Eブック

ランサムウェアを防ぐことができない5つの理由

NetApp

目次

ここ数年、ランサムウェアの攻撃が注目を集める機会が多く、感染すると深刻な影響があることを考えると、近いうちにランサムウェアが完全に撲滅されるくらいまで予防手段が発達しつつあるはずだと思うかもしれません。

かつて、悪名高いAnglerのようなエクスプロイト キットがあちこちで世間を脅かし、当時のセキュリティ チームにとって大きな頭痛の種であったのを思い出してみてください。このようなエクスプロイト キットは、それを駆逐しようとする研究者の絶え間ない努力のおかげで、記憶から消えたも同然です。

しかし、ランサムウェアはまだ至る所に存在しており、ランサムウェアを完全に防ぐことは事実上不可能です。その理由をカウント ダウンでご紹介しましょう。

5

儲かるから

攻撃者のモチベーションがこれまで以上に高まっているのは、攻撃が成功すれば大きな見返りがあるからです。米国、カナダ、欧州の組織が支払った身代金の平均額は、2019年の115,123米ドルから2020年には312,493米ドルに増加しました。これは前年比で171%の増加です。2021年第1会計四半期の平均は850,000米ドルでした。2019年以降、ランサムウェア関連の事案は65%増加しています。攻撃は今後も頻度を増加し、11秒に1回発生している攻撃が、2031年には2秒に1回の攻撃になると推定されています。こうした攻撃は、今後ますます日常茶飯事になるでしょう。このような数字を見れば、ランサムウェアが犯罪行為として好まれ続けている理由がよくわかります。

そして、法執行機関がいくら忠告しても、組織は身代金を払い続けています。企業がデータを守りたいと思うのは当然ですが、ビジネス停止による損害が身代金そのものを上回ることが多いので、身代金を支払うことが最も対費用効果の高い選択肢であることが多いのです。

4

コストが安いから

その反面、ランサムウェア攻撃を仕掛けるための自己負担額は少なくて済みます。今日、攻撃者は既成のランサムウェア キットをごくわずかな額で購入することができます。このキットには、暗号化サービス、ペイロード ドロッパー、難読化ツールなど、攻撃を展開して収益化するために必要なすべてのものが含まれています。一般的なランサムウェア サービス（RaaS）のサブスクリプションは、月額100ドルあまりで利用することができます。より複雑で強力なサービスには数千ドルのコストがかかりますが、その分、見返りも大きくなります。また、攻撃者がサービスから最大限の価値を引き出せるように、サポート プランも用意されています。

3

効果が
実証されているから

ランサムウェアは収益性の高いビジネスです。フードで顔を隠した悪党が暗い部屋に潜んでいる、という固定観念は捨てましょう。これは、企業のパートナー プログラムにも匹敵する洗練されたネットワークです。RaaSの最新事例にDarkSideがあります。これは、2020年8月初旬に初めて発見され、11月にはRaaSのディストリビューション モデルに移行したものです。報告された事案によれば、一般的な要求は、データのロックを解除するための鍵と引き換えに20万ドルから200万ドルの身代金を支払え、というものです。DarkSideランサムウェアを操る者は多額の報酬を得ているだけでなく、自らを「ロビンフッド」と位置づけ、利益を上げている大企業から金銭を奪い、その収益で慈善寄付までしています。リーク サイトの情報に基づく報告によれば、これまでに少なくとも被害企業90社がDarkSideの影響を被っています。現在、DarkSideのサイトでは合計2TB以上の盗難データがホストされていますが、これも企業が支払いに応じる動機の1つです。

2

投資を早く回収できるから

ランサムウェアが魅力的であるもう1つの理由は、組織内に侵入した後の動きが速いからです。ランサムウェアは通常、Eメールの添付ファイルや、悪意のあるURL、安全でないリモート デスクトップ プロトコル、悪質な広告（「マルバタイジング」）などを通じて組織に侵入し、ネットワークをスキャンしてファイルを探し出し、内容を暗号化して身代金を要求します。残念ながら、暗号化処理が進んだ後で、それを元に戻すためにできることはほとんどありません。また、警戒すべき傾向として、暗号化する前に攻撃者がデータを盗み出すという新たな手口も生まれています。2021年5月、米国東海岸の燃料の45%を供給するColonial Pipelineがランサムウェアの攻撃を受けました。攻撃を行ったのは、DarkSideまたはその関連組織でした。DarkSideは、Colonial Pipelineのコンピュータ システムをロックしたうえに、100GBを超える企業データを盗み出しました。今回のデータ盗難は、攻撃者集団が被害企業に金銭を二重に要求するものでした。感染したコンピュータのロックを解除するための金銭を求めるだけでなく、奪取したデータの代金も要求し、被害者が身代金を支払わない場合は、盗んだデータを公に漏えいすると脅しています。

1

人は
信頼できないから

これまで、ランサムウェアが至る所で見られる理由を説明してきましたが、これを阻止する方法については、何も説明しませんでした。更新プログラムを正しく適用してシステムの健全性を維持すれば、多くの攻撃を防ぐことができるのは事実ですが、何よりも完全な防止が不可能である理由が1つあります。それは人です。

