

シマンテックインテリジェンスレポート: 2011 年 10 月

スパマー自らが無料のオープンソースソフトウェアを使用して、スパムに利用しやすい URL 短縮サービスを運営している。また、東欧では、プレミアムレート SMS ダイヤラーアプリケーションによる被害が拡大し、さらに、Stuxnet 再来の前兆と予想される Duqu も出現した。

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 10 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 9 月および 10 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 - 10 月は、74.2%(前月比 0.6% 減): 7 ページ
- フィッシング - メール 343.1 通あたり 1 通でフィッシング攻撃(前月比 0.07% 増): 10 ページ
- マルウェア - メール 235.8 通あたり 1 通がマルウェアを含む(前月比 0.11% 減): 11 ページ
- 悪質な Web サイト - 1 日あたり 3,325 件の Web サイトをブロック(前月比 4.3% 減): 13 ページ
- ブロックされた悪質 Web サイトのうち、10 月に新たに遮断されたものは、全体の 43.9%(前月比 0.7% 減): 13 ページ
- ブロックされた Web ベースのマルウェアのうち、10 月に新たに確認されたものは、全体の 15.2%(前月比 0.7% 増): 13 ページ
- スパマーが開設した URL 短縮サービスが増加: 2 ページ
- 東欧に出現したソーシャルエンジニアリングの例: 4 ページ
- New シマンテックリサーチ: W32.Duqu - Stuxnet 再来の前兆: 5 ページ
- New シマンテックリサーチ: 最近の Android マルウェアが作成される理由: 6 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: 16 ページ

はじめに

ソーシャルネットワークの登場に伴い、URL 短縮サービスはごく一般的なオンラインツールになった。ここ 2、3 年の間に多くのネット犯罪者が URL 短縮サービスを利用し、本来の合法的なこのサービスがさまざまな方法で悪用され、マルウェアやスパムの流行に一役買っている。2011 年 5 月の関連記事以降も、スパマーは独自の短縮サービスを開設してきたが、それは訪問者をその同じスパム Web サイトにリダイレクトするための Web サイトであった。このような Web サイトでは、実際の短縮サービスが提供されることはなく、短縮した URL の外見を装う単純なリダイレクトが行われる。しかし、シマンテックインテリジェンスは今回初めて、一般に公開され、実際の短縮リンクを生成する本物の URL 短縮サービスをスパマーが開設したことを確認した。これまでのところ、実際の例はスパムメールの中にものみ発見されている。

また、今月は、東欧のユーザーを標的にしたプレミアムレート SMS ダイヤラーも発見された。とりわけ東欧では、プレミアム SMS ダイヤラーがモバイルの脅威動向において常に問題となってきた。今回も例外ではない。このダイヤラーは、有名な VoIP/メッセージングアプリケーションとよく似た名前を用いて、正当なアプリケーションになりすまそうとする。J2ME で記述されており、JVM を実行する Apple 社の iPhone™ デバイスが標的である。

今回、シマンテックの研究者は、このレポート執筆時点で、新たに発見された、悪名高い Stuxnet マルウェアと大部分のコードを共有する標的型攻撃の分析の最中であった。注目すべきことだが、「Duqu」と名付けられたこの新しい脅威の作成者が Stuxnet のバイナリだけでなくソースコードにアクセスできたのだ。つまり、Duqu は、Stuxnet を作成した同じ攻撃者によって作成された可能性がある。

Duqu の直接の目的は、産業施設へのサプライヤーなどの組織からインテリジェンスデータや資産を収集することであるが、その真の意図は別の第三者に対する将来の攻撃を実行しやすくすることにある。つまり、攻撃者は、将来、産業施設に攻撃をしかけるのに役立つような設計図などの情報を狙っている。Duqu は本質的に、将来の Stuxnet 同様の攻撃の前兆なのである。

最後に、シマンテックが発表した新しいホワイトペーパーでは、モバイルマルウェアの将来が展望されている。2011 年にはモバイルデバイス、特に Android プラットフォームを標的にする攻撃が著しく増加したことが確認された。今回の報告で特に焦点を当てているのは、モバイルマルウェアを収益につなげようとする最新の試みが、感染数と比べてほとんど収入に結び付いていないという現状の分析である。そのため、攻撃者が達成できる投資利益率はごく限られている。このホワイトペーパーは、現在利用されているマルウェアの機能と実例を取り上げ、それらがどのように実行されるかなど、モバイルマルウェアによる収益化で最近上位を占めている手口についても詳しい洞察を試みている。攻撃者がモバイルマルウェアの作成に投資し続けるのは、最新の収益化技法および近い将来に登場すると思われる同様の技法が成功する場合のみである。

今月号のレポートをご活用いただくと幸いです。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

スパマーが開設した URL 短縮サービスが増加

シマンテック シニアソフトウェアエンジニア Nick Johnston

シマンテックインテリジェンスレポート(当時の呼称はメッセージラボインテリジェンス)の 2011 年 5 月号では、スパマーがスパムサイトを巧妙に隠し、遮断されにくくするために、独自の URL 短縮サービスを開設している状況について説明した。

この 10 月には、80 以上の URL 短縮サイトを運営するスパマーも確認した。これらはすべて、類似の名前パターンを利用し、トップレベルドメイン「.info」を使用している。ところが、これらのサイトは、5 月に確認した URL 短縮サイトとは異なり、実際に公開されている URL 短縮サイトなのである。これらのサイトでは誰でも短縮 URL を作成でき、図 1 に示すようにそのためのフォームも一般に公開されている。

スパマーは、無料のオープンソース URL 短縮スクリプトを使用して、これらのサイトを運営している。このレポート執筆時点で、このような方法で使用されている 87 のさまざまなドメインが特定された。

