

シマンテックインテリジェンスレポート: 2012 年 1 月

スパマーは年末年始の休業期間や行事を利用しようとする。

「シマンテックインテリジェンス月次レポート: 2012 年 1 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 12 月および 2012 年 1 月のデータを始めとするデータ解析結果を基にまとめたものである。

Report highlights

- スパム - 69.0% (前月比 1.3% 増): 5 ページ
- フィッシング - メール 370.0 通あたり 1 通でフィッシング攻撃 (前月比 0.06% 増): 8 ページ
- マルウェア - メール 295.0 通あたり 1 通がマルウェアを含む (前月比 0.02% 減): 10 ページ
- 悪質な Web サイト - 1 日あたり 2,102 件の Web サイトをブロック (前月比 77.4% 減): 11 ページ
- スパマーは休日や行事を利用し続けている: 2 ページ
- 企業ユーザーと個人ユーザーのためのベストプラクティス: 14 ページ

はじめに

今月号は 2012 年最初のシマンテックインテリジェンスレポートであり、新しい年がマルウェアから解放される明るい年になるよう祈りたい。今月号のメインピックを読むとわかるように、新年はスパマーがカレンダーの代表的な日付のいずれかを利用する絶好の時期である。

今月号のレポートで引用されている最新の例では、スパマーは危殆化した Web サイトを利用してスパム Web サイトに次々と人々をリダイレクトした。危殆化した Web サイトは、PHP リダイレクトスクリプトをホストするために使われる。ファイル名には「New Year」が使われていることが多く、これは受信者がリンクをクリックするように仕向けるために使われるソーシャルエンジニアリング要素である。2012 年の代表的な行事としては、中国の新年、2 月のバレンタインデー、6 月のロンドンオリンピックなどがあるが、こうした行事がスパム、フィッシング、マルウェアにより今後ますます悪用されていく可能性がある。

昨年 12 月の全体的なスパムレベルは 67.7% で、前月の 70.5% から 2.8% 減少した。しかし、1 月にはスパム活動が 1.3% 増加し、次第に 2011 年 11 月と同様のレベルに戻っているものの、2011 年の平均を下回っている。2011 年にスパマーに数多くの圧力がかけられた結果、現在スパマーはより高度な標的型手法を使っており、引き続き電子メールの代わりにソーシャルメディアを利用している。

最後に、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。

シニアインテリジェンスアナリスト Paul Wood

paul_wood@symantec.com

[@paulwoody](#)

レポートの分析

スパマーは休日や行事を利用し続けている

大みそかから 2012 年 1 月 1 日、その後の数日にかけて、シマンテックインテリジェンスは、新年の行事を利用しているスパマーを特定した。最初は、ユーザーにメールメッセージに含まれているスパムリンクをクリックさせようとしていると考えていた。

その後の調査によって、スパマーが正規の Web サーバーを危殆化し、主な Web サイトコンテンツには一切手を付けず（検出を回避または遅らせるため）、簡単な PHP スクリプトを追加していたことがわかった。スクリプトには「HappyNewYear.php」、「new-year-link.php」、「new-year.link.php」などの名前が使われていた。これらのスクリプトは、単純にスパム医薬品 Web サイトへとリダイレクトするものであった。

次の図 1 からわかるように、これらのリンクを使用しているメッセージの 1 つを分析すると、スパマーの動機がより明らかになる。

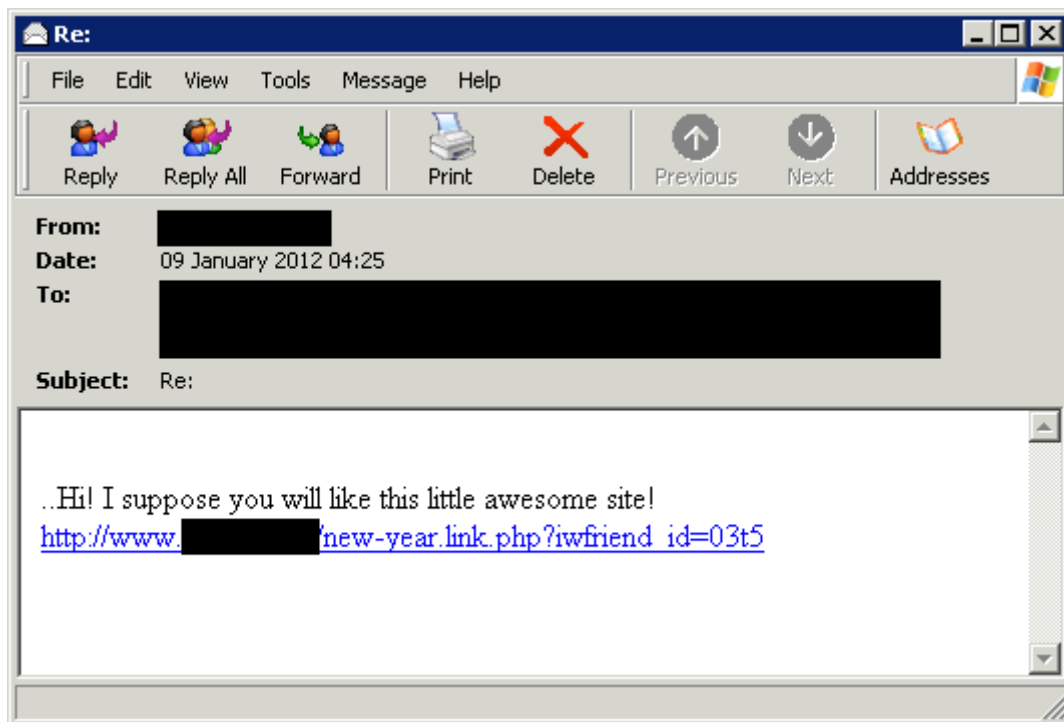


図 1: スпам URL に「New Year」が含まれるスパムメールの例

このメッセージはソーシャルエンジニアリング技法を用いて受信者にリンクを開かせようとしている。URL 内の「friend_id」パラメータから、リンク先が何らかの種類のソーシャルネットワーキング Web サイトであると思わせる。

