レポート

McAfee 脅威レポート：2013 年第 1 四半期

McAfee Labs

目次

序論

McAfee Labs の研究者は、2013 年第 1 四半期の脅威を分析し、従来の傾向がいくつかあることを確認しました。モバイルマルウェアは着実に増加しており、Facebook の脅威である Koobface、オートランマルウェア、マスターブートレコード（MBR）を攻撃するステルスマルウェアなど、一般的なマルウェアが急増しています。世界規模で展開されるスパムがこの四半期の間に倍増しており、1 年以上減少が続いていましたが、勢いを取り戻しています。

対象を絞った攻撃は、金融部門に集中していましたが、工夫が凝らされています。トロイの木馬「Citadel」を分析したところ、サイバー犯罪者は、特定の国の標的を絞り込んだ被害者から様々な個人情報を盗めるように、この従来の銀行口座に対する脅威を変化させていることが判明しました。将来、攻撃者がこうしたデータを利用する可能性があります。

モバイルマルウェアのサンプル数は、ほぼ Android OS のみですが、急増し続けています。全モバイルマルウェアの約 30% がこの四半期に出現しています。悪意のあるスパイウェアや対象を絞った攻撃が、モバイル電話に関する最新の攻撃として目立っています。

クライアント、サーバー、ネットワーク、モバイルに影響を及ぼすとして、マカフィーが監視しているマルウェアのサンプル数は、合計 1 億 2,800 万以上にのぼります。この数は、長期に渡って着実に増加の一途を辿っており、最近の 2 四半期連続で急増しました。Koobface は、オートラン、ランサムウェア、MBR の脅威とともにこの四半期の主要な脅威でした。サイバー犯罪者は、ランサムウェアを利用し、システムを人質に取ってコンピューターのロックを解除するための費用を要求します。しかし、被害者が支払ったとしても、彼らはマシンを解放してくれるでしょうか。保証はない上に、匿名の支払システムによって、彼らの行動を追跡することは基本的に不可能です。MBR の脅威は、被害者に気付かれることなく長期間システムに潜伏し続けて、他のフォームのマルウェアをダウンロードする可能性があります。

McAfee Global Threat Intelligence™ ネットワークは、米国内の IP アドレスが再び悪意のあるネットワーク活動の大半のソースでありターゲットとなっていることを明らかにしています。埋め込まれた iframe や悪意のある Java コードといったブラウザーベースの攻撃は、最も一般的な手口です。

Web の脅威を分析したところ、新たに出現した疑わしい URL の大半は米国内に存在しており、この四半期に 12% 増加したことがわかりました。フィッシング詐欺の新たな攻撃対象は、主にオンラインオークションや金融関係でした。この四半期の最大の話題のひとつは、1 年以上減少が続いていたスパムが増加に転じたことです。3 月には 1 兆 9,000 万件ものメッセージに達しました。この数は新記録ではありませんが、2012 年 12 月の約 2 倍の量です。

サイバー犯罪者は、経験の少ない詐欺師も仲間に加わり被害者につけ込めるようにする、クライムウェアツールを開発および販売し続けています。EU に新たに設立された欧州サイバー犯罪センター（European Cybercrime Centre）は、オンライン犯罪者を逮捕して起訴できるように法執行機関を支援しています。ハクティビストは、仲間を支援するための合法的な手段として DoS 攻撃を使用する危険性が高まりました。また、マカフィーは、この四半期の間のサイバー軍の活動も調査しています。一般的に、こうしたグループは、個人の自由が制限されている国々で出現し、政府のために行動すると主張しています。

トロイの木馬「Citadel」

この数か月のトップニュースは、「銀行取引」を対象とするマルウェア Zeus とその亜種に関することでした。亜種のひとつであるトロイの木馬「Citadel」が、オープンなクライムウェア市場から撤退したというニュースが、2012 年後半に注目を集めました。しかし、この撤退は、Citadel が深刻な世界的脅威でなくなることを意味するとは限りません。McAfee Labs のレポート『Inside the World of the Citadel Trojan』では、Citadel のオリジナルの開発者や別の人物が、Citadel の機能と脅威プロフィールを大幅に拡張した新しい亜種を開発中であることを明らかにしています [1]。2012 年下半期およびこの四半期に見られた主な傾向は以下の通りです。

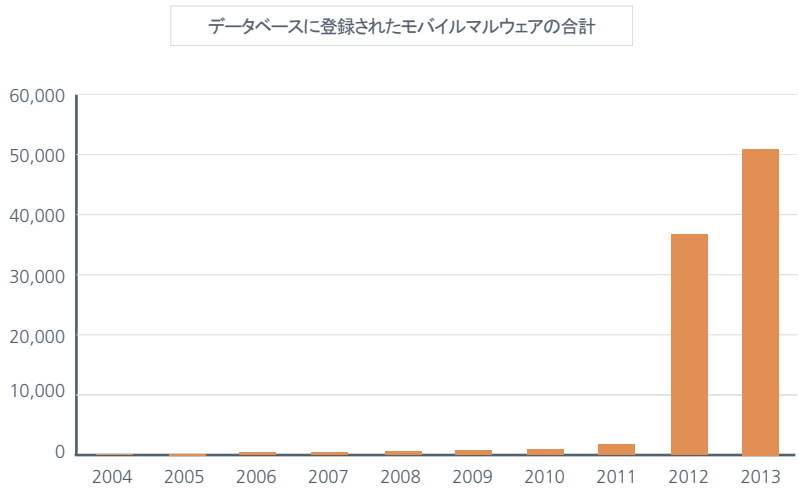
- 主にヨーロッパの公的機関と民間企業に対象を絞った攻撃
- 情報や貨幣の盗難に用いられる機能の強化
- 以前の Zeus マルウェアファミリーの攻撃対象が数万人単位であったのに比べて、攻撃対象を数百人に絞り込んでいる
- 社内アプリケーション、銀行システムアプリケーション、製造システムなどから認証情報を取得して、後からこうしたアプリケーションに対する攻撃に利用
- Citadel ベースの攻撃の主要な加害者として、「Poetry Group」の登場

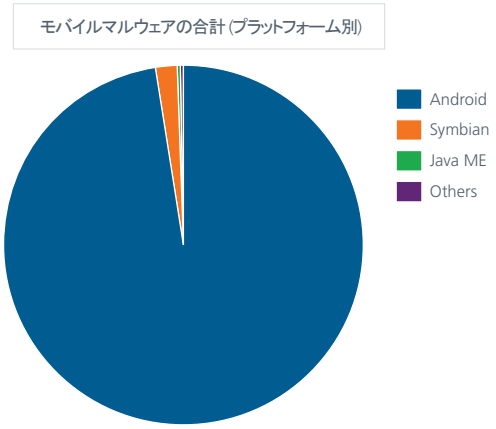
Citadel は、金融サービス業界だけではなく、他の業界でも新たな脅威であるとみなされています。Citadel を利用すれば、サイバー犯罪者は高度なリモート接続を行って、攻撃対象を動的に決定することが可能となります。Citadel はオープン市場から撤退していますが、McAfee Labs は、2013 年中に配布される後継の亜種の監視を引き続き行います。また、多くのサイバー犯罪者が、Citadel が金融詐欺よりもはるかにうまくいく可能性があると認識しているため、攻撃対象が拡がると予想しています。最近の活発な活動から、Citadel を用いた世界中の企業や政府組織への攻撃が続いていくことが予想されます。

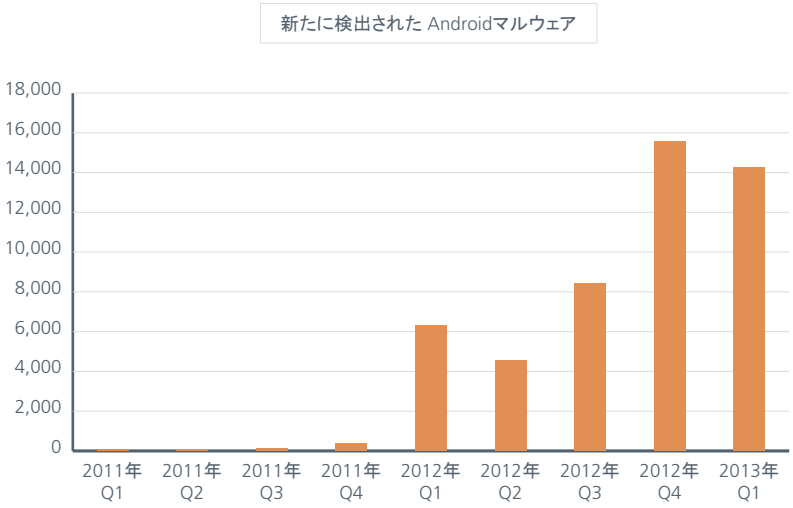
モバイルの脅威

この四半期の終わりに、モバイルマルウェア「zoo」の合計サンプル数は、50,926 に達しました。これは、2013 年に出現しているマルウェアの 28% に相当します。2011 年に収集した合計サンプル数はわずか 792 でした。モバイルマルウェアの拡大は、この四半期に若干衰えましたが、注目を集める記録的な年として、今年もその勢いを増し続けています。

バイナリが最大で 100 万件に達するとの予測により、より多くの新たなモバイルマルウェア数を挙げる研究者もいます。ただし、こうした数には、APK ファイルを再パッケージした悪意のある Android アプリやファミリーにバンドルされたファイルをすべて含んでいる可能性があります。McAfee Labs では、固有のマルウェアファミリーや亜種のみをカウントしているので、一般的な広告ライブラリーや重複する悪意のあるファイルなどは除外しています。







宣伝目的のスパイウェアやアドウェアの脅威は減少していますが、悪意のあるスパイウェアや標的を絞った攻撃はより顕著になっています。最新の脅威に共通するのは、ボットネットを組み合わせた悪意のあるスパイウェアです。

Android/Ssucl.A は、システムのクリーンアップユーティリティを装うトロイの木馬であり、実際は、リモートコントロールサーバーからの指示を受けるボットネットクライアントです。このトロイの木馬は、ユーザーや SMS の情報を盗むだけではなく、攻撃者がこの情報を利用して Dropbox や Google のログイン情報に対してフィッシング攻撃を開始することができます。これだけにとどまらず、Ssucl.A は、autorun.inf 攻撃を用いて PC へのダウンロードおよび感染を試みます。

チベット人とウイグル人の活動家が、この四半期にフィッシング攻撃や Android マルウェアの攻撃対象となりました。Android/Chuli.A は、標的となる活動家に関わりのあるイベントやカンファレンスの案内を装います。このマルウェアが実行されると、攻撃者が感染ユーザーを特定できるような重要な情報が収集されます。位置情報と SMS 情報を受信すると、攻撃者は、各感染デバイスにさらにコマンドを送信することが可能になります。

対象を絞ったトロイの木馬の地域別の蔓延状況

昨年末までは、モバイル攻撃の大部分はロシアと中国で検出されました。しかし、この四半期に、犯罪者が他の地域にも活動を広げていることが確認されました。

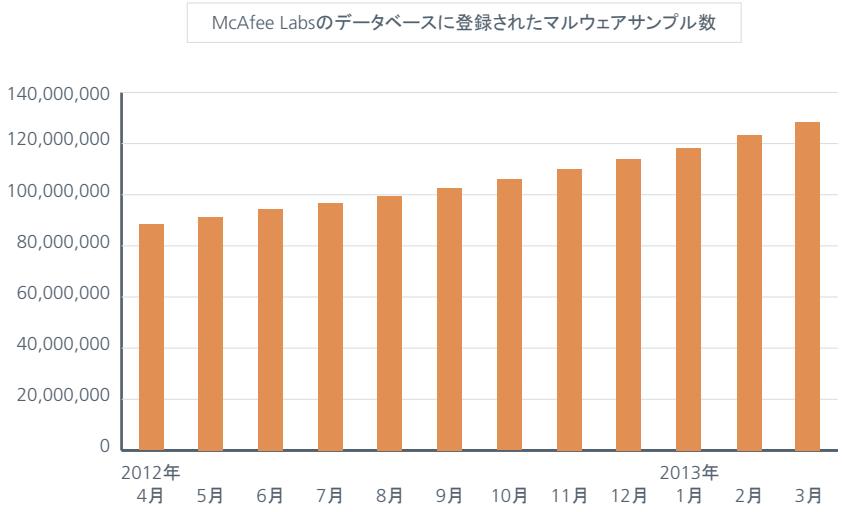
韓国は、人気のあるコーヒーショップチェーンのクーポンアプリを装った Android/Smsilence.A による攻撃の被害を受けました。実行時に、このマルウェアは、サーバーエラーが発生したというメッセージをポップアップで表示しますが、実際は、ユーザーの電話番号を攻撃者に送信していました。このマルウェアは、受信した SMS メッセージを転送して、他の受信テキストの削除を可能にします。Smsilence.A は、韓国でのみ有効となるように電話の国番号をチェックしています。

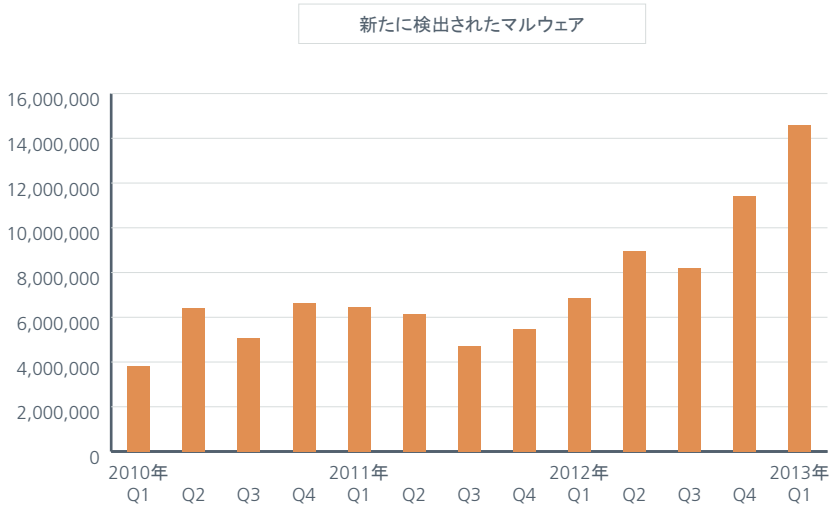
インドのユーザーが、Android/Fakejoboffer.A を利用した前金詐欺の被害を受けました。前金詐欺は、懸賞に当選した、または価値の高い何かを受け取れると被害者に思わせます。この賞品を受け取るために、少額の手数料の支払いが求められます。こうした賞金や賞品は実在しないので、被害者はこの前金を失ってしまいます。被害者が「手数料」を支払うと、Fakejoboffer.A は、仕事の面接の文書の画面を表示し、多数の候補者の中から仕事の面接に選ばれたので、面接を実施する事務所に向かうための旅費を支払う必要があると通知します。被害者は、（存在しない）面接に参加すると旅費の払い戻しが受けられると知らされます。

