レポート

McAfee
An Intel Company

McAfee 脅威レポート：2013 年第 3 四半期

McAfee Labs

目次

序論

McAfee Labs の研究者は、2013 年第 3 四半期の脅威を分析し、よく見られるいくつかの傾向と新たな現象を確認しました。

- モバイルと全般的なマルウェアの着実な増加
- 世界的なスパムの急増
- 非合法活動の匿名性を維持するための、サイバー犯罪者によるデジタル通貨使用の増加
- ドラッグなどの非合法製品を販売していたオンライン市場 Silk Road の閉鎖
- サイバー犯罪者向けのオンラインストア「Deep Web」の登場

マカフィーのレポート『Digital Laundry: An analysis of online currencies, and their use in cybercrime（デジタルマネーロンダリング:オンライン通貨およびサイバー犯罪におけるその利用の分析）』[1] では、オンライン通貨、および犯罪者が追跡可能なクレジットカードや他の一般的な支払い方法を使わずにドラッグ、マルウェア、エクスプロイトなどのサービスを売買できる利点について調査しています。法執行機関と裁判所は反撃を試みていますが、ある通貨がなくなってもまた別の通貨が出現している状態です。

重大なハッキング事件を時系列で記載すると、この四半期に引き起こされた主な犯罪活動が示されます。オンライン通貨 Bitcoin が引き続き話題となりました。このレポートでは、デジタルマネーロンダリングに関する分析に加えて、より多くの Bitcoin を「採掘」するためにシステムをハイジャックする秘密の試みや、通貨の法的地位に関する判決など、最新の Bitcoin 事件について取り上げています。

オンラインのブラックマーケット Silk Road の閉鎖は、法執行機関の勝利に終わりましたが、少なくとも 1 つの同様の Web サイトが、Silk Road の退場後数時間もしないうちに登場しました。このレポートでは、オンライン犯罪者がほとんど制約を受けずに活動している Deep Web の特徴について考察しています。この場所は、お金を払えば武器、児童ポルノ、さらには依頼殺人の検索が可能となる憂慮すべき状態となっています。

活動家のハッカーは、Web サイトの改ざんを行い、反対勢力からの反撃を引き起こしています。中東は政治的表明の活発な地域であり、Syrian Electronic Army（SEA）による The New York Times や他の標的へのハッキング事件が再びトップニュースとなりました。

モバイルマルウェア数は、この四半期に 33% 増加しました。あらゆる種類の新たなマルウェア数はこの期間に 2,000 万を超え、累計数は 1 億 7,200 万バイナリに達しました。システムに侵入して潜み続ける新たなルートキット数は、この四半期で倍増しました。USB ドライブ経由で拡散することの多い AutoRun 脅威の数は高い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は、記録を更新し続けており、50% 近く増加しています。

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、前の四半期からわずかに減少していますが、全体的な数は高い水準のままです。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。

マカフィーの Global Threat Intelligence ネットワークでは、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脅威が、インターネットでの悪意のある活動の半分近くを占めていることを確認しました。

Web 脅威の分析によって、新たな疑わしい URL 数の多くは米国内に存在し、この四半期に 14% 増加したことを確認しました。フィッシング詐欺の標的となる主な業界は、オンラインオークションと金融機関です。スパムの水準は急増しています。この四半期のメッセージ件数は、9 月には 4 兆件に達しており、2010 年以降で最も高くなっています。世界の中からピックアップした国々における様々なスパム件名とボットネットの蔓延に関するレポートも引き続き掲載しています。

デジタルマネーロンダリング

最近発表されたマカフィーのレポートでは、犯罪をサポートする「インターネットマネー」の果たす役割について調査しています。『Digital Laundry: An analysis of online currencies, and their use in cybercrime（デジタルマネーロンダリング：オンライン通貨およびサイバー犯罪におけるその利用の分析）』[2] では、法執行機関による最新の取り組みと、検察による起訴について紹介しており、資金洗浄を行う犯罪者にとってデジタル通貨が重要なサービスであるという理論を裏付けています。

デジタル通貨サービス Liberty Reserve は、事業が停止されるまでに計 60 億米ドルのロンダリングに使用されており、これは、史上最大の国際的な資金洗浄の告発となりました。しかし、サイバー犯罪者によって使用されてきた仮想通貨は Liberty Reserve のみではなく、こうしたサービスが拡散することで、サイバー犯罪が増加し、他の手口によるデジタルの混乱状態の拡大も加速していきました。さらには、こうした通貨が抱える問題は、金融取引への標的を絞った攻撃や、デジタルウォレットを標的として開発されたマルウェアの出現によって、資金洗浄で使用される傾向があるという問題だけにとどまらなくなりました。

Bitcoin などの一部の通貨は、採掘として知られているプロセスを通して新たに通貨を作り出すことができます。当初、人々は自分のコンピューターのリソースを使用して採掘を行っていましたが、2011 年 6 月に JavaScript の Bitcoin ジェネレーター（マイナー）の登場により、通信量の多い Web サイトで訪問者のコンピューターを利用して Bitcoin の生成が可能となりました。このことを訪問者に説明している Web サイトもありましたが、この方法を知らせることなく実行することもできたため、実際には、悪意のあるボットが作成されました。E-Sports Entertainment Association のある社員は、ひそかに Bitcoin を採掘するために、約 14,000 千台のコンピューターに、こうしたマイナーソフトウェアを不正にインストールしました。

欧州中央銀行（ECB）は、仮想通貨と電子マネーの仕組みの明らかな違いについて指摘しています。電子マネーは、従来の通貨単位を使用しており、規制を受けますが、仮想通貨は規制を受けることなく、独自に考案された通貨を利用しています。

Yankee Group は、レポート『Redefining Virtual Currency（仮想通貨の再定義）』[3] において、仮想通貨市場は 2012 年に 475 億米ドルに成長しており、今後 5 年間でさらに 14% 増加して、2017 年には 554 億米ドル相当まで成長すると予想しています。同レポートでは、この並外れた成長は、モバイルデバイスの普及が大きな要因となる可能性があると推測しており、犯罪とは関係のない市場の拡大を示唆しています。

仮想通貨は、顧客に多大なメリットをもたらします。仮想通貨は信頼性が高く、比較的すぐ手に入り、匿名性があります。特定の通貨（特に Bitcoin）でプライバシーの問題が生じた場合にも、市場において機能が拡張され、より大きな匿名性を提供してきました。市場の対応は重要なポイントです。なぜなら、法執行機関が仮想通貨企業に対して取締りを行っても、ユーザーは資金を洗浄する新たなプラットフォームをすぐに発見するからです。主要なプラットフォームを閉鎖しても問題の解決にはなりません。

仮想通貨サービスを閉鎖させる試みは、Liberty Reserve のサービスの経緯を見てもわかるように、犯罪者が他の場所へとビジネスを移行するだけの結果に終わっています。こうした犯罪者にとって魅力的な状況をよそに、国際的な法執行機関は、資金洗浄のプラットフォームに関与した個人を特定、取り押さえ、逮捕するために、国際的に民間企業とも連携して捜査を実施しています。

仮想通貨がなくなることはありません。DoS 攻撃を受けるという明らかな問題、資金洗浄での取引の利用、サイバー犯罪を促進するという側面がありますが、合法的に利用するための機会も数多くあります。この市場の機会を無視することで、潜在的な合法の投資家が大きな収益を得られなくなる可能性がありますが、潜在的なリスクへの対応に失敗すると、さらに大きな代償を支払う可能性があります。

サイバー犯罪

アンダーグラウンドの世界：Deep Web に関する調査

Sefnit ボットネット

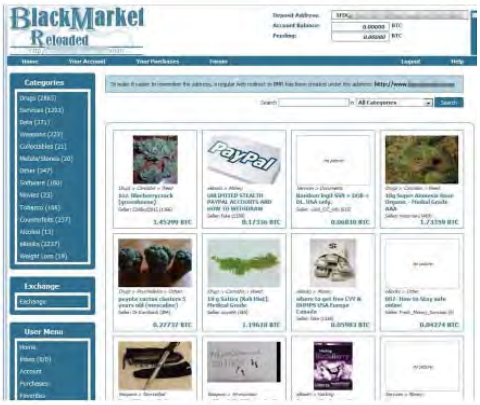
8 月中旬以降、匿名のネットワーク Tor では、1 日当たりのユーザー数が 50 万ユーザーから約 400 万ユーザーまで増加しました。この増加は、Mevade または Sefnit として知られるコンポーネントを含むボットネットが原因です。複数のレポートによれば、このボットネットは、クリック詐欺を専門とするウクライナの犯罪組織によって実行されたと考えられています。

Deep Web のマーケットプレイス

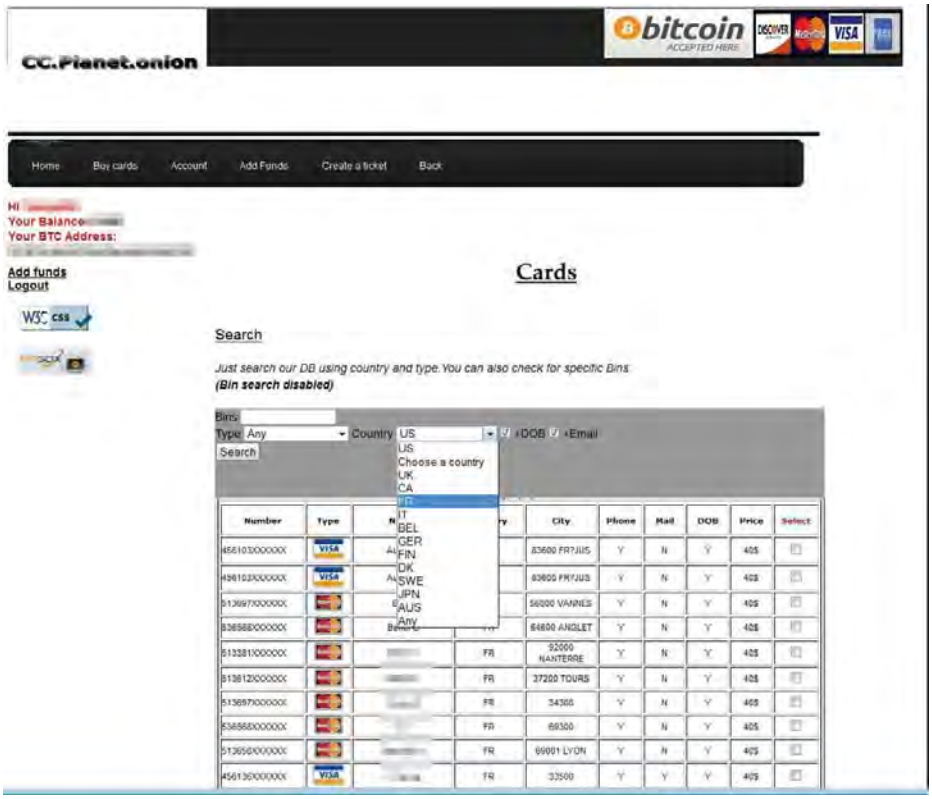
研究者が Tor、Deep Web、Bitcoin に関して言及する際には、多くの場合、アンダーグラウンドのマーケットプレイス Silk Road について取り上げます。2011 年 2 月に誕生して 10 月 1 日に米国連邦捜査局によって閉鎖された[4]、このサイバー犯罪者向けのオンラインスーパーマーケットは、Bitcoin のみで取引していました。この場所は eBay や Craigslist のような市場であり、売買を望む人々がここでやり取りしていました。主にドラッグ市場として知られていましたが、ATM のハッキングといった他の非合法なサービスをはじめとする 200 以上のカテゴリーの商品が販売されていました。

現在、Silk Road はなくなりましたが、これは氷山の一角にすぎませんでした。他の多数の場所が Bitcoin による支払いを受け入れています。他のサイトも確認してみましょう。

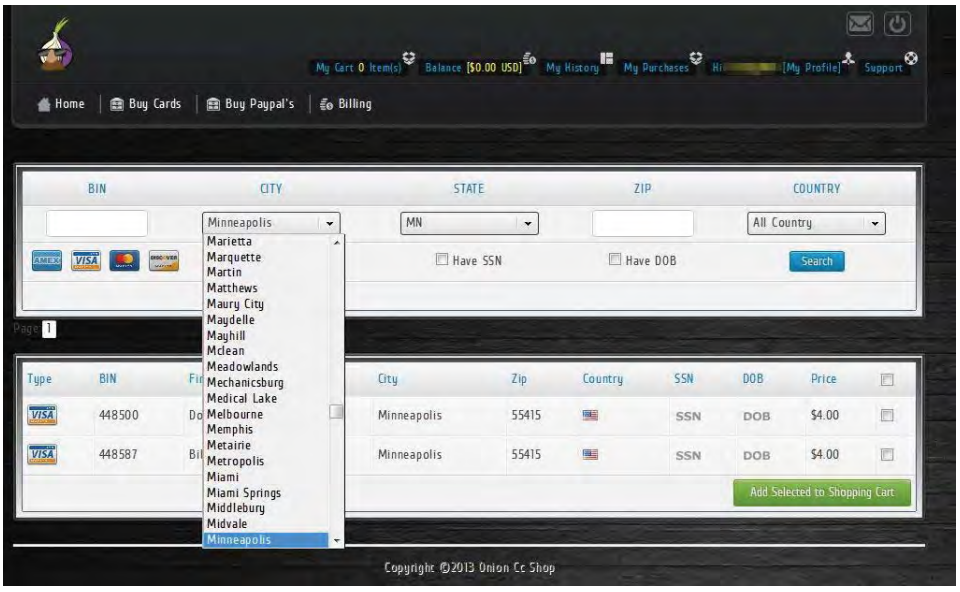
Silk Road の競合相手は、現在も営業中です。これらのサイトの一部は、Silk Road と同じ形式で製品を提供しています。



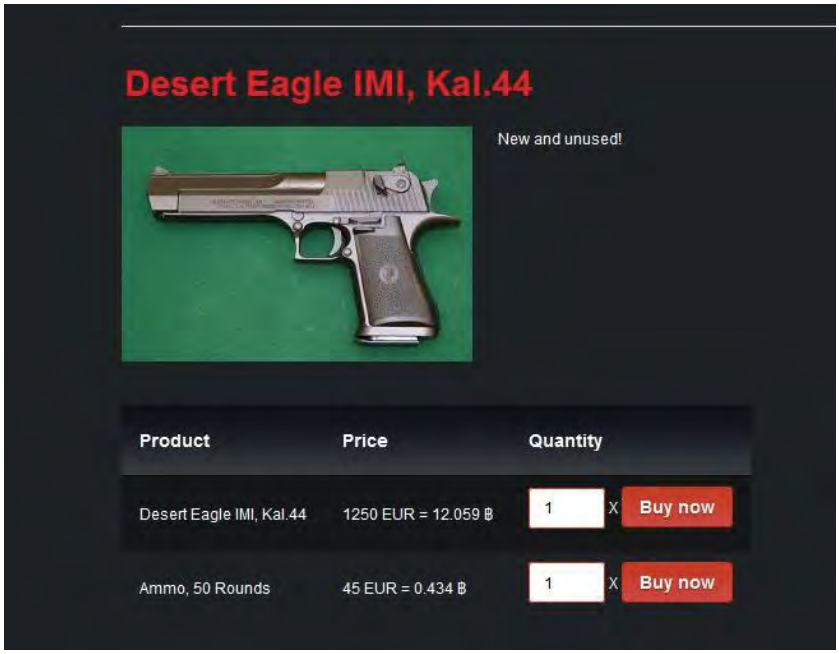
オンラインの買い物客が、ヨーロッパのプレミアのクレジットカードを購入できる場所もあります。下記の例はフランスのカードです。価格はそれぞれ 40 米ドル（0.3BTC）です。



