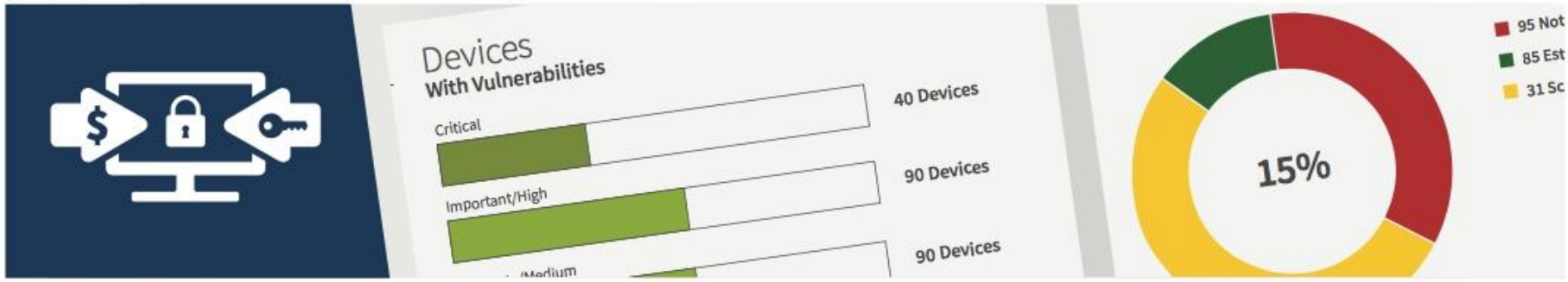
ivanti

ランサムウェアを防ぐ９つのステップ



Contents

イントロダクション

「ただ、ランサム（身代金）を払えばよい」と、あるFBI特別捜査官は2015年ボストンで開催されたサイバーセキュリティ・サミット[1]でそのように発言しました。 しかしその後、FBIはランサムウェアに対して警告を発し、いかにそれに対処するかのベストプラクティスのリストを提供する公式文書を発行しています。その新しい文書には明確に、「FBIは敵に対してランサム（身代金）を支払うことを支持しない」と述べています。

私たちは現在多くのランサムウェアがフィッシングやスパム・メールを利用して流布されていることを知っています。つい最近、報告されたことによれば、米国下院議会のユーザーたちが、Yahooメールアカウントに送られてきた添付ファイルを開封するように仕掛けられ、ランサムウェアの攻撃の犠牲になりました。[2]

エンド・ユーザーの教育及び、認識を高めることは常に良いアイデアではありますが、”悪いヤツら”はプロであると理解することが重要です。彼らはユーザーが不正なメールや添付ファイルを開封するよう罠を掛けるために、多くの専門的なマーケティングや社会工学のツールを駆使しています。したがって、皆さんは最も教育され自覚のあるユーザーでさえ罠に掛かりうると考えるべきです。事実、最新のVerizonデータ漏洩レポートでは受信者の23%がフィッシング・メッセージを開封し、11%が不正な添付ファイルにクリックすると報告されています。[3] そう、あなたは分が悪い立場なのです。

このIvantiのホワイトペーパーではFBIの推奨をレビューし、皆さんが実践すべき9つのステップを説明します。

予防

ランサムウェアに対して、“検知して対応する”モデルではほとんど効果がありません。なぜなら、ランサムウェアが動き出してしまってはもう手遅れなのです。これが、このマルウェアに対する防御が重要であるとの理由です。FBIは以下に示す9つの予防ステップあるいは手法を実践することを推奨しています。

各ステップの詳細は以降に記述します：

1. 重要なオペレーティングシステムやアプリケーションにパッチを適用する
2. ウイルス対策ソフトウェアが最新で、かつ定期的なスキャニングがスケジュール化されていることを確実にする
3. 特権アカウントの利用を管理する
4. データにフォーカスしたアクセスコントロールを実施する
5. ソフトウェアに関するルールを定義、実施、強制する
6. MS Officeファイルでのマクロを使用不可とする
7. アプリケーションのホワイトリスティングを実施する
8. ユーザーを仮想化あるいはコンテナ型仮想化環境に制限する
9. 重要なファイルを頻繁にバックアップする

1 重要なオペレーティングシステムやアプリケーションにパッチを適用する

多くの組織において、パッチを適用することはあらゆる攻撃に対する防御の最前線あるいは第二防御手段であるべきです。これはランサムウェアについても同様です。

PATCHING SHOULD BE THE FIRST LINE OF DEFENSE.

