proofpoint.

脅威概要：ランサムウェア

ポイント

説明：

ランサムウェアは、重要なデータを暗号化したり、ユーザーの端末をロックして使用できないようにしたりして、攻撃者に身代金を支払うように要求します。攻撃者の多くは犯罪者集団のサイバー犯罪エコシステムを構成しています。

使用されるプログラム：

- Cryptolocker
- WannaCry
- Bad Rabbit
- Cerber
- Crysis
- CryptoWall
- GoldenEye
- Jigsaw
- Locky
- Petya
- Conti
- Sodinokibi
- Hermes
- Ryuk
- DarkSide
- BlackMatter
- GandCrab
- REvil
- LockBit

起源：

1989 年の Joseph Popp 博士による AIDS トロイの木馬にはじまります。同博士は、「AIDS 情報—入門編」というラベルをつけた感染させた 2 万個のフロッピーディスクを、WHO の国際的なエイズ会議の参加者に郵送しました。これが初のランサムウェア攻撃と考えられます。

種類：

- **暗号化型ランサムウェア**
  攻撃者がコンピューターにあるファイルを暗号化するため、ユーザーはファイルにアクセスできなくなります。
- **ロック型ランサムウェア**
  マルウェアによりコンピューターがロックされ、ユーザーはデバイスにアクセスできなくなります。
- **スケアウェア**
  マルウェアによりランサムウェアに感染したかのようにユーザーに勘違いさせて、身代金を要求します。技術的にはランサムウェアとして分類されませんが、ユーザーにとってはランサムウェアと同じ効果を持ちます。

リスク要因：

- ソフトウェアやシステムの脆弱性
- すぐにバックアップから復旧できない
- セキュリティ対策の不備 / 欠如
- ユーザーの脆弱性 / トレーニング不足

起こり得る被害：

- 経済的損失
- 機密データや独自データの漏えい
- 信頼性の失墜、ブランド力の毀損
- 事業の中断や生産性の低下

ランサムウェアは、被害者のファイルをロックして支払いを要求することからランサム（身代金）ウェアと呼ばれており、現代のあらゆるビジネスにとって大きな問題になっています。これは現在もっとも破壊的なサイバー攻撃の 1 つであり、時には企業を倒産に追い込み、病院の機能を停止させ、行政業務がおこなえなくなるなど大きな問題を引き起こしています。ランサムウェアに対処するには、ランサムウェアを自社の環境に寄せ付けないことが重要です。この拡大しつつある脅威について、以下で詳しくご説明します。

注目を集めるランサムウェア攻撃

Universal Health Services がランサムウェア「Ryuk」の攻撃を受け 6,700 万ドルの損害

ランサムウェア攻撃を受けた Universal Health Services (UHS) は、攻撃を原因とするダウンタイムと関連経費で、推計 6,700 万ドルの損失となりました。Fortune 500 企業である同社は、米国と英国に数万人の社員のいる、年間収入が 100 億ドルを越える医療サービスの大手です。[1]

UCSF が研究データの回復に 114 万ドルを支払う

カリフォルニア大学サンフランシスコ校 (UCSF) 医学部の IT システムがロックされるなど大学も標的になっています。同大学はただちに感染したシステムを隔離し、複数のシステムを囲い込むことで、大学のコアネットワークにまで被害が及ぶことを阻止しました。[2]

Cognizant が 5,000 万ドルから 7,000 万ドルのランサムウェアによる損失を報告

IT サービスプロバイダーの Cognizant は 2020 年 4 月のランサムウェア攻撃により、同年第 2 四半期の業績に打撃を受けました。攻撃による損失として、法務、コンサルティングのほか、インシデント調査、サービス復旧、システム修復などのコストが含まれています。[3]

1 Phil Muncaster (Infosecurity). “Universal Health Services Estimates $67 Million in Ransomware Losses.”「Universal Health Services、ランサムウェア攻撃による損失を 6,700 万ドルと推計」2021 年 3 月
2 Charlie Osborne (ZDNet). “University of California SF pays ransomware hackers $1.14 million to salvage research.”「カリフォルニア大学サンフランシスコ校、研究回復のため 114 万ドルをハッカーに支払う」2020 年 6 月
3 Catalin Cimpanu (ZDNet). “Cognizant expects to lose between $50m and $70m following ransomware attack.”「ランサムウェア攻撃を受けた Cognizant、5,000 万ドルから 7,000 万ドルの損失を計上」2020 年 5 月

