SE Labs

INTELLIGENCE-LED TESTING

侵害対処テスト
保護モード

BlackBerry Protect
BlackBerry Optics

2021 年 7 月

SE Labs はさまざまなハッキング攻撃を用いて BlackBerry Protect と BlackBerry Optics のテストを行いました。使用した攻撃手法は、システムを侵害してターゲットのネットワークに侵入することを目的に設計されたもので、サイバー犯罪者やその他の攻撃者がシステムやネットワークの侵害に用いる手法と同じものです。

テストには攻撃チェーンの全段階を使用します。すなわち、試験者は実際の攻撃者と同じように、さまざまなツール、手法、ベクトルを用いてターゲットを偵察してから、低レベルなアクセス権の取得を試み、その後より強力なアクセス権の取得を試みます。そして最後に、情報の窃盗、システムの破壊、ネットワーク上の他のシステムへの接続といった攻撃目標の達成を試みました。

マネジメント
CEO（最高経営責任者） Simon Edwards
COO（最高執行責任者） Marc Briggs
CHRO（最高人事責任者） Magdalena Jurenko
CTO（最高技術責任者） Stefan Dumitrascu

テストチーム
Nikki Albesa
Zaynab Bawa
Thomas Bean
Solandra Brewster
Rory Brown
Liam Fisher
Gia Gorbold
Jeremiah Morgan
Joseph Pike
Dave Togner
Dimitrios Tsarouchas
Stephen Withey
Liangyi Zhen

IT サポート
Danny King-Smith
Chris Short

編集
Sara Claridge
Colin Mackleworth

Web サイト selabs.uk
Twitter @SELabsUK
電子メール info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
ブログ blog.selabs.uk
電話番号 +44 (0)203 875 5000
住所 SE Labs Ltd,
55A High Street, Wimbledon, SW19 5BA, UK

SE Labs は IT セキュリティ製品テストの提供に関して、
ISO/IEC 27001: 2013 と、
BS EN ISO 9001: 2015 の認証を受けています。

SE Labs は、Microsoft Virus Information Alliance (VIA)、
Anti-Malware Testing Standards Organization (AMTSO)、
Messaging, Malware and Mobile Anti-Abuse Working Group
(M3AAWG) のメンバーです。

BlackBerry Limited による再配布を許可

目次

ドキュメントバージョン 1.0 作成日：2021 年 7 月 15 日

はじめに

予防的なエンドポイント保護

犯罪者を侵入前に阻止するセキュリティ製品をお望みではありませんか？

攻撃者を検知・阻止するチャンスは数多く存在します。攻撃者がターゲットにフィッシングメールを送信した段階で検知できる製品もあれば、不正なコードへのリンクが含まれるメールを受信した段階で検知する製品もあります。また、マルウェアがシステムに侵入した時点で対処を開始する製品もあれば、攻撃者がネットワーク上で不正な活動を行った時点で検知する製品もあります。

セキュリティ製品がどの段階で効果を発揮するとしても、利用者が望むことは、攻撃の目標を達成される前に攻撃を検知・予防することでしょう。

弊社の侵害対処テストの特徴は、攻撃チェーンを一通り実行して製品をテストする点にあります。可能な限り現実に近い条件でテストを行えるように、侵害を試みる際に用いられるすべてのステップを順番に実行するのです。各製品は違ったやり方で脅威を検知・予防するため、これは重要なポイントです。

結局のところ、導入したセキュリティ製品に利用者が求めることは、どんな手法であれ侵害を予防することです。とはいえ、攻撃が阻止されるまで被害を傍観し、その後の復旧で苦労するよりは、脅威を初期段階で阻止する方が望ましい手法といえます。

セキュリティ製品の中には、監視と通知に特化して設計された製品もあれば、脅威が検知されるか被害が発生すると即座に対処を開始して脅威を除去できる製品も存在します。「監視」を主眼とする製品に対しては、検知モードで侵害対処テストを実施します。また、BlackBerry Protect のような「阻止」を主眼とする製品に対しては、保護モードでテストを実施して製品の有効性を明らかにします。

このレポートでは、一連の侵害の試みに対する BlackBerry Protect の対処能力を確認します。たとえば、どの段階で検知と保護に成功したか、業務に影響を与えなかったか、合法的なアプリケーションを誤検知しなかったか、といった内容が含まれます。

多種多様なセキュリティ製品の能力を把握する場合、実環境で利用を迫られる前に行っておくのが良いやり方です。SE Labs の侵害対処テストレポートは、お客さまの組織に最適な製品を評価する上で役に立ちます。

このレポートで不明な点や議論したい点がある場合は、弊社の Twitter アカウントや Facebook アカウントからご相談ください。SE Labs では、可能な限り現実に近いテストを実現するため、最新の脅威インテリジェンスを利用しています。テスト方法や、「脅威インテリジェンス」に対する弊社の定義、テスト内容の改善に脅威インテリジェンスをどう活用しているかは、弊社の Web サイトを参照するか、Twitter アカウントをフォローください。

エグゼクティブサマリー

BlackBerry Protect と BlackBerry Optics のテストには、さまざまなハッキング攻撃を用いました。これらの攻撃は、システムを侵害してターゲットのネットワークに侵入することを目的に設計されたもので、サイバー犯罪者やその他の攻撃者がシステムやネットワークの侵害に用いる手法と同じものです。

テストで確認した製品の能力は次のとおりです。

- 高度な標的型攻撃を検知する能力
- 高度な標的型攻撃に関連した活動に対する保護能力
- 脅威がもたらす被害やリスクから復旧する能力
- 合法的なアプリケーションやその他のオブジェクトを取り扱う能力

偽陽性や望ましくない相互作用の有無を評価するため、脅威とともに合法的なファイルを使用します。

BlackBerry Protect と BlackBerry Optics は、すべての攻撃に対する完全な検知と保護を達成した上、すべての合法的なアプリケーションの動作を妨げないという素晴らしい成績を収めました。テストの難易度を考慮すると、これは並外れた結果です。

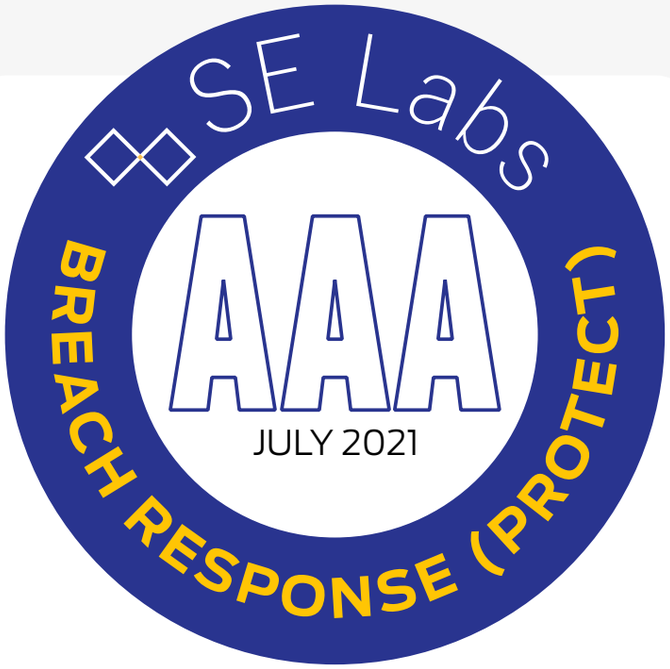
エグゼクティブサマリー			
テスト対象製品	保護精度 (%)	誤検知回避 精度評価 (%)	総合的な 精度評価 (%)
BlackBerry Protect と BlackBerry Optics	92%	100%	95%

緑色の項目は総合的な精度評価が 85% 以上であり、製品の精度が非常に高いことを示します。
また、黄色の項目は総合的な精度評価が 75% から 85%、赤色の項目は 75% 未満であることを示します。

