

シマンテックインテリジェンスレポート: 2011 年 11 月

11 月には、1 日あたりの標的型攻撃の数が 1 月と比べて 4 倍に増加した。全体的なスパムレートは 3 年間で最も低くなったが、ロシアのスパマーはメッセージの偽装を引き続き巧妙化させている。

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 11 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 10 月および 11 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 - 70.5% (前月比 3.7% 減): 13 ページ
- フィッシング - メール 302.0 通あたり 1 通でフィッシング攻撃 (前月比 0.04% 増): 16 ページ
- マルウェア - メール 255.8 通あたり 1 通がマルウェアを含む (前月比 0.03% 減): 18 ページ
- 悪質な Web サイト - 1 日あたり 4,915 件の Web サイトをブロック (前月比 47.8% 増): 19 ページ
- 2011 年の標的型攻撃のレビュー: 2 ページ
- 電話番号を使ったロシア発信のスパムの進化: 10 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: 22 ページ

はじめに

今年は標的型攻撃と APT (Advanced Persistent Threat) がマスコミを賑わせている。年末に近づくため、標的型攻撃を再度分析し直し、「Advanced Persistent Threat」、略して APT と呼ばれてきたものとの違いを調べてみた。APT などの用語は乱用されており、報道では間違っていて使用されていることもあるが、APT は一部の企業や業種にとっては現実の脅威となっている。

11 月において、255 通に 1 通の割合でメールは悪質なものであったが、高度な標的型を含むメールの割合は約 8,300 通に 1 通であった。つまり、高度な標的型攻撃は、APT の前兆である可能性があるものの、割合は約 200 万通に 1 通であり、レートはまだ非常に小さい。また、標的型マルウェアは近年、数が増え、複雑さも増しており、企業秘密を盗むように設計されているため、このレポートで特集するように、攻撃者が説得力のあるソーシャルエンジニアリング技法を用いる場合は特に、受信者が認識することが非常に困難になる。

企業のネットワーク内部に常駐する持続的な脅威は、成功した標的型攻撃の副産物の可能性がある。標的型メール自体に APT が含まれているというよりも、実際の APT のダウンローダコンポーネントが含まれていることが多い。したがって、適切な防御が実装されていないと、この手の標的型攻撃がネットワークへの APT の展開につながる可能性がある。

全体的なスパムは、悪質な ISP である McColo が廃業した 2008 年 11 月以後、最小となった。スパムの量に対する当時の影響は非常に劇的で、スパムが全体的なメールの 68.0% を占めていた。最近になって、減少のペースはずっとゆっくりになっているが、スパマーはより高度な標的型手法を使用し、ソーシャルメディアをメールの代替として悪用するようになっている。さらに、医薬品のスパムは、追跡を開始して以来、最小となっていて、スパムの 35.5% を占めている。2010 年末は 64.2% であった。

今回が 2011 年最後のシマンテックインテリジェンスレポートである。2011 年のセキュリティ動向の年次レビューはすでに進められている。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。

レポートの分析

2011 年の標的型攻撃のレビュー

標的型マルウェアと APT (Advanced Persistent Threat) は、特に 2010 年に起きた Stuxnet 攻撃、つい最近の Stuxnet と同じソースコードから作成された Duqu1 の検出を受けて、2011 年のニュースでひととき目立つ存在となっている。Stuxnet のソースコードはインターネットでは入手できないが、だからといって元の作成者が Duqu の作成者であるとも限らない。ソースコードは共有されたか、もしくは盗まれた可能性すらある。

この増加する脅威の性質を適切に理解し、組織にとって適切な種類の防御に投資したことを確認するには、標的型攻撃と APT の意味を定義することが重要である。

標的型攻撃が登場してから長年経つが、最初に表面化した 2005 年に遡るなら、シマンテックドットクラウドはこのような攻撃を週におよそ 1 件検出しブロックするだろう。その翌年以降、この数は 1 日に 1 ~ 2 件に増え、その後、2010 年には 1 日に約 60 件に、2011 年の第 1 四半期末までに 1 日 80 件に増加した。大規模で有名な多国籍企業が標的になる傾向があり、多くの場合、公共機関、防衛、エネルギー、医薬品などの特定の業界であった。さらに近年では、標的の範囲が広がり、中小規模の企業を含め、ほぼすべての組織が対象となっている。しかし、標的型攻撃と APT (Advanced Persistent Threat) とは実際には何を意味するのだろうか。

標的型攻撃の定義

特定の人物または組織を標的としている場合、攻撃は標的型と見なされる。通常、従来型のセキュリティ防御を回避するために作成され、高度なソーシャルエンジニアリング技法を利用していることが多い。ただし、すべての標的型攻撃が APT につながるわけではない。たとえば、Zeus Banking Trojan は標的型の可能性があり、受信者にマルウェアを有効化させるためにソーシャルエンジニアリングを利用するが、Zeus は APT ではない。攻撃者は個々の受信者が誰であるかを必ずしも気にしない。攻撃者がその個人に関して収集した情報(通常は、ソーシャルネットワーク Web サイトを通じて入手)を不正利用できるからという理由だけで選ばれた可能性がある。

ソーシャルエンジニアリングは、このような高度な種類の攻撃の多くで常に最先端にあった。これらの攻撃は、企業の防御を突き破って知的財産にアクセスすることを目的に、または Stuxnet の場合は、物理的な運転制御システムを妨害することを目的に設計されている。強力なソーシャルエンジニアリングつまり「ヘッドハッキング」がなければ、最も技術的に高度な攻撃であっても成功する可能性は低くなる。ソーシャルエンジニアリングを利用した多くの攻撃は、ソーシャルネットワークやソーシャルメディアサイトに公開されている情報を基にしている。攻撃者が受信者の興味、趣味、交流相手、他の誰がネットワークに参加する可能性があるかを知ることができれば、多くの場合、もっともらしい説得力のある攻撃を作成することができる。

高度な標的型攻撃のプロファイル

高度な標的型攻撃は通常は APT の前兆である。高度な標的型攻撃の標準的な特徴として一般に、悪意を持って作成されたドキュメントまたは実行可能ファイルを悪用する。これらが特定の個人または少人数のグループ宛てにメール送信される。これらのメールは、次の図 1 に示されているように、より興味深く、関連性の高いものにするためにソーシャルエンジニアリング要素をまとめている。

たとえば、「プレー料金」が半額と宣伝するメールに添付されている PDF は、受信者がゴルフファンであれば、より魅力的に映る可能性がある。ゴルフファンはこのような掘り出し物を受け入れる可能性がある。理想としては、攻撃者は受信者が開かずにいられないようなドキュメントを作成したいと考えている。攻撃は危殆化した Web サイトを介して行われる場合がある。この場合、受信者はメールに含まれているリンクをクリックするよう要求され、クリックするとドライブバイ攻撃が行われる可能性がある。または、受信者は危殆化した Web サイトから感染したドキュメントをダウンロードする。

¹ <http://www.symantec.com/connect/blogs/duqu-0>

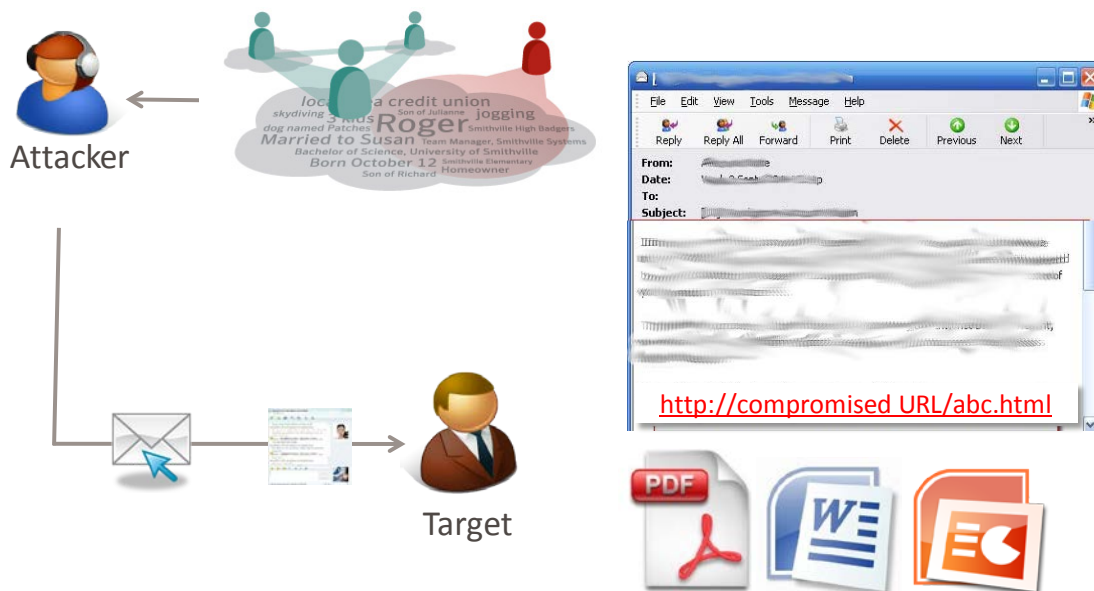


図 1: 標的型攻撃の標準的なライフサイクル

2011年4月、メッセージラポインテリジェンス(現在はシマンテックインテリジェンス)は、CVE-2011-0609の悪用を利用した攻撃について報告した²。これらの攻撃はシマンテックドットクラウドによってブロックされ、同じ悪用を利用した同様の攻撃がRSAの個人にも送信された時点で幅広く報告された。そのケースでは、攻撃は、次の会計年度の採用計画について詳述しているように見えるスプレッドシートドキュメントで構成されていた。また、HRチームと連携した採用エージェントから送信されたように装っていた。これは「スピアフィッシング」と呼ばれる技法である。ゴシップに興味を持つのは人間の性であるため、攻撃者が「staff_salaries.doc」という名前のドキュメントを送信すれば、開かれる確率は高まる可能性がある。