また、年末年始には、多くの Web サイトやブログがこの 1 年のさまざまな「トップ 10」リストや新しい年の予測を発表するため、「new year」というフレーズを含む URL は関連性や話題性が高いように見え、開かれる確率が高まる可能性がある。

しかし、これはまさにソーシャルエンジニアリング要素であり、図 2 からわかるように、URL はよく知られたスパマーである「My Canadian Pharmacy」Web サイトに（危殆化したコンピュータを経由して）リダイレクトする。



図 2: New Year スпам URL からリダイレクトされるスパム Web サイトの例

シマンテックインテリジェンスは、10,000 を超える一意のドメイン名がこの「new year link」リダイレクトスクリプトによって危険化したことを確認した。「new-year-link.php」のような名前前のファイルの存在は Web サーバーが危険化したことを示している可能性があり、すべてのサーバーが適切にパッチ適用され更新されていることを確認するためのタイムリーな警告として役立つであろう。

これは休日や今話題の行事を利用してメールの訴求力を高めようとするスパマーの最近の事例に過ぎない。2011 年のクリスマスに先駆けて、スパマーは多数の正規小売業者になりすまし、さまざまな製品（通常は偽造時計や医薬品）のクリスマス特別価格や特別サービスを提示した。シマンテックインテリジェンスレポートや一部のブログで別途紹介したとおり、419 詐欺犯もまた、代表的な休日、記念日、今話題の行事や出来事を自分に都合よく利用するスキルを身に付けている。たとえば、昨年日本で起きた壊滅的な大震災、「アラブの春」運動などに関連する詐欺の数が増加した。

また、1 月 23 日は中国の新年（「春節」とも呼ばれる）の祝賀が始まる日である。祝賀は数日間続き、中国で最も重要な伝統的な休日である。中国人が多く住む多くの国や地域もこの休日を祝う。辰年を祝うこの行事への関心は非常に高い。このことはスパマーやマルウェアの作成者がこの年に一度の祭りを悪用しようとする可能性があることを意味する。シマンテックインテリジェンスは、目前に迫っているバレンタインデーを利用するスパマーも登場すると予測している。医薬品スパマーがこの日のロマンチックな意味合いを利用して ED 関連の医薬品を宣伝したり、マルウェアの作成者が「片思いの人」というよくある手口を利用して被害者がうっかりマルウェアをインストールするよう仕向けたりする可能性がある。

バレンタインデーに続いて、ウクライナとポーランドが共同開催する UEFA Euro 2012 サッカー欧州選手権を利用するスパムやマルウェアも多数登場すると予測される。UEFA Euro 2012 が終わると、まもなくロンドン夏季オリンピックである。実際、419 詐欺メッセージにはすでにオリンピックという言葉が多数使われている。これらのメッセージには、「London 2012 Olympic Games.doc」、「LONDON 2012 OLYMPIC GAMES RAFFLE PROGRAM.doc」、「LONDON OLYMPICS LOTTERY WINNER!.doc」などの添付ファイルが含まれていた。次の図 3 に示されているものを含め、これらはほんの数例である。

