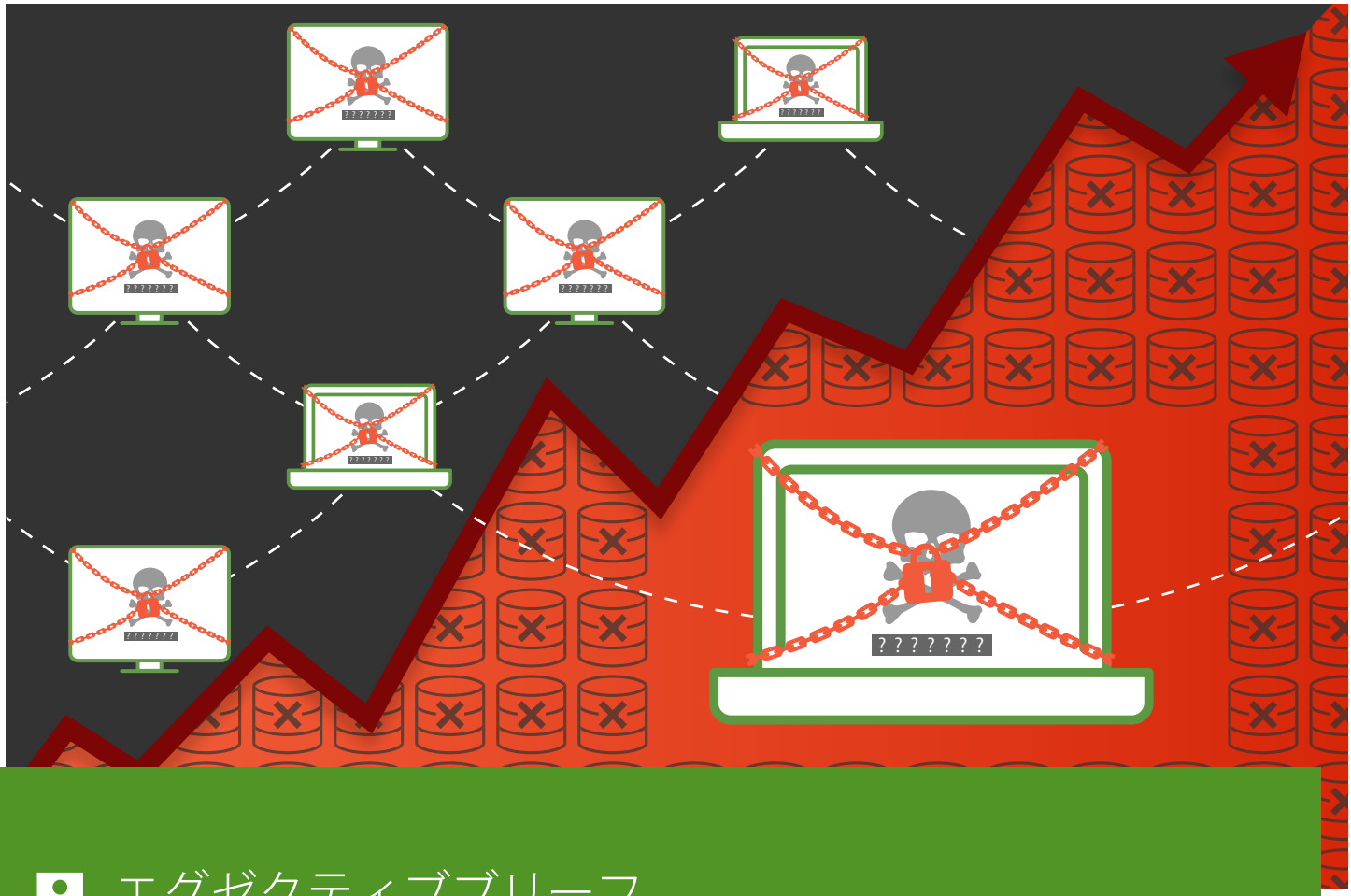
druva



エグゼクティブブリーフ

Druva ランサムウェア 年次レポート

2017年版

概要

ほとんど毎日、ランサムウェアに関するさまざまなニュースが取り上げられています。米国司法省は、2016 年 1 月 1 日から 1 日平均 4,000 件のランサムウェア攻撃が行われていると報告しています [1]。ランサムウェアはかなり大きな国際ビジネスに発展しており、2017 年末までの全世界の被害規模は、2016 年の予想から 400% 増加し、50 億ドルに達すると推測されています。

