ホワイトペーパー

ランサムウェアリカバリーとファイル共有について知っておくべき全てのこと

BlackBerry Workspaces

企業における ランサムウェア脅威の台頭

エンタープライズファイル同期・共有(EFSS) は、分散化とデジタル化が進む職場全体で、安全かつ効果的に組織の情報を共有しやすくするソリューションです。しかし、企業組織を食い物にするサイバー攻撃者に対して脆弱になるという危険性も存在します。攻撃者は、企業が貴重なデータを大量に所有していることを知っており、問題を排除するためなら要求を呑んでお金を払う可能性が高いということを知っているのです。

しかし、攻撃者の要求を呑んだとしても、それだけでランサムウェア攻撃から回復するわけではありません。迅速な解決を図るためには、感染ファイルを特定し、深刻なダメージが生じる前にクリーンなバージョンへと復元することで、システム管理者自身で状況を制圧することのできるEFSSソリューションが必要なのです。

このホワイトペーパーでは、ランサムウェアの危険性、及びリスクやコスト、回復時間を低減しつつ、生産性低下と非稼働時間発生を防ぐEFSSソリューションを選ぶことの重要性について解説します。

ランサムウェア攻撃は2017年に最も広く蔓延したマルウェア[1]による攻撃

ランサムウェアとは？

ランサムウェアとは、デバイスを攻撃するために設計された悪意あるソフトウェアです。不正なメールで、添付ファイルやリンクを開かせ、デバイス上のファイルをロックや暗号化するなどして、身代金（ランサム）を要求します。身代金を支払うと（たいていBitcoinなどの仮想通貨で）、ファイルのロックを解除する解読キーが渡されます。しかし残念ながら現実として、個人や組織が攻撃者の要求を呑む判断をしたとしても、ファイルが無傷で戻る保証はありません。

多くの場合、フィッシングやスピアフィッシングといった攻撃は、その組織を狙うことを意図して仕掛けられています。悪意のある不正なメールが1人または複数人の法人メールアカウントに送られてくるのです。たいていは請求、出荷、その他送り状関連のメッセージを装っています[2]。例えばCFOのもとに、信頼するベンダーから、DocuSignのような有名サイトを通じた支払いを求めるメールがくるかもしれません。しかしリンクをクリックしたとたん、それが悪意あるリンクだったことがわかるのです。ランサムウェアが実行されると、CFOは深刻な被害の拡大を食い止めるため、奔走しなければならなくなります

蔓延している理由

ランサムウェアは10年以上前から存在していましたが、現在でも攻撃方法として1、2を争うほど蔓延している理由は、主に2つあります。

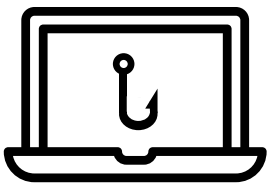
1. **実行しやすい**
   経験豊富な攻撃者はしだいに腕をあげ、従来の防衛手段をかいくぐる方法を新しく見つけ出しています。それに加えて、「サービスとしてのランサムウェア（RaaS）」と呼ばれるモデルが台頭し、サイバー犯罪初心者でもごく基本的な技術知識で、独自にカスタマイズした攻撃を簡単に仕掛けられるようになりました[3]。RaaSの一例がCerberです。これは世界で最も広く配布されているRaaSパッケージの1つとなり、2016年12月から2017年1月にかけて行われたランサムウェア活動の25%を占めています。[4]

2. **成功率が高い**
   攻撃による被害を避けるために、多くの組織が要求を呑み、身代金を支払うことで貴重なデータを安全に取り戻そうとします。攻撃を受けてBitcoinを凍結された例もあります。攻撃者にとっては同じ組織を再び攻撃したり、似たような企業を攻撃したりする資金源が得られるのですから、問題が永遠に続くことになりかねません。

