レポート

McAfee脅威レポート: 2009年第1四半期

McAfee® Avert® Labs

目次

この『McAfee脅威レポート』では、電子メールやWebを狙った脅威について最新の統計情報と分析結果をお知らせします。McAfee Avert Labsでは、世界各地の研究員が個人ユーザや企業を取り巻く脅威を独自の視点で分析し、『McAfee脅威レポート』を四半期に一度発表しています。このレポートでは、過去3か月のセキュリティ脅威の調査結果を報告しています。詳しい情報については、McAfee Threat Center（http://www.mcafee.com/us/threat_center/default.aspまたはwww.trustedsource.org）をご覧ください。

昨年と比べて、2009年第1四半期は大きな変化が見られました。この変化は数か月前と比べても顕著なものです。2008年11月にMcColoが閉鎖されて以来、スパムの量が減少しています。これは1年前には予測のつかないことでした。スパムの量はピーク時よりも30%減少しています。3月にも増加の傾向は見られませんでした。しかし、以前のレベルに戻るのは時間の問題です。新たに作成されているゾンビやボットネットのデータを見ると、遠い将来ではないようです。

マルウェアが存在する不正なWebサイトの数も増えています。1日に数千のサイトが新たに出現し、新しいマルウェアが毎日作成されています。このレポートでは、この状況について詳しく報告します。

セキュリティ脅威としてConfickerワーム（正式名、W32/Conficker.worm）の関心が高まっています。しかし、これは本当の意味で脅威なのでしょうか。マスコミではこれほど騒がれていないものの、より危険な脅威は他にも存在します。このレポートでは、この状況について詳しく報告します。

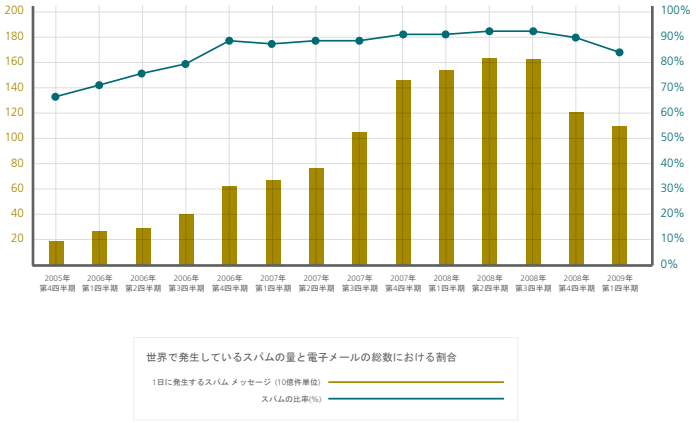
脅威の発生源が拡大し、発生源にも変化が見られます。このレポートでは、スパム発生源、ゾンビの作成、マルウェア サイトの存在場所など、脅威と地理的な関係について分析結果を報告します。また、攻撃者や犯罪者は国境を気にせず、攻撃を仕掛けています。

最後に、1月に発表した『2009年の脅威予測』で行った予測を検証します。警戒心の低いユーザにとって、最新のイベントやソーシャル ネットワーキング サイトが危険な存在になっています。

スパム: 世界的な問題

一時的な減少傾向

2009年第1四半期は電子メールとスパムの量が減少しています。これは過去2年間では見られなかった現象です。この結果は、世界的な景気停滞や厳しい経済状況を反映しているわけではなく、2008年11月にMcColoが閉鎖された影響によるものです。スパムの量は、1年前の同時期と比べ20%減少しました。過去最高を記録した2008年第3四半期と比べると30%の減少です。現在では、スパム サイト閉鎖前の70%程度に戻っていますが、まだ最盛期のレベルには達していません。



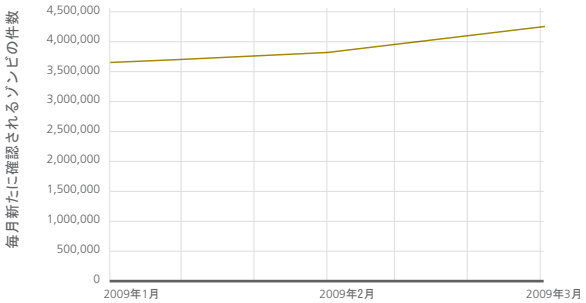
ここ数年間、1年で電子メールの量が最も多い月は3月でしたが、今年は例年通りにはなりませんでした。昨年は1日平均1530億通のメッセージがやり取りされましたが、今年の3月は1000億通に過ぎませんでした。

総メール数に占めるスパムの割合も、2006年以来初めて90%を下回りました。2008年は第4四半期こそ86%でしたが、全体では90%を維持しています。電子メールの用途や使用状況は個人によって差がありますが、平均すると、昨年と比べて1日にやり取りする電子メールの量が6通から12通少なくなっています。