SE Labs

侵害対処アワード

SE Labs アワード
受賞製品



BlackBerry Protect
BlackBerry Optics

1. テスト方法

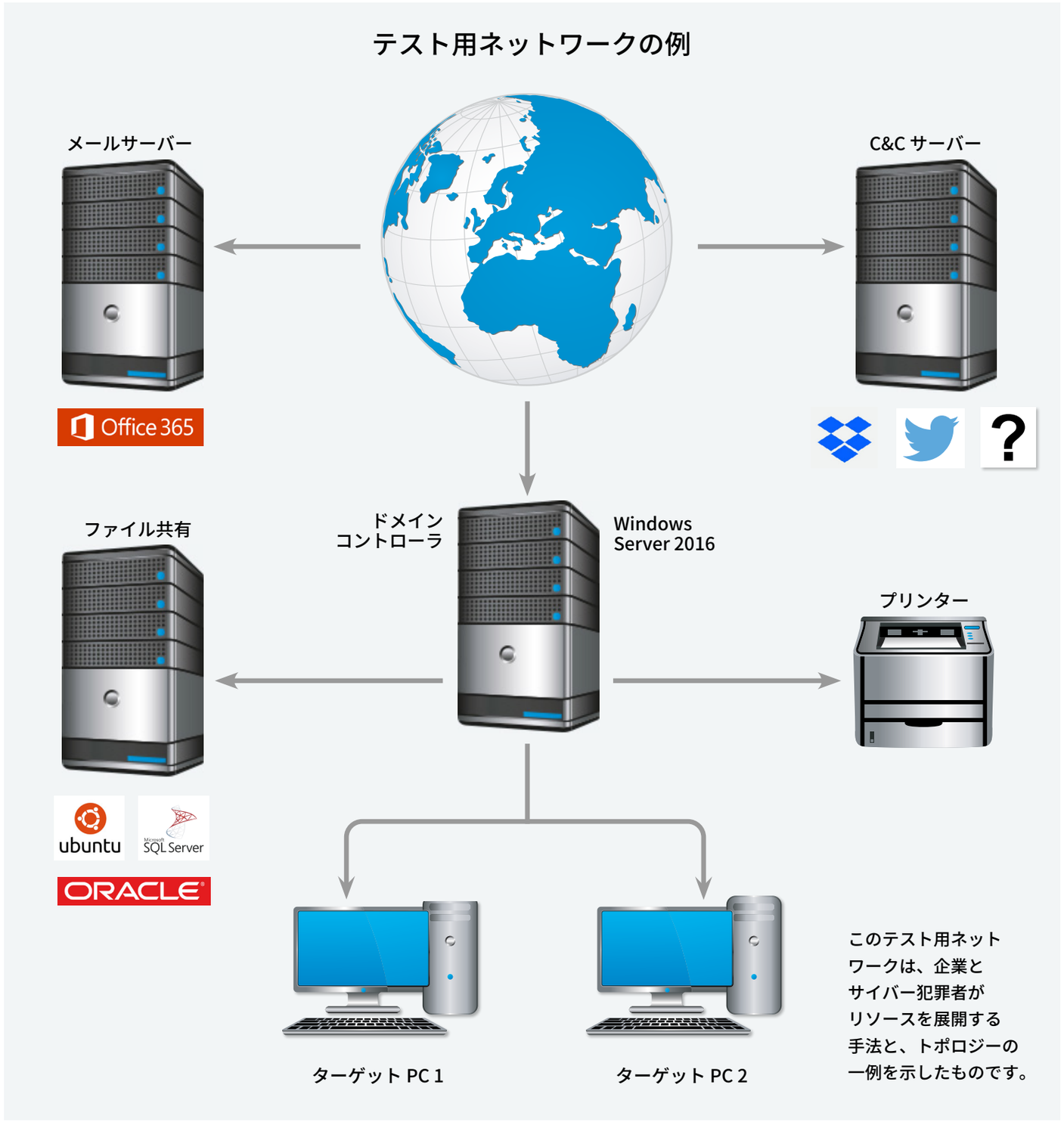
試験者は、製品が一定の内容で動作するとは見なしません。そのため、実際にネットワークを構築して現実の攻撃者と同じやり方でハッキングを行うことで、現実に近い侵害対処テストを実施します。

右の図はネットワークの例です。ワークステーションと、ファイルサーバーやドメインコントローラなどの基本的なインフラに加えて、クラウドベースのメールサーバーや悪意のあるコマンドアンドコントロール（C&C）サーバーなどが含まれます。C&C サーバーには、一般的なコンピューターや、Dropbox、Twitter、Slack などのサービスの他に、前例のないサービスが使用される場合があります。

脅威対処の項目（7 ページ）で解説しますが、攻撃者は「水平移動」と呼ばれる活動において、侵害したシステムの間をジャンプすることがよくあります。製品にこうした活動を検知させるには、利用可能で、脆弱で、侵害に値するシステムを準備して、現実に近いネットワークを構築する必要があります。

また、企業向けのプリンターや IoT（モノのインターネット）機器などのデバイスが侵害を受ける可能性もあります。図にプリンターが含まれているのはそのためです。

各テストケースに使用する手法は、ほとんどが現実のサイバー犯罪者の手口を手本としたものです。弊社では、サイバー犯罪者の戦術を観察し、テストの際にその行動を模擬しています。各攻撃者の行動と、その行動をどのように模擬しているかの詳細は、**ハッカー vs ターゲット**（9 ページ）を参照ください。また、さらに詳細な情報については、**4. 脅威インテリジェンス**（13 ～ 16 ページ）と、**付録 C：攻撃の詳細**を参照ください。



脅威対処

完全な攻撃チェーン：検知・保護の全レイヤーをテスト

攻撃者はあるポイントから攻撃を開始し、目標を達成するか、リソースが尽きる（期日や能力の限界など）まで攻撃を継続します。したがって、テストにおいても試験者は現実的な初期位置から攻撃を開始する必要があります。具体的には、フィッシングメールの送信や、感染した Web サイトの準備から攻撃を開始します。その後、実際に使われる可能性が高い多数のステップを経由して、実際にデータを盗むか、なんらかの形でネットワークに被害を与えます。

仮に、エンドポイントでマルウェアを実行するなど、攻撃チェーンの終盤からテストを開始すると、保護能力と検知能力を十分に発揮する機会を奪われる製品が多数出現することになります。同様に、「十分な」被害を与えるか、「十分な」データを盗む前に結果を判断してしまうと、行動検知などの能力を示す機会を奪われる製品が出てくる可能性があります。

攻撃段階

下図は、典型的な攻撃段階の例を示したものです。テストではセキュリティソリューションの有効性を判断するため、各段階の攻撃を試みる必要があります。テストの結果には、各攻撃段階における検知結果と保護結果が記録されます。

製品が攻撃の初期段階でどのように応答したかを評価するため、検知評価や保護評価を使用します。例として、脅威の実行を阻止できなかったが、検知には成功したという結果があり得ます。また、脅威の実行を一時的に許したが、その後無力化に成功したという結果もあり得ます。理想的には、脅威に実行の機会を与えずに検知とブロックを行うのが望ましい製品です。脅威を削除する製品もあれば、後の解析のため「隔離」やその他の安全な保存メカニズムを用いて脅威を自動的に収容する製品も存在するでしょう。

仮に初期段階の攻撃に成功した場合、エクスプロイト後の段階の評価を行います。下図では、第 2 段階から第 7 段階にあたります。これらの段階のおおまかな分類は次のとおりです。アクセス（第 2 段階）、活動（第 3 段階）、権限昇格（第 4 段階）、権限昇格後（第 5 ～ 7 段階）。

図 1 は典型的な攻撃の流れを示したもので、さまざまな「ハッキング」活動が行われています。この例は、完全に成功した侵害に分類できます。

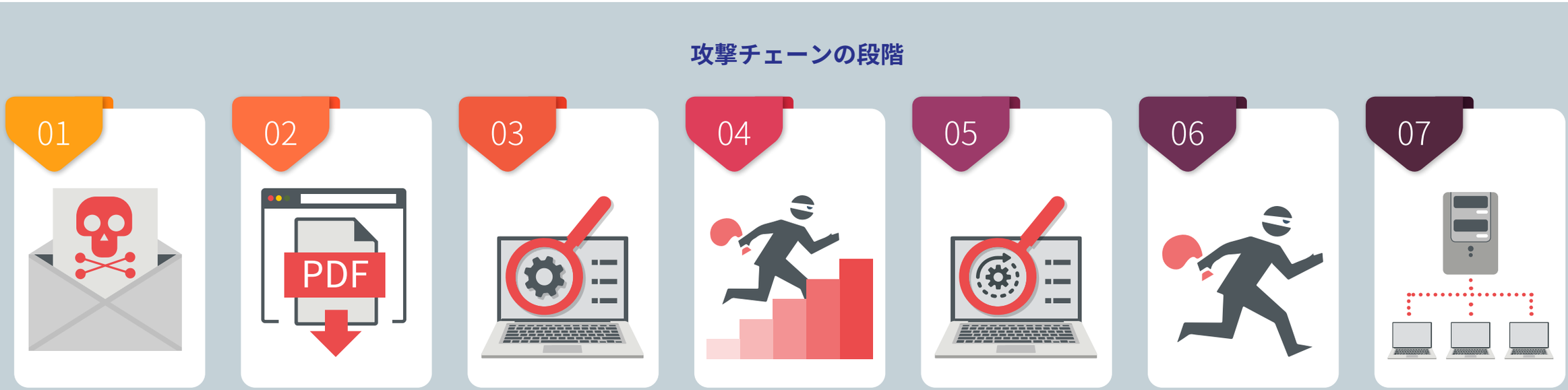


図 1：典型的な攻撃は初期接触から始まり、偵察、データ窃盗、破壊活動といったさまざまな段階を経て進行します。

図 2 は製品またはサービスが攻撃を阻止した例です。第 3 段階までの攻撃を許しましたが、その後検知と無力化に成功しています。そのため、攻撃者は第 4 段階以降に進めませんでした。

