

シマンテックインテリジェンスレポート: 2011 年 9 月

9 月は、ポリモーフィック型マルウェアの比率がウイルスメールの 72% と過去最高になり、ソーシャルエンジニアリング攻撃も急増。ネット犯罪者、ブログプラットフォームで待ち伏せ攻撃

シマンテック ドット クラウドの「メッセージラボインテリジェンスレポート」とシマンテックの「シマンテックスパム & フィッシングレポート」を統合した「シマンテックインテリジェンス月次レポート: 2011 年 9 月号」では、マルウェアやスパムをはじめとするビジネスリスクにつながる危険性に関し、シマンテックインテリジェンスチームが分析したサイバーセキュリティの脅威、傾向および実態の最新情報を提供する。本レポートは、2011 年 8 月および 9 月のデータを始めとするデータ解析結果をもとにまとめたものである。

Report highlights

- スパム - 9 月は、74.8%(前月比 1.1% 減): 11 ページ
- フィッシング - メール 447.9 通あたり 1 通でフィッシング攻撃(前月比 0.26% 減): 14 ページ
- マルウェア - メール 188.7 通あたり 1 通がマルウェアを含む(前月比 0.04% 増): 16 ページ
- 悪質な Web サイト - 1 日あたり 3,474 件の Web サイトをブロック(前月比 1.0% 増): 17 ページ
- ブロックされた悪質 Web サイトのうち、9 月に新たに遮断されたものは、全体の 44.6%(前月比 10.0% 増): 17 ページ
- ブロックされた Web ベースのマルウェアのうち、9 月に新たに確認されたものは、全体の 14.5%(前月比 2.9% 減): 17 ページ
- 悪質なメールがオフィスプリンタのメッセージを装う: 2 ページ
- スパマー、WordPress の脆弱性を悪用して医薬品のスパム Web サイトを宣伝: 6 ページ
- 偽のトラストシールを使った偽の製品販売: 7 ページ
- スパマーやマルウェア作成者による不明瞭化された JavaScript の使用が増加: 8 ページ
- 企業と個人ユーザーのためのベストプラクティス: 20 ページ

はじめに

大量の悪質なメール感染型マルウェアが 9 月の脅威動向に明らかな痕跡を残した。9 月のすべてのメール感染型マルウェアの約 72% は、「シマンテックインテリジェンスレポート 7 月度¹」で初めて識別されたポリモーフィック型マルウェアの攻撃的な亜種であると特徴づけることができる。7 月での割合は 23.7% で、8 月に 18.5% と若干減少したが、9 月は 72% と急上昇した。この前代未聞の高水準は、ネット犯罪者が 2011 年に企業への攻撃をエスカレートさせ、従来のセキュリティ対抗策の弱点を最大限に利用していることを明確に示している。

これらの攻撃の多くの背後にあるソーシャルエンジニアリングも加速しており、スマートプリンタやスキャナから送信され同じ組織内の同僚が転送したメールを装うなど、さまざまな新しい技法が導入されている。これらの攻撃の多くは、依然としてさまざまな既知の国際宅配サービスを偽装しており、プリンタやスキャナはこれらの攻撃で実際に使用されているわけではないので、オフィスプリンタがマルウェアを送信するという考えは思いも寄らないものである。しかし、おそらくこのセキュリティ感覚のままでは限り、このようなソーシャルエンジニアリング攻撃は今後も成功し続けることだろう。

スパムレベルは 9 月中はかなり安定していたものの、スパマーはインターネット上の多数の Web サイトで有名な WordPress ブログソフトウェアの特定の旧バージョンにおいての脆弱性を見つけた。スパマーにとって都合が良いこれらの脆弱性の悪用は、ソフトウェアを最新のパッチとリリースで最新状態にしておく必要があることを改めて注意喚起する。WordPress.com によってホストされているブログはこれらの危殆化の影響を受けていないように見える点に注意する必要がある。

¹ http://www.symanteccloud.com/ja/jp/mlireport/SIR_2011_July.pdf

最後に、JavaScript がネット犯罪者やスパマーなどが好む手段であり続けている理由や、善人と悪人の戦いが続く中で JavaScript が前線でのどのように使われているかを解説する。

今月号のレポートをご活用いただけると幸いです。コメントやフィードバックがあれば気軽に直接私まで。

Paul Wood、シニアインテリジェンスアナリスト

paul_wood@symantec.com

[@paulwoody](#)

レポートの分析

悪質なメールがオフィスプリンタからのメッセージを装う

最新のプリンタの中には、スキャンしてからメールする機能を備えているものがある。これは、ユーザーがスキャン済みのドキュメントを指定したメールアドレスにオンデマンドで送信できる機能である。シマンテックインテリジェンスは、この機能を利用するソーシャルエンジニアリングの手口を使い、メール経由で実行可能ファイルを圧縮した「.zip」アーカイブ形式で送信するマルウェア作成者を特定した。添付ファイルには、図 1 の例に示すように、プリンタからのスキャン済みドキュメントと偽った実行可能ファイルが含まれている。

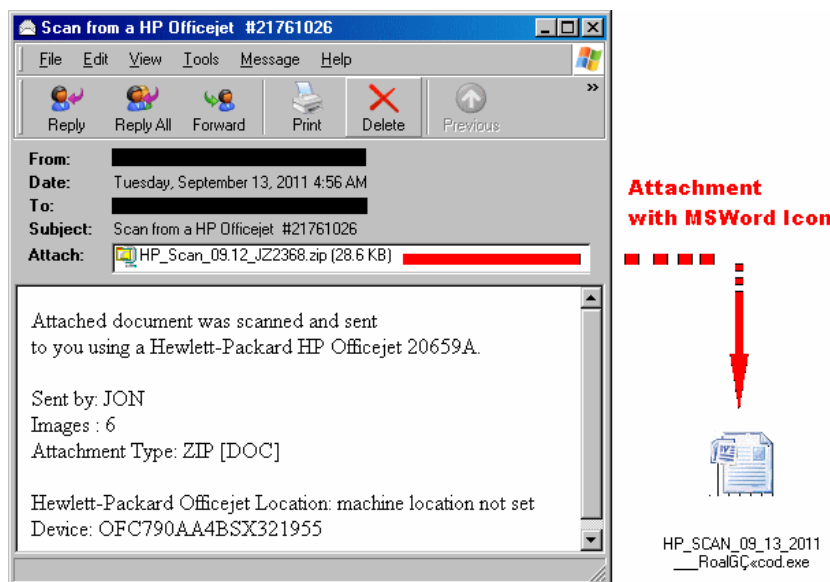


図 1: オフィスプリンタから送信されたスキャン済みドキュメントを装う悪質な電子メールの例

それぞれのケースで、送信者ドメインは受信者ドメインに合致するように詐称されていた。同じ組織の同僚によって受信者宛てに転送されているかのように見えて、このメールが内部から発信されたようにほのめかす場合もあった。

念のため言うておくと、オフィスプリンタやスキャナがマルウェアを含むファイルを送信することはない。また、多くは、スキャン済みドキュメントを「.zip」添付ファイルとして送信する機能を備えていない。プリンタやスキャナのハードウェアは配布プロセスに関与していなかった。一般に、ユーザーは電子メールの添付ファイルを開くとき、特に知らない送信者からの場合は常に注意する必要がある。

いくつかの例を図 2 に示す。

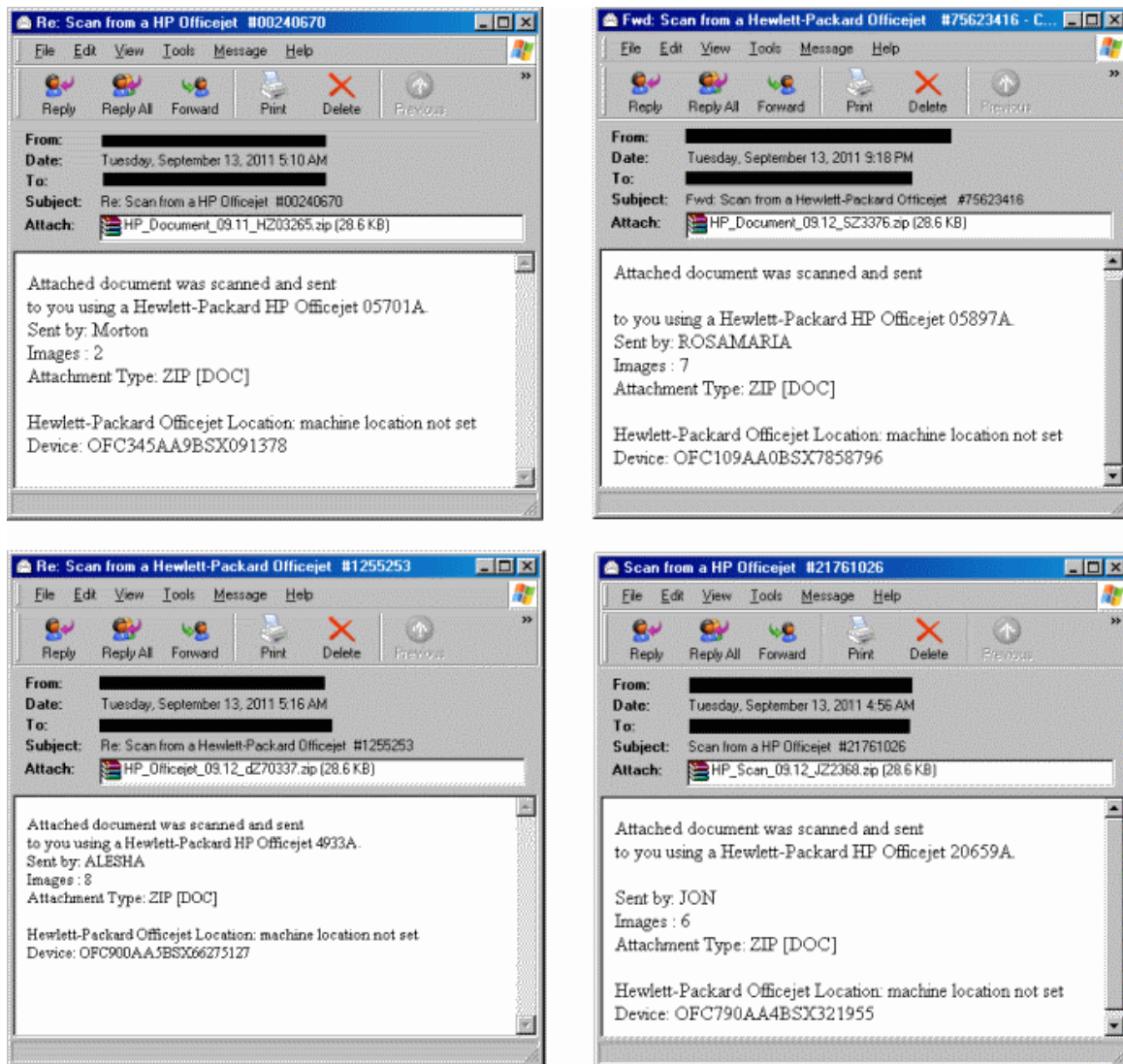


図 2: スマートオフィスプリンタやスキャナになりすます悪質な電子メールの例

図 3 で、シマンテックインテリジェンスは、2011 年 9 月 13 日から 24 時間これらのメールを監視して興味深い情報を収集した。

件名	固有の添付ファイル	
	頻度	数
Scan from a [プリンタ名 A] #{6 から 8 桁のランダムな数字}	742	1,393
Scan from a [プリンタ名 B] #{6 から 8 桁のランダムな数字}	41	779

