IBM Security Services
Managed Security Services

Research Report

ランサムウェアについて知るべき必須事項

サイバー犯罪者たちはどのようにしてユーザー・データを人質にとるか

IBM

目次

要旨

つい最近まで、ランサムウェアは大企業にとって大した問題ではないと思われていました。セキュリティー・プロフェッショナルはランサムウェアについて、高度なマルウェア対策ツールを導入していない個人ユーザーや中小企業のほうをむしろ脅かすと考えていました。しかし、状況は変化しています。IBM の 2014 年最高情報セキュリティー責任者調査（CISO Study）によると、現在、セキュリティー・リーダーの 80% が、金融資産や知的財産の窃盗だけでなくランサムウェアを含む外部の脅威に起因する課題が増加していると考えています。その理由として、CryptoLocker や CryptoWall といったランサムウェアがその目的を遂げ、今や全世界で企業が何百万ドルもの損失を被っていることが挙げられます。

ランサムウェアは、ファイルを暗号化して元のファイルを削除するマルウェアで、感染すると身代金が支払われない限りファイルにアクセスできなくなります。あるいは、単純にシステム全体をロックした後にロックを解除するためのパスワードをユーザーに売りつけるものもあります。通常、ハッカーが構築して被害者に固有キーの入力を要求するウェブサイトにアクセスすることで身代金の支払いが行われます。

ランサムウェアは数多く存在するマルウェアの一種に過ぎないため、企業が戦略的なセキュリティー対策で通常重視する脅威ではありません。しかし、確実に増加して重要度も高まる傾向にあります。攻撃は隠匿性が高い上、攻撃者の組織化が進み多様な方法でユーザーの操作や恐喝が行われています。

ほとんどのランサムウェアは、被害者のコンピューターが不法行為に使われているという理由でロックされたという警告で始まります。手数料を支払いさえすればロックを解除できます。支払いはたいてい、ビットコイン、e-gold をはじめとする電子通貨により行われます。こうしたタイプのマルウェアが「スケアウェア（恐怖心を煽るソフトウェア）」とよく呼ばれる理由はそこにあります。スケアウェアは、被害者が不適切なウェブサイトにアクセスしているという心当たりにまつわる恐怖心や後ろめたさに乗じて被害者を脅して支払わせ、セキュリティー・チームとの連携による問題解決を図れないようにします。

幸運なことに、企業はランサムウェアを検知して感染を食い止める対策を講じることができます。何よりもマルウェア対策ソリューションを実装してパッチを最新の状態に保つことが対策となります。バックアップの定期的な更新は常に不可欠で、最前線の防御に万一失敗した場合にはこれが極めて重要になります。

本レポートについて

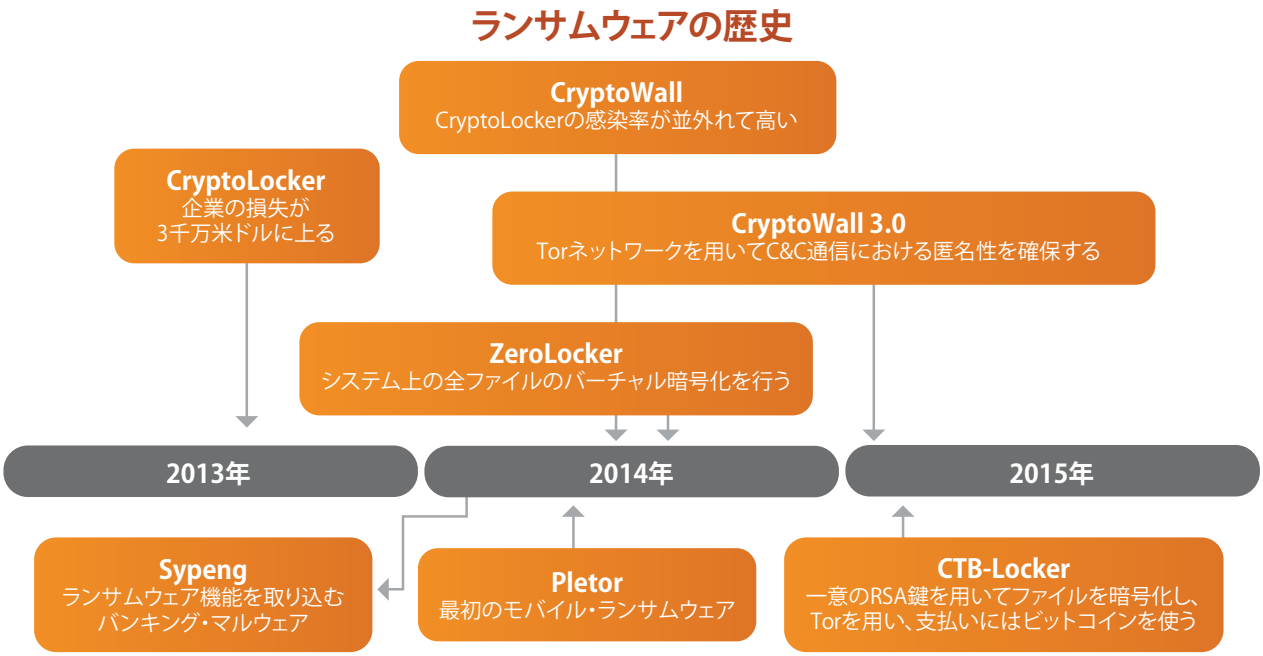
本レポートは、IBM マネージド・セキュリティー・サービスの Threat Research グループが作成しました。Threat Research グループは、豊富な経験と高度なスキルを備えたセキュリティー・アナリストのチームです。IBM のお客様に絶えずサイバー・セキュリティーの脅威に関する最新情報を提供して、常にそうした脅威に備えておくことができるよう尽力しています。
このリサーチ・チームは、社内外のさまざまなソースから収集したセキュリティー・データを分析しています。収集されるデータは、全世界のマネージド・セキュリティー・サービスのお客様のために IBM が管理しモニターしている、何万ものエンドポイントから集められたイベントのデータや、活動、傾向などのデータです。

