SANS

SANS Spotlight

ハンターの思考で取り組む: 脅威ハンティング・プログラムの実装

執筆者 **Matt Bromiley**

2019年4月

スポンサー:

IBM

はじめに

企業環境を守ることは、時として困難な戦いのように感じるかもしれません。情報セキュリティー・チームは、警報が鳴り止まず、攻撃者が常に成功するような堂々巡りから抜けられなくなることがしばしばあります。

残念なことに、このパターンは企業が受け身モードにある症状です。このモードでは、セキュリティーおよび対応チームは、それが社内または社外であろうと、次にどこへ行くかを警報が指示してくれるのを待っています。あるとしても、何かさらに悪いことになる前に *脅威を見つける詳細情報の* 指示はほとんどありません。

真の意味で攻撃者よりも先を行くには、企業はプロアクティブに考え始めなければなりません。言い換えれば、脅威ハンターのように考えるのです。確かに「脅威ハンティング」という言葉は、新しいものではありません。実際、多くの成熟した企業には様々な脅威ハンティング・プログラムがあり、別のチームや、多くの場合、セキュリティー・オペレーション・センター (SOC) やインシデント対応チームと統合されています。

多くの組織で脅威ハンティングという言葉を聞くようになりましたが、しばしば「悪者を見つけに行く」というような間違った解釈がされています。悪者を見つけることは、言うのは簡単です。攻撃者が白旗を振って、すべての手順を教えてくれるわけではないのですから！代わりに、脅威ハンティングは成功するために長期的な視野を必要とする複雑な仕事です。

脅威ハンティング(Threat hunting)は、言うのは簡単ですが、実行には難しいものがあります。チームはプロアクティブに考える必要があり、不必要な反応にとらわれてはいけません。しかし脅威ハンティングがうまくいけば、調査モードに迅速に移行できる準備が整います！

脅威ハンティングの成功要因は、攻撃技術の知識に存在するわけではありません。それは可視性と状況認識に存在するのです。成功する脅威ハンティング・プログラムの真の目的は、2段階であるべきです。

- 最初の目標は、環境内のこれまで知られていない、または進行中（つまりまだ改善されていない）の脅威を特定することです。
- 企業にとって真の利益となる2つ目の目標は、企業の技術的な状況を深く理解することです。

本稿では、この2つの目標の間のギャップを埋めることに焦点を置き、脅威ハンティングとは何か、なぜ実施するのか、そしてその方法について掘り下げます。みなさんの企業環境にも適用して、ハント・チームを新しく構築したり、既存チームを磨き上げるのに役立つテクニックを検証していきます。攻撃者がどのように攻撃するのかを理解することだけでなく、どのようにその手口が特定できるか、環境内でどのように改善できるのかを知ることも重要です。

脅威ハンティングの重要性

チームに思い切って「ハンティング開始！」と指示して始める前に、ハント・チームの目標と目的を定めることが重要です。先に述べたように、どのようなハンティング・プログラムにも、主に2つの目標があるべきです。1) 攻撃者による影響を限定するために、プロアクティブに脅威を探すこと、そして 2) 環境へのより深い理解を得ることです。これから、それぞれについて詳細を見ていきます。

目的を持ったハンティング

すでに述べたように、最初の、そして最も明確な脅威ハンティング・チームの目標は、環境に対する未知の攻撃または脅威を特定することであるべきです。攻撃者が環境内に踏み台を持っている可能性もよくありますが、セキュリティー・チームが対応するのに慣れているような警報を作動させることはありません。さらに悪いことに、攻撃者は見えない領域にいるので、適切な時に適切な場所にいるだけで、無意識のうちに検知をかいくぐっています。

