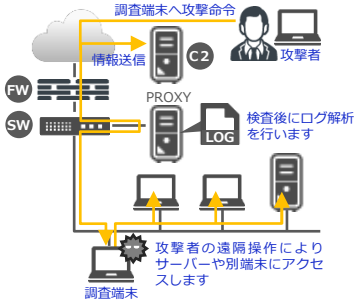
標的型攻撃シミュレーションサービス

擬似マルウェアによる攻撃シミュレーションで組織ネットワークを評価・診断する

サービス概要

近年被害が増加している標的型攻撃に代表されるサイバー攻撃は、その攻撃手法やマルウェアの高度化により、組織における防御を一層困難なものにしています。ウイルス対策ソフト等による入口対策をしていても、僅かな脆弱性から不正プログラムの侵入を許し、情報流出等の実害に至ってはじめて、不正アクセスを認識する事例は後を絶ちません。

本サービスは、お客様のネットワークのセキュリティ対策が、標的型攻撃に対してどの程度検出、遮断できるのかを診断するサービスです。標的型メール攻撃によりPCがマルウェアに感染した事態を想定し（疑似マルウェアを使用）、攻撃者による社内情報窃取が防御・検知できるかを検査します。



サービスの特長

本サービスでは、お客様にご用意頂いたPCに疑似マルウェアを感染させ、当社のホワイトハッカーが外部から感染PCを操作してネットワーク内の探索やファイルの持ち出し等の攻撃を仕掛けます。試験実施後、お客様よりログ等をご提出頂き、お客様のネットワークの安全性について総合的な評価を行います。

特長　本物の標的型攻撃と同様の攻撃をホワイトハッカーが再現

検査は、ホワイトハッカーと呼ばれる高度な専門技術をもったエンジニアが本物の標的型攻撃と同様の手法で行います

（例）標的型攻撃の実際のプロセスと疑似攻撃の例

攻撃プロセス	主な活動	疑似攻撃の一例	調査範囲
計画立案	・攻撃目標設定 ・関連調査	調査範囲外	
攻撃準備	・標的型メール ・C&Cサーバ準備	調査範囲外	
初期侵入	・マルウェア感染	・予め用意したURLより不正プログラムをダウンロードし感染させます	↕
基盤構築	・バックドア開設 ・端末の諜報 ・ネットワーク環の調査・探索	① バックドアの開設が可能かを確認 ② 感染端末の情報を収集	↕
内部侵入調査	・端末間での侵害拡大 ・サーバへの侵入	① ポートスキャンなどによりローカルネットワークを調査します ② 共有フォルダに不正ファイルをアップロードします	↕
目的遂行	・データの外部送信 ・データの破壊 ・業務妨害	・取得情報をC&Cサーバへアップロードします	↕
再侵入	・バックドアを通じ再侵入	調査範囲外	

疑似攻撃による脆弱性診断の流れ

STEP1 ネットワーク環境ヒアリング

お客様ネットワーク環境、経由するネットワークきについてヒアリングを実施します

STEP2 テスト内容の確認

ご担当者様と実施する疑似攻撃のシナリオ作成や試験項目、使用PC等の確認をします

<試験内容（一例）>
・テスト端末の情報取得
・ネットワーク情報取得
・ファイルサーバへのアクセス
・ポートスキャン
・スクリプト実行
・キーストローク取得　等

STEP3 お客様準備

テスト用ログインアカウント作成、ファイルサーバへのアクセス権等テストに合わせた準備をお客様に依頼します

STEP4 弊社準備

疑似マルウェアの作成、C&Cサーバ及びマルウェア配布サーバの作成を行います

STEP5 試験

お客様先にてSTEP2で決定した試験項目を実施します

STEP6 ログ提出

STEP1で確認したネットワーク機器上でテスト時間帯に取得したログをお客様よりご提出頂きます

STEP7 総合評価

ご提出頂いたログと試験結果をもとにお客様ネットワークの安全性の総合評価を実施します

STEP8 報告会

総合評価をもとに報告会を開催しご説明を行います

納品物について

検査完了後は「標的型攻撃評価報告書」にて疑似攻撃の詳細結果と、現状対策の脆弱ポイントや対策についてご報告致します。また担当エンジニアによる報告会も実施可能です。

試験実施までのスケジュール例

ヒアリングから総合評価の報告書納品まで約1.5ヶ月を想定しております。

分類	実施項目	1週目	2週目	3週目	4週目	5週目	6週目
事前確認	お打合せ・現状調査	■					
	環境構築		■				
	ドメインアカウント発行		■				
	ファイルサーバへのアクセス権付与		■				
	実施日程の調整		■				
疑似攻撃	疑似攻撃実施（1日）			★			
	ログの受領			■			
	結果の整理				■		
総合評価	総合評価					■	■
	報告会実施（1日）						★

お問合せはこちら：**株式会社ソリトンシステムズ**　サイバーセキュリティ事業部　cyber-sales@list.soliton.co.jp／ TEL 03-6369-8015