



メッセージラボ インテリジェンス: 2009 年 2 月

「不況スパムの『検索』が行われ、「受信」ヘッダーを偽装する新種のターゲット型トロイの木馬が登場、またCutwailがスパムのキューピッド役に」

「メッセージラボ インテリジェンス月次レポート:2009 年 2 月号」では、2009 年 2 月期における脅威の最新動向を盛り込み、ウイルスやスパムなど歓迎されざるコンテンツとの現在進行中の戦いについて詳しくお伝えいたします。

レポートの主な内容

- スパム — 2 月は 73.6%(前月比 1.3%減)
- ウイルス — 2 月は 304.9 通あたり 1 通にマルウェア(前月比 0.06%減)
- フィッシング — メール 190.4 通あたり 1 通でフィッシング攻撃(前月比 0.27%増)
- 悪意ある Web サイト — 1 日あたり 904 件の新たなサイトをブロック(前月比 22.1%増)
- 「不況スパム」を生成するスパム技術で、検索エンジンのリンクが使用される
- 「受信」ヘッダーを偽装する新種のターゲット型トロイの木馬
- Cutwailがスパムのキューピッド役に

今月の分析

「不況スパム」を生成するスパム技術で、検索エンジンのリンクが使用される

2月には、世界の金融危機が引き続きスパマーの欲望を満たすこととなり、彼らは「不況スパム」とも称すべきスパムを送信しました。不況スパムの主な内容は以下の通りです。

「Money is tight, times are hard. Christmas is over. Time to get a new watch! (経済状況は厳しく、クリスマスシーズンも終わりました。今が時計のお買い替えどきです!)」

「Affordable brand name watches (ブランド時計をお値打ち価格で)」

「Get 15% off these (15%引きいたします)」

「Cheaper than you could imagine (驚きの低価格)」

こうしたメッセージには、知名度の高い主要な検索エンジンへのリンクも記載されています。しかし、メッセージラボ インテリジェンスが2008年1月に報告した、スパムメッセージ内の検索エンジンへのリンクとは異なり、実際のところ、ここでは自動的なダイレクトリンクも使用されておらず、スパマーのサイトが検索結果の一番上に現れるようにするためのキーワード検索も行われていません。その代わりに、この特定の検索エンジンがターゲットサイトのインデックス化を行っていない可能性に望みを寄せるような形で、単にスパマーのドメインの検索を行っています。

検索エンジン スпамとは、スパマーが検索結果リストをもとに作成したリンクをメール本文に張るという手口によるものです。リンクを辿っていくと、ブラウザはスパマーのウェブサイトへ誘導されます。つまり、スパマーはメール本文にスパム サイトのURLが直接書き込まれていないメールを送ることが可能になり、従来型のアンチスパム製品ではメールがスパムであるかどうかの判別が難しくなっています。スパム フィルタには既知のスパムサイトを認識することはできても、深刻な巻き添え被害を発生させることなく、正規の検索エンジンサイトへのリンクを合理的にブロックすることはできません。

主要なインターネット検索エンジンの多くが、こうしたスパムに利用され、2008年1月にはスパムのおよそ17%を占めていました。しかしながら、検索エンジンからのリダイレクトを悪用したスパムはアンチスパム技術が追いついた段階で急速に減少していき、検索エンジンプロバイダではスパマーがこの機能を利用しにくいよう、対策を講じています。

この最新のアプローチの考え方は、一般的に受け入れられている方法とは矛盾しているように思われるかもしれませんが、以下の例でご覧いただけるように、メールでは、「直接移動する」が表示された後のリンクもクリックするよう指示されています。

このリンクをクリックすると、スパムドメインは検索エンジンのデータベース内に見つからないため、以下のように報告されます。



Example of spam containing links to search engine

「[redux].comの検索結果は見つかりませんでした。以下の指示を試してみるか、新たな検索語を上記に入力してください。[redux].comに直接移動する(サイトは存在しない可能性があります)」

ここから、ユーザがリンクをクリックすると、検索エンジンの検索結果ページからスパムサイトへ直接誘導されます。

他の主要な検索エンジンプロバイダは、検索インデックスに見つからない場合にウェブサイトへ直接リンクする機能を提供していないと思われるため、このアプローチは、この手口で使用されている検索エンジンのみで有効です。