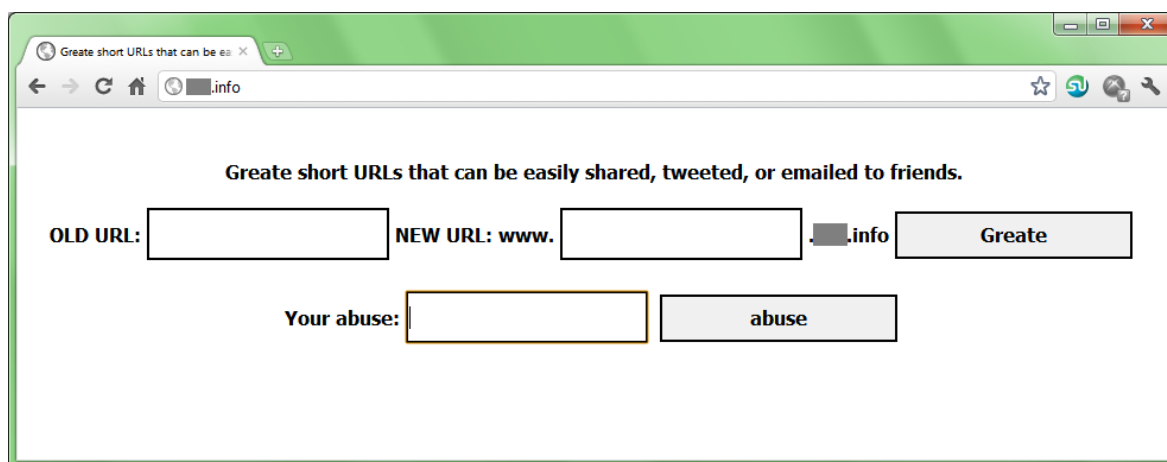


図 1 – スパマーの URL 短縮 Web サイトの待ち受けページ

スパマーは、独自のサービスを使って多数の短縮 URL を作成した後、これらの URL を含むスパムを送信する。スパマーは念入りにも、空の件名と、「It's a long time since I saw you last!(お久しぶりです)」、「It's a good thing you came(来てくださってありがとう)」など、受信者がメッセージを開くように仕向ける件名を混ぜて使用する。図 2 に示すように、これはよくあるソーシャルエンジニアリングの手口である。

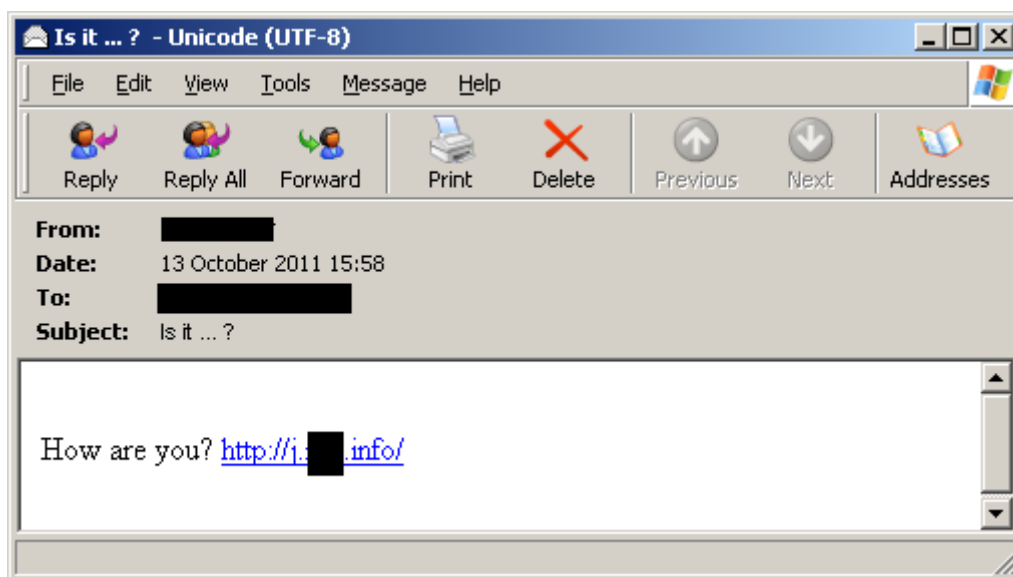


図 2 – スパマー独自の URL 短縮リンクを含むスパムメールの例

メッセージ中の URL は、スパマーの URL 短縮サイトの 1 つを指しており、その後、「Pharmacy Express」という医薬品のスパムサイトにリダイレクトされる。図 3 がその例である。



図 3 – 特注のスパム URL 短縮サービスのリダイレクト先となるスパム Web サイト

URL 短縮サイトに使用されるドメインの連絡先情報はすべて同じで、モスクワを基盤とするものばかりである。これらのドメインはすべて、大規模なホスティング企業の英国子会社によってホスティングされている。この会社には連絡済みである。

長期間悪用されてきた合法的な URL 短縮サイトでスパムその他の悪意ある URL の検出状況が少なくなったことは、スパマーが独自の URL 短縮サイトを開設している可能性があるということである。この種のサイトが公開されている理由はわからないが、おそらく、スパマーの側の怠慢という単純な理由であろう。あるいは、当該サイトをより合法的に見せるためかもしれない。

図 4 のグラフで示されるように、合法的な URL 短縮サービスは引き続き利用されているが、今年の前半で見られたような使用率を維持してはいない。合法的な URL 短縮サービスはかなりの数に上り、常に増加しているものの、大手有名サービスの多くは、スパマーがサービスを悪用することを困難にする処置を完了しており、悪用した場合、リンクはきわめて短時間のうちに解除されるのが普通である。