図 3: プリンタになりすますさまざまな添付ファイルの頻度と数を示す表

また、図 4 に示すように、これらの例で、攻撃者は、一部のアーカイブツールを使って表示したときに「.doc」拡張子を表示するという方法でアーカイブファイルのファイル拡張子を変更した。

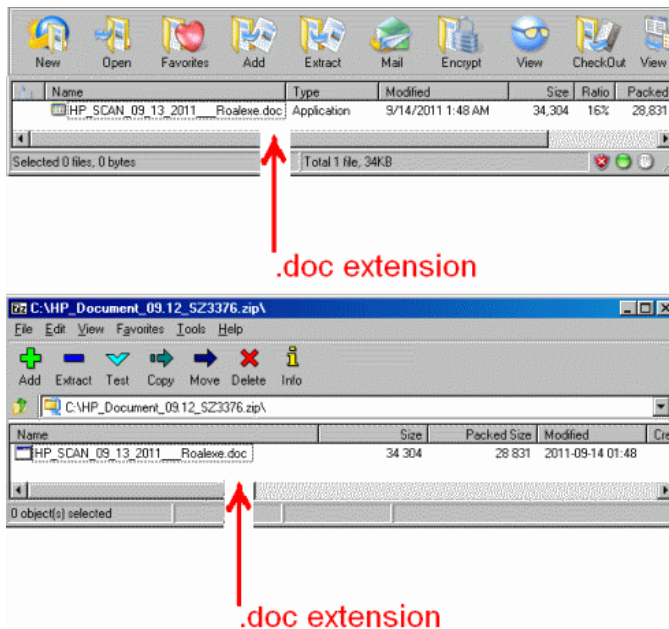


図 4: コンテンツを「.doc」拡張子で不正確に表示する「.zip」アーカイブの例

「.zip」アーカイブに保存されている実際のファイル名は「cod.exe」拡張子で構成されているが、一部のアーカイブツールでこれが誤って表示される。ファイル名の「cod.exe」部分の前に特別な隠し文字（16 進コード 0xAB、以下で強調している部分）があるためである。これにより、ファイルはアーカイブビューアで不正確に「exe.doc」を付加して表示されることになる。

上記の例に加えて、マルウェアの同じ亜種が多数の異なる件名と 2 つの異なるファイル名を使って配布された例も検出した。図 5 に示すように、あるケースではドキュメント、別のケースでは写真となっている。

ファイル名	頻度
Document_NR727875272_Coll=d4=c7=ab cod .exe	410
photo_W71765413082011_Coll=d4=c7=ab gpj .exe	149

図 5: 別の例の頻度を示す表

前と同様、「cod.exe」で終わるファイル名は一部の「.zip」アーカイブ表示ツールで「exe.doc」と誤って表示される。同様に、「gpj.exe」は「exe.jpg」と表示される。

図 6 に示すのは、9 月 13 日からの 24 時間にやはりこの特定のマルウェアを配布するために使われたその他の興味深い件名の例である。

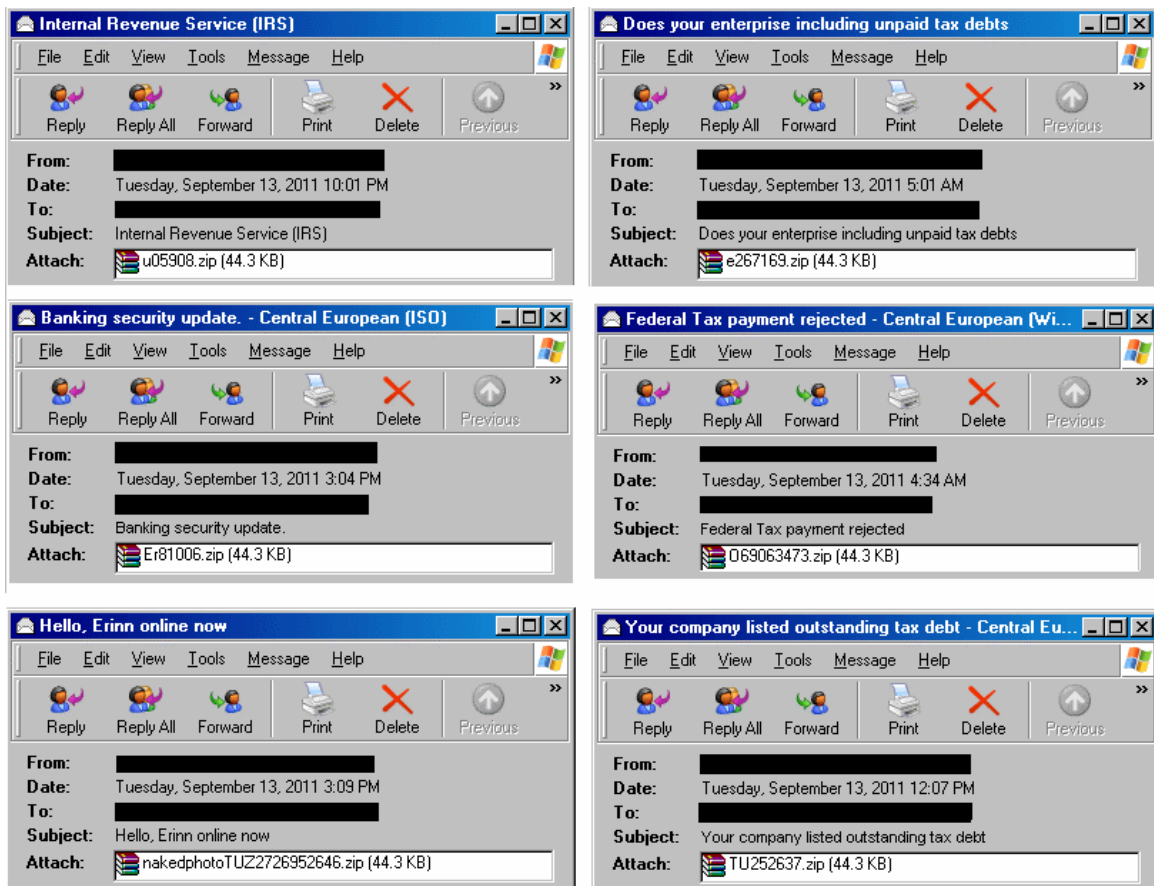


図 6: 同じマルウェアを拡散するために使われたその他のソーシャルエンジニアリングの件名の例

その他の興味深い件名	頻度
Pornographic mail (ポルノメール)	85
Company Contract doc (企業契約ドキュメント)	40
Tax debt notification (税金滞納通知)	34
Revenue (IRS) Department (国税庁 (IRS))	25
Printer Scanned doc (プリンタスキャン済みドキュメント)	21
domain suspension mail (ドメイン停止メール)	9
pornographic picture (ポルノ写真)	3

図 7: マルウェアを配布するために使われるさまざまな件名の頻度を示す 24 時間のスナップショット

これらの例で示されている多様性から、受信者に悪質な添付ファイルを開かせるために、攻撃者が考えられる限りの数多くのソーシャルエンジニアリング戦略を試していることは明らかである。

この記事は、シマンテックのマルウェアアナリストである Bhaskar Krishnappa によって寄稿された。

スパマー、WordPress の脆弱性を悪用して医薬品のスパム Web サイトを宣伝

シマンテックインテリジェンスブログでは、スパマーが複雑なリダイレクトチェーンを介して実際のスパムサイトを隠そうとしている実態を取り上げた。多くの場合、ハッキングされたサイトや危険化したサイト、URL 短縮サイト、不明瞭化技法、またはこれらすべての組み合わせが使われている。

最近、世界の数千台のサーバーで実行されている人気のオープンソースブログである WordPress の脆弱性を悪用するスパマーを発見した。スパマーは、WordPress プラットフォームを使って Web サーバーを危険化し、おそらく検出を回避する(または少なくとも遅らせる)ために、WordPress ディレクトリ構造の奥深くにファイルを配置する。埋められたファイルはシンプルな HTML ページで「Page loading」などのテキストを含んでいて、通常、HTTP「meta refresh」を使って図 8 に示すようなスパマーの「Canadian Health&Care Mall」Web サイトにユーザーをリダイレクトする前に短く表示される。

```
<meta http-equiv="refresh" content="0; url=http://[リダイレクト先の新しいアドレス]" />
```

WordPress.com によってホストされるブログは、これらの脆弱性の影響を受けていないように見える点に注意する必要がある。脆弱であると思われるのは、WordPress.org からダウンロードされるソフトウェアの旧バージョンのみである。シマンテックインテリジェンスでは、影響を受けるバージョンをまだ特定できていないが、引き続き、シマンテックインテリジェンスブログでこの情報を更新する予定である。²

