レポート

McAfee
An Intel Company

McAfee 脅威レポート：2011 年第 4 四半期

McAfee Labs™

目次

世界の脅威状況を見ると、 2011 年の最後の四半期は変化の激しいものとなりました。 この四半期は 2011 年の縮図ともいえます。2011 年は、これまでに見られなかった注目すべき出来事が発生しています。 Duqu[1] などによる攻撃、 Anonymous を中心としたハクティビズムなど、 2011 年はセキュリティ業界にとって大きな一年となりました。 ハクティビストの活動が活発化し、 産業用制御システムに対する攻撃の懸念も高まっています。 2012 年は波乱の年になるでしょう。

この四半期を振り返ってみましょう。 マルウェアとスパムはすべての地域で減少傾向にありますが、 モバイル端末を狙うマルウェアは増加し、この四半期は過去最高の件数を記録しました。 マルウェアの標的となったのは Android です。新種のマルウェアの数は減っているものの、収集したサンプルの累計でみると 7,500 万を超えています。 この数字は 2010 年末の予測どおりです。

世界全体でスパムの量は減少し、 多くの地域がここ数年で最も低い値を記録しています。 スパムの件名は以前と変わらず、 地域ごとに大きな相違が見られます。 スパム送信者は世界的に通用するものと特定の地域に効果があるものをよく理解しています。 この戦術は変わっていません。 この四半期も矛盾する傾向が見られました。 通常、 ボットネットはスパムを送信します。 ボットネットが増えれば、 それに伴いスパムの量も増加するはずですが、 これとは逆の現象が起きています。 世界全体でボットネットの数は増加しています。 特に、 Grum が最も顕著な動きを見せました。

この四半期も米国に不正な Web コンテンツが最も多く存在し、 悪質と評価されるサイトの数も増えています。 活動中の不正な URL の数も増加し、 マルウェアが潜むサイトの数は倍増しました。 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。

今回のレポートでは、 データベースと情報漏えい、 ネットワーク攻撃の 2 つのトピックを新たに追加しました。この四半期、非常に多くの情報漏えい事件が公表されました。ネットワークに対する攻撃手法としては、リモート プロシージャ コール、 SQL インジェクション、 クロスサイト スクリプティングが引き続き上位を占めています。

この四半期は、 2011 年で最も危険なハクティビスト活動とサイバー犯罪が発生しました。 これは 2012 年の前兆です。 サイバー犯罪に使われるツールキットも進化し、 政府機関の関与が疑われる事件も発生しています。 しかし、 悪いことばかりではありません。 サイバー犯罪者の検挙においては大きな成果を挙げています。

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。

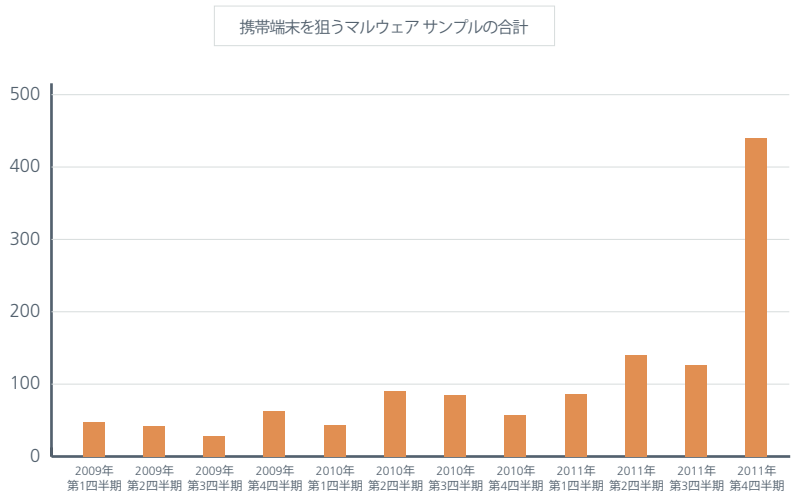
モバイルの脅威

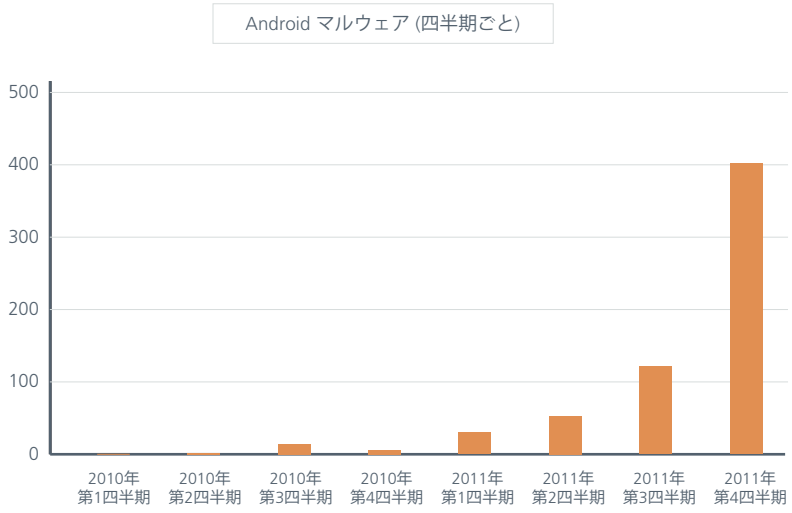
この四半期もマルウェアに最も狙われた携帯端末は Android でした。 PC と同様に、 モバイル環境でも営利目的のスパイウェアやアドウェアが蔓延しています。 モバイル環境で発生したマルウェアの件数は第 4 四半期に過去最高を記録しました。 年間で比較しても 2011 年は過去最高となりました。 この傾向は今後しばらく続くものと思われます。

Android を狙うマルウェアの大半は金銭目的で SMS を送信するトロイの木馬です。 このトロイの木馬は、 携帯電話を乗っ取り、 メッセージを送信します。 サイバー犯罪者は、 携帯電話の所有者に高額な料金を請求することで金銭を稼いでいます。 興味深いことに、 同じ手口がハクティビズムの領域でも使われています。 Android/Arspam の作成者は、 Android Market などにアプリを登録する代わりに、 アラビア語の複数のディスカッション フォーラムにマルウェアをアップロードしました。 このトロイの木馬はイスラム教の礼拝カレンダーアプリの改造版で、チュニジアの暴動の引き金となった人物に関する SMS を送信します。 ディスカッション フォーラムのメンバーは、 携帯電話を初期化してマルウェアを駆除することはせず、 同じ志の人物にトロイの木馬を転送し、 メッセージを拡散させました。

脆弱性を悪用するエクスプロイトを組み合わせたアプリの登場で Android 端末のルート化が以前よりも簡単になりました。 ユーザーにアプリをインストールさせ、 ボタンをクリックさせるだけで端末のルート化を実行できます。 同様に、 マルウェアとルート エクスプロイトを組み合わせれば、 様々な攻撃が可能になります。 この手法は PC のマルウェアで長い間利用されているもので、 新しいプラットフォームを狙う場合によく使われる手口の一つです。 マカフィーでは、 エクスプロイトを含むルート化アプリを数多く検出しています。

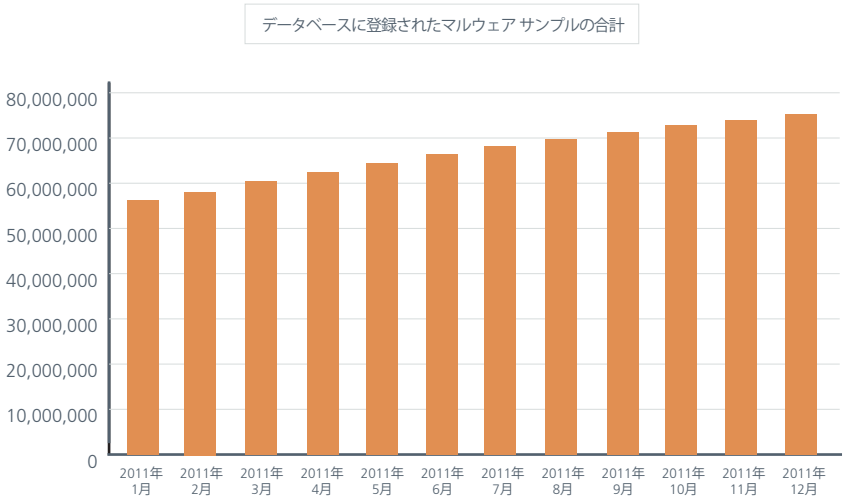
エクスプロイトを使用するのは攻撃者だけではありません。 ペネトレーション テストの実施者やコンピューター セキュリティの専門家も、 自分の仕事に携帯端末が役立つことを認識しています。 ペネトレーション テストで使用すると、 携帯電話やタブレットから Windows PC を攻撃できる Android も存在します。 通常、 ペネトレーション テストを行うにはフルサイズのノート PC やネットブックを持ち込む必要がありますが、 このようなツールを使用すれば、 相手に気付かれずにクライアントのネットワーク構成を把握し、 攻撃を仕掛けることも可能です。 攻撃者が使用する可能性もあるため、 マカフィーでは、 このツールを Android/AnitTool という名前の不審なプログラムとして検出します。

