



Security. Certified.

エンドポイント セキュリティ
ソーシャル エンジニアリングを悪用したマルウェア対策
比較テストの結果

コンシューマー製品

AVG
ESET NOD32
F-SECURE
KASPERSKY
McAFEE

NORMAN
NORTON
PANDA
TREND MICRO



テスト手法バージョン: 1.2
2009年9月8日

NSS Labs 発行。

© 2009 NSS Labs

連絡先:

P.O. Box 130573
Carlsbad, CA 92013

電話: +1.512.961.5300
電子メール: info@nsslabs.com
インターネット: <http://www.nsslabs.com>

無断複写・転載を禁じます。著者の書面による承諾なしに、本書のいかなる部分も複製、複写、検索システムへの記録、または変換を行うことはできません。

このレポートへのアクセスまたは使用は、次の各項目に従うことを条件にしています。

1. 本レポートに記載されている情報は予告なしに NSS Labs によって変更される場合があります。
2. NSS Labs では、本レポートの情報について正確性および信頼性を期していますが、保証するものではありません。本レポートの使用および信頼性については、お客様ご自身の責任でなされるものとします。NSS Labs は、本レポートの過失に起因するいかなる損害、損失、費用について、いかなる責任も負いません。
3. NSS Labs は、いかなる明示もしくは黙示の保証も行いません。商品性、特定目的適合性に関する黙示の保証および法律上の瑕疵担保責任の保証の適用も一切ありません。NSS Labs はいかなる派生的損害、付随的損害または間接的損害、あるいは利益、収益、データ、コンピュータプログラム、または、他の資産の逸失について、予見の有無を問わず、一切の責任を負わないものとします。
4. 本レポートは、テストを実施した製品 (ハードウェアまたはソフトウェア)、あるいは製品テストの際に使用したハードウェアおよびソフトウェアを推奨または保証するものではありません。テストでは、製品にエラーや欠陥がないこと、製品がお客様の期待、要件、ニーズ、仕様を満たしていること、または製品が中断なく稼動することなどを保証していません。
5. 本レポートで使用されているすべての商標、サービス マーク、商号は、それぞれの所有者の商標、サービス マーク、商号であり、あらゆるテスト、本レポートまたは NSS Labs が黙示的に、あるいは架空にも保証、支援、提携、介入するものではありません。

エグゼクティブ サマリー

NSS Labs の実施する一連のテストは第一に、エンドポイント対策製品の防御能力を検証するもので、このレポートではソーシャルエンジニアリングを悪用したマルウェアを検証します。これに続くレポートでは、フィッシングとエクスプロイトに対する防御力を検証します。

ソーシャルエンジニアリングを悪用したマルウェアは別のソフトウェアパッケージに偽装および/または隠匿されており、ユーザーがソフトウェアをダウンロードおよびインストールするように仕向けることで、同時にマルウェアがインストールされるようになっていきます。ソーシャルエンジニアリングを悪用したマルウェアによる攻撃は、機密情報を危険にさらしたり、損失、または漏えいの脅威にさらすことで、個人および組織に多大な危険性をもたらします。50%以上のマルウェアがWeb経由で持ち込まれることから、このような脅威から身を守るためにより洗練された技術とリソースが必要になり、セキュリティ製品がデスクトップレベルで発展するきっかけとなりました。

2009年の7月から8月にかけて、NSS Labs ではソーシャルエンジニアリングを悪用したマルウェアに対して、業界でもっとも実世界に即したウイルス対策/エンドポイント対策スイートのテストを実施しました。NSS Labs の Live Testing は次に示すように、ユーザーが実際に遭遇する可能性の高い、最新の脅威に対する防御力を検証しています。こうした意味で、他のテストに見られるような閉じたラボ環境内で、古いサンプルに対して行われるテストとは一線を画します。ここに示す結果は、17日間連続のテスト期間中、8時間ごとに実施された59回以上の個別のテストで、各回ごとに新しいマルウェア URL を追加することにより収集した経験的に評価された物証が基になっています。それぞれの製品はテスト開始の際に最新の状態に更新され、テスト実施期間中は常時、実際のインターネットにアクセスできるようにしていました。

主要な結果

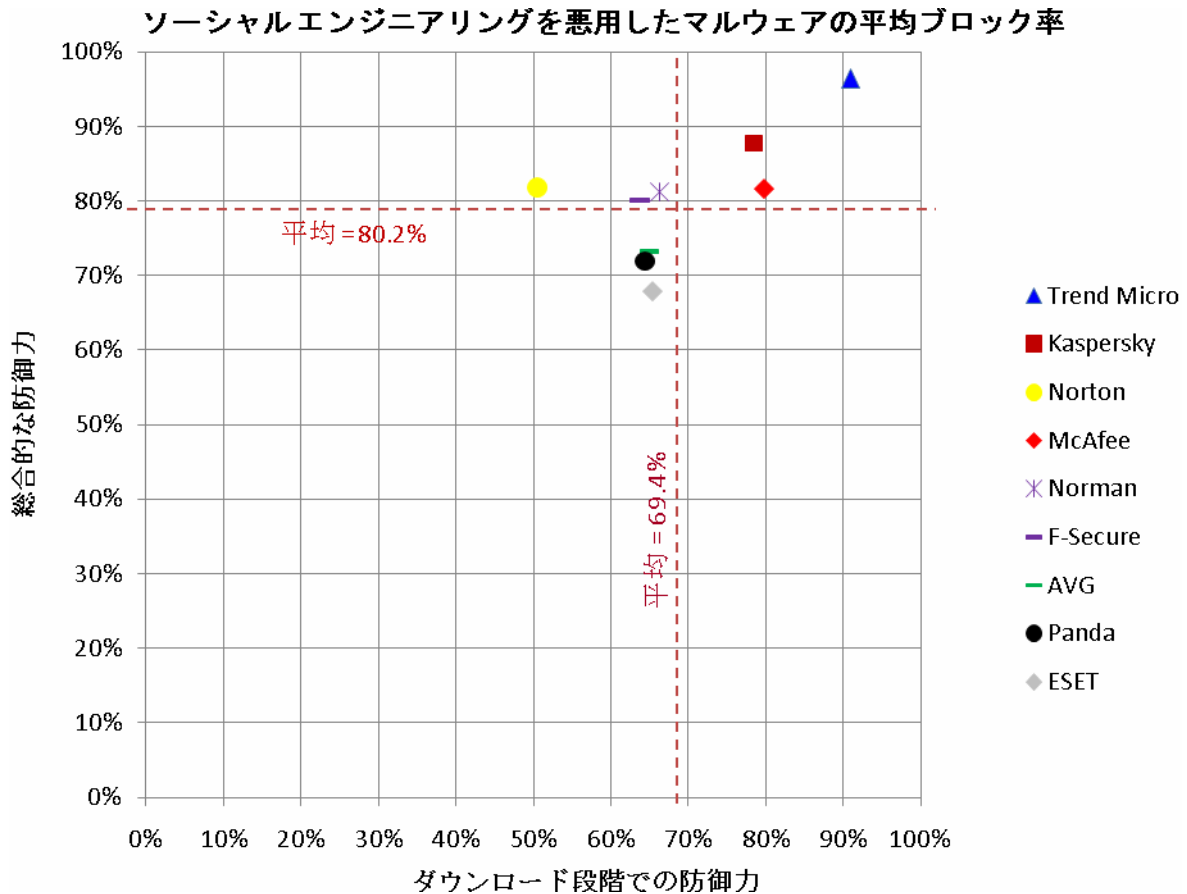
- 「クラウド」の概念を採用したレピュテーション (評価) システムは、平均して大いに安全性を向上しています。
- Trend Micro 社は全体で、最高となる 96.4% のダウンロード時および実行時の防御を達成しました。
- Kaspersky 社は全体で 87.8% のダウンロード時および実行時の防御を達成しました。
- Norton 社のビヘイビア検出による防御は、ダウンロードフェーズにおける低い防御力を補う点で卓越しています。
- McAfee 社は技術的に4位にランク付けされていますが、ブロックの速さでは他社の追随を許さず、賞賛に値します。