これらの危険化した Web サイトへのリンクを含むスパムメールもスパム送信されている。

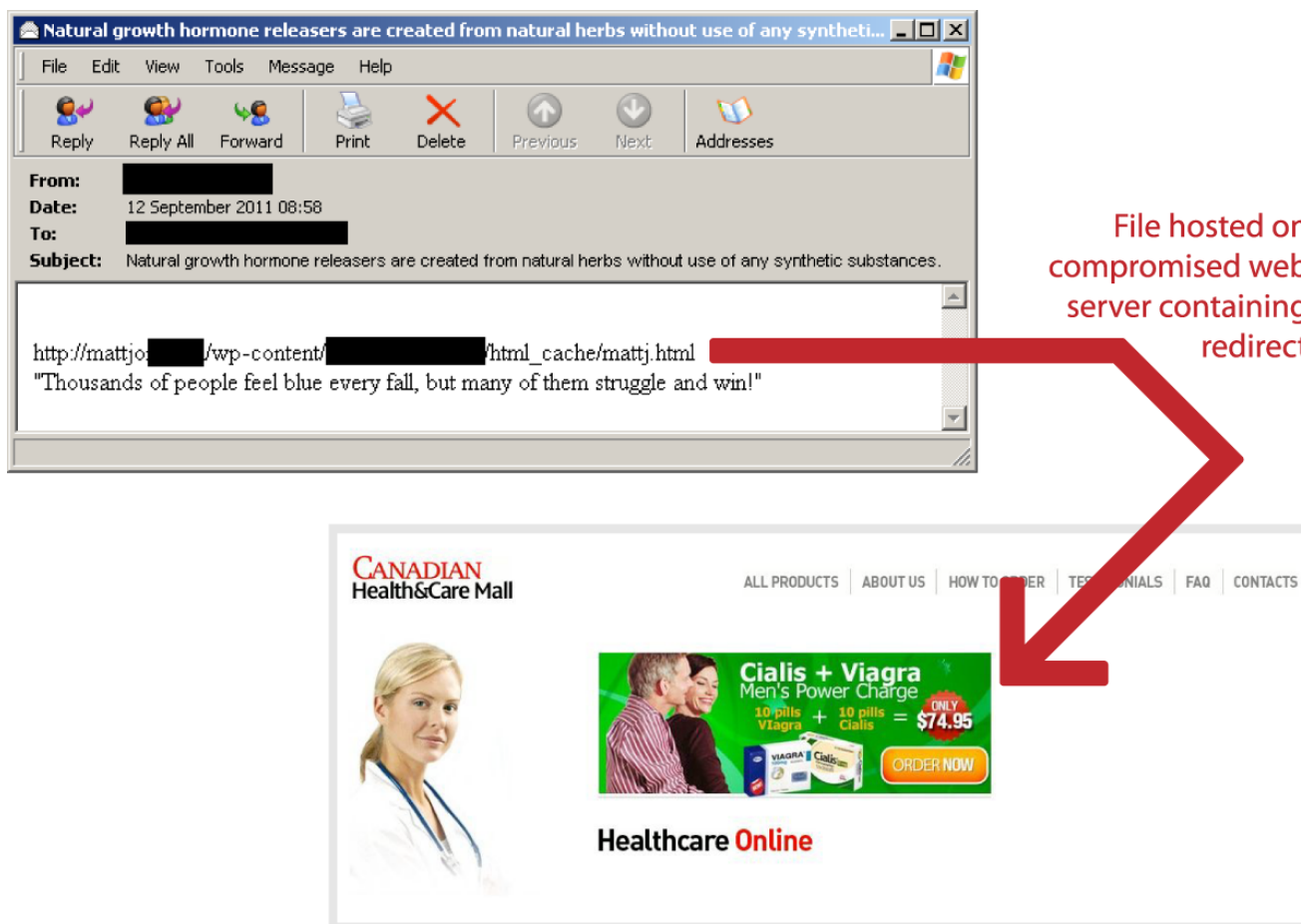


図 8: 危険化したブログを経由したスパムメールからリンクされた薬局の Web サイト

² <http://www.symantec.com/connect/symantec-blogs/symantec-intelligence>

危殆化したサーバーに配置されるファイルに、危殆化したドメイン名の最初の数文字と「.html」拡張子で名前が付けられることがある。上記の例では、危殆化したドメイン名は「mattjo」で始まり、サーバーに配置されたファイルの名前は「mattj.html」であった。

その後の危殆化では、ランダムに生成されたファイル名が使われていた。48 時間で、数千の固有のドメインがこの方法で危殆化されていることを発見した。これらすべてのドメインに共通するのは、いずれも脆弱なバージョンのブログプラットフォームを使用していることだけだろう。おそらく、攻撃者がこれらの Web サイトを危殆化するための準備は、検索エンジンへのクエリを精巧に作ることで十分である。

これは、すべてのソフトウェアを最新のパッチとリリースで最新状態にしておく必要性を注意喚起するのに役立つ。WordPress の最新バージョン(2.7 以上)は、この WordPress サポート記事に記載されているとおり、半自動的に更新できる³。

この記事は、シマンテックのシニアエンジニアである Nicholas Johnston によって寄稿された。

偽のトラストシールを使った偽の製品販売

フィッシャーは常に、エンドユーザーをだますための新しいアイデアを探している。シマンテックインテリジェンスでは、複数の新しいトリックを利用する、あるフィッシングサイトを見つけた。そのフィッシングサイトは、有名なソフトウェア会社を装い、関連するソフトウェア製品を割引価格で販売すると謳っていた。そのフィッシングページでは、それらの偽の製品を「夏の特別価格」と銘打ち、8 割引で販売していた。ユーザーは、購入する際、請求先情報、個人情報、クレジットカードの詳細情報を入力するよう求められた。

図 9 に示すように、要求された個人情報はユーザーのメールアドレスと電話番号であった。要求されたクレジットカード詳細はカード番号、CVV コード、カードの有効期限であった。このフィッシングサイトの犠牲になると、ユーザーは機密情報をフィッシャーによってまんまと盗まれ、金銭的な被害を被ることになる。

The screenshot shows a phishing page designed to look like a legitimate e-commerce site. At the top, it features a 'SECURE TRANSACTION' header with a lock icon and the text '100% Security Guaranteed.' Below this is a table of charges:

Ordering Software:	
Purchase Amount:	\$389.90
Transaction Fee:	\$5.50
Total Amount:	\$395.40

The main body of the page contains two sections of forms:

- BILLING INFORMATION:** Includes input fields for 'First Name:', 'Last Name:', 'Street Address:', 'City:', 'State:' (with a dropdown menu set to 'Outside US/Canada/Australia'), 'ZIP Postab:', and 'Country:' (with a dropdown menu set to 'Australia').
- PERSONAL INFORMATION:** Includes an 'E-mail:' input field.

At the bottom of the personal information section, there is a small disclaimer: 'It is very important to provide working e-mail address to receive order and product download information. We strongly recommend you to disable spam filters until receiving letter from us.'

³ http://codex.wordpress.org/Updating_WordPress#Automatic_Update

Confirm E-mail:

Alternate E-mail:

Phone: +61

Country Code Phone Number

This is my cell phone, send me SMS with order information

CREDIT CARD

Card Number:

16 digits, no spaces or dashes

CVV Code:

Expiration (MM/YY): /

Month Year

図 9: フィッシング Web サイト

これらの偽の商品は餌として使われているが、フィッシングサイトに仕掛けられたトリックの 1 つにすぎない。より多くのエンドユーザーを誘い込もうとする、さらに巧妙な策略が仕込まれていたのである。このフィッシングサイトは新しく登録されたドメイン名でホストされており、その新しいドメイン名は複数の有名な検索エンジンでインデックス化され、ページランクが非常に高くなっていた。フィッシャーは、該当する製品に関してよく使われる検索キーワードをドメイン名に使うことで、ページランクを引き上げていた。たとえば、「<よく使われる検索キーワード>.com」のようなドメイン名である。ユーザーがこれらのキーワードを使って検索エンジンで検索を実行すると、ページランクの高いサイトとして表示されたフィッシングサイトにひっかかってしまう羽目になりかねない。

フィッシャーの手口はこれだけにとどまらない。フィッシングページには、ページの下部に偽のトラストシールも表示されていた。正規のトラストシールは、該当する Web サイトが本物であることを保証するためにサードパーティ(通常はソフトウェアセキュリティ企業)によって Web ページに与えられるシールである。トラストシールをクリックすると、サードパーティによって提供されるウィンドウがポップアップ表示され、サイト名の詳細情報と該当サイトの保証に使用される暗号化データが表示される。

フィッシャーはこのセキュリティ対策をどのようにして突破したのか。フィッシャーは、大手 2 社のソフトウェア企業になりすました偽のトラストシールを使っており、そのシールをクリックすると、偽のサイトを参照するウィンドウがポップアップ表示される。偽のサイトの URL では、サブドメインのランダム化が利用されている。サイトの URL は、以下のような形式になっている。

[http://www.\[ソフトウェアセキュリティ会社名\].com.\[偽のドメイン\].com](http://www.[ソフトウェアセキュリティ会社名].com.[偽のドメイン].com)

この URL は一見、適切なサードパーティにトラストシールがリンクされているように見えるが、実際はそうではない。ポップアップウィンドウの URL 全体を注意深く見れば、それが偽のサイトであることがわかる。正規のトラストシールであることを確認するには、シールをクリックし、ポップアップウィンドウの URL 全体を十分に確認するのが最善の方法である。正規のトラストシールであれば、ポップアップウィンドウには、南京錠アイコン、「https」、緑色のアドレスバーなどが使われている。

この記事は、2011 年 9 月 5 日に Mathew Maniyara によってブログ⁴に投稿された。

スパマーやマルウェア作成者による不明瞭化された JavaScript の使用が増加

JavaScript は豊富な機能を備えた動的なプログラミング言語であり、通常使われているデスクトップアプリケーションと機能や応答性の面で引けを取らない、多彩でインタラクティブな Web アプリケーションを開発する際にますます一般的になっている。

しかし、JavaScript の使用が増えているのは Web 開発者だけではない。スパマーやマルウェア作成者によって、リダイレクト先を隠すために、また、場合によっては Web ページ全体を隠すために不明瞭化された JavaScript が使用されるケースが増えている。

⁴ <http://www.symantec.com/connect/blogs/fake-offers-fake-trust-seals>

スパマーにとっては、不明瞭化されたシンプルな JavaScript ページを無料のホスティングサイトに置くことで、サイト運営者がページが悪質な活動に使用されていることに気付くまで、そのサイトの存続期間を延ばすことができる。一般に JavaScript は、危険化した Web サイトの訪問者をスパマーの待ち受けページへとリダイレクトするために使われる。

これらの技法の一部はこしばらくマルウェア配信の方法として一般的であったが、スパマーはますますこれらを使用するようになっていく。

シンプルなりダイレクト

JavaScript は、Web ブラウザやドキュメントインターフェース DOM(Document Object Model)を介して、ユーザーをあるサイトから別のサイトにリダイレクトすることが可能である。これは、スパムやマルウェアの作成者にとって長い間好まれてきた技法であり、作成するリダイレクトの「チェーン」はますます長く複雑になっている(つまり、最終的に目的のサイトにたどり着く前に、リダイレクトを繰り返す)。

不明瞭化技法により、目的の URL または Web サイトのアドレスを、Web ページの HTML ソースを表示したときにその URL が表示されないような程度まで隠すことができる。

非常にシンプルな技法は、目的のアドレスの一部の文字をエスケープ文字に置き換えることである。この表記は、通常、特殊文字を表したり、引用符で囲まれた文字列内に引用符を含めるために使われる。例:

```
location.href=unescape('%68%74%74%70%3a%2f')+'\u002f\u0077\u0077'+'.w.smswi'+'.fe.c'+'\u006f\u006d'+'
```

このコードスニペットは、URI スタイルのエスケープ処理(パーセント記号(%)に 16 進表現が続く形で各文字が表される)と、JavaScript の文字列エスケープ処理(\u に 文字の Unicode コードポイント値が続く)を組み合わせている。実行されると、このコードはブラウザを <http://www.smswife.com> へとリダイレクトする。

これはシンプルな技法だが、一部の基本的なセキュリティ対策における多くの甘いチェックを迂回するにはおそらく十分である。

もう 1 つの類似の技法はユーザーを直接リダイレクトせず、JavaScript コードがドキュメントを更新して、次の例のようにテキストを追加する。

```
document.write(unescape("%3c%68%74%6d%6c%3e%3c%..."))
```

この特定のコードは、一攫千金サイトを宣伝し、サイトが HTML フレーム内でロードされる。

```
<html><head><title>CityVille Secrets - Get Your Exclusive Secrets Guide Today!</title></head><frameset border="0" framespacing="0" frameborder="0" rows="100%,*"><frame name="mainone" marginwidth="0" marginheight="0" src="http://ca748bqp27uuhz67qf1tpaz19f.hop.clickbank.net/"></frameset></html>
```

