レポート

McAfee
An Intel Company

McAfee 脅威レポート：2012 年第 1 四半期

McAfee Labs™

目次

ギリシャの哲学者ヘラクレイトスは「万物は絶え間なく流転する」と説いていますが、2012 年第 1 四半期の脅威状況はこの言葉通りといえます。2011 年の終わりには、多くの地域でマルウェアと脅威の減少が確認されましたが、今四半期はそれとは対極の状態です。PC を攻撃するマルウェアの数はここ最近で最も多く、携帯端末を狙うマルウェアも大幅に増加しています。すでに確認しているルートキットだけでなく、新しい系列のルートキットも出現しました。これまで分析し、戦ってきた多くのマルウェアが息を吹き返しています。特に、パスワード盗用型トロイの木馬の動きは顕著です。今回の『脅威レポート』では、ZeroAccess ルートキットや署名付きマルウェアなどの新たな脅威について報告します。また、ネットワーク攻撃の詳細についても説明します。

この四半期の初めはスパムの量が増加しましたが、再び減少しています。Mac を狙うマルウェアの数は増加しています。極端な動きではありませんが、勢いを増していることは確かです。

世界で発生しているスパムの量は減少傾向にありますが、詳しく見ると状況は地域ごとに異なります。たとえば、ドイツや中国ではスパムの量が増加しています。この四半期は新しいボットネットの感染は減少していますが、スペイン、日本などの国ではむしろ増加しています。

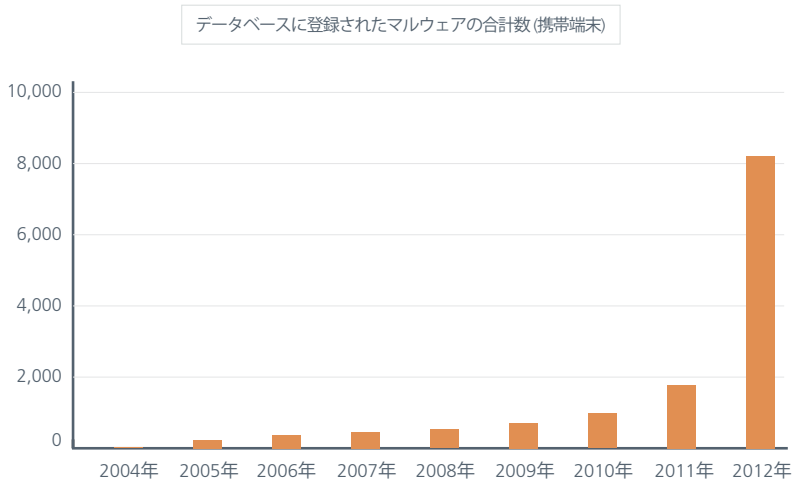
不正なコンテンツの分布を見ると、この四半期も米国がトップになっています。この傾向については「ネットワークの脅威」のセクションで詳しく説明します。攻撃の発生元と攻撃対象に関する国別の統計情報も示します。活動中の不正な URL の数は引き続き増加しています。保護対策が万全でないユーザーにとって Web は引き続き危険な存在となっています。

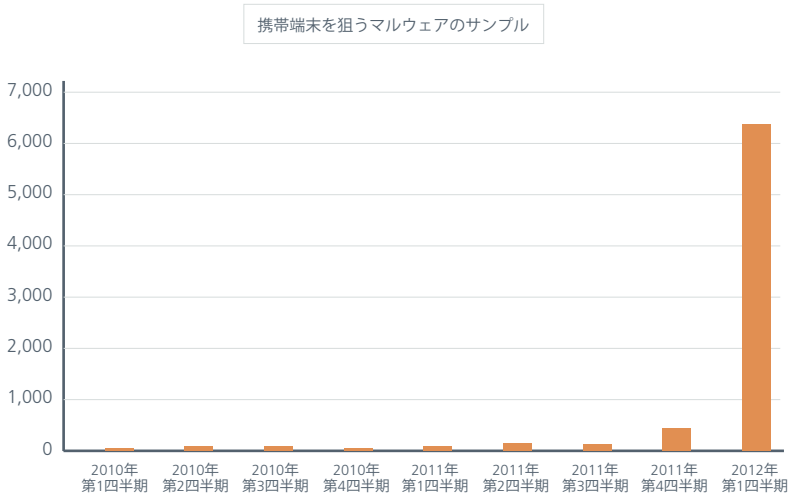
この四半期は Java と Flash の脆弱性を悪用するエクスプロイトが増えています。サイバー犯罪の取り締まりも成果を挙げ、重要なサイバー犯罪者やハクティビストの逮捕に成功しています。最も大きな成果は kelihos/waledac ボットネットの閉鎖と、Anonymous と LulzSec の幹部の逮捕でしょう。他の分野の脅威はいまだに衰えていませんが、捜査当局の成果は賞賛に値するものです。

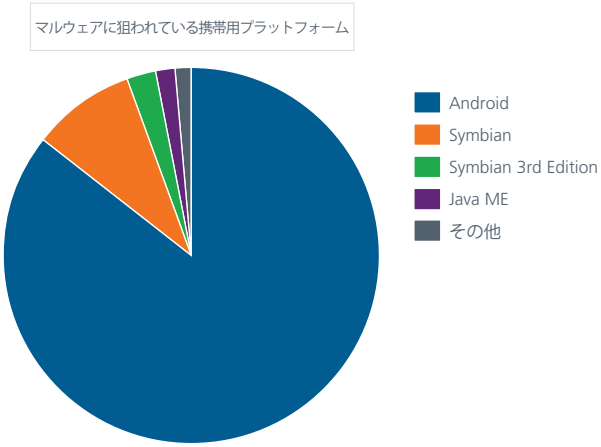
脅威は常に変化しています。攻撃者も自分の技術を磨いています。このような脅威や攻撃者に対抗するには、引き続き十分な警戒が必要です。

モバイルの脅威

この四半期は携帯端末を狙うマルウェアが大幅に増加しました。 その殆どが Android プラットフォームを標的とするもので、 2011 年の中頃は数百単位であった Android の脅威も今年に入り数千単位と勢いを増しています。 この四半期に急増した要因としては、 我々のモバイル マルウェアの収集・検出能力が大幅に向上したことも挙げられます。 現在、 マカフィーのデータベースに登録されている Android の脅威は約 7,000 件、 モバイル マルウェア合計では 8,000 件を超えています。







携帯端末を狙う攻撃やマルウェアの大半は非公式のマーケット、特に中国とロシアのマーケットから発生しています。このようなマルウェアは正規の Android マーケットでは殆ど見られません。Google のアプリストアからマルウェアが配信された事件もありましたが、今までのところ、その数はそれ程多くはありません。ソフトウェアをインストールする際には正規のマーケットを利用するべきです。これだけでも Android 端末の感染リスクが大幅に軽減されます。

この四半期は、プレミアム SMS 送信型の単純なマルウェア以外に新種のアドウェアやバックドア型マルウェアが急増しました。アドウェアは利用者の許可なしに携帯端末に広告を表示します（広告収入で運営しているゲームやアプリを除く）。待ち受け画面に宣伝を追加するもの（Android/Nyearleaker.A）だけでなく、偽のゲームを表示し利用者を広告サイトに誘導するもの（Android/Steek.A）もあります。アドウェアは必ずしもセキュリティを侵害するものではありませんが、不要な広告を表示する迷惑なものであることに変わりありません。

Android に感染するバックドア型トロイの木馬もより巧妙になり、ルート エクスプロイトを利用して別のマルウェアを起動するなど、複雑な処理を行うものが増えています。たとえば、Android/FoncyDropper.A はルート エクスプロイトを使用して携帯電話を乗っ取り、IRC ボットを開始して攻撃者からの命令を待機します。さらに、SIM カードの国情報を読み取り、プレミアム SMS にメールを送信します。

また、Android/Rootsmart.A はルート エクスプロイトを使用してバックドア型トロイの木馬の Android/DrdLive.A をダウンロードし、プレミアム SMS にメールを送信し、制御サーバーからの命令を受信します。

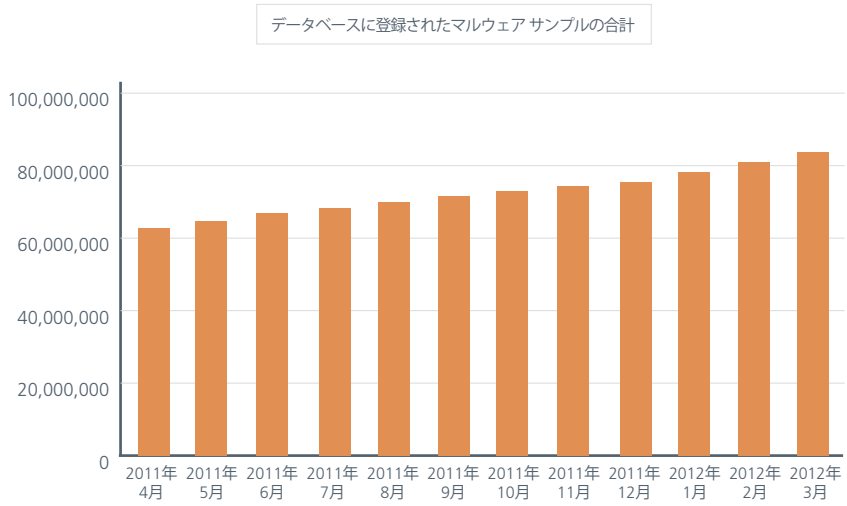
Android/Stiniter.A は、ルート エクスプロイトを利用して別のマルウェアをダウンロードし、携帯電話から収集した情報を攻撃者のサイトに送信します。攻撃者の制御サーバーで SMS の本文と送信先の電話番号を書き換え、プレミアム SMS にメールを送信します。