このような悪質なドキュメントがいったん開かれると、被害者のコンピュータは危殆化し、追加の悪質なコード(「セカンドステージ」と呼ばれることが多い)が続いてダウンロードされ、インストールされる。危殆化したコンピュータへのリモートアクセスを可能にし、データの流出を促進するのは、このセカンドステージである。これが企業ネットワークのその他の部分への足掛かりとなり、一種の拠点形成する。さらに、実際にはこのステージになってようやく攻撃はAPTと見なされる可能性がある。企業のセキュリティ防御によってブロックされておらず、コンピュータは攻撃者の管理下に置かれている。

APTの進化

このように、「APT」という用語は進化するうちに、標的型攻撃の中で、特定の個人または組織を標的とするように設計されている独特のカテゴリを表すようになった。APTは、レーダーをかいくぐり、できる限り長い間、検出を逃れるように設計されている。この特性によりAPTは特に効果的になり、検出を回避するために静かにゆっくりと動く。より一般的な標的型攻撃に特有の手取り早く金を稼ごうとする悪巧みとは異なり、APTは国際的なスパイ目的や妨害工作目的を持つ場合がある。APTの目的には、軍事的、政治的、または経済的な情報収集、機密または企業秘密に対する脅威、業務の中断、または機器の破壊などが含まれる場合がある。Stuxnetは、後者についての極端ではあるものの典型的な例である。このマルウェアは攻撃者が特定の標的のウラン濃縮プロセス内の工業用制御システムを中断できるようにした。

APTのもう1つの特性は、長期的な活動の一部でもあるが、現在流通しているほとんどのマルウェアに特有の日和見的な「スマッシュアンドグラブ」の手法に従っていない点である。その目的は、できる限り長い間、検出を逃れることであり、その期間にさまざまな攻撃を使用すると思われる。1つの攻撃が失敗した場合、継続的な監視プロセスは別の手法を用いたフォローアップ攻撃が数週間後に成功する可能性が高くなるようにする。成功した場合、攻撃者は危殆化したシステムをその後の攻撃の拠点として使用できる。

² http://www.symanteccloud.com/ja/jp/mlireport/MLI_2011_April-%20JPN_Final.pdf

いずれもこれらの攻撃がどのようにして高度かつ持続的な脅威となり得るかを示している。脅威となるのは、その目的がデータを盗んだり標的となる企業の業務を妨害したりすること、および攻撃者の管理下に置かれた危殆化したネットワークを悪用して他の組織のユーザーを標的にすることであるためである。ゼロデイの悪用といった検出を回避するために使われる方法や、コマンドおよび制御ネットワークと通信するために使われる手段から考えて、これらの攻撃は高度である。コマンドおよび制御命令は暗号化されたトラフィックを伴うことが多く、一般に小さなバーストで送信され、通常のネットワークトラフィックとして偽装される。情報を検出されずに盗み出すことができるようにするには、攻撃者は検出されやすい暗号化の使用を避け、不自然に見えない一般的なプロトコルチャネルを使用する必要があるが、その間ずっとデータを隠れた状態にしておく必要がある。

さらに、これらの攻撃は、その目的が危殆化した企業のインフラ内に拠点を維持することであるため、持続的と表すことができる。これを実現するために攻撃者は多数の手段を使用する。攻撃者は非常に明確かつ具体的な目標を持っていて、資金も豊富でうまく組織化されている。適切な保護が実装されていない場合、これらの脅威は望む目標を達成するための能力と意思を兼ね備えている。

標的型攻撃の増加

次の図 2 は、APT につながる可能性がある高度な標的型攻撃の数の増加を示したものである。これらの攻撃は、攻撃の標的になっている各組織内の特定の個人に送信され、年間を通じて拡散する。攻撃では、複数の「キルチェーン」(長期間にわたって複数の悪用を利用するさまざまな種類のマルウェアなど、多様な攻撃ベクトル)が使われる。これらの攻撃ではゼロデイが悪用されることもある。攻撃者がアプリケーションのパッチ未適用の脆弱性を利用する手段を特定し、その悪用を軽減するためのパッチがリリースされていない場合である。ゼロデイ脆弱性は全体的には少数で、2010 年はシマンテックで記録されたのはたった 14 件³、2011 年は現在までで 11 件である。Stuxnet は、4 つのゼロデイ脆弱性を利用した。

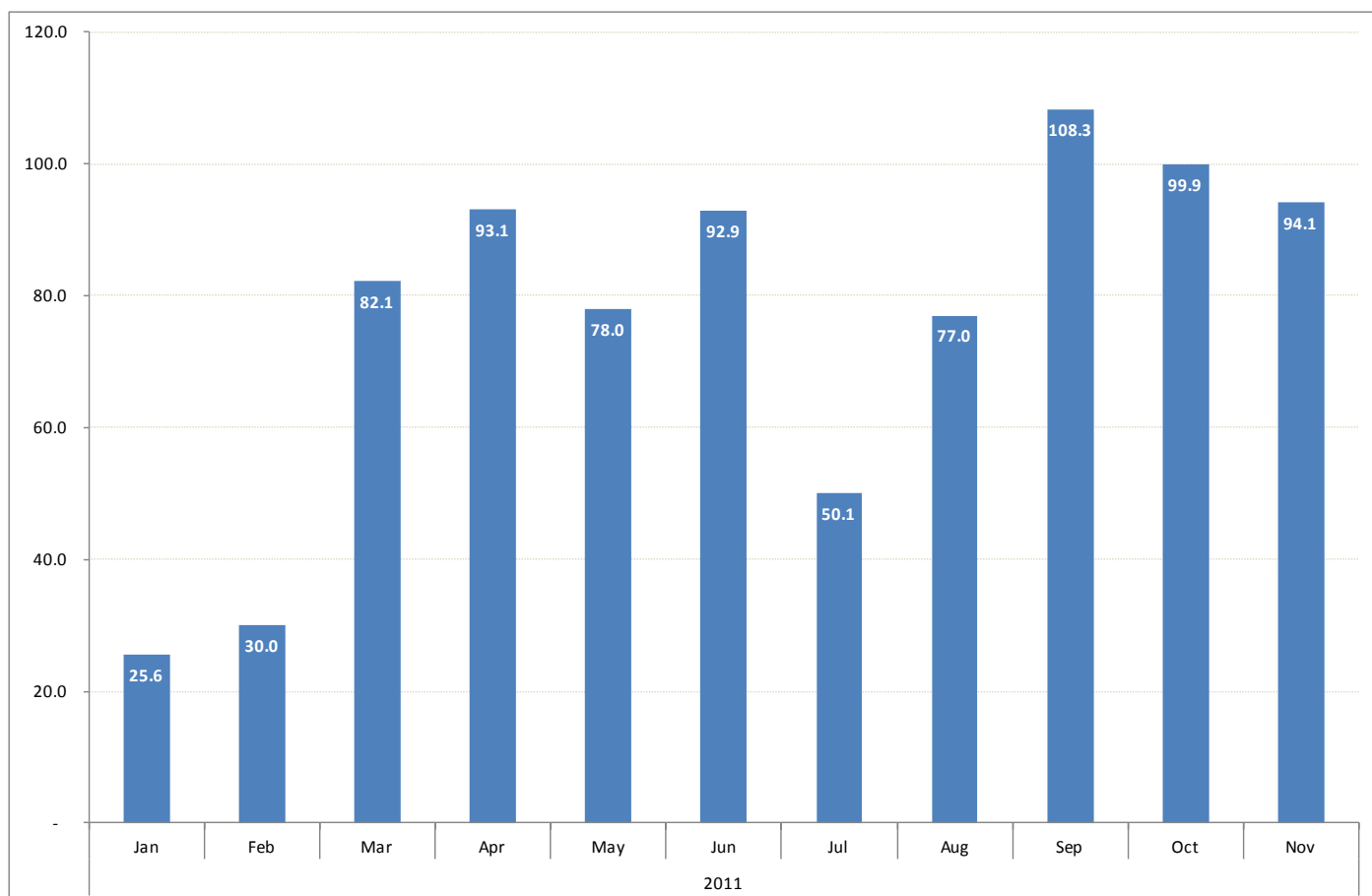


図 2 – 2011 年に世界中でシマンテック ドット クラウドが全面的にブロックした 1 日あたりの標的型攻撃の平均数

³ http://www.symantec.com/ja/jp/business/threatreport/topic.jsp?id=vulnerability_trends&aid=zero_day_vulnerabilities