「受信」ヘッダーを偽装する新種のターゲット型トロイの木馬

ターゲット型トロイの木馬は、特殊性の高いマルウェアであり、少量の特殊なスパイウェアを展開し、組織から機密情報を入手するという明白な意図をもって、特定の企業内の個人をターゲットとしています。2月のターゲット型トロイの木馬の量は1日あたり平均約50件と、大きくは増加しなかったものの、メッセージラボ インテリジェンスのチームは、偽装ヘッダーに関する新たな手口を特定しました。

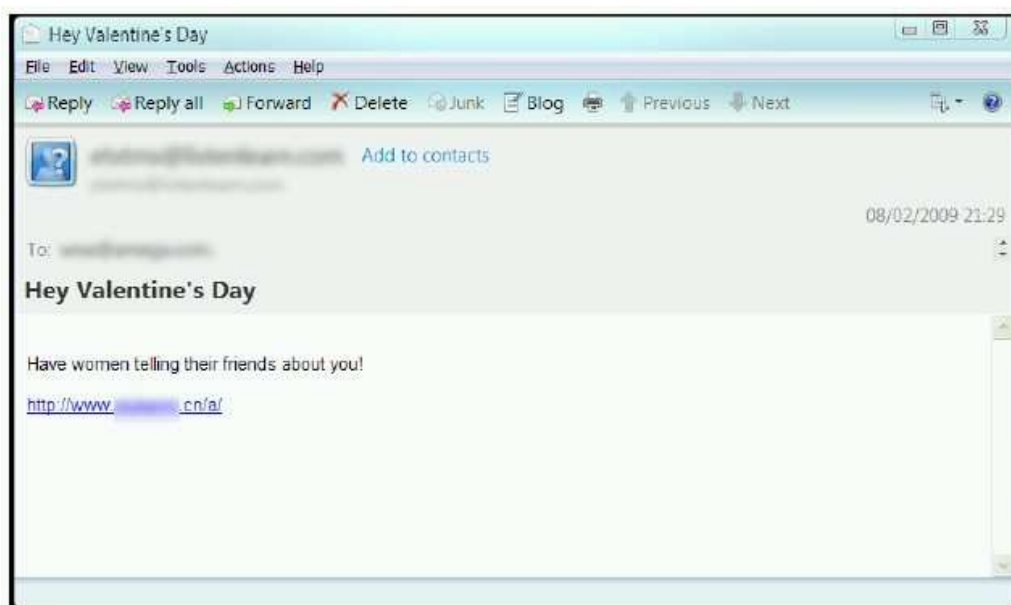
SMTPの「受信」ヘッダーは、メールが各ホップ、すなわち2つのメールサーバの間を移動してインターネットを通過する際に付される特別なヘッダーであり、メール独自の情報が追加されることで、その道筋を追跡できるようになります。この情報は空に残される飛行機雲のようなものですが、SMTPの多くの特性により、偽装が可能となっています。しかし、こうしたターゲット型マルウェアは、正規の無償ウェブメール ホスティング プロバイダから送られるケースが増えていることなどから、多くの攻撃者は、わざわざこれを使用しません。こうした偽装ヘッダーの唯一のメリットは、最終ホップが正確性を保証できる唯一の存在であり、これがメールを最終目的地まで届けるものであることから、詳細な検査の際、メールが正規のもののみとみなされる可能性が高まる点にあると考えられます。

この最新の攻撃では、ヘッダーはメッセージの発信元に信頼性を付与するために追加され、その組織を真に発信元としている可能性のある実在のヘッダーを使用し、メールの最初にこれを付しています。興味深いことに、実際のところは、この手口によって、そのメールは返って疑わしいものとして目立つ結果となりました。というのも、当社のSkeptic™技術は、マルウェアで使用される高度な難読化技術を特定することが可能であり、犯罪者が自らの活動を隠そうとすればするほど、より明白な形で現れるからです。

Cutwailがスパムのキューピッド役に: バレンタインデースパムが過去最高水準に到達

2月に入ってからというもの、バレンタインデーに関するスパムの割合は、スパム全体の2~3%から増加し、このロマンティックな日の数日前には9%以上に上っています。このスパムの圧倒的多数(6.5%)は、Cutwailボットネット(別名Pandex)を発信元としていました。これに引けを取らないのが、スパム全体の1~2%を占めるXarvesterですが、興味深いことに、現在最も活動的なボットネットであるMega-D (Ozdok)は、バレンタインデー関連のスパムの送信には関わっていません。