ランサムウェア攻撃により米国の燃料供給も混乱

2021 年 5 月、ランサムウェアは、米国最大のパイプラインを閉鎖に追い込み、東海岸への燃料供給のおよそ 50% に当たる 5,500 マイルのシステムを停止させる事態となりました。[4] パイプラインの運営会社はデータのロックを解除するために 440 万ドルを支払いましたが、支払いにより「すぐにパイプラインシステムを復旧できたわけではありませんでした。」[5]

世界最大の食肉加工業者がランサムウェア攻撃を受け生産を停止

このブラジルの会社はコロラド州、アイオワ州、ミネソタ州、ペンシルバニア州、ネブラスカ州、テキサス州で食肉工場を運営していますが、ランサムウェア攻撃 (米国政府当局によればロシアを拠点とする攻撃とされている) を受けて工場の操業を停止しました。[6] 発表によれば、同社の北米とオーストラリアのコンピューターネットワークで攻撃が検出されましたが、幸運にもバックアップサーバーに影響は及びませんでした。[7]

ランサムウェア攻撃の仕組み

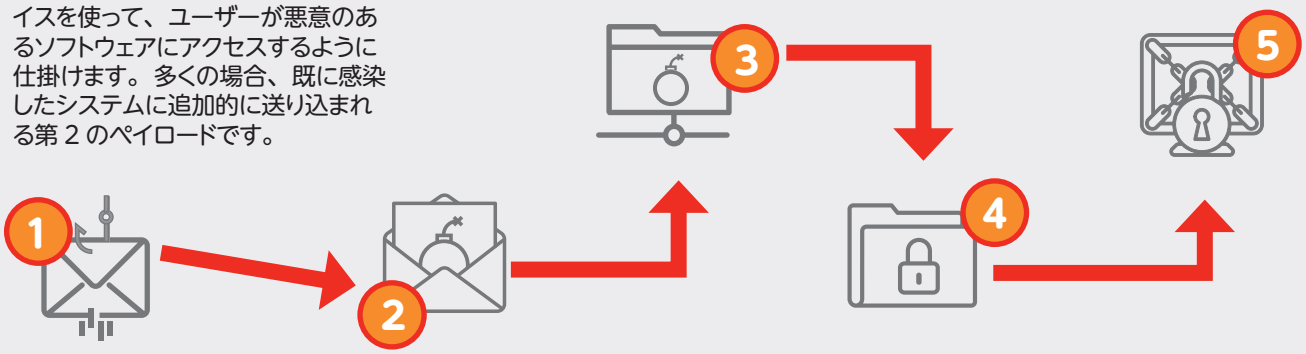
ランサムウェアはここ 30 年ほどでもっとも危険なサイバー攻撃へと進化した脅威の 1 つです。Bitcoin のようなデジタル通貨の出現により、身代金の回収が簡単にできるようになりました。加えて、古く時代遅れのシステムを標的にする攻撃の手口は日に日に巧妙になっています。

ランサムウェア攻撃に感染するまで

1. 配布 | 攻撃者はフィッシングメール、ソーシャルエンジニアリング、悪意のあるリンクを含む偽のウェブサイト、USB のような感染した外部保存デバイスを使って、ユーザーが悪意のあるソフトウェアにアクセスするように仕掛けます。多くの場合、既に感染したシステムに追加的に送り込まれる第 2 のペイロードです。

3. ステージング | 実行可能ファイルから取り込まれたランサムウェア ペイロードはシステム内にその存在を隠して埋め込まれます。

5. 身代金の要求 | ファイルへのアクセス回復と引き換えに支払いを要求するメッセージが被害者に表示されます。

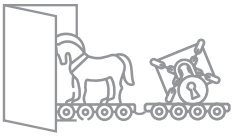


2. 感染 | ユーザーはローダー (またはダウンローダー) と呼ばれる実行可能ファイルをそれと知らずにダウンロードしてしまいます。このローダーはランサムウェアのインストールに使われます。

