レポート

McAfee
An Intel Company

McAfee 脅威レポート：2013 年第 2 四半期

McAfee Labs

目次

序論

McAfee Labs の研究者は、2013 年第 2 四半期の脅威を分析し、よく見られる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などのマルウェア全体が着実に増加しています。韓国に対するサイバースパイ攻撃や世界規模でのスパムの増加が大きな注目を集めています。

韓国の銀行やメディア企業を標的とした Dark Seoul 攻撃をきっかけとして、McAfee Labs は、マスターブートレコードを削除することで機能しなくなったコンピューターの基本部分の範囲を超えて調査を進めました。この事件の背景として、2009 年に始まったサイバースパイ攻撃作戦において韓国軍を標的として現在も侵入工作が進行中であることが明らかになったことがあります。7 月に発表したマカフィーの詳細なレポートでは、損害や監視工作の背後にある経緯とコーディングの詳細について説明しています。

バックドア型のトロイの木馬やバンキングマルウェアは、この四半期に最も蔓延したモバイル脅威です。この期間に 17,000 を超える新たな Android のサンプルが集まりました。今年、記録を更新することは確実です。新たに発見された全種類のマルウェア数は、この四半期に 1,800 万を超えており、バイナリ数は累計で 1 億 4,700 万以上に達しています。USB ドライブ経由の感染が多くみられる AutoRun 脅威は、パスワード窃盗プログラムと同様、記録的な水準を維持しています。認可された合法的なソフトウェアを装う署名付きマルウェア数は、記録を更新し続けており、この四半期に 50% 増加しています。システムのマスターブートレコードを攻撃するマルウェアは、前四半期から減少していますが、依然として危険な水準です。

被害者が身代金を支払うまでコンピューターを人質に取って解放しないランサムウェアは、深刻な問題であり、悪化の一途を辿っています。新たなサンプル数は、前四半期に比べて 2 倍以上増加しています。犯罪者は、この手口を利用することで比較的安全にお金を奪えるだけではなく、多くの場合マルウェアを削除しないため、被害者のシステムの機能は復旧しない状態のままです。

公表されたデータ侵害件数は、過去 3 四半期の間、平均して比較的横ばい状態でした。内部の人間よりも外部の人間によるデータ盗難件数が多いのですが、このデータが被害者から提供される脅威であるため、被害者が組織内の弱みをすべて明らかにしたくないと考え、提供されないものがある可能性があります。MySQL では、依然として、企業のデータベースに関して報告される脆弱性の数が最も多くなっています。

McAfee Global Threat Intelligence ネットワークによって、埋め込まれた ifame や悪意のある Java コードなどのブラウザーベースの脅威が、インターネットの悪意のある活動の 4 分の 3 近くを占めていることが明らかとなっています。再び米国内の IP アドレスがネットワーク脅威の大半のソースとなり、ターゲットにもなっています。

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 16% 増加したことがわかりました。フィッシング詐欺の主な攻撃対象は、米国在住者です。また、フィッシング詐欺攻撃の標的となった主な業界は、金融機関およびオンラインオークション企業です。スパム量は元の水準に戻りつつありますが、この四半期のスパムメッセージの数は、4 月に 2 兆件に達しました。これは 2010 年以降で最も多い数字です。マカフィーでは引き続き、全世界からピックアップした国における様々なスパムの詳細情報やボットネットの流行に関して報告していきます。

重大なハッキング事件を時系列に沿って記載することで、この四半期に登場した主要な犯罪活動を示しています。オンライン通貨 Bitcoin が話題となり、ある Bitcoin のプロバイダーは、サービスを妨害して価格を乱高下させようとする DDos 攻撃の被害を受けました。この四半期に世界中の捜査当局者の捜査がいくつか実り、何億から何十億ドルもの窃盗に関わった集団を逮捕して活動を停止させました。

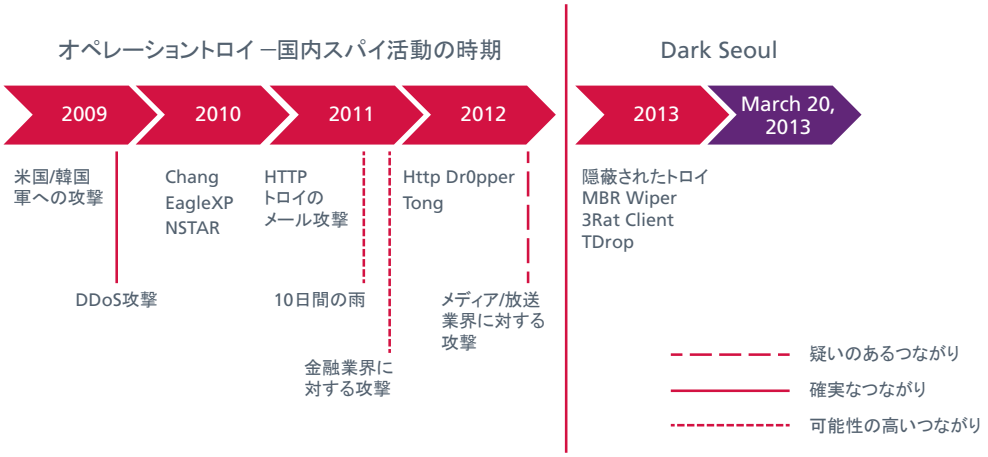
活動家のハッカーは、示威行動や改ざんを行い、反対勢力からの反撃を引き起こしています。グループ Anonymous が関与している活動もありますが、その名前を使って他の活動を支援している可能性もあります。中東地域では、再び政治的表明が活発となっています。

オペレーショントロイ

韓国の金融サービスやメディア企業に対する「Dark Seoul」攻撃の出現が 3 月 20 日に報告されたとき、大きく注目を集めたのは、何千台ものコンピューターのマスターブートレコードが削除されたことでした。この攻撃に感染した PC のハードディスクのデータはすべて消去されました。しかし、この事件以降、McAfee Labs は、Dark Seoul 攻撃にはサイバー破壊行為に留まらない技術と手口が幅広く利用されていることを明らかにしました。

犯罪科学データによって、Dark Seoul が実際には、オペレーショントロイと呼ばれていたマルウェア開発プロジェクトから派生した最新の攻撃であることが判明しています（このトロイという名前は、このマルウェアのコンパイラのパス文字列でこの古代の都市が繰り返し引用されていたことに由来しています）。Dark Seoul 事件に関する McAfee Labs の調査によって、2009 年に作成されたコードをベースとして、韓国の軍隊を標的とした国内スパイ活動への長期的な工作が明らかになりました。

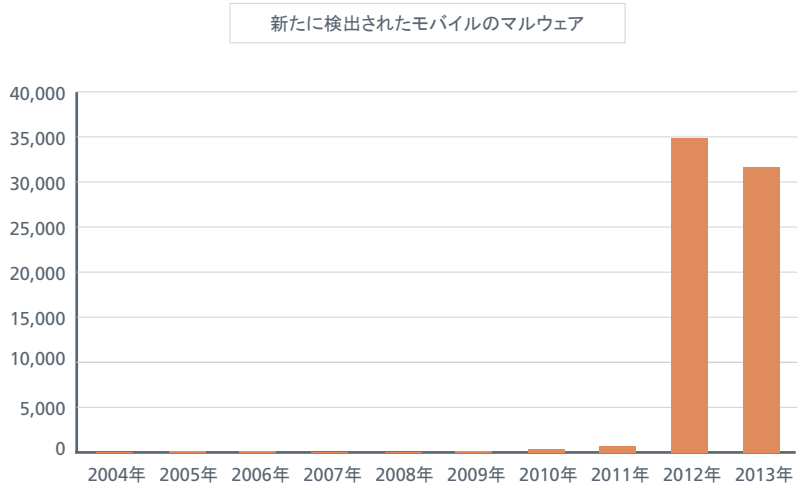
合法であれ非合法であれ、ソフトウェア開発者は、自分が作成したコードに指紋や、ときには足跡を残す傾向があります。犯罪科学研究者は、こうした証拠を利用して、いつどこでコードが開発されたのか突き止めることができます。開発者が不注意すぎる場合を除けば、研究者が製品から個人の開発者まで足跡を辿れることはめったにありません。しかし、多くの場合、こうした作成物を使用して、新しい「製品」のオリジナルソースや開発レガシーを特定することができます。ときには、開発者が新しい脅威の「所有権」を確立する目的でこうした指紋を挿入している場合もあります。McAfee Labs は、新たな脅威のソースを特定する際に高度なコード解析と犯罪科学技術を活用しています。これは、多くの場合、こうした解析を通じて、攻撃を緩和する最適な方法を明らかにしたり、脅威が今後どのように進化するのか予測したりすることができるからです。McAfee Labs の調査によって、Dark Seoul 攻撃が何年間にも渡って計画されたサイバースパイ活動により進行してきたことが判明しました。

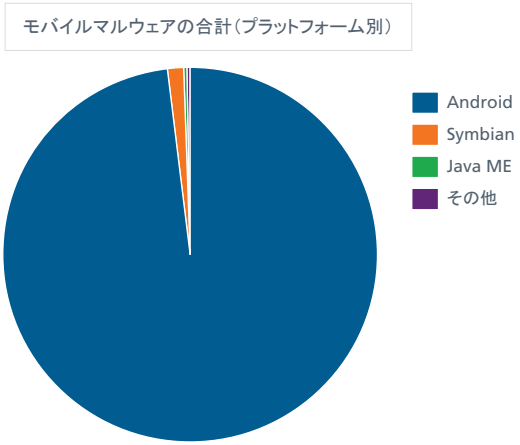


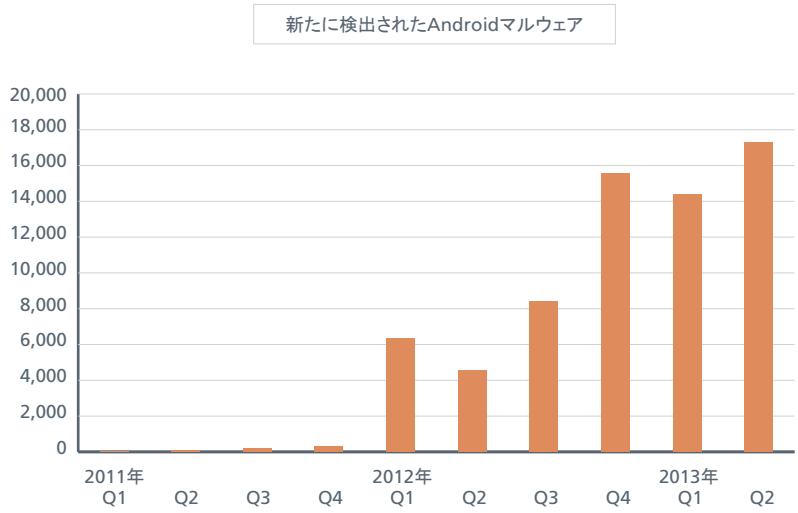
3 月のサイバー攻撃に関する調査によって、隠蔽された機密情報収集作戦が進行中であることが明らかになりました。McAfee Labs は、3 月 20 日の攻撃は、システムの破壊に関係した単独の事件ではなく、2009 年から始まった一連の標的への侵入活動の最新の攻撃であると結論付けました。詳細については、McAfee Labs のレポート『Dissecting Operation Troy: Cyberespionage in South Korea（オペレーショントロイの分析：韓国内でのサイバースパイ活動）』を参照してください[1]。

モバイルの脅威

この四半期に、被害者に気付かれずにデータを盗む、バックドア型トロイの木馬や銀行のログイン情報を追い求めるマルウェアが、新たなモバイルマルウェアファミリー全体で最大の割合を占めてきています。スパイウェアも活発であり、マルウェアの作成者は引き続き活動家を標的としています。2013 年半ばで、既に 2012 年の間に収集されたモバイルマルウェアサンプル数に迫る数字になりました。年末には倍の数になるでしょうか。マカフィーではそれ以上に増加すると予測しています。この四半期に、マカフィーのデータベースには 17,000 を超える Android サンプルが追加されました。







バンキングマルウェア

ヨーロッパとアジアの銀行では、SMS メッセージ経由で 2 要素認証が求められます。顧客が自分の銀行アカウントにログインする場合、モバイル取引認証番号（mTAN）がテキストメッセージで送信されます。自分のアカウントにアクセスする際には、この mTAN コードを入力しなければなりません。この手順によって、ユーザー名とパスワードしか盗んでいない攻撃者が、被害者のお金に手を出すのを防いでいます。

2 要素認証をクリアする方法を求めている攻撃者は、銀行から送信されるテキストメッセージを入手する必要があります。被害者の PC からユーザー名とパスワードを盗んだ攻撃者は、ユーザーに SMS 転送マルウェアをインストールするように仕向ける必要があります。

Android/FakeBankDropper.A と Android/FakeBank.A という一組のマルウェアは、標準的な SMS 転送マルウェアをさらに進化させたものです。通常、どのオンライン銀行に関しても銀行が提供する公式のアプリ以外は利用しないよう、ユーザーにアドバイスしています。しかし、Android/FakeBankDropper.A は、この対策を逆手に取って、銀行の公式アプリを Android/FakeBank.A に置き換えてしまいます。被害者がオリジナルのアプリをインストールしたと思い込んでいる間には、攻撃者は被害者のアカウントにログインして銀行からの最新の SMS を入手します。

同様の手口の SMS 転送アプリの一覧を示します。

- Android/Nopoc.A: 受信した SMS メッセージを攻撃者のサーバーに転送します。
- Android/Pincer.A: ユーザーのデバイスへの証明書のインストールを装い、攻撃者のサーバーに SMS メッセージを転送します。
- Android/Stels.A: Adobe Flash プレイヤーの更新を装い、ユーザーの機密情報を収集し、攻撃者のサーバーにその情報を開示します。
- Android/Wahom.A: 合法的なアプリを装っていますが、ユーザーにエラーメッセージを表示します。このマルウェアは、自身のアイコンを隠すことで、ユーザーにアプリをアンインストールされたと思わせます。ユーザーの機密情報を収集し、SMS を攻撃者のサーバーに転送します。

成人向けソフトウェア

成人向け娯楽ソフトウェアは、攻撃者にとって格好のカモフラージュになります。大きな利益を得られる上に、法執行機関の注目を集めにくくするからです。この四半期には、成人向け娯楽アプリに対する攻撃者の関心の高さが目立ちました。

日本では、不要なプログラム（PUP）の最大のファミリーである Android/DeaiFraud が、人気のある出会い系サイトのアプリを装っています。このマルウェアが直接ユーザーに損害を与えることはありませんが、攻撃者からのスパムが送信されるようになります。また、攻撃者のパートナーが出会い系サイトを利用する実在のシングルを装うことで、ユーザーがこの出会い系サイトに登録していると思い込ませる場合もあります。

PUP の他に、Android/NMPHost.A というマルウェアも確認されています。このマルウェアは、ユーザーに 2 つ目のマルウェア、Android/NMP.A をダウンロードするように促し、このマルウェアを通じてユーザー情報を盗みます。この 2 つのマルウェアは、成人向け娯楽アプリを装っています。一旦インストールされると、Android/NMP.A がユーザーの機密情報を収集し、この情報を攻撃者のサーバーに送信します。

対象を絞ったトロイの木馬

攻撃者は、合法的なアプリは悪意のあるコードの格好の隠れ蓑であることを把握しており、こうしたアプリの人気やユーザーからの信頼性の高さを悪用しています。Android/Kaospy.A では、攻撃者は、カカオトークアプリの修正版を使用しており、チベット人活動家を標的としています。このマルウェアは、フィッシング詐欺のメールを利用して配布されています。悪意のあるスパイウェアは、ユーザーの機密情報（連絡先、通話履歴、SMS メッセージ、インストールされたアプリ、位置情報）を大量に収集し、攻撃者のサーバーにアップロードします。

標的をあまり絞っていないトロイの木馬型のアプリとして、Android/BadNews.A があります。このバックドア型のトロイの木馬は、広告付きの合法的なゲームアプリを装いますが、実際はユーザーの機密情報を収集して攻撃者に送信します。また、偽のニュースの見出しを表示する機能も搭載しています。