Cutwailのスパム活動は、「St. Valentine's Bonus(バレンタインデーのおくりもの)」や「Make this Valentine's Day the most memorable ever(今年のバレンタインを忘れられないものに)」といったバレンタイン関連の件名を用いた非常にシンプルなメールメッセージか、男性機能強化製品を売りつける.cnドメインのウェブサイトへのリンクが本文に記載されたメッセージによるものです。



Example of St. Valentine's Day spam sent from Cutwail botnet

Cutwailからのスパムメールのうち約15件に1件がバレンタインに関するものであり、このボットネットは、送信活動の約90%をバレンタイン関連のスパムに充てています。Cutwailは1日あたり推定70億件のスパムメールを生成していました。これはおそらく、これまでに観察されたバレンタインデーのスパムの中でも最大規模と考えられます。

2008年の場合、バレンタイン スパムは悪名高いStorm (Peacomm)ボットネットを発信元とし、1日のスパムに占める割合はわずか2%でした。今年のアプローチと同様に、Stormによって生成された昨年のバレンタイン スパムは、ハーブ系の男性器増強薬であるVPXLのウェブサイトへ誘導するものでした。今年、バレンタインに乗じたその他のボットネットには、Waledacがあります。これは、Waledacマルウェアへのリンクを含む、バレンタイン関連の悪意あるメールを大量に配信し続けています。

世界的傾向とコンテンツ分析

メッセージラボのアンチスパム、アンチウイルスは、未知の悪意ある送信元から有効なメールアドレス宛に送信される望ましからざるメッセージを特定、回避することに焦点を合わせたサービスです。

Skeptic™ Anti-Spam Protection: 2009年2月、新規および未知の悪意ある送信元から送られたスパムメールが世界全体のメールトラフィックに占める割合は73.3%(メール1.36通に1通)で、前月比1.3%減となっています。



2月期、フランスにおけるスパムの割合は9.2%減となったものの、メール全体に占めるスパムの割合は74.6%で、依然スパム最多受信国となっています。2月期の各国におけるスパムの割合は、アメリカ57.0%、カナダ52.6%、イギリス66.6%、ドイツ69.1%、オランダ67.4%、オーストラリア68.5%、香港72.8%、中国67.8%、日本65.6%となっています。

業界別では、教育業界がスパム最多受信業界となり、スパムの割合は67.9%に達しています。化学/製薬業界ではスパムの割合は59.8%に到達、小売業界では63.3%、公共部門は62.5%、金融業界は58.9%となっています。

2月の最初の週には、スパムの量が初めてMcColo停止依然の水準に戻り、ボットネット活動の増加により、スパムの割合はメールトラフィックの79.5%に達し、インターネットサービスプロバイダのMcColoが2008年11月12日に上流プロバイダから接続停止にされて以来、最高水準となりました。2008年の平均のスパムレベルは約81.2%で、もう1つの有名なISPであるAtrivo(別名Intercage)の閉鎖後の2008年10月には79.5%に落ちました。

全体的なスパムレベルは2月に下落したものの、これは、水面下で進行中の本質とは矛盾していません。McColoの混乱の後も、ボットネットは引き続き、迅速かつ積極的な拡大に力を注いでいます。

1日に全体で600億~900億件のスパムメールの送信元となっているCutwailは、依然最大のボットネットです(ボットネットについての詳細は、メッセージラボインテリジェンス2009年1月度レポートをご参照ください)。疑惑を抱かせないよう慎重に実行されるCutwailは、100万ボット以上という自らの規模を極めて効果的に維持しています。新登場のボットネットですが、Donbotはすでに、Cutwailに次ぐ2番目の規模を誇っています。

しかし、規模がすべてという訳ではなく、Mega-D は Cutwail の約半分の規模ですが、McColo の接続停止以降、他のすべてのボットネットを大幅に上回るスパムに関与しています。

