IBM X-Force IRIS
Incident Response and Intelligence Services

IBM X-Force IRIS サイバー攻撃準備/実行フレームワーク

詳細はこちら

IBM

概要

IBM® X-Force® Incident Response and Intelligence Services (IRIS) サイバー攻撃準備/実行フレームワークは、サイバー攻撃の分析に使用される業界標準の概念的アプローチに基づくフレームワークです。このような業界標準のアプローチには、**Lockheed Martin 社の Cyber Kill Chain*、Mandiant 社の Attack Lifecycle*、MITRE 社の ATT&CK*** などがありますが、X-Force IRIS サイバー攻撃準備/実行フレームワークでは、現代の代表的な攻撃のロジック・フローが提供されているだけでなく、他のフレームワークには通常含まれていないフェーズも組み込まれています。攻撃者の手口がますます巧妙化する中、新たに追加されたこれらのフェーズは一層重要なものになると X-Force IRIS は確信しています。

補強されているものの中でも特に重要なのが、現代のサイバー・インシデントを理解し、それに対応するために不可欠な X-Force IRIS 攻撃準備フレームワークです。フレームワークには、攻撃の計画やネットワーク上での存在、そして特定の国やグループへの帰属を隠すために攻撃者が採用している戦術の情報も組み込まれています。攻撃者は、サイバー攻撃準備、サイバー攻撃実行のどちらのフレームワークでも、読み解くのが困難な戦術を実行します。これらのフェーズをそれぞれ「*オペレーショナル・セキュリティー*」、「*防御の回避とモニタリング*」と呼びます。

最後に、この X-Force IRIS サイバー攻撃準備/実行フレームワークでは、攻撃のフェーズには、同時発生するもの、逐次的に発生するもの、反復して発生するもの、まったく発生しないものがあることや、攻撃者が活動全体を通して攻撃に絶えず修正を加える可能性があることが織り込まれています。X-Force IRIS フレームワークでは、さまざまなタイプの攻撃者を柔軟に把握し、攻撃者の活動全体に対応するフィードバック・フェーズが用意されています。

これらの主要機能によって、セキュリティーの脅威に対する研究者は、単純なインシデントから巧妙なインシデントに至るまでくまなく分析し、既に把握されている攻撃者のあらゆる戦術についてもより明確に伝えることができるようになります。X-Force IRIS のアプローチは、IBM 内外のセキュリティー・チームがサイバー攻撃の設計と実行を詳しくかつ体系的に理解できるよう支援します。セキュリティー・チームは、このアプローチにより得られた洞察を活用して、自社組織に対して脅威を識別し的確な対応を実施できるようになります。

* 以下を参照してください。Lockheed 社の Cyber Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html、Mandiant 社の攻撃ライフサイクル: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf、MITRE 社の ATT&CK: https://attack.mitre.org/wiki/Main_Page

X-Force IRIS サイバー攻撃準備/実行フレームワーク

図 1 は、X-Force IRIS サイバー攻撃準備/実行フレームワークの概略図です。この図は左から右に見ていきます。攻撃の最初の部分が、*準備フレームワーク* になります。攻撃準備のフェーズを開始した後、攻撃者は攻撃を開始します。この結果に応じて、攻撃者は、サイバー攻撃*実行フレームワーク* のフェーズに進むか、あるいは攻撃を成功させるために必要な要件の見直しを行います。*実行フレームワーク* に入ると、攻撃者は自分の目標の達成に必要なすべてのフェーズ、あるいはその一部の遂行を試みます。