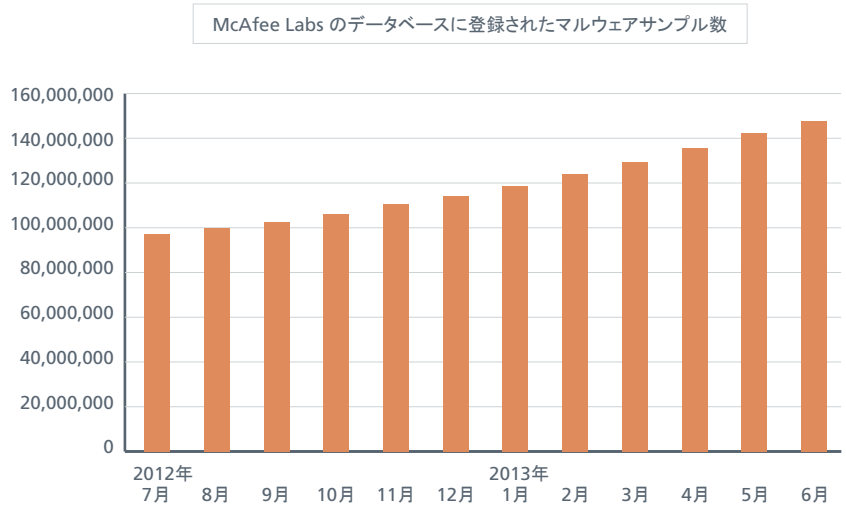
モバイルスパイウェア

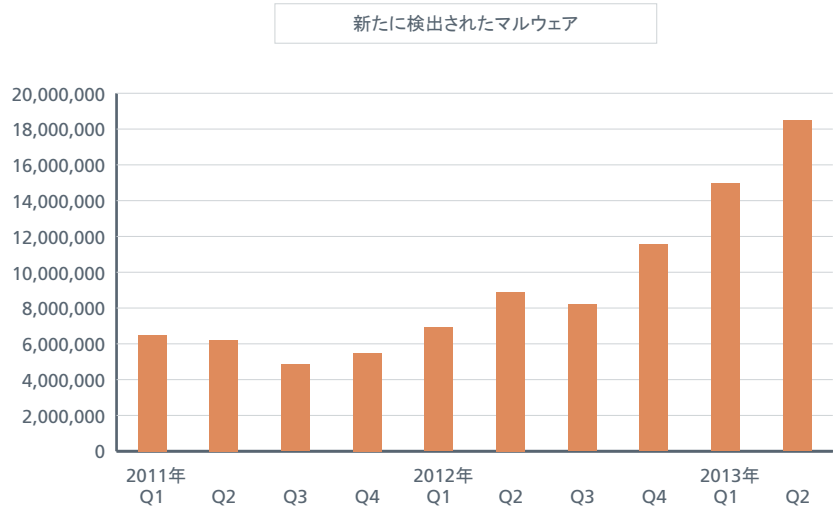
広告を表示するスパイウェアは、前四半期からわずかに増加が見られました。Android./Fzw.A は、攻撃者の Web サイトからスパイウェアをダウンロードします。正体を偽って侵入する他のトロイの木馬と同様、合法的なフォントインストールアプリを装います。ダウンロードされたスパイウェアは SMS メッセージ、通話履歴、位置情報を攻撃者のサーバーに転送します。

Android/Roidsec.A は、ユーザーの電話向けの同期ソフトウェアを装いますが、実際にはユーザーの機密情報と SMS メッセージを攻撃者のサーバーと同期します。このマルウェアは、位置情報、通話履歴、電話のハードウェアに関するデータを収集し、さらには通話を記録する場合もあります。

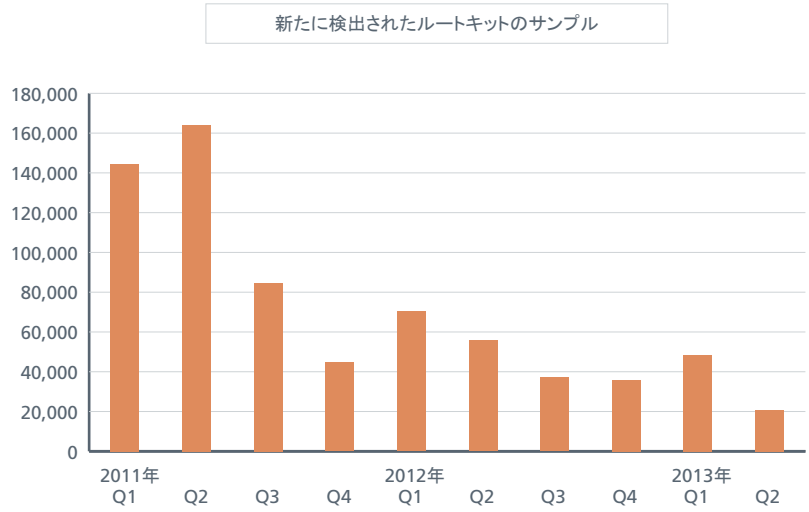
全般的なマルウェアの脅威

マルウェアは、着々と増加し、収まるような兆候が全く見られません。この 3 つの四半期の間に急増しており、この四半期の終わりには、マルウェア「zoo」のサンプル数は 1 億 4,700 万を超えました。

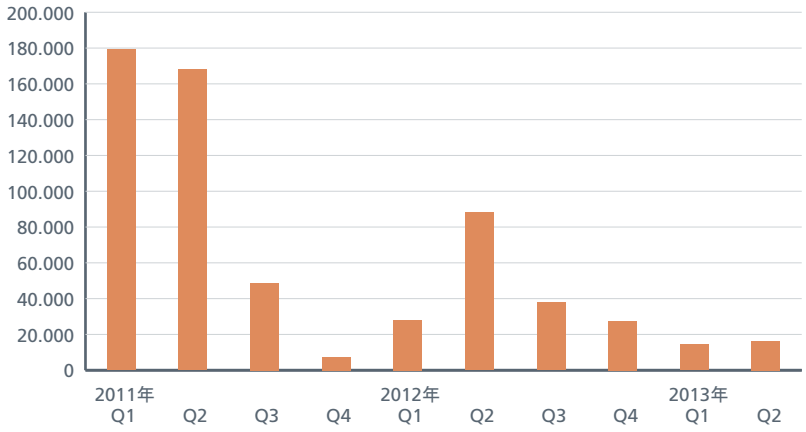




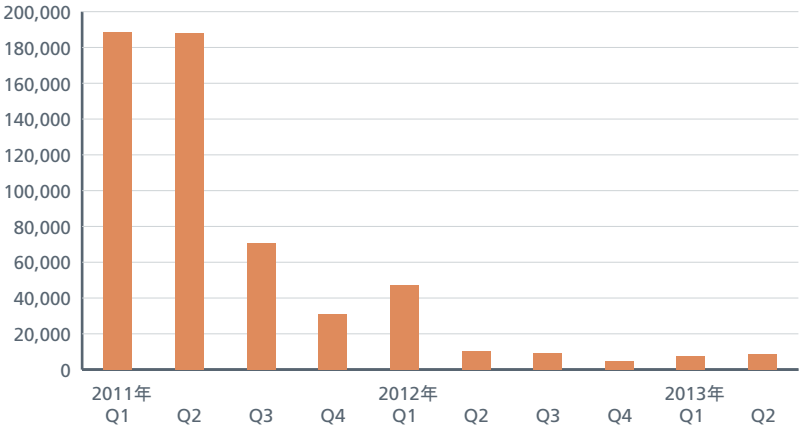
ルートキットやステルスマルウェアは、検出を回避して長期に渡ってシステムに留まるように設計されています。新たなルートキットサンプルの増加は、2011 年半ば以降減少傾向にあります。このレポートで取り上げた 3 種類のルートキットすべてにこうした傾向が当てはまります。



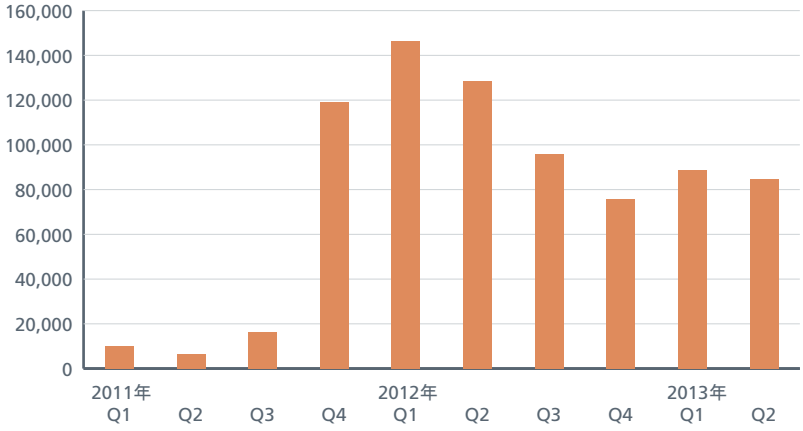
新たに検出されたKoutodoorのサンプル



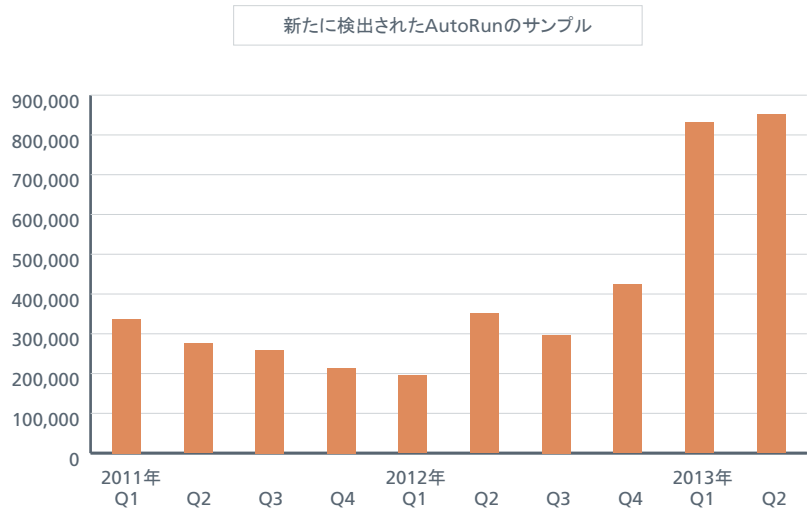
新たに検出されたTDSSのサンプル

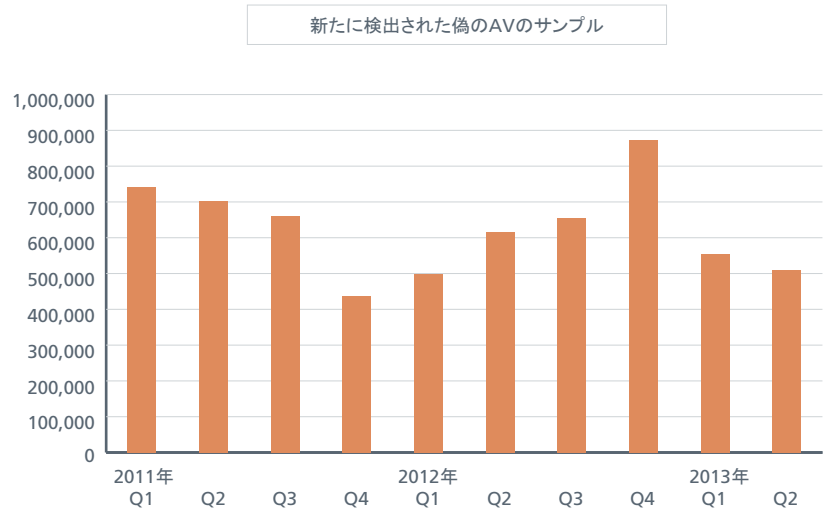


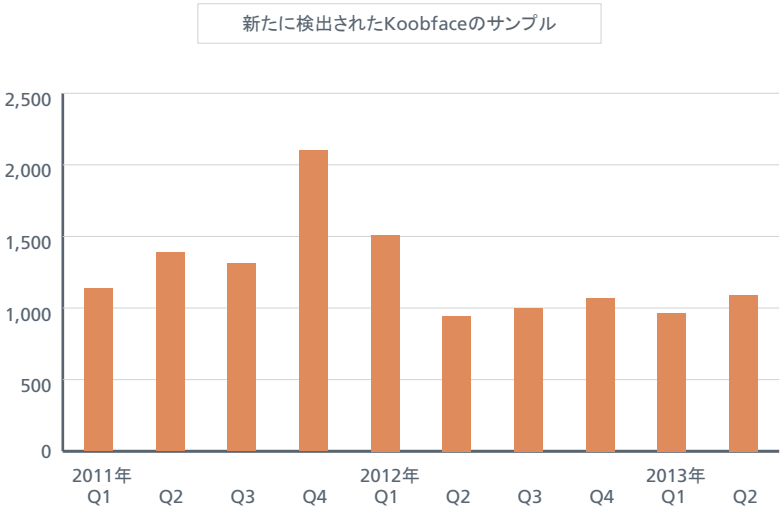
新たに検出されたZeroAccessのサンプル

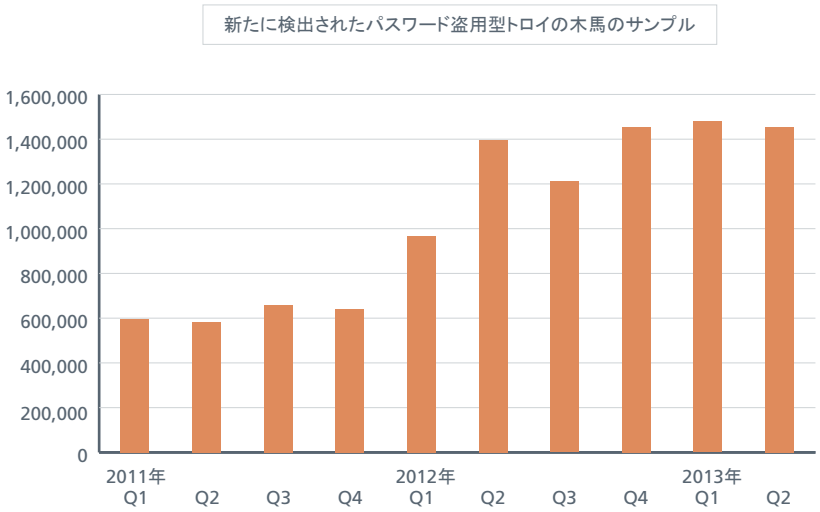


AutoRun マルウェアは、多くの場合、USB ドライブに潜んでおり、攻撃者のシステムコントロール可能にします。その数は今年の初めから倍増し、この四半期にはさらに微増しています。システムが感染したと被害者を脅す偽のアンチウイルス製品の数は、2012 年に記録的な水準まで増加しましたが、この 2 つの四半期の間は減少しています。Facebook ユーザーを対象とした Koobface は、2009 ～ 2010 年にピークを迎えましたが、2012 年の初め以降低い水準に留まっています。被害者の銀行アカウントに侵入しようとするパスワード窃盗型のトロイの木馬の数は、前四半期に記録を更新しましたが、今期もその数字に迫っています。