長期的な防御力

次の表と図は、Web ベースのマルウェアによる攻撃ベクトルに対する総合的な防御力の重要な要因を2つにまとめたものです。「ダウンロード段階での防御」により、マルウェアがマシンに侵入するのを防ぎます。この最初の防御ラインを超えたマルウェアについても、「実行段階での防御」の割合を測定しました。全体はダウンロード段階での防御と、実行段階での防御の両方から成ります。

製品	ダウンロード段階での初期防御	実行段階での防御	総合
Trend Micro	91.0%	5.5%	96.4%
Kaspersky	78.5%	9.3%	87.8%
Norton	50.5%	31.3%	81.8%
McAfee	79.8%	1.9%	81.6%
Norman	66.3%	14.9%	81.2%
F-Secure	63.7%	16.4%	80.0%
AVG	65.0%	8.3%	73.3%
Panda	64.4%	7.6%	72.0%
ESET	65.4%	2.5%	67.9%

次の図は、ダウンロード、実行および総合スコアの関係を示します。上方および右側に位置するほど優れていることを意味します。テストでは、マルウェアを最初にインターネットからダウンロードし、実行するという、実際のユーザーの行動を再現しています。ダウンロード段階での平均的な防御率は69.4%、総合での平均は80.2%でした。



製品ガイダンス

評価	製品
推奨	Trend Micro Kaspersky
中立	Norton McAfee Norman F-Secure
注意	AVG Panda Eset

目次

1	概要	1
1.1	本レポートについて.....	1
1.2	エンドポイント対策製品.....	1
1.3	ソーシャルエンジニアリングを悪用したマルウェアの脅威.....	2
1.4	「クラウド」サービス.....	3
2	Live Test 環境	4
2.1	防御の段階.....	4
2.2	防御にかかる時間と一貫性.....	5
2.3	テスト対象製品.....	5
2.4	クライアントホストの説明.....	5
2.5	ネットワークの説明.....	6
2.6	テスト構成 - 悪質な URL.....	7
3	テスト基準と結果	8
3.1	ソーシャルエンジニアリングを悪用したマルウェアを含む URL を長期間にわたってブロックする.....	8
3.2	予防型および実行段階での防御.....	9
3.3	防御にかかる時間のヒストグラム.....	9
3.4	マルウェアをブロックするまでの平均対応時間.....	11
4	製品の評価結果	12
4.1	推奨.....	12
4.2	中立.....	13
4.3	注意.....	14
5	付録 テスト プロシージャ	15
5.1	テストの期間.....	15
5.2	マルウェア URL のサンプル.....	16
5.3	URL のカタログ.....	16
5.4	サンプル URL の存在の確認.....	17
5.5	ダウンロードと実行.....	17
5.6	削除.....	18
5.7	ポストテスト検証.....	18
6	付録 C: テスト インフラストラクチャ	19

1 概要

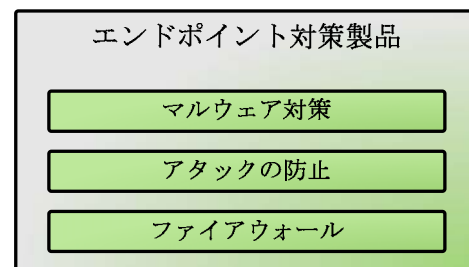
1.1 本レポートについて

NSS Labs のテスト レポートは、IT プロフェッショナルに、情報セキュリティ製品に関する実験から得られた評価データと分析情報を提供します。

このグループ テストでは、個人ユーザーおよび企業にとって最大の脅威と言えるソーシャル エンジニアリングを悪用したマルウェアに対するエンドポイント対策製品のセキュリティ効果を評価しました。これは、4 半期に一度実施する反復テスト シリーズの一環で、読者に製品の適合性と効率の分析結果を提供するため、頻繁に更新されます。すべてのテストは独自に行われたもので、いかなる資金提供も受けずに実施されています。

1.2 エンドポイント対策製品

NSS Labs では、ユーザーまたは従業員がビジネス タスクを実行する上で、もっとも一般的に使用されるクライアントワークステーションを「エンドポイント」と定義付けています。エンドポイント対策は主に 3 つの機能コンポーネントから成ります。土台はクライアント (またはパーソナル) ファイアウォールで明示的に許可されている通信のみにトラフィックを制限する、肯定的なセキュリティモデルです。ファイアウォールでは、エンドポイントへの出入りが許可されるトラフィックの種類と相手を判別する大まかなルールが適用されます。そして、マルウェア対策と攻撃の防止がその他の 2 種類になります。いずれも「悪い」と定義されたコンテンツの明示リストを使用する否定的セキュリティモデル (例外ベース) がベースになっています。



「ウイルス対策」という用語は、より広い範囲の脅威を対象とした防御を取り入れるために「マルウェア対策」と呼ばれるようになりつつあります。これには、通常、ウイルス、ワーム、ルートキット、トロイの木馬、スパイウェア、アドウェア、その他の悪質なアプリケーションが含まれます。

攻撃の防止はオペレーティング システム、ドライバー、ユーザー アプリケーションの脆弱性に対するエクスプロイトからシステムを防御する技術を指します。エクスプロイトはマシンに対する各種攻撃を意味し、悪意のあるまたは汚染された Web サイトにアクセスしただけで、特に何らアクションを実行しなかった場合にも感染する恐れがあります。

エンドポイント対策製品に組み込まれつつある他の機能で、現段階では必要とされていないものに、アプリケーションのホワイト リスト、情報漏えい防止対策 (DLP : Data Leak Prevention)、およびデータ暗号化などがあります。注意:一部のホワイト リストによるアプローチでは、「マルウェア対策」製品と見なされていなくても、マルウェアに対する防御という観点での最終ゴールに到達しそうなものもあります。大規模なセキュリティ ベンダーではこのような技術を取得しようとする流れがあり、今はまさに、既存の製品への統合が図られている段階です。

1.3 ソーシャルエンジニアリングを悪用したマルウェアの脅威

ソーシャルエンジニアリングを悪用したマルウェアによる攻撃は、機密情報を危険にさらしたり、損失、または漏えいの脅威にさらすことで、個人および組織に多大な危険性をもたらします。これらは安全に見えるアプリケーションへのリンクを含む Web ページで、ソフトウェア更新、スクリーンセーバーアプリケーション、ビデオコーデックのアップグレードなどに見せかけてユーザーをだまし、ダウンロードさせるように設計されています。また、ダウンロードリンクにはコンテンツタイプが実行されるように促す、悪意のあるペイロードも含まれています。また、セキュリティの専門家はこれらの脅威に対し別の用語を使用して、合意に基づくダウンロード、危険なダウンロードとも呼んでいます。

現在、50% 以上のマルウェアが Web 経由で広められています。

Web はマルウェアをすばやく広めるため、従来のセキュリティプログラムを回避するために悪用されています。マルウェアの実に 53% がインターネットのダウンロード経路でもたらされるのに比べ、電子メールはわずか 12% にとどまり、一方で、IFrame のエクスプロイトと他の脆弱性はグローバルなマルウェアの感染ベクトルの 7%、5% に相当すると、Trend Micro 社の統計は示しています。¹

