事業継続を脅かす
新たなランサムウェア攻撃について

～「人手によるランサムウェア攻撃」と「二重の脅迫」～

独立行政法人情報処理推進機構 セキュリティセンター

2020 年 8 月 20 日

目次

1. はじめに

サイバー攻撃には多様なものが存在し、攻撃者の目的によってその手口や攻撃手法は様々である。これらサイバー攻撃の中に、ランサムウェアと呼ばれるウイルスを使用し、攻撃先の端末上のデータを暗号化する等して、その復旧と引き換えに（身代金として）金銭を脅し取ろうとするサイバー攻撃（以降、ランサムウェア攻撃）が存在する。

2018 年[1]～2019 年頃[2]から、攻撃者の主な目的が金銭である点は変わらないものの、ランサムウェア攻撃の手口に大きく変化が見られ、特に企業・組織の事業活動への脅威が増大している。

具体的には、次の 2 つの新たな攻撃方法が用いられるようになっている。

- 人手によるランサムウェア攻撃 （human-operated ransomware attacks）
  - ウイルスを添付したメールを機械的にばらまくような手口と異なり、諜報活動を目的とする「標的型サイバー攻撃」と同様の方法、すなわち、攻撃者自身が様々な攻撃手法を駆使して、企業・組織のネットワークへひそかに侵入し、侵入後の侵害範囲拡大等を行う。そして、事業継続に関わるシステムや、機微情報等が保存されている端末やサーバを探し出してランサムウェアに感染させたり、ドメインコントローラのような管理サーバを乗っ取って、一斉に企業・組織内の端末やサーバをランサムウェアに感染させたりする攻撃方法である。復旧を阻害するため、バックアップ等も同時に狙われることがある。一般的に、攻撃の進行を検知しにくく、判明した時点では既に大きな被害が生じている場合がある。
  - 標的型ランサム[3,4]、システム侵入型ランサム[5]等とも呼ばれている。

- 二重の脅迫 （double extortion）
  - ランサムウェアにより暗号化したデータを復旧するための身代金の要求に加え、暗号化する前にデータを窃取しておき、支払わなければデータを公開する等と脅迫する攻撃方法である。
  - 暴露型ランサム[6]等とも呼ばれている。

攻撃者は、企業・組織が金銭を支払わざるを得ないような状況を作り上げることで、より確実に、かつ高額な身代金を得ようとしているものと推測される。実際に海外の企業・組織では身代金を払ってシステムの復旧を行った事例もあり、攻撃者のモチベーションは高いものと考えられ、この攻撃方法を取り入れる攻撃グループが増えている。要求される身代金としては、数千万円から数億円[7]という規模の事例が公開されている。

2020 年 8 月、現時点で、これらのランサムウェア攻撃によって、国内企業や、国内企業の海外関係会社の被害が明らかになっている。この攻撃は、規模の大小、扱っている情報の機密性等に関わらず、IT システムにより事業が成り立っている、あらゆる企業・組織が標的となりうる、非常に注意を要する脅威となっている。また、大金が絡むことから、攻撃者が集まり、組織化し、今後ますます脅威が増大していく可能性がある。

本書では、この脅威について理解と注意を促すべく、まず 2 章で攻撃の近年の変化について説明し、3 章で被害事例を紹介する。4 章では、事例等からこれらの攻撃者の手口を示し、5 章に対策を述べる。また、攻撃者の動向の一部を 7 章に参考情報として示す。

企業の経営者は、事業の継続を脅かすような大規模な被害が生じ得る可能性があることを認識し、事業継続計画（BCP）の策定等において留意すべきであろうと考える。また、企業・組織のセキュリティを扱う方は、従来のランサムウェア攻撃対策に加え、標的型サイバー攻撃と同等の対策が必要であると認識した上で、対策を検討していただきたい。

本書の対象読者

本書では、次の方々を主な対象読者と想定している。

- 企業の経営層の方
- 企業の CSIRT[8]や ISAC[9]等、組織のセキュリティを扱う部門の方

2. ランサムウェア攻撃

本章では、ランサムウェアについて説明するとともに、新たなランサムウェア攻撃が、どのように変化したかについて説明する。

2-1. ランサムウェアとは

ランサムウェアとは、パソコン等の端末およびネットワーク接続された共有フォルダ等に保管されたファイルを、利用者の意図に沿わず暗号化して使用不可にする、または画面ロック等により操作不可とするウイルスの総称である。それらを復旧することと引き換えに、身代金を支払うように促す脅迫メッセージを表示するソフトウェアであることから、「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語で、ランサムウェアと呼ばれている。

ランサムウェアは多くの種類があり、使用不可にする対象によって大別すると、ファイルを暗号化する「ファイル暗号化型」、端末の操作をできないようにロックをかける「端末ロック型」の２タイプがある（表 2-1）[10]。

いずれのタイプのランサムウェアにおいても、攻撃者の目的は同じで、復旧することと引き換えに金銭を得ることである。

表 2-1 ランサムウェアのタイプ

項番	ランサムウェアのタイプ	使用不可にする対象	ランサムウェアの例
1	ファイル暗号化型	画像、文書、データ等のファイル	WannaCryptor 等
2	端末ロック型	端末そのもの	Android 端末のランサムウェア等

ランサムウェアの被害事例は、ファイル暗号化型によるものが多い。ファイル暗号化型のランサムウェアに感染させられた場合、パソコン等の端末に保存されているファイルの暗号化だけでなく、その端末からアクセス可能なファイルサーバや、クラウド上のファイルも暗号化され、使用できなくなる場合がある。更に、2017 年に世界中で流行した「WannaCryptor[11]」（WannaCry、WannaCrypt、WCry 等とも呼ばれる）は、自身を複製し、自動で同一ネットワーク上のパソコンやサーバに感染を拡大する機能（以降、ワーム機能）を有しており、大きな被害を受けた企業もあった。

身代金の要求は攻撃者が用意したウェブサイトやメールを使って、攻撃者と連絡することを求められることが多く、支払い手段としては、追跡のしにくい暗号資産[12]を要求されるといった傾向がある。

例として、WannaCryptor に感染させられた端末の画面を図 2-1 に示す。

図 2-1 WannaCryptor に感染させられた端末の画面

参考：ランサムウェアのような動作をするシステム破壊型ウイルス

ランサムウェアとは別に、ランサムウェアのような動作をする、システム破壊型ウイルス（例えば「NotPetya[13]」というウイルス）の存在が確認されている。このウイルスは、OS やデータを破壊しつつ、復旧のためと偽って身代金を要求する。攻撃者の本来の目的が、システムの破壊であり、それを金銭目的であるかのようにカモフラージュしているのか、あるいは被害者が（復旧できると思い込み）騙されて金銭を支払うことを狙っているのかは不明である。

2-2. 従来のランサムウェア攻撃

これまでのランサムウェア攻撃では、攻撃者は、明確な標的を定めず、ウイルスを添付したメールのばらまき、悪意のあるウェブサイトの閲覧者への攻撃、ワーム機能等によって、個人、企業・組織を問わず、また、端末やサーバといった対象を問わず、ランサムウェアへの感染を試みていた。

これは、不特定多数へ広く攻撃を行い、運悪く感染し、支払いに応じる被害者から身代金を得ようという戦略であった。現時点においても、この攻撃が無くなったわけではないため、引き続き注意が必要である。