スパムの量は2008年の最盛期のレベルに間違いなく戻ると思われます。しかし、サイト閉鎖直後の予測に反して、スパムのコマンド センターやボットネットの再構築には時間がかかっています。スパム送信者にとっても投資効果が最終的な判断基準になっています。

新しいゾンビが急増

この四半期では、ゾンビ コンピュータが利用しているIPアドレスが新たに1200万個見つかりました。昨年の第4四半期と比べると50%の増加です。新しいゾンビの数は2008年第3四半期に最大数を記録していますが、今期はその数よりも100万個多くなっています。スパムの量はMcColo閉鎖前の水準に戻っていませんが、新しいゾンビの急増を見ると、スパム送信者がインフラの整備に力を入れていることは間違いありません。スパムの量もすぐに元に戻ることが予測されます。



感染したシステムの分布を国別にみると、2009年第1四半期は、新しいゾンビが多く確認された上位10か国を合わせると、全体の63%に達しています。この数字は直前の2四半期よりも若干少なくなっていますが、スパム送信者の活動範囲が広がっていることがうかがえます。

2009年第1四半期		2008年第4四半期		2008年第3四半期	
国	IPの比率	国	IPの比率	国	IPの比率
米国	18.0	中国	15.8	中国	20.4
中国	13.4	米国	15.4	米国	16.5
オーストラリア	6.3	ドイツ	6.5	ドイツ	6.8
ドイツ	5.3	英国	6.0	英国	6.0
英国	4.7	ブラジル	4.9	ブラジル	4.8
ブラジル	4.0	スペイン	4.3	スペイン	3.7
インド	3.1	オーストラリア	4.1	インド	2.5
スペイン	3.0	イタリア	3.5	ロシア	2.4
韓国	2.8	ロシア	3.1	韓国	2.4
ロシア	2.5	韓国	2.4	イタリア	2.2
合計	**63.3**	合計	**66.0**	合計	**67.5**

スパム送信用のゾンビ コンピュータが最も多いのは中国と米国です。この2か国は3四半期連続で1位と2位を占めています。顕著な動きが見られるのがオーストラリアです。2008年の第3四半期は上位10か国にも入っていませんでしたが、それ以降ゾンビの数は急増し、現在では全体の6%を占め、第3位となっています。オーストラリアはスパム送信者にとって新たな肥沃な土地となっています。

2009年第1四半期		2008年第4四半期	
国	合計（%）	国	合計（%）
米国	35.0	米国	34.3
ブラジル	7.3	ブラジル	6.5
インド	6.9	中国	4.8
韓国	4.7	インド	4.2
中国	3.6	ロシア	4.2
ロシア	3.4	トルコ	3.8
トルコ	3.2	韓国	3.7
タイ	2.1	スペイン	2.4
ルーマニア	2.0	英国	2.3
ポーランド	1.8	コロンビア	2.0
	70.0		**68.3**

スパムの分布：米国が世界一

米国の自動車メーカーは技術面・販売面で苦戦を強いられている模様ですが、スパム生成という点では米国は世界で群を抜いています。米国で作成されるスパムは世界全体の35%を占めています。スパムの発信は世界中どこでも実行できますが、米国のコンピュータを利用してスパムを作成するスパム作成者はいまだに後を絶ちません。スパムの量が多い上位10か国で世界全体の70%が作成され、他の200近い国々を大きく引き離しています。

直近の2四半期を見ると、インドの伸び率が最も高く、世界全体の約7%を占めています。前の四半期から比べると、インドのスパム数は約2倍になっています。スパムの作成もインドにアウトソーシングされる時代になったようです。

また、タイ、ルーマニア、ポーランドが新たに上位10か国に入りました。スパム送信者がスパム エンジンの原動力となる新しい場所を必死に探している可能性があります。

	2009年 第1四半期		2008年 第4四半期		2008年 第3四半期
処方薬	25.0	処方薬	37.0	精力増強	31.2
広告	21.9	広告	19.3	広告	19.3
複製品	18.8	精力増強	16.8	処方薬	10.7
精力増強	17.5	DSN	9.5	Storm	8.0
DSN	7.1	出会い系	3.9	DSN	7.7
Storm	1.6	複製品	2.6	ニュース速報	6.7
免状	1.1	雇用	1.7	複製品	6.0
ソフトウェア	1.1	ソフトウェア	1.5	借入金	1.6
借入金	1.0	借入金	1.2	銀行取引	1.1
その他	4.9	その他	6.5	その他	7.7
	100.0		100.0		100.0

スパムの内容 : セックス、薬、賞金など

送信されるスパムの内容で最も多いのが精力増強、処方薬、一般的な広告です。過去3四半期を見ると、この3種類でスパムの約60%を占めています。スパムにも「Sex、Drugs and Rock'n' roll」（セックス、麻薬、ロックンロール）というスローガンが当てはまるようです。今では「Sex, Drugs, and Economics」（セックス、麻薬、経済状態）の方が適切かもしれません。