１ヶ月前、Adobe Flashのある脆弱性が”Locky”と”Cerber”のランサムウェアの犠牲となるワークステーションに配布され利用されました。[4]　皆さんは各クライアントシステムにインストールされたOSや必要なサードパーティアプリケーションが最新であることを確実にすることによりこれらの攻撃を予防することが可能です。また、Adobe FlashやJava、Webブラウザー、MS Officeなどのアプリケーションに関して全ての重要なパッチや更新が行われているかを確実にするのに格段の努力を払わなければなりません。さらに、ビジネス上の必要性及びポリシーを基準に、パッチや更新作業について優先順位を付けることが必要です。そしてこれらの作業をユーザーや事業運営の妨げとならないよう実行しなければなりません。

多くの組織では、広範囲でタイムリー、かつ継続的なパッチング作業の実行・維持は非常に複雑です、あるいは重要なビジネス・アプリケーションに壊してしまうかも知れないとの危惧を抱いています。しかし、適用し忘れたパッチのスキャン及びワークステーションやサーバーへの適用のために、最新のパッチ管理ツールを利用することにより、その作業は非常に簡単なタスクに変わります。たとえ最も複雑なシステム環境だとしてもです。

Ivantiは、完全で、フレキシブルな、エンドツーエンドのパッチ管理ソリューションの提供に関して非常に多くの経験があります。当社のエキスパートたちは皆さんがIvantiソリューションによりいかに効率的にパッチ管理を自動化できるか - そして皆さんのビジネスやユーザーに対して最低限の妨げ、あるいは全くなしにこれらの重要なパッチを適用するか - をデモすることが可能です。

2 ウイルス対策ソフトウェアが最新で、かつ定期的なスキャニングがスケジュール化されていることを確実にする

もしパッチの適用が皆さんの防御の最前線であるなら、ウイルス対策ソフトウェアはその次にくるものです。現在セキュリティの研究家たちはランサムウェアの攻撃は従来の定義ファイルを基にしたウイルス対策ソリューションでは防ぐことができないと理解しています。しかし、皆さんがウイルス対策ベンダーにより、既に認識されタグ付けされたマルウェアの脅威の犠牲にはなりたくないでしょう。

皆さんの組織のワークステーションにインストールされたウイルス定義データベースが常に最新のものに維持されることは有効なウイルス対策戦略の最も重要な要素です。Ivantiセキュリティ管理ソフトウェアは皆さんに代わってこのプロセスを自動化します。Ivantiのソリューションはどの規模のシステム環境でも非常に効率的に全ての端末に最新のウイルス定義ファイルを配布することができます。

発見済みのランサムウェアの犠牲にはならないようにIvantiはほとんどのウイルス対策ベンダーをサポートしていますので、Ivantiのソリューションは皆さんの会社のウイルス対策ベンダーと互換性があるはずです。もし皆さんがIvantiのKaspersky Labアンチウイルスエンジンをベースとしたウイルス対策ソリューションを選択すれば、Ivantiのコンソールからスキャン及びウイルス対策管理を自動化することが可能です。

3 特権アカウントの利用を管理する

特権を最小化することは、ランサムウェアを含む、多くのタイプのマルウェアを防護する重要な手段です。例えば、最近発見された”Petya”という名のランサムウェアの攻撃は実行するのに管理者権限が必要で、もしユーザーがそれらの特権を授与されなければ攻撃されません。[5]

管理者権限を取り除くことは簡単ですが、特権によるアクセスと、ユーザーの生産性や企業のセキュリティのバランスを取ることは簡単ではありません。これが、特権管理ソリューションが必要な理由です。Ivantiのセキュリティ・チームは、Ivantiがこの分野の証明済み（その他の優れたツールも含め）のソリューションのプロバイダーであるAppSenseを買収した理由の一つでもある、特権管理の重要性について唱えています。Ivanti Privilege Managementは権限を与えられたユーザーたちが彼らの業務を行うのに必要となるアドミン特権を制限するポリシーを定義するのに役立ちます。

しかしながら、ランサムウェアを防御する際に考慮すべきことの一つは、多くのランサムウェアの攻撃は、ユーザーが騙されて起動させてしまう、まさに実行ファイルであるということです。一度実行されれば、それらのランサムウェアのインスタンスは現行ユーザー空間の内側で起動し、それらにダメージを与えるのに何のアドミン特権も必要としません。（前述の）”Petya”ランサムウェアの最新バージョンの攻撃はアドミン特権を必要せずにファイルを暗号化することを可能にするフォールバック（予備の攻撃）メカニズムを有しています。

MINIMIZING PRIVILEGES IS AN IMPORTANT TACTIC TO PROTECT AGAINST SPECIFIC TYPES OF RANSOMWARE.