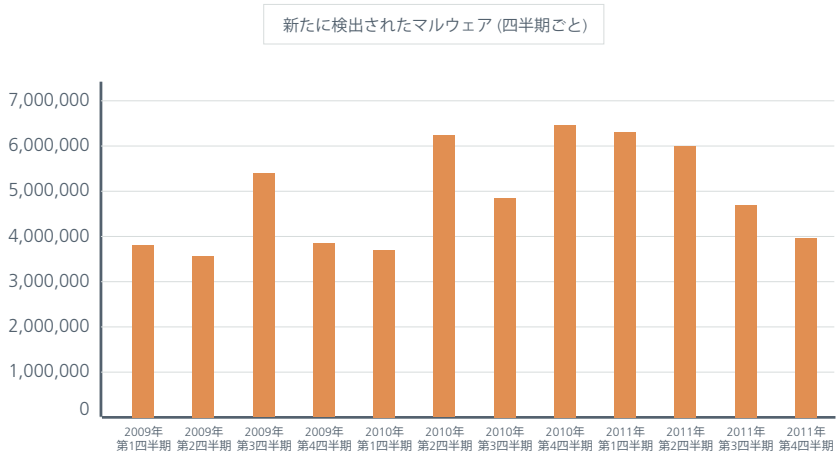




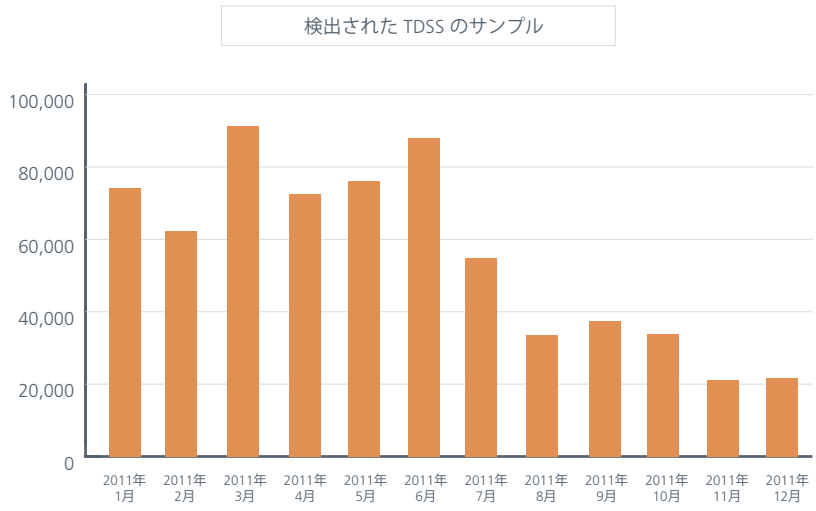
マルウェア

全体でみると、 PC を狙うマルウェアの発生数は引き続き減少し、 昨年同時期と比べると大幅に低下しています。 しかし、 油断は禁物です。 弊社が収集しているサンプルの累積数を見ると、 いまだに 7,500 万件を超えています。これはマルウェアが爆発的に増加する前兆でしょうか。簡単には結論を出せませんが、携帯端末の普及に伴い、 脅威の対象が変化していることは間違いありません。

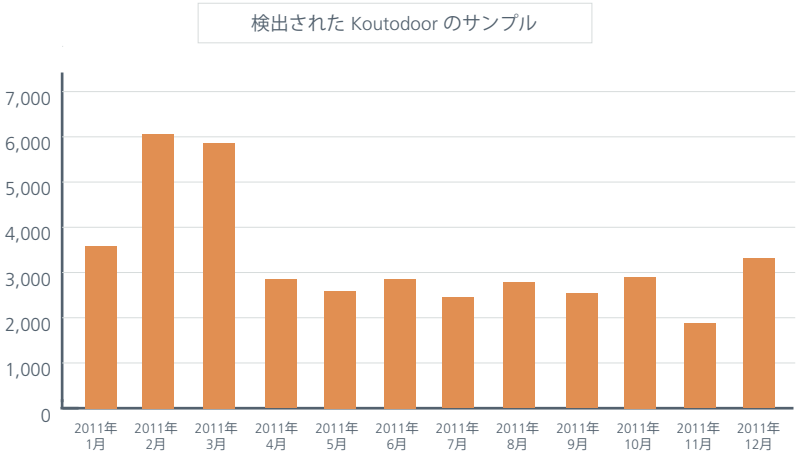


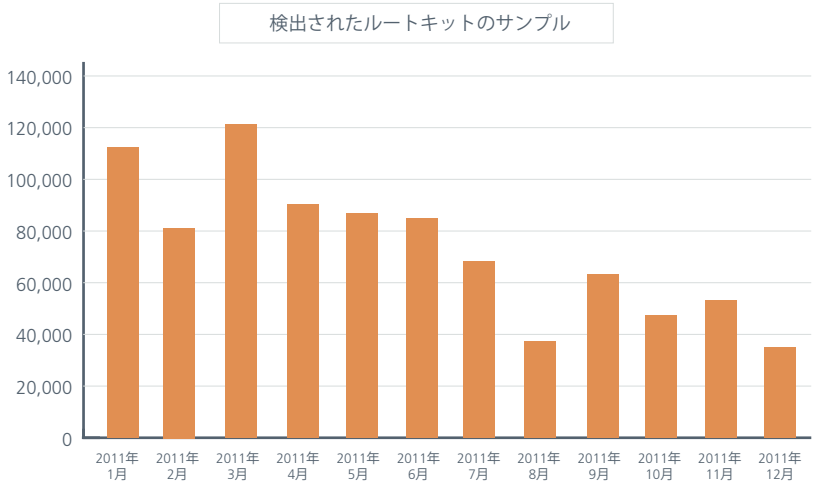


この四半期に検出されたルートキットの件数は減少しましたが、 半数以上のマルウェアが TDSS ファミリーでした。 ルートキット（ステルス性のあるマルウェア）はマルウェアの中で最も厄介な存在で、他のマルウェアにも大きな影響を及ぼします。 ルートキットは検出を回避し、 システムに長期間潜伏します。 以下のグラフでも分かるように、 TDSS の数はいまだに増加しています。

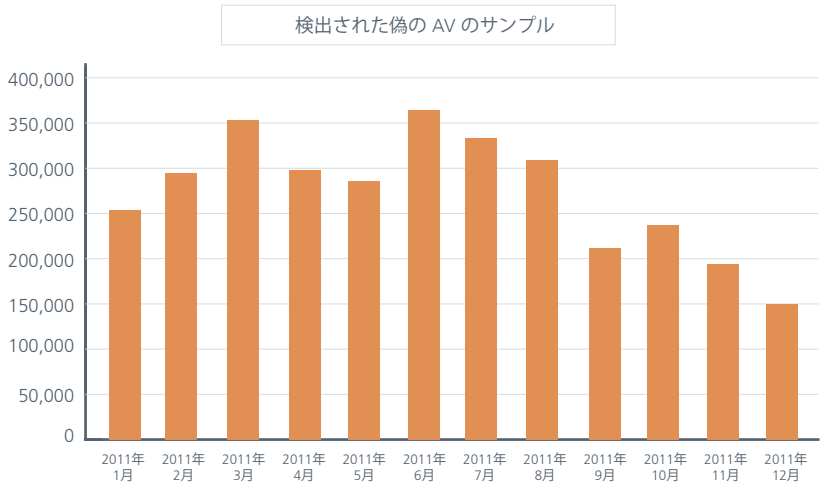


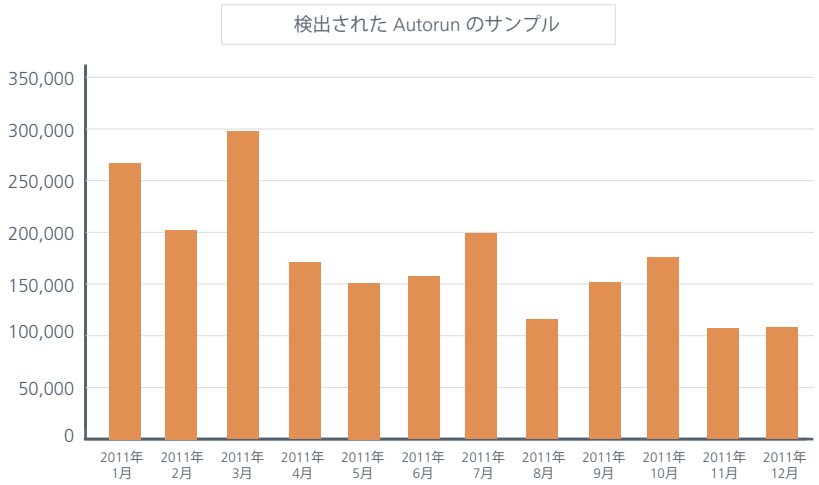
Koutodoor など、 他のルートキットには大きな変化は見られません。 また、 全体としてルートキットの数は減少傾向を示しています。 しかし、 警戒を怠るべきではありません。

