ランサムウェアの風邪を止める3つの秘訣

30年以上の間、[1]人のサイバー犯罪者がランサムウェアを利用して、潜在的に巨額の利益を得るために企業を脅迫し、恐喝してきました。ランサムウェアは継続中世界中のヘッドラインを支配するために、企業を保護するための従来のアプローチは、敵の絶えず進化する戦術に追いついていないためです。

サイバー犯罪者は、セキュリティ制御を回避するために、ターゲットごとに独自に設計された攻撃を計画しています。—基本的に、各グループを新しい患者ゼロにします。これらの以前の、より標的を絞った攻撃に照らして、従来のソリューションではそれらを阻止するには不十分であることがますます明らかになっています実際、2020年だけでも、ランサムウェアが世界中で200億ドルを超える損害を与えたと推定されています, 1時間あたり約8,500ドルのダウンタイムに相当します。[2]

それで、ランサムウェアを防ぐ秘訣はありますか？実際には3つあり、全体的なサイバーセキュリティ体制に対して根本的に新しいアプローチを取ることから始まりますこれは、潜在的に深刻なランサムウェア攻撃からユーザー、アプリケーション、および機密データを保護するために、ゼロからクラウドに組み込まれています。

秘密 #1 駆動のサンドボックス検疫

カスタム作成されたランサムウェア攻撃の台頭。これには、これまでに見たことのない脅威が害を及ぼす前に、常に検出して阻止する機能が必要です。
従来のアプローチは、分析中にこれまでに見たことのないファイルをユーザーに渡す帯域外マルウェア分析に依存しています， その結果、システムが暗号化され、ビジネスが停止する可能性のある損害が発生します。特にランサムウェアの場合、事後にアラートを受信するのは少なすぎ、遅すぎます。これらの重大な攻撃を防ぐには、より優れたサンドボックスアプローチが必要です。

Zscaler™は何をお勧めしますか?

ランサムウェアを最終的に停止するための鍵は、最善の脅威検出を統合するマルウェア分析へのクラウドネイティブアプローチに基づいています疑わしいコンテンツを保持するAI主導の検疫により、ユーザーへの影響を減らしながら保護を強化します。

クラウドネイティブプロキシチット上に作成された業界をリードするサンドボックスとして、ファイルは、患者ゼロの感染のリスクを防ぎながら、配信前に隔離して完全に分析することができます。パススルーアプローチとは異なり、疑わしいファイルやこれまでに見たことのないファイルは、分析のために保持されることが保証されており、環境をターゲットにすることはありません。

さらに、Zscaler Cloud Sandboxのようなソリューションを使用すると、グループ、ユーザー、およびコンテンツタイプによって説明される詳細なポリシーを使用して、検疫の動きを完全に制御できます。さらに、Zscaler Cloud Sandboxは機械学習を活用しており、Zero Trust Exchange™の1つであるため―クラウド用に作成された世界最大のセキュリティプラットフォーム―グローバルコミュニティから参照された未知のファイルのほぼリアルタイムの判定を取得します，一方、危険なファイルは検疫対象としてマークされているため、ユーザーはファイルのダウンロードを高速化できます。

秘密 #2

すべてのSSLトラフィックを検査する

Google,[3] によると、現在、すべてのトラフィックの90%以上が暗号化されており、攻撃者は暗号化を利用して、ランサムウェアを含む攻撃を秘密にしておくことがよくあります。したがって、すべてのトラフィックを検査することは、ランサムウェアと対峙する際のリスクを大幅に削減するために必要です。ただし、完全なSSL検査は困難な場合があります。トラフィックの復号化、検査、および再暗号化は計算集約型であり、次世代ファイアウォールなどのレガシーセキュリティアプローチの処理能力は限られています。レガシーソリューションがアプライアンスであるかクラウド内のVMであるかは関係ありません。どちらのソリューションも、SSLトラフィックを検査するときにパフォーマンスに顕著な影響を及ぼします。

Zscalerは何をお勧めしますか

従来のアプローチとは異なり、クラウド中心のプロキシアーキテクチャでは、上から下へのSSL検査を実行できます。

クラウドネイティブプロキシにより、組織は大規模なSSL検査を正常に提供できます，パフォーマンスの低下や、高価なアプライアンスの処理能力を拡張する必要はありません。

