レポート

McAfee
An Intel Company

2013 年の脅威予測

McAfee Labs

目次

McAfee Labs は 2012 年、エンドポイント、ネットワーク、メール、Web サイトを対象とするマルウェア、脆弱点、脅威についての膨大なデータを収集しました。また、こうした不正侵入をブロックし、弊社のお客様に対する危険を低減するために、このデータを Global Threat Intelligence を用いて分析しました（詳しくは、「McAfee 脅威レポート : 2012 年第 3 四半期」をご覧ください）[1]。McAfee Labs では、2013 年も同様のことがさらに続くと予測しています。サイバー犯罪者やハクティビストは、我々のプライバシー、銀行口座、モバイルデバイス、会社、組織、家庭を襲撃するために使うテクニックやツールを強化し、進化させるでしょう。

McAfee Labs の研究者は最近、2013 年の主な脅威について討議しました。2013 年に増加する、または導入されると McAfee Labs が予測している脅威は、以下のとおりです。

- 被害者のマシン上で、不正アプリを購入したり、タップ決済を通じて盗みを働いたりする、モバイルワーム
- 携帯電話のセキュリティ更新をブロックするマルウェア
- プログラミングスキルを持たない犯罪者が、密かにゆすりを行えるようにするモバイルランサムウェアの「キット」
- Windows の深部や下層での持続的な攻撃
- Windows 8、HTML5 に対する攻撃方法の急速な発展
- 金儲けを目的とせず、インフラ破壊を試みようとする、Stuxnet のような大規模攻撃
- トロイの木馬「Citadel」を使用し、セキュリティ製品が対策しづらく、Zeus と同様の、しかし標的を一段と絞った標的型攻撃
- ボットネットが駆除されても再び接続を始め、感染を再度拡大するマルウェア
- 発信元をあちこちに分散して多数の IP アドレスから正規製品に関するスパムを送信し、厄介なメッセージが流れ続けるようにする「スノーシュー」スパム
- 感染した携帯電話から送信される SMS スパム
- 「サービスとしてのハッキング」: 地下フォーラムの匿名の売り手と買い手による、マルウェアキット、開発サービスの金銭売買
- 政治的な活動グループや過激派グループが増加し、入れ替わりでインターネット上のハクティビストグループ「Anonymous」が減少
- 国家や軍がサイバー脅威の発信元や被害者となる傾向が強まる

モバイルの脅威

マルウェアの活動が激化

犯罪者が効果的な金儲けのテクニックを一旦発見すると、そのテクニックを再利用し、自動化する可能性があります。例えば Android/Marketpay.A は、ユーザーの許可なしにアプリストアからアプリを購入するトロイの木馬プログラムです。詐欺師はこのマルウェアのアプリ購入ペイロードを利用したり、モバイルワームに追加したりすることが起こるでしょう。

マルウェア作者が開発したアプリが購入されると、その売上金は作者のものになります。エクスプロイトを使用し、脆弱な携帯電話上で数多く繁殖するモバイルワームは、こうしたアプリを購入するマルウェアにとって最高のプラットフォームです。攻撃者はもはや、被害者を必要としなくてもマルウェアをインストールできるようになるでしょう。ユーザーのインタラクションが不要な場合、モバイルワームの激化を阻止するものは何もありません。

NFC ワーム

近距離無線通信（NFC）対応の携帯電話は、ますます一般的になります。タップ決済で購入できる場所が増えるに従って、ユーザーはデジタルウォレットをどこにでも持ち歩くようになります。そのような柔軟性もまた、残念なことにサイバー犯罪者にとっては好材料になるでしょう。攻撃者は NFC 機能を使ってモバイルワームを作り、（「行き当たりばったりに感染させる」手法を介して）繁殖させ、金銭を盗みます。

マルウェア作者が盗みを働くのは、人口が密集するエリア（空港、ショッピングモール、テーマパークなど）です。NFC 対応ワームが大群衆の間で飛び交い、被害者を感染させ、ウォレットのアカウントから盗みを働く恐れがあります。

更新をブロック

（例えばマイクロソフト社とは対照的に）マルウェアとの闘いにおけるメリットの一つとして、携帯電話会社はマルウェアを認識した時点で自動的に顧客に強制更新を行わせ、デバイスからマルウェアを駆除することができます。この強制更新は、所有者によってルート化されていない（またはロックされていない）携帯電話上でのみ正しく機能します。マルウェアがモバイルに長く留まるためには、更新を阻止しなければなりません。携帯電話と携帯電話業者との通信をロックするマルウェアを外部からダウンロードするアプリをアプリストアに置けば、更新の阻止は成功です。