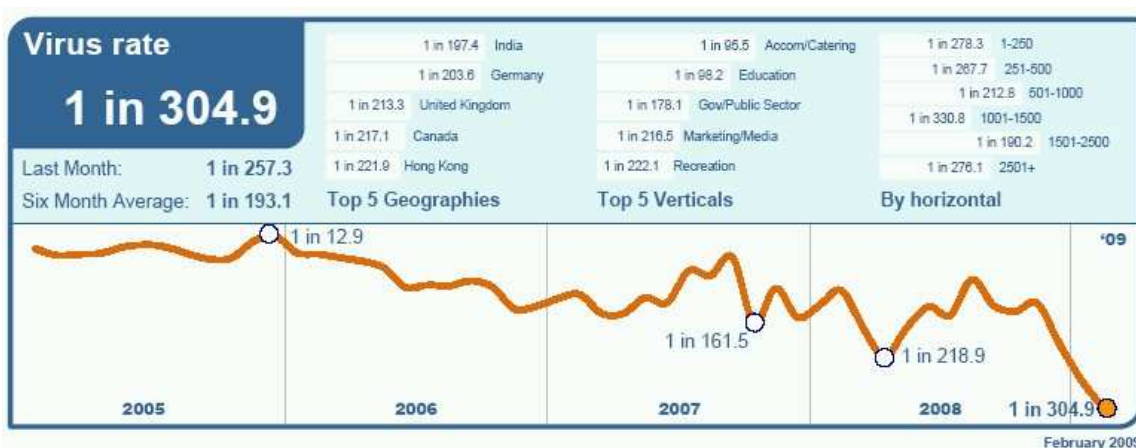
1 月下旬から 2 月初旬にかけてのスパム量の急増は、Cutwail、Xarvester、Rustock の各種ボットネットの積極的な活動によるものです。さらに、すでにスパムの 40%の発信元となっている Mega-D ボットネットが加わることで、この最新の急増は、スパムの量を過去数ヶ月間で最高水準に押し上げるのに十分なものでした。このような猛吹雪はわずか 3 日間しか続きませんでした。これらのボットネットが引き起こすことのできる潜在的な損害を思い出させるには十分な役割を果たしました。

重要なことに、Xarvester ボットネットは現在、送信量の点では Mega-D に並んでおり、最も積極的なボットネットの座を争っている状態です。こうした主要ボットネットの間では、優位性を巡る争いが繰り広げられており、McColo の接続停止以前には、スパムの約 90%がボットネットから送信されていましたが、McColo の閉鎖後、この割合は約 60%まで下落しました。2 月には、Xarvester の拡大により、現在ではスパムの 80%がボットネットを発信元としています。

Cutwail の送信活動が今後継続するか、あるいは Xarvester が先輩の Srizbi と同等の水準に到達できるかは、現時点では不明な状況です。Xarvester は Srizbi と同じ組織の出身と考えられており、1 月以降はすでに大幅な成長を見せており、強烈なパンチ力を持ったボットネットとして、現在も急成長中です。

Skeptic™ Anti-Virus and Trojan Protection: 2 月期、新規および未知の悪意ある送信元から送られたスパムメールが世界全体のメールトラフィックに占める割合は 304.9 通あたり 1 通 (0.33%) で、前月比 0.06%減となっています。

2 月期には、悪質サイトへのリンクが張られたマルウェア感染メールが 3.7%を記録、前月比では 7.6%減となっています。ポストカードを装ったメールは 2 月期、悪意あるリンクのうち 62.9%を占めたほか、復活を遂げた Storm ボットネットが、悪質サイトへのリンクが張られたメールの 3.6%を占めました。



最もウイルス活動が盛んという、羨ましくない立場の国になったのは0.16%増のインドで、197.4通に1通となっています。各国におけるウイルスの頻度は、イギリスで213.3通に1通、アメリカで424.5通に1通、カナダで217.1通に1通、オーストラリアで573.8通に1通、ドイツで203.6通に1通、中国で304.4通に1通、香港で221.9通に1通、日本で450.8通に1通となっています。

最もウイルス活動が盛んだったのは宿泊/ケータリング業界で、ウイルスの割合は0.42%増の95.5通に1通でした。ITサービス業界でのウイルス割合は347.5通に1通、小売業界では356.4通に1通、金融業界で505.5通に1通となっています。

フィッシング: 2月期、フィッシング攻撃の割合においては前月比で0.27%の増加が見られました。メール190.4通あたり1通(0.53%)で、何らかの形のフィッシング攻撃が行われています。ウイルスやトロイの木馬など、メール感染型の脅威全体に占める割合で見ると、フィッシングメールの数は3.4%減少しており、2月期に捕捉されたマルウェア感染メール総数の61.6%となっています。