2-3. 新たなランサムウェア攻撃

近年、従来のランサムウェア攻撃とは異なる、次の 2 つの新たな攻撃方法が使用されている。これにより、企業・組織の事業継続に関わる、非常に危険な脅威となっている。

- 人手によるランサムウェア攻撃 （human-operated ransomware attacks）
- 二重の脅迫 （double extortion）

攻撃者は、企業・組織を標的とし、これらの攻撃方法を用いて、事業継続のため金銭を支払わざるを得ない状況を作り上げ、より確実に、かつ高額な身代金を得ようとしている。

続いて、この 2 つの攻撃方法について説明する。図 2-2 は、従来のランサムウェア攻撃と、新たなランサムウェア攻撃の差異のイメージ図である。

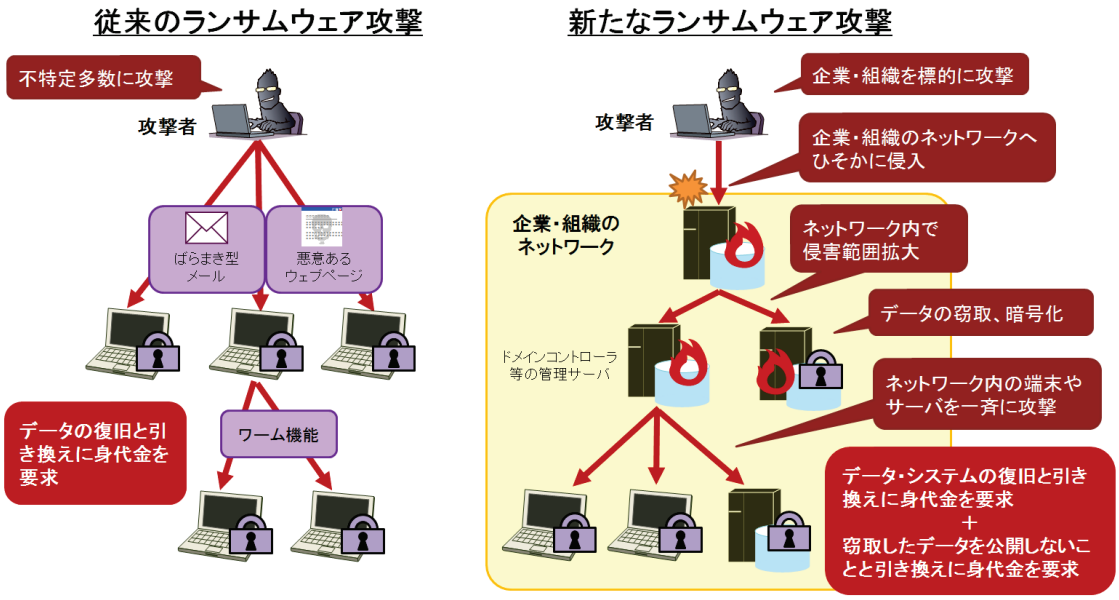

図 2-2 従来の／新たなランサムウェア攻撃の差異

2-3-1. 人手によるランサムウェア攻撃

「人手によるランサムウェア攻撃」(海外では human-operated ransomware attacks[14]等と呼ばれる）では、諜報活動を目的とする標的型サイバー攻撃と同様、攻撃者自身が様々な攻撃手法を駆使して、企業・組織のネットワークへの侵入、侵入後の侵害範囲拡大（側方移動、lateral movement）等をひそかに進める。そして、事業継続に関わるシステムや、機微情報が保存されている端末やサーバ等を探し出してランサムウェアに感染させたり、ドメインコントローラのような管理サーバを乗っ取って、一斉に企業・組織内の端末やサーバをランサムウェアに感染させたりする攻撃が行われる。データやシステムの復旧を阻害するため、バックアップ等も同時に狙われることがある [15]。

攻撃者は、企業・組織の一般的なセキュリティ対策が行われていることを前提として、それらを潜り抜けるように攻撃を進めるため、一般的に、攻撃の進行を検知しにくく、判明した時点では既に大きな被害が生じている場合がある。

この攻撃方法は 2018 年頃から確認されている。人手によるランサムウェア攻撃は、従来のランサムウェア攻撃に比べて、企業・組織のネットワークへの侵入や侵害範囲拡大等、攻撃者の手間はかかるものの、企業・組織の事業継続を妨げるような被害を与えることが可能となる場合があり、身代金として、手間に見合った大金を得られる可能性がある。また、大金が絡むことから、ネットワークへの侵入を行う者、ランサムウェアを提供する者といった分業や組織化が進み [16]、巧妙化していることが懸念される。

2-3-2. 二重の脅迫

「二重の脅迫」（海外では double extortion[17]等と呼ばれる）とは、ランサムウェアにより暗号化したデータを復旧するための身代金要求に加え、暗号化する前にデータを窃取しておき、支払わなければデータを公開する等と二重に脅迫する攻撃方法である。

この攻撃方法は 2019 年末頃から確認されており、身代金の支払いに応じなかった企業・組織について、攻撃者によって窃取されたデータがインターネット上で公開された複数の事例が確認されている。

従来のランサムウェア攻撃への対策として、企業・組織はデータのバックアップを厳重に行うとともに、バックアップをオフラインで保存する等、防御策を進めてきた。攻撃者は、この防御策への更なる対抗策として、データの窃取と公開による脅迫という、新たな攻撃方法を取り入れたものと考えられる。

窃取されたデータは、例えば、攻撃者がインターネットやダークウェブに設置した、データ公開のためのウェブサイト（以降、リークサイト）にて公開される。窃取したデータを一度に全て公開するのではなく、データの一部を公開し、日数の経過に伴い徐々に公開範囲を広げると脅す場合もある。これは、データを窃取した事実や、データを公開することがブラフ（はったり）ではないことを示し、企業・組織に対して身代金の支払いへのプレッシャーを強く与えるための、悪質な手口である。

身代金を支払わせるため、攻撃者がリークサイトで積極的に次のような呼びかけを行っている例も確認している。

- 被害企業・組織が自力でデータやシステムを復旧するのにかかる平均的な費用よりも、身代金を支払った方が安価であるという主張
- 交渉に応じない場合の、データを公開するまでの日数（スケジュール）の予告

3. 被害事例

本章では、公開情報となっている被害事例から、人手によるランサムウェア攻撃によるものを 3 件、二重の脅迫によるものを 1 件紹介する。

3-1. 人手によるランサムウェア攻撃による被害事例

3-1-1. 攻撃対象企業に特化したランサムウェアが使用された事例

2020 年 6 月、アルゼンチンの配電会社に対してランサムウェア攻撃が行われたと報じられた [18]。本事例では、ランサムウェアにより、システムに障害が発生し、カスタマーサービスに影響が出たとされている。リモートデスクトップサービスがインターネット上に公開された端末がいくつかあったというが、これがネットワークへの侵入の原因であるかは断定されていない [19]。

本事例では EKANS[20]と呼ばれるランサムウェアが使用されたとされている。この時期に確認された EKANS は、起動されると、特定企業の内部ネットワークでのみ有効なドメイン名の名前解決を行い、更に名前解決して得られた IP アドレスをチェックし、結果が期待通りである場合のみデータの暗号化を行う動作となっていた [21]。すなわち、攻撃者が、この企業内の端末でのみ動作するように特化したランサムウェアを作成したであろうことを示している。被害を与える範囲を限定することで、第三者への表面化を避けようとしたのか、サンドボックス型セキュリティ機器の検知を逃れようとしたのか等、理由は不明であるが、意図的な行動であったことは確かだと言える。

3-1-2. 18,000 台以上の端末が攻撃された事例

2020 年 7 月、アルゼンチンの最大級のインターネットサービスプロバイダに対してランサムウェア攻撃が行われ、約 11 万モネロ（約 753 万ドル）の身代金が要求されたと報じられた [22]。本事例では攻撃者がドメインコントローラの管理者権限を奪取し、そこから組織内の 18,000 台以上もの端末をランサムウェアに感染させたとされている。同社の、顧客のためのインターネット接続サービスや固定電話、ケーブルテレビへの影響はなかったものの、同社の公式ウェブサイトはダウンしたとのことである。

3-1-3. データ復旧のため被害組織が身代金を支払う選択をした事例

2019 年 12 月、オランダの大学に対してランサムウェア攻撃が行われたと報じられた [23]。本事例では、被害にあった大学は 30 ビットコイン（約 22 万ドル）を攻撃者へ支払って、重大（critical）なシステムを復旧したという。攻撃者は、攻撃メールを起点に同大学のネットワークへ侵入し、脆弱性を悪用して管理者権限を奪取し、同大学のネットワーク内に

侵害範囲を拡大して、267 台のサーバと、その一部のバックアップをランサムウェアに感染させたとされている。

攻撃者の収益は、更なる別の被害者への攻撃の資金源や動機となりうるといった理由から、一般的にはランサムウェア攻撃の被害者は身代金を支払うべきではないとされている。しかし、この事例においては、「研究等のデータを失い、試験や給与支払いを遅延させながら、侵害された全てのシステムを再構築する」という事態を避けるための決断が行われた、とのことであった。

3-2. 二重の脅迫による被害事例

2020 年 4 月、アメリカの航空機メンテナンス会社に対してランサムウェア攻撃が行われたと報じられた [24]。本事例では、攻撃者は同社のネットワークへリモートデスクトップサービスを介して侵入し、その後、ドメイン管理者のアカウントを侵害して、同社のドメインコントローラ等にアクセスした。また、同社のシステムは Maze と呼ばれるランサムウェアに感染させられ、システム内のデータが暗号化された。

更に、この攻撃では、攻撃者によって 1.5TB（攻撃者の主張による）のデータが窃取され、攻撃者のリークサイトで、その一部が公開された。図 3-1 は、リークサイト上で同社を脅迫するために作成されたウェブページである。ページの上部に「1% published」と書かれており、これは実際に窃取した情報の一部だと示している。また、「近い将来この企業の情報をリリースする準備ができている」とも書かれており、身代金が支払われなかった場合、追加の情報を公開することを示唆している。

本事例で確認された更なる事実として、攻撃者が、攻撃後も同社のネットワーク内に潜伏し、データを窃取し続けていた点が挙げられる。具体的には、本件インシデントの調査対応作業に関する同社のファイルまでもが、リークサイトで公開されていたとのことである [25]。