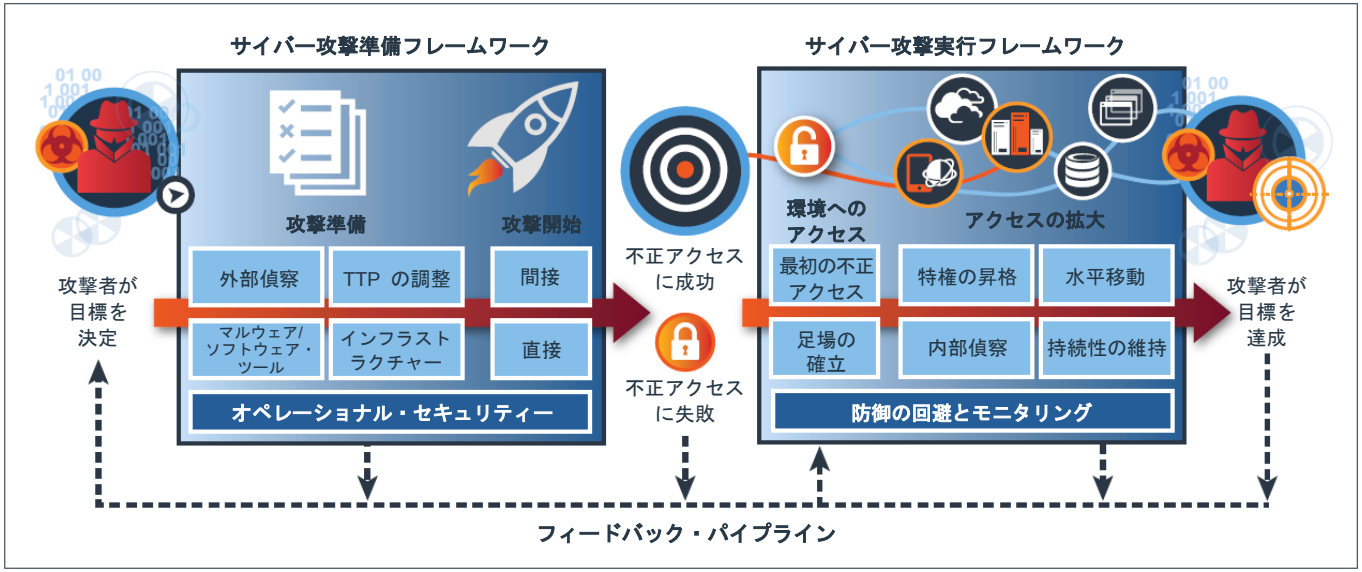


図 1: *X-Force IRIS サイバー攻撃準備/実行フレームワーク*

このフレームワークが対応する主なニーズ

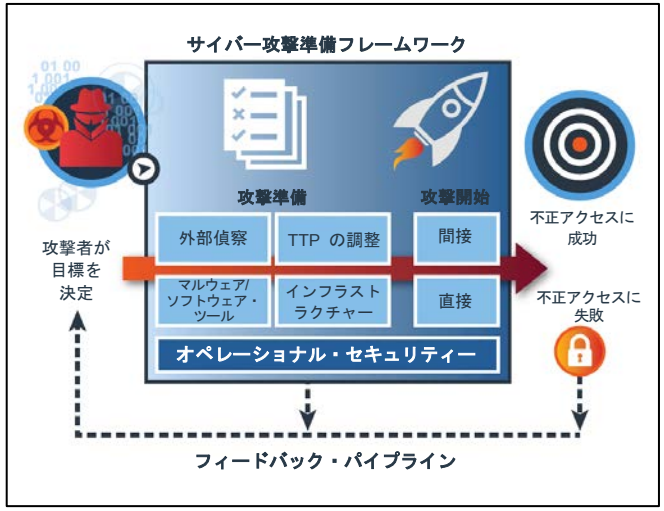
X-Force IRIS サイバー攻撃準備/実行フレームワークによって、脅威データを特徴付けるとともに、脅威インテリジェンスを伝達することができます。これらのフレームワークは、実際の侵入の前とその最中に発生するあらゆる活動を説明するものです。このプロセスで提供されるモデルを使用して、インシデント対応者と脅威インテリジェンス・アナリストは、データの追跡やピア・レビューによる調査、分析結果について、より明確でかつ一貫性が保たれた形で伝達できるようになります。また、お客様も、X-Force IRIS サイバー攻撃準備/実行フレームワークを通じて、自社の業界に関連する多様なサイバー攻撃脅威の状況を簡単かつ効率的に比較できるようになります。

X-Force IRIS サイバー攻撃準備フレームワークは、主として以下のようなニーズに対応します。

- **分析と対応。**サイバー攻撃の計画プロセスを*分析し*、観測された悪質な活動に*対応する* ための、直感的なフレームワークが提供されます。
- **明確なコミュニケーション。**さまざまな知識レベルや観点を持つお客様に対し、脅威の研究者が*分析結果を明確に、しかも一貫性が保たれた形で伝達できる* モデルが提供されます。
- **柔軟性の向上。**既知および未知のサイバー脅威グループが企てる多様な攻撃や攻撃戦術に対応できる*柔軟な* フレームワークが作られます。

X-Force IRIS サイバー攻撃実行フレームワークは、主として以下のようなニーズに対応します。

- **分析。**構造化された形でデータを分類し、*新たなトレンドや予測分析に利用できる* モデルが研究者に提供されます。
- **十分な情報に基づく意思決定。**悪質な活動である検知事例 1 件を深く分析し、その事例を軸として*意思決定と対応計画を迅速に展開するための*、直感的なフレームワークが提供されます。
- **柔軟性の向上。**既知および未知の多様なサイバー脅威グループや攻撃のタイプにも対応できる*柔軟な*フレームワークが提供されます。
- **明確なコミュニケーション。**さまざまな知識レベルや観点を持つお客様に対し、攻撃のコンポーネントを一般化し、さらに詳細なレベルで*伝達するための*、*適応性のあるモデル* が提供されます。



X-Force IRIS サイバー攻撃準備フレームワークを構成するフェーズ

X-Force IRIS サイバー攻撃準備フレームワークには、攻撃者がターゲットを決定し、攻撃の準備を行うために最初に実行するフェーズが含まれています。
これらのフェーズは、攻撃者が最初の足場を築く前に発生します。

X-Force IRIS サイバー攻撃準備フレームワークは、「*目標決定*」フェーズから始まって「*攻撃開始*」フェーズで終わる 8 つのフェーズで構成されています。攻撃者は、攻撃開始後に侵入に成功したかどうかを判定します。この最初のフェーズから最後のフェーズまでの間に、攻撃者には攻撃を設計するための選択肢がいくつか与えられています。また、攻撃者は、*攻撃準備* のフェーズをいくつか組み合わせて使用することもできます。攻撃者は、「*攻撃開始*」フェーズの成否を判定した後、成功の場合は*実行フレームワーク* に進み、失敗の場合は攻撃計画の訂正、変更、取り消しを行います。

攻撃対象者や防御担当者は、準備のフレームワークを構成するフェーズの多くを検知できませんが、場合によっては、攻撃者のオンラインでの足跡を追跡し、攻撃を未然に防止できることもあります。

目標決定

最初の「*目標決定*」フェーズでは、攻撃者はターゲットを特定し、攻撃要件があればそれを決定し、攻撃計画を作成します。さらに、攻撃の全体的な目標を達成するために必要な戦略的および戦術的なターゲットを特定する場合もあります。

戦略的なターゲットとは、その攻撃の全体的な最終目標の達成に必要な情報を保持している相手・宛先です。これは多くの場合、今回狙われているである機密データや財務情報がその業界や会社に存在するかどうかで特定されます。

戦術的なターゲットには、攻撃の完遂に必要なタスクから情報が提供されます。戦術的なターゲットは、攻撃者が戦略的ターゲットにどのように到達して目標を達成するかを管理します。例えば、戦術的ターゲットには、個々のターゲットに入り込むための具体的な感染経路や、攻撃者が目標を達成するための後続のタスクなどが含まれます。

最後に、攻撃者は最初の計画の概要を作成します。これには、必要となる戦術、ツール、さまざまな要件が含まれます。攻撃者がサイバー攻撃準備フレームワークの以後のフェーズに進むにつれて、この最初の計画に変更が加えられることもよくあります。

