デジタル不正対策サービス
情報システムペネトレーションテストサービス
サービス紹介資料

株式会社ラック

セキュリティプロフェッショナルサービス統括部
デジタルペンテストサービス部

はじめに｜高度標的型攻撃（APT）によるセキュリティ侵害事例の変遷

2011

防衛産業、政府機関を対象とした、**標的型メール**による攻撃

- 9月：「三菱重工」へのサイバー攻撃で、国内11拠点でマルウェア感染
- 9月： 同時期に川崎重工業、IHI、三菱電機、NECが標的型メールを受け取っていた
- 11月：「衆議院」で、雑誌記者を装ったメールに添付されていたマルウェアに感染

2012

攻撃対象の範囲拡大と、標的型メールの**手口の巧妙化**

- 2月：「農林水産省」で、窃取したメールを悪用したメールでマルウェア感染
- 3月：「国際協力銀行」で、窃取したメールを悪用したメールでマルウェア感染
- 12月：「日本原子力開発機構」で、対話型のメールによりマルウェア感染

2013

水飲み場型攻撃の増加と、**感染経路の多様化**

2014

- 9月： IEの「ゼロデイの脆弱性」を悪用した水飲み場型のマルウェア感染
- 1月：「ソフトウェアのアップデート機能」を悪用したマルウェア感染
- 6月：「CDNetworkes」のコンテンツか改ざんされ、エンドユーザがマルウェア感染

2015

日本を標的にした組織による攻撃が継続中

2016

- 6月：「日本年金機構」他、複数組織で「Emdivi」による感染と情報漏えい

2017
2018
2019

- 5月：「ホンダ」、ランサムウェア「WannaCry」による感染と生産ライン停止
- 7月：「産総研」、クラウド型メールシステムへのフィッシング攻撃で情報漏えい

2020

業務環境の変化に伴う攻撃手法や脅威の多様化・巧妙化

2021

- 1月：「NEC」、防衛省関連ファイル約2万7000件に不正アクセス
- 8月：「三菱重工」、在宅勤務時に感染したマルウェアから個人情報流出

© 2021 LAC Co., Ltd.

はじめに｜多様化・巧妙化するサイバー攻撃

高度標的型攻撃

標的型攻撃の一種であり、特定の相手に狙いを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数か月から数年にわたって継続するサイバー攻撃。(CYREC 2013)

二重脅迫型ランサムウェア

PCやサーバに保存されているデータを暗号化して復号のための身代金を要求するだけでなく、さらにそのデータを窃取し、インターネット上で不特定多数公開するという「二重の脅迫」を行うサイバー攻撃。

サプライチェーン攻撃

セキュリティ対策が強固とはいえない中小企業を含む取引先や海外展開を進める企業の海外拠点などの「サプライチェーン」を起点とし、目標とする組織への侵害を試みるサイバー攻撃。

