The bridge to possible

ランサムウェアからの保護

現代のワークフォースを保護するゼロトラストセキュリティ

目次

ランサムウェアの拡大 2

広がる境界 6

フィッシング、標的型攻撃、脆弱性 7

ランサムウェアの攻撃プロセス 8

ランサムウェアの侵入を未然に阻止 10

まとめ 11

Duo を利用して MFA を超える新しい防御を構築 12

参考資料 13

The bridge to possible

ランサムウェアの拡大

ランサムウェアは、攻撃戦略として急速に進化しています。かつては個々のコンピュータを乗っ取るだけでしたが、現在では危険性が高まっています。悪質な攻撃者が、地政学的に重要な対象や大規模なビジネスシステム / インフラストラクチャなどを狙うことが増え、かつてない被害がもたらされる可能性があります。現在ランサムウェアは、サイバーセキュリティにおける最大の脅威の 1 つです。コロナ禍によって突然テレワークに移行したことで、2020 年には 150% 増加しています。

ランサムウェアは現在、サイバーテロに分類されていて、バイデン米国大統領が最近発した大統領令は、システムを安全に保つために今すぐ行動を起こす必要があることを示しています。ゼロトラストアプローチは、ランサムウェアから保護するための代表的な手段です。米国国立標準技術研究所（NIST）は、「ゼロトラストアーキテクチャを導入することが、サイバーセキュリティとビジネスにおいて必須になっている」と述べています。

ホワイトハウスのファクトシートは、「SolarWinds、Microsoft Exchange、Colonial Pipeline 社などにおける最近のサイバーセキュリティ インシデントは、米国の公共機関および民間部門の組織が、国家の支援を受けた攻撃者とサイバー犯罪者の両方から、悪意のある高度なサイバー攻撃を受けるリスクが高まっていることを示している」と注意を促しています。

「SolarWinds、Microsoft Exchange、Colonial Pipeline 社などにおける最近のサイバーセキュリティ インシデントは、米国の公共機関および民間部門の組織が、国家の支援を受けた攻撃者とサイバー犯罪者の両方から、悪意のある高度なサイバー攻撃を受けるリスクが高まっていることを示している」

米国ホワイトハウスのファクトシート

ランサムウェアとは？

ランサムウェアを簡単に説明すると、主にマルウェアを利用し、さまざまな戦術を駆使してユーザーを標的に行う攻撃です。通常、電子メールフィッシング、パスワードの窃取、ブルートフォース攻撃などから始まります。その後、ファイルまたはフォルダを暗号化してシステムがハードドライブにアクセスできないようにし、マスターブートレコードを操作してシステムのブートプロセスを妨害します。マルウェアをインストールして拡散させると、ハッカーは、機密データやバックアップデータにアクセスし、暗号化して情報を人質に取ることができます。ハッカーは、迅速に移動することもありますが、ネットワーク インフラストラクチャを把握するために、攻撃を開始する前に、検出されずに何ヵ月もかけて移動することもあります。

データハイジャックは、被害者に恐怖感と切迫感を与えることを目的としています。被害者の情報は、身代金が支払われるまで（支払いは主にビットコイン）アクセスできません。また、たとえ身代金を支払ったとしても、すべてのデータを取り戻せるとは限りません。ランサムウェアには多くの亜種がありますが、cryptoransomware（暗号化ランサムウェア）が主流です。その多相性（マルウェアが絶えず変化する）により、検出を回避する多くの亜種が存在しています。

データをロックする cryptoransomware は、急速に進化しています。2006 年のランサムウェアは、独自の 56 ビット暗号化を使用していましたが、現在の高度なバージョンは、AES 対称アルゴリズムと RSA または ECC 公開鍵暗号化を使用してデータをブロックします。

ビジネスとして発展したランサムウェア

ランサムウェアは勢いを増し続け、犯罪組織（主に中国、ロシア、北朝鮮、東ヨーロッパが拠点）によって運営される専門的なビジネスへと発展し、価値の高い対象を標的として攻撃することで、データと引き換えに金銭を取得することに特化しています。犯罪組織は、身代金を効果的に得るために、コールセンターを設置し、ビットコインを購入して身代金を支払うプロセスを標的に説明することさえ行っています。中には、標的からその顧客サービスを高く評価されている場合すらあります。

攻撃者は、標的が支払う気になるように、身代金の交換後に、どのように攻撃したかを詳細に記した「セキュリティレポート」を提供することもあります。犯罪者集団が身代金と引き換えにファイルを復号することで、次の標的のために自分たちの評判を損なわないようにするのは賢明なやり方ですが、常にそうとは限りません。Sophos 社の『The State of Ransomware 2021』[英語] によると、データを取り戻せたのは被害者の 8% のみで、半分以上回復できた場合でも 29% です。収集されたデータが他の攻撃者との取引に利用される場合や、将来、もう一度身代金を得るために保持される場合があります。