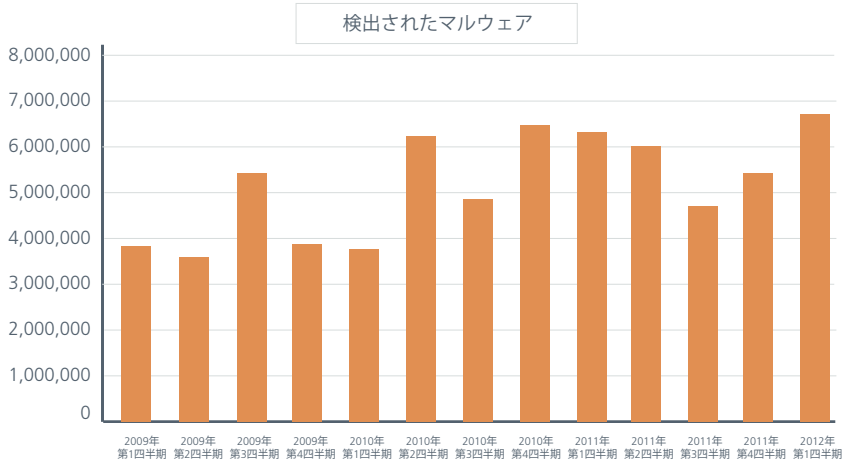
この四半期には Android で破壊行為を行う最初のトロイの木馬である Android/Moghava.A が見つかりました。このマルウェアはアプリケーションや他の実行ファイルを破壊しません。SD カードに保存されている写真を検索し、その画像にイランのホメイニ師の写真を追加します。バグかどうかは分かりませんが、SD カードの空き容量がなくなるまで写真を追加し続けます。

重要なデータを含むすべてのデバイス、携帯端末を保護する必要があります。無防備な状態では、これらの情報がサイバー犯罪者に簡単に盗まれ、悪用されてしまいます。

マルウェアの脅威

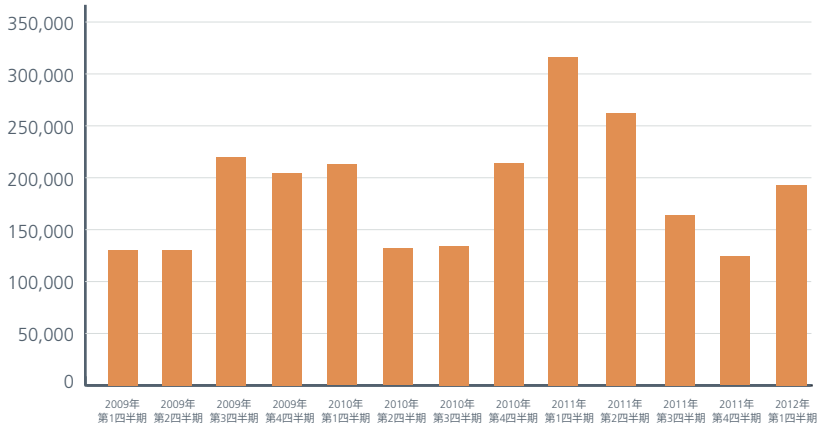
現在のマルウェアの状況を簡単に表すと、Thin Lizzy の "The boys are back in town"（ヤツらは町へ）のような状態と言えるでしょう。PC を狙うマルウェアの勢いは 2011 年後半に一時的な停滞期に入りましたが、この状態は終わりを告げ、この四半期は過去 4 年間で最も多くのマルウェアを検出しました。2012 年に入り、McAfee Labs では 7,500 万件以上の新しいマルウェアのサンプルを検出しています。マカフィーのデータベースにはすでに 8,300 万件のマルウェアが登録されており、恐らくこの 2,3 四半期の間に1億件に達することは確実であると思われます。ルートキットの増加、機能の巧妙化、署名付きのマルウェアの出現、様々な脅威の蔓延など、現在の状況を勘案すると、セキュリティ業界にとって 2012 年は非常に厳しい一年になることが予想されます。



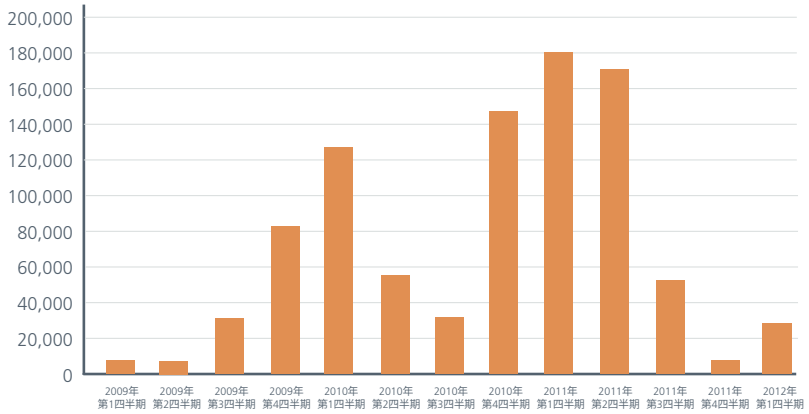


1 年前の最高値には程遠いものの、この四半期は再びルートキットが増加しています。最も活発なルートキットは Koutodoor でしたが、本レポートの冒頭で触れた ZeroAccess も急増しています。このマルウェアはすでにサイバー犯罪者や悪意のあるハッカーの間でよく知られた存在になっています。ルートキット（ステルス性マルウェア）はマルウェアの中で最も厄介な存在で、他のマルウェアにも大きな影響を及ぼします。ルートキットは検出を回避し、システムに長期間潜伏します。

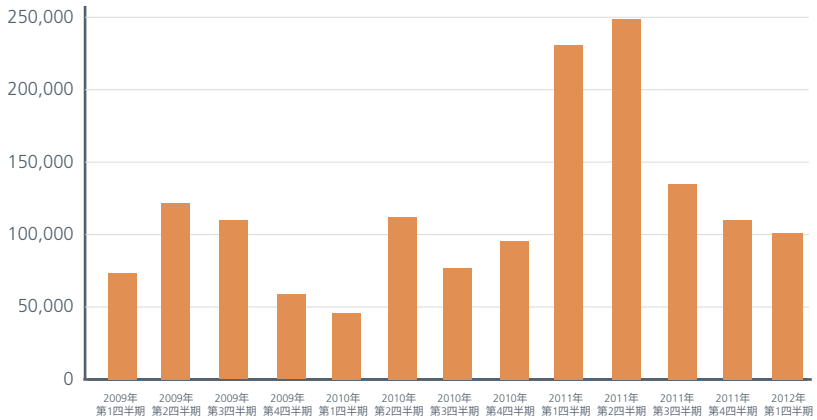
検出されたルートキットのサンプル

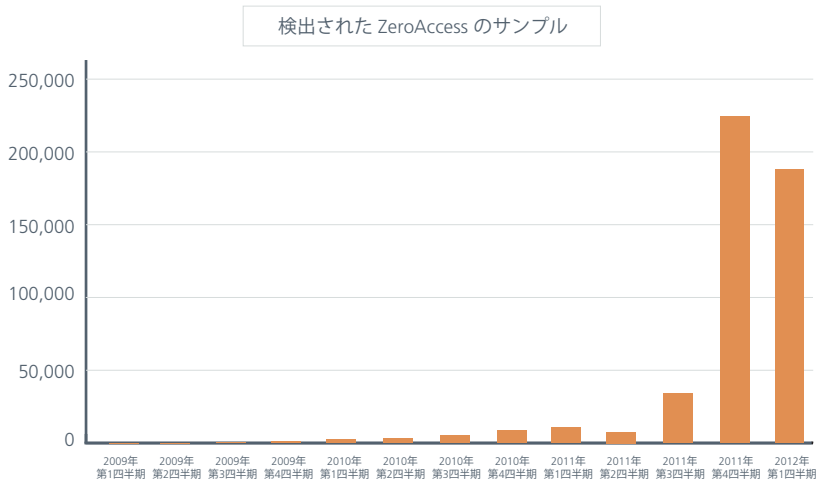


検出された Koutodoor のサンプル

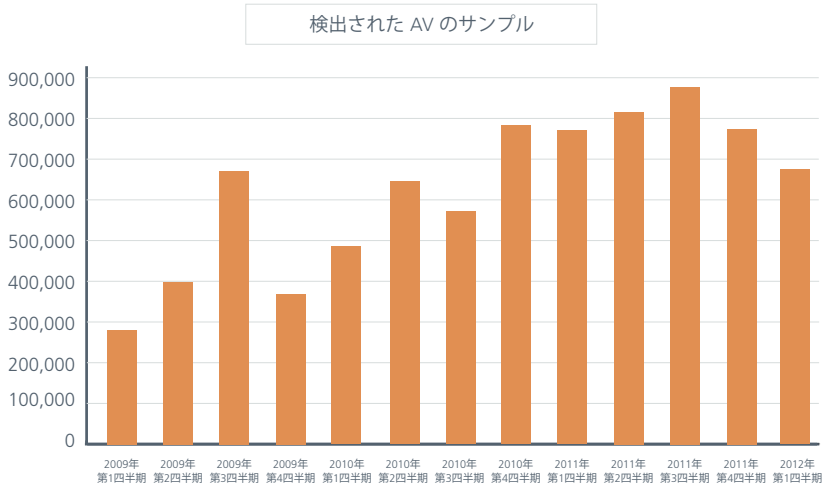


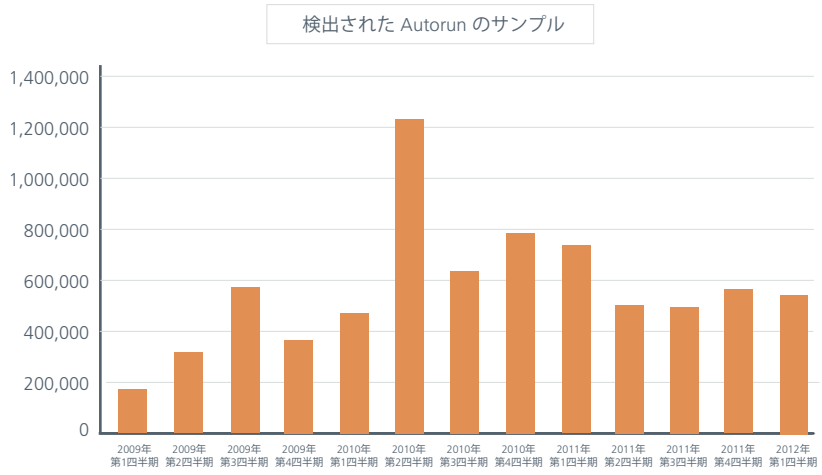
検出された TDSS のサンプル

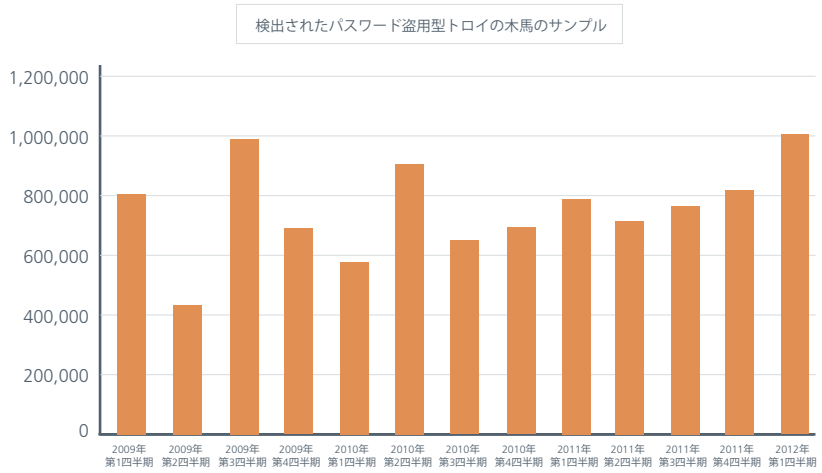




他のマルウェアの状況を見てみると、偽の AV（不正なセキュリティ ソフトウェア）と AutoRun は下降気味ですが、パスワード盗用型トロイの木馬は引き続き増加傾向を維持しています。