Eval 関数呼び出しの利用

JavaScript は、動的な言語であり、「eval()」関数を含む。これにより、JavaScript コードをランタイム時に評価(つまり実行)できる。これは強力な機能だが悪用される可能性もある。スパマーやマルウェア作成者は、JavaScript コードの大量の文字列を作成することがよくある。通常、原始的な方法でエンコードされた文字を含む膨大な文字列または配列を繰り返して作成する。これらの大量の文字列が評価されるため、コードの分析がより難しくなる。

この技法の例を以下に示す。

```
sblrvyn=" " + "h" + "t" + "t" + "p" + ":" + "/" + "/" + "v" + "i" + "p" + "-" + "m" + "e" + "d" + "s" + "2" + "4" + "." + "c" + "o" + "m" + "/" ;  
  
document.write('<script>xlkfgizslh="p" + "a" + "r" + "e" + "n" + "t" + "." + "l" + "o" + "c" + "a" + "t" + "i" + "o" + "n" + "." + "href=" + "sblrvyn"; eval(xlkfgizslh);</scr');
```

```
document.write('ipt>');
```

「sblrvyn」変数は、割り当てられているテキスト文字列「http://vip-meds24.com/」を取得する。次に、コードはさらに JavaScript をページに書き込む。この JavaScript は、「parent.location.href=sblrvyn」を「xlkfgizslh」という変数に割り当てる。「sblrvyn」にはリダイレクト先の URL が含まれている。

最後に、JavaScript は「xlkfgizslh」変数の内容を評価し、これにより、Web ブラウザの JavaScript エンジンがコードを実行し、ユーザーを目的の Web サイトにリダイレクトする。

高度な不明瞭化

JavaScript は、リダイレクトを隠すだけでなく、Web ページ全体を不明瞭化するために使われることがある。これはマルウェアでより一般的であり、マルウェア作成者はこのような不明瞭化されたページにホストされている多くの手口を隠そうとする。

一般的な技法は、ページ全体の不明瞭化されたコンテンツを単一の HTML「div」要素に格納することである。この「div」要素は、CSS (Cascading Style Sheets) を使って隠されることが多いので、一見したところランダムな文字の長い羅列は、Web ページを表示するユーザーには表示されない。たとえば、Web ページに次の HTML が含まれているとする。

```
<div id="ReferenceError"><div style="display:none;">504c364c602c413  
... ]</div></div>
```

注: 約 89,000 バイトの長さなので、ここでは不明瞭化されたデータの一部のみを示している。

不明瞭化は、実際のページ内の各文字を数字として表すことによって機能する。これらの数字は、文字「c」によって分割つまり区切られている。したがって、この例で 504、364、602、412 は最初の数文字を表している。「div」要素は「]」要素で終わっている。

この不明瞭化を解読するコードは、「div」内部の文字「c」すべてをコンマに置き換え、先頭に「[」を追加する。文字列は、「[504, 364, 602, 413]」のようになり、前述のとおり、「eval()」関数を使って JavaScript 配列として評価される。次に、配列の各要素（つまり、リスト内の各数字）は、数字「7」で除算され、結果はルックアップテーブルのインデックスとして使われる。このルックアップテーブルが実際の目的の文字を返し、それが文字列に付加され、評価する JavaScript コードがさらに構築される。

このケースでは、コードはページに追加の JavaScript を書き込み、Java、PDF (PDF 閲覧ソフトウェアのさまざまなバージョンに合わせて調整したさまざまな手口を使用)、Flash などのソフトウェア用の手口を含め、多くの手口を試す。

JavaScript の豊富な機能を備えた動的な性質を Web ブラウザ（および Web ページ）への DOM インターフェースと組み合わせることで、スパマーやマルウェア作成者にとっては、不明瞭化の可能性が増え、Web ページの本当の性質が隠されることになる。

この記事は、シマンテックのシニアエンジニアである Nicholas Johnston によって寄稿された。

世界的傾向とコンテンツ分析

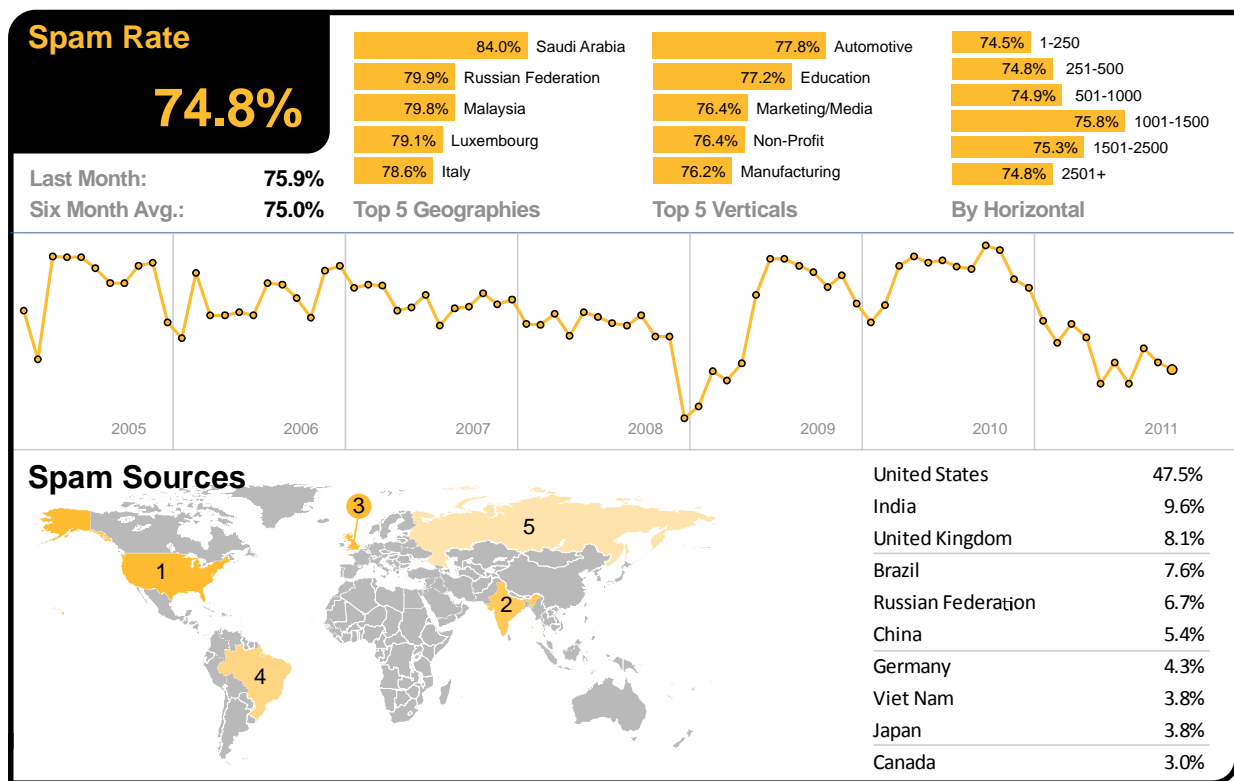
スパム、フィッシング、マルウェアに関するデータは、シマンテックグローバルインテリジェンスネットワーク、シマンテックプロブネットワーク(500万件を超えるダミーアカウントによるシステム)、シマンテックドットクラウドに加えて、シマンテックの数多くのセキュリティ技術を駆使した多彩なソースを通じて収集されている。また、シマンテックドットクラウド独自のヒューリスティック技術である Skeptic™ では、高度なテクニックが用いられた新種のターゲット型攻撃も検知している。

データの収集は、全世界 86 개국以上で行われている。80 億通を超えるメールと 10 億回を超える Web リクエストを通じて得られた情報は、世界 15 か所にあるデータセンターで日々処理され、86 개국の 1 億 3,000 万台以上のシステムからは、悪質なコードに関する情報が収集されている。シマンテックインテリジェンスでは、不正と戦う企業やセキュリティベンダー、さらに 5,000 万人以上の個人ユーザーからなる幅広いコミュニティを通じて、フィッシングに関連した情報を収集している。

こうした多彩なリソースに支えられて、シマンテックインテリジェンスのアナリストは、他に類のないデータを手し、セキュリティに対する攻撃や悪質なコードの動き、フィッシング、スパムの最新動向についての特定や調査を行い、専門的な見地から分析している。悪質な攻撃の発生をいち早く察知して、これを阻止し、お客様への被害を食い止めている。

スパム分析

2011 年 9 月、世界全体のメールトラフィックに占めるスパムの割合は 74.8%(メール 1.34 通に 1 通)で、前月比で 1.1% 減少した。



2011 年 9 月の全体的なスパムレベルが横ばいの中、スパムレート 84.0% であったサウジアラビアが、引き続き最もスパムの標的とされている。ロシアのスパムは 2 番目に多くなっている。中国では、IT サービス業界でのスパムレートが上がり(メールの 89.3% がスパムとしてブロック)、最もスパムレベルが上昇した国となった。

米国とカナダのスパムレベルは、それぞれ 74.5%、74.1% となっている。英国のスパムレベルは 75.5% であった。オランダ、ドイツ、デンマーク、オーストラリアのスパムレベルは、それぞれ 76.4%、75.5%、75.2%、73.3% であった。香港ではメールの

73.9% がスパムとしてブロックされ、シンガポール、日本ではそれぞれ 72.6%、71.6% であった。南アフリカ、ブラジルのスパムレベルは、それぞれ 74.3%、77.1% であった。

9 月に最もスパムの被害を受けた業種は自動車業界で、スパムレートは 77.8% であった。教育業界のスパムレベルは 77.2%、化学/製薬業界は 74.6%、IT サービス業界は 74.4%、小売業界は 74.3%、公共機関は 74.5%、金融業界は 74.3% となっている。

グローバルでのスパム分類

9 月に最も多く見られたスパムは、医薬品関連スパムであったが、アダルト関連のスパムも 2 番目に多くなっている。スパム件名の分析によって、以下のような件名がスパムで多く利用されていることが明らかになっている。

カテゴリー名	2011 年 9 月	2011 年 8 月
Pharmaceutical	52.5%	40.0%
Casino/Gambling	16.0%	7.0%
Unsolicited Newsletters	14.5%	11.5%
Watches/Jewelry	7.5%	17.5%
Unknown/Other	4.0%	2.5%
Adult/Sex/Dating	3.5%	19.0%
Weight Loss	1.5%	<0.5%
Jobs/Recruitments	1.0%	1.0%
Software	0.5%	0.5%
Scams/Fraud/419	<0.5%	0.5%
Degrees/Diplomas	<0.5%	1.5%

スパム件名分析

最新の分析によれば、9 月には、アダルト関連の出会い系のスパム件名の割合が減少し、代わって最も多くなったのが、国際的な配送サービスになりすますポリモーフィック型マルウェアで、医薬品に関連した件名もますます一般的になっている。