近年、攻撃者は、サービスとしてのランサムウェア（RaaS; Ransomware-as-a-Service）を確立しています。これは、コーディング方法を知らなくても、誰でもランサムウェア攻撃をすぐに展開できる、完全統合型のソリューションです。SaaS（Software-as-a-Service）製品と同様に、RaaS も、独自にプログラムを作成するよりも少ない、比較的安価なコストで、この種の悪意あるプログラムを簡単に利用できます。RaaS プロバイダーは通常、身代金の 20 ～ 30% を手数料として受け取ります。現在、攻撃を成功させるのに役立つサブスクリプションモデルやアフィリエイトモデルが登場しています。ハッカーグループ REvil は、ランサムウェア攻撃の成功に貢献した全員と利益を分け合う、アフィリエイトモデルを確立しました。このモデルにより、ランサムウェア攻撃の量が劇的に増加しています。

また、最初は Maze という犯罪者集団から始まったとされていますが、二重恐喝という傾向も見られます。ハッカーは、ハイジャックして情報を入手し、自分たちの要求が満たされない場合は、ダークウェブやインターネットに公開すると脅します。ベライゾン社の『2020 年度版データ漏洩 / 侵害調査報告書』によると、ハッカーは、ハイジャックしたデータダンプを処理するインフラストラクチャを組み込んでいます。現在、「Name and shame（名前公開）」戦術が、ほとんどのランサムウェア犯罪者の間で一般的になっています。また、時間が経つほど身代金が上昇する「Penalty（ペナルティ）」モデルも増えています。

企業がランサムウェア攻撃からコンピュータとネットワークを保護する態勢を強化するにつれて、ハッカーは、モバイルデバイスをエクスプロイトする方向に転換しています。モバイルデバイスは画面がはるかに小さく、一見しただけではすべての情報を得られない（例：電子メール）ため、被害者が悪意のあるリンクをクリックしやすくなります。セキュリティが欠如している Internet of things（IoT）は、デバイスやオブジェクトがランサムウェアツールの侵入ポイントになりやすく、IoT に対する攻撃も増加しています。2020 年には、IoT デバイスを標的としたランサムウェア攻撃が、全米で 109% 増加しました。

これらの要因は、攻撃者にとって安全な避難場所として機能する国の存在と相まって、ランサムウェア犯罪の増加につながっています。2020 年には 10 秒に 1 回ランサムウェア攻撃が成功し、Anomali Harris Poll 社の調査によると、米国人の 5 人に 1 人がランサムウェア攻撃にあっています。さらに、Infosecurity Magazine は、最も一般的な攻撃方法に関して、「トップがボットネットトラフィック（28%）、以下、クリプトマイナー（21%）、情報窃取マルウェア（16%）、モバイルマルウェア（15%）、バンキングマルウェア（14%）と続く」とレポートしています。このような状況に対応するために、企業は、慌ててセキュリティにさらに多く投資しようとしています（2021 年に 1,500 億ドル：Gartner 社調べ）。

ハッカーがより多くの収益を得るために、特定の標的に重点を置くようになり、個人に対する攻撃は減少しています。マネージド サービス プロバイダー（MSP）は、SMB に対する攻撃が 85% 増加したと報告しています。社会基盤、医療機関、政府 / 自治体、製造業の各組織に加え、大規模企業を標的にして、データと引き換えに何百万ドルも要求するケースが、これまで以上に増えています。身代金の額は、この 1 年で 2 倍になっています。ベンダー、請負業者、サードパーティソフトウェアへの攻撃も急増しています。企業は、自社のシステムにアクセスできるこれらの外部関係者については、それぞれのセキュリティに委ねざるを得ませんでした。

ランサムウェア犯罪者集団の急増	ランサムウェアとして最初に明らかになった事例は、1989 年に Joseph Popp 博士が世界中に配布した、エイズに関する調査とマルウェアを含んだフロッピーディスクによるものです。このディスクは、被害者のシステム上のファイルを暗号化し、パナマの私書箱に 189 ドル支払うまでアクセスできないようにします。わなが仕込まれたディスクは、世界保健機関のエイズ会議で配布されました。ただし、支払いには問題があり、ディスクの発送にはコストがかかっていました。
2006	サイバー犯罪者は、ファイルをより高速に暗号化するために、効果の高い形式の 660 RSA 公開鍵暗号化を使用し始めました。その時代の主要なマルウェアは、フィッシングメールを侵入ポイントとして利用する、トロイの木馬の Archiveus と GPcode でした。
2008 ～ 2009	ランサムウェアマルウェアが仕込まれた新しいウイルス対策ソフトウェアが登場し、FileFix Pro で復号できるようにする代わりに金銭を要求しました。
2010	ビットコインによってすべてが変わりました。10,000 に及ぶランサムウェアの亜種が検出され、画面ロック型ランサムウェアが初めて登場しました。
2013	ランサムウェアのサンプルが 25 万にも及び、Cryptolocker とビットコインがすぐに主要な支払い方法になりました。ランサムウェアは、要求を拡大するために 2048 ビットの RSA 暗号化を使用しました。これにより、犯罪者集団に大きな収益がもたらされました。
2015	ランサムウェア型トロイの木馬の Teslacrypt が登場し、ランサムウェアの亜種は 400 万に達しました。また、RaaS（サービスとしてのランサムウェア）が導入されました。
2016	JavaScript と Locky ランサムウェアが広まり、Locky の感染は、1 日あたり 90,000 件に達しました。攻撃者は、病院や学術機関などの大規模組織を標的にしていました。ランサムウェアによる身代金が 10 億ドルを超え、Petya マルウェアによって、100 億ドル以上の経済的損失が発生しました。
2017	WannaCry クリプトワームが登場し、日々さまざまな亜種に進化しながら Microsoft 製品をエクスプロイトすることで、世界中の 300,000 台のコンピュータに急速に拡散しました。
2018	Katsuya が導入されました。SamSam は、複数の自治体サービスを停止させ、アトランタ市に大きな影響を与えました。