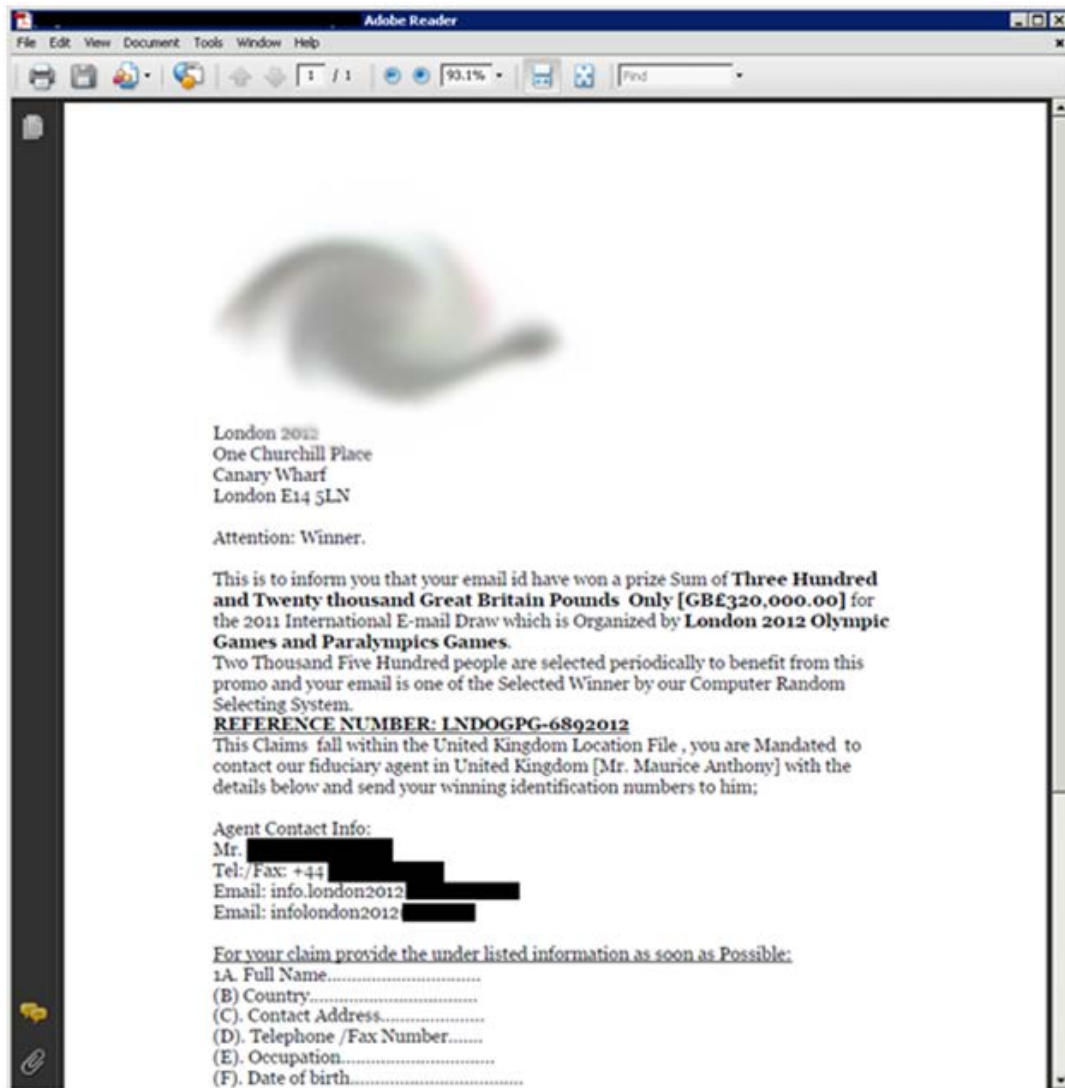


図 3: 大きいスポーツイベントについて触れている 419 詐欺スパムの例

幅広く知られている休日や今世界的な関心が集まる話題の行事にメールを関連付けることにより、スパマーやマルウェアの作成者はメッセージをより興味深いもの(少なくとも一見したところ)にし、受信者がスパム Web サイトを訪問したり感染したりする可能性を高めることができる。

有名な聖バレンタインデーやロンドンオリンピックなどのメジャーな行事が近付いてきており、スパマーが採用するソーシャルエンジニアリングはこれらの行事に対する人々の関心を引くために内容を変更することはほぼ間違いない。これらの行事に関連するスパム活動が増加するだけでなく、フィッシング詐欺や 419 詐欺も増加すると予測される。正規の Web サーバーがこうした最新の攻撃でしばしば悪用されている。引き続き警戒するとともに、Web サーバーやその他の脆弱な可能性があるサーバーのパッチ適用や保守に関するベストプラクティスに従うことが企業にとって特に重要となっている。

世界的傾向とコンテンツ分析

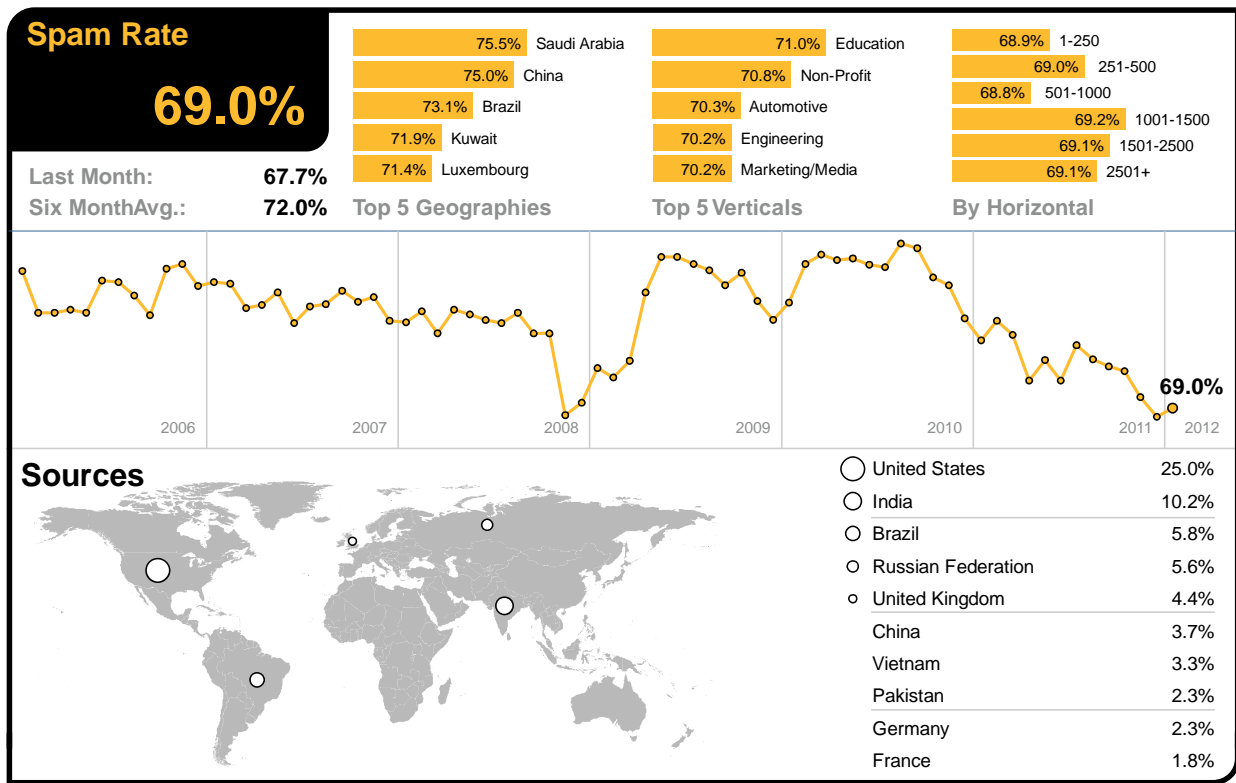
スパム、フィッシング、マルウェアに関するデータは、シマンテックグローバルインテリジェンスネットワーク、シマンテックプロブネットワーク(500 万件を超すダミーアカウントによるシステム)、シマンテックドットクラウドに加えて、シマンテックの数多くのセキュリティ技術を駆使した多彩なソースを通じて収集されている。また、シマンテックドットクラウド独自のヒューリスティック技術である Skeptic™ では、高度なテクニックが用いられた新種の標的型攻撃も検知している。