米国のクレジットカードはさらに安価（約 4 米ドル）です。以下のスクリーンショットは、別の在庫豊富なサービスのページです。ここでは、購入者は州や市を指定して検索が可能です。



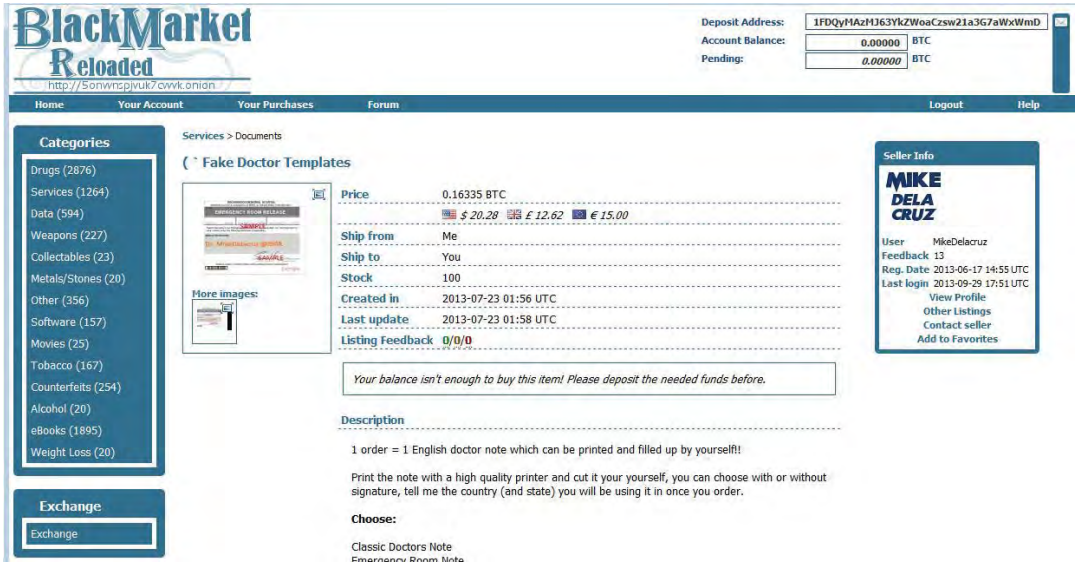
欧州の市民は武器を購入できます。



一部の例を紹介します。

- ワルサー PPK、7.65mm、600 ユーロ（5.8 BTC）
- デザートイーグル IMI、44 口径、1,250 ユーロ（12 BTC）
- シグザウエル P226 AL SO DAO、9mm、790 ユーロ（7.7 BTC）

偽の医者用テンプレートといった偽造書類も検索可能です。

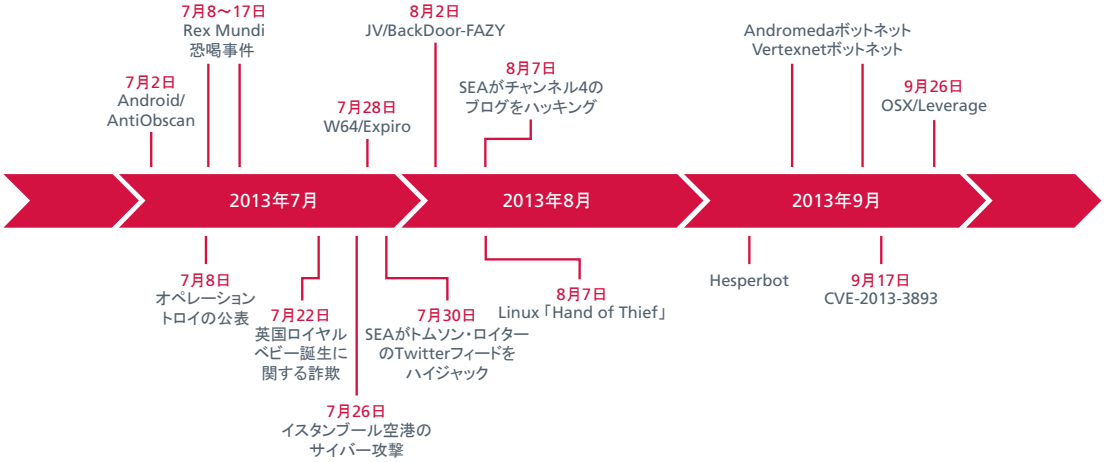


殺人の依頼も可能のようです。こうした申し出が実際に実行に移されるかどうか示すものはないですが（この Web サイトには現在アクセスできません）、これを確認しようとすれば、個人の身に危険が降りかかる可能性があります。しかし、こうした Web サイトは、仮想通貨のプライバシーに対する信頼によって、いくつかの恐ろしいサービスの販売が可能となったことを示しています。

Freedom Hosting の Web サイトは閉鎖されましたが、児童ポルノのコミュニティは未だに活動を続けています。

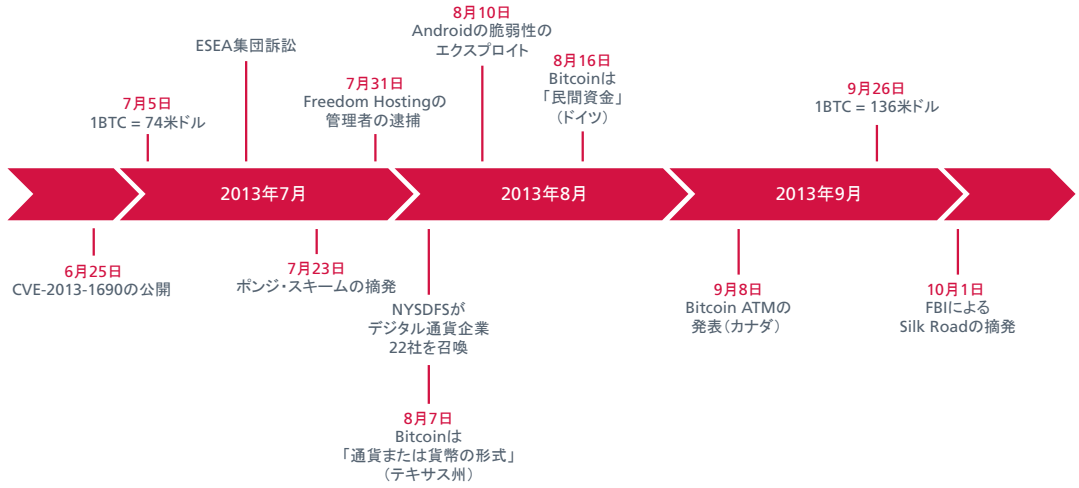
これはアルカイダに寄付を行える Web サイトです。

マルウェア、脆弱性、ハッキング



- 7 月 2 日 : マカフィーモバイルセキュリティは、ラッパー Jay-Z の限定アプリの海賊版コピーに埋め込まれている新たな Android のトロイの木馬、Android/AntiObscan を発見したと発表しました [5]。
- 7 月 8 日 : マカフィーは、韓国内で長期間行われていたサイバースパイ活動、オペレーショントロイを公表しました [6]。
- 7 月 17 日:Rex Mundi グループは、ケーブル TV 事業の Numericable が 22,000 ユーロの身代金の支払いを拒否した後に、同社の 6,000 名の顧客および見込み顧客から盗んだ顧客データを公開しました[7]。7 月 8 日、同グループは Websolutions.it を標的としました [8]。
- 7 月 22 日:予想した通り、英国ロイヤルベビー誕生のニュースはマルウェア配信の恰好の誘い文句となりました。マカフィーでは、このイベントに関する多数のスパムメッセージを記録しました [9]。
- 7 月 26 日 : イスタンブール・アタテュルク空港の出発ターミナルのパスポート管理システムがサイバー攻撃を受けました。それと同時に、現地のメディアは、イスタンブールのサビハ・ギョクチェン国際空港のパスポート管理システムも故障したと報道しました [10]。
- 7 月 28 日 : マカフィーは、以前からあるマルウェアの新バージョン、W64/Expiro を検出したと発表しました。このバージョンは、32 ビットと 64 ビットのファイルに感染する恐れがあります [11]。
- 7 月 30 日:Syrian Electronic Army が、トムソン・ロイターの Twitter フィードをハイジャックしました[12]。同グループは、7 つの暴力的な風刺画を投稿しました。同日、同グループは、米国ホワイトハウスのスタッフメンバー 3 名の個人用メールアカウントの侵害を発表しました [13]。
- 8 月 2 日 : マカフィーは、マルウェアバイナリ JV/BackDoor-FAZY を受信しました。この JAR パッケージは、感染後にコマンドを実行してボットとして活動できるように、攻撃者のためのバックドアを開きます [14]。
- 8 月 7 日 : 英国チャンネル 4 のブログが Syrian Electronic Army にハッキングされました [15]。
- 8 月 7 日:RSA は、フォームグラバーおよびバックドア機能を含み、金融機関を狙う Linux のトロイの木馬、「Hand of Thief」を発表しました [16]。8 月に、マカフィーは、マルウェア製作者による AutoIt スクリプトの使用が増加しているのに注目しました。こうした悪意のあるスクリプトは、主に Bitcoin 採掘者に関係していました[17]。9 月に、ボットネット Andromeda[18] およびボットネット Vertexnet[19] に関する警告がさらに発表されました。
- 9 月 6 日 : マカフィーは、トルコおよびチェコ共和国で活発に活動していた銀行を狙うマルウェア、Hesperus（または Hesperbot）を発表しました [20]。
- 9 月 17 日 : Microsoft は、多用されていた Internet Explorer のリモートコード実行の脆弱性（CVE-2013-3893）に対応するために、セキュリティ アドバイザリ KB2887505 を発行しました [21]。このエクスプロイトコードは広く利用されていました。
- 9 月 26 日 : 新たなトロイの木馬 OSX/Leverage は、Apple OS X コンピューターを標的としており、恒久的なバックドアのインストールを試みます。感染後、ポート 7777 で自身のコントロールサーバーに接続します。このマルウェアは、Java の脆弱性 CVE-2013-2465 と CVE-2013-2471 を利用します [22]。

Bitcoin をめぐる事件（続き）



McAfee Labs の第 2 四半期の脅威レポートでは、オンライン通貨に関するニュースを時系列に沿って紹介しました。本レポートの 4 ページの「デジタルマネーロンダリング」の項で詳しく説明しています。そこに記載されていない事件について以下に記載します。

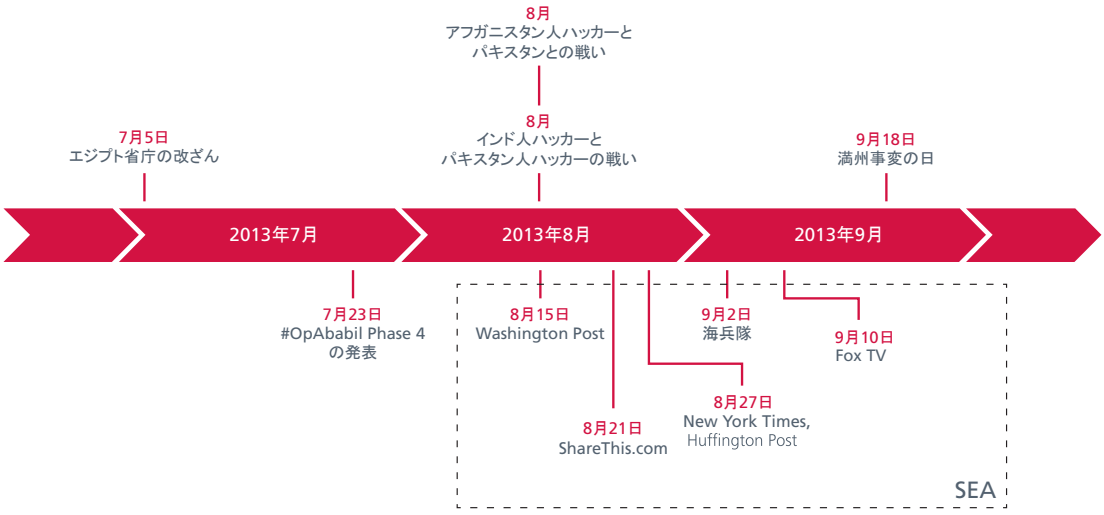
- 4 月に、ゲームネットワーク ESEA の従業員が、同社のサーバーを使用して、個人で使用するための Bitcoin を生成していました [23]。7 月初めに、こうした事実の発覚後、同社は集団訴訟に加わりました [24]。
- 7 月 23 日：米国証券取引委員会（SEC）は、Bitcoin に関するポンジ・スキームを用いた罪で、テキサス在住の男性を訴えました。SEC によると、2011 年 9 月以降、容疑者は、自分の会社 Bitcoin Savings and Trust を通じて少なくとも 70 万 Bitcoin を生成し、新たな投資者の通貨を不正に使用して払い戻しを埋め合わせていました。SEC によれば、彼は、「監視の外」でオンライン通貨の購入を望む個人に迅速に大量に販売するといった、偽の取引によって毎週 7% 相当の利益を投資者に不当に約束していました [25]。
- 7 月 31 日：アイルランドで児童ポルノの販売人が逮捕されました。彼は、匿名の Tor ネットワークの最大手のサービスプロバイダー、Freedom Hosting を所有し運営していたとして告発されました [26]。米国は、この容疑者の引き渡しを正式に要求してきました。当局は、彼を「地球上で最大の児童ポルノの提供者」であると評しました。DailyDot の Web サイトによれば [27]、この容疑者は 2 年前に、Freedom Hosting が運営する、匿名でエスクロー、ミキシング、マーチャントペイメントが利用可能な Onion Bank を創設しました。Hidden Wiki に表示される広告によると、この銀行は、「Bitcoin 用の PayPal のように」営業していました。ラスベガスで開催された Black Hat 2013 カンファレンスの期間中、Tor Browser Bundle[28]（6 月 25 日に発表された CVE-2013-1690/MFSA 2013-53）を特別に標的とした Mozilla Firefox ゼロデイ攻撃が、容疑者の特定のために FBI と国家安全保障局により用いられた可能性があることが、発表によって明らかとなりました。
- 8 月 7 日：テキサスの連邦判事が、Bitcoin は「通貨または貨幣の形式」であると認定し、この投資資金および取引は米国証券取引法の管轄下にあることを宣言しました [29]。ニューヨーク州金融サービス局は、Bitcoin について調査するために主要な Bitcoin 業者を召喚しました [30]。当局は、資金洗浄の管理、消費者保護の実践、資金源、資料（Bitcoin の設立について）、投資戦略（Bitcoin 投資家向け）に関する情報を引き渡すように彼らに求めました。
- 8 月 10 日：bitcointalk.org フォーラムのユーザーが、Java SecureRandom の乱数ジェネレーターの Android 実装における深刻な脆弱性によって、55BTC 以上盗まれたことに気が付きました [31]。4 つの Android Bitcoin クライアント、Bitcoin Wallet、Blockchain、Mycelium Bitcoin Wallet、BitcoinSpinner は、翌日 Bitcoin.org の通知に応じて修正されました。
- 8 月 16 日：ドイツ財務省が、デジタル通貨は多角決済で現金のように使用できる「民間資金」であると認定しました [32]。
- 9 月：初の Bitcoin ATM が 10 月にカナダのバンクーバーに設置されるという発表がありました（このような発表が行われたのは初めてではありませんが、実際に設置が確認できていませんでした）[33]。