もちろん、異なる順番で攻撃を実行することも可能です。たとえば、攻撃者は権限昇格を行わずに他のシステムへの接続を試みることもできます。とはいえ、パスワードを盗み出してから（第 5 段階）、盗んだ認証情報を使用してネットワーク深部への侵入を試みるのが一般的な手法です。

また、攻撃の間に目立った被害が出ない可能性もあります。考えられる要因としては、システム上で永続性を獲得して活動を監視し、徐々に情報を盗み出すなどの、検知が難しい活動を行うことを目的としている場合です。

図 3 は、攻撃者が第 5 段階まで進むことに成功した例です。この場合、システムは重大な侵害を受けていることになります。この攻撃者は高レベルなアクセス権の取得とパスワードの窃盗に成功しました。ですが、ターゲットからのデータの流出や、システムに被害を与える試みは阻止されています。

攻撃チェーン：ハッキング活動の進行

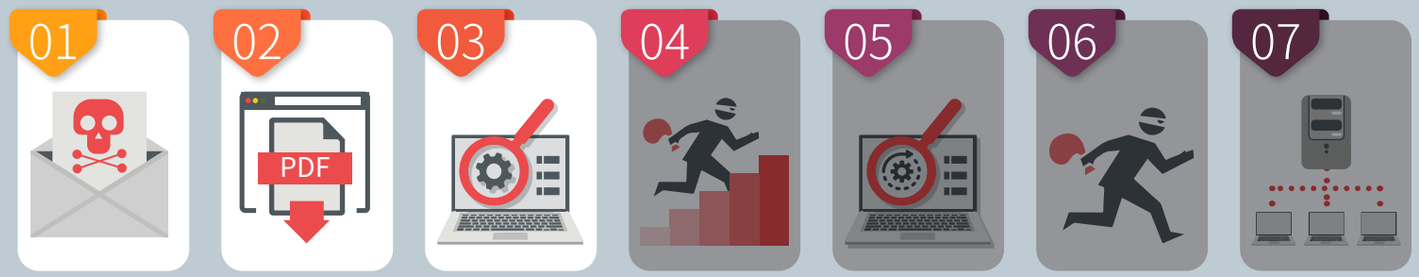


図 2：初期段階では成功したが、偵察フェーズまでしか進めなかった攻撃の例

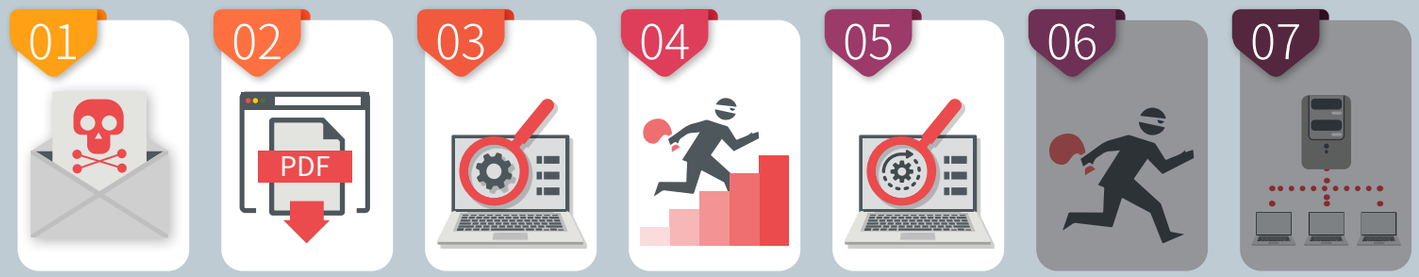


図 3：パスワード窃盗に成功したが、大量のデータ窃盗や破壊活動は阻止された攻撃の例

ハッカー vs ターゲット

標的型攻撃に対するサービスの能力をテストする際は、適切な攻撃手法を選択することが重要です。ターゲットを手あたり次第に攻撃することは、誰にでもできるからです。セキュリティベンダーにとっての課題は、使用頻度の高い攻撃タイプを特定し、その攻撃に対する保護を提供することです。試験者の立場では、何らかの形で現実世界に関連した脅威を作成する必要があります。

テストに使用された攻撃は、どれも組織を侵害した実績のある手法です。ターゲットがセキュリティ対策を施していなければ、どの手法も攻撃に成功するでしょう。攻撃の目標は、システムにランサムウェアを感染させる、ネットワークへのリモートアクセスを行う、データを盗み出すといったものです。

ただし弊社は、会議室でブレインストーミングを行って、さまざまな企業への攻撃手法を検討したわけではなく、最新の脅威インテリジェンスを使用して過去数年のサイバー犯罪者の動向を調査し、その手口を可能な限り模倣しました。この手法によって、各国の政府機関、金融機関、国家インフラが直面している脅威に類似した脅威に対する、サービスの対処能力をテストできます。

右の表は、今回のテストに使用した標的型攻撃の元になった攻撃グループの概要です。テストで使用した標的型攻撃をサービスが検知・保護できれば、現実世界においても類似の攻撃を阻止できる見込みが十分にあります。仮にテストに失敗した場合は、ハッカーを打ち破れるというセキュリティベンダーの大袈裟な宣伝文句を疑うべきかもしれません。

APT グループの詳細は、**4. 脅威インテリジェンス**（13 ページ）を参照ください。

ハッカー vs ターゲット

攻撃者/ APT グループ	手法	ターゲット	内容
FIN7 & Carbanak			スクリプトへの隠ぺいされたリンクが含まれるドキュメント
FIN4			中間者タイプのスピアフィッシング攻撃
FIN10			公開されている攻撃ツールとスピアフィッシングメールの組み合わせ
Silence			スクリプト、リンク、エクスプロイトを含むドキュメント

記号

2. 総合的な精度評価

エンドポイントセキュリティ製品の有効性評価は複雑な作業であり、その能力を評価する際は多数の要素が影響します。理解しやすくするため、レポートに含まれるさまざまな結果を簡潔な表にまとめました。

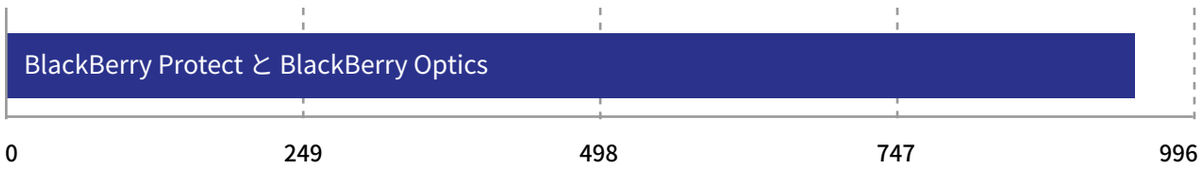
下の表は、脅威に対する製品の検知能力と保護能力だけでなく、Web アドレス（URL）やアプリケーションなどの合法的なオブジェクトを扱う能力も考慮されています。

補足すると、保護能力と検知能力がすべて同等とは限りません。製品によっては、URL を完全にブロックし、一連の有害な活動を試みる前に脅威を阻止できるものもあります。一方で、Web ベースのエクスプロイトの実行は防げないが、ターゲットにコードを追加でダウンロードすることは予防できる製品もあります。また、ターゲット上でのマルウェアの実行を短時間許すものの、その動作を検知して、コードを削除したり、後の解析のためにコードを安全な「隔離」エリアに移動させたりする製品もあります。最終評価を構成する点数の根拠を検討する際は、こうした結果を考慮します。