データの収集は、全世界 86 カ国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 カ所にあるデータセンターで日々処理され、86 カ国の 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入手し、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

2012 年 1 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前月比で 1.3% 増加し、69.0% であった(メール 1.45 通に 1 通)。昨年 12 月の報告では、スパムが 2.8% と大幅に減少して 67.7% となっていた。したがって、この最近の増加は、スパムが 2011 年 11 月と同じレベルにほぼ戻ったことを意味する。



全体的なスパムレートが増加する中、1 月にはスパムレート 75.5% であったサウジアラビアが最もスパムの標的とされている。中国はスパムが 2 番目に多くなっており、ブロックされたメールトラフィック中の 75.0% がスパムであった。

米国とカナダのスパムレベルは、それぞれ 69.0%、68.7% となっている。英国のスパムレベルは 69.3% 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 70.7%、68.2%、69.1%、68.6% であった。香港ではメールの

67.5% 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 66.7%、65.6% 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 69.5%、73.1% であった。

さらに、1 月に最もスパムの被害を受けた業種は教育業界で、スパムレートは 71.0% であった。化学/製薬業界のスパムレートは 69.0%、IT サービス業界は 68.7%、小売業界は 68.4%、公共機関は 68.9%、金融業界は 68.2% となっている。

中小企業(従業員数 1 ~ 250 人)のスパムレートは 68.9%、大企業(従業員数 2500 人超)は 69.1% であった。

グローバルでのスパム分類

1 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、時計/宝飾品のスパムも 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。

カテゴリ名	2012 年 1 月	2011 年 11 月
Pharmaceutical	38.0%	32.5%
Watches/Jewelry	27.5%	19.5%
Adult/Sex/Dating	22.5%	12.5%
Weight Loss	3.5%	8.0%
Unsolicited Newsletters	2.5%	17.5%
Casino/Gambling	2.0%	2.0%
Unknown/Other	1.5%	4.0%
Software	0.5%	2.0%
Scams/Fraud/419	0.5%	1.5%
Degrees/Diplomas	0.5%	<0.5%
Jobs/Recruitments	0.5%	<0.5%
Malware	<0.5%	<0.5%
Phishing	<0.5%	<0.5%

トップレベルドメイン名に基づくスパム URL 分布

次の表に示すとおり、トップレベルドメイン(TLD)が「.com」または「.info」の URL を利用したスパムの割合が 1 月に増加した。

TLD	2012 年 1 月	2011 年 11 月
.com	57.8%	55.1%
.ru	9.4%	9.4%
.info	6.9%	N/A
.org	6.6%	7.4%

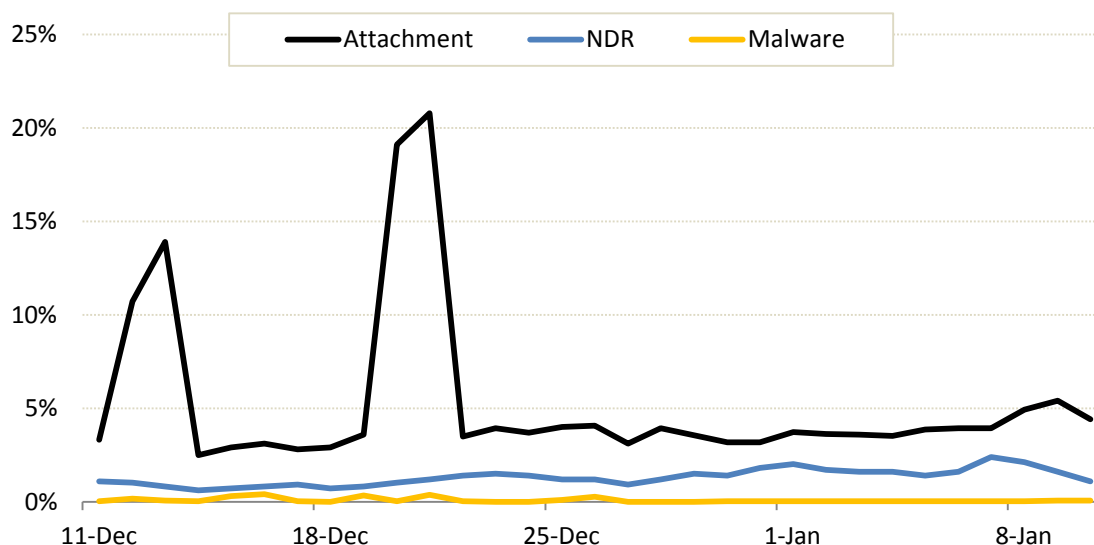
スパムメッセージの平均サイズ

1 月には、サイズが 5 KB 以下のスパムメールの割合は減少した。ただし、次の表からわかるように、サイズが 10KB を超えるスパムメッセージの割合は増加している。

メッセージサイズ	2012 年 1 月	2011 年 11 月
0Kb - 5Kb	55.7%	57.8%
5Kb - 10Kb	30.5%	31.2%
>10Kb	13.8%	11.0%