4 データにフォーカスしたアクセスコントロールを実施する

アクセス・コントロール・ソリューションは皆さんがランサムウェアを防御するのに役立ちます。しかし、そのソリューションがユーザーのアクセス権にフォーカスするとしたら、あまり有効ではないかも知れません。アクセスコントロールは共有ドライブに保存されたファイルを保護するのにとても有益です。それは、一部のユーザーには、全ての共有ドライブにあるファイルを修正するため、正当なアクセス権限を常に有しています。それらのファイルのほとんどは正当なユーザーが作成した文書ファイルです。これは、アクセス権を持つユーザーのシステムにうまく感染したランサムウェア攻撃が、全ての接続された共有ドライブおよびフォルダにある全ファイルを暗号化し人質として取ることを可能にすることを意味します。

Ivanti のセキュリティ・ソリューションは異なったタイプのアクセスコントロールを提供します。ユーザー権限へのフォーカスに対し、当社のソリューションは保護したいデータにフォーカスします。Ivanti は皆さんに（皆さんが指定したものだけでなく）重要で、注意を要する文書やファイルを修正するために全てのプログラムを保護するためのルールを定義してもらいます。例えば、.doc と.docx ファイルを修正すために Microsoft Word のみを許可するルールはそれらのファイルを暗号化するための感染済みのランサムウェアからの攻撃を拒否するでしょう。Microsoft　Office や Adobe PDF、その他頻繁に利用され共有されるファイル・タイプを保護するための同様なルールを追加することにより、多くのランサムウェアからの攻撃に対するベストな防御を提供します。そのようなルールの存在により、ランサムウェアがあるユーザーのシステムに感染したとしても、保護されたファイルを暗号化することは不可能になります。ユーザーたちはこれらのファイルへのアクセスを維持し、混乱がないよう最小限にし、より古くて時代遅れのバックアップ・バージョンを読み戻したりする必要もなく、業務を継続することが可能になります。

（いくつかのランサムウェアは傍目からは正当なソフトウェアの見えるように、かつシステムの起動ルーティンに自身を加えるように侵入を試みようとしてきます。Ivanti ソリューションはこれらも予防します）

伝統的なアクセスコントロールと比較し、データ保護にフォーカスする Ivanti のアプローチはランサムウェアからの防護により効果的です。それはランサムウェアの行動への理解に依るものであり、ユーザー特有の（かつ常に変更を有する）ルールを作ったり管理する必要もありません。したがって、それはまたユーザー権限管理ベースのアクセスコントロールよりも実施・維持し易しくもあるのです。

RANSOMWARE LEVERAGES MICROSOFT OFFICE MACROS. USE IVANTI SECURITY SUITE TO DISABLE THEM.

5 ソフトウェアに関するルールを定義、実施、強制する

Ivantiはまた、他のソフトウェアがどう行動するかを管理するルールを定義し、実施、強制させることを容易にします。これらのルールは、ブラウザーや他のプログラムで利用される一時フォルダを含む特定のフォルダ内のすべてのファイルを実行し、作成し、修正または読み取るために特定されたソフトウェアの能力を制限することができます。これらのルールはグローバル規模、あるいは特定のユーザーやグループにも適用することが可能です。

しかしながら、これらのルールを実施する前に、それらルールの導入によるユーザーエクスペリエンスの低下について考慮することが重要です。例えば、新しいあるいは更新されたソフトウェアをインストールするとき、ユーザーは時々ブラウザーから直接ファイルを解凍(”unzip”)あるいは実行することを要求されます。ユーザーはまた彼らの業務の遂行のためにマクロを作成あるいは呼び出したりする機能に頼ろうとします。ソフトウェア制限ルールは、正当なアクティビティでない限り、これらの行為をブロックします。