ネットワークの防御

多くの場合、ネットワークの防御担当者にとってのゴールは、ネットワークを不正アクセスから完全に保護することです。このゴールは常に達成できるとは限りませんが、攻撃計画が準備されている間に、潜在的な攻撃を把握したり、それを阻止したりするチャンスは存在します。例えば、防御担当者は通常とは異なる閲覧が自社の公開ドメインで行われていないか詳しくモニタリングしたり、社員の認証資格情報が Web に掲載されている兆候がないかを探ったりすることができます。これらの事象は即、攻撃が今まさに行われようとしていることの証拠にはなりませんが、さらに詳しく調査したりモニタリングしたりするきっかけになります。

「攻撃準備」ステージ

「攻撃準備」ステージ 内のフェーズには、ターゲット選択から攻撃開始までの間に攻撃者が使用する、すべての既知の方法が含まれています。これらのフェーズは必ずしも逐次発生するわけではなく、攻撃の進捗に応じて、同時に発生することもあれば、何度も繰り返して発生することもよくあります。また、それらのステップが完全に省略されるケースもあります。

外部偵察

*「外部偵察」*フェーズでは、攻撃者はターゲットを決定し、利用できそうなアクセス・ポイントに焦点を合わせてその組織を調べます。攻撃者はその組織の社員、子会社、顧客、パートナーを調べ、アクセスを許可されたユーザーを通じてその組織に潜入するために不可欠な資格情報を探ります。また、公開されている社員情報を使用してより広いアクセス権限を持つユーザーを特定し、可能な限りそれらのユーザーの資格情報を不正に入手しようと準備します。さらに、社内ネットワークと、攻撃対象の組織が利用しているクラウドのホスティング環境との間で、ネットワークでの足跡のマッピングを試みることもあります。

ターゲットに合わせた TTP の調整

*「ターゲットに合わせた TTP の調整」*フェーズでは、攻撃者はターゲットの攻略に最も有効と考えられる、利用可能な戦術、技術、手法 (TTP: Tactics, Techniques, and Procedures) を決定します。例えば、攻撃準備の以前のフェーズで得られたデータを使用して、本物らしいフィッシング・メッセージを作成したり、パートナーを通じてサード・パーティーでのアクセス権限を入手するオプションがないか判定したりします。また、攻撃の目標を達成するため、ネットワークのどの部分から侵入する必要があるのかを見極めることもあります。さらに、最初のホストに侵入した後、アクセスを拡大するのに最適なマルウェアやソフトウェア・ツールをこのフェーズで判断したりもします。攻撃者によっては、どのステージでもあえて悪質なツールは使わず、代わりにオペレーティング・システムの既存のコマンドを利用してネットワークに侵入するケースもあるので、注意が必要です。マルウェアはどの時点でも導入でき、攻撃フェーズ全体を通して変化または変異させることが可能です。

ネットワークの防御

多くの場合、攻撃用インフラストラクチャーの準備に入る攻撃者の活動を観察することができます。攻撃者は以前に使用したネットワーク・インフラストラクチャーを使い回すことがあるため、防御担当者は既知の悪質な C2 (指揮統制) ネットワークが再利用されていないかモニタリングしたり、疑わしいドメイン登録をモニタリングしたりすることができます。最後に、防御担当者は、ネット上の人物と対話することの危険性について社員を教育し、個人的に知らない相手からソーシャル・メディアや電子メールでコンタクトされた場合の適切な対応方法や、そのような場合の報告の必要性を指導できます。

攻撃用インフラストラクチャーの準備

「*攻撃用インフラストラクチャーの準備*」フェーズでは、攻撃者は C2 ネットワークを構築するほか、自分のリソースが突き止められる恐れのある、観察可能な痕跡を隠す手順を開発する場合もあります。

攻撃に入ると、マルウェアはここで確立された C2 インフラストラクチャーに戻ろうとします。それが完了すれば、攻撃者はそのマルウェアにアクセスし、侵入したホストを制御できます。攻撃者は通常、悪質な C2 インフラストラクチャーと通信リソースの構築を目的として、サーバーの所有権や SSL (Secure Sockets Layer) 証明書、ソーシャル・メディアや電子メールなどの Web サービスのアカウント、そして場合によっては、可用性の高い C2 を運用するためのその他のネットワーク・リソースを違法に購入、登録、取得します。

攻撃者は通常、プロキシーや仮想プライベート・ネットワーク (VPN) を使用して自分の通信を保護し、所在や身元を隠します。さらに、ターゲットによっては、攻撃者は新しい人物の捏造や実在の人物への成りすまし、あるいはその他のソーシャル・エンジニアリングの策略を使って、自分の戦術が合法的な活動であるように見せかけます。例えば、マルウェアを送付する前にターゲットとネット上で親しくなっておけば、攻撃者はより真実味のあるフィッシング・メッセージを作成できるかもしれません。実在しないネット上の人物は、新しい電子メール・アドレスの作成、ソーシャル・メディア・アカウントの設定、偽の企業 Web ページの作成や参加、会議への登録といったさまざまな方法で簡単に作り出すことができます。

ネットワークの防御

攻撃者はしばしば既存のマルウェアを購入または再利用して攻撃に備えますが、その活動を観察することができます。防御担当者は、ダーク Web をモニタリングし、攻撃者がマルウェアを調達している兆候がないか調べることができます。テスト・フェーズでは、不注意な攻撃者が攻撃用のコンポーネントやそのパーツを誤って一般に公開されている環境 (in the wild) に流してしまうことがあります。それを検知プログラムで捕えて、実際に攻撃を開始する前に調査できる場合もあります。