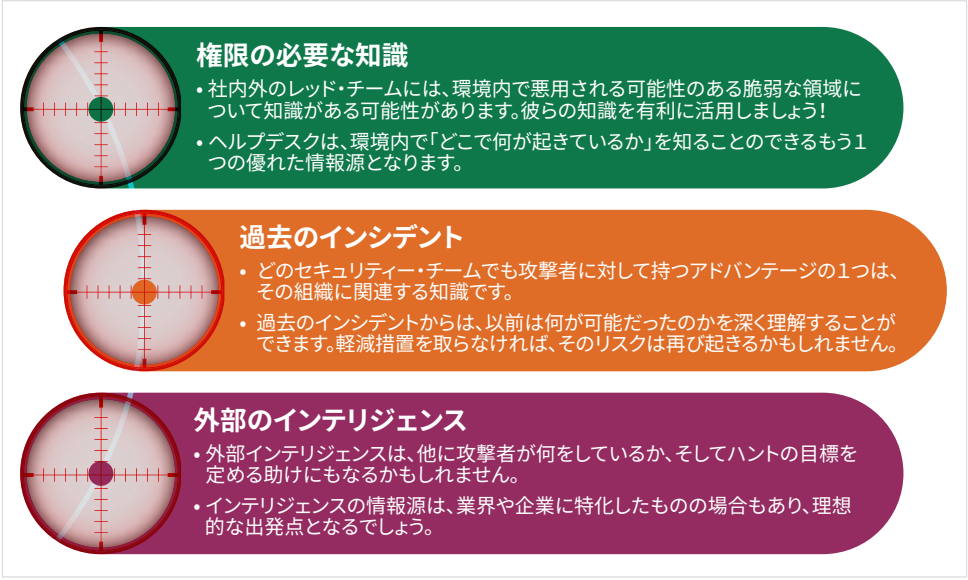

図1：攻撃者による活動の情報源と利用方法

目的のあるハンティングは、様々な攻撃者のテクニックを知り、これを自社環境にいかに適用するかにかかっています。図1 は、攻撃者の活動の情報源と、自社環境にどのように適用できるかを示しています。

脅威ハンティングの実施中に、ハント・チームは過去に特定された攻撃や侵害で、クリアにしたものまたはまだアクティブな残骸を発見することもあるかもしれません。これらは素晴らしいチェックポイントであり、インシデント対応や改善（システム・リイメージング、マルウェアの排除や遮断）の後半の段階が効果的に行われたことを検証するのに利用すべきです。もちろん、対応済みインシデントでまだアクティブなものをハント・チームが見つけることを望んではいるわけではありません！

ハント・チームが過去の攻撃やインシデントに出くわすことも稀ではありません。悪意のある行為を見つけることができる、すばらしいチェックポイントになります。それらを活用して成功へのマイルストーンにしましょう！

明瞭なハンティング

第二に、そして同様に重要なのは、どのようなハント活動の目的も、ハント・チームが入り込む環境の深い理解を得ることでなくてはなりません。攻撃者の活動と特定するため（私たちの第一の目標）、チームは何が利用できるのかを探索する必要があります。脅威ハンティングは、絶対的な可視性があれば簡単です。これがなければ、チームは特定不可能なことを担当していることになるでしょう。

企業が脅威ハンティング・プログラムを実装する最大の理由は、自分たちの知らないことを明らかにすることです。ハンティングでは常に攻撃者を見つけるわけではなく、認識の改善が必要な領域を常に見つけていくことであるべきです。