11 月には、シマンテックドット クラウドはこのような攻撃を毎日約 94 件ブロックした。これは同じ年の 1 月にブロックされた数の 4 倍である。これを視野に入れると、11 月には 255 通に 1 通になんらかのマルウェアが含まれていた。ただし、これらのうち APT につながる可能性がある高度な標的型攻撃は 8,300 通に 1 通のみであった。全体的に見ると、メール 200 万通に 1 通に APT につながる可能性がある標的型攻撃が含まれていることになる。

推定で毎日 480 億通のメールが流通しており、このような性質の高度な標的型攻撃がメールトラフィックに占める割合は非常にわずかであるが、2010 年末ほどまれではないことも確かである。これらの攻撃はいずれも組織に深刻な影響を及ぼす可能性があり、長期的には多くの企業の経済的繁栄にとって大きな脅威となる。

最も多く標的となった業界

図 3 のグラフは、2011 年に最も多く標的となった業界が公的機関であることを示している。1 日に約 20.5 件の標的型攻撃がブロックされた。2 番目に多いのが化学/製薬業界で、1 日に 18.6 件ブロックされた。後者のケースでは、これらの攻撃の多くは年の後半になって表面化し、Nitro4 攻撃のプロファイルに適合した。これは製造業界も同様で、1 日に約 13.6 件の攻撃がブロックされ、3 番目に多い業界となっている。

毎日のこれらの標的型攻撃の目的は、標的となる組織のネットワークへの永続的なアクセスを確立することである。多くの場合、機密データへのリモートアクセスを行うことを目的としている。

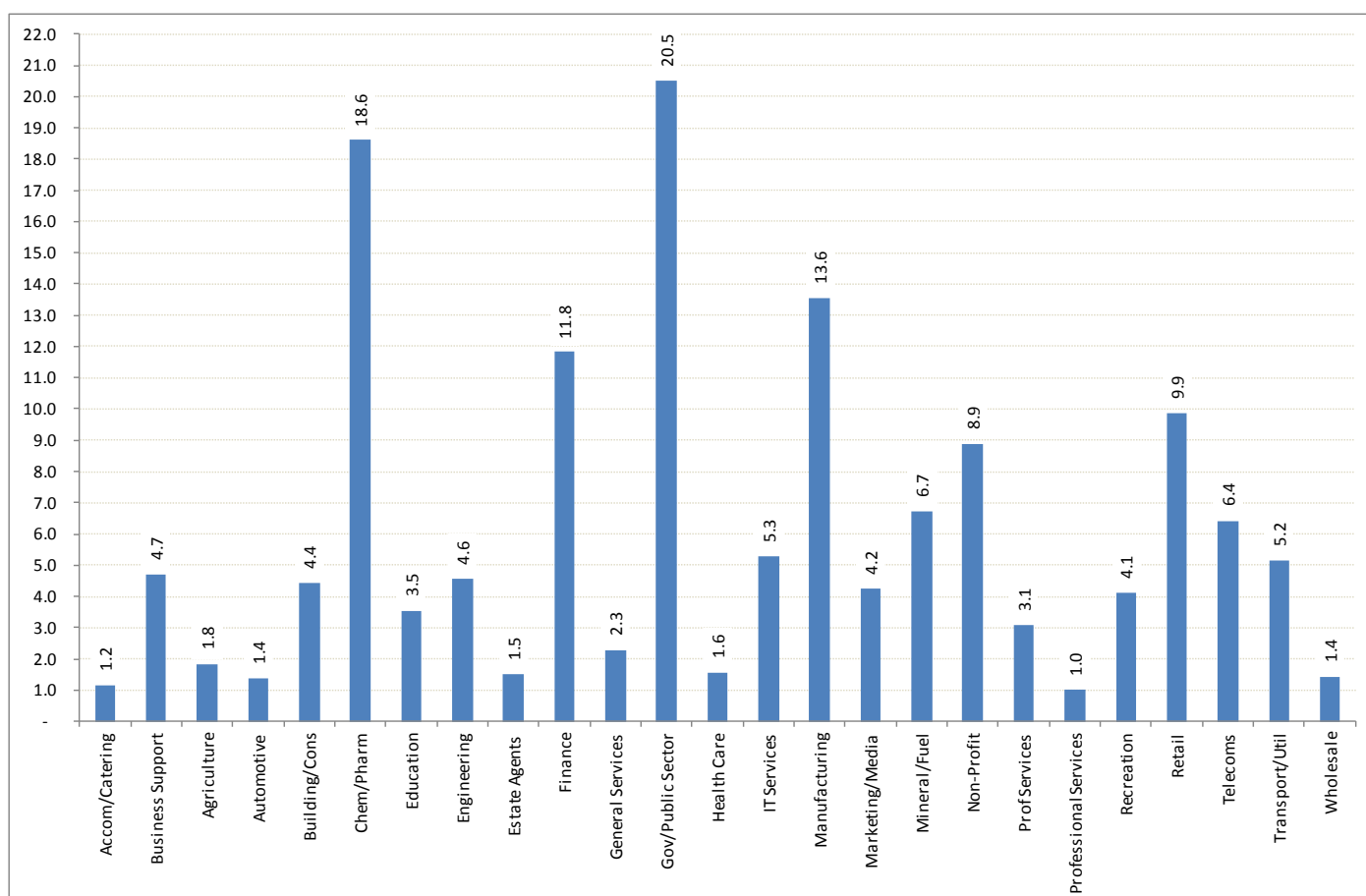


図 3 – 2011 年にシマンテックドット クラウドがブロックした 1 日あたりの標的型攻撃の平均数(業種別内訳)

上記のとおり、APT の目的は業務の中断または場合によっては機器の破壊だと考えられる。マルウェアが物理的な機械を中断させることはまれで、実現は非常に困難だが、Stuxnet 以降に初めて報告された同様の事件の事例が 11 月 8 日に明らか

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

になった。米国の水道施設が危殆化し、ポンプの電源を入れたり切ったりするために SCADA (Supervisory Control and Data Acquisition) システムへの無断アクセスが行われたことから最終的にポンプが故障し、イリノイ州の施設が一部運転停止した。産業用デバイス向けのコントローラソフトウェアの開発元で最初の侵害が発生したのではないかと疑われた。その攻撃で収集された情報とクレデンシャルが水力発電所に対するその後の攻撃に使われたと思われる。ただし、FBI と国土安全保障省は、ネット侵入の証拠は見つかっていないと主張している。

標的型攻撃(組織規模別内訳)

次の図 4 に示すグラフは、標的となる組織を規模別に示したものである。従業員が 2,500 人を超える大企業が最も多く攻撃を受けていて、1 日に 36.7 件がブロックされた。