スパムの攻撃ベクトル

悪質な添付ファイルまたはリンクを含むスパムの割合は、前月より大幅に減少した。期間の前半にスパム活動の急増が2回発生しただけであった。攻撃の頻度は2011年12月末以後、大幅に減少した。サイズが大きい添付ファイルの多くは、これまで多くの¹シマンテックインテリジェンスレポートで説明したとおり、ポリモーフィック型マルウェアの亜種に関連するものであった。

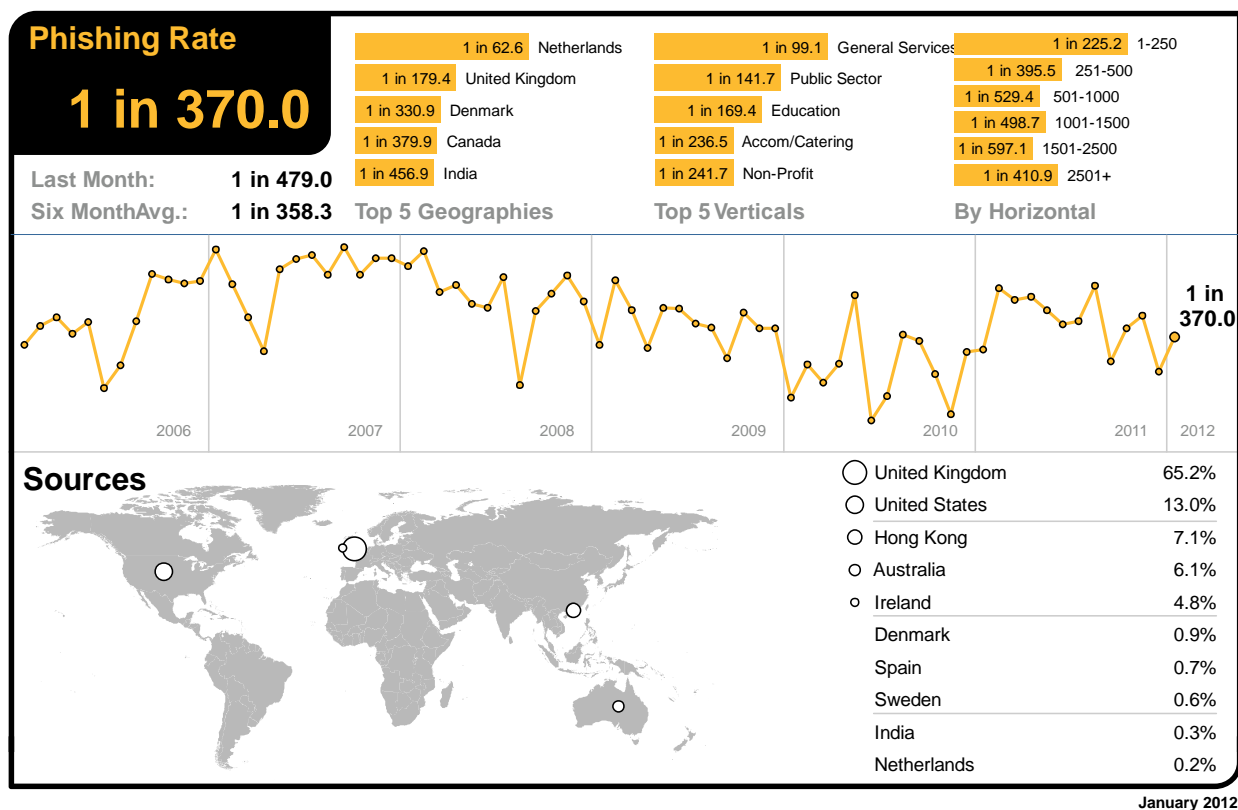


NDR(配信不能レポート)スパムとなったスパムメールの数は、1月も引き続き安定して低くなっており、攻撃者はこれらの攻撃を実行する際に有効なメール配布リストを使い、より高度な標的型手法を使っていると考えられる。NDRスパムは、スパマーが姓名のデータベースを使用してメールアドレスをランダムに生成するスパムキャンペーンでの大規模な辞書攻撃の結果として発生することが多い。この低レベルの活動は、スパマーが配布リストを更新してメールが戻ってくるのを最小限にとどめていることを示す。つまり、IPアドレスが大量の無効な受信者メールと関連付けられると、そのアドレスがスパム対策ブロックリストに載せられる可能性が高まるのである。

¹ http://www.symantec.com/ja/jp/theme.jsp?themeid=state_of_spam

フィッシング分析

1月の全体的なフィッシングレートは前月から0.06%増加し、平均でメールの370.0通に1通(0.27%)にフィッシング攻撃が含まれていた。



1月にフィッシング攻撃で最も大きい割合を占めたのはオランダである。メール62.6通に1通にフィッシング攻撃が含まれており、最大の被害国となった。英国は2位で、メール179.4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1,145通に1通、379.9通に1通となっている。ドイツとデンマークのフィッシングレベルは、それぞれ、797.6通に1通、330.9通に1通となっている。オーストラリアでは、542.2通に1通、香港では942.9通に1通、日本では5,692通に1通、シンガポールでは1,156通に1通となっている。ブラジルでは、1,007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、99.1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838.0通に1通、ITサービス業界は647.8通に1通、小売業界は529.4通に1通、教育業界は169.4通に1通、金融業界は253.7通に1通となっている。

