzlich wird unmittelbar die Selbsterklärung zur IT-Sicherheit gefordert, welche alle 2 Jahre erneut eingereicht werden muss. Störungen, die zur Beeinträchtigung des Betriebs führen und somit der KRITIS schaden können, müssen ebenfalls gemeldet werden [§8a Absatz 1 Satz 1 BSIG].

Um nun die KRITIS sicherer zu gestalten, werden, mit dem Gesetz, Pflichten an die betroffenen Unternehmen erteilt. Davon wurden bereits zwei genannt, nämlich die Registrierung beim BSI, sowie die Meldepflicht bei Störungen. Bei den Meldungen sind die Unternehmen dazu verpflichtet Informationen ans BSI auszuhändigen die für die Beseitigung der Störung benötigt werden. Eine weitere Verpflichtung, ist die Anzeige von kritischen Komponenten, worunter auch die Inventarisierung fällt, außerdem besteht die Möglichkeit, dass der Einsatz dieser kritischen Komponenten, unter bestimmten Bedingungen, vom Innenministerium untersagt werden kann. Dabei handelt es sich um IT-Produkte mit kritischen Funktionen, welche für die Operation der KRITIS notwendig sind [§8a Absatz 1 Satz 1 BSIG].

Die wichtigste Pflicht der KRITIS-Betreiber ist die Angriffserkennung, denn nur dadurch ist es möglich die Angriffe durch schnelle Maßnahmen aufzuhalten und im besten Fall gar nicht erst stattfinden zu lassen. Die Angriffserkennung gehört nun explizit zu den technischen und organisatorischen Sicherheitsvorkehrungen von KRITIS-Anlagen. Da diese Maßnahmen viel Zeit, Geld und Wissen beanspruchen, sind diese ab dem 1. Mai 2023 für alle KRITIS-Betreiber verpflichtend [§8a Absatz 1a Satz 1 BSIG].

Das BSI hat hierauf eine Orientierungshilfe zum Einsatz von System zur Angriffserkennung veröffentlicht [BSI22]. In dieser Orientierungshilfe werden unterschiedliche Bedingungen thematisiert. Die Rahmenbedingungen beinhalten hier die notwendige Technik, Organisation und Personal, welches vorhanden sein muss, um die Maßnahmen umsetzen zu können. Informationen zu den Schwachstellen, den eingesetzten System und die dazu möglichen Angriffe müssen eingeholt werden. Die genutzten Systeme und Software, welche für die Angriffserkennung genutzt werden, müssen auf dem aktuellen Stand und so konfiguriert sein, dass bereits bekannte Angriffe erkannt und verhindert werden können. Signaturen, Regeln und Angriffsmuster müssen stets aktuell gehalten werden, um sich vor neu entdeckten Angriffen schützen zu können [BSI22, SS. 8ff.].

Wenn die oben genannten Pflichten nicht eingehalten werden, müssen die Unternehmen mit Ordnungswidrigkeiten und Bußgeldern rechnen. Als Ordnungswidrigkeiten sind hier

unter anderem fehlende Nachweise und Störungsmeldungen, mangelnde Zusammenarbeit und Maßnahmen sowie die fehlende Registrierung und Kontaktstelle mit dazugehörigen Informationen. Die Bußgelder betragen hier bis zu 2 Millionen Euro [§14 Absatz 5 Satz 1 BSIG].

Nicht zuletzt durch die hohen Bußgelder liegt es im Interesse des Unternehmens die Verpflichtungen und Maßnahmen umzusetzen. Da nicht für jedes Unternehmen die Möglichkeit besteht, eine eigene Abteilung mit Infrastruktur und Arbeitskräften aufzubauen, ist es möglich Dienstleister, welche über alles Nötige verfügen, zu beauftragen große Teile der technischen Bedingungen zu übernehmen. Um die Frist vom 1. Mai 2023 einhalten zu können, ist die Zahl der Anfragen an Dienstleiter in der letzten Zeit stark gestiegen, wie sich aus der in der Statistik und Prognose für den Marktwert des Security Operations Center (SOC-) Marktes der Polaris Market Research ableiten lässt. Die Entwicklung der Marktgröße für SOCs wird in Abbildung 2 gezeigt.

Abbildung 2 – Security Operations Center Marktwert 2018-2030 [Pola22]

Die Aufgaben der Überwachung übernimmt meist das sogenannte SOC, worauf im nächsten Abschnitt näher eingegangen wird.
Bei den Anfragen an das beauftragte SOC wurden durch die steigende Anzahl von Angriffen immer öfter auch die Vorgehensweise bei bestimmten Angriffen angefragt. Auf die Details von Ransomware-Angriffen wird in Kapitel 2.2 eingegangen.

1.2 Zielstellung der Arbeit

Diese Arbeit soll Unternehmen, Security Operation Center Mitarbeiter/innen und IT-Sicherheitsinteressierte ansprechen. Dabei sind die folgenden Fragen zentraler Bestandteil dieser Arbeit:

- Welche Ransomware Gruppen gibt es zurzeit?
- Wie findet man heraus gegen welche Gruppen man sich schützen soll?
- Wie schützt man sich gegen diese Gruppen?

Das Endergebnis soll eine Methode sein, wie mit Threat Intelligence, Ransomware Gruppen priorisiert werden können, die für bestimmte Unternehmen von besonderem Interesse sind. Darüber hinaus sollen für diese Gruppen Erkennungsmuster und Regeln definiert werden, um sich als Unternehmen gegen ihre Angriffe schützen zu können.

1.3 Aufbau der Arbeit

Zuerst wurde in der Einführung erläutert, was das IT-Sicherheitsgesetz ist und wieso dieses vom Bund erlassen wurde, sowie die Erklärung, was Unternehmen beachten müssen. Dadurch wird die Bedeutsamkeit eines SOCs bekannt.

Im Hauptteil werden die technischen Grundlagen für das Verständnis dieser Arbeit gelegt. Zum oben genannten SOC kommen die genutzten Tools eines SOCs mit deren Vergleich. Der Begriff Ransomware wird vorgestellt und erklärt, sowie die Phasen der Cyber Kill Chain. Im letzten Abschnitt wird die Bedeutung von Threat Intelligence thematisiert, mit einer anschließenden Zusammenfassung des Kapitels.

Kapitel 3 stellt das Konzept vor, wie die gestellten Fragen beantwortet werden können. In Kapitel 4 wird die Implementation vorgestellt und wie Threat Intelligence, die Cyber Kill Chain genutzt wurden, sowie die Entstehung der Erkennungsmuster und Regeln für die Alarmierung durch ein Security Information and Event Management (SIEM). Anschließend wird die Implementation evaluiert.

Im letzten Kapitel wird ein Fazit gezogen und ein Ausblick, welche Tätigkeiten und Ideen zur Fortführung dieser Arbeit dienen können, vorgestellt.

2 Grundlagen

In diesem Kapitel werden die Grundlagen für das Verständnis dieser Arbeit vorgestellt und geklärt. Hierzu wird erläutert was ein SOC ist und wie bei einem SOC gearbeitet wird, um die Sicherheit eines Unternehmens gewährleisten zu können. Zusätzlich werden unterschiedliche Produkte, welche in einem SOC genutzt werden, vorgestellt.

Der zweite Teil befasst sich mit Ransomware, wo diese definiert wird, mit einer kurzen historischen Entwicklung und warum diese sich in den letzten Jahren so verbreitet hat.

Folgend wird die Kill-Chain präsentiert, welche sich genauer mit dem Schutz vor Angriffen auseinandersetzt.

Zuletzt wird die Thematik Threat Intelligence behandelt. Diese wird definiert, sowie die unterschiedlichen Schritte des Vorganges vorgestellt, um erfolgreich die Ziele von Threat Intelligence zu erreichen.

2.1 Security Operations Center (SOC)

Ein SOC ist oft ein wichtiger Bestandteil der IT-Abteilung eines Unternehmens. Das SOC ist dafür da, die digitale Infrastruktur von Unternehmen zu überwachen, sei es extern als Dienstleister oder als interne/r Mitarbeiter/in.

„Security Operations Center is a generic term describing part or all of a platform whose purpose is to provide detection and reaction services to security incidents“ [Bido05, S. 2].

Für die Überwachung werden unterschiedliche Methoden und Tools verwendet, um die Sicherheit gewährleisten zu können. Die Hauptaufgaben sind hierbei das Monitoren und die Bewerkstelligung von möglichen Gefahren, diese Gefahren werden dann analysiert, das jeweilige Risikolevel bestimmt und beruhend auf Erfahrungen und Wissen werden für die Gefahren Empfehlungen ausgesprochen, die zur zukünftigen Vermeidung oder auch Behebung von den gefundenen Gefahren führen sollten. Die Tätigkeiten eines SOCs dienen also ganz allein der Sicherheit des Unternehmens [Nath15, SS. 2ff.]. Beim SOC kann man die Aktivitäten in drei Phasen einteilen.

Die erste Phase widmet sich der Vorbereitung und Planung. Um ein Netzwerk mit den teilnehmenden Geräten schützen zu können, ist es nötig die Komponenten zu kennen. Hier wird besonderer Fokus auf die Komponenten gelegt, welche für das Unternehmen kritisch sind. Dabei ist es egal, ob es sich um Software, Datenbanken, Server, Endgeräte

wie Laptops oder Workstations, Firewalls oder Switche handelt. Die genutzten Komponenten müssen jeweils an die Überwachungssysteme angebunden werden, um die nächste Phase erfolgreich beginnen zu können [IBM].

Phase zwei besteht aus dem Monitoring, der Erkennung und Reaktion. Hier werden die oben genannten Komponenten auf unterschiedliche Zeichen eines Angriffs oder Anomalien geprüft [IBM]. Dafür sind Erkennungsmuster bzw. Erkennungsregeln nötig, die mit Events abgeglichen werden. Auf den folgenden Seiten werden die Dinge beschrieben, welche für die Umsetzung der Phase zwei nötig sind.

Events sind Aktionen, die auf einem System zu einem bestimmten Zeitpunkt geschehen sind. Dazu sind oft Metadaten vorhanden, damit die Aktionen in einen Kontext gesetzt werden können. Zu den Daten gehören Zeitangaben, Benutzerinformationen und Eventinformationen. Die Zeitangabe bezieht sich auf den Zeitpunkt der Aktion, also des Events. Benutzerinformationen können Dinge wie Benutzername, Gruppe und Domain enthalten. Die Eventdaten an sich sind genauere Informationen zur jeweiligen Aktion. Hierbei können es Anmeldeversuche, das Starten eines Prozesses oder Ausführen eines Kommandos sein. Events werden somit von Menschen und deren Tätigkeiten am System, sowie automatische Aktionen, die das System selbstständig ausführt, wie beispielsweise automatische Updates generiert. Ergänzend dazu sind Logs der Ort, wo diese Events gespeichert werden, dabei sind dies meistens Textdateien auf dem System. Zu den unterschiedlichen Events existieren ebenso mehrere unterschiedliche Log Typen, um die Events zu kategorisieren. Zu den Log Typen gehören System Logs (Syslog), Server Logs, Authorization Logs, Access Logs, Change Logs, Availability Logs, Resource Logs und Threat Logs. Bei den System Logs werden Informationen vom Betriebssystem niedergeschrieben, wie Warnungen, Fehler, Neustarts und das Herunterfahren des Systems. Events werden von fast allen Geräten und Applikationen in einem Netzwerk generiert, Beispiele hierfür sind Firewalls, Endgeräte und Server, aber auch Datenbanken und Webservices erstellen Events und schreiben diese in Logfiles. Da Events so weit verbreitet sind, ist die Verwendung dieser ebenfalls breit gefächert. Die Anwendungsgebiete für Events reichen von Workload balancing und Performance von Applikationen bis hin zur Compliance Verwaltung, Reporting und die Erkennung von verdächtigen Aktivitäten von Hackern [Shar22].

Bei Windows existieren fünf unterschiedliche Log Typen, nämlich Applikationen, Security, Setup, System und Forwarded. Zusätzlich existierten Application and Service Logs für die Administration, Analyse und Debugging von DHCP-Diensten [Nxlo22]. Da sich diese Arbeit sich mit dem Thema Security befasst, werden nur diese Art von Event Logs betrachtet. Im Security Log speichert Windows sicherheitsrelevante Events des Systems, welche durch die Sicherheitsüberwachung generiert werden. Dieses Tool wurde dafür entwickelt, um Angriffe, erfolgreich oder nicht, zu identifizieren [Pamn22a]. Die grundlegenden Sicherheitsüberwachungsrichtlinien sind [Pamn22b]:

- Anmeldeversuche

- Kontenverwaltung
- Verzeichnisdienstzugriff
- Anmeldeereignisse
- Objektzugriffsversuche
- Richtlinienänderungen
- Rechteverwendung
- Prozessverfolgung
- Systemereignisse

Unabhängig von den unterschiedlichen Richtlinien enthalten die Events bestimmte Elemente mit Informationen, welche für die Analyse genutzt werden.
Zum Unterscheiden des Events, wird jedem eine Event ID zugeordnet, hierdurch lässt sich bestimmen, was auf dem System passiert ist. Zusätzlich werden Events mit weiteren Informationen, wie Datum und Zeit, Computer, Benutzer angereichert. Laut der „Windows 10 and Windows Server 2016 security auditing and monitoring reference" existieren 410 unterschiedliche Event IDs [Miro16]. Die Liste aller Security Events werden im Anhang „Event IDs" aufgelistet.

Zusätzlich zu den Windows internen Event Logs existiert die Möglichkeit eine zusätzliche Software namens Sysmon, von Sysinternals, zu installieren. Sysmon wird als Systemdienst und Treiber installiert, welches die Systemaktivitäten überwacht und die Ereignisse im Windows-Ereignisprotokoll speichert. Das Ziel von Sysmon und der bereits vorhandenen Windows Security Logs ist dasselbe, jedoch erweitert Sysmon die Richtlinien, die geloggt werden können und stellt somit mehr Informationen zur Verfügung.
Sysmon hat zum Zeitpunkt des Verfassens 29 unterschiedliche Event IDs. Da zu einem späteren Zeitpunkt in dieser Arbeit die Events von Sysmon relevant sind und genutzt werden, werden einige Event IDs, die in dieser Arbeit genutzt werden, kurz erläutert [MHKR22].

Tabelle 1 – Sysmon Event Beispiele [MHKR22]

Event ID	Kategorie	Beschreibung
1	Prozesserstellung	Informationen zu einem neu erstellten Prozess, vollständige Befehlszeile, ProcessGUID für Ereigniskorrelation in der Domäne, Hash der ausführbaren Datei
3	Netzwerkverbindung	TCP/UDP-Verbindungen, mit ProcessID und ProcessGUID mit einem Prozess verknüpft, IP-Adressen, Ports, Hostnamen

5	Prozess beendet	Zeit, ProcessGUID und ProcessID des beendeten Prozesses
8	CreateRemoteThread	Ein Prozess startet einen Thread in einem anderen Prozess, Quell- und Zielprozess
10	ProcessAccess	Ein Prozess öffnet einen anderen Prozess, wird häufig genutzt, um Informationen aus Prozessen zu lesen oder schreiben
11	FileCreate	Datei wird erstellt oder überschrieben, nützlich für bestimmte Verzeichnisse wie „Startup“, „temp“ und „Downloads“
22	DNSEvent	DNS-Abfrage, unabhängig davon ob erfolgreich oder fehlgeschlagen
25	ProcessTampering	Wird generiert, wenn Prozesse ausgeblendet werden
26	FileDeleteDetected	Datei wurde gelöscht, jedoch wird die Datei nicht als Kopie gespeichert

Um die generierten Events analysieren zu können, müssen diese an einer Stelle zentral gesammelt werden. Dafür existiert bei Windows ein weiteres Tool namens Windows Event Forwarding (WEF). Beim WEF werden Logs von den Endgeräten an einen zentralen Server, Windows Event Collector (WEC), übermittelt. Bei der Übertragung ist es möglich die Logs vom Client zum Server zu schicken, das sogenannte Push, zusätzlich kann man die Übertragung als Pull stattfinden lassen, dabei werden die Logs vom Server angefordert. WEF ermöglicht eine verschlüsselte Übertragung. Die Verschlüsselung wird in einer Domäne mittels Kerberos und einer zertifikatsbasierten Authentifikation zur Verfügung gestellt. Durch die Verschlüsselung wird sichergestellt, dass Unbefugte die Events, durch das Abhören des Netzwerkverkehrs, abfangen können und somit Informationen zum Client bekommen, welche nicht zugänglich sein sollten. Zur Sicherstellung der Verbindung des Clients zum Server, sendet der Client einen Heartbeat an den Server. So weiß der Server, dass der Client verbunden ist, ohne das Events gesendet werden, wenn beispielsweise eine längere Zeit keine Events generiert wurden. Falls jedoch die Verbin-

dung abbrechen sollte, ist es nicht möglich die generierten Events zum Server zu schicken. Hier wird aber gewährleistet, dass die Events auf dem Client im Event Log gespeichert werden, sodass nach einer Neuverbindung zum Server dieser die Events nachreichen kann. Dies ist allerdings nur so lange sichergestellt bis der Event Log vollgeschrieben wurde und bisher vorhandene Events dadurch überschrieben werden. Wenn die gewünschten Logs auf dem WEC liegen, besteht die Möglichkeit, die Logs an ein Security Information and Event Management System (SIEM) zu schicken [MLMM22].

„… SIEM systems are an important tool in SOCs – collecting, normalizing, and analysing security events from diverse sources…" ist die Definition eines SIEMs nach Sandeep Bhatt, Pratyusa K. Manadhata und Loai Zomlot von Hewlett-Packard Laboratories [BhMZ14, S. 35].

Ein SIEM ist ein Tool, womit Analysten/innen im SOC täglich arbeiten. Das SIEM hat die Aufgabe die Events aus dem Netzwerk von allen teilnehmenden Geräten (siehe SOC-Phase 1 und Abbildung 3, Links) zentral zu sammeln und den Nutzern des SIEMs diese Daten zur Verfügung zu stellen. Jede dieser angebundenen Quellen schicken dauerhaft Events an spezielle Konnektoren, die auf das Produkt abgestimmt sind. Oft werden diese von den SIEM-Herstellern mit ausgeliefert, jedoch ist es möglich, dass für weniger genutzte Produkt, eigene Konnektoren geschrieben werden müssen. Die Konnektoren sind dafür da, die Events in ein normalisiertes Format zu übertragen, damit Regeln erstellt werden können, welche weitgreifend funktionieren. Bei den Konnektoren wird somit auf Hersteller, Produkttyp und Version Rücksicht genommen, um so viele Produkte wie möglich zu unterstützen. Nach dem Normalisieren und Parsen der Events werden diese Informationen an die Security Management Plattform weitergeleitet. Hier wird jedes eintreffende Event auf die implementierten Regeln überprüft. Bei einer Übereinstimmung werden die betroffenen Events meist zusammengefasst und in einer generierten Meldung den Analysten/innen in einer grafischen Oberfläche zur Verfügung gestellt, sodass eine kurze Reaktionszeit ermöglicht werden kann [BhMZ14, SS. 35ff.].

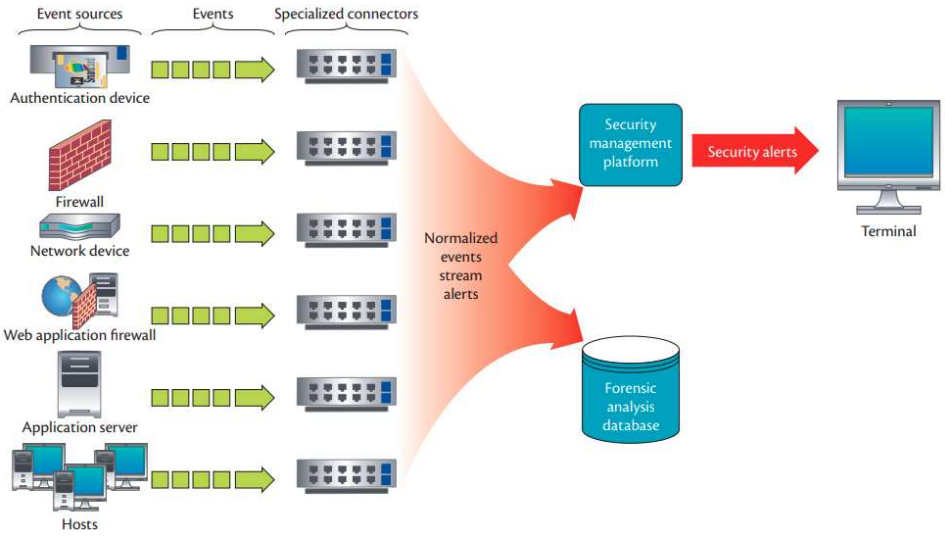


Abbildung 3 – Vereinfachte Architektur eines SIEMs [BhMZ14, S. 36]

Ein Endpoint Detection and Response System (EDR) ist das, was früher als Anti-Virus bezeichnet wurde. Dabei werden heutzutage die Anti-Virus Technologien in die EDR-Systeme integriert und ist eine Sicherheitslösung für Echtzeit Überwachung eines Endgerätes, meistens Laptops und Workstations [Chec]. Die Funktionen eines EDR-Systems sind das Überwachen und Sammeln von Daten, welche potenziell durch schadhafte Aktionen und Programmen auf Endgeräten generiert wurden, durch künstliche Intelligenz werden diese Daten analysiert, um dadurch schadhafte Tätigkeiten erkennen. Ebenfalls ergreift das EDR automatisch Gegenmaßnahmen, indem das EDR beispielsweise die betroffenen Programme schließt. Diese Aufgabe übernimmt das Response Modul [BrNu21, S. 2f.].

“The evolution of EDR, which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tolls such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.” [Mell21], wie von Forrester definiert, ist ein XDR eine Erweiterung des bereits bekannten EDR-Systems in Verbindung mit anderen Produkten. Es ist eine Methode, um die Gefahrenerkennung und das Reagieren auf diesen für die gesamte technische Infrastruktur zu schaffen, folglich ist es realisierbar, die potenziellen Gefahren, durch weniger Arbeit miteinander zu korrelieren sowie einen breiteren Kontext zu erhalten. Ein XDR ermöglicht so den Analysten/innen auf Gefahren direkt auf dem betroffenen Endgerät zu reagieren, das Verhalten von Benutzern zu analysieren, Threat Intelligence Feeds einbinden, um die Fehlerrate zu verringern [BrNu21, S. 4].

In einem SIEM sind die Erkennungsregeln das Herzstück, diese haben den Zweck Gefahren und ungewöhnliche Dinge im Netzwerk und im Netzwerk zu erkennen, zu melden und dabei den Analysten/innen eine schnelle und effiziente Maßnahme zu ermöglichen. Da es viele unterschiedliche Produkte gibt, welche das gleiche Ziel verfolgen, jedoch vollkommen unterschiedlich operieren und die Erstellung der Regeln unterschiedlich ablaufen und mit unterschiedlicher Syntax verfasst werden, wurde eine Möglichkeit geschaffen, die erstellten Regeln in einem einheitlichen Format abzubilden. Somit existiert mit Sigma eine Möglichkeit, Regeln zwischen den bekanntesten SIEM-Systemen auszutauschen. Dieses Format wurde von einem IT-Sicherheits Forscher namens Florian Roth erstellt und verfolgt das Ziel, Regeln für SIEM-Systeme in einer simplen, aber flexiblen Art zu verfassen und dabei für jede Art von Logs abdecken zu können. Der Aufbau einer Sigma Regel ist wie folgt, dass es Parameter gibt, wie den Titel der Regel, eine Beschreibung, den Autor, die Logquelle und die Schlüsselereignisse für die Erkennung. Bei einigen Parametern ist es möglich oder notwendig eine Unterteilung zu erstellen. Bei den Ereignissen für die Erkennung, gibt es eine Unterteilung für die Keywords nach denen gesucht werden soll, ebenso wird eine Bedingung angegeben, welche die Logik der Regel darstellt [Roth22].

```yaml
title: Sysmon Crash
id: 4d7f1827-1637-4def-8d8a-fd254f9454df
status: experimental
description: Detects application popup reporting a failure of the Sysmon service
author: Tim Shelton
date: 2022/04/26
tags:
    - attack.defense_evasion
    - attack.t1562
logsource:
    product: windows
    service: system
detection:
    selection:
        Provider_Name: 'Application Popup'
        EventID: 26
        Caption: 'sysmon64.exe - Application Error'
    condition: selection
falsepositives:
    - Unknown
level: high
```

Abbildung 4 – Sigma Regel für den Absturz von Sysmon [Shel22]

Obige Regel beschreibt eine Erkennung von Events, wenn Sysmon abgestürzt ist. Im SIEM wird ein Event mit der Event ID 26 generiert, worauf anschließend geprüft werden kann, ob das Feld „Caption“ den String „sysmon64.exe – Application Error“ enthält. Um die Regeln mit anderen Unternehmen, Personen und IT-Sicherheitsinteressierten teilen zu können, gibt es mehrere Möglichkeiten diese zu zur Verfügung zu stellen, beispielsweise über das GitHub Repository von Florian Roth. Um die Sigma Regeln für sein spezifisches SIEM-System zu übersetzen, ist es möglich dies per Hand durchzuführen, jedoch gibt es einige Möglichkeiten, diese automatisiert mit Tools zu generieren. Diese Regeln und Suchen, sind dann in der Lage dazu Events zu analysieren und dabei die definierten Muster wie bestimmte Event IDs zu finden.

Durch die Notwendigkeit, das Verhalten der Angreifer systematisch in Kategorien einteilen zu können, hat sich die MITRE dazu entschieden dies umzusetzen. Dabei wurde die Frage gestellt, wie gut man das Verhalten von Angreifern in seiner Infrastruktur erkennt.