要求された身代金の平均は 2,500 ドル [2] に上昇しましたが、この金額は企業が苦しむ生産性低下の時間、データリカバリに費やされたリソース、インシデントの範囲特定や被害があったかどうかを確認するために必要な時間や労力に比べるとそれほど大きくはありません。

最終的に重要なデータが回復できなくなり、それに起因する計り知れない影響によってコストがさらに悪化するかもしれないことを考えると、ランサムウェア攻撃が組織に与える潜在的有害性は非常に深刻なものであることが明らかです。

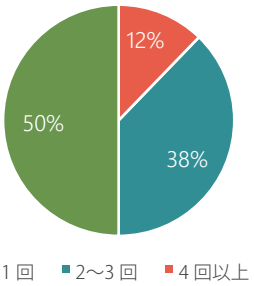
ランサムウェア攻撃の増加に伴い、あらゆる規模の企業が脆弱で、リスクの軽減や攻撃への対応に苦慮していることが判明しました。

このような状況を背景に、Druva はランサムウェアが企業に与えた影響、企業がインシデントにどう対応したか、これらマルウェア攻撃の将来の見通しについて理解を深めるために、ランサムウェア年次調査を実施しました。本年の調査は、2017 年 5 月と 6 月に世界中の複数業界で 832 人の IT 技術者を対象に実施されました。本レポートに、調査で判明した結果をまとめます。

調査結果

ランサムウェアは一度かぎりではない

適切な保護を実施していない組織はランサムウェア攻撃によって崩壊する可能性があります。残念なことに、ランサムウェア攻撃から復旧したとしても、将来の攻撃に対する免疫ができるわけではありません。調査回答者からは、ランサムウェアは継続的な脅威であり、50% の組織が複数の攻撃に遭っていたことが示されました。



50%
の組織が攻撃に
複数回遭遇

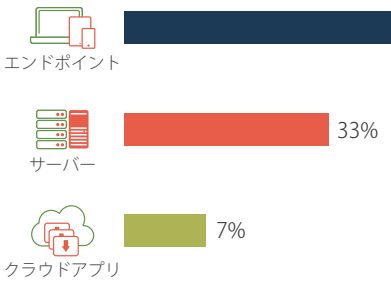
攻撃後に通常業務へ戻ろうとしている組織に対して、繰り返し攻撃が行われることでさらに大きな被害を受ける可能性があります。ミシガン州のラジオ局オーナー [3] は、業務が正常に戻った翌日に別の攻撃を受け、攻撃からの復旧に 1 週間を費やしたと報告しています。

ランサムウェアからの防御戦略を策定している組織にとって、考慮すべき唯一の要素がリカバリ機能です。ランサムウェアのレスポンス計画 (チェックリスト) には、リカバリを行うまでの時間と、必要なすべての手順について責任者や時間軸とともに示されるべきです。

しかし総合的な計画を立てても、すべての攻撃はある程度のダウンタイムをもたらすため、企業はダウンタイムを最小限に抑え、業務への全体的な影響を減らすことができなければなりません。

エンドポイントだけの問題ではない

組織内で注目されることの多くは、従業員が理解できていないことと、コンピューター活用習慣に問題があることによる脆弱性でした。運用ポリシーが不適切である、または無視されていることによって残されたセキュリティホールが悪用



33%
が**企業サーバー**
を攻撃

「ランサムウェアは増加しており、バックアップをとることがデータ消失に対する最善の防御策です。組織はフェールセーフとしてラップトップやワークステーション向けに企業型エンドポイントバックアップを実装し、組織が許容可能なデータ損失時間に基づいて、ランサムウェア被害のリスクが高いと思われるサーバーに RPO (目標復旧時点) を設定する必要があります。」

- Gartner 社、データセンターバックアップおよびリカバリソフトウェアのマジッククワドラントより

---

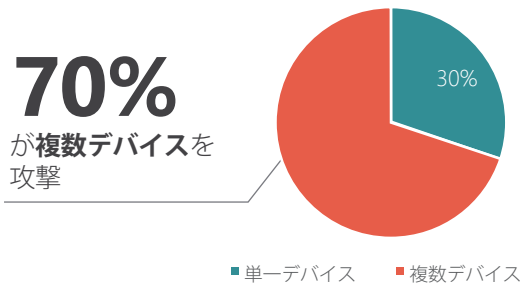
1) How to Protect Your Network from Ransomware, U.S. Department of Justice, 2017.
2) The Rise of Ransomware, Ponemon Institute LLC, January 2017.
3) "Tiny Michigan radio station hacked with 'ransomware'—twice in two weeks," CBC Radio-Canada, January 20, 2015.