イタリア、タイ、オーストラリアのオンラインバンキングユーザーも、モバイル犯罪者の攻撃対象になりました。Android/Fksite.A は、バンキングソフトウェアを保護すると主張していますが、実際はモバイル取引承認番号（mTAN）を攻撃者に転送します。mTAN は、有効期限が限られており、銀行口座へのログイン時に無効になります。mTAN を捕捉した攻撃者は、口座からお金を盗むためにこの番号がアクティブであることを確認する必要がありました。Android/Fksite.A は、転送する前にこの番号が「有効」であるかどうかチェックすることで、新鮮な mTAN を入手できるようにします。

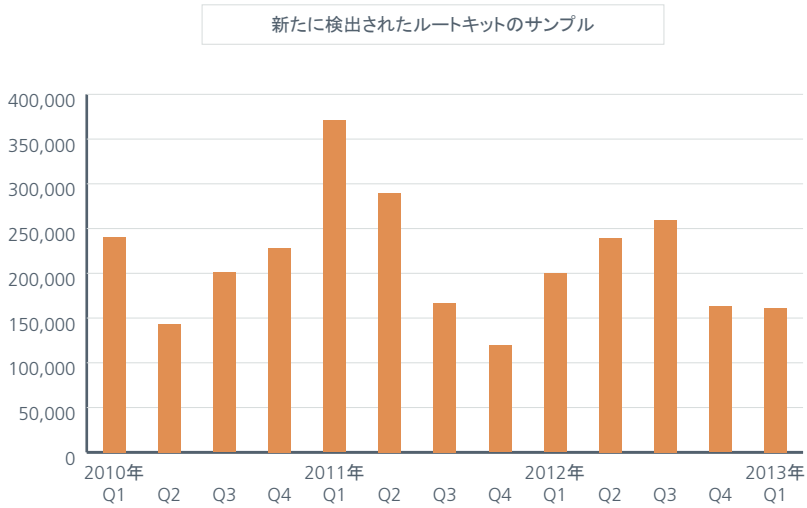
全般的なマルウェアの脅威

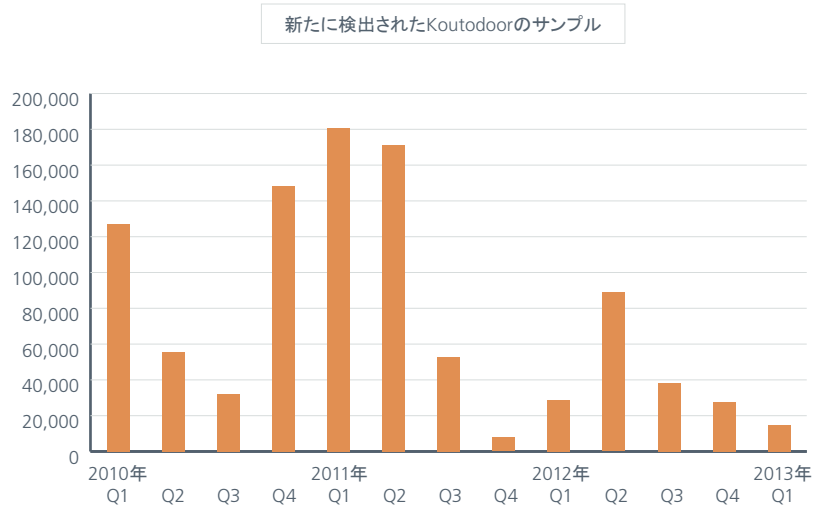
マルウェアは、着実な増加が収まるような兆候が全く見られず、この 2 四半期連続で急増しています。この四半期の終わりには、マルウェア「zoo」の中のサンプル数は 1 億 2,800 万以上にのぼりました。

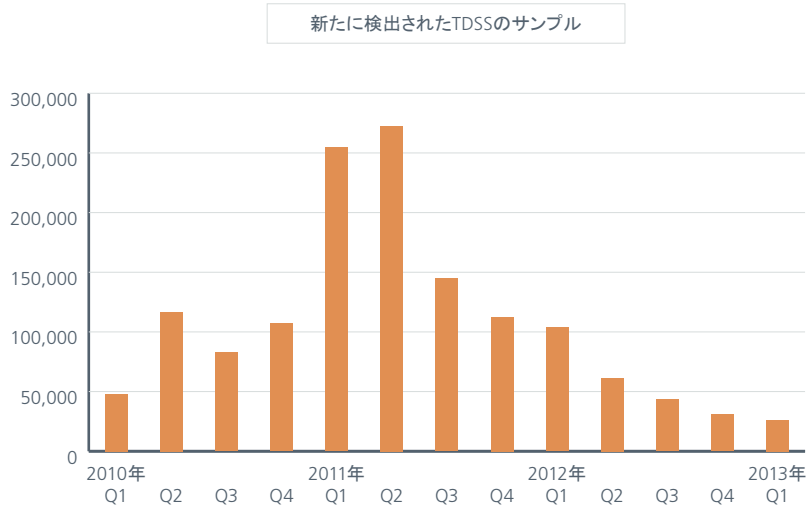


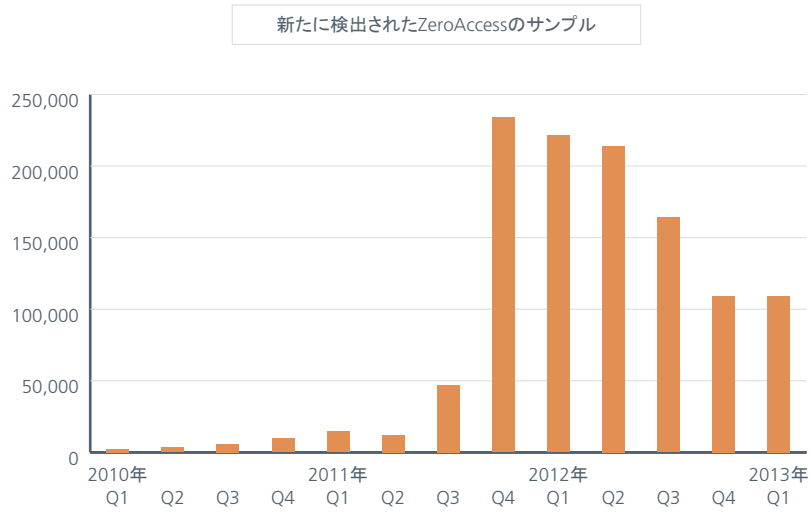


ルートキットやステルスマルウェアは、これまでで最も悪質なマルウェアの種類のひとつです。これらは、検出を回避して長期に渡ってシステムに常駐するように設計されています。この 1 年間の大部分で増加傾向にありましたが、新たなルートキットサンプルの増加は、この 2 四半期連続で横ばい状態になっています。このレポートで取り上げた 3 種類のルートキットすべてにこうした傾向が当てはまります。



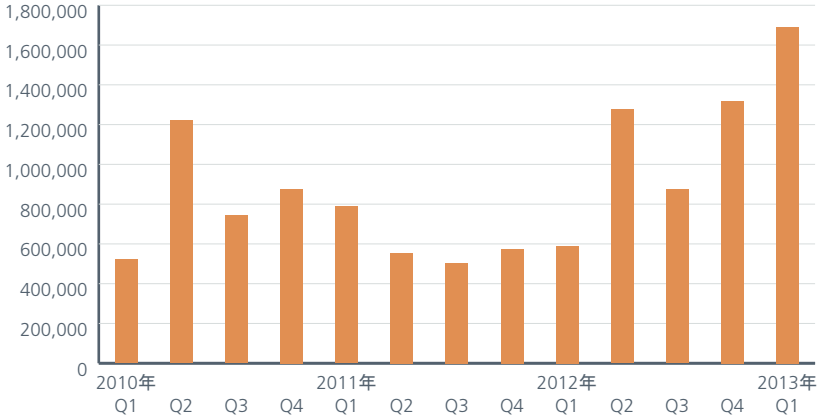




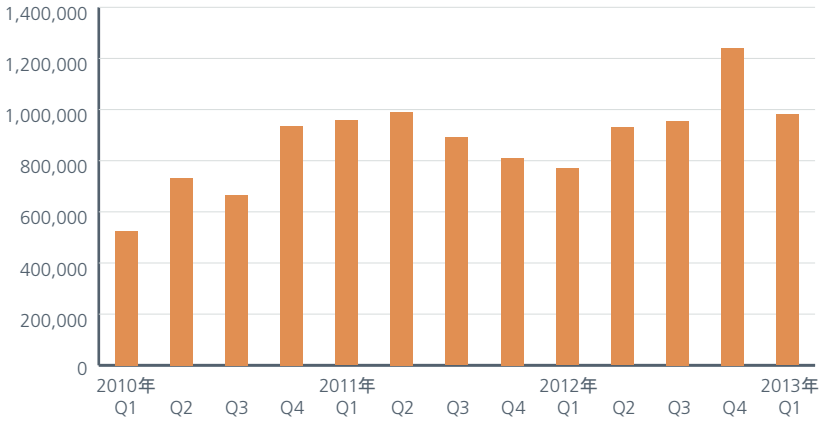


多くの場合、USB ドライブに潜んでおり、攻撃者がシステムをコントロールすることを可能にするオートランマルウェアは、この 2 四半期連続で急増しており、新たな脅威が約 170 万に達して最高記録を更新しました。ランサムウェアのフォームとして動作可能であり、コンピューターのウイルスを「駆除」するといって被害者からお金を巻き上げる偽のマルウェア対策製品の数は、昨年末の記録的な水準から減少しましたが、全体の数は高い状態です。Facebook ユーザーを対象とした Koobface によって、この四半期は前の四半期の約 3 倍ものサンプル数が検出されました。これは、もうひとつの記録的な数字であり、2009 年の第 4 四半期に達したこれまでの記録の 2 倍の量となりました。被害者の銀行アカウントを乗っ取ろうとするパスワード盗難型のトロイの木馬の増加は横ばい状態ですが、最高記録を更新しています。