サイバー犯罪者に対する取締り

この四半期の間の法執行機関の取り組みについて紹介します。

- 7 月：米国連邦機関は、1 億 6,000 万枚以上のクレジットカード番号を盗んだとして、ロシア人 4 名とウクライナ人 1 名を告発しました。検察官は、これによって、世界中の大企業に何億ドルもの損害を発生させたと述べています。この集団は、2007 年に約 1 億 3,000 万枚ものカード番号を公開したクレジットカード決済処理会社 Heartland Payment Systems のデータ侵害、2011 年に 100 万近くのアカウントを巻き込んで 1 億米ドル近くの損害を Global Payments に与えたデータ侵害に関与したと考えられています [34]。
- 世界中で開催される「ハイローラー」のポーカートーナメントの一流プレーヤーが、400 万米ドル近く獲得したとされるマルウェア組織に彼の会社が関与していた罪で、他 8 名とともに逮捕されました [35]。彼らは、マルウェアプログラム Android/Enesoluty を使用して、被害者のモバイルフォンの情報を収集し、ユーザーに支払いを請求して実際には何もサービスを提供しない偽のデーティングサイトへの招待状を送信していました。合計すると、このマルウェアは、81 万台の Android 携帯とタブレットから 3,700 万件以上のメールアドレスを収集したとされています。
- 9 月 19 ～ 20 日：ロンドン警察は、ロンドンの Barclays Plc の支店からコンピューターを使用して 130 万ポンド（210 万米ドル）を奪った強盗に関与したとして、8 名の男性を逮捕しました。捜査官は、支店のコンピューターの中の 1 台に接続されている 3G ルーターに取り付けられた KVM スイッチ [36] を発見しました。この発見は、ロンドン警察が銀行ハッキングの容疑で逮捕を発表した同じ週に起きた出来事でした。9 月 13 日には、ロンドン警視庁は、同様の装置を使用して Banco Santander SA のコンピューターにハッキングを試みた容疑で、12 名の男性を拘束しました [37]。

ハクティビズム



8 月に、FBI の職員が The Huffington Post に、2012 年の数々の逮捕によって Anonymous の活動の拡大を食い止めたと語りました [38]（McAfee Labs は、『2013 年の脅威予測』において Anoymous の衰退を予測していました）[39]。実際のところ、同ハッカー集団は、この四半期に目立ったサイバー攻撃を実施しておらず、様々な「擬似的な」サイバー軍および彼らのより曖昧な目的が横行する状態となりました。

7 月 5 日、Anonymous Jordan の一員であると主張するハッカーが、ムスリム同胞団政府の退陣に抗議するために 8 つのエジプト省庁の Web サイトを改ざんしました [40]。

8 月 14 日、パキスタンは自国の独立記念日を祝っていました。その翌日には、インドでも独立記念日を迎えました。ハッカーにとっては、こうした祝祭日は不適切な愛国主義を表明する機会となりました。インドでは、ムンバイの Mahanagar Telephone Nigam Limited や Pune Traffic Police などの複数の Web サイトがハッキングされました。これは明らかに Napsters Crew[41] のパキスタン人ハッカーによるものでした。これに対する報復として、インド人ハッカーは、パキスタンの Web サイトを標的にしました。Godzilla として知られるハッカーは、パキスタン軍の公式 Web サイトに侵入して改ざんを行いました。Web サイトへの侵入に加えて、彼は、3 つのパキスタン陸軍の Facebook ページに不正アクセスを行いました [42]。同時期に、Afghan Cyber Army と名乗るハッカーグループが、パキスタン国境沿いにあるアフガニスタンの村へのロケット攻撃を非難する国家主義的なメッセージを用いて、およそ 300 のパキスタン政府と企業の Web サイトを改ざんしました [43]。

これまでの McAfee Labs の脅威レポートでは、イランの Izz ad-Din al-Qassam Cyber Fighters と Syrian Electronic Army という 2 つのグループの活動を取り上げてきました。前者のグループは、米国の銀行および金融サービス企業への一連の攻撃を実施したことで有名です。彼らは、インターネットから削除されることを望んでいる動画「イノセンス・オブ・ムスリム」に対する攻撃であると正当化しました。後者は、バッシャール・アル・アサド大統領の体制を支持しており、敵とみなしている国の勢力やメディアを攻撃しています。

7 月 23 日、Cyber Fighters は、新たなオペレーション Ababil の Phase 4 の開始を発表しました。8 月 15 日、米国の銀行 JPMorgan Chase と Citigroup が、分散 DoS 攻撃の被害者となりました [44]。

また、8 月15 日には、SEA がWashington Post のWeb サイトをハッキングし、一部の読者を自身のWeb サイトにリダイレクトしました。さらには、同社のスタッフライターの個人アカウントが、SEA のメッセージの送信に使用されました[45]。

これ以降に引き起こされた攻撃について紹介します。

- 8月21日:SEAが、オンラインコンテンツ共有サイトShareThis.comを自身の公式Webサイトにリダイレクトしました[46]。
- 8 月 27 日 : The New York Times および The Huffington Post を含む複数のドメインが、SEA がこれらの会社のドメイン名登録機関 Melbourne IT に侵入した後に、リダイレクトされました [47]。
- 9 月 2 日 : SEA が、米国海兵隊の採用 Web サイトを改ざんしました。問題を抱えたシリアの体制を支持する SEA は、オバマ大統領を非難する声明を残して、海兵隊員にシリアで戦う命令に背くように促しました。
- 9 月 10 日 : Fox TV の公式の Hootsuite アカウントがハッキングされて、世界中の国際 Fox TV ネットワークにオンラインコンテンツを投稿するのに使用されました [48]。SEA は、リンクされた 200 以上の Facebook と Twitter アカウントにアクセスしたと主張しました。

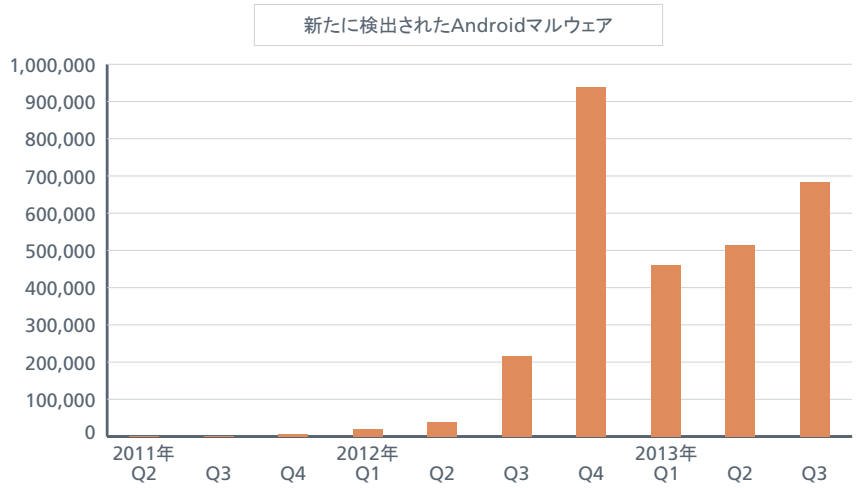
8 月 30 日、政府やメディアの巨大企業へのこうした攻撃によって、FBI が公式に SEA を警告リストに載せることとなりました。FBI は、SEA を、2011 年のシリアの反政府抵抗活動の間に登場した「体制支持のハッカーグループ」と呼んでいます [49]。

こうしたハッキングの成功実績にもかかわらず、SEA のスキルに疑問を抱く人々もいます。8 月 31 日、フランスの Web サイト reflets.info は、Anonymous とつながりがあると主張するグループが SEA のデータベースとサーバーに侵入したと発表しました [50]。Deep Web で入手できると言われていた、漏えいしたデータには、Hotmail、Outlook、Gmail などのアカウントで現在使用されている多数のユーザー名とパスワード、さらにはこれらのアカウントからダウンロードされた 6 ギガバイトのメールメッセージが含まれていました [51]。

別の地域では、Honker Union の中国人のハクティビストが、日本を標的としたオンライン攻撃を実施することによって、満州事変の日（1931 年 9 月 18 日）に注目を集めさせました [52]。この前日には逆の攻撃が起きており、正体不明のハッカーが、紹興市の Web サイトに中国政府を非難する写真を投稿しました [53]。

モバイルの脅威

モバイルデバイスに感染するマルウェアについて言及する場合は、Android マルウェアのことを指しています。Apple の iOS などの他のモバイルOS に対する脅威は、悪意のあるAndroid アプリに比べるとそれほど大きくありません。この四半期に確認したAndroid マルウェア数は、3 分の1 増加して、サンプル数は68 万を超えました。この数字は、過去2 つの四半期に比べて大幅に増加しています。2012 年後半の最高記録を上回る数を近々目にすることになるでしょうか。



この四半期に、Android の多くのバージョンに影響を与える深刻なモバイル脅威、Exploit/MasterKey.A を確認しました。また、次の段階のマルウェアをデバイスにダウンロードするトロイの木馬アプリで構成された2 つの部分に分かれたマルウェアも確認しました。金銭を目的とする攻撃者は、銀行を標的とする新たなトロイの木馬をリリースしました。

あらゆる Android にとって重要

ほぼすべての Android デバイスに影響を与える脆弱性が、コンピューターセキュリティの研究者によって発見されました。この脆弱性によって、攻撃者はインストールされるアプリの署名チェックを回避することができます。MasterKey として知られるこのバグは、Black Hat コンピューターセキュリティカンファレンスで公表されました。研究者は事前に Google に通知して、この脆弱性の詳細情報を提供しました。Google はパッチを作成し、Android デバイスのメーカーにこのパッチを提供しました。

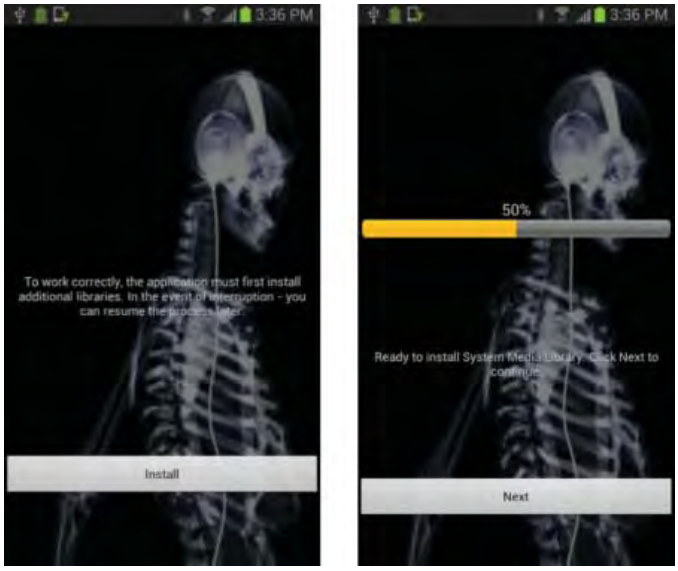
デジタル証明書は、Androidアプリ（APK）に署名して、同じディベロッパーのものであることを確認するために使用されています。アプリをアップグレードする際に、Androidは、アップグレードに元のディベロッパーの署名があるかどうかチェックします。これにより、犯罪者が、電話を乗っ取ることが可能な悪意のあるアップグレードを作成できないようにしています。現在のところ、攻撃者は、特殊なAndroidアプリを作成して、このアプリを被害者にインストールさせる必要があります。この方法で変更されたAPKが、Exploit/MasterKey.Aとして検出されています。

Google は、MasterKey の脆弱性を悪用して特別に作成された APK は正式な Play ストアには存在しないと主張しています。サードパーティのストアや Web からアプリを取得した場合は、必ずモバイルセキュリティソフトウェアをインストールしておく必要があります。

2 つの部分にわかれたマルウェア

多くの場合、攻撃者は、数多くのコンポーネントの中でマルウェアの機能を分けることによって、検出を逃れようとします。あるパーツには、インターネットにアクセスして 2 番目または 3 番目の悪意のあるパーツをダウンロードする以外の機能は付いていません。ユーザーは悪意のあるパーツをダウンロードしていないので、このマルウェア全体が疑われることなくデバイスに入り込むことができます。

Android/Repane ファミリーは、ダウンローダーAndroid/RepaneDropper.A と、ユーザーの情報を攻撃者に送信する悪意のあるパーツで構成されています。このドロッパーは、ユーザーに気付かれないようにやり過ごし、ユーザーが Android デバイスを使用してX 線を当てることができるアプリであるように装います。電話およびタブレットのカメラはいずれもX 線を発することはないので、このアプリを動作させる技術的な方法は存在しませんが、攻撃者が被害者にアプリを使わせようとするのを止めることも、ユーザーが友人や飼い犬をスキャンしようとするのを止めることもできません。残念なことに、実行してしまうと、Android/Repane.A が電話にダウンロードされる結果となります。



Android/Repane.A は、人目を引く X 線アプリとして配布されます

Android/Repane.A がダウンロードされても、被害者にこれをインストールさせる必要があります。これは、友人のスキャンに戻るためには必須のシステムライブラリを新たにインストールする必要があると、Android/RepaneDropper.A がユーザーに通知することによって、首尾よく実行できます。

銀行を標的として金銭を求めるトロイの木馬

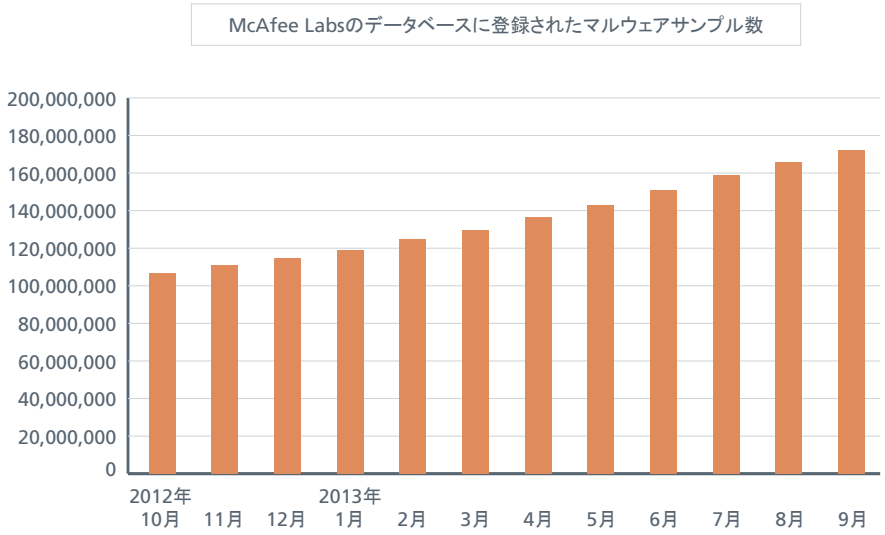
攻撃者は、銀行の口座には財布よりも多くのお金が保管されていることを知っているので、より大きな獲物を求め続けています。この四半期には、Android/Hesperbot がトルコと英国在住のユーザーを攻撃しました。