他のマルウェアと同じく、ランサムウェアには拡散力があります。そのため従業員1人がよかれと思って間違った対処方法をとったことが組織全体に危機をもたらし、業務が遅滞もしくは停止に至る可能性もあるのです。

フィッシング vs. スピアフィッシング

どちらも広く普及している攻撃手法ですが、アプローチが明確に異なります。フィッシングは、網を広く投げて被害者が食いつくのを期待する手法であるのに対し、スピアフィッシングは、巧妙な偽装を駆使して特定の被害者に的を絞る手法です。



フィッシング
相手を騙して悪意あるリンクや添付ファイルをクリックさせる、もしくは悪意あるウェブサイトへアクセスさせようとする。

スピアフィッシング
フィッシングよりも狙いを狭く絞った攻撃。同僚や取引相手など、受け手にとって既知の信頼できる人物からのメールに偽装する。本文が受け手の関心事項や業界にあわせた内容になっていることもある[5]。

EFSSによる問題悪化

EFSSソリューションは、ランサムウェアに感染したファイルを複数のエンドポイントで同期・共有してしまい、事態を悪化させる可能性があります。ほとんどのEFSSソリューションは、新規ファイルが作成または保存されるたび、ユーザーのデバイスから中央（クラウド）レポジトリへ自動的にファイルを同期します。ファイルが他のユーザーと共有されると、最新バージョンをユーザーのデバイスに同期させます。

ファイルがランサムウェアによって暗号化されると、ファイルの新バージョンが作成されます。この新バージョンが中央レポジトリに同期され、感染したユーザーとファイルを共有する（EFSSを通じて）全ユーザーのデバイスに同期されます。ファイルは暗号化されているので、もはや中央レポジトリでも、エンドポイント全般でも、アクセスできなくなります。

EFSSは本来、デバイスやエンドユーザー間での安全なファイル保管、アクセス、共有を可能にするソリューション。

リスクを考えてみましょう

ランサムウェア攻撃の頻度および深刻さの高まりについて、全ての組織―零細事業から大企業まで―が真剣に考える必要があります。ランサムウェア攻撃の件数は2016年に3倍になりました。同年の第1四半期の時点では2分に1回のペースで攻撃が生じていましたが、第3四半期には40秒に1回になっています[6]。ランサムウェアの攻撃を受けない組織は存在しません。一方で、他よりも頻繁に狙われやすい業界は存在しています。

例えば医療業界では、2020年までにランサムウェア攻撃が400%増加すると予想されています[7]。2017年5月に、イギリスの国民保健サービスを含む2万件以上のシステムに不正アクセスするWannaCryという攻撃が起きた際には、医療業界が大規模攻撃の被害を受けやすい主な脆弱性が浮き彫りになりました。その脆弱性とは次のようなものです:

- 患者の健康情報(PHI)がデジタル化されている
- リスク耐性が低い（患者の命にかかわる）
- ネットで繋がったエンドポイントやテクノロジーの数が多い
- サイバーセキュリティ技術に対する投資が少ない[8]

とはいえ、狙われやすいのは医療業界だけではありません。実のところ教育、IT/通信、エンターテインメント/メディア、金融サービスといったセクターでも、20%以上の組織が攻撃を受けた経験があります[9] 。次に挙げる攻撃は、こうした狙われやすい業界の一部で、特に広範囲な被害をもたらしたものです。