一方、従業員が 250 人未満の小規模から中規模の企業では 1 日に 11.6 件の攻撃がブロックされた。

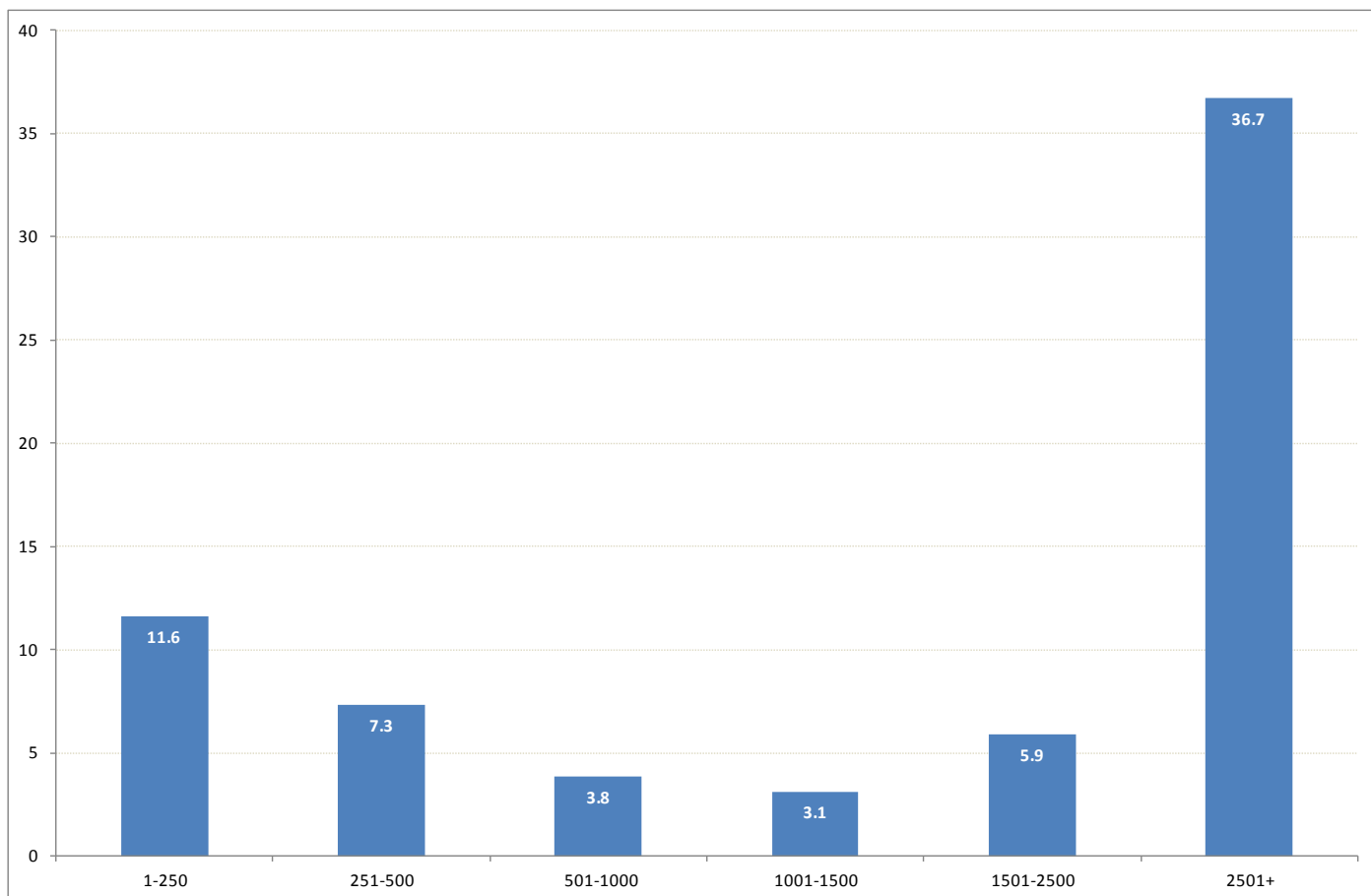


図 4 – 2011 年にシマンテック ドット クラウドがブロックした 1 日あたりの標的型攻撃の平均数(会社規模別内訳)

標的型攻撃(地理的分布別内訳)

最後の分析では、対象となった受信者の場所を基に、標的型攻撃を地理的分布別に分類して調べた。これを次の図 5 に示しており、米国では毎日少なくとも 1 件の攻撃がブロックされている。389 人に 1 人のユーザーがこのような攻撃の受信者となっている。これとは対照的に、日本では、約 9 日おきに少なくとも 1 件の攻撃がブロックされており、520 人に 1 人に送信されているだけである。

国/地域	N 日に 1 件の攻撃	N 人のユーザーに 1 件の攻撃
米国	1.0	389
英国	1.2	407
香港	2.9	127
オーストラリア	3.1	1,139
フランス	3.2	396
シンガポール	3.3	114
スイス	3.4	455
中東	4.0	539
インド	4.4	82
ベルギー	4.5	176
デンマーク	5.1	666
オランダ	7.0	3,307
カナダ	8.8	513
日本	8.8	520
ドイツ	9.4	2,790
フィリピン	14.0	99
ノルウェー	14.7	2,591
中国	16.3	4
マレーシア	17.2	7,433
ハンガリー	18.2	196
イタリア	28.1	1,310
スペイン	28.1	6,522
スウェーデン	30.9	24,134
台湾	44.1	68
イスラエル	44.1	880
フィンランド	44.1	3,686
ニュージーランド	61.8	3,479
アイルランド	61.8	5,104
スリランカ	77.3	2,241
ルクセンブルグ	154.5	665
ベトナム	154.5	843
南アフリカ	154.5	4,878

図 5 – 最も多く標的となった地域での攻撃の頻度とユーザーあたりの比率を示す表

標的となる組織のケーススタディ

ケーススタディとして使用する最近の例を図 6 に示している。テレビゲームを製造する会社のケースで、少なくとも 2 年間にわたって一連の攻撃が実行された。これらの攻撃は、製品内で使われる知的財産へのアクセスが目的であると思われる。

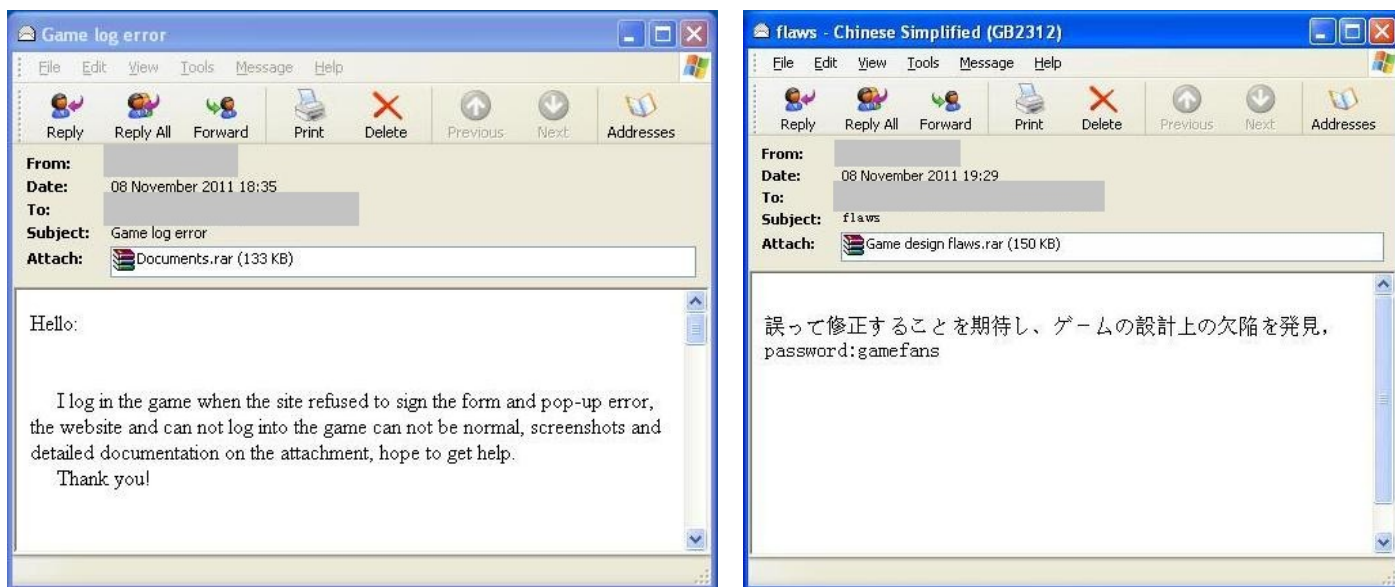


図 6 – ビデオゲーム会社宛ての標的型攻撃メールの例

これらの攻撃の大半は米国から発信されたが、多くのメールがさまざまな無料のオンライン Web サービスから送信されていることを考えると、意外なことではない。同様のメールは、やはり発信元として無料の Web メールプロバイダを使用して日本、韓国、台湾からも送信されている。

次の図 7 は、これらの攻撃が 2、3 カ月の間隔で行われる傾向があること、また、多くの場合、小さな波のような形で発生していることを示している。最新の攻撃は 2011 年 11 月に発生している。

