COMMVAULT®

ランサムウェアの 5 つの一般的なタイプ

& 自分自身を守る方法

どのランサムウェアも似たようなものなので、そのすべてに対応できる単一の防御策や備えがあると考えがちです。しかし、この思い込みは正しくありません。このような思い込みから医療機関のダウンタイムが発生し、データや患者の信頼を失う可能性があります。ランサムウェアのタイプによって、その由来やネットワークを攻撃する方法は異なるため、現在使用されているさまざまなタイプを理解することが重要です。さまざまなタイプのランサムウェアが使用されることを理解していないと、攻撃を受ける可能性が高くなり、財務面でより大きな打撃を被ることも考えられます。

常にハッカーよりも賢く:なぜ最新のランサムウェアのタイプを知っておく必要があるのか

ランサムウェアの亜種は絶えず進化および変化を続けています。現存するウイルスのタイプをよく知らない場合、他のタイプのランサムウェア向けの保護戦略を使用してしまっているため、新しい種類に対してネットワークが保護されないということになります。複数の亜種が蔓延している現在では特に注意が必要で、ネットワークに接続しているすべてのファイルに影響を及ぼす可能性があります。その結果、バックアップにも簡単に感染してしまいます。もしバックアップが感染していると、攻撃後に稼動するのは非常に困難になり、身代金を支払わざるをえない状況になってしまいます。

ランサムウェアの攻撃を受けた場合にネットワークをすぐに遮断するなどの初期対応をとると、攻撃によるダメージ コントロールに大きな効果があります。自身の受けた攻撃のタイプを知ることや、攻撃を受けた直後にに取るべき最善の対応策を知ることは、組織のデータがこれ以上失われるのを防ぐことができます。

ここでは、医療機関を攻撃する 5 つの一般的なランサムウェア ウイルスのタイプを紹介します。

1: CRYPTOWALL

組織がランサムウェアに攻撃される場合、それは CryptoWall の可能性が高いと言えます。Solutionary の Security Engineering Research Team Quarterly Threat Report for Q2 2016[1] によると、CryptoWall は、医療関係のランサムウェア攻撃全体の 94% を占めます。一般的に、このタイプのランサムウェア攻撃は、フィッシングメールを通して行われます。しかしながら、CryptoWall の作成者は、セキュリティ保護をくぐり抜けるように新しいバージョンのウイルスをリリースし続けているため、CryptoWall の進化に関するニュースに注意を払うことが重要です。

Healthcare IT News[2] では、2016 年 7 月に New Jersey Spine Center が CryptoWall の攻撃を受け、金額は未公開ですが、身代金を支払ったと報じています。犯人は、ユーザー パスワードをハッキングしてネットワークにアクセスしました。攻撃により、EHR ファイル、バックアップ ファイル、電話システムが暗号化されました。このタイプのランサムウェアのもっとも危険なところは、バックアップ システムも暗号化できるという点です。これにより、病院は多くの場合、身代金を支払わざるをえなくなります。

最善の防御: すべてのデータのオフライン バックアップを1 つは持つようにし、攻撃後すぐにファイルをリストアできるようにする。

ソリューション ブリーフ: 医療用データの保護、リカバリ、セキュリティ

効果的なバックアップ ソリューションにより、医療機関は身代金を支拂うことなく事業の中断を回避できます。

今すぐ読む

PDF commvau.lt/2jgwtUb

1 commvau.lt/2j8v67N 2 commvau.lt/2gg2njd

2: LOCKY

このウイルスの名前はその攻撃方法 (ファイルをロックして、拡張子を .locky に置き換える) を表していますが、そこから伝わらないのは、このタイプのランサムウェアの感染速度の恐ろしさです。Locky は、他のランサムウェアの亜種よりも速くネットーワークを介して他のファイルに広がるという特徴があります。FireEye[3] のレポートによると、医療業界は Locky の攻撃の対象になりやすく、昨年の 8 月のように大規模な攻撃が行われる場合は特にそうです。