図 2に示されている、シンプルなスピアフィッシュとマッルウェア投下の例を考えてください。

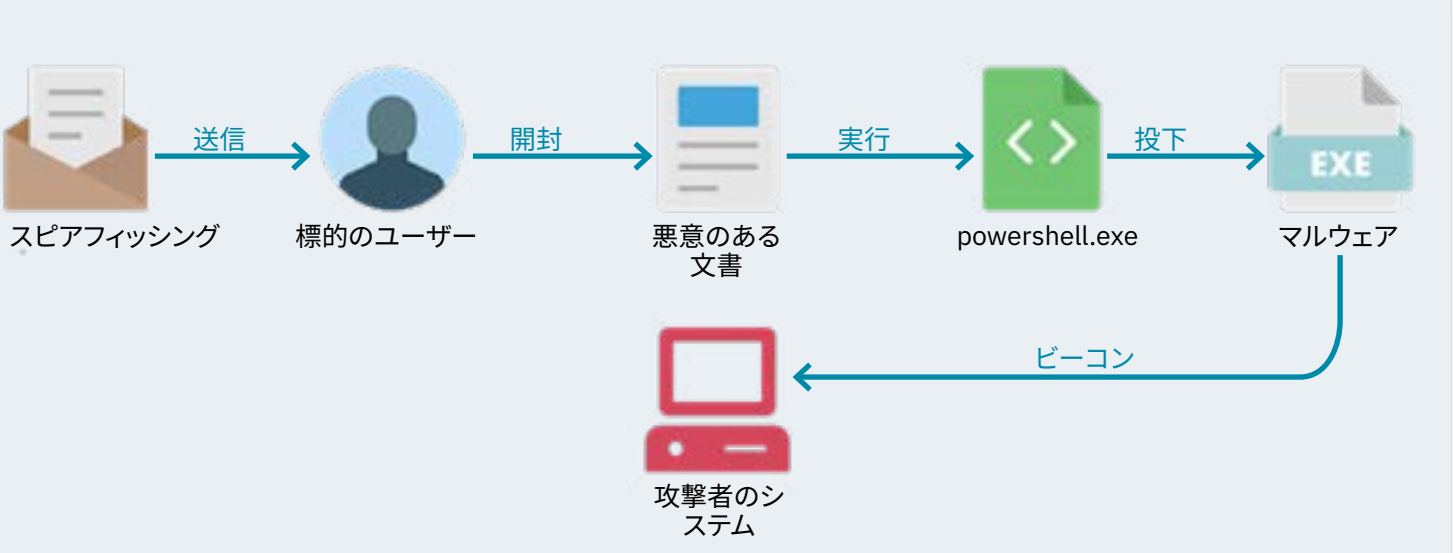

図2：標的型フィッシングと悪意のある攻撃の実行例

図 2では、ユーザーは悪意のあるメールを受け取り、これを開封すると、システムに追加のマルウェアを投下するPowerShellwコードを実行します。このマルウェアは実行後、攻撃者のところへ戻って感染を伝えます。この例から、数多くの優れた脅威ハンティングの手がかりを引き出すことができます。

- 大量のスピアフィッシングを受け取るユーザーについては、潜在的な攻撃キャンペーンを特定するために隔離し、電子メールを遮断します
- 悪意のあるまたは通常と異なる文書名や場所
- 文書作成プログラム（Microsoft® Wordなど）がpowershell.exeなどのコマンドライン・ツールを実行します
- powershell.exe は疑わしいプロセスをダウンロードまたは生み出します
- 疑わしいプロセスが未知または疑わしいネットワークに呼び出しを実施します

おそらく、これ以上のことも思いつくことでしょう！

繰り返しになりますが、我々は「言うは易し」の脅威ハンティングの世界にいます。上記のポイントは素晴らしいハンティングの出発点となり、これらも可視性にすべて依存しています。ハンティングの初期段階では、チームはそれが何をするか、可視化できていないことなどにすぐに気がつくでしょう。ハント・チームは、見えないものを見つけるように依頼されたら、直ちに壁にぶち当たるでしょう！

チームがこれらの障害物に当たったら、2つの行動が推奨されます

1) 企業は、ハント・チームが特定した可視性におけるギャップが、実行中のセキュリティー・プログラムの根本的原因であり、それらを増加させるものなのかを見極める必要があります。例えば、図 2では、親と子のプロセスの組み合わせに強く依存しています。このデータに対する洞察を得るためには、複数の方法があります。

2) 初期のハントでは、可視性が増加したら立ち戻り、修正またはハンティングを再実行することを検討しながら、企業が見えるものをうまく構成して進める必要があります。

ハンティングを成功させるためのテクニック

前節でお話ししたことを考えると、ハンティングが非常に環境に特定したものであることは驚きではありません。ほぼどんな環境にも適用できるテクニックもあります。例えば、特定の実行可能チェーンやサービスを侵害する攻撃者の技術は、環境にかかわらず同じに見えます。しかし、攻撃者が特定のテクニックに向かわせるのは環境の変動要素であり、間違いなく悪を見つけることが簡単になります。図 3 には、コアとなる脅威ハンティングのテクニックが示されています。