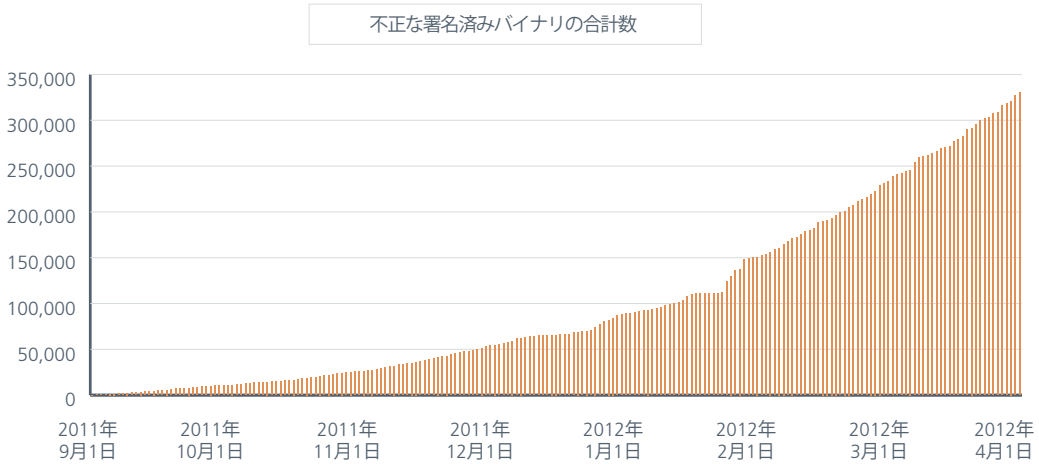


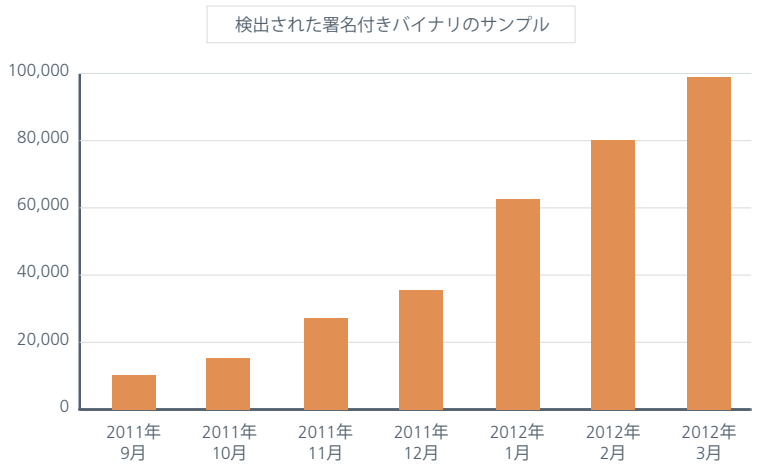
署名付きのマルウェア

マルウェアの作成者がマルウェアに署名を付ける理由について、 McAfee Labs の上級研究員である Craig Schmugar はブログで次のように説明しています。

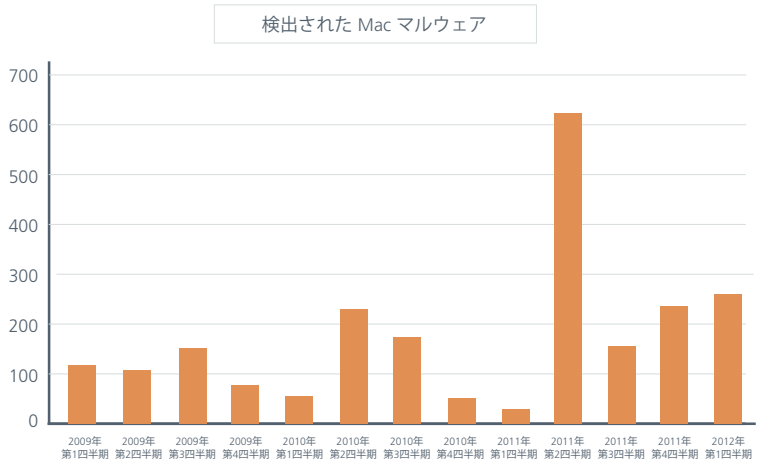
「攻撃者がマルウェアに署名を付けるのは、 ユーザーや管理者を騙してファイルを信用させるためだけではない。 セキュリティ ソフトウェアやシステム ポリシーによる検出を回避させる目的もある。 このようなマルウェアの大半は盗まれた証明書で署名されているが、 自己署名またはテスト署名の付いたバイナリも存在する。 テスト署名はソーシャル エンジニアリングでも利用されている。」[1]

この四半期は、 有効なデジタル署名が付いている新しいマルウェア バイナリが 200,000 種類以上検出されています。『2012 年の脅威予測』では、 Duqu や Stuxnet の成功に刺激を受けてこのようなマルウェアが増加すると予想しましたが[2]、 この予測は 3 か月後に現実のものとなりました。

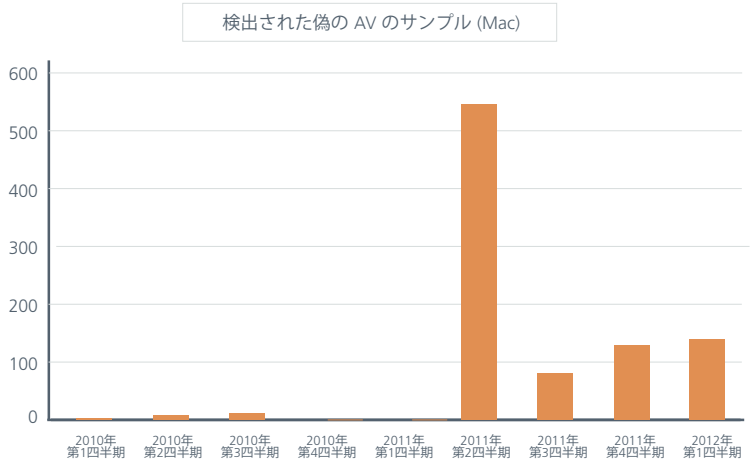




Apple の Mac OS を狙うマルウェアも引き続き増加しています。 PC のマルウェアと比較すると、 それほど多くはありませんが、 マルウェアの標的にならないオペレーティング システムやプラットフォームはありません。 使用している OS やプラットフォームに関わらず、 予防策を講じるべきしょう。