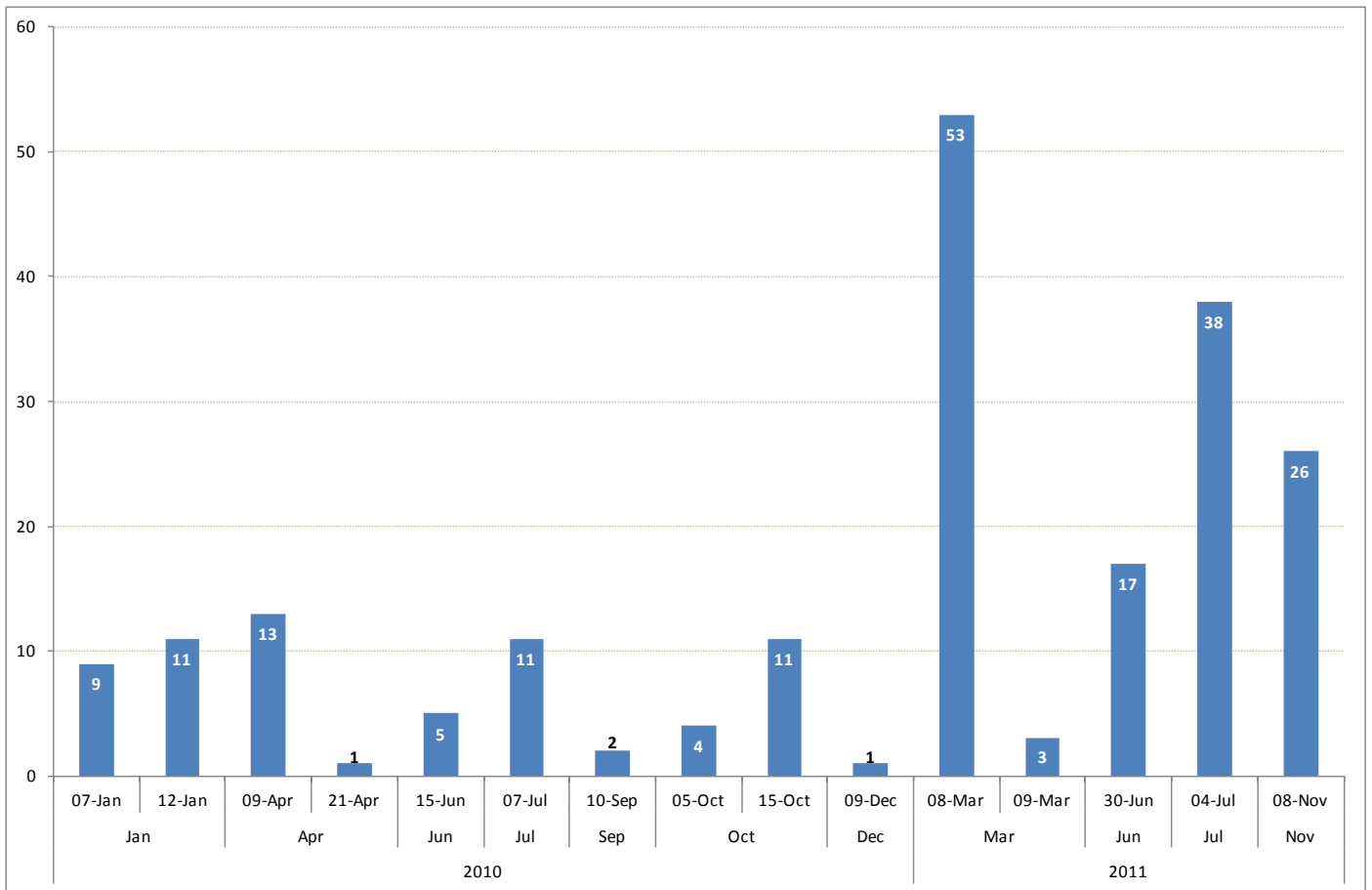


図 7 – 長期にわたって 1 つの企業に対してシマンテックドット クラウドがブロックした標的型攻撃のパターン

各攻撃で使われるファイルの種類は、さまざまな一般的なオフィスアプリケーションの脆弱性を悪用しようとして、徐々に変化している。以前の試みが阻止されたため、攻撃者は他の侵入方法を見つけることを余儀なくされた。

標的型攻撃の影響の可能性

この問題の正確な規模を数量化することは困難だが、このレポートでのシマンテックドット クラウドからのデータがこの問題の重大性を示すのに役立てば幸いである。現在の課題は、組織がこのような方法で標的となる可能性があるかどうかを把握することにあるが、それは非常に困難な場合がある。自分の会社が第一の標的ではないものの、攻撃者が組織を他の企業を攻撃するための足掛かりとして使用する可能性がある。自社をサプライチェーンで最も弱いリンクにしたいわけではないであろう。情報はパワーであり、攻撃者はこれを知っていて、攻撃の成功はその背後にいるネット犯罪者にとって大きな金銭的利益をもたらす可能性がある。知的財産や戦略情報へのアクセスは、ネット犯罪者に競争市場における大きな強みを与える可能性がある。これらの攻撃の手段がますます高度になり、時間とともに大きく進化している状況をご理解いただければ幸いである。

シマンテックは、APT の被害に遭った企業と協力し、サポートしてきた。少なくとも、これらの新しい技法について理解し、自身や企業を保護するために何ができるかを学ぼうとするべきである。今すぐ防御を強化することから始めよう。

標的型攻撃と APT の詳細については、このトピックに関する最新のホワイトペーパー⁵ をダウンロード

⁵ <http://go.symantec.com/apt>

電話番号を使ったロシア発信のスパムの進化

ロシアから発信されるスパムメールの大半は、オンライン広告、商品のプロモーション、トレーニングワークショップに関するものである。このようなスパムメールは通常、フリーメールアカウントや個人になりすましたメールアカウントからユーザーの許可なく一方的に送り付けられ、スパムフィルタに掛からないように件名がランダムに付けられている。シマンテックでは、ランダムな件名が使われているメールについても、唯一の連絡手段として直接 URL リンクではなく電話番号をメール内に記載するスパマーを監視し続けている。

一例として、ロシアから最近発信されたイベントプロモーションスパムを次の図 8 に示す。

Детский день рождения в [redacted]

**Лазерные бои на арене 460м2,
стилизованной под трансформеров!**

Холл для проведения
праздничного фуршета/можно с собой.

Шоссе Энтузиастов [redacted]

(4~9~5)1~2~3~40~0~0

この英語訳は次のとおりである。

Children's Birthday at [redacted]

Laser ball
Super cool Transformers
buffet table

Highway Street [redacted]

(4~9~5)1~2~3~40~0~0

図 8: ロシア語のプロモーションスパム

このメッセージのおかしな点にお気づきだろうか。電話番号をよく見て欲しい。一部の桁が、数字ではなくアルファベットで書かれている。スパマーが電話番号の数字を、それに似たロシア語や英語の文字に置き換えたのである。これは、下記のようなスパム検出を避けるためのテクニックである。

まず、ここ数年間スパマーがこの手法をどのように使ってきたかを、いくつかの例で説明する。最初に、次のようなシンプルな連絡先電話番号のセットがあるとする。

```
(495)1234000
(495) 4321000
7(495)1234000
7-495-4321000
```

次に、スパマーはこれらの数字の間にランダムな記号をいくつか挿入して、電話番号に手を加える。

```
(4~9~5)1~2~3~40~0~0
(4^95)1^2^3^40^00
495 43:21;000
(4_9_5) 4_3_21000
```

スパマーの手法は次第に精巧になり、数字をそれに似たロシア語または英語のアルファベットに置き換えるようになる。数字に似たロシア語と英語の文字のリストを次に示す。

	英語	ロシア語
1	l i l	N/A
2	Zz	N/A
3	N/A	ЗзЭэ
4	N/A	Чч
6	N/A	ЬьБб
0	Oo	Оо

図 9 – 数字に似たロシア語と英語のアルファベット

図 9 の表を使い、多少の創造力を働かせると、普通の電話番号だった元のリストを次のように変えることができる。

```
(4^95)1^2^3^40^Oo
(495) l 2 3 – 4O – 0 0
/495/ Ч 3=21;0 00
(4~9~5) 43~2~1~0~0~0
```

スパム対策テクノロジーは、しばらくするとこれらのスパムパターンを識別し、フィルタで除外し始めるため、スパマーはさらに創造力を駆使し、さらに巧妙な新しいトリックを考案しなければならない。たとえば、シマンテックでは 2010 年に、スパマーが電話番号を次のような実際のロシア語の単語でスペルアウトし始めたことを確認した。

	ロシア語	英語
1	один	one
2	два	two
3	три	three
4	четыре	four
5	пять	five
6	шесть	six
7	семь	seven
8	восемь	eight
9	девять	nine
0	ноль	ten

図 10 – 数字を表すロシア語と英語の単語

この手法と、最初に示した元の電話番号リストを使うと、連絡先電話番号は次のようにさらに複雑になる。

(4^95)1 ^2^ три ^40^ 00 } (495)123400
(495) один 2 3 - 4 0 - 00

/495/ 4;3 =2 | 00 0 } (495)432100
(4~9~5) 43~2~ один~0~0~0

しかしながら、スパマーの創造力はこれで終わりではない。彼らは、市外局番をそれに対応する実際の都市名に置き換えるというアイデアも生み出した。たとえば、モスクワという都市で考えてみよう。モスクワの市外局番は 495 である。したがって、市外局番 495 はモスクワのロシア語表記「Москва」、英語表記「Moscow」、または単に略記の都市名コード (MOW/Moc) に置き換えられる。

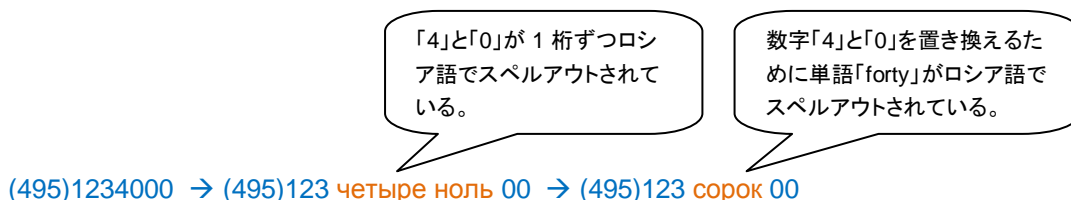
(Москва) 1 ^2^ три ^40^ 00 } (495)123400
(Moscow) один 2 3 - 4 0 - 00

(MOW) 4~3~2~1~0~ 00 } (495)432100
(Moc) четыре 3 2;|=00 ноль

もっと最近では、数字をもじる別の手法も確認された。これまでの例では、一部の数字がロシア語でスペルアウトされていたが、一度に 1 桁のみだった。それが今度は、図 11 の例のようにスペルアウトが 2 桁 (1 桁だけでなく 2 桁分の数字) に進歩しているのである。

英語のスペル	ロシア語のスペル
10 ten	десять
40 forty	сорок

図 11 – スпамで使われている 2 桁のスペルアウトの例



スパマーがスパムフィルタによる検出を逃れようとするトリックを見破るのは面白いものである。幸い、前述したトリックはすべて最新のテクノロジーで検出することができる。スパマーにしてみれば、さらに知恵を絞って新しいトリックを生み出さなければならない。シマンテックインテリジェンスでは、スパムの最新傾向を常に注意深く監視しているため、ここで取り上げたロシアの電話番号パズルのようなトリックに対処する最善策を開発できる。

