脅威を阻止する VOTIRO ソリューション

VOTIRO SECURED.

未知の脅威から守ります。

目次

Votiro について

2010年に設立されたVotiroは、サイバー攻撃のターゲットでありながら、従来の企業向けITソリューションから十分な保護を受けていない組織のために保護対策を提供するサイバー保護テクノロジーの業界リーダーです。

Votiroは、諜報、政府、および企業向けセキュリティにおいて豊富な経験を積んだセキュリティ専門家のチームによって創立されました。

組織における機密性の高いデータの保護の必要性に精通しているVotiroチームは、ネットワークやインフラをサイバー攻撃から保護するための独自のソリューションを開発しています。

Votiroのお客様には、ネットワーク機器ベンダー、ソフトウェアベンダー、政府、防衛機関、金融機関、通信事業者、製薬会社、医療機関などがあります。

詳細は、
https://www.asgent.co.jp/ をご覧いただくか
info@asgent.co.jp までご連絡ください。

高度なコンテンツ無害化と再構築技術

CDR：Content Disarm and Reconstruction
（コンテンツ無害化と再構築）

サマリー

どんな企業においても、サイバー防衛対策は必須課題です。しかし、未知の攻撃やゼロデイ攻撃がありふれている中で、多くの企業がいまだに無力なソリューションを利用しています。
サイバー犯罪者が以前にも増して専門的かつ、標的型攻撃を成功させるための巧妙化している今日、サイバー保護への革新的なアプローチが必要となります。Votiroが提供する高度なCDR（Content Disarm and Reconstruction）技術は、未知の脅威やゼロデイ攻撃を一刻も早く阻止するための究極のソリューションを実現します。

ニーズ

データに依存するようになった現在、その中に潜在するリスク、脅威、および脆弱性が顕著になります。また、このような脅威の多くは従来のネットワークセキュリティデバイスでは検知できません。
以前は、サイバーセキュリティの脅威は組織の活動に限定的な影響しか与えませんでした。しかし、データへの依存性が増していくにつれて、組織の活動におけるサイバーセキュリティの脅威による悪影響も増しています。組織を効果的に保護するためには、ますます悪質になりつつあるサイバー攻撃に対して、セキュリティの新たなアプローチが必要になります。

標的型攻撃による脆弱性の悪用

仕様上、エクスプロイトはアプリケーション内の脆弱性を攻撃し、侵入者が仕掛けたコードを呼び起こすように設計されています。

脆弱性とは、アプリケーション (例えば、Adobe Reader) 内の " 穴 " のようなものであり、特定のコンピュータやネットワークシステムに対して攻撃を実行するために利用されます。脆弱性を悪用する方法として、スピアフィッシング攻撃が最も一般的です。これは、一見、無害そうなメールに悪意のあるファイルを添付して受信者に送信する攻撃手法です。受信者が添付ファイルを開くと、マルウェアがデプロイされ、標的型攻撃が成立します。

脆弱性のライフサイクル

ソフトウェアの脆弱性はサイバー犯罪へのドアを開く働きをします。脆弱性を利用すると、システムに侵入し、そしてデータへのアクセス権を不正に取得することができます。脆弱性の脆弱性のライフサイクルは、未知、ゼロデイ、そしてパッチ済みの3つの段階に分けられます。

脆弱性のライフサイクル

	 **第1段階** 未知	 **第2段階** ゼロデイ	 **第3段階** パッチ済み
脅威	高	高	低
期間	年	月	該当しない
シグネチャによる検知	NO	提供されたサンプルに依存	提供されたサンプルに依存
Votiroによる保護	**YES**	**YES**	**YES**

とその悪用

第1段階

未知

この段階では、アプリケーション、システム、あるいはハードウェアに存在する脆弱性がベンダーやセキュリティコミュニティーには知られていないが、何者か、例えばサイバー防衛専門の組織（あるいはより悪質な者）の研究者などに発見されています。
この種の脆弱性は誰にとっても危険性の高いセキュリティ脅威となり、何年も発見されないままに残る場合もあります。当該ベンダーはその脅威に気づいていないため、その悪用を防止、阻止するためのいかなる対策も開発しません。未知の脆弱性は通常、サイバーインテリジェンスを収集するグループ、または金儲けを目的に情報売買を行うグループに利用されます。

第2段階

ゼロデイ

この時点では、脆弱性はベンダーおよびセキュリティコミュニティに発見されています。ゼロデイ脆弱性とは、初めて出現した脅威のことで、対策のパッチがまだ開発されていない脆弱性のことです。この種の脆弱性は悪用の危険性が高いです。シグネチャ型検知を利用する侵入検知システムまたは、従来の保護システムは多数のサンプルを収集、抽出して悪用の行為を特定しますが、ハッカーによって改ざんされたエクスプロイトはシグネチャ検知を回避することもあります。
また、ベンダーが脅威が報告されてから長時間（場合によっては90日以上）かけてはじめて対応する場合もあるので、ゼロデイ脆弱性は一定期間そのまま存在することがあります。

第3段階

パッチ済み

この段階では、ベンダーが脆弱性対策のパッチをすでに提供しているにもかかわらず、アプリケーションが旧バージョンでパッチをあてないまま使用されており、無差別型攻撃によりその脆弱性が悪用されることがあります。特に、小規模な組織に比べてパッチ管理がより困難となる大規模な組織は、無差別型攻撃の影響をうけやすいとされています。ただ、この段階では、ベンダーがすでにパッチを提供しているので、脅威度は比較的低いと言えます。