されて、マルウェアがラップトップや他のエンドユーザーデバイスに感染することで大半のランサムウェア攻撃が成功しますが、サーバーに対するランサムウェア攻撃のリスクは非常に大きく、エンドポイントと同様に重要に扱いながら検討する必要があります。調査回答者は、組織で発生したランサムウェア攻撃の 33% が、サーバーも攻撃対象にしていたことを報告しています。

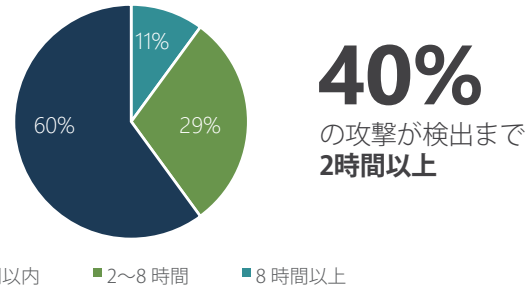
最近のニュースでは、企業のサーバー環境にランサムウェア攻撃がもたらすリスクが強調されています。韓国のウェブホスティング企業である Nayana 社は最近、153 台の Linux サーバーが Erebus と呼ばれるランサムウェアの亜種に感染していたことを発見しました。150 カ国で 20 万ユーザーに影響を与えた WannaCry 攻撃は、Microsoft Windows Server 2003 を含むさまざまなオペレーティングシステムで既知の脆弱性を悪用しました。Samsam と呼ばれる別の亜種では、Red Hat JBoss ソフトウェアの脆弱性に特化して攻撃が行われました。これらインスタンスに関して、各ソフトウェアベンダーは脆弱性を認識しており、修正パッチを作成していました。しかし、定期的にサーバーにパッチを当てて最新の状態を保つという必要対策を講じていない組織においては、マルウェアがそれら既知の脆弱性を標的として攻撃しつづけることでしょう。

スピードと拡散に関連する影響

ランサムウェアが社員のデバイスやサーバー、またはクラウドアプリケーション経由で組織の侵入ポイントを発見すると、すぐに拡散します。感染デバイスの 1 台が共有ファイルサーバーやクラウドアプリケーションに同期し、その共有に接続された他の全デバイスを介して、マルウェアを組織全体に広めてしまう場合もあります。調査回答者は、組織内のランサムウェア攻撃の 70% が複数デバイスに感染したと報告しています。



ロンドン大学ユニヴァーシティ・カレッジ・ロンドンにおける最近のランサムウェア攻撃[4] は、従業員がフィッシング詐欺に遭って感染開始したと考えられています。マルウェアは IT 部門に報告される前の 5 時間で拡散し、報告された時点ではすでに大学のネットワークと共有ドライブに侵入していました。



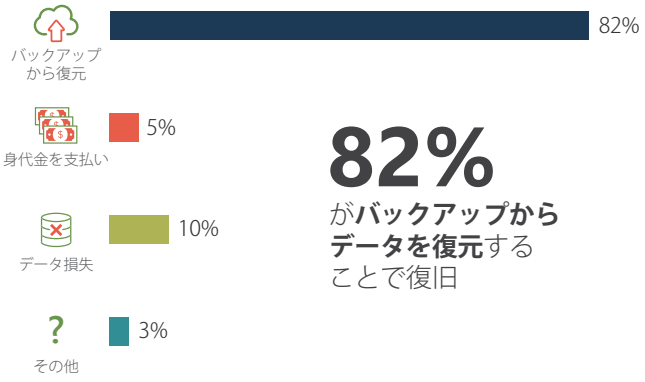
ランサムウェアが検出される前に組織内部で拡散する時間が長くなればなるほど、被害も大きくなります。潜在的な攻撃をできるだけ早く IT 部門に認識させることが重要ですが、調査結果によると攻撃の多くはすぐには検出されませんでした。感染した組織の約 40% で、IT 部門が問題を認識するまでに 2 時間以上の時間が経過していました。

ランサムウェアはエンドユーザーの不注意な操作によって組織内部に侵入することが多いため、感染したユーザーは IT 部門に連絡して事象について報告することを嫌がるかもしれません。潜伏型のマルウェアは、データを実際には暗号化しなかったり、IT 部門が気づくような振舞いを引き起こしたりせず、組織内部のデバイス間で拡散します。