10 月には、すべてのスパムの約 0.5% が合法的なサービスからの短縮 URL を含んでいた(瞬間的には 2% ないし 3% のピークを示している)。

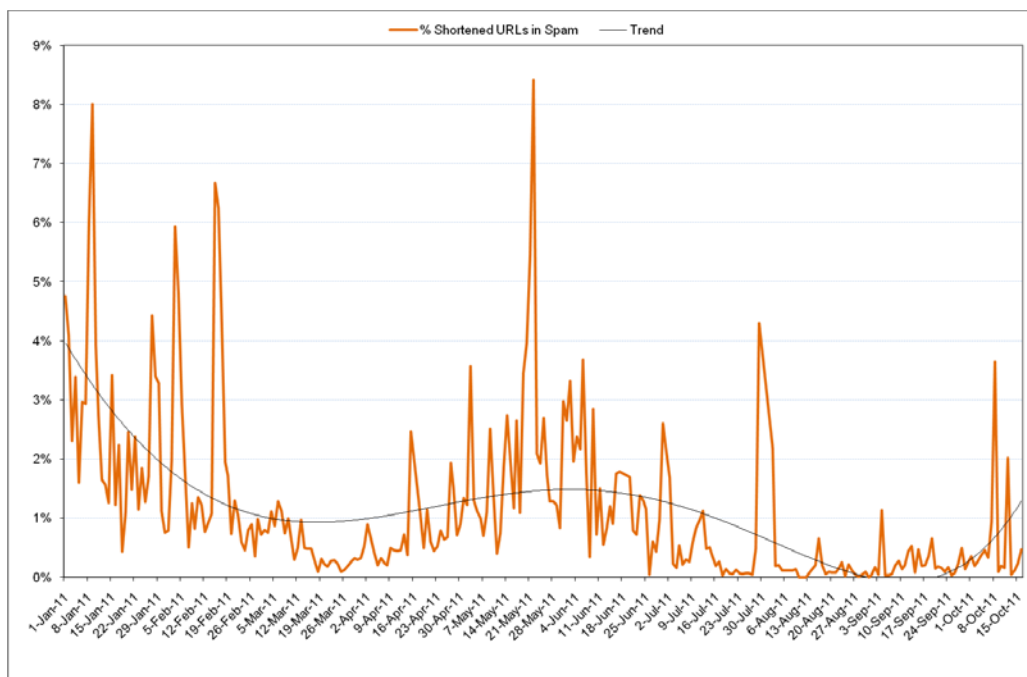


図 4 – 合法的な URL 短縮サービスからのリンクを含むスパムの割合

いずれにせよ、スパマーが URL 短縮サービスを悪用し、自分たちのスパムサイトをできるかぎり隠そうとすることは、今後も続くと思われ。

東欧に出現したソーシャルエンジニアリングの例

シマンテック シニアセキュリティレスポンスマネージャ 今野俊一

最近、新しい脅威 [Android.Fakeneflic](#)¹ が、北米のモバイルユーザーを標的にするために、合法的なビデオストリーミングサービスの[可用性に存在する格差を利用](#)²した。ここにもソーシャルエンジニアリングが働いている。ただし、今回の記事では、標的は東欧のユーザーである。

とりわけ東欧では、プレミアム SMS ダイヤラーがモバイルの脅威動向において常に問題となってきた。東欧では、モバイルデバイス用の Java 仮想マシン (JVM) Micro Edition の登場後まもなく、モバイルフォン向けのダイヤラーが現れた。この有利な収益源への投機を引き起こせるアプリケーション作成者は、より新しいプラットフォームに標的を切り替えていくことは、自然の成り行きである。

ちなみに最近、私たちの注意を引いたダイヤラーは、有名な VoIP/メッセージングアプリケーションを模倣して、正当なアプリケーションになりすまそうとする。このダイヤラーは J2ME で記述されており、JVM を実行する Apple 社の iPhone™ デバイ

¹ http://www.symantec.com/ja/jp/business/security_response/writeup.jsp?docid=2011-101105-0518-99

² <http://www.symantec.com/connect/blogs-231>

スが標的である。このダイアラーの場合、図 5 に示すように、作成者はアプリケーションを宣伝するためダミーの Web サイトさえ開設していた。



図 5 – 詐欺のダイアラーアプリケーションを宣伝するダミー Web サイトの例

手のひらにぴったり収まるサイズながらもコンピュータと同様の機能を持つようになったスマートフォンは、企業のコミュニケーションツールとして使われている。この便利な機能を持つスマートフォンは、同時に大きな危険を引き起こす。スマートフォンは、保護という観点からはしばしば見過ごされている。本来であれば、これらのデバイスにも企業コンピュータと同種の適切な権限とポリシーを実装することが重要である。この詐欺の Web サイトとその脅威は、10 月初めに初めて発見された後、今はアクセスできなくなっている。

New シマンテックリサーチ: W32.Duqu - Stuxnet 再来の前兆

10 月 14 日、シマンテックは、ブダペスト工科大学 (Budapest University of Technology and Economics) の電気通信学部 に所属する CrySyS (Laboratory of Cryptography and System Security) から、新たに発見された標的型攻撃についての警告を受け取った。それは、そのコードの大部分を悪名高い Stuxnet マルウェアと共有している。シマンテックの研究者はこの脅威を分析してきたが、中でも最大の注目点は、W32.Duqu と呼ばれるこの新しい脅威の作成者が明らかに Stuxnet のバイナリだけでなく Stuxnet のソースコードにアクセスできたことである。つまり、Duqu は、Stuxnet を作成した同じ攻撃者によって作成された可能性がある。

ただし、Duqu は、産業施設へのサプライヤーなどの組織からインテリジェンスデータや資産を収集するように設計されており、その直接の目的は Stuxnet とは異なる。その真の意図は別の第三者に対する将来の攻撃を実行しやすくすることにある。攻撃者は、将来、産業施設に攻撃をしかけるのに役立つような設計図などの情報を狙っている。つまり、Duqu は本質的に、将来の Stuxnet 同様の攻撃の前兆なのである。

この脅威についてのテクニカルペーパーもシマンテックから公開されている。詳しくは、[こちら](#)³を参照されたい。

シマンテックは、W32.Duqu 脅威と関連する一部のマルウェアファイルはコードサイン証明書と関連付けられた秘密鍵を用いて署名されており、その証明書はすぐ後に取り消されたことも確認した。また、この鍵の使用状況を調査した結果、Duqu の署名に使われた秘密鍵は盗まれたもので、このマルウェアのために不正に作成されたのではないという結論に達した。なお、いかなる時点でもシマンテックのルート CA および中間 CA がリスクにさらされたことはなく、中間であれ他のベリサインや Thawte ブランドの証明書であれ、いかなる CA にも何の問題も生じなかった。

³http://www.symantec.com/ja/jp/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

要点:

- Stuxnet ソースコードを使用した実行可能ファイルが発見された。最後の Stuxnet ファイルのリカバリ後に開発されたと思われる。
- この実行可能ファイルは、キー操作、システム情報などの情報を取得するように設計されている。
- 最新の分析で、産業用制御システム、悪用、自己複製と直接関係するコードは見つかっていない。
- この実行可能ファイルは、産業施設向けサプライ品の製造に関係する企業など、限られた組織で発見されている。
- 漏えいしたデータは、将来の Stuxnet 同様の攻撃を実現するために利用されるおそれがある。