マルウェア

OS X やモバイル向けマルウェアの激増につながるキット

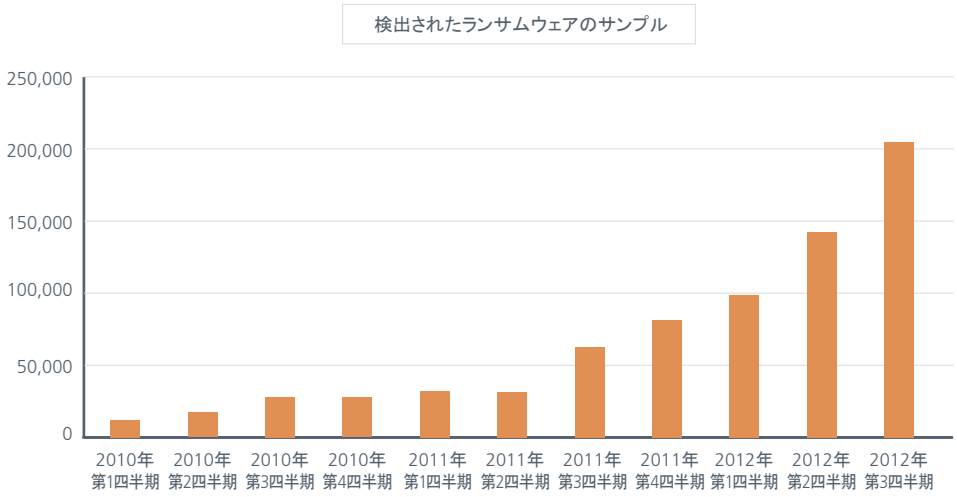
モバイルコンピューティングの人気を考えると、サイバー犯罪者がこの領域の大規模なエクスプロイトにかなり時間をかけてきたことは意外なことかもしれません。しかしその一方で、2012 年にはモバイルの脅威の件数が激増しました。その点をさらに詳しく調べると、地下市場でマルウェアキットが入手しやすいために、Windows ベースのマルウェアが大量に存在していることが分かります。2013 年には、ランサムウェアキットがマルウェアキットの先頭に立つ可能性が十分にあります。McAfee Labs では、Android や OS X がランサムウェアの標的となったケースを確認しています。目下、最初のランサムウェアキットが地下で販売されています。さしあたって、このキットの攻撃先は今のところ Windows システムのみですが、すぐに変わるかもしれません。

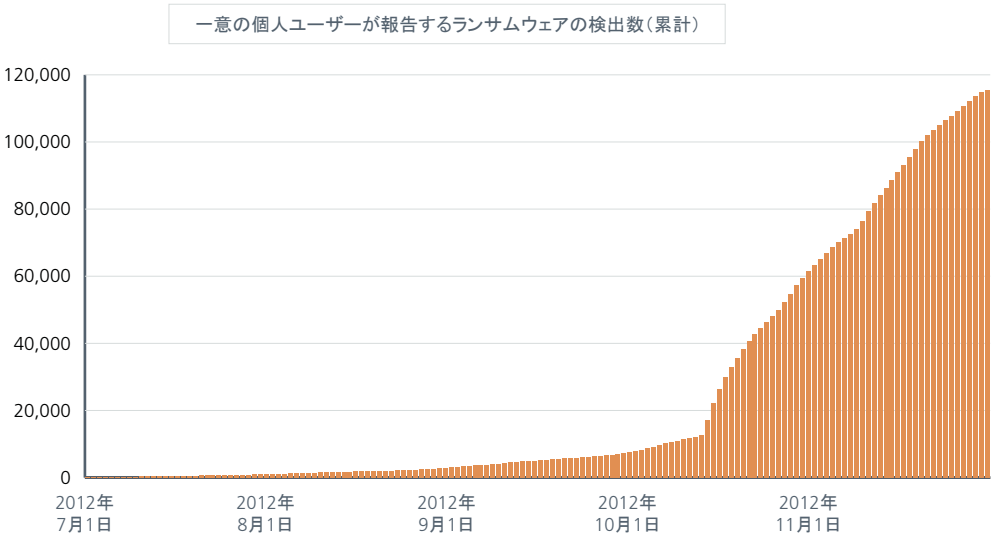
モバイルデバイスに広まり続けるランサムウェア

Windows PC 上のランサムウェアは、昨年中に 3 倍以上に増えました。この「ビジネスモデル」が功を奏していることを攻撃者はすでに証明し、攻撃をスケールアップして儲けを増やしつつあります。一方向性のランサムウェアは、ほかの種類のマルウェア（バックドア、キーロガー、パスワードスティーラーなど）とは異なり、お金を奪うために、被害者が感染したシステムを使用してオンライン取引をすることに依存しません。その代わりに、こうした犯罪者は、ユーザーのデータアクセス機能や通信機能、システム利用機能を完全に乗っ取ります。被害者は、アクセス復旧を望んでデータ紛失や身の代金支払いに悩まされることになります。