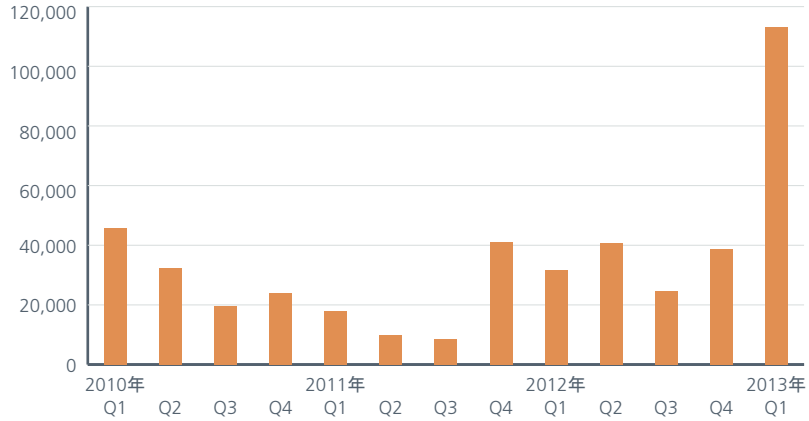
新たに検出されたAutoRunのサンプル

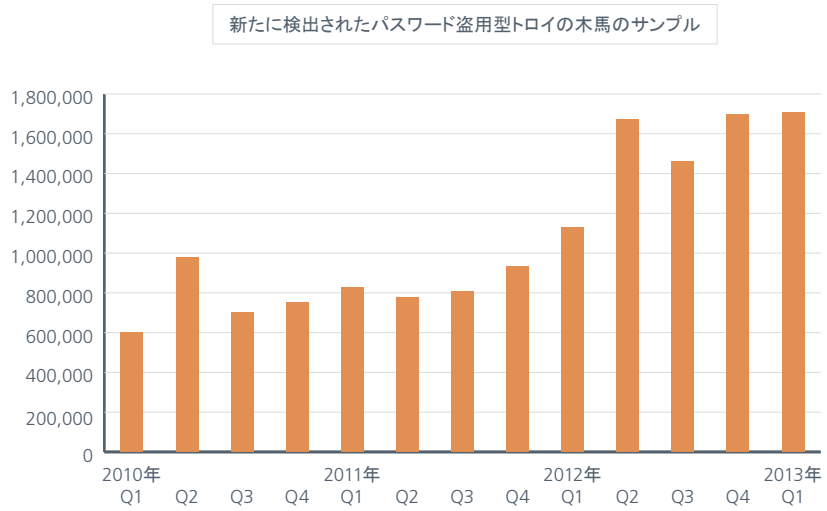


新たに検出された偽のAVのサンプル

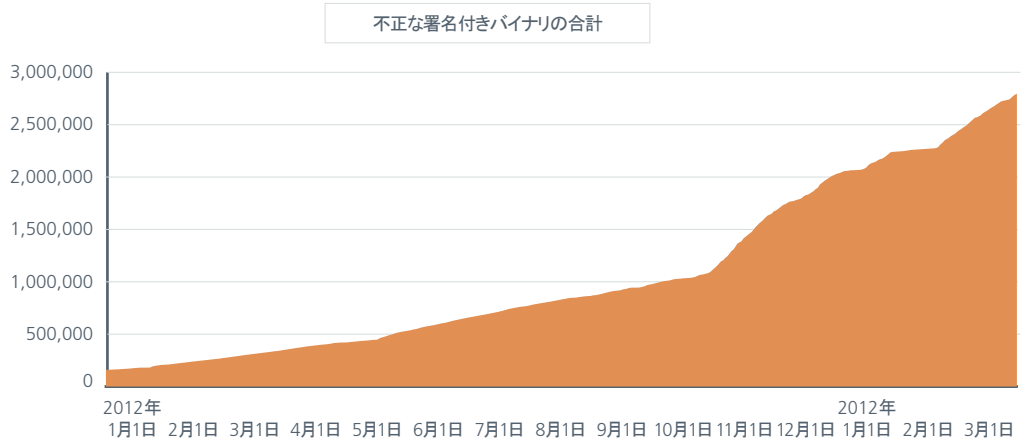


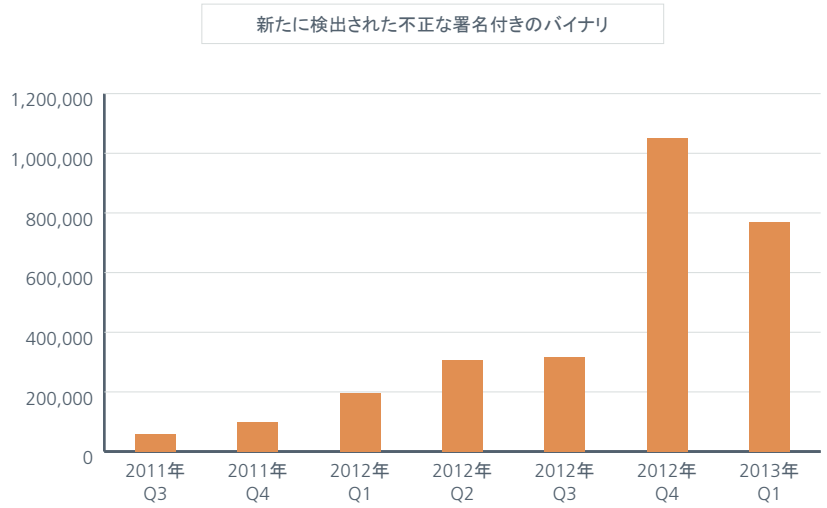
新たに検出されたKoobfaceのサンプル



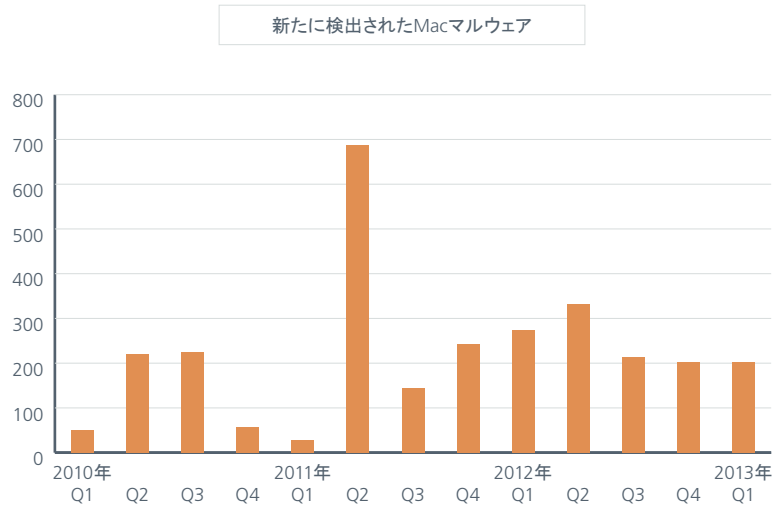


署名付きマルウェアは、第 4 四半期の急増から大幅に減少しましたが、依然としてこれまでの記録のなかで 2 番目に高い数字です。

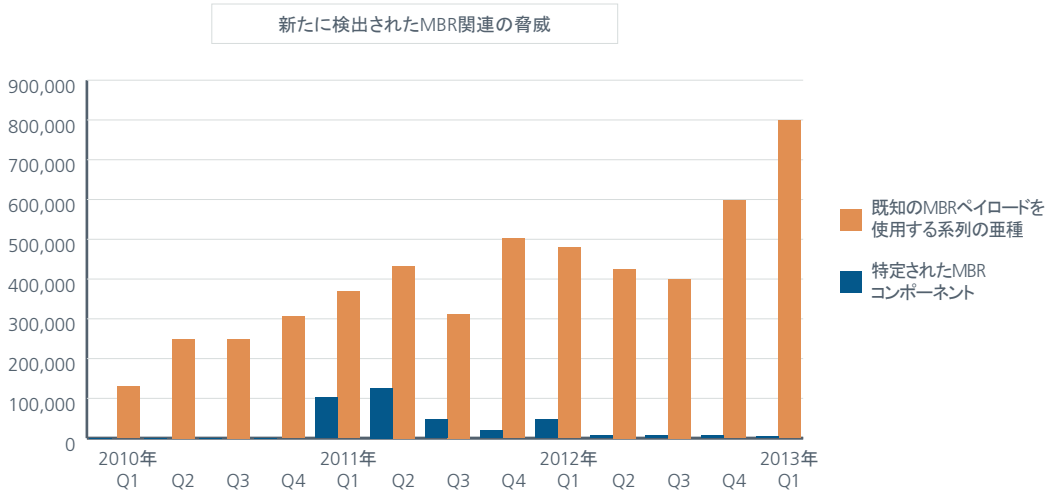




Mac を攻撃する新たなマルウェアは、この 3 四半期連続で横ばい状態です。PC の脅威に比べて数は少ないですが、Mac ユーザーも対策が必要です。



マルウェアのなかには、重要なスタートアップ操作を実行する領域であるコンピューターのマスターブートレコード（MBR）を標的にする種類があります。MBR のセキュリティが侵害されると、攻撃者はコンピューターをコントロールして潜伏し、奥深くまで侵入することが可能になります。mebroot、Tidserv、Cidox、Shamoon などの攻撃は、数が急増しており、この 2 四半期連続で最高記録を更新しています。

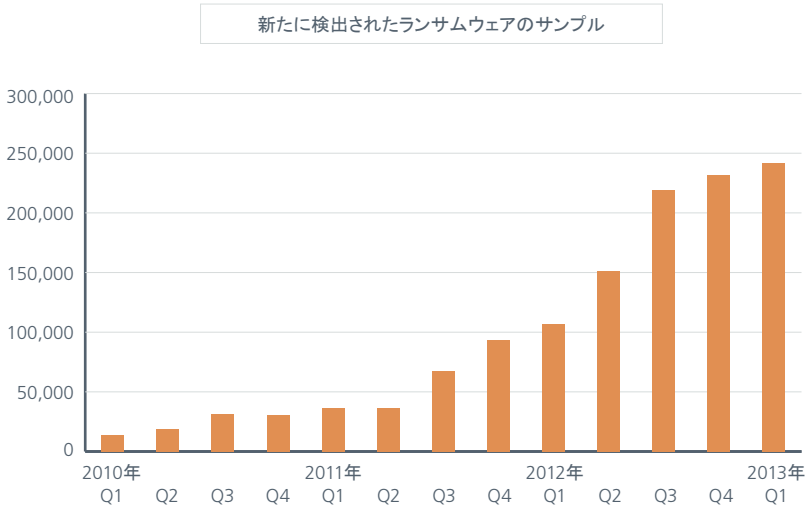


ランサムウェア

ランサムウェアは、ここ数四半期の間に深刻な問題となっており、状況は悪化し続けています。この四半期で、新たな固有のサンプル数は 25 万に迫っていますが、最も懸念される点は、報告された感染数です。検出データを共有できるのはマカフィーのコンシューマー製品のみなので、公表される数字は部分的なものになります（マカフィーはこの情報を公開しています [2]）。また、この傾向は、世界中の法執行機関や連邦政府機関からの警告も反映されています。

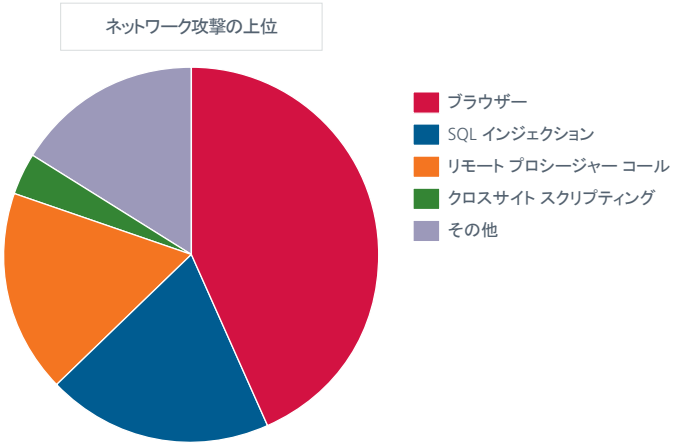
ランサムウェアが普及した理由のひとつは、様々な匿名支払サービスを利用できるため、犯罪者が利益を獲得できる非常に効果的な手段であることです。こうした資金を収集する方法は、偽のソフトウェアのためにクレジットカード注文の処理が必要となるような、偽のウイルス対策製品を利用する方法よりも優れています。もうひとつの理由としては、アンダーグラウンドのエコシステムがすでに確立しており、Citadel のような、他のマルウェアによって感染したコンピューターへのペイ・パー・インストールといったサービスを利用することが可能で、使い勝手の良い犯罪パックをアンダーグラウンド市場で入手できるからです。犯罪者は、Lyposit のようなキットを購入できます。これは、（コンピューターの地域設定に基づいて）現地の法執行機関を装うマルウェアで、被害者に特定の国の支払いシステムを使用するように指示を出します。これにより、固定額ではなく利益を配分することができます。

こうしたメリットがあるため、ランサムウェアの問題は当分なくなることはないでしょう。ユーザーは常に予防措置を取って重要なデータのバックアップを作成する必要があります。

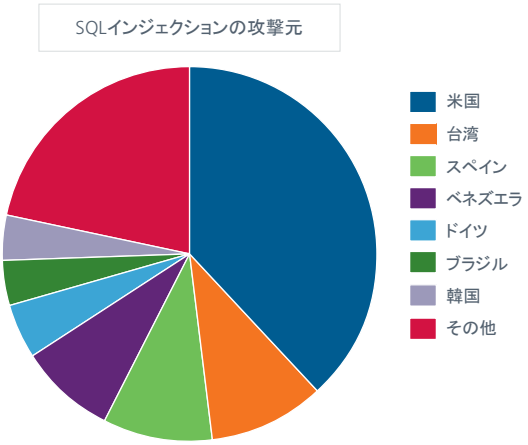


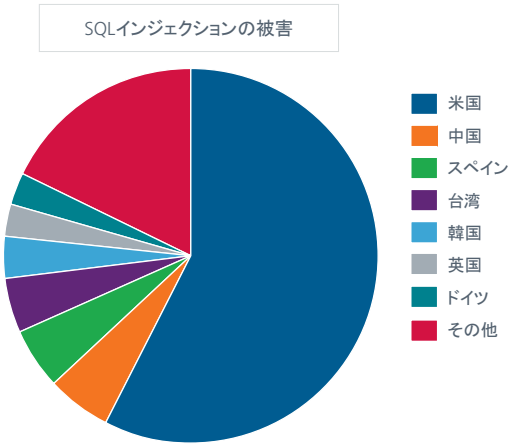
ネットワークの脅威

McAfee Global Threat Intelligence™ ネットワークによれば、例によって、米国は悪意のあるインターネット活動の大半のソースでありターゲットとなっています。ブラウザーベースの脅威がすべてのネットワーク攻撃の中で一番多く、前の四半期から増加しています。SQL インジェクションとリモートプロシージャコールは、それぞれ、2 番目と 3 番目に多い脅威です。

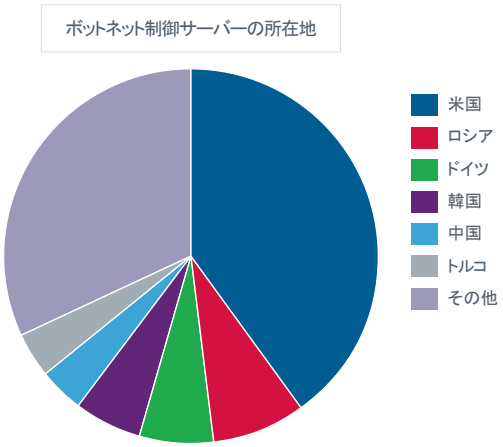


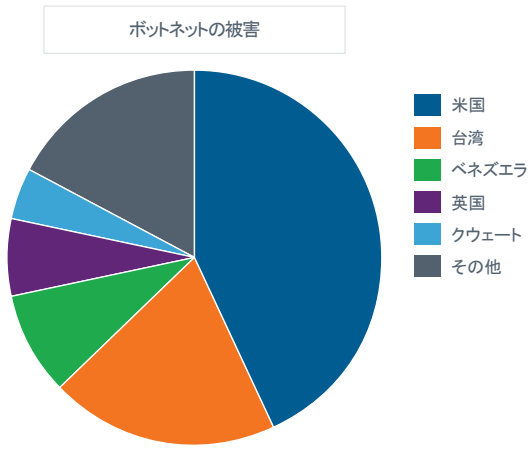
合法的な Web サイトを悪用する SQL インジェクション攻撃の加害者における米国の割合は、この四半期で小さくなりました。台湾とスペインは、前の四半期に第 2 位であったベネズエラを上回っています。これらの攻撃の被害者の大半は、米国在住です。



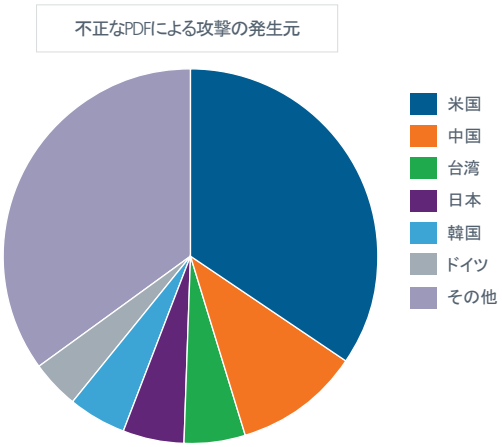


ボットネットの監視調査では、米国が第 1 位であり、その割合は前の四半期からほとんど変わりません。コントロールサーバーに関しては、ロシアとドイツが再び後に続いています。被害者に関しては、台湾がこの四半期で第 2 位に順位を上げており、ベネズエラは第 3 位となりました。





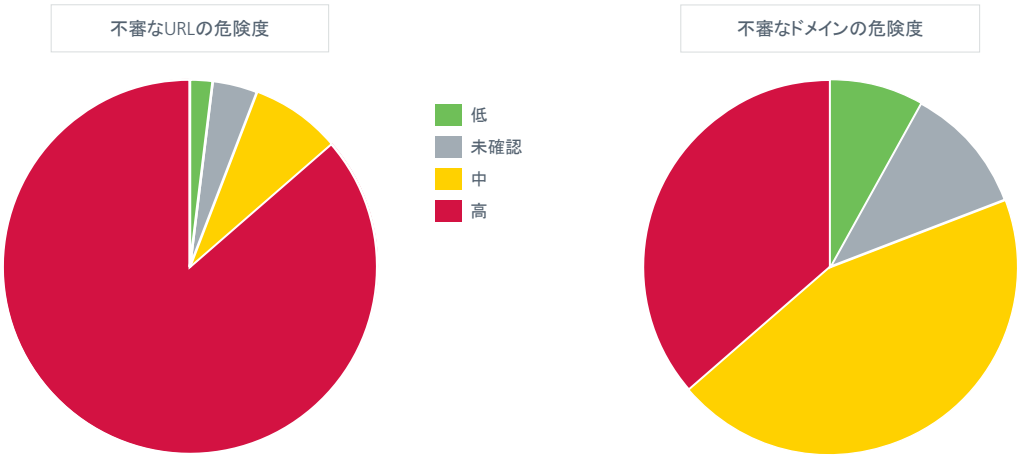
米国が、最大の割合（35%）を再び占めており、この四半期で最も多くの PDF エクスプロイトをホスティングしています。第 1 位だった韓国は第 5 位となり、11% を占めている中国が第 2 位となっています。