この四半期では複製品（主に高級腕時計の偽造品）に関わるスパムが急増し、スパム全体の約19%を占めています。この種類のスパムは昨年から存在していますが、この四半期に急激に増えています。スパム送信者は厳しい経済情勢につけ込み、偽物を安価で売り付け、利益を得ようとしているようです。

配信状況の通知を装うスパムも全体の8%を占めています。フィッシング詐欺者はこのようなスパムをよく利用し、盗み出したメールアドレスに宛先不明を通知する偽のメッセージを送信します。フィッシング詐欺はまだ下火にはなっていません。このようなスパムの多くは金銭に絡む内容が多く、ユーザを騙して個人情報を盗み出すために利用されています。

スパム送信者は国を気にしない

サイバーセキュリティのコミュニティでは、オンライン犯罪者の大半は東ヨーロッパの国々に存在し、その攻撃対象は西側諸国で、自国の企業やユーザへの攻撃は避けようとする、という通説があります。しかし、これは実情にあったものはないようです。インターネットには地理的な境界がありません。サイバー犯罪者はどの国の標的でも攻撃できます。サイバー詐欺師はロシアと東ヨーロッパ諸国の主要な政府機関や要人にも攻撃を仕掛けています。

最近、McAfee TrustedSource™は、マルウェアに感染した電子メールとスパムがロシアの政府機関と金融機関から送信されたことを確認しました。調査の結果、ロシアの次の金融機関が被害を受けていることが判明しました

- Rusfinance Bank
- OGO Bank
- Tusarbank
- Link Capital Investment Bank
- The Maritime Bank
- Vladivostok Alfa Bank
- Bank Eurotreid
- Bank Voronezh
- Bashcreditbank
- Enisey's United Bank
- Inter-Svayz Bank

また、ロシアの次の政府機関のコンピュータ システムがサイバー犯罪者に乗っ取られている可能性があります。

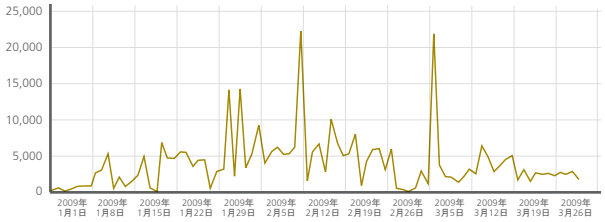
- ナズラン地区税務署
- ロシア国営インターネット ネットワーク
- 地方財政経済研究所
- 原子核科学総合研究所
- ロシア連邦政府付属医療センター
- ロシア連邦年金基金
- ロシア連邦裁判所のパーソナル ネットワーク
- チェチェン無線通信

このデータを見ると、オンライン犯罪者は地域や場所に関係なく、関心のある金融機関や組織に攻撃を実行しています。ロシアではこの種の攻撃が頻繁に発生し、膨大な量のスパムが発生していますが、ウクライナ、ベラルーシ、アルメニア、アゼルバイジャン、グルジア、カザフスタン、キルギスタン、モルドバ、ダジクスタン、トルクメニスタン、ウズベキスタンなどの旧ソ連の諸国でも同様の傾向が見られます。

Web: 悪質と評価される新しいサイトが毎日出現

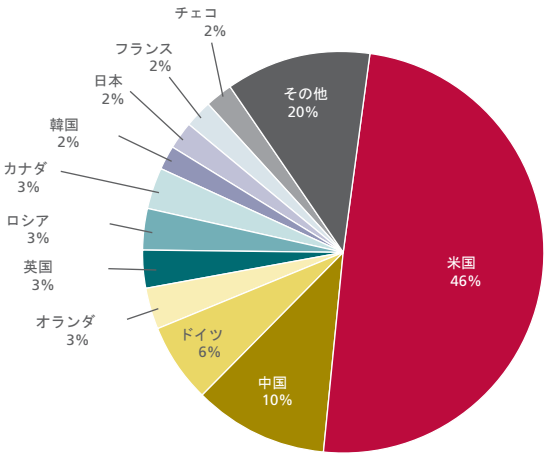
2008年第4四半期に存在していた脅威はこの四半期で危険度を増しています。マスコミで騒がれたためConfickerに関心が集まりましたが、これ以外にも脅威は存在しています。Confickerを除いても、不正な活動は前年よりも若干増えています。前の四半期と比較すると、その増加傾向は明らかです。不正なウイルス対策アプリケーションの存在は、フィッシング詐欺などの詐欺行為の増加とともに大きな問題となっています。

