レポート

McAfee
An Intel Company

McAfee 脅威レポート：2012 年第 2 四半期

McAfee Labs

目次

老子は古代中国の思想家です。「道徳経」の著者とされる老子は紀元前 6 世紀に実在したと言われていますが、 その言葉は現代でも価値を失っていません。 変化の激しい脅威の状況を見ると、 老子の名言が思い出されます。 至るところに脅威が存在する今の状況はまさに戦場です。 古代中国の兵法家である孫子は「勝つべからざる者は守なり。 勝つべき者は攻なり」という言葉を残しています。 この数年でマルウェアなど様々な脅威に関する多くの情報を得ていますが、 これらの脅威は四半期ごとに進化を続けています。 サイバー上の脅威に勝てるかどうかは様々な要因によって決まります。 孫子は「虞をもって、 不虞を待つものは勝つ」とも述べています。 答えは戦いへの備えにありそうです。

2012 年第 2 四半期で目立った動きとしては、 携帯端末（Android）を攻撃する新たな手段としてドライブ・バイ・ダウンロードの利用、 Twitter によるモバイル ボットネットのコントロール、 金銭を盗み出すモバイル用のランサムウェアの出現などが挙げられます。前の四半期に見られた脅威の傾向はこの四半期も継続しています。 前の四半期、 PC を攻撃するマルウェアは過去最高を記録しましたが、 この四半期はこの記録をすでに塗り替えています。 ルートキットは増加していますが、 他のマルウェアの勢いは収まっています。 殆どのマルウェア ファミリーは増加しています。 その中でも特にパスワード盗用型トロイの木馬の動きが顕著です。 ZeroAccess ルートキットは若干減少しましたが、 署名付きマルウェアはやや増えています。 Mac を狙うマルウェアも、 極端ではありませんが、 確かな増加傾向にあります。

世界の特定の地域でスパムが若干増えていますが、 長期的には依然として下降傾向が見られます。コロンビア、 日本、 韓国、 ベネズエラでは 10% 以上で増加しました。 ボットネットの感染数は 5 月に急増しましたが、 6 月には減少しました。

不正な Web コンテンツが最も多かった国はこの四半期も米国でした。 本文で詳しく説明しますが、 米国は様々な脅威の最大の発生元であり、最大の被害国でもあります。 保護対策が万全でないユーザーにとって Web は引き続き危険な存在となっています。 十分な警戒が必要です。

今回のレポートでもネットワーク攻撃を採り上げています。 SQL インジェクションとクロスサイト スクリプティング、 またその他の脅威について、 様々な観点から解説します。

サイバー犯罪の項では、 防弾ホスティングから「サービスとしてのクライムウェア」について説明し、 今期中に起こった主な逮捕、起訴案件を紹介します。 最後に、Anonymous のハクティビストグループとハクティビズム全般の最近の動向についても説明します。

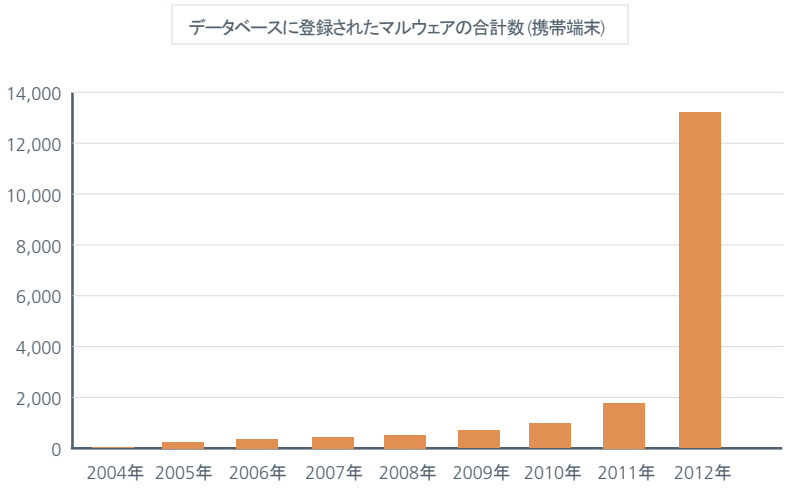
サイバー犯罪者は金銭を盗み出すために長期的な戦いを仕掛けてきます。 新しいオペレーティング システムや防御技術を検討する際には次の言葉を思い出してみてはいかがでしょうか。