ランサムウェアの昔と今

ランサムウェアはここ数年、攻撃者がよく用いるようになっていますが、その起源は、PC Cyborg というトロイの木馬（別名：Aids Info Disk（AIDS））が存在した 1980 年代後半にさかのぼります。PC Cyborg はファイルを暗号化した上で、パナマ共和国に開設された私書箱経由で架空の企業である PC Cyborg 社に 189 米ドルを支払って「ライセンスを更新する」ようユーザーに促すものでした。PC Cyborg は、現在の基準からすると未熟ではありましたが、対称暗号方式を採用していました。対称暗号方式では、暗号化されていないテキストの暗号化と暗号化されたテキストの復号に共通の暗号鍵を用います。

非対称暗号方式あるいは公開鍵暗号方式を用いた初期のクリプトウィルスの場合、2 つの異なる鍵、つまり秘密鍵と公開鍵が求められます。こうしたウィルスの存在は 1990 年代中盤に表面化しました。そしてその後 20 年をかけて、攻撃者はさらに高度な RSA 暗号化を用いたランサムウェアを開発しました。2008 年までには、暗号化を利用する Trojan Gpcode の亜種（PGP Coder とも言う）が、ファイルの復元がほぼ不可能な RSA 1024-bit 鍵を用いるようになっていました。[1]

2013 年になって、ビットコインなどのデジタル通貨あるいは仮想通貨を用いて身代金を回収する CryptoLocker の登場とともに土俵が再び変わりました。このランサムウェアは、ロシアやウクライナのハッカーが管理する大規模なネットワークがトーヴァー作戦によって崩壊させられたことでその悪名を馳せました。この大規模なネットワークは Gameover プラットフォームにより CryptoLocker を拡散させ、システムを CryptoLocker に感染させていました。FBI はこの窃盗者たちのネットワークを閉鎖した際、企業の推定損失額は 3 千万米ドルに上ると見積もりました。[2]



出典：IBM Security

図 1. ここ数年の間に出現した注目すべきランサムウェア

2014 年に出現した ZeroLocker は、データ・ファイルを暗号化するにとどまらず、C:/ ドライブ上のすべてのファイルを最大 20 MB まで暗号化します。CryptoLocker の亜種の 1 つである CryptoWall は、感染率の点では CryptoLocker を上回っています。CryptoWall のマルウェアとその基本的な構造は CryptoLocker ほど高度ではないかもしれませんが、現在出回っているものの中では間違いなく最も有害なランサムウェアの一種です。最新バージョンの CryptoWall v3 は、コマンド & コントロール（C&C）通信に匿名性のある Tor ネットワークを用い、特に攻撃的で悪質なランサムウェアです。CryptoWall v3 への感染は上昇傾向にあります。

攻撃の手法と機能

ランサムウェアはたいてい、スパム・メールやフィッシングメールにより送り付けられます。メールのメッセージには悪意のあるファイルへのリンクが含まれていたり、悪意のあるファイルが添付されています。ランサムウェアがいったんアクティブになると、身代金の支払いタイムリミットが設定される場合があります。