「悪質と評価されるWebサイトの分布」を除き、ここで示すグラフやデータには、Confickerが接続した不正なドメインは含まれていません。Confickerのデータは脅威分析に重要なものですが、このデータを入れてしまうと不正な活動の全体像がぼやけてしまいます。この他にも現在蔓延している脅威は数多く存在します。マルウェアの作成者や詐欺師は現在の経済情勢を悪用してユーザの不安感を煽り、詐欺サイトに誘導しようとします。担保権執行を回避する方法やフィッシング詐欺サイトの被害を逃れる手段を宣伝したり、ポイントカードの提供を餌にする攻撃もあり、警戒心の低いユーザは不正なウイルス対策サイトの餌食となります。ユーザを誘い込む手口も巧妙化しています。Confickerの活動が全くなかったとしても、2008年後半の2四半期と比べて「悪質」または「危険」と評価されたURLの数は劇的に増加しています。



新たに確認された不正なWebサイト

このような悪意のあるURLが存在する場所を見てみると、予測とは異なる結果になりました。



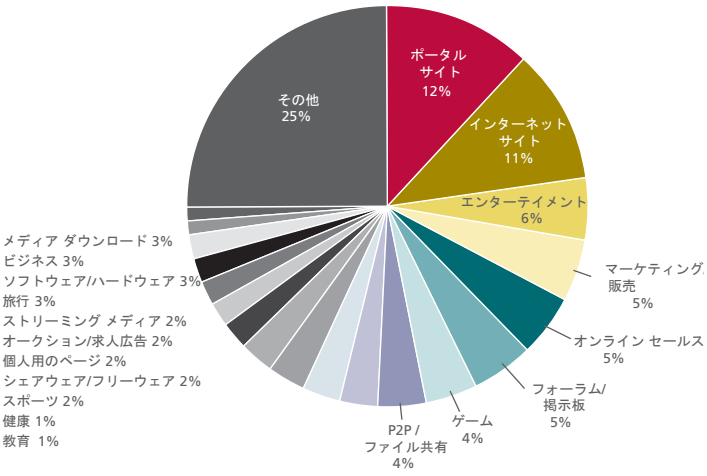
悪質と評価されるWebサイトの分布

これまで不正なWeb活動の多くは米国、中国、ロシアで行われていると見られていました。この突然の変化にはどのような背景があるのでしょうか[1]。これらの国々で悪意のあるURLが少なくなったのではなく、むしろ、他の国々で著しく増えているのです。この増加には、Conficker が接続先として利用したドメインの存在場所が関係しています。実際、Conficker の影響だけでオランダが第4位に入っています。オランダには以前からフィッシング詐欺サイトが数多く存在していましたが、Conficker によってマルウェアや不正なコンテンツに感染したWebサイトが急増しました。しかし、この変化の原因がすべてConficker にある訳ではありません。不正なWebサーバが存在する上位10か国にカナダが入っていますが、これらのサイトには様々なマルウェアやスパイウェアが存在しています。

重要な点は、これらの国々には不正なサイト、スパイウェア/アドウェアが存在するサイト、フィッシング詐欺サイト、スパムサイトなども多いことです。悪意のあるWebサイトが多い上位7か国は、フィッシング詐欺、スパム、マルウェア/スパイウェアが存在するサイトが多く存在する上位10か国にも入っています。

悪質と評価されたサイトも様々です。如何わしいサイトや詐欺目的のサイトだけでなく、合法的なサイトもあります。合法的なビジネスと無関係のアダルトサイトやカジノサイトを閲覧すれば、他のサイトよりも被害を受ける危険度は高くなりますが、攻撃者に狙われないサイトはありません。どのような種類でも、ユーザがアクセスするコンテンツはマルウェアの散布に利用される可能性があります。

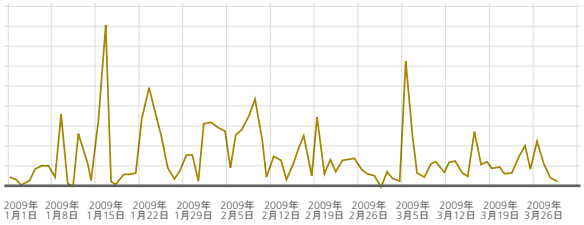
1. 2008年第3四半期の順位は上から順に、米国（41%）、中国（12%）、ロシア（7%）、ドイツとオランダ（5%）、韓国（4%）、香港（3%）、台湾、カナダ、チェコ（2%）、その他（17%）です。



Trusted Sourceで不正なWebサイトとして評価された上位20のカテゴリ

この四半期で、悪質なコンテンツの散布手段としてコンテンツ サーバが利用されるケースが増えています。よく知られていない怪しいプロバイダだけでなく、有名で信頼性の高いプロバイダが運営しているサイトでも同じ傾向が見られます。このような攻撃に利用者の多いブログや検索エンジン最適化（SEO）が悪用される可能性があるため、すべてのコンピュータに完全なセキュリティ対策を施すことが以前にもまして重要になっています。