マルウェアとソフトウェア・ツールの準備

「*マルウェアとソフトウェア・ツールの準備*」フェーズは、攻撃者が攻撃に関する一般的な要件を定義した後に始まります。ただし、他の攻撃準備フェーズから詳細な情報が収集されるのに応じて、ツールやマルウェアを適宜調整する必要があります。攻撃用のツール・セットの準備にあたり、攻撃者はマルウェアを使用したり、合法的な用途のソフトウェア・ツールを作り替えたりします。また、新しいマルウェアを開発したり、過去に開発されたカスタム・ツールを再利用/購入したり、バックドアや資格情報のハッキング・ツールといった、一般公開されているマルウェアを作り替えたりすることもあります。同様に、既知の脆弱性を利用するためのエクスプロイトを調達したり、攻撃が検知されるリスクが減るよう、確実にゼロディ攻撃を実施できるようにしたりします。このプロセスは、オペレーティング・システムの制御やマルウェア検知に関わるアプリケーションを騙し、そのコードが信頼できるソースからのものであるかのように見せかけて、コードの実行を許可させます。これらのエクスプロイトやツールは、攻撃者の目標を達成するために、この後の「*攻撃開始*」フェーズ中や、不正アクセスに成功した後に使用されることがあります。

マルウェアとツールの準備が整うと、攻撃者はターゲットに向けて攻撃を開始する前に、それらの機能をテストします。テストでは、攻撃者のテスト用 C2 ネットワークまで戻って接続するバックドアを構築したり、検知される恐れがないか評価するために複数のアンチウィルス・エンジンでマルウェアをスキャンしたりします。また、攻撃者自身のアドレスにフィッシング・メールを送信したり、仮想マシンを使用して攻撃が正しく機能するか確認したりします。

継続的攻撃準備ステージ

X-Force IRIS サイバー攻撃準備フレームワークの中には、フレームワーク全体を通して実施されることから「*継続的攻撃準備*」ステージに含まれると考えられるフェーズが 2 つあります。それは、攻撃対象者やその他の外部の観察者からの検知を回避するための対策などが含まれる「*オペレーショナル・セキュリティー*」フェーズと、攻撃者が攻撃計画を見直して訂正するための「*フィードバック・サイクル*」フェーズの 2 つの*継続的攻撃* フェーズです。

オペレーショナル・セキュリティー

「*オペレーショナル・セキュリティー*」フェーズは、攻撃対象者やサイバー・セキュリティーの防御担当者から攻撃準備をしていることを隠すために攻撃者が取るすべての活動のことです。攻撃者、特に経験豊富な攻撃者は、自分のターゲットがこの作戦に気付いたり、自分の身元が知られたりする恐れがないか注意を払います。攻撃者は、偵察目的の検索、マルウェアの購入、ネットワーク・インフラストラクチャーの購入などのネット上での活動で使用した実際のネットワーク・アドレスを隠し、自分自身の重要情報を外部の観察者から保護しようとします。また、マルウェア・ツールのコードを解読できないようにしたり、マルウェアのサンプルをネット上にあるコードやサンプルのリポジトリーに置かないようにしたり、バックドアのステージング用のエコシステムを作成して、一部のツールは最も機密性の高いターゲット以外には使わないようにしたりするといった対策をしながら、それらの保護に務めます。

フィードバック・サイクル

「*フィードバック・サイクル*」フェーズは継続的なプロセスで、この間に攻撃者は以前のフェーズで集まった情報のレビュー、レビュー用のツールの評価、攻撃準備の修正などを行います。これらのフェーズで得られた知識から、サイバー攻撃フレームワークの随所で下される意思決定に必要な情報が提供されます。つまり、このフェーズは攻撃中、常に存在します。

攻撃開始

前述の X-Force IRIS サイバー攻撃準備ライフサイクルに含まれるすべてまたは一部のフェーズを完了すると、攻撃者は、ターゲットを直接、あるいは間接的に攻撃しはじめます。

直接攻撃のタイプ:

- 窃取した資格情報を使用する
- ターゲットとなった場所にあるコンピューターにアクセスする
- 悪質なファイルが添付されたフィッシング・メール
- 悪質なドメインに誘導するフィッシング・メール

間接攻撃のタイプ:

- 仕事用のラップトップが自宅のネットワークに接続されている間に感染させる
- Web サイトに不正アクセスする
- Web サイトの広告に不正アクセスする
- オンライン・コードを「トロイの木馬化」する

直接攻撃

直接攻撃 でターゲット・ネットワークにアクセスできるようにするために、攻撃者はいくつかの戦術を使用します。窃取した資格情報を使用してネットワークにリモート・アクセスしたり、ターゲットの場所にあるコンピューターに物理的にアクセスし、ネットワークへの直接アクセスを試みたりします。また、汎用的なフィッシング・メールに悪質なファイルやドメインを添付して送信し、ターゲットがそれを開くように仕向けることもあります。偽物をより本物らしく見せるために、フィッシング・メールをターゲットの 1 人以上のユーザーに合わせて作り替えたりもします。狙ったネットワークのユーザーに焦点を当てるのではなく、攻撃者がサーバーを直接利用することもあります。攻撃はありとあらゆる形態で行われ、それはドメイン・ネーム・システム (DNS) のポイゾニング、電子メールの資格情報の盗用、外部ネットワークから到来した自己増殖型ワームなど、多岐に渡ります。

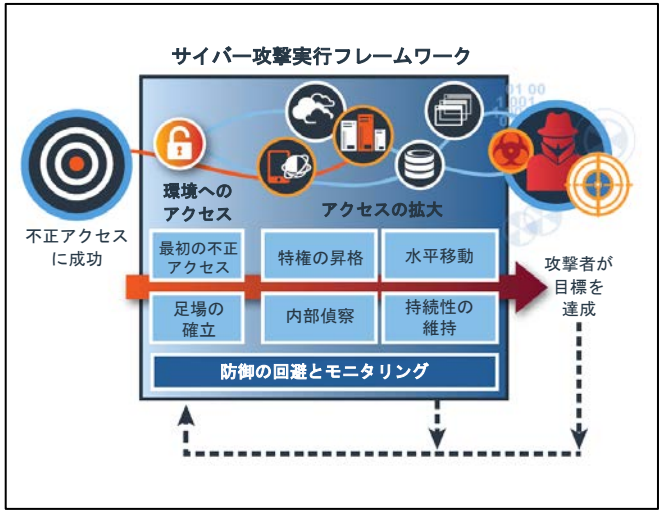
間接攻撃

攻撃者はネットワークに不正アクセスするために、*間接攻撃* によるアクセスを試みる場合もあります。例えば、仕事用のラップトップが自宅のネットワークに接続されている間に感染させることもあります。他にも、Web サイトや Web サイト上の広告に不正アクセスし、狙った組織のユーザーがその Web サイトを訪問し、マルウェアをうっかり自社のエンドポイントに取り込むのを待つ選択肢もあります。また、本来なら合法的なアプリケーション、Web ページ、ファイル、コード・ベースに悪質なコードを隠し、オンライン・コードを「トロイの木馬化」する場合もあります。

