



メッセージラボ インテリジェンス: 2009 年 4 月

「画像スパムの再燃によってスパム レベルは 85%を超え、過去 19 ヶ月で最高に」

「メッセージラボ インテリジェンス月次レポート: 2009 年 4 月号」では、2009 年 4 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 — 4 月は 85.3% (前月比 9.6%増)
- ウイルス — 4 月は 304.9 通あたり 1 通にマルウェア (前月比 0.08%減)
- フィッシング — メール 404.7 通あたり 1 通でフィッシング攻撃 (前月比 0.10%減)
- 悪意あるウェブサイト — 1 日あたり 3,561 件の新たなサイトをブロック (前月比 27.3%増)
- リダイレクト リンクと画像スパム — レピュテーション ハイジャッキング (信頼できるドメインの使用)
- G20 サミットが金融機関に対するターゲット型攻撃のテーマに
- Downadup (別名 Conficker - エイプリル フール)

今月の分析

画像スパムが再燃し、リダイレクト リンクを使用することでスパム レベルが 2007 年 9 月以降初めて 85%を超過

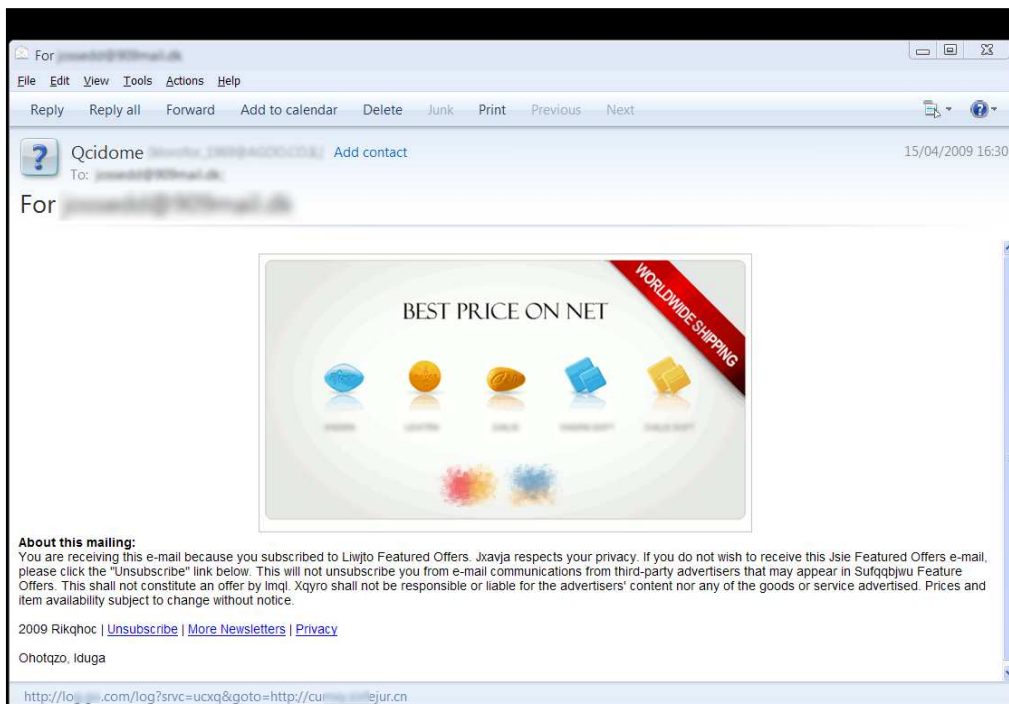
メッセージラボ インテリジェンスでは、スパム レベルが過去 19 ヶ月で初めて 85%を超えたことが確認されています。画像スパムは 2007 年にピークを迎えた現象で、スパム コンテンツを含む.gif や.jpg などの画像ファイルが添付されたメールによるものでした。多くの場合、このような画像には、メール内の単語のパターンを分析する従来のスパム フィルタリング手法を回避するために画像として描画されたテキストが表示されていました。

現在では、このような画像は信頼できるホスティング サイトのように見える場所でホストされており、画像ホスティングの実際の場所をわかりにくくするために、信頼できるサイトからのリダイレクト リンクを利用できるようになっています。これは、メールに含まれるハイパーリンクのドメインの性質とスパム