ランサムウェア攻撃を受けた企業の約60%は従業員数が100人以上。25%は1,000人以上の企業[10]。

ランサムウェアによる特に顕著な被害例

•WannaCry: 2017年5月、Windowsの脆弱性に乗じて、医療を含む多様な産業の組織を攻撃した。

•Locky: 2016年2月、攻撃的なフィッシングキャンペーンで拡散。不正送金インフラDridexを利用した。

•TeslaCrypt: 2015年2月、ゲームファイルを狙って攻撃。非暗号化鍵と引き換えにBitcoinを要求した。

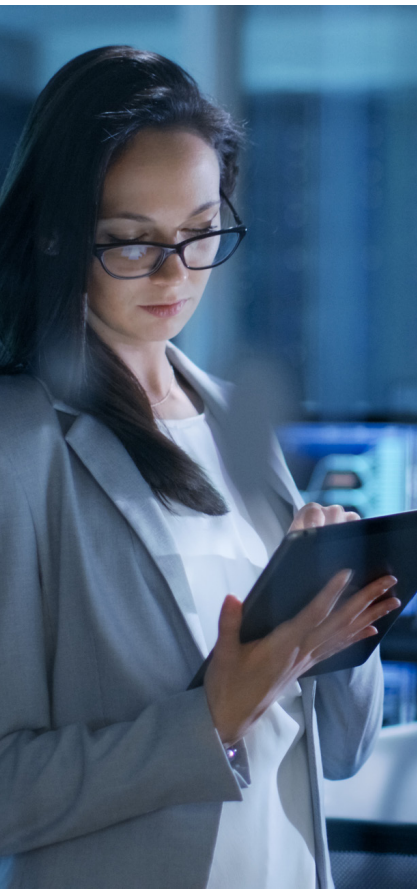
•SimpleLocker: 2014年後半、スクリーンをロックするマルウェアが、新しいアプリを提供するというスパムメールを通じてAndroidユーザーに広まった。

•CryptoLocker: 2013年8月、公開および非公開の暗号化キーを使って、被害者のファイルのロックとロック解除を行った。[13]

公的機関も攻撃を受けています。2018年3月22日に、アトランタ市全域のシステムがランサムウェア攻撃を受け、ファイルをロックされ、Bitcoinで約5万ドルを要求されました。攻撃から数日間、アトランタ市民は駐車料金や光熱費の支払いといった簡単な手続きをすることができず、また市職員は5日後に警報解除通知があるまでコンピューターの電源を入れることができませんでした。攻撃後、アトランタ市警察署長は、このサイバー攻撃により、パトカー搭載カメラの映像が数年分ほど破壊されたことを発表しています[11]。

2017年1月から3月に生じた新しいランサムウェアの数は、2016年の同時期の4.3倍[12]。

金融サービスのように厳しく規制されている業界は、サイバーセキュリティ技術に対し全体的に多額の投資をしていますが、それでもランサムウェア攻撃に狙われ続けています。これを受けて米証券取引委員会（SEC）は、2018年にサイバーセキュリティ要件を厳格化しました。



ランサムウェアによる金銭的被害の大きさ

ランサムウェア攻撃の影響範囲は、最初の身代金支払いでは終わりません。身代金支払いの有無にかかわらず、セキュリティ侵害への対応・修正・回復にかかるコストがかかってくる可能性があります。

次に挙げる影響が組織の業績にどれほど大きく響くか想像してみてください。

- **金銭的損失:**
  最初の身代金支払いに加えて、インシデント対応、修正対策、セキュリティ侵害に対する罰則金など、さらなるコストが生じる。
- **生産性低下:**
  数分の攻撃で、業務が数時間、数週間、場合によっては数年分も失われかねない。それに加えて、ファイルの回復や作業全体のやり直しに膨大な時間とリソースがかかり、著しいコストが生じる。
- **日常業務の破綻：**
  ランサムウェア攻撃により、感染したファイルを除去しクリーンなバージョンを復元するまでの間、企業のITシステムが凍結される。これによりプロジェクトや日常業務の遂行が阻害されビジネスの円滑な続行が不可能になる。
- **評判へのダメージ：**
  セキュリティ侵害を受けたことが報じられると、苦労して築いてきた評判が一気に失われかねない。侵害が公になれば、株価、ブランド価値、競争力にダメージがおよぶ。
- **顧客離れ、取引先離れ：**
  顧客や取引先は、自分たちの貴重なデータがきちんと扱われていると思いたい。その信頼が揺らぐと、背を向けられる可能性が高い。