寄稿: シマンテック セキュリティレスポンス技術者 Emily Liu

世界的傾向とコンテンツ分析

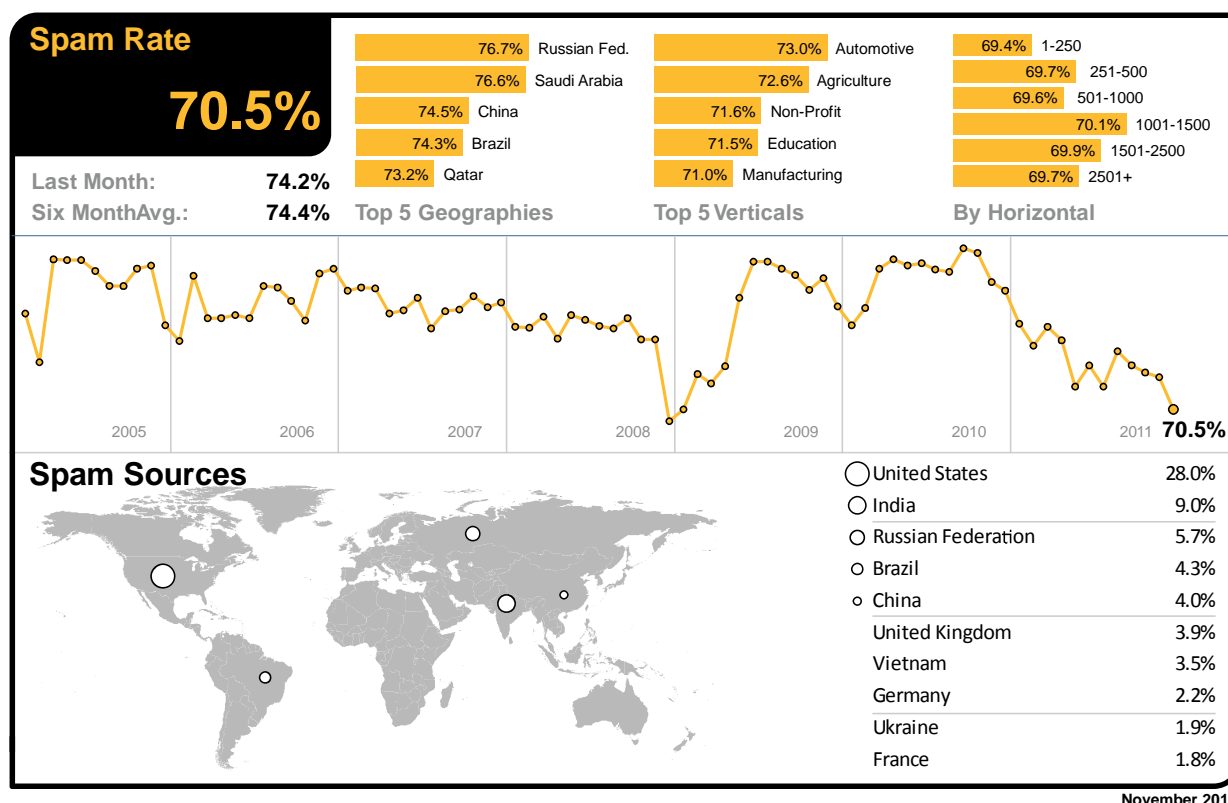
スパム、フィッシング、マルウェアに関するデータは、シマンテックグローバルインテリジェンスネットワーク、シマンテックプロブネットワーク(500 万件を超えるダミーアカウントによるシステム)、シマンテックドットクラウドに加えて、シマンテックの数多くのセキュリティ技術を駆使した多彩なソースを通じて収集されている。また、シマンテックドットクラウド独自のヒューリスティック技術である Skeptic™ では、高度なテクニックが用いられた新種の標的型攻撃も検知している。

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

2011 年 11 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 3.7% 減少し、70.5% であった(メール 1.42 通に 1 通)。



全体的なスパムレートが低下する中、11 月にはスパムレート 76.7% であったロシアが最もスパムの標的とされている。サウジアラビアはスパムが 2 番目に多く増えており、ブロックされたメールトラフィック中の 76.6% 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 69.9%、69.5% となっている。英国のスパムレベルは 69.5% 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 70.5%、70.1%、70.4%、68.6% であった。香港ではメールの 69.2% 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 68.0%、66.6% 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 70.1%、74.3% であった。

今月スパムが減少したものの、自動車業界は 11 月に最もスパムの被害を受けた業種となり、スパムレートは 73.0% であった。教育業界のスパムレートは 71.5%、化学/製薬業界は 69.1%、IT サービス業界は 69.3%、小売業界は 69.0%、公共機関は 68.8%、金融業界は 69.2% 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 69.4%、大企業(従業員数 2500 人超)は 69.7% であった。

グローバルでのスパム分類

11 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。

カテゴリ名	2011 年 11 月	2011 年 10 月
Pharmaceutical	32.5%	37.5%
Watches/Jewelry	19.5%	15.0%
Unsolicited Newsletters	17.5%	6.5%
Adult/Sex/Dating	12.5%	2.5%
Weight Loss	8.0%	4.5%
Unknown/Other	4.0%	1.5%
Casino/Gambling	2.0%	23.5%
Software	2.0%	1.5%
Scams/Fraud/419	1.5%	6.0%
Degrees/Diplomas	<0.5%	0.5%
Jobs/Recruitments	<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、11 月には、スパム件名がソフトウェアの値引きを宣伝するスパムや時計/宝飾品に関連する電子メールの割合が多くなっている。スパマーの一部が休暇シーズンや 12 月のクリスマスの時期に先駆けてシフトしていると考えられる。医薬品に関連したメッセージのスパム件名の割合も引き続き多くなっている。

順位	2011 年 11 月		2011 年 10 月	
	スパムで利用された件名	日数	スパムで利用された件名	日数
1	Re: Windows 7, Office 2010, Adobe CS5 ...	9	NACHA security nitification	2
2	New notification from Facebook	9	ACH Payroll Cancelled	2
3	Re: Re: Re: Re: Re: Windows 7, Office 2010, Adobe CS5 ...	9	ACH Transfer Review	6
4	Penis Enlargement Pills - Enlarge you Penis Naturally Gain Up To 4 Inches In Length	9	Re: Back to School Software Sale	6
5	Enlarge you Penis Naturally Gain Up To 4 Inches In Length And Up To 25% Girth Increase.	9	0	6
6	Re: software outlet online purchase	9	Facebook Administration has sent you a notification	9
7	(blank subject)	9	Fw: Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 ...	18
8	High quality Replica Watches at Watch Replica World at \$145	9	Re: Windows 7, Office 2010, Adobe CS5 ...	18
9	Replica watches - THE MOST POPULAR MODELS All our replica watches have the same look and feel of the original product	9	Fw: Fw: Fw: Windows 7, Office 2010, Adobe CS5 ...	18
10	Save-80%-Off-Viagra©-Cia1is©-Levitra©	9	Re: Re: Re: Re: Re: Windows 7, Office 2010, Adobe CS5 ...	18

トップレベルドメイン名に基づくスパム URL 分布

トップレベルドメイン(TLD)が「.com」または「.net」の URL を利用したスパムの割合は、それぞれ 2.2%、0.5% 低下し、1% 増加したのは TLD が「.ru」のスパムのみであった。

TLD	11 月	10 月	変化 (%)
.com	55.1%	57.3%	-2.2
.ru	9.4%	8.4%	+1.0
.net	6.0%	5.3%	-0.5
.org	7.4%	N/A	N/A

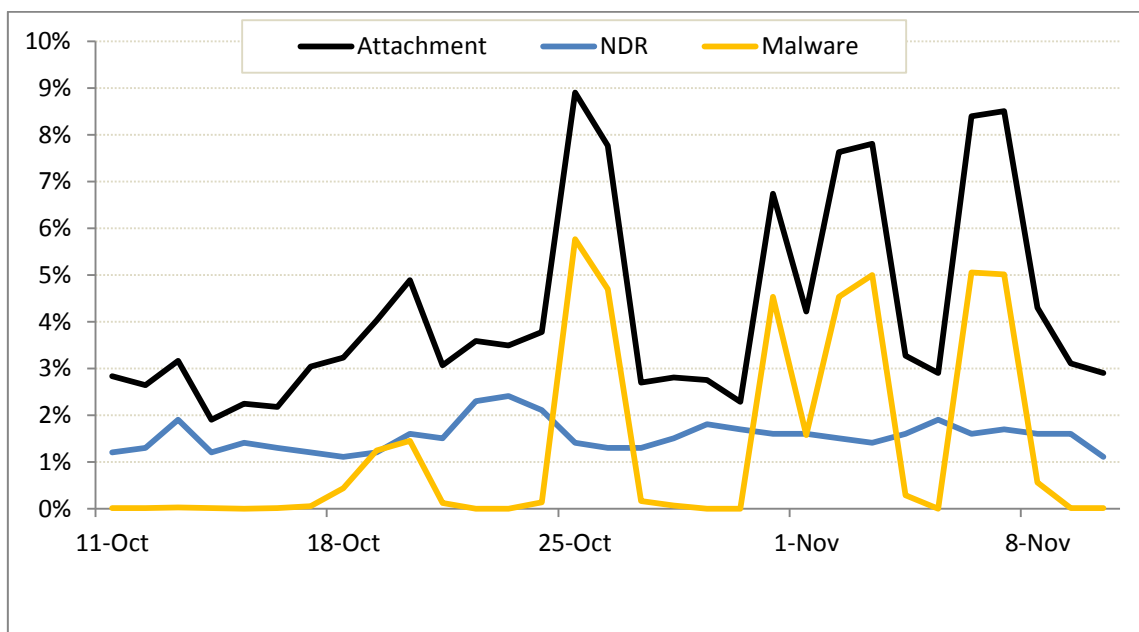
スパムメッセージの平均サイズ

11 月には、わずかに減少し、5 通のうち約 3 通が 5KB 以下であった。また、サイズが 5KB ~ 10KB のスパムは 4.9% 増加した。

メッセージサイズ	11 月	10 月	変化 (%)
0Kb - 5Kb	57.8%	59.0%	-1.2
5Kb - 10Kb	31.2%	26.3%	+4.9
>10Kb	11.0%	14.7%	-3.7