タブレットや携帯電話ではなくデスクトップ PC 上で取引を行うユーザーが増加しており、モバイルデバイスで儲けようとしている多くのマルウェア作者にとっては限界となっています。ただし、この傾向が長く続くことはないでしょう。ポータブルブラウザーの便利さから、取引を外出先で行う人々が増える見込みです。攻撃者はすでに、モバイルデバイス向けランサムウェアを開発済みです。身の代金要求に、当の携帯電話で録音した通話や撮影した画像をばら撒くという脅しが含まれていたら、どうなるでしょうか。

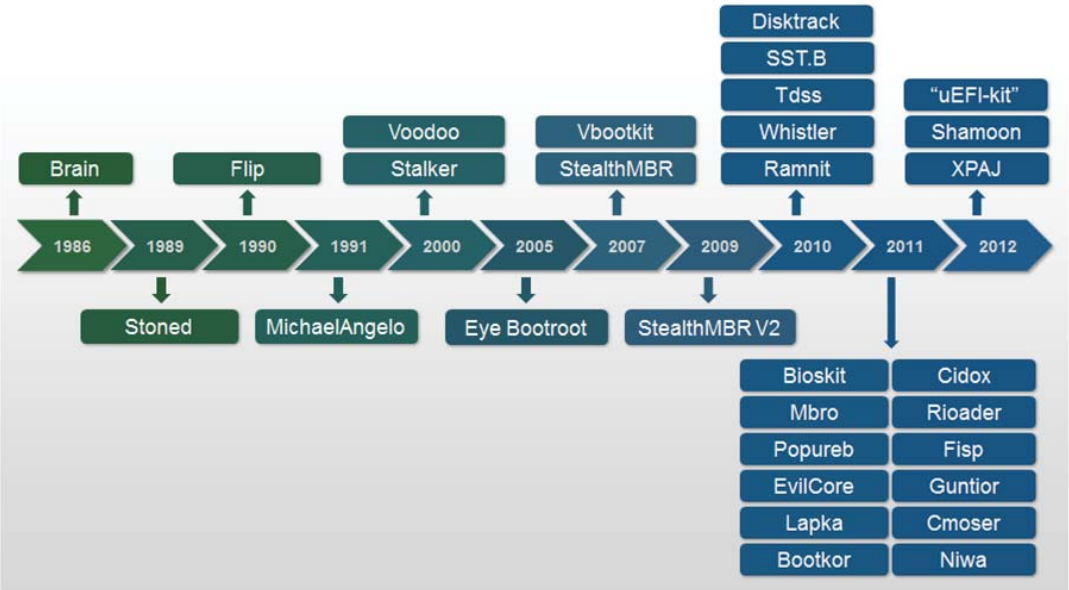
McAfee Labs では、2013 年中に、この領域での活動が大幅に増えると予測しています。


検出されたランサムウェアのサンプル
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


一意の個人ユーザーが報告するランサムウェアの検出数（累計）
120,000
100,000
80,000
60,000
40,000
20,000
0
2012年 7月1日
2012年 8月1日
2012年 9月1日
2012年 10月1日
2012年 11月1日

MBR や、その他のブートキットテクニックを使うルートキットの多様化

クライアントエンドポイントでのコンピューターセキュリティソフトウェアなどの防御が進化していることが後押しになって、脅威が OS スタックのさまざまな領域に進撃しています。しつこい潜伏攻撃者は特に顕著です。カーネル下で Microsoft Windows を攻撃する脅威の頻度は増えつつあります。標的にされている重要資産の中には、BIOS、マスターブートレコード（MBR）、ボリュームブートレコード（VBR）、GUID パーティションテーブル（GPT）、NTLoader などがあります。これらの脅威の数が、Windows やアプリケーション上で実行される、非常にシンプルな攻撃の数に迫る可能性は低いとはいえ、こうした複雑な攻撃によって、はるかに破壊的な影響が生じる恐れがあります。McAfee Labs では、この領域の脅威は 2013 年中に増加すると見込んでいます。