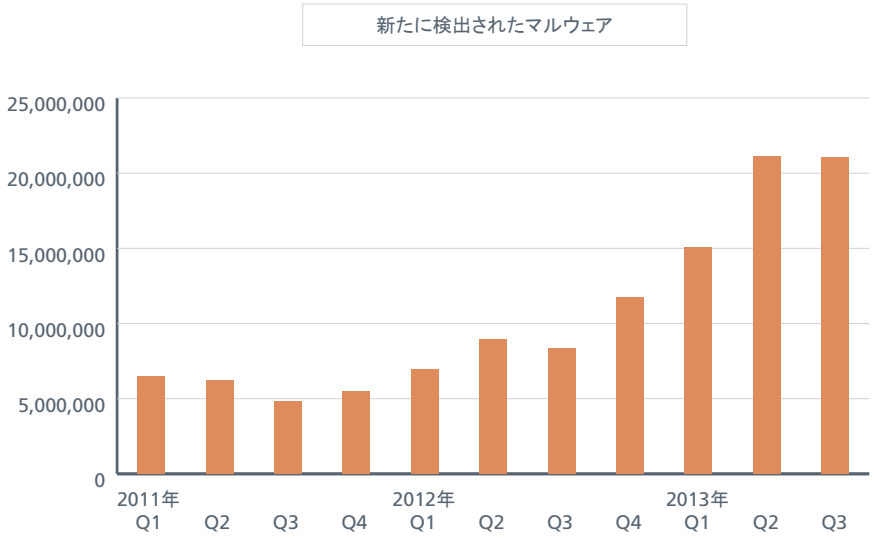
Android/Hesperbot.A もまた、被害者に見つからないように試みます。このマルウェアは気付かれることのないように自身のアイコンを削除します。プロセスリストには表示されますが、Certificate という紛らわしい名前を用いています。これは、一般的にユーザーが削除しようと考える名前ではありません。「Certificate」（証明書）は何か重要なファイルのように思われるからです。

このマルウェアは、オンラインバンキングの認証コードを生成するアプリのように装いますが、実際は被害者のログイン情報を盗みます。疑いを抱いていないユーザーは、銀行にログインするための最終認証コードを取得するために、コードを入力します。しかし、このマルウェアは、実際にはユーザーが入力したコードを攻撃者に送信するため、悪意を持った人物がこのコードを使用して、有効な認証コードを生成し、アカウントにアクセスできるようになってしまいます。

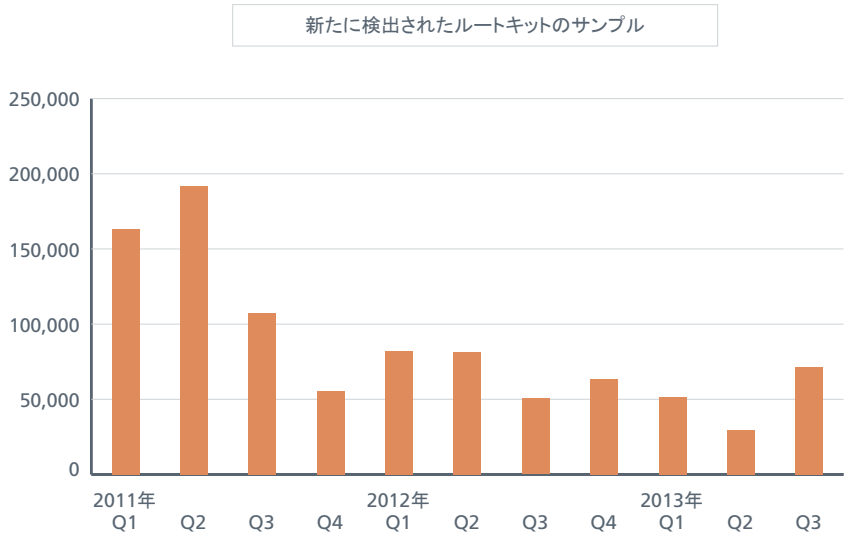
全般的なマルウェアの脅威

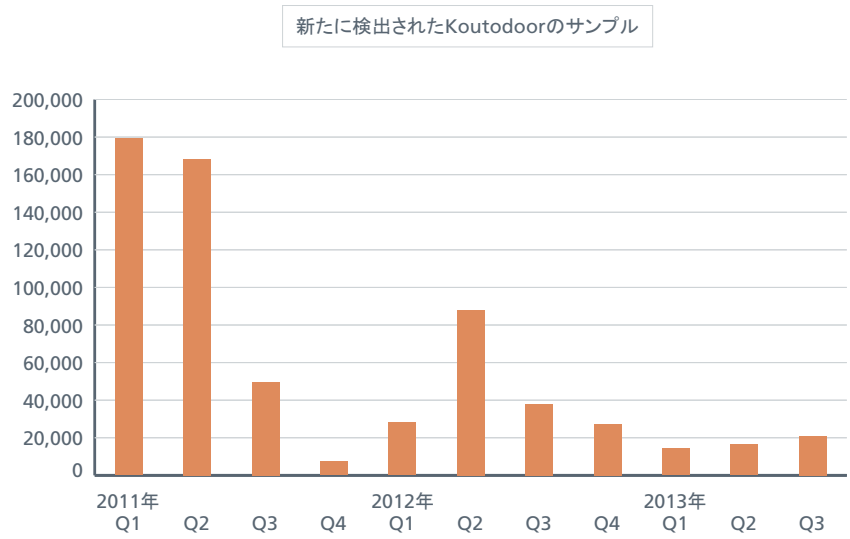
マルウェアの増加はこの四半期に若干衰えましたが、この期間に発見された新たな脅威は 2,000 万で、記録を開始して以来 2 番目に大きな数字のため、喜ばしい状況ではありません。マルウェア「zoo」の中のサンプル数は 1 億 7,200 万近くに迫っています。

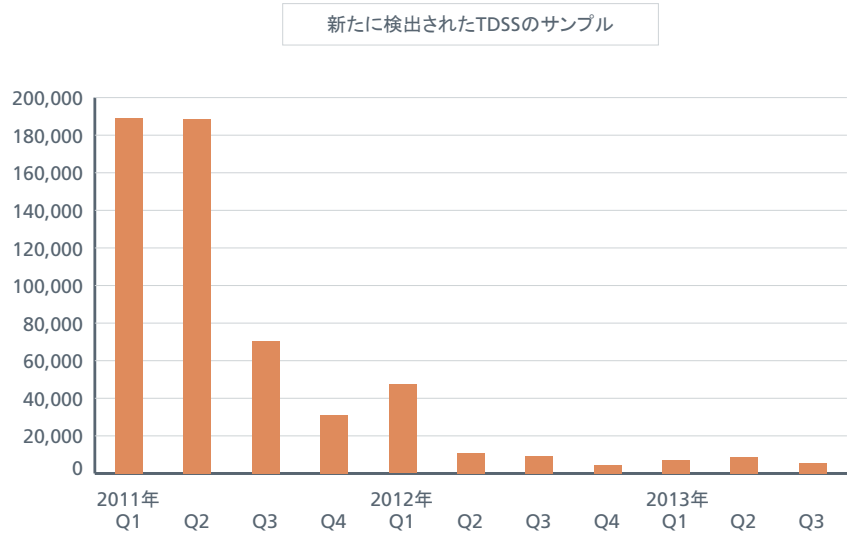


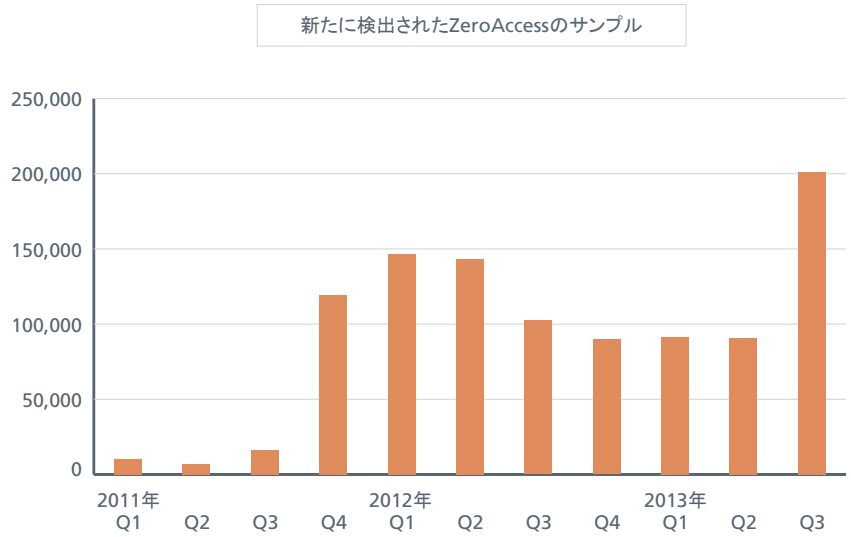


ルートキットやステルスマルウェアは、検出を回避して長期に渡ってシステムに常駐するように設計されています。新たなルートキットサンプルの増加は、2011 年半ば以降減少傾向にありますが、この四半期は増加に転じており、新しいサンプル数は前の四半期の 2 倍以上となっています（ZeroAccess ファイルの合計数が新しいルートキット全体の合計数を上回っていることが確認できますが、これは、ZeroAccess はルートキットを利用するマルウェアファミリーですが、すべての ZeroAccess ファイルがルートキットであるわけではないからです）。



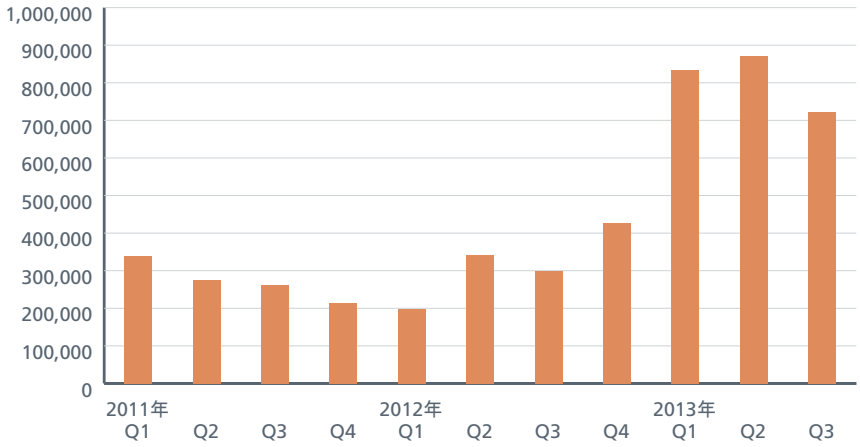




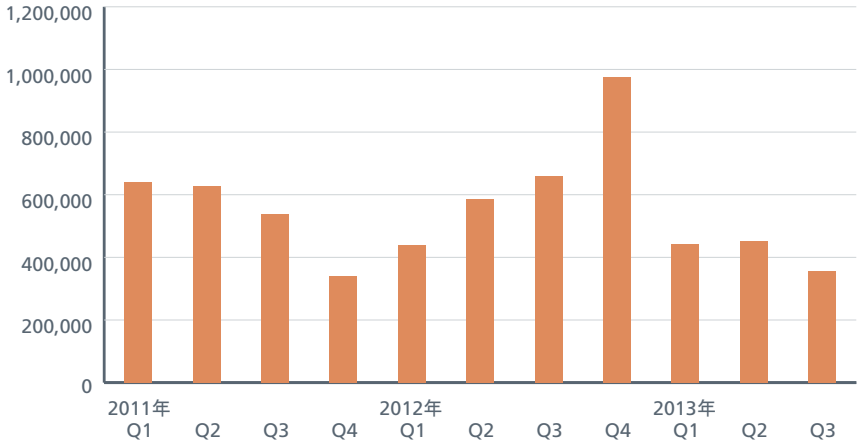


多くの場合、USB ドライブに潜んでおり、攻撃者がシステムをコントロール可能にする AutoRun マルウェアは、今年の初めから倍増し、この四半期にも高い水準を維持しています。システムが感染したと被害者を脅す偽のアンチウイルス（マルウェア）製品の数は、2012 年の新しいサンプルが 100 万近くという記録的な水準から、この四半期には 35 万 6,000 までに減少しています。被害者の銀行アカウントに侵入しようとするパスワード窃盗型のトロイの木馬は、20% 以上減少し、新しいサンプル数も 120 万を下回っていますが、依然として非常に高い水準を維持しています。