The bridge to possible

2019	私的な RaaS 犯罪者集団である REvil がロシアから登場しました。Ryuk は、コストのかかっている高度なランサムウェアの亜種で、悪意ある添付ファイルやフィッシングメールに埋め込まれています、同様の攻撃に比べて高額な身代金を要求し、米国のすべての主要な新聞を事実上停止に追い込みました。
2020	Darkside、Egregor、Sodinokibi が主要なランサムウェアとして台頭しました。Ryuk は、1 日 1 件だったのが、9 月までに 1,990 万件に増加しました。これは、1 秒あたり 8 件に相当します。
2021	REvil/Sodinokibi、Conti、Lockbit が、医療機関に大打撃を与えています。CryptoLocker は、大手保険会社 CNA Financial 社から 4,000 万ドルを搾り取りました。ランサムウェアによる身代金としては、これまでで最大の 1 つです。DarkSide は、Colonial Pipeline 社への攻撃に成功し、米国の重要インフラに対するハッキングとして公開されている中で最大規模となりました。

The bridge to possible

広がる境界

ランサムウェアはどのようにしてこれほど広まったのでしょうか。以前の境界は、データとアプリケーションを一箇所の門で管理する壁でした。また、仮想プライベートネットワーク（VPN）ファイアウォールやモバイルデバイス管理（MDM）ソリューションを、ネットワークという城を囲む堀のように利用していました。現在仕事は、あらゆる場所やデバイス（個人のモバイルデバイス含む）から行われ、クラウドのサードパーティ アプリケーションからデータにアクセスする必要があります。堀はなく、城への入り口がたくさんあるような状態です。コロナ禍によるテレワークの急増により、従来の境界は「ソフトウェアで定義された境界」に変わりました。従業員の勤務環境確保を急ぐ中、多くの企業にとってセキュリティは後回しになり、攻撃者がランサムウェアを仕込むチャンスが拡大しました。

リモートアクセス

『2021 年のセキュリティとリスクのトップ・トレンド』によると、従業員の 64% が在宅勤務できるようになり、実際に 40% が行っています。コロナ禍により在宅勤務が義務付けられている間、従業員の大半は 100% テレワークに移行し、クラウドやオンプレミスの SaaS アプリケーションにアクセスしながら、自分のデバイスで作業する必要がありました。多くの企業には、この変化に対応できるインフラストラクチャがありませんでした。今日、リモートアクセスは、従業員にとって新たな現実です。組織がこの運営基準に適応するにつれて、従業員の勤務形態は、テレワークを続ける人とオフィスに戻る人のハイブリッドモデルになると予測されます。

Gartner 社の VP アナリストである Peter Firstbrook 氏は、ブログに次のように投稿しています。「ニューノーマル（新たな常態）の実体が明らかになるにつれ、すべての組織に、常時接続された防御体制の確立と、リモートユーザーが高めるビジネスリスクを明確にしてセキュリティを維持することが求められています」

この変化に対応できるようにセキュリティ態勢を強化していない企業や、社内のセキュリティ教育を促進していない企業は、簡単に攻撃されてしまいます。Gartner 社は、侵害の 57% が、従業員やサードパーティの過失に関連しているとレポートしています。ZDNet によると、攻撃者が Windows コンピュータにアクセスしてランサムウェアなどのマルウェアをインストールする方法のトップは、Remote Desktop Protocol（RDP）で、電子メールフィッシングや VPN バグのエクスプロイトが続いています。

VPN の制約

VPN でのハッキングエクスプロイトは、ランサムウェアハッカーが 3 番目によく利用する侵入方法です。Colonial Pipeline 社を停止に追い込んだハッキングは、未使用の VPN から 1 つのパスワードが漏洩したことが原因でした。VPN は、オンプレミスアプリケーションへのアクセスを制限できますが、クラウドアプリケーションへのアクセス制御には一貫性がなく、脆弱性につながる可能性があります。VPN が侵害されると、ハッカーがネットワークにバックドアからアクセスし、内部システムにマルウェアをインストールできるようになります。

Google 社の調査によると、階層型 VPN およびファイアウォールを利用したゼロトラストアプローチと MFA で、自動ボットの 100%、バルクフィッシング攻撃の 99%、標的型攻撃の 90% を防げます。

保護されていないエンドポイント

企業ネットワークに接続するデバイスが増えるにつれ、個人のデバイスとシャドウデバイスも増加しています。これらのデバイスは、モニターされていなかったり、最新でなかったりする可能性があるため、主要なエンドポイントで検出されずに、侵害される可能性があります。ハッカーは細心の注意を払って侵入経路を探しているため、保護されていないエンドポイントが存在する場合や、ネットワークに接続しているユーザー / デバイスの状態を明確に把握できていない場合、侵害される可能性があります。