一部の注目すべきカーネル下の攻撃は、ここ数年の間に大幅に増加

次の大きな標的は Windows 8

犯罪者はお金を稼げるところで活動します。安全性が向上した Windows の新バージョンに対処すればお金になるのなら、迷わずそうするでしょう。多くの場合、犯罪者の攻撃対象は OS ではなく、ユーザーです。フィッシングなどのテクニックによってすっかり騙されたユーザーは、情報を明かしたり、不正プログラムをインストールしたりしてしまいます。したがって、アップグレードする場合はシステムの防御を Windows だけに頼ってはいけません。常に油断せず、フィッシング詐欺に警戒してください。

Windows 8 は、少なくとも当面は、マルウェアやエクスプロイトに対して、Windows の旧版よりも強力なセキュリティを用意するはずです。攻撃やマルウェアキットの地下市場における競争が 3 年前よりもずっと激しくなっている以上、Windows 8 固有のマルウェアの出現が、Windows 7 固有のマルウェアの出現よりも早まる恐れがあります。あるリサーチ会社によると、新しい UEFI（Unified Extensible Firmware Interface）を実行しているシステムは、OS の旧バージョンと同様に、依然として MBR ベースのルートキットに対して脆弱であるということです。Windows 8 のリリース日、マイクロソフト社は顧客への販売に際し、Windows 8 と Internet Explorer 10 の新たなセキュリティ強化点すべてを回避するゼロデイ脆弱性が存在する可能性を発表しました。

弱点があったとしても、Windows 8 は安全が強化された OS なので、アップグレードを検討する価値があるというわけです。なおも多くの人が Windows XP を利用していましたが、それも 2012 年秋に止まり、ついに Windows 新バージョンのユーザー数が XP ユーザーの数を上回りました。

大規模攻撃

マルウェアの有害なペイロードがめったに見られなくなったのは、攻撃者が儲けを得るために被害者のコンピューターを制御したり、知的財産を盗んだりすることを好むからです。しかし最近、McAfee Labs が確認した数件の攻撃では、明らかに標的を狙ったものもあれば、ワームとして実行されたものもありました。可能な限りのダメージを引き起こすことが、攻撃の唯一の目的だったのです。McAfee Labs では、こうした悪意のある活動パターンが 2013 年には増えると見込んでいます。

これが、一部の人が言うように新たな段階に進んだハクティビズムなのか、単なる悪意なのかは言い難いものの、気掛かりなのは、企業がこうした攻撃に対して脆弱性を感じさせるということです。分散型サービス拒否（DDoS）攻撃と同様に、ハッカーの技術的なハードルは、いくぶん低くなっています。攻撃者が破壊的マルウェアを多数のマシンにインストールできれば、壊滅的な結果が生じる恐れがあります。

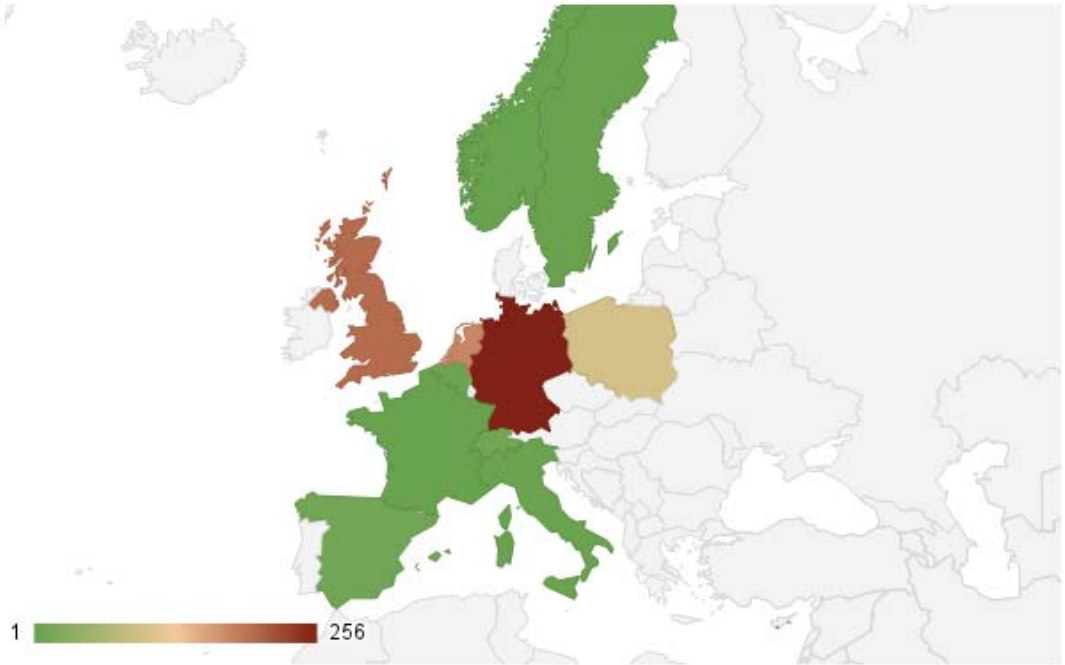
私たちは、どのようにすればこうしたインシデントに備えることができるでしょうか。さらに重要なことを言えば、どのようにすれば、いくらかでもダメージを軽減・防止できるでしょうか。必要なのは、最悪の事態を考えることかもしれません。長い時間をかけてネットワーク上の特権を向上させた内外の攻撃者は、複数サイトの多数のシステムに時限爆弾を仕掛けることも可能です。この影響は、多くの災害復旧計画で想定されている事項よりも深刻度が高い恐れがあります。IT 担当スタッフが何かしらの更新を行わなければならないのは、そのためです。最優先事項は、事業運営の維持です。運営維持を達成する最良の方法は、通常のネットワークから完全に遮断されている生産ネットワーク、SCADA システムなどを用意して、水際で攻撃を阻止することです。そしてその後にユーザーがデータをローカルマシンに保存することを好むことから紛失につながった大量のデータに対処することになるでしょう。時限爆弾が二度と現れないようにしながら、数千台のマシンの再インストールを行うことが一つの課題となるでしょう。有用性が証明されるであろうテクノロジーとしては、PC や OS の状態に左右されないリモート管理機能などがありますが、こうした機能については、インシデントが発生する前に試験を行う必要があります。