メッセージである可能性について判断するためにそのドメインを調べるスパム フィルタの回避手段として、スパマーが使用する手法の 1 つでもあります。

次の例では、配信停止依頼のオプトアウトやプライバシー リンクなどの標準のメール テキストがメッセージに表示されているようにも見えますが、これは全体的な見た目が米国の CAN-SPAM などの法律に準拠している正規のもののようにデザインされたテキストです。

スパムのフィンガープリント認識手法を回避するために、メッセージのコンテンツ内にランダムな単語も挿入されています。



上記の例では、メッセージに画像を表示するために、メッセージに次の URL が含まれています。

```

```

この別のサイトへのリダイレクトパスをたどると、以下に示すように Web サーバによって再度リダイレクトされ、最終的に画像が表示されます。画像がダウンロードされると元のハイパーリンクのドメイン名が保持され、`http://[redux redirected ip address]/10.gif?[redux original domain]`などのようにパラメータとして URL に渡されることにも注目してください。

これは、スパマーがおそらく時間をかけて各ドメインの有効期限と有効性を特定するために、各ドメインの使用状況の追跡に使用する場合があると考えられています。

```

[ewood@marple ~]$ wget -S http://spammer.cn/10.gif
--2009-04-17 16:05:36-- http://spammer.cn/10.gif
Resolving spammer.cn...
Connecting to spammer.cn|192.168.1.100|:80... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 302 Moved Temporarily
  Server: nginx/0.6.35
  Date: Fri, 17 Apr 2009 15:06:31 GMT
  Content-Type: text/html
  Content-Length: 161
  Connection: keep-alive
  Location: http://spammer.cn/10.gif?spammer.cn
Location: http://spammer.cn/10.gif?spammer.cn [following]
--2009-04-17 16:05:51-- http://spammer.cn/10.gif?spammer.cn
Connecting to spammer.cn:80... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 200 OK
  Server: nginx/0.6.35
  Date: Fri, 17 Apr 2009 15:05:52 GMT
  Content-Type: image/gif
  Content-Length: 18492
  Last-Modified: Tue, 14 Apr 2009 07:50:53 GMT
  Connection: keep-alive
  Accept-Ranges: bytes
Length: 18492 (18K) [image/gif]
Saving to: '10.gif?spammer.cn'

100%[=====>] 18,492      19.1K/s   in 0.9s

2009-04-17 16:05:53 (19.1 KB/s) - '10.gif?spammer.cn' saved [18492/18492]

```

スパム フィルタをさらに回避できるようにデザインされたスパム メッセージで使用されている難読化のその他の例には、HTML スタイル タグを使用してアンチスパム フィルタを混乱させるよう意図した、ランダム テキストを隠す方法などがあります。以下に例を示します。

```
<STYLE>Ysavu ujkuibito Yna wuc</STYLE>
```

スタイル タグ間のテキストは、実際にはメール メッセージに表示されず隠れたままになりますが、このシンプルな手法が使用されることで、従来型のアンチスパム フィルタでは手に負えなくなる場合があります。この手法は、次のようにハイパーリンクのドメインを分断するためにも使用されています。

```
www.spammerdomain<STYLE>Zowjqz otuwaqito Fodi ahqwu</STYLE>name.cn
```

上記の例では、HTML スタイル タグ間のテキストは表示されませんが、アンチスパム ツールの中には、分析の実行前に単純に HTML タグを除外して混乱し、この例のドメインを ahqwh.name.cn と見なしてしまう可能性があります。