フィッシング、標的型攻撃、脆弱性

ランサムウェア攻撃ではどんな手法が利用されているのでしょうか。ランサムウェア攻撃は複数のステップから成るプロセスですが、比較的短期間の場合もあれば、数ヵ月にわたって実行される場合もあります。後者の場合、最も価値が高く、人質にした場合に最も大きな損害を与えられるデータにアクセスして暗号化しようとします。CSOonline.com によると、マルウェアの 94% は電子メールで配信され、フィッシング攻撃は、セキュリティインシデントの 80% 以上を占めています。その他の侵入ポイントには、パッチが適用されていない更新プログラムやゼロデイ脆弱性などがあります。これらの攻撃のほとんどすべてが、ログイン情報を盗むことから始まります。

ランサムウェアの手法

乱射攻撃、広範なフィッシング攻撃

脅威エージェントは、ブラックマーケットから電子メールのリストを取得し、ログイン情報を分析してフィッシングメールを配布します。攻撃には、2、3 件のログイン情報があればよく、多くの場合、悪意ある添付ファイルを含む電子メール、正当に見える詐欺 Web サイト、価値の高い従業員を対象とした偽のアイデンティティなどを利用して取得されます。

スピアフィッシング

特定のユーザーグループに対する組織的な標的型攻撃は、正当に見える送信元から、パーソナライズされたメッセージを送信することで実行されます。メッセージは、ソーシャルエンジニアリングに基づいていて、好奇心や恐怖を抱かせたり、報酬を匂わせたりするようなものになっています。電子メールと Web サイトには、ログイン情報を盗むためのマルウェアが仕込まれています。マルウェアは、ソーシャルメディアやインスタント メッセージング アプリケーションを介して拡散することもあります。

ブルートフォース攻撃

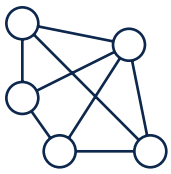
LastPass 社の調査によると、回答者の 91% が、パスワードを使い回していることを認めています。ハッカーはそれをよく知っているため、ログイン情報のダンプやダークウェブからパスワードを収集します。ハッカーは次に、自動化されたツールを利用してさまざまなサイトで複数のパスワードをテストします。これは、クレデンシャル スタッフィングまたはブルートフォース攻撃と呼ばれています。うまくログインできると、攻撃が開始されます。

既知の脆弱性のエクスプロイト

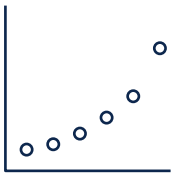
高いセキュリティを維持するには、自社のネットワークに接続しているデバイスを可視化することに加え、デバイスの状態と、パッチや更新プログラムの最新状況を把握しておくことが重要です。Security Boulevard 社は、次のようにレポートしています。「放棄された古いオープン ソース コンポーネントが増えています。また、コードベースの 91% に、4 年超の古いコンポーネントや、過去 2 年間更新されていないコンポーネントが含まれていました」

The bridge to possible

ランサムウェアの攻撃プロセス



ランサムウェアによる暗号化	攻撃の調整	垂直移動
最も一般的なランサムウェア攻撃は、ターゲットシステム上のデータを暗号化し、被害者が復号を求めて身代金を支払うまで、データにアクセスできないようにします。最新の戦術は二重暗号化で、ハッカーがシステムを 2 回暗号化するか、2 つの異なる犯罪者集団が同じ被害者を標的にするものです。このアプローチでは、攻撃者は、身代金を 2 回得るチャンスがあります。最初の暗号化で一度身代金を獲得し、それとは別の暗号化で再度身代金を得ます。最も一般的な暗号化手法は、非対称方式または対称方式です。	この時点でランサムウェアのハッカーは、標的とする特定の企業について事前に調査します。ハッカーは、ダークウェブから電子メールリストを購入し、重要なリーダーを特定します。次に会社の財務状況を調べて、ソーシャルメディアのプロファイルを調査し、請負業者、ベンダー、パートナーなどの主要な関係者のリストを作成します。ハッカーが侵入するために利用する戦術にはどんなものがあるでしょうか。2020 年における上位 3 つの攻撃は、セキュリティが不十分な RDP エンドポイントを利用した攻撃、電子メールフィッシング攻撃、VPN のゼロデイ脆弱性をエクスプロイトした攻撃でした。ログイン情報の侵害は、攻撃者がアクセス権を得る最大の手段です。	侵入と感染のフェーズでは、攻撃者が外部から内部に移動する、垂直移動が発生します。攻撃者は、内部に侵入するとファイルをスキャンし、エンドポイントとネットワークデバイスに対して悪意あるコードを実行します。マルウェアは感染したシステムを移動し、ファイアウォールとウイルス対策ソフトウェアを無効にします。攻撃者はこの時点でデータを乗っ取っていますが、まだ暗号化はしていません。垂直移動の一般的な侵入ポイントには、フィッシングされた電子メールアカウント、低レベルの Web サーバー、セキュリティが不十分なエンドポイントなどがあります。