New シマンテックリサーチ: 最近の Android マルウェアが作成される理由

シマンテック テクニカルディレクタ Eric Chien

モバイルマルウェアが爆発的に増加する日も遠くない。サイバーセキュリティ業界は、しばらく前からそう警告してきた。それが今年に入って本格化し、実際にモバイルデバイスを標的とする脅威は急増した。そのなかでも顕著なのは Android プラットフォームに対する脅威である。ただし、予測されていたように爆発的に増えたわけではなく、現実には、サイバー犯罪はまだまだ手探り状態であり、モバイルデバイスの悪用から利益を上げる方法を見出そうとしている段階だからである。今回の報告で特に焦点を当てているのは、モバイルマルウェアを収益につなげようとする最新の試みが、必ずしも感染数と比べてほとんど収入に結び付いていないという現状である。そのため、攻撃者が達成できる投資利益率はごく限られている。

弊社のホワイトペーパーでは、モバイルマルウェアによる収益化で最近上位を占めている手口についても詳しく書かれており、それぞれの動作と、実行に使われているマルウェアのサンプルを示しているが、特に以下のような手口が知られている。

- 有料電話料金請求詐欺
- スパイウェア
- 検索エンジンポイズニング
- ペイパークリック詐欺
- ペイパーインストール手法
- アドウェア
- mTAN(モバイルトランザクション認証番号)の窃盗

感染数に対する収益率は今でこそまだ足踏み状態を続けているものの、上昇に転じる時期が来たとも指摘している。その引き金となるのは、モバイル向けに有料サービスの技術が進歩すること、金銭の支払いだけでなく受け取りにも広くモバイルデバイスが活用されることだろうと考えられるからである。これらの用途で重要なのは、モバイルバンキングの口座情報のように、実際の資金に裏付けられた財務情報がデバイス上で送信される点である。そのため、組織的なサイバー犯罪者たちは、この情報を狙っている。彼らは、この情報の悪用や売買がいかにか大きな儲けとなるか、PC の世界で理解しているからである。

現在、多くのベンダーが、スマートフォンやタブレットなどのモバイルデバイスを POS 機器として利用している。たとえば、農作物直販ベンダーやタクシー運転手は専用の POS 端末など使わず、客のクレジットカードを自分のスマートフォンにさっとかざすだけだ。また大規模小売店でも、従来の POS 端末の代わりに一般的なスマートフォンやタブレットが当たり前になってきている。悪質な攻撃者がこうした機器に侵入するのは、従来型の POS 端末よりはるかに簡単であり、感染に成功すればクレジットカードの取引はすべて盗み出されてしまう恐れがある。

このほか、近い将来に登場しそうな収益確保手法の候補として、次のような手口も紹介されている。

- IMEI(国際移動体装置識別)番号を盗み出し、以前に遮断された電話や偽造電話などに利用する。
- 偽のセキュリティ製品を売り込む。これも、PC の世界で大きな成果を上げてきた戦術の応用である。

このホワイトペーパーでは、すでに確認されているものでも、今後予想されるものでも、収益化の手口が成功しさえすれば、攻撃者は Android マルウェアの作成に今後も投資を続けるだろうと予測している。

正式のホワイトペーパー(PDF): [Motivations of Recent Android Malware](#)⁴

⁴http://www.symantec.com/ja/jp/content/en/us/enterprise/media/security_response/whitepapers/motivations_of_recent_android_malware.pdf

世界的傾向とコンテンツ分析

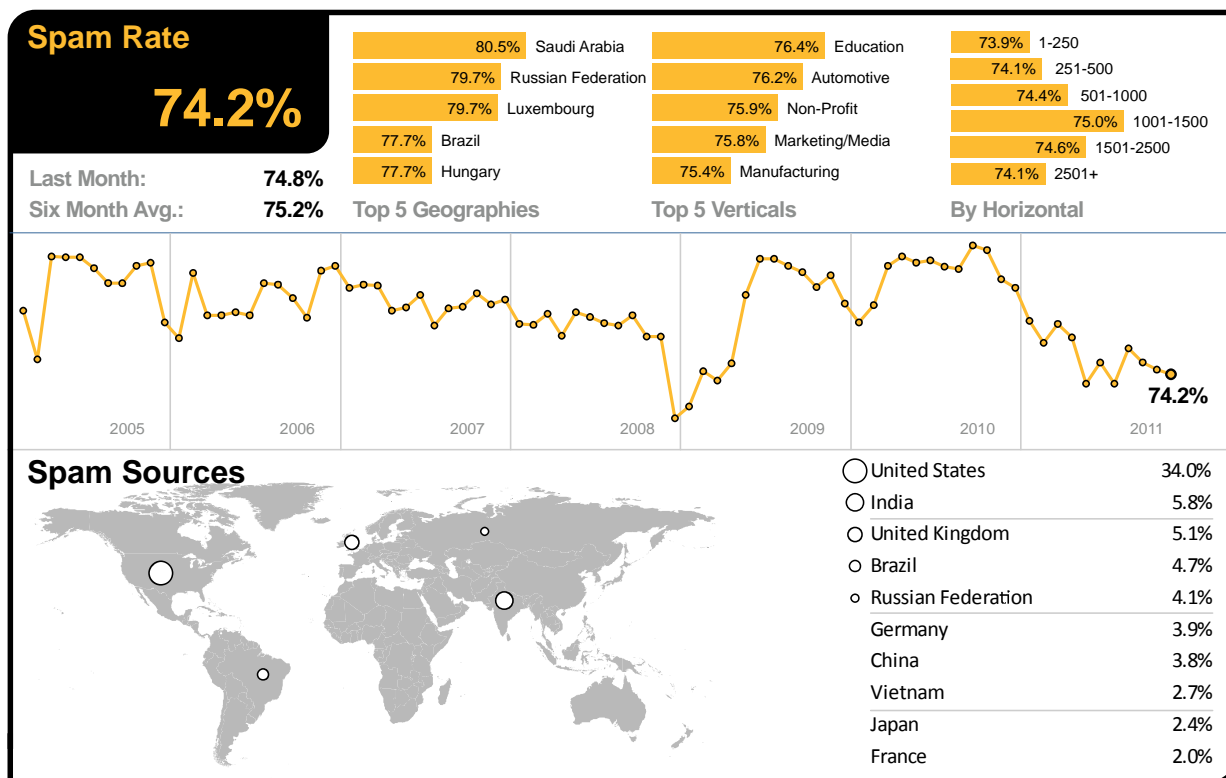
スパム、フィッシング、マルウェアに関するデータは、シマンテックグローバルインテリジェンスネットワーク、シマンテックプロブネットワーク(500万件を超すダミーアカウントによるシステム)、シマンテックドットクラウドに加えて、シマンテックの数多くのセキュリティ技術を駆使した多彩なソースを通じて収集されている。また、シマンテックドットクラウド独自のヒューリスティック技術である Skeptic™ では、高度なテクニックが用いられた新種の標的型攻撃も検知している。