Diese Kategorien spiegeln dabei den Zyklus eines Angriffes wider und gehen dabei auf die Systeme ein, die vermutlich angegriffen werden. Tactics, Techniques and Trocedures (TTPs) sind Verhaltensweisen, Methoden und/oder Verhaltensmuster die Angreifer beschreiben. Dabei werden hier auf die TTPs für das Microsoft Windows System eingegangen. TTPs werden dabei in unterschiedliche Kategorien der MITRE ATT&CK eingeteilt und erhoffen die Erkennung von schadhaftem Verhalten zu verbessern. ATT&CK ist somit ein Modell mit Taktiken von Angreifern, wodurch die kurzzeitigen Ziele behandelt werden. Techniken, welche genutzt werden, um das taktische Ziel des Angriffs zu erreichen. Untertechniken beschreiben die einzelnen Techniken mit mehr Detail. Zuletzt werden diese Daten zusammen mit Metadaten, zu den einzelnen Angreifern, dokumentiert.

Definiert wird das ATT&CK Modell so:

„The basic of ATT&CK is the set of techniques and sub-techniques that represent actions that adversaries can perform to accomplish objectives. Those objectives are represented by the tactic categories the techniques and sub-techniques fall under. This relatively simple representation strikes a useful balance between sufficient technical detail at the technique level and the context around why actions occur at the tactic level.” [SAMN18, S. 6]

Genutzt wird das ATT&CK für mehrere Zwecke:

1. Angreifer Emulation

   Ein Prozess, um die eigene Sicherheit mit Hilfe von Cyber Threat Intelligence mit Bezug auf bestimmte Angreifer zu prüfen.

2. Red Teaming

   In die Rolle des Angreifers schlüpfen ohne das Hintergrundwissen von Cyber Threat Intelligence mit dem Ziel, in der Infrastruktur eine Operation erfolgreich abzuschließen, ohne durch die Sicherheitssysteme erkannt zu werden.

3. Entwicklung von Verhaltensanalysen

   Ermöglicht die Erkennung von neuem Verhalten durch Gefahren, die vorher nicht bekannt waren.

4. Mängelanalyse mit Bezug auf Sicherheit

   Ein Prozess, um die Bereiche in der Infrastruktur zu finden, wo keine oder wenig Einblick ins Netzwerk und Systeme existiert und somit auch mangelnder Schutz herrscht.

5. Reife eines SOCs bestimmen

   Bestimmen der Reife eines SOCs ist wichtig, um zu verstehen wie effektiv es die eigenen Ziele erreichen und verfolgen kann.

6. Cyber Threat Intelligence Daten anreichern

   Erweiterung der Daten von Gefahren, Angreifer Gruppen, sowie Informationen zu Malware, Tools, TTPs, Verhalten und anderen Indikatoren, die mit Gefahren in Verbindung gebracht werden können.

Für eine Übersicht wurde die ATT&CK Matrix geschaffen. Beziehungen zwischen Taktiken, Techniken und Sub-Techniken können dadurch visuell dargestellt werden [SAMN18, SS. 1ff.].

Abbildung 5 - MITRE ATT&CK Matrix [MITR22]

Zurzeit existieren 14 Taktiken mit einer Vielzahl an Techniken wie in der Grafik oben zu sehen ist.

An der Abbildung rechts kann man die Taktik „Reconnaissance“ (kurz Recon), was so viel wie Erkundung bedeutet. Recon beschäftigt sich mit der Erkundung des Netzwerkes und Systeme in einer Infrastruktur. Dieser Taktik sind insgesamt zehn Techniken zugewiesen, welche jeweils Sub-Techniken besitzen, dies ist an der grauen Fläche links neben der Technik zu erkennen.

Neben Recon sind die Taktiken:

Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration und Impact.
Durch diese Taktiken werden alle Bereiche eines Angriffes abgedeckt von dem Eintritts Vektor bis hin zum Sammeln von Daten und deren Ausschleusung.
Ein detaillierter Blick auf alle Taktiken sind in den Anlagen MITRE möglich.

Die gesamten Bausteine ergeben zusammen das MITRE ATT&CK Framework.

Abbildung 6 – ATT&CK Recon [MITR22]

Durch die gesamten aufgeführten Tools und Methoden ist es möglich im SOC mithilfe von SIEM-Systemen alles zu monitoren, zusätzlich werden durch die Regeln, Suchen, EDR

und XDR-Systeme die Erkennung von Gefahren sichergestellt und die Reaktion für Gegenmaßnahmen zu erleichtern.

Die letzte Phase des SOCs beschäftigt sich mit der Wiederherstellung und „Sanierung“, Verbesserung und Compliance Management. Nach einem Sicherheitsvorfall werden die betroffenen Systeme wiederhergestellt, indem sie entweder neu installiert oder durch ein Backup wiederhergestellt werden, sowie das Neustarten von Prozessen und Applikationen. Zu beachten ist, dass Zugangsdaten wie Passwörter neu vergeben werden. Eine Verbesserung der Infrastruktur besteht darin die Prozesse und Richtlinien im Unternehmen, mit dem Wissen, was man im Vorfall erlangt hat, zu überarbeiten. Ebenfalls ist es eine Überlegung wert, die genutzten Sicherheitstools zu ändern. Sicherheitslücken, bereits bestehende sowie neue, sollten mehr Aufmerksamkeit bekommen, um diese mit kurzen Reaktionszeiten zu beheben. Zum Compliance Management gehört die Sicherstellung, dass alle Applikationen, Systeme, Tools und Prozesse mit den lokalen Regeln für Datenschutz einhalten, wie beispielsweise die Datenschutz-Grundverordnung. Zusätzlich muss das SOC die Daten, für die Beweisführung und auditieren des Vorfalles, behalten und bereitstellen können [IBM].

2.2 Ransomware

Um die Funktionsweise einer Ransomware zu verstehen und die Einordnung dieser, werden vorab einige Begriffe geklärt und erläutert.

Der Begriff Malware ist eine Kurzform des englischen Wortes „malicious software“, dazu die deutsche Übersetzung lautet „Schadsoftware“. Den Ursprung hat dieser Begriff aus den 1980er Jahren, als 1985 die Bayerische Hackerpost von „Trojanern“ gegen die Systeme der Apple II bekannt wurden. Es existieren viele Definitionen des Begriffs Malware, jedoch ist man sich einig, dass Malware schädliche Software ist, die oftmals den Betrieb eines Computers beeinträchtigt [Hube19, SS. 76f.]. Mit der Zeit wurden immer mehr unterschiedliche Arten von Malware entwickelt, davon ist eine Art die Ransomware [RiNo17, S. 10].

Die Verschlüsselungstechnik der Ransomware dient dazu die Vertraulichkeit von Nachrichten und Daten zu schützen. Dabei existieren unterschiedliche Arten von Verschlüsselung, wobei hier kurz auf die symmetrische und asymmetrische Verschlüsselung eingegangen wird. Bei der symmetrischen Verschlüsselung wird zur Ver- und Entschlüsselung derselbe Schlüssel verwendet. Das führt dazu, dass jeder der diesen Schlüssel besitzt, die Daten Ver- und Entschlüsseln kann. Deshalb ist es bei der symmetrischen Verschlüsselung nötig, den Schlüssel auf eine sichere Art auszutauschen, jedoch ist dies in großen Kommunikationsnetzen aufwändig. Aus diesem Grund wurde ein asymmetrisches Verfahren entwickelt. Für die asymmetrische Verschlüsselung werden zwei Schlüssel generiert, einer davon wird privat gehalten und sollte nicht mit anderen geteilt werden, jedoch darf der zweite, öffentliche Schlüssel für jedermann zur Verfügung stehen, um Nachrichten damit zu verschlüsseln [Buch16, S. 76]. Obwohl einer der Schlüssel öffentlich gemacht

wird, ist es nicht möglich auf den privaten Schlüssel zu schließen, da zur Berechnung ein mathematisches Verfahren genutzt wird, welches in eine Richtung einfach zu berechnen ist, jedoch in die andere Richtung sehr schwer zu knacken ist und somit viel Zeit benötigt, wenn die Methoden der Schlüsselerstellung korrekt umgesetzt wurden. Dadurch wird das Verfahren als sicher empfunden, da die Zeit für das Knacken des privaten Schlüssels für Menschen zu lange dauern würden. Bei RSA liegt die durchschnittliche Zeit für die Berechnung des Schlüssels bei etwa 74 Jahren, wenn die Länge der genutzten Zahlen bei der Erstellung des Schlüssels eine Länge von 100 betragen. Die Empfehlung, laut den Erfindern von RSA, liegt aber bei mindestens 200-stelligen Zahlen, somit steigt die Zeit für das Knacken, bei aktuellen Standards, auf über 1 Milliarde Jahren [Mila09, S. 9]. Da aber asymmetrische Verschlüsselungsverfahren deutlich langsamer sind als symmetrische, werden diese Verfahren zusammen genutzt, auch hybride Verschlüsselung genannt, indem der Schlüssel des symmetrischen Verfahrens, asymmetrisch verschlüsselt wird, damit dieser sicher übertragen werden kann [DGTY18, SS. 239ff.].

Durch die obige Klärung von den Begrifflichkeiten von Malware und die Nutzung von Verschlüsselung erläutert wurde, ist es einfacher die Funktionsweise und Bedeutung von Ransomware zu verstehen. Definiert wird Ransomware wie folgt:

„A ransomware is a kind of malware which demands a payment in exchange for a stolen functionality.” [Gaze08]

Leider besteht für jeden das Risiko von Ransomware angegriffen zu werden, ob Privatpersonen, Unternehmen oder Staaten. Bei den Angriffen werden zwischen Locker- und Krypto Ransomware unterschieden. Ersteres „verschließt“ den Computer und verhindert den gesamten Zugriff auf das System, sodass ein Nutzen nicht mehr möglich ist, bis entweder eine Lösegeldsumme gezahlt wurde und dann der Zugang, durch beispielsweise eine PIN, die durch die Ransomware gesetzt wurde, oder die Ransomware manuell entfernt wird, welches jedoch nicht immer so einfach ist. Bei der Locker Ransomware werden die Daten auf dem Gerät/ der Festplatte nicht beeinträchtigt. Dadurch ist es möglich die Daten, durch das Anschließen der Festplatte an einen anderen Computer, zu sichern. Dadurch wird ermöglicht, dass man das Betriebssystem neu installieren kann, ohne einen Verlust der Daten zu erleiden. Aus dem Grund, da es als betroffene Person möglich ist die Daten zu sichern ohne Lösegeld zu zahlen, wird Krypto Ransomware eingesetzt. Bei dieser Art der Ransomware, wird, wie der Name suggeriert, Kryptographie eingesetzt, um die Daten zu verschlüsseln [RiNo17, S. 10]. Hierbei werden die oben genannten Verfahren der symmetrischen und asymmetrischen Verschlüsselung genutzt, sowie teilweise eine hybride Verschlüsselung, beispielsweise ChaCha8 als symmetrische und RSA (Rivest–Shamir–Adleman) als asymmetrische Verschlüsselung [Lifa21, S. 2; HeCC20, S. 3]. Durch die Verschlüsselung der Daten, sind diese nicht aufrufbar, dabei macht es keinen Unterschied, ob man das Medium, worauf die Daten gespeichert sind, an einem anderen Gerät anschließt. Das liegt daran, dass eine Krypto Ransomware keine systemrelevanten Dateien verschlüsselt, sodass das Gerät noch bis zu einem gewissen Punkt genutzt werden kann. Der Grund dafür ist, dass in der heutigen Zeit die Zahlung des Lösegeldes mit

Kryptowährungen getätigt werden soll. Somit ist es der betroffenen Person möglich, auf dem Gerät die gewählte Kryptowährung zu kaufen und diese an das angegebene Konto zu schicken [RiNo17, S. 10]. Wie Kryptowährungen in der kriminellen Welt genutzt werden, wird später in diesem Kapitel behandelt.

Die erste Art von Ransomware wurde **1989** entwickelt. Diese wurde mit Floppy Disks auf der Aids Konferenz der WHO (World Health Organization) verbreitet, daher erhielt die Ransomware die Bezeichnung AIDS. Zum Einsatz kam hier eine simple symmetrische Verschlüsselung. Gefordert wurden damals 189$ für die Entschlüsselung der Daten, jedoch wurde der Verschlüsselungsalgorithmus nach recht kurzer Zeit geknackt [RiNo17, S. 11; HeCC20, S. 3].
Durch den Durchbruch des Internetzeitalters im Jahre **1997**, hatten Angreifer die Möglichkeit, ihre Malware durch E-Mail, FTP (File Transfer Protocol) und IRC (Internet Relay Chat) zu verteilen. Diese Methoden der Vervielfältigung hatte zur Folge, dass das Infizieren schneller verlief und weitere Ausmaße hatte als zuvor mit Disketten [Schm06, S. 14].
2005 wurde allerdings erst die erste moderne Ransomware, namens GPCoder, entdeckt, welche die Vervielfältigung, durch die Verteilung, im Internet nutzte [RiNo17, S. 11].
Im nächsten Jahr, **2006**, wurde Ransomware entwickelt, wo die Daten in einem Passwortgeschützten Ordner verschoben und im Anschluss die Originaldaten gelöscht wurden. Die Locker Ransomware erhielt im Jahr 2007 die meiste Aufmerksamkeit, da Russland davon stark betroffen war. Kurze Zeit darauf verbreiteten sich diese Versionen jedoch auch nach Europa und den USA.
GPCode.AK, eine neue Version der Ransomware GPCoder aus 2005, wurde **2008** öffentlich genutzt, dabei wurde als Lösegeld eine Überweisung von e-gold oder Liberty Reserve gefordert. Onlinewährungen werden also bereits mindestens seit 14 Jahren in der Cyberkriminalität genutzt.
2011 gab es den ersten großen Ausbruch von Ransomware als mehrere anonymisierte Zahlungsdienste auf den Markt gekommen sind. In der ersten Hälfte von 2011 sind insgesamt 60000 neue Ransomware Varianten erschienen.
Citadel und Lyposit waren mit die ersten Ransomware Toolkits aus dem Jahre **2012**, wodurch sich die Möglichkeit ergeben hat, seine Ransomware zu personalisieren und automatisiert durch das Toolkit zu vertreiben.
Die bisher bekannteste Ransomware erschien **2013** und wurde CryptoLocker genannt. Verteilt wurde diese durch ein Botnet namens Gameover ZeuS oder über Mails, welche so aussahen, also würden sie von UPS oder FedEx stammen. Drei Tage hatten die Betroffenen Zeit zu zahlen, die Summe betrug zwei Bitcoins. Falls die Frist von drei Tagen nicht eingehalten wurde, bestand das Risiko, dass die Summe auf zehn Bitcoins erhöht wurde. Schätzungen zufolge waren etwa 600.000 Systeme von CryptoLocker betroffen. Laut einer Studie von Kaspersky ist die Anzahl der Angriffe von Ransomware Gruppen von 2014 auf 2015 um 448% gestiegen sind.
Ransomware-as-a-Service (RaaS) ist im Jahr **2015** erschienen. Durch den Vertrieb im TOR-Netzwerk war es möglich die Ransomware gegen eine Gebühr zu mieten. Das Prinzip hinter RaaS wird im nächsten Abschnitt genauer erläutert. Da die Idee des RaaS ge-

boren wurde, kann man aus der steigenden Anzahl an Ransomware Varianten in den darauffolgenden Jahren vermuten, dass der Einstieg in die RaaS Branche, durch das neue Geschäftsmodell, für viele attraktiv wurde, siehe folgende Abbildung.

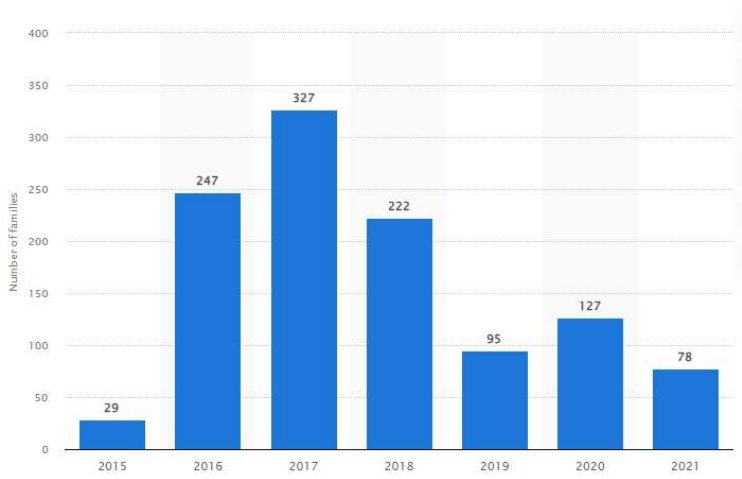


Abbildung 7 – Neue Varianten von Ransomware 2015-2021 [Stat22a]

Petya ist eine Ransomware aus dem Jahr **2016**. Diese hat es unmöglich gemacht, das Gerät zu benutzen, da es den Master Boot Record überschieben hat, welches dazu geführt hat, dass es ebenfalls nicht möglich war die nicht verschlüsselten Daten zu rekonstruieren. [RiNo17, SS. 11ff.]
Wahrscheinlich einer der bekanntesten Ransomwares, WannaCry hat **2017** etwa 150 Länder betroffen und insgesamt 300.000 Computer infiziert. Geführt hat dies zu einem Schaden in Milliardenhöhe. Zwar schwankt die Anzahl der Ransomware Angriffe jedes Jahr, jedoch ist in Abbildung 8 zu erkennen, dass immer Angriffe durchgeführt werden. Dabei werden ständig neue Methoden in die Ransomware eingebaut, um es den Betroffenen schwieriger zu machen die Zahlung zu umgehen ohne Verluste einzubüßen.

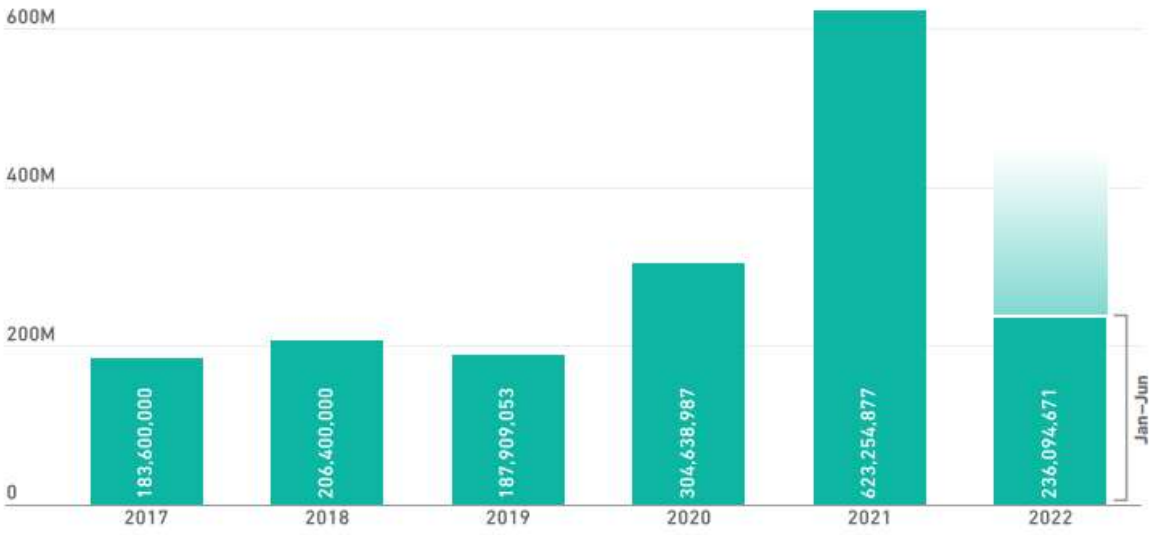


Abbildung 8 – Anzahl der Ransomware Angriffe 2016-2022 H1 [Soni22, S. 14]

Wegen der Prominenz vom Betriebssystem Windows, bei etwa 75% der weltweiten Nutzung von Betriebssystemen, werden die genannten Ransomwares und TTPs, wenn nicht explizit genannt, sich auf Windows beziehen. [Stat22b]

Die neue Art, um mit Ransomware Geld zu verdienen basiert auf einem Modell, welches in der gewöhnlichen Wirtschaft ebenfalls genutzt wird. Hierbei werden Produkte für eine Gebühr angeboten und an mehrere Parteien vertrieben. Bekannt ist dies von Software-as-a-Service, Platform-as-a-Service und Infrastructure-as-a-Service, die zusammen als Cloud Computing bekannt sind. Ziel dieses Modells ist es bestimmte Teile oder die gesamte Infrastruktur an einen Käufer bereitzustellen [WeXY14, S. 1]. Mittlerweile ist dieses Modell auch in der kriminellen Welt der Ransomware übernommen worden. Der Grund dafür ist, dass die Wirtschaft sich dauerhaft weiterentwickelt, dadurch auch Anzahl der teilnehmenden Parteien, die genutzten Techniken, Fähigkeiten und somit auch die Ziele. An einem Angriff sind somit in der Welt des RaaS mindestens zwei Parteien, aber häufig drei oder mehr, involviert.

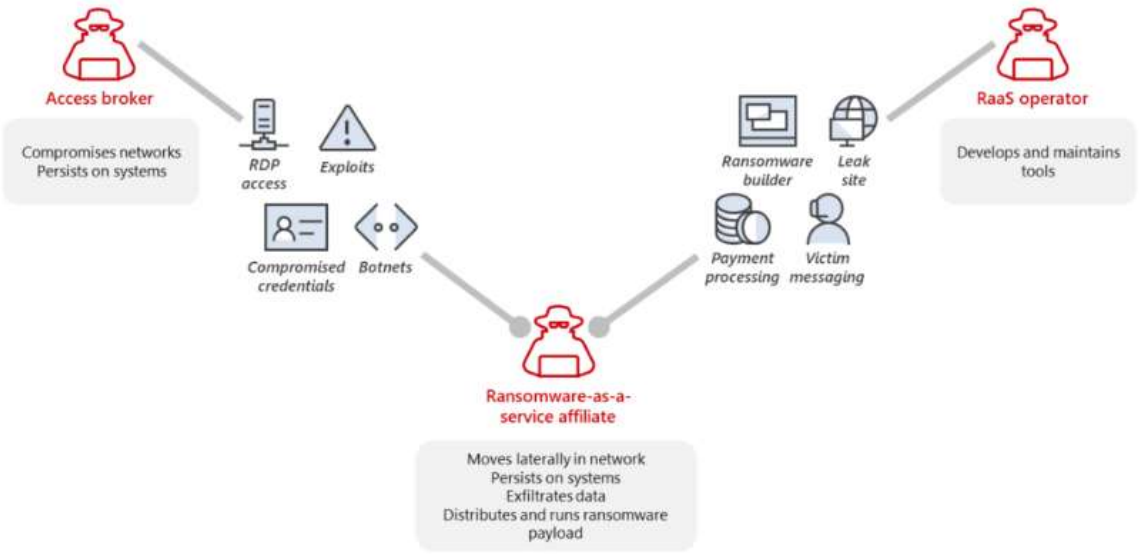


Abbildung 9 – Struktur der RaaS Infrastruktur [Micr22a]

Die Hauptakteure sind wie in Abbildung 9 zu erkennen, die RaaS Betreiber, die Access Broker und der RaaS Partner. Der RaaS Betreiber ist für die Ransomware an sich zuständig, hier wird die Ransomware programmiert und entschieden welche Funktionen die Ransomware erhalten soll. Oft stellen die Betreiber ebenfalls einen so genannten Builder zur Verfügung. Der Builder ist wie ein Baukasten für die Ransomware. So kann der Partner aus den Funktionen entscheiden, was endgültig beim Betroffenen passieren soll, dies wird entweder mit einer Konfigurationsdatei oder einer grafischen Oberfläche ermöglicht [Abra22, Thre22]. Zudem werden Zahlungsplattformen angeboten, welche beim Betroffenen nach dem Angriff angegeben werden, um das Lösegeld zu erhalten. Neben der Zahlungsplattform übernehmen die Betreiber oft das Verhandeln mit den Betroffenen. Zuletzt existieren von den meisten Betreibern Leak Seiten, hier werden die betroffenen Unter-

nehmen aufgelistet, welche sich dazu entscheiden die Lösegeldsumme nicht zu zahlen. Durch die Leak Seiten werden die gestohlenen Daten für dritte zur Verfügung gestellt und zum Kauf angeboten [Wues20]. Die Methode, welche ein Lösegeld fordert und zusätzlich damit droht die Daten zu veröffentlichen, wird Double Extortion genannt, da die betroffenen mit zwei Erpressungen belangt werden, einmal die Daten nicht wiederzubekommen und zweitens die Daten an die Allgemeinheit oder Mitstreiter in der Wirtschaft zu veröffentlichen. Der Access Broker hat die Aufgabe die Netzwerke von Unternehmen zu kompromittieren und diese ebenfalls an jegliche Interessenten zu verkaufen. Zugänge zu den Netzwerken beinhalten unter anderem Zugangsdaten für Remote Desktop Protocol (RDP), VPN-Sitzungen und Zugangsdaten der Benutzer in den Netzwerken. Die Computer, welche den Zugang in das Netzwerk ermöglichen sind meist Teil eines Botnets. Wenn der Partner die Zugänge erworben hat, kundschaftet dieser das Netzwerk und ist für die restlichen Operationen zuständig, bis die Ransomware ausgeführt wurde und die Verhandlungen zwischen den Betroffenen Unternehmen und den RaaS Betreibern stattfinden [Micr22a]. Nach einem erfolgreichen Angriff werden die Gewinne zwischen Betreiber und Partner aufgeteilt [MeBS20, Seite 1]. Da es bei Ransomware um das finanzielle Interesse handelt, ist die Art der Bezahlung ein wichtiger Bestandteil der Branche. In den früheren Stadien der Ransomware wurden die Zahlungen meist direkt auf bestimmte Bankkonten eingezahlt. Solche Zahlungen sind jedoch transparent und lassen sich leicht zurückverfolgen [ZiCh19, Seite 10]. Durch die Entwicklung von Kryptowährungen haben diese einen besonders hohen Einfluss auf den Erfolg von Ransomware gehabt. Da Kryptowährungen einen einfachen Zahlungsprozess bieten, mit den zusätzlichen Eigenschaften von Anonymität und Sicherheit, stellen Kryptowährungen ein starkes Tool dar [HeCC20, S. 3]. Zu den meistgenutzten Kryptowährungen in der Welt der Ransomware finden sich Ethereum, Monero und Bitcoin. Wenn man sich die Daten zu der Anzahl von Ransomware Varianten ansieht (Abbildung 7) und die Daten zur Entwicklung des Bitcoin Preises (Abbildung 10), kann man daraus schließen, dass das Geschäft mit Ransomware sich an den Bitcoin Kurs anpasst [MeBS20].