誰もが、従業員が意図的に組織に害を及ぼすことはないと信じていますが、それでもランサムウェアへの感染は発生します。これは、従業員が悪意のあるリンクやEメール、フィッシング攻撃などの危険性に対して常に過敏な状態になっていないからです。

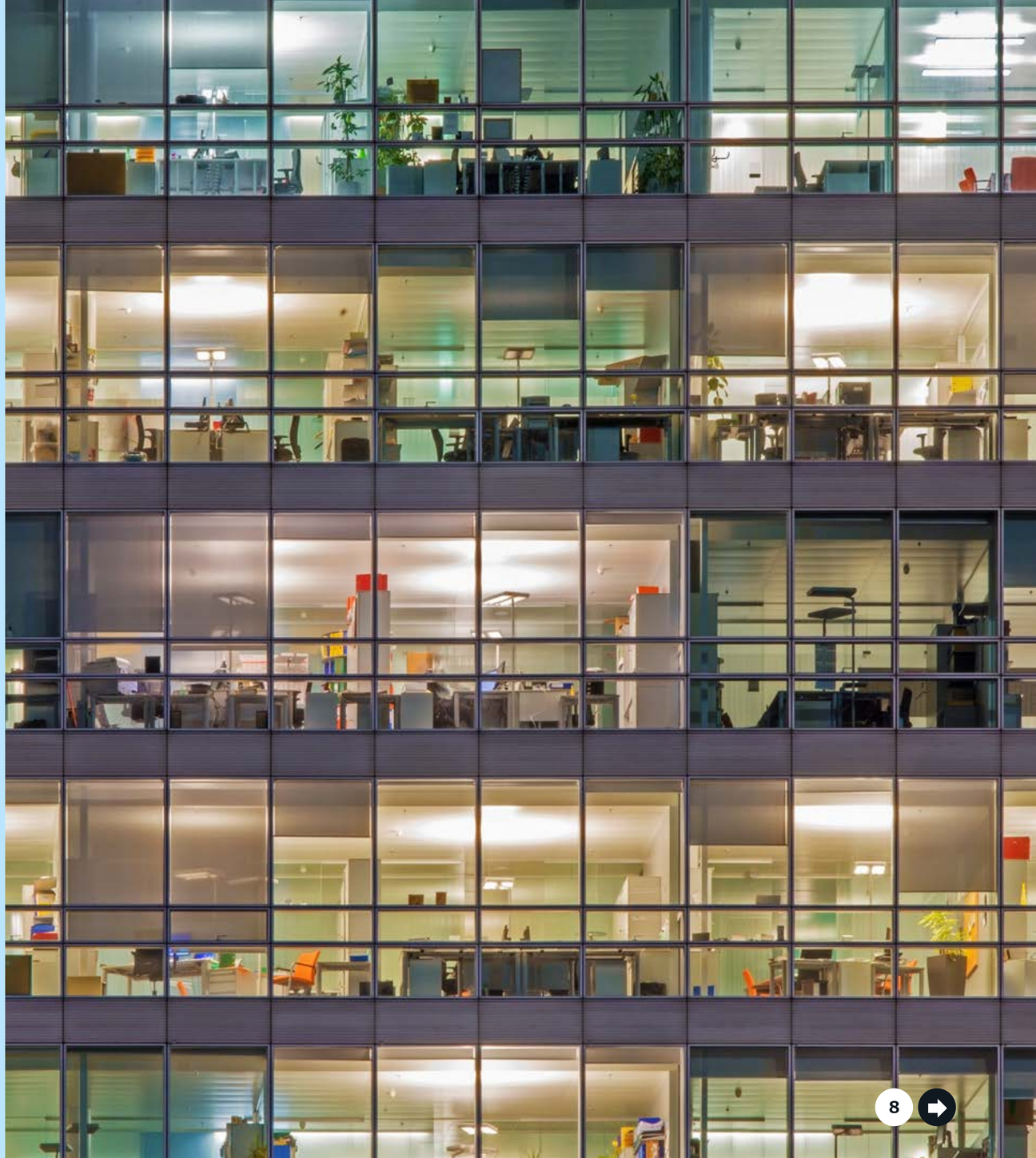
おそらく多くの読者は、定期的に義務付けられるセキュリティ意識向上のためのコンピュータによるトレーニングに馴染みがあるでしょう。確かにトレーニングは受けた方が良いのですが、どんなにセキュリティ意識の高い従業員でも、リンクをクリックしたりEメールを開いたりするときに、一瞬の判断ミスを犯してしまうことがあります。また、実際に仕事をする人の邪魔になるような厳格すぎるセキュリティ ポリシーでもない限り、一瞬の判断ミスさえあれば十分です。検出は秒単位で行われる必要があり、数分や数時間、あるいはそれ以上の時間をかけることは許されません。

