攻撃の痕跡
VS
侵害の痕跡

この2つの
違いとは

Indicator of Attack

Indicator of Compromise

重要なデータの保護を担う組織にとって、脅威はかつてないほど高度化しています。実際、最近のニュースに裏付けられているように、高いスキルを持った執拗な敵による標的型攻撃の影響をまったく受けない企業や機関は存在しません。

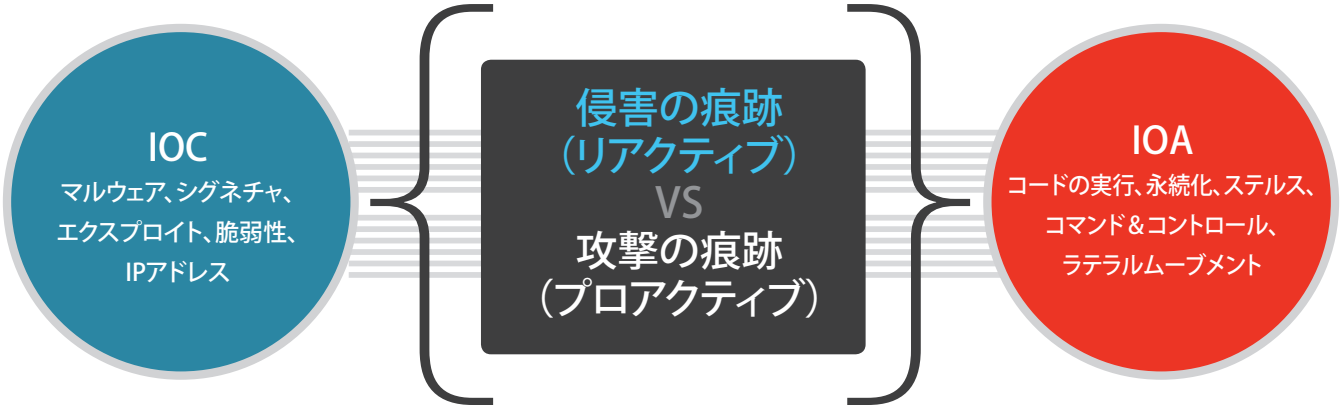
世界中で過去に例を見ないほど、備えを十分行なっていた大規模組織に対する標的型攻撃が成し遂げられていることから、多くのセキュリティ担当エグゼクティブは、従来の多層防御による標的型攻撃対策を疑問視しています。同時に、多くの組織が、組織を弱体化させるサイバー攻撃を受ける前に、セキュリティのベストプラクティスの見直し、改定を始めています。

CrowdStrikeのセキュリティエキスパート、脅威ハンティング担当、インテリジェンスアナリスト、インシデント対応担当は、CrowdStrikeの次世代エンドポイント保護プラットフォームを存分に利用して、大規模組織に対する巧妙な攻撃を検知、防御してきました。この経験に基づき蓄積した知識をもとに、企業の情報セキュリティ手順をプロアクティブに強化し、よくあるミスや落とし穴を回避する有用な情報を提供しています。

根本的な違い

IOCとIOA

以下の図からわかるように、IOCはリアクティブ（事後対応的）な性質を持ちます。マルウェア、シグネチャ、エクスプロイト、脆弱性、IPアドレスの存在は、侵害が発生したときに残される一般的な証拠です。これに対して、IOAはプロアクティブ（事前予防的）な性質を持ち、防御側が探している攻撃が水面下で行われていることを示す初期のサイン、例えばコードの実行、永続化、ステルス、コマンド＆コントロール、ネットワーク内のラテラルムーブメントなどに当たります。2つの違いは、犯罪が起きた後で事件現場に到着して、残された証拠を基に犯罪を再現しようとするか、攻撃が差し迫っているかすでに進行中であることを示すわずかなサイン（痕跡）を注意深く見るかの違いです。