水平移動の足がかり

APT（Advanced Persistent Threat）は、水平移動により成功を収めています。犯罪者は、足がかりを得るために、コンピュータを暗号化し、ランサムウェアをできるだけ多くのシステムに拡散する必要があります。アクセス権を得ると、ハッカーによる攻撃が始まります。ハッカーは、コマンド アンド コントロール センター（C2）、非対称鍵、バックアップファイルなどの主要なターゲットを特定するために、数週間または数ヵ月にわたって、検出されることなくネットワークを水平方向に移動します。同時に、新たなシステムやユーザーアカウントに感染することでアクセス権や実行権限を高め、永続化してデータをハイジャックするための準備を整えます。水平移動の例としては、リモートサービスのエクスプロイト、内部スピアフィッシング、盗んだパスワードの利用（「Pass the Hash 攻撃」とも呼ばれる）などがあります。

データの窃取

インベントリの評価が完了すると、暗号化が始まります。システムバックアップを削除し、ローカルのファイルとフォルダを破壊します。次に、マッピングされていないネットワークドライブを、感染したシステムに接続し、コマンド アンド コントロール センターと通信しながら、ローカルシステムで使用する暗号化鍵を生成します。そして、ネットワークデータをローカルにコピーし、暗号化してアップロードすることで元のデータを置き換えます。盗んだデータは、2 回身代金を要求するために使用できます。その場合、暗号化したデータを復号する代わりにまず身代金を要求し、次に、盗んだデータを漏洩しない代わりに、2 回目の身代金を要求します。

身代金の支払いとロックの解除

その後、攻撃者はマルウェアを起動し、データをブロックして、侵害した場所で身代金を要求します。要求には、支払い方法に関する具体的な指示（通常はビットコインで支払い）が含まれています。ランサムウェアに攻撃されると、システムがダウンして多くの損害が発生します。しかも、解決は非常に困難です。解決できずにいると脅迫され、カウントダウンが始まります。こうなると企業は、脅迫を受け入れて身代金を払う、自らファイルを復元する、身代金の一部しかカバーされないサイバーセキュリティ保険を利用する、のいずれかを選択する必要があります。これらはいずれもよい選択ではないため、組織は、ゼロトラストアーキテクチャに基づいて、強化されたセキュリティのベストプラクティスを導入し、このような状況におちいらないようにする必要があります。

脆弱な業界

医療、政府 / 自治体、小売、教育、金融は、ランサムウェア攻撃の影響を最も受けやすい業界です。これらの業界には、複雑なレガシーソリューションが残っていて、堅牢なクラウドセキュリティを活用できない場合があります。医療、教育、政府 / 自治体の各組織は、更新プログラムや新しいテクノロジーを導入してセキュリティ態勢を適応させるのが遅いため、収益を得やすい格好の標的になっています。

ランサムウェアの侵入を未然に阻止

ランサムウェア攻撃では、攻撃者は、最初にアクセス権を取得する必要があります。攻撃者は、Colonial Pipeline 社への攻撃の場合と同様に、ログイン情報を侵害することでアクセス権を取得します。

Duo の多要素認証（MFA）を利用すれば、ランサムウェアが最初にアクセス権を取得するのを防げます。Duo MFA では、ログイン時にアイデンティティを確認するために、ユーザーに、2 つ以上のログイン情報の組み合わせを求めます。たとえば、リソースへのアクセスを許可する前に、ユーザー名とパスワードに加えて、ユーザーが持っている別の情報（信頼できるデバイス、ソフトウェア / ハードウェアトークンなど）を要求します。このように追加情報を要求することで、ランサムウェアが最初の足がかりを得にくくなります。

ランサムウェアは、RDP や VPN などのリモートサービスを利用して、ネットワークにアクセスすることも狙っています。Colonial Pipeline 社に攻撃したとされる Darkside は、企業の VPN アクセスを利用して、被害者の環境に侵入したと思われます。単なる MFA だけでなく、Duo MFA、Duo Device Trust、Duo Network Gateway（DNG）、Duo Trust Monitor を、1 つの信頼できるアクセスソリューションに統合することで、オンプレミス インフラストラクチャへのリモートアクセスを保護し、ランサムウェアが最初にアクセスするのを防止できます。

Duo MFA では、認証する際に、ユーザー名とパスワード以外のものが必要です。DNG を使用すれば、ユーザーは、VPN のログイン情報を気にすることなく、オンプレミスの Web サイト、Web アプリケーション、SSH サーバー、RDP にアクセスできます。Duo Device Trust は、リソースにリモートからアクセスするデバイスが信頼でき、攻撃者のデバイスではないことを保証します。最後に Duo Trust Monitor は、ランサムウェア攻撃者が活動していることが知られている国や、従業員がいない組織の国から発信されたものなど、不審な認証リクエストを検出します。

マルウェアを使用することも、一般的なランサムウェア感染手法です。そのためシスコは、Secure Endpoint や Email Gateway などの補完ソリューションを提供しています。これらのソリューションは、マルウェアベースのランサムウェアがエンドポイントに感染する前に検査し、検出してブロックします。