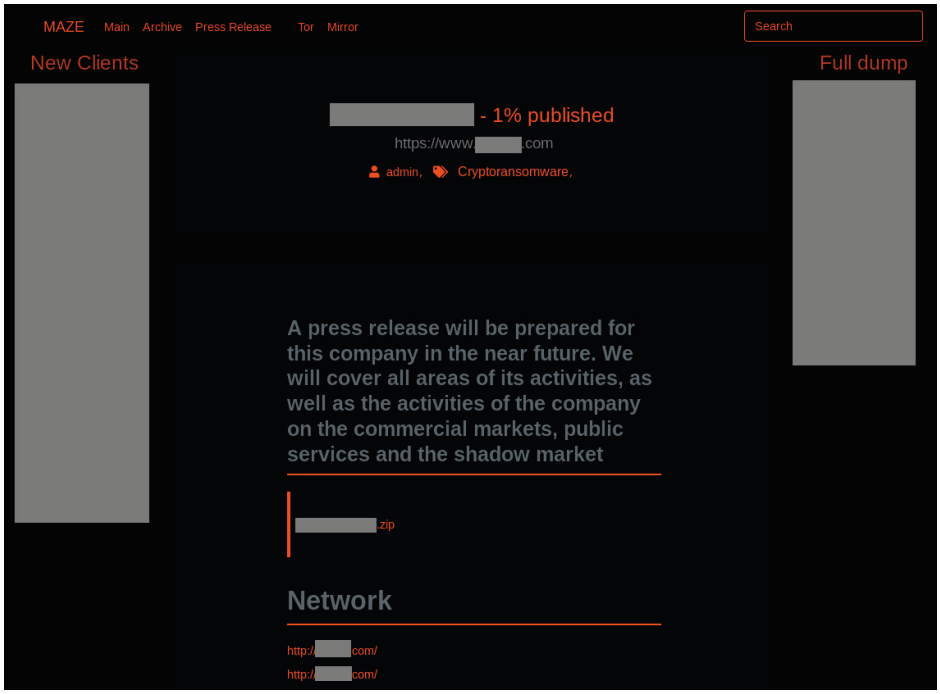

図 3-1 リークサイト上の脅迫ページ

4. 攻撃手口

公開情報を整理すると、新たなランサムウェア攻撃において、攻撃者の活動は次の 5 つのステップに分けることができる。本章では、各ステップで用いられると推測される攻撃手口について紹介する。

1. ネットワークへの侵入
2. ネットワーク内の侵害範囲拡大
3. データの窃取 （※二重の脅迫の場合）
4. データの暗号化・システム停止
5. 窃取したデータの公開 （※二重の脅迫の場合）

また、標的型サイバー攻撃全般で使用される攻撃手口について、米国 MITRE 社が「ATT&CK[26]」というデータベース（知識ベース）を公開している。新たなランサムウェア攻撃においても、これら手口が用いられることが考えられるため、関係する情報として、併せて紹介する。

4-1. ネットワークへの侵入

攻撃は、攻撃者が企業・組織のネットワークへ侵入するところから始まる。これは、従来のランサムウェア攻撃のような、ばらまかれたメールに添付されたウイルス（ランサムウェア）を受信者が実行してしまうことで、その端末（のみ）がランサムウェアに感染させられる手口とは大きく異なる点である。

被害事例に関する報道[23,25,27]やセキュリティベンダ等のレポート[28,29]等から、インターネット上に公開されているサーバや機器等に対し、設定の不備や脆弱性を悪用する手口や、攻撃メールを送り付ける手口が確認されている。例えば、次に挙げるような侵入手口が事例として報告されている。

- リモートデスクトップサービスを経由した侵入
  - 攻撃者は、企業・組織がインターネット上に公開しているリモートデスクトップサービスを調査し、アクセス制御、認証に関する設定、パスワードの強度が不十分であることを狙い、認証を突破し、侵入する。
  - セキュリティに関する職員が手薄であることを期待し、土曜日に攻撃を開始する。

- VPN 装置の脆弱性を悪用した侵入
  - 攻撃者は、企業・組織が使用している、脆弱性が残存する VPN 装置の脆弱性を悪用して侵入する。
  - 例えば、次のような脆弱性を悪用するとされている。
    - 認証情報を窃取することが可能な VPN 装置の脆弱性（CVE-2018-13379, CVE-2019-11510 等）。攻撃者は窃取した認証情報を用いて侵入することが可能となる。
    - 遠隔で任意のコードを実行することが可能な VPN 装置の脆弱性（CVE-2019-1579, CVE-2019-19781 等）。
  - 脆弱性を解消済みであり、攻撃を確認できていなくとも、脆弱であった期間に認証情報が窃取されていた可能性がある。

- 不正なメールを送り付けて遠隔操作ウイルス等に感染させ、端末を乗っ取ることによる侵入
  - 攻撃者は、企業・組織へ遠隔操作ウイルス等を添付したメールや、遠隔操作ウイルス等をダウンロードさせる URL リンクを記載したメールを送り付ける。受信者が不用意に添付ファイル等を開くことで、遠隔操作ウイルス等へ感染させられ、端末が乗っ取られる。攻撃者は、その端末を足掛かりとして組織内ネットワークへ侵入する。

ランサムウェア攻撃に限らず、サイバー攻撃における企業・組織のネットワークへの侵入経路として、インターネットからアクセス可能な様々なネットワーク機器や、サーバ等の脆弱性が悪用される事例が多く公表されている。これらの機器については、脆弱性の解消等による対策を最優先で行う必要がある。また、リモートデスクトップサービスや VPN 接続のアカウントについては、フィッシング攻撃やリスト型攻撃によって狙われることも考えられるため、認証情報の適切な管理・設定も重要である。

2019 年頃には、IT システム運用保守等のサービスを提供している MSP（マネージドサービスプロバイダ）を経由し、企業・組織がランサムウェアに感染させられたという事例が明らかになっている。侵入経路の可能性として、見落とすべきではないと思われる。

この他、企業・組織のネットワークへの侵入手口と緩和策については、MITRE 社の ATT&CK 内「Initial Access[30]」も参考情報としていただきたい。

4-2. ネットワーク内の侵害範囲拡大

攻撃者は、企業・組織のネットワークへの侵入に成功した後、データの窃取やランサムウェアに感染させる範囲を拡げる目的で、ネットワーク内の侵害範囲拡大を行う。標的型サイバー攻撃同様、ネットワーク構成の把握や管理者権限の奪取を行い、これらの情報を基にして、機微情報等が保存されている端末やサーバ、ドメインコントローラ等の管理サーバ、そしてバックアップ用のサーバ等を狙い、移動を行うと考えられる。

セキュリティベンダによると、これらの侵害範囲拡大の活動で、攻撃者は標的型サイバー攻撃と同様のツールや手口を用いるとのことである[4]。侵害範囲拡大の手口と緩和策については MITRE 社の ATT&CK 内「Privilege Escalation[31]」や「Credential Access[32]」、「Discovery[33]」、「Lateral Movement[34]」等を参照いただきたい。

4-3. データの窃取

二重の脅迫を狙っている場合、攻撃者は、企業・組織の機微情報等の窃取も行う。遠隔操作ウイルスを使用するなど、攻撃者自身の操作によって、データの探索・収集、攻撃者のサーバやクラウドストレージへのアップロード等が行われるものと推測される。持ち出しの際、データの圧縮や分割といった手口も併用されるであろう。

データの窃取の手口と緩和策については MITRE 社の ATT&CK 内「Collection[35]」や「Exfiltration[36]」等を参照いただきたい。特に、不審な大量のファイルアクセスや、圧縮ファイルが生成されるといった挙動、組織内から組織外に向かうネットワークトラフィックの制限や急な増加を検知するといった対策が考えられる。

4-4. データの暗号化・システム停止

攻撃者は、身代金要求の脅迫のため、ランサムウェアを使用して企業・組織のデータを暗号化する。暗号化によって、システム（業務やサービス）の停止にも繋がる。場合によっては、当該企業・組織の事業継続に関わるデータやシステムが被害に遭う可能性があり、攻撃者も、まさにそれを狙っていると考えられる。バックアップデータ等による業務復旧を妨害するため、攻撃者は、ネットワーク経由で到達可能であれば、それらのデータも狙う可能性がある。

使用されている暗号方式や鍵長から考えて、データやシステムを復旧するためのツールや復号鍵等を攻撃者から入手する以外の方法で得ることは、非常に難しい仕組みとなっていると思われる。

被害事例に関する報道やセキュリティベンダ等のレポート等に、次のような手口の情報がある。

- 企業・組織内の端末を一斉にランサムウェアに感染させて暗号化する
  - 攻撃者がドメインコントローラにアクセスした事例があり、ドメインコントローラ等の管理サーバ経由で、ドメインに属する端末を一斉にランサムウェアに感染させたものと推測される。攻撃者は、企業・組織に対して事業の継続を妨げるような大規模なランサムウェア感染を引き起こすことで、企業・組織が身代金を支払わざるを得ない状況を作り上げようとしていると考えられる。
  - 組織内の端末へ一斉にランサムウェア等のウイルスを配信する手口については、MITRE 社の ATT&CK 内「Software Deployment Tools[37]」に言及がある。

- 1 台ずつランサムウェアに感染させて暗号化する
  - 攻撃者が、ネットワークで繋がった端末をリモートで操作するツールを用いて、1 台ずつランサムウェアに感染させた事例もあったとのことである [38]。

なお、MITRE 社の ATT&CK 内「Data Encrypted for Impact[39]」で、データの暗号化を行う攻撃の全般的な紹介がある。

4-5. 窃取したデータの公開

二重の脅迫が行われる場合、窃取したデータの公開方法として、リークサイトでの公開や、オークションサイトでの販売が挙げられる。

攻撃者が、窃取したデータをリークサイトで公開するにあたって、攻撃者が窃取したデータを一度に全て公開するのではなく、窃取したデータの一部を公開し、日数の経過に伴い徐々に公開するデータの範囲を広げると声明を出している場合がある。そして、攻撃者が指定した期日までに身代金が支払われない場合に、攻撃者は窃取したデータをすべて公開するとしている。