4. スキャンと暗号化 | マルウェアがシステムとネットワークをスキャンして、ファイルを暗号化します。

ランサムウェアの被害を受けるユーザーの多くはすでにデータのバックアップをとってあり、身代金の支払いを行わないようになっています。こうした傾向を理解したサイバー犯罪者は、その手口を進化させて、ファイルを盗み、暗号化した後に、情報を公開すると脅迫するようになっています。盗まれた情報は高度に機密であるものや、個人情報の可能性があり、公表されれば大きな被害につながりかねません。高度なランサムウェアの中には、バックアップデータにも手を伸ばし、暗号化するものすらあります。

4 David E. Sanger, Clifford Krauss および Nicole Perlroth (The New York Times) “Cyberattack Forces a Shutdown of a Top U.S. Pipeline.” 「サイバー攻撃を受けた米国最大手のパイプラインが停止に追い込まれる」2021 年 5 月
5 Collin Eaton および Dustin Volz (The Wall Street Journal). “Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom.” 「コロニアルパイプラインの CEO 、440 万米ドルの身代金をハッカーに支払った理由を語る」2021 年 5 月
6 Jacob Bunge (The Wall Street Journal) “Meat Buyers Scramble After Cyberattack Hobbles JBS.” 「サイバー攻撃を受けた JBS の操業停止で食肉買付市場も混乱」2021 年 6 月
7 Hamza Shaban, Ellen Nakashima および Rachel Lerman (The Washington Post) “JBS, world’ s largest meat processor, shut down U.S. beef plants amid cyberattack.” 「世界最大の食肉加工業者 JBS にサイバー攻撃、米国牛肉工場が閉鎖」2021 年 6 月



ランサムウェア攻撃はどう進化したのか

ランサムウェアはかつて悪意あるメールキャンペーンの主なペイロードでしたが、現在では第 2 の感染として機能する例が増えてきました。

トロイの木馬などのマルウェアを配布するサイバー犯罪者が、金銭の見返りに、感染したシステムへのバックドアをランサムウェア グループに利用させます。

このため、初期感染から守ることが、ランサムウェアに対する第一の防衛線になります。ローダーをブロックできれば、ランサムウェアを防ぐことができることを意味しています。

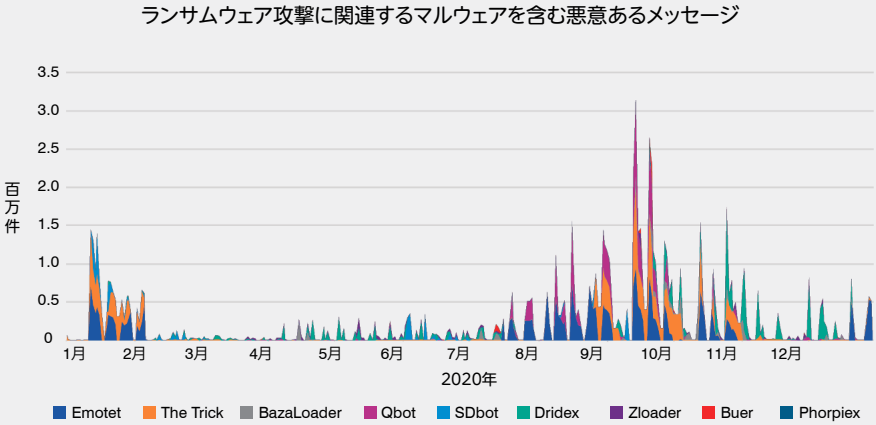
研究から得られた知見

ランサムウェアは、通常、悪意のあるメールから第 1 の感染を起こしたシステムに対して、第 2 の感染を目的として送られます。プルーフポイント独自の観測や他の研究者による調査から、活発なマルウェアとその後のランサムウェアの感染との間には一定の関連性が推測されています。

よく見られるマルウェアと、関連性の強いランサムウェアは以下のとおりです。

マルウェア / ダウンローダー	関連するランサムウェア
Emotet	Ryuk
The Trick	Conti
Dridex	BitPaymer/DoppelPaymer
Qbot	Egregor
SDBbot	Clop
ZLoader	Egregor および Ryuk
Buer (Buer Loader)	Ryuk
Phorpiex/Trik	Avaddon