たとえば、最終的に脅威を阻止できたとしても一時的に脅威の実行を許した製品は、脅威を完全にブロックできた製品より評価が低くなります。また、マルウェアの感染をまったく阻止できなかった製品や、使用頻度の高い合法的なアプリケーションをブロックした製品は、大きく減点されます。

起こりうる侵害に対する製品の対処能力を評価するには、きめ細かい手法が必要です。その概要は、**3. 対処の詳細**（11 ページ）を参照ください。

総合的な精度評価			
製品	**総合的な精度評価**	**総合的な精度（%）**	**アワード**
BlackBerry Protect と BlackBerry Optics	946	95%	**AAA**



総合的な精度評価には保護結果と偽陽性が反映されています。

侵害対処テスト、保護モード：BlackBerry Protect と BlackBerry Optics

3. 対処の詳細

このテストでは、セキュリティ製品に対して複数の段階から成る攻撃を仕掛けます。完璧な製品であれば、攻撃に直接関連するすべての要素を検知・保護できるはずです。ここで重要なのは、「直接関連する」という点です。なぜなら、初期段階で攻撃を完全に阻止できれば、それ以降の段階に対処する必要はありません。

各テストケースでは、攻撃を正常に検知してシステムを悪影響から保護できれば、最大 4 ポイントが与えられます。また、なんらかの形で最善の対応を取れなければ、最大ー 9 ポイントのペナルティが課されます（すなわち、合計ー 5 ポイント）。ペナルティの大きさは次のルールに従います。このルールから分かるように、攻撃の各段階で製品が予防に失敗すると、複数のペナルティが課されます。

検知（ー 0.5）
製品が脅威の検知に失敗し、有用な情報をまったく得られなかった場合、0.5 ポイントのペナルティが課されます。

実行（ー 0.5）
脅威の実行を許すと、0.5 ポイントのペナルティが課されます。

活動（ー 1）
攻撃が 1 つ以上の活動を実行し、ターゲットの遠隔操作に成功すると、追加で 1 ポイントのペナルティが課されます。

権限昇格（ー 2）
攻撃による被害の深刻さが増すほど、ペナルティも重くなります。攻撃者がシステムの権限昇格を行えるようになると、追加で 2 ポイントのペナルティが課されます。

権限昇格後の活動（ー 1）
権限昇格によって、より強力で検知の難しい活動が可能になります。こうした活動に成功すると、さらに 1 ポイントのペナルティが課されます。

水平移動（ー 2）
攻撃者はターゲットを踏み台にして、他の脆弱なシステムへの移動を試みる場合があります。成功した場合、追加で 2 ポイントのペナルティが課されます。

水平活動（ー 2）
新しいターゲットでの活動に成功すると、攻撃者の影響はネットワーク全体に及びます。よって、製品には追加で 2 ポイントのペナルティが課されます。

保護評価は、最終的なポイントを 4 倍した値です。弊社が使用する重みづけシステムは、読者のリスクに対する受け止め方と、さまざまなレベルの保護をどう評価するかに応じて、調整できます。ペナルティレベルと総合的な保護の重みづけを変更することで、各読者の評価システムに適合させることが可能です。

総合保護評価を計算するには、まず保護に成功したテストケースの数を 4 倍（デフォルトの最大スコア）し、ペナルティを反映します。さらに合計を 4 倍（保護評価の重み値）した値が、総合保護評価です。

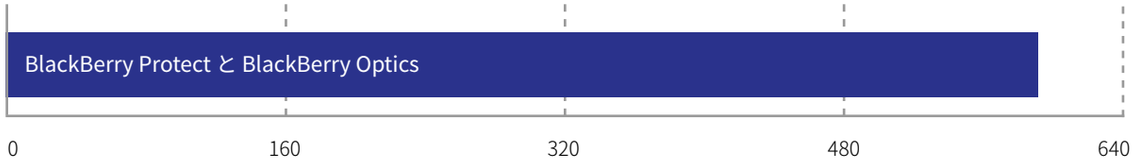
対処の詳細											
攻撃者 /APT グループ	テストケース数	検知	配布	実行	活動	権限昇格	権限昇格後の活動	水平移動	水平活動	保護成功	ペナルティ
FIN7 & Carbanak	13	13	0	13	0	0	0	0	0	13	10
FIN4	12	12	0	12	0	0	0	0	0	12	2
FIN10	9	9	0	9	0	0	0	0	0	9	7
Silence	6	6	0	6	0	0	0	0	0	6	6
総計	**40**	**40**	**0**	**40**	**0**	**0**	**0**	**0**	**0**	**40**	**25**

このデータは、各 APT グループのさまざまな攻撃段階に対する製品の対処能力を示すものです。「配布」から「水平活動」の列は、攻撃者が目標を達成した回数を示します。すなわち、「0」が理想です。

保護精度評価の詳細					
攻撃者 /APT グループ	テスト ケース数	保護成功	ペナルティ	保護スコア	保護評価
FIN7 & Carbanak	13	13	10	47	188
FIN4	12	12	2	47	188
FIN10	9	9	7	32.5	130
Silence	6	6	6	21	84
総計	**40**	**40**	**25**	**147.5**	**590**

保護評価の算出には、さまざまなレベルの保護結果と、保護に失敗した結果を使用します。

保護精度評価		
製品	保護精度評価	保護精度評価（%）
BlackBerry Protect と BlackBerry Optics	590	92%



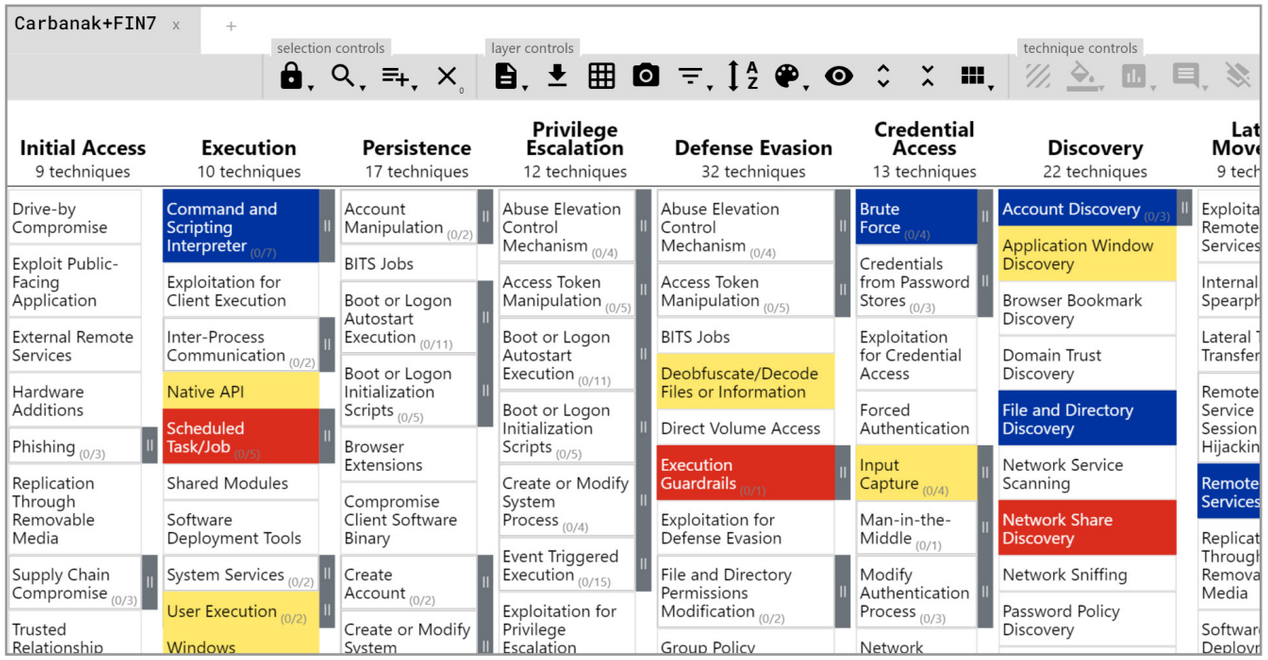
単なる成功 / 失敗ではなく、製品の脅威対処能力の微妙な違いを示せるように、保護評価は重みづけされています。