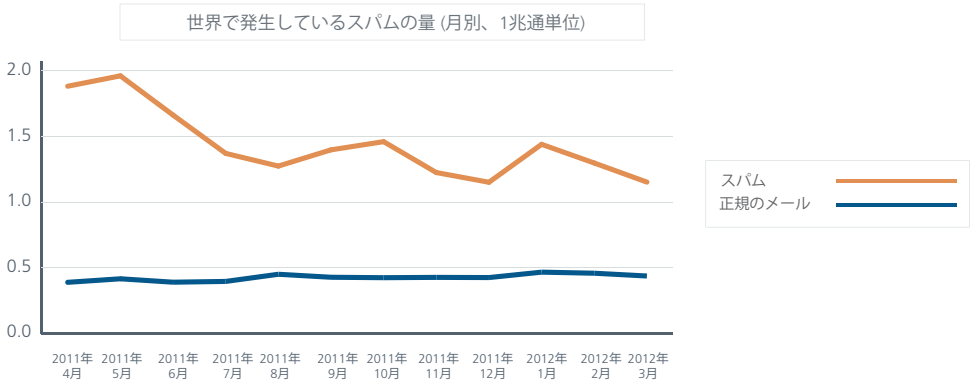


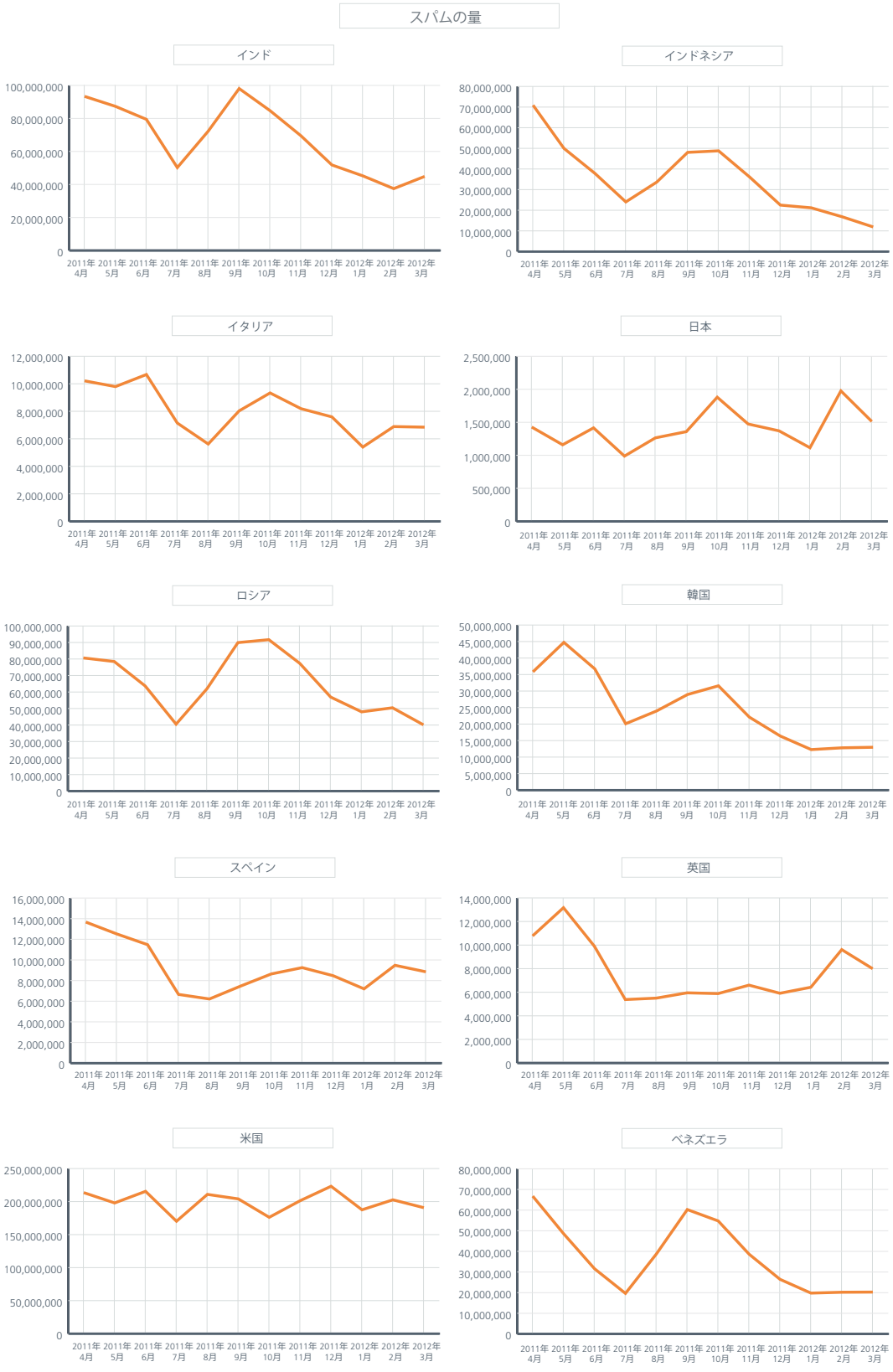
Mac を狙う偽の AV マルウェアは、昨年の中頃に急増しましたが、現在は落ち着いた状態が続いています。



メッセージングの脅威

前回の脅威レポートで報告しましたように、 世界で発生したスパムの量は 2011 年の終わりに過去数年で最低の値を記録しました。 今年の 1 月に一時的に増加しましたが、 この四半期の最後には前の四半期の最低水準に戻っています。 この 3 か月間を見ると、 中国、 ドイツ、 ポーランド、 スペイン、 英国で増加していますが、ブラジル、インドネシア、ロシアでは減少しています。 世界全体では減少傾向にあるものの、スピアフィッシングやスパムの危険性は依然として衰えていません。 現在の脅威は非常に巧妙です。 個人ユーザー、 企業にかかわらず、 引き続き警戒が必要です。

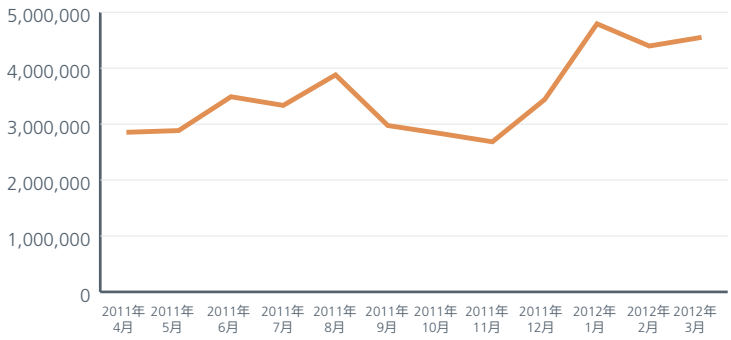



スパムの量
インド
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
インドネシア
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
イタリア
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
日本
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
ロシア
100,000,000
90,000,000
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
韓国
50,000,000
45,000,000
40,000,000
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
スペイン
16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
英国
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
米国
250,000,000
200,000,000
150,000,000
100,000,000
50,000,000
0
ベネズエラ
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
2011年 4月
2011年 5月
2011年 6月
2011年 7月
2011年 8月
2011年 9月
2011年 10月
2011年 11月
2011年 12月
2012年 1月
2012年 2月
2012年 3月

ボットネットの詳細

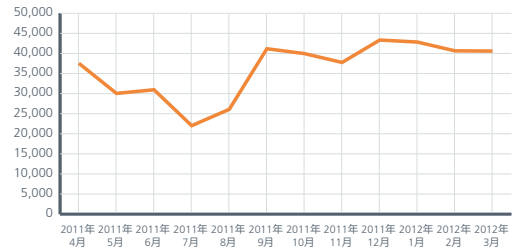
メッセージを送信するボットネットが急増しています。 国別にみると、 コロンビア、 日本、 ポーランド、 スペインでは増加、 米国、 インドネシア、 ポルトガル、 韓国では減少傾向が続いています。

世界のボットネット感染

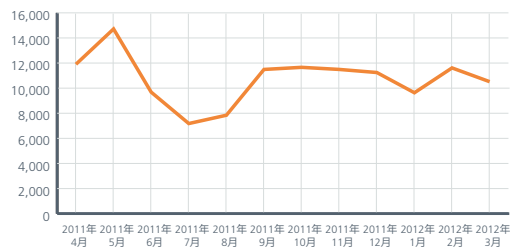


検出されたボットネットの送信者 (国別)

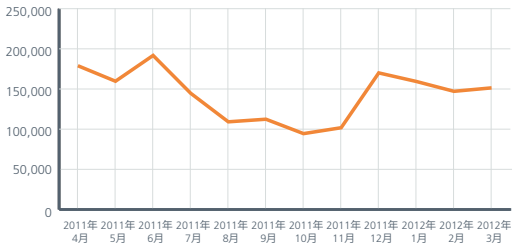
アルゼンチン



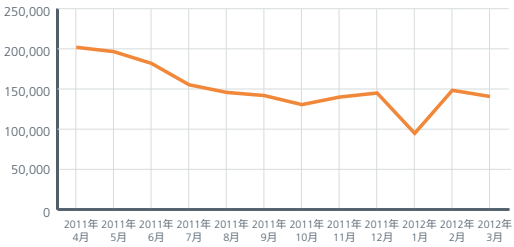
オーストラリア



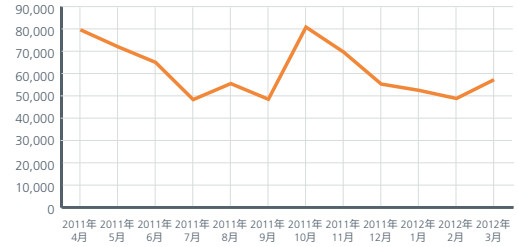
ブラジル



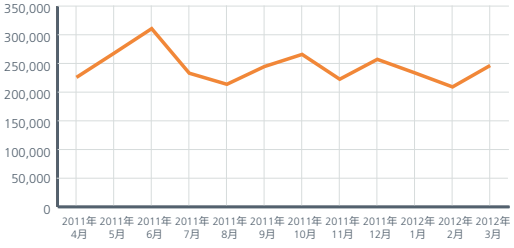
中国



ドイツ

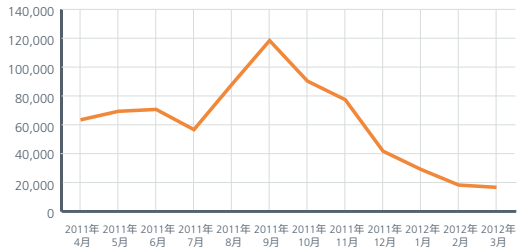


インド

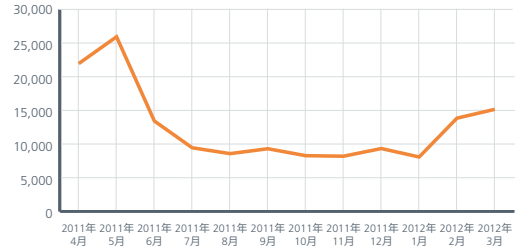


検出されたボットネットの送信者 (国別)