**Votiro独自の技術は、脆弱性のいずれの段階においても、
その悪用によるサイバー攻撃から保護します。**

ソリューション：未知・ゼロデイエクスプロイトの無害化

Votiroが提供する高度なCDR技術とは、スピアフィッシングやその他のAPT攻撃をはじめとするサイバー攻撃によって最も頻繁に悪用されるファイル形式を対象にしたプロアクティブかつシグネチャレス型の保護技術のことです。本技術は、エクスプロイトがエンドユーザー環境に侵入する前に無害化を行います。

エクスプロイトを成功させるために、マルウェア作成者は通常、複数の不審なオブジェクトを精密に設計、構築し、そしてこれらを悪質な複合ファイルに埋め込みます。例えば、Microsoft®Wordのファイルには、攻撃を実行するためのActiveX®あるいはOLEオブジェクトが含まれており、さらに悪意のある画像やマクロに呼び起こされるシェルコードも含まれている可能性があります。（シェルコードとは、特定のソフトウェア脆弱性のペイロードとして使用されるコードの一片のことです。）Votiroが提供するCDRエンジンは、ファイルを精密に検査し、悪質あるいは不審なコンテンツを特定し、そしてその悪質なコンテンツを抽出した後、ファイルの機能性を維持しながらファイルを再構築することができます。

「マルウェアのサンドボックス回避技術が向上していくと同時にコンテンツ無害化と再構築（CDR：Content Disarm and Reconstruction）をメールゲートウェイにおいてサンドボックスの代替策あるいは補強策として利用する動きも強まるでしょう。」[1]

[1] Neil Wynne、Andrew Walls、Peter Firstbrook、"Fighting Phishing: Optimize Your Defense"、Gartner出版、2016年3月17日（https://www.gartner.com/doc/3256817/fighting-phishing-optimize-defense）

ファイルでの作業にあたってユーザーが必要とする全ての機能、すなわちテキストのコピー、ブックマーク、コンテンツ、検索などが全て維持されます。

Votiroの高度なCDR技術のワークフロー

Votiroが提供する高度なCDR技術は3つの段階にわたってファイルを無害化、再構築します。

第1段階 | 形式の特定

ファイルはそれぞれのファイル形式の特有の仕様に適合している必要があります。Votiroが提供する高度なCDR技術は各ファイルを徹底的に検査し、その形式がベンダー規定の仕様に適合していることを確認するとともに、なりすまし攻撃を検出します。

ファイルのコンテンツタイプと形式を特定するために、独自のフィンガープリント技術を利用します。次に、ファイルを検査し、ベンダー規定の仕様と比較します。例えば、Microsoft Wordドキュメントの場合は、ファイルがMicrosoftのファイル形式に適合しているかどうかを確認します。Votiroエンジンはファイル構造をスキャンし、エクスプロイトの可能性を指し示すような異常なフィールドや属性を検出します。高度なCDRアルゴリズムは、ファイル特有のフィンガープリントに基づいて、そのファイルが悪意かどうか、また無害化が必要かどうかを判定します。異常なファイルがブロックされ、そしてアラートが発行されます。

第2段階 | ファイルの無害化

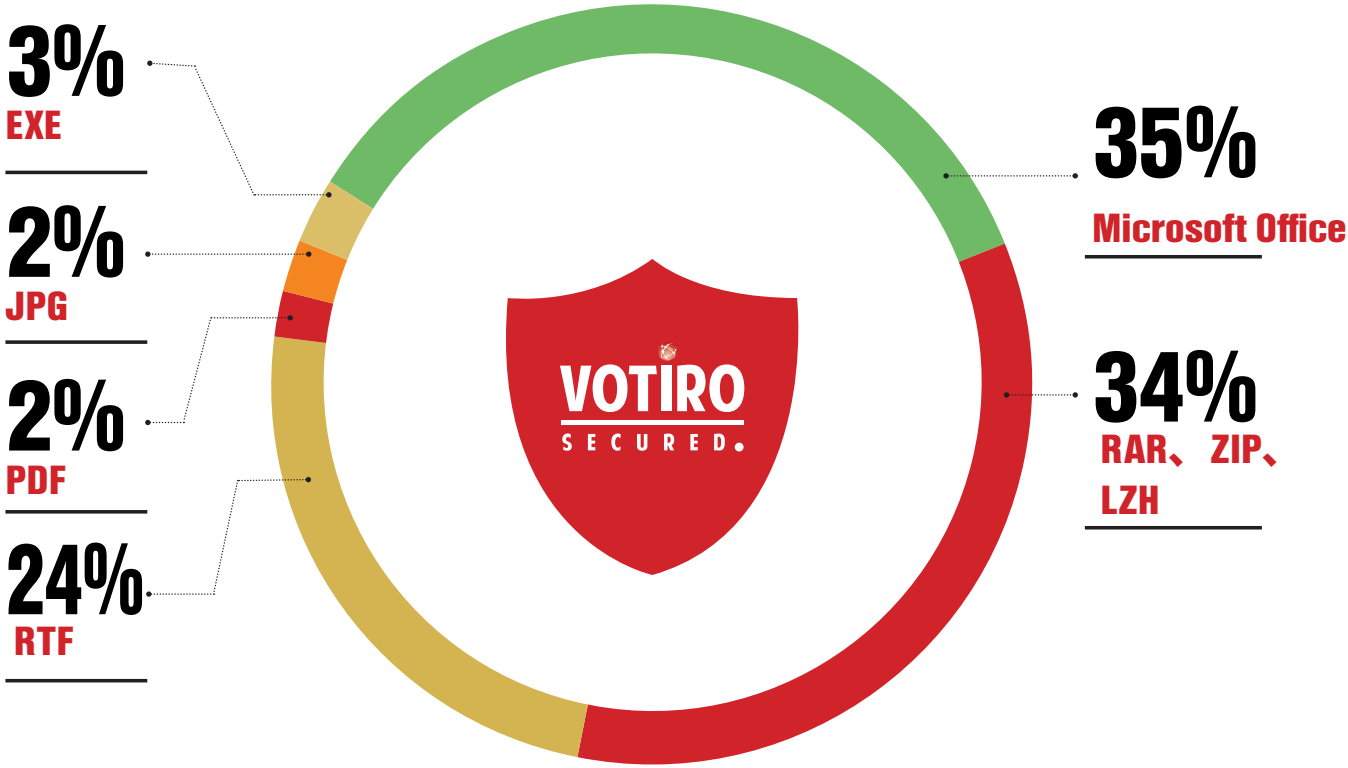
この段階では、Votiroが提供するCDR技術はエクスプロイトの実行フローに細かい変更とロードブロックを注入します。マクロ、スクリプトなど、その他の埋め込まれた不審なオブジェクトと要素が特定され、除去されます。また、その他にOLEオブジェクトや添付データなどの有効なコンテンツが再帰的に処理されます。こうして、ファイルはエクスプロイト保護プロセスによって生の形式に変換されます。これらの動作はシェルコードの実行を妨害するので、エクスプロイトは無効化されます。