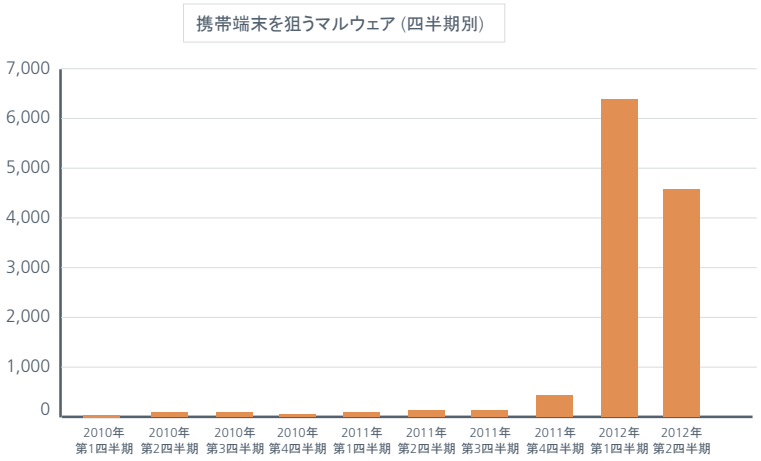
> 道具以下にも片分けて好く事あるべからず、余りたることは足ぬと同じ事なり、人真似をせずとも
> 我身にしたがいひ武具は手合うやうに有べし
> — 宮本武蔵「五輪書」より

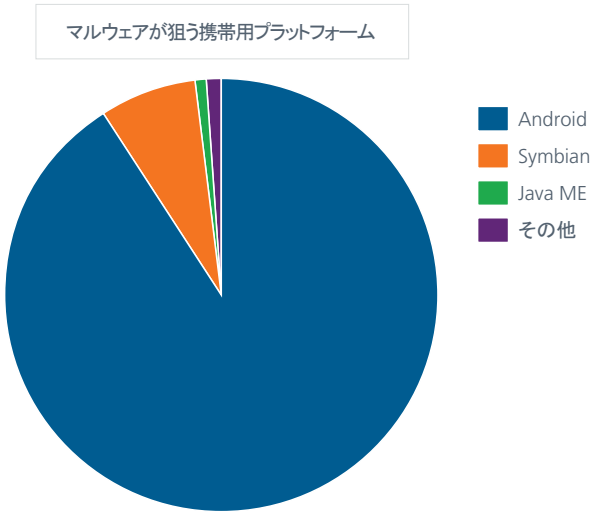
モバイルの脅威

携帯端末を攻撃するマルウェアの作成者が最もターゲットとするのが Android OS です。この傾向はしばらく前から続いていますが、この四半期も状況は変わりません。実際、この四半期に新たに見つかったモバイル マルウェアはすべて Android プラットフォームを狙ったものでした。主なものとして、SMS を送信するマルウェア、モバイル ボットネット、スパイウェア、破壊行為を行うトロイの木馬などが確認されています。

前の四半期ほどの爆発的な数ではないものの、この四半期も非常に多くのマルウェアが出現しました。今年以降続く増加の勢いに衰えは見られません。







この四半期は Android でもドライブ・バイ・ダウンロードのマルウェア（Android/NotCompatible.A）が見つかりました。 PC のドライブ・バイ・インストールでは、 サイトを閲覧しただけでコンピューターがマルウェアに感染してしまいますが携帯端末のドライブ・バイ・ダウンロードも同様で、 サイトの閲覧時にマルウェアが携帯端末にダウンロードされます。 ユーザーが操作を行わない限り、 このマルウェアがインストールされることはありませんが、 このファイルに Android System Update 4.0.apk のような名前が付いていると、 大半のユーザーは何の疑いも持たずにインストールしてしまうでしょう。

また、Twitter でコントロールされるボットネット クライアント（Android/Twikabot.A）も見つかりました。 このマルウェアは、 Web サーバーに接続する代わりに攻撃者が管理する Twitter アカウントを使用して命令を受信します。 攻撃者が命令をツイートすると、 感染したすべてのデバイスがその命令に従います。 Twitter のようなサービスを使用することで、 専用サーバーを用意したり、 被害者の情報を盗み出すことなく、 他人のリソースを利用することができます。 かつては同様の理由でインターネット リレー チャットが利用されていました。しかし、Web サービスを利用しているため、匿名性の点ではそれほどメリットはなかったようです。

前の四半期に SD カード上のすべての写真を破壊する Android/Moghava.A トロイの木馬が見つかりましたが、 この四半期は日本の人気歌手グループのファンを狙った新しい亜種（Android/Stamper.A）が出現しました。 この亜種では、 昨年「What would your baby look like?」で使用された赤ちゃんの写真を使用しています。 また、 書き換えコード内の文字列がいくつか変更されていますが、 それ以外は Android/Moghava.A と全く同じで、 写真を破壊する機能も持っています。 被害を受けたユーザーは端末内の写真がすべて赤ちゃんの写真に変えられてしまい、 見ようとしていたファン投票の結果を見ることはできません。