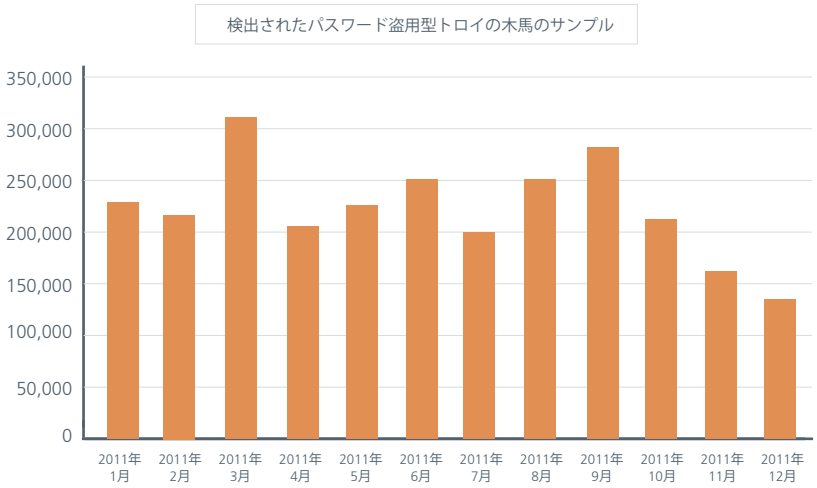




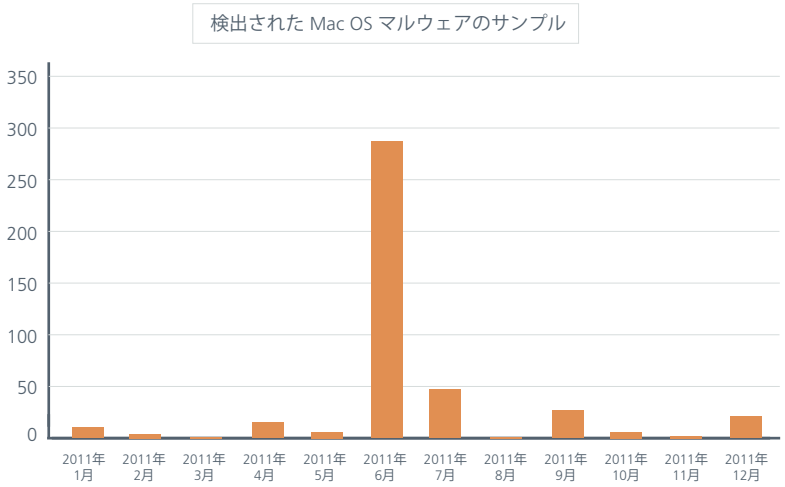
次に、 偽のウイルス対策 （偽のアラート、 不正なセキュリティ ソフトウェア）、 AutoRun ソフトウェア、 金融機関を狙うパスワード盗用型トロイの木馬の状況を見てみましょう。 偽のウイルス対策は、 前の四半期よりも大幅に減少しましたが、 最も多く検出されたマルウェアの一つに入っています。 AutoRun とパスワード盗用型トロイの木馬はやや減少しています。



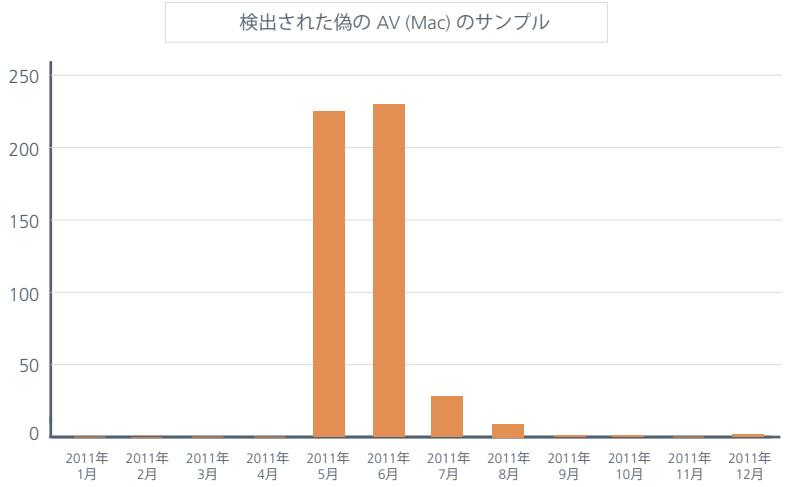




Mac のマルウェアは第 2 四半期に急増しましたが、その後はなりを潜めています。PC を狙うマルウェアの件数と比べると、Mac のマルウェアは大した数ではありませんが、システムの保護は行うべきです。MacBook Air も例外ではありません。



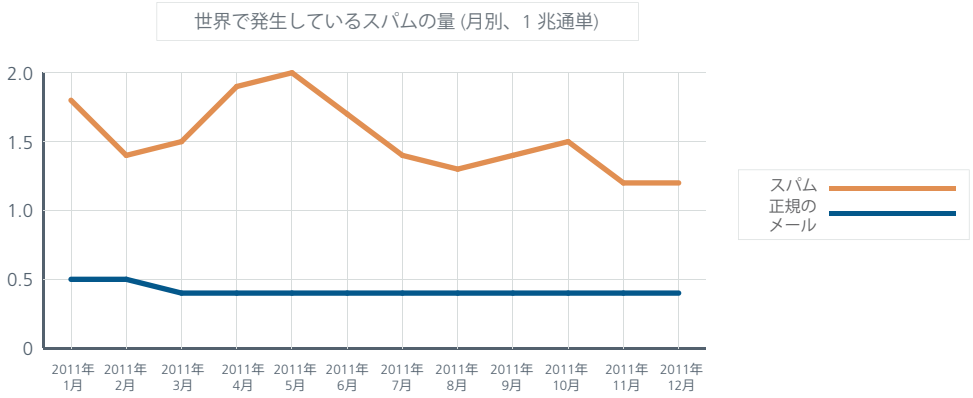
Mac を狙う偽のウイルス対策は第 2 四半期に急増しましたが、この四半期はほとんど検出されていません。



年末にかけて Mac に対する攻撃はほとんど発生していませんが、 現在ではどの OS も攻撃の対象になっています。

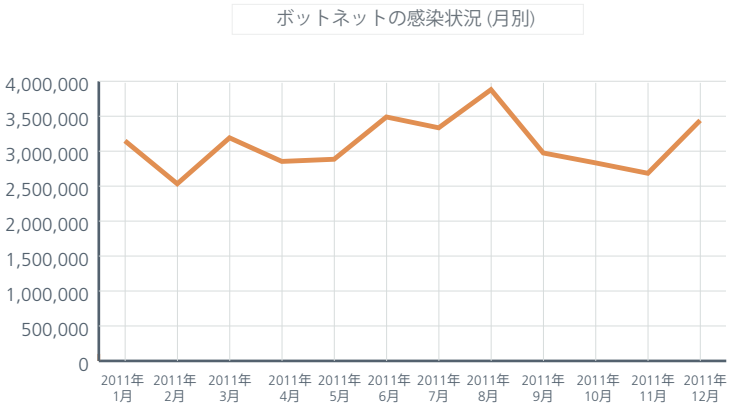
メッセージングの脅威

2011 年の終わり、 世界で発生したスパムの量がここ数年で最低となりました。 ブラジル、 アルゼンチン、 英国、 トルコ、 韓国は 2007 年以降の最低値を記録しています。 一方、 米国とドイツでは若干増加しています。 世界的には減少傾向を示していますが、 標的型スパムとスパムの脅威は以前と変わりません。 量は少なくなっていますが、 危険度と巧妙さは増しています。 数年前は無作為にメールを送信していたスパム送信者も、 現在では精度の高いアドレス帳を使用しています。



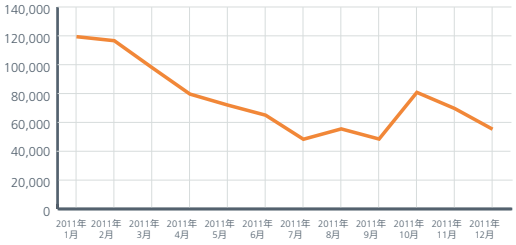
ボットネットの詳細

ボットネットの数は 8 月以降減少していましたが、 11 月から 12 月にかけて再び増加しました。 増加した国はブラジル、 コロンビア、 インド、 スペイン、 米国で、 逆に減少した国はドイツ、 インドネシア、 ロシアでした。