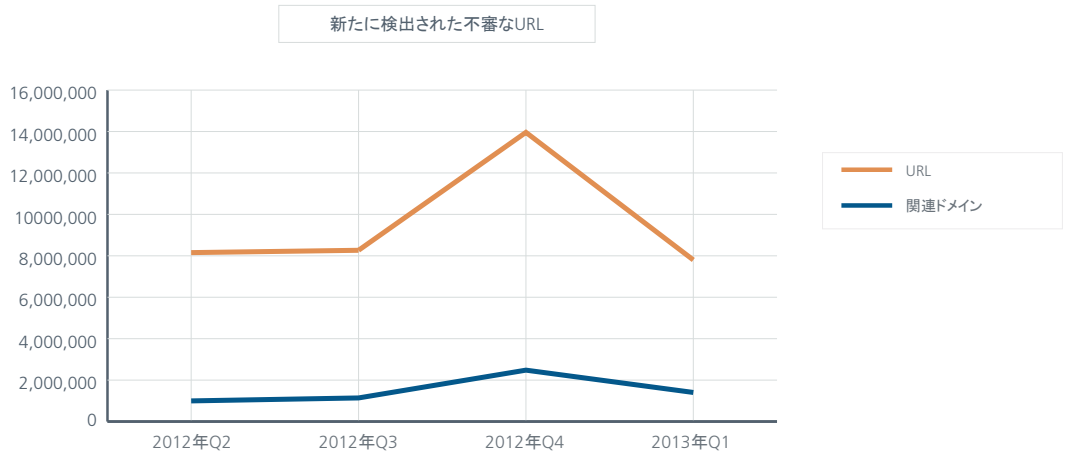
Web の脅威

Web サイトは、様々な理由によって不正や悪質であるという評価を受ける可能性があります。この評価は、ドメイン全体と任意の数のサブドメインに加えて、単独の IP アドレスまたは特別な URL に基づいて行われます。悪質であるとの評価は、マルウェア、潜在的に不要なプログラム、フィッシング詐欺サイトのホスティングの影響を受けます。多くの場合、マカフィーは疑わしいコードと機能の組み合わせに注目します。これらは、マカフィーが実施する Web サイトの評価に影響するごくわずかの要因にすぎません。

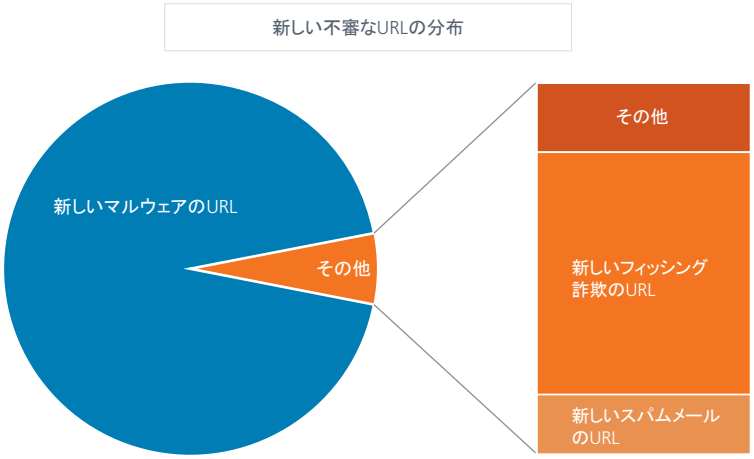
3 月末に、McAfee Labs が集計した疑わしい URL の合計数は 6,430 万を上回り、第 4 四半期から 12% 増加しています。これらの URL は 2,770 万ものドメイン名を参照しており、以前の期間から 6% 上昇しています。マカフィーのデータベースでは、リスク評価に従ってこれらの URL とドメインを分類しています。



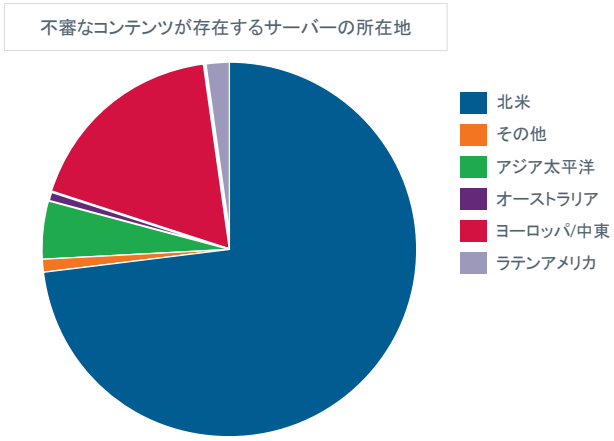
この四半期に、約 47 万のドメインに関して、1 か月の平均で 260 万の新たな疑わしい URL を検出しました。これらの数字は、2012 年の第 2 および第 3 四半期に記録した水準に戻っています。



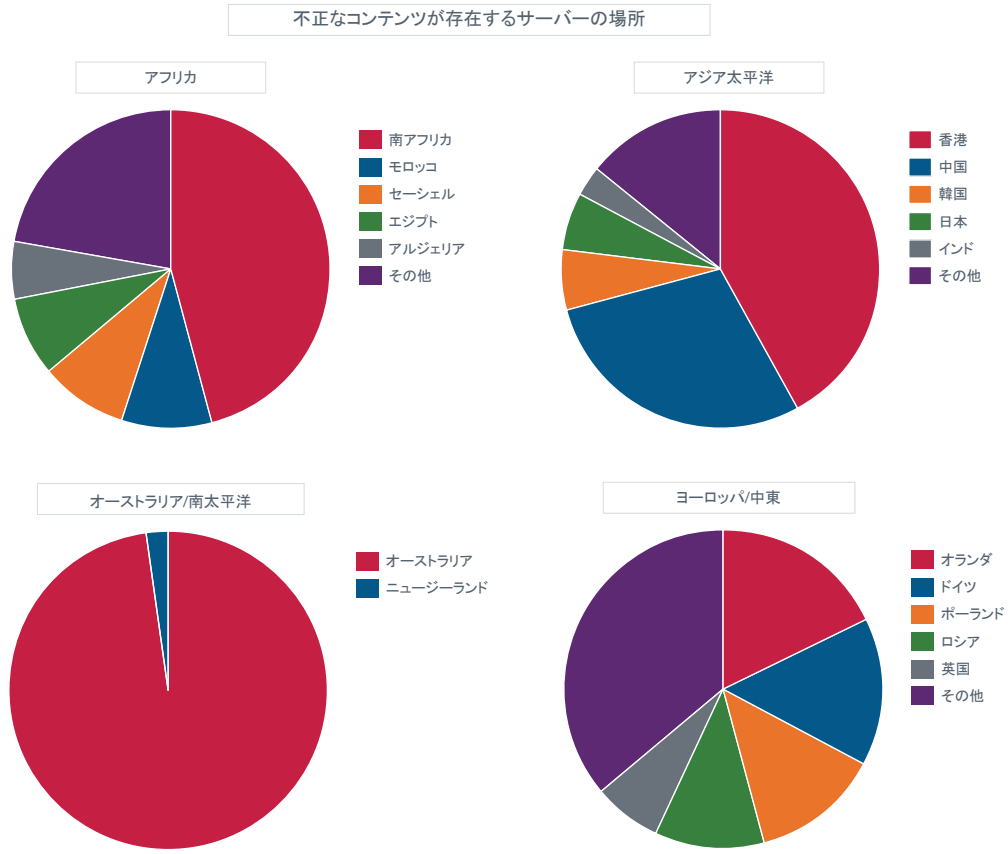
これらの疑わしい URL の大半（94%）には、マルウェア、エクスプロイト、コンピューターのセキュリティを侵害するために設計されたコードが存在します。フィッシング詐欺とスパムは、それぞれ 2.5% と 1.8% です。

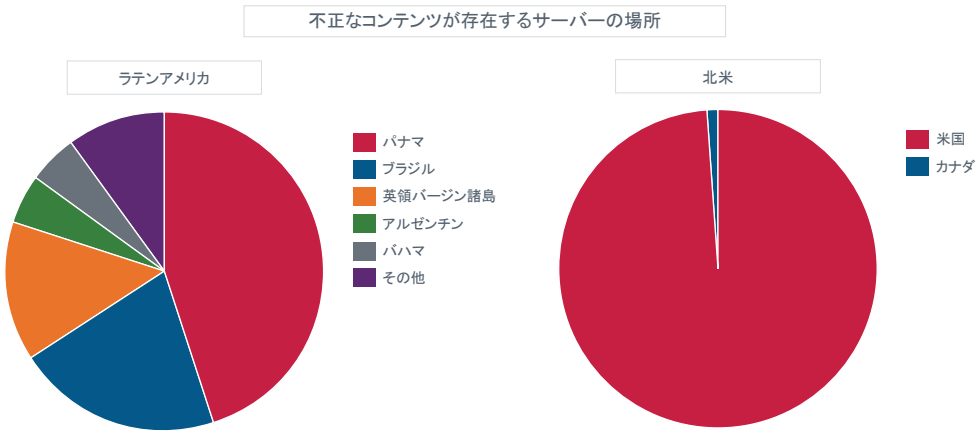


新たな疑わしい URL に関連するドメインは、主に北米（主に米国）およびヨーロッパと中東（主にオランダ）に存在します。この傾向は、新しいものではありません。歴史的に見ても、北米にはかなりの数のマルウェアや疑わしいコンテンツが存在しています。



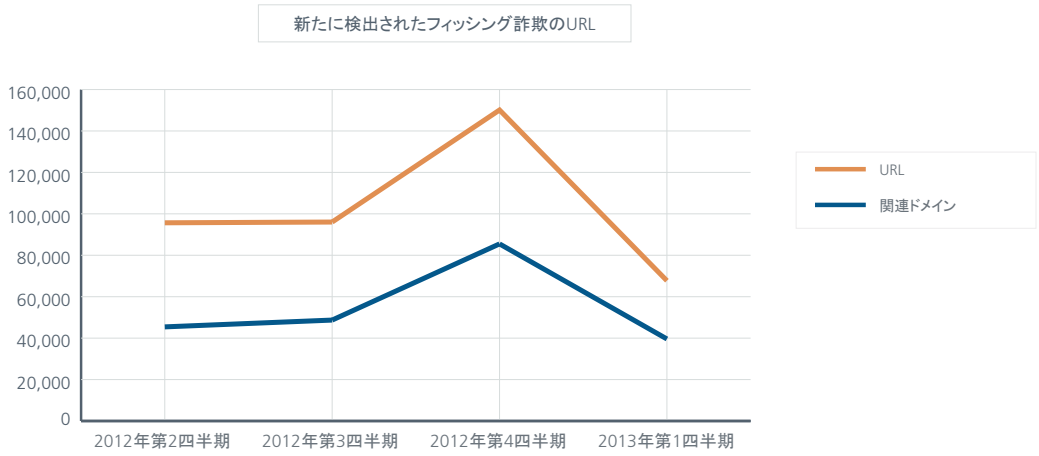
他の国々の悪質なコンテンツをホスティングしているサーバーの場所を詳しく見ていくと、非常に多様であることがわかります。それぞれの地域では、1 つまたは 2 つの国が大部分を占めています。



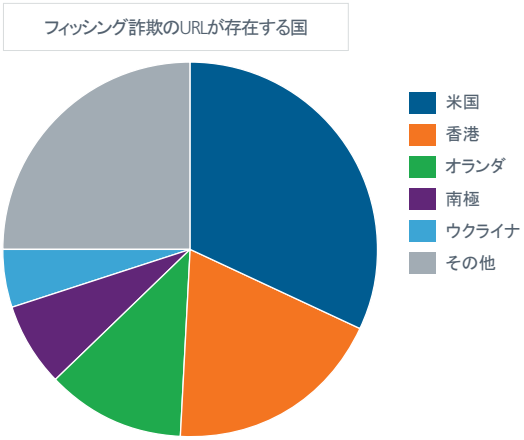


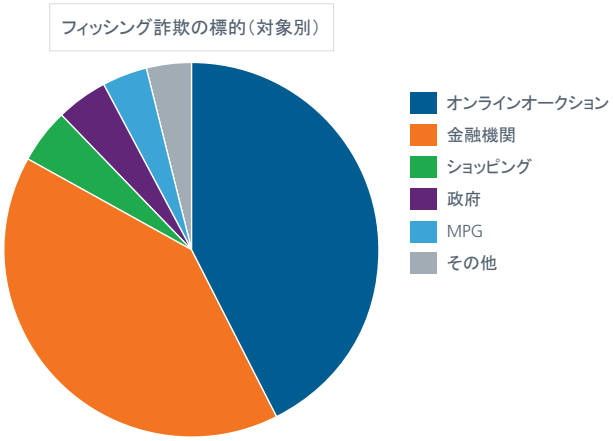
フィッシング詐欺

前の四半期では、新たなフィッシング詐欺の URL 数が 50% 増加しましたが、この四半期は、以前の四半期の水準以下に減少しています。



こうした URL の大半は、米国に存在しています。この四半期に南極がこのリストに登場したことに驚きました。



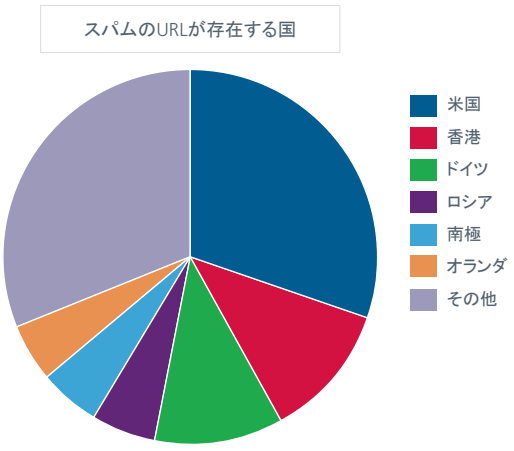


米国の企業が最大の標的となっており、すべての攻撃の 80% を占めています。英国とブラジルがそれぞれ、5% と 3% で続いています。フィッシング詐欺は、金融、政府、ショッピング、オンラインオークション、マルチプレイのゲームといった、いくつかの重要な産業を対象としています。

米国	英国	ブラジル	イタリア	オーストラリア
Amazon	Barclays	Banco Bradesco	Intesa Sanpaolo	ANZ (Australia and New Zealand Banking Group)
Blizzard Entertainment	HM Revenue & Customs	Banco do Brasil	Posteitaliane	Westpac Bank
eBay	HSBC	Banco Itau	UniCredit	
Internal Revenue Service	Lloyds TSB			
J.P. Morgan Chase	Natwest			
PayPal	Royal Bank of Scotland			
Wells Fargo				