侵入されることを前提とした多層的な対策が重要

全てが未知ではない

ボットやツールは検知できる可能性

C2通信を見つける

既知のボットのC2通信は検知できる

内部ネットに注意

ツール実行などの感染拡大の兆候をつかむ

認証管理に注意

ActiveDirectoryの管理者が狙われやすい

認証つきプロキシ

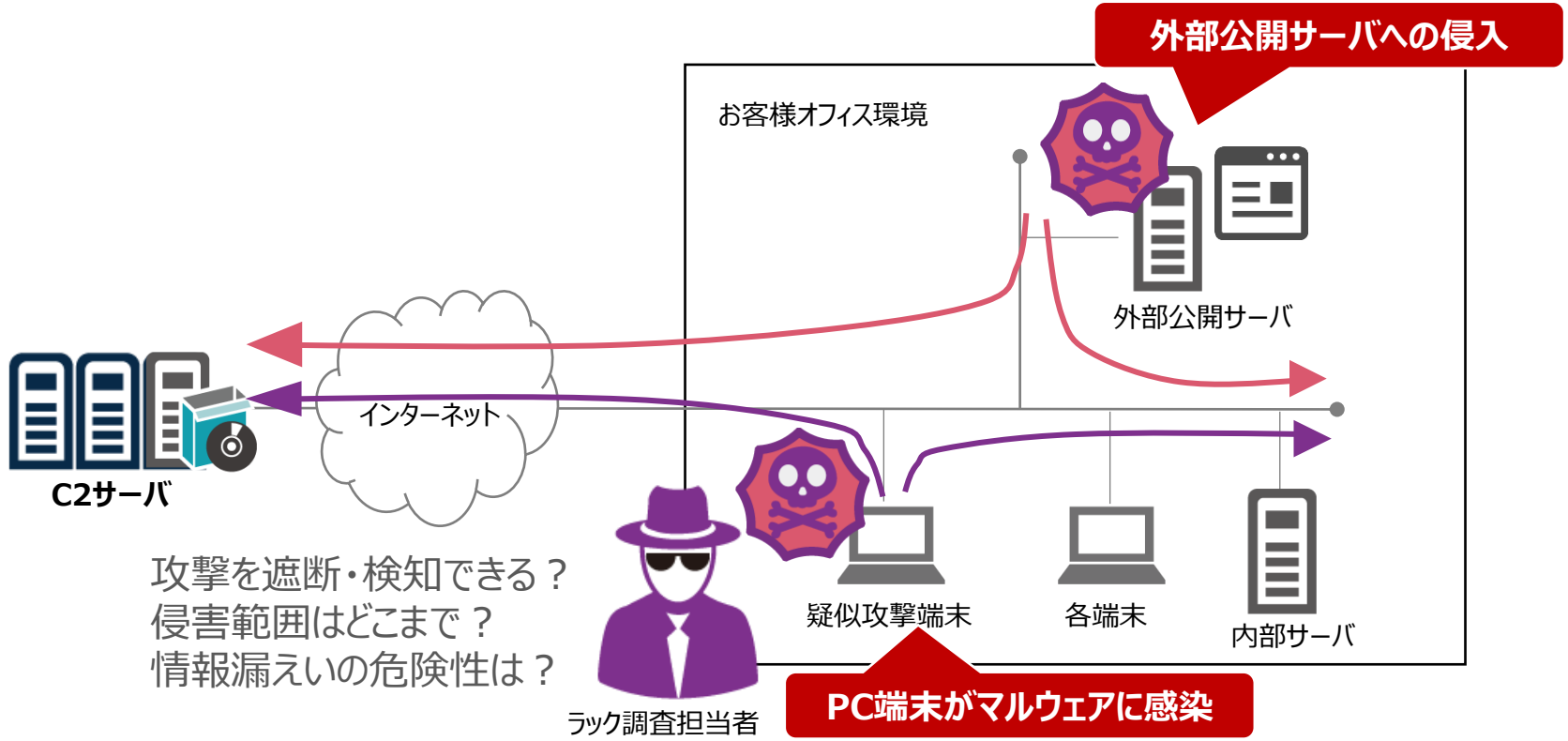
認証未対応のボットによる拒否ログ

【参考】弊社ブログ「相次ぐ「二重脅迫型ランサムウェア」の被害と対策～今、ペネトレーションテストにできること～」
https://www.lac.co.jp/lacwatch/service/20210827_002700.html

© 2021 LAC Co., Ltd.

情報システムペネトレーションテストサービスとは

お客様の情報システム（社内外のネットワークシステム）において、PC端末のマルウェア感染または外部公開サーバへの侵入を前提として、ネットワーク経由での疑似攻撃による侵入可否や、侵入後の展開可能範囲を攻撃的手法により検証するサービスです。

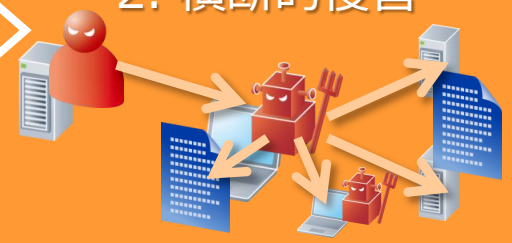


【参考】弊社ブログ「相次ぐ脆弱性診断とペネトレーションテストの使い分け―サイバー攻撃から企業を守る」
https://www.lac.co.jp/lacwatch/service/20201112_002314.html

© 2021 LAC Co., Ltd.