データの収集は、全世界 86 か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 か所にあるデータセンターで日々処理され、86 か国の 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

2011 年 10 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 74.2%(メール 1.35 通に 1 通)で、わずかではあるが前月比で 0.6% 減少した。



October 2011

2011 年 10 月の全体的なスパムレベルが横ばいの中、スパムレート 80.5% 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。ロシアも引き続きスパムが 2 番目に多くなっており、メールトラフィック中の 79.7% 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 73.8%、73.2% となっている。英国のスパムレベルは 74.8% 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 75.6%、74.8%、75.7%、72.8% であった。香港ではメールの 73.4% 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 72.2%、70.8% 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 74.8%、77.7% であった。

10月に最もスパムの被害を受けた業種は教育業界で、スパムがわずかながら減少したにもかかわらずスパムレート76.4%で、自動車業界を上回った。化学/製薬業界のスパムレベルは74.0%、ITサービス業界は73.8%、小売業界は74.0%、公共機関は73.8%、金融業界は73.5%となっている。

中小企業のスパムレートは73.9%、大企業は74.1%であった。

グローバルでのスパム分類

10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10月	2011年9月
Pharmaceutical	37.5%	52.5%
Casino/Gambling	23.5%	16.0%
Watches/Jewelry	15.0%	7.5%
Unsolicited Newsletters	6.5%	14.5%
Scams/Fraud/419	6.0%	<0.5%
Weight Loss	4.5%	1.5%
Adult/Sex/Dating	2.5%	3.5%
Unknown/Other	1.5%	4.0%
Software	1.5%	0.5%
Jobs/Recruitments	0.5%	1.0%
Degrees/Diplomas	0.5%	<0.5%
Malware	0.5%	0.5%
Phishing	0.5%	0.5%

スパム件名分析

最新の分析によれば、10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10月、スパムで利用された件名	日数	2011年9月、スパムで利用された件名	日数
1	NACHA security nification	2	UPS notification	6
2	ACH Payroll Cancelled	2	Uniform traffic ticket	4
3	ACH Transfer Review	6	You have notifications pending	22
4	Re: Back to School Software Sale	6	SALE OFF: Pharmacy store!	2
5	0	6	(blank subject line)	31
6	Facebook Administration has sent you a notification	9	Re: Windows 7, Office 2010, Adobe CS5 ...	12
7	Fw: Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 ...	18	Sarah Sent You A Message	11
8	Re: Windows 7, Office 2010, Adobe CS5 ...	18	Ed-Meds-Antidepressants-And-Pain Relief-Meds-80%-OFF	25
9	Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 ...	18	Fw: Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 ...	9
10	Re: Re: Re: Re: Re: Windows 7, Office 2010, Adobe CS5 ...	18	Fw: Windows 7, Office 2010, Adobe CS5 ...	9

スパム URL TLD 分布

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は、それぞれ 2.2%、2.3% 低下し、増加したのは TLD が「.ru」のスパムのみであった。

TLD	10月	9月	変化 (%)
.com	57.3%	59.5%	-2.2
.info	8.2%	10.5%	-2.3
.ru	8.4%	8.1%	+0.3
.net	5.3%	5.8%	-0.5

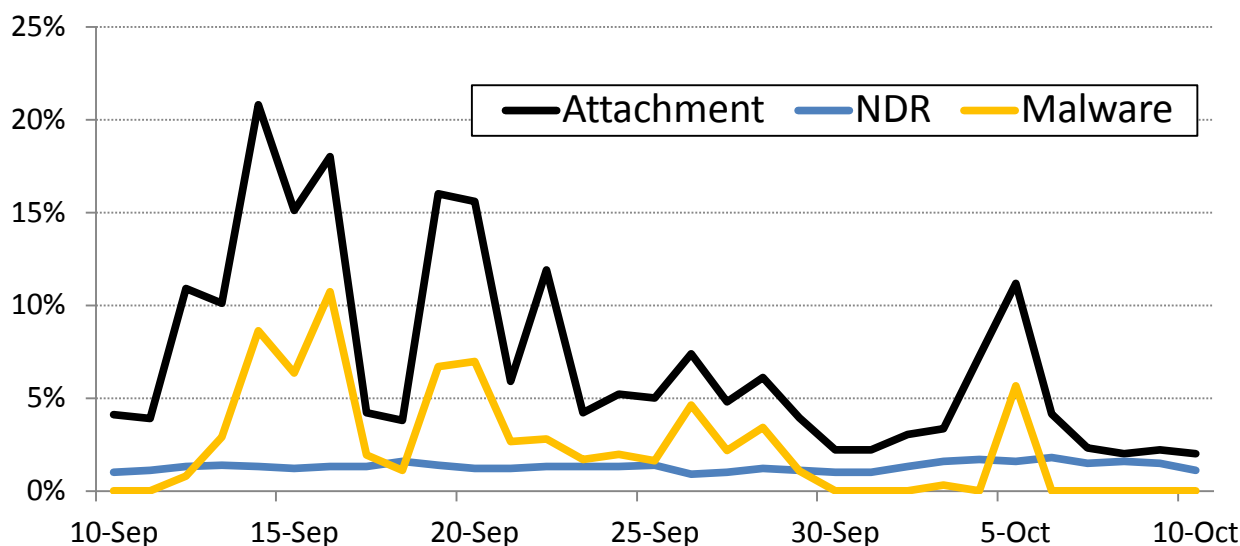
スパムメッセージの平均サイズ

10月に送信されたスパムメールでは、5通のうち約3通の割合でサイズが5KB以下であったが、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9月に比べて11.5%減少した。これは、10月に、ポリモーフィック型マルウェアの亜種を利用したマルウェア攻撃の件数が減少したためである。