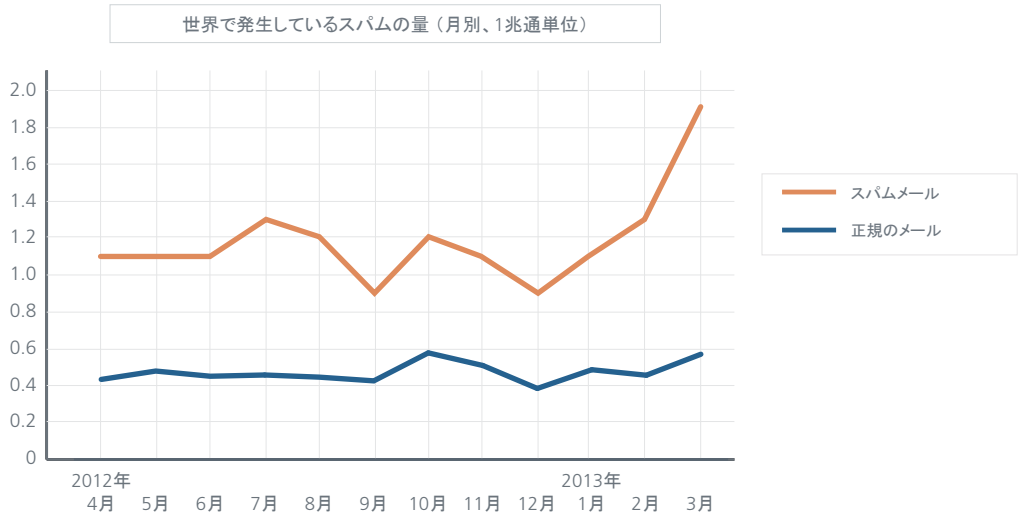
スパム URL

スパムのリンクは、未承諾のスパムメールによって送信されます。このファミリーには、スパムブログやコメントスパムといった、スパミング目的のためだけに構築された Web サイトが含まれています。新たに検出された URL は、前の四半期には約 3 万件でしたが、この四半期には 4 万 5 千件以上と急増しました。こうした URL をホスティングしている主要な国は、米国、香港、ドイツです。南極が再びこの分布に加わっています。



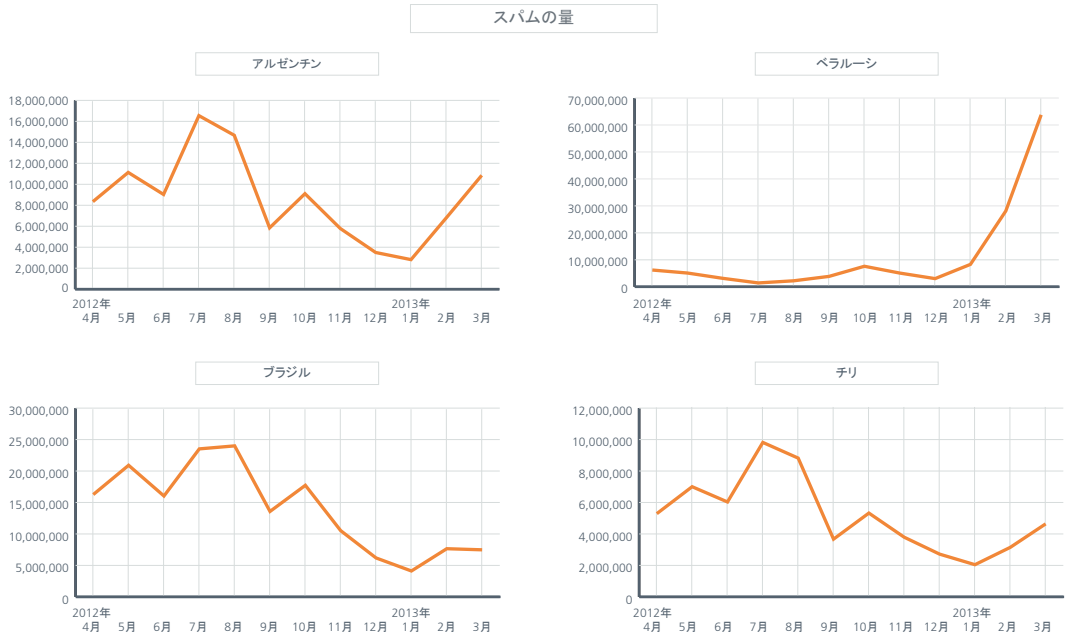
メッセージングの脅威

長期間減少傾向にありましたが、2012 年のスパムレベルは、7 月と 10 月に小さな上昇が見られたものの横ばい状態でした。しかし、この四半期には、2011 年 5 月以来となる量に達するほどの急増が確認されました。



スパムの量

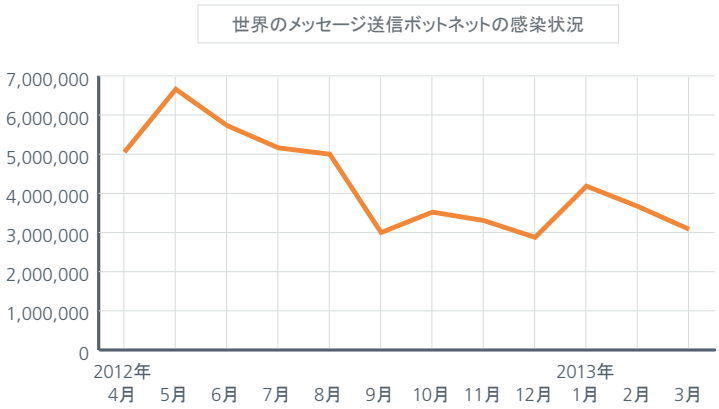
全世界のスパムの量は減少傾向にありますが、国別の統計では、四半期ごとに大きな違いが見られます。最も印象的な例はベラルーシで、この期間で 540% も増加しています。続いて、カザフスタンが 150%、ウクライナが 41% 増加しています。ペルー（58%）、韓国（54%）、ドイツ（53%）では大幅な減少が見られました。

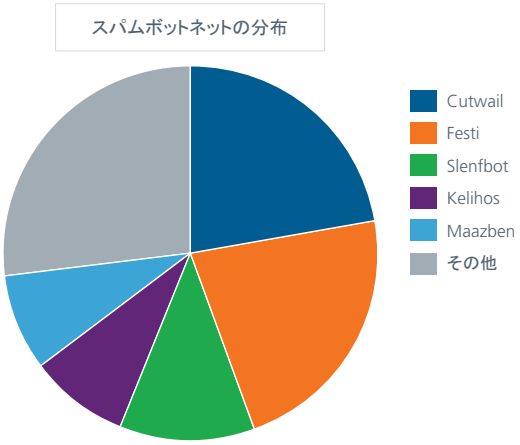



スパムの量
中国
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
2012年
2013年
4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月
コロンビア
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
2012年
2013年
4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月
ドイツ
16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
2012年
2013年
4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月
インド
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
2012年
2013年
4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月
日本
2,000,000
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
2012年
2013年
4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月
カザフスタン
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
2012年
2013年
4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月
ルーマニア
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
2012年
2013年
4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月
ロシア
40,000,000
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
2012年
2013年
4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月

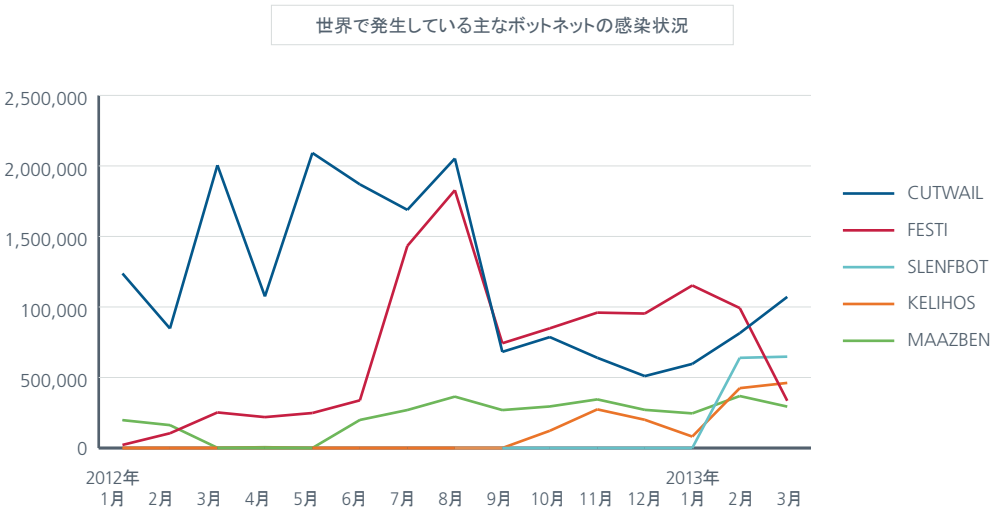
ボットネットの詳細

メッセージングボットネットによる感染は、2012 年 5 月以降、全体的に減少しています。この前の期間の水準は、2011 年第 4 四半期の水準と一致しています。この四半期では、1 月に上昇が見られましたが、その後は 3 か月前と同じ水準まで減少しました。



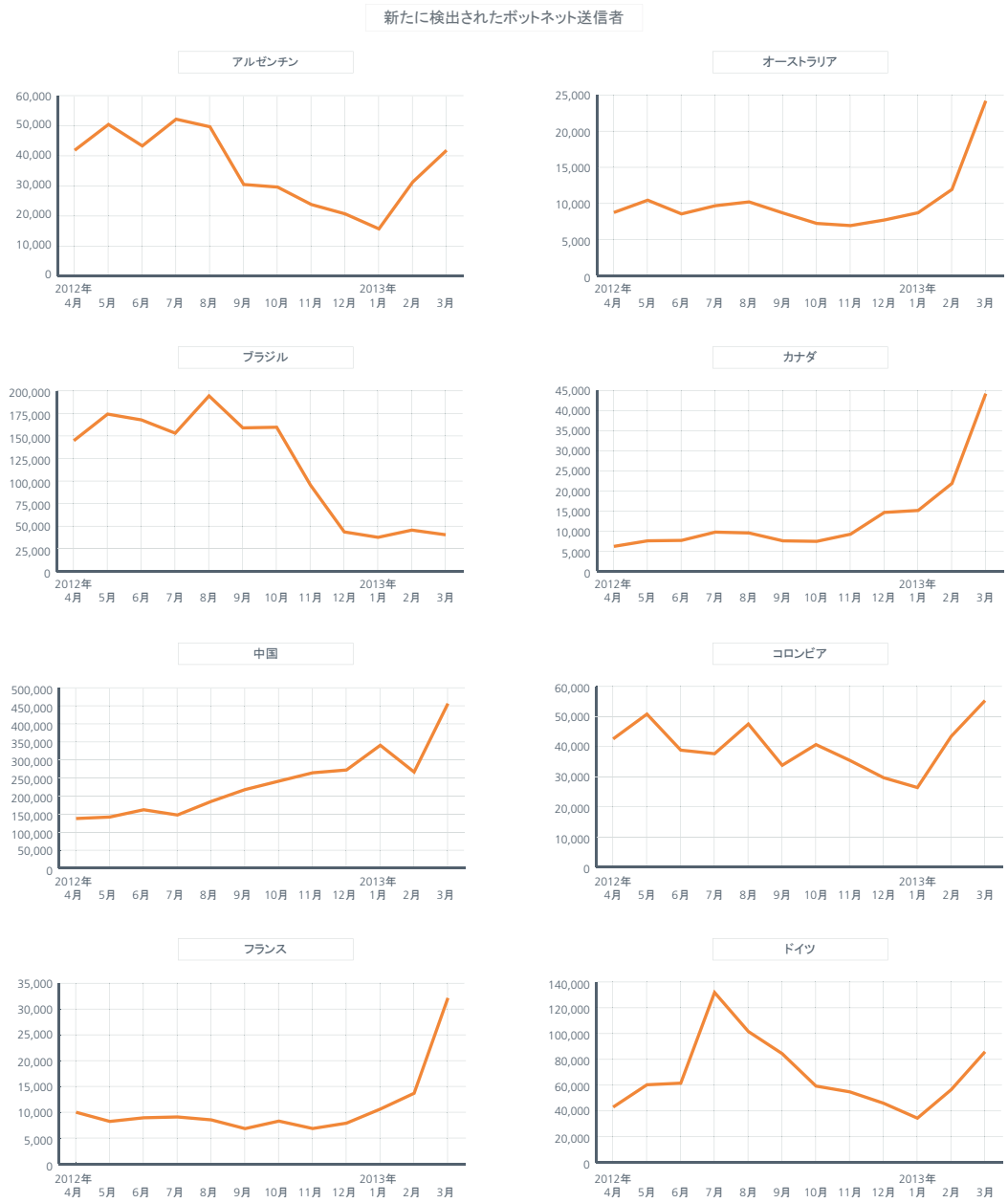


Waledac が昨年末に活動を停止したため、マカフィーの表から姿を消しました。この四半期には、Lethic が主要なラインナップからなくなりました。Kelihos は前の四半期から新たに登場しました。この期間に登場したのは Slenfbot です。Cutwail は現在最も蔓延しているボットネットです。Festi は、数か月前には一番多かったのですが、現在は第 4 位に順位を下げています。



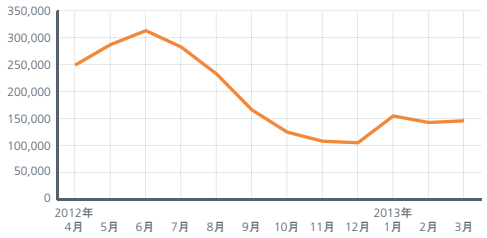
新たに検出されたボットネットの送信者

国に特有のボットネットの統計は、国に特有のスパムと同様、前の四半期とこの四半期において、国ごとに大きく異なっていることがわかります。日本では、ボットネットの送信者数が 420% 増加し、オランダが 270%、カナダが 160%、フランスが 145% 増加しました。その一方で、ブラジルは 60%、ペルーは 50% 減少しました。