4. 脅威インテリジェンス

FIN7

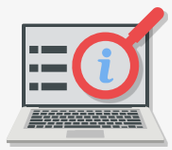
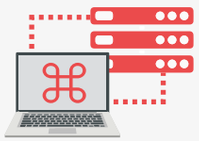
FIN7 は小売業界、飲食業界、ホテル業界をターゲットとしたスピアフィッシング攻撃を用いるグループです。攻撃には、顧客からの苦情や、履歴書、料理の注文を装った、Word 形式や RTF 形式のドキュメントを使用します。ドキュメントに含まれる隠ぺいされたリンクをクリックすると、悪意のある（VBS）コードが実行されます。

参照資料：
https://attack.mitre.org/groups/G0046/



攻撃手法は
MITRE ATT&CK
フレームワークで
文章化されています。

FIN7 による攻撃の例

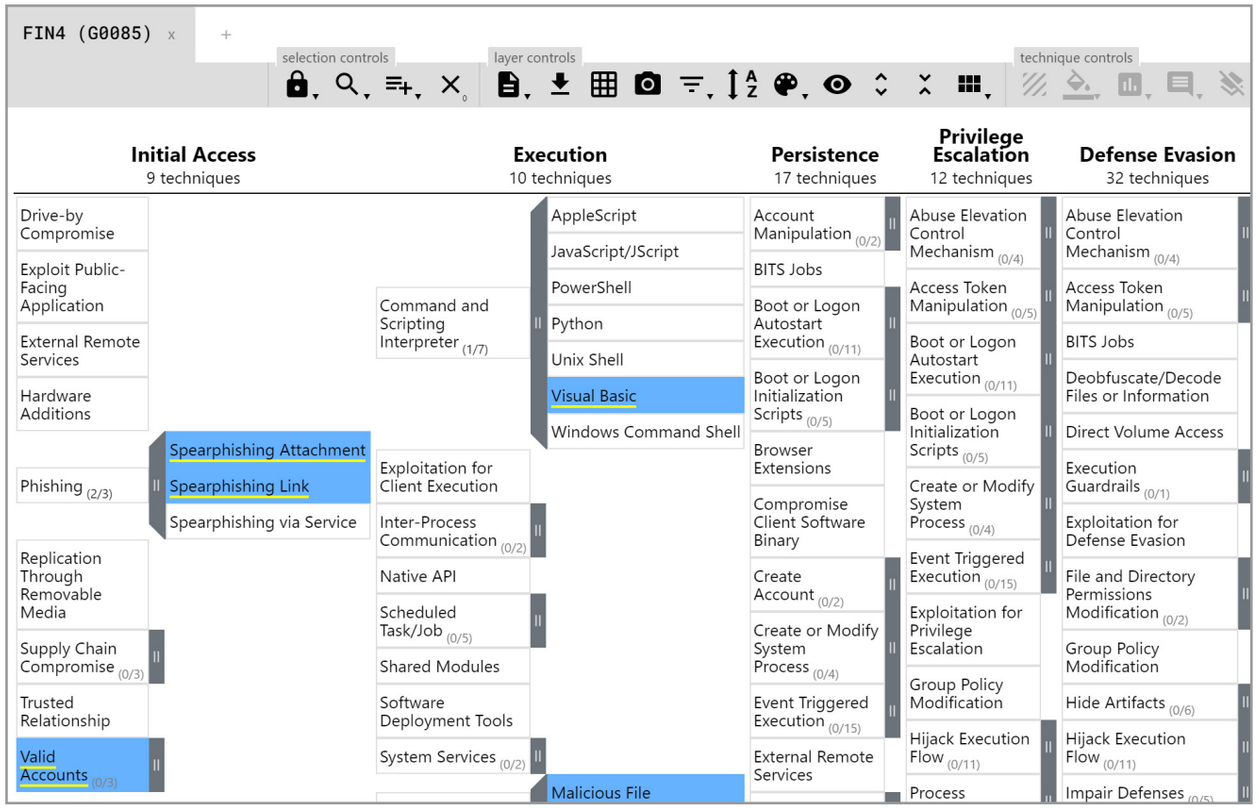
初期アクセス	実行	永続化	権限昇格	防御回避	認証情報へのアクセス	探索	水平移動	収集	コマンドアンドコントロール	流出
スピアフィッシングの添付ファイル	コマンドラインインターフェイス	レジストリ Run キー / スタートアップフォルダー	UAC 回避	コードサイニング	ブルートフォース	ファイルとディレクトリの探索	リモートデスクトッププロトコル	ローカルシステムのデータ	一般的に使用されるポート	圧縮データ
	サービス実行	正規アカウント		セキュリティツールの無効化	Web ブラウザの認証情報	プロセス探索		ステージングされたデータ	標準的な非アプリケーション層プロトコル	暗号化データ
	ユーザーによる実行			マスカレーディング		システム情報の探索		スクリーンキャプチャ	リモートアクセスツール	コマンドアンドコントロールチャネル経由の流出
				プロセスインジェクション		クエリレジストリ				
						許可グループの探索				
						システムネットワーク設定の探索				
 電子メールリンク - ファイルレス攻撃	 サービス実行	 正規アカウント	 UAC 回避	 セキュリティツールの無効化	 Web ブラウザの認証情報	 システム情報探索	 リモートデスクトッププロトコル	 スクリーンキャプチャ	 リモートアクセスツール	 コマンドアンドコントロールチャネル経由の流出

FIN4

このグループはターゲットから正規の Office ドキュメントを盗み、有害なマクロを埋め込みます。

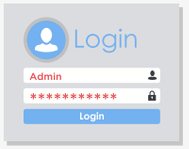
侵害したアカウントから盗まれた、本物の情報を含む正しい形式のドキュメントを使用するため、メールの受信者が騙されてドキュメントを開き、システムを侵害される可能性が高くなります。

参照資料：
https://attack.mitre.org/groups/G0085/



攻撃手法は
MITRE ATT&CK
フレームワークで
文章化されています。

FIN4 による攻撃の例

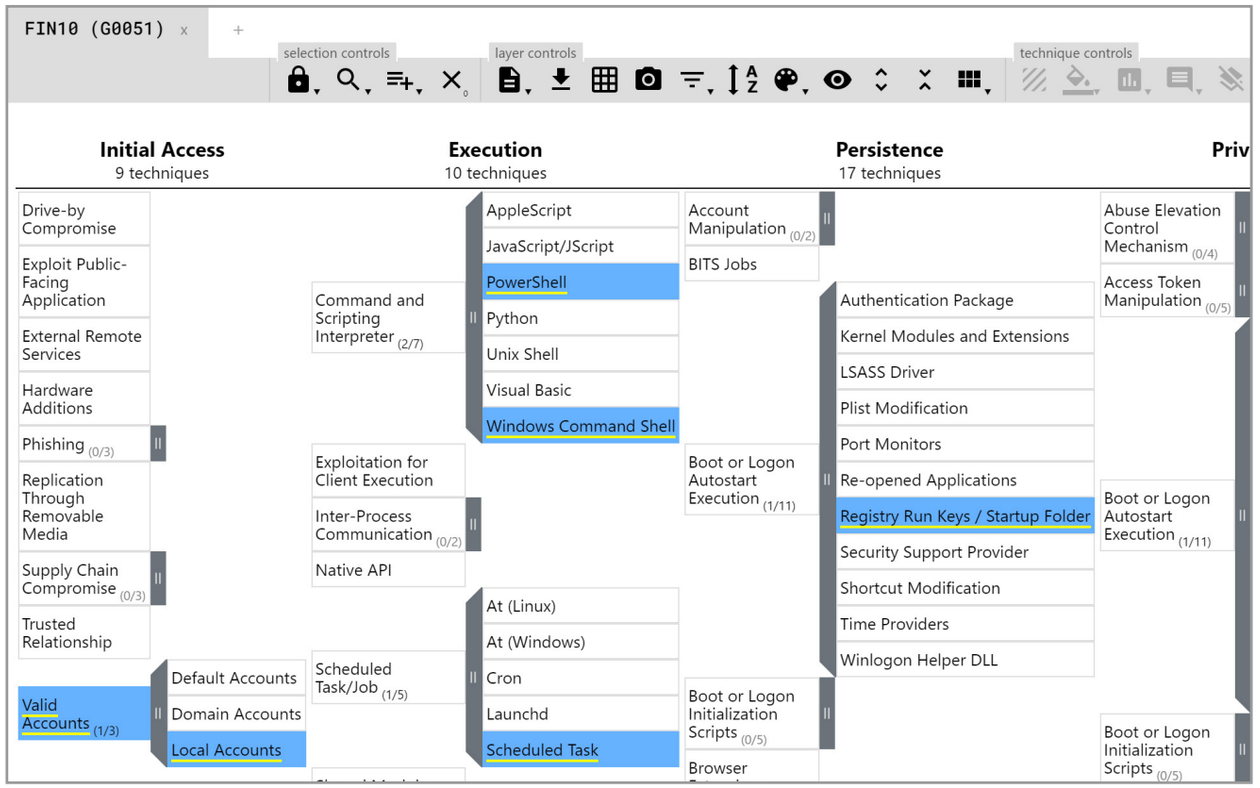
初期アクセス	実行	永続化	権限昇格	防御回避	認証情報へのアクセス	探索	水平移動	収集	コマンドアンドコントロール	流出
スピアフィッシングのリンク	スケジュール済みタスク	スケジュール済みタスク	正規アカウント	ソフトウェアパッキング	入力キャプチャ	アカウントの探索	Pass the Hash 攻撃	画像キャプチャ	一般的に使用されないポート	圧縮データ
	ユーザーによる実行				入力プロンプト	ファイルとディレクトリの探索			データ符号化	暗号化データ
						プロセス探索				コマンドアンドコントロールチャネル経由の流出
						システム情報の探索				
										