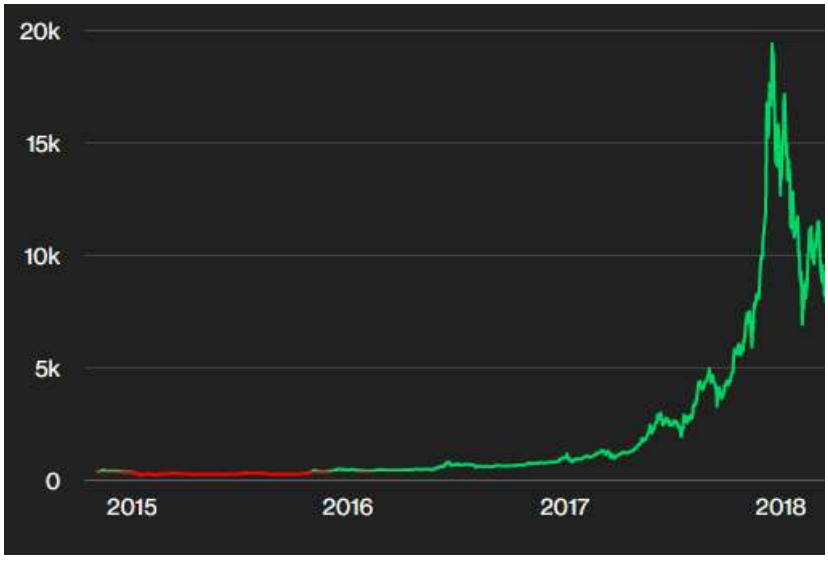


Abbildung 10 – Entwicklung des Bitcoin Preises in USD [Coin23]

Die Höhe der Zahlungen sind bei Privatpersonen meistens um 500$ bis 1000$ angesiedelt, bei Unternehmen werden die Zahlungen meist auf das Unternehmen abgestimmt, hier werden beispielsweise die Umsätze aus den letzten Jahren betrachtet, dabei können die Beträge bis in einen neun-stelligen Bereich gehen [Kasp22, S. 3].

2.3 Cyber Kill Chain

Cyber Kill Chain ist ein verbreitetes Modell in der IT, um Angriffe modellieren zu können und zusätzlich Threat Intelligence und TTPs über die Angreifer zu erstellen, es kann jedoch ebenso für denselben Zweck von Angreifern genutzt werden. [DDBC19, S. 279] denn ursprünglich hat die Kill Chain ihre Herkunft aus einem militärischen Modell, um Ziele zu identifizieren, sich auf den Angriff vorzubereiten, den Angriff durchzuführen und das Ziel zu zerstören [MBMS21, S. 58f.].

Die Cyber Kill Chain hat insgesamt sieben Phasen [DDBC19, S. 280; MBMS21, S. 59; YaRa15, S. 439ff.]:

1. Reconnaissance

Die erste Phase dient der Informationsbeschaffung über das Ziel und erhofft die Entdeckung einer Schwachstelle in deren System oder Infrastruktur.
Es ist möglich diesen Teil in drei weitere Teilaktionen zu unterteilen, Identifikation, Selektion und Profiling. Hauptsächlich wird bei der Informationsbeschaffung das Crawlen von öffentlichen Daten wie Webseiten, Blogs, Soziale Medien und Maillisten genutzt. Viele dieser Informationen, besonders Soziale Medien und Maillisten, werden häufig in späteren Phasen wiederverwendet, um beispielsweise Exploits zu verteilen. Unterschieden wird zwischen passiver und aktiver Reconnaissance. Bei der passiven ist es nicht möglich, dass das Ziel mitbekommt, dass Informationen gesammelt werden, durch die aktive Recon jedoch schon und somit werden möglicherweise Meldungen an das Ziel gesendet.

2. Weaponization

Hier werden bestimmte Programme und Techniken entwickelt, um die gefundene Schwachstelle auszunutzen, auch Exploits genannt. Ein Exploit ist der Teil der „Waffe“, welche für das Ausnutzen der gefundenen Schwachstelle zuständig ist und dabei beispielsweise ein Remote Access Tool (RAT) ausführt.
Ein RAT, ist eine Software, die versteckt auf einem Zielrechner laufen kann, wenn diese ausgeführt wird, und dem Angreifer den Zugang zum System ermöglicht. Hierbei sind Funktionen wie System-Erkundung, Daten hoch- und runterladen, ausführen von Dateien, Keylogging, Bildschirm-, Kamera- und Mikrofonaufnahmen häufig in einem RAT integriert. Mit höheren Berechtigungen auf dem System besteht die Gefahr, dass das RAT sich im Netzwerk ausbreitet, Netzwerkdatenverkehr mitschneidet oder Module installiert, um die

Entdeckung des RATs zu verhindern. Auch bei RATs wird das Client-Server Modell genutzt, hier ist der Client das befallene System, welches die Informationen zum Server meldet. Der Server hat die Funktion die Funktionen des RATs auszuführen. Diese Art von Kommunikation zwischen Client und Server in der Welt der Kriminalität wird Command and Control bzw. C2 oder C&C genannt.
Es existieren Methoden wie ein RAT ohne Exploit genutzt werden kann, jedoch sind diese auf das Ausführen der Benutzer am System angewiesen und da immer mehr Aufmerksamkeit auf das Thema Sicherheit gerichtet wird, sind diese Methoden nicht so zuverlässig wie die Nutzung eines Exploits. Hierzu zählen Beispiele wie das Einbetten eines RAT in Bild/Video/Musik Dateien oder Word/Excel Dokumenten.

3. Delivery

Die Verteilung der Exploits wird geplant, beispielsweise durch Mail. Dabei ist diese Phase eine der kritischen, da es sich hier entscheidet, ob der Angriff weitergeführt werden kann oder nicht. Daher werden die Informationen aus der Reconnaissance Phase genutzt, um die höchstmögliche Erfolgsrate zu erreichen. Des Weiteren ist es risikoreich, da bei dem Verteilen, Spuren hinterlassen werden können. Aus diesem Grund werden meistens Dienste genutzt, welche Anonymität versprechen oder sogar bereits kompromittierte Webseiten und E-Mail Accounts. Somit werden die Spuren nicht direkt auf die Angreifer selbst gelenkt.

4. Exploitation

Für die Exploitation Phase müssen besonders die Phase 2 und 3 erfolgreich angeschlossen werden. So ist der Exploit auf das Zielsystem gelangt und der Nutzer hat die erstelle Datei ausgeführt, was dazu führt, dass die Sicherheitslücke in der dazu passenden Software ausgenutzt wird und das RAT gestartet werden kann, um eine Verbindung zum C2 Server herzustellen. Jedoch muss die Software dazu auf dem System vorhanden sein, es muss eine Version der Software sein, wo die Sicherheitslücke noch nicht behoben wurde und das installierte EDR darf das RAT nicht erkennen und blockieren.

5. Installation

Ziel ist es einen dauerhaften Zugang zum System oder zur Infrastruktur zu erlangen und behalten. Dabei werden so genannte Backdoors erstellt, welche beispielsweise durch die Installation von weitern Tools erfolgen kann. Diese Backdoors sollten bestmöglich nicht von Sicherheits- und Überwachungssystemen entdeckt werden, so ist es möglich als Angreifer heimlich im Netzwerk zu bleiben. Da Malware immer mehr Funktionen über die Zeit erhalten, werden diese meist auch in mehreren Schritten an das befallene System übermittelt. Dropper und Downloaders wurden dafür kreiert die vorhandenen DER zu umgehen oder sie zu deaktivieren und dabei die Malware entweder über externe Seiten herunterzuladen und auszuführen oder den bereits mitgelieferten Schadcode zu installieren und zu starten.

6. Command & Control (C2/C&C)

Diese Phase dient der Kommunikation zwischen installierten Tools und den Angreifern mit dem Ziel, die Kontrolle über das Netzwerk zu gelangen, ebenfalls können Daten darüber exfiltriert werden. Die Kommunikation beinhalten Kommandos mit Befehlen und Aktionen, die auf dem kompromittierten System ausgeführt werden sollen. Da es normaler Netzwerkverkehr ist, ist es möglich die C2 Verbindungen zu erkennen. Jedoch werden immer unterschiedliche Methoden implementiert, die Kommandos und den Netzwerkverkehr zu verstecken. Eine Technik, die genutzt wurde, war es Internet Relay Chats (IRC) zu nutzen und durch die Nutzung von öffentlichen oder privaten Chats den C2 Verkehr zu verstecken. Weitere Techniken sind die Nutzung von TCP, HTTP, FTP oder DNS, welche gewöhnliche Protokolle sind, die überall im Internet genutzt werden.

7. Actions on Objectives

Der letzte Schritt im Angriff ist es seine Aufgabe im Netzwerk, mit der vorhin erlangten Kontrolle durch C2 Server, zu erfüllen. Dabei können gezielte oder Massen Angriffe gestartet werden, beruhend darauf, ob der Angreifer so viel wie möglich kompromittieren möchte, für beispielsweise Bank-, E-Mail-, Social Media-Daten oder die Systeme in Botnetze integrieren möchte, um mit diesen Bots andere Angriffe ermöglichen zu können. Gezielte Angriffe werden ausgeführt, wenn bestimmte Daten gesucht werden, um so lange wie möglich nicht entdeckt zu werden, bevor die Daten gefunden wurden, die der Angreifer haben wollte. Jedoch werden in beiden Angriffsvarianten die Zerstörung in einer Form geplant durchgeführt oder in Kauf genommen.

Basierend auf den obigen Phasen ist es nun möglich ein Modell zu erstellen, welches die Möglichkeit bietet intelligente Gegenmaßnahmen gegenüber den Aktionen der Angreifer zu entwickeln und in deren Infrastruktur zu implementieren, um die Angriffe schnellstmöglich erkennen und verhindern zu können [DDBC19, S. 280].

2.4 Threat Intelligence

In der Lawrence Berkley National Laboratory wurde im Jahr 1986 eine Diskrepanz in der Abrechnung bemerkt, dass jemand die Labor Computer, ohne zu zahlen, genutzt hatte. Da jedoch Einbrüche in Netzwerke nichts Alltägliches waren, und Tools wie tcpdump und nmap, um Netzwerkartefakte zu sammeln, noch nicht existierten, hatte sich keiner etwas dabei gedacht. Cliff Stoll, ein Student, entdeckte jedoch, dass es kein Fehler war, sondern ein Angreifer, der Zugang zu Staatscomputern, sowie White Sands Missle Range und der NSA, erlangt hatte. Dies war möglich, da die meisten Computer im Internet damals zum Staat gehörten. Stoll war es gelungen, durch die vorhandenen Drucker im Netzwerk, die Zeiten zu dokumentieren, wann der Angreifer aktiv war, welche Kommandos der Angreifer absetzte und er hatte herausgefunden, dass eine Sicherheitslücke in einer movemail Funktion ausgenutzt wurde, um Zugriff zum Netzwerk zu erlangen. Da Stoll die Tätigkei-

ten des Angreifers verstand, war es möglich seine nächsten Tätigkeiten vorauszusagen und das Netzwerk zu schützen [BrRo17, Teil 1 Kap. 1].

Die Angreifer zu verstehen, ist einer der kritischen Bausteine der IT-Sicherheit, besonders, weil die Angreifer in den letzten Jahrzehnten gewachsen und sich verändert haben. Dabei wird Threat Intelligence genutzt, mit dem Ziel, die Angreifer mit deren Motivationen, Zielen und Fähigkeiten analysieren zu können. Cyber Threat Intelligence beschäftigt sich mit der Analyse wie die Angreifer den Cyberspace nutzen, um ihre Ziele zu erfüllen.

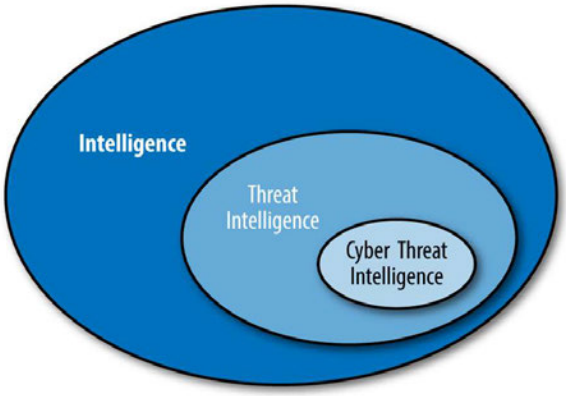


Abbildung 11 – Von Intelligence zu Cyber Threat Intelligence [BrRo17, Teil 1 Kap. 1]

Intelligenz wird als einer der ältesten Konzepte der menschlichen Geschichte angesehen, da Menschen dauerhaft nach Informationen suchen, um beispielsweise den Tag planen zu können. Dabei werden Erfahrungen und Prioritäten mit den externen Daten verglichen und abgewogen, um eine subjektive Entscheidung treffen zu können [BrRo17, Teil 1 Kap. 2]. Bei den Begrifflichkeiten muss man jedoch zwischen Daten und Intelligence unterscheiden, Daten sind Informationen, um Dinge zu beschreiben. Daraus wird Intelligence, nachdem diese Daten gesammelt, bearbeitet und analysiert wurden und im Anschluss als nützlich oder nicht nützlich eingestuft werden, um an die richtigen Interessenten zu gelangen. Somit ist der Unterschied zwischen Daten und Intelligence die Analyse, um die Daten in einen Kontext zu setzen und damit Fragen beantworten zu können [BrRo17, Teil 1 Kap. 2].

„Information on ist own may be of utility to the commander, but when related to other information about the operational environment and considered in the light of past experience, it gives rise to a new unterstanding of the information, which may be termed intelligence.” [BrRo17, Teil 1 Kap. 2]

Der erste Schritt ist es, die Daten zu beschaffen, dafür existieren unterschiedliche Arten von Quellen:

HUMINT wird als Human-Source Intelligence bezeichnet und beschreibt die Intelligenz, welche von Menschen erlangt wurden. Hierbei werden besonders die Interaktionen mit Menschen gemeint.

SIGINT beschreibt die Signal Intelligence und beinhaltet das Abfangen von technischen Signalen, somit wird alles, was innerhalb eines Computers oder Netzwerkes passiert als SIGINT bezeichnet.

OSINT ist die Sammlung von öffentlich zugänglichen Quellen wie Nachrichten und Soziale Medien aber auch viele Quellen, welche nicht klassifiziert werden können, also Open Source Intelligence. Technische Daten wie Domain Namen oder IP-Adressen können ebenfalls zu OSINT gezählt werden, da diese meist öffentlich zugänglich sind.

IMINT wird mit Hilfe von visuellen Repräsentationen erstellt, wie Radar und Photographie. Jedoch wird diese Quelle meist nicht in der Cyber Threat Intelligence genutzt.

MASINT sind Messungen aus technischen Geräten, wie Radio Frequenzen, jedoch nicht, was zu SIGINT und IMINT zugeordnet werden kann. Diese Quelle wird ebenfalls nicht in der Cyber Threat Intelligence genutzt, da sie explizit die SIGINT nicht einbezieht.

GEOINT beinhaltet alle geographischen Daten, wie Satellit, Karten und GPS. Wie IMINT, wird GEOINT ebenfalls nicht direkt für Cyber Threat Intelligence genutzt, jedoch können die Daten eventuell mehr Kontext, zu bereits erhaltener Intelligenz, bieten.

In den letzten Jahren sind noch weitere Quellen wie CYBINT (Cyber Intelligence), TECHNINT (Technical Intelligence) und FININT (Financial Intelligence) erschienen, jedoch ist es möglich die neuen in den bereits oben genannten INT-Quellen unterzuordnen [BrRo17, Teil 1 Kap. 2].

Für die Beschaffung von Intelligenz werden bei Cyber Threat Intelligence noch weitere Quellen hinzukommen, die nicht zu den klassischen Quellen, wie oben genannt, gezählt werden. Meist genutzt, sind die Daten aus bereits geschehenen Untersuchungen und Vorfällen, da hier direkt die genutzten Tools, Techniken und Ziele raus abgeleitet werden können. Honeypots werden beispielsweise dafür genutzt, um Computer und Netzwerke zu simulieren und dadurch Daten zu sammeln, da eventuell Angreifer diese Honeypots angreifen, ohne zu wissen, dass es sich um einen Honeypot handelt. Somit können dieselben Daten wie aus einem echten Angriff gesammelt werden, ohne dass wichtige Systeme tatsächlich angegriffen werden. Zuletzt können noch Daten aus Foren und Webseiten, welche meistens durch das TOR-Netzwerk erreichbar sind, gesammelt werden. Hier werden oftmals zugangsbeschränkte Chaträume und Foren genutzt, um Informationen zwischen Angreifern auszutauschen. Jedoch ist es unmöglich alle Daten aus dem TOR-Netzwerk zu erhalten, da zu viele Seiten existieren, wo solche Daten ausgetauscht werden [BrRo17, Teil 1 Kap. 2]. Es ist dabei angedacht, dass Intelligenz in unterschiedliche Gruppen eingeteilt werden können. Dabei wird zwischen Tactical, Operational und Strategic Intelligence unterschieden.

Bei der Tactical Intelligence werden die kurzlebigen Informationen betrachtet. Zu den Interessenten dieser Daten gehören SOC-Analysten/innen und Incident-Response Teams und die Daten beinhalten Indicator of Compromise (IOC) und TTPs.

In Operational Intelligence werden Daten behandelt, die nicht so granular sind, sondern Überbegriffe der TTPs und Kampagnen der Angreifer, die nicht nur ein Ziel haben, sondern beispielsweise eine gesamte Branche betrifft. Wenn aktiv ausgenutzte Sicherheitslücken zur Tactical Intelligence gezählt wird, würde man das Ausmaß und Verbreitung der Sicherheitslücken in der Operational Intelligence finden.

Zuletzt werden in der Strategic Intelligence die Daten behandelt, welche zur Risikobewertung und Strategien genutzt werden können. So können basierend auf der Technical Intelligence die Strategic Intelligence gebildet werden und beschreiben welche Änderungen in einem Netzwerk oder Infrastruktur durchgeführt werden müssen, um diese Angriffe zu beheben [BrRo17, Teil 1 Kap. 2].

Eine verbreitete Methode wie Daten gesammelt und damit Intelligenz generiert und evaluiert werden kann ist der sogenannte „Intelligence Cycle“.

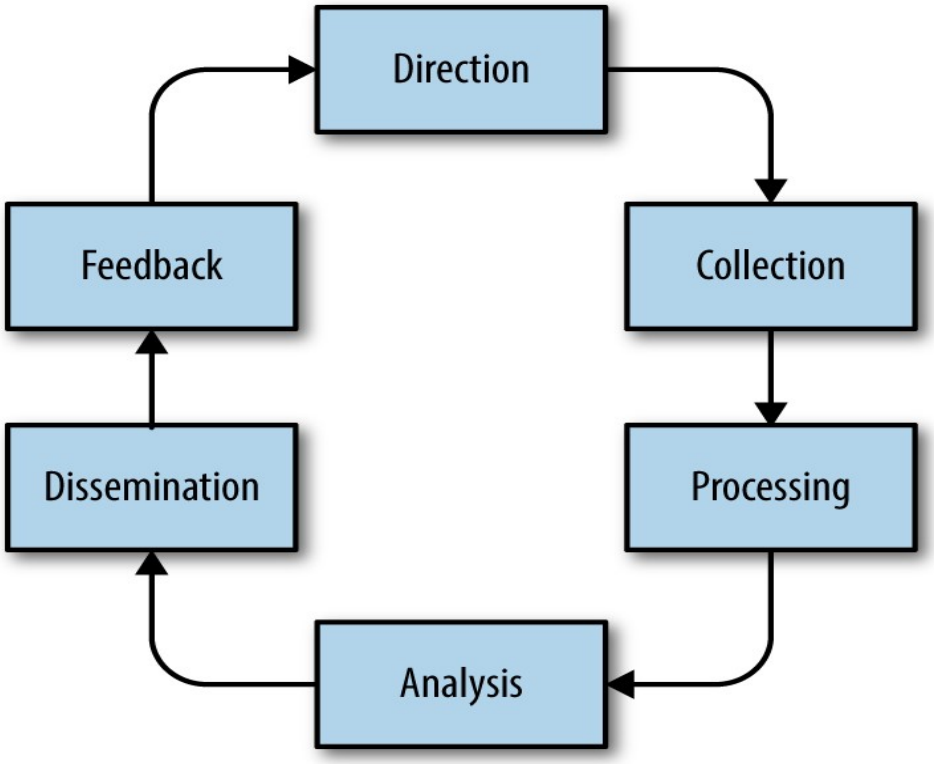


Abbildung 12 - Intelligence Cycle [BrRo17, Teil 1 Kap. 2]

Dieses Modell besteht aus sechs Phasen:

1. **Direction**: Der erste Schritt ist dafür da, eine Frage zu schaffen, die in den nächsten Schritten beantwortet werden soll

2. **Collection**: Daten, die für das Beantworten der Frage benötigt werden, müssen gesammelt werden. Hierbei sind viele Quellen, welche dieselben Informationen enthalten

von großem Wert, da die Informationen dadurch bestätigt werden. Die Schwierigkeit damit kann sein, dass von Anfang an nicht klar ist, welche Informationen nützlich sind und welche nicht. Zusätzlich sollte notiert werden, woher die Informationen bezogen werden, da die Herkunft von Daten mehrmals genutzt werden können, somit hätten Informationen aus unterschiedlichen Quellen keinen höheren Stellenwert mehr. Weiteres ist das Sammeln von Informationen immer ein Prozess und keine einmalige Sache.

3. **Processing**: Um mit Daten zu arbeiten und diese miteinander vergleichen zu können, müssen die Daten in einem einheitlichen Format verfügbar sein. Normalisierung, Indizierung, Übersetzung, Anreicherung, Filterung, Priorisierung und Visualisierung sind die Prozesse, die genutzt werden können, um die Daten miteinander vergleichen zu können. Dabei sollte man den Prozess nutzen, der für die vorhandenen Daten am sinnvollsten ist und sich dabei Zeit nehmen, um die Intelligenz der Daten zu verbessern.

4. **Analysis**: Bei der Analyse wird die Frage aus der ersten Phase beantwortet. Jeder kann dabei ein eigenes Modell zur Analyse erstellen, welches auf die vorhandene Intelligenz angewandt werden kann. Oft muss die Analyse mit unvollständigen Informationen durchgeführt werden, da sollten jedoch die Informationslücken identifiziert und klar aufgezeigt werden, um auf eventuelle Schwachpunkte der Analyse aufmerksam zu machen. Wichtig ist es, dass die Intelligenz Analyse von Menschen durchgeführt werden, da es bei einer Automatisierung zur Phase processing gehören würde.

5. **Dissemination**: Nachdem die Frage beantwortet werden konnte, muss das Ergebnis mit den Interessenten der Frage geteilt werden, da sonst der Prozess der Beantwortung der Frage keinen Wert hat, weil die erschaffene Intelligenz nicht genutzt werden kann.

6. **Feedback**: Beim Feedback wird gefragt, ob die generierte Intelligenz die gestellte Frage erfolgreich beantwortet hat. Dabei kann dies Gelungen sein, wobei der Prozess abgeschlossen werden kann, falls dadurch keine weiteren Fragen und somit einen neuen Prozess gestartet wurde. Ansonsten wird die Antwort mit einem Scheitern bewertet. Beim Scheitern wird die Fragestellung nochmals kritisch angeschaut. Falls das Scheitern an der eventuell nicht konkret gestellten Frage lag, bestimmte Teile der Frage nicht beantwortet wurden oder ob das Sammeln der Daten nicht ausreichend durchgeführt wurde, wird der Prozess am Punkt erneut begonnen, wo der Fehler gefunden wurde [BrRo17, Teil 1 Kap. 2].