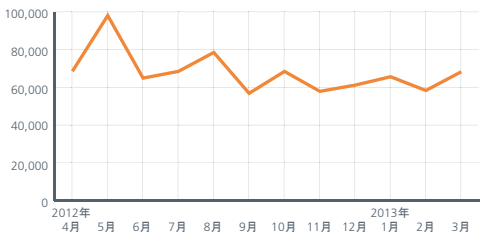


新たに検出されたボットネット送信者

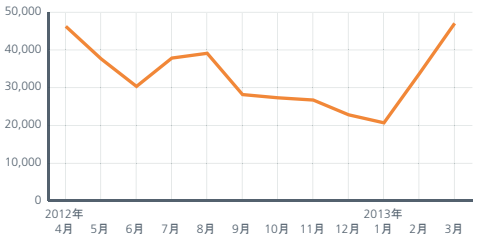
インド



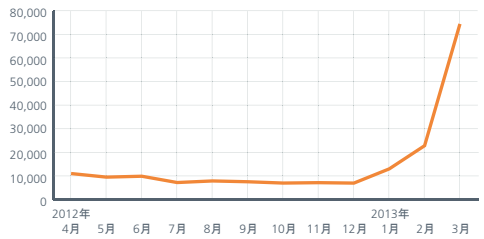
イラン



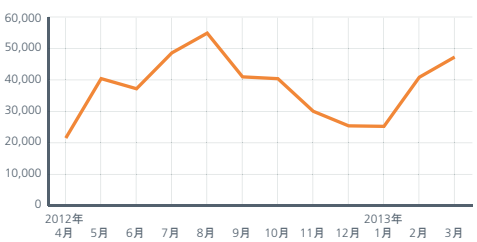
イタリア



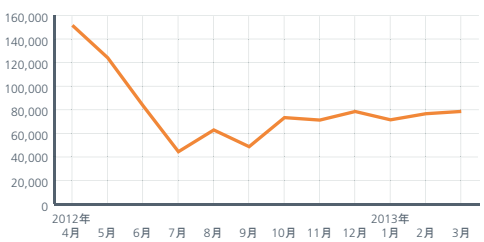
日本



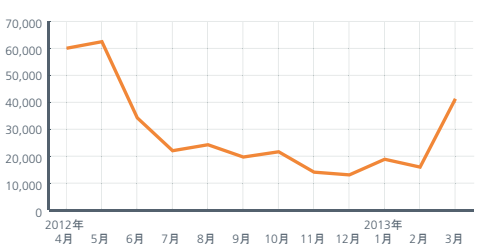
メキシコ



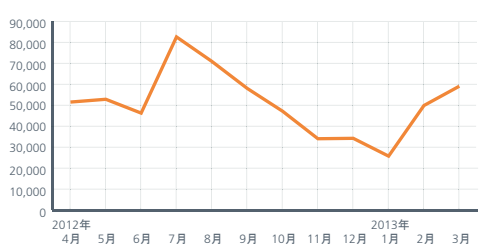
ロシア



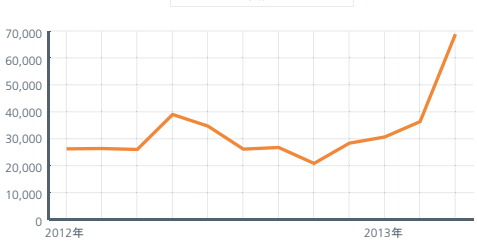
韓国



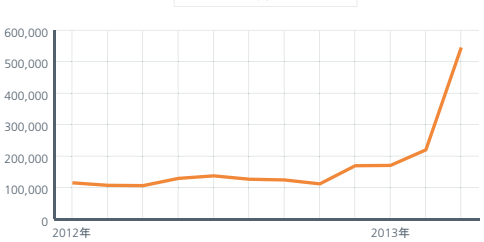
スペイン



英国



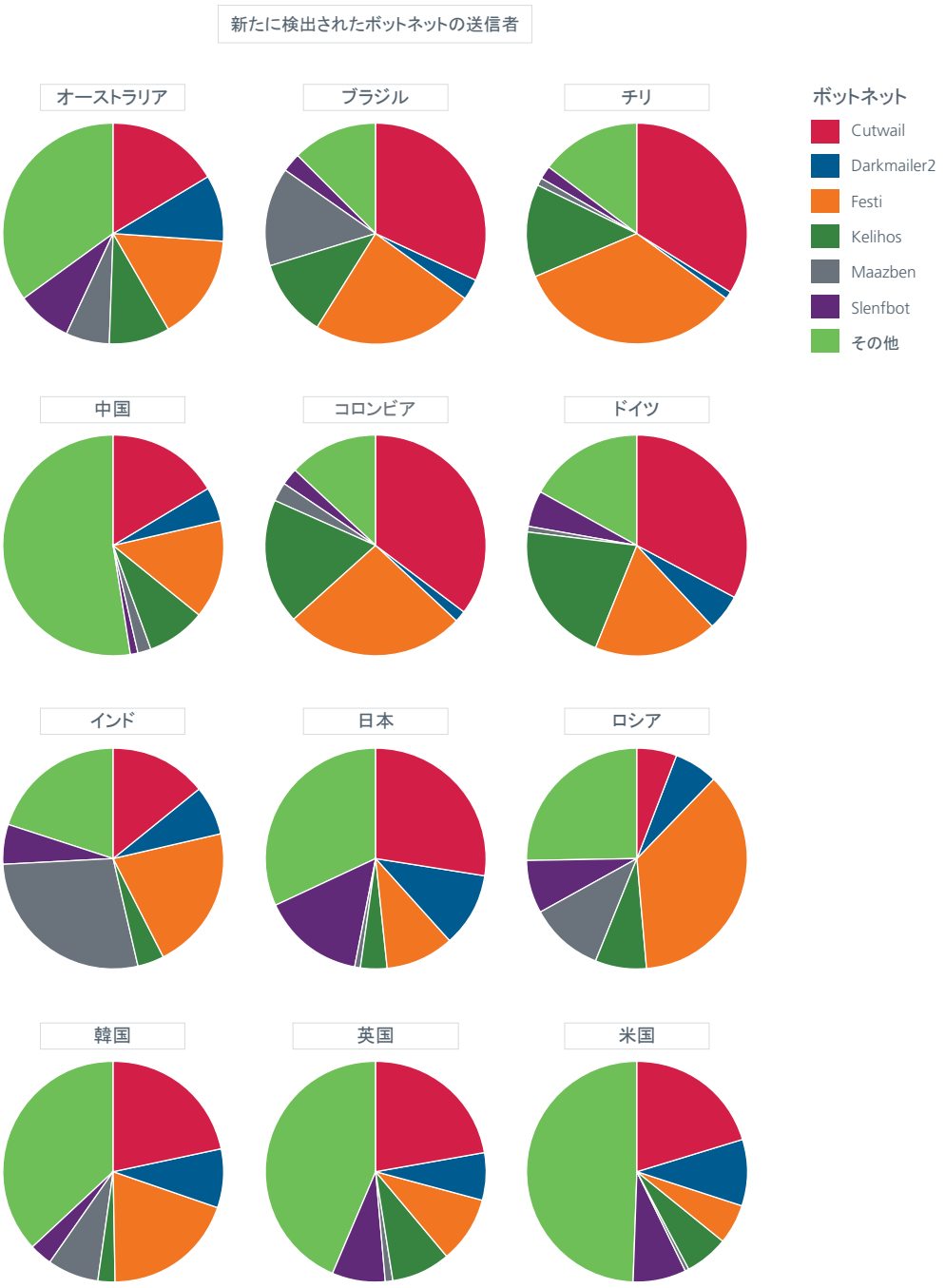
米国



メッセージを送信するボットネットの分布

ボットネットの詳細を見ると、最も蔓延している 5 つのボットネットファミリーが、世界中の様々な国で増加しており、Cutwail と Festi が世界的に上位を占めています。その他には、以下のボットネットの蔓延が目立ちました。

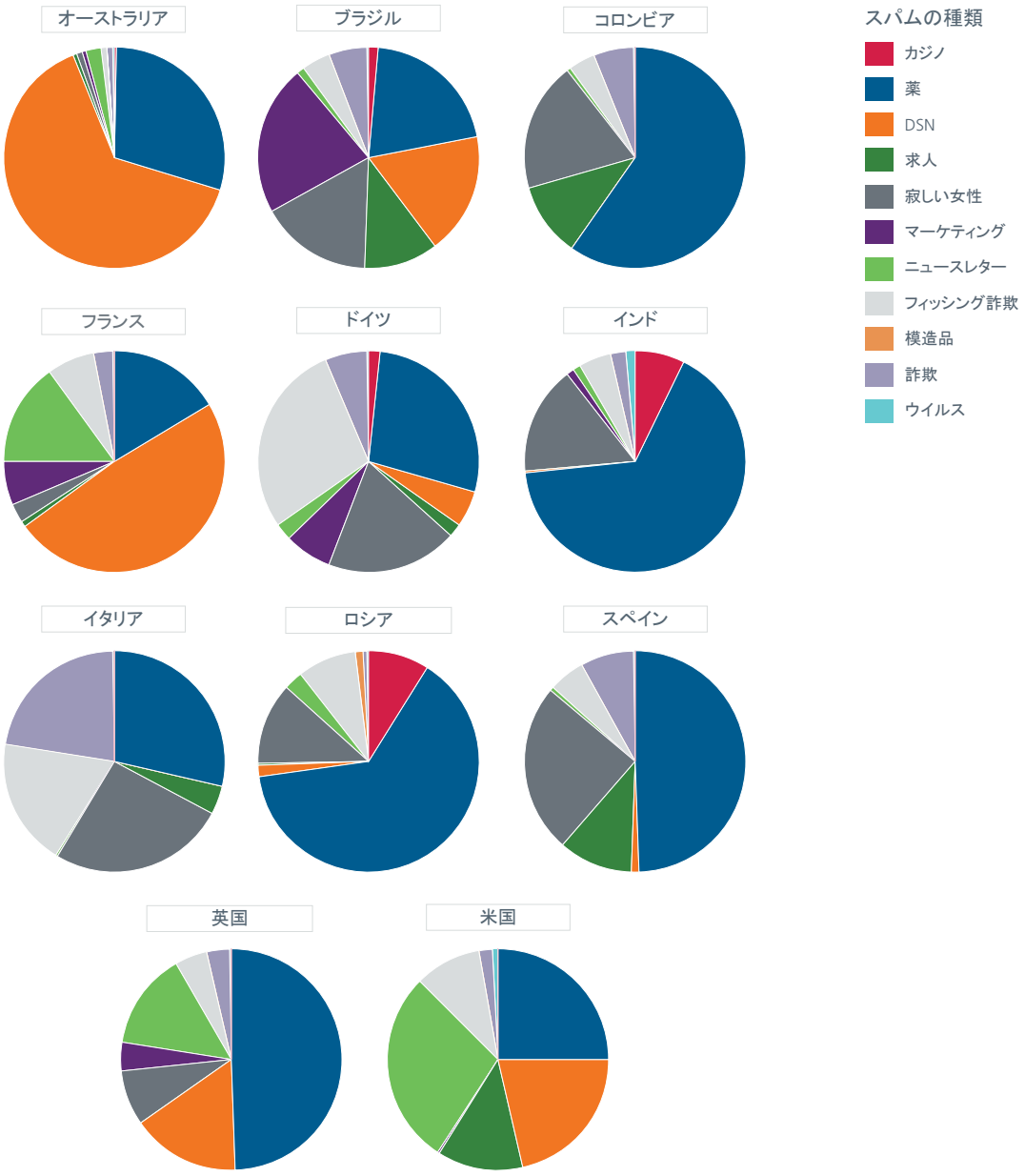
- Darkmailer（ベラルーシ、カザフスタン、パキスタン、インドネシア）
- Cutwail（アルゼンチン、スペイン、ギリシャ、メキシコ）
- Festi（ロシア、モロッコ）
- Slenfbot（ベラルーシ、カザフスタン、ウクライナ）



ドラッグと DSN

世界中のスパムの件名を調べると、ドラッグと DSN（配信通知サービス）の広告が幅広く蔓延していることがわかります。一般的に、ドラッグに関するスパムはボットネットベースであるため、数多くの感染に関連付けられます。とりわけ、英国がこの四半期の大きな標的となっていました。ドイツでは、フィッシング詐欺の広告が非常に高い順位でした。インド、イタリア、ポーランド、スペインでは、「寂しい女性」が交際を頻繁に求めており、幸せではない潜在的な花嫁に関するスパムでいつも第 1 位となるロシアを上回っています。米国とフランスでは、ニュースレターの「購読」を呼びかけています。

アルゼンチン、ブラジル、スペインでは、ポーランド語の仕事系スパムが確認されました。これは、ポーランド人の労働者を雇用するための陰謀である可能性もありますが、おそらく、スペイン語を話す「スノーシュー」スパムの送信者が、ISP による迅速なエビクションを回避するために、多くの IP アドレスにロードを拡散していただけだと考えられます。スパム宣伝による pump and dump の計画が、この四半期に上位になりました。これは、高い利益を求める不用心な投資家にアピールするために、最新の市場の動きを利用していると思われます。しかし、こうした種類の株に巻き込まれるのは、トレーダーとして決して賢明な策とはいえません。



サイバー犯罪

クライムウェアツール

複数の脆弱性がこの四半期のトップニュースとなりました。この脆弱性に関連するエクスプロイトが、蔓延している複数のエクスプロイトのフレームワークに組み込まれていました。

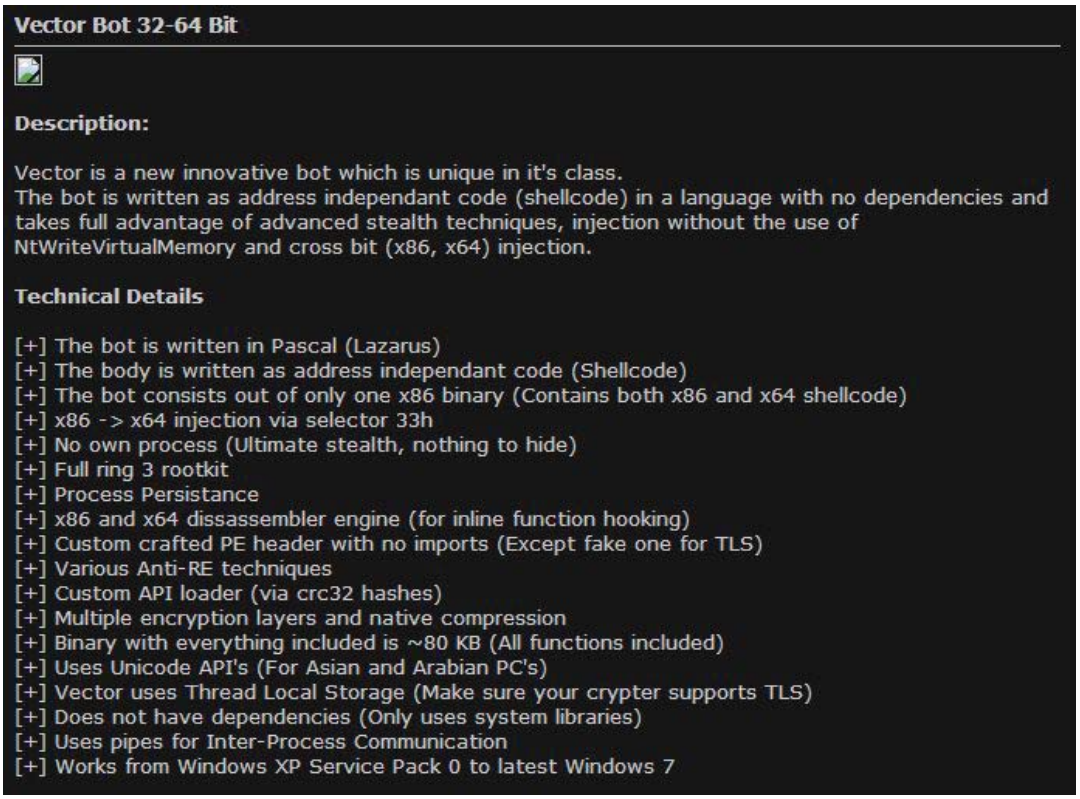
- CVE-2013-0422 (CButton): Oracle Java Runtime Environment setSecurityManager() のコード実行。Blackhole、Nuclear、Cool、Sakura、Sweet Orange などに組み込まれています。
- CVE-2013-0431 (MBeanInstantiator): Oracle Java SE Java Runtime Environment JMX III のリモートコード実行。Blackhole、Nuclear、Cool、Sakura、Styx、Sweet Orange などに組み込まれています。
- CVE-2013-0437: Oracle Java SE Java Runtime Environment 2D 1 のリモートコード実行。
- CVE-2013-0634: Adobe Flash Player Malformed Regular Expressions のリモートコード実行。Gong Da、Fiesta などに組み込まれています。
- CVE-2013-1493: Oracle Java JVM Process のリモートコード実行。Styx などに組み込まれています。