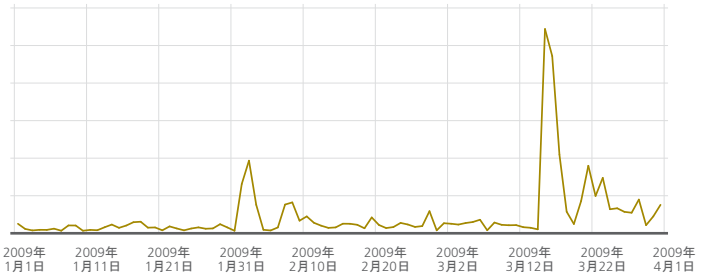
さて、脅威が存在する場所を確認したので、次に脅威の種類について見てみましょう。この四半期は、Conficker以外にもWebを利用する新種のマルウェアやエクスプロイトが数多く出現しています。



マルウェアとPUPを配布する新しいWebサイト

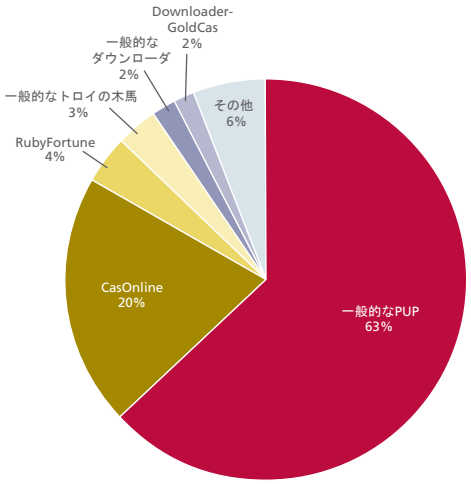
上のグラフは、マルウェアと不審なプログラム（PUP）を散布しているWebサイトの件数を表しています。この件数は、この四半期にMcAfee TrustedSourceネットワークで検出したもので、実際にマルウェアが存在しているホストの数を表しており、このサイトに対するユーザ トラフィックを反映しています。このグラフには、ユーザをマルウェアのサイトに誘導するために利用された正規のサイトは含まれていません。また、標準的なWeb閲覧（学校、仕事場、家庭）で被害を受ける可能性がある新しい脅威を調べるため、事前調査の結果は除いています。

下のグラフは、事前調査でWebサイトからダウンロードした新種のマルウェアの数を表しています。グラフを見ると分かるように、新しいエクスプロイトの大量発生や、事前調査でのマルウェアとPUPの大量検出には傾向があります。



事前調査で確認されたマルウェアとPUPダウンロード (日別)

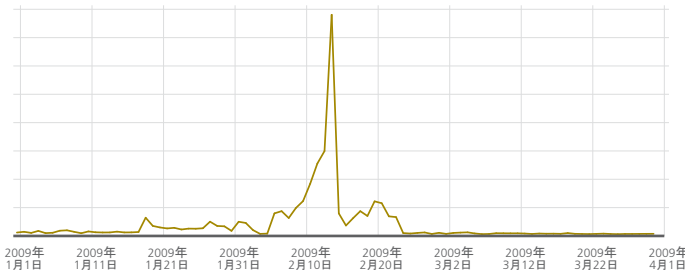
Avert Labsでは事前調査としてWebサイトを定期的に巡回し、不正な行為やコンテンツに関する情報を収集しています。その結果を見ると、1月末から2月の初めにかけて、カジノ関連の新しいマルウェアのダウンロードが大量に発生しています。また、この四半期末には一般的なPUPが大量に確認されています。これは、四半期で検出されたマルウェア ダウンロード タイプの上位を占めています（次のグラフを参照）。この他にも、この3か月間で活動を活発化させているVundoトロイの木馬にも注意が必要です。



マルウェアとPUPダウンロードの種類

現在直面しているWeb脅威の一つにエクスプロイトがあります。この用語は、研究者やユーザの間で様々な意味で使用されています。Avert Labsでは、Webを巡回・監視し、ブラウザ エクスプロイトが存在する新しいページを記録しています。また、ブラウザの新しい脆弱性を定期的に確認しています。最新の状態でないブラウザとそのプラグインは、マルウェアの作成者にとって格好の標的となります。侵入に成功すると、マルウェア作成者はユーザのコンピュータにプログラム コードを潜ませ、コンピュータにアドウェアを感染させたり、キーストロークを盗み出すなど、様々な不正行為を行います。