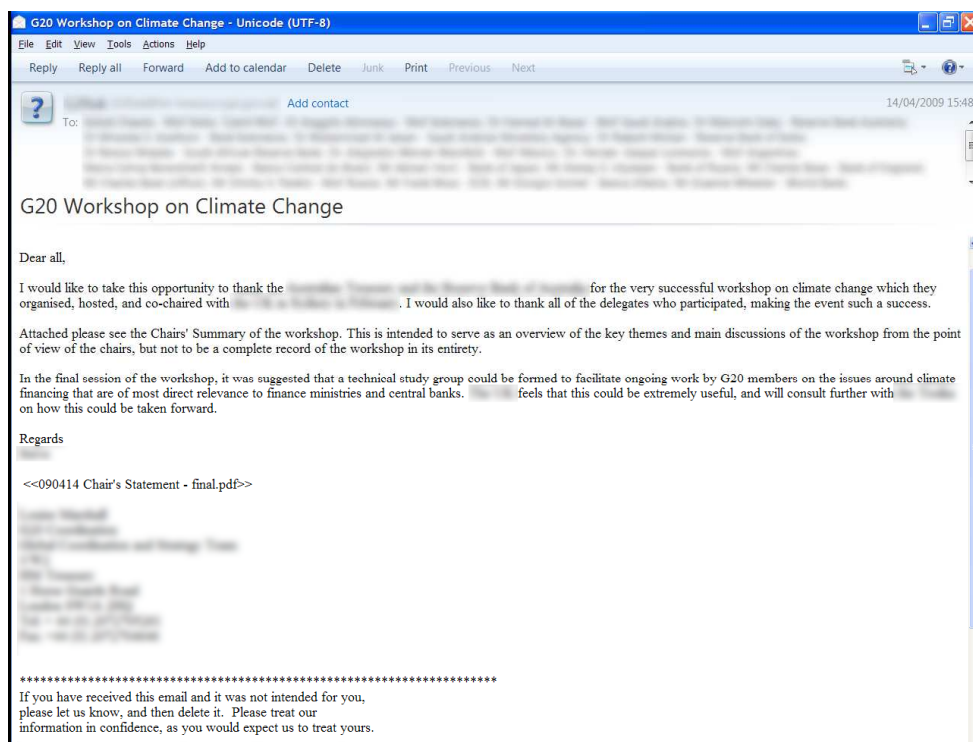
さらに、画像をホストするために使用されるトップレベル ドメインの多くは、中国に割り当てられている.cn ドメイン サフィックスに登録されています。これは、スパム ドメインの登録に関連付けられている TLD ドメインのメイン登録機関の関連会社の多くが活動の正常化を迫られており、このようなドメインを登録するのがかなり難しくなっているためであると考えられます。結果として、スパマーは、このような厳しい規制がないと思われる海外の登録機関にドメインを登録せざるを得なくなっています。

最近ロンドンで開催された G20 サミットが 3 月から 4 月の間にさまざまなターゲット型トロイの木馬攻撃の対象に

2009 年 4 月 2 日に、20 人の財務大臣や中央銀行総裁で構成される G20 がロンドンで一堂に会し、世界中のメディアから大いに注目を集めたため、このサミットは過去 2 ヶ月にわたってターゲット型マルウェア攻撃の増加の原因にもなりました。

2008 年のこのような攻撃の数は 1 日あたり平均約 53 件で、2009 年第 1 四半期は 1 日あたり約 60 件に増加しています。G20 サミットの直前とその後数日間は 1 日あたり約 100 件に増加し、それ以降は 1 日あたり約 60 件に落ち着きました。

このような攻撃を受けたのは、G20 に関わったいくつかの中央銀行の個人などでした。このようなメールの一例を次に示します。



メールには、開くとトロイの木馬ダウンローダがインストールされて実行される PDF ファイルが添付されていました。これにより、さらにスパイウェア コンポーネントがターゲット コンピュータにダウンロードされます。

このようなターゲット型攻撃は、2 月下旬にソーシャル エンジニアリングのために G20 関連のトピックを使用して開始され、3 月上旬に金融機関や中央銀行に対して攻撃が集中するようになり、これが 4 月上旬まで続きました。活動のピークは、主要な金融利害関係者による G20 に先立つ会談の直前である 3 月中旬頃に始まりました。攻撃の中には、実際の悪質でないメールに対する返信として作成されたものもあると報告されており、受信者のうち少なくとも 1 人は既に感染していたということになります。

Downadup (別名 Conficker または Kido) - 4 月 1 日

4 月 1 日のエイプリル フールは年に一度、互いにちょっとしたいたずらをするのが許容される日ですが、最近の Downadup マルウェアの発生に関連付けられるようになると、この日は別の理由でも重要になりました。セキュリティアナリストが、このマルウェアの旧型に既に感染しているコンピュータが 4 月 1 日にさらに新しい、進化したバージョン(Downadup.C)に更新される可能性があるとは指摘したのです。

この更新では、検知や阻害の可能性をさらに防げるようにマルウェアに機能が追加され、アンチウイルス製品に関連するプロセスを強制終了できる新しい検知対策が導入されました。