オークションサイトには、攻撃者がデータを窃取した企業・組織に関する情報と、窃取したデータに関する情報が掲載されている場合がある。オークションサイトでの攻撃者が窃取したデータの販売は、データを窃取した企業・組織から身代金が支払われない場合に、金銭を得る代替手段として用いているものと考えられる。

現時点において、リークサイトを停止させたり、リークされたデータを回収したりするような手段が存在せず、また、身代金を支払ったとしても、今後一切のリークが発生しないことが保証されるわけでもない。被害企業・組織においては、窃取されたデータの範囲の特定、ビジネス上のインパクト（顧客への影響も含む）等を見極め、最悪の状況を想定した、経営層レベルの判断と対応が必要となる。

5. 対策

新たなランサムウェア攻撃は、標的型サイバー攻撃と同様の手口で企業・組織のネットワークへ侵入し、侵害範囲を拡大し、サーバ等をランサムウェアに感染させたり、情報を窃取したりする。このため、従来のランサムウェア攻撃の対策に加え、標的型サイバー攻撃と同様の全般的な対策を行う必要がある。

事業継続のため守るべき資産（データ・システム）の特定と、リスク分析、それに見合うコストとのバランスの見極めを含む、非常に難しい課題であるが、最優先で維持する必要のあるデータ・システム等、着手できる部分から、リスク低減のための多層的な防御策を講じていただきたい。

以降、対策を検討する上で、特に重要と考えられる点を示す。

5-1. 対策全般

この脅威に限らず、サイバー攻撃から企業を守る観点で経営者が認識すべき点等について、経済産業省がガイドラインを公開している。実際の対策を進めるには、経営者のリーダーシップと組織力が必要となるため、未読であれば参照いただきたい。

- サイバーセキュリティ経営ガイドライン（経済産業省）
  - https://www.meti.go.jp/policy/netsecurity/mng_guide.html

全般的に、本件はランサムウェアに加え標的型サイバー攻撃への対策と同様であると考える必要があり、システム設計、端末・サーバ・ネットワークのセキュリティ、運用管理（監視・監査）、人的体制等で多層の対策を講じていくことが目標となる。

IPA や JPCERT/CC が公開している、従来のランサムウェア攻撃への対策情報を次に示す。これらの内容は、引き続き重要である。

- ランサムウェア対策特設ページ（IPA）
  - https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html
- ランサムウエア対策特設サイト（JPCERT/CC）
  - https://www.jpcert.or.jp/magazine/security/nomore-ransom.html

また、標的型サイバー攻撃への対策ガイドとして、IPA や JPCERT/CC が公開している次の資料も参照いただきたい。

- 『高度標的型攻撃』対策に向けたシステム設計ガイド（IPA）
  - https://www.ipa.go.jp/security/vuln/newattack.html

- 高度サイバー攻撃（APT）への備えと対応ガイド～企業や組織に薦める一連のプロセスについて（JPCERT/CC）
  - https://www.jpcert.or.jp/research/apt-guide.html
- 高度サイバー攻撃への対処におけるログの活用と分析方法
  - https://www.jpcert.or.jp/research/apt-loganalysis.html

5-2. 企業・組織のネットワークへの侵入対策

４章で紹介した通り、本件の攻撃は、攻撃者が企業・組織内のネットワークへ侵入することから始まる。従って、特に挙げるとすれば、次のような侵入対策を行うことが重要と考える [40]。これらは、必ずしも新たな投資を要するものばかりではなく、設定変更や見直しで実現できる範囲も多い。リモートデスクトップサービスの不用意な露出の停止、VPN 装置の脆弱性の解消等、悪用事例のある箇所への対策は優先的に実施していただきたい。

- 攻撃対象領域（attack surface）の最小化：インターネットからアクセス可能な、あるいは意図的に公開するサーバやネットワーク機器を最低限にするとともに、アクセス可能なプロトコルやサービスも最低限のものにする。それら装置が乗っ取られる可能性を考慮し、そこからアクセス可能な範囲を限定する。
- アクセス制御と認証：組織外からアクセスが必要な対象や範囲を特定し、限定する。強固な認証方式を使用する。アクセスや認証のログを取得し、監視する。
- 脆弱性対策：OS および利用ソフトウェア、ネットワーク機器のファームウェア等を常に最新の状態に保つ。最近は、脆弱性が公開されてから、その脆弱性を悪用する手法が出回るまでの期間が短いため、迅速に対応できるよう体制や計画を整備する。
- 拠点間ネットワーク：ランサムウェア攻撃に限らず、複数の拠点（特に海外拠点）をネットワークで接続している場合、防御の弱い拠点から侵入され、中枢が侵害される事例が散見される。必要に応じ、拠点間のアクセス制御の見直しを行う。
- 攻撃メール対策：メールによる侵入は依然として脅威である。攻撃メールへのセキュリティ装置等による対策や、従業員の啓発や訓練を行う。
- 内部対策：攻撃者による侵害範囲拡大を検知・防御するため、統合ログ管理、内部ネットワーク監視、エンドポイント監視といった仕組み（製品等）も有効だと考えられる [41]。ただし、同時に導入・運用のコストも高くなる可能性があり、まずは、これ以外に挙げた、より基本的な対策を先に実施してから検討すべきである。

5-3. データ・システムのバックアップ

事業継続のため、データやシステムのバックアップを行うことは引き続き重要な対策である。ランサムウェアの影響は感染端末のみならず、感染端末からアクセス可能な別の端末やクラウド上のデータにも及びうるため、データをバックアップする際には、次の点に留意する必要がある。

- 重要なファイルは定期的にバックアップを取得する。
- バックアップに使用する装置・媒体は、バックアップ時のみ対象機器と接続する。
- バックアップ中に感染する可能性を考慮し、バックアップに使用する装置・媒体は複数用意する。
- バックアップの妥当性（バックアップが正常に取得できているか、現状のバックアップ手法が攻撃に対して有効か）を定期的に確認する。
- データのみならず、システムの再構築を含めた、復旧計画を策定する。

なお、バックアップを取得していても、復旧においてそれを活用できないと意味がない。バックアップからのデータやシステムの復旧を迅速かつ確実に行えるように、対応フローの整備、訓練、復旧テスト等を実施しておくことも重要である。

5-4. 情報窃取とリークへの対策

情報が窃取され、意図せず公開される脅威について、次のような対策が考えられる。

- IRM（Information Rights Management）等の情報漏えい対策（情報が窃取されても被害を限定的な範囲に留める対策）
- 重要データ・システムのセグメント化（ネットワーク経由での侵害範囲拡大のハードルを上げるか、攻撃者が到達できないよう、ネットワークを分離する[42]）

5-5. 事業継続計画（BCP）・対応方針

この攻撃は、一部の端末や一部のデータが失われるといった、局所的な IT 障害の問題に収まらない可能性があり、事業継続計画（BCP）の策定時にも想定対象となりうる脅威であると考えられる。実際に、1 万台を超えるマシンが攻撃され、数 TB ものデータが窃取された事例が報告されている状況にある。

攻撃者に対しては、一般的に次の理由から身代金を支払うべきではないとされている。政府機関等の方針で、支払ってはならないと指針が示されている場合もある。

- 身代金が攻撃者の資本源（収入源）となってしまう。
- 攻撃者が同種の犯罪を続けるモチベーションになり得る。
- データが公開されない保証は無く、更に金銭を要求される可能性もある。

被害者となってしまった場合、非常に厳しい状況でインシデント対応を進めることになることが避けられない。この時、最終的に自組織をとりまくステークホルダ（例えば、顧客、取引先、株主、監督省庁等）に対し、どのような状況下で、どのような考え方で対応方針を定めたのかを説明可能な状態としておくことが望ましい。現場の IT 部門だけでなく、経営層や法務部門等を含めた方針策定が必要である。

5-6. インシデント対応

攻撃の被害を受けてしまった際のインシデント対応はケースバイケースとなるが、全体的には、標的型サイバー攻撃への対応と同様、影響範囲の特定、計画（対応優先度の策定を含む）、封じ込め、そして根絶と復旧という手順を着実に進めていくことが必要になる。CSIRT やそれに準じた組織が中心となり、経営層・広報部門・法務部門等とが連携した体制で臨むとともに、必要に応じて外部の専門ベンダの活用を検討する。被害が甚大な場合は、経営判断が求められるような場面が多く発生するため、冷静な意思決定のための情報の整理が不可欠である。

インシデント対応（インシデントハンドリング）の一般的な進め方について、JPCERT/CC がマニュアルを公開しているため、次の URL を参照いただきたい。また、5-1 で挙げた「高度サイバー攻撃（APT）への備えと対応ガイド」の「第 3 章 インシデント対応プロセス」も、同様に参照いただきたい。

- CSIRT マテリアル 運用フェーズ ： インシデントハンドリングマニュアル（JPCERT/CC）
  - https://www.jpcert.or.jp/csirt_material/operation_phase.html