犯罪者たちは迅速な公開と匿名での利用が可能なソーシャルネットワークサイト (Facebook、MySpace、LinkedIn など) とユーザー投稿型コンテンツ (ブログ、ツイッターなど) に見られる黙示的な信頼関係を悪用しています。さらに、こうした脅威が新しい場所に「飛び火」するスピードに、セキュリティベンダー各社は手を焼き、困難を余儀なくされています。

こうした脅威の検出と防御は、犯罪者がその攻撃の手を緩めることがないため、常に困難を極めます。2008 年および 2009 年のマルウェアの増加統計から、その勢いに拍車がかかっていることがわかります。ウイルスリサーチャーは 1 日に 15,000 件から 50,000 件の悪意のある新種プログラムを検出し、Kaspersky によれば、その数は「月に数万件」にもおよぶそうです。²Eset は毎日、100,000 件以上の新種が生み出されていると述べています。³

このような脅威から身を守るには、より高度な技術とリソースが必要になり、セキュリティ製品がデスクトップレベルで発展するきっかけとなりました。

¹ マッキー クルーズ、"Most Abused Infection Vector" (もっとも悪用された感染ベクトル)。Trend Labs Malware Blog 2008 年 12 月 7 日。 <http://blog.trendmicro.com/most-abused-infection-vector/>

² ユージーン カスペルスキー:

<http://www.examiner.com/x-11905-SF-Cybercrime-Examiner-y2009m7d17-Antimalware-expert-and-CEO-Eugene-Kaspersky-talks-about-cybercrime>

³ <http://www.darkreading.com/security/client/showArticle.jhtml?articleID=219501248>

1.4 「クラウド」 サービス

セキュリティベンダー各社は、シグネチャやヒューリスティックなどのクライアント上での検出技術を補う「クラウド」コンポーネントの投入と向上を図っています。これらの新しいURLおよびファイルレピュテーション (評価) ベースのマルウェア警告システムでは、**もう 1 枚の防御レイヤ**を提供しています。

このようなレピュテーション (評価) システムはクライアントのフィードバックと Web クローラを活用し、ブラックリストかホワイトリストのいずれかに追加するか、スコアを付ける (ベンダーのアプローチの仕方による) 方法で、追加の URL およびファイルをカテゴリ化します。これは手動、自動、またはそれらの組み合わせで実行できます。エンドポイント対策製品は判別のために、固有の URL およびファイルについて「クラウド」システムのレピュテーション情報を要求できます。さらに、このデータの用途はベンダー各社の製品ごとに異なり、ユーザーに警告を発するか、ファイルのダウンロードまたは実行をブロックします。

2 LIVE TEST 環境

これらのプロシージャの目的は、制御された立証可能な方法で、マルウェア対策の実環境でのテストを提供することです。新たな脅威がインターネットを介して到達し、蔓延する速さを考慮すると、従来型のテスト技術はもはや製品の性能を評価する上で、適切とは言えません。

- ワイルドリストのサンプルに依存したテストや、100% のスコア目標を推定するテストは現在の脅威の防御力を評価するには適していません。マルウェアは新種で、これまでのマルウェアファミリーの類型ではなく、インターネットで現在広がっている種類を反映したものでなければなりません。
- テスト中にベンダーのレピュテーション システムへのアクセスを封じるテストでは、防御におけるキー コンポーネントを拒否することになり、より高度な製品を不当に不利にしています。
- 統計テストまたはオンデマンド スキャンでは、通常、もっとも堅牢な検出技術が有効になりません。また、動的テストだけではリアルタイムの「クラウド」レピュテーション システムに対し、増加しつつある信頼性を十分に与えることができません。レピュテーション/ダウンロードおよび実行の組み合わせによる分析が、実世界での製品性能を分析する上で最高と言えます。

そのため、NSS Labs では平均的なユーザー エクスペリエンスをエミュレートする、固有の「ライブクラウド」テストフレームワークを開発しました。この新しいテスト技法は、NSS Labs の広範囲なインテリジェンス ネットワークから収集した、現在、インターネット上でアクティブな脅威に焦点を当てています。反復テストでは、発見後数時間以内のマルウェアを使用して、テストを行います。

2.1 防御の段階

Web ベースの脅威に対する防御は、防御の段階を評価する一連のプロシージャを通して、この固有のテスト環境で効果的に測定されます。この複雑な技法により、NSS Labs のエンジニアは固有の脅威をブロックするために製品のどのコンポーネントがその働きを担っているかを判別できます。防御の段階が早ければ早いほど、より予防型と見なされます。

防御の段階	サンプル	ブロック	%ブロック
A. URL/ファイル アクセス (レピュテーション)			
B. ダウンロード			
C. 実行			
総合的な防御力			

マルウェアが完全にクライアント コンピュータにダウンロードされる前に、早い段階で検出することが理想的であり、ネットワーク パフォーマンスに影響する可能性のある帯域幅を節約できるという付随的な利点もあります。別の一般的な検出方法として、インターネットからダウンロードされていると仮定し、ファイルの内容を分析するものがあります。評価とダウンロード フェーズでの検出をすり抜けた悪意のあるファイルは、実行段階で検証できます。この動的実行 テストでは、サンドボックス、ヒューリスティック、ビヘイビアブロックなど、より高度な分析の機会をもたらします。

総合的な防御力はそれぞれ個別の防御率 A + B + C を足して算出されます (上記を参照)。

2.2 防御にかかる時間と一貫性

NSS Labs ではマルウェア対策製品の効果の測定に、複数の重要な方法を使用します。もっとも重要なのは、任意の指定した時点での効果を検証することで、これはソーシャルエンジニアリングを悪用した「マルウェアの総合的な防御力」の表のほか、「防御力の表」に報告されます。変動は自然なものであり、この視点は一貫性、ならびに視覚的な指標となります。

NSS Labs ではさらに、与えられたマルウェア サンプルに対し、マルウェア対策製品が対策を行うまでにかかった時間も測定します。**URL 対応ヒストグラム**には、予防型のゼロアワーブロック、総合的なユニークブロック、そして、製品がいかに速やかに対策を追加するかの対応時間を示しています。これはサンプルの反復テストによってのみ判別が可能になります。**対応までの平均時間**には、対策が追加されるまでの経過時間が記録されています。

2.3 テスト対象製品

エンドポイント対策製品は、特に一部のベンダーのように、出荷間際のベータ版の提出を選択した場合を除き、各ベンダーが市場に出回っているソフトウェア (GA) として提供したものです。次に示すのは、テストされ、アルファベット順にソートされた製品の最新リストです。

1. AVG Internet Security、バージョン 8.5.375
2. Eset Smart Security 4、バージョン 4.0.437
3. F-Secure Internet Security 2009、バージョン 9.00 ビルド 149
4. Kaspersky Internet Security 2009、バージョン 8.0.0.506
5. McAfee Total Protection Suite 2009
6. Norman Security Suite 7.1
7. Norton Internet Security 2009、バージョン 16.5.0.135
8. Panda Internet Security、バージョン 14
9. Trend Micro ウイルスバスター 2009、バージョン 17.1.1250

ベンダーはデフォルトの設定が最適でないと感じられた場合、構成を変更することができました。コンシューマー製品では、カスタム設定は一切使用していません。

テストの開始後は、テストの完全性を保つために製品バージョンを凍結しました。マルウェア対策製品の性質上、ウイルスのシグネチャおよび定義の更新は、製造元によるデフォルトの頻度で有効としました。このテストはレピュテーションシステムへのアクセスおよび、ライブコンテンツ、さらにライブアップデートにインターネットアクセスを利用します。