2.5 Zusammenfassung der Grundlagen

Für die Sicherheit in einem Unternehmen ist hauptsächlich ein SOC verantwortlich, dabei kann ein SOC eine interne Abteilung sein, aber auch als externer Dienstleister eingekauft werden. Dies spart besonders viel Zeit, da sonst erst die passende Infrastruktur aufgebaut und Mitarbeiter/in mit den richtigen Qualifikationen eingestellt werden müssen.
Die SOC-Analysten/innen arbeiten mit unterschiedlichen Tools wie EDR und XDR, um potenzielle Sicherheitsrisiken stoppen zu können. Dabei sorgt das EDR für eine direkte Sicherheit auf den Endgeräten und meldet dem Benutzer, falls verdächtige Dateien auf dem Gerät gefunden wurden. Das XDR ist einer Erweiterung des EDR und besitzt dieselben Funktionen, wobei zusätzlich noch automatisierte Reaktionen auf dem Gerät ausgeführt werden können. Ebenfalls wird ein XDR deutlich variabler im Netzwerk genutzt und nicht nur auf Endgeräten. Funktionen, wie eine Trennung vom Netzwerk und mehr dynamische Ansätze werden zur Verfügung gestellt. Somit werden noch schnellere Reaktionszeiten geboten.
Ebenfalls werden SIEMs eingesetzt um die gesammelten Events und Logs, von Geräten im Netzwerk, normalisieren, speichern, durchsuchen und visualisieren zu können. Die Events werden bei Windowsmaschinen, welche mit Abstand am meisten genutzt werden, durch das interne Windows Event Log oder Sysmon von Sysinternals an das SIEM übermittelt. Sysmon bietet dabei tiefgründigere Events, die nicht in den standardmäßigen Windows Event Logs vorhanden sind.
Damit Analysten/innen sich um die wichtigsten Geschehnisse in einem Netzwerk kümmern können, werden in SIEMs Regeln erstellt, welche jedes Event überprüfen und bei Übereinstimmungen Meldungen generieren, um bei einer realen Gefahr schnellstmöglich erkannt und behoben werden zu können. Damit Regeln bei SIEMs herstellerübergreifend implementiert werden können, ist es von Vorteil, die Regeln in einem einheitlichen Format namens Sigma zu verfassen und entweder manuell oder automatisiert in das gewollte Format seines SIEMs zu übersetzen. Zusätzlich sollten sich Analysten/innen mit der MITRE ATT&CK befassen und ihre bereits erstellten Regeln auf die ATT&CK Matrix abbilden, so wird auf einem Blick ersichtlich in welchen Bereichen mögliche Angriffe nicht erkannt werden können.
Zusätzlich werden von der MITRE die TTPs von bekannten Angreifern in der ATT&CK Matrix aufgezeigt, wodurch es erleichtert wird seine Abdeckung der Regeln zu verifizieren.
Ein Teil dieser Angreifer sind Ransomware-Gruppen. Dabei ist in den letzten Jahren das Vertriebsmodell RaaS entstanden, wobei Personen diese zur Verfügung gestellte Ransomware mieten können, um eigene Angriffe durchzuführen. Erfolgreiche Angriffe, führen zu verschlüsselten Systemen und verhindern den Zugriff auf die vorhandenen Daten. Um wieder Zugriff zu erlangen, wird Lösegeld von einigen Hundert Euro bis hohen Millionensummen, je nach betroffener Person oder Unternehmen, gefordert. Falls dieses Lösegeld nicht gezahlt wird, besteht die Wahrscheinlichkeit, dass die verschlüsselten Daten, die vor der Verschlüsselung vom Angreifer exfiltriert wurden, auf so genannten Leak-Seiten zum öffentlichen Verkauf gestellt werden. Die Daten können, sowie das Lösegeld, mithilfe von Kryptowährungen gezahlt werden. Kryptowährungen gewährleisten dabei ein

gewisses Maß an Sicherheit und Privatsphäre, welches dazu führt, dass Angreifer durch die Nachverfolgung der Zahlungen nur schwer gefunden und gefasst werden können.
Da jedes Unternehmen irgendwann von Angriffen betroffen ist, ist es empfehlenswert sich von Vornherein zu schützen. Zusätzlich zu der MITRE ATT&CK wird die Cyber Kill Chain genutzt, um das Verhalten der Angreifer zu modellieren. Die Angriffe sollten daher immer in einer der Phasen der Kill Chain erkannt werden, um das Ziel der Angreifer rechtzeitig aufhalten zu können. Die Informationen, mit denen die Angreifer, in Modellen wie die Cyber Kill Chain und der ATT&CK Matrix, abgebildet werden, stammen oft aus einem Prozess, welcher Threat Intelligence genannt wird. Hier werden Daten, die aus unterschiedlichen Quellen stammen zusammengetragen und analysiert. Durch die Analyse stellt der Mensch Zusammenhänge der Daten fest und setzt sie in einen Kontext, welcher diese Daten für den spezifischen Zweck wertvoll macht. Die analysierten Daten in einem Kontext werden dann Intelligenz genannt. Diese Intelligenz kann weiter vertieft werden, indem es in einem bestimmten Thema stattfindet, somit wird aus Threat Intelligence die fachspezifische Cyber Threat Intelligence. Diese Cyber Threat Intelligence wird von Analysten/innen genutzt, um Erkennungsmuster und Regeln zu erstellen.

3 Anforderungsanalyse und Konzept

3.1 Anforderungen

Bei der Planung des Projektes wurde eine Analyse der Anforderungen durchgeführt. Dabei wurde auf die Fragestellung der Arbeit eingegangen und überlegt, wie diese erfolgreich beantwortet werden können. Es soll somit möglich sein, die momentan aktiven Gruppen durch das Recherchieren von öffentlichen Daten ausfindig zu machen. Gleichzeitig müssen diese Daten Informationen dazu liefern, wie aktiv die Gruppen sind, wann, wo und wer angegriffen wird. Dadurch ist es möglich eine Einteilung und Priorisierung der Gruppen durchzuführen. Für die Erkennung der Gruppen ist es notwendig die Taktiken und Techniken der Gruppen zu kennen, diese sollen durch bereits bekannte Angriffe zusammengetragen werden. Zudem könnte es wichtig sein eine längere Zeitspanne der Angriffe zu betrachten, so ist es möglich die Entwicklung der Taktiken und Techniken zu analysieren und sich auf die Methoden mit der höchsten Nutzungsrate zu konzentrieren, um die einzelnen Techniken über einen möglichst langen erkennen zu können.

3.2 Konzept

Die erste Beschaffung von Informationen bezieht sich auf die Frage, welche Gruppen momentan aktiv sind. Hierbei werden Beiträge von bekannten IT-Sicherheitsanalysten/innen, Reports von Unternehmen und Open Source Projekte, die sich mit dem Thema befassen, in Betracht gezogen. Hierbei stammen die Daten oft von Honeypots oder aus bereits durchgeführten Angriffen. Bei diesen Arten von Quellen handelt es sich um OSINT, da diese Daten oft von den Forschern öffentlich zugänglich gemacht werden. Diese Art von Daten werden in die Klasse der Tactical Intelligence Daten eingeordnet, siehe Kapitel Threat Intelligence.
Es existieren Projekte, welche die Recherchen bereits durchgeführt und die bekannten Gruppen zusammengetragen haben.
Falls es sich um eine Gruppe handelt, die das RaaS System nutzt, werden dabei oft die URLs für die entsprechenden Leak-Seiten beigelegt. Die Links werden teilweise von den Gruppen selbst veröffentlicht und ermöglichen so den Zugang zu gestohlenen Daten, welche zum Verkauf angeboten werden [ILAS22].

Nachdem ein Überblick über die Gruppen verschafft wurde, werden Informationen zu den betroffenen Unternehmen benötigt. Die Frage, gegen welche Gruppen man sich schützen soll, soll dadurch beantwortet werden. Zu den benötigten Informationen gehören:

- Wie viele Unternehmen wurden bereits durch die jeweilige Gruppe angegriffen?
- Wo haben die Unternehmen ihre Sitze?

- In welcher Branche sind die Unternehmen tätig?

Durch die Häufigkeit der Angriffe einer bestimmten Gruppe kann man erste Entscheidungen treffen und herausfinden, wie aktiv die Gruppe ist und dadurch erste Schlüsse ziehen, ob diese Gruppe von großem Interesse ist. Der Sitz der betroffenen Unternehmen ist wichtig, um eine geographische Einordnung durchführen zu können. Mit Hilfe von der geographischen Einordnung wird der nächste Schritt der Priorisierung durchgeführt, so kann man sich im folgenden Schritt auf die Gruppen konzentrieren, die im Land tätig sind, wo das Unternehmen selbst agiert.

Der letzte Schritt beinhaltet die Informationen zur Branche der Unternehmen.
Am Ende sollte man höchstens eine Hand voll Gruppen haben, die in letzter Zeit mehrere Unternehmen, aus derselben Region, angegriffen haben. Um die Erkennungsregeln für die bereits bestimmten Gruppen erstellen zu können, werden die genutzten Taktiken und Techniken benötigt. Diese werden ebenfalls aus bereits ausgeführten Angriffen abgeleitet. Hierzu nutzt man ähnliche oder dieselben Quellen wie beim ersten Schritt, nur mit dem Unterschied, dass nach bestimmten Gruppen gesucht wird, die in den vorherigen Schritten gefunden wurden. Gesucht werden die Reports, welche sich auf den genauen Ablauf der Angriffe beziehen und die genutzten Tools, Befehle und Ziele näher beleuchten. Funde aus den Reports werden mithilfe von der MITRE ATT&CK Matrix abgebildet und ermöglichen somit ein ganzheitliches Bild des Angreifers. Ebenfalls ist somit gegeben, die TTPs von allen Gruppen leichter miteinander zu vergleichen und dadurch Überlappungen schnell zu erkennen. Diese Überlappungen sollten mit einer höheren Priorität betrachtet werden, da diese zu einer hoffentlich erfolgreicheren Erkennung führen, denn mit hoher Wahrscheinlichkeit nutzen noch weitere Gruppen diese TTPs, um ihre Ziele zu erreichen. Basierend auf den TTPs können Erkennungsregeln definiert werden und in einer Testumgebung getestet werden. Eine solche Testumgebung besteht dabei aus einem Netzwerk und einigen Systemen, die zur Ausführung der Befehle und Tools genutzt werden, sowie ein SIEM zur Bereitstellung der Events und der Alarmierungen bei einer erfolgreichen Implementation der Erkennungsregeln.

4 Implementation

In diesem Kapitel wird das Konzept aus dem vorrangehenden Teil der Arbeit praktisch umgesetzt und das Vorgehen näher erläutert. Dabei wird auf die spezifische Implementation des Intelligence Cycles in Bezug auf jede Frage aus der Zielstellung der Arbeit eingegangen.

Der Intelligence Cycle beginnt immer mit einer Direction-Phase. Hier wurde überlegt welche Frage zuerst gestellt werden kann, um den Schutz von Ransomware-Gruppen sicherstellen zu können. Dabei wurde die Frage „Welche Ransomware-Gruppen gibt es zurzeit?“ erarbeitet. Mit dieser Frage wird die Collection-Phase eingeleitet und mit Recherchen in Reports von IT-Sicherheitsunternehmen und Leak-Seiten ausgeführt. Anschließend werden die gefundenen Daten zu den Ransomware-Gruppen in der Phase Processing in einem Dokument gespeichert, um die notwendigen Arten des Processing durchführen zu können. Beim Processing wurden die gesammelten Daten dann gefiltert, um die redundanten Daten von unterschiedlichen Quellen zu entfernen. Nach dem Processing müssen die Daten analysiert werden. Dabei werden die Daten in Bezug auf die gestellte Frage von der Direction ausgewertet. Da für diese Arbeit kein direkter Interessent existiert, wird die Dissemination-Phase nicht berücksichtigt, dies wird in den folgenden Prozessen ebenfalls so übernommen. Die letzte Phase dient des Feedbacks für die erarbeitete Intelligenz. Es wird geschaut, ob die Daten ausreichend waren, um die Frage zu beantworten, oder falls Lücken in den Informationen zu finden sind, die zu einem späteren Zeitpunkt ausgebessert und geschlossen werden sollen. Ziel ist es dann eine klare Antwort zu finden, welche diesen Prozess als abgeschlossen sieht, indem die Frage zufriedenstellend beantwortet wurde oder falls dieser Prozess erneut bearbeitet werden muss mit eventuellen neuen Quellen oder einer neuen Formulierung der Frage, da sich diese nicht wie gewünscht beantworten lässt. Zum Schluss dieses Prozesses sollte eine Liste von Ransomware-Gruppen, die Leak-Seiten besitzen, existieren.

Nachdem die Gruppen gefunden wurden, ergibt sich aus den Ergebnissen die Frage "Gegen welche Ransomware-Gruppen soll man sich schützen?". Somit existiert eine neue Frage, wodurch ein neuer Prozess angestoßen wird, welcher mit der Collection-Phase beginnt. Da die Erstellung der Frage in der Direction-Phase nicht mehr notwendig ist, fällt diese Phase weg und wird zukünftig nicht weiter betrachtet, da die Fragen sich aus dem vorherigen Prozess ergeben werden.
Bei der Beschaffung der neuen Daten werden dieses Mal die betroffenen Unternehmen in Betracht gezogen. Diese Unternehmen sollen einen Aufschluss darüber geben, in welchen Regionen der Welt die Gruppen aktiv sind und eventuell auf welche Branchen ein höherer Fokus gelegt wird. Dafür wurden die Leak-Seiten der einzelnen Gruppen genutzt, dabei wird auf eine Technik namens Scraping bzw. Webscraping gesetzt. In dieser Arbeit

wurde das Scraping mittels Python und dem Modul Selenium durchgeführt. Der Begriff wird im Laufe des Kapitels näher erläutert.

Um mit Selenium arbeiten zu können, wird mit Python-Pip das Selenium-Modul installiert [Sele22a], zudem benötigt Selenium einen Treiber für den genutzten Browser. In dieser Arbeit wurde dabei mit dem Firefox Browser gearbeitet [Sele22b]. Da Selenium die Nutzung des Browsers simuliert, können jegliche Browsereinstellungen im Python-Code bestimmt werden. [Sele22c]
Die ganzen Leak-Seiten der Ransomware-Gruppen sind nur im TOR-Netzwerk zugänglich, daher wird noch der Zugang zum TOR-Netzwerk benötigt. Diesen kann man in Linux durch den verwendeten Paketmanager installieren und durch das Starten des TOR-Dienstes wird der Netzwerkverkehr durch das TOR-Netzwerk geleitet und ermöglicht somit den Zugriff auf die Leak-Seiten der Ransomware-Gruppen. Um nun den installierten TOR-Dienst mit Firefox zu nutzen, werden die Proxy-Einstellungen in Firefox geändert,

```
options=Options()
options.set_preference('network.proxy.type', 1)
options.set_preference('network.proxy.socks', '127.0.0.1')
options.set_preference('network.proxy.socks_port', 9050)
options.set_preference('network.proxy.socks_remote_dns', True)
options.set_preference('network.dns.blockDotOnion', False)
```

um den Netzwerk-Verkehr durch den TOR-Dienst zu senden.

Hierbei wird der Proxy aktiviert, die lokale IP-Adresse mit dem Port 9050 des TOR-Dienstes genutzt, zusätzlich wird die Namensauflösung mit DNS durch den Proxy und die Option auf „.onion“ Seiten zugreifen zu können aktiviert [Torp22]. Onion ist dabei die Endung der Webseiten im TOR-Netzwerk. Wenn diese Einstellungen für den Browser gesetzt sind, können die Leak-Seiten der Ransomware-Gruppen gescraped werden.

Beim Scrapen wurden unterschiedliche Arten angewandt, die Informationen zu bekommen, dabei wurden die einzelnen Elemente auf den Seiten unterschiedlich angesprochen. Genutzt wurden der Klassen-Name oder der XPath der Elemente. Die Klassen-Namen werden beim Erstellen der Webseite an Elemente vergeben, dabei können die Klassen der einzelnen Elemente eingesehen werden [Muth22, S. 21]. Eine Webseite besteht dabei aus HTML und wird durch unterschiedliche Bausteine, mit unterschiedlichen Funktionen, aufgebaut. So sieht dann beispielsweise die Unterteilung auf der Leak-Seite von Lockbit aus:

Abbildung 13 – Aufbau HTML Dokument bei Lockbit [Lock23]

Um die gewollten Informationen zu erhalten, kann in Selenium die jeweilige Klasse angesprochen werden. In der Klasse „post-title“ wird hier die Webseite des betroffenen Unternehmens angegeben [Lock23]. Haben die unterschiedlichen Events keine Klasse, ist es möglich die Elemente über den XPath anzusprechen, dieser XPath setzt sich aus den Bausteinen eines XML-Dokuments zusammen, dabei kann das HTML durch XML implementiert werden. Dadurch kann aus dem HTML-Dokument, siehe Abbildung 13, ein XPath gebildet werden. Für den „post-title“ würde der XPath wie folgt aussehen: „/html/body/div[1]/div/div/div/div/div/div/div“. Mit den Klassen und XPaths können nun die gewünschten Informationen automatisch durch Selenium gesucht und gespeichert werden. Bei einigen Leak-Seiten werden Bilder von gestohlenen Dokumenten hochgeladen. Um das Laden der Bilder zu verhindern und somit die Stabilität der Seite zu erhöhen, muss in den Browseroptionen eine weitere Einstellung vorgenommen werden. Hierbei wird die Einstellung

```
options.set_preference('permissions.default.image', 2)
```

gesetzt, wodurch keine Bilder mehr geladen werden [Mozi13].

Zusätzlich zur eigenen Lösung wurde das Produkt „RansomLook“ genutzt, um eine breitere Masse an Informationen zu erhalten. Dadurch wurde eine lokale Instanz der „RansomLook“ Software installiert und konfiguriert [Rans22], aber da diese Software auf einem Server ohne grafische Oberfläche installiert wurde, war es nicht möglich einen Browser auf dem Server zu nutzen, um die bereitgestellte Weboberfläche zu erreichen. Um dies zu umgehen konnte in der Konfigurationsdatei, welche im Ordner „/config“ zu finden ist, der Eintrag für die IP-Adresse geändert werden. Anstatt der vorhandenen 127.0.0.1 wird die privat genutzte IP-Adresse eingetragen, welche im lokalen Netzwerk des Servers erreichbar ist. Somit wurde der Zugriff auf die Oberfläche von anderen Computern ebenfalls ermöglicht. Nach der erfolgreichen Einrichtung erhält man eine Oberfläche mit denselben Informationen, die auf der offiziellen Instanz von „RansomLook“ angezeigt werden, jedoch ist es möglich auf die gesamten Daten im Hintergrund zuzugreifen. Somit konnten die alle Gruppen und die angegriffenen Unternehmen aus einer Datei, welche für die Speicherung

der Informationen zuständig war, ausgelesen werden. Diese Datei ist in einem JSON-Format und erstellt für jedes neue betroffene Unternehmen einen neuen Eintrag.

Nachdem die Beschaffung der Daten für die betroffenen Unternehmen abgeschlossen war, mussten die Daten noch mit Informationen zu der Geolokation und Branche ergänzt werden. Für diese Informationen wurde Google Maps genutzt und wieder mittels Scraping umgesetzt. Dafür werden die einzelnen Elemente der Webseite, wo die Informationen enthalten sind, benötigt. Die Webseite wird manuell geöffnet und eine Suche gestartet, um den Vorgang der Automatisierung zu testen.

Um abschätzen zu können mit welchen Ergebnissen gerechnet werden kann, wurden einige Suchen mit den Namen oder Webseiten der betroffenen Unternehmen durchgeführt. Bei den Suchen wurden drei unterschiedliche Resultate beobachtet:

1. Das Unternehmen wurde gefunden und als einziger Treffer angezeigt. Dadurch erhält man eine Anzeige der Informationen wie Name, Adresse, Branche, Webseite und Telefonnummern. Die Informationen, welche benötigt werden, werden mithilfe von der HTML-Datei ausfindig gemacht und mit dem Klassen-Namen oder XPath identifiziert. So kann die automatische Suche aller betroffenen Unternehmen die Informationen erhalten, wenn nur ein Treffer gefunden und angezeigt wird.
2. Es werden mehrere Treffer bei Google Maps angezeigt. Hier wird eine Liste von möglichen Treffern angezeigt, dabei enthält man möglicherweise die Informationen, wie Name des Unternehmens, Branche, Adresse und Telefonnummer. Jedoch werden hier nur die Straße und Hausnummer des Unternehmens angezeigt.
3. Die Suche konnte keine möglichen Unternehmen finden und es werden keine Treffer angezeigt.

Um nun alle genannten Fälle abzudecken, werden unterschiedliche Methoden für die Automatisierung implementiert. Hierbei wird die Suche auf Google Maps durchgeführt. Nach der Ausführung wird davon ausgegangen, dass ein einzelner Treffer angezeigt wird. Daher werden die Klassen-Namen und XPath Elemente gesucht, als würde nur ein Treffer angezeigt werden. Ist dies der Fall, werden die Informationen zurückgegeben und in das Dokument geschrieben, wo die Daten des betroffenen Unternehmens gespeichert sind. Sollte es nicht der Fall sein wird hier eine Fehlermeldung generiert, da die gesuchten Elemente nicht gefunden werden konnten. Somit wird die Suche so gehandhabt, dass mehrere Treffer angezeigt werden.
Bei mehreren Treffern existieren nun mehrere Elemente derselben Art. Diese Elemente werden in einer Liste aufgezeigt und nach und nach geprüft. Bei dieser Prüfung werden wieder die Elemente für die Adresse und die Branche des Unternehmens gesucht. Jedoch sind dies andere Klassen-Namen und XPaths, da die Anzeige bei mehreren Treffern anders ausfällt. Falls diese Elemente Daten beinhalten, werden diese in das Dokument zu den anderen Informationen des Unternehmens geschrieben. Wenn jedoch keine Daten gefunden wurden, wird der nächste Treffer in der Anzeige in Betracht gezogen. Als letzte

Option werden keine Treffer angezeigt und somit können zu dem jeweiligen Unternehmen, mit dieser Methode, keine weiteren Daten bezogen werden. Dabei wird zuerst getestet, ob nur ein Treffer gefunden wurde, falls dies nicht der Fall ist, wird die Suche gleichermaßen behandelt, als wären mehrere Treffer gefunden worden. Wenn keine Daten zur Adresse und Branche des Unternehmens angezeigt werden, weiß das Programm, dass entweder keine Treffer angezeigt werden oder dass keine Daten, außer dem Namen verfügbar sind. Nach einer erfolgreichen Ausführung des Skripts werden die gesammelten Daten in dasselbe JSON-Dokument geschrieben, wie die Informationen zu den betroffenen Unternehmen.

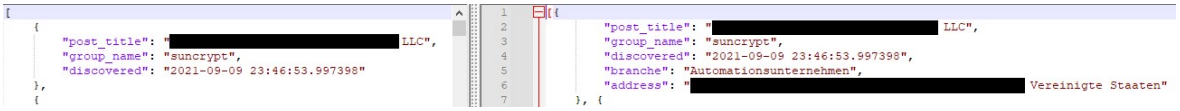


Abbildung 14 – Eintrag eines betroffenen Unternehmens

In der Phase des Processing werden nun die gesamten Daten über die betroffenen Unternehmen gefiltert und indiziert. Gefiltert werden primär die Unternehmen, zu denen keine Informationen gefunden werden konnten. Die daraus entstehenden Daten, werden in ein neues Dokument geschrieben, welches die Indizierung der Daten abdeckt.

Für die Analyse der Daten werden beide Datensätze betrachtet. Als erstes wurden die beiden Dokumente verglichen, um feststellen zu können bei wie vielen Unternehmen keine Daten zu Adresse und Branche zu finden waren. Die Differenz der beiden Listen kann anschließend in die Bewertung der Prioritäten berücksichtigt werden. Dabei wird generell die Rate der Unternehmen bestimmt, zu denen keine Informationen bestimmt werden kann. Anschließend werden für alle Ransomware-Gruppen die betroffenen Unternehmen analysiert, zu denen Informationen verfügbar sind. Bei der Analyse wird zunächst die Lokalisierung in Betracht gezogen. Hier wird nach den Adressen und Namen der Gruppen geschaut. Indikatoren sind hier die Namen des Landes in der Adresse, sowie Länderkürzel der Webseiten. Um zu prüfen, ob ein Unternehmen in Europa säßig ist, wird somit zuerst in der Adresse nach europäischen Ländern gesucht, wenn in der Adresse kein Land angegeben ist, kann nach Anzeichen von bekannten Mustern von Straßennamen oder nach bekannten Städten gesucht werden. Für deutsche Straßen wären das beispielhaft die Namen Straße/Strasse oder Weg.
Teilweise beinhalten die Namen der Unternehmen entweder zusätzlich oder ausschließlich die Webseite, dort kann nach den länderspezifischen Kürzeln in den Webseiten gesucht werden. Ebenso kann nach bekannten Unternehmensformen wie GmbH, Co. KG oder e.V. gesucht werden, diese Indikatoren zeigen an, dass es sich um ein deutsches Unternehmen handelt.
Wie in den beiden vorherigen Prozessen existiert hier kein direkter Interessent. Dadurch werden die Ergebnisse der Analyse-Phase nicht direkt geteilt, sondern es wird direkt die Feedback-Phase eingeleitet. Da durch die Analyse nun Gruppen bestimmt werden können, welche nach den gesammelten Daten in einer gewählten Region tätig sind, wird diese Phase als erfolgreich angesehen.

Mit der neuen Intelligenz aus dem vorangehenden Prozess kann nun die neue Frage „Wie kann man sich gegen diese Gruppen schützen?“ gestellt werden, die sich auf die priorisierten Ransomware-Gruppen bezieht.

In der Collection-Phase dieser Frage werden unterschiedliche Dinge in Betracht gezogen. Um zu wissen, wie die Gruppen arbeiten und ihre Angriffe ausführen, werden die TTPs der Gruppen benötigt. Zusätzlich werden für diese TTPs die spezifischen Methoden der Gruppen gesucht, um diese so gut wie möglich erkennen zu können. Diese Informationen werden von bekannten Unternehmen in der IT-Sicherheitsbranche bezogen, da sie aus bekannten Angriffen stammen.
Nach der Beschaffung der Daten müssen diese in der Phase des Processing indiziert, angereichert, priorisiert und visualisiert werden. Für die Visualisierung und Indizierung werden die Daten in eine Excel-Datei übertragen und in die einzelnen Taktiken eingeteilt. Da die Daten von unterschiedlichen Quellen stammen, werden diese ebenfalls getrennt voneinander eingetragen, um somit die Entwicklung von alten und neuen Angriffen zu unterscheiden. Zusätzlich wird dadurch ersichtlich welche TTPs durch die Weiterentwicklung der Ransomware und der Techniken beibehalten wurden. Auf diese TTPs sollte dann besonderen Fokus gelegt und priorisiert werden. Die Anreicherung der Daten erfolgt durch dieselben Quellen, dabei werden zu den einzelnen TTPs die dazugehörigen Kommandos und genutzten Tools mit indiziert.