最新の状態でないブラウザとそのプラグインは、マルウェアの作成者にとって格好の標的となります。

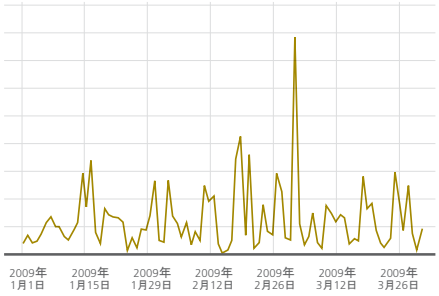


ブラウザ エクスプロイトが存在するWebサイト

アノニマイザを巡る動き

アノニマイザやWeb 2.0インターフェースを介して、コンテンツ サーバを狙ったURLリダイレクト攻撃を行うマルウェア作成者が増えています。この攻撃は、ソースURLでなく埋め込まれたURLとして機能するため、標準的な方法では検出されない場合があります。また、サイトの信頼性を悪用して、マルウェアが散布される可能性もあります。

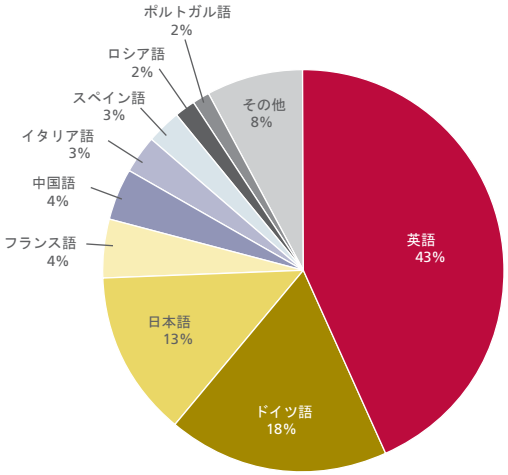
アノニマイザは、オンライン上でユーザの情報を隠すツールです。多くの場合、不正なものではないため、これまではセキュリティ リスクとしては見ていませんでした。しかし、アノニマイザによって仲介者攻撃も可能です。不正なアノニマイザや乗っ取られたアノニマイザが、ユーザとサーバ間でやり取りされるメッセージにコードを挿入する可能性もあります。この攻撃による影響は、ユーザだけでなく、保護されていないホストやネットワークにも及びます。前の四半期と比べると、アノニマイザの活動は全般的に増えています。また、昨年と比較しても若干増えています。



新しいアノニマイザ (日別)

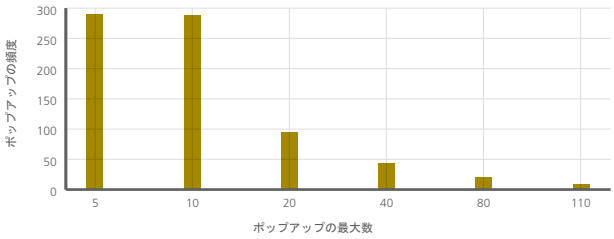
Webの全般的な傾向

Webはグローバルなコミュニティです。専門家同士のコミュニケーションもあれば、ソーシャル ネットワーキングサイトもあります。また、Webページで使用できる言語も増えています。米国で注目を集めているブログへの攻撃が、中国のブログやブラジルのブログを介して行われる可能性もあります。現在の攻撃は広範囲に普及したネットを介して行われます。有名なスポーツ イベントに便乗してマルウェアが散布されたり、トーナメント ブラケットや選手のJPGにマルウェアが埋め込まれることもあります。マルウェア作成者は、言語に関係なく世界中のユーザを攻撃対象にしています。



Webコンテンツで使用されている言語

ポップアップ画面の煩わしさも変わりません。ポップアップ ブロッカーなどのツールが存在しているにも関わらず、いまだに多くのWebサイトでポップアップが使用されています。これまでに最も多い例では、116個のポップアップを使用しているサイトを確認しています。



5個以上のポップアップを使用しているサイト

訪問販売と同じように、Web上のサイトも十分に警戒する必要があります。

マルウェアの散布に悪用される正規のWeb 2.0や合法的なビジネスのURLも増えています。10年以上前は特定のコンテンツにアクセスしなければ問題はありませんでしたが、現在では閲覧する内容に関係なく被害を受ける危険性があります。脆弱なWebサイトは攻撃を受ける可能性があります。管理者は定期的にサーバをスキャンし、悪用されていないかどうかを確認していますが、このようなスキャンは不正なソフトウェアや不正なサイトに関連するサイトやサーバでも実行されています。大量のトラフィックが発生しているWebサイトに脆弱性が存在する場合、攻撃を受けるのは時間の問題です。

Web上での詐欺行為も著しく増加しています。詐欺師はスパム メールやWebを介して世界中のユーザを標的としているため、この傾向は今後も続くことが予測されます。合法的な組織かどうかの判断は非常に困難です。訪問販売と同じように、Web上のサイトも十分に警戒する必要があります。オンライン募金や偽のサービスでクレジットカード番号を入力してしまったら、すべてを失う可能性があることを認識するべきです。