ランサムウェア被害は2019年までに115億米ドルに到達する見込み[14]

不可避の事態に対する備え

知識と予防策は何より重要ですが、どんなに強固な防衛策でも全ての攻撃を防ぐことはできません。だからこそ、セキュリティ侵害を受けたときに迅速かつ効果的に回復する計画およびツールセットをもつことが重要なのです。

「業務継続計画」とは、ランサムウェアなどのサイバー攻撃を含め、事業および従業員に対する脅威への予防策と回復手段を定めた計画のことです。先手を打ったソリューションが導入されていれば、IT管理者が迅速に行動し、従業員の生産性を維持しながら脅威からの回復を図ることが可能です。

シナリオ: EFSS導入環境でのランサムウェア攻撃

ボブは大手金融サービス会社の社員として、M&A関連の業務に携わっています。その職務の性質上、必要不可欠な知的財産情報や顧客情報を日常的に扱っており、MS　Officeファイルの形式で全て自分のデスクトップパソコンに保管しています。また、自社のEFSSソリューションを利用してファイルを同期し、チームメンバーと簡単に共同作業ができるようにしています。これは彼の仲間内ではごく当たり前に行われていることです。

ある日ボブは、無害そうなメールのリンクをクリックしました。そしてすぐに、自分がランサムウェア攻撃を受けたと悟りました。彼のパソコンにあるファイルは全て暗号化され、アクセスできなくなったのです。日常業務を遂行できなくなったボブは、慌てて解決策を探しました。

ボブにとって不幸なことに、チームでクラウドのコラボレーションに頼っていたことが、事態を悪化させます。パソコン上の感染したファイルがクラウドに同期されたことで、そちらも暗号化され、彼だけでなくファイルを共有してきた全員がアクセス不可になったことが、すぐに判明しました。なお悪いことに、感染したファイルが同僚全員のデバイスにも同期されてしまったのです。チームプロジェクトには何千というファイルがあるので、ランサムウェアのさらなる感染拡大のリスクに鑑み、プロジェクトを停止せざるを得なくなりました。

アンディは同じ会社のIT部門で働いています。彼の仕事は重要な業務とエンドユーザーのサポートをして、全てのシステムとテクノロジーが円滑に回るようにすることです。この会社のビジネスにとって、時は金なり。生産性低下は莫大なコストにつながります。

その日アンディは、業務の最前線に立つユーザーサポートチームから緊急連絡を受けました。アンディはボブに事情を聞き、最初に問題に気づいたタイミングを把握します。そして攻撃があった時間を特定し、対策に乗り出します。

一般的なEFSSソリューションの場合

ボブとアンディの会社が一般的なEFSSソリューションを導入していた場合、アンディが採る対策は次のようなものになります。

1.コンピューターが感染した時間帯に、ボブがアップロードしたことになっているファイルの集計レポートを出し、感染ファイルを特定する。

2.各ファイルを調べ、感染ファイルを手作業で復元し、一番最近のクリーンなバージョンへと1件ずつ戻していく。ランサムウェア攻撃は複数のエンドポイントに広がっていたので、アンディはこの作業を感染したユーザー全員のデバイスで繰り返さなければならない。

3.別の対策としては、API経由でファイルを復元する専用プログラムの開発を外注する。

この解決策では、ファイルを1本1本調べ、感染ファイルをクリーンな状態へ復元する作業に、アンディが膨大な時間をかけることになります。さらには感染が疑われるデバイス全てに同じ作業を実行しなければなりません。アンディが対策に取り組んでいる間、ボブとチームメンバーは、日業業務の遂行に必要なファイルにアクセスできません。専用プログラムでファイルを回復する方法を選んだとしても、そのプログラムの開発・実行を依頼する先を見つけるのに時間がかかり、それ自体がリスクとなる可能性があります。