	A	B	C	D	E	F	G	H	I	J
1		Count	TTP	Lockbit NCC	Lockbit	Old Lockbit	BlackBasta	BlackBasta TM	Hive	Old Hive
2	Account Discovery	3	T1087				Domain Discovery			
10	Debugger Evasion	2								
11	Domain Trust Discovery	1								
12	File and Directory Discovery	4	T1083							
15	Network Share Discovery	3	T1135							
18	Peripheral Device Discovery	1								
20	Process Discovery	3	T1057							
22	Remote System Discovery	5	T1018							
24	System Information Discovery	3	T1082							
26	System Network Configuration Discovery	1								
27	System Network Connections Discovery	2								
29	System Service Discovery	1								
31	Virtualization/Sandbox Evasion	1								

Abbildung 15 – Auswertung der TTPs

In der Analyse werden die Tabellen der einzelnen Taktiken und dazugehörigen Techniken ausgewertet. Dabei werden die TTPs betrachtet, die durch mehrere Gruppen und über einen längeren Zeitraum genutzt wurden. Diese TTPs werden anschließend hervorgehoben, siehe Abbildung 15. Durch das Zusammentragen der TTPs und Priorisierung der meist genutzten, kann die Frage als erfolgreich beantwortet angesehen werden. Der nächste Schritt besteht darin, die Suchen und Erkennungsregeln basierend auf den Tools und Befehlen zu bauen. Diese werden genutzt, um die Tools und Befehle in einem SIEM zu erkennen. Bei der Erstellung von Suchen und Regeln ist es notwendig, dass die Befehle oder Tools ausgeführt werden. So werden die benötigten Events auf dem System generiert und in das SIEM weitergeleitet. Um die passenden Events zu finden, wird eine Suche im SIEM durchgeführt, welche die Quell-IP des Test-Systems beinhaltet und der Zeitraum so konfiguriert, dass keine älteren Events gefunden werden. Durch diese Art von Filterung

der Events sollten nun jene angezeigt werden, die zur Ausführung des Befehls oder Tools gehören. In diesen Events werden nun die einzelnen Bestandteile betrachtet, welche die Art des Events beschreiben. Eine der wichtigsten Informationen sind die Event IDs, da diese aussagen, ob es sich beispielsweise um eine Ausführung eines Programms bzw. Befehls handelt, oder eine Netzwerkverbindung getätigt wurde. Nachdem die dazugehörigen Events gefunden wurden, muss der Inhalt dieser analysiert werden. Dabei sollten Indizien gefunden werden, die mit dem Befehl oder Tool zu tun haben. Merkmale dabei sind die Namen, das Verzeichnis, aus dem das Tool oder der Befehl ausgeführt wurde und eventuelle CMD-Parameter bei Befehlen in PowerShell oder der CMD. Wenn diese Indizien in den einzelnen Events gefunden wurden, können diese nun durch Filter in die Suche implementiert werden, um ausschließlich die Events zu sehen, die einer bestimmten Aktion zugeordnet werden können. Zum Schluss können diese Suchen als Erkennungsregel im jeweiligen SIEM implementiert werden, um zukünftige Aktionen zu erkennen.

5 Evaluation

In diesem Kapitel werden die Ergebnisse aus den unterschiedlichen Prozessen aufgezeigt und ausgewertet.

Der erste Prozess beschäftigte sich mit der Frage „Welche Ransomware-Gruppen gibt es zurzeit?“

Um die momentan aktiven Gruppen zu finden, wurde nach den Leak-Seiten der Raas Gruppen gesucht und einige mögliche Quellen gefunden. Für den ersten Überblick der Gruppen wurden Sicherheitsreports von bekannten Unternehmen in der IT-Sicherheitsbranche, wie Kaspersky, Sophos, PaloAlto und SentinelOne ausgewertet. Bei den Reports wird allerdings häufig nur auf die größeren Gruppen eingegangen, wie sich herausgestellt hatte. Dadurch mussten zusätzliche Tools genutzt werden, welche diese Recherche bereits übernommen haben und Listen von den aktiven, aber auch von älteren Gruppen bereitstellen. Die Dienste, welche hier genutzt wurden, sind „ecrime.ch“, „RansomWatch“, „RansomLook“ und „darkfeed.io“.

Bei „darkfeed.io“ werden Gruppen dargestellt mit der Anzahl an Angriffen in einer bestimmten Zeit, die betroffenen Länder und Neuigkeiten mit Threat Intelligence Daten. In einer tabellarischen Darstellung werden die unterschiedlichen Gruppen aufgelistet. Die Informationen, die man erhält, sind: Name, Anzahl der Opfer, Namen des letzten Opfers und den Link mit einem Status zur Leak-Seite, die im TOR-Netzwerk erreicht werden kann. Aufgelistet sind hier 38 unterschiedliche aktive Gruppen [Dark23].

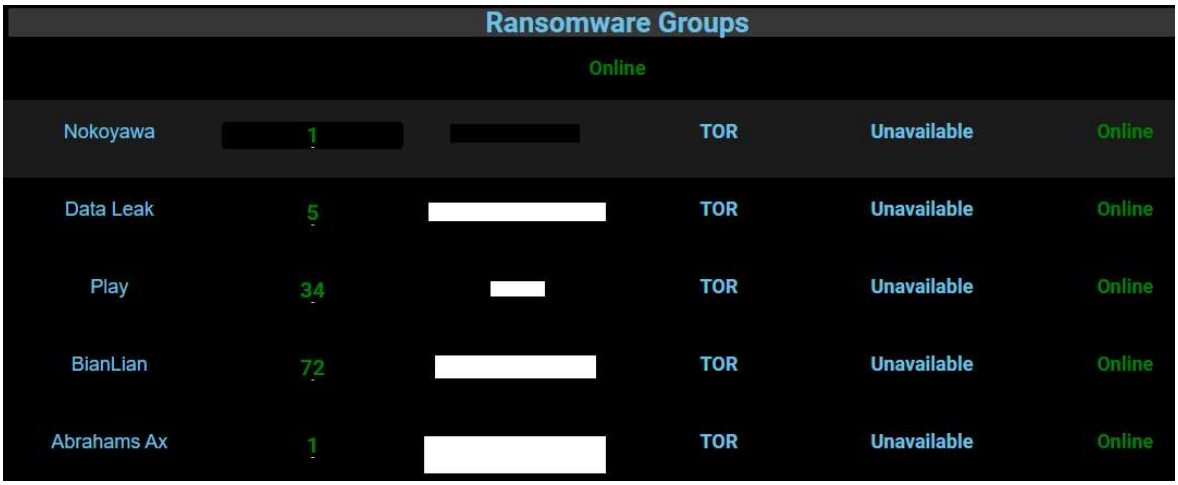


Abbildung 16 – Übersicht auf darkfeed.io [Dark23]

„Ecrime.ch“ stellt auf deren Webseite kleine Screenshots von den bekannten Leak-Seiten von Ransomware-Gruppen zur Verfügung, dabei werden bei der Vorschau 67 Gruppen gelistet [Ecri23].

„RansomWatch“ und „RansomLook“ sind Open-Source Projekte, die auf GitHub veröffentlicht wurden, um die Leak-Seiten der Gruppen zu scrapen und den Nutzern die Informationen in einem Webinterface zur Verfügung zu stellen. Bei „RansomWatch“ werden zum Zeitpunkt des Schreibens 131 Seiten von Gruppen überprüft, davon sind 91 Seiten aktiv, jedoch haben viele Gruppen, aus Redundanz Gründen, mehrere Leak-Seiten [Rans23a]. Im Vergleich werden bei „RansomLook“ 43 Seiten aktiv überprüft [Rans23b]. Durch die Auswertung der Daten ergibt sich eine Liste von insgesamt 123 Ransomware-Gruppen mit Leak-Seiten, jedoch stellen die Dienste teilweise die Information zur Verfügung, wann der letzte Zugriff auf die Leak-Seite geschehen ist. Wenn diese klar als offline gekennzeichnet wurde oder die Seite über einen langen Zeitraum nicht mehr erreichbar war, kann davon ausgegangen werden, dass die Gruppe nicht mehr aktiv ist und kann so aus den folgenden Betrachtungen herausgenommen werden. Die gesamte Liste der Namen der gesammelten Ransomware-Gruppen ist in den Anlagen „Ransomware-Gruppen“ zu finden.

Gegen welche Ransomware-Gruppen soll man sich schützen?

Durch die Collection-Phase aus dem ersten Prozess wurden die Open-Source Projekte „RansomLook“, „RansomWatch“ und das Projekt „darkfeed.io“ betrachtet. Bei „darkfeed.io“ wird das letzte betroffene Unternehmen einer Ransomware-Gruppe aufgelistet. Um aber die Ransomware-Gruppen genauer einordnen zu können, ist es notwendig nicht nur das letzte Opfer zu kennen, sondern Zugriff auf historische Daten mit bereits betroffenen Unternehmen zu haben. Da dies nicht möglich ist, werden die bereitgestellten Daten von „darkfeed.io“ nicht weiter betrachtet [Dark23]. Jedoch stellt „darkfeed.io“ von den aufgelisteten Ransomware-Gruppen die jeweiligen Leak-Seiten im TOR-Netzwerk zur Verfügung. Mit diesen Links ist es möglich, die auf den Seiten verfügbaren Informationen zu sammeln. Um einen Überblick zu erhalten, wurden sieben von den eher aktiveren Gruppen, laut „darkfeed.io“, ausgesucht, um die Leak-Seiten zu betrachten. Diese Gruppen waren BlackBasta, Blackcat, Cl0p, Hive, Lockbit, Ransomexx und Revil. Auf den Seiten dieser Gruppen werden die erfolgreich angegriffenen Unternehmen aufgelistet mit weiteren Informationen zu den jeweiligen Unternehmen. Dabei beinhalten die Informationen meistens einige interne Dateien, die Menge an exfiltrierten Daten, einen Preis, um die gesamten Daten zu erhalten, Name des Unternehmens und bei vereinzelten Gruppen werden auch Informationen wie Webseite, E-Mail, Telefonnummer und Adresse angegeben, ein Beispiel dafür ist die Gruppe BlackBasta.

Um mit den wichtigen Informationen arbeiten zu können, die auf den Leak-Seiten bereitgestellt wurden, wurde eine Technik namens Scraping genutzt, welche diese Informationen sammelt.

„Scraping is the process of extracting, copying, screening, or collection data. Scraping or extracting data from the web […] is normally termed web scraping." [Chap19, S. 8]

Es wird dafür genutzt, Informationen für einen besonderen Zweck zu sammeln. Da sich Informationen sehr schnell ändern, aber auch die Menge ständig wächst, ist es nötig die Beschaffung dieser zu automatisieren. Daher ist scrapen ein wichtiger Prozess für viele Teile der Industrie [Chap19, S. 8]. Genutzt wurde Selenium, da es einen Webbrowser emuliert und dieselben Aktionen durchführt wie ein Mensch, dadurch ist es möglich bestimmte Probleme, wie bestimmte HTTP-Fehler oder das Blockieren von automatisierten Lösungen mit BeautifulSoup, zu umgehen. BeautifulSoup kann ebenfalls für Scraping genutzt werden, hier wird jedoch der Zugriff nicht emuliert und automatisch erkannt und blockiert werden kann [SSDG22, S. 2], daher wurde dies nicht als priorisierte Methode genutzt.

Durch die große Anzahl an Gruppen wäre der Zeitaufwand, diese 123 Gruppen zu überwachen und die Informationen durch personalisierte Skripte zu sammeln, zu groß gewesen. Dies wurde klar, nachdem der Aufwand für die sieben beispielhaften Gruppen im ersten Prozess bereits groß war. Dazu kamen noch Probleme wie Captcha Abfragen auf einigen Seiten, welche dazu geführt haben, dass eine Implementation für eine Lösung dieser Captchas noch mehr Zeit in Anspruch genommen hätte. Deshalb wurde entschieden, die Daten durch das bereits vorhandene Projekt „RansomLook" zu nutzen.
Die einzelnen Einträge bei RansomLook enthalten den Namen der Ransomware-Gruppe, Datum und Uhrzeit der Veröffentlichung des Eintrags und den Namen des betroffenen Unternehmens. Somit gab es zum Zeitpunkt der Bearbeitung 5499 Einträge von unterschiedlichen Gruppen in „RansomLook". Des Weiteren mussten aus den nun vorhandenen Daten die geographische Einordnung der betroffenen Unternehmen hervorgehen. Da diese nur von bestimmten Ransomware-Gruppen zur Verfügung gestellt wurden, müssen diese anderweitig beschafft werden.
Gesucht wurde hier nach einer Quelle, welche eine hohe bis weltweite Abdeckung hat. Durch diese Voraussetzung wurden Quellen wie das deutsche Handelsregister ausgeschlossen.
Es existiert ein europäisches Portal für die Handelsregister der gesamten EU, jedoch würde hier die Implementation einer automatisierten Lösung zu lange dauern, da hier nach jeder Suche ein Captcha ausgefüllt werden muss, was technisch bewältigt werden müsste. Zu dem kommt noch, dass eine Eingabe, welche nicht genau dem Firmennamen entspricht, zu keinem Treffer führen würde.
Als dritte Option wurde Google Maps für die Beschaffung der weiteren Daten ausgewählt. Bei Google Maps kann jedes Unternehmen seine Präsenz selbst aufbauen und die gewünschten Informationen wie Adresse, Kategorie bzw. Branche, Webseite und Telefonnummer angeben [Goog]. Dies machen viele Unternehmen, um deren Online-Präsenz zu stärken. Dadurch existiert auf Google Maps eine große Datenbank an Unternehmensinformationen, welche Unternehmen auf der gesamten Welt beinhaltet. Zwar stellt Google Maps ein Application Programming Interface (kurz: API) zur Verfügung, das mit einem

Client in Python angesprochen werden kann, allerdings wird für die API von Google Maps Places ein bestehendes Abonnement benötigt, welches kostenpflichtig ist. Daher ist die Google Place API keine Option für diese Arbeit [Goog23]. Jedoch besteht die Option, wie bei den Leak-Seiten der Ransomware-Gruppen, mit der Methode des Webscrapings die Informationen zu erhalten.
Bei Google Maps existieren unterschiedliche Anzeigemöglichkeiten für die Suchergebnisse, daher mussten die drei Anzeigemöglichkeiten betrachtet und in einem Skript abgedeckt werden. Bei der Anzeige von mehreren und keinem Treffer wird die Seite mit der gleichen Liste angezeigt, bei einem Szenario ist diese Liste voll und bei dem anderen leer. Da aber das Skript nicht weiß, ob die Liste leer ist, wird diese immer als voll behandelt und wenn nach fünf potenziellen Treffern keine Daten gefunden wurden, wird die Liste als leer betrachtet. Dieses Vorgehen musste so umgesetzt werden, da die Möglichkeit besteht, dass in den ersten Treffern keine Daten eingetragen waren. Somit konnte nicht direkt gesagt werden, dass die Liste leer ist, da in späteren Treffern eventuell noch Daten vorhanden sind. Bei der manuellen Suche von Unternehmen konnte hier beobachtet werden, dass die Ergebnisse nach etwa fünf Treffern immer irrelevanter wurden und somit der Schwellenwert von fünf für einen Abbruch im Skript eingeführt wurde.
Beim Scrapen der zusätzlichen Informationen ist das Skript in einen Fehler gelaufen, welcher nicht behoben werden konnte, dadurch wurde die Liste, welche alle betroffenen Unternehmen enthielt, in kleinere Dateien mit jeweils 50 Unternehmen unterteilt, um die Fehler auf das fehlhafte Dokument runterbrechen zu können. Dadurch wurden zwei Dokumente als fehlerhaft identifiziert und konnten deshalb nicht ausgewertet werden.

Nach dem Scrapen wurden die Unternehmen, die keine Informationen zu Adresse und Branche enthalten herausgefiltert, weil eine Einordnung in entsprechende Branchen und eine Lokalisierung nicht möglich ist und diese Daten dadurch nicht vergleichbar sind. Übriggebliebene Unternehmen wurden in eine gesonderte Datei geschrieben. Somit ist der Vergleich zwischen allen Unternehmen mit Adresse und Branche möglich. Um alle angegriffenen Unternehmen einer Gruppe zu sehen, wurden diese mit folgendem Befehl herausgefiltert:

```
cat all_victims.json | grep “gruppenname” -B 1 -A 1  >> “gruppen-
name”_victims.txt
```

Des Weiteren wurde dies ebenfalls mit den Daten gemacht, die durch Google Maps angereichert wurden:

```
jq . posts* | grep “gruppenname” -B 1 -A 3 >> “gruppen-
name”_victims_enriched.txt
```

Zuletzt wurden daraus die Unternehmen gefiltert, welche keine Adresse oder Branche eingetragen hatten:

```
tac | sed '/null/I,+5 d' "gruppenname"_victims_enriched.txt >>
"gruppenname"_mod.txt
```

Bei der Analyse der erhaltenen Daten in der Datei „gruppenname“_mod.txt kann der Schluss gezogen werden, dass die Gruppen Lockbit, HiveLeak und BlackBasta in Europa am aktivsten sind.
Lockbit hat 336 Unternehmen auf deren Seite gelistet, davon konnten bei 229 Unternehmen eine Adresse und Branche festgestellt werden, dies ist ein Prozentsatz von ca. 68%. Von diesen 229 Unternehmen konnten in der Analyse 67 Unternehmen Europa zugeordnet werden. Dies beträgt einen Anteil von ca. 29%.
Bei BlackBasta konnten bei insgesamt 142 Einträgen auf deren Leak-Seite 102 Unternehmen mit Adresse und Branche automatisch angereichert werden. Dabei konnten 36 Europa zugeordnet werden, das ergibt einen Prozentsatz von etwa 35%.
Die letzte Gruppe, welche in dieser Arbeit weiter betrachtet wurde, ist HiveLeak. Bei dieser Gruppe wurden auf der Leak-Seite 187 betroffene Unternehmen gefunden. Davon konnten 121 eine Adresse und Branche zugeordnet werden. 32 Unternehmen wurden als europäisch identifiziert und somit ergibt sich etwa ein Prozentsatz von 26%.

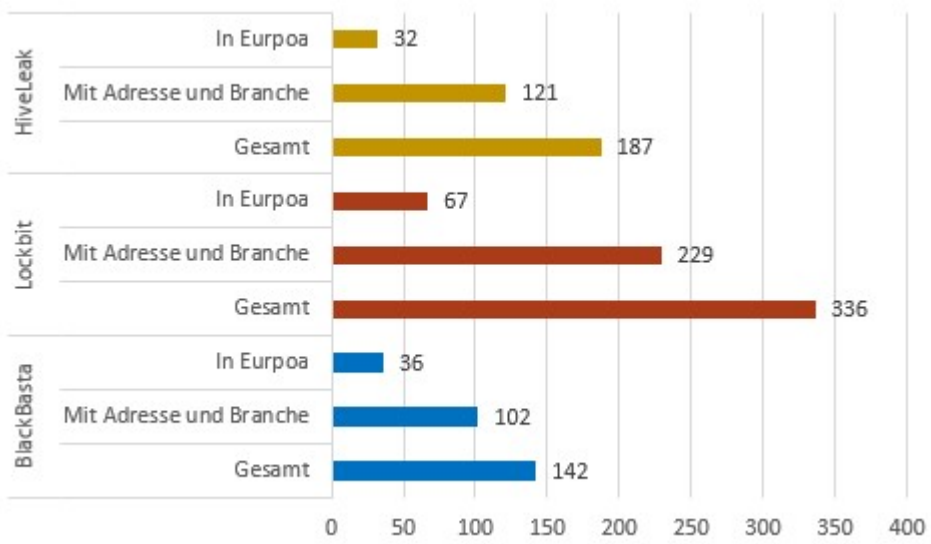


Abbildung 17 – Vergleich der Betroffenen Unternehmen

Durch die manuelle Analyse der Daten ist auffällig geworden, dass die Branchen, welche in der Collection-Phase gefunden wurden, sich nicht für eine gute Einordnung und Priorisierung eignen. Das liegt daran, dass diese Angaben zu spezifisch angegeben werden oder bei Unternehmen mit mehreren Standorten die Branche "Geschäftsstelle" angegeben wird, welches keine Aussage zur eigentlichen Branche tätigt. Des Weiteren ist bei einigen Testläufen aufgefallen, dass in mehreren Abläufen unterschiedliche Informationen zu Unternehmen gefunden wurden. Da drei Ransomware-Gruppen trotz teilweise fehlender Daten priorisiert werden konnten und mithilfe von externen Recherchen zu dem Thema ähnliche Ergebnisse, mit kleineren Abweichungen, dieselben priorisierten Gruppen festgestellt werden konnten, wird dieser Prozess als erfolgreich angesehen.

Diese drei Ransomware-Gruppen wurden für weitere Recherchen betrachtet und die TTPs, sowie die Befehle und Tools der spezifischen Gruppen zusammengetragen. Die TTPs für die Gruppe BlackBasta sehen wie folgt aus [CoPi22, S. 5ff.; Elsa22; Tren22]:

Initial Access: Der Angreifer versucht ins Netzwerk zu gelangen.

1. Phishing: Angreifer sendet Nachrichten, um Zugriff zu Systemen zu bekommen.
2. Valid Accounts: Angreifer bekommt Zugriff zu funktionierenden Zugangsdaten und nutzt diese bei Angriffen.

Execution: Der Angreifer versucht schadhaften Code auszuführen.

1. Command and Scripting Interpreter: Angreifer nutzt vorhandene Interpreter aus, um Kommandos, Skripte oder Binärdateien auszuführen.
    a. Powershell
    b. Windows Command Shell (CMD)
2. System Services: Angreifer nutzt System Dienste aus, um schadhafte Programme oder Befehle auszuführen.
3. Windows Management Instrumentation (WMI): Angreifer führt Code mit dem WMI-Tool in Windows aus.

Persistence: Der Angreifer versucht seinen Zugang zum Netzwerk/System beizubehalten.

1. Account Manipulation: Angreifer bearbeitet bestimmte Eigenschaften eines Benutzerkontos, sowie das Passwort oder die zugeteilten Gruppen und Berechtigungen.
2. Create Account: Angreifer erstellt neue Benutzer, die für beispielsweise für einen zweiten Zugang zu Systemen dienen können.
3. Create or Modify System Process: Angreifer erstellt systemweite Prozesse, die beim Starten des Systems ebenfalls gestartet werden, um einen dauerhaften Zugang zum System zu erhalten.
4. Scheduled Task/Job: Angreifer erstellt Scheduled Tasks, um Prozesse in einem bestimmten Intervall zu starten.
5. Valid Accounts

Privilege Escalation: Der Angreifer versucht mehr Rechte zu erlangen.

1. Create or Modify System Process
2. Domain Policy Modification: Angreifer modifiziert Einstellungen in der Domain, um bestimmte Ziele zu erreichen.
3. Exploitation for Privilege Escalation: Angreifer nutzt Sicherheitslücken in Software aus, um beispielsweise schadhaften Code ausführen zu können oder Zugriff auf Systeme zu erhalten.
4. Valid Accounts

Defense Evasion: Der Angreifer versucht von Sicherheitsmechanismen nicht entdeckt zu werden.

1. Debugger Evasion: Die Software des Angreifers erkennt automatisch die Versuche des Debuggings, um die Funktionalität der Software zu verstehen.
2. Deobfuscate/Decode Files or Information: Angreifer verschleiert Dateien oder Informationen, um eine Analyse dieser Artefakte zu erschweren.
3. Domain Policy Modification
4. Hijack Execution Flow: Angreifer nutzt die Technik aus, welche genutzt wird, um Programme zu starten und kann so schadhaften Code in diesen Prozess einschleusen.
5. Impair Defenses: Angreifer modifiziert Komponenten in einer Umgebung, um diese daran zu hindern defensive Maßnahmen ergreifen zu können.
    a. Disable or Modify Tools: Angreifer deaktiviert oder verändert Tools, die für die Erkennung von sicherheitsrelevanten Aktionen verantwortlich sind.
    b. Safe Mode Boot: Angreifer startet das System in einem abgesicherten Modus, da gewisse Dienste nicht gestartet werden und der Schutz des Systems dadurch geschwächt wird.
6. Indicator Removal: Angreifer entfernt Artefakte auf den Systemen, um deren Spuren zu verwischen.
    a. File Removal: Angreifer entfernt die genutzten Dateien.
7. Modify Registry: Angreifer bearbeitet Einträge in der Registry, um Konfigurationen zu verschleiern oder Informationen zu entfernen.
8. Reflective Code Loading: Angreifer kann hierdurch die Ausführung von Code verschleiern, da dies direkt im Arbeitsspeicher passiert und somit keine Artefakte auf dem System hinterlässt.
9. System Binary Proxy Execution: Angreifer nutzt systemeigene Programme, um durch diese den eigenen Code auszuführen, welche eine signaturbasierte Erkennung aushebelt, da nur die Signaturen der internen Programme geloggt werden.
10. Valid Accounts

Credential Access: Der Angreifer versucht Benutzernamen und Passwörter zu erlangen.

1. Credentials from Password Stores: Angreifer beschafft sich Zugriff für bekannte Orte an denen Passwörter gespeichert werden.
2. OS Credential Dumping: Angreifer erstellt Kopien von Passwörtern, die auf den Systemen hinterlegt sind.

Discovery: Der Angreifer versucht einen Überblick von der Infrastruktur zu bekommen.

1. Account Discovery: Angreifer sucht nach Listen von bekannten Nutzernamen im Netzwerk.

2. Debugger Evasion: Angreifer versucht durch unterschiedliche Methoden die vorhandenen Debugger zu identifizieren, um diese zu einem späteren Zeitpunkt zu umgehen.
3. File and Directory Discovery: Angreifer sucht auf Systemen und Netzlaufwerken nach spezifischen Dateien und Ordnern, welche nützliche Daten, wie Passwörter oder Erpressungsmaterial, enthalten können.
4. Remote System Discovery: Angreifer versucht eine Liste von genutzten IP-Adressen im Netzwerk zu erstellen oder durch Netzwerkscanner und interne Programme zu erhalten.
5. System Information Discovery: Angreifer versucht detaillierte Informationen über das System herauszufinden, dazu gehören Betriebssystem, genutzte Software und deren Versionen, installierte Updates und die genutzte Hardware.
6. System Network Configuration Discovery: Angreifer versucht Details über das Netzwerk und dessen Konfiguration zu erhalten.

