すべてを変える
AI時代のランサムウェア

Barracuda

生成AIの台頭

2023年には人工知能（AI）がほぼ毎日ニュースの見出しを飾り、ChatGPT、Bard、Midjourney などの生成AIツール（GenAI）の開発が、技術者とアマチュアの両方から称賛されています。生成AIが脚光を浴びている今、AIは職場の生産性向上などの前向きな活動に使用できる一方で、より邪悪な目的にも導入できる可能性を忘れないことが重要です。悪意のある人物が AI を新たに有害な用途に利用している分野の1つに、ランサムウェアがあります。

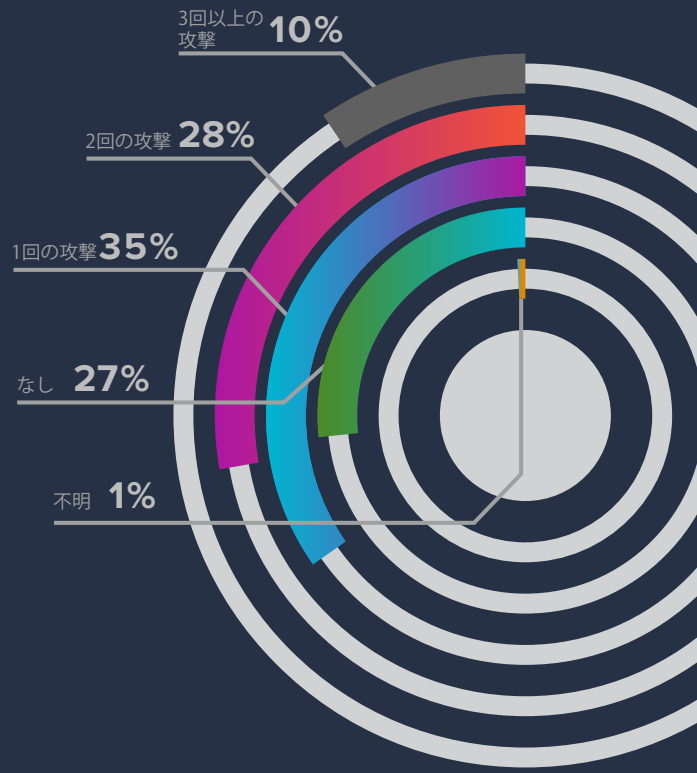
今日のランサムウェアの状況

ランサムウェアは、サイバー犯罪者が狙ったネットワークを感染させてシステムを停止させ、データを暗号化するように設計、展開できる悪意のあるソフトウェアです。ランサムウェアは、近年蔓延しており、その目的は、機密情報を盗み、データを公開すると脅迫して身代金を取ることです。

ランサムウェアに関する事件のうち53%で、攻撃者は機密データを窃取し、その貴重なデータ公開の対価として、追加の身代金を要求しています。ランサムウェア攻撃への参入障壁はこれまでになく低くなり、その報酬はかつてないほど高くなっています。ランサムウェア攻撃は、非常に利益が高く、リスクが低い形態のサイバー犯罪であり、年々巧妙化し、その頻度が増しています。

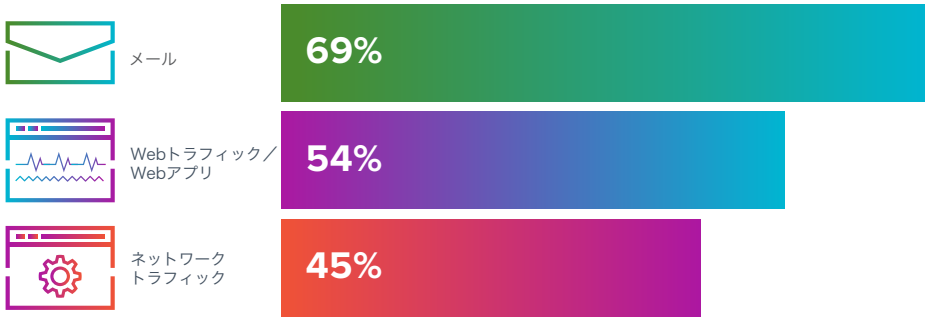
Barracudaの最新市場レポートである「2023 ランサムウェアに関する洞察」によると、回答者のほぼ4分の3（73%）が、2022年にランサムウェア攻撃の実際の被害に遭い、63%が攻撃を受けたことが明らかになりました。