BlackBerry Workspacesの場合

ボブとアンディの会社がBlackBerry® Workspacesを導入していた場合、ランサムウェアリカバリー機能を使って、次のような対策を採ります。

1.アンディはボブに事情を聞き、Workspacesのプラグインを通じてボブのパソコンから同期しているワークスペースを特定する。

2.マルウェア攻撃により、ボブが自分のローカル環境へのアクセス権を失っている場合は、アンディがWorkspaces管理者用コンソールからユーザーログを確認。ボブのパソコンと同期しているワークスペースを特定し、共有ワークスペースで同期された感染ファイルをつきとめる。

3.必要に応じて、アンディがボブのユーザーアカウントを一時的に凍結し、システムの被害拡大を防ぐ。

4.ボブが所属するワークスペースが特定できたら、ユーザーと、復元したい日付および時間、そして感染の疑われる全ワークスペースを特定する（ユーザーインターフェイスには、そのユーザーがアクセス可能なワークスペースしか表示されない）。

5.リカバリー機能を使用し、感染したファイルを、ランサムウェア攻撃を受ける前の最新版のクリーンな状態へ復元する（特定した日付と時間をもとに）。他のバージョンがないファイルはそのままとなる。

6.ファイルの最新版がクリーンなバージョンになると、それがシステムに同期されて、ボブがファイルを共有する全ユーザーに亘るようにする。これでランサムウェアによって暗号化されたファイルがネットワーク全体で事実上除去される。

BlackBerry®Workspacesでは、アンディが簡潔な手順でボブのアカウントを凍結してファイルを特定し、感染したファイルを全てクリーンなバージョンへ復元し、それを他のユーザーのアカウントに同期させることができます。アンディが手作業でファイルを1本ずつ復元したり、同じ手順を複数のデバイスで繰り返したりして、膨大な時間を費やすことはありませんし、会社の他のユーザーは復元作業中も業務を続けることができます。

> セキュリティの優先度が高いなら、セキュリティおよびリスク管理のリーダーは、サポート対象のプラットフォーム全てに最高のソリューションを導入すべきである。[15]

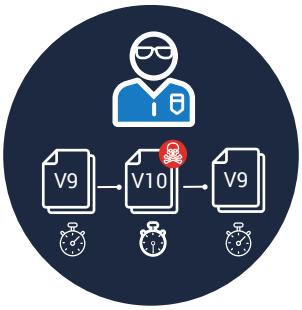
Gartner

*Gartner社レポート 「高セキュリティ・モビリティ管理の必須ケイパビリティ」ジョン・ジラード、 ディオニシオ・ズメール、ロブ・スミス 2017年8月24日。

対策の流れ

1 ランサムウェアの影響を受けたユーザーを特定し、Workspacesのデスクトッププラグイン経由でユーザーのデスクトップから同期しているWorkspacesのリストを抽出することができます。もし、ユーザーが影響を受けたWorkspaces、フォルダおよびファイルの確認ができない場合、管理者はWorkspaces管理コンソールよりログをチェックして、影響を受けたWorkspaces、フォルダおよびファイルを確認できます。

2 必要に応じて、管理者は影響を受けたユーザーを一時的にシステムからロックできます。



3 管理者はランサムウェア攻撃直前のユーザー、日付、時刻を特定することができます。クリックひとつで、管理者は影響を受けたすべてのファイルをランサムウェア攻撃の前の最新バージョンにロールバックすることができます。この操作で指定された日付と時刻のバージョンに戻すことができます。(攻撃を受けた時刻以降更新されていないファイルは影響を受けません。)アクセス権は、以前の「最新バージョン」と同じままです。またこの操作は指定したユーザーによって最後に更新されたファイルにのみ適用されます。(指定したユーザー以外のユーザーによって更新されたファイルは元には戻りません。