現実世界の犯罪にたとえると

銀行に強盗が入ったとき、警察は犯罪が起きた後に到着し、証拠の収集を始めます。たとえば、銀行強盗が紫のワゴン車に乗り、ボルチモア・レイブンズの帽子をかぶり、液体窒素を使って金庫に押し入ったことが、防犯カメラから判明するとします。これらの証拠のそれぞれが、銀行が侵害されたことを示す痕跡です。現金は失われましたが、証拠の跡を辿ることで最終的に犯罪者に辿り着く可能性もあります。ただしそれは、犯罪者が手口を変えなければの話です。同じ人が次の犯罪で赤い車に乗り、カウボーイハットをかぶり、バールを使って金庫に近づいたらどうなるでしょうか。そうなれば、また強盗に成功してしまいます。それは、監視チームが古い分析結果によって示された侵害の痕跡（IOC）に頼っていたからです。

しかし、調査チームが攻撃の痕跡（IOA）を中心としたアプローチを利用していた場合、その結果は大きく変わるでしょう。たとえば、賢い泥棒はまず銀行の「事前調査」を行い、偵察に行って、防御面で脆弱な場所を把握します。犯罪を行うための最善の日時と作戦を決定したら、銀行への侵入を開始します。セキュリティシステムを停止させて金庫に向かって進み、暗証番号の解除を試みます。もし、銀行の警備を担当するチームが、強盗の成功につながるような振る舞いを検知できたなら（言い換えれば、攻撃の痕跡（IOA）を識別できたなら）、銀行の施設内から現金を少しでも盗み出される前にその試みを阻止できたでしょう。

情報漏洩のケースでは、MD5ハッシュ、C2ドメイン、ハードコーディングされたIPアドレス、レジストリキー、ファイル名など、残されるさまざまな電子的証拠がIOCに含まれます。ただし、これらのIOCは常に変わるために、保護に対してプロアクティブなアプローチをとることは不可能です。IOCは悪党を追跡するためのリアクティブな手法であるため、IOCを見つける頃には、すでに侵害を受けている可能性が高いと言えます。

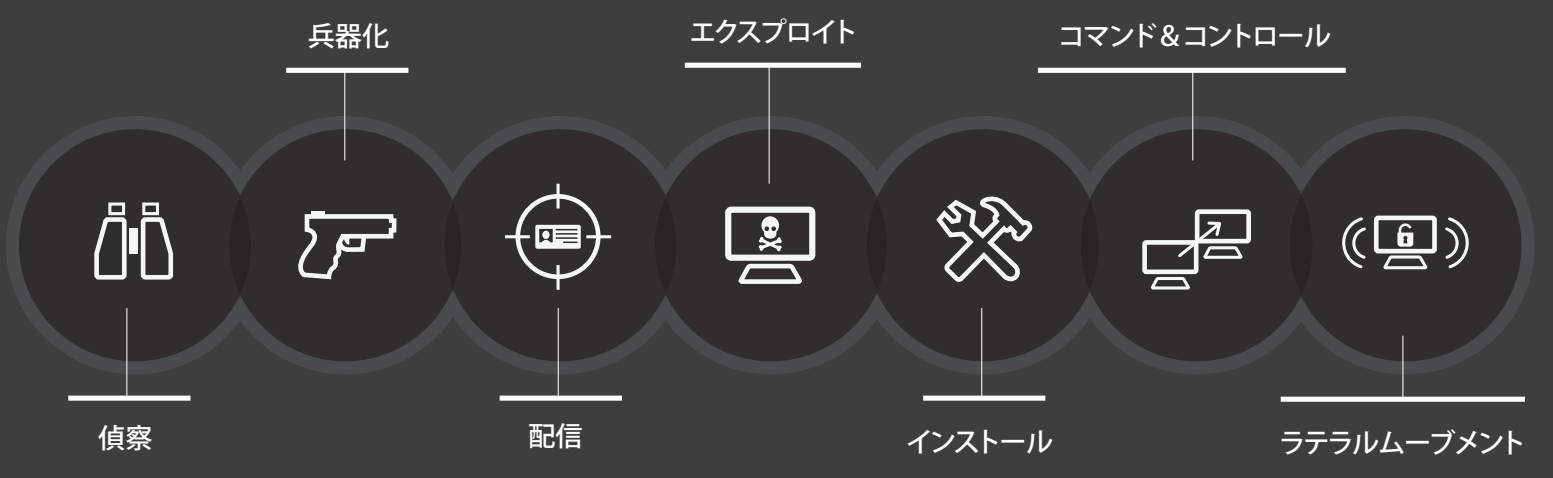
これに対して、サイバー空間におけるIOAは、敵が攻撃を達成するために実行しなければならない一連の行動を表します。執拗な敵による最も一般的かつ最も成功率の高い戦術、すなわちスピアフィッシング攻撃を分解して考えれば、このポイントが分かりやすくなるでしょう。