Lateral Movement: Der Angreifer versucht sich in der Infrastruktur zu bewegen und zu verbreiten.

1. Lateral Tool Transfer: Angreifer nutzt Tools, um Aktionen zwischen unterschiedlichen Systemen durchzuführen, wie Dateien zu kopieren oder Befehle auszuführen.
2. Remote Services: Angreifer benutzt valide Benutzerkonten, um sich mit diesen Nutzern im Netzwerk auf anderen Systemen anzumelden, dies geschieht mit Tools wie SSH, Telnet, Remote Desktop Protocol (RDP) oder weiteren nachinstallierten Tools.
    a. Remote Desktop Protocol (RDP)

Collection: Der Angreifer versucht Daten von Interesse zu finden und sammeln.

1. Active Collected Data: Angreifer verschlüsselt oder komprimiert Dateien, bevor diese aus der Infrastruktur entwendet werden.
    a. Archive via Utility: Die Verschlüsselung oder Komprimierung wird mittels installierter Programme durchgeführt.

C&C: Der Angreifer versucht mit den übernommenen Systemen zu kommunizieren und diese zu kontrollieren.

1. Encrypted Channel: Angreifer kann zusätzliche Verschlüsselungen nutzen, um deren Netzwerkverkehr zusätzlich zu verschleiern.
2. Remote Access Software: Angreifer nutzt weit verbreitete Software, wie TeamViewer, AnyDesk und LogMein, um Systeme zu kontrollieren.

Exfiltration: Der Angreifer versucht die gesammelten Daten zu entwenden.

1. Exfiltration Over C2 Channel: Angreifer entwendet Daten über die bereits bestehende C2 Verbindung, indem die Daten in den gewöhnlichen Netzwerkverkehr integriert werden.
2. Exfiltration Over Web Service: Angreifer nutzt weit verbreitete Dienste im Internet, um dort die geklauten Daten hochzuladen.

Impact: Der Angreifer versucht die Systeme und Daten zu manipulieren, stören und zerstören.

1. Data Encrypted for Impact: Angreifer verschlüsselt die geklauten Daten, um diese für den Nutzer unzugänglich und unbrauchbar zu machen.
2. Defacement: Angreifer verändert das optische Aussehen, durch beispielsweise das Ändern des Hintergrundbildes.
3. Inhibit System Recovery: Angreifer löscht interne Dienste, welche das Wiederherstellen des Systems erschweren.
4. Service Stop: Angreifer deaktiviert Dienste für alle Nutzer auf einem System, um die Bedienung einzuschränken.

Die nächste Gruppe ist Lockbit und um einen Überblick der TTPs zu erhalten, wurden diese ebenfalls zusammengetragen [Tida22; Rift22; Walt22]:

Initial Access: Drive-by Compromise; Exploit Public-Facing Application; External Remote Services; Valid Accounts

Execution: Command and Scripting Interpreter: Powershell, Windows Command Shell (CMD); Inter-Process Communication; Native API; Scheduled Task/Job; Serverless Execution; System Services; User Execution; Windows Management Instrumentation:

Persistence: Account Manipulation; Boot or Logon Autostart Execution: Registry Keys, Startup Folder; Create or Modify System Process; External Remote Services; Scheduled Task/Job; Valid Accounts

Privilege Escalation: Abuse Elevation Control Mechanism: Bypass UAC; Access Token Manipulation; Boot or Logon Autostart Execution; Create or Modify System Process; Process Injection; Scheduled Task/Job; Valid Accounts

Defense Evasion: Abuse Elevation Control Mechanism; Access Token Manipulation; Debugger Evasion; Deobfuscate/Decode Files or Information; Impair Defenses: Disable or Modify System Firewall, Disable or Modify Tools, Disable Windows Event Logging, Safe Mode Boot; Indicator Removal: Clear Windows Event Logs, File Removal; Masquerading; Modify Registry; Obfuscated Files or Information; Process Injection; System Binary Proxy Execution; Valid Accounts; Sandbox Evasion

Credential Access: Brute Force; OS Credential Dumping

Discovery: Account Discovery; Debugger Evasion; Domain Trust Discovery; File and Directory Discovery; Network Share Discovery; Process Discovery; Remote System Discovery; System Information Discovery; System Network Connections Discovery; Sandbox Evasion

Lateral Movement: Lateral Tool Transfer; Remote Services: Remote Desktop Protocol, SMB/Windows Admin Shares

Collection: Active Collected Data: Archive via Utility

C&C: Application Layer Protocol: Web Protocols; Encrypted Channel

Exfiltration: Exfiltration Over C2 Channel; Exfiltration Over Web Service: Exfiltration to Cloud Storage

Impact: Data Destruction, Data Encrypted for Impact, Defacement, Inhibit System Recovery, Service Stop

Die letzte Gruppe ist Hive mit deren TTPs [Tida22; Micr22b; Cisa22, S. 1ff.; LSBA22]:

Initial Access: Exploit Public-Facing Application, External Remote Services, Phishing und Valid Accounts

Execution: Command and Scripting Interpreter mit Powershell und CMD, Scheduled Tast/Job, User Execution und WMI

Persistence: Account Manipulation, BITS Jobs, Boot or Logon Autostart Execution mit Registry Keys und Startup Folder, Create or Modify System Process, External Remote Services, Scheduled Task/Job und Valid Accounts

Privilege Escalation: Boot or Logon Autostart Execution, Create or Modify System Process, Exploitation for Privilege Escalation, Process Injection, Scheduled Task/Job und Valid Accounts

Defense Evasion: BITS Jobs, Debugger Evasion, Deobfuscate/Decode Files or Information, Impair Defenses, Indicator Removal mit Clear Windows Event Logs und File Removal, Masquerading, Modify Registry, Obfuscated Files or Information, Process Injection, System Binary Proxy Execution, Valid Accounts und Sandbox Evasion

Credential Access: Brute Force, OS Credential Dumping

Discovery: Account Discovery, File and Directory Discovery, Network Share Discovery, Process Discovery, Remote System Discovery, System Network Connections Discovery, System Service Discovery

Lateral Movement: Lateral Tool Transfer, Remote Services mit RDP und SMB/Windows Admin Shares

Collection: Active Collected Data mit Archive via Utility

C&C: Application Layer Protocol mit Web Protocols

Exfiltration: Exfiltration Over C2 Channel, Exfiltration Over Web Service, Transfer Data to Cloud Account

Impact: Data Encrypted for Impact; Inhibit System Recovery; Service Stop

Durch das Filtern und die Priorisierung der TTPs können mehrere aus der Betrachtung rausgelassen werden, da diese beispielsweise nur von einer Gruppe genutzt werden oder weil bereits in dieser Technik mehr Taktiken existieren, die über einen längeren Zeitraum von mehreren Gruppen genutzt wurden und daher eine stärkere Gewichtung erhalten haben. Anschließend entsteht eine Liste aller TTPs, welche näher betrachtet werden:

Initial Access: Exploit Public-Facing Application, External Remote Services, Phishing, Valid Accounts

Execution: Command and Scripting Interpreter, Scheduled Task/Job, User Execution, WMI

Persistence: Account Manipulation, Boot or Lohon Autostart Execution, Create Account, Create or Modify System Process, External Remote Services

Privilege Escalation: Abuse Elevation Control Mechanism, Boot or Logon Autostart Execution, Create or Modify System Process

Defense Evasion: Abuse Elevation Control Mechanism, Deobfuscate/Decode Files or Information, Impair Defenses, Indicator Removal, Modify Registry, Process Injection, System Binary Proxy Execution, Valid Accounts

Credential Access: OS Credential Dumping

Discovery: Account Discovery, File and Directory Discovery, Network Share Discovery, Process Discovery, Remote System Discovery, System Information Discovery

Lateral Movement: Lateral Tool Transfer, Remote Services

Collection: Active Collected Data

C&C: Application Layer Protocol

Exfiltration: Exfiltration Over C2 Channel, Exfiltration Over Web Service

Impact: Data Encrypted for Impact, Inhibit System Recovery, Service Stop

Die gefilterten und priorisierten TTPs werden mit den bekannten Informationen in Bezug auf die genutzten Tools und Befehlen der einzelnen Gruppen, erweitert. Bei Initial Access werden Mails mit angehängten ZIP-Dateien, welche weitere Dateien wie „.doc“, „.pdf“ oder „.xls“ enthalten. In Discovery werden mehrere Windows interne Tools genutzt, dazu gehören net.exe, ipconfig.exe, arp.exe, whoami.exe, nslookup.exe und netstat.exe. Ebenfalls werden hier PowerShell Cmdlets genutzt, welche ähnliche Funktionalitäten bieten. Für die Persistence werden Nutzer angelegt wie „temp“, „r“ und „admin“, diese Nutzer werden ebenfalls in privilegierte Gruppen hinzugefügt und unterschiedliche Systemdienste installiert. Um Sicherheitsmechanismen zu umgehen, werden wieder Windows interne Tools genutzt. Mit regsrv32.exe werden schadhafte DLLs ausgeführt, powershell.exe wird genutzt, um mit Befehlen wie „DisableAntiSpyware“ die installierte Überwachung zu deaktivieren. Zusätzlich installierte Tools, wie PsExec führen die wmic.exe aus, um bestimmte Prozesse und Services zu finden und diese zu beenden. Damit die Angreifer weitere Benutzerdaten erhalten, wird das Tool Mimikatz genutzt. Da in den vorherigen Taktiken auch Powershell genutzt wird, wird bei Execution definiert, welche Tools genutzt werden, um Befehle auszuführen, unter anderem sind hier Powershell mit encoded commands, CMD und WMI aufgelistet. Für die Ausschleusung der Daten werden Tools, wie Cobalt Strike und Rclone genutzt, zusätzlich wird der Service Mega.io verwendet, teilweise mit Rclone oder mit dem Mega eigenem Synchronisationstool. C2 wird mittels Cobals Strike, Qakbot und teilweise TeamViewer oder AnyConnect durchgeführt. Die letzte Taktik ist Impact und wird mittels vssadmin.exe, wevutil.exe, wbaadmin.exe, wmic.exe und bcdedit.exe durchgeführt, dabei werden Shadowcopies und Event Logs gelöscht. Eine Übersicht der gesammelten Befehle und Tools sind in den Anlagen unter Tools und Befehle zu finden [Tren22; Elsa22; CoPi22, S. 5ff.; Walt22; Rift22; Cisa22, S. 1ff.; Micr22b].

Das Feedback fällt für diesen Prozess ebenfalls positiv aus, da für die genannten Gruppen die TTPs bestimmt werden konnten. Die Techniken, welche am häufigsten genutzt werden, konnten hervorgehoben und zusätzlich die genutzten Kommandos und Tools ergänzt werden.

Basierend auf diesen TTPs mit Tools und Befehlen können die Suchen und Erkennungsregeln erstellt werden. Nach einer Ausführung von Befehlen und/oder Tools können die generierten Events im SIEM betrachtet und analysiert werden. Bei kleineren Erkennungsregeln, wie die Nutzung von „net.exe“ in der Taktik Discovery, sind es nur einzelne Events, die betrachtet werden müssen. Das von Sysmon generierte Event erhält die Event ID, da die Ausführung von Befehlen zu einem neuen Prozess führt und somit ein „Process Create“ Event generiert. Durch einige Filter, wie die IP-Adresse des Testsystems, die Event ID 1, was für „Process Create“ steht, sowie der Zeitraum, in dem der Befehl auf dem Testsystem ausgeführt wurde, werden die angezeigten Events in einer Suche begrenzt. Dies ermöglicht die gewollten Events schneller zu finden. Die oben genannten Filter zeigen dann folgendes Ergebnis:

Event Name	Username	Parent Process Name (custom)	ImageName (custom)	Process CommandLine (custom)
Process Create	knordqvi	cmd.exe	net.exe	net user /domain
Process Create	knordqvi	net.exe	net1.exe	C:\Windows\system32\net1 user /domain

Abbildung 18 – Suchergebnis nach „Process Create“

In Abbildung 18 ist zu erkennen, welcher Benutzer das Event ausgelöst hat, um welche Event Art es sich handelt, welcher Prozess gestartet wurde (hier ImageName), aus welchem Elternprozess dieser entstanden ist und die Kommandozeilenparameter, die ausgeführt wurden. Durch diese Informationen ist es möglich Regeln zu definieren, welche dieses Verhalten erkennen. Da die Implementation von Regeln in jedem SIEM unterschiedlich ist wird hierfür die allgemeine Variante mit Sigma-Regeln genutzt. So eine Sigma-Regel würde wie folgt aussehen:

```
logsource:
        category: process_creation
        product: windows
detection:
        net:
          - ImageName:
                - ‘\net.exe’
                - ‘\net1.exe’
        selection:
          - Process CommandLine | contains:
                - ‘user /domain’
        condition: net and selection
```

Diese Sigma-Regel würde jedoch nur diesen einen Befehl erkennen, wie aber in den gesammelten Kommandos zu sehen war, werden unterschiedliche Befehle mit „net.exe“ ausgeführt. Um alle davon erkennen zu können kann die Regel einfach erweitert werden. Die Befehle sind folgende:

net user /domain ; net group /domain ; net view /all ; net share ; net localgroup ; net group 'Domain Admins' /domain ; net group 'Enterprise Admins' /domain ; net localgroup Administrators /domain ; net localgroup Administrators ; net user […] /delete

Um die gelisteten Befehle zu erkennen, wird zuerst nach gleichen oder ähnlichen Teilen geschaut. Hierbei fällt auf, dass „/domain“ oft abgefragt wird, sowie die „group“ und „localgroup“. Daher wird die Regel um die selection für „/domain“ und „group“ erweitert. Zu beachten ist, dass der Begriff „group“ ebenfalls „localgroup“ erkennt, da das Word in dem anderen enthalten ist. Für die Abfragen über „Admins“, „Administrators“, „Enterprise Admins“ kann die Regel mit einer selection von „Admin“ erweitert werden, da dieses Wort in allen Varianten enthalten ist. Anschließend werden noch die Begriffe „user“, „view“, „/all“, „/delete“ und „share“ integriert, um alle genutzten Befehle zu erkennen. Durch die Betrachtung der Parameter „user“ und „group“ wird zusätzlich erkannt, wenn neue Benutzer erstellt und diese zu Gruppen hinzugefügt wurden. Somit ergibt die folgende Sigma-Regel:

```
logsource:
        category: process_creation
        product: windows
detection:
        net:
           - ImageName:
                - '\net.exe'
                - '\net1.exe'
        selection:
           - Process CommandLine | contains:
                - 'user'
                - 'view'
                - 'share'
                - 'Admin'
                - 'group'
                - '/domain'
                - '/all'
                - '/delete'
        condition: net and 1 of selection
```

Weitere Regeln können jedoch weit aus umfangreicher sein und benötigen einen größeren Aufwand an Analyse, um die Zusammenhänge zu erkennen und diese in eine Regel umwandeln zu können. Ein Beispiel hierfür ist eine mögliche Exfiltration von Daten an den Dienstleister MEGA.io. Bei der Recherche über Exfiltration zu MEGA.io wurde die Nutzung von einem Tool namens Rclone angesprochen, jedoch ist es möglich durch ein Mega eigenes Tool Dateien hochzuladen oder den Browser dafür zu nutzen, sodass kein Rclone mehr nötig ist [ScDi22]. Dadurch wird diese Regel die Nutzung von MEGAsync, Rclone und der Zugriff auf die MEGA.io Domain erkennen.
Bei der Ausführung des MEGAsync Tools wird ein Event mit der Event ID 1 generiert,

dabei enthält das Event Informationen, womit das Tool eindeutig identifiziert werden kann. Die Felder, welche genutzt werden, sind „Product Company“, „Producy Description“ und „Product Name“. Der Grund, warum diese Felder genutzt werden, ist weil die Namen von Dateien umbenannt werden können. Wenn in der Regel auf das Feld „ImageName“ geschaut wird und auf es seinen Inhalt „MEGAsync“ überprüft wird, kann es passieren, dass das Event nicht erkannt wird, da das Tool umbenannt wurde. Dies passiert jedoch nicht bei den Feldern, die oben genannt wurden, da es sich hierbei um interne Daten des jeweiligen Tools handelt, welche nicht ohne weiteres geändert werden können [ScDi22].

Process CommandLine (custom)	"C:\Users\knordqvi\AppData\Local\MEGAsync\ichbinkeinsynctool.exe"
Process Guid (custom)	7DFEB6B1-872E-63DB-1F05-D60000000000
Process Id (custom)	5212
Product Company (custom)	Mega Limited OriginalFileName: MEGAsync.exe
Product Description (custom)	MEGAsync
Product Name (custom)	MEGAsync

Abbildung 19 – Process Create MEGAsync

Wie oben in Abbildung 19 zu erkennen ist, wird das Programm „ichbinkeinsynctool.exe“ gestartet, allerdings handelt es sich hierbei um MEGAsync, wie in den drei unteren Feldern zu erkennen ist. Durch diese Informationen lässt sich bereits ein Teil der Sigma-Regel abbilden:

```
logsource:
        category: process_creation
        product: windows
detection:
        megasync:
          - Product Company | contains:
                - ‘MEGAsync’
          - Product Description | contains:
                - ‘MEGAsync’
          - Product Name | contains:
                - ‘MEGAsync’
        condition: 1 of megasync
```

Darüber hinaus sind weitere Events zu sehen, die durch den Upload einer Datei zu MEGA.io, generiert wurden. Davon hat eins die Event ID 3, welche besagt, dass ein Prozess eine Netzwerkverbindung aufgebaut hat. Dabei ist wie in Abbildung 19 das umbenannte

MEGAsync Tool zu sehen und zusätzlich die Ziel IP-Adresse und Hostname der Verbindung. Dabei enthält das „Destination Host Name“ Feld „mega.co.nz“, welches auf einen Zugriff auf einen MEGA-Server hindeutet. Da die MEGA-Internetseite mittels „mega.io“ aufgerufen wird, werden diese beiden Domainnamen in die Regel eingepflegt.

```
detection:
        mega_domain:
          - Destination Host Name | contains:
                - ‘mega.io’
                - ‘mega.co.nz’
        condition: 1 of mega_domain
```

Des Weiteren soll die Nutzung von Rsync erkannt werden. Wie bei MEGAsync werden hier Metadaten genutzt, um trotz einer Umbenennung der Datei den „Process Name“ zu erkennen. Hierbei wird auf den Inhalt „rclone“ bzw. „rsync“ geprüft. Um Rclone erfolgreich zu nutzen, werden mehrere Kommandozeilenparameter mitgegeben, welche die Funktionsweise minimal verändert. Dabei wird auf Parameter, wie „copy“, „config“, „create“, „user“ und „pass“ geachtet, da diese für die Erstellung der Konfigurationsdatei verantwortlich sind, um anschließend erfolgreich auf ein MEGA-Konto Daten hochzuladen. Bei Betrachtung der häufig genutzten Parameter sieht die Sigma-Regel so aus [ScDi22]:

```
detection:
        rsync:
          - Product Company | contains:
                - ‘rclone’
          - Product Description | contains:
                - ‘Rsync’
          - Product Name | contains:
                - ‘Rclone’
        parameters:
          - Process CommandLine | contains:
                - "config"
                - "create"
                - "remote"
                - "user"
                - "pass"
                - "sync"
                - "copy"
                - "--config"
                - "--progress"
                - "--no-check-certificate"
                - "--ignore-existing"
                - "--auto-confirm"
                - "--multi-thread-streams"
                - "--transfers"
                - "ftp:"
                - "\\"
```

Um aus diesen drei Sigma Teilen eine Regel zu erstellen, werden diese mit einer Oder-Verknüpfung kombiniert, um zu gewährleisten, dass jeder der einzelnen Teile eine Meldung generieren können. Die weiteren erstellten Sigma-Regeln sind in den Anlagen Sigma-Regeln zu finden. Somit kann für den letzten Prozess, aus den TTPs mit Befehlen und Tools, Erkennungsregeln zu erstellen, gesagt werden, dass dieser ebenfalls erfolgreich abgeschlossen werden konnte.

6 Fazit und Ausblick

Zum Schluss wird die vorliegende Arbeit zusammengefasst, ausgewertet und Möglichkeiten beschrieben, wie diese weitergeführt werden kann. Das Ziel dieser Arbeit war es Erkennungsmuster für Ransomware-Gruppen zu erstellen, basierend auf Gruppen, die auf bestimmte Merkmale priorisiert wurden.

Um dies zu erreichen, wurden zunächst die aktiven Ransomware-Gruppen erörtert, dies wurde mittels aktueller Reports und Open Source Projekten durchgeführt. Dabei wurden die Informationen von den bekannten Leak-Seiten der Gruppen entnommen, wodurch nur Daten gesammelt wurden, welche von den Gruppen selbst an die Öffentlichkeit weitergegeben wurden. Jedoch stellten die erhaltenen Informationen im Rahmen dieser Arbeit ein sehr zufriedenstellendes Ergebnis dar und bieten einen guten Einblick in das Umfeld der einzelnen Gruppen.

Für die Priorisierung wurden Informationen zu den Ransomware-Gruppen benötigt, hier wurde sich auf die bereits angegriffenen Unternehmen mit deren Standort und Branche bezogen. Dabei stellte sich heraus, dass eine zuverlässig automatisierte Lösung für die Beschaffung dieser Daten schwieriger ist als am Anfang gedacht. Als Lösungsansatz wurde hier versucht von Handelsregistern der Länder die Informationen zu den Unternehmen zu erhalten. Dabei wurden Probleme ersichtlich, wie die Abfragen von Captchas und, dass bei der Suche nach Unternehmen, der gesuchte Name kaum bis keine Abweichung haben durfte, im Vergleich zum Namen im Handelsregister, da sonst die Wahrscheinlichkeit groß war, dass kein Treffer gefunden wurde. Daraufhin wurde als Quelle Google Maps gewählt, da hier, im Gegensatz zu lokalen Handelsregistern in unterschiedlichen Ländern weitreichende Informationen verfügbar sind. Trotz der großen Masse an Informationen war es nicht möglich für jedes Unternehmen, den Standort und Branche zu erhalten, da diese Informationen von den einzelnen Unternehmen selbst gepflegt werden. Zusätzlich wurde beobachtet, dass sich nicht drauf verlassen werden konnte, dass die vorhandenen Informationen wie erhofft angezeigt werden. Dies fiel auf, da bei mehrfachem Suchen von einigen Unternehmen manchmal Treffer gefunden wurden und manchmal nicht. Aus diesem Grund wurden zu vielen Unternehmen keine Daten gefunden, obwohl diese eventuell bei Google Maps vorhanden sein könnten. Dadurch entstanden an einigen Stellen Informationslücken, die bei der Analyse dieser Daten berücksichtigt werden mussten. Bei der Priorisierung der Gruppen wurden die betroffenen Unternehmen zunächst nach Standorten und anschließend nach Branchen sortiert. Allerdings gelangte dies nur für die Standorte, da die Angaben der Branchen durch die Unternehmen selbst vorgenommen werden und dabei Angaben wie "Geschäftsstelle" eingetragen werden, falls das Unternehmen mehrere Standorte besitzt. Die Priorisierung wurde somit nur nach den Standorten durchgeführt.

Nach der Analyse wurden die drei aktivsten Gruppen in Europa weiter betrachtet und mit den genutzten TTPs und darauf basierten Befehlen und Tools angereichert. Hierbei wurden die TTPs verwendet, welche am meisten genutzt wurden, um eine möglichst weitreichende Erkennung zu erreichen.

Zuletzt konnten die nötigen Suchen und Erkennungsregeln durch das Ausführen dieser Kommandos und Tools sowie durch Recherche von bereits durchgeführten Forschungen und Tests dieser Tools erstellt werden. Hierbei ist jedoch zu beachten, dass viele genutzte Tools von Windows Interne Tools sind, welche von Angreifern, aber auch von Administratoren genutzt werden. Somit ist es möglich, dass die Erkennung von Befehlen und Tools Falschmeldungen auslösen. Aus diesem Grund ist die Erstellung und Weiterentwicklung von Erkennungsregeln ein stetiger Prozess, der darauf basiert, dass diese in jeder Infrastruktur genaustens betrachtet und für die jeweiligen Infrastrukturen angepasst werden. So ist es beispielsweise möglich TeamViewer als valides Tool in einem Unternehmen zu nutzen, ohne dass dies als schadhaft empfunden wird.

Als mögliche Weiterführung dieses Projektes, sollten die Recherchen zu den betroffenen Unternehmen durch mehrere Quellen ergänzt werden, um mögliche Informationslücken zu schließen. Zusätzlich können für die einzelnen Länder die Handelsregister genutzt werden, um genauere Informationen zu den Unternehmen zu finden, welche es ermöglichen, zuverlässigere Daten und somit auch eine bessere Priorisierung der Unternehmen durchzuführen. Als letztes sollten Regeln und Suchen für weitere TTPs erstellt werden und dauerhaft das Verhalten der Gruppen betrachtet werden, um sich gegen zukünftige Änderungen und Anpassungen schützen zu können.

Insgesamt wurden die Fragen der Arbeit erfolgreich beantwortet und stellen eine Möglichkeit dar, wie der Prozess aussehen könnte, um sich gegen Ransomware-Gruppen schützen zu können.