攻撃の成否を定義する

最後に、攻撃を開始した後、攻撃者はその攻撃によって不正アクセスに成功したかどうかを見極めます。攻撃が完全に、あるいは部分的に失敗した場合、攻撃者は準備フェーズのいずれかに戻ることを選ぶ場合もあります。また、攻撃のほとんどの部分はそのままで、いくつかの側面に変更を加えて、成功の可能性を高めようとするかもしれません。また、完全に失敗した場合には、より保護の緩い、他のターゲットに狙いを移すこともあります。

攻撃に成功したら、通常、攻撃者は準備フレームワークで入手したアクセス権限を使用して、X-Force IRIS サイバー攻撃実行フレームワークのフェーズを開始します。



X-Force IRIS サイバー攻撃実行フレームワークのフェーズ

X-Force IRIS サイバー攻撃実行フレームワークには、攻撃者が X-Force IRIS サイバー攻撃準備フレームワークの主要なフェーズを経て、ネットワーク内の少なくとも 1 つのホストへのアクセスの取得か、1 つ以上のユーザー・アカウントへのログインに成功した後に発生するフェーズが含まれています。

X-Force IRIS サイバー攻撃実行フレームワークには 8 種類のフェーズが含まれ、それらが 3 つのステージに分かれています。攻撃フレームワークのフェーズは、使用されるツールや攻撃者の目標に応じて、自動化スクリプトとイベント・ベースの命令および構成によって自律的に、あるいは手動で実施されます。どちらの方法にもそれぞれ利点と欠点があります。例えば、ネットワーク内でより速く拡散させられるのは自律型のマルウェアですが、さらにターゲットを絞って目立ちにくい方法で作戦を展開できるのは手動での攻撃です。自律型・手動型のどちらのタイプの攻撃戦術も、この攻撃フレームワーク内でモデル化できます。

- 最初の 2 つのフェーズは、「*環境* へのアクセス」ステージの一部です。「*最初の不正アクセス*」は攻撃者が攻撃を開始してそれに成功した後に行われます。また、これはサイバー攻撃実行フレームワークに必要な最初のステップです。
- 2 番目のフェーズである「*足場の確立*」は、攻撃者がネットワークへのアクセスを取得すると行われます。このフェーズは攻撃者が後続のいずれかのフェーズに進むための最初の要件です。
- 次のステージである「*アクセスの拡大*」には、「*特権の昇格*」、「*水平移動*」、「*内部偵察*」、「*持続性の維持*」の 4 つのフェーズが含まれています。これらのフェーズは同時に発生し、攻撃目標が達成されるまで何度か繰り返されます。攻撃者が、「*アクセスの拡大*」ステージ内のいくつかのフェーズをあえて行わない場合や、技術的な知識がないために一部のフェーズしか実行しない場合もあります。
- 「*防御の回避とモニタリング*」と「*フィードバック・サイクル*」の 2 つのフェーズは、悪質な活動の全体を通して発生するため、「*継続的攻撃*」ステージに含まれています。
- 「*防御の回避とモニタリング*」には、オペレーショナル・セキュリティーの手段と、攻撃者がセキュリティー・ツールを回避するための TTP が含まれており、多くの場合はこれを見ることでグループのスキル・レベルが分かります。
- 「*フィードバック・サイクル*」では、攻撃者は今と同じミッション、あるいは新しいミッションの目標を進めるために、攻撃フレームワークの以前のフェーズに戻る必要があるか判定します。
- 最後に、特定の攻撃に必要なフェーズが完了すると、攻撃者はそのミッションでの狙いを達成して、*目標を遂行*します。

「環境へのアクセス」ステージ

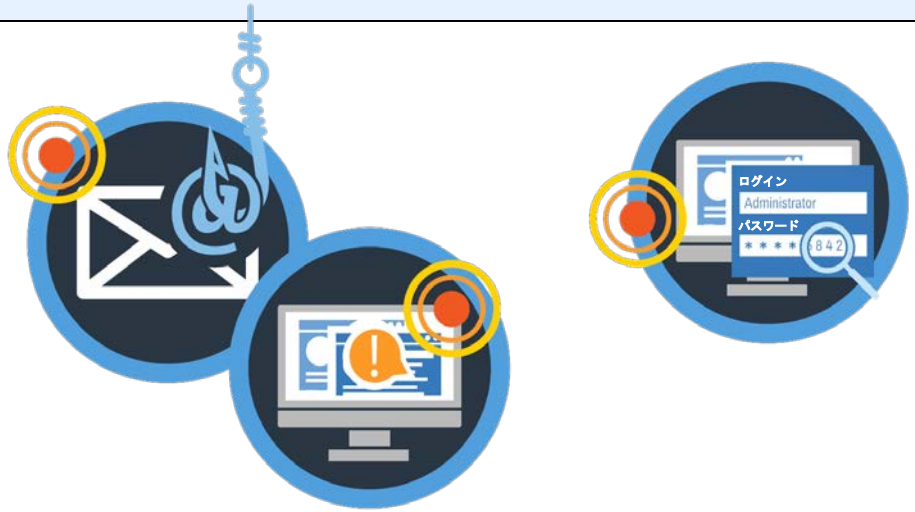
攻撃が成功したと判定されると、攻撃者は最初の不正アクセスを行って、速やかに*足場の確立* 作業を実施します。