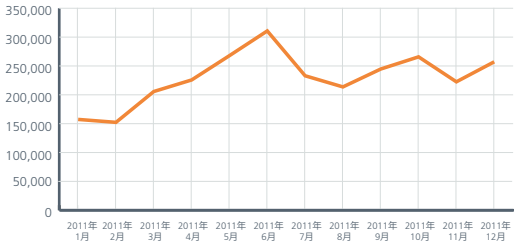


新たに検出されたボットネットの送信者 (国別)

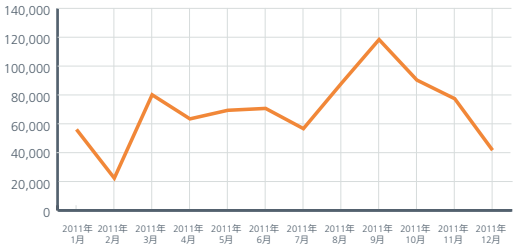
ドイツ



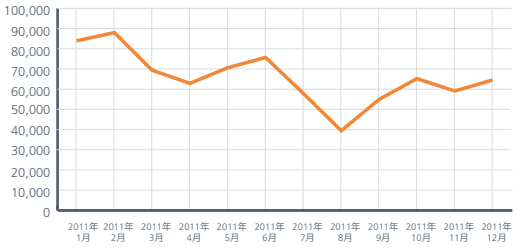
インド



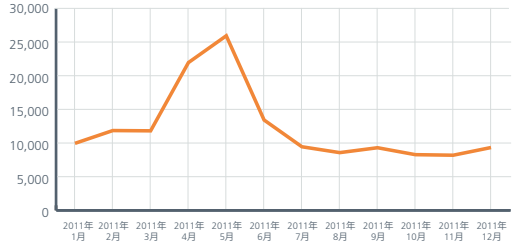
インドネシア



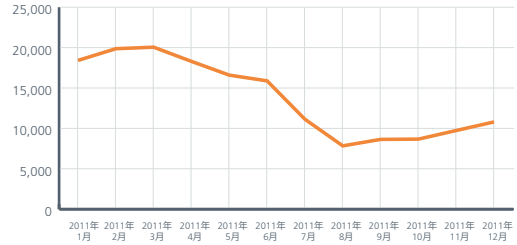
イタリア



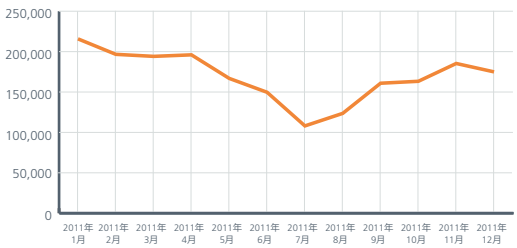
日本



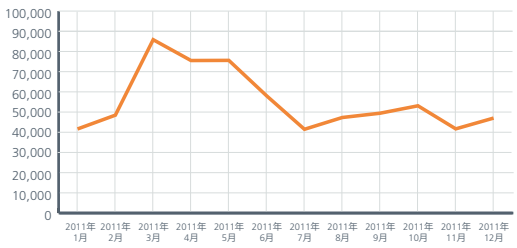
ポルトガル



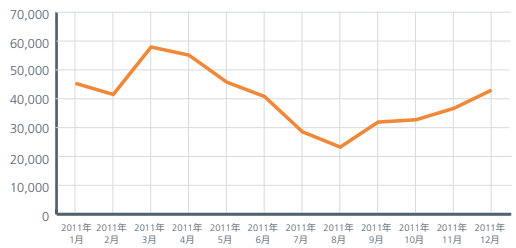
ロシア



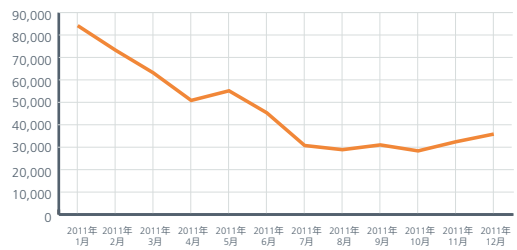
韓国

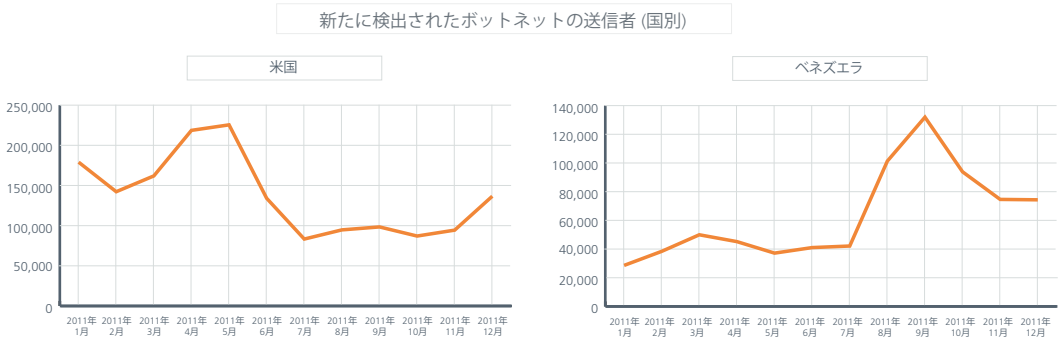


スペイン

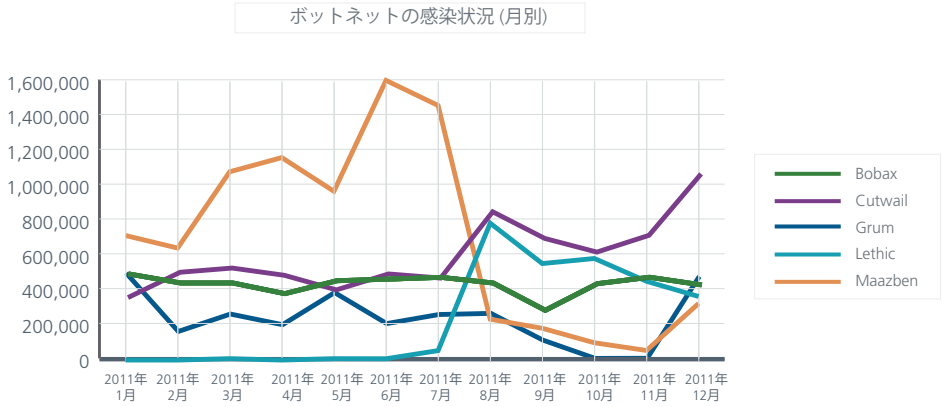


英国

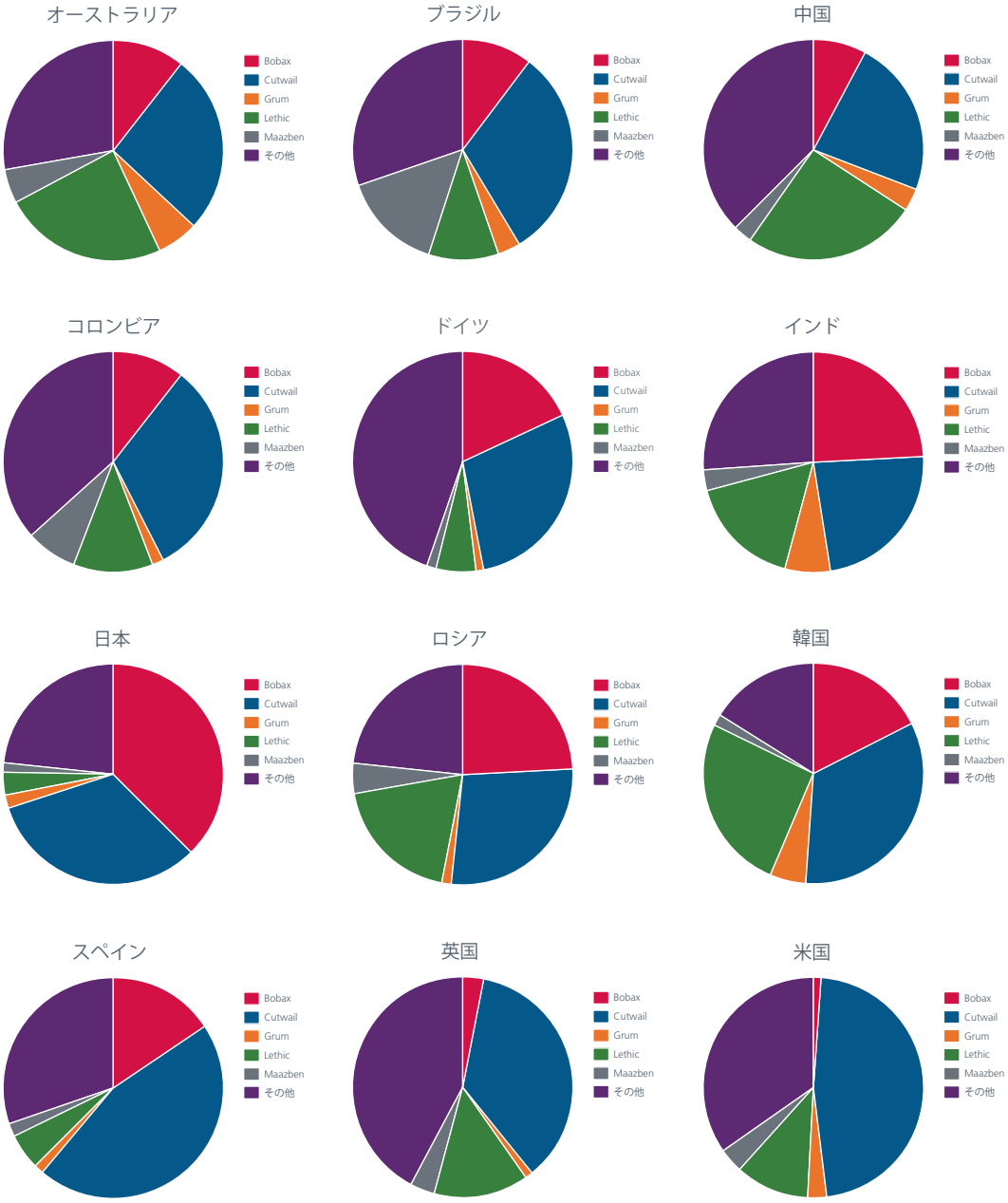




ボットネットの種類には大きな変化は見られません。Bobax は 10 月と 11 月に増加し、12 月に減少しました。Lethic は前四半期にピークを迎えましたが、 その後は減少しています。 Cutwail と Maazben は 12 月に急増しました。この四半期に最も顕著な動きを見せたのは Grum です。長期間減少傾向を示していましたが、12 月には数年前の水準に戻っています。



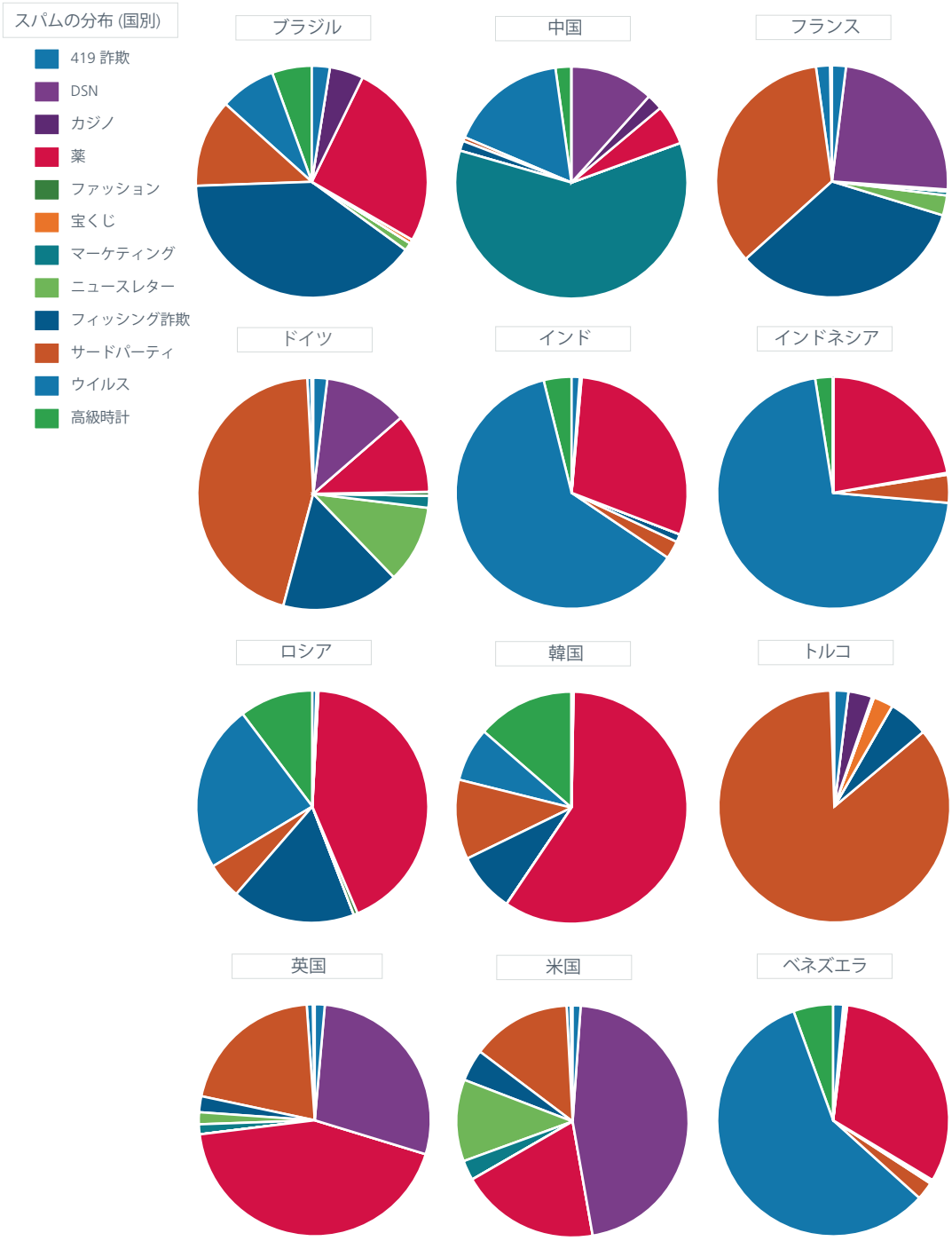