2.4 クライアントホストの説明

すべてのテスト対象ブラウザソフトウェアが下記の仕様に従って仮想マシンにインストールされました。

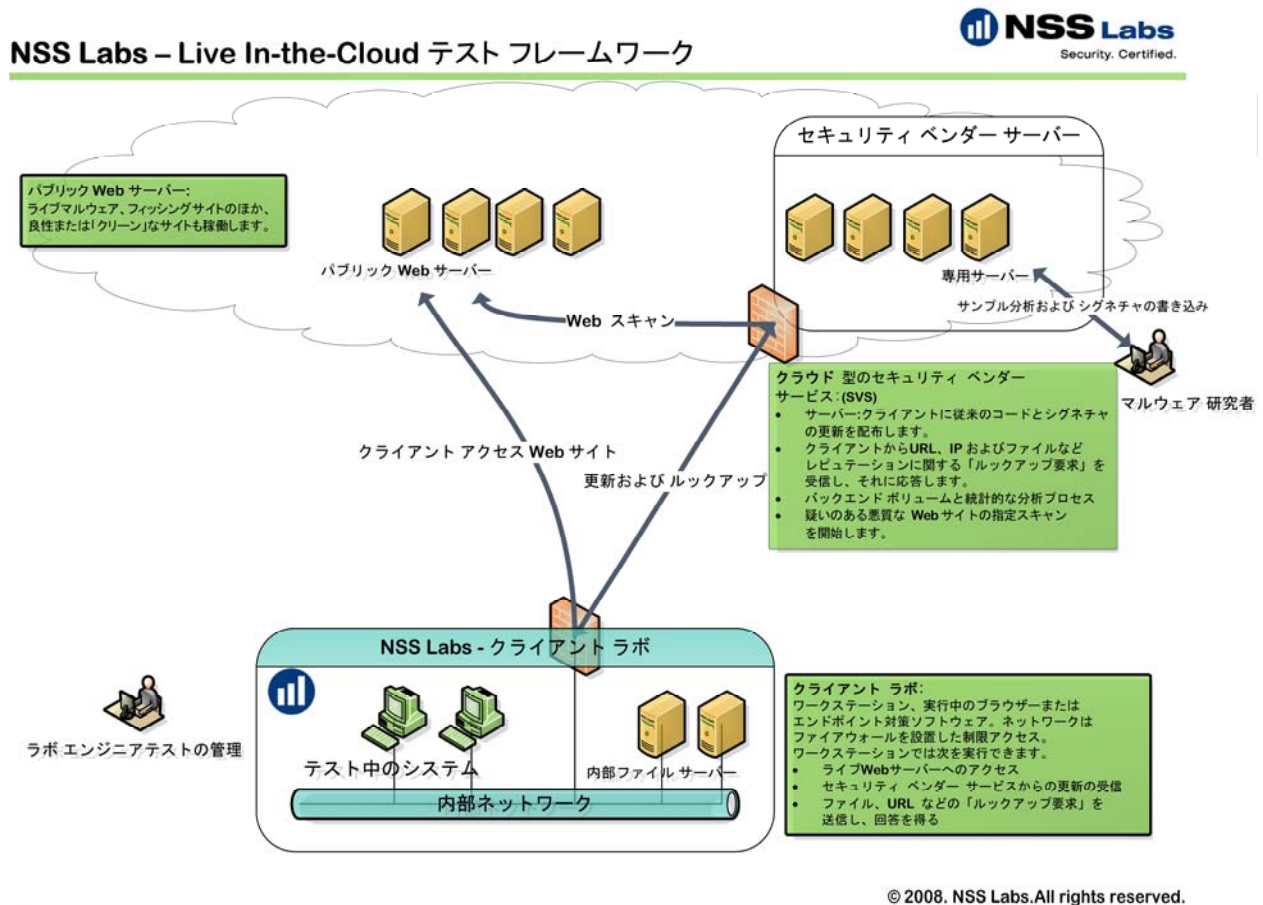
- Microsoft Windows XP SP3
- 1GB RAM
- 15GB HD

テストマシンはテスト開始前、およびテスト実施中に正常に機能しているか確認されました。ブラウザーではインターネットへのフルアクセスを許可し、実際のライブサイトにアクセスできるようにしました。Internet Explorer 7を使用し、テスト中にブラウザーの他のレピュテーションサービスにより製品のマルウェアブロック機能が妨げられることのないようにしました。

2.5 ネットワークの説明

エンドポイント対策製品では、「インターネット接続」状態での使用を想定してクライアントの対策機能をテストしました。そのため、当社のテストでは電子メール、ファイルサーバーアクセス、Webメールなど、さまざまな関連アプリケーションを使用し、ネットワークを介したエンドポイント対策製品の機能と性能を考慮および分析しています。

テスト対象製品はWebブラウザーにより実行されたURLリクエストを介してテストネットワークへ接続されるライブマルウェアを対象としました。それぞれの脅威は適切な分析を行うために、テストの開始前、実行中、終了後に保存されました。最終テスト結果から異常なサンプルは削除されました。



ホストシステムは1枚のネットワークインターフェイスカード(NIC)を備え、1Geスイッチポート経由でネットワークに接続されています。NSS LabsのテストネットワークはCisco Catalyst 6500シリーズの

スイッチ (ファイバーおよび銅線のギガビット インターフェイスの両方) をベースにしたマルチギガビット インフラストラクチャを採用しています。

2.6 テスト構成 - 悪質な URL

本レポートのデータは、2009 年 7 月 7 日から 7 月 24 日のまでの 17 日間のテスト期間中にわたります。テスト期間中、ブラウザーがテスト対象のライブ インターネット サイトにアクセスできること、また、「クラウド」の AV レピュテーション サービスにアクセスできることを確認するために、定期的に接続をモニターしました。この検査を通して、テスト対象の各製品を妨げることなく、59 回の分散テストを (8 時間ごと) 実行しました。

テスト サンプルが新しいことに重点が置かれたため、最終的に結果セットの一部として記録された数より多くのサイトが評価されました。詳細についてはテスト手法を参照してください。

2.6.1 テスト中の悪質な URL の合計数

テスト結果の算出に 3,243 件の URL が使用され、テストを通して合計で 231,351 件のテスト結果が収集されました。

ライブテストではインターネット上の現在のマルウェアを捕捉し、ウイルス対策ベンダーにより分類されていない新種の脅威 (およそ 10% がその動作から悪質と確実に特定されました) のほか、一部の既存のウイルス、トロイの木馬、ワームなどの一部も含まれました。

- Net-Worm.Win32.Koobface (ワーム/拡散)
- Net-Worm.Win32.Kolab (ワーム/拡散)
- Rootkit.Win32.Banker (ルートキット)
- Trojan.Win32.VapSUP (ブラウザーの設定改変/トロイの木馬)
- Backdoor.Win32.SdBot (IRC ボット/C&C)
- Backdoor.Win32.PcClient (HTTP C&C トロイの木馬)。

17,000 件のユニークな疑わしいサイトの初期リストから、テスト対象とするために 4,134 件の潜在的な悪質な URL を事前スクリーンし、それらを対象としてテストを開始しました。これらは少なくとも一度、ブラウザーから正常にアクセスできたものです。無効なサンプルも含め、評価基準を満たさなかったサンプルを削除しました。初期に 4,134 件あった URL は最終的に 3,243 件に絞られ、当社のポスト検証プロセスを経て、最終結果としてまとめました。最終的に信頼できる範囲が 95%、許容誤差が 1.58% という結果が得られました。