The bridge to possible

Duo によるランサムウェアからの保護

Gartner 社は、ランサムウェアの 90% は防止できるとレポートしています。Duo は、次の 3 つの面で組織を支援する、他に類を見ない製品です。

1. ランサムウェアが環境内で最初の足がかりを築けないようにする
2. ランサムウェアが組織に侵入した場合、拡散を防止または遅らせる
3. 攻撃者が環境内にまだ存在している間、完全に修復されるまで、重要な資産と組織を保護する

拡散を防ぐ

限られたシステムにだけ感染するランサムウェアの影響は限定的であり、組織が機能を停止して身代金を支払うような状況になることはほとんどありません。そのためランサムウェアは、組織の大部分を効果的に機能停止させ、迅速にビジネスを回復するためには身代金を払わざるを得ないようにすることを重視しています。2017 年に遡ると、WannaCry と NotPetya は、External Blue エクスプロイトを利用して Microsoft 製品の脆弱性につけ込み、ユーザーの介入なしに拡散しました。

Duo の Device Health Application を利用すれば、デバイスにパッチを適用して最新の状態に保つことができるため、ランサムウェアが自動的に拡散するのを防止できます。さらに、ログインを試みるたびに、デバイスの更新状況など、デバイスの正常性ステータスを可視化し、チェックできます。また、Duo の自己修復機能により、ユーザーは IT 部門のサポートなしに、簡単にデバイスにパッチを適用できます。

安全に修復する

ランサムウェア攻撃から回復してシステムがオンラインに戻っても、攻撃者が環境からいなくなったとは限りません。後で戻ってくるために、永続化しようとしているかもしれません。永続化の一般的な手法は、既存のアカウントを侵害するか、新しいアカウントを作成することです。多くの場合、Active Directory や、ユーザーアカウントを含む他のディレクトリにアクセスして行います。Duo MFA は、ネットワーク上に残っている攻撃者が、侵害したログイン情報を利用して簡単に標的を変えたり、水平移動したりできないようにするため、安心できます。また、攻撃を完全に修復し、永続化の痕跡をすべて削除するまでの時間を稼ぎ、攻撃者がそれ以上の被害を与えられないようにします。

ゼロトラスト セキュリティ モデルの導入

ゼロトラスト セキュリティ モデルは、「決して信頼せず、常に検証する」という原則に基づいて構築されています。そのため、組織がベストプラクティスをプロアクティブに導入すれば、ランサムウェアなどのサイバー攻撃から保護することができます。

ゼロトラストは非常に重要なため、ホワイトハウスは、ゼロトラストと MFA を明確に義務付ける大統領令を発しています。

Duo は、簡単に導入できて使いやすい MFA を提供しています。また Duo の MFA は、ユーザーとそのデバイスが検証されて信頼できる場合にのみ、アクセスを許可します。アクセスを制御して管理するこの機能は、ゼロトラストの基本的な柱の 1 つとして、ゼロトラストフレームワークを導入する上で最初のステップの 1 つになります。

まとめ

ランサムウェアはさらに拡大すると思われるため、企業は警戒を強める必要があります。ソーシャルエンジニアリングとスピアフィッシングは、組織のセキュリティの人的側面につけ込むことで成功を収めています。強力な MFA と信頼できるアクセスプラットフォームから始まるゼロトラストのセキュリティ哲学を採用して導入することは、ランサムウェア攻撃の先を行くために重要です。

The bridge to possible

Duo を利用して MFA を超える新しい防御を構築

組織は、デバイスのセキュリティ態勢や場所などのコンテキスト情報に基づいた、条件付きアクセスポリシーを導入することで、ユーザーおよびそのデバイスの信頼を確立し、ソーシャルフィッシング攻撃や標的型フィッシング攻撃によるランサムウェアの影響を回避できます。

Duo のクラウドベースのセキュリティ プラットフォームは、場所やユーザー、デバイスを問わず、すべてのアプリケーションへのアクセスを保護します。Duo の 6 つの重要な機能を利用すれば、アイデンティティとデバイスのリスクに応じたセキュアなアクセスを容易に実現できます。

1. 安全で柔軟な多要素認証方式でユーザーのアイデンティティを検証します。
2. Duo Single Sign-On は、一貫したログインエクスペリエンスを実現し、オンプレミスおよびクラウドのいずれのアプリケーションにも一元的にアクセスできるようにします。
3. すべてのデバイスを可視化し、企業アプリケーションにアクセスするすべてのデバイスの詳細なインベントリを維持します。
4. アプリケーションへのアクセスを許可する前に、管理対象 / 管理対象外両方のデバイスの正常性チェックとセキュリティ態勢チェックを行い、デバイスの信頼を確立します。
5. きめ細かいアクセスポリシーを適用し、組織のリスク許容レベルを満たすユーザーおよびデバイスにのみアクセスを制限します。
6. Duo Trust Monitor や SIEM へのエクスポートログを利用することで、リスクの高いログイン操作をモニターして検出し、認証が必要な新しいデバイスの登録や、想定していない場所からのログインなどの不審なイベントを修復します。

Duo を選ぶ理由

迅速なセキュリティ対応

Duo は、迅速かつ簡単にユーザーに展開できる単一のソリューションで、ゼロトラストの構成要素を提供しています。特定のユースケースによっては、数分で実行できるクライアントもあります。