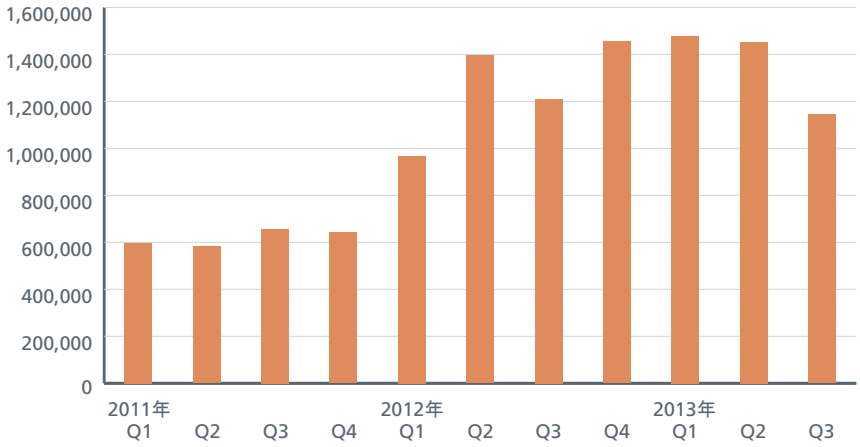
新たに検出されたAutoRunのサンプル



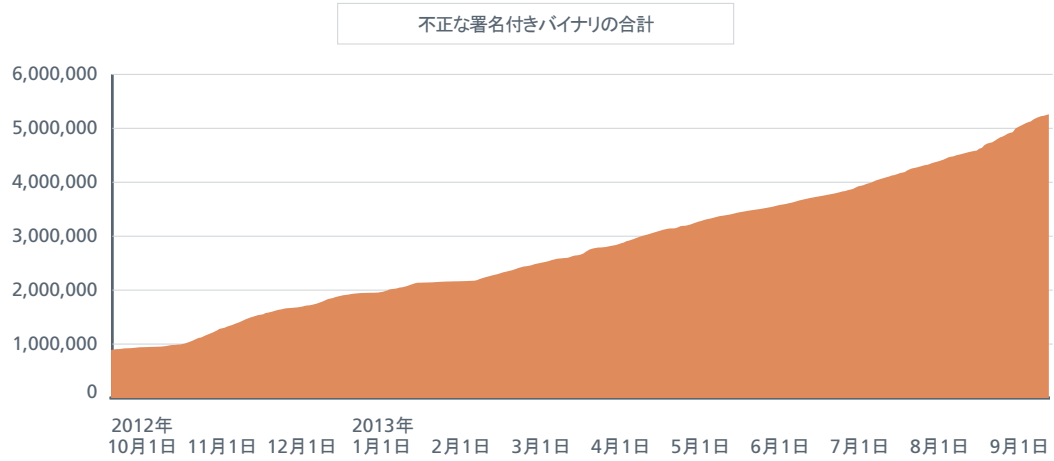
新たに検出された偽のAVのサンプル

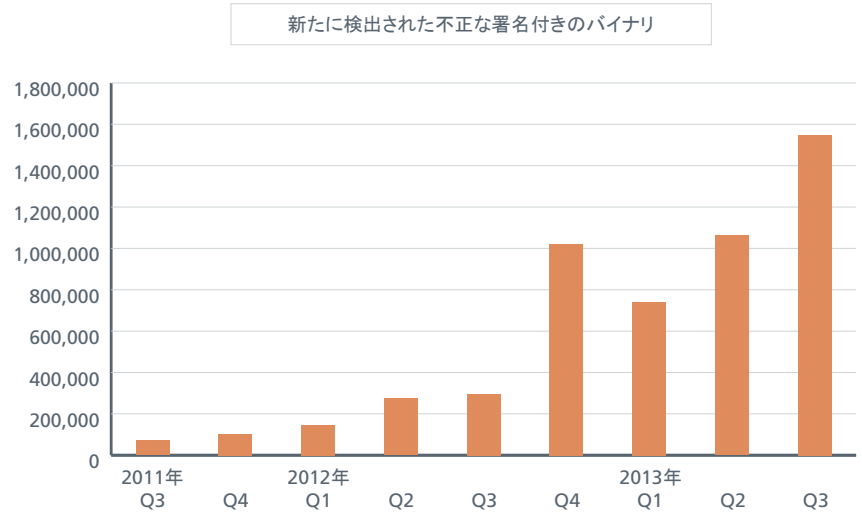


新たに検出されたパスワード盗用型トロイの木馬のサンプル

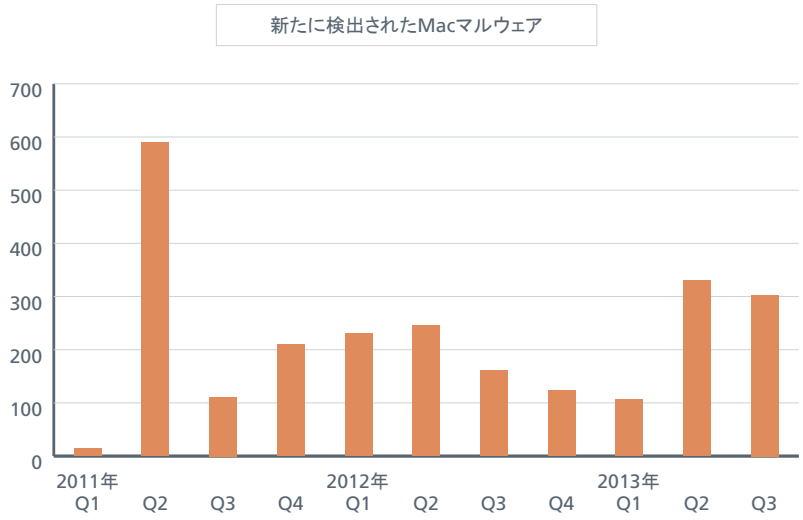


署名付きマルウェアは急増し続けています。検出された新たなサンプル数は 150 万を超え、この四半期に 50% 近く増加して最高記録を更新しています。

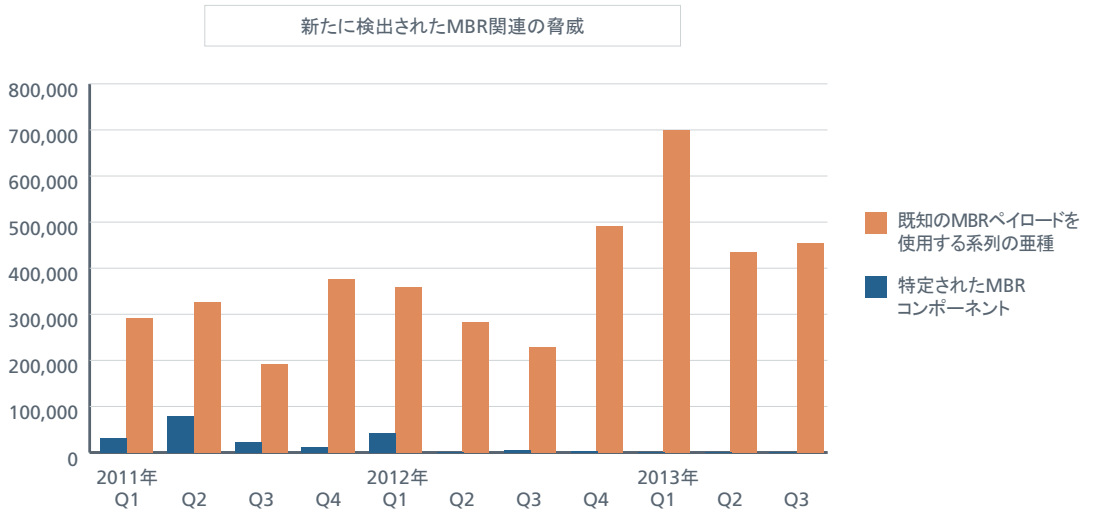




Mac を攻撃する新たなマルウェアは、3 つの四半期に渡って減少した後に、第 2 四半期には 3 倍以上増加しました。この四半期は新たなサンプル数は 300 で、約 10% 減少しました。



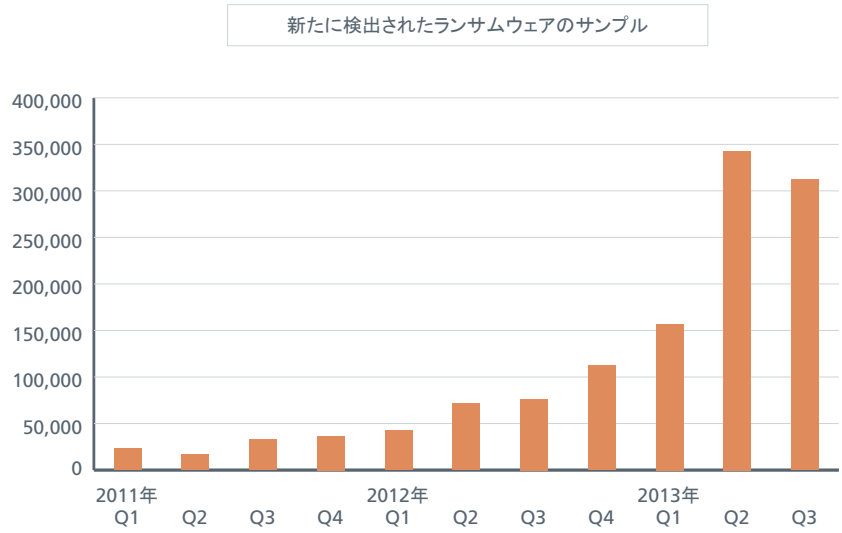
マルウェアの中には、重要なスタートアップ操作を実行する領域であるコンピューターのマスターブートレコード（MBR）を標的にする種類があります。MBR のセキュリティが侵害されると、攻撃者がコンピューターを様々な面でコントロールして潜伏し、奥深くまで侵入することが可能になります。2 つ前の四半期には、記録的な水準に達しましたが、この四半期は前の四半期から微増となっています。



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 31 万 2,000 を超えており、前の四半期からわずかに減少していますが、依然としてこれまでで 2 番目に大きい数字です。

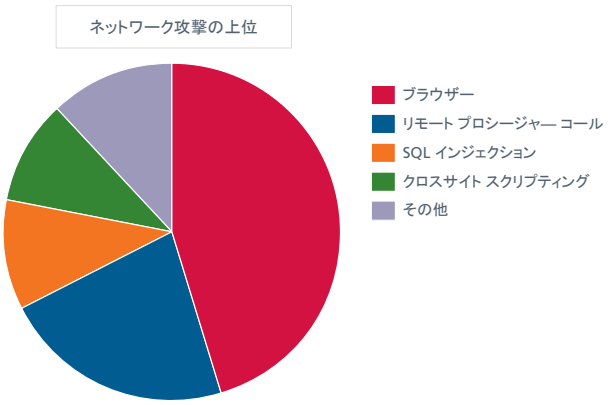
ランサムウェアが普及した理由のひとつは、様々な匿名支払サービスを利用できるため、犯罪者が利益を獲得できる非常に効果的な手段であることです。こうした資金を収集する方法は、たとえば偽のソフトウェアのためにクレジットカード注文の処理が必要となるような、偽のウイルス対策製品を利用する方法よりも優れています。もうひとつの理由としては、アンダーグラウンドのエコシステムがすでに確立しており、Citadel のような、他のマルウェアによって感染したコンピューターへのペイパーインストールといったサービスを利用することが可能で、使い勝手の良い犯罪パックをアンダーグラウンド市場で入手できるからです。



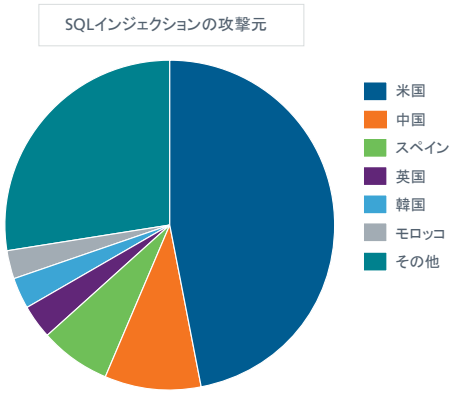
ネットワークの脅威

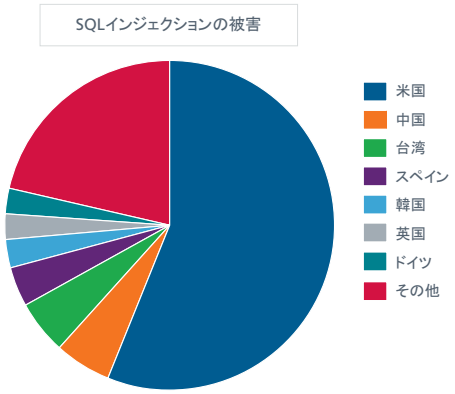
McAfee Global Threat Intelligence ネットワークによれば、ブラウザーベースの脅威は、検出したすべてのネットワーク攻撃の中の 45% を占めており、前の四半期の 73% から減少しています。リモートプロシージャコールは倍増しており、この四半期の攻撃の 22% を占めています。この四半期に大流行した以下の 4 つの検出シグネチャの最初の 2 つは、ブラウザー攻撃が最も多くブロックされたことを明確に示しています。後の 2 つは、リモートプロシージャコール攻撃です。

- HTTP: Mozilla Firefox Click Event Classification Vulnerability
- RTSP: Apple QuickTime Overly Long Content-Type Buffer Overflow
- DCERPC: Suspicious DCERPC Call
- NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability

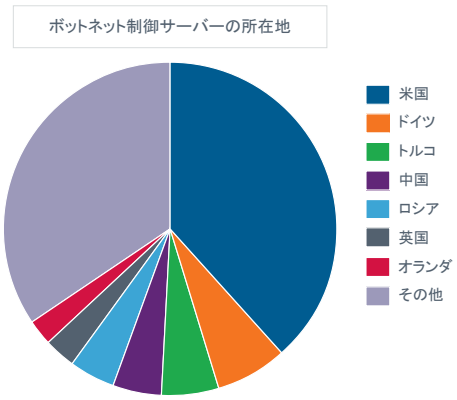


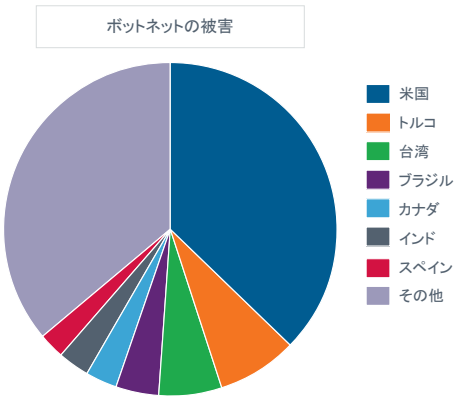
合法的な Web サイトを悪用する SQL インジェクション攻撃の加害者における米国の割合は、この四半期に再び増加し、すべてのインシデントの半分近くを占めています。中国が 9% で、第 2 位となっています。これらの攻撃の被害者の大半（前の四半期の 60% から 56% に減少）は、米国在住です。



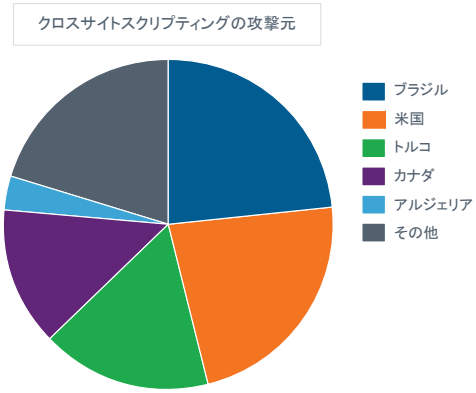


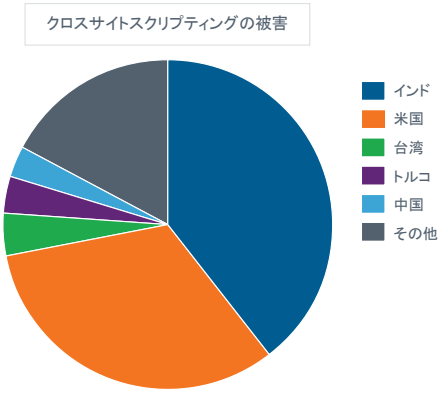
ボットネットの監視調査では、米国および上位を占める残りの国々は、前の四半期とほぼ同じ結果となっており、コントロールサーバーと被害者の場所も同様です。





米国がすべての項目で第 1 位を獲得しているわけではありません。クロスサイトスクリプティングの脅威では、ブラジルが加害者として第 1 位となっており、一方ではインドが他のどの国よりも多くの被害を受けています。