電子メールリンク - ファイルレス攻撃	ユーザーによる実行	スケジュール済みタスク	正規アカウント	ソフトウェアパッキング	入力プロンプト	システム情報の探索	Pass the Hash 攻撃	画像キャプチャ	データ符号化	暗号化データ

FIN10

この攻撃グループは公に知られたツールと手法を用いて、カナダを拠点とするカジノと天然ガス企業を攻撃しました。その目的は、盗んだデータを公開すると脅して、金銭を恐喝することです。

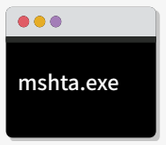
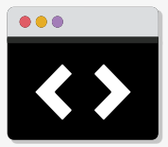
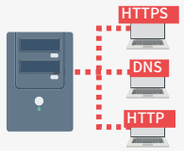
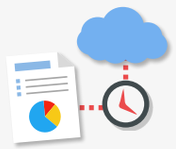
攻撃には、Metasploit、Powershell スクリプト、SplinterRat リモートアクセスツールを組み合わせたスピアフィッシングメールが使用されます。

参照資料：
https://attack.mitre.org/groups/G0051/



攻撃手法は MITRE ATT&CK フレームワークで文章化されています。

FIN10 による攻撃の例

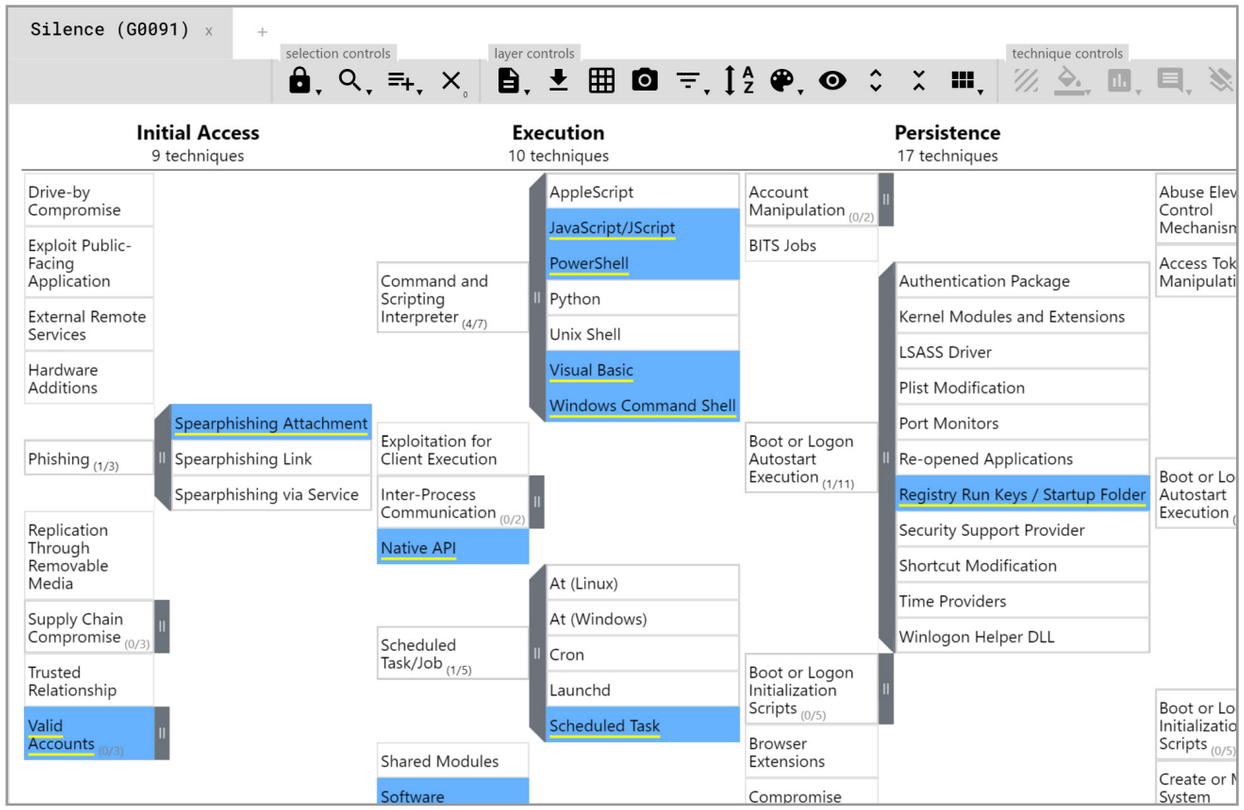
初期アクセス	実行	永続化	権限昇格	防御回避	認証情報へのアクセス	探索	水平移動	収集	コマンドアンドコントロール	流出
スピアフィッシングのリンク	mshta	レジストリ Run キー / スタートアップフォルダー	スケジュール済みタスク	スクリプティング	FIN10 に対する調査では認証情報へのアクセスは確認されていません。	アカウントの探索	リモートデスクトッププロトコル	自動収集	一般的に使用されるポート	定期送信
	スクリプティング		正規アカウント			ファイルとディレクトリの探索				
	ユーザーによる実行					プロセス探索				
						システム情報の探索				
						システム所有者 / ユーザーの探索				
										
電子メールリンク - ファイルレス攻撃	mshta	レジストリ Run キー / スタートアップフォルダー	正規アカウント	スクリプティング		プロセス探索	リモートデスクトッププロトコル	自動収集	一般的に使用されるポート	定期送信

Silence

Silence グループは、主にスクリプトベースの攻撃を行うグループであり、.CHM ファイルと .LNK ファイルの他に、マクロやその他のエクスプロイトを悪用します。攻撃には悪意のある Microsoft Office ドキュメントが使用され、金融機関がターゲットとなります。

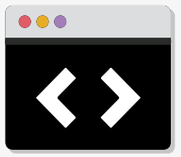
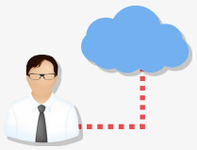
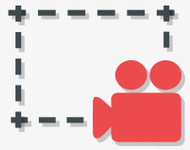
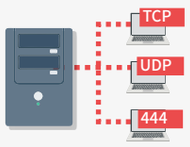
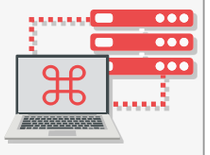
狙われた金融機関は世界各国に存在しますが、これまでのところ、東欧諸国を中心に ATM をターゲットとした攻撃が行われています。

参照資料：
https://attack.mitre.org/groups/G0091/



攻撃手法は
MITRE ATT&CK
フレームワークで
文章化されています。

Silence による攻撃の例

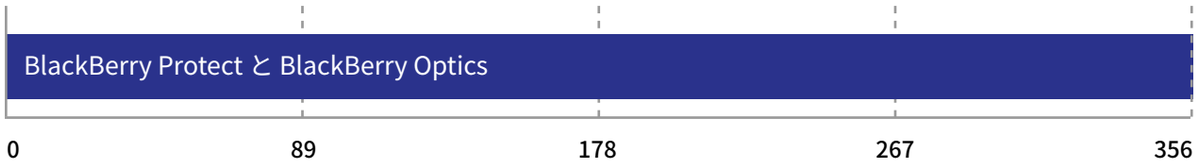
初期アクセス	実行	永続化	権限昇格	防御回避	認証情報へのアクセス	探索	水平移動	収集	コマンドアンドコントロール	流出
スピアフィッシングの添付ファイル	スクリプティング	スケジュール済みタスク	スケジュール済みタスク	ファイル削除	Silence に対する調査では認証情報へアクセスする手法は確認されていません。	ネットワーク共有の探索	Windows の管理共有	動画キャプチャ	一般的に使用されないポート	コマンドアンドコントロールチャネル経由の流出
	サービス実行			難読化されたファイルや情報		リモート共有の探索				
	ユーザーによる実行			スクリプティング						
										