メッセージサイズ	10月	9月	変化 (%)
0Kb - 5Kb	59.0%	48.1%	+10.9
5Kb - 10Kb	26.3%	25.6%	+0.7
>10Kb	14.7%	26.2%	-11.5

スパムの攻撃ベクトル

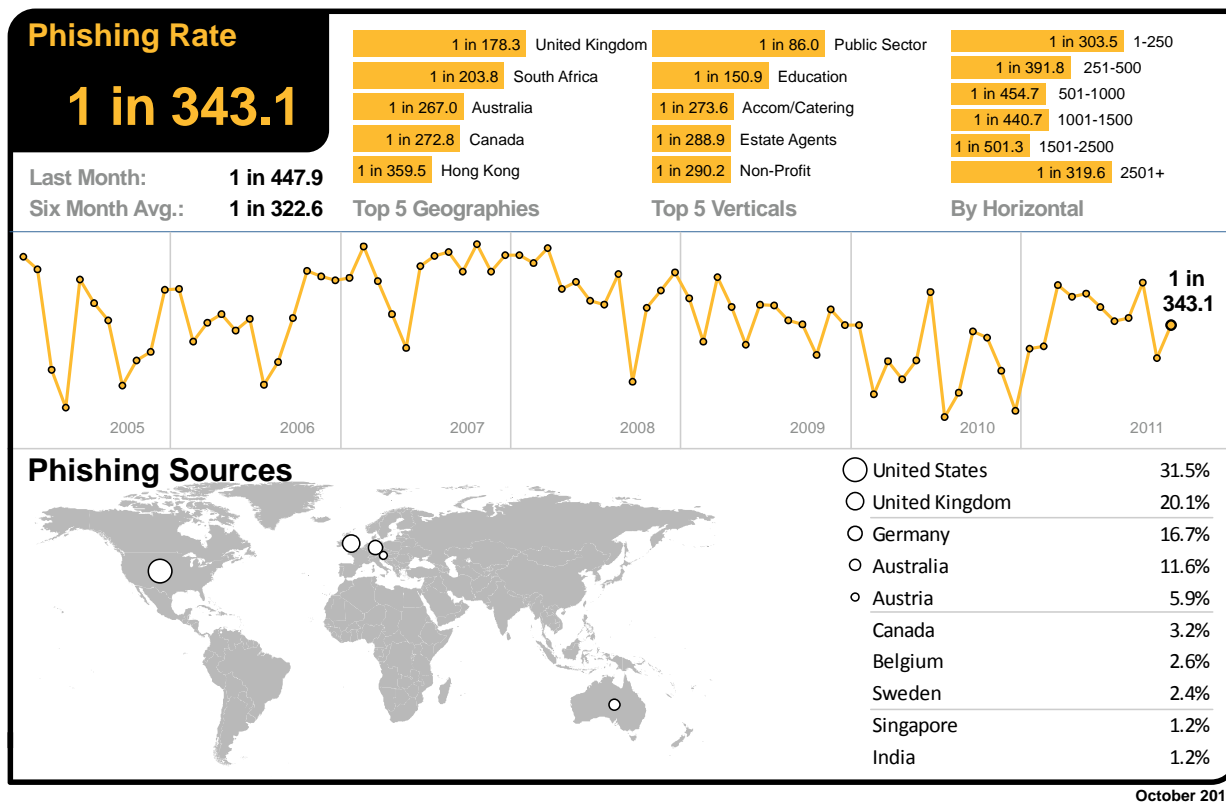
下のグラフで示されるように、悪質な添付ファイルを含んだ悪質な攻撃の件数は、9月末から減少し、10月は攻撃件数が大幅に減少した。これらの添付ファイルの多くは、9月のレポートで説明したように、ポリモーフィック型マルウェアの亜種が増加したことと関連付けられる。



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、10月も引き続き安定しており、攻撃者はこれらの攻撃を実行する際に有効なメール配信リストを使っていると考えられる。NDRは通常、姓名のデータベースを使用した大規模な辞書攻撃の後に発生する。これらの状況は、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。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からである。

フィッシング分析

10月のフィッシング活動は前月から0.07%増加し、メールの343.1通に1通(0.29%)にフィッシング攻撃が含まれていた。



10月にフィッシング攻撃で最も大きな割合を占めたのは英国で、メール178.3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。南アフリカが2位で、メール203.8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646.0通に1通、272.8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、897.4通に1通、デンマークは、631.8通に1通、オランダは、518.3通に1通となっている。オーストラリアでは、267.0通に1通、香港では359.5通に1通、日本では3385通に1通、シンガポールでは500.1通に1通となっている。ブラジルでは、547.3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、86.0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543.3通に1通、ITサービス業界は500.5通に1通、小売業界は562.7通に1通、教育業界は150.9通に1通、金融業界は304.4通に1通となっている。

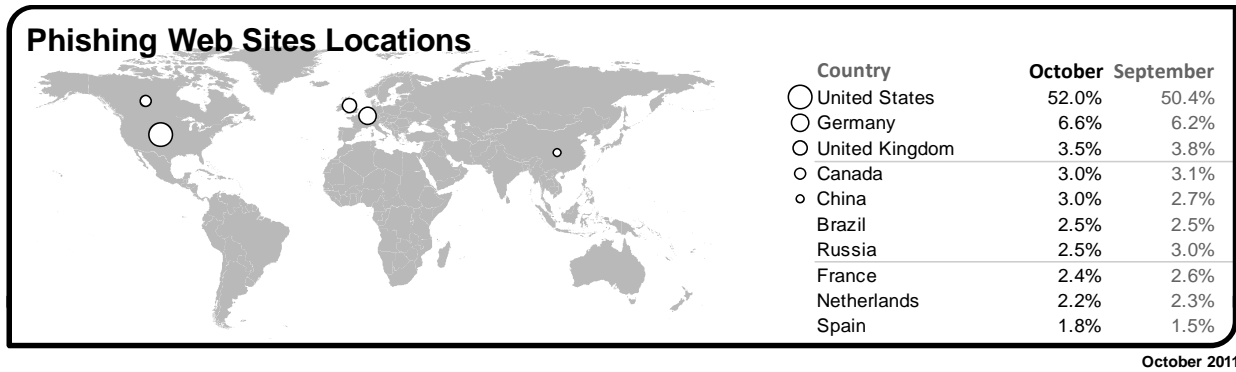
中小企業を標的にしたフィッシング攻撃は303.5通に1通、大企業では319.6通に1通であった。