中小企業(従業員数1~250人)を標的にしたフィッシング攻撃は225.2通に1通、大企業(従業員数2500人超)では410.9通に1通であった。

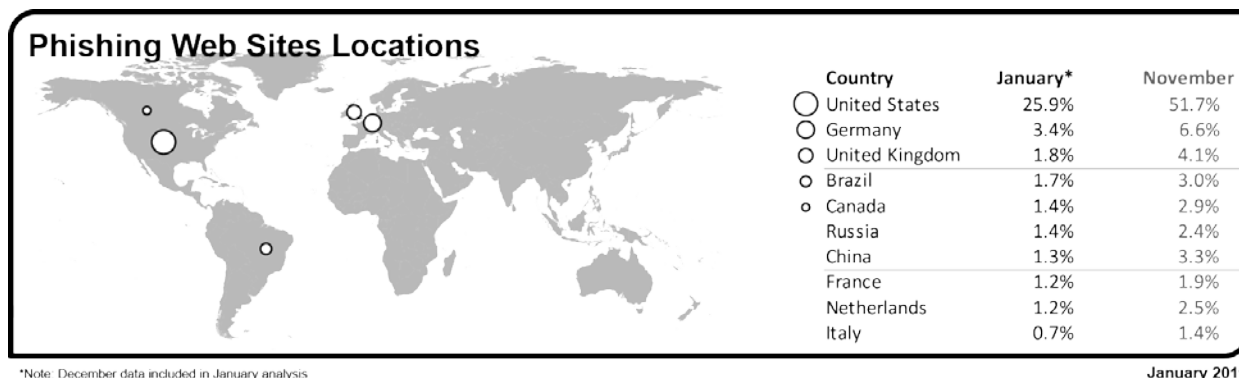
フィッシングサイトの分析

1月、フィッシングサイトの数は18.2%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41.4%減少していて、フィッシングサイトの約42.6%を占めている。これには、有名なソーシャルネットワーキングWebサイトやソーシャルネットワーキングアプリケーションに対する攻撃も含まれている。

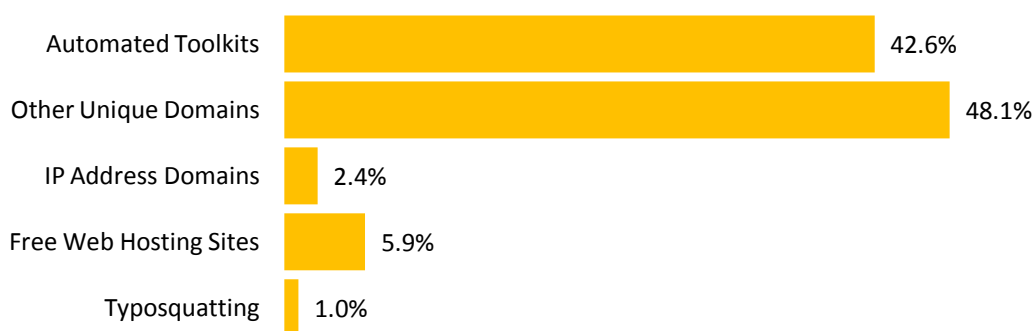
一意のフィッシングドメインの数は15.9%増加しており、ドメイン名でなくIPアドレスを使ったフィッシングサイト(例: <http://255.255.255.255>)は78.0%増加している。フィッシングサイト全体のうち、正規のWebホスティングサービスを悪用したものの割合は約5.9%で、前月から21.2%増加した。英語以外の言語によるフィッシングWebサイトは、41.5%増加した。

1月、英語以外のフィッシングサイトでは、ポルトガル語、イタリア語、フランス語、スペイン語が最も多かった。

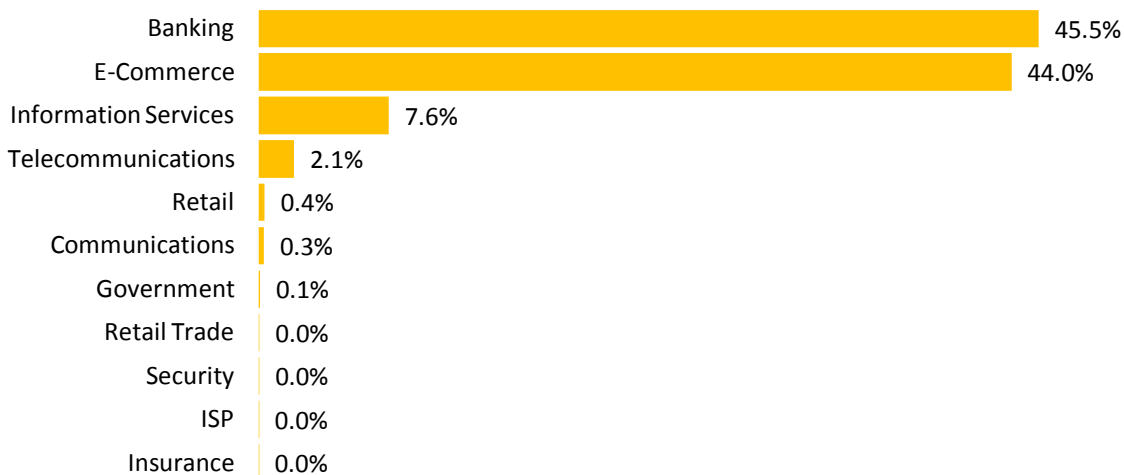
フィッシングサイトの所在地



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)