第3段階 | 無害化ファイルの生成

ファイルは元のファイルと異なる形で再構築され、ファイル形式の仕様に基づいた構造になります。悪意のあるコードやエクスプロイトの全て無害化されますが、ファイルの本来の機能性は維持されています。

プロセスはユーザーの目の見えないところで実行されるので、いかなる活動も一切妨害しません。また、その処理は通常一秒以内に行われます。

標的型攻撃によく狙われるファイルタイプ



トレンドマイクロ社 "Targeted Attack Trends: 2014 Annual Report"より
(http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-targeted-attack-trends-annual-2014-report.pdf)。

Votiroが提供する高度なCDR技術は、ZIPやその他のアーカイブファイル、そして重複圧縮ファイルに対応しています。重複圧縮ファイルの場合は、複数の圧縮したレイヤーが再帰的に解凍、無害化され、そしてファイルの本来の機能性を保ちながら、再び圧縮されます。

対応ファイル形式

Votiroの高度なCDR技術は多種多様なファイルタイプを処理します。

Adobe PDF

Votiro独自の技術はPDFファイルの構造を検査し、テキスト、ページ、画像、スクリプト、ブックマーク、およびその他の要素を抽出します。設定されたポリシーによって、本プロセスではJavaScriptなどの有効なコンテンツも無害化します。その後、ファイルコンテンツを再構築し、元の構造に戻ります。

アーカイブ

Votiro独自の技術はZIP、RAR、7-Zip、CABといった一般的なアーカイブ形式をサポートします。コンテナーが解凍されると同時に、高度なコンテンツ無害化と再構築プロセスは再帰的に実行されます。コンテンツの安全性が確認されたら、元の形式に再び圧縮されます。

メール

高度なCDR技術はEMLやMSGを含む様々なメールコンテナーに対応しています。メールは件名、本文、MIMEでエンコードされた添付ファイル、およびその他の要素に分解されます。このプロセスは再帰的に実行されます。コンテンツの安全性が確認されると、メールは再構築され、宛先に送信されます。

Microsoft Officeファイル

高度なコンテンツ無害化と再構築プロセスはMicrosoft Officeファイルを分解し、画像やドキュメントなどの埋め込みオブジェクトおよびOLEオブジェクトを再帰的にチェックします。不正あるいは禁止されたオブジェクトが除去され、プレースホルダーやテキスト表記と交換されます。ファイルが安全と見なされると、再構築されます。

Microsoft RTF

テキスト、埋め込みオブジェクト、レイアウトなどのRTFファイルの要素が抽出され、そしてファイルは再構築されます。

画像

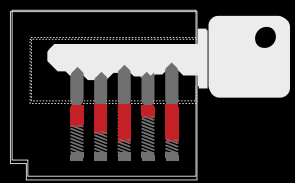
JPEG、GIF、BMP、PNG、TIFF、EMF、およびWMFといった一般的な画像形式から悪意のあるコンテンツを無害化します。

例

悪意のある画像が標的型攻撃メールに添付されています。画像は埋め込みシェルコードを含んでいます。エクスプロイトが成功するには、シェルコードがビットごとに書かれたとおりにプロセッサーで実行される必要があります。例えるなら、錠が開けられるために全てのピンが精密に位置付けられている必要があるように、シェルコードも同様の要件があると言えます。

本来、画像ビューアは添付画像のピクセルを表示するようになっています。しかし、画像に悪意あるコードが埋め込まれている場合、脆弱性のある画像ビューアであれば、画像のピクセルを表示すると同時に悪意のあるコードも実行されてしまいます。

Votiroが提供する高度なコンテンツ無害化と再構築プロセスでは、生の画像データを分析し、ビット（画像に埋め込まれた悪意のあるコード）を再構成し、そして悪意あるコードを含めずにファイルを元の形に再構築します。画像ビューアは悪意のあるコードを実行することなくピクセルを表示することができます。