世界規模の金融危機以降、M&Aの周辺で大きな注目を集めている銀行関連を中心に、フィッシング活動は一定の増加を見せています。最近のフィッシング活動は、マスコミの報道やニュースに即したメッセージを作成することで、こうした動きに乗じようとしているように思われます。馴染みのない銀行からのメッセージを受信することに多くの人が驚かないであろう時期では、消費者がこうした詐欺に騙される可能性はこれまで以上に高くなり、自身の家計用の銀行に関する指示であれば、消費者がこれに従おうとする可能性はさらに高まると考えられます。

おそらくはMcColo接続停止の破壊的な影響により、2008年の終わり頃には、こうした傾向は縮小しました。最近のポットネット活動の復興により、フィッシングはスパムの送信よりも収益性の高い活動であるように思われます。



Skeptic™ Web Security Version 2.0: メッセージラボ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2月期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、前月比11.2%減の33.2%になっています。

ウェブセキュリティ活動を分析した結果、2月に捕捉されたウェブベースのマルウェアのうち、26.1%が新種のものでした。メッセージラボ インテリジェンスではまた、1日平均941件もの有害なウェブサイトを新たに特定しています。平均件数は1月比で22.1%減少。これら有害サイトにはマルウェアのほか、スパイウェアやアドウェアなど潜在的に問題のあるプログラムが潜んでいます。

Web Security Services (Version 2.0) Activity:

Policy Based Filtering	Web Viruses and Trojans	Potentially Unwanted Programs
Chat 35.2%	Exploit-MS06-006.gen 15.1%	PUP:Server-FTP.Win32.Tftpd.274 60.7%
Advertisements & Popups 33.2%	JS/Obfuscated 7.7%	PUP:WebToolbar.Win32.MyWebSear... 11.6%
Unclassified 13.5%	JS/Tenia.d 6.6%	PUP:Coupon 11.1%
Streaming Media 4.7%	Suspicious: Possible New Virus 4.6%	PUP:RemoteAdmin.Win32.WinV... 2.7%
Downloads 2.5%	Trojan.Win32.RaMag.a 4.6%	PUP:ZangoSA 1.9%
Games 1.9%	HTML/FakeAV 4.4%	PUP:RemoteAdmin.Win32.WinVNC.ad 1.8%
Personals & Dating 1.8%	JS/Generic Exploit.j 2.4%	PUP:WebToolbar.Win32.Zango.bw 1.4%
Computing & Internet 1.0%	Suspicious IFrame.b 2.3%	PUP:RemoteAdmin.Win32.WinVNC.ab 1.0%
Adult/Sexually Explicit 0.9%	Exploit-IFrame.gen.c 2.0%	PUP:BDSearch 0.6%
Infrastructure 0.7%	Suspicious IFrame.a 1.8%	PUP:NetTool.Win32.STunnel.404 0.5%

February 2009

上の表で「Unclassified (未分類)」とされているのは、新種もしくは未分類のサイトです。これらサイトは、フィッシングやスパムをホスティングした怪しい目的に使われるおそれのあるサイトだけでなく、正規の会社による分類作業中の新規サイトやドメインである可能性があります。メッセージラボのサービスを使用することで、顧客はこうしたサイトに対し、柔軟なアプローチを採用することができます。これらのサイトからダウンロードされるすべてのコンテンツは、商用ウイルス エンジンとSkeptic 技術を組み合わせた当社独自の手法によってスキャンされるため、セキュリティの維持を目的に、こうしたサイトを初期設定でブロックする必要はありません。

下のグラフは、2月中にスパイウェアおよびアドウェアの新規サイトをブロックした数の1日あたりの平均と、ウェブベースの新規マルウェアサイトをブロックした数の1日あたりの平均とを比較したものです。

Web Security Services (Version 2.0) Activity:



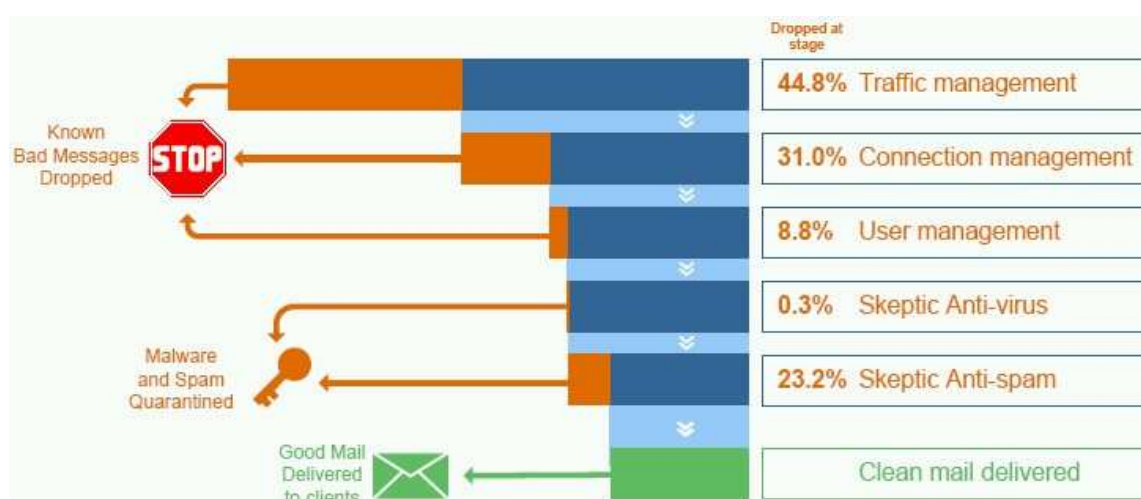
February 2009

2月にブロックされたサイトのうち、実に14%が悪意あるJavaScriptコードによるものでした。

トラフィック マネジメント

プロトコル レベルで運用されるトラフィック マネジメント技術により、メッセージの総数は減少を続けています。問題のある送信元が特定されると、TCP プロトコルに組み込まれた機能によってメールサーバへの接続がスローダウンします。これによって既知のスパムの流入は大きく減少しますが、正規のメールについては迅速な処理が保証されます。

メッセージラボのサービスでは2月期に、一日平均26億のSMTPコネクションを処理。このうち44.8%はトラフィック マネジメントを行った結果、明らかに悪質もしくは問題のあるトラフィックであると判断され、遮断されました。残りのコネクションは次に、メッセージラボのコネクション マネジメント機能とSkeptic™によって処理されました。



コネクション マネジメント機能

コネクション マネジメント機能は、アカウント獲得を狙ったディレクトリ ハーベスト攻撃や、機械的に生成した暗号やパスワードを総当たりに試すブルートフォース攻撃、メールサービス妨害 (DoS) 攻撃など、問題のある送信元から多数のメッセージを送信して組織にスパムを浸入させたり、ビジネス上のコミュニケーションを混乱させたりすることを狙った攻撃を阻止する上で、特に有効です。コネクション マネジメント機能は SMTP レベルで働き、「SMTP 認証」技術によってメールサーバへのコネクションが正規のものであるかどうかの認証を行うものです。送信元がオープンプロキシまたはボットネットであることが明らかな、既知のスパムやウイルス発信元から送信された問題のあるメールを特定し、コネクションを遮断することができます。2 月には、受信されたインバウンド メッセージのうち平均 31.0%が、ボットネットなど既知の悪意ある送信元からのものとして補足、遮断されています。

ユーザ マネジメント機能

ユーザ マネジメント機能は「登録ユーザの有効メールアドレス検証機能」を用い、受信側のメールアドレスが無効または存在しないと特定された場合はコネクションを廃棄して、登録ドメインからのメール総数を減らしています。2 月にはインバウンド メッセージのうち平均 8.8%が無効なものと特定されました。これらはドメインのディレクトリ攻撃を目論んだものでしたが、失敗に終わっています。

メッセージラボについて

メッセージラボは、中小企業からフォーチュン 500 社まで、世界 86 か国以上の国々で 19,000 社以上のクライアントを擁し、メッセージングと Web を対象に統合セキュリティ サービスをご提供するリーディング プロバイダです。メールや Web、インスタント メッセージによるコミュニケーションの保護から管理、暗号化、アーカイブ保存にわたる幅広い管理セキュリティ サービスをご提供しています。

これらサービスを提供するのは、世界各地に配置されたメッセージラボのインフラストラクチャと、セキュリティのエキスパートによる 24 時間 365 日のサポート体制です。これによってリスクを管理、削減するための便利でかつ費用効果の高いソリューションをご提供し、ビジネス情報の交換を確かなものにします。また、世界的に著名なマルウェアとスパムの専門家を多数擁する「MessageLabs Team Skeptic™」は、毎日数十億件の Web ページ、電子メール、インスタント・メッセージ(IM)の監視を行うことにより、さまざまな通信プロトコルを網羅する、世界的な視点からの脅威分析能力を有しています。

詳しくは、メッセージラボの Web サイトをご覧ください。 <http://www.messagelabs.co.jp/>