情報システムペネトレーションテストサービスとは｜特長

最新のセキュリティ対策を実装したものの…
・実際のサイバー攻撃が来ないと効果が測定できない
・各フェーズで評価を実施すると莫大なコストがかかる

攻撃の流れ	1. 潜入	2. 横断的侵害	3. 活動
			
	攻撃者は標的組織のセキュリティ防御を破り、マルウェアが添付された電子メールや改ざんされたWebサイトからマルウェアを侵入させる	攻撃者はマルウェアを利用して、内部ネットワーク情報を収集。他サーバや端末の認証を突破し、侵害範囲を拡大する	機密データなど攻撃者がターゲットとする重要な情報を探索・収集。外部へ送信・情報の改ざん等、攻撃者の目的を達成する
評価サービス	◆ 標的型メール訓練	◆ 内部サーバ脆弱性調査調査 ◆ ネットワークフォレンジック	◆ ネットワークフォレンジック

情報システムペネトレーションテスト

予防対策の効果測定

実際の手法と同等の疑似攻撃を**内部から網羅的**に行うことで、導入済みのAPT攻撃対策の評価や、**内部システムを含めた多層防御**の対策につなげます。

インシデント対応の効果測定

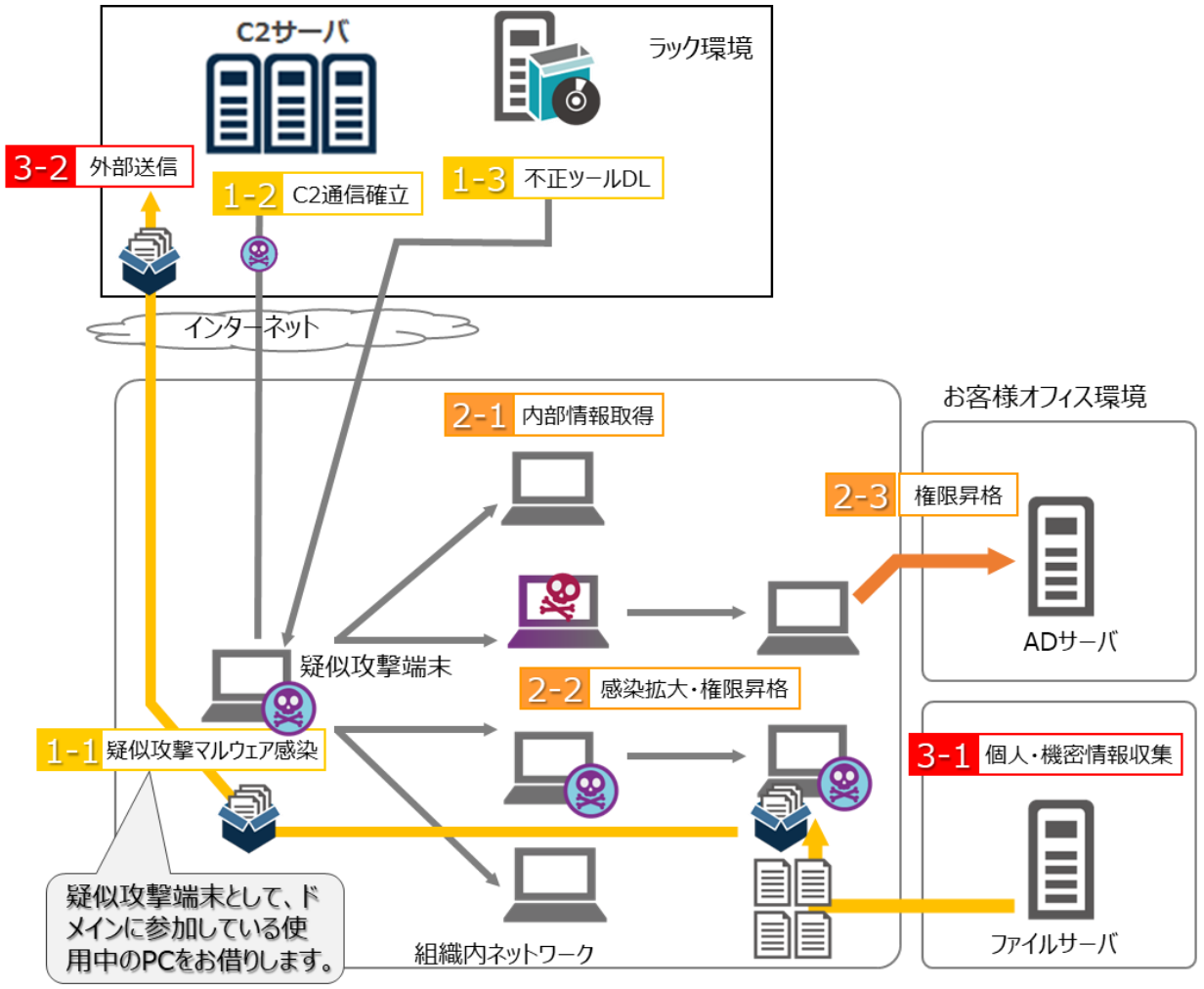
疑似攻撃によって発生する各種ログを確認することで、**インシデントレスポンスにおけるログの有効性**を評価できます。