マルウェアの拡散スピードと、一刻を争う緊急な対処の必要性を合わせて考えると、ネットワーク内の脅威を検出して通知するための自動機構を IT 部門が備えていることが重要です。

復旧にはバックアップが重要

ランサムウェア攻撃を操る攻撃者は一般的に、復号化されたデータに対していくらかの金額を要求します。しかし、身代金を支払ってもデータが戻ってくることは保証されません。セキュリティ企業のカスペルスキー社によると、身代金を支払った組織のうち 20% は実際にはデータを取り戻すことができなかったと推測しています[5]。そして多くの場合、感染した組織が身代金を払ったとしても、攻撃者はデータ返却を同意する前に次の身代金を要求します。



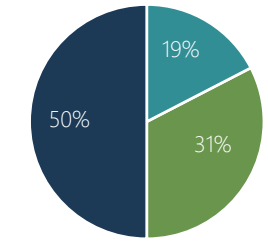
4) "University College London hit by ransomware attack," The Guardian, June 2017.
5) "To Pay or Not To Pay? Kaspersky Lab Urges More Internet Users to Join the Fight against Ransomware," AO Kaspersky Lab, November 2016.

調査回答者の大多数は、身代金を支払うのではなく、バックアップデータによって組織がランサムウェア攻撃から復旧したと回答しています。実際、回答者の 82% がバックアップを使用して復旧し、業務を再開させていました。

どの組織も被害を受ける確率は同じ

調査対象組織の規模はさまざまでしたが、調査結果は全体的に一貫しており、ランサムウェア攻撃の頻度や影響、解決策について組織の規模による明確な違いはありませんでした。あらゆる規模の組織が同じ問題を抱えており、ランサムウェア攻撃から受ける恐れのある損害を軽減するために同じ解決策として、定期的で総合的なバックアップを探しています。

病院や大学、ソニーや日産自動車などの大企業のような重要な機関に対する攻撃はメディアの注目を集めることが多いです。しかし、規模や業界を問わず、あらゆる企業でこれら攻撃の影響を感じており、生産性や収益の低下への対処に苦戦しています。



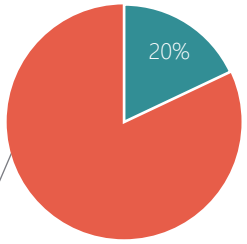
50%
の調査回答組織が
従業員数1,000人以上

■ 従業員数 1,000 人未満 ■ 1,000 ～ 10,000 人 ■ 10,000 人超

増加傾向の攻撃

残念ながら、近い将来ランサムウェア攻撃が鎮圧されるようには見えません。調査対象者の 80% は、組織に対する攻撃は実際に増加していると考えています。つまり、総合的なランサムウェア復旧計画の実現は、組織にとって無視したり、延期し続けたりすることはできないことなのです。毎日何千もの攻撃が発生しており、組織の保護対策を後回しにしている余裕はありません。

80%
の回答者がランサムウェア
被害が**増加している**と報告



■ 増加している ■ 増加していない

復元への道筋を突き止める

調査結果によると、大多数の組織がランサムウェア攻撃からの復旧をバックアップに頼っています。組織のデータが常に安全かつ利用可能であることを保証するため、データが置かれている場所に関わらず、構造化データと非構造化データの両方をバックアップ対象にする総合的な計画を立てることが重要です。

スケーラブルで効率的なバックアップ計画は、ランサムウェアだけでなくマルウェアやシステム障害、ユーザーの操作ミスによるデータ損失時に大きなメリットをもたらすとともに、一元的なデータの可視性とガバナンスも提供します。

オンサイトシステムの場合、復旧しようにも同じ攻撃によって使用できなくなることがよくあります。オフサイトストレージを活用するクラウドベースのバックアップソリューションを実装することで、このようなリスクを削減し、可用性とセキュリティを向上させることができます。

各組織は、業務上の特定要件とデータ状況に応じて、適切で詳細な計画を準備する必要があります。計画を立てる場合、以下の基本手順から始めてください。

1. 身代金を支払わない
2. すべてのデバイスをオフにする
3. デバイスをネットワークから切断する
4. 攻撃の発生源を検出する
5. すべてのユーザーに警告を行う
6. バックアップから新しいデバイスに復元する
7. 感染したデバイスのイメージを再構成する

druva
〒100-0004 東京都千代田区大手町1-9-2
大手町フィナンシャルシティ グランキューブ
グローバルビジネスハブ東京 BD342
E-mail: japan-sales@druva.com
URL: jp.druva.com

2017年7月版