図3: 脅威ハンティングのコア・テクニック

自社のベースラインを知ることが強みに

前節で、可視性の必要性と重要性について示しましたが、チームが可視性を得ても、作業はまだ半分しか終わっていません。次のステップは、自社内での「通常状態」とはどのようなものであるかを理解することです。これは、ベースラインと言われるますが、ハント・チームが実施する中でも重要なステップの1つと言えます。英語で「needle in a haystack」と言うように、藁の中に落ちた針のように見つかる望みのないものを探すのは決して楽しいことではありませんが、二桁のパーセンテージで邪魔な藁を取り除くことができれば、針もすぐにに見えるようになるかもしれません。

ベースライン策定の質問項目

ベースラインの策定が、手のかかるタスクであることは間違いありません。費やす時間を最小限に抑えられるように、ベースライン分析と攻撃者のテクニック（前述）を組み合わせます。例えば、以下の質問を考えてみましょう:

- 環境内ではPowerShellはどのくらい一般的ですか？
- 普及している場合、システム管理者の通常の活動はどのようなものですか？
- PowerShellの活動は、通常どこからくるか、そしてどのユーザー・アカウントで通常実行されているでしょうか？

PowerShellのすべての *ベースラン策定をする必要は* ありません。代わりに、予期しない外れ値を探すか、または攻撃者に特有のコマンド構造を見つけてください。

自社環境のベースラインを理解しておくことは、手間のかかる作業かもしれません。しかし、自社環境にどの程度ノイズがあるのか、あるいは静かなのかを知っておくと、異常を見つけることは非常に簡単になります。

攻撃に特化したハント

ベースラインの策定がハント・チームが環境を理解する助けとなる一方で、攻撃に特化したハントは悪意のある活動の追跡をスピードアップし、勝利を得るのを早められるでしょう。攻撃に特化したハントには、通常特定の脅威の実行者もしくは脅威を調査し、そして特有の痕跡からハントをモデル化することが含まれます。前節で、スピアフィッシングについて簡単に説明しましたが、これは、ほぼ真実と言える発見をするための優れた出発点を与えてくれます。

しかし注意が必要です。攻撃に特化したハントは、偽陽性を出すこともしばしばあります。例えば、貴社でどれくらいのBase64-エンコード PowerShell が見つかると思いますか？利用中のセキュリティー・ツールとシステム管理者の行動によって、考えているよりも多くが見つかるかもしれません。従って、ベースライン策定と攻撃に特定したハントの組み合わせは、良い結果を生み出すことがよくあります。

ハントには時間制限がある

ハントチームにとってもう1つの重要な考慮点は、これはいつでもですが、時間制限があるということです。ベースラインの観点からは、一度十分なベースライン条件を確立したら、定期的にそれを評価することを忘れないでください。IT管理もしくはエンドポイント・セキュリティーなどの、新しいソフトウェアの実装によって、偽陽性のデータをより多く吐き出すような不必要なトラフィックを生じさせないようにします。新しいソフトウェアが環境に導入された場合、調整する必要があります。

攻撃者の観点から、攻撃者は必要とあらば、すぐにそのテクニックを変えるということを忘れないでください。昨日「最新鋭」の攻撃であったものも、明日には古くなっているかもしれず、攻撃者は何か新しいものに移行したかもしれません。その場の事態に対応した、脅威インテリジェンスに基づいたハントは、時間の経過とともに検証されるべきです。しかし、攻撃者はテクニックを復活させることもあることを忘れないでください。ですから、必要に応じて一度そのハントを保留しておきますが、古いテクニックの復活に気づいたら、再びハントできる準備をしておいてください。