2.6.2 1 日に追加される悪質な URL の平均数

平均で、1 日に 191 件の検証済み URL がテストセットに追加されました。犯罪活動レベルの変動により、日によって変動がありました。

2.6.3 マルウェアの混合

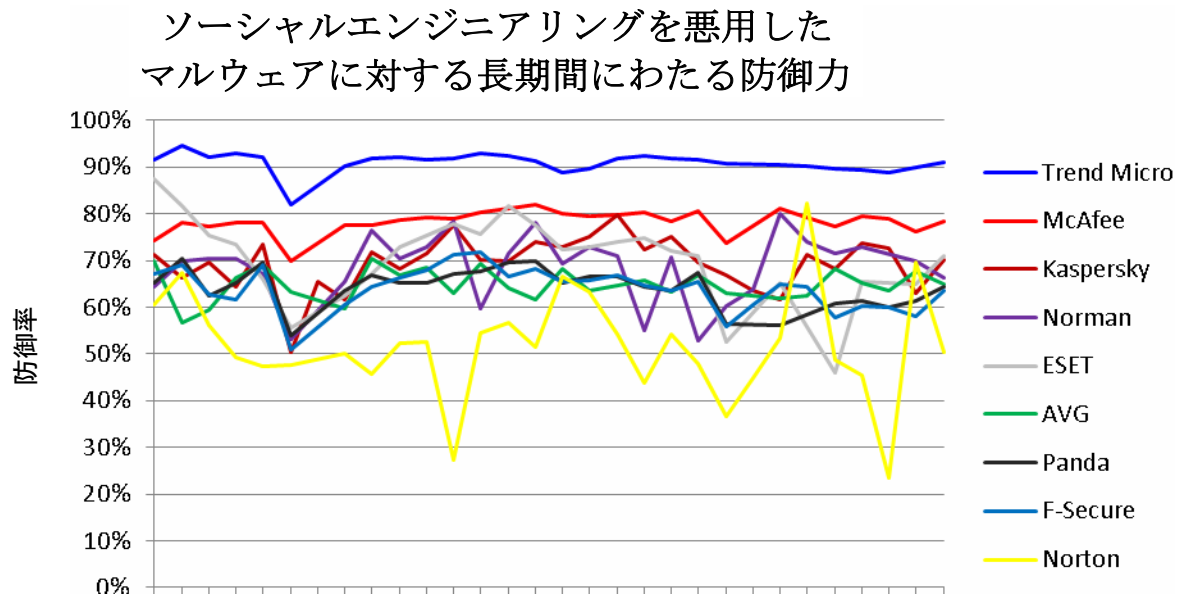
テストで使用された URL の混合は、インターネットの脅威の典型です。1 つのドメインがテストセットのうち 3% 以上に相当しないように注意を払いました。そのため、その制限に近づいた時点で、サイトの数を減らしました。

3 テスト基準と結果

このテストは Web の閲覧、Web メールの確認、HTTP 経由でのファイルのダウンロードなどの際の防御の必要性を対象とします。各マルウェアのバイナリまたはスクリプトはエンドポイント対策ソフトを実行した状態で HTTP 経由でライブの外部 Web サイトから内部のクライアントにダウンロードされます。NSS Labs では、ウイルス対策製品の機能を、NSS Labs が悪質な URL をインターネット上で発見するのと同じ速さで、ウイルス対策製品がブロックできるかによって評価します。NSS Labs は 8 時間ごとにテストを続け、ベンダーが対策を追加した場合には、それにどの程度の時間がかかったかも判別します。

3.1 ソーシャルエンジニアリングを悪用したマルウェアを含む URL を長期間にわたってブロックする

個別の URL をブロックするための基準には 1 つの側面しかありません。日常的に使用するシナリオに関して言えば、ユーザーはすばやく変化する可能性のある広範囲なサイトを訪れています。そのため、出現する悪質な URL のセットは常時循環しているため、継続してこれらのサイトをブロックすることは、効果を上げるための重要な基準と言えます。従って、NSS Labs はライブ URL のセットを 8 時間ごとにテストしました。次に示す表とグラフには、テスト期間全体の中で繰り返されたブロック結果を示しています。各スコアは一定の時間における対策を意味します。



平均的な防御率は、複数の理由によって、固有の URL の結果からはずされます。最初に、このデータには URL のテストが複数回含まれます。そのため、その URL が早い段階でブロックされると、スコアは向上します。もし、その URL が繰り返し見過ごされた場合は、スコアが減点されます。この個別 URL のテスト結果が防

御力評価を割り出すために、時間の経過とともにまとめられます。この結果は「指定した時間にウイルス対策ソフトに対し、どのような防御力を期待できますか?」という質問の答えを導き出します。

3.2 予防型および実行段階での防御

マルウェアが完全にクライアント コンピュータにダウンロードされる前に、早い段階で検出することが理想です。この予防型のダウンロード時の測定において、Trend Micro 社はダウンロード段階でのマルウェアの検出率 (91%) において、追従する他の競合 2 社、McAfee (79.8%) および Kaspersky (78.5%) を大きく引き離しています。

悪質なファイルのダウンロードが成功してしまった場合、次のゴールは悪質なコードの実行を阻止することです。マルウェアには検出から逃れるために複数の方法が備わっているため、実行段階での検出はより困難になります。下記の表の「実行段階での検出」の列は、ダウンロードの列に対する付加的な扱いになります。31% は Norton 社の示した実行時検出の割合で他社を抜き出しています。この値により、同社は総合ランクで 3 位を獲得することができました。

製品	ダウンロード段階の初期防御	実行段階での防御	総合
Trend Micro	91.0%	5.5%	96.4%
Kaspersky	78.5%	9.3%	87.8%
Norton	50.5%	31.3%	81.8%
McAfee	79.8%	1.9%	81.6%
Norman	66.3%	14.9%	81.2%
F-Secure	63.7%	16.4%	80.0%
AVG	65.0%	8.3%	73.3%
Panda	64.4%	7.6%	72.0%
ESET	65.4%	2.5%	67.9%

リアルタイム レピュテーション システムを組み入れた製品のうち、これらのシステムに起因する検出率の平均的な増加率は 16% でした。Trend Micro 社の検出では平均 23% をあげ、一方、McAfee の Artemis レピュテーション システムでの検出では 8% 向上しています。また、Kaspersky および Panda でも同様に一種のリアルタイム レピュテーション システムを組み入れましたが、これらは内部での機能に留まり、分離したテストを実施するには至りませんでした。Eset、F-Secure、Norman にはレピュテーション システムはありません。AVG の Linkscanner は検索エンジンの結果に制限されているため、本テストの対象にはなりません。