Emotet、The Trick、Dridex および Qbot は、2020 年にプルーフポイントが観測したもっとも活発なマルウェアで、年間を通じて確認され、特に秋に急増しました。



支払いを決断する組織が増加するも、結果は分かれる

プルーフポイントの 2021 年 State of Phish レポートでは、調査に参加した米国組織の 78% が 2020 年にランサムウェアに感染し、そのうち 87% が身代金を支払ったと回答しました。これは世界平均の 2 倍に相当します。

一方で、日本は 54% の組織が 2020 年にランサムウェアに感染しましたが、そのうち身代金を支払ったのは 33% と調査の中ではもっとも低い数値がでました。

ただし、身代金を支払った日本の企業のうち 55% は追加的な身代金の要求を再び受けていることに注意が必要です。

組織を守るには

ランサムウェアに対処するには、そもそも組織に寄せ付けないことが重要です。

攻撃を受ける前

ランサムウェアの被害者になるという想定で準備を始めます。まずなすべきことは、防御、検知、対応策の検討です。たとえば、

- 重要なデータのバックアップ、データ回復手続きの確認、主なファイルシステムからバックアップをセグメント化
- システムの更新とパッチの適用
- ユーザー教育とトレーニング
- People-Centric なセキュリティ ソリューションの構築
- 拡散を防ぐためのネットワーク セグメンテーションの利用
- 攻撃を受ける前に、組織としていくらの身代金を、どのような状況で支払う用意があるか検討

攻撃を受けている最中

攻撃を受けてしまった場合、なすべきことは被害拡大の防止、および対応策の実施です。たとえば、

- 法執行機関 (警察) への連絡
- ネットワークからの切断
- 脅威インテリジェンスを用いた問題の範囲の確認
- 対応の調整
- 拡散を防ぐためのネットワーク セグメンテーションの利用
- ランサムウェアとともに組み込まれた可能性のある他の脆弱性、マルウェア、システムへの不正アクセスの確認
- 無料のランサムウェア復号ツールに頼らない
- 重要データの回復 - 他のデータに滞留しているマルウェアなどがないことを確認

攻撃を受けた後

ランサムウェア攻撃の後には、復旧作業とインシデントから生じた問題の解決に取り組みます。たとえば、

- クリーンアップと修復作業
- 事後のセキュリティレビュー
- ユーザーの意識の評価
- リスクベースの People-Centric なコントロール
- セキュリティ体制の再検討、最大のリスクエリアに照準を合わせた体制の構築

身代金は支払うべきか?

身代金を払うことは、犯罪行為に資金を提供することになります。他方、攻撃から生じる被害はビジネスにとっても組織の顧客にとっても、厳しいものになりかねません。一概にどうすべきかは難しいところです。

組織としては、何らかの方向性を決定する前に次のような事項について検討します。

- 顧客と従業員の安全
- 回復に必要となる時間とリソース
- 事業を継続するという株主に対する責任
- 身代金の支払いがどのような犯罪活動の資金になるか

どのような決定を下すのであれ、実際に攻撃を受け、期限に迫られたり、ビジネスに深刻な被害が及ぶというプレッシャーが生じたりする前に検討することが重要です。身代金の支払いの是非以上に、組織では、いくらまで、どのような状況で支払いをおこなう用意があるのかを判断する必要があります。米国制裁リストの対象となる相手に支払う場合は、法に抵触する可能性があることも忘れてはなりません。

詳細

ランサムウェアを阻止するには、プロアクティブな対応策が必要です。強固なランサムウェア対策は People-Centric なセキュリティからはじまります。実際の攻撃手法に基づく意識向上トレーニングを提供してユーザーの意識を高め、ユーザーを標的にするランサムウェアやマルウェア ローダーを検知してブロックします。そして迅速に対応し、事態が悪化する前に必要な措置を採ることができるようにしてください。

ランサムウェアの効果的な阻止についての詳細は、プルーフポイントのランサムウェア サバイバル ガイドからご確認ください。

詳細は **proofpoint.com/jp** でご確認ください。