6 MS Office ファイルでのマクロを無効とする

Officeファイルからマクロを無効とすることでランサムウェアを含む多くのタイプのマルウェアをブロックします。例えば、”Locky”は主に添付ファイルを持つスパム経由で広まった比較的新しい”隠れ-ランサムウェア”です。このランサムウェアは端末上にマルウェアをダウンロードさせるワード文書内のマクロを実行するようユーザーをそそのかします。Ivanti Security Suiteは ITアドミニストレータがマクロを無効にするポリシーを設定することを可能にします。マクロの使用を求めないというこのポリシーを作業者に対して展開していくことはこの種のタイプのランサムウェアが実行されることから効果的にブロックするでしょう。

その他考慮すべきこと

FBI はシステム環境の保護を高めることを意図して、追加の推奨を発行しました。FBI は複数のタイプのマルウェアやその他の攻撃に対する皆防御を助けることを意味していますが、正確に利用すれば、ランサムウェアからの防御にもなります。

7 アプリケーションのホワイトリスティングを実施する

すべてのランサムウェアは信頼できないため、このソリューションはすべてのランサムウェアの機能が実行されるのを効果的に削除します。これは信頼できると特定された既知のアプリケーションのみがユーザーの端末で実行できることを確実なものとします。ホワイトリスティングが成功するための最大のチャレンジは信頼できるアプリケーションの最初のリストを作成し、そのリストを正確、完全、最新のものに維持することです。

Ivanti Application Management を含む Ivanti ソリューションは包括的で、フレキシブル、効率的、簡単なホワイトリスティングのための複数のオプションを用意しています。そして、Ivanti はホワイトリストを作成し維持することを容易くします。例えば、Ivanti ソリューションは“クリーン”なシステムで作動している全てのアプリケーションを自動的に“発見”し、自身のアプリケーションのレピュテーションデータベースに対してアプリケーションの整合性を検証します。所有者（例えば承認された管理者）及びベンダー（例えば Microsoft や Oracle）をベースとするアプリケーションを信頼するためのルールを追加することは、さらに信頼されるアプリケーション・リストの作成に求められる構成の量を削減します。

8 ユーザーを仮想化あるいはコンテナ型仮想化環境に制限する

ほとんどの場合、ランサムウェアは E メールへの添付ファイルとして配布されます。仮想化またはコンテナ型仮想化環境へユーザーを制限することはユーザーへのアクセスを獲得する全てのランサムウェアがユーザーの主要な業務環境が害されることのないよう確実にします。

Ivanti ONEのパートナーの一つであるBufferzoneは、Ivantiセキュリティ・ソリューションと統合するエレガントで脅威から隔離されたソリューションを提供します。Bufferzoneに関する詳しい情報はこちらをご覧ください：http://www.Ivanti.com/partners/Ivanti-one/bufferzone/。

9 重要なファイルを頻繁にバックアップする

FBI の論文は、事業継続性の観点から重要なファイルのタイムリーで頻繁なバックアップの実施を推奨しています。バックアップを正しく行えば、もしランサムウェアに攻撃されたとしても危機を救うでしょう。しかしながら、もし皆さんがこのホワイトペーパーに推奨された防御、特に Ivanti が提供するアクセスコントロール機能を実践すれば、ランサムウェアと闘うためにバックアップだけに依存する必要はないでしょう。

PREVENT RANSOMWARE FROM RUNNING IN THE FIRST PLACE

DYNAMICALLY WHITELIST YOUR APPS

ランサムウェアインシデントは増加しています。攻撃を防ごう!

Ivanti のソリューションにより、全ての端末を管理・保護し、新旧の脅威から保護することができ、新しいレベルの防御に向かい前進することが可能になります。
Ivanti セキュリティ・ソリューションのお問い合わせは、03-5226-5960 までお電話ください

参照：

1. http://www.businessinsider.com/fbi-recommends-paying-ransom-for-infected-computer-2015-10
2. http://www.computerworld.com/article/3068623/security/ransomware-attacks-on-house-of-representatives-gets-yahoo-mail-blocked.html
3. http://www.verizonenterprise. com/verizon-insights-lab/dbir/201 6/
4. https://threatpost.com/latest-flash-zero-day-being-used-to-push-ransomware/117248/
5. https://blog.malwarebytes.org/threat-analysis/2016/04/petya-ransomware/.