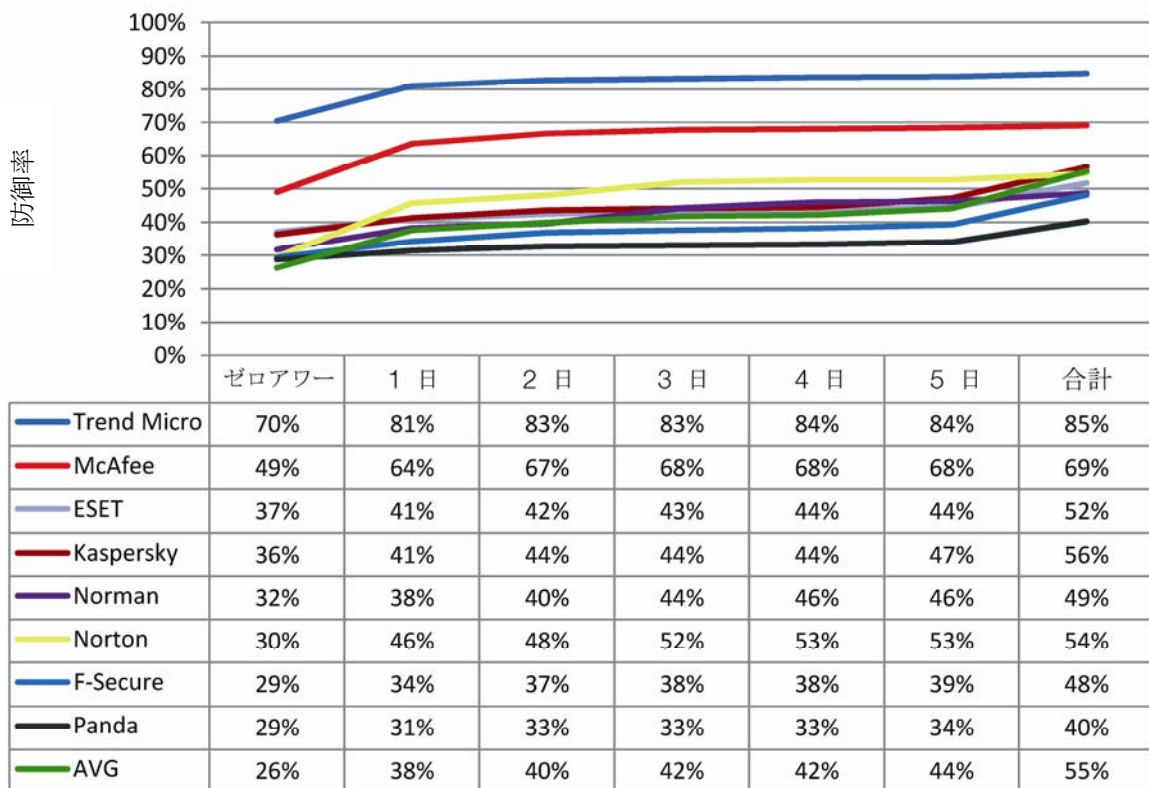
3.3 防御にかかる時間のヒストグラム

次の対応時間に関するグラフには、テスト中、脅威がテスト サイクルに入ったとき、その脅威をブロックするまでにどの程度の時間がかかったかを製品別に示しています。累積的な防御率は「ゼロアワー」および、最初の 5 日間にわたってリストされています。URL テスト期間中の総合的な防御率は、「総合」列の下にまとめられています。概ね、少なくとも製品による防御のうちの半分はゼロアワーで達成され、優れ

た製品ほど、ゼロアワー ブロックの比率が高くなりました。Trend Micro 社が次のランクの競合他社を 21% も引き離れたことは、特筆に値します。

最終的に、この結果からソーシャル エンジニアリングを悪用したマルウェアから防御するためのウイルス対策製品の機能には、大きな格差があることが浮き彫りになりました。Trend Micro (70%-85%) および McAfee (49%-69%) は他のウイルス対策製品に比べてより迅速に、ユーザーをマルウェアから防御しました。この 2 製品は、下記のグラフでも一群の中でずば抜けていることが明らかです。データ分析から、他のウイルス対策製品のすべては、8 日目ごろ、防御率では 50% 未満から巻き返しが始まります。つまり、マルウェアの対策が顧客に配布されるまでの速さには、運用上の差もあることがわかりました。

マルウェア URL 対応ヒストグラム



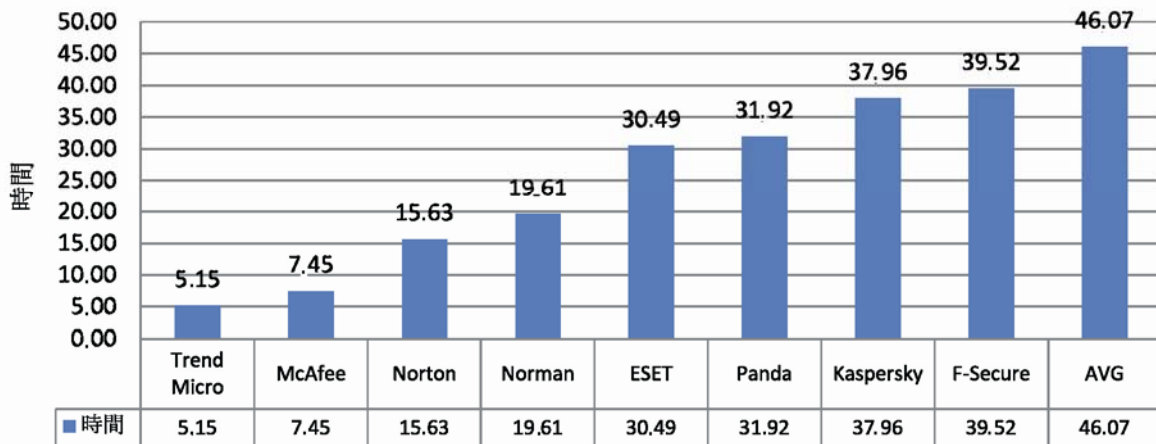
悪質なサイトの寿命は、実生活および当社のテストにおいてそのスコアに差異をもたらします。従来型のテストではマルウェアの対策が再サンプル化されることはなく、これは NSS Labs のテストにおける主な特長と言えます。McAfee 社では、すばやく姿を消した悪質なサイトをロールアップにより多数検出しました。Kaspersky 社は初期に、こうした寿命の長いサイトの多くを見逃しましたが、McAfee 社はテスト期間中、これらを繰り返し見逃しました。ブロックまでの平均時間は、繰り返しテストで引き続きブロックされたサイトによって割り出します。Trend Micro 社ではサイトの寿命の長短にかかわらず防御しました。

3.4 マルウェアをブロックするまでの平均対応時間

多くの人々を守るためには、レピュテーションシステムは迅速で正確である必要があります。この表は「訪問した悪質なサイトがブロックリストに加えられるまで、ユーザーが待機しなけりばならなかった平均時間は？」という質問への回答になります。マルウェアサイトがテストセットに入れられてから、マルウェアサイトがブロックされるまでの平均時間を示します - ただし、テスト中にサイトがブロックされた場合に限られます。ブロックされなかったサイトは含まれません。

この表の値は、総合的なブロック率を表します。つまり、ある製品がマルウェアを 100% ブロックしても、ブロックまでに 240 時間 (10 日) かかった場合は、平均対応時間 10 時間で 70% の防御率を示した製品より、防御率が少なくなるということです。

ブロックまでの平均時間



サイトをブロックするまでにかかった時間 (ブロックされた場合) は 30.37 時間でした。そのため、Trend Micro 社、McAfee 社、Norton 社、Norman 社は、新たなブロックの平均時間を上回っていたことを示しています。

4 製品の評価結果

テストデータと分析は次のとおり、製品別にまとめました。NSS Labs の評価では、長期間にわたる総合防御力を若干高く評価しています。これは、実世界の使用において、長期間にわたる平均をもっともよく反映しているためです。

製品	長期間にわたる総合防御率	ユニーク URL	ゼロアワーブロック	ブロック対象サイトへの対応時間
Trend Micro	96.4%	85%	70%	5.2
Kaspersky	87.8%	56%	36%	38.0
Norton	81.8%	54%	30%	15.6
McAfee	81.6%	69%	49%	7.5
Norman	81.2%	49%	32%	19.6
F-Secure	80.0%	48%	29%	39.5
AVG	73.3%	55%	26%	46.1
Panda	72.0%	40%	29%	31.9
Eset	67.9%	52%	37%	30.5

