cobaltstrike

近年、その脅威を増している“サイバー攻撃”に対して事前の演習で対策強化
“脅威に対して脅威で備えるエミュレーションツール”

Introduction

“予期せぬ攻撃に万全な対策を”

年々増加するセキュリティインシデントは、
大手企業・中小企業問わず、あなたを狙っています。
そして、*日本国内では、ほぼ毎日どこかしらでサイバー攻撃の被害が発生しています。

そんな予期せぬ攻撃に対して、
同じ脅威による“エミュレーション”という観点から対策をしませんか？

*トレンドマイクロ社「2024年上半期セキュリティインシデントを振り返る」より参照

コンセプト Concept

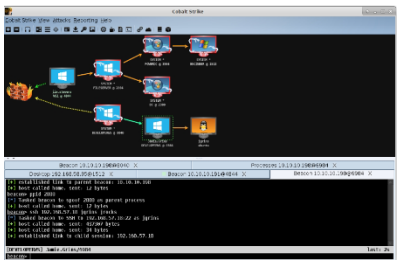
Cobalt Strileは、脅威を”脅威”でエミュレーションするツールです。
ビーコンと呼ばれるエージェントにより、強力なポストエクスプロイト（攻撃モジュール）を提供します。
また、ネットワークインジケーターを変更して、C&Cサーバとの通信を秘匿し、様々なマルウェアやソーシャルエンジニアリング攻撃を模倣します。
その結果、サイバー攻撃を長期的かつ秘密裏にシミュレーションすることができます。

C&Cサーバとは、サイバー攻撃者がマルウェアに指令を出したり、盗み出した情報を受け取ったりするためボットネットワークをコントロールする指令サーバのことです。

ベネトレーションテストでは、パッチが適応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及び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、セキュリティ運営とインシデント対応をより強化することが可能です。

ベネトレーションテストとは、ネットワーク、PC・サーバーやシステムの脆弱性を検証するテスト手法の1つです。
実際にネットワークに接続しシステムに攻撃を仕掛け侵入を試みることから、
「侵入テスト」と呼ばれることもあります。


攻撃対象の操作


ピポットによる水平移動

主な機能 Main Features

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
- キーストロークの取得・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

など、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 Product overview

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
- OS ※サポートOSを参照
- CPU 2GHz+プロセッサー
- メモリー 2GB以上
- HDD 500MB以上の空き容量
- Java
  - ➢Oracle Java 1.8
  - ➢Oracle Java 11
  - ➢Open JDK 11

サポートOS
- Cobalt Strike Server
  - ➢Debian
  - ➢Ubuntu
  - ➢Kali Linux
- Cobalt Strike Clients
  - ➢Windows 7/8/10/11
  - ➢Mac OS 10.13以降
  - ➢GUIベースLinux
    例）Debian,Ubuntu,Kali Linux

PLATINUM helpsystems PARTNER
株式会社アンフェイクは、Fortra（旧Helpsystems）のプラチナパートナーです

CS2025

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ル303号
Tel: 042-702-0890 E-mail: sks-sales@unfake.co.jp

主な機能 Main Features

2. 秘匿通信

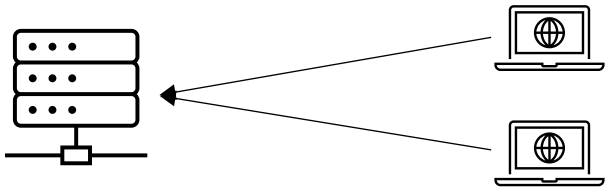
ビーコンは、非同期の低速通信を検出されないようにすることで、攻撃を隠匿することができます。
ビーコンがサポートするMalleable C2により、ネットワークインジケータを変更し、
HTTP,HTTPS,DNSを使用して、別のアクセスに見えるようにネットワークを設定します。

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P2Pでビーコン間通信を行います。


Malleable C2の設定

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・プラグインおよびそれらのバージョン情報を検出・取得します。
また、メッセージをインポートし、リンクと添付ファイルを使用した、
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。
メールでは、Javaアップレット・MSマクロやexeファイル・Webサイトのクローンなどあらゆる方法での攻撃が可能です。



4.レポートとログ

Cobalt Strikeにてシミュレーションした内容を複数のレポートとして、
生成し、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
を確認することが可能です。

生成されるレポートは、下記の6つです。
- ●活動のタイムライン
- ●ホストごとのデータ概要
- ●サイバー攻撃の兆候
- ●すべてのセッションとアクティビティの詳細説明
- ●ソーシャルエンジニアリング
- ●シミュレーションの際に行った侵入戦術・テクニック・手順の説明

生成されたレポートは、Microsoft Wordまたは、PDF形式で出力され、
必要に応じて、調整が可能です。
また、レポートにはカスタムロゴやタイトル・説明・対象ホストの構成が追加
できますので、社内の重要書類として使用する際にも、使用が可能です。

製品紹介・お問い合わせはこちらから

製品紹介ページはこちら

https://unfake.co.jp/solution/cobalt strike

お問い合わせはこちらから

Web：https://unfake.co.jp/inquery/
Mail：sks-sales@unfake.co.jp

株式会社アンフェイクは、Fortra(旧Helpsystems)のプラチナパートナーです

CS2025

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ル303号
Tel: 042-702-0890 E-mail: sks-sales@unfake.co.jp