使いやすさ

ユーザーは、アプリストアからアプリをダウンロードしてサインインするのと同じように、自分で簡単に登録できます。管理者は、メンテナンスとポリシー管理を簡単に実施し、明確に可視化できます。

すべてのアプリケーションと統合可能

Duo の製品は他のベンダー製品に依存せず、レガシーシステムと連携して機能することもできるように設計されています。お客様がどの IT ベンダーやセキュリティベンダーを利用されていても、Duo を利用すれば、すべてのユーザーが、どこからでも安全にアプリケーションにアクセスできます。

総所有コスト（TCO）の削減

Duo は導入が容易で、システムを交換する必要がないため、必要なリソースや時間、コストを大幅に削減しながら、すぐに利用してゼロトラスト セキュリティ モデルへの移行を始められます。

参考資料

『**The Pandemic-hit World Witnessed a 150% Growth of Ransomware**』[英語] (https://cisomag.eccouncil.org/growth-of-ransomware-2020/)、CISO Magazine、2021 年 3 月 5 日

『**Exclusive: U.S. to give ransomware hacks similar priority as terrorism**』[英語] (https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/)、Reuters、2021 年 6 月 3 日

『**NIST Announces Tech Collaborators on NCCoE Zero Trust Project**』[英語] (https://www.hstoday.us/industry/emerging-innovation/nist-announces-tech-collaborators-on-nccoe-zero-trust-project/)、Homeland Security Today、2021 年 9 月 24 日

『**FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware**』[英語] (https://www.whitehouse.gov/briefingroom/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware)、ホワイトハウス、2021 年 10 月 13 日

『**Types of Encryption: Symmetric or Asymmetric? RSA or AES?**』[英語] (https://preyproject.com/blog/en/types-ofencryption-symmetric-or-asymmetric-rsa-or-aes/)、Prey Project、2021 年 6 月 15 日

『**What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast**』[英語] (https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hackergroup-just-wreaked-havoc)、The Heritage Foundation、2021 年 5 月 20 日

『**What We Can Learn From Ransomware Actor“ Security Reports”**』[英語] (https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports)、Coveware、2021 年 6 月 24 日

『**The State of Ransomware 2021**』[英語] (https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx)、Sophos、2021 年

『**Data Mining Process: The Difference Between Data Mining and Data Harvesting**』[英語] (https://www.import.io/post/the-difference-between-data-mining-data-harvesting)、Import.io、2019 年 4 月 23 日

『**Ransomware: Enemy at The Gate**』[英語] (https://ussignal.com/blog/ransomware-enemy-at-the-gate)、US Signal、2021 年 9 月 3 日

『**2020 年度版データ漏洩 / 侵害調査報告書**』(https://www.verizon.com/business/resources/ja/reports/2020-data-breach-investigations-report.pdf?_ga=2.93683037.1790228182.1647404112-1981552274.1647404112)、ベライゾン、2020 年

『**Malware is down, but IoT and ransomware attacks are up**』[英語] (https://www.techrepublic.com/article/malwareis-down-but-iot-and-ransomware-attacks-are-up/)、Tech Republic、2020 年 6 月 23 日

『One Ransomware Victim Every 10 Seconds in 2020』[英語] (https://www.infosecurity-magazine.com/news/oneransomware-victim-every-10/)、Infosecurity Magazine、2021 年 2 月 25 日

『Terrifying Statistics: 1 in 5 Americans Victim of Ransomware』[英語] (https://sensorstechforum.com/1-5-americansvictim-ransomware/)、Sensors Tech Forum、2019 年 8 月 19 日

『Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021』[英語] (https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwidesecurity-and-risk-managem)、Gartner、2021 年 5 月 17 日

『1 in 5 SMBs have fallen victim to a ransomware attack』[英語] (https://www.helpnetsecurity.com/2019/10/17/smbsransomware-attack/)、Help Net Security、2019 年 10 月 17 日

『Ransomware – how to stop this growing, major cause of downtime』[英語] (https://polyverse.com/blog/ransomware-how-to-stop-this-growing-major-cause-of-downtime)、Polyverse.com

『The strange history of ransomware』[英語] (https://theworld.org/stories/2017-05-17/strange-history-ransomware)、PRI The World、2017 年 5 月 17 日

『Ransomware Timeline』[英語] (https://www.tcdi.com/ransomware-timeline)、tcdi.com、2017 年 12 月 27 日

『**A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time**』[英語] (https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time)、Digital Guardian、2020 年 12 月 2 日

『**One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack**』[英語] (https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5)、Business Insider、2021 年 5 月 22 日

『**Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare**』[英語] (https://www.wired.com/story/atlantaspent-26m-recover-from-ransomware-scare)、Wired.com、2018 年 4 月 23 日

『**Cyber-attack: US and UK blame North Korea for WannaCry**』[英語] (https://www.bbc.com/news/world-uscanada-42407488)、BBC.com、2017 年 9 月 19 日

『**Ransomware: Now a Billion Dollar a Year Crime and Growing**』[英語] (https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646)、NBCNews.com、2017 年 1 月 9 日