最初の不正アクセス

「*最初の不正アクセス*」は、X-Force IRIS サイバー攻撃フレームワークに欠かせない最初のフェーズであり、攻撃者が「*攻撃開始*」フェーズを無事完了した後、準備ステップの一環として行われます。*最初の不正アクセス* は、攻撃者がネットワーク上の少なくとも 1 つのホストへのアクセスを取得したときか、いずれかのユーザーのアカウントにログインしたときに始まります。

最初の不正アクセスを実施するために使用される戦術には以下のものがあります。

- **フィッシングまたはスピア・フィッシング:** 特定のユーザーや特定の業界を狙った詐欺的な電子メールや電子的コミュニケーションで、ユーザーを騙して個人情報や機密情報を聞き出したり、リンクをクリックするように促したり、違法な目的で攻撃者が使用するマルウェアを忍ばせた、一見問題のない添付ファイルをダウンロードするよう誘導したりします。
- **Web 不正アクセス:** 攻撃者が悪質なコードを合法的な Web サイトや Web アプリケーションに注入する際に使用される一般的な用語。広告に悪質なコードが注入された「マルバタイジング」や、特定のユーザー群が頻繁にアクセスする Web ページにドライブ・バイ・ダウンロードが仕込まれる「水飲み場型攻撃」などはいずれもこの例です。



足場の確立

「*足場の確立*」フェーズでは、攻撃者は、ネットワーク内の少なくとも 1 つのホストまたはユーザー・アカウントに対して継続的にアクセスし、制御できるようにします。攻撃者の狙いは、確立された C2 インフラストラクチャーを使用して、バックドアをインストールしたり、その他の目に付かない足場をネットワーク内に確保したりして、感染したコンピューターをリモート制御することです。

攻撃者は、この足場から C2 ネットワークへのアウトバウンドの通信リンクを確立できます。攻撃対象者と攻撃者の指揮統制サーバーの間の通信は、多くの場合複数のレイヤーでエンコードまたは暗号化され、その送付先は特定を防ぐために解読不能な状態になっています。

足場を確立するために使用される戦術には、以下のものがあります。

- **バックドア:** 攻撃者がホストにアクセスする際に、そのホストの一般的なセキュリティーや認証のメカニズムを迂回するために使用する何らかの手段を指します。
- **ユーザー・アカウント・アクセス:** 攻撃者はリモート・アクセスの資格情報、ソーシャル・ネットワークの資格情報、電子メールの資格情報といった、ユーザーのオンライン・アカウントのアクセス権限を入手して、自分の目標を直接達成したり、そこから他のネットワーク・リソースに移ったりします。

ネットワークの防御

ネットワークを不正アクセスから完全に保護することが理想ではあるものの、そのような望みはなかなか叶うものではなく、ビジネス・リーダーは、ネットワークに対する不正アクセスのリスクを前提として事業を運営しなければなりません。そのため、攻撃者が彼らの目標に到達するのを防ぐことにゴールを設定して、ネットワークを社内で防御するか、外部のサービス・プロバイダーを利用するかのいずれかを行う必要があります。防御担当者の役割は、攻撃の開始を「最初の不正アクセス」と「足場の確立」のフェーズで阻止することであり、それにはエンドポイントでの検知と被害軽減のための強力な戦略を実装することが重要です。防御担当者は、スピア・フィッシングなどの、ネットワークに最初に不正アクセスする際に使われる一般的な技法を社員に周知させる必要があります。加えて、すべてのネットワーク・トラフィックを緊密にモニタリングする、マルウェアが自動的にインストールされないように何らかのインストールに制限を設ける、既知のエクスプロイトや悪質な Web サイトをフィルタリングするなどの方法を取ることができます。

ネットワークの防御

攻撃が複雑または高度な場合、攻撃者はしばしば「アクセスの拡大」ステージで相当な時間と手間を取られます。防御担当者がしっかり準備を行っていれば、このステージは、これらのフェーズで攻撃者が行う活動を観察し、対抗できる好機です。防御担当者は、インストール・プロセスの制限、強力なアクセス制御の実施、ネットワーク内およびネットワークから離れるすべてのトラフィックのモニタリングを行うことができます。これらのステップは攻撃対象のネットワーク内で、しかも最終目標が達成される前に発生するため、防御担当者が被害の発生を防ぐ上で最高のチャンスといえます。

「アクセスの拡大」のオプション:

- 特権の昇格
- 水平移動
- 内部偵察の実施
- 持続性の維持

「アクセスの拡大」ステージ

「*アクセスの拡大*」ステージ内のフェーズには、*最初の不正アクセス* から *目標の遂行* までの間に攻撃者が使用する、すべての方法が含まれています。これらのフェーズは必ずしも逐次的に発生するのではなく、同時に、何度も繰り返して発生することも多くあります。電子メール・アカウントの不正アクセスなどでは、これらのフェーズが完全に省略されるケースもあります。

ネットワークへの最初のアクセスを取得すると、攻撃者は攻撃対象のネットワークに関するさらに詳しい洞察を収集し、アクセスを拡大しようと試みます。攻撃者がアクセスを拡大するために使用するオプションとしては、*特権の昇格*、*水平移動*、*内部偵察の実施*、*持続性の維持* があります。

特権の昇格

「*特権の昇格*」フェーズでは、攻撃者は不正アクセスしたネットワーク内の、さらに多くのリソースに対するアクセスを取得します。より広いアクセス権限を持つユーザーのユーザー名とパスワードを入手する、公開鍵インフラストラクチャー (PKI) 証明書を盗み出す、特権が設定されたアカウントやコンピューターにアクセスするなどのよくある手口を使った追加の資格情報の入手もこのようなアクセスに含まれます。最初に侵入したホストよりも多くのアクセス権限を持つユーザーの資格情報を攻撃者が入手し、自分の目標の達成に役立つような、管理者用アクセス権限やシステムに対する全アクセス権限の入手を試みることもよくありますが、これも特権の昇格と見なされます。