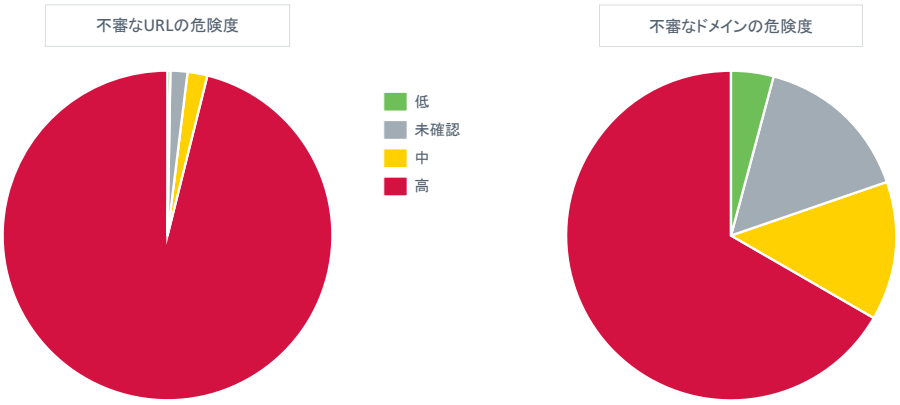




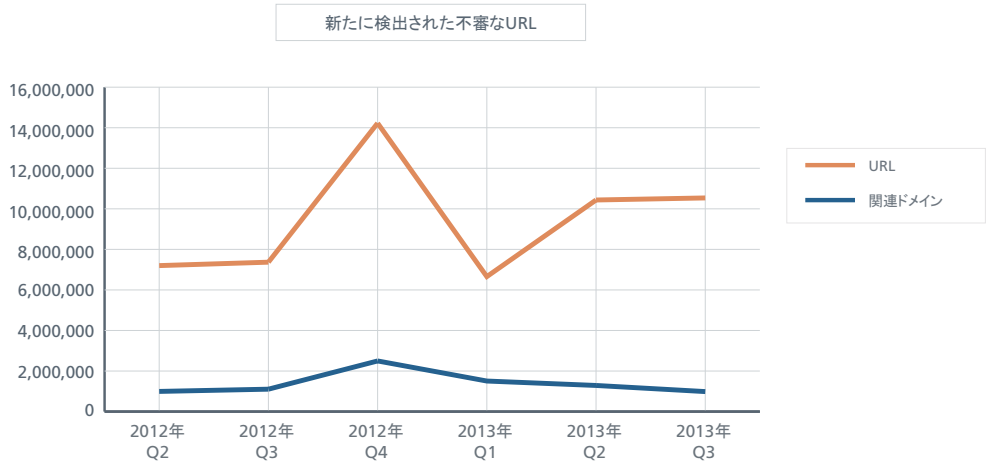
Web の脅威

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。特定の Web オブジェクトのリスク水準をユーザーが把握しやすいように、この評価は、具体的なドメイン、サブドメイン、IP アドレス、具体的な URL に加えて、他の多くのネットワークやファイルの属性に基づいて判断されます。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、登録、ホスティングのパターンといった様々な側面の影響を受けます。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。

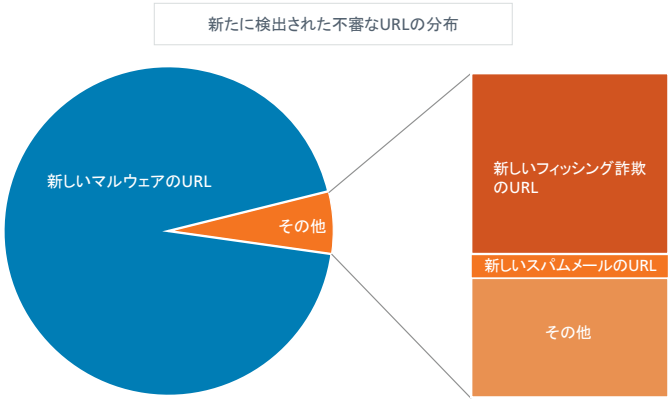
9 月末に、McAfee Labs が集計した疑わしい URL の合計数は、8,500 万を上回り、前の四半期と比べて 14% 増加しています。これらの URL は、3,000 万ものドメイン名を参照しており、以前の期間から 3% 増加しています。



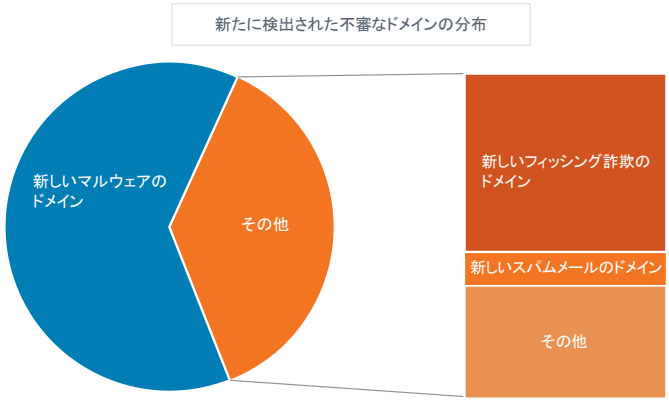
この四半期に、約 33 万のドメインに関して、1 か月あたり平均で 350 万の新たな疑わしい URL を検出しました。



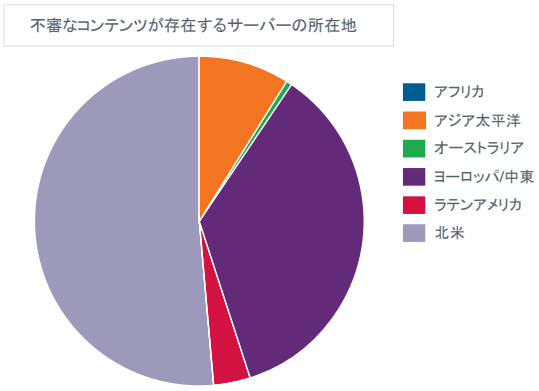
これらの疑わしいURLの大半(94%)には、コンピューターのセキュリティを侵害するために設計されたマルウェア、コード、エクスプロイトが存在します。フィッシング詐欺とスパムメールは、それぞれ 3.5% と 0.4% です。



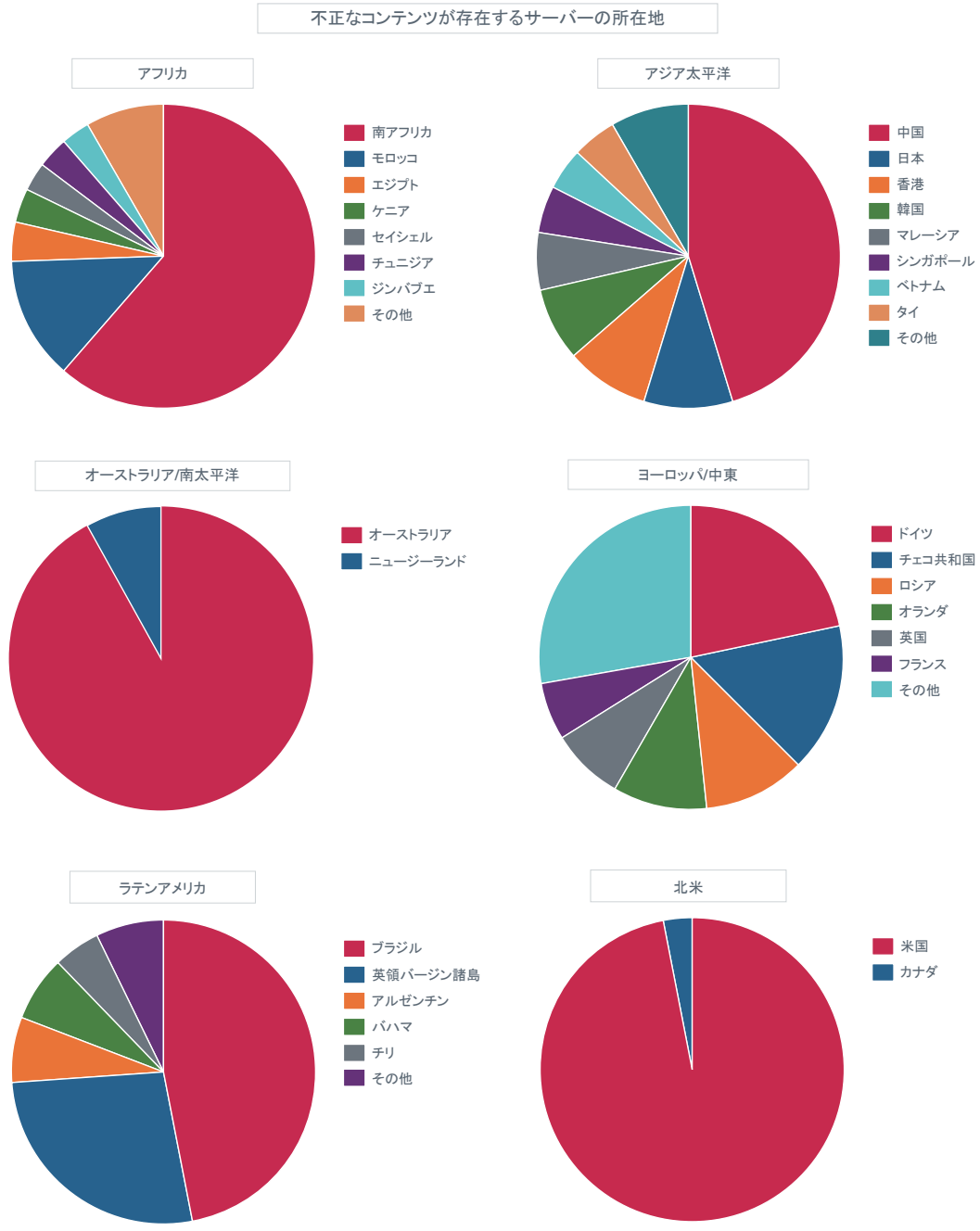
ドメインレベルの分布では、様子が異なっており、フィッシング詐欺ドメインが 20%、スパムメールドメインが 4% です。



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（主にドイツ）と中東に存在します。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、2013 年第 1 四半期の 74% に比べて、この四半期は 51% に落ち込んでいます。

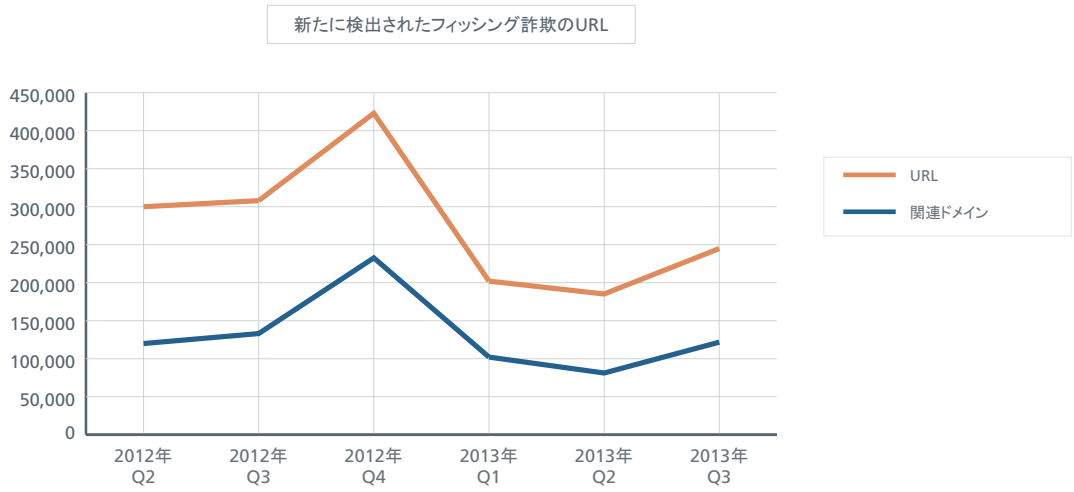


他の国々の悪質なコンテンツをホスティングしているサーバーの場所を詳しく見ていくと、非常に多様であることがわかります。ヨーロッパを除いた各地域では、1 つまたは 2 つの国が大部分を占めています。

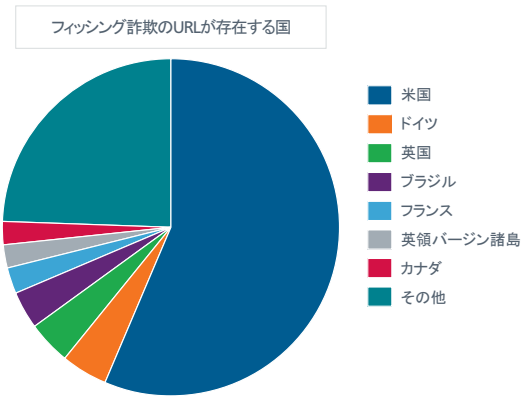


フィッシング詐欺

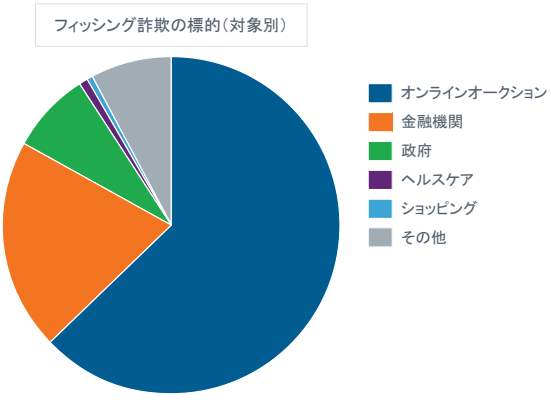
新たなフィッシング詐欺の URL 数は、2012 年第 4 四半期にピークを迎えた後に、2013 年の前半では激減しました。この四半期は増加に転じています。