順位	2011 年 9 月、スパムで利用された件名	日数	2011 年 8 月、スパムで利用された件名	日数
1	UPS notification	6	(blank subject line)	31
2	Uniform traffic ticket	4	ED-Meds-Antidepressants-And-Pain Relief-Meds-80%-OFF	31
3	You have notifications pending	22	Buy Advanced Penis Enlargement Pill now, it is selling fast.	31
4	SALE OFF: Pharmacy store!	2	Made of the most potent clinically proven natural herbs.	31
5	(blank subject line)	31	Permanently increases length and width of your erection.Advanced Penis Enlargement Pill.	31
6	Re: Windows 7, Office 2010, Adobe CS5 ...	12	Advanced Penis Enlargement Pill.Permanently increases length and width of your erection.	31
7	Sarah Sent You A Message	11	my hot pics :)	23
8	Ed-Meds-Antidepressants-And-Pain Relief-Meds-80%-OFF	25	found you :)	23
9	Fw: Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 ...	9	new pics for you..	24
10	Fw: Windows 7, Office 2010, Adobe CS5 ...	9	im online now	23

スパム URL TLD 分布

トップレベルドメイン(TLD)「.info」の URL が使われたスパムの割合は、9 月には 7.9% 低下し、逆に最も大きく増加したのは「.com」TDL のスパムであった。

TLD	9月	8月	変化 (%)
.com	59.5%	57.6%	+1.9
.info	10.5%	18.4%	-7.9
.ru	8.1%	7.1%	+1.0
.net	5.8%	5.8%	0

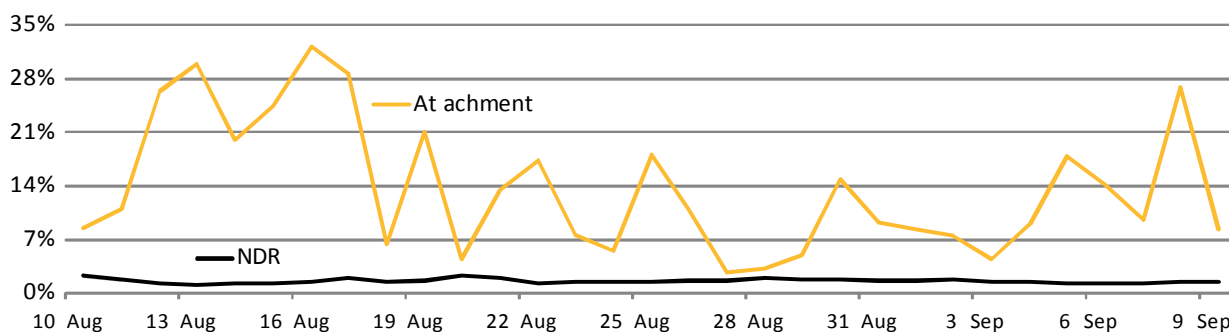
スパムメッセージの平均サイズ

9 月に送信されたスパムのうち、約半数がサイズが 5KB 以下のものだが、添付ファイルを含む、より大きなファイルサイズのスパムが 8 月に比べて 11.2% 増加している。これは、9 月にポリモーフィック型マルウェアの亜種の流通が増加したためである。

メッセージサイズ	9月	8月	変化 (%)
0Kb - 5Kb	48.1%	49.7%	-1.6
5Kb - 10Kb	25.6%	35.2%	-9.6
>10Kb	26.2%	15.0%	+11.2

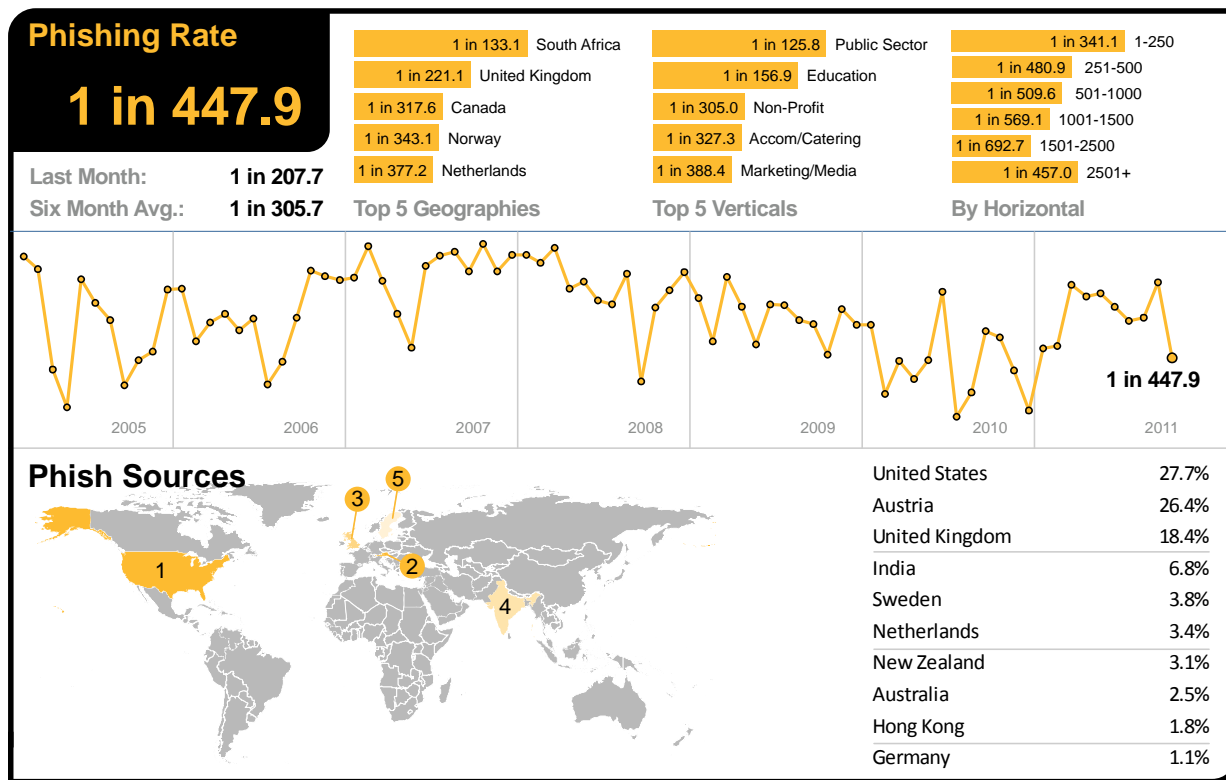
スパムの攻撃ベクトル

下のグラフで示されるように、8 月末から、添付ファイルを伴ったスパムの急増がほぼ 2 日ごとに発生した。これらの添付ファイルは、このレポートの冒頭で説明したように、ポリモーフィック型マルウェアの亜種が増加したことと関連付けられる。さらに、これらの攻撃では、大規模な辞書攻撃の後に通常見られるような、大量の NDR (配信不能レポート) スパムの発生は確認されず、攻撃者はこれらの攻撃を実行するために有効なメール配信リストを使っていると考えられる。また、無効な受信者メールを大量に生成すると IP アドレスがブロックリストに載せられる可能性があるため、配布リストを巧妙に更新してメールが戻ってくるのを最小限にとどめていることも考えられる。



フィッシング分析

9月のフィッシング活動は前月から0.26%減少し、メールの447.9通に1通(0.223%)にフィッシング攻撃が含まれていた。



9月にフィッシング攻撃で最も大きな割合を占めたのは、南アフリカをターゲットとしたもので、メールの133.1通に1通にフィッシング攻撃が含まれており、再び最大の被害国となった。英国は引き続き2位で、メール221.1通に1通にフィッシング攻撃が含まれていた。

米国、カナダのフィッシングレベルは、それぞれ、メール985.9通に1通、317.6通に1通となっている。また、ドイツのフィッシングレベルは、1,125通に1通、デンマークは、1,071通に1通、オランダは、377.2通に1通となっている。オーストラリアでは、740.0通に1通、香港では1,882通に1通、日本では12,812通に1通、シンガポールでは1,958通に1通となっている。ブラジルでは、439.0通に1通がフィッシングとしてブロックされた。

フィッシング活動を業種別に見ると、公共機関では、125.8通に1通にフィッシング攻撃が含まれており、引き続き1位となっている。化学/製薬業界のフィッシングレベルは797.3通に1通、ITサービス業界は754.6通に1通、小売業界は664.5通に1通、教育業界は156.9通に1通、金融業界は388.6通に1通となっている。

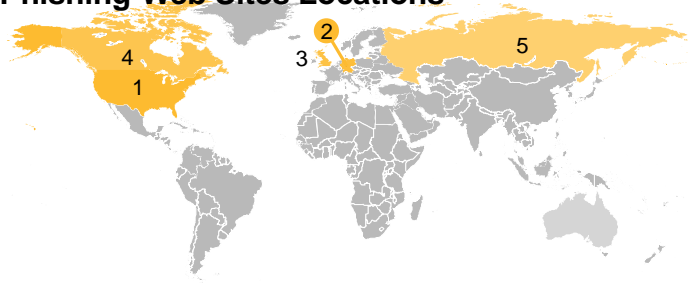
フィッシングサイトの分析

9月、フィッシングサイトの数は12.2%減少した。自動生成ツールによって作成されたフィッシングサイトの数は約38.6%減少している。一意のフィッシングURLの数も2.6%減少しており、ドメイン名でなくIPアドレスを使ったフィッシングサイト(例: http://255.255.255.255)は16.9%減少している。フィッシングサイト全体のうち、正規のWebホスティングサービスを悪用したものの割合は約6%で、前月から32.7%減少した。英語以外の言語によるフィッシングサイトは、14.1%減少した。