フィッシングメールを成功させるには、標的にマシンを感染させるリンクをクリックさせるか文書を開くよう促す必要があります。侵入に成功したら、攻撃者は気づかれることなく別のプロセスを実行し、メモリ内またはディスク上に潜伏、システムが再起動されても持続できるようにします。次に、コマンド＆コントロールサイトと通信して、自らのハンドラに対して、追加の命令待ち状態であることを通知します。

IOAはこれらのステップの実行に関係するもので、敵の目的と達成しようとしている成果を暴きます。IOAは、犯罪者が目標達成のために使う具体的なツールには注目しません。そのため、犯罪者が目標達成に向けて採用する、変わり続ける戦術に、より柔軟に対応できます。

これらの実行ポイントを監視し、痕跡を収集して分析することにより、犯罪者がネットワークへのアクセス権を手に入れる方法を突き止めることができ、その目的を推測することもできます。具体的なツールやマルウェアに関する高度な知識（IOC）は、進行中の攻撃を阻止するためには不要です。事実、IOAによって、マルウェアが使われない攻撃も検知できます。

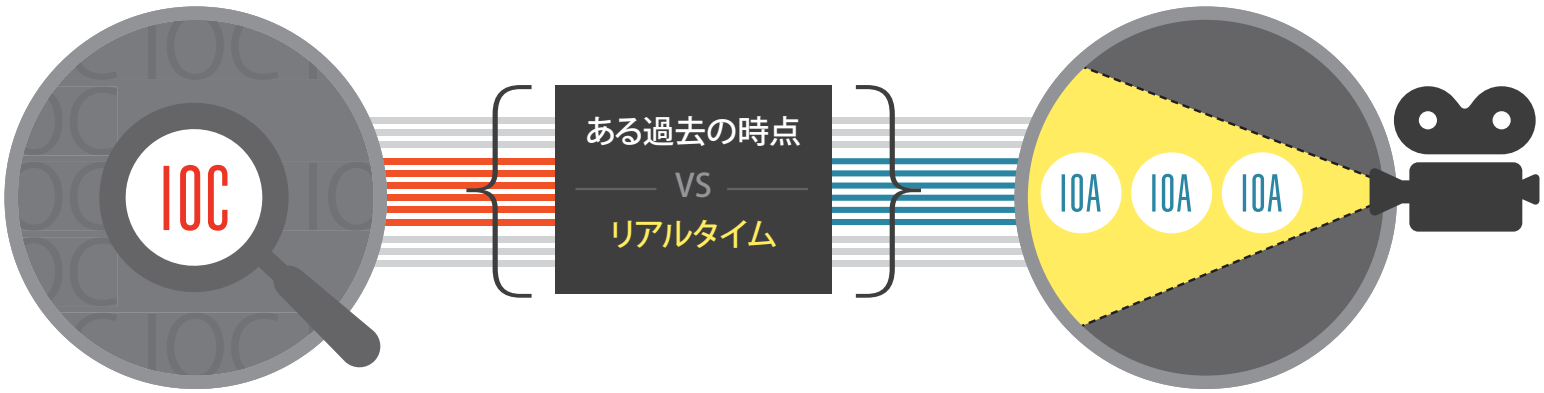
攻撃の痕跡



IOAによって
リアルタイムの記録と
可視化が可能に

IOAアプローチの副次的効果として、ネットワークの状況をリアルタイムで正確に収集し、分析できるようになります。実行中の振る舞いを監視するという性質は、まさにビデオカメラで監視し、環境内のフライトレコーダーにアクセスするようなものです。