各製品はスコアに応じて、「推奨」、「中立」、「注意」のいずれかのガイド評価とともにランク別にリストされています。

4.1 推奨

NSS Labs の「推奨」評価は、優れた性能を備え、個人での使用に適した製品に与えられます。NSS Labs の「推奨」評価を得た製品は、購入を前提とした積極的な考慮に値し、あらゆるユーザーに最終候補として考慮されるべき製品であることを意味します。

市場シェア、企業サイズ、ブランドの知名度に関係なく、NSS Labs の「推奨」評価は最高の技術を備えた製品にのみ認められます。

4.1.1 TREND MICRO ウイルスバスター 2009

本テストから、Trend Micro 社はレピュテーション ベースの対策を取り入れたことで、大きな前進を遂げたことが明らかとなりました。長期間にわたる総合防御力の評価では 96.4%、および悪質な URL の防御率では 85% を実現した Trend Micro ウイルスバスター 2009 は、ソーシャルエンジニアリングを悪用したマルウェアに対する防御で最高の評価を得ました。Trend Micro 社はゼロアワー、または初回のテスト実行で 70% をブロックしました。予防型防御の特性を強く示しています。すり抜けたマルウェアは 5 時間以内に対応され、全テスト対象製品の中で最速でした。

4.1.2 KASPERSKY INTERNET SECURITY 2009

第2位にランク付けされた Kaspersky はテスト期間中、87.8% の脅威をブロックし、悪質なユニーク サイトのブロック スコアは56% をマークしました。Kaspersky はテストの初回実行で脅威の36% を検出し、マルウェアの対策が追加されるまでに平均38時間かかりました。

4.2 中立

NSS Labs の「中立」評価は、ある程度の性能を備え、ユーザーが現在使用しているのであれば、継続的に使用すべきであることを意味します。NSS Labs の「中立」の評価を得た製品は、購入の際に考慮の対象とすることができます。

4.2.1 NORTON INTERNET SECURITY 2009

この市場シェア リーダーは長期的なマルウェアのダウンロードの81% を検出しましたが、ダウンロード時の検出のみを見ると、50.5% に留まりました。Norton はテスト期間中、81.8% の脅威を防御し、悪質なユニーク サイトの防御率は54% をマークしました。Norton はテストの初回実行で脅威の30% を検出し、マルウェアの対策が追加されるまでに平均15.6時間かかりました。しかし、これは一貫性に欠け、長期間にわたる防御力ではかなりの変動が記録されました。Norton はまた、実行時の検出に大きく依存しています。

一部の感染ファイルが「駆除」されると、Norton では再起動が必要になりました。再起動を選択した場合(表示される選択肢の1つ)、再起動するまで Norton の防御力はほぼ0% に落ち込みました。プロンプトが表示されただけではユーザーは再起動をほとんどしない(特にタスクの途中である場合)ことを考え合わせると、この製品要件は予防型には逆行するもので、早い段階で修正されるべき特性と言えます。

当社のテストが完了して間もなく、オンライン レピュテーション システムを備えた Norton 2010 がリリースされました。次回のテストではこの製品も検証していきます。

4.2.2 McAfee TOTAL PROTECTION SUITE 2009

McAfee 社は総合的なマルウェアのダウンロードで81.6% を検出し、統計的には Norton および Norman に匹敵します。McAfee 社はユニーク URL の69% をブロックし、初回テストでは49% を検出、競合他社に12% の大差を付けて名誉ある2位を獲得しました。すり抜けたマルウェアの対策は平均7.45時間以内に追加され、全テスト対象製品の中で2番目に速い記録でした。

4.2.3 NORMAN SECURITY SUITE 7.1

Norman は総合的なマルウェアのダウンロードで81.2% を検出し、統計的には Norton および McAfee に匹敵します。Norman はユニーク URL を49% ブロック、初回テスト実行時に32% を検出しました。すり抜けたマルウェアへの対策は平均19.6時間で追加されました。

4.2.4 F-SECURE INTERNET SECURITY 2009、バージョン 9

F-Secure は総合的なマルウェアのダウンロードで 80% を検出し、統計的には Norton に匹敵します。F-secure はユニーク URL を 48% ブロック、初回テスト実行時に 29% を検出しました。F-Secure は対策の追加までの経過時間は 39.5 時間で、2 番目に長い値です。

4.3 注意

NSS Labs の「注意」評価は、製品の性能が不十分であったことを意味します。これらの製品を使用しているユーザーはセキュリティに対する姿勢および脅威の軽減などの要因を見直し、別の構成方法や乗換えなどを考慮してください。NSS Labs の「注意」の評価を受けた製品を最終候補として絞り込んだり、更新したりするべきではありません。

4.3.1 AVG INTERNET SECURITY SUITE 8.5.375

AVG は総合的なマルウェアのダウンロードを 73.3% 検出し、ユニーク URL を 26% ブロック、初回テスト実施での検出は 26% でした。AVG は対策の追加までに 46 時間かかりました。グループ内で最低の結果です。

4.3.2 PANDA INTERNET SECURITY 2009、V14

Panda は総合的なマルウェアのダウンロードを 72% 検出、下から 2 番目のスコアでした。Panda はユニーク URL を 40% ブロック、初回テスト実行時に 29% を検出しました。Panda は対策の追加に 31 時間かかりました。

4.3.3 ESET SMART SECURITY 4

Eset は総合的なマルウェアのダウンロードを 67.9% 検出、グループのテストで最下位でした。Eset はユニーク URL を 52% ブロックしましたが、ゼロアワーでは 37% に留まりました。新しいマルウェアの対策の追加には平均で 30.5 時間かかりました。Eset 製品にはレピュテーション コンポーネントは含まれていません。

5 付録:テスト プロシージャ

テストの目的は、テスト対象のウイルス対策製品が、今日インターネット上に出回っている多くの重大なマルウェアの脅威からどの程度ユーザーを守ることができるかを判別することにあります。重要なのはタイミングです。犯罪の広がりを早急かつ積極的に察知し、悪質な Web サイトを封じ込めるためには、重要な目標はできるだけ「最新」のサイトをテストに含めることでした。

NSS Labs はユニークな「Live Testing」という環境と技法を開発しました。NSS Labs では今現在も、パートナーや独自のサーバーなど、多様なソースから Web ベースの脅威を集めています。テスト素材について、テストに参加したベンダーからは、一切、提供を受けていません。潜在的な脅威は当社のテストキューに入る前に、アルゴリズム的に綿密に調査されます。いずれの脅威もその後取り込まれ、24 時間体制で調査されます。メモ:このプロシージャでユニークなのは、NSS Labs がテストの前後でサンプルを検証している点です。脅威の実際のテストは 4 時間ごとに実行され、最初はサイトが存在すること、テスト定義に適合することなどが検証されます。

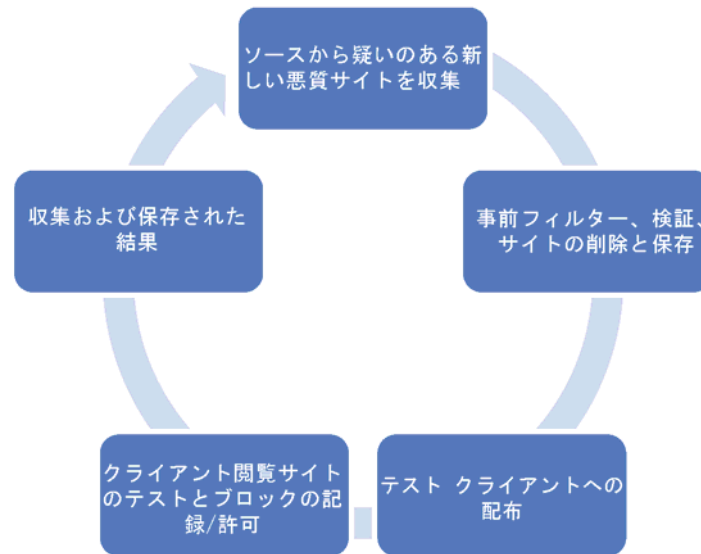
すべてのテストは高度に制御された手法で実行され、結果は各テスト周期において記録、保管されます。