4 クリーンバージョンのファイルは、Workspacesを共有するすべてのユーザーに自動的に同期され、ネットワーク上の攻撃を受け破損したファイルを効果的に排除します。

5 管理者は、脅威が排除された後にユーザーのブロックを解除します。 管理者がユーザーのシステムをワイプすることを選択した場合、Workspacesは、復旧が行われた後、クリーンなバージョンのすべてのファイルをデバイスに再同期します。

BlackBerry Workspacesで リスク、コスト、回復時間を 低減する

ランサムウェア攻撃に対する最善の防御は、強固なファイアーウォール、メールセキュリティ、そしてエンドユーザーのトレーニングを含む多層的なアプローチを採ることです。しかし、最善の予防策をしていても攻撃は起きますし、往々にして成功してしまいます。BlackBerry Workspacesならば、セキュリティ侵害が起きた際にも独自のソリューションで、組織の迅速かつ効率的な対応を可能にし、業務の阻害も最小限にします。

以下のようなランサムウェアリカバリー機能によって、侵害後の結果が変わります。

•感染ファイルを迅速に封じ込めて、感染拡大を制限。

•ランサムウェア攻撃に迅速な対応と回復を図るためのツールを管理者が持つので、攻撃があっても速やかに業務に復帰。

•きめのこまかいコントロールで、影響を受けたユーザー、ファイル、フォルダーだけを選択して攻撃前のバージョンへと復元。システム全般におよぶ復元作業や回復メカニズムのせいで作業や生産性が失われる可能性を排除。

•サービスプロバイダーの高額なサポートやアシスタントに頼る必要がない。BlackBerry Workspacesの ランサムウェア・リカバリー・ツールがあれば、攻撃発生直後に管理者がシステム復元作業を実行可能。

まとめ

簡単に言うと、貴重なデータを大量に所有し非稼働時間に対する耐性が低い組織は、例外なくサイバー攻撃の第一標的になります。だからこそ、多層的な防衛モデルを配備し、避けられないセキュリティ侵害を念頭に置いて設計された法人向けテクノロジーを備えておくことが、組織にとって必要不可欠です。

攻撃に備えたEFSSソリューションならば、システム管理者が迅速に感染ファイルを特定・隔離し、簡単な数ステップの手順でクリーンなバージョンに復元して、業務を大きく阻害せずに済ませることが可能です。業務の進行が止まることはありません。従業員は連携作業を続けることができ、金銭面や評判面で厳しい影響を被ることもなくなるのです。

BlackBerryについて

BlackBerryはIoTエンドポイントの保守・管理に主眼を置くエンタープライズ・ソフトウェアおよびサービスの会社です。企業内のコミュニケーションやコラボレーションソフトウェアと、安全認証を受けた組み込み型ソリューションで構成されるエンド・トゥ・エンドのEnterprise of Thingsプラットフォーム「BlackBerry Secure」 で、これを実現します。

詳細はウェブサイトをご覧ください。 www.blackberry.com

出典:

1. https://www.verizonenterprise.com/verizon-insights-lab/dbir/
2. https://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html
3. https://blog.barkly.com/ransomware-statistics-2017
4. https://blog.barkly.com/cerber-ransomware-statistics-2017
5. https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/
6. https://blog.barkly.com/ransomware-statistics-2017
7. https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
8. https://healthitsecurity.com/news/hipaa-data-breaches-cyber-attacks-reported-by-47-of-orgs
9. https://blog.barkly.com/ransomware-statistics-2017
10. https://www.prnewswire.com/news-releases/report-identifies-ransomwares-biggest-cost-to-be-business-downtime-300236505.html
11. https://techcrunch.com/2018/06/06/atlanta-cyberattack-atlanta-information-management/
12. https://blog.barkly.com/ransomware-statistics-2017
13. https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html
14. https://www.csoonline.com/article/3237674/ransomware/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html
15. https://www.gartner.com/doc/3799963/critical-capabilities-content-collaboration-platforms