特に挙げるとすれば、この新たなランサムウェア攻撃への対応にあたっては、次のような点に留意しつつ進める必要がある。

- 侵入経路の特定（特定できない場合、可能性のある箇所全てを見直し）と、攻撃者が設置した別の侵入経路（遠隔操作ウイルス、外部向けサーバに仕掛けられたバックドア等）の根絶。
  - 情報窃取が目的の攻撃であれば、情報を窃取した時点で目的が達成されていることになるが、この攻撃の場合、金銭が支払われるまで攻撃が繰り返される可能性がある。暗号化等の被害に遭っていない端末、サーバ、ネットワーク機器であっても、攻撃者が侵入経路として悪用し続けている可能性に留意する。
- 業務停止や、顧客・取引先の情報の漏えいについて、できる限りの影響範囲の特定と、それらに関わるステークホルダとのコミュニケーション。
  - 自組織内に閉じたインシデントで終わらない可能性がある。窓口の一本化、応対内容の一貫性の維持、適切な連絡のタイミング、安全な連絡経路の確保等を行う。
  - リークサイトに掲載された場合、インシデント下にあるという情報が非常に広く、また速く世間に出回ってしまう可能性がある。問い合わせ等に適切に対応できるようにするため、広報部門の迅速な体制作りが必要である。

進行中の攻撃を止めるため、業務に影響が生じるような対処、例えば、重要データ・重要システムのネットワークからの隔離、シャットダウン、組織のインターネット接続の遮断（または大幅な制限）等を緊急で実施することが必要となる場合がある。そのためには、CSIRT やそれに準じた組織が、その判断や実行が可能なよう、適切な体制や権限付与がなされていなければならない。

6. おわりに

ランサムウェア攻撃は、攻撃者が金銭を得ることを主な目的としたサイバー攻撃である。従来のランサムウェア攻撃は、不特定多数へ広く攻撃を行い、支払いに応じる被害者から身代金を得られればよいという攻撃であった。

ところが、新たなランサムウェア攻撃では、攻撃者は明確に企業・組織を標的として定め、企業・組織のネットワークに侵入する。その後、侵害範囲拡大を経て、機微情報等が保存されているサーバ等の端末を狙ったランサムウェア感染や、企業・組織内の端末の大規模な一斉暗号化、情報の窃取、公開による脅迫等、企業・組織の事業継続を妨げるような状況を作り上げる。その技術的な側面は、高度な標的型サイバー攻撃とも共通しており、大金が絡むことから、攻撃者が集まり、組織化し、今後ますます脅威が増大していく可能性がある。

このような攻撃に対し、企業の経営者は、事業の継続を脅かすような大規模な被害が生じ得る可能性があることを認識し、事業継続計画（BCP）の策定等において留意すべきであろうと考える。企業・組織のセキュリティを扱う方は、従来のランサムウェア攻撃対策に加え、標的型サイバー攻撃と同等の対策が必要であると認識した上で、対策を検討していただきたい。

情報提供・届出のお願い

この脅威については、情報が非常に不足している。また、本書の内容について、ご意見・ご指摘事項、関連する情報の提供をいただけると幸いである。また、被害に遭われた場合は、可能な範囲にて、ウイルス・不正アクセスの届出にご協力をいただきたい。

- 本書に関するご意見・情報提供等の送付先 （IPA セキュリティセンター）
  - isec-info@ipa.go.jp

- コンピュータウイルスに関する届出について
  - https://www.ipa.go.jp/security/outline/todokede-j.html
- 不正アクセスに関する届出について
  - https://www.ipa.go.jp/security/ciadr/index.html

7. 参考情報：攻撃グループの動向

2020 年 8 月現在、「人手によるランサムウェア攻撃」および「二重の脅迫」を行っている攻撃グループが、公開情報より確認可能な範囲でも複数存在する。本章では、これらの動向の一部を紹介する。

7-1. Maze

Maze というランサムウェアを使用する攻撃グループがある。Maze は 2019 年 5 月に初めて観測され、北米、南米、ヨーロッパ、アジア、オーストラリアの企業・組織を標的にしているとされている [28]。実際に Maze ランサムウェアを使用した攻撃を受けた企業・組織は様々で、アメリカの医療研究所 [43]やアメリカの市 [44]、フランスの建設会社 [45]等の被害が報じられた。

この攻撃者は、2019 年 11 月、企業から窃取したデータを公開した。二重の脅迫が行われた、最初の事例だとされている。以降、リークサイトを設置して窃取したデータの公開を行っているほか、身代金を支払わず、自力で復旧しようとした企業・組織の名称の公開等、積極的にサイトの更新を行っている。

更に、この攻撃者は、利益の増加や攻撃の成功を収めるために、別の攻撃者との協力を開始することを発表した。そして、実際に Maze とは異なる Ragnar Locker と呼ばれるランサムウェアを使用する攻撃者によって窃取された企業のデータを Maze のリークサイトで公開した [46]。

また、被害を受けた企業・組織の中には、被害の調査レポートを公開されたケースがあるという [25]。このことから、攻撃者はランサムウェアに感染させた後も企業・組織内のネットワークに潜伏して、データを窃取していることが分かる。

なお、脅迫に際し、ランサムウェアによる暗号化を行わず、情報の窃取のみを行ったと主張している事例もある [27]（よって、厳密には「二重の脅迫」や「ランサムウェア攻撃」という呼び方も、今後的確でなくなっていく可能性がある）。

図 7-1 にリークサイトの攻撃者からの声明文（交渉の方法等が示されている）、図 7-2 に被害企業掲載ページ、図 7-3 にデータを窃取した企業向けの脅迫ページの例を示す。