フィッシングサイトの分析

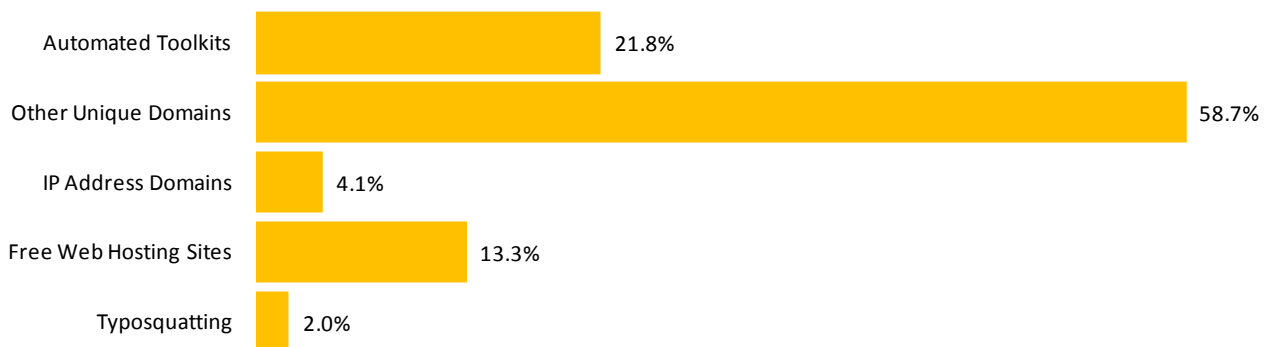
10月、フィッシングサイトの数は17.1%増加した。自動生成ツールによって作成されたフィッシングサイトの数は約36.1%増加している。一意のフィッシングURLの数も12.7%増加しており、ドメイン名でなくIPアドレスを使ったフィッシングサイト(例: http://255.255.255.255)は15.9%減少している。フィッシングサイト全体のうち、正規のWebホスティングサービスを悪用したものの割合は約13.3%で、前月から133.6%増加した。英語以外の言語によるフィッシングサイトは、7.4%増加した。

10月、英語以外のフィッシングサイトでは、ポルトガル語、フランス語、イタリア語、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)

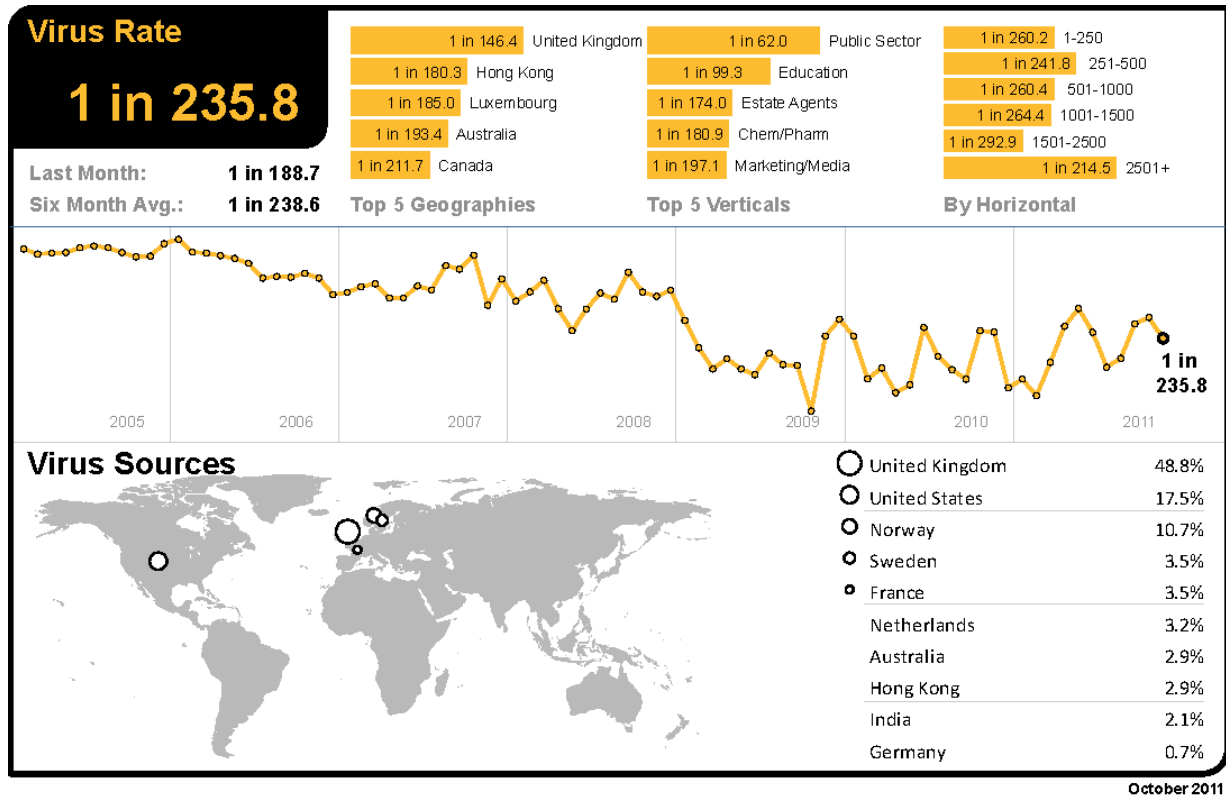


マルウェア分析

メールによる脅威

10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、235.8 通に 1 通(0.42%)で、前月比で 0.11% 減少した。