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、10 月前半よりもはるかに減少した。ただし、攻撃の頻度は 10 月末と比べて増加した。これらの添付ファイルの多くは、これまでの⁶シマンテックインテリジェンスレポートで説明したように、引き続きポリモーフィック型マルウェアの亜種と関連付けられている。



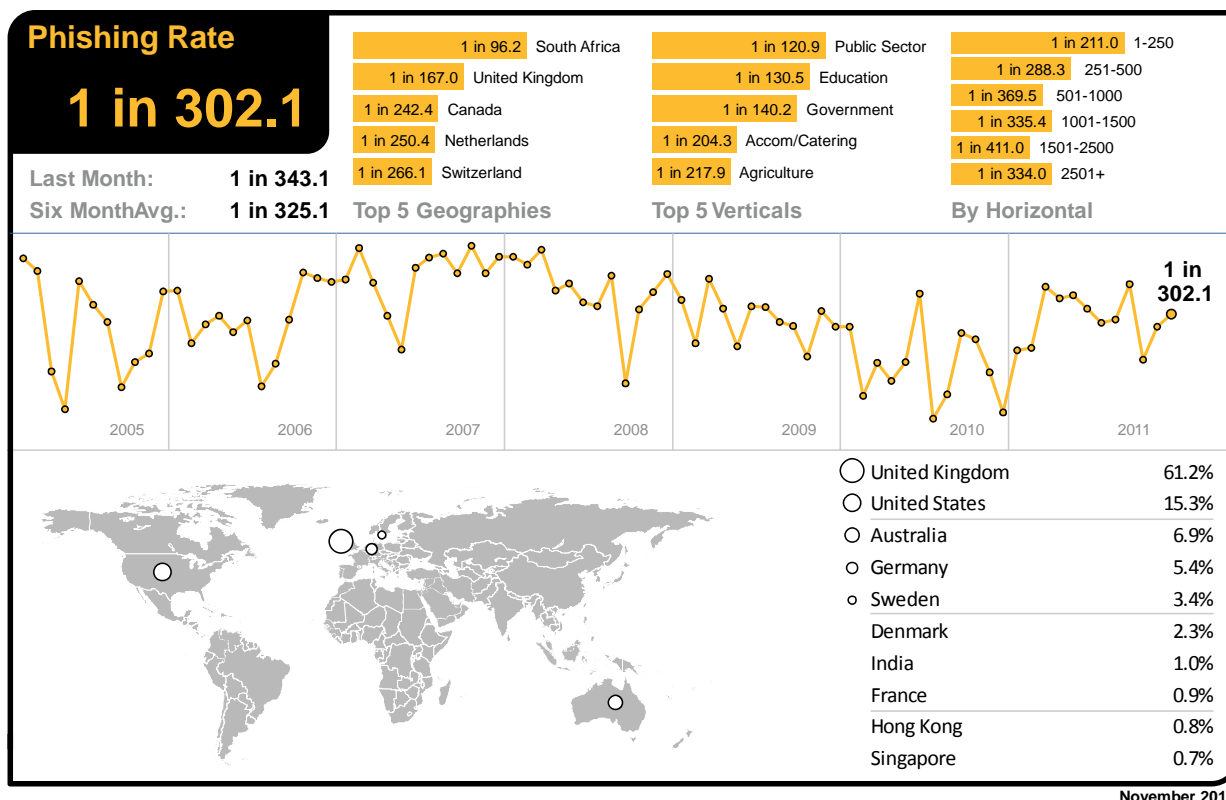
NDR (配信不能レポート)スパムとなったスパムメールの数は、11 月も引き続き安定しており、攻撃者はこれらの攻撃を実行する際に有効なメール配信リストを使っていると考えられる。NDR は通常、姓名のデータベースを使用した大規模な辞書攻撃の後に発生する。これらの状況は、スパマーが配布リストを更新してメールが戻ってくるのを最小限にとどめていることを示す。

⁶ http://www.symantec.com/ja/jp/business/theme.jsp?themeid=state_of_spam

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

11 月の全体的なフィッシングレートは前月から 0.04% 増加し、平均でメールの 302.0 通に 1 通(0.33%)にフィッシング攻撃が含まれていた。



11 月にフィッシング攻撃で再び最も大きな割合を占めたのは南アフリカで、メールの 96.2 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 2 位で、メール 167.0 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 461.8 通に 1 通、242.4 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、426.2 通に 1 通、デンマークは、781.5 通に 1 通、オランダは、250.4 通に 1 通となっている。オーストラリアでは、361.0 通に 1 通、香港では 517.0 通に 1 通、日本では 2,058 通に 1 通、シンガポールでは 609.7 通に 1 通となっている。ブラジルでは、775.3 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、120.9 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 407.5 通に 1 通、IT サービス業界は 377.0 通に 1 通、小売業界は 397.0 通に 1 通、教育業界は 130.5 通に 1 通、金融業界は 331.7 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 211.0 通に 1 通、大企業(従業員数 2500 人超)では 334.0 通に 1 通であった。

フィッシングサイトの分析

11 月、フィッシングサイトの数は 66.1% 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 316.1% と 4 倍に増加していて、フィッシングサイトの約 54.6% を占めている。これらの大半は有名なソーシャルネットワーキング Web サイトに対する攻撃と関連付けられ、ツールベースのすべての攻撃の約 78% を占めている。

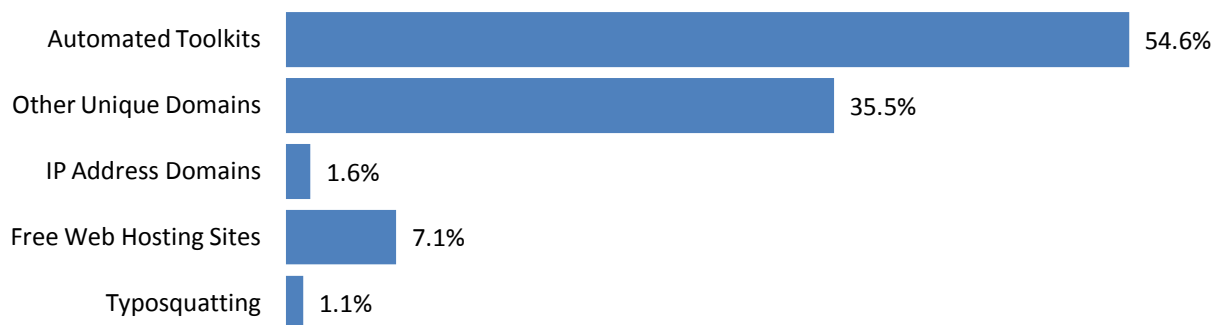
一意のフィッシング URL の数は 3.7% 減少しており、ドメイン名でなく IP アドレスを使ったフィッシングサイト(例: http://255.255.255.255)は 36.1% 減少している。フィッシングサイト全体のうち、正規の Web ホスティングサービスを悪用したものの割合は約 7.1% で、前月から 10.7% 減少した。英語以外の言語によるフィッシングサイトは、4.0% 減少した。

11 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、ドイツ語が最も多かった。

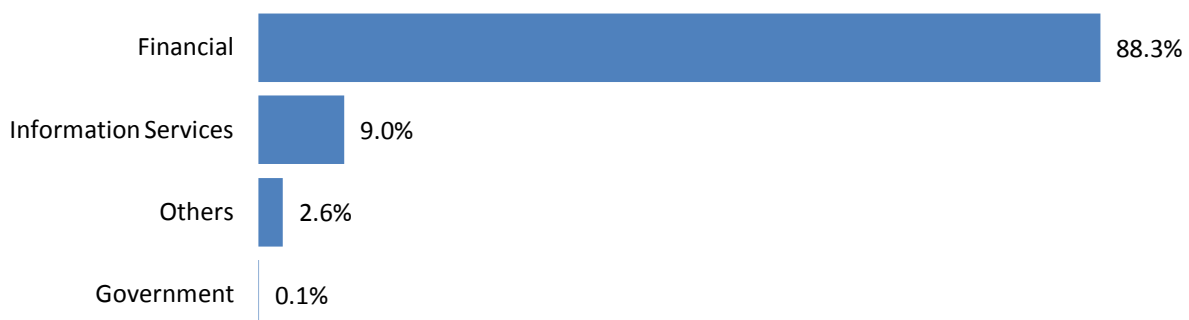
フィッシングサイトの所在地



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)