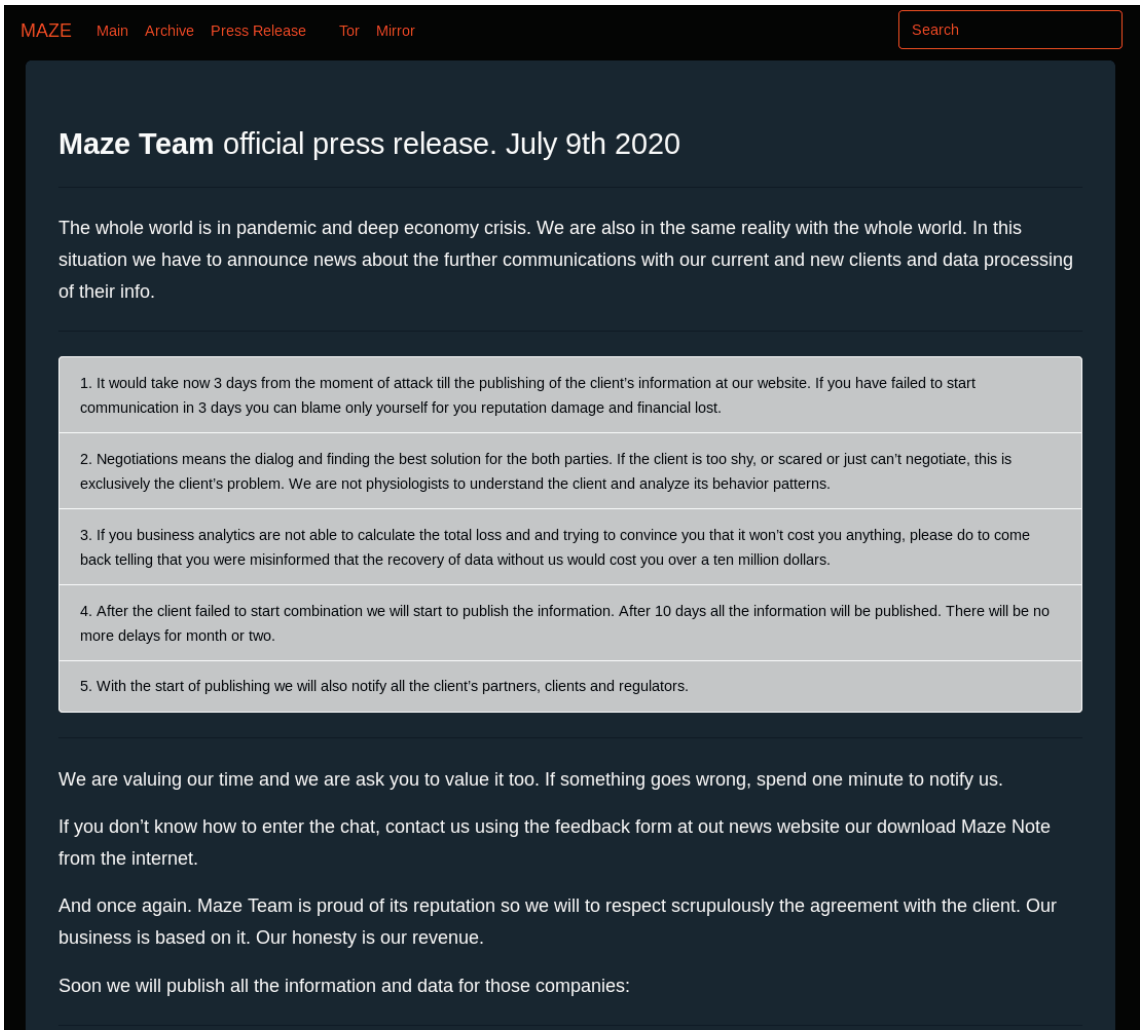

図 7-1 攻撃者からの声明文（Maze）

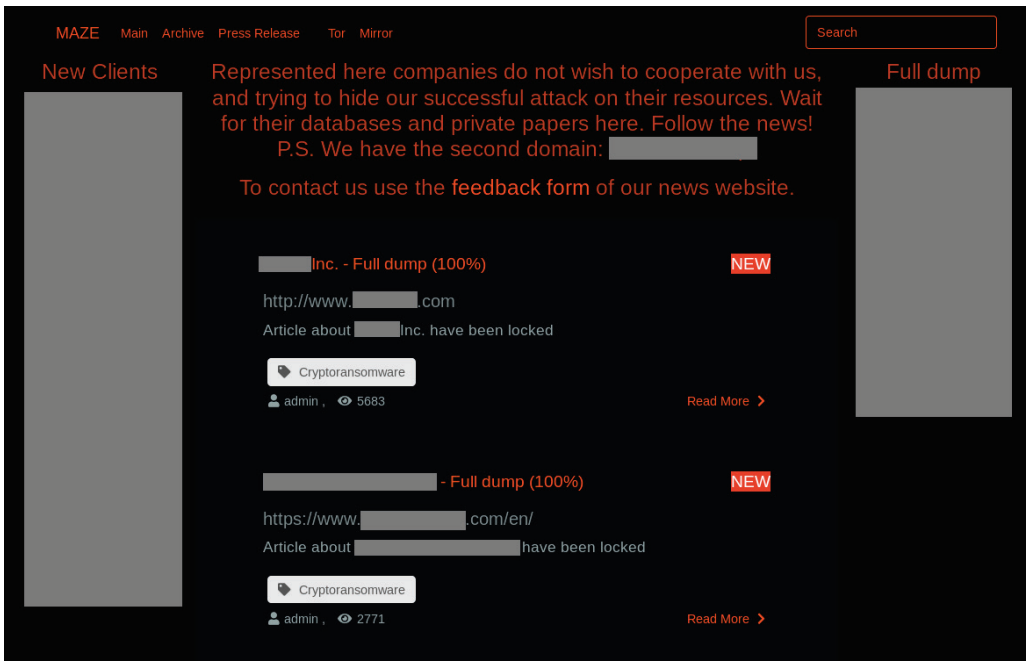

図 7-2 被害企業・組織の一覧ページ（Maze）

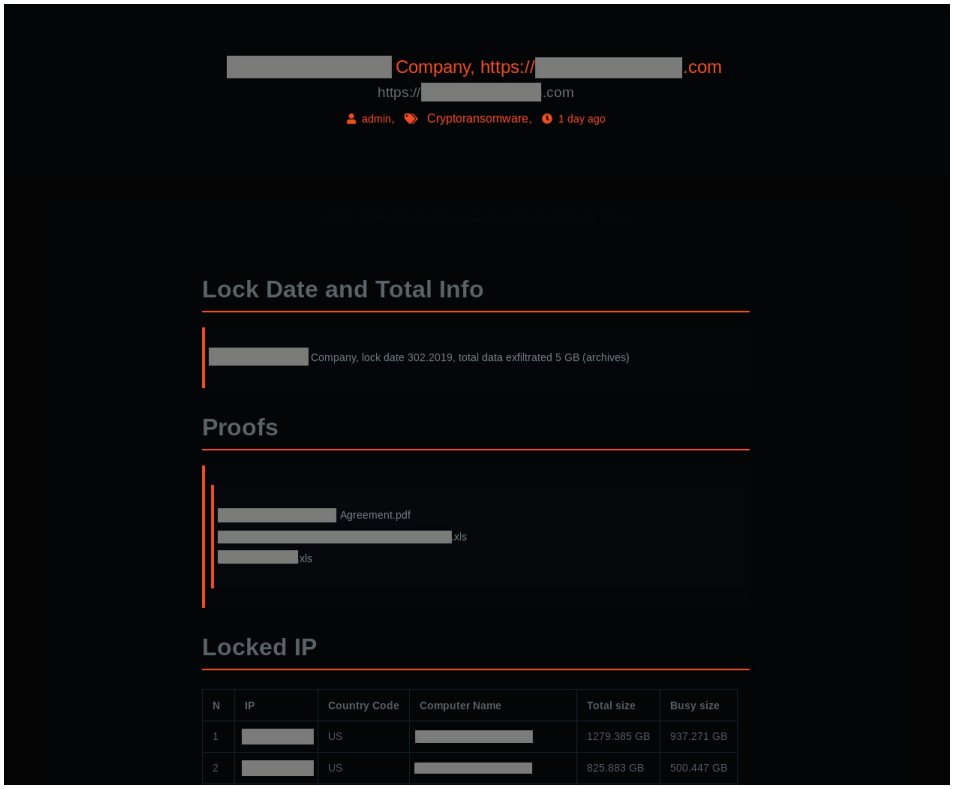

図 7-3 個別企業・組織向け脅迫ページ（Maze）

7-2. Sodinokibi

Sodinokibi（別名 REvil）というランサムウェアを使用した攻撃が、2019 年 4 月以降、海外だけでなく日本でも観測されている [47]。Sodinokibi ランサムウェアへの感染は、Oracle 社の WebLogic サーバの脆弱性の悪用や、ワーム機能による感染拡大、リモートデスクトップサービスを介して感染させる等の方法が確認されている [48]。2019 年 12 月、アメリカの国際空港が被害に遭った事例では、その国際空港が利用するマネージドサービスプロバイダへのネットワークに侵入し、そこから、ランサムウェアが国際空港のネットワークおよびバックアップサーバに広がったと報じられている [49]。これは、脆弱性の悪用やワーム型ウイルスによる感染とは異なり、サプライチェーンが侵害された事例と言える。

2019 年 12 月以降、Sodinokibi ランサムウェアを使用する攻撃者は、Maze の攻撃グループの後を追うようにして、二重の脅迫を行うようになった。アメリカの IT 人材派遣社から窃取したデータについて、その一部を公開し、身代金が支払われない場合はさらに多くのデータを公開すると表明した [50]。アメリカの不動産投資信託会社から窃取したデータについては、身代金が支払われなかった場合、データを公開するか競合他社へ売ると表明した [51]。

2020 年 6 月には、同攻撃者が企業・組織から窃取したデータを販売するためのオークションサイトを公開したとも報じられた [52]。図 7-4 に当該サイトの画面を示す。

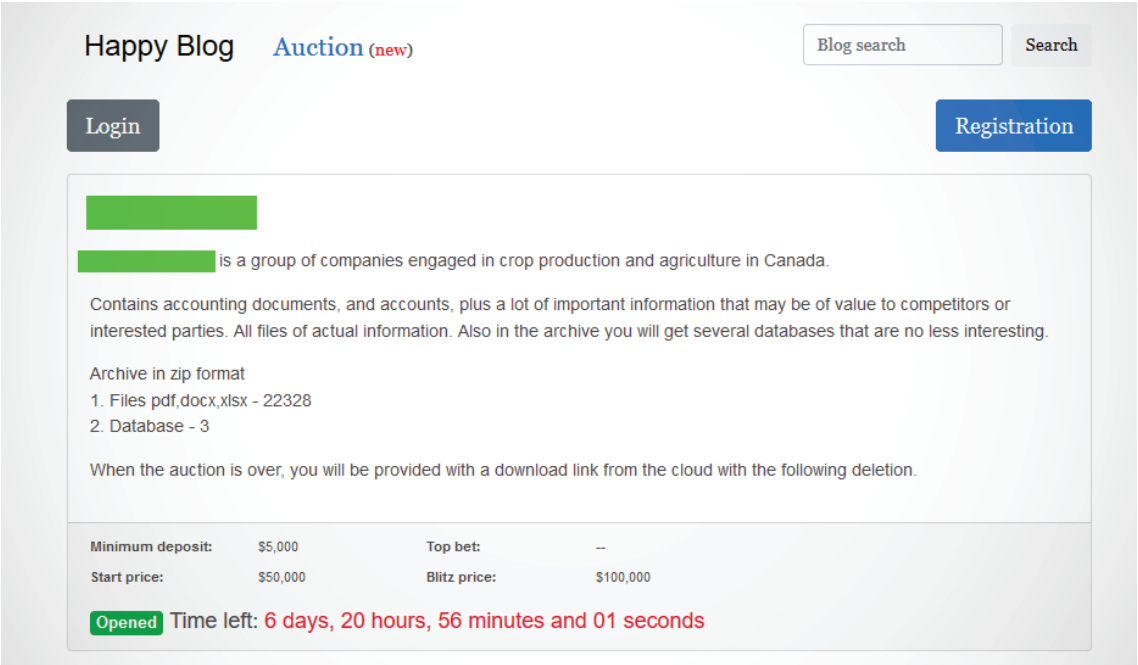

図 7-4 オークションサイト（Sodinokibi）

（出典）ZDNet「REvil ransomware gang launches auction site to sell stolen data」[52]

7-3. DoppelPaymer

DoppelPaymer というランサムウェアを使用した攻撃が 2019 年半ば頃から観測されており、アメリカの精密部品を生産している企業等が攻撃を受けたと報道されている [53]。