Literatur

Abra22 Abrams L.: LockBit ransomware builder leaked online by “angry developer”, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-builder-leaked-online-by-angry-developer-/, 2022, Abruf am 13.12.2022

BhMZ14 Bhatt, S.; Manadhata, P.; Zomlot, L.: The Operational Role of Security Information and Event Management Systems, IEEE, 2014

Bido05 Bidou, R.: Security operations center concepts & implementation, Researchgate, 2005 https://www.researchgate.net/profile/Renaud-Bidou/publication/228587242_Security_Operation_Center_Concepts_Implementation/links/0f3175318a296d7219000000/Security-Operation-Center-Concepts-Implementation.pdf

BrNu21 Brandao, P.; Nunes, J.: Extendet Detection and Response Importance of Event Context, kriativ.tech, 2021

BrRo17 Brown, R.; Roberts, S.: Intelligence-Driven Incident Response Outwittin the adversary, Oreilly, 2017

BSI Definition Kritis, https://www.bsi.bund.de/dok/12211940, Abruf am 03.01.2023

BSI22 Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, 2022, Bundesamt für Sicherheit in der Informationstechnik

Buch16 Buchmann, J.: Einführung in die Kryptographie, 6. Auflage, Springer Sprektrum, 2016

Bush22 BushidoToken: The Difficulties and Dubiousness of Darkweb Data Leaks Sites, https://www.curatedintel.org/2022/11/the-difficulties-and-dubiousness-of.html, 2022, Abruf am 31.01.2023

Chap19 Chapagain, A.: Hands-On Web Scraping with Python, Packt, 2019

Chec EDR vs Antivirus, https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-detection-and-response/endpoint-detection-and-response-edr-benefits/edr-vs-antivirus/, Abruf am 26.01.2023

Cisa22 Cybersecurity & Infrastructure Security Agency (CISA): #StopRansomware: Hive Ransomware, CISA, 2022

Coin23 Bitcoin Price, 2023, https://www.coindesk.com/price/bitcoin/, Abruf am 04.01.2023

CoPi22 Cocomazzi, A.; Pirozzi, A.: Black Basta ransomware | Attacks deploy custom EDR evasion tools tied to FIN7 threat actor, Sentinel LABS, 2022

Dark23 Ransomware Groups, https://darkfeed.io/ransomgroups/, 2023, Abruf am 19.01.2023

DDBC19 Dargahi, T.; Dehghantanha, A.; Bahrami, P.; Conti, M.: A Cyber-Kill-Chain based taxonomy of crypto-ransomware features, Springer, 2019

DGTY18 Dixit, P.; Gupta, A.K.; Trivedi, M.C.; Yadav, V.K.: Traditional and

Hybrid Encryption Techniques: A Survey. In: Perez, G., Mishra, K., Tiwari, S., Trivedi, M.: Networking Communication and Data Knowledge Engineering. Lecture Notes on Data Engineering and Communications Technologies, Ausgabe 4, Springer, 2018

Ecri23 Leak site gallery, https://ecrime.ch/screenshots/, 2023, Abruf am 19.01.2023

Elsa22 Elsad, A.: Threat Assessment: Black Basta Ransomware, https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/, 2022, Abruf am 30.01.2023

Gaze08 Gazet, A.: Comparative analysis of various ransomware virii, Springer, 2008

HeCC20 Hernandez-Castro, J.; Cartwright, A.; Cartwright, E.: An economic analysis of ransomware and its welfare consequences, The Royal Society, 2020

Hube19 Huber, E.: Cybercrime Eine Einführung, Springer VS, 2019

IBM Security Operations Center (SOC), https://www.ibm.com/topics/security-operations-center, 2022, Abruf am 03.01.2023

ILAS22 Ilascu, I.: Ransomware gang now lets you search their stolen data, https://www.bleepingcomputer.com/news/security/ransomware-gang-now-lets-you-search-their-stolen-data/, 2022, Abruf am 30.12.2022

Kasp22 Common TTPs of modern ransomware groups, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-

the-modern-ransomware_low-res.pdf, 2022, Abruf am 13.12.2022

Lifa21 A Detailed Analysis of The Last Version of Conti Ransomware, Lifars, 2021

LSBA22 Ladores, D.; Silva, L.; Burden, S.; Agcaoili, J.: Play Ransomware´s Attack Playbook Similar to that of Hive, Nokoyawa, https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html, 2022, Abruf am 30.01.2023

MBMS21 Mirza, Q.; Brown, M.; Malling, O.; Shand, L.: Ransomware Analysis using Cyber Kill Chain, IEEE, 2021

MeBS20 Meland, P.; Bayoumy, Y.; Sindre, G.: The Ransomware-as-a-Service economy within the darknet, Elsevier, 2020

Mell21 Mellen, A.: Introducing The Forrester New Tech: Extended Detection And Response (XDR) – A Battle Between Precedent And Innovation, https://www.forrester.com/blogs/introducing-the-forrester-new-tech-extended-detection-and-response-xdr-a-battle-between-precedent-and-innovation/, 2021, Abruf am 12.12.2022

MHKR22 Mihaiuc, A.; Hewardt, M.; Kim, L.; Russinovich, M.: Sysmon v14.12 2022, https://learn.microsoft.com/de-de/sysinternals/downloads/sysmon, Abruf am 03.01.2021

Micr22a Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself, https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/, 2022, Abruf am 13.12.2022

Micr22b Microsoft Threat Intelligence Center (MSTIC): Hive ransomware gets upgrades in Rust, https://www.microsoft.com/en-us/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/, 2022, Abruf am 30.01.2023

Mila09 Milanov, E.: The RSA Algorithm, Washington, 2009

Miro16 Miroshnikov, A.: Windows 10 and Windows Server 2016 security auditing and monitoring reference, Microsoft, 2016

MITR22 ATT&CK Matrix for Enterprise v12, https://attack.mitre.org/#, 2022, Abruf am 03.01.2023

MLMM22 Montemayor, D.; Long, L.; Matarazzo, P.; Mandalika, S.: Use Windows Event Forwarding to help with intrusion detection 2022,

Nath15 Nathans, D., Designing and Building A Security Operations Center, Syngress, 2015

Nxlo22 Windows Event Log, https://docs.nxlog.co/userguide/integrate/windows-eventlog.html, 2022, Abruf am 26.01.2023

Pamn22a Pamnani, V.: Sicherheitsüberwachung, https://learn.microsoft.com/de-de/windows/security/threat-protection/auditing/security-auditing-overview, 2022, Abruf am 12.12.2022

Pamn22b Pamnani, V.: Grundlegende Sicherheitsüberwachungsrichtlinien, https://learn.microsoft.com/de-de/windows/security/threat-protection/auditing/basic-security-audit-policies, 2022, Abruf am 12.12.2022

Pola22 Security Operations Center (SOC) Market Share, https://www.polarismarketresearch.com/industry-analysis/security-operation-center-market, 2022, Abruf am 03.01.2023

Rans23a Ransonwatch profiles, https://ransomwatch.telemetry.ltd/#/profiles, 2023, Abruf am 19.01.2023

Rans23b RansomLook Group Profiles, https://www.ransomlook.io/groups, 2023, Abruf am 19.01.2023

Rift22 RIFT: Research and Intelligence Fusion Team: Back in Black: Unlocking a LockBit 3.0 Ransomware Attack, https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack/, 2022, Abruf am 30.01.2023

RiNo17 Richardson, R.; North, M.: Ransomware: Evolution, Mitigation and Prevention, Kennesaw State University, 2017

Roth22 Roth, F.: Sigma, https://github.com/SigmaHQ/sigma, 2022, Abruf am 12.12.2022

SAMN18 Strom, B.; Applebaum, A.; Miller, D.; Nickels, K.: MITRE ATT&CK®: Design and Philosophy, MITRE, 2018

ScDi22 Schoenfeld, J.; Didier, A.: Transferring leverage in a ransomware attack, https://redcanary.com/blog/rclone-mega-extortion/, 2022, Abruf 02.02.2023

Schm06 Schmid, O.: Analyse der Entwicklung von Malware, In: Armknecht, F.; Stegemann, D.: Kryptowochenende 2006 – Workshop über Kryptologie, Universität Mannheim, 2006, 14-15

Sele22a Selenium, Install a Selenium library, https://www.selenium.dev/documentation/webdriver/getting_started/install_library/, 2022, Abruf am 03.02.2023

Sele22b Selenium, Install browser drivers, https://www.selenium.dev/documentation/webdriver/getting_started/install_drivers/, 2022, Abruf am 03.01.2023

Sele22c Selenium, Browser Options, https://www.selenium.dev/documentation/webdriver/drivers/options/, 2022, Abruf am 03.01.2023

Shar22 Sharif, A.: Log Files Explained, https://www.crowdstrike.com/cybersecurity-101/observability/log-file/, 2022, Abruf am 09.01.2023

Shel22 Shelton, T.: Sysmon Crash, https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/system/win_system_application_sysmon_crash.yml, 2022, Abruf am 03.01.2023

Soni22 2022 Sonicwall Cyber Threat Report, Sonicwall, 2022

SSDG22 Singh, S.; Shukla, A.; Devanshu; Gandhi, A.: Web Scraping Using Selenium, International Journal of Novel Research and Development, 2022

Stat22a Number of newly discovered ransomware families worldwide from 2015 to 2021, https://www.statista.com/statistics/701029/number-of-newly-added-ransomware-families-worldwide/, 2022, Abruf am 04.01.2023

Stat22b Desktop Operating System Market Share Worldwide,

https://gs.statcounter.com/os-market-share/desktop/worldwide, 2022, Abruf am 13.12.2022

Thre22 Threat & Detection Research Team: The story of a ransomware builder: from Thanos to Spook and beyond (Part 2), https://blog.sekoia.io/the-story-of-a-ransomware-builder-from-thanos-to-spook-and-beyond-part-2/, 2022, Abruf am 13.12.2022

Tida22 Tidal, Ransomware Threatening Schools: 2021-22, https://app.tidalcyber.com/share/8d9f212a-0312-4c2f-bba5-85ab7c7224c6, 2022, Abruf am 30.01.2023

Torp22 Tor-browser, https://gitweb.torproject.org/tor-browser.git/tree/browser/app/profile/000-tor-browser.js?h=tor-browser-52.5.2esr-7.0-2, 2022, Abruf am 20.01.2023

Tren22 Trend Micro Research, Ransomware Spotlight Black Basta, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta, 2022, Abruf am 30.01.2023

Walt22 Walter, J.: LockBit 3.0 Update | Unpicking the Ransomware´s lastest Anti-Analysis and Evasion Techniques, https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/, 2022, Abruf am 30.01.2023

WeXY14 WeiTek, T.; XiaoYing, B.; Yu, H.: Software-as-a-Service (Saas): perspectives and challenges, Springer, 2014

Wues20 Wuest, C.: Ransomware leaking more data than many data breaches, https://www.acronis.com/en-us/blog/posts/ransomware-leaking-more-data-many-data-breaches/, 2020, Abruf am 13.12.2022

YaRa15 Yadav, T.; Rao, A.: Technical Aspects of Cyber Kill Chain, Springer, 2015

ZiCh19 Zimba, A.; Chishimba, M.: On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems, Springer Nature, 2019

Anlagen

Anlagen, Event IDs

4774(S): An account was mapped for logon.
4775(F): An account could not be mapped for logon.
4776(S, F): The computer attempted to validate the credentials for an account.
4777(F): The domain controller failed to validate the credentials for an account.
4768(S, F): A Kerberos authentication ticket (TGT) was requested.
4771(F): Kerberos pre-authentication failed.
4772(F): A Kerberos authentication ticket request failed.
4769(S, F): A Kerberos service ticket was requested.
4770(S): A Kerberos service ticket was renewed.
4773(F): A Kerberos service ticket request failed.
4783(S): A basic application group was created.
4784(S): A basic application group was changed.
4785(S): A member was added to a basic application group.
4786(S): A member was removed from a basic application group.
4787(S): A non-member was added to a basic application group.
4788(S): A non-member was removed from a basic application group.
4789(S): A basic application group was deleted.
4790(S): An LDAP query group was created.
4791(S): An LDAP query group was changed.
4792(S): An LDAP query group was deleted.
4741(S): A computer account was created.
4742(S): A computer account was changed.
4743(S): A computer account was deleted.
4749(S): A security-disabled global group was created.
4750(S): A security-disabled global group was changed.
4751(S): A member was added to a security-disabled global group.
4752(S): A member was removed from a security-disabled global group.
4753(S): A security-disabled global group was deleted.
4759(S): A security-disabled universal group was created.
4760(S): A security-disabled universal group was changed.
4761(S): A member was added to a security-disabled universal group.
4762(S): A member was removed from a security-disabled universal group.
4763(S): A security-disabled universal group was deleted.
4744(S): A security-disabled local group was created.
4745(S): A security-disabled local group was changed.
4746(S): A member was added to a security-disabled local group.
4747(S): A member was removed from a security-disabled local group.
4748(S): A security-disabled local group was deleted.
4782(S): The password hash an account was accessed.
4793(S): The Password Policy Checking API was called.
4727(S): A security-enabled global group was created.
4737(S): A security-enabled global group was changed.
4728(S): A member was added to a security-enabled global group.
4729(S): A member was removed from a security-enabled global group.
4730(S): A security-enabled global group was deleted.

4731(S): A security-enabled local group was created.
4732(S): A member was added to a security-enabled local group.
4733(S): A member was removed from a security-enabled local group.
4734(S): A security-enabled local group was deleted.
4735(S): A security-enabled local group was changed.
4754(S): A security-enabled universal group was created.
4755(S): A security-enabled universal group was changed.
4756(S): A member was added to a security-enabled universal group.
4757(S): A member was removed from a security-enabled universal group.
4758(S): A security-enabled universal group was deleted.
4764(S): A group’s type was changed.
4799(S): A security-enabled local group membership was enumerated.
4720(S): A user account was created.
4722(S): A user account was enabled.
4723(S, F): An attempt was made to change an account's password.
4724(S, F): An attempt was made to reset an account's password.
4725(S): A user account was disabled.
4726(S): A user account was deleted.
4738(S): A user account was changed.
4740(S): A user account was locked out.
4765(S): SID History was added to an account.
4766(F): An attempt to add SID History to an account failed.
4767(S): A user account was unlocked.
4780(S): The ACL was set on accounts which are members of administrators groups.
4781(S): The name of an account was changed.
4794(S, F): An attempt was made to set the Directory Services Restore Mode administrator password.
4798(S): A user's local group membership was enumerated.
5376(S): Credential Manager credentials were backed up.
5377(S): Credential Manager credentials were restored from a backup.
4692(S, F): Backup of data protection master key was attempted.
4693(S, F): Recovery of data protection master key was attempted.
4694(S, F): Protection of auditable protected data was attempted.
4695(S, F): Unprotection of auditable protected data was attempted.
6416(S): A new external device was recognized by the System.
6419(S): A request was made to disable a device.
6420(S): A device was disabled.
6421(S): A request was made to enable a device.
6422(S): A device was enabled.
6423(S): The installation of this device is forbidden by system policy.
6424(S): The installation of this device was allowed, after having previously been forbidden by policy.
4688(S): A new process has been created.
4696(S): A primary token was assigned to process.
4689(S): A process has exited.
5712(S): A Remote Procedure Call (RPC) was attempted.
4928(S, F): An Active Directory replica source naming context was established.
4929(S, F): An Active Directory replica source naming context was removed.
4930(S, F): An Active Directory replica source naming context was modified.
4931(S, F): An Active Directory replica destination naming context was modified.
4934(S): Attributes of an Active Directory object were replicated.

4935(F): Replication failure begins.

4936(S): Replication failure ends.

4937(S): A lingering object was removed from a replica.

4662(S, F): An operation was performed on an object.

4661(S, F): A handle to an object was requested.

5136(S): A directory service object was modified.

5137(S): A directory service object was created.

5138(S): A directory service object was undeleted.

5139(S): A directory service object was moved.

5141(S): A directory service object was deleted.

4932(S): Synchronization of a replica of an Active Directory naming context has begun.

4933(S, F): Synchronization of a replica of an Active Directory naming context has ended.

4625(F): An account failed to log on.

4626(S): User/Device claims information.

4627(S): Group membership information.

4978: During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.

4979: IPsec Main Mode and Extended Mode security associations were established.

4980: IPsec Main Mode and Extended Mode security associations were established.

4981: IPsec Main Mode and Extended Mode security associations were established.

4982: IPsec Main Mode and Extended Mode security associations were established.

4983: An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

4984: An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

4646: Security ID: %1

4650: An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.

4651: An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.

4652: An IPsec Main Mode negotiation failed.

4653: An IPsec Main Mode negotiation failed.

4655: An IPsec Main Mode security association ended.

4976: During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.

5049: An IPsec Security Association was deleted.

5453: An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.

4977: During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.

5451: An IPsec Quick Mode security association was established.

5452: An IPsec Quick Mode security association ended.

4634(S): An account was logged off.

4647(S): User initiated logoff.

4624(S): An account was successfully logged on.

4625(F): An account failed to log on.

4648(S): A logon was attempted using explicit credentials.

4675(S): SIDs were filtered.

6272: Network Policy Server granted access to a user.

6273: Network Policy Server denied access to a user.

6274: Network Policy Server discarded the request for a user.

6275: Network Policy Server discarded the accounting request for a user.

6276: Network Policy Server quarantined a user.
6277: Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
6278: Network Policy Server granted full access to a user because the host met the defined health policy.
6279: Network Policy Server locked the user account due to repeated failed authentication attempts.
6280: Network Policy Server unlocked the user account.
4649(S): A replay attack was detected.
4778(S): A session was reconnected to a Window Station.
4779(S): A session was disconnected from a Window Station.
4800(S): The workstation was locked.
4801(S): The workstation was unlocked.
4802(S): The screen saver was invoked.
4803(S): The screen saver was dismissed.
5378(F): The requested credentials delegation was disallowed by policy.
5632(S, F): A request was made to authenticate to a wireless network.
5633(S, F): A request was made to authenticate to a wired network.
4964(S): Special groups have been assigned to a new logon.
4672(S): Special privileges assigned to new logon.
4665: An attempt was made to create an application client context.
4666: An application attempted an operation.
4667: An application client context was deleted.
4668: An application was initialized.
4868: The certificate manager denied a pending certificate request.
4869: Certificate Services received a resubmitted certificate request.
4870: Certificate Services revoked a certificate.
4871: Certificate Services received a request to publish the certificate revocation list (CRL).
4872: Certificate Services published the certificate revocation list (CRL).
4873: A certificate request extension changed.
4874: One or more certificate request attributes changed.
4875: Certificate Services received a request to shut down.
4876: Certificate Services backup started.
4877: Certificate Services backup completed.
4878: Certificate Services restore started.
4879: Certificate Services restore completed.
4880: Certificate Services started.
4881: Certificate Services stopped.
4882: The security permissions for Certificate Services changed.
4883: Certificate Services retrieved an archived key.
4884: Certificate Services imported a certificate into its database.
4885: The audit filter for Certificate Services changed.
4886: Certificate Services received a certificate request.
4887: Certificate Services approved a certificate request and issued a certificate.
4888: Certificate Services denied a certificate request.
4889: Certificate Services set the status of a certificate request to pending.
4890: The certificate manager settings for Certificate Services changed.
4891: A configuration entry changed in Certificate Services.
4892: A property of Certificate Services changed.
4893: Certificate Services archived a key.
4894: Certificate Services imported and archived a key.
4895: Certificate Services published the CA certificate to Active Directory Domain Services.

4896: One or more rows have been deleted from the certificate database.
4897: Role separation enabled.
4898: Certificate Services loaded a template.
5145(S, F): A network share object was checked to see whether client can be granted desired access.
5140(S, F): A network share object was accessed.
5142(S): A network share object was added.
5143(S): A network share object was modified.
5144(S): A network share object was deleted.
5168(F): SPN check for SMB/SMB2 failed.
4656(S, F): A handle to an object was requested.
4658(S): The handle to an object was closed.
4660(S): An object was deleted.
4663(S): An attempt was made to access an object.
4664(S): An attempt was made to create a hard link.
4985(S): The state of a transaction has changed.
5051(-): A file was virtualized.
4670(S): Permissions on an object were changed.
5031(F): The Windows Firewall Service blocked an application from accepting incoming connections on the network.
5150(-): The Windows Filtering Platform blocked a packet.
5151(-): A more restrictive Windows Filtering Platform filter has blocked a packet.
5154(S): The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
5155(F): The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
5156(S): The Windows Filtering Platform has permitted a connection.
5157(F): The Windows Filtering Platform has blocked a connection.
5158(S): The Windows Filtering Platform has permitted a bind to a local port.
5159(F): The Windows Filtering Platform has blocked a bind to a local port.
5152(F): The Windows Filtering Platform blocked a packet.
5153(S): A more restrictive Windows Filtering Platform filter has blocked a packet.
4658(S): The handle to an object was closed.
4690(S): An attempt was made to duplicate a handle to an object.
4656(S, F): A handle to an object was requested.
4658(S): The handle to an object was closed.
4660(S): An object was deleted.
4663(S): An attempt was made to access an object.
4671(-): An application attempted to access a blocked ordinal through the TBS.
4691(S): Indirect access to an object was requested.
5148(F): The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
5149(F): The DoS attack has subsided and normal processing is being resumed.
4698(S): A scheduled task was created.
4699(S): A scheduled task was deleted.
4700(S): A scheduled task was enabled.
4701(S): A scheduled task was disabled.
4702(S): A scheduled task was updated.
5888(S): An object in the COM+ Catalog was modified.
5889(S): An object was deleted from the COM+ Catalog.
5890(S): An object was added to the COM+ Catalog.
4663(S): An attempt was made to access an object.

4656(S, F): A handle to an object was requested.
4658(S): The handle to an object was closed.
4660(S): An object was deleted.
4657(S): A registry value was modified.
5039(-): A registry key was virtualized.
4670(S): Permissions on an object were changed.
4656(S, F): A handle to an object was requested.
4658(S): The handle to an object was closed.
4663(S): An attempt was made to access an object.
4661(S, F): A handle to an object was requested.
4818(S): Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy.
4715(S): The audit policy (SACL) on an object was changed.
4719(S): System audit policy was changed.
4817(S): Auditing settings on object were changed.
4902(S): The Per-user audit policy table was created.
4906(S): The CrashOnAuditFail value has changed.
4907(S): Auditing settings on object were changed.
4908(S): Special Groups Logon table modified.
4912(S): Per User Audit Policy was changed.
4904(S): An attempt was made to register a security event source.
4905(S): An attempt was made to unregister a security event source.
4670(S): Permissions on an object were changed.
4706(S): A new trust was created to a domain.
4707(S): A trust to a domain was removed.
4716(S): Trusted domain information was modified.
4713(S): Kerberos policy was changed.
4717(S): System security access was granted to an account.
4718(S): System security access was removed from an account.
4739(S): Domain Policy was changed.
4864(S): A namespace collision was detected.
4865(S): A trusted forest information entry was added.
4866(S): A trusted forest information entry was removed.
4867(S): A trusted forest information entry was modified.
4703(S): A user right was adjusted.
4704(S): A user right was assigned.
4705(S): A user right was removed.
4670(S): Permissions on an object were changed.
4911(S): Resource attributes of the object were changed.
4913(S): Central Access Policy on the object was changed.
4709(S): IPsec Services was started.
4710(S): IPsec Services was disabled.
4711(S): May contain any one of the following:
4712(F): IPsec Services encountered a potentially serious failure.
5040(S): A change has been made to IPsec settings. An Authentication Set was added.
5041(S): A change has been made to IPsec settings. An Authentication Set was modified.
5042(S): A change has been made to IPsec settings. An Authentication Set was deleted.
5043(S): A change has been made to IPsec settings. A Connection Security Rule was added.
5044(S): A change has been made to IPsec settings. A Connection Security Rule was modified.
5045(S): A change has been made to IPsec settings. A Connection Security Rule was deleted.
5046(S): A change has been made to IPsec settings. A Crypto Set was added.

5047(S): A change has been made to IPsec settings. A Crypto Set was modified.

5048(S): A change has been made to IPsec settings. A Crypto Set was deleted.

5440(S): The following callout was present when the Windows Filtering Platform Base Filtering Engine started.

5441(S): The following filter was present when the Windows Filtering Platform Base Filtering Engine started.

5442(S): The following provider was present when the Windows Filtering Platform Base Filtering Engine started.

5443(S): The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.

5444(S): The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.

5446(S): A Windows Filtering Platform callout has been changed.

5448(S): A Windows Filtering Platform provider has been changed.

5449(S): A Windows Filtering Platform provider context has been changed.

5450(S): A Windows Filtering Platform sub-layer has been changed.

5456(S): PAStore Engine applied Active Directory storage IPsec policy on the computer.

5457(F): PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.

5458(S): PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.

5459(F): PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.

5460(S): PAStore Engine applied local registry storage IPsec policy on the computer.

5461(F): PAStore Engine failed to apply local registry storage IPsec policy on the computer.

5462(F): PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.

5463(S): PAStore Engine polled for changes to the active IPsec policy and detected no changes.

5464(S): PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.

5465(S): PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.

5466(F): PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.

5467(F): PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.

5468(S): PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.

5471(S): PAStore Engine loaded local storage IPsec policy on the computer.

5472(F): PAStore Engine failed to load local storage IPsec policy on the computer.

5473(S): PAStore Engine loaded directory storage IPsec policy on the computer.

5474(F): PAStore Engine failed to load directory storage IPsec policy on the computer.

5477(F): PAStore Engine failed to add quick mode filter.

4944(S): The following policy was active when the Windows Firewall started.

4945(S): A rule was listed when the Windows Firewall started.

4946(S): A change has been made to Windows Firewall exception list. A rule was added.

4947(S): A change has been made to Windows Firewall exception list. A rule was modified.

4948(S): A change has been made to Windows Firewall exception list. A rule was deleted.

4949(S): Windows Firewall settings were restored to the default values.

4950(S): A Windows Firewall setting has changed.

4951(F): A rule has been ignored because its major version number was not recognized by Windows Firewall.

4952(F): Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.