4 月 8 日に、Waledac マルウェアの劣化コピーにも見える新種が特定されました(Downadup.E)。

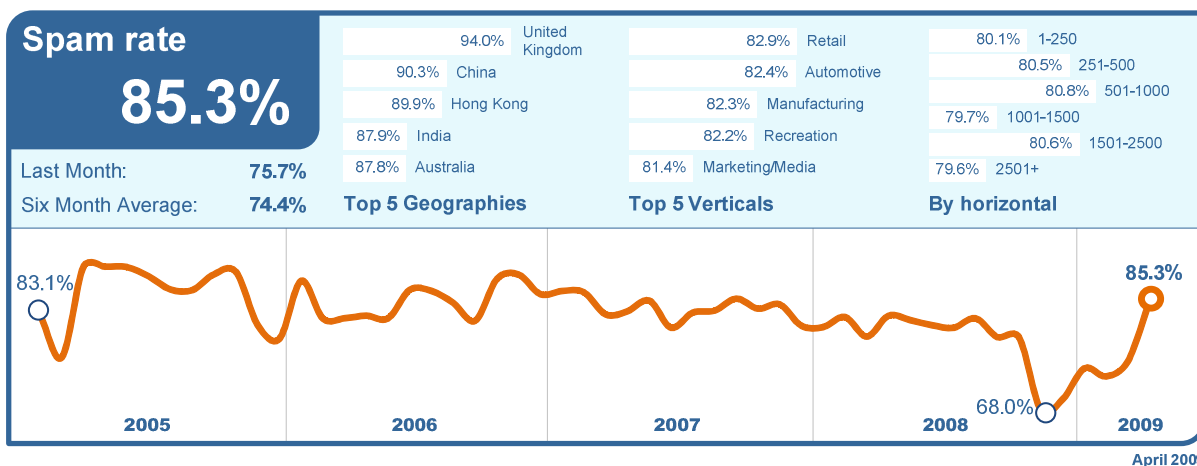
Downadup マルウェアの詳細とそのマルウェアから保護するための簡単な手順については、次のシマンテックのウェブサイトを参照してください。

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2009033012483648>

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4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85.3%(メール1.17通に1通)で、前月比9.6%増となっています。

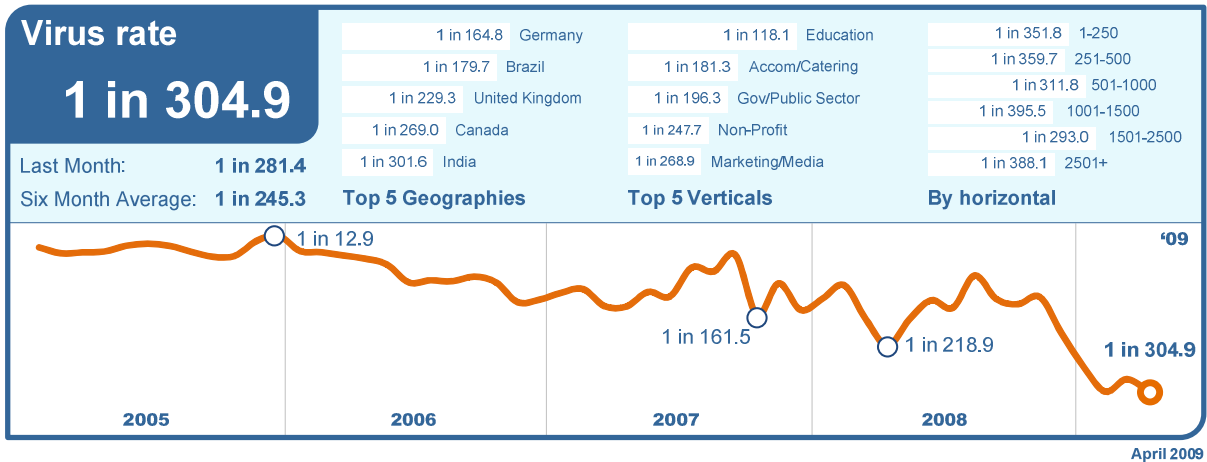


スパムレベルについては、4月に25.6%増加してすべてのメールの94%を占めるようになった英国が最大のスパム被害国となっています。米国のスパムレベルは79.4%に増加しました。カナダは77.4%、香港は89.9%でした。ドイツ83.3%、オランダ78.0%、オーストラリア87.8%、中国90.3%、日本86.4%となっています。