所属する組織は、過去12ヶ月間に何回のランサムウェア攻撃を経験しましたか？



出典: 2023 ランサムウェアに関する洞察

この調査結果でも、調査対象の組織の69%で、ランサムウェア攻撃の一部は悪意のあるメールから始まっていたことが示されています。そして、調査対象となった大規模な組織、つまり従業員数250名を超える組織の場合、その割合はさらに高くなり、75%となりました。このような攻撃はフィッシング攻撃であることが多く、悪意のあるリンクが貼られたメールが組織からのメールであるかのように偽装され、例えば、不正アクセスされた個人がパスワードをリセットするためにログイン認証情報を入力するよう要求したり、あるいは他の同様の行為を要求したりします。



出典: 2023 ランサムウェアに関する洞察

フィッシングメールのリンクは、キーロガーなどの悪意のあるファイルを自動的にダウンロードして実行し、時間の経過とともにログイン認証情報を盗むことがあります。認証情報は、ネットワークに侵入して攻撃を助長するための鍵です。

最初の攻撃が、メールから始まらないケースもあります。複数の攻撃を経験している場合には、複数の媒体から攻撃を受けるという状況が多く発生していました。上記のレポートでは、被害ケースの54%が Web アプリケーションを通じて最初の攻撃を受けたとし、その内の45%で実際に被害に遭った最初の攻撃は、組織のネットワークを通じて行われたとしています。多くの場合、攻撃者はさまざまな手法を組み合わせて脆弱性を悪用し、攻撃から最大限の価値を引き出します。

攻撃の発端がどのようなものであれ、最終的な目標は、抜き出せるデータを求めてネットワーク内を移動しランサムウェア攻撃の下地を作ることです。いったんデータが盗まれると、攻撃者は実際のランサムウェアの要求を開始する前に、大抵の場合、バックアップデータを暗号化するか、削除して復旧を妨げようとします。

AIを活用したランサムウェア

AI を活用したランサムウェアは、その名の通り、従来のランサムウェアと新たな AI技術を組み合わせたものです。サイバー犯罪者はAIを利用してランサムウェア攻撃をこれまで以上に効果的にし、自分たちの生産性を向上させるでしょう。今後、フィッシングからデータの身代金の交渉まで、ランサムウェアのあらゆる側面で AI が使用されるようになります。

AIと自動化により、フィッシング、ビッシング（電話による音声フィッシング）、スミッシング（SMSベースのフィッシング）メッセージを作成できます。ネットワーク攻撃やアプリケーション攻撃を開始したり、通常のトラフィックでのデータ漏洩を隠す方法を最適化したり、ランサムウェアの金額を調査して交渉することができます。AI はそのようなすべてを最適化するために存在します。これは将来的な見通しではなく、現在すでに起こっており、当社独自のランサムウェアレポートの最新の数字でわかるように、ランサムウェア攻撃は新たなレベルに達することが可能になっています。

AI を活用したフィッシング攻撃はおそらく、悪意のある攻撃者がこれらの新機能を利用した最も初期の例でしょう。ChatGPTのようなツールが公開されるとすぐに、サイバー犯罪者は悪質な目的のために独創的な方法でそのツールを使用しようと試みます。

GenAI チャットボットやその他の自然言語処理（NLP）ツールのおかげで、大規模言語モデル（LLM）を使用して、人間が書いたように見えるテキストを生成できます。そのためサイバー犯罪者は、タイプミスや文法的な間違いなど、メール、SMS、その他の通信が本物ではない可能性を示す兆候なしに、フィッシングリンク用のメッセージを作成することができます。非母語話者であっても、身元の偽造が自分の口調からばれてしまう心配なしに、AI を使用して他の言語でメッセージを生成できます。これは、説得力のある攻撃を計画できるサイバー犯罪者集団の規模が劇的に増加し、フィッシング、スミッシング、フィッシングのメッセージを悪意のあるものと見抜くのがはるかに困難になったことを意味します。

AI が自然言語プロンプトを使用して作業の多くを実行するため、攻撃者はネットワーク、アプリケーション、その他の IT の脆弱性を見つけ出して悪用する能力が向上します。これに高度なコーディングスキルは必要ありません。

現時点では、AI にはまだ知識のある個人によるある程度の操作が必要ですが、AI と自動化は、高速で誘発できる膨大な量の攻撃を予定している、これらの犯罪グループにとって、状況を一変させるものであることは疑いの余地がありません。また、カスタマイズされた攻撃は実行コスト効率がはるかに高くなるため、サービスとしてのランサムウェア（RaaS）も強化されます。

AI を活用した
ランサムウェアの防御方法

Barracuda は、AI を活用したランサムウェア攻撃から組織を守る3段階の保護対策を推奨します。

基本的な手順は次のとおりです。

1. メールの保護
2. ネットワークとアプリケーションのセキュリティ保護
3. データのバックアップ

メールを保護するためには、複数の層に分けての対応が必要になります。組織で、メールセキュリティソリューションが認証情報も保護し、弱点や特に攻撃対象となりやすい個人を特定するために AI を使用したトレーニングを組み込み、異常を検出するためにセキュリティオペレーションセンター（SOC）を使用していることを確認する必要があります。