このマルウェアは、感染したホームページや悪意のあるサイトに埋め込まれたエクスプロイト・キットを利用して送られる場合もあります。ユーザーがエクスプロイト・キット・コードが埋め込まれたサイトにアクセスすると、そのコードがユーザーのシステム上の潜在的な脆弱性の特定を試み、その結果に応じて脆弱性を悪用します。ドライブ・バイ・ダウンロード（DBD 攻撃）も別の感染ベクターを発生させます。

攻撃者は、システムのハード・ディスクに保存されたファイルを暗号化する（比較的新しい一般的なアプローチ）か、あるいは単純にシステムをロックした上でユーザーをうまく誘導して支払わせるようなメッセージを表示する（図 2 参照）かして、支払いを強制します。

図 2. この ZeroLocker のメッセージは、攻撃者がユーザーにファイルが暗号化されたことを伝え、復号に利用する鍵を入手するための支払い方法も記載している例です。

ランサムウェアには以下のような機能が組み込まれています。

- ファイルの RSA 暗号化
- C&C サーバーとの通信
- Domain Generation Algorithm（DGA）による C&C サーバーのリストの生成
- キー・ロギングの有効化
- わずかなネットワーク・フットプリントの利用
- 実行中の複数のプロセスの強制終了
- バンキング・トロージャン（オンライン・バンキングを狙うトロイの木馬）をペイロードとして組み込む
- Tor を用いて悪意のあるサーバーを配置（撲滅は極めて困難）
- ビットコインによる支払いの要求（サイバー犯罪者を追跡可能な正規の決済システムを回避）
- 虚偽の通知の表示（図 3 参照）

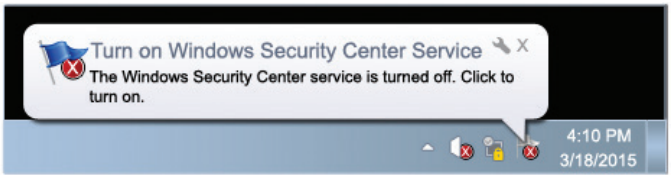


図 3. 一部のマルウェアは虚偽のシステム警告を表示する。ユーザーが警告をクリックすると、システムは身代金が支払われるまで使用できなくなる。

金融サービス業界に対するランサムウェア攻撃は、多数の個別ユーザーを標的にして従来の保護手段を乗り越えてアクセスを獲得しています。また、こうした攻撃は、支払い手段があって詐欺に対する認識がほとんどない企業に焦点を当てています。ある悪名高いよく知られたシナリオの場合、被害者は（南米、オーストラリア、欧州、米国の個人）全世界に存在しており、不審な非合法的な Web 覧活動を検知する「連邦警察」が被害者個人のファイルをロックしているのですぐに「罰金」を支払ってファイルの暗号化を解除するよう求める電子メールを受け取っています。[3] 最近では思いがけない展開を見せた皮肉なシナリオもあり、ランサムウェア・キャンペーンの標的となった米国のいくつかの警察部門がファイルを復号できずに屈服し、身代金を支払いました。[4]

不幸なことに、このシナリオはあまりにもありふれたものです。多くの企業は、犯罪に伴う取引を成立させるか否かを決定する状況に直面すると、各自の貴重なデータの回復を優先します。最近の調査によると、セキュリティー・プロフェッショナルの 30％は交渉に応じる意思がありました。サイバー犯罪の被害に遭ったことのある企業だけで見ると、その割合はさらに上昇して 55% でした。[5]

モバイル・ランサムウェア

ほとんどのサイバー攻撃の脅威は最終的にはモバイル領域に矛先を向けています。そのため、現在、全世界の携帯電話はランサムウェアを用いた脅威にさらされています。特に、オペレーティング・システムとして Android を実装した携帯電話は脅威が高まっています。2014 年初頭、モバイル・バンキング・マルウェアである Svpeng がランサムウェア機能を組み込んだときに、その攻撃の第一波が起きました。Svpeng はユーザーの携帯電話のブロックを試み、犯罪活動疑惑の代償として「手数料」500 ドルの支払いを求めるメッセージを表示します。

モバイルだけを狙ったランサムウェアも後れを取ってはいませんでした。Pletor は昨年 5 月に広がりを見せ始め、変更に次ぐ変更で各国から大陸全体に感染が拡大し、その戦いは続いていました。程なくして、非常に大な影響を及ぼすモバイル・ランサムウェアの一群が出現しました。特に、ScarePakage、ScareMeNot、ColdBrother、Koler などが挙げられます。モバイル・マルウェアの展望について 2014 年に実施されたある調査によると、ScareMeNot と ScarePakage は、米国、英国、ドイツといった国々において最も流行している 5 大モバイル脅威に選ばれています。[6]