『**The Untold Story of NotPetya, the Most Devastating Cyber Attack in History**』[英語] (https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world)、Wired.com、2018 年 8 月 22 日

『**Ransomware in Healthcare Facilities: The Future is Now**』[英語] (https://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=mgmt_faculty)、Marshall University Digital Scholar、2017 年秋

『**New ransomware holds Windows files hostage, demands $50**』[英語] (https://www.networkworld.com/article/2265963/new-ransomware-holds-windows-files-hostage--demands--50.html)、NetworkWorld.com、2009 年 3 月 26 日

『**Preventing Digital Extortion**』[英語] (https://subscription.packtpub.com/book/networking_and_servers/9781787120365/4/ch04lvl1sec24/the-advancement-of-locker-ransomware-winlock)、PackIt、2017 年 5 月

『**The Irreversible Effects of Ransomware Attack**』[英語] (https://www.crowdstrike.com/blog/irreversible-effectsransomware-attack)、CrowdStrike、2016 年 7 月 20 日

『**New Era of Remote Working Calls for Modern Security Mindset, Finds Thales Global Survey of IT Leaders**』[英語] (https://www.businesswire.com/news/home/20210914005014/en/New-Era-of-Remote-Working-Calls-for-Modern-Security-Mindset-Finds-Thales-Global-Survey-of-IT-Leaders)、Business Wire、2021 年 9 月 14 日

『**FBI sees spike in cyber crime reports during coronavirus pandemic**』[英語] (https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic)、The Hill、2020 年 4 月 16 日

『**シマンテックセキュリティ概観 - 2021 年 9 月**』(https://symantec-enterprise-blogs.security.com/blogs/japanese/shimantetsukusekiyuriteigaiguan-2021nian9yue)、Symantec Security、2021 年 9 月 27 日

『**INTERPOL report shows alarming rate of cyberattacks during COVID-19**』[英語] (https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19)、Interpol、2020 年 8 月 4 日

『**2021 年のセキュリティとリスクのトップ・トレンド**』(https://www.gartner.co.jp/ja/articles/gartner-top-security-and-risk-trends-for-2021)、Gartner、2021 年 4 月 5 日

『**Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time**』[英語] (https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time)、Gartner、2020 年 7 月 14 日

『**Gartner Highlights Identity-First Security as a Top Security Trend for 2021**』[英語] (https://www.attivonetworks.com/blogs/gartner-identity-first-security-in-2021)、Attivo、2021 年 4 月 27 日

『**2021 SonicWall Cyber threat Report**』[英語] (https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyberthreat-report.pdf)、SonicWall、2021 年

『**Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme**』[英語] (https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme)、ZDNet.com、2020 年 8 月 23 日

『**VPN exploitation rose in 2020, organizations slow to patch critical flaws**』[英語] (https://www.cybersecuritydive.com/news/trustwave-network-security-remote-access/602044/)、Cybersecurity Dive、2021 年 6 月 18 日

『**最新の研究結果：アカウントの不正利用を防止する基本的な方法とその効果**』(https://japan.googleblog.com/2019/05/new-research-how-effective-is-basic.html)、Google Japan Blog、2019 年 5 月 17 日

『**Top cybersecurity statistics, trends, and facts**』[英語] (https://www.csoonline.com/article/3634869/top-cybersecuritystatistics-trends-and-facts.html)、CSOonline.com、2021 年 10 月 7 日

『**Protecting Companies From Cyberattacks**』[英語] (https://www.inc.com/knowbe4/protecting-companies-fromcyberattacks.html)、Inc.com、2021 年 9 月 20 日

『**ThreatList: People Know Reusing Passwords Is Dumb, But Still Do It**』[英語] (https://threatpost.com/threatlistpeople-know-reusing-passwords-is-dumb-but-still-do-it/155996/)、Threatpost、2020 年 5 月 25 日

『**Synopsys Study Shows 91% of Commercial Applications Contain Outdated or Abandoned Open Source Components**』[英語] (https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-ofcommercial-applications-contain-outdated-or-abandoned-open-source-components)、Security Magazine、2020 年 5 月 12 日

『**Ransomware's Dangerous New Trick Is Double-Encrypting Your Data**』[英語] (https://www.wired.com/story/ransomware-double-encryption/)、Wired.com、2021 年 5 月 17 日

『**Combating Lateral Movement and the Rise of Ransomware**』[英語] (https://www.msspalert.com/cybersecurityguests/combating-lateral-movement-and-the-rise-of-ransomware)、MSSP Alert、2021 年 6 月 24 日

『**Lateral Movement**』[英語] (https://attack.mitre.org/tactics/TA0008/)、MITRE| ATT&CK、2019 年 10 月 17 日

『**Industries Impacted by Ransomware**』[英語] (https://airgap.io/blog/industries-impacted-by-ransomware)、AirGap.com

『**Defend Against and Respond to Ransomware Attacks**』[英語] (https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks)、Gartner Research、2019 年 12 月 26 日

『**Executive Order on Improving the Nation's Cybersecurity**』[英語] (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)、ホワイトハウス、2021 年 5 月 12 日

C11-3233828-00　10/22