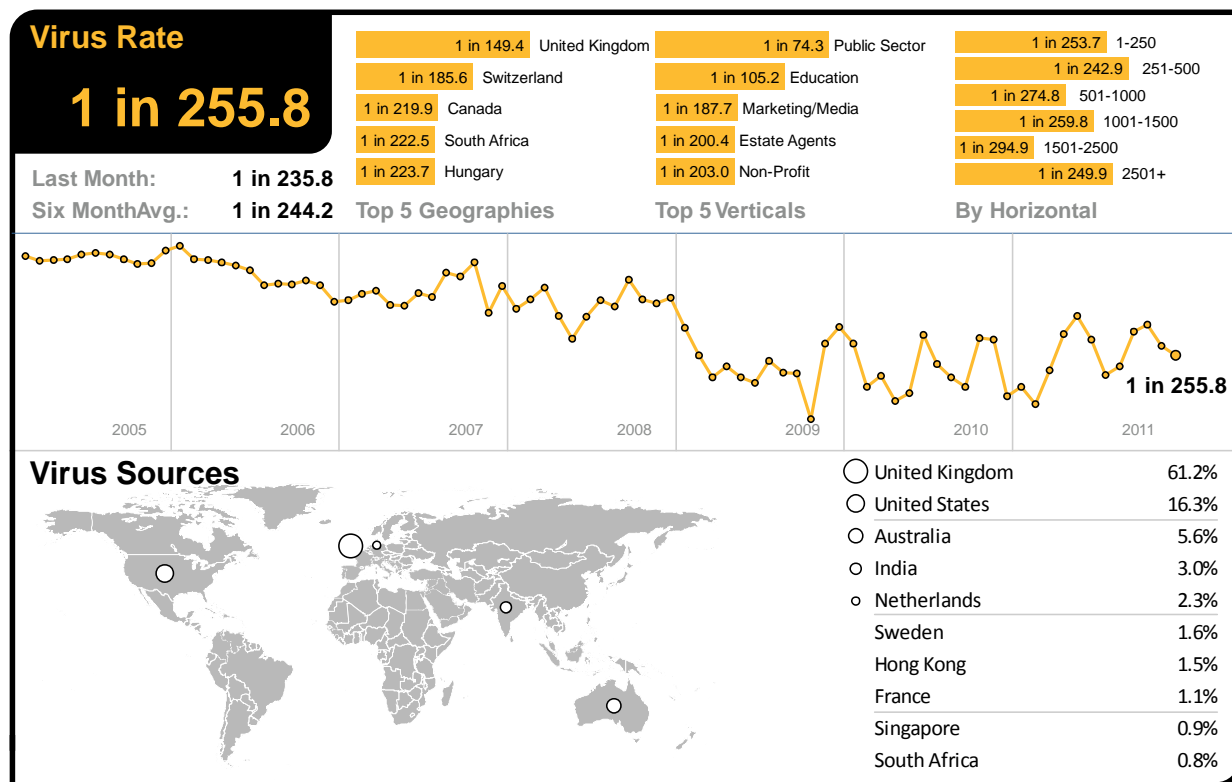


マルウェア分析

メールによる脅威

11 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、255.8 通に 1 通(0.39%)で、前月比で 0.03% 減少した。

11 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 40.2% を占め、前月比で 20.1% 増加している。



11 月、悪質メールの割合が最も高い国は引き続き英国で、メール 149.4 通に 1 通が悪質メールであった。2 番目がスイスで、185.6 通に 1 通が悪質であると識別された。

南アフリカは、222.5 通に 1 通が悪質であるとブロックされ、再び 5 位内となった。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 360.1 通に 1 通、219.9 通に 1 通であった。ドイツのウイルスレベルは、275.0 通に 1 通、デンマークは、710.5 通に 1 通、オランダは、238.2 通に 1 通となっている。オーストラリアでは、メール 326.2 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 1,147 通に 1 通、450.0 通に 1 通となっている。ブラジルでは、570.6 通に 1 通に悪質なコンテンツが含まれていた。

また、11 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 74.3 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 275.5 通に 1 通、IT サービス業界は 276.6 通に 1 通、小売業界は 337.1 通に 1 通、教育業界は 105.2 通に 1 通、金融業界は 386.6 通に 1 通となっている。

中小企業(従業員数 1 ~ 250 人)を標的にした悪質なメール感染型攻撃は 253.7 通に 1 通、大企業(従業員数 2500 人超)では 249.9 通に 1 通であった。

次の表は、11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40.8%が、ジェネリックな検出を用いて識別、ブロックされた。

11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、すべてのメール感染型マルウェアの29.6%を占め、すべてのジェネリックマルウェアの50.4%に相当する。

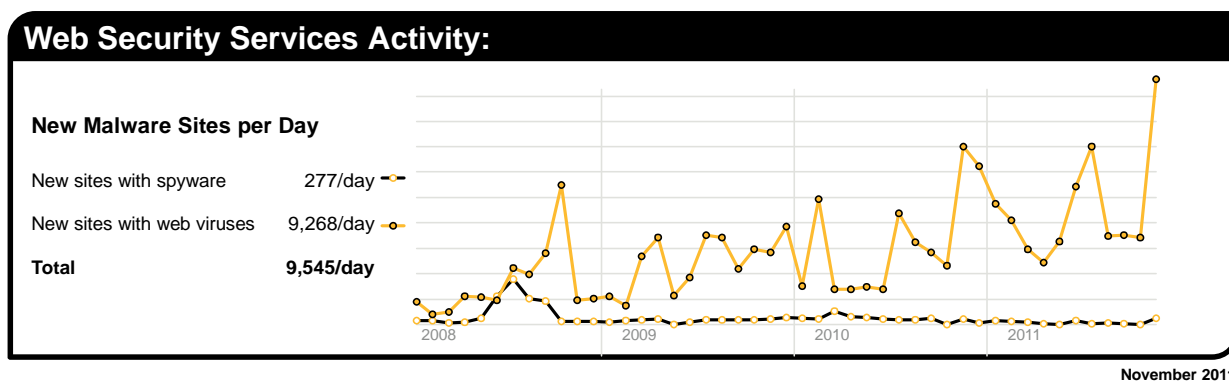
マルウェア名	マルウェアの割合
Exploit/Link-generic-ee68	6.53%
Exploit/Link-generic.dam	3.83%
Trojan.Bredolableml-6c19	3.58%
W32/Generic-fdc7-c476-c476	2.48%
Trojan.Bredolableml-f101	1.98%
W32/Generic-6900	1.90%
W32/Generic.dam	1.72%
W32/NewMalware!0575	1.61%
W32/Generic-8426-e566	1.54%
Trojan.Bredolableml-47bf	1.51%

最も多くブロックされたマルウェアの上位10個が11月のすべてのメール感染型マルウェアの約26.7%を占めた。

Webベースのマルウェアの脅威

11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4,915件特定した。これは、前月比で47.8%の増加となる。これは、Webサイトが危殆化されるか、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。



上のグラフは、11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、11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、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 19.3% 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。

11 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 11.1% 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%	Trojan.Gen.2	22.1%	PUP:ZBL	25.2%
Social Networking	19.3%	Suspicious.Emit	14.5%	PUP:MyWebSearch.EC	18.6%
Streaming Media	11.1%	Gen:Trojan.Heur.amKfbDF29Mpi	12.3%	PUP:JS.Script.C	8.8%
Computing and Internet	4.6%	Gen:Trojan.Heur.Cu9@Y!CHhQgi	8.5%	PUP:W32/Eshoper.B	8.0%
Search	4.1%	Gen:Trojan.Heur.amKfbr2TVGoi	4.1%	PUP:FakeAntiVirus.L	6.4%
Chat	3.4%	Trojan.Script.12023	2.9%	PUP:Generic.192950	4.5%
Hosting Sites	2.6%	Gen:Trojan.Heur.Mx9@XcmYEfei	2.7%	PUP:Clkpotatolgen3	3.3%
Peer-To-Peer	2.5%	VBS/Generic	2.2%	PUP:Generic.183433	2.8%
News	2.0%	Trojan.Maljava	1.7%	PUP:9231	2.6%
Entertainment	1.7%	Trojan.JS.Redirector.MY	1.5%	PUP:Agent.NGR	2.3%

November 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。

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 (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 ⁷	マルウェアの割合
WS.Trojan.H	21.93%
W32.Sality.AE	6.37%
W32.Ramnit!html	6.29%
Trojan.Bamital	5.74%
W32.Ramnit.B!inf	5.40%
W32.Downadup.B	3.00%
Trojan.ADH.2	2.25%
W32.SillyFDC.BDP!lnk	1.89%
Trojan.ADH	1.78%
W32.Virut.CF	1.73%

⁷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)

10月に最も多くブロックされたマルウェアは、WS.Trojan.H⁸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。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.AE⁹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11.9%をW32.Ramnitの亜種が占め、W32.Salityの全亜種は7.2%であった。

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15.0%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。

⁸ http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2011-102713-4647-99

⁹ http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2006-011714-3948-99

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、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。

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経由で公開された個人情報、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。