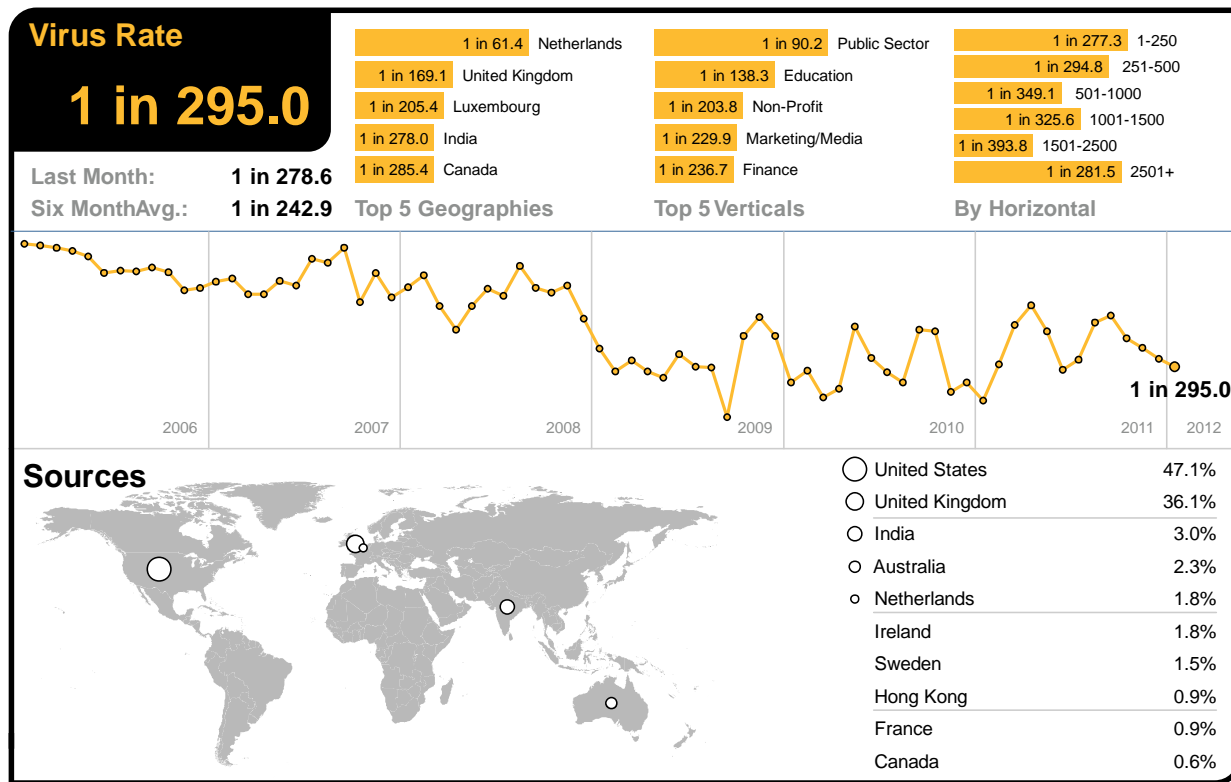


マルウェア分析

メールによる脅威

1 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、295.0 通に 1 通(0.33%)で、前月比で 0.02% 減少した。

1 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 29.0% を占めているが、これは前月から変わっていない。



January 2012

1 月、悪質メールの割合が最も高い国はオランダで、メール 61.4 通に 1 通が悪質メールであった。2 番目が英国で、169.1 通に 1 通が悪質であると識別された。

南アフリカでは、305.9 通に 1 通が悪質であるとしてブロックされた。米国、カナダのメール感染型マルウェアのウイルスレートの、それぞれ 592.5 通に 1 通、285.4 通に 1 通であった。ドイツとデンマークでは、ウイルス活動がそれぞれ 471.7 通に 1 通、318.1 通に 1 通に達した。オーストラリアでは、メール 327.9 通に 1 通が悪質と判定された。日本、シンガポールのウイルスレベルは、それぞれ 1,573 通に 1 通、482.9 通に 1 通となっている。ブラジルでは、681.7 通に 1 通に悪質なコンテンツが含まれていた。

また、1 月にマルウェア攻撃の最大の標的となったのは、前月に引き続き公共機関で、メールの 90.2 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ートの 381.3 通に 1 通、IT サービス業界は 399.4 通に 1 通、小売業界は 407.1 通に 1 通、教育業界は 138.3 通に 1 通、金融業界は 236.7 通に 1 通となっている。

中小企業(従業員数 1 ~ 281.5 人)を標的にした悪質なメール感染型攻撃は 277.3 通に 1 通、大企業(従業員数 2500 人超)では 281.5 通に 1 通であった。

頻繁にブロックされたメール感染型マルウェア

次の表は、1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、メールで配布される悪質な添付ファイルの亜種と悪質なハイパーリンクを利用している。すべてのメール感染型マルウェアのうちおよそ 28.7% が、ジェネリックな検出を用いて識別し、ブロックされた。

1月に、Bredolab、Zeus、SpyEye など、ジェネリックな検出でポリモーフィック型マルウェアの攻撃的な亜種として識別されたマルウェアは、ブロックされたすべてのメール感染型マルウェアの 22.0% を占め、ブロックされたすべてのジェネリックマルウェアの 76.8% に相当する。