特権を昇格するために使用される戦術には、以下のものがあります。

- **パスワード・ダンピング:** これはオペレーティング・システムからユーザー名とパスワードの情報を取得するツールを指す用語です。パスワード・ダンピング・ツールの例としては、Mimikatz や Windows Credential Editor (WCE) などがあります。
- **Pass the hash:** パスワードのハッシュは、パスワードそのものを表面に出さずに、平文パスワードの固有の ID を提供する、一方通行のアルゴリズムです。「Pass-the-hash」攻撃は、窃取したハッシュ値を使用して、攻撃者が平文パスワードを必要とする認証を迂回するときに行われます。
- **内部アプリケーションまたはシステムの破壊:** システムの構成や利用可能なアプリケーションによっては、攻撃者はコマンドを注入したり、コードを上書きしてパーミッションのレベルをリモートで昇格させることができます。

水平移動

「*水平移動*」フェーズでは、攻撃者はそのネットワーク上の他のホストや、系列会社、合併先、サード・パーティー・プロバイダーなどの他のネットワークに移動します。このフェーズでは「*特権の昇格*」フェーズの場合と同様、さまざまな戦術を使用することも、また時には窃取した資格情報のように、同じ戦術を使用することもあります。攻撃者は追加のホストへのアクセスを取得し、最初に侵入したホストでは入手できなかったデータの入手のほか、窃取や破壊といったゴールの達成を試みます。

水平移動のために使用される戦術には、以下のものがあります。

- **リモート・アクセス:** 企業が社員に社内ネットワークへのリモート接続を許可することはよく行われています。このようなケースでは、攻撃者は窃取した資格情報を使用してそのネットワークにリモートでアクセスしたり、ユーザー等級のアクセス権限を入手したり、自分の活動を合法的なユーザーの活動であるかのように偽装したりすることができます。
- **タスクのスケジュール:** これは Windows の機能で、ユーザーはこれを使用することにより、プログラムやスクリプトが特定の時間に実行されるようにスケジュールを組むことができます。攻撃者はこの機能を使用して、例えば持続性を確立するコードを起動時に実行したり、将来のある特定の日時にイベントをスケジュールしたりすることができます。さらに、スケジュールしたタスクを利用して、同じネットワーク経由で接続された別のホストに対し、悪質なコマンドや破壊的なコマンドをリモートで実行することもできます。
- **net use コマンド:** このコマンドによって、攻撃者はそのネットワークにマッピングされている他リソースへの接続を構成したり、ネットワークに接続を追加したりできます。
- **PsExec または PowerShell:** これらは Windows ツールで、いずれも攻撃者によるリモートでのコマンドの実行を可能にします。

内部偵察

攻撃者はネットワークに入ると、内部ネットワークに関する追加の情報を「*内部偵察*」フェーズを通じて収集します。侵入によってネットワークのユーザーやグループに関する情報の収集、使用されるアクセス・レベルの確認、利用可能なファイルやデータベースの特定などが可能になります。また、侵入した攻撃者は、自分がどの情報に対するアクセス権限を持っているのか、ミッションの完遂にはさらにどのデータが必要か、などを確認する必要があります。*内部偵察* は通常、オペレーティング・システムに備わっているコマンドを使用して実施できますが、ポート・スキャナーなどの外部ツールも使用できます。

内部偵察のために使用される戦術には、以下のものがあります。

- **システム、アカウント、アプリケーションの列挙:** 悪意のある人物が、標準装備されているコマンドやアプリケーション機能を使用して、システム内にユーザー名が存在するかを調べ、それに対応するパスワードをブルート・フォースの技法を使って割り出します。
- **ポート・スキャン:** ポート・スキャンまたはポート・スキャナーは、ネットワークで開いているポートを照会し、ネットワークを保護しているファイアウォールがあるかどうかを判断するために攻撃者が使用するツールです。この偵察ツールによって、脆弱なアクセス・ポイントを特定できます。
- **ファイルの閲覧:** ホスト・コンピューターや共有ドライブ上のドキュメントを閲覧し、興味を引くデータを探します。
- **サービス・チケット:** パスワード・ダンピング・ツールを使用してサービス・チケットにアクセスし、そこから特定のリソースへのアクセスを入手します。

持続性の維持

「持続性の維持」フェーズでは、攻撃者は、その環境全体から外部に継続的にアクセスできるようにして、自分の足場を強化し、それを維持する活動を完了します。ここでの目標は、システムが再起動されたり、アクセス・ポイントの障害が発生したり、窃取した資格情報が拒否されたりする場合に備えて、ネットワークに冗長性が高い、オーバーラップしたアクセスを確保することです。攻撃者はホストへの不正アクセス後、直ちに最初のバックドアをレジストリーの場所に置き、ホストが再起動するたびにそれが実行されて、持続性が確立されるようにします。

持続性を維持するために使用される戦術には、以下のものがあります。

- **バックドア:** 攻撃者は「足場の確立」フェーズで説明した追加のバックドアを使用して冗長性を高め、1 つのアクセス・ポイントが削除または中断されても、他のエントリー・ポイントを使って引き続きコントロールを維持できるようにします。
- **VPN の悪用:** 攻撃者は許可されたユーザーの PKI や VPN の資格情報を使用することで、バックドア経由でシステムに侵入しなくても済むようにします。攻撃者はこの方法を使用して、自分のトラフィックを合法的なユーザーの活動のように見せかけ、それによってネットワーク内に身を隠すことができます。
- **Webshell:** Webshell は Web サーバーにアップロードされた悪質なスクリプトで、それによって攻撃者はそのホストをリモートで制御できるようになります。

「継続的攻撃」ステージ

X-Force IRIS サイバー攻撃実行フレームワークの中には、「*継続的攻撃*」ステージに指定されているフェーズが 2 つあり、攻撃者は侵入中を通してこれを実施します。「*防御の回避とモニタリング*」には、攻撃対象や防御担当者からの検知を回避するための対策が含まれています。また、「*フィードバック・サイクル*」は、ネットワーク内に入った後にゴールと戦術を見直す機会があります。