4953(F): Windows Firewall ignored a rule because it could not be parsed.

4954(S): Windows Firewall Group Policy settings have changed. The new settings have been applied.

4956(S): Windows Firewall has changed the active profile.

4957(F): Windows Firewall did not apply the following rule.

4958(F): Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.

4714(S): Encrypted data recovery policy was changed.

4819(S): Central Access Policies on the machine have been changed.

4826(S): Boot Configuration Data loaded.

4909(-): The local policy settings for the TBS were changed.

4910(-): The group policy settings for the TBS were changed.

5063(S, F): A cryptographic provider operation was attempted.

5064(S, F): A cryptographic context operation was attempted.

5065(S, F): A cryptographic context modification was attempted.

5066(S, F): A cryptographic function operation was attempted.

5067(S, F): A cryptographic function modification was attempted.

5068(S, F): A cryptographic function provider operation was attempted.

5069(S, F): A cryptographic function property operation was attempted.

5070(S, F): A cryptographic function property modification was attempted.

5447(S): A Windows Filtering Platform filter has been changed.

6144(S): Security policy in the group policy objects has been applied successfully.

6145(F): One or more errors occurred while processing security policy in the group policy objects.

4673(S, F): A privileged service was called.

4674(S, F): An operation was attempted on a privileged object.

4985(S): The state of a transaction has changed.

4985(S): The state of a transaction has changed.

4673(S, F): A privileged service was called.

4674(S, F): An operation was attempted on a privileged object.

4985(S): The state of a transaction has changed.

4960(S): IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.

4961(S): IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.

4962(S): IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.

4963(S): IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.

4965(S): IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.

5478(S): IPsec Services has started successfully.

5479(): IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.

5480(F): IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.

5483(F): IPsec Services failed to initialize RPC server. IPsec Services could not be started.

5484(F): IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.

5485(F): IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.

5024(S): The Windows Firewall Service has started successfully.

5025(S): The Windows Firewall Service has been stopped.

5027(F): The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.

5028(F): The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.

5029(F): The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.

5030(F): The Windows Firewall Service failed to start.

5032(F): Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.

5033(S): The Windows Firewall Driver has started successfully.

5034(S): The Windows Firewall Driver was stopped.

5035(F): The Windows Firewall Driver failed to start.

5037(F): The Windows Firewall Driver detected critical runtime error. Terminating.

5058(S, F): Key file operation.

5059(S, F): Key migration operation.

6400(-): BranchCache: Received an incorrectly formatted response while discovering availability of content.

6401(-): BranchCache: Received invalid data from a peer. Data discarded.

6402(-): BranchCache: The message to the hosted cache offering it data is incorrectly formatted.

6403(-): BranchCache: The hosted cache sent an incorrectly formatted response to the client.

6404(-): BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.

6405(-): BranchCache: %2 instance(s) of event id %1 occurred.

6406(-): %1 registered to Windows Firewall to control filtering for the following: %2.

6407(-): 1%.

6408(-): Registered product %1 failed and Windows Firewall is now controlling the filtering for %2.

6409(-): BranchCache: A service connection point object could not be parsed.

4608(S): Windows is starting up.

4609(S): Windows is shutting down.

4616(S): The system time was changed.

4621(S): Administrator recovered system from CrashOnAuditFail.

4610(S): An authentication package has been loaded by the Local Security Authority.

4611(S): A trusted logon process has been registered with the Local Security Authority.

4614(S): A notification package has been loaded by the Security Account Manager.

4622(S): A security package has been loaded by the Local Security Authority.

4697(S): A service was installed in the system.

4612(S): Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.

4615(S): Invalid use of LPC port.

4618(S): A monitored security event pattern has occurred.

4816(S): RPC detected an integrity violation while decrypting an incoming message.

5038(F): Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.

5056(S): A cryptographic self-test was performed.

5062(S): A kernel-mode cryptographic self-test was performed.

5057(F): A cryptographic primitive operation failed.

5060(F): Verification operation failed.

5061(S, F): Cryptographic operation.

6281(F): Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error.

6410(F): Code integrity determined that a file does not meet the security requirements to load into a process.

1100(S): The event logging service has shut down.

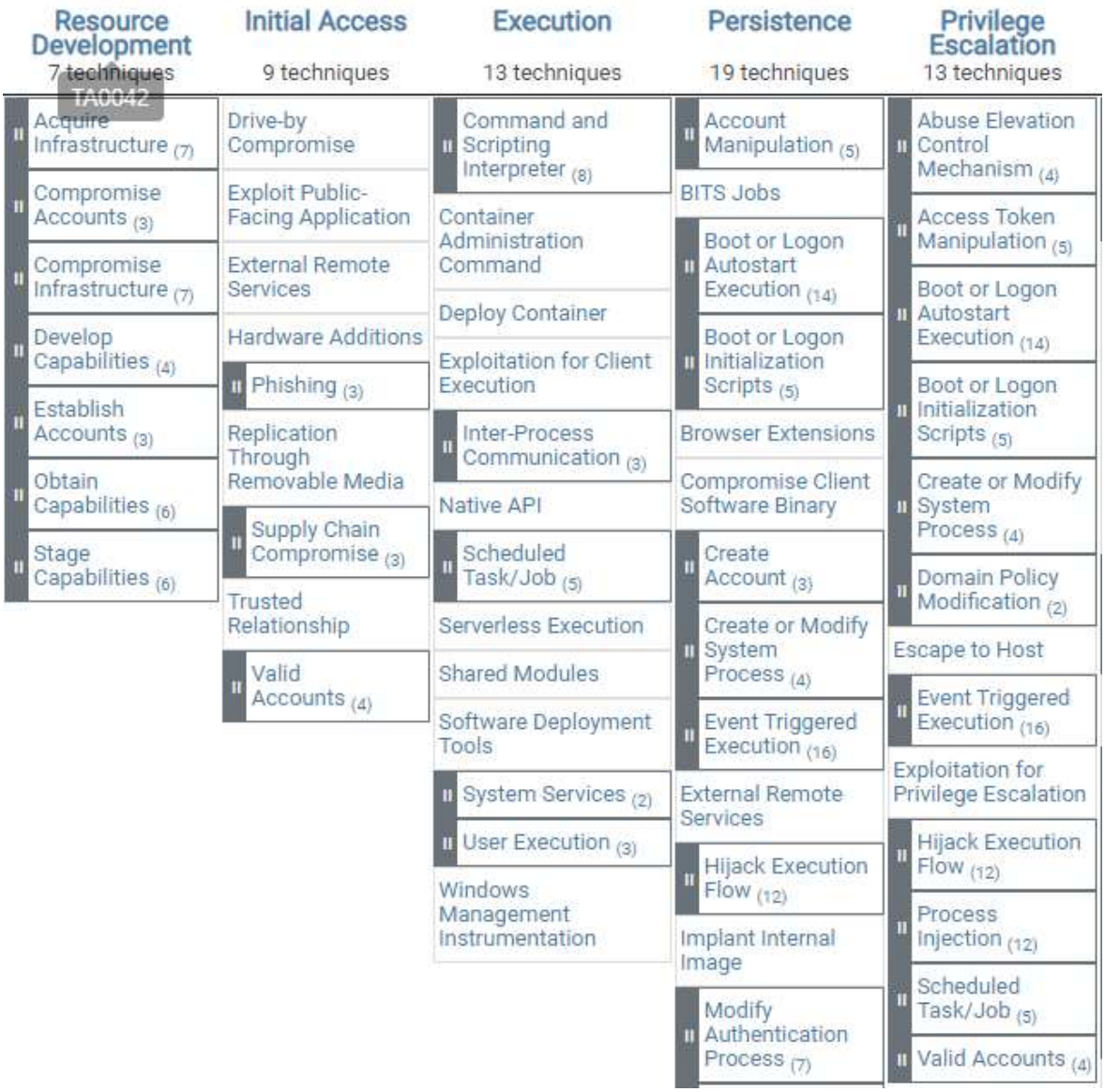
1102(S): The audit log was cleared.

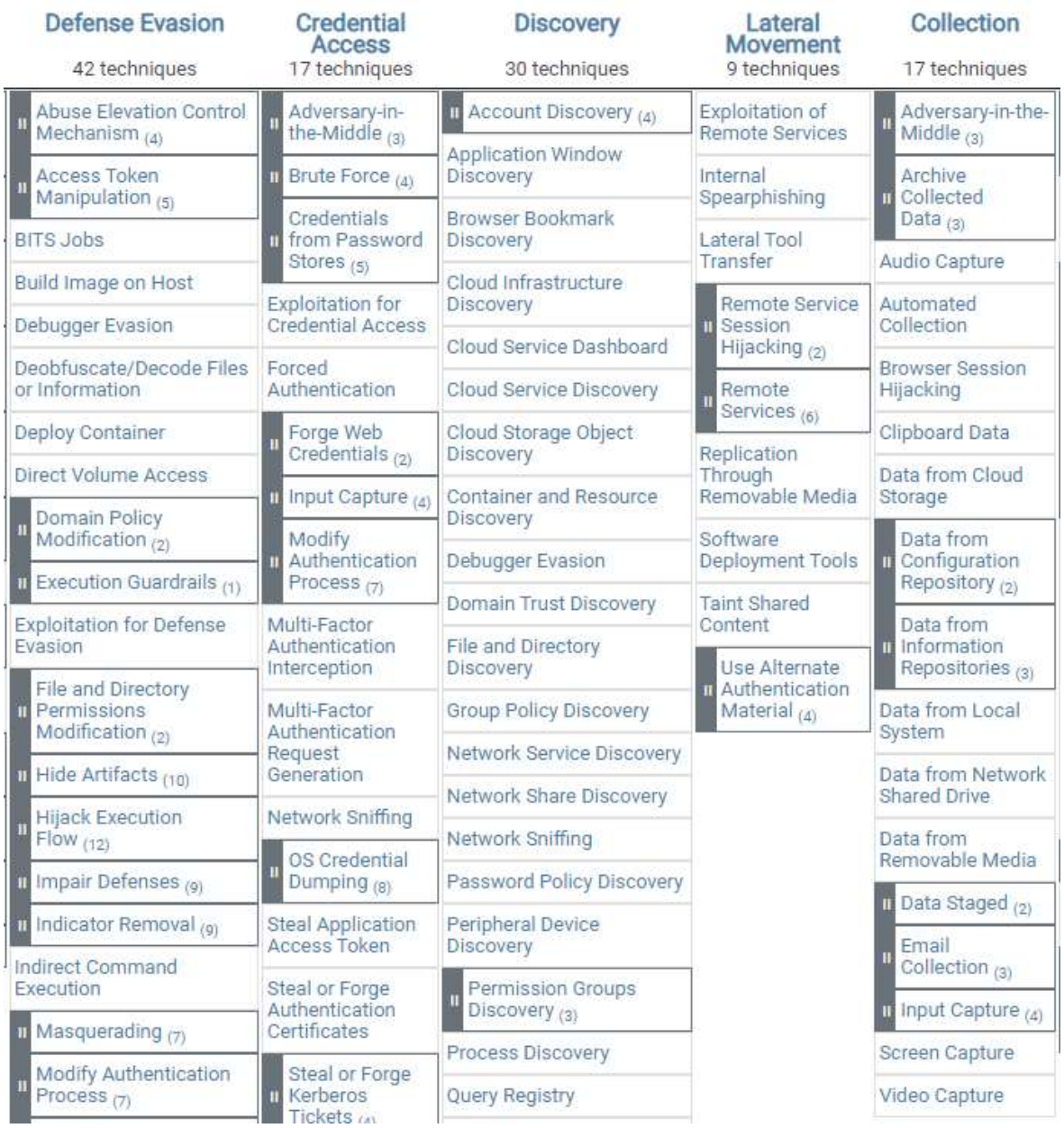
1104(S): The security log is now full.

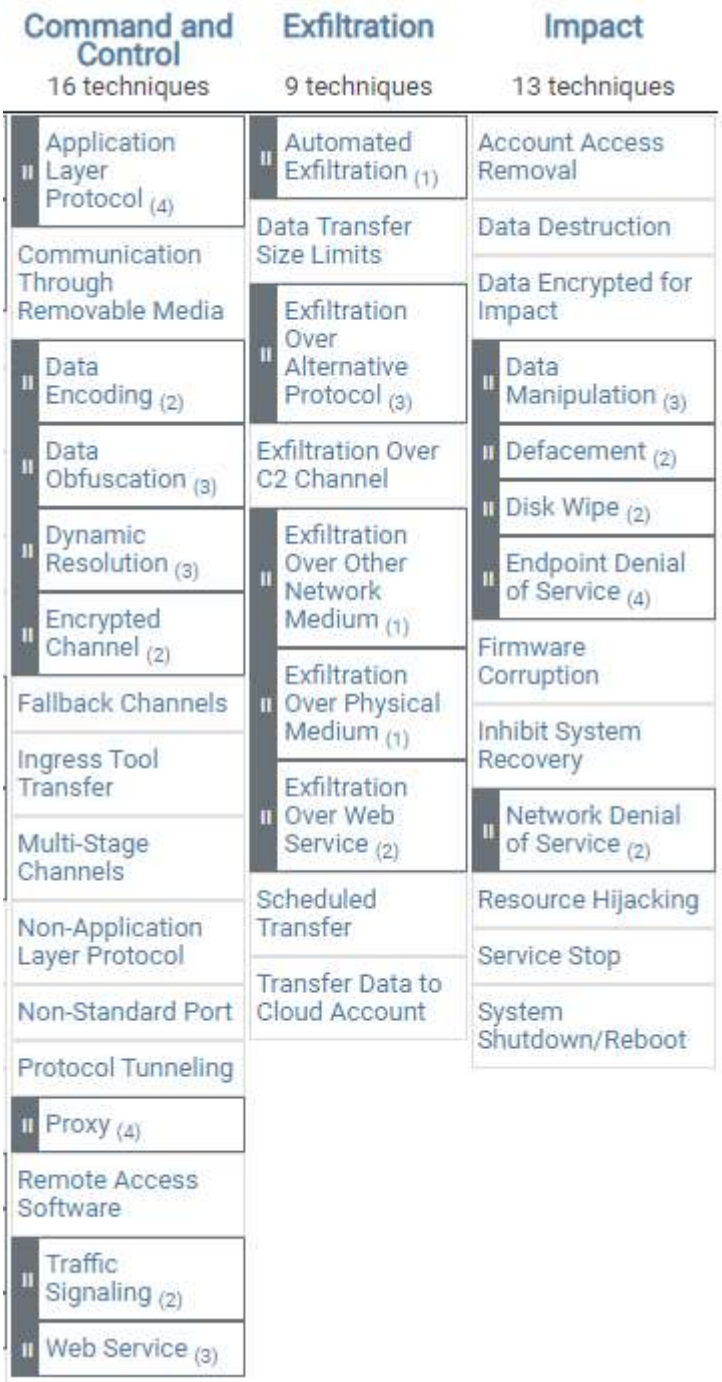
1105(S): Event log automatic backup.

1108(S): The event logging service encountered an error while processing an incoming event published from %1.

Anlagen, MITRE




Defense Evasion
42 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (10)
Hijack Execution Flow (12)
Impair Defenses (9)
Indicator Removal (9)
Indirect Command Execution
Masquerading (7)
Modify Authentication Process (7)
Credential Access
17 techniques
Adversary-in-the-Middle (3)
Brute Force (4)
Credentials from Password Stores (5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (7)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (4)
Discovery
30 techniques
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Adversary-in-the-Middle (3)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (2)
Data from Information Repositories (3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Screen Capture
Video Capture


Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (2)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

Anlagen, Ransomware-Gruppen

0Mega, Abrahams_Ax, Agl0Bgvycg, Ako, Alphv, Arvinclub, Atomsilo, Avaddon, Avos, Avoslocker, Aztroteam, Babuk-Locker, Babyduck, Bianlian, Blackbasta, Blackbyte, Blackmatter, Blackshadow, Blacktor, Bluesky, Bonacigroup, Cheers, Clop, Conti, Cooming, Crylock, Cuba, Daixin, Darkangel, Darkside, Dataleak, Diavol, Donutleaks, Doppelpaymer, Ech0Raix, Endurance, Entropy, Ep918, Everest, Exorcist, Freecivilian, Fsteam, Grief, Groove, Hades, Haron, Hellokitty, Hive, Hotarus, Icefire, Justice_Blade, Karakurt, Karma, KelvinSecurity, Lapsus$, Lilith, Lockbit, Lockbit3, Lolnek, Lorenz, Lv, Mallox, Maze, Mbc, Medusa, Midas, Moisha, Monte, Monti, Mount-Locker, Mydecryptor, N3Tworm, Nefilim, Nemty, Netwalker, Nightsky, Nokoyawa, Onepercent, Pandora, Pay2Key, Payloadbin, Play, Prolock, Prometheus, Pysa, Qilin, Qlocker, Quantum, Ragnarlocker, Ragnarok, Ramp, Ransomcartel, Ransomexx, Ransomhouse, Ranzy, Redalert, Relic, Revil, Robinhood, Rook, Royal, Rransom, Sabbath, Snatch, Solidbit, Sparta, Spook, Stormous, Suncrypt, Synack, Unknown, Unsafe, Vfokx, Vicesociety, Vsop, Xinglocker, Xinof, Yanluowang, BlogXX, Mindware, Izis, MosesStaff, IndustrialSpy

Anlagen, Tools und Befehle

Initial Access: Mail with Zip containing doc pdf or xls file

Discovery: Netcat, net user /domain; net group /domain; net.exe view /all; ipconfig.exe /all; arp.exe -a; cmd.exe /c set; cmd.exe /c set; whoami.exe /all; net.exe share; nslookup.exe; net.exe localgroup; netstat.exe -nao; route.exe print; BloodHound; Seatbelt; powershell /c nltest /dclist: ; nltest /domain_trusts ; cmdkey /list ; net group 'Domain Admins' /domain ; net group 'Enterprise Admins' /domain ; net localgroup Administrators /domain ; net localgroup Administrators ; powershell /c Get-WmiObject win32_service -ComputerName localhost | Where-Object {$_.PathName -notmatch 'c:\\win'} | select Name, DisplayName, State, PathName | findstr 'Running'

Persistence: users created (temp, r admin); users added to groups (administrators); exploit calc (cmd.exe /q /c calc.exe); scheduled task (schtasks.exe with powershell.exe -Command); installation of System Services (SecurityHealthService, Sense, sppsvc, WdBoot, WdFilter, WdNisDrv, WdNisSvc, WinDefend, wscsvc, vmicvss, vmvss, VSS, EventLog)

Privilege Escalation: PrintNightmare (CVE), exploit calc maybe dll injection, modify group policys

Defense Evasion: modify group policys; regsvr32.exe (execute malicious DLL); deleting files (batch, txt, zip, bin files, cmd.exe /C del ...., mod reg, disable defender (.bat scripts, powershell -ExecutionPolicy Bypass DisableAntiSpyware, -DisableRealtimeMonitoring, Uninstall-WindowsFeature -Name Windows-Defender); firewall mod (.bat scripts), cmd.exe /C net user [...] /delete; sc config ... start= disabled; sc stop; bat file with PsExec (wmic service where [...] call delete; wmic process where [...] call delete; cmd /c wmic service/product where call terminate, call uninstall /nointeractive); powershell.exe -c stop-servive...; cmd.exe /c .... -DisableIOAVProtection

Credential Access: Mimikatz

Lateral Movement: BITSAdmin, Coroxy, PsExec, RDP x2, WMI

Execution: PowerShell (encoded commands), CMD, WMI (Invoke-TotalExec, PATH AntiVirusProduct, AntiSpywareProduct, FirewallProduct Get /value), PsExec for remote hosts

Exfiltration: Cobeacon, Rclone, Mega.io

C&C: Cobeacon x2, Qakbot x2, TeamViewer, Anyconnect

Impact: Delete shadowcopy with vssadmin.exe x2 (wevtutil.exe cl..., wbadmin.exe delete systemstatebackup/catalog -quiet, vssadmin.exe delete shadows /all /quiet, wmic.exe shadowcopy /nointeractive oder delete, bcdedit.exe /set {default} bootstatuspolicy ignore-allfailures oder recoveryenabled no, stoping services (sc stop, taskkill [...] backup, GxBlr, GxCIMgr, GxCVD, GxFWD, GxVss, memtas, mepocs, msexchange, sophos, sql, svc$, veeam, vss, agntsvc, dbeng50, dbsnmp, encsvc, excel, firefox, infopath, isqlplussvc, msaccess, mspub, mydesktopqos, mydesktopservice, notepad, ocautoupds, ocomm, ocssd, onenote, oracle, outlook, powerpnt, registry, sqbcoreservice, steam, synctime, tbirdconfig, thebat, thunderbird, visio, winword, wordpad, xfssvccon); delete event logs (system, security, application); stops services (windefend, msmpsvc, kavsvc, antivirservice, zhudongfungyu, vmm, vmwp, sql, sap, oracle, mepocs, veeam, backup, vss, msexchange, mysql, sophos, pdfservice, backupexec, gxblr, gxvss, gxclmgrs, gxvcd, gxcimgr, gxmmm, gxvsshwprov, gxfwd, sap, qbcfmonitorservice, qbidpservice, acronis-agent, veeam, mvarmor, acrsch2svc; stops process (dbsnmp, dbeng50, bedbh, excel, encsvc, visios, firefox, isqlplussvc, mspub, mydesktopqos, notepad, ocautoupds, ocomm, ocssd, onenote, outlook, sqbcoreservice, sql, steam, tbirdconfig, thunderbird, winword, wordpad, xfssvccon, vxmon, benetns, bengien, pvlsvr, raw_agent_svc, cagservice, sap, qbidpservice, qbcfmonitorservice, teamviewer_service, teamviewer, tv_w32, tv_x64, cvd, saphostexec, sapstartsrv, avscc, dellsystemdetect, enterpriseclient, veeam, thebat, cvfwd, cvods, vsnapvss, msaccess, vaultsvc, beserver, appinfo, qbdmgrn, avagent, spooler, powerpnt, cvmountd, synctime, oracle, wscsvc, winmgmt, *sql*

Anlagen, Sigma-Regeln

whoami.exe:

```
detection:
        whoami:
          - Product Description | contains:
                - ‘whoami’
        condition: whoami
```

Zugriff auf LSASS.exe:

```
detection:
        lsass:
          - TargetImage | endswith:
                - ‘lsass.exe’
          - GrandedAccess: 0x1010
        condition: lsass
```

Event Logs gelöscht:

```
detection:
        wevutil:
          - Process Name:
                - ‘wevtutil.exe’
          - Process CommandLine | contains:
                - ‘cl’
                - ‘system’
                - ‘security’
                - ‘application’
        condition: wevutil
```

Shadowcopies gelöscht:

```
detection:
        tools:
          - Process Name:
                - ‘vssadmin.exe’
                - ‘wmic.exe’
        parameters:
          - Process CommandLine | contains:
                - ‘delete’
                - ‘shadow’
                - ‘SHADOW’
                - ‘/nointeractive’
        condition: tools and parameters
```

Automatische Reperatur deaktivieren:

```
Detection:
        bcdedit:
          - Process Name:
                - ‘bcdedit.exe’
          - Process CommandLine | contains:
                - ‘/set’
                - ‘{default}’
                - ‘recoveryenabled no’
                - ‘bootstatuspolicy ignoreallfailures’
        condition: bcdedit
```

Windows Defender deaktivieren:

```
detection:
        powershell:
          - Process Name:
                - ‘powershell.exe’
          - Process CommandLine | contains:
                - ‘DisableRealtimeMonitoring 1’
                - ‘DisableAntiSpyware -value 1’
                - ‘Uninstall-WindowsFeature -Name Windows-Defender’
        condition: powershell
```

Informationen zu Sicherheitsprodukten:

```
detection:
        wmic:
          - Process Name:
                - ‘wmic.exe’
          - Process CommandLine | contains:
                - ‘get /value’
                - ‘AntiVirusProduct’
                - ‘AntiSpywareProduct’
                - ‘FirewallProduct’
        condition: wmic
```

Anlagen, Beigelegte Dokumente

Bachelorarbeit

-> **mapsinfos**

- -> **bearbeitete_dokumente**
  - -> **„gruppenname“_victims.txt** enthalten alle betroffenen Unternehmen ohne Adresse und Branche.
  - -> **„gruppenname“_victims_enriched.txt** enthalten alle betroffenen Unternehmen mit angereicherten Informationen.
  - -> **„gruppenname“_mod.txt** enthalten alle betroffenen Unternehmen, zu denen eine Adresse und Branche gefunden wurden.
- -> **all_victims.json** enthält alle betroffenen Unternehmen zu allen Gruppen.
- -> **posts*.json** enthält je Datei 50 betroffene Unternehmen mit angereicherten Informationen.
- -> **geckodriver** ist der genutzte Firefoxtreiber für Selenium.
- -> **filesplitter.py** ist das Pythonskript, um die Unternehmen von all_victims.txt in die posts*.txt Dateien zu unterteilen.
- -> **gmapsinfos.py** ist das Pythonskript, um die Daten in posts*.txt durch Google Maps anzureichern
- -> **victim_analyser.py** ist das Pythonskript, um die Anzahl Einträge als der Gesamtübersicht von all_victims.json der einzelnen Gruppen auszuwerten.

-> **scrapers**

- -> **helpers**
  - -> **json_parser.py** ist das Pythonskript, welches die Ergebnisse aus den Scrapern in eine JSON-Datei in einem einheitlichem Format schreibt.
- -> **„gruppenname“.py** sind die Pythonskripte, welche die betroffenen Unternehmen von den Leak-Seiten der jeweiligen Gruppe beziehen.

-> **übersicht_ttps.xlsx** ist das Excel Dokument, wo die TTPs notiert, priorisiert und analysiert wurden, ebenso existiert hier eine Übersicht von Befehlen und Tools.

Selbstständigkeitserklärung

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

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

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

Würzburg, den 05.02.2023

Kim Rikard Nordqvist