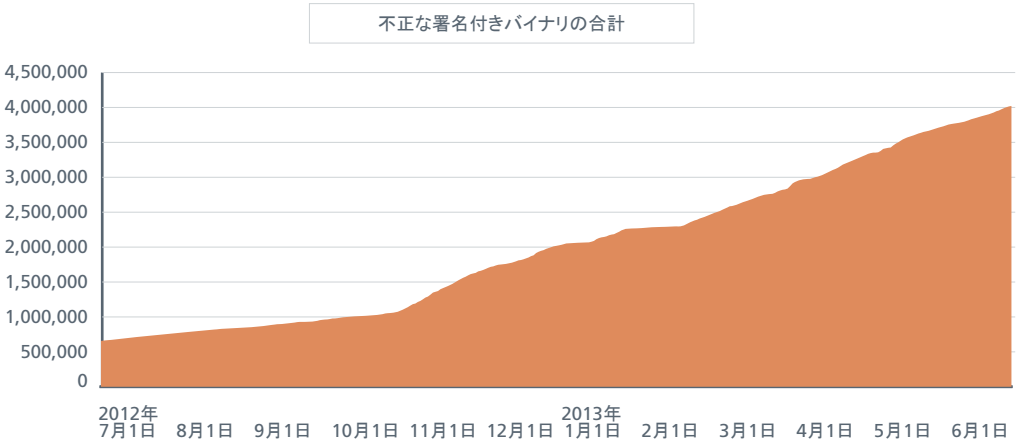


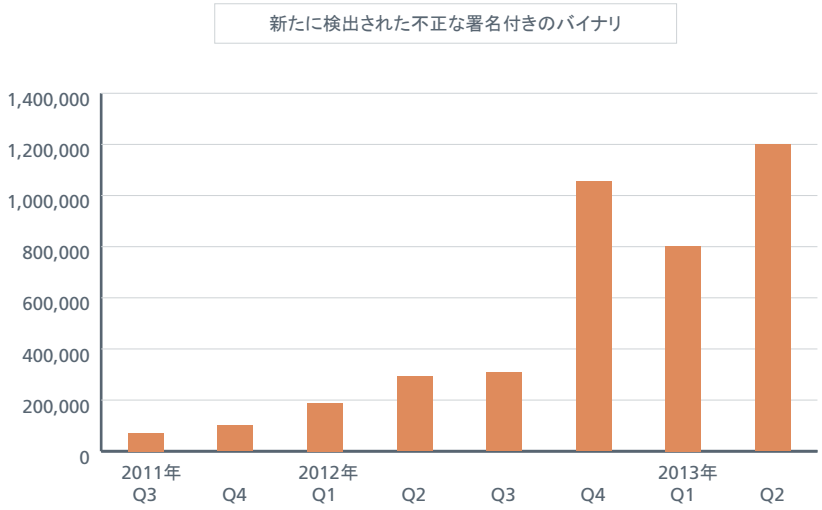




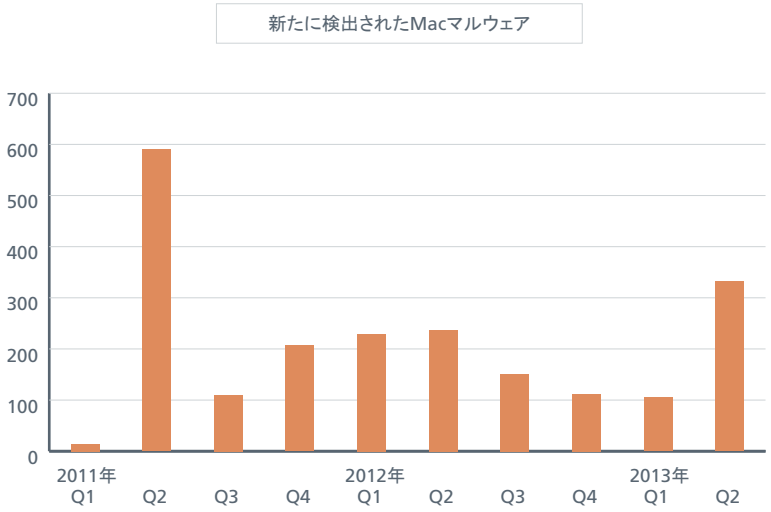


署名付きマルウェアは、第 1 四半期の減少から急増に転じて再び記録を更新し、この四半期に検出された新しいサンプル数は 120 万を超えています。

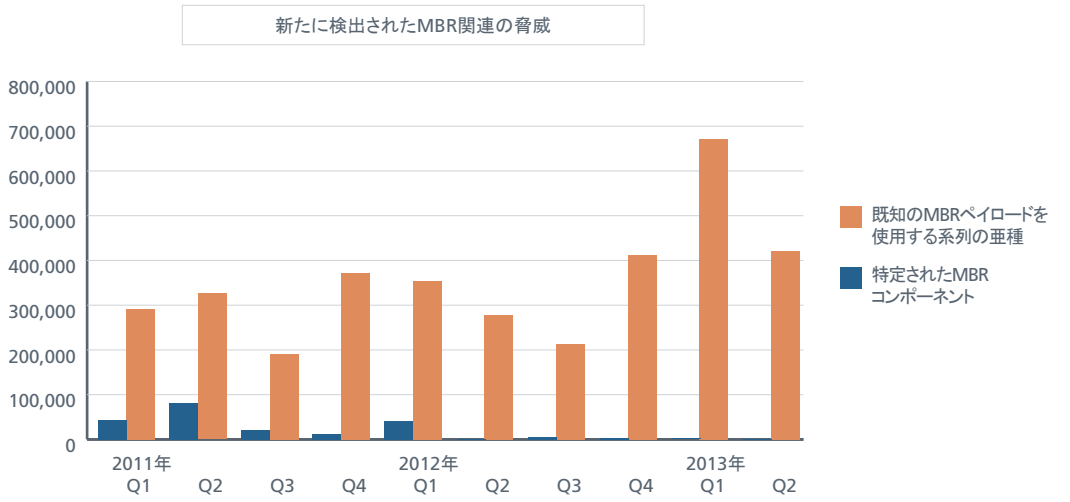




Mac を攻撃する新たなマルウェアは、前の 3 四半期の間減少した後に、3 倍以上増加しています。PC の脅威に比べて数は少ないですが、Mac ユーザーも対策が必要です。



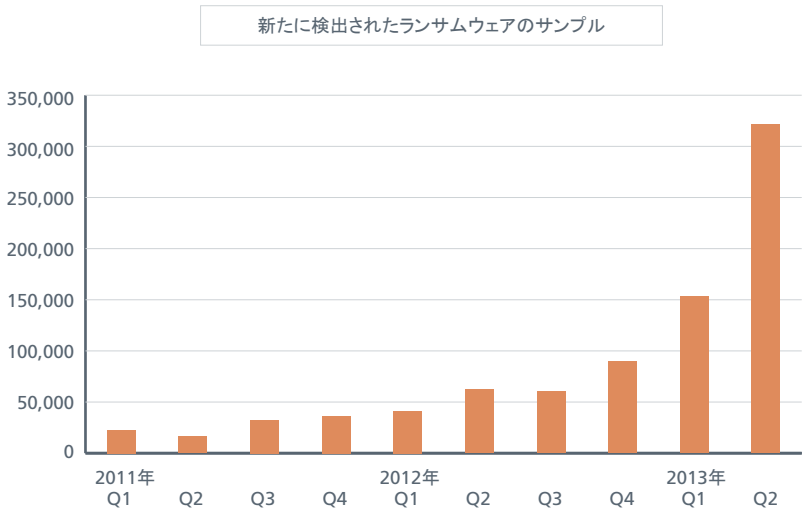
マルウェアの中には、重要なスタートアップ操作を実行する領域であるコンピューターのマスターブートレコード（MBR）を標的にする種類があります。MBR のセキュリティが侵害されると、攻撃者がコンピューターをコントロールして潜伏し、奥深くまで侵入することが可能になります。mebroot、Tidserv、Cidox、Shamoon などの攻撃は、数が急増しており、この四半期には、前四半期の記録的な水準から減少していますが、依然としてこれまでで 2 番目に多い数字となっています。



ランサムウェア

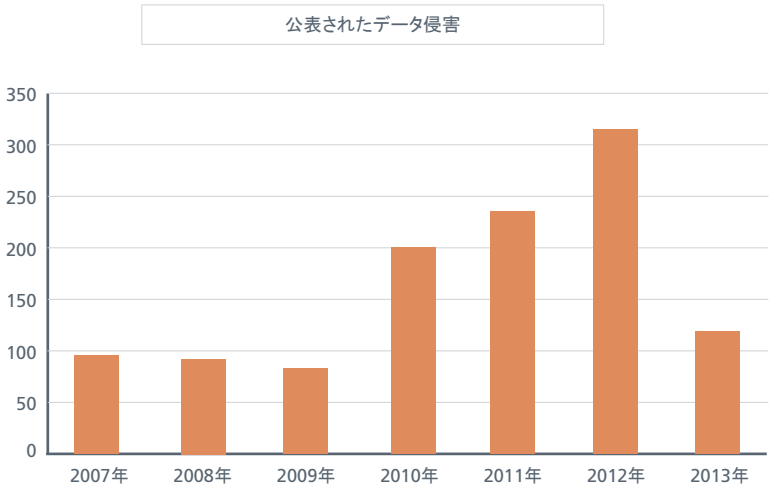
ランサムウェアは、ここ数四半期の間に深刻な問題となっており、状況は悪化し続けています。この四半期で、新たな固有のサンプル数は 32 万を超えており、第一四半期の倍以上となっており、今年上半期だけで過去 2 年間の累計数を超えるランサムウェアを分類しました。また、この傾向には、世界中の法執行機関や連邦政府機関からの警告も反映されています。

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することができるため、犯罪者にとって、極めて効果的に利益を獲得できる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いるために、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あり、そして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。こうしたメリットがある限り、ランサムウェアの問題がなくなることは当分ないと考えられます。



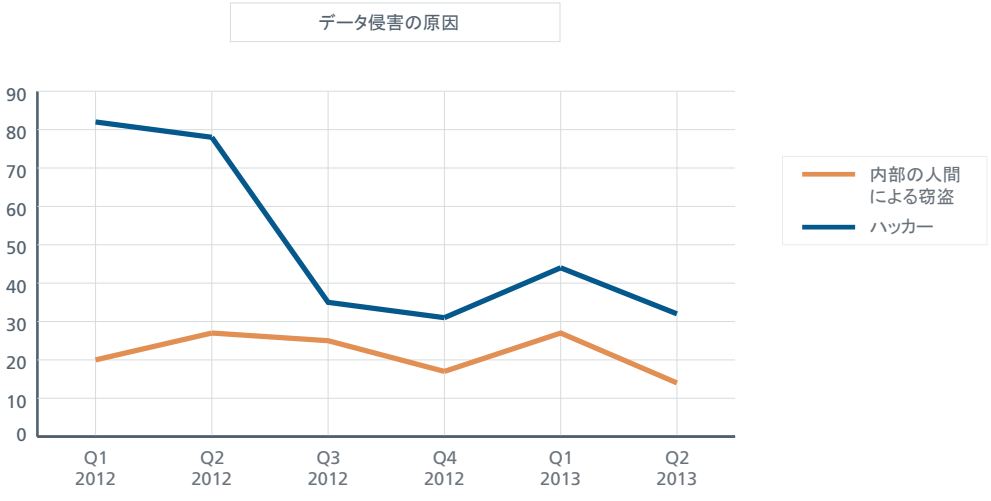
データベースの脅威

2012 年第 4 四半期の脅威レポートでは、公表されたデータベース侵害件数に関して、この期間の侵入はわずか 47 件であり、減少傾向が見られたことを報告しました。その時点では、傾向と例外のどちらを観察しているのかわかりませんでした。6 か月を経た現在、この領域の数字が安定していることを確認できました。2013 年の最初の 6 か月のデータ侵害は 119 件であり、2012 年末と同様比較的低い水準でした。この数字は、記録を更新した 2012 年のデータ侵害 315 件の 3 分の 1 をわずかに超える程度です。これが長期的な傾向なのか、嵐の前の静けさに過ぎないのかはまだわかりません。



出展: privacyrights.org

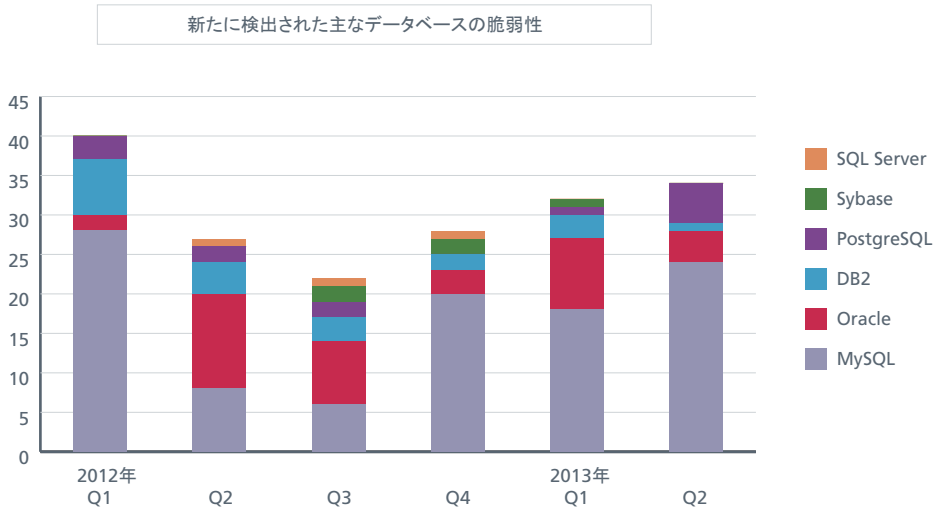
外部のハッカー（犯罪者またはそれ以外）によるデータ侵害件数の割合は、2012 年に大幅に減少しており、最近一年の間も比較的一定となっています。割合の低い企業内部の人間による窃盗も、大幅な減少はないものの、比較的一定の数値となっています。外部の人間による侵害件数の減少から、データベースセキュリティよりも周辺機器の保護に多く投資している企業や組織が想定されますが、1 ～ 2 年前よりも中規模および大規模な企業ではデータベースセキュリティへの関心が高まっていることも確認されています。



出展: privacyrights.org

上のグラフから確認できるように、ハッカーは依然として、組織内部の人間よりも多くの侵害事件を引き起こしています。しかし、データ侵害の統計データはその性質上、客観性が乏しいことに留意する必要があります。企業がデータ侵害の被害を公表するよりも、ハッカーが窃盗したデータを公表する場合が多いからです。

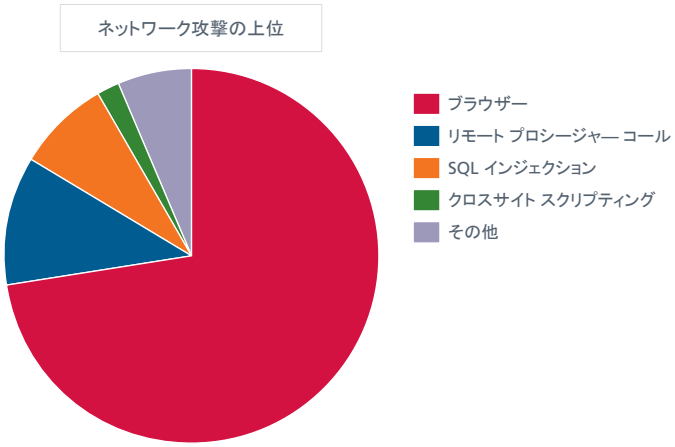
開発者または第三者から報告されたデータベースの脆弱性は、MySQL が大半を占め続けており、過去 6 つの四半期に発見されたすべての脆弱性の 60% 近くを占めています。



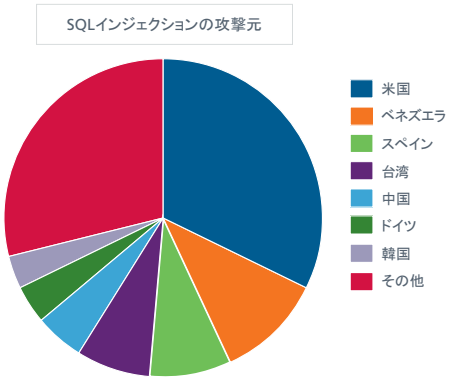
ネットワークの脅威

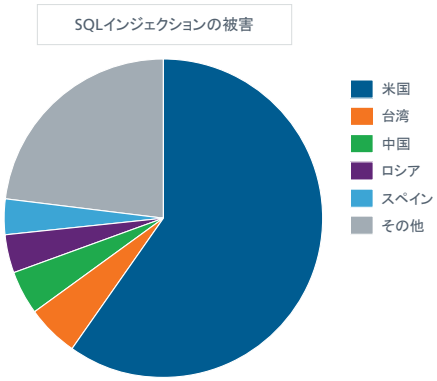
McAfee Global Threat Intelligence ネットワークによれば、例によって、米国は悪意のあるインターネット活動の大半のソースでありターゲットとなっています。ブラウザーベースの脅威は、すべてのネットワーク攻撃の中の 73% を占めており、前四半期の 44% から増加しています。以下の検出シグネチャは、マカフィー製品が最も多くブロックした攻撃の種類を示しています。