あなたは一人ではありません

脅威ハンティングの時、アナリストやチームの多くが、データの海に乗り出して、たった一雫のマルウェアを見つけようとしていると感じるかもしれません。このような場合には、救助艇を呼びましょう！脅威ハントは、サードパーティーの情報源によって容易に充実させることができ、偽陽性を除外して、興味深い手がかりに集中できることを忘れないでください。サードパーティーのIPルックアップ、地理的情報、暗号化されたトラフィックのメタデータを用いることで、ネットワーク・データはさらに有効となります。ホスト・ベースのデータも、ログ検出と攻撃者のテクニックを重ね合わせることで、チームの脅威ハントを成功へと導く助けとなります。さらに、可視化が達成された後、サードパーティーのツールで検出を自動化して、ハントを補うこともできるでしょう。

サードパーティーのデータを取得した後には、脅威ハンターはリンク分析ツールを活用して、さらにデータを豊かにすることができます。相互関係を可視化して表示するリンク分析ツールは、社内と社外、ネットワーク・データ・ポイントの間の相互関係を特定するのに助けとなでしょう。リンク分析機能は、サードパーティー・ソースに組み込まれていることもあれば、スタンドアロンのツールとして提供されることもあります。

残念なことに、まだプロアクティブなスタンスに変わる準備ができていないと考えて、脅威ハンティングを始めるときに非常に懸念を示す企業もあります。「攻撃者はすでに内側にいる」という不変の、時として真実ではない信念がありますが、それならば、なぜそれを追い出すように働きかけないのでしょうか？さらに悪いことには、脅威ハンティングを実施すると、「ハンターはこの他に何を見つけるのだろうか？」と恐れを抱く経営者もいます。

このような考え方は、攻撃者が常に自信の点で上を行っているので、決して効果的なセキュリティーには繋がりません。さらに、何を見つけるのか恐れている企業は、セキュリティー・チームの本当の意味での環境の理解と、これをより良く守る機会を奪っています。今こそ、その型を破り、企業の効果的な保護を始める時です。

常に受身的なスタンスから抜け出せない、警告と偽陽性の山を登ることができないという場合には、自社のセキュリティー・プログラムにプロアクティブな脅威ハンティングの実践を加えることを検討する時かもしれません。プロアクティブな脅威ハンティングを活用すれば、チームは自社環境を探索し、悪用される可能性のある弱点を見つけ出すことができるでしょう。さらに、企業はその弱点にパッチを当て、攻撃領域の排除に取り組むことができるようになります。

先に述べた通り、優れたハント・チームは、既知およびモダンな攻撃テクニックを元にして、そのアプローチをモデル化します。しかし、最高の調査であっても何の成果もあげられないことがあります。これはむしろ朗報です。なぜなら特定の攻撃者やテクニックによって脅かされていない可能性を意味するからです！このプロセスを経て、チームが達成したことは第二の目標、つまり、ベースラインを確立して、環境を理解したということです。

最後に、ハントは一時的なものであることを覚えておいてください。攻撃者は、テクニックをリサイクルするかもしれないですし、廃棄するかもしれません。そしてハンティングは決して終わりがあるものではなく、常に学習の実践です。ハントは決して終了しません。ただその時点での結果を得るだけです。セキュリティー・プログラムが拡大し、ハンティング・チームの環境理解が深まれば、企業のセキュリティー対策はより豊かに、より強力になったと感じることでしょう。

さあ、ハンティングを始めましょう！

執筆者について

Matt Bromiley はSANS Digital Forensics and Incident Responseのインストラクターで、「高度デジタル・フォレンジクス、インシデント対応そして脅威ハンティング（FOR508）」そして「高度ネットワーク・フォレンジクス：脅威ハンティング、分析、およびインシデント対応（FOR572）」を教え、GIAC Advisory Boardのメンバーです。彼はまた、インシデント対応ならびにフォレンジック分析企業の主要インシデント対応コンサルタントで、デジタル・フォレンジクス、インシデント対応/トリアージおよびログ分析を組み合わせています。彼には、ディスク、データベース、メモリおよびネットワーク・フォレンジクスそしてネットワーク・セキュリティー監視のスキルがあります。Mattは、多国籍の複合企業から、小さな、地域的な商店までありとあらゆる種類や規模のクライアントと協業してきました。彼は、オープンソース・ツールについて学び、教え、これで作業を行うことに情熱を傾けています。

スポンサー

SANSは、本稿のスポン サーに謝意を表します。

IBM®