【参考】弊社ブログ「脅威ベースの検証で問題点検出実績100%！ラックのペネトレーションテストのヒミツ」
https://www.lac.co.jp/lacwatch/service/20210714_002660.html

© 2021 LAC Co., Ltd.

情報システムペネトレーションテストサービスとは｜調査内容イメージ

情報システムペネトレーションテストサービスでは、PC端末がマルウェア感染したことを前提として、実際のお客様の端末から疑似攻撃を行い、組織内の情報システムのサイバー攻撃に対する耐性を評価いたします。



© 2021 LAC Co., Ltd.

ラックの強み｜多層防御の全体に対する検証

当社のペンテストは、多層防御の全体をまるごと検証して深みのある検証を実施、改善点をすべてお伝えします。

© 2021 LAC Co., Ltd.

ラックの強み｜各サービスの高度な知見をペネトレーションテストに反映

弊社のAPT攻撃に対する研究活動をはじめ、フォレンジック調査やマルウェア解析など多数の高度な知見を基に、ペネトレーションテストサービスにおける調査内容に随時反映しています。また、得られた技術情報を文書・レポートや無償サービスの形で公開し、お客様の情報セキュリティの啓蒙活動に役立てています。

■LAC WATCH（オウンドメディア）

オウンドメディアにてテクニカルレポートや注意喚起を随時発信

■脅威対策に関する文書の公開

発行日	内容
2015年06月09日	「日本年金機構の情報漏えい事件から得られる教訓」公開
2015年07月28日	標的型攻撃対策専門組織を設置し、「標的型攻撃 対策指南書」を無償公開
2015年08月31日	日本年金機構の事件報告を受けて、なすべき最低限の対策に関する提言書を公開
2020年08月25日	企業戦略としてテレワーク推進をする企業に向け「テレワーク導入便覧」を公開