- HTTP: Microsoft JPEG Processing Buffer Overrun
- HTTP: Multiple Browser Window Injection Vulnerability
- RTSP: Apple QuickTime Overly Long Content-Type Buffer Overflow
- HTTP: Microsoft Internet Explorer CHTML Use-After-Free Remote Code Execution

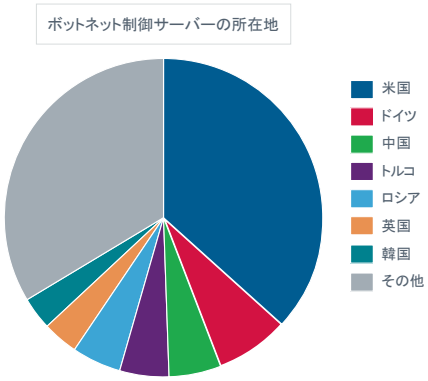


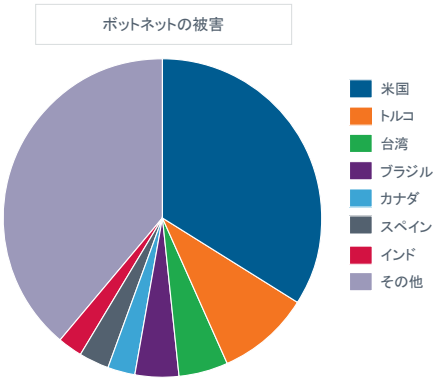
合法的な Web サイトを悪用する SQL インジェクション攻撃の加害者における、今期の米国の割合は、前四半期の 35% から、32% へとわずかに減少しました。ベネズエラは 11% で再び 2 位になりました。これらの攻撃の被害者の大半（前四半期の 55% から 60% に増加）は、米国在住です。



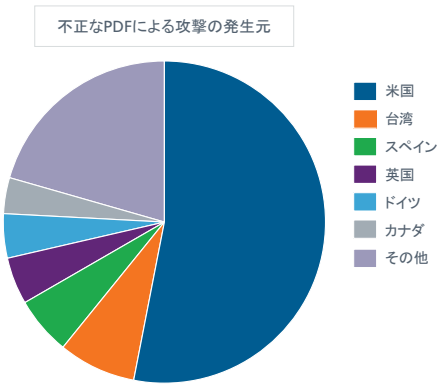


ボットネットの監視調査では、米国が再度第 1 位でした。ホストするコントロールサーバーの割合は 3% 減少し、37% になっています。ボットネットの被害者に関しては、第 1 四半期の 43% から 34% に大幅に減少しています。





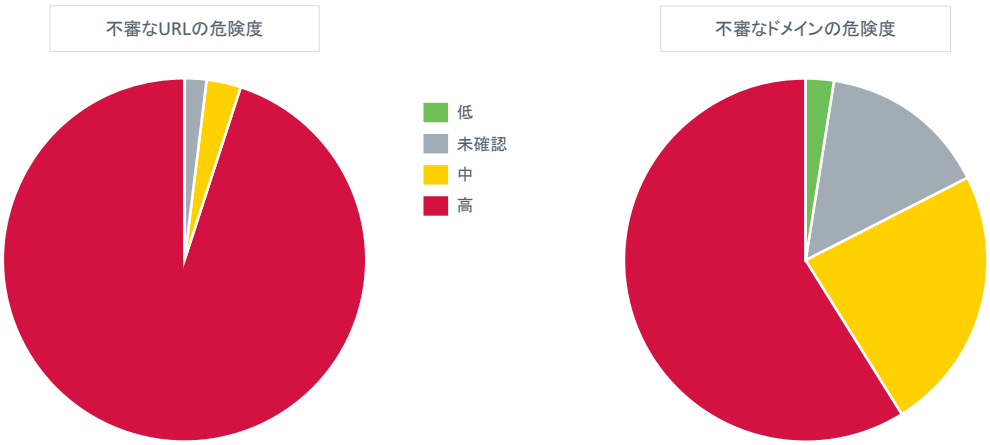
PDF ベースの攻撃のホストに関して、米国は最大の割合を占めており、前四半期の 35% に比べて、この四半期は 53% に上昇しています。台湾が 8% を占めており第 2 位です。中国は前四半期は 11% でしたが、この四半期はわずか 2% までに減少しました。



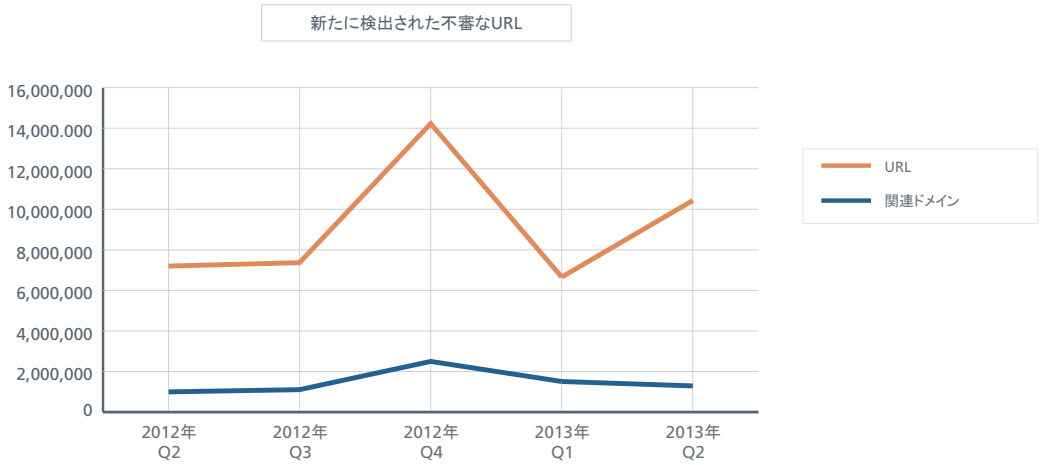
Web の脅威

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 アドレスまたは特定の URL に基づいて行われます。悪質であるという評価は、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ています。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。

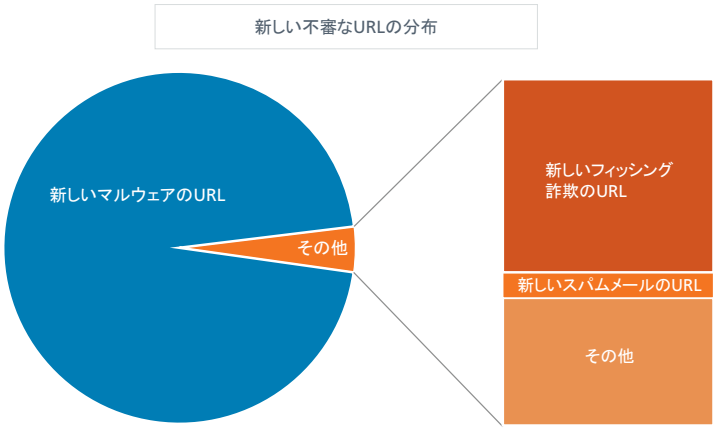
6 月末に、McAfee Labs が集計した疑わしい URL の合計数は、7,470 万を上回り、第 1 四半期と比べて 16% 増加しています。これらの URL は、2,900 万ものドメイン名を参照しており、前四半期から 5% 増加しています。



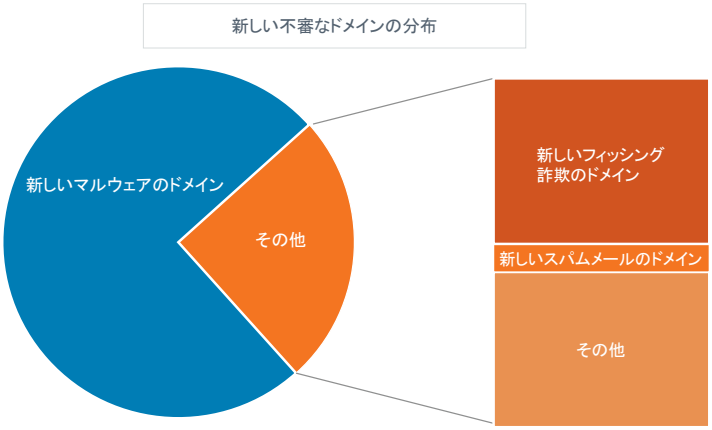
この四半期に、約 43 万のドメインに関して、1 か月あたり平均で 350 万件の新たな疑わしい URL を検出しました。



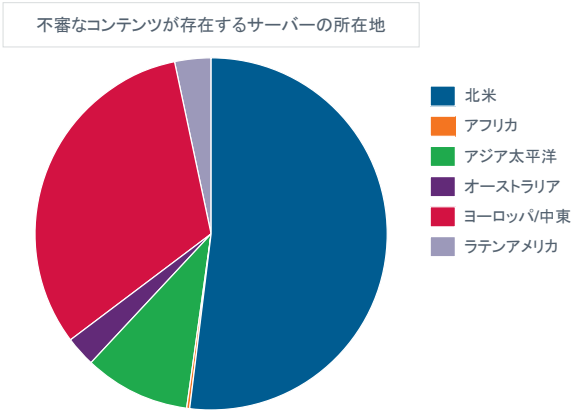
これらの疑わしい URL の大半（96%）には、マルウェアや、エクスプロイト、コンピューターのセキュリティを侵害するために設計されたコードが存在します。フィッシング詐欺とスパムの割合は、それぞれ 2.1% と 0.3% でした。



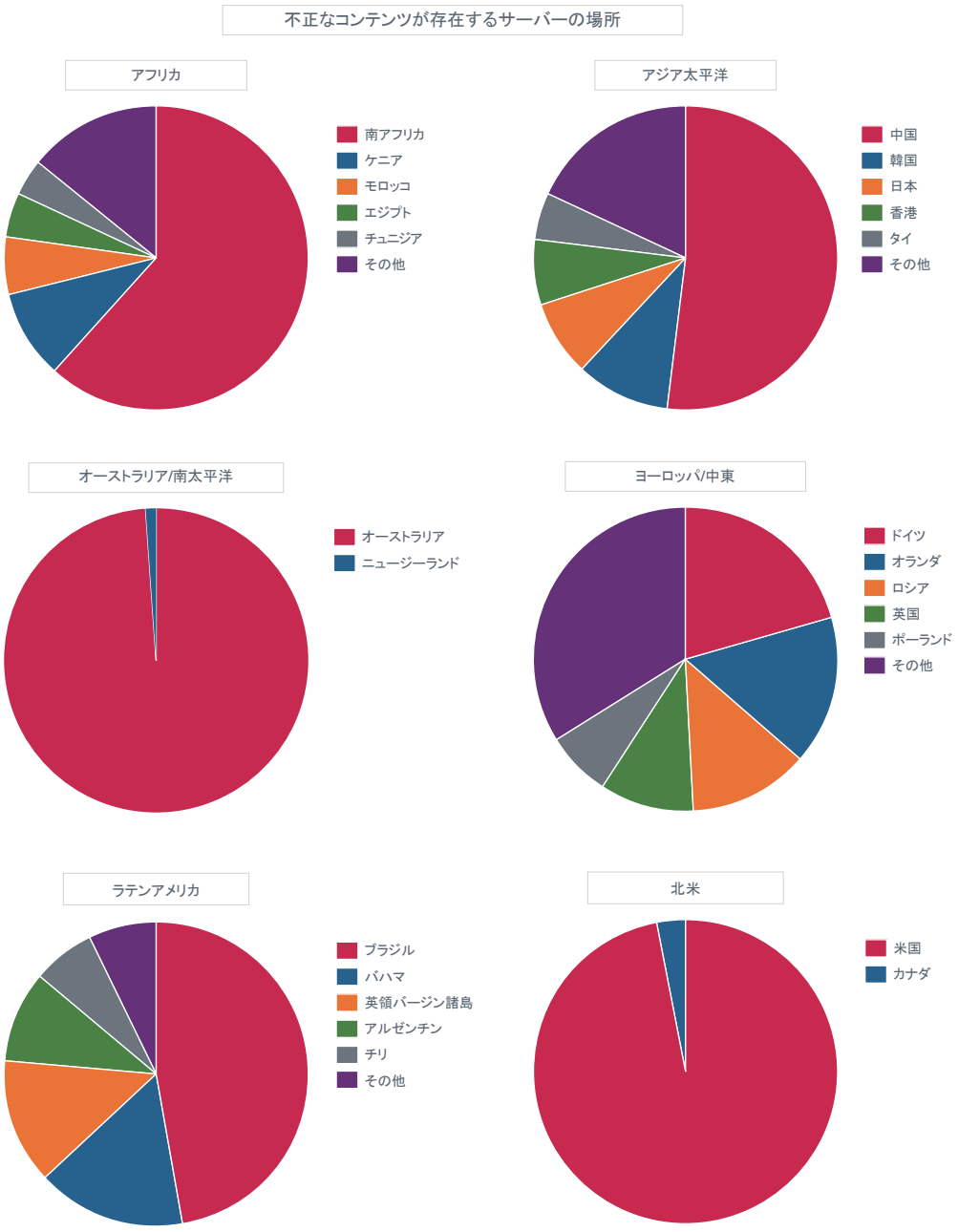
ドメインレベルの分布では、様子が異なっており、フィッシング詐欺ドメインが 12%、スパムドメインが 2% です。



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（主にドイツ）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。ただし、その勢力は、前四半期の 74% に比べると、52% に落ち込んでいます。

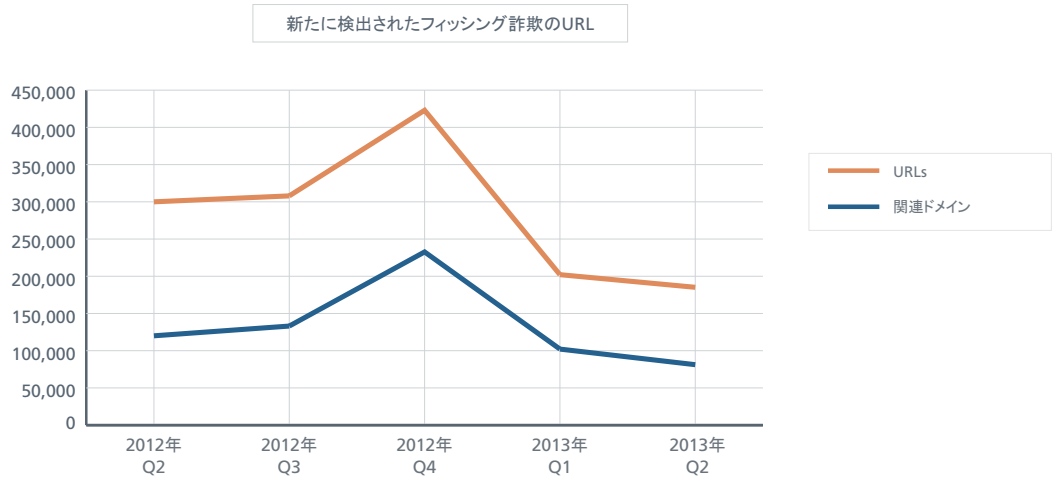


他の国々の悪質なコンテンツをホスティングしているサーバーの場所を詳しく見ていくと、非常に多様であることがわかります。それぞれの地域では、1 ～ 2 カ国が大部分を占めています。

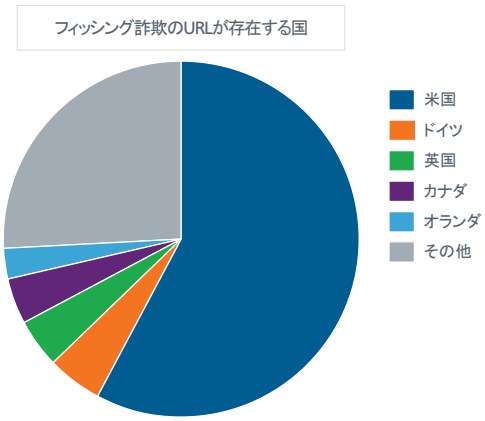


フィッシング詐欺

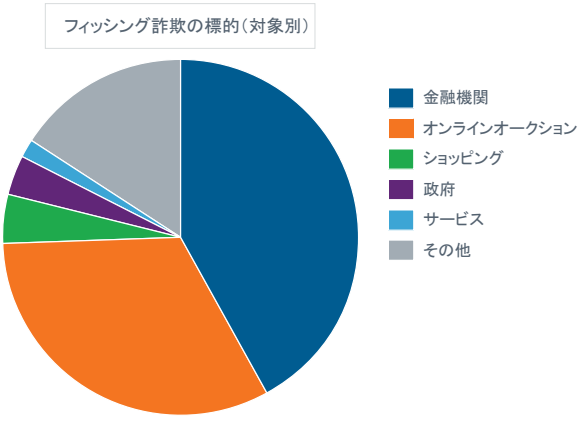
新たなフィッシング詐欺の URL 数は、2012 年第 4 四半期にピークを迎えた後に激減しました。この四半期も若干減少しています。