推奨事項と緩和方法

マルウェア保護を実装していれば、おそらく数多くの種類のランサムウェアに対応できますが、単一のスパイウェア駆除プログラムだけでシステムから悪意のあるすべてのプログラムを駆除することはできません。侵入する脅威の即時検知が企業の目標であり、またベンダーごとの更新状況もさまざまであることから、数種類のスパイウェア駆除プログラムを組み合わせて階層化して検知を行うことで、保護を強化することができます。少なくとも最初に 1 つの階層で検知に失敗しても次の階層で検知できるようにします。

ネットワークの観点からランサムウェアの影響を緩和する方法もあります。一部の亜種の場合、予測可能なネットワーク GET リクエストを出すか DGA ドメインを使用することから予測可能なパターンを特定できます。その結果、いくつかの汎用 IDS/IPS ルールを適用することである程度対応できます。しかし、これはランサムウェアのすべての亜種に当てはまるわけではありません。この場合、ホスト・ベースの制限が役に立ちます。マルウェア作成者は戦術を頻繁に変更するため、マルウェア作成者による脅迫にはさまざまなレベルで反撃する必要があります。

ホスト・レベルにおいていくつかの実行ポリシーを設定することは、特定のランサムウェアで使用が確認されているパスからの実行をブロックする上で役に立つ可能性があります。多くのマルウェアは概して、そしてランサムウェアは特に、発動するとホスト上で特定の振る舞いをします。最も効果的な対策の 1 つとして、\temp フォルダーからのすべての .exe ファイルの実行禁止が挙げられますが、この場合、\temp フォルダーから実行されるいくつかの正当なアプリケーションにも影響が及ぶというリスクがあります。

攻撃者は、ランサムウェアが侵入できる既知の脆弱性を持つ古いソフトウェアを実行するユーザーを巧みに利用します。そのため、最新のセキュリティー・パッチを適用したソフトウェア・アップデートを定期的に行うことは、PC とモバイル・デバイスの双方にとって極めて重要です。

ランサムウェアがユーザーの PC やモバイル・デバイスに配信される方法はいくらでもあります。しかし、良好な包括的予防対策として挙げられるのは、不審なウェブサイト、検索、ダウンロードを避けることです。また、「マルウェア駆除」プログラムであると主張する一部のインターネット・サービスはまったくそれには当てはまらないものであると認識することも重要です。こうしたサービスはスパイウェアです。この場合にはユーザー教育が役に立ちます。

新たなランサムウェア・リリースは頻繁に姿を現しますが、アンチウィルス・ソフトウェアだけではそれに対応できません。ほとんどのスパイウェアを駆除するプログラムは本質的に事後対応です。つまり、シグニチャーのアップデートが適用されると保護され、パッチを完全に当ててシステムをアップデートした場合でもまだ多くのタイプのランサムウェアに対して脆弱です。事前対応な検知と悪意のあるコードのブロックをうまく行えるのは、行動分析技術を採用したソフトウェアだけです。

自社の重要な情報やリソースを効果的に保護するために、ゲートウェイ、ネットワーク、ホストの各レベルで事前対応型の多くの層からなる戦略を策定する必要があります。ランサムウェア侵入防止ソリューションには、以下のような機能が必要になります。

- ランサムウェアがネットワーク・リソースに影響を与える前にランサムウェアの侵入を阻止する
- 既存のランサムウェアが増殖したりネットワークでアウトバウンド・データを送信したりしないようにする
- 望ましくない内容を含むウェブサイトへのアクセスをブロックする
- ホストをマルウェアのインストール、実行、通信から保護する

マルウェアの脅威を緩和するためにその他の予防措置を講じることもできます。

- ブラウザーのセキュリティー設定を修正して不正なダウンロードを検知する
- 未知のプログラムをインストールしない
- ソフトウェアのダウンロードに先立ち、関連するすべての使用許諾契約書や個人情報の保護方針の説明を必ず確認する
- ポップアップ・ウィンドウ内のリンクをクリックしない。ウィンドウ内のボタンをクリックせず、右上端にある「×」をクリックしてポップアップを閉じます。