非常にスケーラブルなZscalerクラウドは、150を超えるデータセンターにまたがるグローバルな地区であるため、労力をかけることなくすべてのSSLトラフィックを検査できます。このスケーラビリティの容易さにより、ユーザーの帯域幅が劇的に増加した場合でも、追加の費用が発生して、ユーザーごとに必要なだけのトラフィックを検査できます。隠されたランサムウェアの分析の難しさに起因するセキュリティの失効を取り除くために、これらすべてが混在しています暗号化されたトラフィックで。

秘密 #3

オフネットワーク接続に従ってください

常時オンのセキュリティは、ランサムウェアに関して組織が苦労している追加の課題です従来のアプローチがデータセンターに固定されている場合、ユーザーがVPNとネットワークをドロップオフするとどうなりますか？残念ながら、リモートワークの増加に伴い、攻撃者はゲームを強化し、多くのユーザーがセキュリティ制御と保護の範囲外で作業していることを知ってランサムウェアを実行しています, ホームネットワークとパブリックWi-Fiを介して接続し、多くの場合、制御されていないデバイスを使用します。

Zscalerは何をお勧めしますか?

常時接続の保護を実現するには、ユビキタスなクラウド配信プラットフォームから始めます。

Zscalerを使用すると、最初の2つの秘密-AI主導のサンドボックス検疫と無制限のSSL検査—ユーザーがどこにいても実行できます。ネットワーク上のすべての接続は同じ保護を受けます, 新しい未知の脅威を発見するための完全な検査を含みます。この常時接続の保護により、組織はランサムウェアや患者ゼロの感染の脅威から安全に保たれます。

ランサムウェアについて議論するためのこの包括的なアプローチは、すべてのユーザー接続がZscaler Zero Trust Exchangeを通じて保護されることから始まります。オフネットユーザーは、Zscaler Client Connectorを追加するだけです, 当社の軽量エンドポイントエージェントは、ラップトップまたはモバイルデバイスに対して、本社にいるかのように同じセキュリティ、ポリシーパフォーマンス、およびアクセス制御を提供します。さらに、Zscalerは世界中の150のデータセンターに分散しているため、ユーザーは、VPNログインを繰り返したり、VPNの遅延を発生させたりすることなく、常に最寄りのデータセンターを介して高速接続を利用できます。

ランサムウェアに別れを告げる

調査と見出しが示すように、ランサムウェアはどこにも行きません。従来のツールは、すべてのトラフィックを検査し、パフォーマンスを低下させることなく危険を大規模に隔離するという要求に対応することはできません, 患者ゼロの攻撃を防ぐために必要な常時接続の保護を提供します。ただし、Zscalerは、ランサムウェアやその他の多くのセキュリティ攻撃が比類のないスケーラビリティと優れた方法でネットワークに到達するのを防ぐために、すでに何千もの顧客を支援してきました。ユーザーエクスペリエンス。

高度な脅威の後の緊張に対して防御がどのように積み重なるかを知りたい場合は、インターネット脅威エクスポージャー分析ツールを使用してセキュリティを分析してみてください。無料で安全であり、脅威の悪用を促進したセキュリティ体制の一般的なギャップをすばやく特定します。

セキュリティをテストする

[1] https://www.zdnet.com/article/30-years-of-ransomware-how-one-bizarre-attack-laid-the-foundations-for-the-malware-taking-over-the-world/

[2] https://purplesec.us/resources/cyber-security-statistics/ransomware/

[3] https://transparencyreport.google.com/https/overview?hl=en

Zscalerについて

Zscaler（NASDAQ：ZS）はデジタルトランスフォーメーションを加速し、顧客がより機敏で、効率的で、回復力があり、安全になるようにします。Zscaler Zero Trust Exchangeは、どこにいてもユーザー、デバイス、アプリケーションを安全に接続することにより、サイバー攻撃やデータ損失から何千もの顧客を保護します。SASEベースのZeroTrust Exchangeは、世界中の150を超えるデータセンターに分散しており、世界最大のインラインクラウドセキュリティプラットフォームです。

©2020Zscaler、Inc。無断複写・転載を禁じます。 Zscaler、Zscaler Digital Exchange、Zscaler Internet Access、ZIA、Zscaler Private Access、およびZPAは、（i）米国およびその他の国におけるZscaler、Inc。の登録商標またはサービスマークまたは（ii）商標またはサービスマークのいずれかです。その他の商標は、それぞれの所有者の所有物です。