電子メールリンク - ファイルレス攻撃	スクリプティング	スケジュール済みタスク	スケジュール済みタスク	ファイル 削除		ネットワーク共有の探索	Windows の管理共有	動画 キャプチャ	一般的に使用されないポート	コマンドアンドコントロールチャネル経由の流出

5. 合法的なソフトウェアに対する評価

この評価は、製品が合法的なアプリケーションと URL を分類する精度を示すものであり、製品がユーザーに与えた影響も考慮されます。理想的には、製品が合法的なオブジェクトを有害と分類しないか、無害と分類することが望まれます。さもなければ、ユーザーに負担をかけることになります。

また、評価にはこのテストで使用されたアプリケーションと Web サイトの普及状況（人気）が反映されており、非常に利用者の多いソフトウェアや Web サイトの分類に失敗すると、厳しいペナルティが課されます。

合法的なソフトウェアに対する評価		
製品	誤検知回避 精度評価	誤検知回避 精度（%）
BlackBerry Protect と BlackBerry Optics	356	100%



合法的なソフトウェアに対する評価は、ベンダーが検知エンジンを適切に調整できているかを示します。

6. 結論

今回のテストでは、BlackBerry Protect と BlackBerry Optics に対してエクスプロイト攻撃、ファイルレス攻撃、マルウェア添付ファイルといった多様な攻撃を行いました。このテストには、現在公開されているテストの中でも最も幅広い脅威が含まれます。

使用した攻撃はいずれも、ここ数年で実際に確認されたタイプの攻撃です。これらは現実に世界各地のネットワークを脅かしている、最新の脅威に対処します。また、このテストで使用した脅威は、**ハッカー vs ターゲット**（9 ページ）と、**4. 脅威インテリジェンス**（13 ～ 16 ページ）に記載した脅威グループが用いる脅威と類似または同一です。

留意点として、使用した攻撃の種類は同じでも、ファイルは新しいものを使用しています。これは、システムを攻撃する特定のアプローチに対する、テスト対象製品の検知能力と保護能力を実証するためです。単に、過去数年で確認された有害なファイルを検知する能力を試すわけではありません。その結果、製品が過去の攻撃を検知できるかを試した単なるコンプライアンスチェックの結果ではなく、今後発生しうる攻撃に対する製品の能力の指標が得られます。

この製品は、すべての脅威を完全に検知・保護することに成功しました。どのテストケースでも、攻撃チェーンの最初の段階で脅威が阻止されました。すなわち、ターゲットのシステムが脅威にさらされると、即座に攻撃を検知して実行を阻止しています。そのため、データ盗難などの被害はまったく発生していません。

この製品は優れた成果を収めました。試験者がターゲットに対するハッキングを開始できる地点まで進行した攻撃は 1 つもありません。製品の中には、過剰に積極的で脅威と合法的なオブジェクトを区別せず検知してしまう製品もあります。期待通り、BlackBerry Protect と BlackBerry Optics のテストでは、このような偽陽性は発生していません。BlackBerry Protect と BlackBerry Optics は、卓越したパフォーマンスによって AAA アワードを勝ち取ったのです。

付録

付録 A：用語集

用語	意味
侵害された	攻撃に成功し、ターゲット上で妨害を受けずにマルウェアを実行できたことを意味します。標的型攻撃の場合、攻撃者が妨害を受けずにシステムを遠隔操作して、さまざまなタスクを実行できたことを意味します。
ブロックされた	攻撃によるターゲットの改変を予防したことを意味します。
偽陽性	セキュリティ製品が合法的なアプリケーションや Web サイトを誤って有害と分類した場合、「偽陽性」の結果を出力したと見なされます。
無力化された	ターゲット上でエクスプロイトやマルウェアペイロードが実行されたが、その後削除されたことを意味します。
完全修復	セキュリティ製品が攻撃に関する重要な痕跡をすべて削除した場合、完全修復を達成したと見なされます。
ターゲット	セキュリティ製品によって保護されたテスト用システムを意味します。
脅威	なんらかのレベルでターゲットのコントロールを不正に取得することを目的に設計された、ターゲットに対する一連の活動や、プログラムを指します。
更新	最新の脅威に対処するため、セキュリティベンダーが製品に情報を提供することを意味します。こうした更新は、1 つ以上のファイルとしてまとめてダウンロードされる場合もあれば、個別に要求され、インターネット経由で配信される場合もあります。

付録 B：FAQ

このテストで使用した手法の詳細は、弊社の Web サイトを参照ください。

- このテストは、2021 年 4 月 7 日から 2021 年 5 月 11 日の間に実施されました。
- テストした製品は、ベンダーの推奨に従って設定されました。
- 標的型攻撃は SE Labs が選択して検証しました。
- 有害なデータと合法的なデータは、テスト完了後にパートナー組織に提供されました。
- このエンドポイントセキュリティテストは、仮想マシンではなく物理 PC 上で実施されました。

Q パートナー組織とは？私もパートナー組織になって、このテストで使用された脅威データにアクセスできますか？

A パートナー組織は、テストの実行後に弊社のコンサルタントサービスの恩恵を受けられます。さらに、製品の改善に向けた取り組みに活用できる、低レベルデータへのアクセスを許可されます。必要に応じて、マーケティング用途に受賞ロゴを使用することも可能です。あるパートナーのデータを、弊社が他のパートナーと共有することはありません。また、テストに参加していない組織をパートナー組織に認定することもありません。

Q エンドポイント保護製品や、エンドポイント検知・対処（EDR）製品の購入や変更を検討しています。支援を受けられますか？

A はい、弊社ではセキュリティ製品の変更を検討している組織を対象に、プライベートテストを頻繁に実施しています。詳細は、info@selabs.uk までご相談ください。

付録 C：攻撃の詳細

FIN7											
インシデント No.	**初期アクセス**	**実行**	**永続化**	**権限昇格**	**防御回避**	**認証情報へのアクセス**	**探索**	**水平移動**	**収集**	**コマンドアンドコントロール**	**流出**
1	スピアフィッシングの添付ファイル	コマンドラインインターフェイス	新規サービス	UAC 回避	難読化されたファイルや情報	認証情報のダンプ	アカウントの探索	リモートファイルコピー	ローカルシステムのデータ	一般的に使用されるポート	圧縮データ
		PowerShell	スケジュール済みタスク	正規アカウント	レジストリの変更	入力キャプチャ	ファイルとディレクトリの探索	Pass the Hash 攻撃	ステージングされたデータ	標準的なアプリケーション層プロトコル	暗号化データ
		スクリプティング			ファイル削除		プロセス探索		入力キャプチャ	標準的な暗号化プロトコル	コマンドアンドコントロールチャネル経由の流出
		リモートファイルコピー			プロセスハロウイング		クエリレジストリ				
		ユーザーによる実行			仮想化 / サンドボックスの回避		システム情報の探索				
							システム所有者 / ユーザーの探索				
2	スピアフィッシングの添付ファイル	コマンドラインインターフェイス	レジストリ Run キー / スタートアップフォルダー	UAC 回避	コードサイニング	ブルートフォース	ファイルとディレクトリの探索	リモートデスクトッププロトコル	ローカルシステムのデータ	一般的に使用されるポート	圧縮データ
		サービス実行	正規アカウント		セキュリティツールの無効化	Web ブラウザの認証情報	プロセス探索		ステージングされたデータ	標準的な非アプリケーション層プロトコル	暗号化データ
		ユーザーによる実行			マスカレーディング		システム情報の探索		スクリーンキャプチャ	リモートアクセスツール	コマンドアンドコントロールチャネル経由の流出
					プロセスインジェクション		クエリレジストリ				
							許可グループの探索				
							システムネットワーク設定の探索				
3	スピアフィッシングの添付ファイル	コマンドラインインターフェイス	アプリケーション Shim の利用	UAC 回避	ファイルや情報の難読化解除	ブルートフォース	ファイルとディレクトリの探索	リモートファイルコピー	ローカルシステムのデータ	一般的に使用されるポート	圧縮データ
		mshta			実行ガードレール	認証情報のダンプ	プロセス探索	Pass the Hash 攻撃	ステージングされたデータ	接続ポリシー	暗号化データ
		ユーザーによる実行			ソフトウェアパッキング		システム情報の探索	Windows の管理共有		標準的な非アプリケーション層プロトコル	コマンドアンドコントロールチャネル経由の流出
		スクリプティング					ネットワーク共有の探索				
							システムネットワーク設定の探索				
							システム所有者 / ユーザーの探索				
							アカウントの探索				