こうした URL の大半は、米国に存在しています。



米国の企業が最大の標的となっており、全攻撃の 67% を占めています。英国とオーストラリアがそれぞれ、6% と 3% で後に続いています。フィッシング詐欺が標的としている主要な業界の上位 5 つは、金融（攻撃の 42%）オンラインオークション（32%）、政府、ショッピング、サービスです。

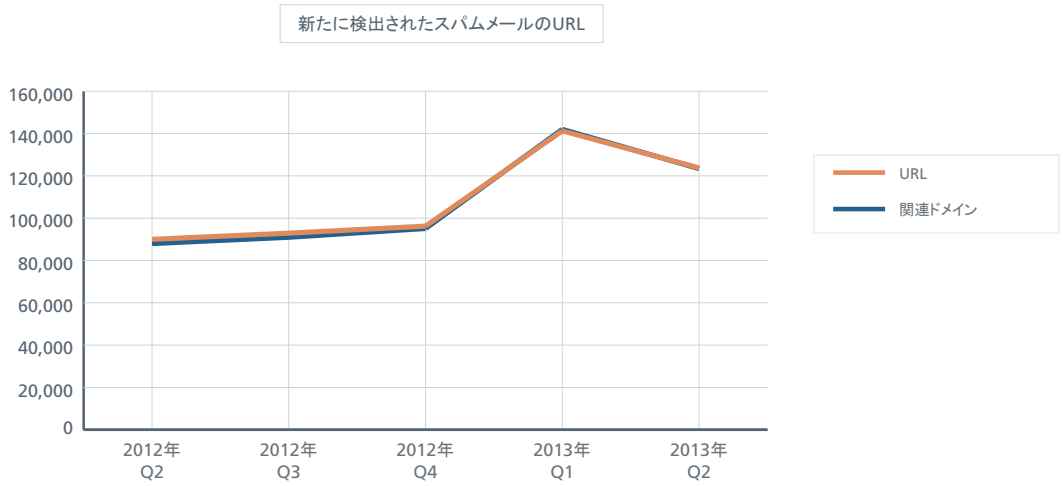


米国の企業が最大の標的となっており、英国とオーストラリアがその後に続いています。

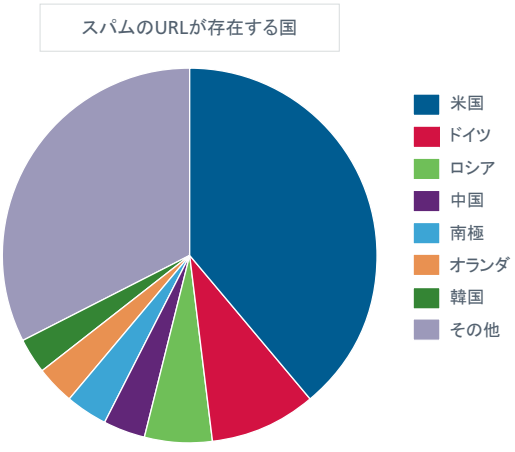
米国	英国	オーストラリア	カナダ	インド
Amazon	Barclays	ANZ (オーストラリア・ニュージーランド銀行)	Capital One	HDFC Bank
American Express	HM Revenue & Customs	Westpac Bank	Royal Bank of Canada	ICICI Bank
Deloitte	HSBC		TD Bank Group	
eBay	Lloyds TSB			
JPMorgan Chase	Natwest			
PayPal	Santander			
Wells Fargo				

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。

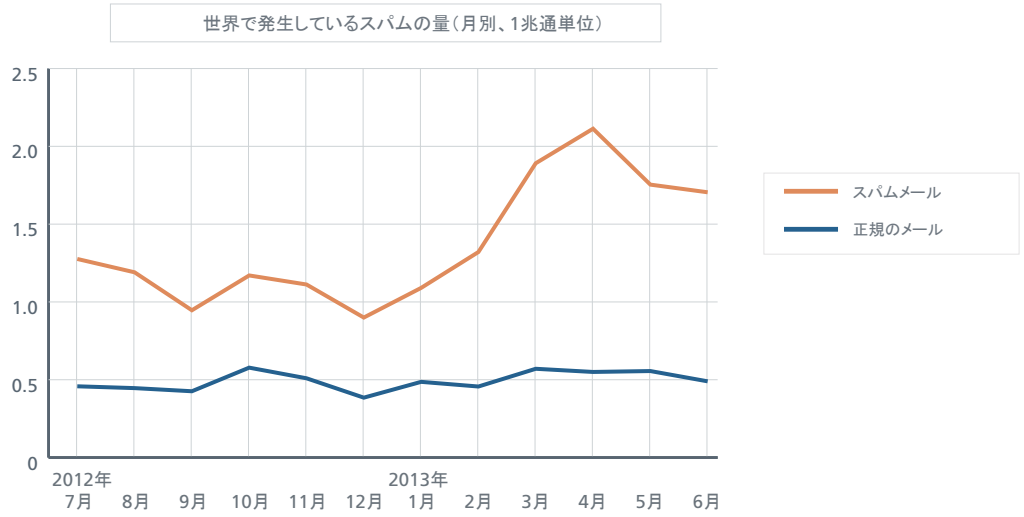


こうした URL をホスティングしている主要な国は、米国（全体の 39%）であり、ドイツ（9%）、ロシア（6%）が後に続いています。



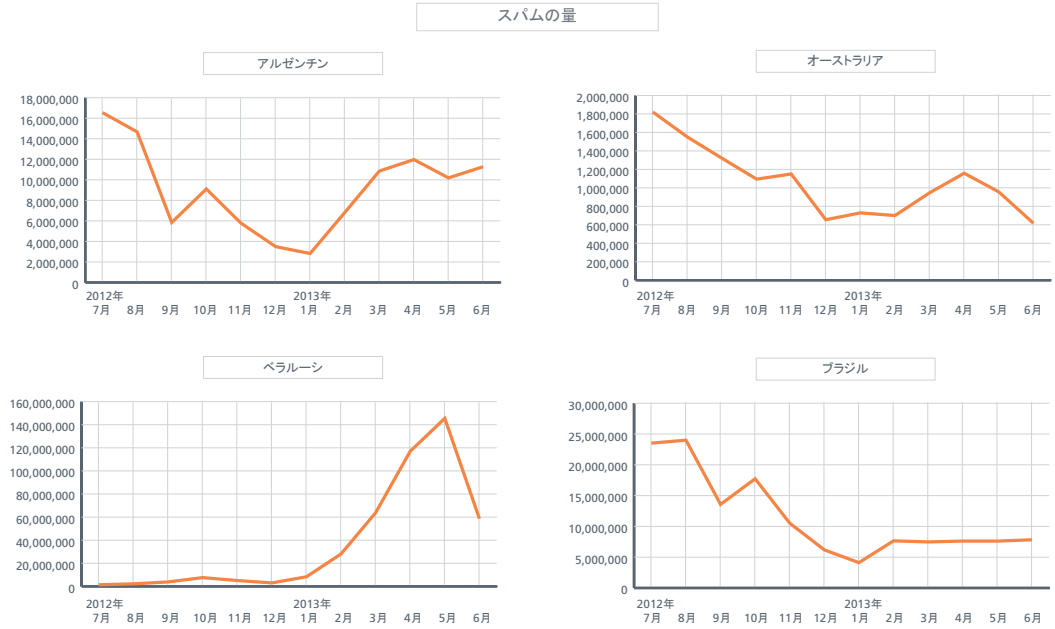
メッセージングの脅威

4 月に、スパムの量は 2 兆件を上回りました。これは、2010 年 12 月以降で最も高い数字です。5 月と 6 月には若干減少しましたが、それでもなお 2011 年 5 月以降のどの時期よりも高い数字となりました。



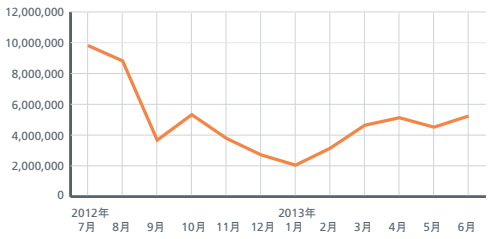
スパムの量

国別の統計を調べると、四半期ごとに大きな違いが見られます。最も印象的な例はウクライナとベラルーシで、それぞれこの期間で 200% 以上増加しています。日本は 142% 増加しました。その一方で、パキスタン（59% 減）とルーマニア（56% 減）は激減しました。フランスは 25% 減少し、米国は 16% 減少しました。