すべてのアクションを発生中に記録することで、攻撃者がどのように環境に侵入し、ファイルにアクセスして、パスワードをダンプし、ネットワーク内でラテラルムーブメントを行い、最終的にデータを盗み出したか（攻撃が成し遂げられてしまった場合）をIOAは正確に示します。



現実世界の攻撃例

既存の防御体制をどう逃れているか

CrowdStrikeのインテリジェンスチームがまとめた、中国人の攻撃者による活動の例を以下に示します。以下の例では、ある攻撃者の活動が既存の防御を逃れる手法が明確にわかります。

この攻撃者は以下のノウハウを活用しています。
{1} インメモリのマルウェア – ディスクには書き込まれない
{2} 一般に知られた、無難なITツール – Windows PowerShellおよびコマンドラインのコード
{3} 痕跡を残さないため、自身でのログクリーンアップ

このノウハウを念頭に入れ、エンドポイントソリューションが直面する課題を詳しく見ていきましょう。

アンチウイルス – マルウェアがディスクに書き込まれないため、オンデマンドスキャンを行うほとんどのアンチウイルスソリューションはアラートを発しません。オンデマンドスキャンは、ファイルへの書き込みまたはアクセスがあったときのみ起動します。また、積極的に対応する組織でも、そのほとんどは、エンドユーザーへのパフォーマンス面の影響を考慮して、フルスキャンを週1回しか実行しません。仮にこのフルスキャンを実行しており、かつアンチウイルスベンダーによって更新済みのシグネチャを使いメモリをスキャンすることができれば、このマルウェアの活動についてアラートを発することができるでしょう。

アンチウイルス2.0ソリューション – 機械学習やその他の手法を利用して、ファイルが良質か悪質かを判断するソリューションです。PowerShellは正規のWindowsシステム管理ツールであり、悪質として識別されません（また、識別されるべきではありません）。そのため、アンチウイルス2.0ソリューションでも、この振る舞いについて顧客にアラートを発することはできません。

ホワイトリスト – Powershell.exeは既知のITツールであり、ほとんどの環境で実行が許可されるはずであるため、ホワイトリストソリューションが配備されていても、回避されます。

IOCスキャンソリューション – この攻撃はディスクへの書き込みを一切行わず、目的の仕事を果たした後にクリーンアップされるため、検索できるものではありません。IOCは既知のアーティファクトであり、このケースの場合は、検知されるアーティファクトは残りません。さらに、ほとんどのフォレンジック駆動型ソリューションでは、標的となったシステムの定期的な「スイープ」が必要です。このスイープとスイープの合間に攻撃された場合、その攻撃は検知されないままです。

次世代保護への移行

CrowdStrikeでは、お客様が単なるマルウェアの問題にとどまらない極めて多くの問題を抱えていることを認識しています。実際、各種調査によれば、データ侵害インシデントの60%で、マルウェアはまったく使われていません。しかし、真の意味での次世代エンドポイント保護技術を利用すれば、攻撃の痕跡（IOA）をリアルタイムで検知できます。

この革新的なアプローチによって、企業のセキュリティ専門スタッフは、巧妙な攻撃者が利用する戦術、手法、手順をすぐに理解することができます。そうすることで、敵は誰なのか、何にアクセスを試みているのか、その理由は何なのかを究明できます。

これらの情報を基に、攻撃を最も早い段階でブロックするための明確な行動指針を立てることができます。

CROWDSTRIKEについて

CrowdStrikeは、世界最大規模の先進性の高い企業および政府機関に対して次世代エンドポイント保護、脅威インテリジェンス、24時間の監視とインシデント対応サービスを提供しています。100% SaaSベースのCrowdStrike Falconプラットフォームは、極めて包括的なエンドポイント保護技術を提供しており、このプラットフォームを利用すれば、リアルタイムで検知、防御、記録、検索を行って、ダメージを受ける前に標的型攻撃を阻止できます。

詳細は、 crowdstrike.com/sites/jp/ をご覧ください。
CrowdStrike Japan 株式会社
〒100-0005
東京都千代田区丸の内 1 丁目 6-5