高度なコンテンツ無害化と再構築API

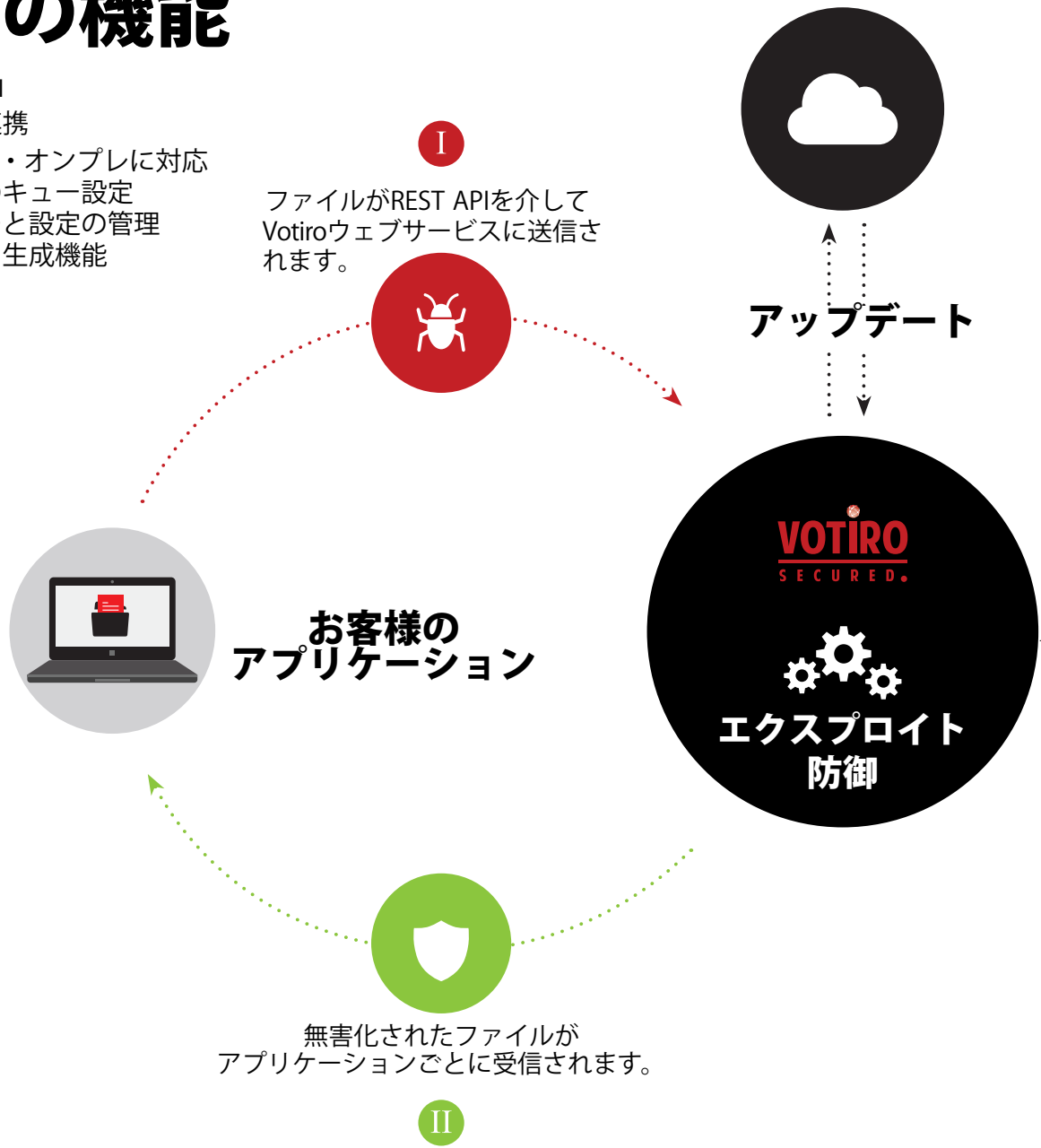
CDR：Content Disarm and Reconstruction
（コンテンツ無害化と再構築）

Votiroが提供する特許取得済みの高度なCDR（コンテンツ無害化と再構築）技術でセキュリティソリューションをパワーアップします。

ゼロレイテンシーと拡張性のあるデプロイメントを特徴とするVotiro技術はいかなる規模のアプリケーションにも対応します。

APIの機能

> RESTful API
> 簡単な連携
>クラウド・オンプレに対応
>無害化のキュー設定
>ポリシーと設定の管理
>レポート生成機能



高度なCDR技術：

1

複数のアンチウイルス
エンジンを使って
ファイルをスキャンします

2

実際のファイルタイプ
を特定します

3

アクティブコンテンツ
を無害化します

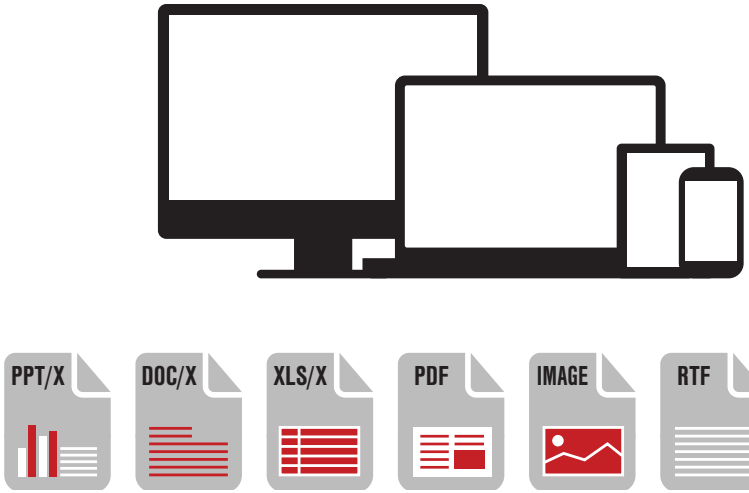
Votiro APIの利点

- アクティブコンテンツのCDR技術（特許取得済）
- ドキュメントに埋め込まれた悪意あるコードに対する100%の保護対策
- ファイルタイプとその機能性の維持
- ゼロレイテンシー
- 誤検知ゼロ
- 高度な脅威からの保護
- CISOのニーズに適したデザイン
- 柔軟な設置オプション（クラウドベースとオンプレミス）