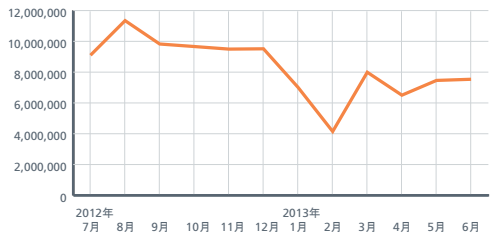


スパムの量

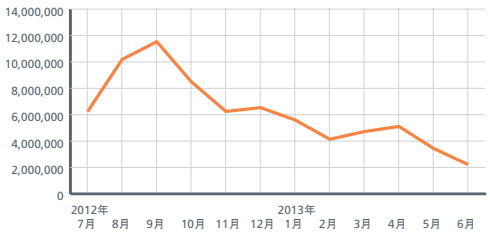
チリ



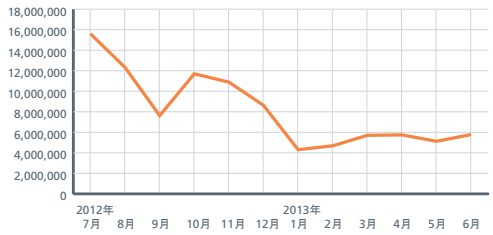
中国



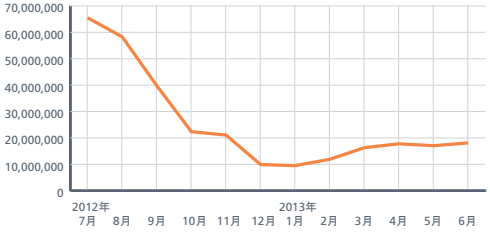
フランス



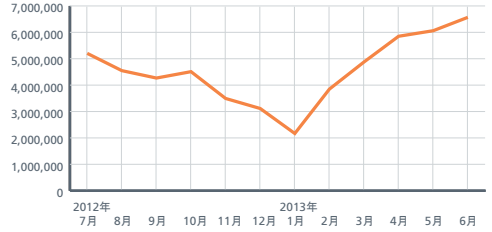
ドイツ



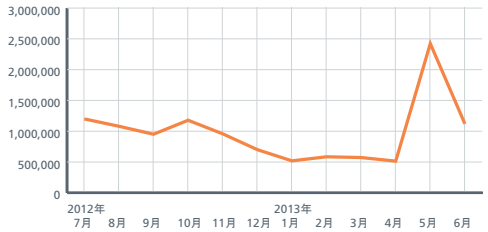
インド



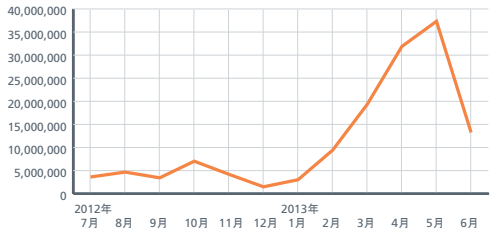
イタリア



日本

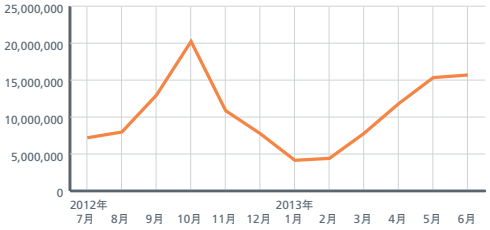


カザフスタン

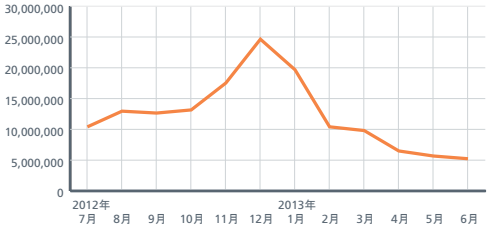


スパムの量

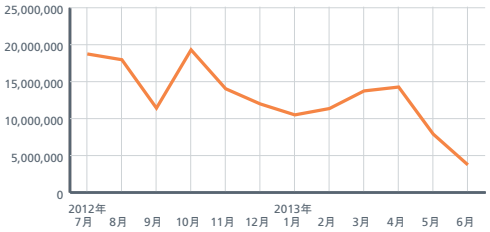
ペルー



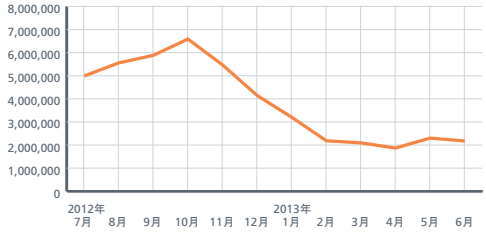
ルーマニア



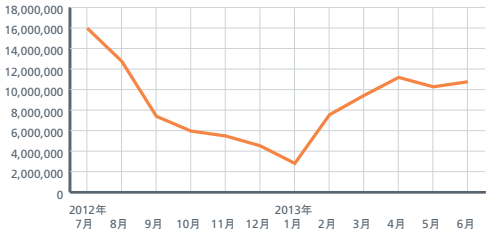
ロシア



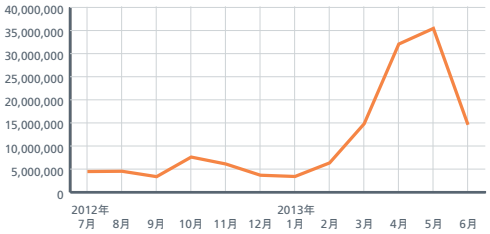
韓国



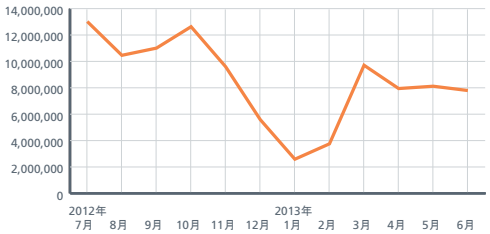
スペイン



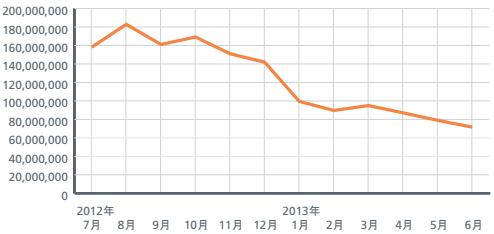
ウクライナ



英国

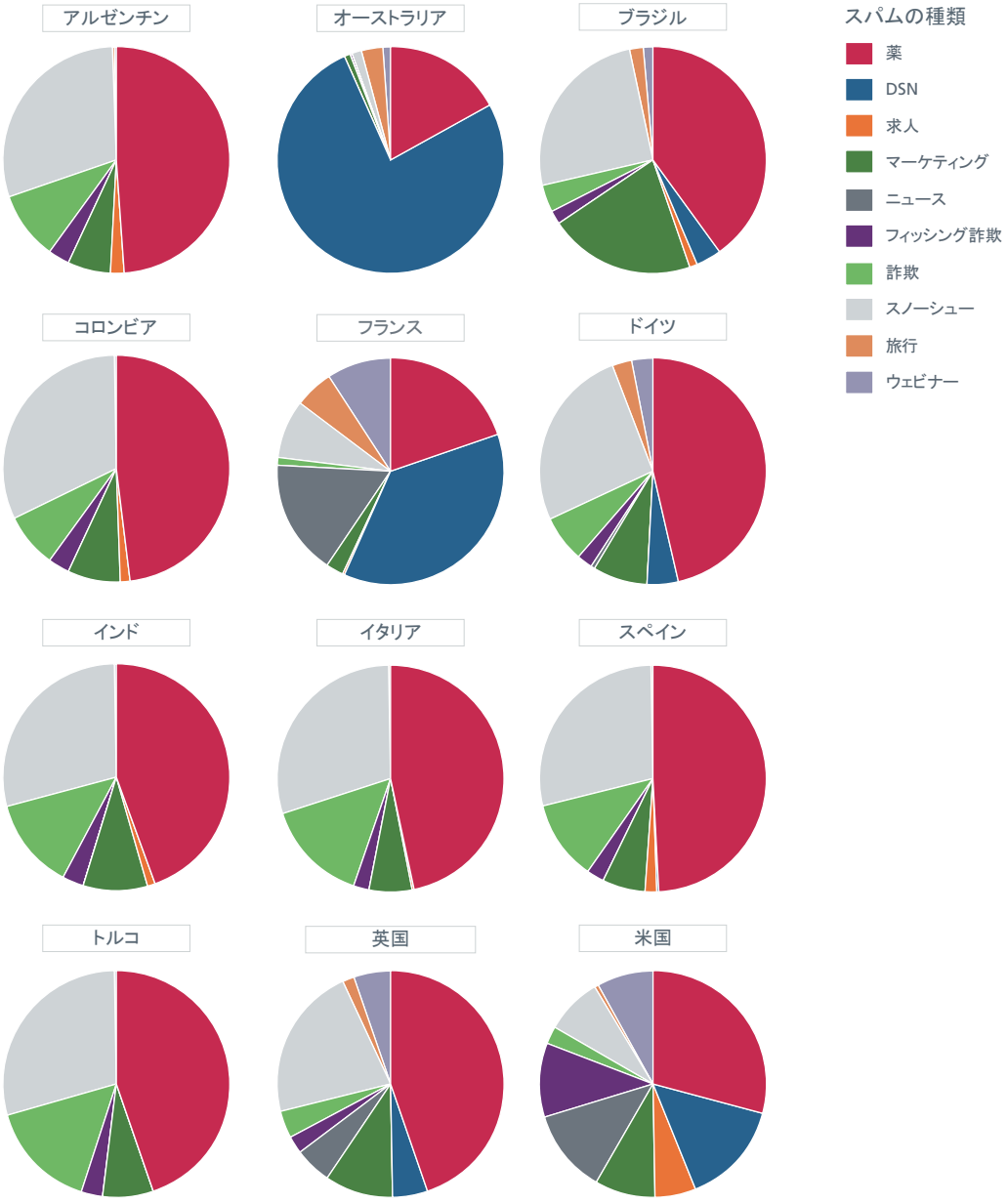


米国



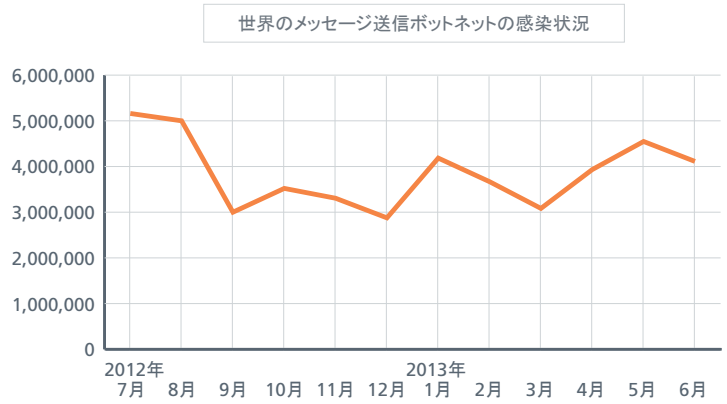
ドラッグ、DSN、スノーシュー

世界中のスパムの件名を調べると、ドラッグの人気は衰えていないことがわかります。このレポートで取り上げた国々では、ドラッグは主要なスパム件名のうちの少なくとも 17% から 50% 以上を占めています。オーストラリア、フランス、米国では、DSN（配信通知サービス）スパムの人気が続いています。多くの国々で、「スノーシュー」スパムは主要な件名の少なくとも 4 分の 1 を占めています。スノーシュースパムは、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ます。この四半期のスパムの多くに、ボストンマラソン爆発事件に関連する件名が含まれていました。こうしたメッセージの大半にはマルウェアへのリンクが含まれていました。時計などの模造品に関するスパムが比較的少なかったことは驚きでした。こうした件名は長年人気があったからです。なくなることはありませんが、数が激減していることは確実です。

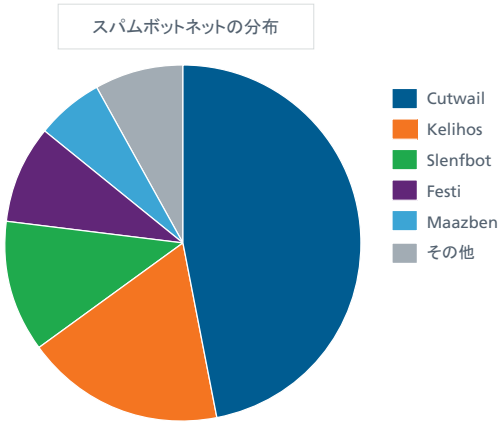


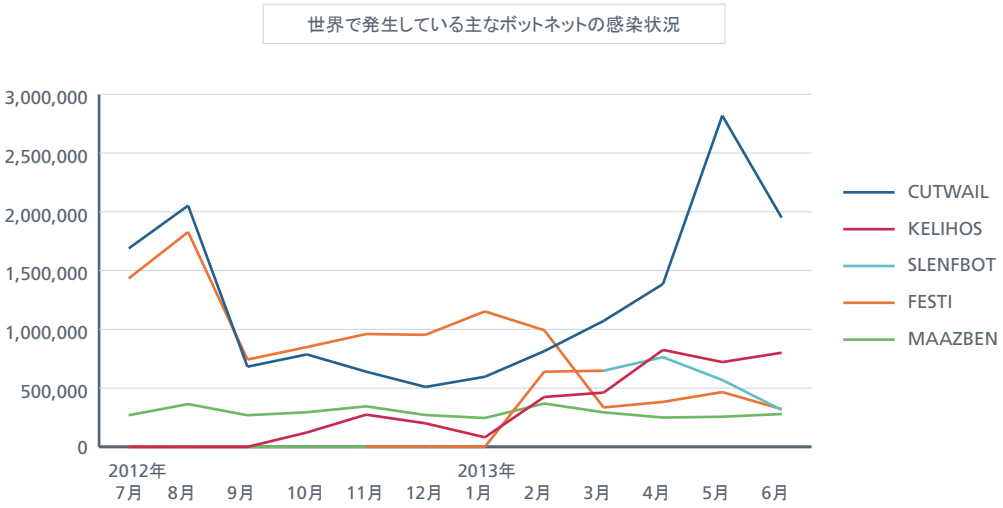
ボットネットの詳細

スパムを世界規模で拡散する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が、この四半期は再び上昇傾向でした。



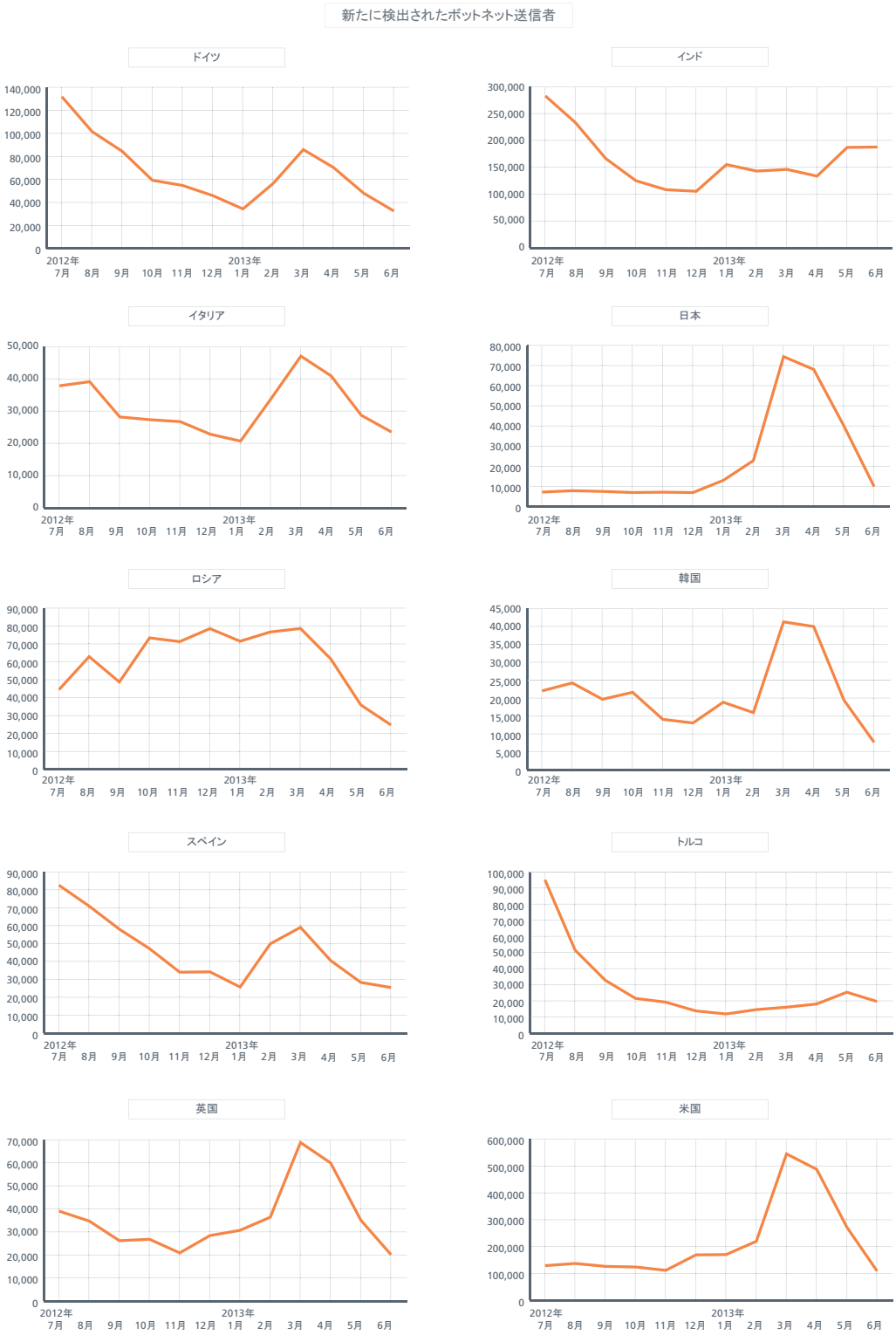
Cutwail は第 1 位の座を維持しているボットネットであり、この四半期の新たな感染数は 600 万台以上です。Kelihos は大きく差をつけられて第 2 位でした。感染数は 230 万台です。前四半期から新しく登場した Slenfbot の感染数は 160 万台です。





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、前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。例えば、ペルーではボットネットの送信者数は 300% 近く増加しました。グラフで取り上げた国の中では、インドが 14% 増加しました。また、ベラルーシは 66%、ロシアは 46%、中国は 31%、それぞれ減少しています。

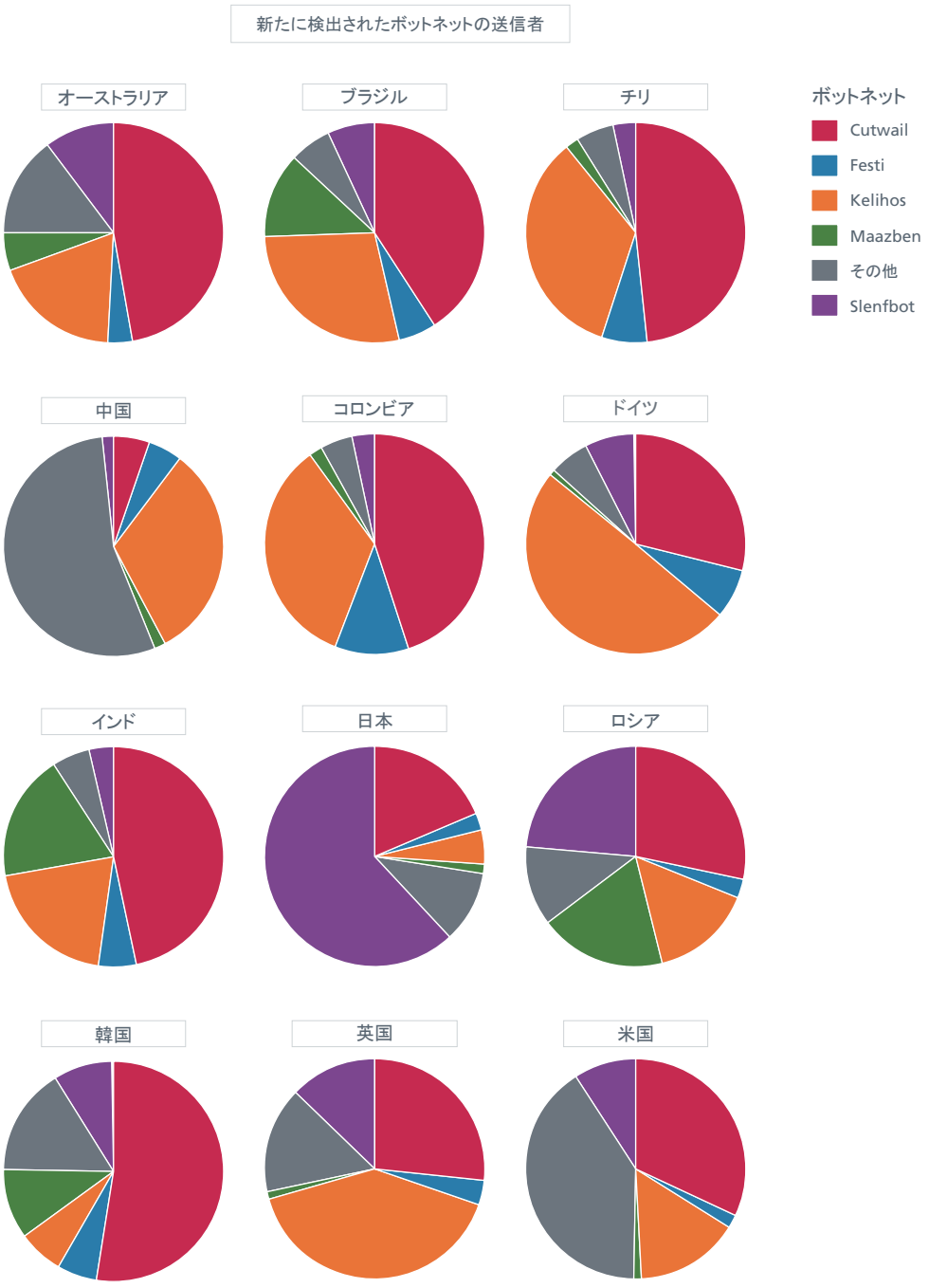

新たに検出されたボットネット送信者
ドイツ
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
2012年
7月 8月 9月 10月 11月 12月
2013年
1月 2月 3月 4月 5月 6月
インド
300,000
250,000
200,000
150,000
100,000
50,000
0
イタリア
50,000
40,000
30,000
20,000
10,000
0
日本
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
ロシア
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
韓国
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
スペイン
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
トルコ
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
英国
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
米国
600,000
500,000
400,000
300,000
200,000
100,000
0

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、最も蔓延しているボットネットファミリーが、世界中の様々な国に存在していることがわかります。Cutwail と Kelihos 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。