このウイルスはしばらくの間存在していましたが、Healthcare IT News[4] によると、最新の Locky の攻撃方法は、感染した DOCM ファイル (Microsoft Word テンプレート ファイル) をメールに添付して攻撃することであると報じられました。最近では、Locky 攻撃は、実在していそうな会社からの ZIP ファイルが添付されたメール、または Facebook メッセンジャーを介して開始されると報告されています。[5]

最善の防御: 知らない送信者からのメールの添付ファイルは開かないように従業員をトレーニングする。

3: CRYSIS

このタイプのランサムウェアは、データ攻撃のレベルが新しい段階に入っています。実際にデータを誘拐して、新たな仮想の場所に移動するのです。Becker's Health IT and CIO Review[6] によると、このランサムウェアの攻撃で重要なことは、これは法律違反になるので、コンプライアンスに準拠し、医療機関は患者に連絡する必要があるということです。Crysis の攻撃は、他のタイプのランサムウェアと同様に、従業員がリンクをクリックしたり添付ファイルを開いたりしたときに開始されます。ただし、HealthcareIT News[7] によると、最近 Crysis の復号キーがリリースされたため、現在は攻撃を受けた医療システムでもファイルのロックを解除できます。

最善の防御: バックアップを独立した IT リカバリ環境で運用し、可能であればネットワーク セグメンテーションを作成する。

4: SAMSAM

ネットワーク上でインターネットに接続している箇所にパッチを当てていない JBOSS アプリケーション サーバーがある病院は、このタイプのランサムウェアに対して脆弱であると言えます。このランサムウェアは、いったんネットワークに侵入すると、他のシステムを探して攻撃します。Health Data Management[8] によると、病院では多数の JBOSS サーバーを使用していることが多いため、医療機関がこのタイプの攻撃の大きな対象になります。また、病院ではデータの緊急性が高いため、ハッカーにとっては身代金を稼げる可能性が高くなります。

最善の防御: JBOSS アプリケーション サーバーを使用している場合、必ずすべてのサーバーにパッチを当てる。

3 commvau.lt/2jge61D 4 commvau.lt/2iQgetM 5 commvau.lt/2it7QTh
6 commvau.lt/2jgmcat 7 commvau.lt/2jMPrTk 8 commvau.lt/2jFeXG4

5: CERBER

Cerber は、他のランサムウェアのようにファイルを追跡するのではなく、データベース サーバーのプロセスを攻撃してアクセスします。興味深いことに、このランサムウェアでは回収した身代金の一部が犯罪者から作成者に支払われます。ComputerWorld[9] は、2016 年の被害額が 100 万ドル以上になると推測しています。eSecurity Planet[10] では、Cerber は Locky、CryptoWall と並び、活発に活動しているランサムウェア トップ 3 の 1 つであると報じられました。

最善の防御: Cerber は、管理者アカウントでアクセスする必要があるため、ワークステーションの管理者アカウントの使用を制限するか、IT スタッフが特別なタスクの実行が必要なときのみこうした管理アカウントを使用する。

2017 年もランサムウェアの脅威は続く見込み

ランサムウェアの知識と予防に注目し、先頭に立って医療機関のセキュリティに取り組むことが必要です。残念なことに、Health Data Management は、2017 年も引き続きランサムウェアは医療機関の最大の懸念事項になると予測しています。ハッカーはデータを暗号化する手法を高度化して、次々と新しいランサムウェアを開発しているため、医療システムも継続的にそのような状況を監視する必要があります。さらに、最も重要なのは、新しい攻撃方法に合わせて、セキュリティを確実に変更し、従業員をトレーニングすることです。患者のデータを保護できるかどうかは、あなたにかかっています。

9 commvau.lt/2jNac17　10 commvau.lt/2jfF7Cw

臨床データから医療業務データに至るまで、医療機関のあらゆるデータを完全に保護し、アクセス可能な状態に保つ単一ソリューションを提供しているのは、Commvault だけです。詳細については、commvault.com/healthcare をご覧ください。

COMMVAULT

COMMVAULT SYSTEMS JAPAN 株式会社　〒141-6008 東京都品川区大崎 2-1-1 THINKPARK TOWER 8F

WWW.COMMVAULT.COM | PHONE: 03-5747-9610 | JPSALES@COMMVAULT.COM