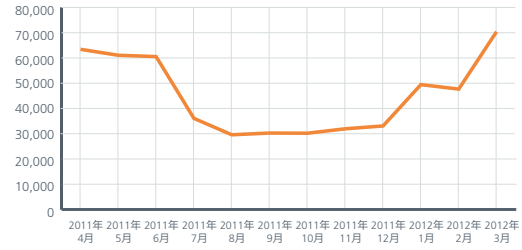
インドネシア



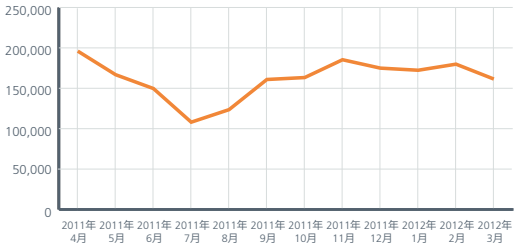
日本



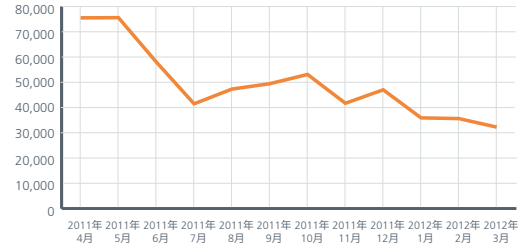
ポーランド



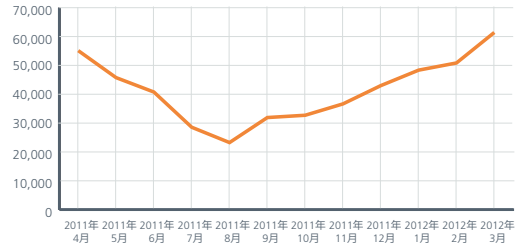
ロシア



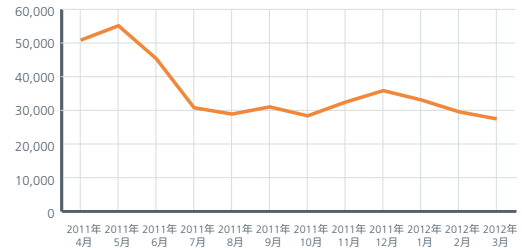
韓国



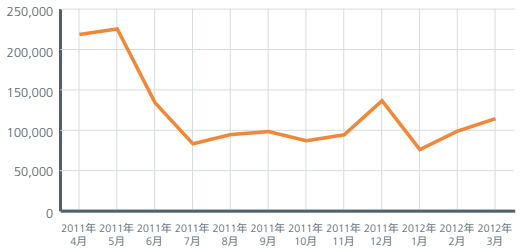
スペイン



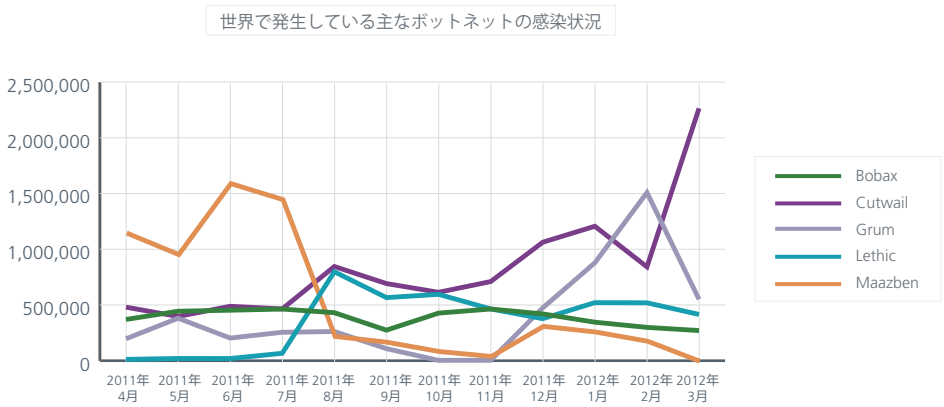
英国



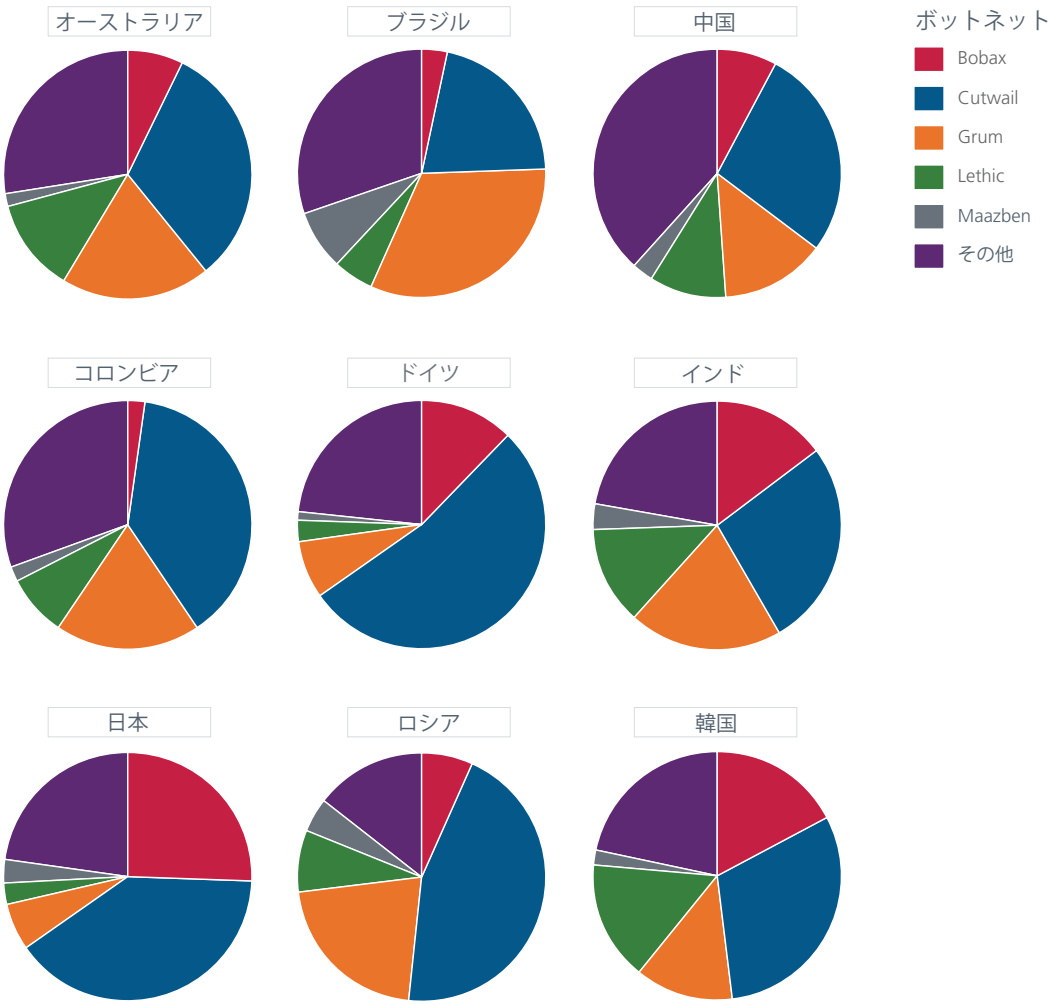
米国

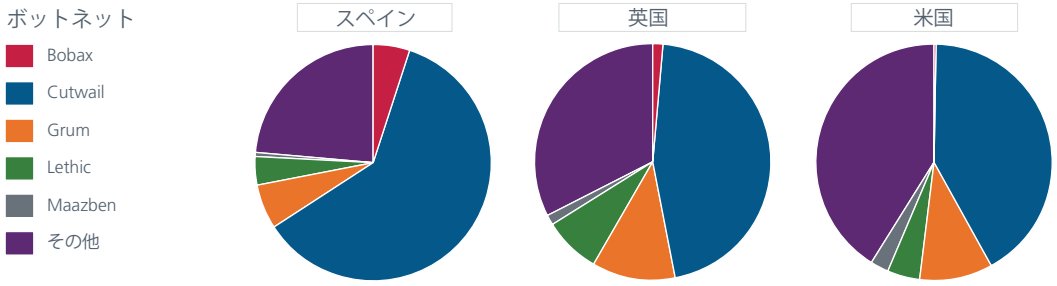


主なボットネットの新しい感染件数を見ると、この四半期は横ばい状況か若干減少しています。例外的に急増しているのは Cutwail です。

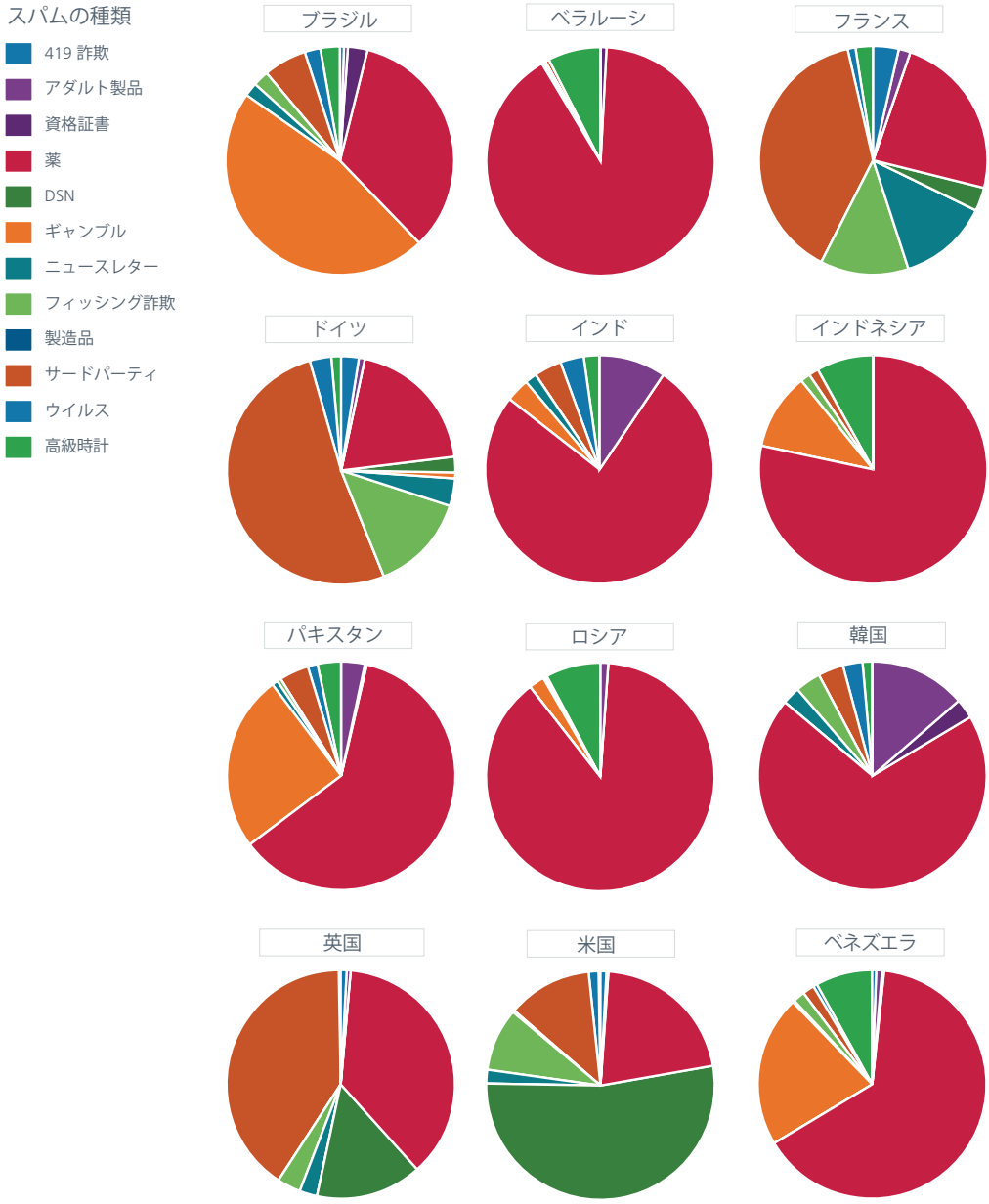


新規感染率が減少していても、既存の脅威がなくなったわけではありません。国別にボットネットの詳細を見ると、多くのボットネットが世界中で活発に活動しています。Cutwail は、新たな感染数だけでなく、ブラジルを除く各国で最も蔓延しているボットネットになっています（ブラジルは Grum がトップです）。