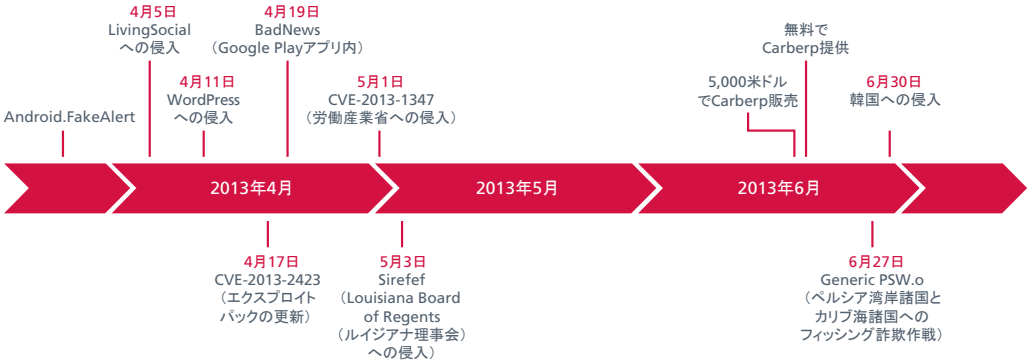
- Darkmailer（ベラルーシ、カザフスタン、パキスタン、インドネシア）
- Cutwail（ギリシャ、ベトナム、イラン（60% 以上））
- Slenfbot（ベラルーシ（81%））
- Slenfbot（日本、ウクライナ）
- Kelihos（ドイツ、イタリア、アルゼンチン、英国（40% 以上））

これらの差異は、国ごとに固有の攻撃者が存在している可能性があることを示しています。



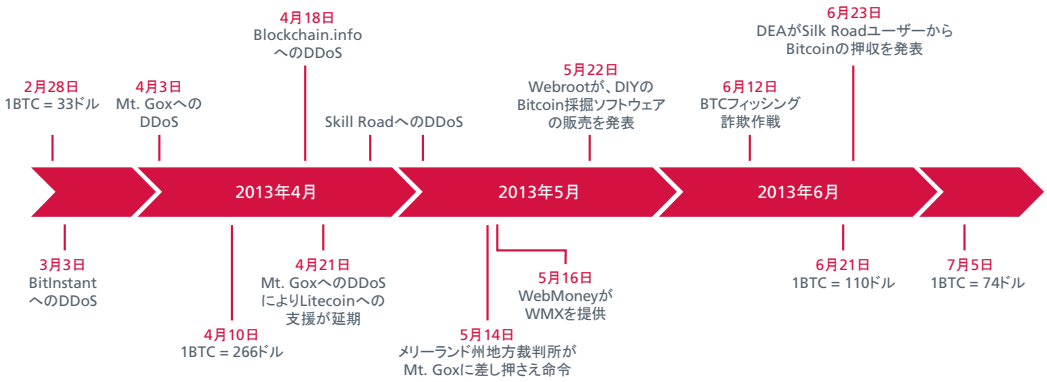
サイバー犯罪者

マルウェア、脆弱性、ハッキング



- 6 月に、様々なセキュリティ企業から、スケアウェア Android.Fakedefender が 3 月末以降モバイル環境を通じて蔓延しているという報告がありました。Fakedefender は、感染したドライブが動作しないようにして、偽のセキュリティ警告を表示します。そして、被害者に存在しないマルウェアやセキュリティリスクを取り除くためのアプリを購入するように仕向けます。
- 4 月 5 日：Amazon が一部出資しているオンライン取引サイト、LivingSocial のコンピューターシステムに大規模なサイバー攻撃がありました。このデータ侵害によってワシントン D.C. に拠点を置く同社の 5,000 万人の顧客に影響を及ぼしました。顧客はパスワードを再設定する必要があります [2]。
- 4 月 11 日：セキュリティ企業 CloudFare は、WordPress の管理ポータルを狙ったブルートフォース攻撃について警告しました。攻撃を開始するボットネットが出現し、そして、WordPress がインストールされたマシンへの侵入や、ユーザー名「admin」を使用して何千ものパスワードを入力するために、何万もの固有の IP アドレスが記録されました [3]。
- 4 月 17 日：Java エクスプロイト CVE-2013-2423 が公開されました [4]。このエクスプロイトは、あっという間に WhiteHole、Cool、Neutrino、Styx、Sweet Orange といった様々なエクスプロイトキットに組み込まれました。
- 4 月 19 日：何百万人ものユーザーが対象となる「BadNews」：Google Play のアプリ内で蔓延しているマルウェアが発見されました [5]。
- 5 月 1 日：Invincea は、米国の労働省の Web サイトがハッキングされて、バックドア型トロイの木馬 Poison Ivy をインストールさせるために Internet Explorer のエクスプロイトの自動ダウンロードを実行するサイトに閲覧者がリダイレクトされました。中国の Deep Panda Group による仕業で、この種類の「水飲み場型」攻撃は、Microsoft の IE 8 ブラウザーに存在するパッチ未適用の未知のセキュリティバグ（CVE-2013-1347）を悪用していました [6]。
- 5 月 3 日：別の水飲み場型攻撃が Louisiana Board of Regents（ルイジアナ理事会）の Web サイトで発見されました [7]。この攻撃で、マルウェア Sirefef がまき散らされました。
- 6 月 15 日頃：銀行を狙うトロイの木馬 Carberp ツールキットが、アンダーグラウンドフォーラムを通じてわずか 5,000 米ドルで提供されていました。以前の価格は 40,000 米ドルでした [8]。数日後には、無料でダウンロード可能になりました。
- 6 月 27 日：マカフィーの Foundstone Incident Response（ファウンドストーンインシデントレスポンス）チームが、フィッシング詐欺作戦の間に送信されたマルウェア（Generic PWS.o）を 3MB 入手しました。この作戦は、アラブ首長国連邦、オマーン、バーレーン、カリブ海諸国の複数の企業や組織を標的にしていました [9]。
- 6 月 30 日：ソウル中央地方検察庁が、不正な Web サイトを運営して何百万人もの個人情報を盗むために中国在住の北朝鮮人ハッカーと協力した罪で、2 名の韓国人を起訴しました。捜査官は、被告のコンピューターから 1 億 4,000 万件もの韓国人の個人情報を発見しました。これらの情報は北朝鮮と共有されている可能性があると思われます [10]。

Bitcoin をめぐる事件



前四半期に、仮想通貨 Bitcoin（BTC）が話題になりました。2 月末に、BTC の価格は 2011 年 6 月の最高取引高を更新し、33 米ドルを超えました[11]。数日後、攻撃者によって 12,000 米ドル以上に相当する BTC を持ち去られたため、BitInstant 取引所は業務を停止せざるを得ませんでした[12]。そして、これはこの四半期に起きた事件の序章に過ぎませんでした。

4 月に、東京に拠点を置く最大の Bitcoin 取引所の Mt. Gox が、事業の混乱を招く様々な DDoS 攻撃を受けました。最初の攻撃は 4 月 3 日頃に発生しました。この当時、BTC の交換レートは 1BTC あたり 140 米ドルを超えていました[13]。4 月 10 日、価格は 266 米ドルに跳ね上がり、その翌日には 125 米ドルで取引を終了しました[14]。この価格の乱高下に強い関心が集まり、毎日 2 万ものアカウントが新たに開設されました。Mt. Gox で開設された新規ユーザーのアカウント数は、3 月全体で 60,000 であったのに対し、4 月のわずか数日間で 75,000 にまでなりました[15]。

この市場での突発的な活動は、当然のごとくあらゆる種類のサイバー犯罪者の関心を引き寄せました。彼らは、Mt. Gox に対してさらなる DDoS 攻撃を仕掛けたため、Mt. Gox は Litecoin を支援する計画を延期せざるを得ませんでした[16]。そして、Blockchain. info に対する新たな攻撃が仕掛けられました[17]。Bitcoin を電子マネーとして使用する悪名高いアンダーグラウンドのマーケットプレイスである Silk Road が、DDoS による攻撃を複数回受けました[18]。

立法議員もまた、Mt. Gox に注目しました。5 月 14 日、メリーランド州地方裁判所が、Mt. Gox の資金の差し押さえを命じました。Mt. Gox は送金企業の Dwolla と契約を結んでおり、Dwolla は、Bitcoin の取引のために米国民の資金を Mt. Gox に送金していました[19]。

5 月に、WebMoney が WMX と呼ばれる Bitcoin 建ての「財布」の提供を開始しました。Bitcoin は、WebMoney によって提供されるアドレスに送金され、財布に資金が供給されます。Bitcoin は、Bitcoin のアドレスへ引き出すことが可能です[20]。WMX の財布に保管された Bitcoin は、他の財布に送金することができます。この方法を利用して、WebMoney は、このサービスでサポートしている他の通貨に Bitcoin を交換できます。

Bitcoin のレートが上昇するにつれて、悪意のある Bitcoin 採掘者は、マルウェアに感染させることでコンピューターのリソースを利用して被害者に気付かれずに採掘することに興味を示しました。サイバー犯罪者は利益を得られますが、被害者のコンピューターの動作は低下します。例えば、5 月に、Webroot は、こうしたマルウェアをカスタマイズして購入するマーケットプレイスに関するブログを投稿しました[21]。このマルウェアは、2 月初めの数日以降に販売されました。

6 月 13 日、セキュリティ研究者の Brian Krebs 氏が、Yahoo と Bing 検索エンジンを利用して MtGox.com のアカウント所有者を標的にするフィッシング詐欺作戦について報告しました[22]。

6 月 23 日、米国の麻薬取締局（DEA）は、4 月に、ある Silk Road ユーザーから 11.02BTC を押収し、ドラッグ流通の罪で摘発したことを発表しました。押収した資金は、DEA の BTC の口座に送金されました[23]。

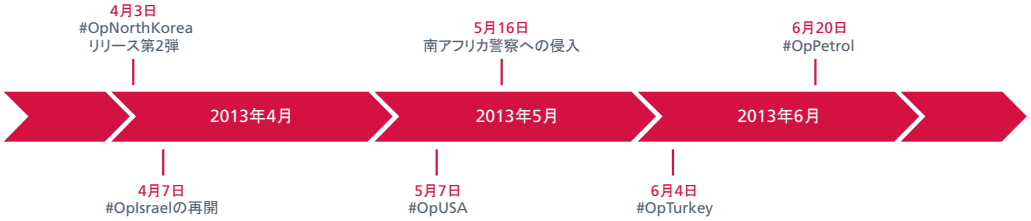
サイバー犯罪者に対する取締り

この四半期の間に、数多くの警察の捜査が実を結びました。

- 4 月、ロシア連邦保安庁（FSB）とウクライナ保安庁（SBU）は、銀行を狙ったトロイの木馬 Carberp の開発に関わった疑いのある複数の人物を逮捕したと発表しました [24]。このグループのリーダーは 28 歳のロシア人でした。25 歳から 30 歳までの約 20 名の残りのメンバーは、キエフ、ザポリージャ、リヴィウ、オデッサ、ヘルソンで逮捕されました [25]。この組織は、ウクライナとロシアだけで 2 億 5,000 万米ドル（1 億 9,300 ユーロ）の窃盗に関与していると言われていました。
- 1 月にタイで逮捕された 24 歳のアルジェリア人、Hamza Bendelladj が、4 月に米国に引き渡されました。彼は「Bx1」としても知られており、SpyEye のコンポーネントの開発を支援した共謀者として、ジョージア州北地区の起訴状に名前を連ねていました。トロイの木馬「SpyEye」の作者と推定される彼のパートナーは、アンダーグラウンドでは「Gribodemon」や「Harderman」として知られています。その実名については、まだ逮捕されていなかったため、起訴状には記載されていませんでした [26]。
- 5 月 9 日、連邦検事は、世界中の銀行から 4,500 万米ドルを盗んだ罪で、国際的なサイバー窃盗組織とつながりのある 8 名のニューヨーク市民に対して起訴を申し立てました。訴えられた容疑者は、アラブ首長国連邦に拠点のある RAKABANK（National Bank of Ras Al-Khaimah PSC）や、オマーンの Bank of Muscat（マスカット銀行）から発行された MasterCard のプリペイド式デビットカードを利用していました。被告は、昨年 12 月と今年 2 月に 2 回の個別の攻撃によって、ニューヨークの銀行から 280 万米ドルを引き出しました [27]。この 8 名がニューヨークの銀行から資金を引き出している間に、別の共謀者達が、世界中の他の銀行から 4,200 万米ドル以上を引き出しました。
- 5 月に、米国でデジタル通貨システム Liberty Reserve の創業者と他 6 名が、60 億米ドルのマネーロンダリングを計画した罪で起訴されました [28]。この通貨システムの創業者であり、ウクライナ出身のコスタリカ人の Arthur Budovsk は、スペインで逮捕され、他のメンバーは、コスタリカとニューヨークで逮捕されました。AP 通信によると、コスタリカ警察は、Liberty Reserve と関係のある家宅 3 か所と事業所 5 か所を強制捜査しました。このデジタル通貨のサイトは現在オフラインになっており、トップページには、このドメインは United States Global Illicit Financial Team（米連邦グローバルイリシットフィナンシャルチーム）によって差し押さえられたと通知が表示されています。
- 2006 年にコスタリカで設立された Liberty Reserve は、米国内に少なくとも 20 万の顧客がいます。サイバー犯罪者を支援する事業内容の疑いがあったため、米国では送金サービスとして登録することができませんでした。6 月 4 日、同様の方法で電子マネー取引所 WM Center が、米国政府により差し押さえられ、閉鎖させられました [29]。
- 6 月 5 日、米国連邦保安官の同行のもとで、Microsoft の技術者が、ニュージャージーとペンシルベニアにある 2 つのデータセンターのサーバーを押収しました。そして、FBI の支援を受け、87 ヶ国のコンピューター緊急応答チームと登録機関と連携して、マルウェア Citadel で作成された 1,452 のボットネットを使用しているドメインをシンクホールに捕捉しました [30]。一部のセキュリティ研究者からは、追跡中であった悪意のあるデータが取り出されたことで、現在行っているセキュリティ研究の成果が台無しになったとして、この作戦を批判する声がありました [31] が、その一方、今回の個別の解体作業による長期的な影響はおそらく大したものではないという意見もありました [32]。
- 6 月に、英国の重大組織犯罪局は、ベトナムの High-Tech Crime Unit（ハイテク犯罪ユニット）、ベトナム公安省 Criminal Investigative Division（犯罪捜査局）、ロンドン警視庁サイバー犯罪合同捜査本部、および FBI からの協力を得た事件で、11 名を逮捕したと発表しました。8 名の犯罪者がベトナムで逮捕され、残りの 3 名が英国で逮捕されました。容疑者全員が、Web サイト「mattfeuter」ファミリーに関係しており、申し立てによれば、このサイトでは、約 16,000 人のメンバーが、110 万件以上のクレジットカードのデータを売買しており、全世界で 2 億米ドル相当を超える詐欺を支援しました [33]。
- 6 月に、米司法省が、ウクライナのサイバー犯罪組織のメンバー 8 名を告訴しました。申し立てによると、彼らはシティバンク銀行、JP モルガン・チェース銀行、TD Ameritrade、PayPal といった多くの金融機関や、さらには米国の Department of Defense’s Finance and Accounting Services（国防予算経理局）に対するネットワークへの不正アクセスを働いたと罪で告訴されたとのことです [34]。2012 年 3 月から 2013 年の 6 月の間、容疑者たちは、これらのサーバーに侵入し、連邦の訴状に「Sharapka Cash Out Organization」と記載された活動の一部として、合法の銀行口座から資金を横領してデビットカードに資金を供給し、ATM 経由または買い物をするふりをして口座から資金を引き出していました。
- 6 月に、フランスでは、OCLCTIC と DCP の捜査官が、金融機関へのハッキングを専門とする犯罪者集団を解体し、5 名を逮捕しました。容疑者は、オンラインショッピングによって 900 万ユーロを奪った疑いがあります。この際、合計で 27,000 人の銀行データの流用が可能でした。集められた資金は、その後ハイエンドのハードウェアの購入に使われました [35]。