新規感染率が低下しても、 ボットネットの勢力が落ちたわけではありません。 国別の詳細を見ると、 ボットネットの多くがいまだに活発に活動しています。 この円グラフは各国でのボットネットの分布状況を表していますが、 国によって検出総数がかなり異なるため、 この円グラフを単純に比較することはできません。



ソーシャル エンジニアリングの詳細

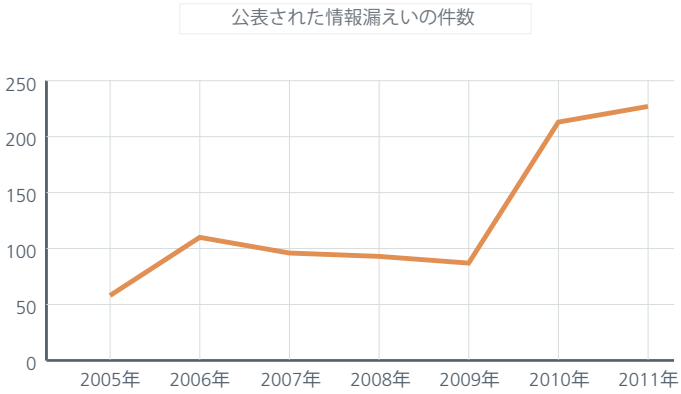
前回と同様に、 ソーシャル エンジニアリングの手口とスパム メールの件名は国によって大きく異なります。

メッセージの内容は国ごとに特化しています。 月や季節によっても異なりますが、 休日やスポーツ イベントがよく利用されています。スパムの内容を見ると、ブラジルではフィッシング詐欺がよく利用されていますが、中国では販促目的のスパムが一般的です。ドイツではサードパーティが大半を占めていますが、 フランスではサードパーティとフィッシング詐欺が上位を占めています。 英国では薬関連がトップですが、 インドとインドネシアではウイルス警告が第 1 位です。



情報漏えいとネットワーク攻撃

この四半期と昨年に発生したデータベース攻撃を見ると、いくつかの傾向が確認できます。数年前から情報漏えいが公表されるようになりましたが、過去 2 年間で報告件数が急増しています。privacyrights.org によると、2009 年以降、ハッキング、マルウェア、オンライン詐欺、侵入者による情報漏えいの件数は倍以上になっています。



この四半期だけを見ても、40 件以上の情報漏えいが公表されています。この 3 か月の数字が過去最高ではありませんが、情報漏えい事件は今後も増加するでしょう。

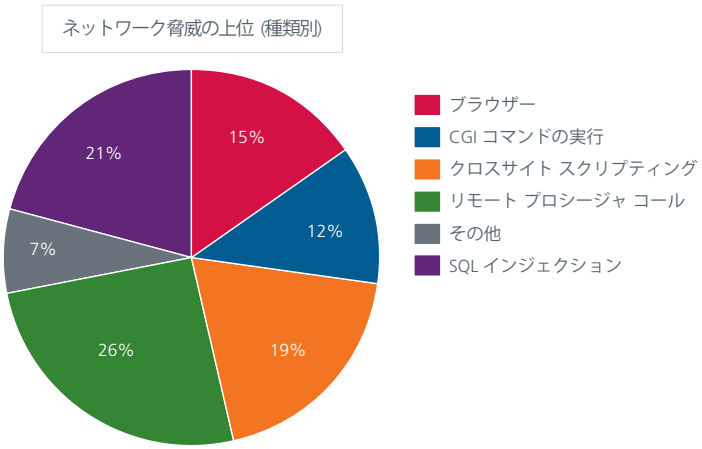
前述の傾向にも関係していますが、IT スタッフとセキュリティ担当者のデータベース侵入に対する警戒心が高くなっています。漏えい事件の件数が増加したため、その結果、セキュリティに対する意識が高まりました。