前回と同様に、ソーシャル エンジニアリングの手口とスパム メールの件名は国によって大きく異なります。月や季節によっても異なりますが、休日やスポーツ イベント、大きな事件などがよく利用されています。ブラジルでは、ギャンブル関連のスパムが一般的ですが、多くの国では薬関連の件名がよく利用されています。米国では、不正な DSN（配信状態通知）が多用されています。文化の違いが詐欺の手口にも表れています。



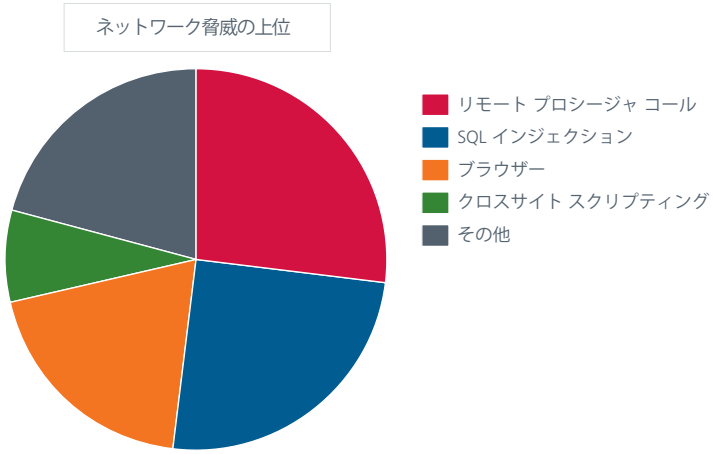
ネットワークの脅威

サイバー攻撃が最も多く発生しているのは米国でしょうか。 攻撃元とその帰属を特定するのは困難な作業です。 2、3 年前まで「この攻撃の発生源はどこか」、「この攻撃の首謀者は誰か」という質問は、個人ユーザーからも企業からもほとんど出てきませんでした。 現在ではこのような質問をよく聞くようになりましたが、正確に答えることは簡単ではありません。 攻撃元の特定には IP アドレスや基本的な地理的情報を使用しますが、 これらの情報だけでは不十分です。 こういった情報が攻撃者のものであるとは限りません。

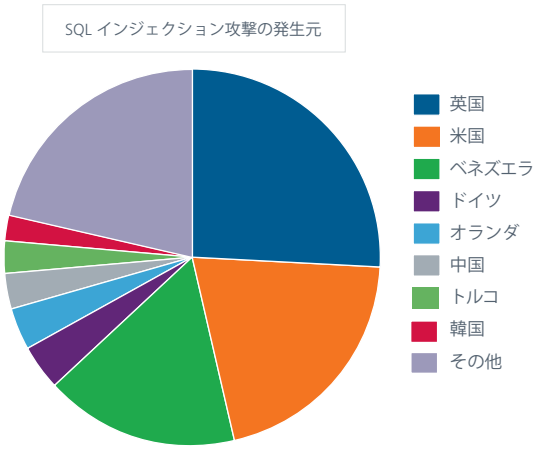
多くの場合、 感染したコンピューターはスパム、 ボットネット、 サービス拒否などの不正な活動の踏み台に使用されます。 このような感染コンピューターは世界中に存在します。 この四半期の統計によると、 感染コンピューターの多くは米国で確認されています。

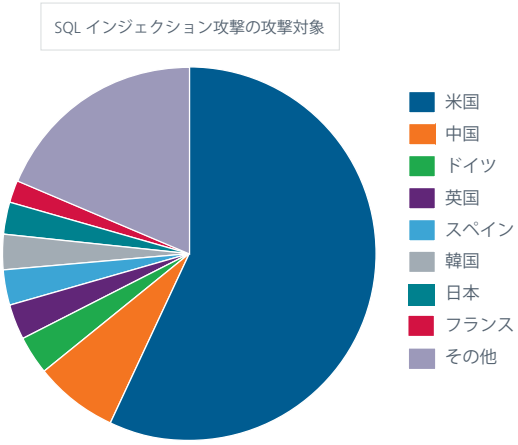
McAfee Global Threat Intelligence™ネットワークで収集した情報の分析結果を見てみましょう。 この四半期の脅威レポートでも、 マカフィーのネットワーク分析レポートを利用しています。

主要なネットワーク脅威はリモート プロシージャ コールと SQL インジェクション攻撃です。 クロスサイト スクリプティングの脅威は前の四半期の 19% から 8% に低下しています。

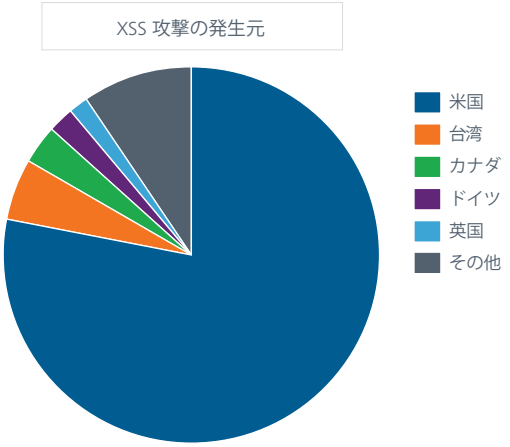


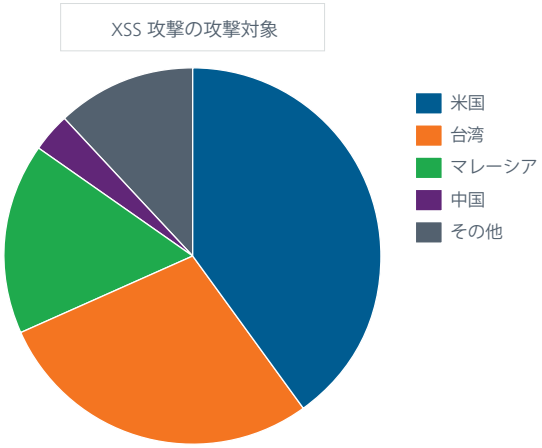
SQL インジェクション攻撃では、 攻撃元でも攻撃対象でも米国がトップになっています。



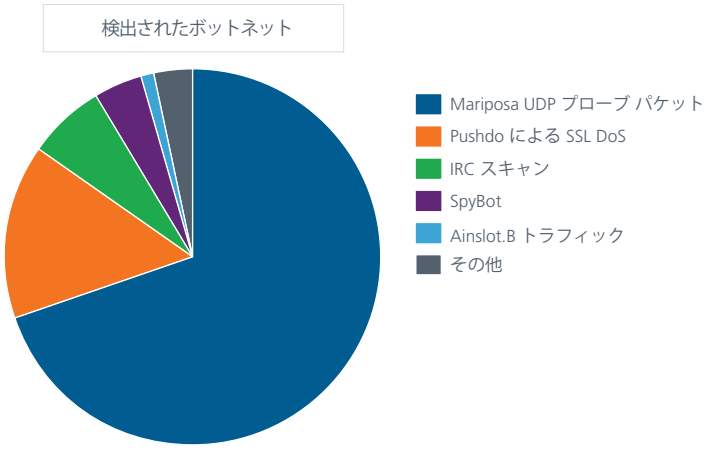


この四半期に検出されたクロスサイト スクリプティング（XSS）でも、 米国は攻撃元と攻撃対象の第 1 位になっています。 第 2 位はどちらも台湾でした。

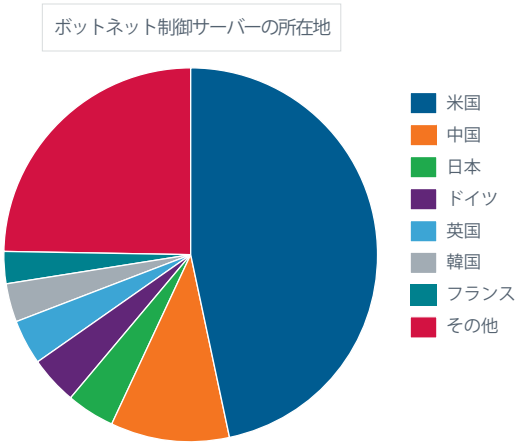




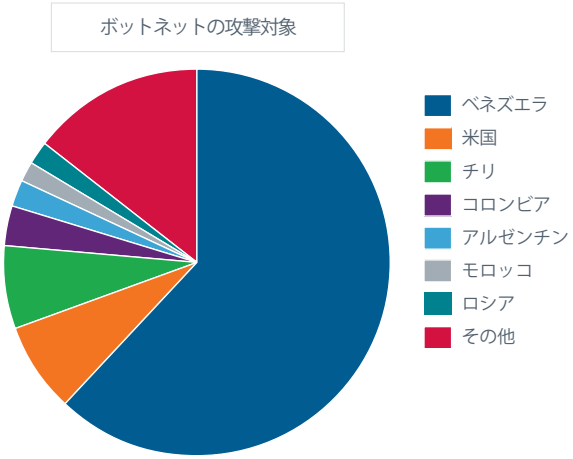
この四半期は、 ネットワークで検出されたボットネットについても統計をまとめました。 トップは、 クレジットカード情報や銀行の口座情報を盗み出す Mariposa で、 2 位以下を大きく引き離しています。 第 2 位は Pushdo（Cutwail の別名）です。



他の統計でも米国は 1 位になっています。 McAfee Global Threat Intelligence が新たに検出したボットネット制御サーバーの半分以上が米国に存在します。