この攻撃者もリークサイトを運用している。例として、その被害企業一覧の掲載ページを図 7-5 に示す。

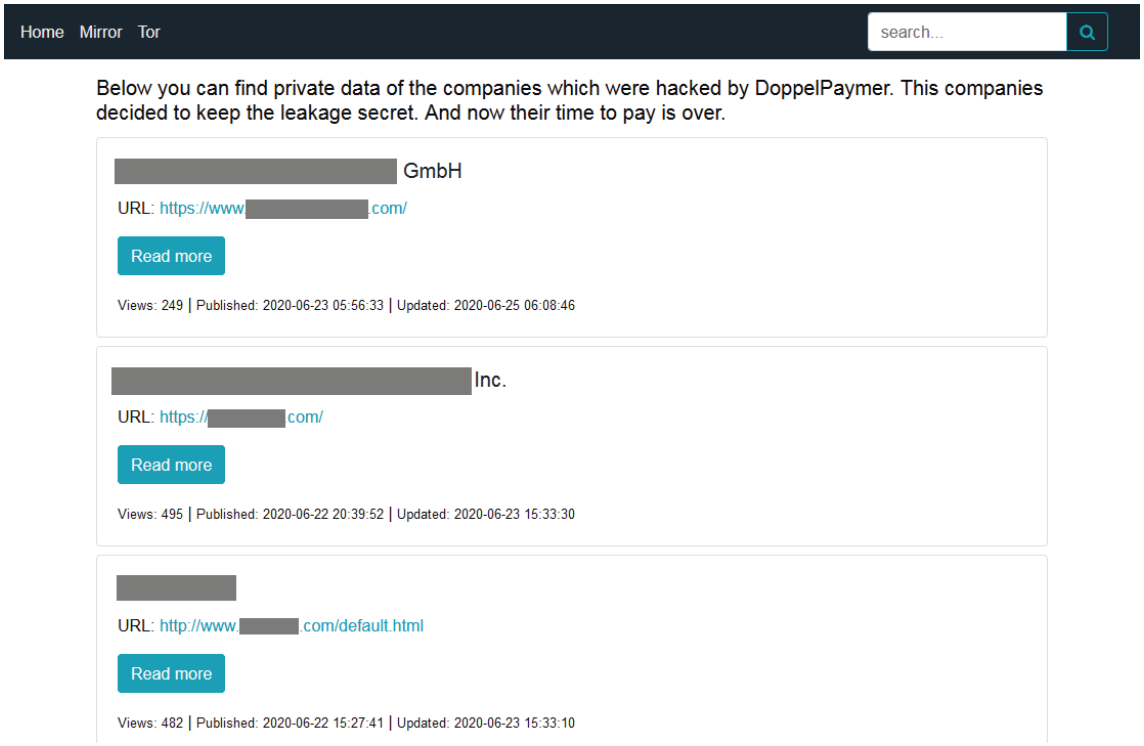

図 7-5 リークサイト（DoppelPaymer）

7-4. Nefilim

Nefilim というランサムウェアを使用した攻撃が 2020 年 3 月頃から観測されており [54]、日本企業の海外グループ会社が攻撃を受けたと報道されている [55]。この会社は 2020 年 1 月に、Mailto と呼ばれる、Nefilim ランサムウェアとは別のランサムウェアに感染していた。Mailto ランサムウェアを使用する攻撃者が、攻撃時に仕掛けたバックドア（再侵入するためにシステムに密かに設けられた経路）が残っており、Nefilim ランサムウェアを使用する攻撃者は、このバックドアを再利用して攻撃を行ったとされている [56]。

Nefilim ランサムウェアを使用する攻撃者は、事前に攻撃対象の企業・組織の内部 IP アドレスや管理者ユーザ名およびパスワード、Windows サービス、プロセスを把握して攻撃を行ったとされている [54]。

この攻撃者が運用しているリークサイトの画面（被害企業一覧の掲載ページ）を図 7-6 に示す。

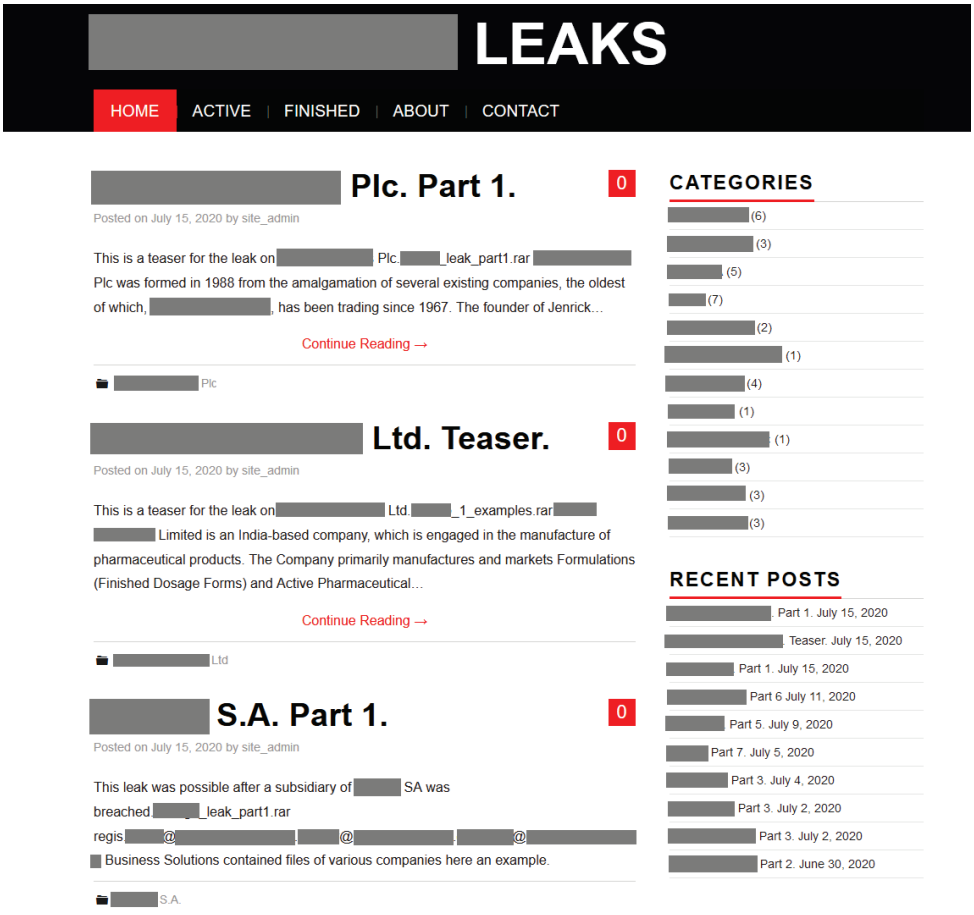

図 7-6 リークサイト（Nefilim）

7-5. CLOP

CLOP というランサムウェアを使用した攻撃が 2019 年 2 月頃から観測されており [57]、オランダの大学 [23] やアメリカの製薬会社 [58]が攻撃を受けたと報道されている。日本企業の海外グループ会社も攻撃の対象となっている。CLOP ランサムウェアに感染したオランダの大学は実際に金銭を支払うことで、暗号化されたデータの復号を行ったという。