攻撃者がアクセスを試み、向上させようとする一方、このような持続的な脅威を検出してブロックするためのあらゆる手段は、前述の脅威の前段階に対して有効です。攻撃者が更新プロセスを完全にコントロールしていない限り、アプリケーションの遠隔制御によって、サーバーや主要システムの被害は阻止されるはずです。これは、管理システム上で誰が何をしているかを慎重に監視することで判断できます。データ紛失を最小限に止めるために、信頼性の高いネットワークバックアップと復元のプロセスを整える必要があります。また、ローカルデータのバックアップや、攻撃者にネットワーク上の共有デバイスや共有フォルダのデータを破棄させないようにすることも必要です。

トロイの木馬「Citadel」の照準

Citadel は、Zeus の多彩な機能や専用サポートを求めるサイバー犯罪者に好まれるトロイの木馬になりそうです。最近リリースされたトロイの木馬「Citadel Rain」は今や、詐欺師がターゲットのペイロードを一人でも複数でも、選択した被害者ユーザーに送信できるように、動的に設定ファイルを取得することができます。これによりサイバー犯罪者が、それぞれの基準に応じてアカウントのセキュリティを 1 回で侵害し、非常に的を絞った攻撃を展開できるようになります。攻撃が開始するまではエンドポイントのフットプリントが極めて小さいため、検索はより困難になります。概して、Zeus 攻撃はかなり拡散しました。Citadel Rain とその亜種を採用し、的を絞った攻撃に焦点を合わせて最大の利益を得ようとするサイバー犯罪者が増えるため、2013 年には変化が起こる可能性があります。

大半の Citadel による感染は欧州のごくわずかな人々に集中していますが、その数は 2013 年に増加すると McAfee Labs では予測しています。下の地図は、ドイツが最も感染件数の多い地域であることを示すものです。現在までに 200 件以上の感染が起こっています。



トロイの木馬「Citadel」が最も拡散しているのは西欧で、特にドイツでの拡散が最大。このマルウェアの攻撃は 2013 年に増加する見込み。

HTML5

HTML5 は、インターネットブラウザーの次期標準言語です。言語が改良され、プラグイン不要な機能、新しいレイアウトレンダリングオプション、ローカルデータストレージに対応する強力な新型 API、デバイスアクセス、2D/3D レンダリング、Web ソケット通信など、多くの機能が備わっています。現在、北米の 74 パーセント、アジアの 72 パーセント、欧州の 83 パーセントのユーザーが HTML5 の機能の大半に対応するブラウザーを使用しています [2]。Web サイトは、より充実したユーザー体験を得られるように HTML5 を速やかに導入中です。アプリケーション実行プラットフォームとしての OS から離れて、HTML5 へのブラウザーの移行は続きます。アプリストアが存在しないこと、互換性が向上して特定のブラウザーやデバイスに依存しなくなっていることを主要企業が上手く利用していることに伴い、HTML5 ベースのアプリケーションの数が増加中です。