10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 20.1% を占め、前月比で 3.6% 増加している。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 10 月には 45.1% で、9 月の 72.0% と比べて減少している。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。



10月、悪質メールの割合が最も高い国となったのは英国で、メール 146.4 通に 1 通が悪質メールであった。2 番目が香港で、10月には 180.3 通に 1 通が悪質であるとしてブロックされた。

前月トップの座を占めた南アフリカは、10月には 326.0 通に 1 通が悪質であるとしてブロックされ、11 位に後退した。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 330.2 通に 1 通、211.7 通に 1 通であった。ドイツのウイルスレベルは、330.9 通に 1 通、デンマークは、457.1 通に 1 通、オランダは、319.4 通に 1 通となっている。オーストラリアでは、メール 193.4 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 1048 通に 1 通、272.4 通に 1 通となっている。ブラジルでは、421.7 通に 1 通に悪質なコンテンツが含まれていた。

また、10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 62.0 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 180.9 通に 1 通、IT サービス業界は 257.3 通に 1 通、小売業界は 355.4 通に 1 通、教育業界は 99.3 通に 1 通、金融業界は 332.9 通に 1 通となっている。

中小企業を標的にした悪質なメール感染型攻撃は 260.2 通に 1 通、大企業では 214.5 通に 1 通であった。

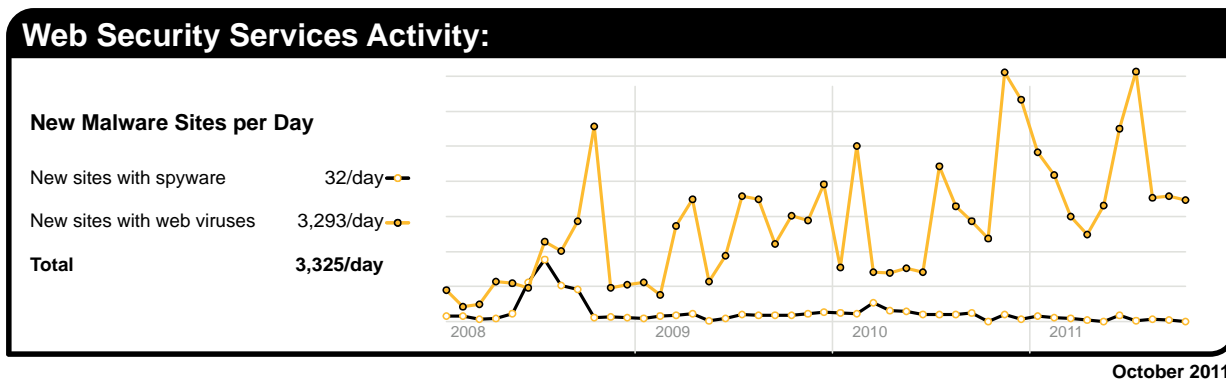
下記の表は、10月にブロックされたメール感染型マルウェアを表している。これらの多くが、メールで配布される悪質な添付ファイルの亜種と悪質なハイパーリンクを利用している。全体として、メール感染型マルウェアの45.1%に Bredolab、Sasfis、SpyEye、Zeus の亜種などのポリモーフィック型マルウェアの亜種が関与していた。

マルウェア名	マルウェアの割合
Gen:Trojan.Heur.FU.bqW@a8hiAJoi	6.51%
W32/Generic-0922-13ca-13ca	5.95%
Exploit/Link-generic-ee68	5.86%
Gen:Variant.Ursnif.16	3.91%
Trojan.Bredolab!eml-866c	3.28%
Gen:Trojan.Heur.FU.bqW@aS39a0fi	2.02%
Trojan.Bredolab!eml-4e1b	1.96%
Gen:Trojan.Heur.FU.bqW@a0CDPdfi	1.74%
W32/Generic-703e-4489	1.55%
Exploit/FakeAttach	1.43%

Web ベースのマルウェアの脅威

10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 日平均 3,325 件特定した。これは、前月比で 4.3% 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、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、10月に新たにブロックされた悪質ドメインは全体の 43.9% で、前月比で 0.7% の減少となっている。また、10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、10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、10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、37.5% 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 18.1% を占めていた。これは、ブロックされた Web サイト 5.5 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 日のうち一定回数のみアクセスを認め、それを超えるアクセスは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。

10 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 8.9% 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、ブロックされた Web サイト 11.2 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	37.5% VBS/Generic	45.3% PUP:Generic.188886	34.7%
Social Networking	18.1% Trojan.ADH.2	16.2% PUP:9231	20.4%
Streaming Media	8.9% Trojan:GIF/GIFrame.gen!A	7.2% PUP:W32/CnsMin.S	7.4%
Computing and Internet	4.1% Gen:Trojan.Heur.gq0@vj7DnZiix	6.2% PUP:Generic.192303	6.0%
Unclassified	3.8% W32.Downadup.B	1.8% PUP:Generic.62006	4.5%
Chat	3.4% Trojan.Gen	1.6% PUP:Generic.183433	3.4%
Search	3.0% Trojan.Gen.2	1.3% PUP:Generic.183172	3.0%
Peer-To-Peer	2.3% Infostealer.Gampass	1.2% PUP:Keylogger	2.9%
Hosting Sites	2.0% Gen:Variant.Kazy.32829	1.2% PUP:Agent.NGG	2.2%
Gambling	1.6% Trojan.Maljava	1.0% PUP:JS.Script.C	2.0%

October 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 ⁵	マルウェアの割合
W32.Sality.AE	7.19%
W32.Ramnit!html	7.18%
Trojan.Bamital	6.03%
W32.Ramnit.Blinf	5.72%
WS.Trojan.H	5.70%
W32.Downadup.B	3.19%
W32.SillyFDC.BDP!lnk	3.05%
W32.Virut.CF	2.74%
Trojan.ADH.2	2.58%
Trojan.ADH	2.55%

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)

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。

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13.1%をW32.Ramnitの亜種が占め、W32.Salityの亜種は8.1%であった。

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。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17.6%が、ジェネリックな検出を用いて識別、ブロックされた。

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

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、意図的である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、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。

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、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 © 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。