この傾向は、Oracle ユーザーに対する最近の調査結果にも表れています。

「回答者の 25% 以上は、今後 12 か月以内に情報漏えいが < 必ず発生する > または < 発生する可能性がある > と答えています。組織内でデータベース セキュリティを担当する回答者に限定すると、3 分の 1 以上が SQL インジェクション攻撃の防止対策を講じ、本稼働環境のデータベースを監視するシステムを導入していると答えています。これは非常に心強い結果です。特に、何年もの間、データベースのセキュリティ ソリューションが軽視されていた点が考慮されていることは評価すべきでしょう」[2]

理想には程遠いものの、データベース セキュリティに対する意識はかなり向上しています。被害の大きい情報漏えいが多発するまで改善されなかったのは残念ですが。

マカフィーでは、ネットワーク攻撃に関するデータを McAfee Global Threat Intelligence™ ネットワークから収集し、分析を行っています。



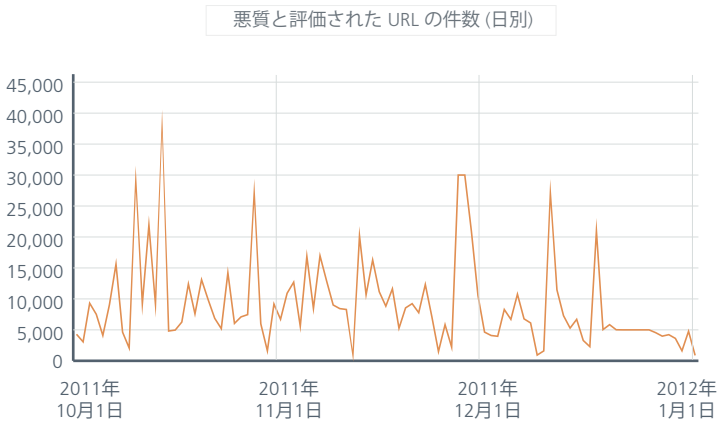
この四半期の主なネットワーク脅威は、Microsoft Windows リモート プロシージャ コールの脆弱性による

ものです。 この脆弱性の次に多かったのは SQL インジェクションとクロスサイト スクリプティングです。 この 2 つの攻撃はリモートから実行されるため、 世界中から標的を選択して攻撃を行うことが可能です。 これに対し、 ブラウザーに対する攻撃は一般にクライアント側の脅威です。 この傾向が、 情報漏えいをもたらすリモート攻撃の増加とハクティビズムなどの活動の増加に関係しているかどうかは分かりません。 この問題については引き続き調査を行います。

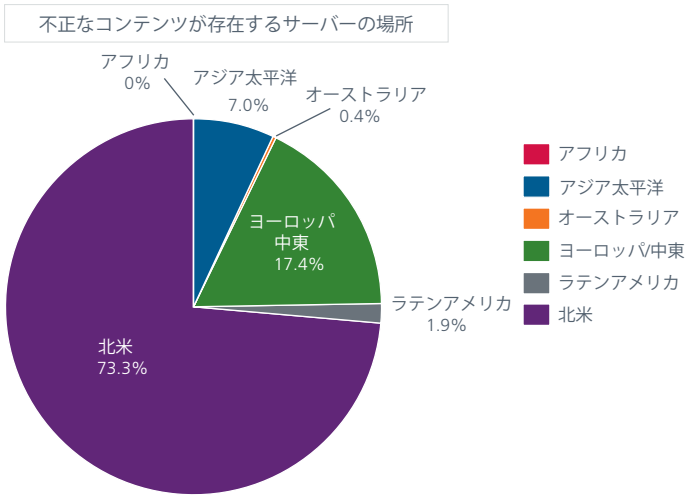
Web 脅威

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、 振る舞い自体も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。

McAfee Labs では、 第 3 四半期に一日平均 6,500 件の悪質なサイトを新たに記録しました。 この四半期はこの数字が 9,300 件に増加しています。 また、確認した URL の中で 400 件に 1 件は悪質なものでした。 200 件に 1 件の割合で悪質な URL が見つかった日もあります。 サイバー犯罪者にとって休暇シーズンは稼ぎ時です。 この時期に件数が急増しても不思議ではないでしょう。

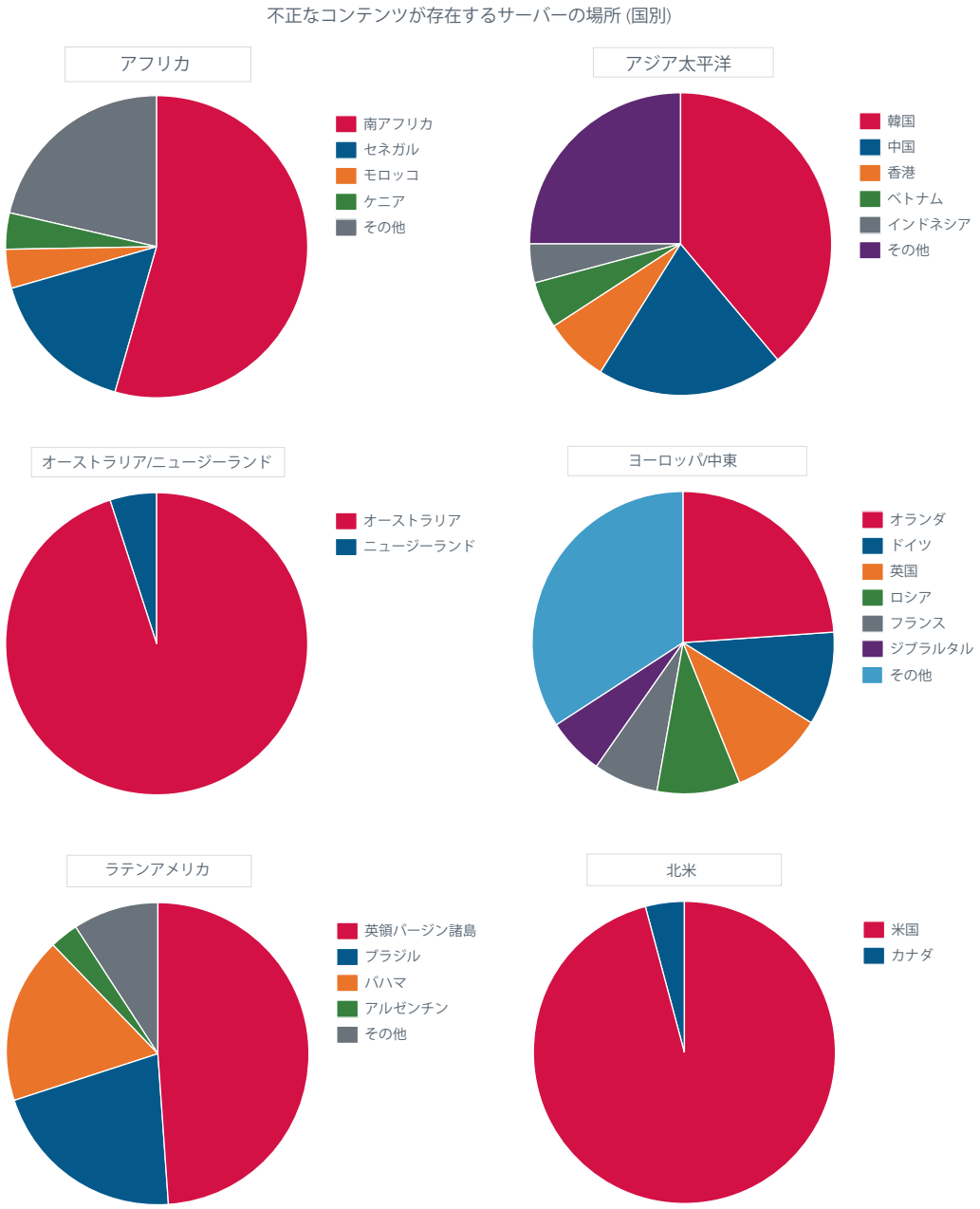


新しい悪質サイトの殆どは米国で見つかっています。 次いでオランダ、カナダ、韓国、ドイツ、英国、ロシア、中国に多くの悪質サイトが確認されています。 前四半期と上位 8 か国に変化はありませんが、 順番は異なります。 地域別の詳細を見ると、 不正なサーバーが最も多く存在する場所が分かります。