ブラウザーは、長い間、主要なセキュリティ脅威ベクトルの一つでした。その点を HTML5 が変えることはないでしょう。HTML5 により、脅威の展望は変わり、広範化します。ブラウザーは新しいメディア機能と API を介してプラグインを提供するため、プラグインに焦点を合わせたエクスプロイトは減少する見込みです。その一方で、追加機能によって攻撃面が広がるため、HTML5 は、攻撃者に新たな機会をもたらすことになります。デバイスアクセスを可能にする強力な JavaScript API は、Web サイトがハードウェアに直接アクセスする時にブラウザーを危険に晒します。

3D レンダリングを実行する WebGL が、その一例です。WebGL 以前は、プラグインベースでない HTML コンテンツは、ブラウザーに解釈されて表示されていました。これにより、インターネット上の信頼できないデータと OS の間にテクノロジー層が置かれました。一方で、WebGL ブラウザーはグラフィックスドライバースタックとハードウェアを危険に晒し、攻撃ベクトルを著しく増加させます。研究者はすでに、Web アプリケーションがデスクトップからスクリーンショットを盗み取れるようにするグラフィックスメモリー盗難、WebGL 対応の一般的なブラウザーすべてと普及しているグラフィックスドライバースタックプロバイダーを使ったサービス拒否攻撃（DoS 攻撃）を立証しています。[3]

ネイティブアプリケーションと HTML アプリケーションを分ける主なものの一つは、ネイティブアプリケーションがクライアント側で任意のネットワーク接続を実行できる能力でした。HTML5 は、あらゆるユーザーに対する攻撃面を広げます。HTML5 の機能が、広範なポリシーやアクセス制御を必要としていないためです。したがって、HTML5 の機能によって、インターネットから取得したページが WebSocket 機能をエクスプロイトしたり、ユーザーのローカルネットワークをのぞき回ったりすることができるようになります。これまでは、同一生成元ポリシーによって不正使用が阻止されていたため、このような攻撃者にとってのチャンスは限られていました。また、このポリシーは、HTML ベース製品のセキュリティにとって不可欠なものでした。一方で HTML5 を使用すると、クロスオリジンリソース共有（CORS）は、あるドメインのスクリプトにネットワーク要求、データ投稿、対象ドメインから取得したデータへのアクセスを行わせ、それによって HTML ページがユーザーネットワーク上で偵察や制限付きオペレーションを実行できるようにします。

2013 年、各ブラウザーが HTML5 機能に対応するようになり、HTML5 互換性が向上するでしょう。HTML5 ベースのアプリケーションと Web サイトは、今後も増え続けます。また、2013 年には攻撃者が HTML5 セキュリティホール探しに目を向けるだろうと McAfee Labs では確信しています。問題は、攻撃者がどの程度早く成功を収めるかということです。

ボットネットとスパム

ボットネット復活

ボットマスターにとって最大の脅威は、ボットネットが回復不能な損失となることです。スパム、マルウェア、児童労働搾取、違法薬物の取り締まりにおける国際協力によって、ここ数年の間に主要なボットネットの多くが撲滅されました。この国際協力は、今後も引き続き、ボットネットの増殖を脅かし続けるでしょう。最大のボットネットが解体されると、その後、2 番手のボットネットが新たなターゲットになります。ボットマスターはすでにボットネットを細分化し、容易に検出可能なアクティビティ（DDoS やスパムなど）に伴うコストを増大させることによって、この活動に対処しています。ボットマスターが安全装備を実行し、通常時管理しているコントロールサーバーをすべて失ったボットネットのコマンドを再構築するようになるのも、時間の問題です。

多くの場合、ボットネットは、善意のセキュリティ研究者に一時的に乗っ取られます。ただし、起こり得るマイナスの副作用のために、こうした乗っ取りが感染ホストにたどり着く新しいコマンドにつながることはありません。いかに動機が正しかったとしても、システムの無許可遠隔操作には大きな責任問題が付随します。病院で使われている古い Windows マシンに新しいコマンドをプッシュすると、その PC は使い物にならなくなり、誤治療や、患者の死にすらつながります。ボットマスターは、ボットネットを形成することによって干渉し、解体後に再度制御を行うために、善意の人々によるこうした抵抗を利用するでしょう。