9月に発見された英語以外のフィッシングサイトで最も多かったものには、ポルトガル語、フランス語、イタリア語、スペイン語が挙げられる。

フィッシングサイトの所在地

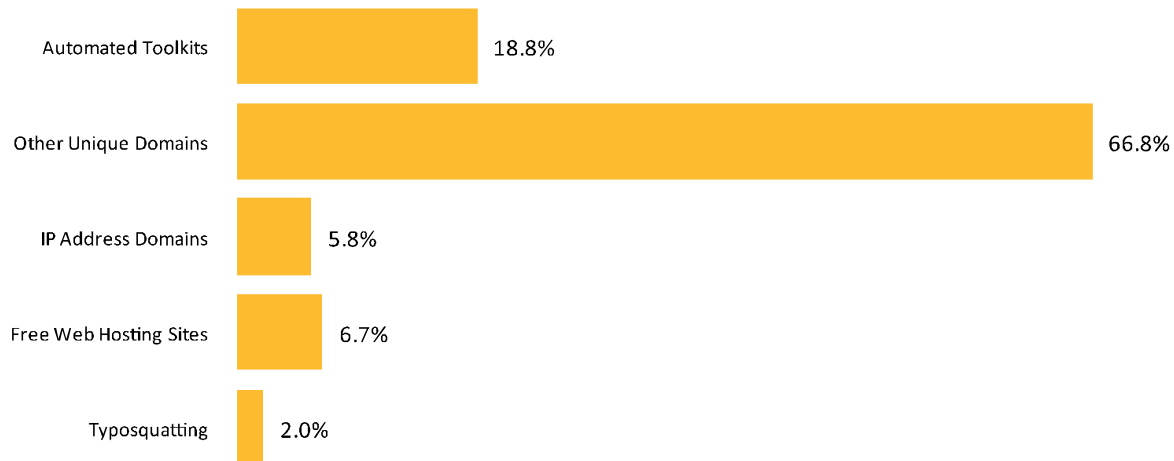
Phishing Web Sites Locations



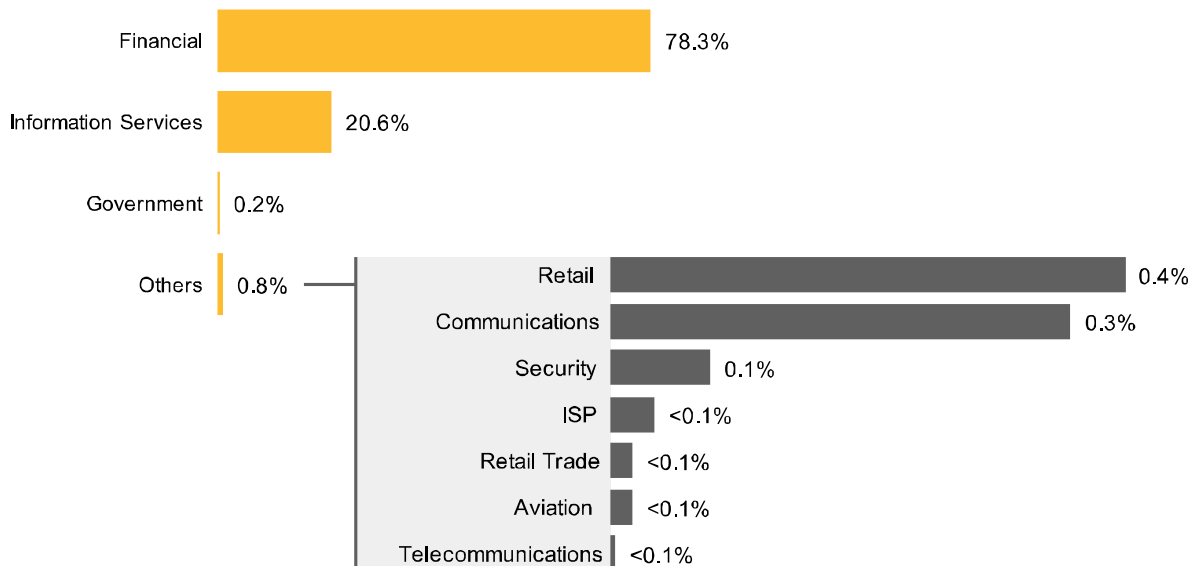
Country	September	August
United States	50.4%	49.8%
Germany	6.2%	6.5%
United Kingdom	3.8%	3.8%
Canada	3.1%	3.7%
Russia	3.0%	3.0%
China	2.7%	2.5%
France	2.6%	2.7%
Brazil	2.5%	2.6%
Netherlands	2.3%	2.3%
Spain	1.5%	<0.5%

September 2011

フィッシング流通の戦術



フィッシングの攻撃のなりすましに利用された企業(業種別内訳)

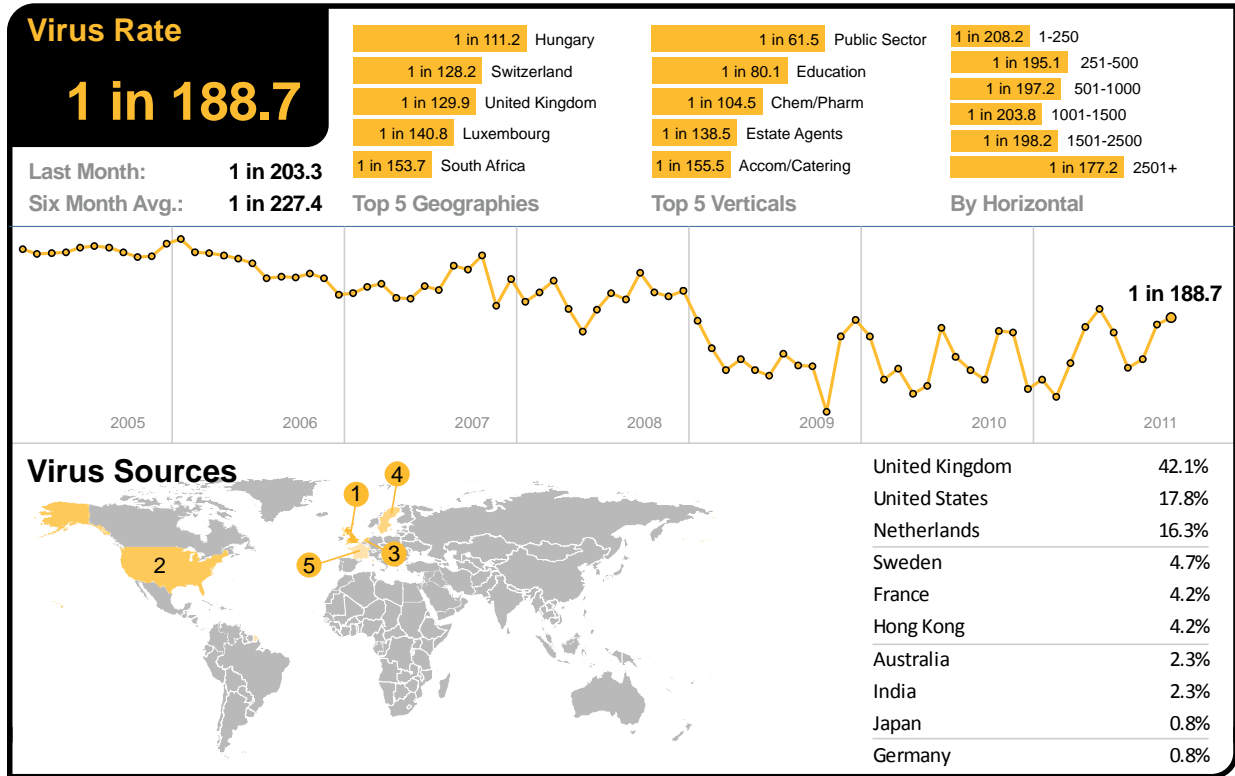


マルウェア分析

メールによる脅威

9月、メール感染型ウイルスがメールトラフィック全体に占める割合は、188.7通に1通(0.53%)で、前月比で0.04%増加した。

9月には、悪質なWebサイトへのリンクが張られたメール感染型マルウェアが、全体の16.5%を占め、前月比で20.5%減少している。ポリモーフィック型マルウェアの亜種を含んだメールのメール感染型マルウェア全体に占める割合は9月には72.0%で、8月の18.5%と比べて増加している。この攻撃では、多くの場合、マルウェアを含んだZIP形式のファイルがメールに添付されている。



9月、ハンガリーでは、メール感染型マルウェアによる攻撃が111.2通に1通の割合に増加し、悪質メールの割合が最も高い国となった。2番目がスイスで、128.2通に1通が悪質であるとしてブロックされた。

英国では、129.9通に1通が悪質であるとしてブロックされ、米国、カナダのメール感染型マルウェアのウイルスレベルは、それぞれ224.8通に1通、164.8通に1通であった。ドイツのウイルスレベルは、197.9通に1通、デンマークは、488.8通に1通、オランダは、174.9通に1通となっている。オーストラリアでは、341.5通に1通、香港では215.6通に1通、日本では658.3通に1通、シンガポールでは307.2通に1通となっている。ブラジルでは、363.5通に1通に悪質なコンテンツが含まれていた。

また、9月にマルウェア攻撃の最大のターゲットとなったのは、前月に引き続き公共機関で、メールの61.5通に1通が悪質であるとしてブロックされている。化学/製薬業界のウイルスレベルは104.5通に1通、ITサービス業界は192.2通に1通、小売業界は276.1通に1通、教育業界は80.1通に1通、金融業界は240.9通に1通となっている。

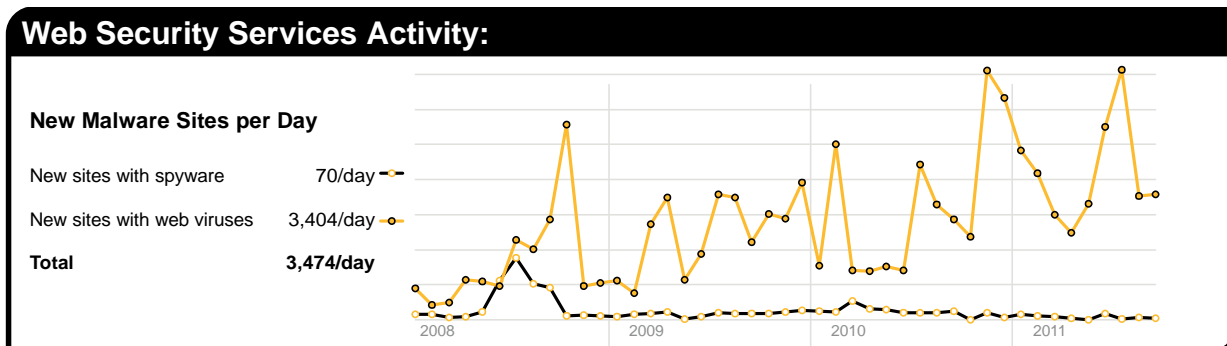
下記の表は、9月にブロックされたメール感染型マルウェアを表している。これらの多くが悪質な添付ファイルを利用したものである。全体として、メール感染型マルウェアの72.0%にBredolab、Sasfis、SpyEye、Zeusの亜種などのポリモーフィック型マルウェアの亜種が関与していた。

マルウェア名	%
Gen:Trojan.Heur.FU.bqW@amtJU@oi	5.1%
Gen:Trojan.Heur.BDT.bqW@b8J!Mvci	4.2%
Gen:Trojan.Heur.BDT.bqW@bS6mfcai	4.1%
Exploit/Link-generic-ee68	3.8%
Gen:Trojan.Heur.FU.bqW@a8Y5GDei	3.6%
Gen:Trojan.Heur.BDT.bqW@bC6h06ii	3.4%
Trojan.Zbot	3.1%
Gen:Trojan.Heur.FU.bqW@aiZha1gi	3.0%
Gen:Trojan.Heur.FU.bqW@a4wN11gi	2.9%
Gen:Trojan.Heur.FU.bqW@a0jG0qpi	2.8%

Web ベースのマルウェアの脅威

9月、シマンテックインテリジェンスでは、マルウェアやその他の不要と思われるプログラム(スパイウェアやアドウェアなど)をホストするWebサイトを1日に平均3,473件特定した。これは、前月比で1.0%の増加となる。これは、Webサイトが危険化されるか、悪質なコンテンツをまき散らす目的で作成された割合を示している。Webベースのマルウェアの流通が長期に及ぶほど数値は高まり、さらに幅広く長期間にわたって生存する可能性が高まる。

検知されるWebベースのマルウェアの数が増加し、新たなマルウェアが確認される例が少数のWebサイトで増え始めているが、新たにブロックされるWebサイトの数は減少している。さらに分析した結果、9月に新たにブロックされた悪質ドメインは全体の44.6%で、前月比で10.0%の増加となっている。また、9月に新たにブロックされたWebベースのマルウェアは、全体の14.5%で、前月比で2.9%の減少となった。