以下の表は、この四半期に確認された有料のエクスプロイトパックの概要です。

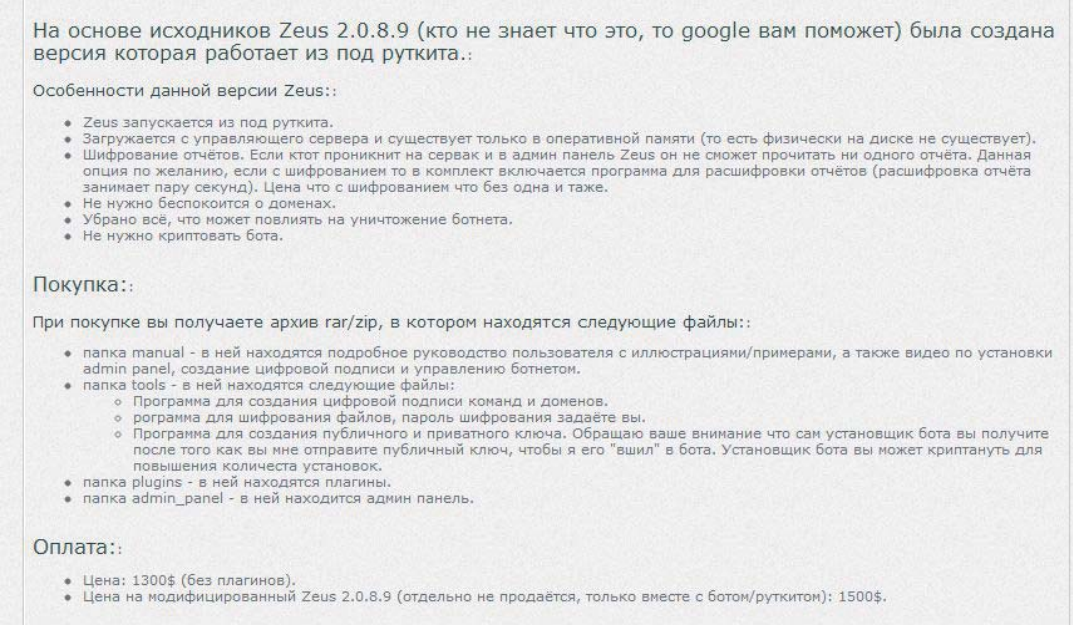
Exploit Pack	Vulnerabilities
Gong Da 1.3[3] (January)	• CVE-2011-3544: Java Rhino • CVE-2012-0507: Java Atomic • CVE-2012-1535 • CVE-2012-1723: Java Applet Field • CVE-2012-1889: MS XML Core • CVE-2012-4681: Java Gondvv • CVE-2012-5076: JAX-WS • CVE-2013-0422: CButton
Gong Da 1.4[4] (February)	• Same as Gong Da 1.3 with two exceptions: °CVE-2012-1535 (Removed) °CVE-2013-0634 (Added)
WhiteHole[5] (January)	• CVE-2011-3544: Java Rhino • CVE-2012-1723: Java Applet Field • CVE-2012-4681: Java Gondvv • CVE-2012-5076: JAX-WS • CVE-2013-0422: CButton
Neutrino[6] (March)	• CVE-2012-1723: Java Applet Field • CVE-2013-0431

また、この四半期にボットネットを作成する有料のマルウェアが確認されました。

・ Vector Bot、1,000 ユーロ、Liberty Reserve により支払い可能



- Namtar Bot 1.0、Zeus 2.0.8.9 のリークソースコードをベースとしており、価格は 1,500 米ドル、ルートキットを含む。他のモジュールは以下の通り
  - DDoS モジュール : 350 米ドル
  - Socks モジュール : 120 米ドル
  - HOSTS File Modifier モジュール : 50 米ドル
  - Backconnect Socks モジュール : 380 米ドル



На основе исходников Zeus 2.0.8.9 (кто не знает что это, то google вам поможет) была создана версия которая работает из под руткита.:

Особенности данной версии Zeus::

- Zeus запускается из под руткита.
- Загружается с управляющего сервера и существует только в оперативной памяти (то есть физически на диске не существует).
- Шифрование отчётов. Если ктот проникнит на сервак и в админ панель Zeus он не сможет прочитать ни одного отчёта. Данная опция по желанию, если с шифрованием то в комплект включается программа для расшифровки отчётов (расшифровка отчёта занимает пару секунд). Цена что с шифрованием что без одна и таже.
- Не нужно беспокоится о доменах.
- Убрано всё, что может повлиять на уничтожение ботнета.
- Не нужно криптовать бота.

Покупка::

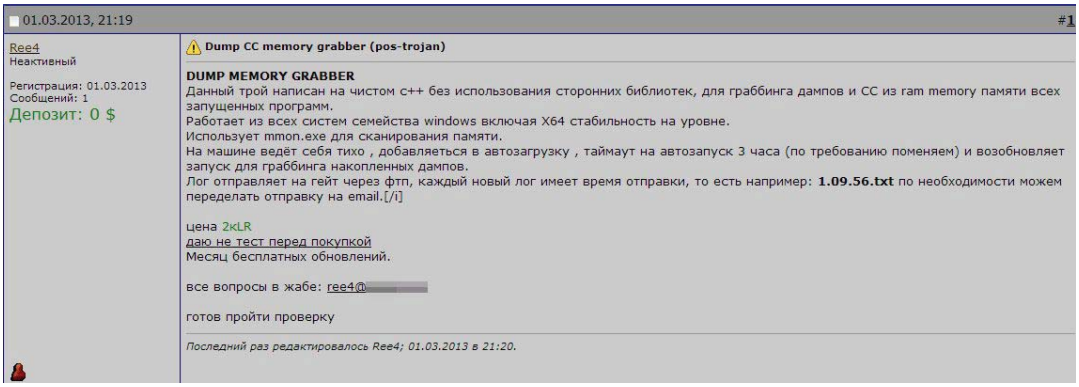
При покупке вы получаете архив rar/zip, в котором находятся следующие файлы::

- папка manual - в ней находятся подробное руководство пользователя с иллюстрациями/примерами, а также видео по установки admin panel, создание цифровой подписи и управлению ботнетом.
- папка tools - в ней находятся следующие файлы:
  - Программа для создания цифровой подписи команд и доменов.
  - программа для шифрования файлов, пароль шифрования задаёте вы.
  - Программа для создания публичного и приватного ключа. Обращаю ваше внимание что сам установщик бота вы получите после того как вы мне отправите публичный ключ, чтобы я его "вшил" в бота. Установщик бота вы может криптануть для повышения количеста установок.
- папка plugins - в ней находятся плагины.
- папка admin_panel - в ней находится админ панель.

Оплата::

- Цена: 1300$ (без плагинов).
- Цена на модифицированный Zeus 2.0.8.9 (отдельно не продаётся, только вместе с ботом/руткитом): 1500$.

- Groupe-IB と CERT-GIB により検出された Dump Memory Grabber は、Chase、Capital One、Citibank、Union Bank of Californiaといった米国の銀行から支払いカード情報を盗むマルウェアです[7]。POS や ATM に取り付けられ、Track1 と Track2 のデータを収集し、生成されたログファイルをリモートサーバーに送信します。このマルウェアの作成者は、ロシアのサイバー犯罪集団とつながりがあると見られており、2,000 米ドルを要求しています。



01.03.2013, 21:19 #1

Ree4
Неактивный

Регистрация: 01.03.2013
Сообщений: 1
Депозит: 0 $

Dump CC memory grabber (pos-trojan)

DUMP MEMORY GRABBER
Данный трой написан на чистом c++ без использования сторонних библиотек, для граббинга дампов и CC из ram memory памяти всех запущенных программ.
Работает из всех систем семейства windows включая X64 стабильность на уровне.
Использует mmon.exe для сканирования памяти.
На машине ведёт себя тихо , добавляеться в автозагрузку , таймаут на автозапуск 3 часа (по требованию поменяем) и возобновляет запуск для граббинга накопленных дампов.
Лог отправляет на гейт через фтп, каждый новый лог имеет время отправки, то есть например: **1.09.56.txt** по необходимости можем переделать отправку на email.[/i]

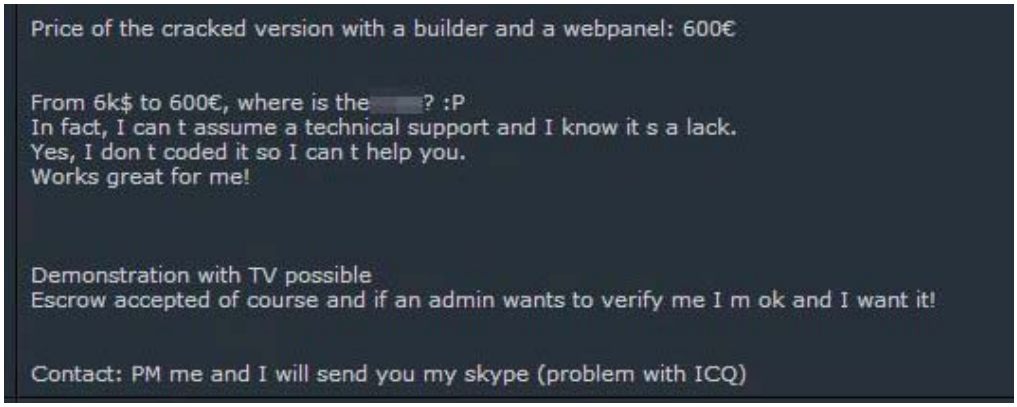
цена 2кLR
даю не тест перед покупкой
Месяц бесплатных обновлений.

все вопросы в жабе: ree4@[redacted]

готов пройти проверку

Последний раз редактировалось Ree4; 01.03.2013 в 21:20.

- もうひとつの金融系マルウェアは VSkimmer です。このマルウェアは、金融取引やクレジットカードによる支払いを実行中の Windows マシンからクレジットカード情報を盗むことが可能です。カードリーダーを検出し、こうしたリーダーが取り付けられている Winodws マシンからあらゆる情報を取得し、データをコントロールサーバーに送信します [8]。3 月に、2012 年に 6,000 米ドルで vSkimmer を購入したと主張しているサイバー犯罪者が、ビルダーと Web パネル付きのクラック版を 600 ユーロで提供していました。



サイバー犯罪者に対する取締り

EU では、1 月 11 日ハーグに欧州サイバー犯罪センター（EC3）が新たに開設されました。米国の FBI やシークレットサービスなど他国の機関との緊密な協力により、EC3 は、法執行機関、裁判官、検事の調査と捜査を支援し、傾向の分析、予測、早期の警告といった脅威の評価を作成します。また、EC3 は、EU 諸国に対して捜査支援（侵入、詐欺、オンラインの児童性的虐待などの対策）を行い、EU の共同捜査において技術、解析、犯罪科学に関する高水準の専門知識を提供します [9]。

この四半期に EC3 が関与して成功した主な警察の取締りを紹介します。

- 1 月、FBI は、3 年にわたる追跡により、銀行をハッキングしたとして、タイで 24 歳のアルジェリア人を逮捕しました。米国当局は、世界中の 200 以上の銀行と金融機関の個人口座に侵入し、何百万ドルもの損害を与えた罪で彼を告訴します。当局は、彼を米国に引き渡すよう求めており、米国の連邦地方裁判所が逮捕令状を発行します [10]。裏社会のサイバー犯罪者を監視し続けているセキュリティアナリスト、Brian Krebs 氏によると、このハッカーは、Zeus を搭載したボットネットの主要なオペレーターの疑いのある有名なサイバー犯罪者、「bx1」のプロフィールに一致しています [11]。

- 1 月、FBI は、Gozi マルウェアの作成と配布において重要な役割を果たしたとして、3 名の個人（ロシア人、ラトビア人、ルーマニア人）を起訴したことを発表しました [12]。このマルウェアは、世界中の 100 万台以上のコンピューターを感染させたことで知られており、米国内では NASA に所属するコンピューターをはじめとして、少なくとも 4 万台のコンピューターが感染し、ドイツ、英国、ポーランド、フランス、フィンランド、イタリア、トルコなどのコンピューターも被害を受けました。Gozi は、個人、企業、政府機関に対して何千万ドルもの損害を与えました。

- 2 月、EC3 との緊密な協力により、スペインの警察が、「警察」を装ったランサムウェアを蔓延させた大規模で複雑なサイバー犯罪ネットワークを摘発したとして、Operation Ransom の成果を発表しました [13]。この犯罪者たちは世界中の何千万台ものコンピューターに影響を与えて、1 年あたり 100 万ユーロを超える利益を得ていたと推定されました。この作戦により 11 人が逮捕されました。主犯格は 27 歳のロシア人で、様々なバージョンのマルウェアの作成、開発、国際的な配布に関与したとされています。彼は、2012 年 12 月にアラブ首長国連邦（UAE）で逮捕されました。残りの 10 名は、金融系の組織とつながりがあり、ロシア人 6 名、ウクライナ人 2 名、グルジア人 2 名が、スペインのコスタデルソルで逮捕されました。

- 3 月、フィンランドの法執行機関当局と EC3 が、不法なインターネット取引と航空券購入に関与していたアジアの犯罪ネットワークを摘発しました。この作戦の成功によって、偽造文書で旅行中の犯罪集団の 2 人のメンバーがヘルシンキ空港で逮捕されました。さらには、約 15,000 件の不正に入手されたクレジットカード番号が犯罪者のコンピューターから発見されました。この犯罪ネットワークは、カード所有者から盗んだクレジットカード情報を悪用していました。ヨーロッパだけで、カード所有者と銀行は 7 万ユーロ以上の損害を受けました。さらに、大規模な国際的な支払詐欺や不法移民に関する犯罪活動の証拠が発見されています [14]。