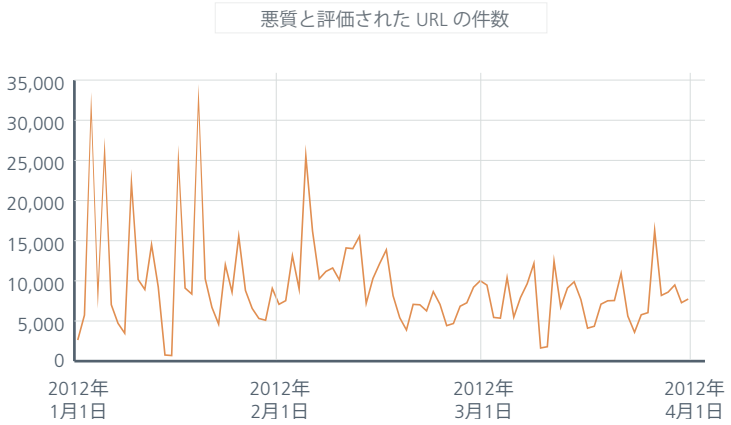
このレポートでは、 ボットネットの攻撃対象についても統計をまとめています。 このカテゴリのトップはベネズエラで、 米国は第 2 位でした。



Web 脅威

Web サイトが不正または悪質と評価されるには様々な理由があります。 この評価は、ドメイン全体とサブドメインの他に、 単一の IP アドレスや特定の URL に対しても行われます。 マルウェアや不審なプログラムが存在しているサイトやフィッシング詐欺サイトは悪質なサイトと見なされます。 不審なコードが存在するだけでなく、 振る舞い自体の怪しいサイトもあります。 サイトの評価には、 いくつかの要因が考慮されます。

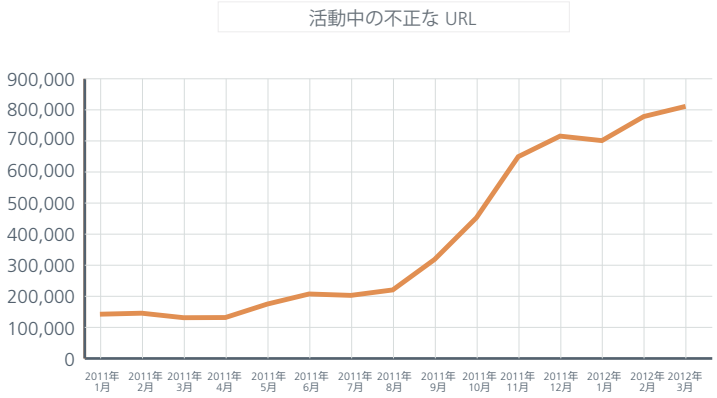
前の四半期、 McAfee Labs では 1 日平均 9,300 件の新しい不正なサイトを記録しました（スパム メールの URL を含めると 11,000 件）が、 この四半期の検出件数は 1 日平均 9,000 件に減少しています。



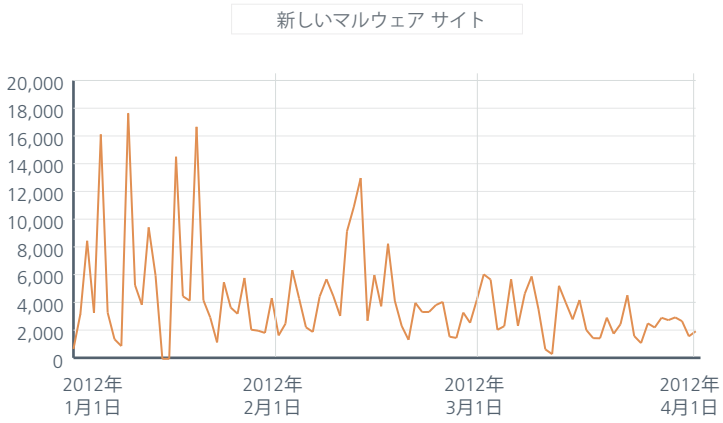
悪質と評価される URL の件数は減少していますが、 不正なサイトにリダイレクトされる顧客の数は増加しています。 前の四半期、 マカフィーがリダイレクトを阻止した顧客数は一日平均 8 人に 1 人の割合でした（残りの 7 日は危険なサイトを閲覧していません）が、 この四半期はこの割合が 6 人に 1 人と増加しています。 この数字は期を通じて一定で、 この結果はサイバー犯罪者が不正なサイトへの誘導に成功していることを表しています。 新しい悪質サイトの殆どは米国で見つかっています。 各地域の状況を見ると、 世界中のインターネットが例外なく危険にさらされていることが分かります。


不正なコンテンツが存在するサーバーの場所
アフリカ
南アフリカ
レユニオン
モロッコ
その他
アジア太平洋
韓国
中国
シンガポール
アジア太平洋地域
香港
インドネシア
その他
オーストラリア/ニュージーランド
オーストラリア
ニュージーランド
ヨーロッパ/中東
オランダ
英国
ドイツ
スイス
フランス
その他
ラテンアメリカ
バハマ
ブラジル
英領バージン諸島
ケイマン諸島
その他
北米
米国
カナダ

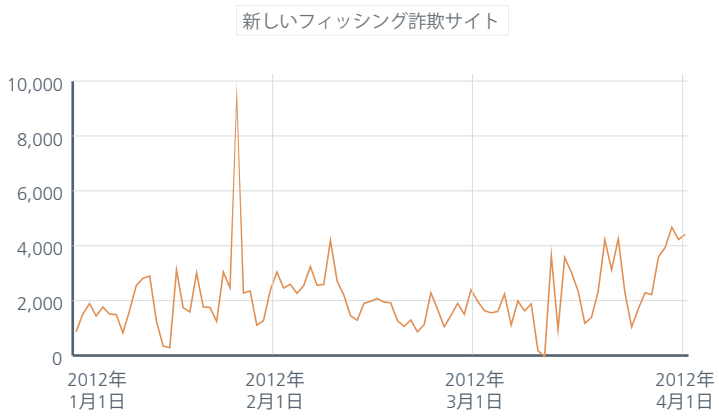
不正なダウンロードやブラウザー エクスプロイトが存在する Web サイトの数も引き続き増加しています。



この四半期はマルウェアと不審なプログラムを配布する Web サイトの数が約 1/3 減少し、一日平均 4,200 件のサイトが新たに見つかりました（2011 年第 4 四半期は一日平均 6,500 件）。



フィッシング詐欺サイトの状況は前回の四半期から変化はありません。この四半期に新たに見つかったフィッシング詐欺 URL は一日平均で約 2,200 件です。フィッシング詐欺サイトは依然として重大な脅威です。現在でも、不正なダウンロードやスパム配信を行うサイト数よりもフィッシング詐欺関連のサイト数の方が上回っています。



サイバー犯罪

クライムウェア ツール

この四半期は、既存のエクスプロイト パックの更新だけでなく、新しいクライムウェア ツールが見つかっています。これらのツールは当初、2011 年 10 月に開示された Java Rhino の脆弱性（CVE-2011-3544）を悪用していましたが、今年に入り次の 2 つの脆弱性を攻撃するようになりました。

- 不正な MIDI ファイルでリモートからコードの実行が可能な Windows Multimedia Library の脆弱性（CVE-2012-0003）。1 月に公開されたセキュリティ情報（MS12-004）で解決されています。
- Java Runtime Environment サンドボックスの脆弱性（CVE-2012-0507）。2 月中旬に公開された Oracle Java SE の Critical Patch Update で解決されています [3]。この脆弱性は Java AtomicReferenceArray の脆弱性ともいいます。

以下の表で、CVE-2012-0507 の Java Atomic エクスプロイトを含むツールは Phoenix Exploit Kit だけですが、様々なブログやフォーラムの情報によると、BlackHole、Eleonore、Incognito にも同様の変更が行われているようです。この数か月の間に、この脆弱性を利用するエクスプロイト キットが増えてくるでしょう。

名前	場所	エクスプロイトの詳細
Sakura 1.0	ロシアまたは東ヨーロッパ	Java Rhino（CVE-2011-3544）を含む 3 個のエクスプロイト
Hierarchy	ロシアまたは東ヨーロッパ	16 個のエクスプロイト。2011 年以降に追加されたのは次の 2 つ。 • Flash 10（CVE-2011-0611） • Java Rhino
Yang Pack （1 月）	中国	4 個のエクスプロイト : • Flash 10.3.181.x（CVE-2011-2110） • Flash 10.3.183.x（CVE-2011-2140） • Java Rhino
Zhi Zhu （2 月）	中国	5 個のエクスプロイト : • HTML+TIME（CVE-2011-1255） • Flash 10.3.181.x • Flash 10.3.183.x • WMP MIDI（CVE-2012-0003）
Gong Da Pack （2 月）	中国	3 個のエクスプロイト : • Flash 10.3.183.x • Java Rhino • WMP MIDI
Phoenix Exploit Kit 3.1 （3 月）	ロシア	2011 年第 4 四半期の脅威レポートでは、Java Rhino エクスプロイト（CVE-2011-3544）を含むバージョン 3.0 を報告しました。バージョン 3.1 では、Java Atomic（CVE-2012-0507）が追加されました。

以前の中国語パックについては、Kahu Security のブログに詳しい情報があります [4]。

ボットとボットネット

地下フォーラムでは数多くのボットネット パッケージが宣伝されています。 以下の表は、 高額で売買されているボットネットの一部です。

名前	価格（単位：米ドル）
Darkness（SVAS/Noncenz） 分散型サービス拒否（DDoS）攻撃用のボット	1 月にバージョン 10 に更新。 $ 120 パッケージ • Minimum: DDoS ボット、 更新無料、 モジュールなし = $ 450 • Standard: DDoS ボット、 1 か月の無料更新、 パスワード収集モジュール = $ 499 • Bronze: DDoS ボット、 3 か月の無料更新、 パスワード収集モジュール、 1 モジュール再ビルド無料 = $ 570 • Silver: DDoS ボット、 6 か月の無料更新、 パスワード収集モジュール、 3 モジュール再ビルド無料 = $ 650 • Gold: DDoS ボット、無制限無料更新、パスワード収集モジュールと hosts エディター モジュール、5 モジュール再ビルド無料、 他の製品 8% を割引 = $ 699 • Platinum: DDoS ボット、 無制限無料更新、 パスワード収集モジュール、 無制限再ビルド無料、他の製品 20% を割引 = $ 825 • Brilliant: DDoS ボット、 無制限無料更新、 無制限無料再ビルド、 すべてのモジュールを無料提供、 他の製品を 25% 割引 = $ 999 その他 : • 再ビルド（URL の変更）= $ 35 • ソース提供 = $ 3,500 から $ 5,000 • Web パネルの再インストール（初回は無料）= $ 50
Citadel5 Zeus の亜種、 口座情報を狙うボットネット	• ボット作成ツールと管理パネル = $ 2,399 と毎月のレンタル料金 $ 125（2011 年 12 月現在） • アンチウイルス回避の自動更新 = $ 395。 1 回の更新料 $ 15。
THOR（TheGrimReap3r） 多目的の P2P ボットネット	• モジュールなしのパッケージが $ 8,000。 最初の 5 ユーザー分は $ 1,500 の割引。 • ボット キラー、DDoS、フォーム収集、キーロガー / パスワード収集、大量メール配信用のモジュールが開発中の模様。
Carberp 口座情報を狙うボットネット	• ローダー、 収集ツール、 すべての基本機能（以下のものを除く）= $ 2,500 • 500 回の接続、 Internet Explorer と Mozilla FireFox に対するインジェクション = $ 5,000 • 隠しブラウザー（VNC と同様）= $ 8,000