上のグラフは、9月に新たにブロックされたスパイウェアサイトとアドウェアサイトの1日あたりの平均数の増加具合を、Webベースのマルウェアサイトと比較したものである。

不適切なWebサイト利用によるWebポリシーリスク

シマンテックWebセキュリティドットクラウドが、法人顧客向けに採用しているポリシーベースのフィルタリングで、9月に最も頻発したトリガーは、「広告およびポップアップ(Advertisements & Popups)」であり、41.0%となった。「malvertisement」いわゆる不正広告によって、Webベースの広告が悪用されるリスクが高まっている。正規のオンライン広告プロバイダが感染することによって、マルウェアを活動させるバナー広告が、それ以外はまったく無害のWebサイト上に掲載される可能性がある。

2番目に頻繁にブロックされたトラフィックは、ソーシャルネットワーキングとして分類され、ポリシーベースのURLフィルタリングのうち17.7%を占めていた。これは、Webサイト6件に1件がブロックされたことになる。ソーシャルネットワーキングサイトへのアクセスは、多くの企業で許可されているが、アクセスのログ記録を促して利用パターンを追跡したり、1日のうち一定時

間内のみアクセスを認め、それ以外の時間はすべてアクセスを遮断したりするというポリシーを導入するケースもある。こうした情報は、パフォーマンス管理のために用いられることが多く、ソーシャルネットワーキングの多用が生産性の低下を招いた結果の措置だと考えられる。

9月には、ストリーミングメディア (Streaming Media) ポリシー関連のアクティビティが URL ベースのフィルタリングブロックの 8.8% を占めていた。大きなスポーツイベントの開催期間中や国際的に関心の高いニュースが起こると、ストリーミングメディアに人気が集まり、結果として多くのサイトがブロックされる結果となる。企業としては、貴重な帯域をストリーミングメディア以外の目的のために確保しようとしているのである。この数字は、11 件に 1 件の割合でストリーミングメディアを含む Web サイトがブロックされていることを意味する。

Web Security Services Activity:					
Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement & Popups	41.0%	VBS/Generic	42.3%	PUP:9231	37.9%
Social Networking	17.7%	Trojan:GIF/GIFrame.gen!A	24.4%	PUP:W32/CnsMin.S	19.6%
Streaming Media	8.8%	Trojan.Gen	2.8%	PUP:Generic.62006	8.6%
Chat	4.7%	W32.Downadup	2.6%	PUP:Generic.188886	5.3%
Computing & Internet	3.9%	W32.Downadup.B	2.4%	PUP:Generic.183433	3.4%
Peer-To-Peer	2.4%	Gen:Variant.Kazy.34674	2.2%	PUP:WinPump.A	2.8%
Gambling	1.9%	Trojan.Gen.2	1.9%	PUP:Generic.188088	2.7%
Games	1.8%	Bloodhound.Flash.7	1.7%	PUP:Keylogger	1.9%
Hosting Sites	1.7%	New Unclassified Trojan	1.2%	PUP:Heur.xq1@RihoWSii	1.9%
Search	1.6%	Gen:Variant.Kazy.32829	1.0%	PUP:Generic.183172	1.8%
News	1.6%				

September 2011

エンドポイントの脅威

エンドポイントが、防御と分析の最後の砦となっているというケースが多々ある。しかし、USB ストレージ機器や安全とは言えないネットワークへの接続を通じて拡散される攻撃では、多くの場合エンドポイントが防御の最前線となる。この最前線での検知結果を分析することで、企業が直面している脅威、中でも、モバイルワーカーが直面する混合型攻撃による脅威の実態を詳しく知ることが可能である。エンドポイントに到達する攻撃の多くは、ゲートウェイフィルタリングなど、すでに導入されている他の保護層を回避してきたものであると考えられる。

下の表は、エンドポイントデバイスに対する脅威の中で先月最もブロックされたものをまとめたものである。これらは、シマンテックテクノロジーにより保護されている世界中のエンドポイントデバイスのデータ (シマンテック Web セキュリティドット クラウドサービスやシマンテック メール アンチウイルスドット クラウドサービスといった他の保護層を利用していないクライアントのデータを含む) をまとめたものである。

マルウェア名	%
W32.Sality.AE	7.8%
W32.Ramnit!html	7.1%
W32.Ramnit.B!inf	6.2%
Trojan.Bamital	6.1%
W32.Downadup.B	3.9%
W32.SillyFDC.BDP!lnk	3.1%
Trojan.ADH.2	2.8%
Trojan.ADH	2.5%
W32.Virut.CF	2.4%
W32.Almanahe.B!inf	2.2%

9月に最も多くブロックされたマルウェアは、W32.Sality.AE⁶であった。W32.Sality.AE は、実行可能ファイルに感染して拡散し、悪質なファイルをインターネットからダウンロードしようとするウイルスである。2010 年末以降初めて、Sality は Ramnit を

⁵ これらの脅威について詳しくは: http://www.symantec.com/ja/jp/business/security_response/landing/threats.jsp (日本語版)

⁶ <http://www.symantec.com/connect/blogs/sality>

追いついてエンドポイントで最も多くブロックされたマルウェアとなった。2010 年中を通してエンドポイントで最も多くブロックされた悪質な脅威は W32.Sality.AE であった。

W32.Ramnit!html は、W32.Ramnit⁷ に感染した .HTML ファイルを総体的に検知する。W32.Ramnit は、リムーバブルドライブや実行可能ファイルへの感染によって増殖していくワームである。9 月中にエンドポイント保護技術によってブロックされた悪質なソフトウェアのうち、13.5% を Ramnit ワームの亜種が占めている。

新しいウイルスやトロイの木馬の多くが以前のバージョンを基にしており、コードをコピー、または修正することにより、新種や亜種を作成している。これらの亜種の作成には、多くの場合ツールキットが使われ、1 つのマルウェアから数百～数千の亜種を作ることができるようになっている。従来、亜種を検出、ブロックするには、シグネチャを 1 つずつ正確に識別する必要があるため、この方法はシグネチャベースの検出を回避する戦術として広く用いられている。

ヒューリスティック分析やジェネリック検出などの技術を採用することで、同一のマルウェアファミリの複数の亜種を正確に識別、ブロックできるだけでなく、ジェネリックな識別の対象となる特定の脆弱性を狙った新たな悪質コードを見つけることも可能である。先月最も頻繁にブロックされたマルウェアのうちおよそ 20.8% が、ジェネリックな検出を用いて識別、ブロックされた。

⁷ http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2010-011922-2056-99&tabid=2 (日本語版)

企業のためのベストプラクティスガイドライン

- 多重防御戦略の導入:** あらゆるテクノロジーや保護策の単一障害点を防御することができ、互いに重複し相互にサポートできる、複数のレイヤーによる防御システムを構築することが重要である。更新機能を備えたファイアウォールに加え、ゲートウェイ向けウイルス対策、侵入検知、侵入防御システム、ゲートウェイ向け Web セキュリティソリューションなどネットワーク全体をカバーするシステムの導入が必要である。
- ネットワークの脅威、脆弱性、ブランド侵害の監視:** ネットワークへの不正侵入、ワームの侵入行為を始めとする疑わしいトラフィックパターンを監視し、悪質だと判明している管理ホストや疑わしいサイトからの接触を特定する。各種ベンダーのプラットフォーム全体にわたる新たな脆弱性や脅威に対しては、事前に改善措置を講じられるよう、警告を受信するほか、ドメイン警告によるブランド侵害の追跡や偽サイトの通報も必要である。
- エンドポイントでのウイルス対策だけでは不十分:** エンドポイント上のシグネチャベースのウイルス対策機能だけでは、今日の脅威や Web ベースの攻撃ツールから防御しきれない。包括的なエンドポイント向けセキュリティ製品を導入し、次のような防御レイヤーを追加する必要がある。
 - エンドポイントへの侵入防御機能によって、パッチ未提供の脆弱性への攻撃を防ぐとともに、ソーシャルエンジニアリング攻撃から防御し、マルウェアがエンドポイントに到達することを阻止
 - 不明瞭化された Web ベースの攻撃から防御するブラウザ防御機能
 - 未知の脅威に対して未然の防御手段を講じる、クラウドベースのマルウェア対策
 - 急速に変異し多様化するマルウェアを阻止するため、あらゆるアプリケーションや Web サイトのリスクやレピュテーション評価をするファイルおよび Web ベースのレピュテーションソリューション
 - アプリケーションやマルウェアの動作を監視して、マルウェアの動きを阻止することのできる動作阻止機能
 - アプリケーションやブラウザのプラグインによって悪質な不正コンテンツがダウンロードされることを防ぐアプリケーション制御設定機能
 - USB 端末の使用を阻止し、使用できる USB 端末の種類を制限するデバイス制御設定機能
- 暗号化を使って機密情報を保護:** セキュリティポリシーを導入し、機密データを必ず暗号化するよう徹底する。機密情報へのアクセスを制限する。情報漏えい防止 (DLP) ソリューションを導入し、データの特定と監視、保護を実施する。このソリューションの導入によって、データの侵害を防止するだけでなく、組織内からのデータ漏えいの危険性と、それによる損害の発生を軽減することができる。
- データの侵害を防止する情報漏えい防止ソリューション:** DLP ソリューションを導入して、機密データの所在を確認し、使用状況を監視してデータの損失を防ぐ。情報漏えい防止ソリューションによってデータの流れを監視し、ネットワーク上でのデータの組織外への持ち出しや、外部デバイスや Web サイトへの機密データの複製を監視する。DLP が機密データの複製行為やダウンロードを特定して、これを阻止できるよう設定することも必要である。さらに、DLP によってネットワーク上のファイルシステムや PC にある機密、重要情報資産を特定し、暗号化などの適切な対策を講じてデータ漏えいのリスクを軽減できる。
- リムーバブルメディアの使用ポリシーを導入:** 外付けのポータブルハードドライブを始めとするリムーバブルメディアなど、認証されていないデバイスの使用を可能な範囲で制限する。これらは、いずれもマルウェアをネットワークに持ち込む恐れがあると同時に、意図的かどうかにかかわらず、知的所有権の侵害をもたらす恐れもある。もし、外付けメディア機器の使用を許可するのであれば、こうしたデバイスがネットワークに接続されると同時に、ウイルススキャンをかけ、DLP ソリューションを利用して監視を行って、暗号化されていない外部ストレージデバイスへの機密データのコピーを制限する必要がある。
- セキュリティ対策は高頻度かつ迅速に更新:** 2010 年中に、シマンテックが検知したマルウェアの種類は、2 億 8,600 万種を超えており、企業は、ウイルス定義や侵入防止定義を、1 日に何度も更新することは不可能でも、少なくとも 1 日 1 回は更新する必要がある。
- 積極的に更新やパッチを活用:** ベンダーの自動更新機能を活用して、安全性の低い旧バージョンのブラウザやアプリケーション、ブラウザのプラグインについて、更新やパッチ、最新バージョンに移行する必要がある。多くのソフトウェアベンダーが脆弱性に対応するパッチ開発に熱心に取り組んでいるが、パッチ対応は現場で実際に導入されなければ効果がない。安全性の低い旧バージョンを含むブラウザやアプリケーション、ブラウザプラグインの社内使用には、あくまで慎重でなくてはならない。パッチの導入を可能な限り自動化し、組織全体で脆弱性が常に保護された状態を維持しなければならない。