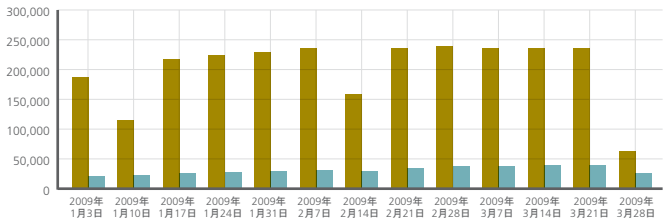
調査結果を見ると経済的によい兆候も見られます。この四半期で不動産関係のサイトが急増し、ユーザが利用できるコンテンツの上位10カテゴリに入りました（スポーツは上位グループから外れました）。

マルウェア: Conficker への過剰反応と AutoRun

この数ヶ月間はConfickerが頻繁に話題になり、あたかも憂慮すべき唯一の脅威のような印象を受けました。しかし、件数を見る限り、そのようなことはありません。Conficker以外にも脅威は存在しているのです。

確かに、Confickerは脅威的なマルウェアであり、大量のホストに感染しています。また、現在もまだ手が加えられています。しかし、このような注目を集めるほど、検出数が多いわけではありません。

この四半期では、AutoRunを利用した厄介なマルウェアを確認しています。このマルウェアは主にUSBドライブやフラッシュメモリを利用して増殖します。数だけを見ると、Confickerよりもはるかに多く確認されています。この2つを比べてみると、次のような結果になります。



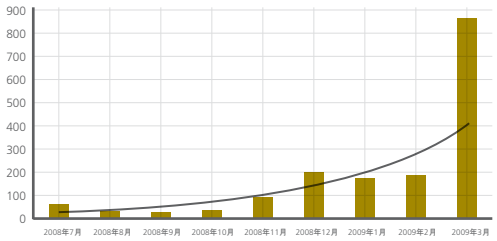
過去30日間で報告されたすべての検出で、AutoRunワームが占める割合は10%未満です。Confickerは1%から始まり、その後12倍になりましたが、その量は後半のピーク時に検出されたAutoRunワームの15%未満です。

予測とその後

今年の初め、McAfee Avert Labsは『2009年の脅威予測』[2]を公開しました。いくつかの予測はこの四半期に現実のものとなりました。

身近な人物から受ける被害

この10年間、友人からのメッセージでウイルスに感染する事例は激減しました。しかし、Web 2.0の出現で、この古典的な攻撃方法が息を吹き返しています。この四半期では、Facebookの友人を介して数千のユーザがKoobfaceの亜種に感染しました。この事件では、ウイルスを含むメッセージにはワームを散布するWebサイトへのリンクが含まれ、ウイルスに感染するとすぐに別の友人にウイルスを含むメッセージが送信されました。ソーシャル ネットワークは、ソーシャル エンジニアリングを行う攻撃者にとって効果的な媒体になっています。

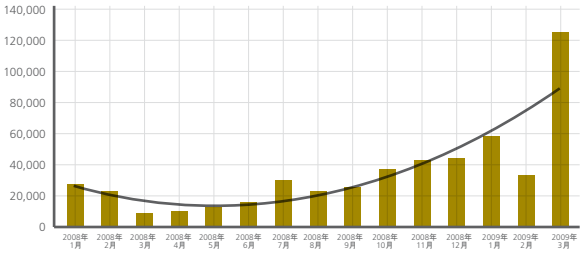


検出されたKoobfaceバイナリの件数

2. McAfee Avert Labs Threat Center。http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report_ja.pdf

世界中に存在する不正なWeb

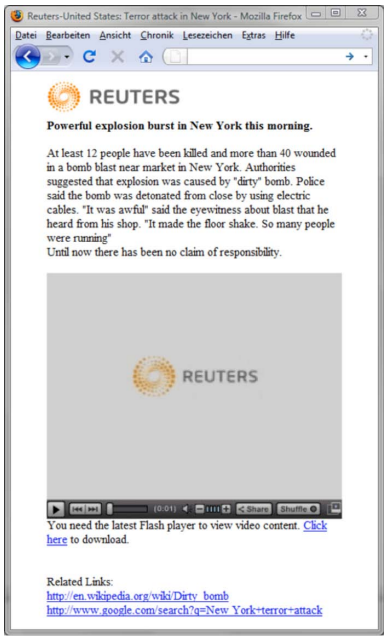
今年の2月、Facebookが攻撃を受け、多くのユーザがFacebook プラットフォームを使用した不正なアプリケーションをインストールしてしまいました。この事件はメディアでも取り上げられ、McAfee Avert LabsはGoogleの上位SEOを行う大規模な検索エンジンを発見しました。攻撃者は、有名なサイトから著作権で保護された資料を盗み出すだけでなく、Democrats.orgなどの有名サイトを悪用し、Googleランキングを上げていました。攻撃者の狙いは、不正なウイルス対策ソフトウェアをインストールさせるために検索結果を最適化することでした。これは、検索結果の操作と不正なセキュリティ ソフトウェアのインストールに、不正なFacebookアプリケーションが利用された事例です。