攻撃対象の環境は、攻撃者にとってはほぼ未知であり、防御担当者の操作に応じて変化するため、攻撃者にはこの動的な環境に対処できる柔軟性が必要です。

ネットワークの防御

攻撃者は、防御担当者がネットワーク上の攻撃者の足場を探して排除する能力を、「防御の回避とモニタリング」の戦術を使用して妨害します。防御担当者は、すべてのネットワーク・トラフィックを緊密にモニタリングし、エンドポイントをモニタリングして、異常な挙動を頻繁に検索しなければなりません。さらに、防御担当者は、攻撃者がネットワークに侵入する方法が複数あることを認識し、それに対処できるよう備える必要があります。複数のバックドアを除去し、感染した一連のホストのイメージを回復しても、ネットワークの攻撃者のアクセスを完全に排除することはできません。

防御の回避とモニタリング

「*防御の回避とモニタリング*」フェーズには、ネットワーク上の足跡を隠すために攻撃者が使用する戦術が含まれています。攻撃フレームワークで説明した他のフェーズとは異なり、「*防御の回避とモニタリング*」は単独で実施することも、あるいは他のすべての攻撃実行フェーズと組み合わせて実施することもできます。このフェーズには、合法的なプロセス内への悪質なコードの隠蔽、ログの削除やログの破壊、コマンド履歴の消去、パッキング、通信やコマンドの暗号化とエンコーディングが含まれます。さらに、他の脅威実行者が採用する戦術を使用して、その攻撃を別のグループになすりつけようとする、「偽旗」作戦を実施する攻撃者もいます。攻撃者はこの戦術を、外国語の使用やタイム・スタンプの調整などによって、この攻撃が別の国から行われたことをさりげなく匂わす形で行うことも、あるいはもっとあからさまに、自分の身元を偽名を使って公にすることもあります。

エンドポイントの脅威検知機能やインシデント対応チームによって身元が特定されたことに気付くと、それへの対応を行う攻撃者もあります。これらのケースでは、侵入した攻撃者はインシデント対応者とそのシステムをモニタリングし、検知プログラムを無効化しようとしたり、インシデント対応者から自分のマルウェアが特定される前にそれをネットワークから削除しようとしたりします。最後に、攻撃者は、ネットワーク内でうまく隠蔽できたエントリー・ポイントを維持し、今後も侵入できるようにします。

防御の回避のために使用される戦術には、以下のものがあります。

- **ルート・キット:** これは悪質なコンピューター・ソフトウェアで、オペレーティング・システムの API (アプリケーション・プログラミング・インターフェース) へのコード注入およびその修正によってアンチウィルス・プログラムを騙し、自らの存在だけでなく、他の悪質なプログラムの存在も隠すように設計されています。
- **暗号化とステガノグラフィー:** 暗号化とは、データや通信を鍵がなければ読み取れないテキストにマスキングすることを指します。一方、ステガノグラフィーは、データ内にデータを隠すプロセスであり、メッセージの存在そのものが隠蔽されます。画像やオーディオ、ビデオなどのファイルにデータを隠すケースなどがこの例です。
- **マスカレード:** マスカレードは、攻撃者が、悪質なコードに信頼できる名前や一般的な名前を付けて、エンドポイントの検知システムを迂回できるようにし、それを既知の信頼できる場所に置くことによって行われます。

ネットワークでの足跡を隠すために攻撃者が使用する戦術には、以下のものがあります。

- 合法的なプロセス内への悪質なコードの隠蔽
- ログの削除
- ログの破壊
- コマンド履歴の消去
- パッキング
- 通信の暗号化およびエンコード
- コマンドの暗号化およびエンコード
- 「偽旗」
- 外国語の使用
- 偽名を使った自分の身元の公開

フィードバック・サイクル

「*フィードバック・サイクル*」では、攻撃者は侵入の状況を見直し、その結果をミッションの目標と比較して、いずれかの攻撃のフェーズに戻ったり、改善したりします。また、他のすべてのフェーズで集められた情報に基づき、攻撃中に、あるいは以後に備えて、戦術を変更することもあります。例えば、攻撃対象者がその環境から攻撃者のアクセスを排除しようとすると、攻撃者は TTP を訂正してマルウェア機能を強化し、その同じネットワークにアクセス・ポイントを再び挿入したり、他の攻撃対象者への今後の攻撃に備えたりします。

目標の遂行

攻撃者が望むのは、X-Force IRIS サイバー攻撃フレームワークで説明されているすべてのフェーズ、あるいはその一部を完了し、侵入のミッションを完了することです。攻撃者が国家の支援を受けているかどうか、あるいは攻撃者の動機に応じて、その目標はさまざまです。例えば、スパイ行為が目的の攻撃者であれば、データの抜き取りか偵察が主要な目標になるでしょう。攻撃者の目標としては、他にも、サイバー攻撃による破壊や混乱、金銭的な窃盗、イデオロギーの伝達、国家の「ソフト・パワー」の影響力の誇示などが挙げられます。

ネットワークの防御

防御担当者の観点での目標は、この最後のフェーズの前に攻撃者を検知することです。ただし、攻撃者がこのフェーズに到達したとしても、防御担当者はアプリケーションの制御を制限し、データ損失防止ツールを使用して厳格なデータ転送制御を実施することにより、データの不正アクセスの影響を最小限に抑えることができます。さらに、防御担当者は、外に出ていくネットワーク・トラフィックをモニタリングし、外部への指揮統制通信を停止させることができます。

著者:

Jonathan Wrolstad、Alexandrea Berninger
X-Force IRIS 脅威インテリジェンス作成チーム

X-Force IRIS の連絡先

IBM X-Force Incident Response and Intelligence Services の詳細については、IBM 担当員または IBM ビジネス・パートナーにお問い合わせいただくか、https://www.ibm.com/security/services/xforce-incident-response-and-intelligence をご覧ください。

セキュリティー・ブリーチの被害に遭われているお客様は、以下の IBM X-Force インシデント対応者にご連絡ください。
1-888-241-9812 (米国およびカナダ)
(001) 312-212-8034 (米国およびカナダ以外)

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町 19-21

Produced in Japan
2018 年 7 月