ハクティビズム

この四半期の活動は、多くの陣営にハクティビストが存在し、様々なイデオロギーをサポートしていることをはっきりと示しています。



4 月 3 日、「OpNorthKorea Release #2」が Pastebin で発表されました [36]。北朝鮮の最高指導者である金正恩の退位、核武装政策の放棄、国民が自由かつ無検閲でインターネットにアクセスする権利を要求しました。この体制を支持する複数の Web サイトが（DDoS によって）ブロックまたは、1 か月に渡って改ざんされました。Anonymous から出されたと称する声明では、北朝鮮のプロパガンダサイト「uriminzokkiri.com」でホストされている 15,000 人のユーザー記録を入手したとの発表がありました。しかしながら、一方が声明を出すと、もう一方から反応が返ってくるようです。6 月の最終週、北朝鮮と韓国の両方の政府の Web サイトが、Anonymous の名前の下での活動を主張する攻撃者の標的となりました（いわゆる公式の Anonymous チャンネルは、ツイートを通じて、韓国の攻撃への関与を否定しています）。一部の研究者は、この攻撃者は、グループのシンボルとして頭蓋骨と銃弾を使うことの多い北朝鮮の「Whois Team」ではないかと疑っています（この攻撃に関する詳細については 4 ページの「オペレーショントロイ」を参照してください）。

前四半期の脅威レポートで取り上げた #OpIsrael の後も、世界各地のおよそ 30 のハクティビスト集団が対立し続けることを選んでいます [37]。4 月 7 日、#OpIsraelReloaded が発表されました。ハッカー側は多大な損害を与えたと主張していますが、イスラエルの当局者は、攻撃による実際の損失はほとんどなかったとして、この事件は大したことではないと捉えています [38]。ハッカー Dr FreeDom は、3 万人分の Visa カードの顧客情報を漏えいさせたと主張しています [39]。

また、こうしたハッカー行為は報復を招きました。イスラエルを支持するハッカーチーム Israel Elite Force は、専用の Web サイト上で #OpIsraelReloaded の攻撃者の疑いのある複数の人物名を公表しました。彼らの名前は、ヨルダン、インド、レバノンの出身者でした。別のイスラエル支持者は、Anonymous の #OpIsrael の Web サイトを改ざんしました [40]。

米国および他の西側諸国に対する攻撃が、#OpUSA（5 月 7 ～ 9 日）と #OpPetrol（6 月 20 日）という作戦名で開始されました [41]。これらの作戦は、Anonymous の名前の下で開始したように見えますが、攻撃者のシグネチャを調べたところ、自由主義への反対活動を展開している中東および北アフリカ出身のハッカーグループが大半であったことが明らかになりました。

これらの活動の多くは、ジハードをテーマに掲げることを好むハッカーチーム AnonGhost と関わりがあります。あらゆる種類の中東の同調者が Anonymous の名前を騙って抗議活動を行っていることは明らかです。

6 月、トルコ国内での抗議活動をきっかけとして、Anonymous は、ラジオ・テレビ最高評議会（RTUK）の Web サイトへのハッキング活動、#OpTurkey を開始しました。サイバー軍も活発でした。バッシャール・アル・アサド大統領政府を支持する Syrian Electronic Army は、様々な公的なトルコの Web サイトを閉鎖させて改ざんしました [42]。2 つの集団が、トルコの首相府のネットワークに侵入し、タイイップ・エルドアン首相のスタッフのメールアドレス、パスワード、電話番号を入手しました（エルドアン首相は、シリア内戦でのアサド大統領の行動を声高に非難していました）。Crescent and Star Team という別のグループが、トルコのイシュバンクを標的としましたが、これはタクシム広場の抗議活動の支持者によるものであると言われています [43]。

これらの出来事は、ハクティビズムが拡大しており、Anonymous の名前で行われる攻撃は問題の一部にすぎないことを示しています。

南アフリカで注目を集めた doxing 作戦（個人情報の公開）では、南アフリカの警察が運営している匿名の内部告発者の Web サイトに Anonymous が侵入し、何千人ものユーザーの身元を公表し、彼らの安全を脅かした可能性があります [44]。

この四半期には司法側の活動も話題になりました。

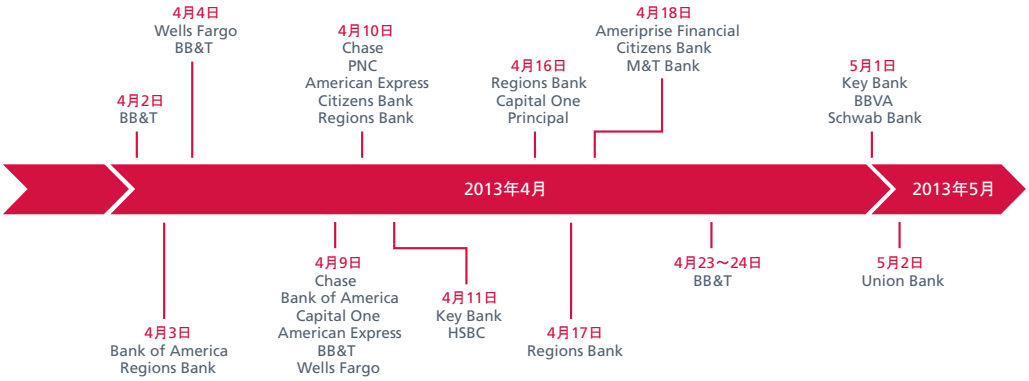
- 4 月に、チュニジア、ヨルダン、モロッコで、#OpIsrael に関連して逮捕されたハッカーに関する相反する情報が広がりました。このニュースの真偽は別として、これらの国々は彼らの「行動」に脅かされました。

- 悪名高いハッキンググギャング LulzSec のメンバーが刑務所に送られました [45]。
  - Jake Davis（別名「Topiary」）: 同組織リーダーとして 24 か月
  - Ryan Cleary（別名「Viral」）: 32 か月からその半分に減刑
  - Mustafa Al-Bassam（別名「T-Flow」）: 20 か月が 2 年間延期され、300 時間の社会奉仕活動
  - Ryan Ackroyd（別名「Kayla」）: 30 か月からその半分に減刑
- 4 月、FBI は、スチューベンヴィル強姦事件を暴露した疑いのあるハッカーの家宅捜索を行いました。KYAnonymous として知られるこの容疑者は、Anonymous の分派である KnightSec のリーダーであり、16 歳の少女を強姦した 2 名のフットボール選手に関して、スチューベンヴィルを標的とする「Operation Roll Red Roll」を実行したと言われています [46]。
- 5 月、イタリア警察は、20 歳から 34 歳の 4 名のハッカーを逮捕しました。彼らは、Anonymous ネットワークのイタリア支部の監視によって告発されています [47]。2 年間に渡る警察の捜査「Tango Down」の成果として、さらに 6 名が正式に取り調べを受けており、また、合計 10 か所の家宅捜索を行いました。

サイバー軍

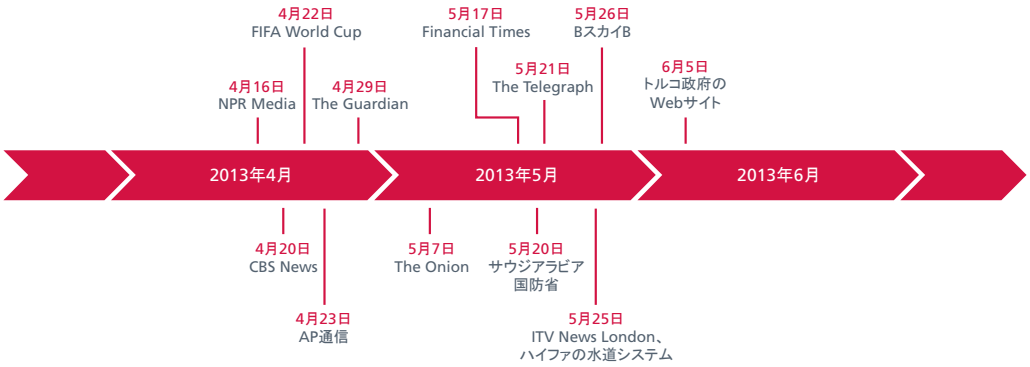
注目を集めることの多い Syrian Electronic Army と Izz ad-Din al-Qassam Cyber Fighters が、この四半期に再び話題になりました。

2012 年後半の 2 つの四半期の脅威レポートでは、2012 年に米国の銀行や金融サービス企業に対する様々なサイバー攻撃に関与したと主張しているイラン人グループ、Izz ad-Din al-Qassam Cyber Fighters を紹介しました。イランと関わりのあるこうした行動は、現在は Operation Abadil として知られています。以下の図表で示すように、彼らはこの四半期も活動を続けていました。



5 月 6 日、Cyber Fighters は、#OpUSA の妨げとならないように、攻撃を停止したと発表しました。6 月 12 日、Google は、イランの選挙が近づくにつれて、イラン周辺でのフィッシング詐欺活動の全体量の「急増」が見られたとブログで述べていました [48]。一部の研究者は、おそらく特定の候補者を支持するグループや個人に関する機密情報を収集するために、多くの攻撃者がスキルや攻撃力を国内に集中的させたのではないかと推測しました [49]。

Syrian Electronic Army は、アサド大統領を支持しています。この四半期は、メディアや政府を標的とした活動を継続していました。



- 4 月 16 日 : NPR メディアネットワークがハッキングされて Web サイトが改ざんされました。
- 4 月 20 日 : CBS News の番組に関する 4 つの Twitter アカウントがハッキングされました。
- 4 月 22 日 : 2 つの FIFA World Cup の Twitter アカウントがハッキングされました。
- 4 月 23 日 : ハッキングされた AP 通信の Twitter フィードで、ホワイトハウスで 2 度爆発がありオバマ大統領が負傷したというニュースが何百万人ものフォロワーに向けて発表されました。このニュースは、米国の証券取引に混乱を招き、またたく間に 1,365 億米ドルの利益が吹き飛び、AP の Twitter フィードを停止させました [50]。

- 4 月 29 日 : Guardian の 11 個のアカウントがハッキングされました。
- 5 月 7 日 : 風刺報道機関 The Onion の Twitter アカウントがハッキングされました。
- 5 月 17 日 : Financial Times の Web サイトと Twitter フィードがハッキングされました。
- 5 月 20 日 : 同グループが、サウジアラビア国防省のメールシステムをハッキングして、機密メールのやりとりをいくつか公開したと主張しました。
- 5 月 21 日 : The Telegraph の Twitter と Facebook がハッキングされました。
- 5 月 25 日 : SEA がハイファの水道システムコンピューターに侵入を試みたと、イスラエルが発表しました。
- 5 月 25 日 : ITV News London がハッキングされました。
- 5 月 26 日 : B スカイ B の Android のアプリと Twitter のアカウントがハッキングされました。
- 6 月 5 日 : 複数のトルコ政府の Web サイトが、トルコ人ハッカーと SEA の共謀によりハッキングされました。

筆者について

本レポートは、McAfee Labs の Toralv Dirro、Paula Greve、Haifei Li、François Paget、Vadim Pogulievsky、Craig Schmugar、Jimmy Shah、Ryan Sherstobitoff、Dan Sommer、Bing Sun、Adam Wosotowsky、Chong Xu が準備し、作成しました。

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/report/default.asp

1 http://www.mcafee.com/uk/resources/white-papers/wp-dissecting-operation-troy.pdf
2 http://www.usatoday.com/story/news/nation/2013/04/26/liviing-social-hacked-passwords-amazon/2116485/
3 http://blog.cloudflare.com/patching-the-internet-fixing-the-wordpress-br
4 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2423
5 http://blogs.mcafee.com/consumer/badnews-for-good-people
6 http://www.invincea.com/2013/05/part-2-us-dept-labor-watering-hole-pushing-poison-ivy-via-ie8-zero-day/
7 http://news.softpedia.com/news/State-of-Louisiana-Website-Hacked-Spreads-Sirefef-Malware-350944.shtml
8 http://www.theregister.co.uk/2013/06/18/carberp_trojan_source_code_sale/
9 http://blogs.mcafee.com/mcafee-labs/targeted-campaign-steals-credentials-in-gulf-states-and-caribbean
10 http://english.chosun.com/site/data/html_dir/2013/04/08/2013040800970.html
11 http://www.bbc.co.uk/news/technology-21601608
12 http://blog.bitinstant.com/blog/2013/3/4/events-of-friday-bitinstant-back-online.html
13 https://mtgox.com/press_release_20130404.html
14 http://dollarvigilante.com/blog/2013/4/17/bitcoin-price-march-15-april-14-2013-the-bubble-heard-round-.html
15 https://mtgox.com/press_release_20130411.html
16 https://mtgox.com/pdf/20130424_ddos_statement_and_faq.pdf
17 http://news.softpedia.com/news/Bitcoin-Block-Explorer-Blockchain-info-Disrupted-by-DDOS-Attack-346497.shtml
18 http://www.wired.co.uk/news/archive/2013-05/3/silk-road-ddos
19 https://s3.amazonaws.com/s3.documentcloud.org/documents/701175/mt-gox-dwolla-warrant-idg-news-service.pdf
20 http://blog.wmtransfer.com/en/blog/wmx-the-new-type-of-title-units
21 http://blog.webroot.com/2013/05/22/new-commercially-available-diy-invisible-bitcoin-miner-spotted-in-the-wild/
22 http://krebsonsecurity.com/2013/06/mtgox-phishing-campaign-hits-bing-yahoo/
23 http://techcrunch.com/2013/06/27/the-dea-seized-bitcoins-in-a-silk-road-drug-raid/
24 http://sbu.gov.ua/sbu/control/uk/publish/article?art_id=116410&cat_id=39574
25 http://www.net-security.org/malware_news.php?id=2458
26 http://krebsonsecurity.com/2013/05/alleged-spyeye-seller-bx1-extradited-to-u-s/
27 http://www.nydailynews.com/new-york/cyber-thieves-busted-45-million-heist-article-1.1339051
28 http://www.wired.com/threatlevel/2013/05/liberty-reserve-indicted/
29 http://www.coindesk.com/wm-center-e-currency-exchange-seized-by-us-government/
30 http://www.eweek.com/security/microsoft-fbi-shutter-citadel-botnets-seeking-to-end-500m-crime-spree/
31 http://www.infoworld.com/t/security/microsoft-accused-of-friendly-fire-in-citadel-botnet-takedown-220438
32 http://nakedsecurity.sophos.com/2013/06/12/microsoft-citadel-takedown/
33 http://garwarner.blogspot.fr/2013/06/vietnamese-carders-arrested-in.html
34 https://threatpost.com/feds-bust-cybercrime-ring-targeting-payroll-financial-firms/
35 http://www.leparisien.fr/espace-premium/actu/les-pirates-du-net-pillent-27-000-coordonnees-bancaires-12-06-2013-2888529.php
36 http://pastebin.com/4g44jfNF
37 http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q1-2013.pdf
38 http://news.softpedia.com/news/Hacktivists-Target-Over-100-000-Israeli-Sites-Officials-Say-There-s-No-Real-Damage-343610.shtml
39 http://technologynewsforday.wordpress.com/2013/04/07/30000-visa-cards-leaked-by-dr-freedom/
40 http://www.dreuz.info/2013/04/attaque-danonymous-israel-leur-a-mis-la-honte-le-w00t-ultime/
41 http://news.softpedia.com/news/Anonymous-Hackers-to-Launch-OpPetrol-on-June-20-Video-352816.shtml
42 http://www.ibtimes.com/opturkey-syrian-electronic-army-joins-anonymous-turkey-protests-hacks-erdogans-network-access-staff
43 http://www.worldbulletin.net/?ArticleID=111010&aType=haber
44 http://www.wired.co.uk/news/archive/2013-05/22/south-africa-whistleblower-leak
45 http://www.dailymail.co.uk/news/article-2324884/Lulzsec-hackers-thought-day-pirates-caused-millions-pounds-damage-cyber-attacks-CIA-Pentagon-Home-Office-agency.html
46 http://gawker.com/the-fbi-raided-steubenville-anonymous-guys-house-here-511634071
47 http://www.pcworld.com/article/2039020/police-arrest-anonymous-suspects-in-italy.html
48 http://googleonlinesecurity.blogspot.fr/2013/06/iranian-phishing-on-rise-as-elections.html
49 http://krebsonsecurity.com/2013/06/iranian-elections-bring-lull-in-bank-attacks/#more-21113
50 http://www2.macleans.ca/2013/04/23/associated-press-twitter-feed-gets-hacked-claiming-explosions-at-white-house-president-injured/

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）