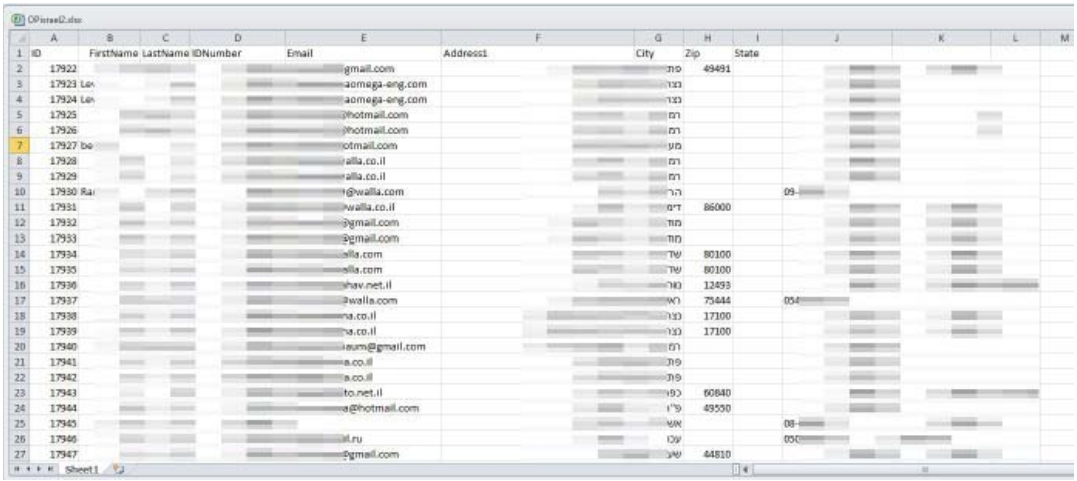
- 3 月、スロベニア警察が、共同捜査によって 5 名のスロベニア市民を拘束し、2012 年半ばに始まった中小企業に対する一連の攻撃の調査を終了しました。これらの攻撃には、被害者のコンピューターへの感染時にパスワードを記録してコンポーネントをインストールし、攻撃者が感染したシステムの活動を監視できるようにするマルウェアが関わっていました。通常、この攻撃は、金曜日または国民の休日の前日に、被害者がコンピューターをシャットダウンしていない場合や、カードリーダーから銀行発行の証明書が含まれるスマートカードを削除していない場合に、実行されました。これにより、週末または休日の間に気付かれることなく、攻撃者は銀行の振替指図の待ち行列に入れる時間を確保できました。この犯罪グループは、25 人の資金の運び屋を利用して、約 200 万ユーロを送金しました。資金の運び屋は、架空の英国の保険会社の名前の在宅勤務の詐欺師として雇われました [15]。
- 3 月、欧州警察機関、EC3、ルーマニア警察が、ヨーロッパ中の支払い端末を改ざんして、何万枚ものカード情報を盗んだとされる、世界的な詐欺組織のメンバー 44 名を逮捕しました。警察の作戦 Pandra Storm では、400 人以上の捜査官がルーマニアと英国の 82 世帯を家宅捜索し、44 人を逮捕して不法な電子機器、金融データ、クローンのカード、現金を押収しました。報道によれば、この詐欺師たちは、偽造を行って、アルゼンチン、コロンビア、ドミニカ共和国、日本、メキシコ、韓国、スリランカ、タイ、米国で取引を行う前に、ヨーロッパ 16 ヶ国で約 36,000 人のカード番号や個人識別情報を盗んだとされています。

ハクティビズム

最近 McAfee Labs が発表したホワイトペーパー、『ハクティビズム - 政治的発言の新たな媒体となったサイバー空間』では、行動主義を支持する DDoS 攻撃形式の合法化に関する問題を議論しました [16]。この四半期に、こうした考えは行動となって現れました。1 月に、ホワイトハウスの「We the People」の Web サイトに、正当な抗議の形式としてコンピューターシステムに対する分散型 DoS 行動を認めるように求める嘆願書が投稿されました [17]。ホワイトハウスの対応を引き出すには、25,000 人の署名が必要でしたが、6,000 人しか集まりませんでした [18]。

1 月 11 日には、ハッカーでありデジタル権利の活動家であった若者アーロン・スワーツ氏の悲劇的な自殺が、活動家の世界に衝撃を与え、Anonymous が米国のコンピューター犯罪対策法の改正を要求する Operation Last Resort を開始しました。この作戦によってハッキングされたのは、Anonymous 発行のログイン、ハッシュ化されたパスワード（非プレーンテキスト）、4,000 件以上の個人の連絡先データ、携帯電話の番号といった個人情報でした。Anonymous は、この作戦の被害者には米国の銀行役員（社長、副社長、COO、支店長、VP）などが含まれていると主張しました。スプレッドシートが .gov の Web サイトと Pastebin に掲載され、Twitter や Facebook の様々な Anonymous アカウントによって公開されました [19]。

#OpIsrael は、イスラエルのガザ地区への攻撃に対する報復として、2012 年 11 月に始動し、この四半期に相次いで攻撃を組織しました。Anonymous に近い様々なハッカーチームが、イスラエルの公的な Web ドメインを攻撃対象として、データを盗み、自称「高度な DDoS」攻撃によって諜報機関モサドの公式 Web サイトに断続的な混乱を引き起こすと述べていました。今回の場合、2 つの Excel ファイルがトルコ人のグループ「The Red Hack」によって公開され、「Sektor 404」が、モサドへの DoS 攻撃に携わったと主張しました。



中東のインターネットの専門家 Tal Pavel 博士は次のように述べています。「（攻撃者が）イスラエルに関する識別情報の一部を入手したのは間違いありません。しかし、モサドの Web サイトをハッキングしてモサドの諜報員のリストを入手したという主張はおそらく心理戦であり、重要なデータベースにはハッキングしていないでしょう[20]」。反イスラエル活動は、第 2 四半期の間も続くと予想されています。

サイバー軍

『ハクティビズム - 政治的発言の新たな媒体となったサイバー空間』では、サイバー軍は、全体主義の傾向のある国の愛国者によって組織されており、愛国的かつ過激な行動を支持することで、政府の利益となる行動を合法または非合法な方法で主張していると定義しました。一部の読者から、より詳細な説明を McAfee Labs に求める声がありました。この四半期の間に活発に活動していたサイバー軍をいくつか紹介します。

- 3xp1r3 Cyber Army: 大量に改ざんを行ったとして知られるバングラデシュのハッカーです。1月に、メンバーの1人が 600 以上のインドの Web サイトを改ざんしました[21]。
- Afghan Cyber Army: 1 月に、34 のパキスタンの Web サイトに侵入して改ざんしました[22]。
- Alarakai Cyber Army: 最近、ウサマ・ビンラディンの写真と「我々アルカイダ・インターネットの戦士は、ミャンマー（ビルマ）のアラカンでのムスリムとの戦いの停止を望む」というメッセージを用いてサイトの改ざんを行いました[23]。
- Armenian Cyber Army: このグループが行った攻撃の主な動機が 1915 年のアルメニア人の虐殺であることを、トルコは認めていません。2 月に、アゼルバイジャンの Web サイトを改ざんしました[24]。
- Bangladesh Cyber Army: 別のバングラデシュのグループが、バングラデシュとインドの国境紛争に関するインドとバングラデシュのハッカーによるサイバー攻撃に関わっていました[25]。
- Brazilian Cyber Army: 2 月に、このグループは、シエラレオネ警察の公式 Web サイトをハッキングしたと主張しました[26]。
- Indian Cyber Army: Pakistan Cyber Army との抗争で知られるナショナリストのグループです。2012 年に、ある特定の作戦に関して Anonymous に参加しました。
- Iranian Cyber Army: イラン政府を支持しています。このグループの反対者は、このグループが革命防衛隊の情報部門のもとで活動していると述べています[27]。3 月に、数多くの Web サイトを改ざんしました[28]。
- Muslim Liberation Army: カシミールのインド軍駐留に抗議するために、2012 年にインドの Web サイトに攻撃したことで知られるパキスタン人のグループです。2 月に、このグループのメンバーが 25 以上のイスラエルの Web サイトをハッキングして改ざんし、パレスチナを支持するメッセージを配信しました[29]。
- Pakistan Cyber Army: ハッキングまたはクラッキング集団ではなく、違法な活動はしていないと主張していますが、パキスタンのサイバー空間をハッキング攻撃から保護したいと望むパキスタン人のセキュリティの専門家全員の象徴となっています。2 月に、このグループは様々なインドの Web サイトをハッキングしました[30]。
- Philippine Cyber Army: 3 月に、このグループは、175 のマレーシアの Web サイト（国有のページを含む）を攻撃し、フィリピン政府にサバ州から立ち退くようにメッセージを送信するよう人々に呼びかけるマレーシアのハッカーに対抗しました[31]。彼らは、Anonymous に近い立場です。
- Syrian Electronic Army: シリアのバシャル・アサド大統領を支持していることで知られています。このグループが最初に登場したときに、2011 年 6 月に大統領は演説のなかで Electronic Army の若者たちを称賛しました[32]。2 月に、AFP の写真部門の Twitter フィードを乗っ取りました[33]。3 月に、ヒューマン・ライツ・ウォッチの管理者アカウントへのアクセスを取得し、アサド大統領がクラスター爆弾を使用しているというこの組織のレポートは「嘘」であると主張しました[34]。
- Tunisian Cyber Army: 3 月に、（#opBlackSummer の一環として）米国政府の Web サイトに侵入しました[35]。Al-Qaeda Electronic Cyber Army と合同で攻撃を行いました。
- Turkey Cyber Army: 自身の Facebook アカウントから様々な改ざんを行ったと発表しました。

民主主義に関する見方が人によって異なるように、全体主義に関する見方も人それぞれです。このため、基準を設けることを提案します。「Reporters Without Borders World Press Freedom Index（国境なき記者団の報道の自由ランキング）」を見ると、最も自由な国の第 1 位はフィンランドであり、最下位は第 179 位のエリトリアです [36]。米国を除けば、サイバー軍が存在している国はすべて、100 位以下の順位であり、13 ヶ国のうち 9 ヶ国が第 138 位～ 176 位の間にいます。市民の自由度が高い国は、サイバー軍が「象徴」となることはありません。

McAfee Labs について

McAfee Labs は、世界各地に存在する McAfee の研究機関で、マルウェア、Web、メール、ネットワークなどに対する脅威を研究・調査し、脆弱性の報告を行っています。McAfee Labs は、世界各地に数百万台のセンサーを配備し、クラウド型サービスの McAfee Global Threat Intelligence™ により情報収集を行っています。世界 30 か国に存在する McAfee Labs には、様々な分野を専門とする 500 名の研究者が在籍し、企業や一般のユーザーを保護するため、リアルタイムの脅威検出、アプリケーションの脆弱性特定、リスクの相関分析、迅速な問題解決に努めています。詳しくは、www.mcafee.com/labs をご覧ください。

マカフィーについて

マカフィーは、インテルコーポレーション（NASDAQ:INTC）の完全子会社であり、企業、官公庁・自治体、個人ユーザーが安全にインターネットの恩恵を享受できるよう、世界中のシステム、ネットワーク、モバイルデバイスを守るプロアクティブで定評あるセキュリティソリューションやサービスを提供しています。マカフィーは、Security Connected 戦略、セキュリティにハードウェアを活用した革新的なアプローチ、また独自の Global Threat Intelligence により、常に全力でお客様の安全を守ります。詳しくは、http://www.mcafee.com/jp/ をご覧ください。マカフィーでは、セキュリティに関する様々な研究成果や調査結果を web 上で公開しています。詳しくは下記ページをご覧ください。http://www.mcafee.com/japan/security/publication.asp

[1] http://www.mcafee.com/us/resources/white-papers/wp-citadel-trojan.pdf
[2] http://home.mcafee.com/virusinfo/global-virus-map
[3] http://eromang.zataz.com/2013/01/13/gong-da-gondad-exploit-pack-add-java-cve-2013-0422-support/
[4] http://eromang.zataz.com/2012/12/02/cool-exploit-kit-remove-support-of-java-cve-2012-1723/
[5] http://malware.dontneedcoffee.com/2013/02/briefly-wave-whitehole-exploit-kit-hello.html
[6] http://malware.dontneedcoffee.com/2013/03/hello-neutrino-just-one-more-exploit-kit.html
[7] http://www.securityweek.com/exclusive-new-malware-targeting-pos-systems-atms-hits-major-us-banks
[8] https://blogs.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals
[9] http://europa.eu/rapid/press-release_IP-13-13_en.htm
[10] http://www.security-faqs.com/alleged-algerian-bank-hacker-arrested-by-fbi-in-thailand.html
[11] http://krebsonsecurity.com/2013/01/police-arrest-alleged-zeus-botmaster-bx1/
[12] http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusPR.php
[13] https://www.europol.europa.eu/content/police-dismantle-prolific-ransomware-cybercriminal-network
[14] https://www.europol.europa.eu/content/international-network-line-card-fraudsters-dismantled-newsletter
[15] http://www.cert.si/obvestila/obvestilo/article/slovenian-police-cracks-down-on-a-gang-netting-almost-2-million-EUR-from-companies-via-e-banking-hac.html
[16] Page 32. http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf
[17] http://news.cnet.com/8301-1009_3-57563188-83/anonymous-petitions-u.s-to-see-ddos-attacks-as-legal-protest/
[18] http://njtoday.net/2013/02/06/petition-to-have-white-house-recognize-ddos-as-legitimate-protest-unlikely-to-draw-response/
[19] http://www.zdnet.com/anonymous-posts-over-4000-u-s-bank-executive-credentials-7000010740/
[20] http://www.timesofisrael.com/dont-believe-hack-claims-against-mossads-website-expert-says/
[21] http://news.softpedia.com/news/Over-600-Indian-Websites-Defaced-by-3xp1r3-Cyber-Army-Hacker-318967.shtml
[22] http://www.thehackerspost.com/2013/01/34-pakistan-sites-hacked-defaced-by.html
[23] http://www.cyber-expertz.net/2013/01/68-italy-sites-include-3-govt-hacked-by.html
[24] http://www.armenews.com/article.php3?id_article=87754
[25] http://news.softpedia.com/news/Bangladesh-Cyber-Army-Attacks-Indian-Sites-in-Memory-of-15-Year-Old-Girl-Video-319234.shtml
[26] http://www.ehackingnews.com/2013/02/sierra-leone-police-website-hacked-by.html
[27] http://www.popsci.com/technology/article/2013-03/how-iran-censors-internet-infographic
[28] http://www.innsalzach24.de/innsalzach/waldkraiburg/waldkraiburg/waldkraiburg-homepage-realschule-ziel-eines-hacker-angriffs-innsalzach24-2783344.html
[29] http://www.thehackerspost.com/2013/02/israeli-server-hacked-by-hitcher-from.html
[30] http://hackread.com/bangalore-city-police-website-hacked-defaced-by-pakistan-cyber-army/
[31] http://www.malaysia-chronicle.com/index.php?option=com_k2&view=item&id=64242:sabah-crisis-sparks-cyberwar&Itemid=2
[32] http://www.npr.org/2011/09/25/140746510/pro-assad-army-wages-cyberwar-in-syria
[33] http://www.esecurityplanet.com/hackers/afp-twitter-feed-hacked-by-syrian-electronic-army.html
[34] http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/syria-rebel-hackers-syrian-electronic-army-anonymous-support
[35] http://hackread.com/tunisian-cyber-army-founds-xss-vulnerability-on-pentagon-website/
[36] http://fr.rsf.org/IMG/pdf/classement_2013_gb-bd.pdf

McAfee
An Intel Company

マカフィー株式会社
www.mcafee.com/jp

東京本社　〒 150-0043 東京都渋谷区道玄坂 1- 12- 1 渋谷マークシティウェスト 20F
TEL 03-5428-1100（代）FAX 03-5428-1480
名古屋営業所　〒 460-0002 愛知県名古屋市中区丸の内 3-20-17 中外東京海上ビルディング 3F
TEL 052-954-9551（代）FAX 052-954-9552
西日本支店　〒 530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F
TEL 06-6344-1511（代）FAX 06-6344-1517
福岡営業所　〒 810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F
TEL 092-287-9674（代）FAX 092-287-9675