疑うべくもなく、あらゆる対策を講じてランサムウェアを検知し、阻止するべきです。しかしながら、自社の保護戦略に従ってもランサムウェアに感染し、データが暗号化されて回復できなくなった場合の次善の戦略となるのが定期的なバックアップの更新です。それでもやはり一部のデータの喪失は免れませんが、喪失の程度は前回のバックアップからの経過時間によって決まります。そうはいっても、バックアップを一切取っていないケースに比べれば打撃ははるかに抑えられるはずです。しかし、バックアップを取るだけでは不十分です。バックアップ・テストを行う必要もあります。IBM Emergency Response Services（ERS）は、バックアップ・テストを実施していなかった企業がデータの回復を試みても回復できなかったケースをいくつか確認しています。

ランサムウェアは確実に増加傾向にあります。[7] しかし、セキュリティーに関する上記の推奨事項を実施する企業は、重要な資産を脅威から守る体制を強化できます。

コストと複雑さを軽減させながら企業を守る

インフラストラクチャー、データ、アプリケーションの保護からクラウドおよびマネージド・セキュリティー・サービスに至るまで、IBM Security Services は企業の重要な資産の保護に役立つ専門知識を有しています。IBM は、世界で最も複雑なネットワークの一部を保護し、この分野の優秀な人材を採用しています。

IBM は、企業のセキュリティー・プログラムの最適化、高度な脅威の阻止、データの保護、クラウドとモバイルの保護に役立つサービスを提供しています。IBM の Managed Security Services を利用することで、お客様は業界トップのツール、セキュリティー・インテリジェンス、専門知識を活用することができます。お客様はこれらを活用することでセキュリティー態勢を、たいていは社内セキュリティー・リソースの何分の 1 かのコストで改善できるようになります。IBM Managed SIEM（security information and event management）は 24 時間体制でセキュリティー・インフラストラクチャーとエンドポイントの監視を行い、お客様が脅威を特定できるように支援しています。また、IBM Cybersecurity Assessment and Response サービスは、お客様がサイバー攻撃に対する準備を整え、こうした攻撃により迅速に対処するのを支援します。

IBM のセキュリティーについて

IBM Security は、企業向けセキュリティー製品およびサービスで構成された、最も高度な統合ポートフォリオの 1 つを提供しています。IBM のセキュリティー・ポートフォリオは、世界的に有名な IBM X-Force® の研究開発を背景に、企業の人材、インフラストラクチャー、データ、アプリケーションを全体的に保護するセキュリティー・インテリジェンスを提供しています。また、IBM は、ID およびアクセス管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、ネットワーク・セキュリティーをはじめとしたさまざまなソリューションを提供しています。また、セキュリティーの研究・開発、デリバリーを行う世界最大級の組織を運営し、さらに 3,000 を超えるセキュリティー関連の特許を有するとともに、130 カ国を超える各地域で 1 日 150 億件のセキュリティー・イベントを監視しています。

詳細情報

IBM のセキュリティー・ポートフォリオの詳細は、IBM 担当員または IBM ビジネス・パートナーにお問い合わせいただくか、または次の Web サイトをご覧ください。
ibm.com/security

セキュリティー・サービスの詳細については、次のサイトをご覧ください。
ibm.com/services/security

参考文献

Trojan.Cryptolocker

Analysis of ‘TorrentLocker’ – A New Strain of Ransomware Using Components of CryptoLocker and CryptoWall

CryptoWall surpasses CryptoLocker in infection rates

CryptoWall ransomware is back with new version after two months of silence

All You Need to Know About CTB Locker, the Latest Ransomware Generation

Police Department Pays Cybercriminals Following Ransomware Infection

U.S. targeted by coercive mobile ransomware impersonating the FBI

Ransomware

Fake-police ransomware reaches Australia

The first mobile encryptor Trojan

Latest version of Svpeng targets users in US

著者について

Michelle Alvarez、Researcher/Editor、Threat Research Group

協力者

Zubair Ashraf、Team Lead and Security Researcher、IBM X-Force Advanced Research

Lance Mueller、Senior Incident Response Analyst、Emergency Response Services (ERS)

[1] Who's behind the GPcode ransomware?

[2] Crime pays very well: CryptoLocker grosses up to $30 million in ransom

[3] Fake-police ransomware reaches Australia

[4] Police Department Pays Cybercriminals Following Ransomware Infection

[5] Negotiating with Cybercriminals: 30% of Security Professionals Say They Would Pay for the Return of Their Data

[6] Lookout 2014 Mobile Threat Report

[7] IBM X-Force Threat Intelligence Quarterly – 1Q 2015

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
2015 年 6 月

SEL03042-JPJA-00