Votiroが提供する高度なCDR技術とは？

Votiroが提供する高度なCDR技術とは、サイバー攻撃、高度なAPT攻撃、また特にスピアフィッシングによって最も頻繁に悪用されるファイル形式を対象にしている、プロアクティブかつシグネチャレス型の保護技術のことです。本技術は、エクスプロイトが対象の組織のシステムに影響を及ぼす前に無害化を行います。

Votiroの技術は、Microsoft® Office ファイル、Adobe® PDFファイル、画像ファイル、アーカイブ、RTFファイルなどを含む様々なファイル形式のモバイル版とデスクトップ版を保護します。



Votiroによって無害化されたファイルは安全であり、機能性も保たれます

Votiroが提供する高度なコンテンツ無害化と再構築のAPIは、Votiroの革新的なセキュリティ技術をアプリケーションに簡単に統合することができるので、アプリケーションの機能が強化され、また向上したセキュリティソリューションを利用できるようになります。

Votiro APIによって、全ての脅威が無効になり、ユーザーは完全に無害化されたバージョンのファイルを取得します。また、これらの安全なファイルは本来の機能性も維持されているため、ユーザーはいつも通りに編集することができます。

メール コンテンツ 無害化 ゲートウェイ

Votiroが提供する特許取得済みの
CDR技術を利用

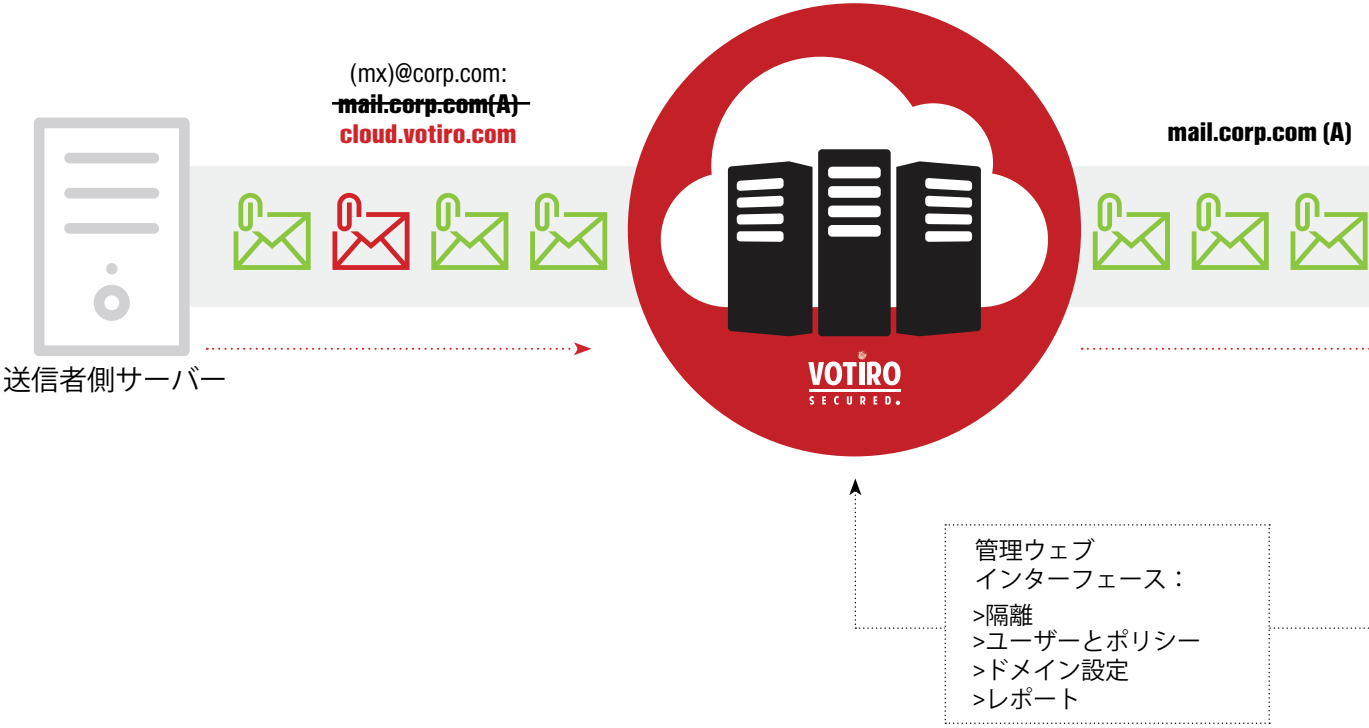
メールコンテンツ無害化ゲートウェイでデータを保護

次の事態を想像してください。ある社員が同僚から送信されたと思ってメールを開きます。そして、突然マルウェアがネットワークに密かに潜り込み、機密データを盗み出そうとします。
サイバー犯罪者が高度な技を使って作られた正当に見えるメールの場合、セキュリティリスクの訓練を受けている受信者でも、思わず添付ファイルを開いてしまう可能性が高いのです。