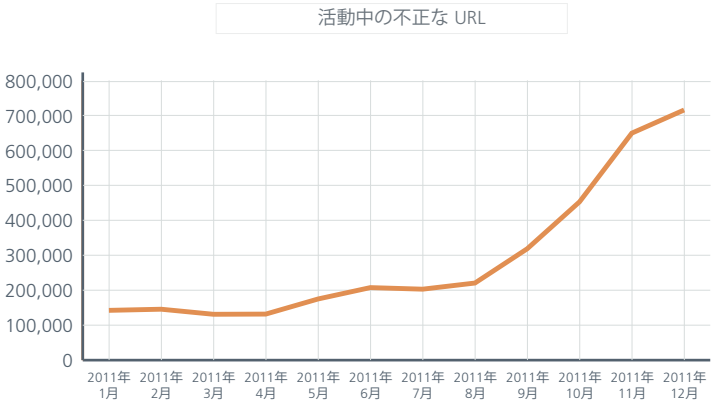


前のページのグラフは 1 年間の結果を表しています。 北米が他の地域を大きく引き離し、 一位になっています（最も低い値は第 2 四半期の 60%）。 これに続くのがヨーロッパと中東です（他の 3 四半期は 18% から 25%）。

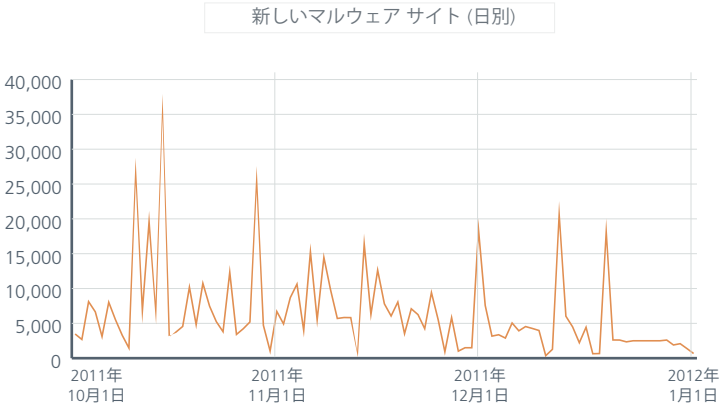
地域別の詳細を見てみると、 インターネットのリスクは世界中に蔓延していることが分かります。



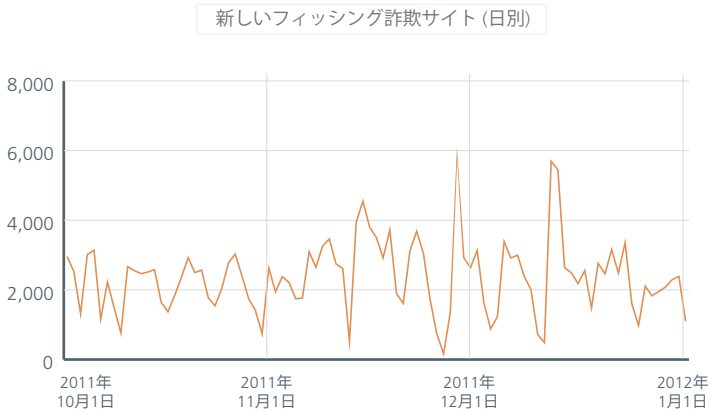
不正な URL をホスティングしている Web サイト（悪質なダウンロードとブラウザー エクスプロイトが存在するサイト）の数は確実に増加しています。



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 サイトの数が急増し、一日平均 6,500 件のサイトが新たに見つかりました（第 3 四半期は一日平均 3,500 件）。



フィッシング詐欺サイトはわずかに減少しています。前四半期は一日平均 2,700 件でしたが、この四半期は約 2,200 件でした。



サイバー犯罪

クライムウェア ツール

10 月、 Rhino スクリプト エンジンを攻撃する新しい Java の脆弱性が見つかりました。 この脆弱性を悪用すると、署名なしの Java アプレットを実行して上位の権限を取得し、サンドボックスの外で任意の Java コードを実行することができます。 この脆弱性が発表されてまもなく、 Metasploit プロジェクトにエクスプロイト モジュールが公開されました。 このモジュールは様々なクライムウェア キットに組み込まれています。

名前	価格（すべて米ドル）	
Phoenix Exploit Kit 3.0 （12 月）	$ 2,200（シングル ドメイン） $ 2,700（マルチスレッド ドメイン）	第 2 四半期の脅威レポートでバージョン 2.7 を報告しましたが、この四半期では 3 つのアップデートを確認しています。 バージョン 3.0 には Java Rhino エクスプロイト（CVE-2011-3544）も含まれています。
BlackHole Exploit Kit 1.2.1 （11 月）	年間ライセンス : $ 1,500 半年ライセンス : $ 1,000 3 か月ライセンス : $ 700	このアップデートには Java Rhino も含まれています。

主な事件

この四半期には、 産業システムや国家インフラを狙った様々な攻撃が発生しています。 この中の 2 件は米国南部で起きています。

- 11 月の初め、 ニュージーランドにある St John Ambulance の通信センターがマルウェアの攻撃を受け、自動応答システムが停止しました。 このセンターでは、 年間 100 万件以上の救急連絡に対応していますが、 この攻撃で自動機能が使用不能になり、 救急車の手配が人手で行われました [3]。
- 11 月 18 日、 Pr0f と名乗る攻撃者が、 テキサス州ヒューストン南部にある上下水道施設の監視・制御を行うユーザー インターフェースの画像を公開しました [4]。
- 12 月 7 日から 12 月 10 日にかけて、ジョージア州の Lawrenceville and Duluth のネットワークからマルウェアが検出されました。 このマルウェアは地域の病院システムを乗っ取り、「患者の受け入れ不能」状態を宣言しました [5]。

11 月 10 日、 イリノイ州の Statewide Terrorism & Intelligence Center が Intelligence Note で SCADA[6] 水道施設がハッキングされたことを発表しました。 この攻撃の発生源はロシアでした [7]。 この 6 日後、 Industrial Control Systems の CERT は、 この事件がサイバー攻撃に関連していないことを発表しました [8]。 サイバー攻撃との関連性が否定されるまでに数日を要したことは興味深い点です。

サイバー犯罪に対する取締り

11 月はサイバー犯罪者の摘発に成功した月となりました。

- FBI は 11 月 9 日、 400 万台以上のコンピューターをハッキングして、 オンライン広告詐欺で 1400 万米ドルを盗み出したとして、 6 人のサイバー犯罪者がエストニアで逮捕されたことを発表しました。 これは、 2 年間に及ぶ Ghost Click 作戦の成果です [9]。 米国への引き渡しはまだ行われていません。この 6 人は、 DNSChanger ファミリーのマルウェアを使用し、 被害者が意図したサイトではなく、 自身が制御している不正なサーバーに被害者を誘導したようです。 この逮捕は、 この数年で最も大きな成果の一つといえるでしょう。
- 11 月 15 日、2010 年 12 月に NASA のサーバーに不正アクセスを行った容疑で、26 歳のルーマニア人（ハンドル名は Iceman）がルーマニアの組織犯罪テロ対策チームに逮捕されました [10]。
- 11 月 23 日、 フィリピン警察と FBI は、 AT&T などの電話会社の PBX 電話回線をハッキングし、 銀行口座から残高を盗み出したとして 4 人の容疑者を逮捕しました。 捜査当局によると、 この 4 人は、 インドのムンバイで 2008 年に発生したテロ攻撃に資金を提供していたテロ集団に関与していた可能性があります [11]。
- 12 月 5 日、 タイ人とナイジェリア人のグループと企業に 6 億 1000 万ドルの支払いが命じられました。 このグループと企業は、 2006 年から 2009 年にかけて Yahoo ユーザーに架空の宝くじに関するスパムを配信した容疑で起訴されていました [12]。

- 12 月 9 日、英国の Police Central e-Crime Unit の捜査員が、2011 年 8 月に英国の学生を狙ったフィッシング詐欺を行ったとして 6 人の容疑者を逮捕しました。このフィッシング詐欺では 100 万ポンド以上が盗まれました [13]。
- 12 月 9 日、米国とイタリアの企業から 140 万米ドル以上を盗み出したサイバー犯罪集団の一味として、3 人のウクライナ軍人がルーマニアで逮捕されました [14]。この 3 人は、インターネット バンキングのログイン データを盗み出し、被害者の口座から自身の会社に送金した容疑で起訴されました。
- 12 月 9 日、米連邦取引委員会はウクライナの Innovative Marketing との和解が成立したと発表しました。Innovative Marketing は、騙されて同社のスケアウェアプログラムを購入した 320,000 人に払い戻しを行うことに同意しました [15]。払戻金額は平均で 20 米ドルになります。Innovative Marketing は 2003 年から 2008 年にかけてスクエアウェアを大量に販売しました。McAfee Labs の主任研究員である François Paget は『スケアウェア : 世界中で被害を拡大する偽のセキュリティ ソフトウェア』でこの会社について詳しく報告しています [16]。