9. **効果的なパスワードポリシーの強化:** 少なくとも 8 文字から 10 文字の長さで、文字と記号を併用した強力なパスワードを設定するよう、ポリシーを強化すべきである。各ユーザーには、同じパスワードを複数の Web サイトで使用しないよう徹底し、パスワードの共有を禁止する。パスワードは定期的に変更し、少なくとも 90 日に一度は変更することが推奨される。パスワードをメモすることも避けなければならない。
10. **メールの添付ファイルを制限:** メールサーバーの設定によって、ウイルス拡散に悪用されがちな .VBS、.BAT、.EXE、.PIF、.SCR などの添付ファイルをブロック、あるいは削除する。また企業ごとにメールへの添付が許されている PDF ファイルの扱い方についても適切なポリシーを検討すべきである。
11. **感染した場合のインシデント対応プロセスを確立する:**
- セキュリティベンダーの連絡窓口を周知し、複数のシステムが感染した場合には、どの担当者に連絡し、どのような対応を取るのかを十分理解する。
 - 外部からの攻撃によってデータが壊滅的な損害を受けた場合にも、データの損失や漏えいをカバーできるバックアップや復元ソリューションを整えておく。
 - Web ゲートウェイ、エンドポイントセキュリティソリューション、ファイアウォールによる感染後の検知機能を活用し、感染したシステムを特定する。
 - 感染したコンピュータを切り離し、組織での感染拡大リスクを防止する。
 - ネットワークサービスが悪質なコードやその他の脅威に利用された場合、パッチが適用されるまでサービスへのアクセスを無効化、ブロックする。
 - 感染コンピュータのフォレンジック分析を実施し、信頼できる媒体を用いてマシンを回復させる。
12. **最新の脅威動向をユーザーに十分伝えること:**
- 受け取ることが事前にわかっている、信頼できる相手から送信されたものでない限り、メールに添付されたファイルを開いてはならない。インターネットからダウンロードしたソフトウェアは、ウイルススキャンなしに実行してはならない(ダウンロードが認められている場合)。
 - 信頼できる発信元や友人から送信されたものであっても、メールやソーシャルメディアプログラムに含まれている URL をクリックするときは十分注意が必要である。
 - あらかじめツールやプラグインを使ってプレビューや展開をすることなしに、短縮 URL をそのままクリックしてはならない。
 - ソーシャルネットワーキングソリューションでの情報のやり取りは慎重に行うことが推奨される。入力した情報が、ターゲット型攻撃や、悪質な URL や添付ファイルの展開の誘いに悪用される恐れがある。
 - 検索エンジンの検索結果に対して警戒を忘れてはならない。検索を行った場合には完全に信頼できるソースを通じてのみリンクをクリックすべきであり、特にメディアで注目されている話題については一層の注意が必要である。
 - 検索結果に Web サイトの評価(レピュテーション)を表示する、Web ブラウザの URL レピュテーションプラグインソリューションを導入すべきである。
 - ポリシーで許されている場合でも、ソフトウェアのダウンロードは、会社の共有ソフトウェア、もしくは、ベンダーの Web サイトから直接ダウンロードを行う場合に限るべきである。
 - ユーザーが、URL をクリックあるいは検索サイトを利用した際、「感染サイト」の警告が表示された場合(偽のウイルス対策の感染)には、Alt-F4 キーもしくは CTRL+W キー、あるいはタスクマネージャを使ってユーザーにブラウザを強制終了させる。

企業ユーザーおよび個人ユーザーのためのベストプラクティスガイドライン

- 1. 個人のセキュリティ対策:** 次のような機能を備えた最新のインターネットセキュリティソリューションを使用して、悪質なコードを始めとするさまざまな脅威に対し、最大限のセキュリティ対策を自ら講じなければならない。
 - 悪質な未知の脅威が実行されることを防ぐ、ウイルス対策(ファイルおよびヒューリスティックベース)やマルウェアの動作阻止機能
 - アプリケーションや使用コンピュータ上で稼働するサービスに脆弱性が見つかった場合に、マルウェアからの攻撃を阻止できる双方向ファイアウォール
 - Web 攻撃ツールや未パッチの脆弱性、ソーシャルエンジニアリング攻撃から防御するための侵入検知機能
 - 不明瞭化された Web ベースの攻撃から防御するブラウザ防御機能
 - 検索エンジンを使った検索結果からファイルや Web サイトをダウンロードする前に、レピュテーション技術を用いたツールで、ファイルや Web サイトの評判や安全性を確認
- 2. 常に最新の情報に更新:** ウイルス定義や安全性情報は、1 時間ごととはいかないまでも、少なくとも 1 日 1 回更新して、常に最新の情報を入手する必要がある。最新のウイルス定義を実装することによって、最新のウイルスやマルウェアから使用端末を守り、これらの拡散を防止する。また、可能であれば、プログラムの自動更新機能を使って、オペレーティングシステムや Web ブラウザ、ブラウザのプラグイン、各種アプリケーションも最新バージョンに更新しておくことが望まれる。古いバージョンを動作させることは、Web ベースの攻撃にさらされるリスクを高める。
- 3. 自分の行動を理解する:** マルウェアや悪質なアプリケーションは、ユーザーの使用端末が感染しているかのように信じ込ませ、ファイル共有プログラムや無料ダウンロード、フリーウェアやソフトウェアのシェアウェアバージョンをユーザーにインストールさせることで、自動的にコンピュータにインストールされる。ユーザーは、次の点に注意しなければならない。
 - 「無料版」「特別提供版」「海賊版」などのソフトウェアにもマルウェアやソーシャルエンジニアリング攻撃が含まれている可能性があり、搭載したプログラムによって、ユーザーの使用コンピュータがあたかも感染しているかのように信じ込ませ、これを削除するために支払を要求してくることがある。
 - インターネット上で Web サイトを訪問する際にも十分な注意が必要である。マルウェアの大半は、依然として人気の Web サイトから侵入するが、マイナーなアダルト系サイトやギャンブル系サイト、違法ソフトウェアサイトなどからも簡単に侵入する。
 - エンドユーザー向け使用許諾契約書(EULA)に同意する前に、注意深く読んで内容を理解すること。EULA に同意すると、セキュリティ上の何らかのリスクをインストールすることにつながる場合がある。
- 4. 効果的なパスワードポリシーの使用:** パスワードには必ず数字と文字を混在させ、頻繁に変更を行うこと。辞書に載っているような一般的な単語をパスワードに使用するべきではない。複数のアプリケーションや Web サイトで、同じパスワードを使ってはならない。大文字と小文字を混ぜたり句読点を使ったり、パスフレーズを使用するなどして、できるだけ複雑なパスワードを使用すること。
- 5. 本当にクリックして大丈夫?:** 受け取ることが事前にわかっている、信頼できる相手から送信されたものでない限り、メールに添付されたファイルを閲覧したり、開いたり、実行したりしてはならない。信頼できる相手から送信されたものであっても、まず、疑ってみるべきである。
 - 信頼できる発信元や友人から送信されたものであっても、メールやソーシャルメディアプログラムに含まれている URL をクリックする時は、十分注意が必要である。あらかじめプレビューやプラグインを使って展開することなしに、短縮 URL をそのままクリックしてはならない。
 - ソーシャルメディアアプリケーション内で、友人から発信されたものであっても、派手なタイトルやフレーズのついたリンクをクリックしてはならない。いったんクリックしてしまうと、リンク以外をクリックしたとしても、クリックのたびにリンクを友人全員に送りつけてしまうようになるかもしれない。リンクをクリックせずに、アプリケーションを閉じてブラウザを終了すること。
 - Web ブラウザの URL レピュテーションソリューションを使って、検索した Web サイトの評判や安全性の評価を確認すること。検索エンジンの検索結果に対して警戒を忘れてはならない。検索を行った場合には完全に信頼できるソースを通じてのみ、リンクをクリックすべきで、特にメディアで注目されている話題については一層の注意が必要である。

- メディアプレーヤーのインストールやドキュメントビューア、セキュリティの更新などを求めるポップアップメッセージは信用しないこと。ソフトウェアのダウンロードは、ベンダーの Web サイトから直接行うこと。
6. **個人データを保護する:** インターネット上、特にソーシャルネットワークで公開された個人情報は、ターゲット型攻撃やフィッシングに悪用される恐れがある。個人情報の公開は必要最小限にとどめること。
- 個人的な秘密情報や個人財務情報は、間違いなく合法である確証がない限り、決して公開すべきではない。
 - 銀行口座、クレジットカード、個人の信用情報をできるだけ頻繁に確認すること。図書館やインターネットカフェなど、公共のコンピュータや、暗号化されていない Wi-Fi 接続を使つてのオンラインバンキングやショッピングは避けること。
 - Wi-Fi ネットワーク経由でのメールやソーシャルメディア、共有サイトへの接続の際には、HTTPS を使うこと。使用中のアプリケーションや Web サイトの設定や個人設定を確認すること。

シマンテック ドット クラウド インテリジェンスについて

シマンテック ドット クラウド インテリジェンスは、セキュリティに関する問題やその動向、統計についての信頼すべきデータと分析を提供している。シマンテック ドット クラウド インテリジェンスは、数 10 億通のメールや Web サイトのスキャンによって得たグローバルセキュリティの脅威に関するデータを、世界 15 カ所を超えるデータセンターからリアルタイムで集め、毎週発表している。世界的に著名なマルウェアやスパムの専門家からなる Skeptic™ チームは、世界 100 カ国で 31,000 社に及ぶクライアントに代わって、日々、数 10 億単位の Web ページやメール、インスタントメッセージの監視を続け、複数の通信プロトコルを通じて引き出されるグローバルの脅威の動向を把握している。詳細情報の参照先:
www.message-labs.com/ja/jp/intelligence

シマンテックについて

シマンテックは、企業および個人の情報を守り、管理を実現するためのセキュリティ、ストレージおよびシステム管理ソリューションを提供する世界的リーダーです。シマンテックのソフトウェアおよびサービスは、さらなるリスクからより多くのポイントを保護し、より完全、かつ効率的に、情報がどこであろうと、使用または保存されている場所で安心を提供します。詳細は www.symantec.com/jp をご覧ください。

Copyright © 2011 Symantec Corporation. All Rights Reserved.

Symantec 社、Symantec ロゴ、Checkmark ロゴは、米国 Symantec Corporation の米国内およびその他の国における登録商標または商標である。その他製品名などはそれぞれ各社の登録商標または商標である。

免責: このレポートに含まれている情報は、無保証として皆様にお届けしており、シマンテック社は、その正確性や使用に際し、一切保証しない。ここで紹介している情報は、ユーザーの責任において使用すること。このレポートは、技術的やその他の誤り、誤植が含まれている場合もある。シマンテックは、事前通告なしで内容の変更をする権利を有する。Symantec Corporation, 350 Ellis Street, Mountain View, CA94043 への明確な書面による許可なしでは、この発行物のいかなる情報も引用、コピーできないものとする。