この攻撃者が運用しているリークサイトの画面（被害企業一覧の掲載ページ）を図 7-7 に示す。

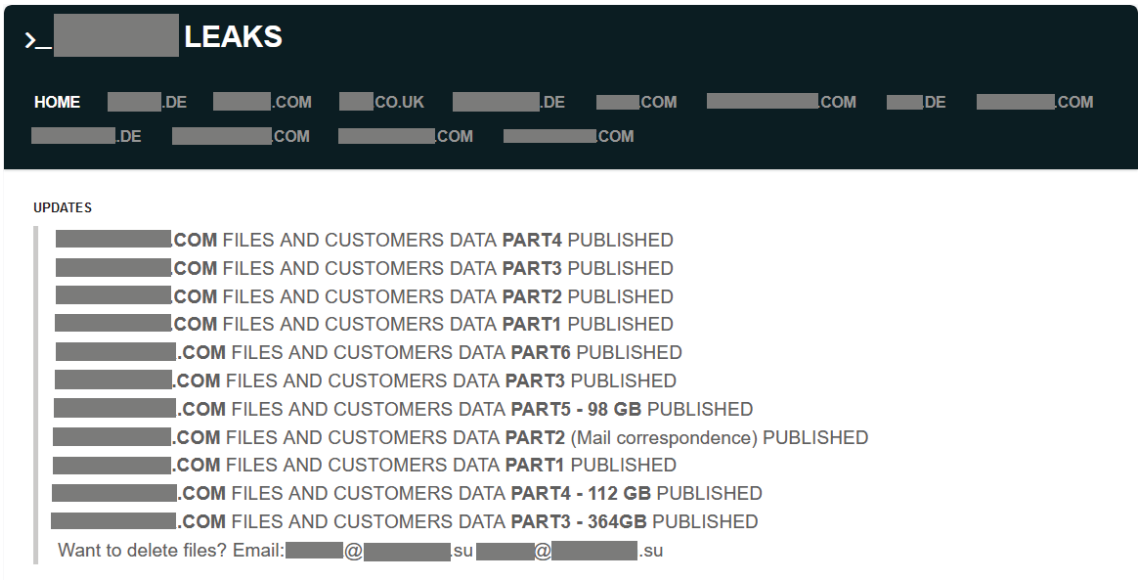

図 7-7 リークサイト（CLOP）

脚注

[1] FFRI: 標的型ランサムウェアの脅威
https://www.ffri.jp/blog/2020/06/2020-06-29-Targeted-ransomware-threat.htm
[2] Kaspersky: ランサムウェアを操る脅迫犯、盗んだデータを公開
https://blog.kaspersky.co.jp/ransomware-data-disclosure/26862/
[3] ITmedia: ランサムウェア＋標的型攻撃＝？　新たな攻撃、被害は数百万ドル
https://www.itmedia.co.jp/news/articles/1903/11/news101.html
[4] Secureworks: 日本国内で増加する 標的型ランサムウェアインシデント
https://www.secureworks.jp/resources/at-targeted-ransomware-spreading-in-japan
[5] システム侵入型ランサム: https://twitter.com/58_158_177_102/status/1287582571690303488
[6] マクニカネットワークス: マクニカネットワークス、暴露型ランサムウェアの手口と対応例を公開～ADや関連機器のログの”迅速な“調査や緊急対応、事業再開に向けた助言を実施～
https://www.macnica.net/pressrelease/mnc_20200624.html/
[7] 一部は 10 億円を超える身代金が要求されたという事例も報じられている。
[8] CSIRT: Computer Security Incident Response Team（CSIRT、シーサート）。組織内の情報セキュリティ問題を専門に扱う、インシデント対応チーム。
[9] ISAC: Information Sharing and Analysis Center（ISAC、アイザック）。同じ業界の民間事業者同士でサイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織。
[10] IPA: ランサムウェアの脅威と対策 ～ランサムウェアによる被害を低減するために～
https://www.ipa.go.jp/files/000057314.pdf
[11] JPCERT/CC: ランサムウエア ″WannaCrypt″ に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170020.html
[12] 日本銀行: 暗号資産（仮想通貨）とは何ですか？
https://www.boj.or.jp/announcements/education/oshiete/money/c27.htm/
[13] JPCERT/CC: 制御システム・セキュリティの現在と展望 ～ この 1 年間を振り返って ～
https://www.jpcert.or.jp/present/2018/ICS2018_02_JPCERTCC01.pdf
[14] Microsoft: Human-operated ransomware attacks: A preventable disaster
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
[15] BLEEPINGCOMPUTER: DoppelPaymer Ransomware hits Los Angeles County city, leaks files
https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-hits-los-angeles-county-city-leaks-files/
[16] KELA: The Secret Life of an Initial Access Broker
https://ke-la.com/the-secret-life-of-an-initial-access-broker/
[17] Check Point Software Technologies: Ransomware Evolved: Double Extortion
https://research.checkpoint.com/2020/ransomware-evolved-double-extortion/

[18] PROTECCION INFORMATICA: EDESUR, entre los afectados por EKANS/SNAKE
https://www.proteccioninformatica.com/2020/06/edesur-entre-los-afectados-por-ekans-snake/
[19] Malwarebytes: Honda and Enel impacted by cyber attack suspected to be ransomware
https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/
[20] 三井物産セキュアディレクション: SNAKE(EKANS)ランサムウェアの内部構造を紐解く
https://www.mbsd.jp/blog/20200616.html
[21] IPA サイバー情報共有イニシアティブ（J-CSIP）運用状況[2020 年 4 月～6 月]《付録》～EKANS ランサムウェアの解析事例～ https://www.ipa.go.jp/files/000084401.pdf
[22] ZDNet: Ransomware gang demands $7.5 million from Argentinian ISP
https://www.zdnet.com/article/ransomware-gang-demands-7-5-million-from-argentinian-isp/#ftag=RSSbaffb68
[23] BLEEPINGCOMPUTER: TA505 Hackers Behind Maastricht University Ransomware Attack
https://www.bleepingcomputer.com/news/security/ta505-hackers-behind-maastricht-university-ransomware-attack/
[24] BLEEPINGCOMPUTER: US aerospace services provider breached by Maze Ransomware
https://www.bleepingcomputer.com/news/security/us-aerospace-services-provider-breached-by-maze-ransomware/
[25] BLEEPINGCOMPUTER: Ransomware operators lurk on your network after their attack
https://www.bleepingcomputer.com/news/security/ransomware-operators-lurk-on-your-network-after-their-attack/
[26] MITRE: ATT&CK https://attack.mitre.org/
[27] ZDNet: Ransomware gang publishes tens of GBs of internal data from LG and Xerox
https://www.zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/
[28] Palo Alto Networks: 脅威に関する情報: Maze ランサムウェアのアクティビティ
https://unit42.paloaltonetworks.jp/threat-brief-maze-ransomware-activities/
[29] SentinelOne: Case Study: Catching a Human-Operated Maze Ransomware Attack In Action
https://labs.sentinelone.com/case-study-catching-a-human-operated-maze-ransomware-attack-in-action/
[30] MITRE: ATT&CK https://attack.mitre.org/tactics/TA0001/
[31] MITRE: ATT&CK https://attack.mitre.org/tactics/TA0004/
[32] MITRE: ATT&CK https://attack.mitre.org/tactics/TA0006/
[33] MITRE: ATT&CK https://attack.mitre.org/tactics/TA0007/
[34] MITRE: ATT&CK https://attack.mitre.org/tactics/TA0008/
[35] MITRE: ATT&CK https://attack.mitre.org/tactics/TA0009/
[36] MITRE: ATT&CK https://attack.mitre.org/tactics/TA0010/
[37] MITRE: ATT&CK https://attack.mitre.org/techniques/T1072/
[38] Secureworks: ランサムウェアに標的型攻撃手法を求めるのは間違っているだろうか
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_jp.pdf

[39] MITRE: ATT&CK https://attack.mitre.org/techniques/T1486/

[40] 境界防御という考え方が限界であるという見方もあるが、現実問題として、依然ネットワーク境界は 1 つの大きな防衛点であると思われる。また、考慮不要というわけではないが、内部犯行対策についてはここでは触れない。

[41] これらの仕組みを駆使し、企業・組織内ネットワークにおける不審な活動を検知することで、早期発見と対応に繋げる。例えば、ネットワークのスキャン活動、通常発生しない不正な通信の試行や認証の試行、不正なユーザアカウント作成等の操作、不正なプログラム設置・実行、イベントログの削除、シャドウコピーの削除、といった観点が挙げられる。

[42] ネットワーク分離は、運用コストや利便性に著しい影響があるため、重要性やリスクを踏まえた上での検討が必要である。

[43] BLEEPINGCOMPUTER: Maze Ransomware Not Getting Paid, Leaks Data Left and Right https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/

[44] BLEEPINGCOMPUTER: Maze Ransomware Behind Pensacola Cyberattack, $1M Ransom Demand https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/

[45] BLEEPINGCOMPUTER: Bouygues Construction Shuts Down Network to Thwart Maze Ransomware https://www.bleepingcomputer.com/news/security/bouygues-construction-shuts-down-network-to-thwart-maze-ransomware/

[46] BLEEPINGCOMPUTER: Maze Ransomware adds Ragnar Locker to its extortion cartel https://www.bleepingcomputer.com/news/security/maze-ransomware-adds-ragnar-locker-to-its-extortion-cartel/

[47] キヤノンマーケティングジャパン株式会社: 2019 年 7 月・8 月 マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1908.html

[48] McAfee: マカフィー、RaaS である Sodinokibi、別名 REvil を分析：エピソード 1 https://blogs.mcafee.jp/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us

[49] TRENDMICRO: 「SODINOKIBI」被害事例に見るランサムウェアの攻撃手法 https://blog.trendmicro.co.jp/archives/23716

[50] BLEEPINGCOMPUTER: Sodinokibi Ransomware Publishes Stolen Data for the First Time https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-for-the-first-time/

[51] BLEEPINGCOMPUTER: Another Ransomware Will Now Publish Victims' Data If Not Paid https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/

[52] ZDNet: REvil ransomware gang launches auction site to sell stolen data https://www.zdnet.com/article/revil-ransomware-gang-launches-auction-site-to-sell-stolen-data/

[53] TechCrunch: Visser, a parts manufacturer for Tesla and SpaceX, confirms data breach https://techcrunch.com/2020/03/01/visser-breach/

[54] TRENDMICRO: ランサムウェア「Nefilim」事例の内部活動調査から見えた事前の情報窃取の可能

性
https://blog.trendmicro.co.jp/archives/24767

[55] itnews: Toll Group suffers second ransomware attack this year
https://www.itnews.com.au/news/toll-group-suffers-second-ransomware-attack-this-year-547757

[56] itnews: Toll Group may have lost over 200GB of data in ransomware attack
https://www.itnews.com.au/news/toll-group-may-have-lost-over-200gb-of-data-in-ransomware-attack-548362

[57] McAfee: Clop Ransomware
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/

[58] TechCrunch: Hackers publish ExecuPharm internal data after ransomware attack
https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/