「スノーシュー」スパムは今後も増加

怪しげなマーケティング会社が企業のマーケティング担当者に接近して、どんな広告も受信することに同意しているメールアドレスのリストを持っていると言ってきたら、それは警鐘です。残念なことに、そうした警鐘はめったに鳴りません。携帯電話から葉巻や語学学習用ソフト、衛星テレビ、医療用品までに至る商品を販売している有名企業は、こうした怪しげな広告主と契約してしまうことがあります。怪しい企業は、サブネットから強制退去させられるまで、あるいはアドレスや時にはサブネットが永久ブラックリスト入りした後で立ち退くまで、毎日、新たにレンタルしたホストから大量の違法スパムメッセージを放出します。（多数の IP から送信することによって負荷を拡散することから、「スノーシュー（かんじき）」に例えられています。）受信者の受信箱はスパムメッセージ攻めに遭っており、メッセージを止めることは不可能です。

この種の活動は、大半の報道価値のあるハッキングやマルウェアほど悪質ではありません。そのため、この領域は当局からほとんど無視されてきました。とはいえ、こうしたスノーシュースパムの実行は、過去 2 年の間に激増しました。現在では、スパム界で一二を争う大問題です。この種の活動を白日の下に晒そうという研究者の試みは、このような怪しい広告主を利用している企業による名誉毀損訴訟の脅威という結果に終わりました。そういった環境下では（マーケティング予算が乏しい、または完全にカットされるような景気も相まって）、この種の活動は、すでに我々が経験したような猛烈なスピードで増え続けるばかりです。

感染した携帯電話から送信される SMS スパム

携帯電話業者は SMS スパム防止に取り組んでいます。顧客からレポートを受け取る第一の手段として、携帯電話業者は、受信したメッセージを携帯電話上で SPAM（7726）に転送して報告し、そのメッセージをブロックできるようにします。感染した携帯電話も、スパムテキストメッセージを送信する可能性があります。そうなると、被害者は自分のアカウントを携帯電話業者が閉鎖してしまうという問題に直面します。2013 年には、SMS によって薬物広告やフィッシングの誘いが送信されると McAfee Labs では予測しています。

クライムウェア

サービスとしてのハッキング

長い間、サイバー犯罪者は公開フォーラムに参加して、ほかの犯罪者との話し合いや取引を行っていました。このような集まりでサイバー犯罪者は、ソフトウェアだけなくサービスも売り込みます。プロ意識の高いサイバー犯罪者は、フォーラムを（「新参者」であふれているため）時間の無駄であり、（どの取引でもおとり捜査員かもしれないクライアントと直接連絡を取る必要があるので）機密性に欠けている上、（購入者が値下げ交渉しようとするため）損だと考えています。このような理由で、登録料や保証人（バウチャー）を求める招待客限定犯罪者フォーラムの数が増えています。

この傾向は続きますが、買い手の買う気をそぐことなく匿名性を高めるために、合法取引をモデルにしたオンライン販売サイトが 2013 年には増えるでしょう。こうしたサイトでは、買い手はマウスをクリックして好きなものを選択できます。また、匿名オンライン決済手段（Liberty Reserve など）を利用し、交渉抜きで購入品を受け取ったり、売り手に直接連絡を取ったりできます。

クライムウェアの購入を求める犯罪者のショッピングカート

より安全で匿名性の高いオファーを、インターネット上で見つけやすくなると予測されます。また、こうしたオファーの多様化も進みます。McAfee Labs では、サイバー犯罪者向けのハイレベルな監査やプロジェクト開発などのサービスを確認しています。[4]

ゼロデイ攻撃を売り込む疑わしいツールや、政府・シークレットサービス専用スパイサービスの売り出しが増えるでしょう。善悪を区別したり、本物の活動や顧客を見極めたりすることが難しくなります。

「サービスとしてのハッキング」の広告

ハクティビズム

Anonymous（アノニマス）の減少

Anonymous の支持者が苦しんでいます。多数のまとまりがなくあいまいな作戦により、Anonymous の評判に悪影響を及ぼしました。これに加えて、虚偽の情報、不当な主張、純粋なハッキング行為により、Anonymous は従来に比べて政治的に目立たなくなるでしょう。Anonymous の技術的洗練度のレベルは伸び悩んでおり、その戦術は、ターゲットとなる可能性のある人々に把握されています。そのため、彼らは以前ほど成功しないでしょう。ただし、ハクティビストと反グローバル化支持者の間や、ハクティビストと環境テロリストの間で意見が合致することによって、短期間の大々的な活動が起こることは、容易に想像することができます。