ゼロ トラストのランサムウェア対策

ランサムウェアが防げないのであれば、ランサムウェアから保護するために何ができるでしょうか？

従業員は仕事をするためにデータにアクセスする必要がありますが、これはランサムウェアも同じです。だから、従業員が攻撃を媒介する手段となるのです。データへのアクセスを制限するポリシーや役割は有効ですが、その数が多すぎると生産性の妨げになる場合があります。

その答えは早期発見です。ユーザの挙動を分析し、不審なパターンが発生したときに数秒以内に自動で対処することです。



NetApp® Cloud Insightsは、このような検知を行うCloud Secureという機能を備えています。Cloud Secureでは、アクティビティを監視し、異常を検知し、自動で対応することができます。

- **ユーザ アクティビティを監視**
  侵害を正確に識別するために、オンプレミス環境とハイブリッド クラウド環境の全域にわたって、ユーザの挙動を1つ1つ把握し、分析します。データの収集は、お客様の環境のVMにインストールする軽量なステートレス データ コレクタ エージェントで行います。対象のデータには、Active DirectoryやLDAPサーバのユーザ データのほか、自社データセンターまたはクラウドにあるNetApp ONTAP®ストレージのユーザ ファイル アクティビティが含まれています。

  Cloud Secureは、ユーザの行動の異常を検出するために、ユーザごとの行動モデルを作成します。この行動モデルに基づいて、ユーザ アクティビティの異常な変化を検出し、その行動パターンを分析して、悪意のあるユーザやランサムウェアの脅威かどうかを判断します。この仕組みによって、誤検出のノイズも減らすことができます。

- **異常を検出し、攻撃の可能性を特定**
  昨今のランサムウェアやマルウェアは巧妙です。ランダムな拡張子やファイル名を使って、シグネチャ方式（ブロック リスト）のソリューションによる検出をかいくぐります。Cloud Secureは、高度な機械学習アルゴリズムを使って、通常と異なるデータ アクティビティを探り出し、攻撃の可能性を検出します。臨機応変で正確な検知を実現し、誤検出のノイズを減らすことができます。

- **自動応答ポリシー**
  Cloud Secureは、ランサムウェア攻撃の可能性を警告し、攻撃からデータを守るための複数の自動応答ポリシーを提供します。

  異常な動作を検出すると、NetApp Snapshot™コピーを作成します。データを保護することで、誤検知によるシステム停止の可能性を抑えながら、迅速なリカバリを可能にします。

以下の場合に、ユーザのデータ アクセス能力をブロックします。
- ユーザの異常な（読み取り / 書き込み）動作が検出された場合
- 異常なファイル削除の動作が検知された場合

Cloud Secureは、詳細なアクセス監査情報を提供するため、管理者は侵害されたデータとその攻撃元をすばやく特定し、迅速な問題解決とリカバリを行うことができます。

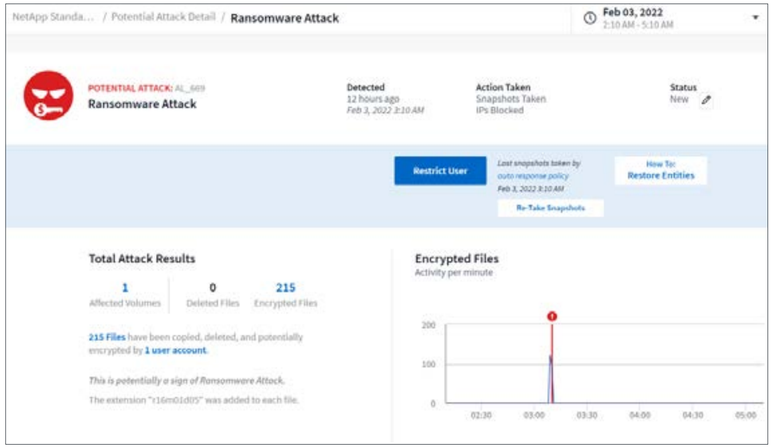


図1）Cloud Secureのダッシュボードに表示されたランサムウェア攻撃

Cloud Secureについてより詳しくお知りになりたい場合は、
30日間の無料トライアルにお申込みください。
詳細情報と無料トライアルのお申し込みはこちら

NetApp

ネットアップについて

ジェネラリストが多い世界で、ネットアップはスペシャリストとしての存在感を示しています。お客様がデータを最大限に活用できるようにすることを1つの目標として、支援に全力を注いでいます。ネットアップは、信頼できるエンタープライズクラスのデータ サービスをクラウドにもたらし、またクラウドのシンプルな柔軟性をデータセンターにもたらします。業界をリードするネットアップのソリューションは、さまざまなお客様の環境や業界最大手のパブリック クラウドに対応します。

クラウド主導のData-Centricなソフトウェア企業であるネットアップは、お客様に最適なデータ ファブリックの構築をサポートし、クラウド対応をシンプルに実現し、必要なデータ、サービス、アプリケーションを適切なユーザにいつでも、どこからでもセキュアに提供できる唯一のベンダーです。