Votiro™メールコンテンツ無害化ゲートウェイの紹介

Votiroの高度なCDR技術を利用するクラウドベースのVotiroメールコンテンツ無害化ゲートウェイは、受信されるメールに埋め込まれた全ての脅威を無害化することによって、お客様のクレジットカード情報、パスワード、およびその他の機密データの安全性を保護することができます。世界各地の銀行、政府、防衛機関、製薬会社および公益会社に導入されているVotiroの安全なコンテンツ無害化ゲートウェイは実績のある成熟した技術および性能を提供します。

図1 Votiroデータセンター



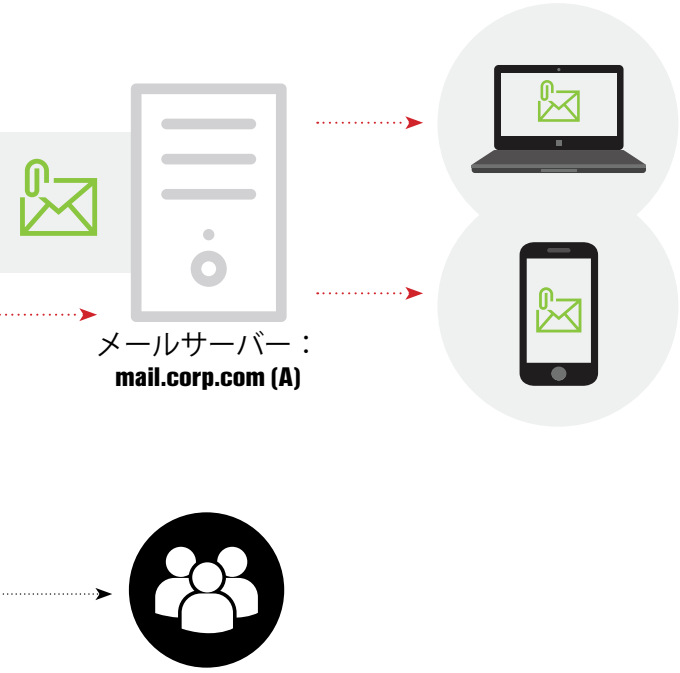
Votiro メール コンテンツ無害化 ゲートウェイの 利点

Votiroが提供する特許取得済みの高度なCDR技術を利用して受信メールを無害化することによって、未知とゼロデイ脅威に対してお客様の組織を保護します。

商用のウィルス対策およびマルウェア対策ソリューションを活用することによって、既知の脅威に対してお客様のネットワークを保護します。

マネージドセキュリティサービスとして提供されるので、追加サーバーの維持、またエンドポイントのインストールにかかる時間および費用の負担軽減に繋がります。

自動で動作するので、社員の監視や組織の保護措置に依存しません。



どうやって動くのか？

お客様の組織に送信されたメールが自動的にVotiroのクラウドベースのメールサーバーに直接届けられます。既知の脅威を検出するためには、Votiroコンテンツ無害化ゲートウェイはメッセージに添付された全てのファイルにアンチウィルス対策を適用します。
未知とゼロデイのエクスプロイトを阻止するためには、添付ファイルから悪意のあるコンテンツを抽出し、そして添付ファイルの本来の機能性を維持しながら無害化します。その後、無害化したメールとその添付ファイルはお客様の組織のメールサーバーに送られます。プロセス全体は通常1秒以内に完了します。
お客様の組織のプライバシーを確保するためには、Votiroは自らのサーバー内に、いかなるメール、添付ファイル（元のバージョン、無害化したバージョン含む）も保存しないことを保証します。

Votiroが提供する高度なCDR技術を利用することによって、Votiroゲートウェイはスピアフィッシングによって最も頻繁的に狙われるファイル形式をサポートします。これらのファイルには、Microsoft® Word、Excel® 、およびPowerPoint®ファイル、またRTF、PDF、画像、およびアーカイブされたファイルなどが含まれます。加えて、本技術は実行ファイルや暗号化ファイルも検出することができ、ブロックすることもできます。Votiro提供のゲートウェイは、Microsoft Office 365®、ホスト内、オンプレミス、Microsoft Exchange、Google Apps、およびその他のメールボックスサービスで動作します。

セットアップと管理

Votiroが提供するメールコンテンツ無害化ゲートウェイのセットアップは、DNSのMXレコードを変更して全てのメールをVotiroクラウドにリダイレクトするだけです。操作が簡単なVotiroのウェブインターフェースでは社員別のファイルスキャンのポリシーを簡単に定義することができます。本サービスはユーザーが定義したポリシーとパラメーターに基づいて受信メールを処理し、そして社員別のサイバー攻撃の報告を表示します。

「組織は少なくとも年4回狙われるのが一般的と思っていたほうがよい。攻撃者は一回だけ成功すればそれで十分だが、一方企業は安全性を確保するためにすべての攻撃を阻止しなければなりません。企業は侵害を必然的（偶然的ではなく）なものとして認識し、発生したらどうすればいいかすでに考慮しておく必要があります。」

—Symantec 2016年インターネットセキュリティ脅威報告

事例紹介
ある銀行の話

背景

新たなセキュリティ脅威の急増に対して自らのメールゲートウェイを保護するためのソリューションを選定するにあたって、ある銀行が2013年に提案依頼を出しました。2014年初頭、銀行は、侵害してくる全ての脅威を検出するために、最も有名なメールリレーサーバーとサンドボックスソリューションを導入しました。銀行はまた、Votiroのメールコンテンツ無害化ゲートウェイソリューションのライセンスを購入しました。

