cobaltstrike

データシート（サイバーセキュリティ）

COBALT STRIKE

脅威エミュレーションツール

アンフェイクはFORTRAのプラチナパートナーです

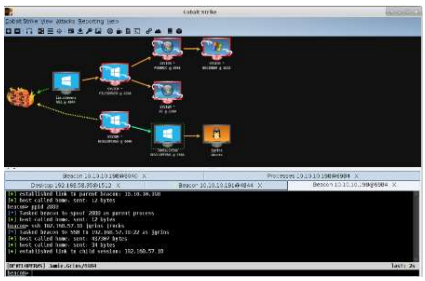
コンセプト

Cobalt Strikeは脅威をエミュレーションするツールです。ビーコンと呼ばれるエージェントにより、強力なポストエクスプロイト（攻撃モジュール）を提供します。また、ネットワークインジケータを変更してC＆Cサーバとの通信を秘匿し、様々なマルウェアやソーシャルエンジニアリング攻撃を模倣します。その結果、サイバー攻撃を長期的かつ秘密裏にシミュレーションすることができます。

ペネトレーションテストは、パッチが適用されていない脆弱性と設定ミスに焦点を当てますが、Cobalt Strikeが提供するサイバー攻撃シミュレーション、レッドチーム演習では、サイバー攻撃の戦術と技術を評価し、セキュリティ運用とインシデント対応を強化することができます。

攻撃対象の操作

ピボットによる水平移動



主な機能

1. ポストエクスプロイト

システム侵入（エクスプロイト）後にビーコンを埋め込み、PowerShellスクリプトの実行、キーストロークの記録、スクリーンショットの取得、ファイルダウンロード、他のペイロード生成等、強力な攻撃モジュールを提供します。

ビーコン攻撃モジュールの一部

製品概要

機能概要

- ポストエクスプロイト
- 秘匿通信
- 初期アクセス
- 攻撃パッケージ
- ブラウザのピボット
- スピアフィッシング
- レッドチームのコラボレーション
- レポートとログ

システム要件

- 2 GHz+ プロセッサー
- 2 GB RAM
- 500MB以上の空きディスク容量
- Java
- **Oracle Java 1.8**
- **Oracle Java 11**
- **OpenJDK 11**

サポートされているOS

Cobalt Strikeサーバー

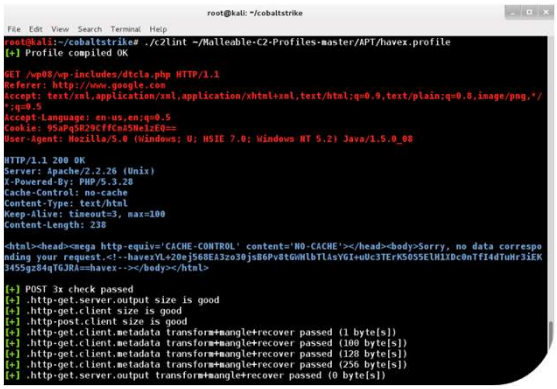
- Debian
- Ubuntu
- Kali Linux

Cobalt Strikeクライアント

- Windows 7 以降
- MacOS X 10.13 以降
- Debian, Ubuntu, Kali Linux などの GUI ベースの Linux

株式会社アンフェイク
〒252-0303 神奈川県相模原市南区相模大野8-3-3センチュリーKIビル303号
Tel: 042-702-0890 E-mail: sks-sales@unfake.co.jp

Malleable C2の設定



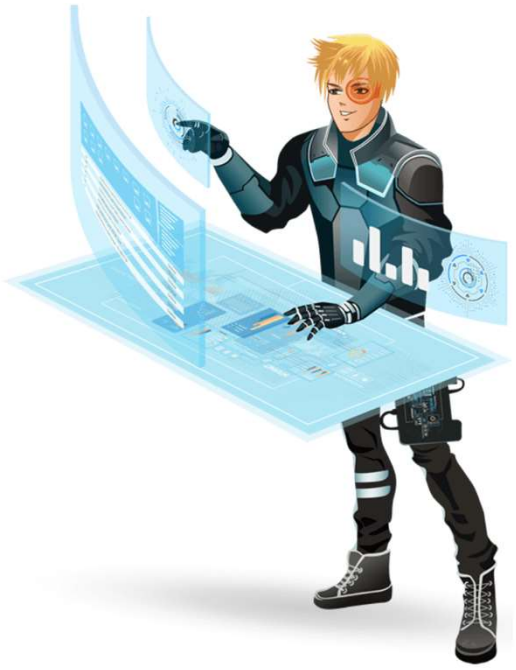
2. 秘匿通信

ビーコンは、非同期の低速通信を検出されないようにすることで攻撃を隠蔽することができます。ビーコンがサポートするMalleable C2により、ネットワークインジケータを変更し、HTTP、HTTPS、DNSを使用して別のアクセスに見えるようにネットワークを設定します。

また、SMBプロトコルによるネームドパイプを使用し、ネットワークワイドにピアツーピアでビーコン間通信を行います。

3. 初期アクセス

Cobalt Strikeは、ローカルWebサーバにアクセスしたユーザーのフィンガープリントを取得し、内部IPアドレス、アプリケーション、プラグイン、およびバージョン情報を検出します。また、メッセージをインポートし、リンクと添付ファイルによる説得力のあるフィッシングメールを作成することができます。メールは、Javaアップレット、MSマクロやexeファイル、Webサイトのクローンによる攻撃が可能です。



4. レポートとログ

Cobalt Strike は複数のレポートを生成して、エンゲージメント中に発生したすべてのアクティビティの全体像を提供できます。レポートの種類は次の通りです。

- 活動のタイムライン
- ホストごとのデータの概要
- 侵害の兆候
- すべてのセッションとアクティビティの詳細な説明
- ソーシャルエンジニアリング
- 侵入戦術、テクニック、手順

レポートは MS Word または PDF としてエクスポートされ、
必要に応じて調整できます。カスタム ロゴを追加したり、タイトル、説明、ホストを構成したりできます。

株式会社アンフェイク
〒252-0303 神奈川県相模原市南区相模大野8-3-3センチュリーKIビル303号
Tel: 042-702-0890 E-mail: sks-sales@unfake.co.jp