Anonymous は、ハクティビズムの一面でしかありません。強い政治的目的を持ち、長期間熱心に活動できる人々は、さらに強い影響力を持ちえます。MIT Technology Review 誌により 2012 年 4 月に発表された『Power People 2.0』というエピソードで説明されたリビア暴動への支持は、この好例でした [5]。また、こうした活動家の行為を支持するべく、Telecomix グループは、（ Anonymous と混同しないでください。）活動家の高度なハッキングテクニックに貢献しました。これらの人々のために、活動は大きな影響力を持つものとなったのです。このような活動は今後、ハクティビストの信念に人々が賛同するたびに、更に目立ってくるでしょう。

それと同時に、組織化してサイバー軍となった愛国者グループが自分たちの過激な考え方を広め、活発に活動を行うでしょう。これまで、同グループの取り組み（ほとんどは Web サイトの改ざんやごく短い期間の DDoS）にはあまり影響力がありませんでしたが、その活動の洗練度と攻撃性は向上するでしょう。彼らは間違いなく仲間割れするでしょうが、私たちが彼らの支持する過激派政府を非難するたびに、民主主義社会は彼らの本命の標的になるはずです。

国家や軍によるサイバー脅威への関与と、その被害の頻度が増大

世界の軍隊の多くが、ソーシャルネットワークの最前線にいます。軍隊の通信はますます頻繁に行われています。「CompanyCommand」のような専門フォーラムや、専門ウィキは、インターネット上のコラボレーションの開発を助長しています [6]。さらに、軍事作戦ではメール送信、ソーシャルネットワーキングや、残念ながら行われてしまう疑わしい Web サイトへのアクセスのために、インターネットを使います。これらの要素すべてが、侵入や故意でない情報漏えいの可能性を高めるでしょう。

Stuxnet や Shamoon の場合のように、専門家はもはや、物理的損害を招く軍事スパイや産業スパイ、あるいは精度の高い攻撃の国家的責任を予測することに消極的ではありません。国家関連の脅威が増大し、世間の注目を浴びるでしょう。また、政府支援による攻撃の疑惑も増えるでしょう。ゼロデイ脆弱点と高度なマルウェアを使うこうした攻撃には、先進の APT と考えられるものもあれば、従来型マルウェアを含むものもあります。

2012 年 1 月、米国大西洋評議会（Atlantic Council of the United States）は、特定の攻撃や攻撃活動の責任の所在を特定するにあたってアナリストをサポートするためのスペクトラムを発表しました [7]。このスペクトラムは、国が攻撃を無視、先導、実施するかどうかに基づく 10 のカテゴリーを用いて、極めて消極的な責任から極めて積極的な責任までを網羅しています。McAfee Labs では、攻撃を招くようなセキュリティ保護されていないシステムの採用から、同システムを計画・実行する国への攻撃までに及ぶ国の活動を判断するために、この測定ツールが 2013 年に効果を発揮すると見込んでいます。

戦闘に従事しない相手を対象にサイバー攻撃を仕掛けないとしても、テロリストの中には、インターネットを愛用する者もいます。こうしたテロリストが Web を利用するのは、情報伝達、新メンバー補充、プロパガンダ活動、資金調達、人物や標的に関する情報検索、そして襲撃準備を行うためです。多数の事例を各種レポートで読むことができます。国連薬物犯罪事務所（United Nations Office on Drugs and Crime）が発行した『The Use of the Internet for Terrorist Purposes（インターネットのテロ目的利用）』もその一つです[8]。次のステップとなるのは、サイバー攻撃と物理的攻撃の組み合わせです。これは、インターネット上の攻撃を物理的攻撃と連動して実行するものです。あるグループが防御システムや通信システムなどの重要インフラを遠隔で破壊できるならば、通常攻撃によってより簡単に、より大きな損害を引き起こすことができます。こうしたテロ事件が 2013 年に発生するという兆候はありませんが、今の私たちの懸念は絵空事ではありません。

筆者について

本レポートは、McAfee Labs の Xiao Chen、Toralv Dirro、Paula Greve、Prashant Gupta、Haifei Li、William McEwan、François Paget、Craig Schmugar、Jimmy Shah、Ryan Sherstobitoff、Dan Sommer、Bing Sun、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、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

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エスト 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

1 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf
2 http://arstechnica.com/information-technology/2012/08/forrester-report-urges-html5-adoption-says-most-browsers-can-support-it/
http://www.forrester.com/The+Coming+Of+HTML5/fulltext/-/E-RES70341
3 http://www.contextis.com/research/blog/webgl-new-dimension-browser-exploitation/
4 http://blog.xmco.fr/index.php?/page/2
5 http://www.technologyreview.com/featuredstory/427640/people-power-20/
6 http://companycommand.army.mil/index.htm
7 http://www.acus.org/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF
8 http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

MCARPT-1211-MC