FIN7

インシデント No.	初期アクセス	実行	永続化	権限昇格	防御回避	認証情報へのアクセス	探索	水平移動	収集	コマンドアンドコントロール	流出
4	スピアフィッシングの添付ファイル	コマンドラインインターフェイス	フッキング	DLL 検索順のハイジャック	間接コマンド実行（新規）	フッキング	ファイルとディレクトリの探索	Windows Management Instrumentation（新規）	ローカルシステムのデータ	一般的に使用されるポート	圧縮データ
		PowerShell			ファイル削除	入力キャプチャ	プロセス探索		ステージングされたデータ	標準的なアプリケーション層プロトコル	暗号化データ
		スクリプティング			実行ガードレール		システム情報の探索			標準的な暗号化プロトコル	コマンドアンドコントロールチャネル経由の流出
		コンポーネントオブジェクトモデル（COM）と分散 COM					アプリケーションウィンドウの探索				
		API 経由実行					許可グループの探索				
							ネットワーク共有の探索				

FIN4

インシデント No.	初期アクセス	実行	永続化	権限昇格	防御回避	認証情報へのアクセス	探索	水平移動	収集	コマンドアンドコントロール	流出
5	スピアフィッシングの添付ファイル	スクリプティング	新規サービス	正規アカウント	スクリプティング	入力キャプチャ	アカウントの探索	リモートデスクトッププロトコル	電子メール取集	一般的に使用されるポート	自動流出
		ユーザーによる実行				入力プロンプト	ファイルとディレクトリの探索			標準的なアプリケーション層プロトコル	代替プロトコル経由の流出
							プロセス探索				データ送信サイズの制限
							システム情報の探索				
6	スピアフィッシングのリンク	スケジュール済みタスク	スケジュール済みタスク	正規アカウント	ソフトウェアパッキング	入力キャプチャ	アカウントの探索	Pass the Hash 攻撃	画像キャプチャ	一般的に使用されないポート	圧縮データ
		ユーザーによる実行				入力プロンプト	ファイルとディレクトリの探索			データ符号化	暗号化データ
							プロセス探索				コマンドアンドコントロールチャネル経由の流出
							システム情報の探索				
7	スピアフィッシングの添付ファイル	Regsvcs/Regasm	新規サービス	正規アカウント	プロセスインジェクション	入力キャプチャ	アカウントの探索	リモートファイルコピー	画像キャプチャ	標準的なアプリケーション層プロトコル	定期送信
		ユーザーによる実行				入力プロンプト	ファイルとディレクトリの探索			プロセスインジェクション	代替プロトコル経由の流出
							プロセス探索			一般的に使用されるポート	
							システム情報の探索				
8	スピアフィッシングのリンク	スクリプティング	スタートアップアイテム	正規アカウント	スクリプティング	入力キャプチャ		リモートファイルコピー	電子メール取集	一般的に使用されないポート	圧縮データ
		ユーザーによる実行				入力プロンプト				Web サービス	暗号化データ
											コマンドアンドコントロールチャネル経由の流出

FIN10											
インシデント No.	**初期アクセス**	**実行**	**永続化**	**権限昇格**	**防御回避**	**認証情報へのアクセス**	**探索**	**水平移動**	**収集**	**コマンドアンドコントロール**	**流出**
9	スピアフィッシングの添付ファイル	ユーザーによる実行	スケジュール済みタスク	スケジュール済みタスク 正規アカウント	ファイル削除	FIN10 に対する調査では認証情報へのアクセスは確認されていません。	アカウントの探索 ファイルとディレクトリの探索 プロセス探索 システム情報の探索 システム所有者 / ユーザーの探索	リモートファイルコピー	ローカルシステムのデータ ステージングされたデータ	一般的に使用されるポート	コマンドアンドコントロールチャネル経由の流出
10	スピアフィッシングのリンク	mshta スクリプティング ユーザーによる実行	レジストリ Run キー / スタートアップフォルダー	スケジュール済みタスク 正規アカウント	スクリプティング	FIN10 に対する調査では認証情報へのアクセスは確認されていません。	アカウントの探索 ファイルとディレクトリの探索 プロセス探索 システム情報の探索 システム所有者 / ユーザーの探索	リモートデスクトッププロトコル	自動収集	一般的に使用されるポート	定期送信
11	スピアフィッシングのリンク	PowerShell スクリプティング Regsvcs/Regasm ユーザーによる実行	スケジュール済みタスク	スケジュール済みタスク 正規アカウント	Regsvcs/Regasm スクリプティング	FIN10 に対する調査では認証情報へのアクセスは確認されていません。	アカウントの探索 ファイルとディレクトリの探索 プロセス探索 システム情報の探索 システム所有者 / ユーザーの探索	リモートファイルコピー	自動収集	一般的に使用されるポート	定期送信

Silence											
インシデント No.	**初期アクセス**	**実行**	**永続化**	**権限昇格**	**防御回避**	**認証情報へのアクセス**	**探索**	**水平移動**	**収集**	**コマンドアンドコントロール**	**流出**
12	スピアフィッシングの添付ファイル	コマンドラインインターフェイス コンパイルされた HTML ファイル API 経由実行 ユーザーによる実行	スケジュール済みタスク	スケジュール済みタスク	コンパイルされた HTML ファイル ファイル削除	Silence に対する調査では認証情報へアクセスする手法は確認されていません。	ネットワーク共有の探索 リモート共有の探索	Windows の管理共有	スクリーンキャプチャ	一般的に使用されるポート	コマンドアンドコントロールチャネル経由の流出
13	スピアフィッシングの添付ファイル	スクリプティング サービス実行 ユーザーによる実行	スケジュール済みタスク	スケジュール済みタスク	ファイル削除 難読化されたファイルや情報 スクリプティング	Silence に対する調査では認証情報へアクセスする手法は確認されていません。	ネットワーク共有の探索 リモート共有の探索	Windows の管理共有	動画キャプチャ	一般的に使用されないポート	コマンドアンドコントロールチャネル経由の流出

SE Labs

SE Labs レポートの免責条項

1. 本レポートに含まれる情報は、通知なしで SE Labs により変更および改訂されることがあります。
2. SE Labs は、いかなる時点でも本レポートを更新する義務を負いません。
3. SE Labs は、本レポートに含まれる情報が、本文のページ下部に示される公開の時点で正確であり、信頼性が高いと確信していますが、SE Labs は、いかなる意味でもこれを保証しません。
4. 本レポートまたは本レポートに含まれる情報を利用し、またはこれに依拠することは、読者自身のみのリスクで行ってください。SE Labs は、何らかの意味で本レポートに起因するいかなる逸失利益（直接的または間接的のいずれによって発生したかを問わない）、信用もしくはビジネス上の評判の損失、被害を受けたデータの損失、純粋な経済的損失、代替的な商品もしくはサービスの調達コスト、その他の無形の損失、または間接的、付随的、特別もしくは結果的な損失、費用、損害賠償、請求、経費もしくは懲罰的な損害賠償に対しても責任を負いません。
5. 本レポートの内容は、列挙、言及またはテストされたいずれかの製品の推奨、保証、支持またはその他に当たるものではありません。
6. テストおよびその後の結果によって、製品にエラーのないこと、または読者によって同一もしくは類似の結果が得られることは保証されません。SE Labs は、製品が読者の期待、要件、仕様またはニーズを満たすことをいかなる意味でも保証しません。
7. 本レポートで使用されるすべての商標、商用名、ロゴまたは画像は、それぞれの所有者の商標、商用名、ロゴまたは画像です。
8. 本レポートの内容は「現状有姿」ベースで提供されます。したがって SE Labs は、その正確性または完全性に関して明示的または黙示的ないかなる保証または表明も行いません。