こうした URL の大半は、米国に存在しています。

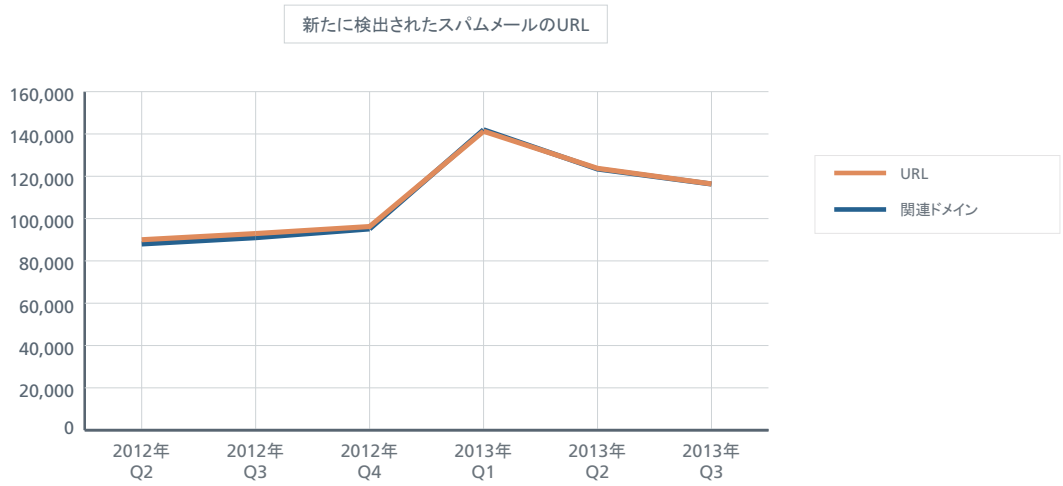


フィッシング詐欺の攻撃者は複数の主要な業界を標的としています。上位 3 つの業種は、オンラインオークション、金融、政府機関です。

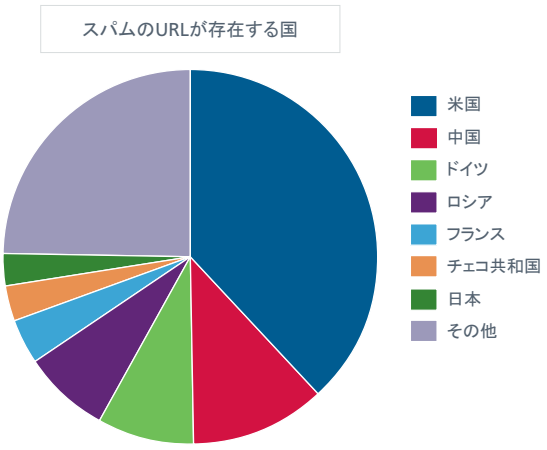


スパム URL

スパムの URL 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。

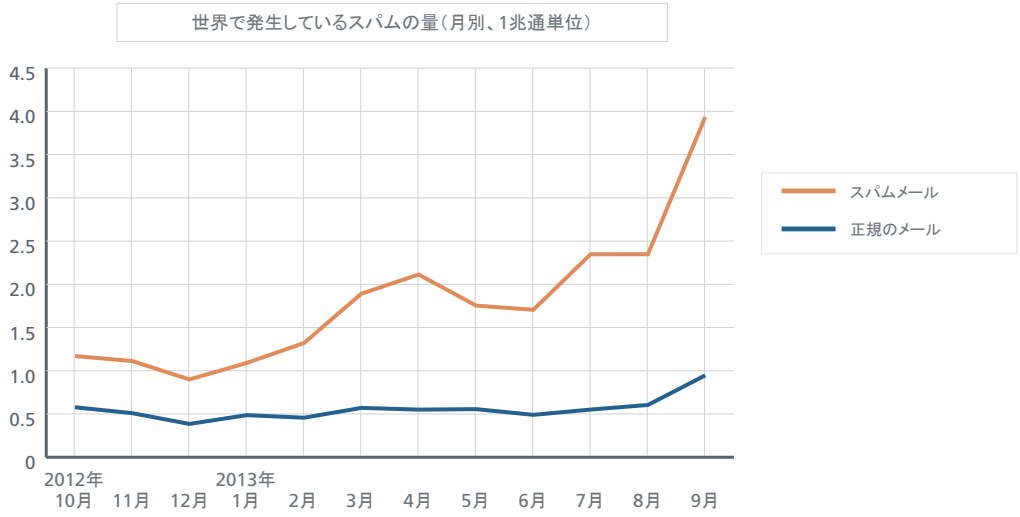


こうした URL をホスティングしている主要な国は、米国、中国、ドイツ、ロシアです。



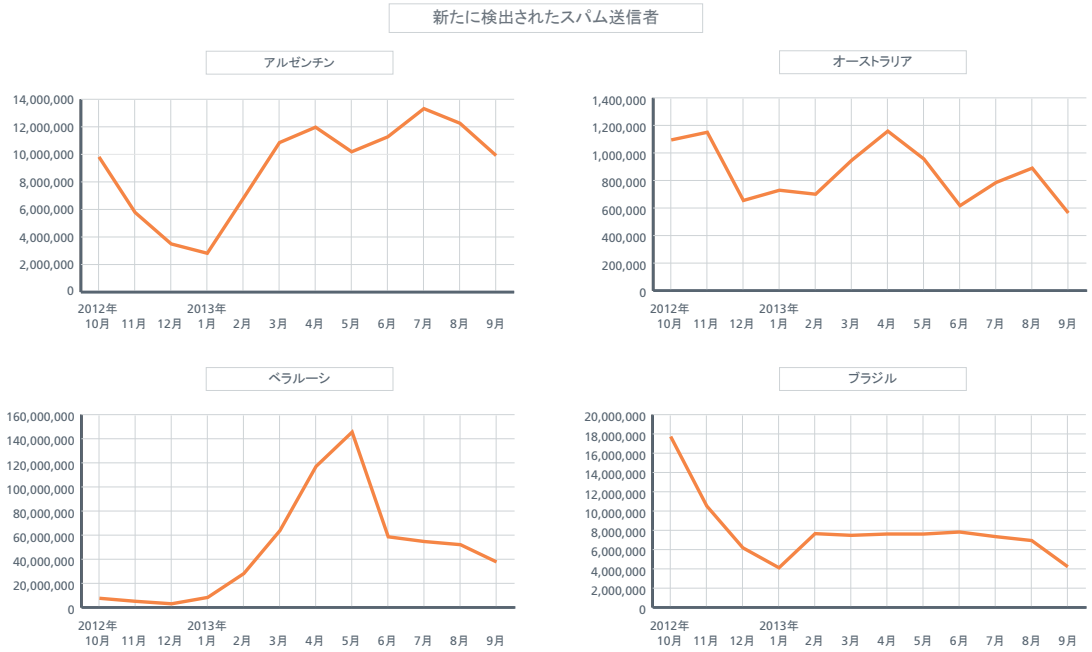
メッセージングの脅威

この四半期の全世界のスパムの量は、5 月と 6 月に若干減少した後に倍以上増加しました。スパムの量は、2010 年 8 月以降では最も高い水準に達しました。



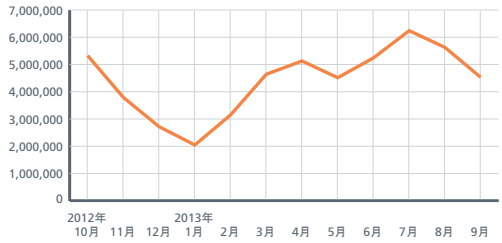
スパムの量

様々な国々の新たなスパムの送信者を調べると、四半期ごとに大きな違いが見られます。中国とイタリアはこの四半期に 50% 以上増加しましたが、カザフスタン（61% 減少）、ベラルーシ（55% 減少）、ウクライナ（51% 減少）では激減しています。

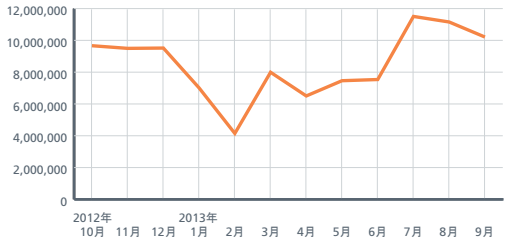


新たに検出されたスパム送信者

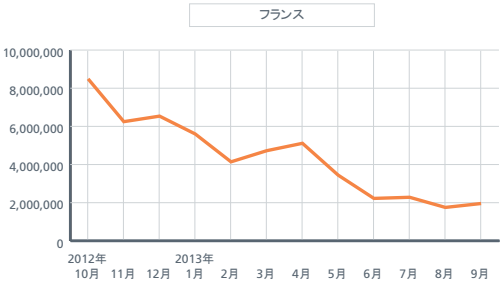
チリ



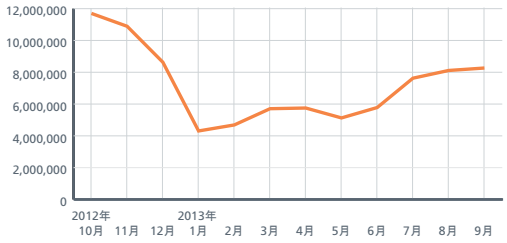
中国



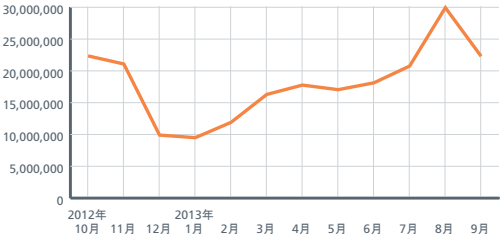
フランス



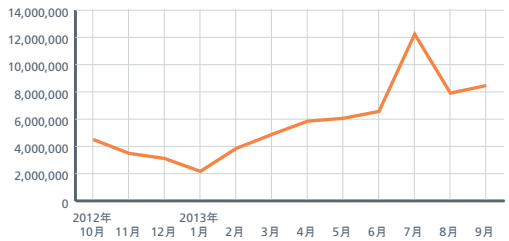
ドイツ



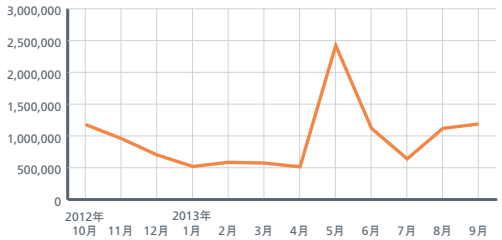
インド



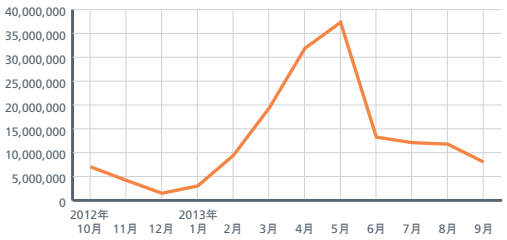
イタリア



日本

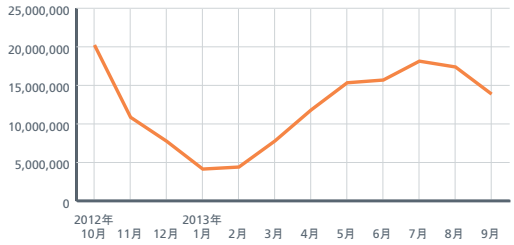


カザフスタン

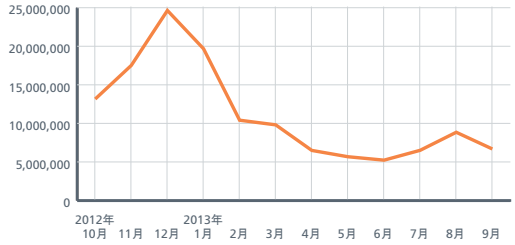


新たに検出されたスパム送信者

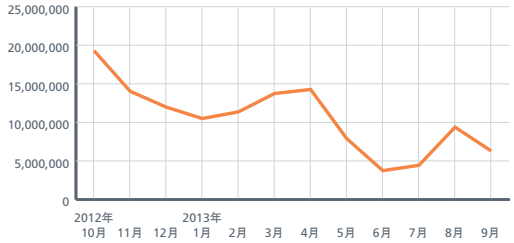
ペルー



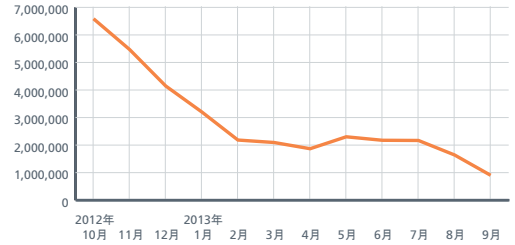
ルーマニア



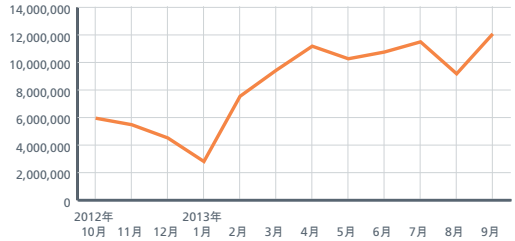
ロシア



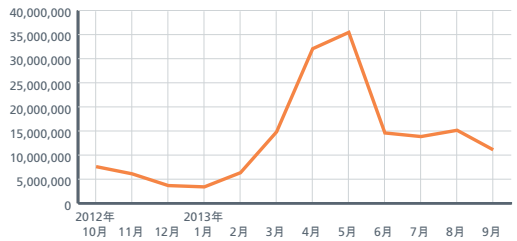
韓国



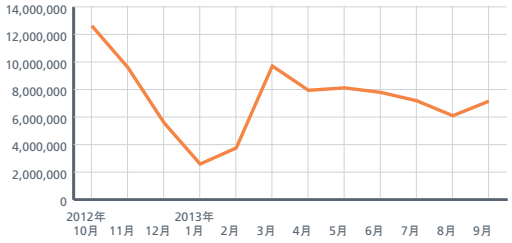
スペイン



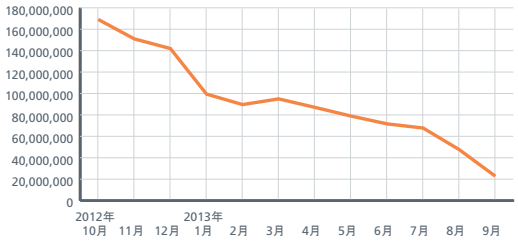
ウクライナ



英国



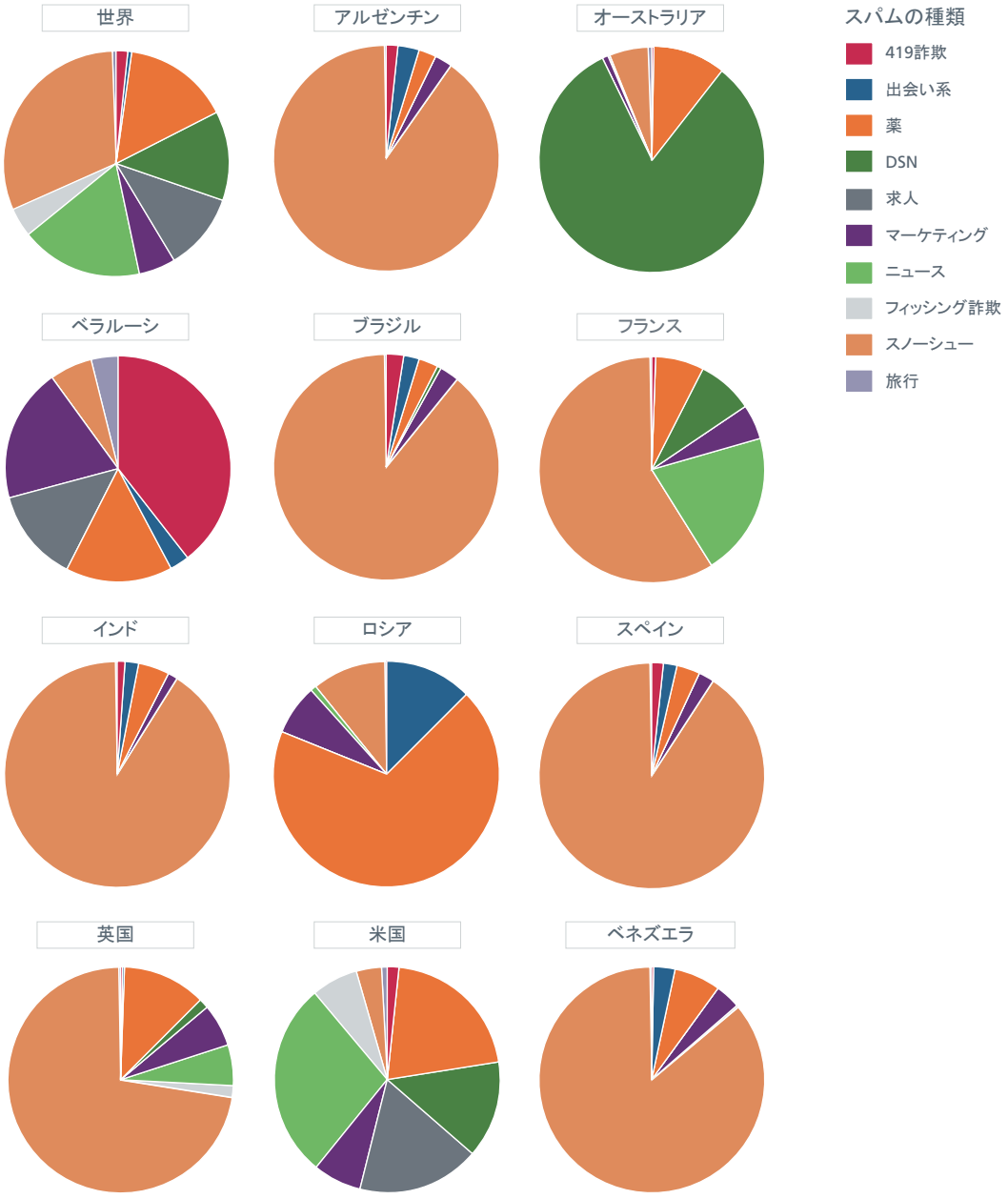
米国



スノーシューを介して世界を駆け巡るスパム

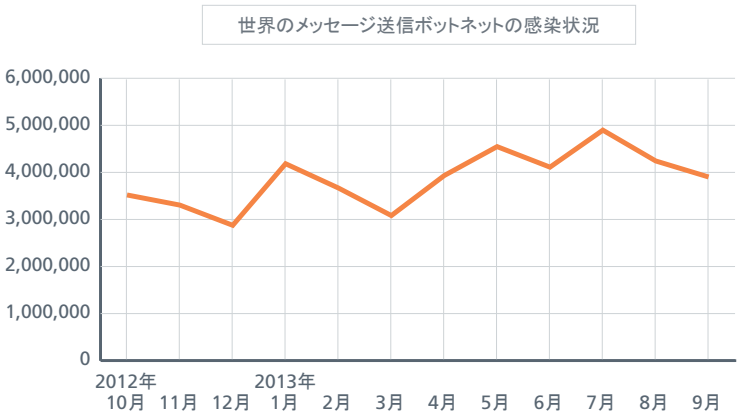
この四半期に最も多かったスパムの種類は、「スノーシュー」スパムでした。このスパムは、ISP による迅速なエビクションを回避するために、多くの IP アドレスにロードを拡散するので、このような名称が付けられました。大半の国々では、スノーシュースパムがかなりの部分を占めているのが確認されており、多くの場合、主要な件名の 85% から 95% を占めています。これは、国の過剰なホスティング能力が利用されている証拠であると考えられます。通常、この種類のスパムは、ホスティング施設がスパム送信者を強制的に排除するかブラックリストに掲載するまで、ホスティング施設のサーバーを借りてスパムを送信します。