検出された不正なウイルス対策バイナリ

多言語対応になった脅威

攻撃者は、より身近で関連性の高い内容にすれば、リンクのクリック、ユーザ名とパスワードの入力、アプリケーションのインストールなどを行う確率が高いことを知っています。地球の裏側で起きた事件よりも、身近で起きたイベントの方がユーザの関心は集めやすいものです。2月と3月にWaledacウイルスを使ったサイバー詐欺師はこの心理を利用しています。ユーザの住んでいる地域用にWebをカスタマイズし、信憑性を増したため、警戒心の低いユーザは簡単に騙されてしまいました。ユーザが「地域のニュース」を読んでいる隙に、ドライブバイ エクスプロイト コードがウイルスをインストールしました。



McAfee Avert Labsのブログ

Googleと検索エンジンの悪用

Googleは多くのユーザが様々な用途で使用しています。たとえば、最新の求人情報の検索、人材発掘、魅力的な価格で商品を販売している店の検索などに利用されています。マルウェア作成者やサイバー犯罪者にとって、Googleはマルウェアの散布や犯罪行為の実行に非常に効果的なツールです。現在の検索エンジンの利用状況を見れば、マルウェア作成者が手段として利用しようと考えるのも当然のことです。McAfee Avertのブログにもこのトピックに関する記事が掲載されています。

- http://www.avertlabs.com/research/blog/index.php/2009/03/15/democratsorg-cans-the-spam/
- http://www.avertlabs.com/research/blog/index.php/2009/03/10/democratsorg-blog-spam-contributes-to-google-search-poisoning/
- http://www.avertlabs.com/research/blog/index.php/2009/02/27/google-bucking-the-trend/
- http://www.avertlabs.com/research/blog/index.php/2009/02/25/google-trends-abused-to-serve-malware/
- http://www.avertlabs.com/research/blog/index.php/2009/01/07/google-code-project-abused-by-spammers/
- http://www.avertlabs.com/research/blog/index.php/2009/01/17/do-not-worry-obama-di-not-refuse-to-be-a-president/

インデックスと人気のあるキーワードで簡単に金銭を得ることができるため、このような悪用は今後も続くでしょう。

厳しい経済情勢と先行きに対する不透明感

世界的な不況は多くの人々に影響を与えています。安全性とテロの問題も悩ましい問題です。マルウェア作成者やサイバー犯罪者は、このような不安感につけ込み、利益を得ようとしています。2009年の脅威予測でも述べたように、この経済状況は様々な面で影響を及ぼしています。サイバー犯罪者はソーシャルエンジニアリングを行う際にこのような恐怖心を悪用しています。

- http://www.avertlabs.com/research/blog/index.php/2009/03/16/breaking-news-waledac-terror-attack-in-a-city-near-you/
- http://www.avertlabs.com/research/blog/index.php/2009/02/23/malware-riding-on-the-tides-of-the-economic-crisis/
- http://www.avertlabs.com/research/blog/index.php/2009/02/06/cybercrime-online-threats-and-the-recession/
- http://www.avertlabs.com/research/blog/index.php/2009/01/05/one-hacker-may-conceal-another/
- http://www.avertlabs.com/research/blog/index.php/2009/01/20/fake-antivirus-and-a-real-threat/
- http://www.avertlabs.com/research/blog/index.php/2009/01/29/hoax-or-not-treat-it-the-same/

オンライン詐欺やフィッシング詐欺を行うにはよい状況になっています。犯罪者や攻撃者は同じニュース記事を見て騙しの手口を考えています。用心深く注意していないと、被害を受けることになります。

McAfee Avert Labsについて

McAfee Avert Labsは、世界各地に展開するMcAfee, Inc.の研究機関です。マルウェアやPUP、ホスト侵入、ネットワーク侵入、モ バイル マルウェア、脆弱性の調査に特化した研究チームにより、セキュリティを幅広く多面的に研究しています。この広大なビジョンにより、セキュリティ技術の継続的な向上とユーザ保護を実現しています。

McAfee, Inc.について

McAfee, Inc.は、米国カリフォルニア州サンタクララに本社を置く、セキュリティ技術の業界最先端の企業で、世界中のシステムおよびネットワークをセキュアにする画期的で優れたソリューションを提供し、ユーザに安心安全なWeb利用を提供しています。個人ユーザをはじめ、企業、官公庁・自治体、ISPなど様々なユーザは、McAfeeの卓越したセキュリティ ソリューションを通じて、法令順守、データ保護を実現し、脆弱 性を特定して破壊活動を阻止でき、またセキュリティ レベルを絶えず監視することができます。http://www.mcafee.com/japan

マカフィー株式会社
〒150-0043 東京都渋谷区道玄坂1-12-1
渋谷マークシティウエスト20階
03-5428-1100
www.mcafee.com/japan/

5395rpt_avert_quarterly-threat_0409