■研究・調査レポート

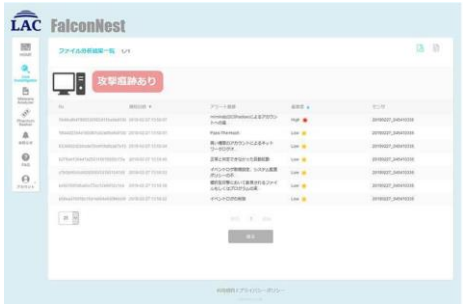
研究部門の技術レポート
「Cyber GRID View」

セキュリティインシデントの発生傾向の分析
「JSOC INSIGHT」

診断サービスの結果の分析および傾向や知見
「セキュリティ診断レポート」

■無償サービス

PC端末のセキュリティ対策のチェックツール「自診くん」



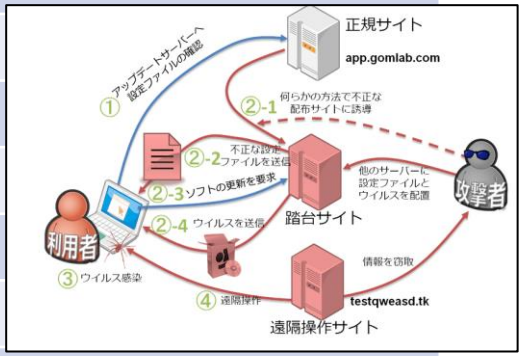
サイバー攻撃の痕跡確認やマルウェアの判定を支援する「FalconNest」

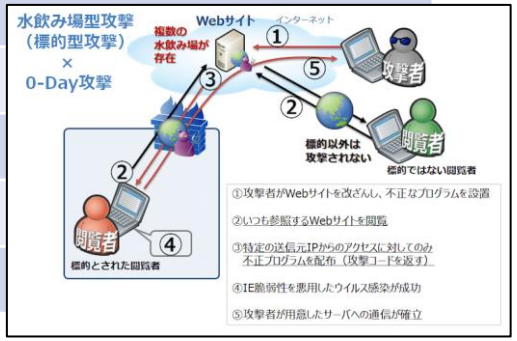
© 2021 LAC Co., Ltd.

ラックの強み｜各サービスの高度な知見をペネトレーションテストに反映

■LAC WATCH（オウンドメディア）における標的型攻撃に関連する研究・技術情報発信

発行日	内容
2021年05月21日	Microsoft社のデジタル署名を悪用した「Cobalt Strike loader」による標的型攻撃～攻撃者グループAPT41
2020年12月01日	【緊急レポート】Microsoft社のデジタル署名ファイルを悪用する「SigLoader」による標的型攻撃を確認
2020年04月24日	標的型攻撃の新たな手口判明。診断ツール「PoshC2」を悪用する攻撃の流れを解説
2020年02月12日	オープンソースのポート転送／トンネリングツールを悪用する標的型攻撃に注意
2020年01月21日	【注意喚起】無料ツール「FalconNest」を使用し、標的型サイバー攻撃の痕跡有無を調査してください
2019年02月13日	オープンソースのツール「PoshC2」を悪用した新たな標的型攻撃を確認
2018年05月21日	APT攻撃者グループ menuPass(APT10) による新たな攻撃を確認
2018年04月25日	攻撃者グループ "BlackTech"による "PLEAD"を使った日本への攻撃を確認
2017年08月07日	PowerShell Empireを利用した標的型攻撃
2017年04月13日	標的型攻撃を受けた場合の組織へのダメージを事前に把握するには？
2017年02月23日	攻撃者グループmenuPassとマルウェア「Poison Ivy、PlugX、ChChes」の関連性
2015年06月16日	水面下で侵攻するサイバースパイ活動急増に関する注意喚起
2014年01月23日	正規のソフトウェアのアップデートで、不正なプログラムが実行される事案について
2013年10月09日	日本における水飲み場型攻撃に関する注意喚起
2013年09月19日	Internet Explorerの「ゼロデイの脆弱性」を悪用した攻撃に対する注意喚起





© 2021 LAC Co., Ltd.

Thank you. Any Questions ?

※ 本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※ 本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。
※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。
※ その他記載されている会社名、製品名は一般に各社の商標または登録商標です。

株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1 平河町森タワー
sales@lac.co.jp
www.lac.co.jp