さらに、Votiroゲートウェイを回避した脅威を考慮して念のために二番目のサンドボックスを別のベンダーから導入しました。このサンドボックスは元の電子メール（まだいずれかの保護プロセスにも処理されていない受信メール）の遡及的スキャンを実行するように設定されていました。スキャンはメールの着信数日後、そして数か月後にまた実行して、新たな脅威のシグネチャを確認するようになっていました。

「当社の機密情報の安全性を確保するのは我々の最優先課題となっています。Votiroの高度なCDR技術はその役目を確実に果たしています。」

—大手銀行の最高セキュリティ責任者

脅威と保護対策

2016年、銀行において重大な事件が起きました。

銀行について

200支店、1万1千人の社員、数百万の顧客、世界各地にわたる系列子会社、60億ドルの年収を誇る銀行です。毎日、数千のメールも銀行のネットワークに送られてきます。

02:06:23

侵入

特定のエクスプロイトがメールリレーサーバーを回避しました。これは送信者のIPアドレスとメールアカウントがメールリレーのブラックリストに登録されてなく、また当該の脅威がメールリレーに知られていなかったためでした。

02:06:24

検知試行

このエクスプロイトはサンドボックスを回避するために、サンドボックスでのサービスを監視し、そして特定のサンドボックスベンダーに関するサービスをインターネットで検索しました。

図1 オンプレミス型の脅威無効化

02:08:48

無害化

Votiroが提供する特許取得済みのコンテンツ無害化技術は、未知とゼロデイのエクスプロイトを除去するように設計されているので、エクスプロイトを効果的に無害化することができました。

02:08:50

検証

無害化したメールが分析のために二番目のサンドボックスに送信されました。

02:11:20

配信

全ての脅威が除去された後、メールがユーザーのメールボックスに送信されました。

その後の展開

数日後、オリジナルのメールの遡及的スキャンによって最近のアップデートで追加されたシグネチャにより脅威が検知され、アラートが発行されました。その脅威は、Votiroのソリューションが除去したエクスプロイトのことでした。もし無害化されていなかったら、このエクスプロイトはバックドアを開け、未知のランサムウェアを銀行のネットワークに浸入させていたかもしれません。

「Votiroを選定したのは、そのユニークなコンセプトと、メールチャンネルを介するあらゆるエクスプロイトを阻止できるという実績からでした。 Votiroの技術は実際に我々の期待に応えてくれました。」
—銀行の最高情報セキュリティ責任者

「遡及的なスキャンでアラートが出た時は本当に恐ろしかったです」と銀行のITマネージャーが語ります。「直ちに損害の有無を確認しはじめました。各ネットワークセグメントにおいて同シグネチャに起因するアラートがなかったことを確認するたびにため息をついて安心しました。全てのセグメントをスキャンし、脅威の証拠が見つからなかった時に、脅威のシグネチャの履歴を確認しました。「脅威の形跡はVotiroによる無害化前の段階、つまり元のメッセージにしかありませんでした。そして、元のメッセージをVotiroがゲートウェイソリューションで再び処理してみましたが、驚いたことに、エクスプロイトは完全に無効になってしまったのです！」

結局、Votiroのゲートウェイを回避したエクスプロイトがなかったので、銀行は2番目のサンドボックスのライセンスを更新しなかったということは言うまでもありません。

事例紹介
ランサムウェアに対する保護

Votiro提供の高度なCDRによるランサムウェア攻撃の防止

Bar-Oz保険会社は、日常業務を妨害する複数のランサムウェア攻撃に襲われていました。これらの攻撃は会社全体の財務と評判に重大な損害を与えかねない存在でした。高度なCDR技術を利用するVotiroのメールゲートウェイを設置した後、Bar-Ozは再度ランサムウェア攻撃に襲われることはありませんでした。

ランサムウェアとは何か？

ランサムウェアとは、悪意のあるソフトウェアの一種ですが、有効になると被害者のコンピューターをロックしたり、あるいはコンピューター内のファイルを暗号化することを特徴とします。アクセス権を取り戻すためには、被害者がランサムウェアを注入したハッカーに対して身代金を支払わなければなりません。サイバー犯罪者の中で最も人気のあるランサムウェアの一つは被害者のファイルを暗号化するCryptolockerです。身代金を支払えば、被害者はファイルをロック解除するための復号キーを入手できます。オンラインで利用可能な様々なランサムウェア駆除ツールがありますが、これらは、最新のランサムウェアに対して、ほとんど役に立たないものばかりです。

Votiroが提供する特許取得済みの高度なCDR技術は、ファイル内の悪意のあるコンテンツをプロアクティブに無害化し、そして本来の機能性を維持しながら元のファイルの無害化したバージョン、つまり編集が安全なバージョンを再構築します。

Votiroは、シグネチャに依存せず、また脅威を無害化するためにその脅威を特定する必要がありません。アプリケーション内の脆弱性を悪用するために、ランサムウェア攻撃はファイルのコンテンツを改ざんする必要があります。Votiroが提供する実績のある高度なコンテンツ無害化と再構築技術はいかなるランサムウェア攻撃を無力化します。

特定のユーザーが添付ファイルのある標的型攻撃メールを受信します。

ユーザーは添付ファイルを開いて、エクスプロイトを引き起こします。ランサムウェアがダウンロードされます。

ランサムウェアはコンピューター内の全てのファイルを暗号化して、アクセス不可能にします。

ユーザーは身代金を要求するメッセージを受信します。

ユーザは身代金を支払って復号キーを受け取るか、身代金を支払わずファイルを使用できないままやり過ごすか、どちらか一方を選択しなければなりません。

ランサムウェアによる被害

Cyber Threat Allianceの2015年の報告によると、CryptoWallによるランサムウェアは2015年に3.25億ドルの被害を起こしたそうです。