セキュリティ意識向上トレーニング（SAT）は不可欠です。従業員が潜在的なフィッシング攻撃を特定する方法と、侵害の疑いがある場合の対処方法を正確に理解することは重要です。これは一度行ったら終わりというものではありません。トレーニングは定期的に行われ、サイバー攻撃の最新の傾向に沿ったものでなければなりません。

ネットワークとアプリケーションセキュリティの確保も多面的な取り組みであり、これを十分に網羅するにはEbookがもう1冊必要になるでしょう。基本は、ネットワークの各部分やさまざまなアプリケーションに誰がアクセスできるかを制限する ZTNA（Zero Trust Network Access）を使用し、ネットワークをセグメント化し、SOCとXDR（Extended Detection Response）を使用して異常なネットワークトラフィックを識別し、エンドポイント、メール、ファイアウォール、サーバなどを保護します。セキュアアクセスサービスエッジ（SASE）は、クラウドアーキテクチャとオンプレミスアーキテクチャの両方が連携して機能し、最も効果的かつ効率的なセキュリティレベルで保護されるようにするための優れた方法です。

データのバックアップは、ランサムウェアから身を守るもう一つの重要な要素です。ランサムウェア攻撃はシステムをオフラインにしてデータを暗号化しようとするため、組織は身代金を支払わずにデータを復元できるように、不変で安全なバックアップを確保する必要があります。このバックアップには、必要な個人のみがアクセスできるように、複数のレベルのロールベースアクセス制御が必要です。また、攻撃が開始された場合に、ランサムウェア攻撃者がバックアップを見つけて回復を妨ぐために暗号化できないように、メインネットワークとは別に保管する必要があります。

侵害の防止と修復にAIを活用する方法

AIは、悪意のある攻撃者がランサムウェア攻撃を扇動するために使用できるのと同様に、組織のセキュリティチームが侵害を防御し、攻撃の試みや実際の攻撃に対する修正措置の実施に使用することもできます。

- AI を活用したランサムウェア検出では、ネットワークトラフィックやファイルアクセスの分析に加え、ランサムウェア攻撃が予期されているのか、またはすでに進行中であるのかをその活動から分析できます。

- AI を活用したアクティビティ監視では、ユーザの行動を観察して、ログイン試行の失敗や異常なファイルアクセスなどについて、不審な活動によるものか、通常業務によるものかを識別できます。

- 多要素認証（MFA）は AI を使って強化でき、タイピング速度を分析したり、機密データに対して複数の認証レベルを要求したりするほか、異常なアクセスを試みるユーザをブロックすることで、組織のセキュリティを強化できます。

まとめ

AIランサムウェア攻撃が進化し続けるにつれて、攻撃を防御し軽減するために開発される AI ツールも進化します。組織にとって、これらの深刻で高度な侵害への防御と修復に役立つ最先端の技術ソリューションをすべて最新の状態に保つことが重要です。よく引用される「準備を怠ることは失敗するための準備をするのと同じだ」という言葉がここには当てはまります。攻撃に遭ってから修復しようとするよりも、ランサムウェアに備えて阻止する方がはるかに効率的であり、コストも低くなります。

このEbookが、AI を活用したランサムウェア攻撃を真剣に受け止め、それを防御するための方法を講じるとともに、そのために利用可能な AI ツールの活用の重要性に光を当てる一助となれば幸いです。

Barracuda のランサムウェアソリューションは、AI による攻撃を含むあらゆるランサムウェア攻撃からユーザを保護するために 3 段階のアプローチを採用しています。まずメール認証情報を保護し、次にアプリケーションとアクセスを保護し、次に安全なバックアップでデータを保護します。詳細またはご相談については、ランサムウェアソリューションのページをご覧ください。

バラクーダについて

バラクーダは世界をより安全な場所にするために尽力しています。

バラクーダは、すべてのお客様が購入、導入、使用しやすい、クラウド対応かつエンタープライズレベルのセキュリティソリューションを使用できることが当然であると考えています。また、お客様のビジネスとともに成長および変化する革新的なソリューションによってメール、ネットワーク、データ、アプリケーションなどを保護しています。

世界中の20万を超えるお客様がバラクーダを信頼しています。お客様がリスクにさらされていることを知らない場合でも、バラクーダはお客様を保護できます。このため、お客様はビジネスを次の段階に移行することに注力できます。

詳細については、barracuda.co.jpをご参照ください。