Carberp には法外な値段が付いています。 この情報は 3 月 21 日付のものですが、 ロシアの捜査当局は 3 月 20 日に Carberp グループの逮捕を発表しました（次のセクションを参照）。

サイバー犯罪に対する取締り

この四半期はサイバー犯罪組織の取り締まりに成果が見られ、 いくつかの組織の解体に成功しています。 Microsoft は 1 月、 Kelihos（別名 Waledac）ボットネットを管理していた疑いでロシア・サンクト・ペテルブルク在住の人物を告訴しました [6]。 セキュリティ専門家の Brian Krebs 氏によると、 この人物は 2005 年から 2007 年にかけてロシアのアンチウイルス会社 Agnitum でシステム開発者、プロジェクト マネージャーとして勤務していました [7]。 この人物は Gazeta.ru 紙のインタビューの中で容疑を否定しています [8]。

2011 年 3 月にスイス・チューリッヒで身柄を拘束されたロシア人が 1 月ニューヨークに送還されました。この人物は手配中の息子とともに、2005 年以降、不正な Web サイトで行った共同謀議、メール詐欺、不正通信、コンピューター不正行為、個人情報の窃盗、セキュリティ侵害など、9 件の容疑で逮捕されました [9]。

3 月 16 日、米財務省検察局と移民税関捜査局は、「Open Market」作戦の成果として個人情報の窃盗やクレジットカード偽造の容疑で 50 人を逮捕したことを発表しました [10]。報道によると、逮捕した容疑者はすべて、複数のサイバープラットフォームを運営し、盗み出した個人情報や口座情報をオンライン フォーラムで売買する国際的な犯罪組織 Carder.su のメンバーだった模様です（この組織は Carder.info、Crdsu.su、Carder.biz、Carder.pro を運営しています）。

ロシア内務省とロシア連邦保安庁（FSB）は 3 月 20 日、Carberp トロイの木馬を使用して 90 人以上の被害者から口座情報を収集し、6,000 万ルーブル（米ドルで 200 万ドル）以上を盗み出した容疑で 8 人のサイバー犯罪者を逮捕したと発表しました [11]。

英国では 3 月、2011 年 5 月に逮捕された 2 人の人物が Sony Music のコンピューターに侵入し、16,000 万ポンド相当の音楽ファイルを盗み出した容疑で起訴されました [12]。英国重大組織犯罪庁によると、この事件は、昨年他のハッカーが PlayStation ネットワークに不正侵入し、7700 万人以上の登録ユーザーの個人情報をダウンロードした事件と同じ時期に発生しています。このハッキングと Anonymous または LulzSec との関係はない模様です。

この四半期は数人の Anonymous メンバーが逮捕されました。このハッキング グループの幹部の逮捕に成功した背景には LulzSec のメンバーだった Sabu の関与があった模様です。Sabu は 2011 年 8 月に罪状を認めた後、FBI の協力者となっています。この取り締まりでは英国で 2 人、アイランドで 2 人、米国で 2 人が検挙され、ニューヨーク南部連邦地裁に提訴されました [13]。この四半期の初めには国際刑事警察機構がアルゼンチン、チリ、コロンビア、スペインで 25 人の Anonymous メンバーを逮捕しています [14]。また、3 月 20 日には Anonymous に近いハッカー グループ CabinCr3w のメンバー W0rmer と Kahuna が米国で逮捕されました [15]。

サイバー犯罪組織の取り締まりに成果を挙げたのは捜査当局だけではありません。1 月、著名なセキュリティ研究者である Dancho Danchev 氏が Koobface の背後にある犯罪組織に関係するロシア人に関する情報を公開しました [16]。その数日後、セキュリティ研究者グループが公開を予定していた 4 人の犯罪者の名前がニューヨーク・タイムズ紙に掲載されました [17]。

最後に、Zeus、SpyEye、Ice-IX の亜種を使用するボットネットの閉鎖を狙って Microsoft が実施した「Operation B71」作戦に触れておきましょう。Microsoft は 3 月 23 日、FS-ISAC（Financial Services - Information Sharing and Analysis Center）と NACHA（National Automated Clearing House Association）とともに作戦の結果について公開しました。この作戦では、Microsoft と捜査員が 4 時間にわたりネットワーク トラフィックを傍受し、ペンシルベニア州とイリノイ州にホスティングされている 2 台のサーバーを突き止めました。さらに、1,700 以上のドメイン名を解析し、犯罪行為での役割の特定に成功しました [18]。

ハクティビズム

Sabu の逮捕に関係する事件以外にも、この四半期は Megaupload の強制閉鎖に対する報復攻撃が話題になりました。 Anonymous は Twitter とプレスリリースを通じて、 #OpMegaupload に数千人が参加し、米司法省、 全米レコード協会、 米国映画協会、 BMI、 FBI などの Web サイトの閉鎖に成功したと声明を発表しました。 Megaupload の閉鎖を口実に、 Anonymous は 2 月 11 日と 2 月 25 日に SOPA、 PIPA、 ACTA 法に対する抗議活動を 15 か国で 100 以上の都市で展開しました。これは、デジタル世界のハクティビストと現実の行動主義が融合した興味深い事例です。 これは何かの前兆でしょうか。

2 月 11 日にヨーロッパ各地で発生した ACTA 法に対する抗議活動

この四半期は、 この他にも世界各地で活動が行われました。 いずれも大きな影響はなかったため、 選択は難しいのですが、 いくつかの活動を挙げておきましょう。

- 3 月 31 日に世界のインターネットを停止させる #OpGlobalBlackout が予告されましたが、 実際には何も発生しませんでした。 多くのセキュリティ研究者はこの攻撃は技術的に不可能と見ていますが、 この作戦に対して真面目な議論が展開されていることには注意が必要です。 Anonymous は今後もこのような情報を流していくでしょう。
- ArcelorMittal のハッキング : ベルギー・リエージュにある 2 基の溶鉱炉の閉鎖決定に対する抗議活動 [19]
- バチカンに対する DDoS 攻撃 : カトリック教徒に対する攻撃ではなく「腐敗した」教会に対する攻撃 [20]
- Anonymous の Linux OS リリース直後に偽物と発表 [21]

筆者について

本レポートは、 McAfee Labs の Zheng Bu、 Toralv Dirro、 Paula Greve、 Yichong Lin、 David Marcus、 François Paget、Craig Schmugar、Jimmy Shah、Dan Sommer、Peter Szor、Adam Wosotowsky 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、 電子メール、 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 350 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。

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、 セキュリティ・テクノロジー専業のリーディング カンパニーです。 世界中で使用されているシステム、 ネットワーク、 モバイルデバイスの安全を実現する革新的なソリューションとサービスを提供し、 ユーザーのインターネットへの安全な接続、Web の閲覧およびオンライン取引の安全を確実に支えています。 マカフィーは、 他の追随を許さないクラウドベースのセキュリティ技術基盤 Global Threat Intelligence™ （グローバル スレット インテリジェンス）を活用して、 革新的な製品を送り出しています。 個人ユーザーをはじめ、 企業、 官公庁・自治体、サービス プロバイダーなど、様々なユーザーはコンプライアンスの確保、データの保全、破壊活動の阻止、脆弱性の把握を実現し、 またセキュリティ レベルを絶えず管理し、 改善することができます。 お客様の安全を確保するため、 マカフィーは、 新しい手法の開発に日々真摯に取り組んでいます。 詳しくは http://www.mcafee.com/jp/ をご覧ください。

[1] http://blogs.mcafee.com/mcafee-labs/signed-malware-you-can-runbut-you-cant-hide
[2] http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf
[3] http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html
[4] http://www.kahusecurity.com/
[5] http://krebsonsecurity.com/2012/01/citadel-trojan-touts-trouble-ticket-system/
[6] http://blogs.technet.com/b/microsoft_blog/archive/2012/01/23/microsoft-names-new-defendant-in-kelihos-case.aspx
[7] http://krebsonsecurity.com/2012/01/microsoft-worm-author-worked-at-antivirus-firm/
[8] http://en.gazeta.ru/news/2012/03/07/a_4030561.shtml
[9] http://www.justice.gov/usao/nys/pressreleases/January12/zdoroveninvladimirandzdoroveninkirillindictmentpr.pdf
[10] http://www.secretservice.gov/press/GPA03-12_OpenMarket2.pdf
[11] http://garwarner.blogspot.fr/2012/03/russian-mvd-announces-arrest-of-carberp.html
[12] http://www.huffingtonpost.com/2012/03/05/michael-jackson-hacking-james-marks-james-mccormick_n_1321912.html
[13] http://www.smashtheman.com/2012/03/news/the-legal-attack-against-anonymous-and-lulzsec
[14] http://www.interpol.int/News-and-media/News-media-releases/2012/PR014
[15] http://blogs.mcafee.com/mcafee-labs/hacker-leaves-online-trail-loses-anonymity
[16] http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html
[17] http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html
[18] http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx
[19] http://www.cyberguerrilla.info/?p=3747
[20] http://geeks.thedailywh.at/2012/03/07/geek-news-anonymous-vatican-hack-of-the-day/
[21] http://www.tomshardware.com/news/Anonymous-Anonymous-OS-Viruses-Trojans-Fake,15027.html

44605rpt_quarterly-threat-q1_0512_fnl_ETMG

マカフィー株式会社
www.mcafee.com/jp

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