ランサムウェアに起因する損失はただランサム自体にとどまりません。2016年に発生した事件では、Hollywood Presbyterian Medical Centerが自らのファイルへのアクセス権を取り戻すために、1万7千ドルの身代金をビットコインで支払うことを余儀なくされました。しかし、このような事件がもたらすその他の費用は身代金をはるかに超える場合があります。InfoSec InstituteのBrad Brooks氏によると、「コンピューターフォレンジック調査の費用は、必要なシステムの数と種類、および証拠の回復プロセスの複雑性によって、幅広く変動します（時給100ドル～600ドル）。」ということです[1]。さらに、システムのダウンタイムに起因する財務的損害、組織の評判の損害に起因する既存・潜在的顧客の損失、およびシステムの脆弱性を改善するのに必要な支出も加わります。結局、ランサムウェア攻撃は2016年に約10億ドルの被害を引き起こすと見込まれています。

ランサムウェアに感染する経路は？

ランサムウェアに感染する最も一般的な経路は標的型メール攻撃です。具体的にいうとスピアフィッシングです。メッセージは信頼性の高い送信元からのものに見せかけ、Microsoft Office、Adobe PDFなどのファイルが添付されます。ユーザーが添付ファイルを開き、エクスプロイトを実行され、そしてランサムウェアがコンピューターにインストールされます。

社員教育

ある保険会社の社員はサイバーセキュリティに関する訓練セッションを数回受け、サイバー攻撃を検出し、防止する方法について何回も指示を受けているにも関わらず、エクスプロイトが含まれている可能性のある添付ファイルを開きました。

[1] http://resources.infosecinstitute.com/computer-forensics-investigation-case-study/

攻撃への対応

2週間にわたって、この会社はランサムウェアを含むMicrosoft Wordの添付ファイルが付いたメールメッセージを多数受信しました。

Votiroの特許取得済みの高度なコンテンツ無害化と再構築（CDR）技術を利用するメールコンテンツ無害化ゲートウェイを導入しました。ゲートウェイは、全ての受信トラフィックを無害化することによってランサムウェアを阻止することができ、本来の機能性を維持しながら編集ができる安全なファイルを提供しました。無害化プロセス全体は1秒以内に完了し、企業活動のいかなる側面も妨害しませんでした。

悪意のあるメールはまだ送られてきます。しかし、Votiro独自の技術はこれらのファイルを無害化し、攻撃を効果的に防御しています。

「我々は1日につき何千ものメールを受信しているので、素早く動作し、日常業務を妨害しないソリューションを探していました。クラウドベースサービスとして、Votiroが提供するゲートウェイはデプロイメントが簡単で、すぐに動作しはじめました。悪意のあるメールはまだ受信しているが、今ではVotiroに無害化されるので、安心です。」

— Amir Bar-Oz最高経営責任者（CEO）

Bar-Oz保険会社について

Bar-Ozは住宅保険を専門とする、長年の実績をもつ企業です。Bar-Ozは毎日膨大なメールとファイルを受信するため、機密データが常にサイバー攻撃にさらされる可能性がありました。

結論

Votiroが提供する特許取得済みの高度なCDR（コンテンツ無害化と再構築）技術は、現在のエクスプロイトと未知およびゼロデイの脅威に対して防御するための最適な方法となります。 Votiroのソリューションはサイバーセキュリティの脅威を事前に特定できなくても、無害化できます。初回のネットワークへの侵入行為で脅威を駆除することによって、ゼロデイエクスプロイトと高度なAPT攻撃に対して真なる保護方法を提供します。

脅威の無害化は、ファイルの構造とメタデータに細かい変更加えることにより実現されます。ユーザーの目に見えない所で行われるこの変更はファイルの機能性に影響を及ぼすことなく、そのファイルから悪意のあるコードが実行される可能性を確実になくします。一般的なファイルの場合、脅威の無害化は1秒未満で完了します。Votiro独自の保護方法は一般的な方法より勝っており、脅威を事前に検出することなく全てのファイルを処理することによって、ゼロデイ脅威が対象の組織に浸入する前に駆除します。Votiroが提供する高度なコンテンツ無害化と再構築プロセスは実績のある成熟した技術および性能を実現して提供します。

以下のウェブサイトでオンラインでもが体験できます。
(https://www.votiro.com/demo-jp)

Votiroが提供する高度なCDR術はユーザー体験に変更を加えることなくファイルから全ての脅威を無害化します。ファイルは本来の機能性とコンテンツで再構築されます。

標的型攻撃に対する、
将来性のある保護

ヨーロッパ、中東、アフリカ

126 Yigal Alon St.
Tel Aviv 67443（イスラエル）
Tel：+972 73 737 4102
E-mail：sales-emea@votiro.com

北米および南米

640 W. California Ave., 2nd Floor Sunnyvale, CA
94086（アメリカ合衆国）
Tel：+1 415 231 3725
E-mail：sales-us@votiro.com

アジア太平洋地域

435 Orchard Road
238877（シンガポール）
Tel：+65 3159 1224
E-mail：sales-apac@votiro.com

VOTIRO
SECURED.
www.votiro.com

日本
株式会社アズジェント
東京都中央区明石町6-4
Tel：03-6853-7402
E-mail：info@asgent.co.jp

One Step Ahead of The Game
Asgent
アズジェント
www.asgent.co.jp