業界別では、小売業界がスパム最多受信業界となり、スパムの割合は82.9%に達しています。教育業界ではスパムの割合は81.1%に到達、化学/製薬業界では77.3%、公共部門は76.1%、金融業界は78.2%となっています。

Skeptic™ Anti-Virus and Trojan Protection: 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件(0.28%)で、前月比0.08%減となっています。

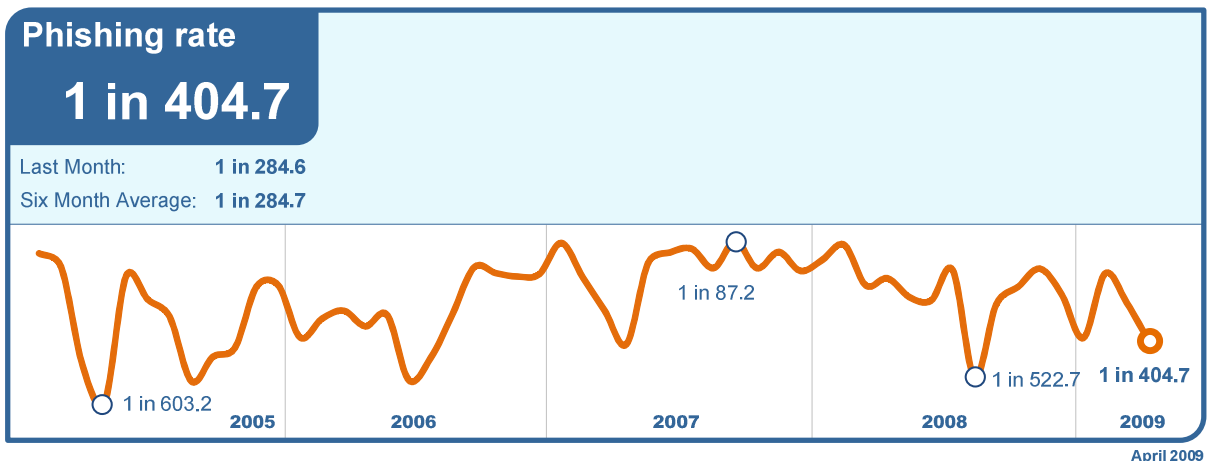
4月期には、悪質サイトへのリンクが張られたマルウェア感染メールが13.3%を記録、前月比では6.9%減となっています。ポストカードを装ったメールは4月期、悪意あるリンクのうち61.5%を占めたほか、Storm または Waledac に関連するメールがさらに8.6%を占めました。



4月に最もウイルス活動が盛んだったのは0.07%増のドイツで、164.8通に1通となっています。米国のウイルスレベルは1/512.1、カナダは1/269.0、オーストラリアは1/908.8でした。英国のウイルスレベルは1/229.3、中国は1/338.1、香港は1/370.8でした。日本は1/1,883.2に達しました。

0.19%減となったものの、最もウイルス活動が盛んだったのは依然教育業界で、ウイルスの割合は118.1通に1通でした。ITサービス部門のウイルスレベルは1/367.3、小売り部門は1/506.1、金融部門は1/446.9でした。

フィッシング: 4月期、フィッシング攻撃の割合においては前月比で0.10%の減少が見られました。メール404.7通あたり1通(0.25%)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、フィッシング攻撃の割合は9.2%減少しており、4月期に捕捉されたマルウェア感染メールおよびフィッシング攻撃総数の89.7%となっています。



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4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 21.6%増の 61.6%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、4月期に捕捉されたウェブベースのマルウェアのうち、63.3%が新種のものでした。また、メッセージラボ インテリジェンスでは、マルウェアやその他の迷惑プログラム(スパイウェアやアドウェアなど)をホストする新しいウェブサイトも、1日に平均 3,561 件特定されています。これは、前月比で 27.3%の増加になります。

Web Security Services (Version 2.0) Activity:

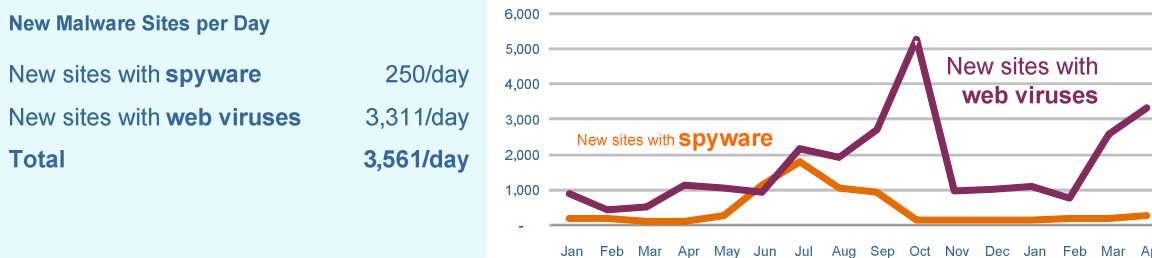
Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	61.6%	Trojan.Win32.Agent.bxgd	29.8%	PUP:Cinmus	40.3%
Streaming Media	8.7%	Trojan-Downloader.JS.Iframe.aqo	21.9%	PUP:WebToolbar.Win32.MyWebSear...	26.9%
Games	4.6%	Generic.dx	9.5%	PUP:WebToolbar.Win32.Zango.bw	4.5%
Downloads	4.2%	Trojan-Downloader.JS.Agent.dwf	3.4%	PUP:AdWare.Win32.AdMedia.ed	4.0%
Chat	3.5%	Generic PWS.y	2.3%	PUP:SAHAgent	2.1%
Blogs & Forums	2.9%	Refpron.gen	2.0%	PUP:AdWare.Win32.BHO.gei	2.1%
Personals & Dating	1.8%	Trojan-Clicker.HTML.IFrame.zm	1.6%	PUP:ZangoSA	2.0%
Adult/Sexually Explicit	1.8%	Trojan.JS.Agent.xl	1.6%	PUP:AdWare.Win32.SearchPage	1.4%
Infrastructure	1.3%	JS/Tenia.d	1.6%	PUP:BDSearch	1.3%
Gambling	1.1%	JS/Obfuscated	1.3%	PUP:AdWare.Win32.Shopper.ar	1.0%

April 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。これらのサイトは、フィッシングやスパムをホスト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、4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:

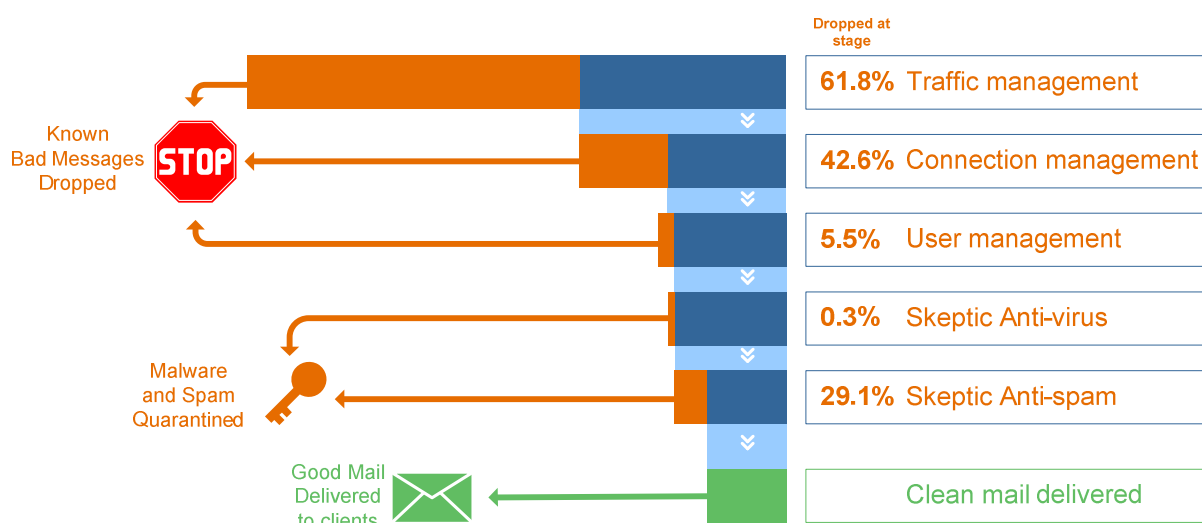


April 2009

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 4 月期に、一日平均 55.8 億の SMTP コネクションを処理しました。このうち 61.8%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侵入させたり、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。4 月には、受信されたインバウンド メッセージのうち平均 42.6%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捕捉、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」技術を用い、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。4 月にはインバウンド メッセージのうち平均 5.5%が無効なものとして特定されました。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 サイトでご覧いただけます。 <http://www.messagelabs.co.jp/>