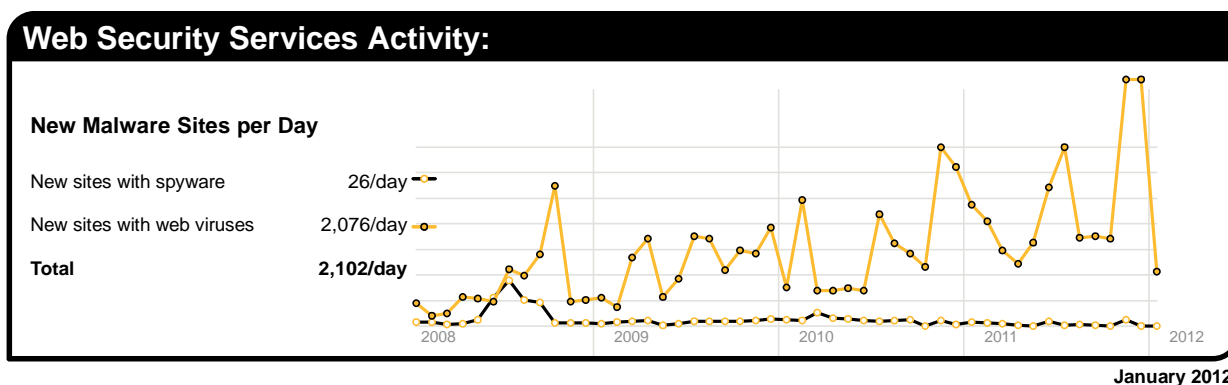
マルウェア名	マルウェアの割合
Exploit/SpoofBBB	7.31%
Exploit/Link-generic-ee68	6.71%
Suspicious.JIT.a	4.36%
VBS/Generic	4.20%
Exploit/LinkAliasPostcard-4733	2.79%
Trojan.Bredolab	2.10%
Trojan.Bredolableml-3a2a	1.58%
HeurAuto-14d6	1.55%
W32/Zbot-gen-c30b-54b2	1.47%
Link-Trojan.IFrame.QZ-544e	1.42%

最も多くブロックされたマルウェアの上位 10 個が 1月にブロックされたすべてのメール感染型マルウェアの約 33.5% を占めた。

Web ベースのマルウェアの脅威

1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望ましくない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 2,102 件特定した。これは、前月比で 77.4% の減少となる。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たものの、新たにブロックされる Web サイトの数は減少し、もともと少数の Web サイトで確認されていた新たなマルウェアが増え始めている。さらに分析した結果、1月に新たにブロックされた悪質ドメインは全体の 39.9% で、前月比で 4.8% の減少となっている。また、1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 15.2% で、前月比で 0.7% の増加となった。



上のグラフは、1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

Symantec Web Security.cloud 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、1 月に最も頻発したトリガーを調べてみると、「広告およびポップアップ (Advertisements & Popups)」であり、32.4% 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。このような不正広告は、正規のオンライン広告プロバイダが感染したり、本来無害な Web サイトでマルウェアを活動させるバナー広告が使われたりするのが原因の一部である。

2 番目に多く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 19.4% を占めていた。これは、ブロックされた Web サイト 5 件のうち 1 件に相当する。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 日のうち決まった時間帯のみアクセスを認め、それ以外はアクセスをすべて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。こうしたことは、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。

1 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 11.0% を占めていた。大きい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、結果としてブロック数が増える結果となる。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、ブロックされた Web サイト 9 件に 1 件の割合に相当する。

Web Security Services Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisement and Popups	32.4%	JS:Trojan.Script.DR	25.3%	PUP:JS.Script.C	21.4%
Social Networking	19.4%	Trojan.JS.WPress.A	18.2%	PUP:MyWebSearch.EC	14.1%
Streaming Media	11.0%	Gen:Variant.Graftor.8369	5.2%	PUP:9231	11.9%
Computing and Internet	4.5%	Trojan.Maljava	3.5%	PUP:Clkpotato!gen3	10.6%
Search	4.0%	Trojan.Script.475646	3.1%	PUP:Generic.183433	9.3%
Chat	3.1%	Trojan.ADH.2	2.4%	PUP:Generic.62006	5.3%
Hosting Sites	2.9%	Trojan.Gen.2	2.0%	PUP:Relevant.BH	3.4%
Games	2.7%	JS.AddedIframe	1.9%	PUP:Generic.183457	2.3%
Peer-To-Peer	2.3%	Trojan.Malscript!html	1.8%	PUP:Generic.391406	1.9%
News	2.0%	Trojan.Script.12023	1.7%	PUP:Generic.376539	1.5%

January 2012

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。

次の表は、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 (Symantec Web Security.cloud サービスや Symantec Email AntiVirus.cloud 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 ²	マルウェアの割合
WS.Trojan.H	26.52%
W32.Sality.AE	6.09%
W32.Ramnit!html	5.88%
W32.Ramnit.B!inf	5.75%
W32.Ramnit.B	5.18%
W32.Downadup.B	2.63%
W32.Virut.CF	1.65%
W32.Almanahe.B!inf	1.63%
Trojan.ADH.2	1.50%
W32.SillyFDC	1.40%

先月最も多くブロックされたマルウェアは、WS.Trojan.H³であった。WS.Trojan.Hは、未分類の脅威に該当するファイルに対するジェネリックなクラウドベースのヒューリスティック手法による検出名である。この検出名で検出されるファイルは、シマンテックによってユーザーにリスクをもたらすと判断され、コンピュータへのアクセスが遮断される。

2011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.AE⁴とW32.Ramnit⁵の亜種であった。1月にエンドポイントでブロックされた全マルウェアのおよそ17.0%をW32.Ramnitの亜種が占め、W32.Salityの全亜種は6.8%であった。

また、Ramnitは最近、主要ソーシャルネットワーキングWebサイトからのIDの盗難に関与している。これらの盗まれたクレデンシャルの多くが感染したユーザーのプロファイルページを介して悪質なリンクの配布に使用され、複数のオンラインアカウントで同じパスワードを使用しているユーザーのリスクを高め、企業ネットワークへの踏み台を攻撃者に提供してしまう可能性があることが報告された。

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13.5%が、ジェネリックな検出を用いて識別、ブロックされた。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。

²これらの脅威について詳しくは：http://www.symantec.com/ja/jp/security_response/landing/threats.jsp (日本語版)

³ http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2011-102713-4647-99

⁴ http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2006-011714-3948-99

⁵ http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2010-011922-2056-99

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、更新やパッチの適用、最新バージョンへの移行を行う必要がある。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、標的型攻撃や、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。

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。
 - 「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て、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経由で公開された個人情報は、標的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 カ国超の 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 © 2012 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。