ベラルーシでは、「419」詐欺が最も多くなっています。こうしたメールでは、通常は「裕福」である不運なアフリカ人にお金を送ると、助けてくれた人に後から十分なお礼をするとアピールします。お金を送った後に何が起こるかは予測がつくと思います。オーストラリアと米国では、配信通知サービス（DSN）が一般的です。ロシアではドラッグとオンラインの花嫁のスパムが人気です。米国では、スパム送信者は、主要な誘い文句としてドラッグに加えて、偽のニュースと仕事を利用することで、バランスのとれた攻撃を行っています。下記の「全世界」の円グラフは、このページに記載した国々のみ対象としており、世界のすべての国々が含まれているわけではありません。

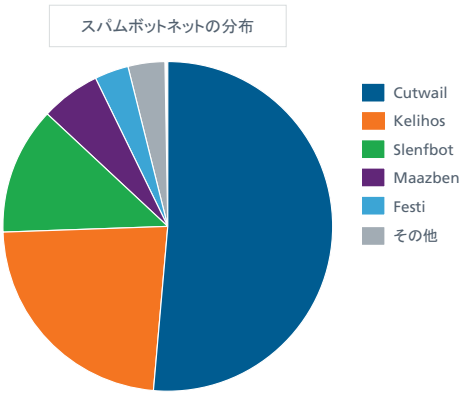


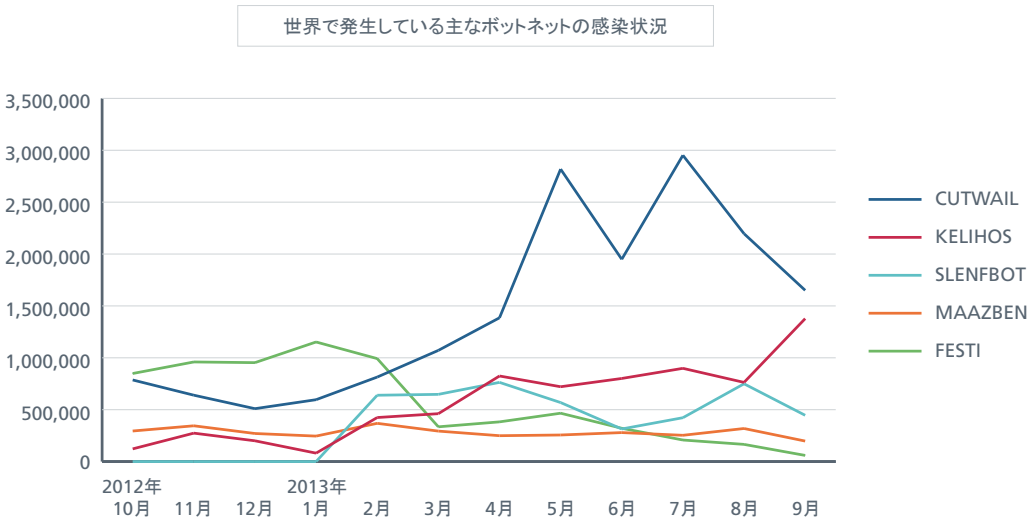
ボットネットの詳細

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が、四半期を追うごとに、全体的に上昇する傾向を伴って増加と減少を繰り返しています。



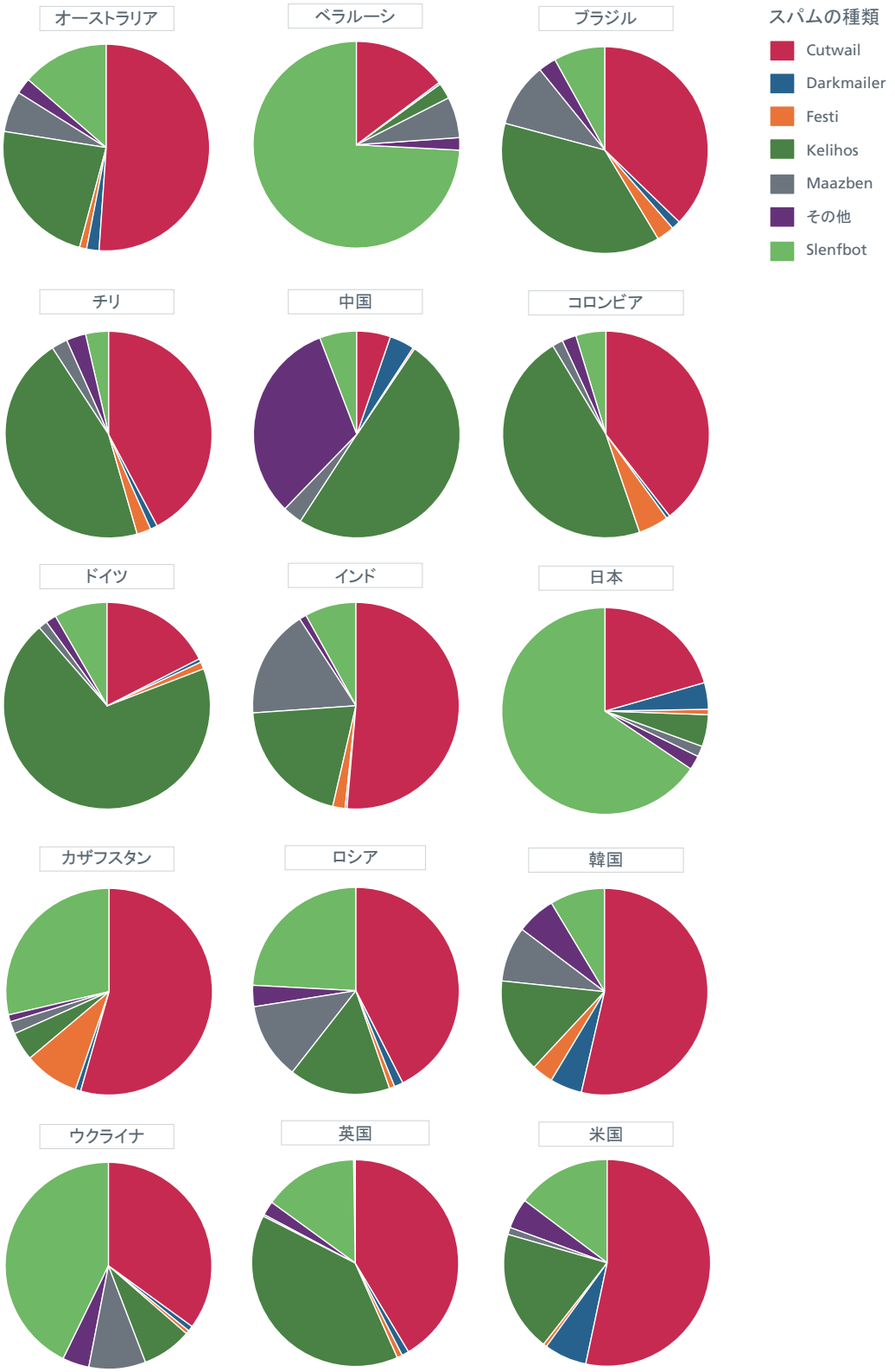
Cutwail は第 1 位の座を維持しているボットネットであり、2012 年の終わりに初めて登場した Kelihos が再び第 2 位となっています。2013 年の第 1 四半期に新しく登場した Slenfbot は引き続き第 3 位です。





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、世界中の様々な国に存在していることがわかります。Cutwail が世界的に大部分を占めており、9 月には Kelihos が第 1 位に迫りました。



筆者について

本レポートは、McAfee Labs の Benjamin Cruz、Paula Greve、François Paget、Craig Schmugar、Jimmy Shah、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—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/us/resources/white-papers/wp-digital-laundry.pdf
2 http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf
3 http://info.tapjoy.com/wp-content/uploads/sites/4/2013/05/RedefiningVirtualCurrency_WhitePaper-1MAY2013-v1.pdf
4 http://krebsonsecurity.com/2013/10/feds-take-down-online-fraud-bazaar-silk-road-arrest-alleged-mastermind/
5 http://blogs.mcafee.com/consumer/android-malware-set-for-july-4-carries-political-message
6 http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf
7 http://www.infosecurity-magazine.com/view/33544/rex-mundi-hackers-post-data-stolen-from-numericable/
8 http://news.softpedia.com/news/Rex-Mundi-Hackers-Blackmail-Italian-Hosting-Service-Websolutions-it-366685.shtml
9 http://blogs.mcafee.com/mcafee-labs/the-dangers-of-a-royal-baby-scams-abound
10 http://news.xinhuanet.com/english/world/2013-07/26/c_132577334.htm
11 http://www.welivesecurity.com/2013/07/30/versatile-and-infectious-win64expiro-is-a-cross-platform-file-infector
12 http://www.buzzfeed.com/michaelrusch/thompson-reuters-twitter-account-apparently-hacked
13 http://www.dailydot.com/news/sea-syrian-electronic-army-white-house-staffers/
14 http://blogs.mcafee.com/mcafee-labs/java-back-door-acts-as-bot
15 http://www.ehackingnews.com/2013/08/exclusive-british-channel-4-blog-hacked.html
16 https://blogs.rsa.com/thieves-reaching-for-linux-hand-of-thief-trojan-targets-linux-inth3wild
17 http://blogs.mcafee.com/mcafee-labs/bitcoin-miners-use-autoit-complied-programs-with-antianalysis-code
18 http://blogs.mcafee.com/mcafee-labs/andromeda-botnet-hides-behind-autoit
19 http://blogs.mcafee.com/mcafee-labs/vertexnet-botnet-hides-behind-autoit
20 http://blogs.mcafee.com/mcafee-labs/hesperus-evening-star-shines-as-latest-banker-trojan
21 http://blogs.technet.com/b/srd/archive/2013/09/17/cve-2013-3893-fix-it-workaround-available.aspx
22 McAfee MTIS13-154.pdf: https://community.mcafee.com/docs/DOC-5302
23 http://www.escapistmagazine.com/news/view/123676-Rogue-Bitcoin-Code-Found-in-Competitive-Counter-Strike-Servers
24 http://www.wired.com/wiredenterprise/2013/07/esea-2/
25 http://www.theguardian.com/technology/2013/jul/24/bitcoin-alleged-ponzi-fraud
26 http://www.irishmirror.ie/news/irish-news/extradition-case-child-porn-accused-2170785
27 http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/
28 https://community.rapid7.com/community/metasploit/blog/2013/08/07/heres-that-fbi-firefox-exploit-for-you-cve-2013-1690
29 http://ia600904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf
30 http://www.forbes.com/sites/kashmirhill/2013/08/12/every-important-person-in-bitcoin-just-got-subpoenaed-by-new-yorks-financial-regulator/
31 http://thegenesisblock.com/security-vulnerability-in-all-android-bitcoin-wallets/
32 http://www.welt.de/finanzen/geldanlage/article119086297/Deutschland-erkennt-Bitcoin-als-privates-Geld-an.html
33 http://rt.com/business/bitcoin-atm-canada-vancouver-717/
34 http://krebsonsecurity.com/2013/07/hacker-ring-stole-160-million-credit-cards/
35 http://www.pokernewsdaily.com/poker-professional-masaaki-kagawa-arrested-for-malware-ring-24285/
36 A KVM (keyboard, video, and mouse) switch is a hardware device that can allow users to remotely operate their work computer systems.
37 http://www.dailymail.co.uk/news/article-2426519/Gang-arrested-1-3million-Barclays-hijack-plot-carbon-copy-Santander-scam.html
38 http://www.huffingtonpost.com/2013/08/21/anonymous-arrests-fbi_n_3780980.html
39 http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf
40 http://hackread.com/egyptian-ministry-sites-hacked-anonymous-jordan/
41 http://post.jagran.com/pakistan-launches-cyber-war-against-india-hacks-72-websites-1376474598
42 http://news.softpedia.com/news/Indian-Hacker-Breaches-Pakistan-Army-s-Website-and-Facebook-Pages-374298.shtml
43 http://www.stripes.com/news/hackistan-afghan-cyber-guerrillas-step-up-attacks-on-pakistani-websites-1.234947
44 http://www.foxbusiness.com/industries/2013/08/15/chase-website-suffers-intermittent-outage/
45 http://www.washingtonpost.com/blogs/ask-the-post/wp/2013/08/15/editors-note
46 http://hackread.com/syrian-electronic-army-hacks-sharethis-godaddy-acc-and-redirects/
47 http://qz.com/119245/how-the-syrian-electronic-army-hacked-the-new-york-times-twitter-and-the-huffington-post/
48 http://hackread.com/sea-hacks-fox-tv-hootsuite-social-media-account/
49 http://info.publicintelligence.net/FBI-SEA.pdf
50 (Explicit content) http://reflets.info/opsyria-syrian-electronic-army-was-hacked-and-d0xed-warning-explicit-content/
51 http://krebsonsecurity.com/2013/08/syrian-electronic-army-denies-new-data-leaks/
52 http://www.theregister.co.uk/2013/09/18/honker_union_270_japan_targets_manchurian_incident/
53 http://beijingcream.com/2013/09/hackers-post-anti-ccp-mooncakes-to-shaoxing-website/

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）