5.1 テストの期間

NSS Labs のライブ マルウェア テストは、17 日間無休で継続的に実施されました。テスト期間中、新しい URL が検出されるたびに、追加されました。

5.1.1 テストの頻度

テスト期間中、各 URL は成功か失敗かに関係なく、8 時間ごとにテスト環境で実行され、NSS Labs はテストの期間中 Web ブラウザーでマルウェアのサンプルのダウンロードを継続的に試みました。



5.2 マルウェア URL のサンプル

この種のテストでは、マルウェア サイトの「鮮度」が重要な特質と言えます。最新のもっとも典型的な URL を使うため、NSS Labs では多数の異なる収集源から広範囲にわたるサンプルを受け取ります。

5.2.1 収集源

まず、NSS Labs では独自のスパム トラップとハニーポットを運用しています。このような大容量のトラフィックを伴う電子メール アカウントからは、1 日に数千通におよぶユニーク電子メールと、数百件のユニーク URL が収集されます。NSS Labs の誇るマルウェアおよびウイルスのアーカイブには、確認されたサンプルがギガ単位で保存されています。さらに、NSS Labs は他にも、URL や悪質なコンテンツへのアクセスを提供する独立系セキュリティ研究者、ネットワーク、セキュリティ企業などと連携しています。サンプルセットには次のような手法で拡散された悪質な URL が含まれます: スпам、ソーシャル ネットワーク、悪質な Web サイト。マルウェア ペイロードを含むエクスプロイト (エクスプロイト + マルウェア) (「clickjacking (クリックジャッキング)」、「drive-by downloads (ドライブ バイ ダウンロード)」などとも呼ばれる) はテストからは除外されました。マルウェアの実世界での分布が、カテゴリ的にも、地理的にも、プラットフォーム別にも反映されるよう、細心の注意を払いました。

また、NSS では Yahoo、Amazon、Microsoft、Google、NSS Labs、主要な銀行などの「クリーンな URL」の収集も行い、システムで定期的にクリーンな URL を実行することで、ウイルス対策製品が過剰反応的にブロックしていないことも確認しました。

5.3 URL のカタログ

新たなサイトは URL の検討セットに、できる限り速やかに追加されました。各サンプルを取り入れた日付と時刻も記録されています。ソースのほとんどは自動的に、即座に追加されましたが、一部には手動に

よる処理が必要な方法もあり、これらについても 30 分以内に処理されました。検討セットに含まれるすべての項目は、その有効性に関係なく固有の NSS Labs ID でカタログ化されました。これにより、サンプルソースの効果を追跡できるようになりました。

5.4 サンプル URL の存在の確認

最新の潜在的マルウェア サイトに対する効果をテストすることがテストの目的であることから、時間は根本的要素と言えます。フィードの性質上、および、変化の速度から、テストの前に各サイトを細部まで評価することは不可能です。サイトは瞬く間に消えてしまうためです。そのため、テスト項目には、項目が存在しているか、ライブ インターネットからアクセスできるかというおおまかな確認のみ実施されます。

実行セットに含まれるためには URL がテストの実行中ライブである必要があります。各テスト サイクルの始めに、URL がアクセス可能であるかどうか (到達可能であり、Web ページから 404 エラーが返らないなどアクティブであること) を確認します。

この評価は当社のソースからサンプルを受け取るまでの数分以内に実施されます。メモ:これらの分類はテストの後にさらに検査され、URL は内容によって再分類化されるか、削除されます。

5.4.1 アクティブな URL コンテンツのアーカイブ

アクティブな URL コンテンツはダウンロードされ、固有の NSS ID 番号とともに、アーカイブ サーバーに保存されます。これにより、NSS Labs は制御および評価目的のために URL を保存できます。

5.5 ダウンロードと実行

カスタマイズされたクライアント自動化ユーティリティーは、テスト中、各製品を介して URL へのリクエストを行います。NSS はマルウェアがダウンロードされたかどうか、ダウンロードの試行によって製品のマルウェア対策からの警告がトリガされたかを記録します。**注意:**このテストの場合、レピュテーションとファイルダウンロードスコアは一緒にまとめられます。

5.5.1 WEB レピュテーション スコアリング

この結果の応答は「許可」または「ブロックおよび警告済み」のいずれかで記録されます。

- 成功:NSS Labs は製品がマルウェアのダウンロードの阻止に成功したか、警告を正しく発行できたかに基づいて「成功」を定義します。
- 失敗:NSS Labs は製品がマルウェアのダウンロードの阻止に失敗したか、警告の発行に失敗したかに基づいて「失敗」を定義します。

5.5.2 HTTP ファイル ダウンロードの採点

この結果の応答は「許可」または「ブロックおよび警告済み」のいずれかで記録されます。

- 成功:NSS Labs はダウンロード中、またはマルウェアがダウンロードされた直後に、製品が正しく警告を発行できたかに基づいて「成功」を定義します。
- 失敗:NSS Labs は製品がマルウェアのダウンロードの阻止に失敗したか、警告の発行に失敗したかに基づいて「失敗」を定義します。

5.5.3 ファイルの実行の採点

この結果の応答は「許可」または「ブロックおよび警告済み」のいずれかで記録されます。

- 成功:NSS Labs はファイルの実行中、正しく警告を発行できたかを基に「成功」を定義します。
- 失敗:NSS Labs は製品がマルウェアの実行の阻止に失敗したか、警告の発行に失敗したかに基づいて「失敗」を定義します。

5.6 削除

テストを通じて、ラボのエンジニアはテスト実行セットから未確認の URL およびコンテンツを検証して削除します。たとえば、マルウェアと分類された URL が、一般的なスプラッシュ ページに Web ホストにより置き換えられた場合はテストから削除されます。

URL サンプルがテスト中にダウンロードできなくなった場合、そのサンプルは実行中のテストコレクションから削除されます。NSS Labs は各サンプルの存在 (ダウンロードの可用性) を継続的に確認し、それに応じてテストセットへサンプルを追加したり、削除したりしています。マルウェアのサンプルがテスト実行時に利用できなくなり、次のテスト実行時に再度利用できるようになった場合は、テスト コレクションに再度追加されます。利用できなくなったサンプルは、Web ブラウザーの成功または失敗を計算する際には含まれません。

5.7 ポストテスト検証

ポストテスト検証により、NSS Labs は悪質でなかったまたはテストの開始前に使用可能でなかったサンプルを再分類するか削除できるようになります。NSS Labs は2つの異なるサンドボックス (Sunbelt の CW Sandbox および Norman Analyzer) を使用し、マルウェアの削除と検証を行い、必要に応じて、複数のウイルス対策スキャナーを使用して、疑いのあるサンプルをさらに検証します。

6 付録 C: テスト インフラストラクチャ

多くの機材、ソフトウェア、ならびに本テストに不可欠なサポートをご提供いただいたテスト インフラストラクチャ パートナーに謝意を表します。

AutomatedQA
test, debug, deliver!

assurent 
secure technologies | a TELUS Company

solidcore 

 Sunbelt Software
we keep the bad guys out™

 mailshell™