ハクティビズム

この四半期は、ハクティビスト集団 Anonymous の内紛が目立ちました。

- Occupy Wall Street に対する支援の一環として、Anonymous は Invade Wall Street 作戦を宣言し、10 月 10 日にニューヨーク証券取引所 (NYSE) に対して分散型サービス拒否 (DDoS) 攻撃を実行し、インターネット上から NYSE を抹消すると予告しました。Anonymous 内部からの反対があったためか、大規模な攻撃には至らず、影響は殆どありませんでした。
- トロント証券取引所に対しても 11 月 7 日に同様の攻撃を行うと予告しましたが [17]、攻撃は実行されず、通常通りに取引が行われました。今回も Anonymous 内部の対立が原因のようです。
- 11 月 5 日には Facebook に対する攻撃が予告されていましたが、これも反対派に潰され、攻撃には成功していません。
- 12 月 24 日、Anonymous のメンバーを名乗る人物が、米民間調査機関 Stratfor のネットワークをハッキングしたと声明を出しました。この攻撃では顧客リストが盗まれ、4,000 件以上のクレジットカード番号、パスワード、自宅の住所が流出しました。攻撃者は、盗み出したクレジットカード情報を使用し、米国赤十字社や CARE などの慈善団体に寄付を行いました。Anonymous グループはすぐにこの情報漏えいに対する関与を否定し、Sabu や LulzSec を非難しました [18]。
- 年末には #lulzxmas 作戦が展開されました。Anonymous は、この作戦を世界的な金融機関、軍組織、政府機関に対する 1 週間にわたるハッキング活動としていますが、この作戦の目標と標的はいまだに不明です。

この四半期のハクティビストの活動としては、警察関係者の情報開示が目立ちました。多くの警察関係者の写真、個人情報、家族の詳細がネット上に公開されています。

- 10 月 26 日、Occupy Oakland の取締りに対する抗議として、カリフォルニア州オークランドの警察官に関する情報がネット上に流出しました [19]。
- 11 月 18 日、カリフォルニア州司法局は、コンピューター犯罪調査を担当する特別捜査官の Gmail/Google アカウントが不正にアクセスされたことを発表しました [20]。同日、2 つのアカウントから送信された 38,000 通の電子メールと Tor ネットワークの非公開サイトに保存されていた個人文書がファイル共有サイトに公開されました。
- 11 月 18 日にカリフォルニア大学デービス校で警官がデモ隊に催涙スプレーを噴射している写真が公開されると、この警官の個人情報がネット上に流出しました [21]。
- 11 月の終わりに、LulzSec Portugal が政府機関、政治団体、警察の Web サイトに DDoS 攻撃を実行し、緊縮政策、格差社会、11 月 24 日のデモに対する警察の横暴を非難しました。このグループは、リスボン警察の 107 人以上の氏名、階級、ID 番号、連絡先、職歴を公開しました [22]。
- フランスでは、暴力行為を行った、あるいは極右思想の持ち主として警察官の個人情報が数か月間 Copwatch サイトに掲載されました。最高裁判所はフランスの主要な ISP に対し、このサイトをブロックするように指示しました [23]。

このような攻撃の対象は警察だけではありません。政治家などの有名人がハクティビストの主張に反する立場をとったり、行動を起こせばすぐに攻撃対象と見なされます。12 月 15 日、Anonymous は、国防授権法（NDAA）を通過させた米上院議員の情報を大量に流出させました。フランスでは、右派や極右派の政治家が物議を醸す意見や声明、政策を発表した後に、その政治家の個人情報がネット上に流される事件が起きています。

サイバー上の争い

ハクティビズムという言葉が話題になるようになったのは 2010 年のことです。このとき、サイバー上の活動してエストニア（2007 年）とグルジア（2008）の例を挙げましたが、この四半期も政府や政党の資金援助が考えられる事件がいくつか発生しました。

- 11 月 1 日、パレスチナ自治政府の Mashur Abu Daqqa 通信相は、パレスチナのサーバーを攻撃し、パレスチナ通信省、ヨルダン川西岸やガザ地区電話回線とインターネット サービスを切断したと世界中のハッカーを非難しました。この事件は、米国とイスラエルが反対していたパレスチナの UNESCO 加盟が決定した後に発生しました。イスラエルが攻撃の糸を引いていると同大臣は非難しています [24]。
- 12 月 3 日、韓国警察庁サイバーテロ対応センターは、10 月 26 日の投開票日の朝に中央選挙管理委員会の Web サイトに対するサービス拒否攻撃を指示したとして 4 人の容疑者を逮捕し、拘置状を請求したと発表しました。このサイバー攻撃により、投票所に関する情報がアクセス不能になりました。容疑者の一人は与党ハンナラ党議員の元秘書でした。今回のソウル市長選の 6 日前に元国会議長の秘書の銀行口座から容疑者の口座に合計で 1,000 万ウォン（8,619 米ドル）の送金があったとの情報もあります。選挙の 5 日後に攻撃の実行犯と見られる人物への送金が行われていたことが判明しています [25]。
- ロシアでは、12 月初めに実施された選挙で、ロシアの人気ラジオ局と選挙監視団体がサービス拒否攻撃を受け、Web サイトがアクセス不能になりました。選挙違反について報じていた他の独立系メディアのサイトもサイバー攻撃の被害を受けました [26]。
- League and Cup Channel がパンアラブ競技大会（12 月 9 日から 12 月 23 日）のモロッコ代表団の写真と一緒にモロッコ領サハラが抜けている地図を使用したことに抗議して、Moroccan Deterrence Force を名乗る攻撃者がカタール政府の Web サイトに Moroccan Vengeance という攻撃を行いました [27]。

サイバー攻撃に対する政府の関与を証明するのは容易ではありません。今後も引き続きサイバー犯罪、ハクティビズム、サイバー戦争の可能性について調査を続けていきます。

筆者について

本レポートは、McAfee Labs の Zheng Bu、Toralv Dirro、Paula Greve、David Marcus、François Paget、Ryan Permeh、Vadim Pogulievsky、Craig Schmugar、Jimmy Shah、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。www.mcafee.com/jp

[1] https://blogs.mcafee.com/mcafee-labs/the-day-of-the-golden-jackal-%E2%80%93-further-tales-of-the-stuxnet-files
https://blogs.mcafee.com/mcafee-labs/of-kernel-vulnerabilities-and-zero-dayz-a-duqu-update
[2] 「データベースの危険性は増している」ー『Oracle 2011 IOUG Data Security Survey』（Oracle 2011 IOUG データセキュリティ調査）
[3] http://www.stuff.co.nz/waikato-times/news/5953497/Computer-virus-hits-ambulances
[4] http://news.cnet.com/8301-27080_3-57327968-245/hacker-says-he-broke-into-texas-water-plant-others/
[5] http://www.securitynewsdaily.com/computer-worm-shuts-down-atlanta-hospitals-1416/
[6] Supervisory Control and Data Acquisition（リモート監視・制御システム）の略
[7] http://community.controlglobal.com/content/water-system-hack-system-broken
[8] http://us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf
[9] http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911
[10] http://news.softpedia.com/news/Romanian-NASA-Hacker-Graduates-From-University-of-Weed-235069.shtml
[11] http://www.reuters.com/article/2011/11/26/us-philippines-usa-idUSTRE7AP06320111126
[12] http://news.cnet.com/8301-27080_3-57338828-245/yahoo-awarded-$610-million-from-lottery-spammers/
[13] http://content.met.police.uk/News/Six-arrested-arrested-in-million-pound-phishing-scam/1400005228273/1257246745756
[14] http://krebsonsecurity.com/2011/12/ukrainian-general-arrested-in-cyber-heists/
[15] http://www.ftc.gov/opa/2011/12/rebates.shtm
[16] http://www.mcafee.com/japan/media/mcafeeb2b/international/japan/pdf/threatreport/1012_running-scared-fake-security-software.pdf
[17] http://www.nowtoronto.com/news/webjam.cfm?content=183319
[18] http://www.talkleft.com/story/2011/12/25/124727/35
[19] http://www.scmagazineus.com/anonymous-downs-oakland-police-site-after-violence/article/215433/
[20] http://arstechnica.com/tech-policy/news/2011/11/anonymous-exposes-cybercrime-investigators-gmail-voicemail.ars
[21] http://www.washingtonpost.com/blogs/blogpost/post/anonymous-targets-pepper-spraying-uc-davis-cop/2011/11/22/gIQA0Pr8lN_blog.html
[22] http://tek.sapo.pt/noticias/internet/lulzsec_ataca_mai_e_divulga_dados_pessoais_de_1204169.html
[23] http://blog.indexoncensorship.org/2011/10/17/france-copwatch-site-blocked/
[24] http://www.google.com/hostednews/afp/article/ALeqM5hsZ6qUDvnFIrgo9CyZ9u_NhGu-Og
[25] http://english.hani.co.kr/arti/english_edition/e_editorial/510303.html
[26] http://www.euronews.net/2011/12/04/russian-election-hackers-attack-opposition-sites/
[27] http://moroccoworldnews.com/2011/12/moroccan-hackers-attack-media-websites-in-qatar/18702

41604rpt_quarterly-threat-q4_0112_fnl_ETMG

McAfee
An Intel Company

マカフィー株式会社
www.mcafee.com/jp

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