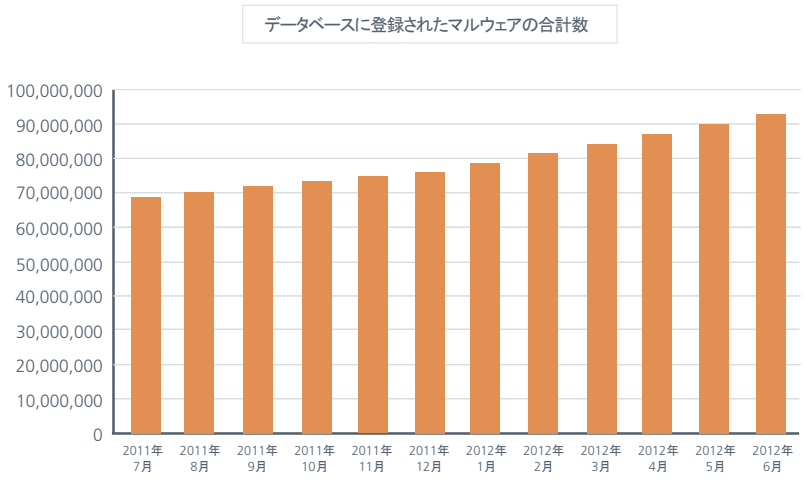
Android マルウェアの大半が PC のマルウェアに似ていても不思議はありません。 多くのマルウェア作成者は他のプラットフォーム用のマルウェアを作成し、 そこで積み重ねた技術と経験を生かしています。 携帯端末を狙うマルウェアは概念検証レベルでも、 初心者レベルでもありません。 完全に機能し、 十分に成熟しています。 モバイル マルウェアの作成者が狙っているのは消費者と企業のデータです。

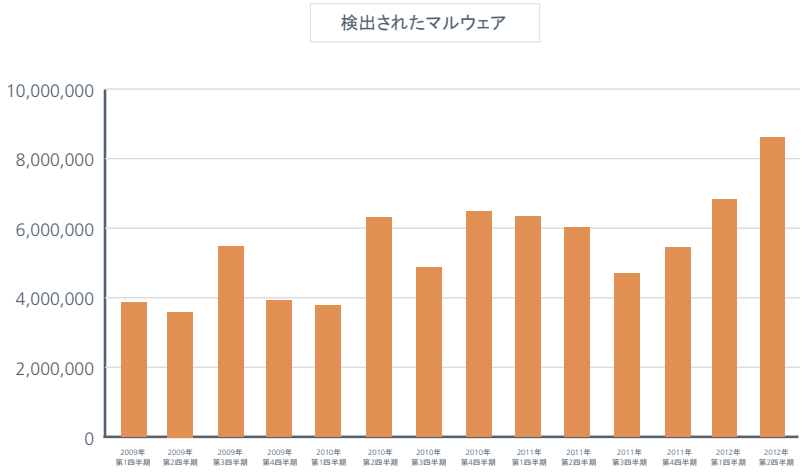
マルウェアの脅威

アルベール・カミュの有名なエッセイ『シーシュポスの神話』には不条理に対するカミュの哲学が書かれています。 カミュは、 理性では割り切れない世界に対して必死に明瞭な意味を求めようとする状態を不条理な状態としています。 このエッセイの最後の章ではギリシャ神話のシーシュポスを例に人生の不条理性が描かれています。 神々の怒りを買ったシーシュポスは大きな岩を山頂に運ぶという罰を受けますが、 山頂まで運ぶと岩はすぐに転がり落ちてしまい、 この意味のない行為を永遠に繰り返すことになります。

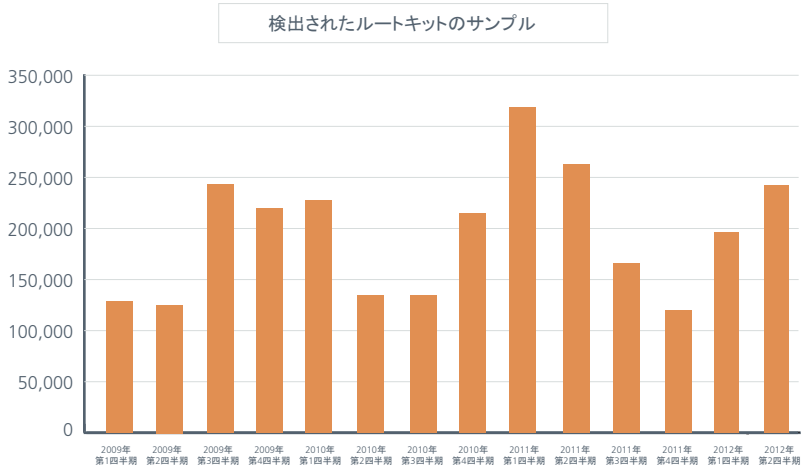
この 10 年間のマルウェアの動向をみると、 シーシュポスの山と同じ状況かもしれません。 この山はこの数年でより高く、より険しくなっています。 前回のレポートで四半期ごとのマルウェア検出数が過去 4 年間で最多になったことを報告しましたが、 この記録はあっさり塗り替えられました。 我々のラボに集まるマルウェアのサンプルは前の四半期よりも 150 万件も増えています。 このペースで進むと、 次の四半期には初めて 1 億を突破するほどの勢いです。 この数字は何を示唆しているのでしょう。 防御重視の情報セキュリティでは限界なのでしょうか。

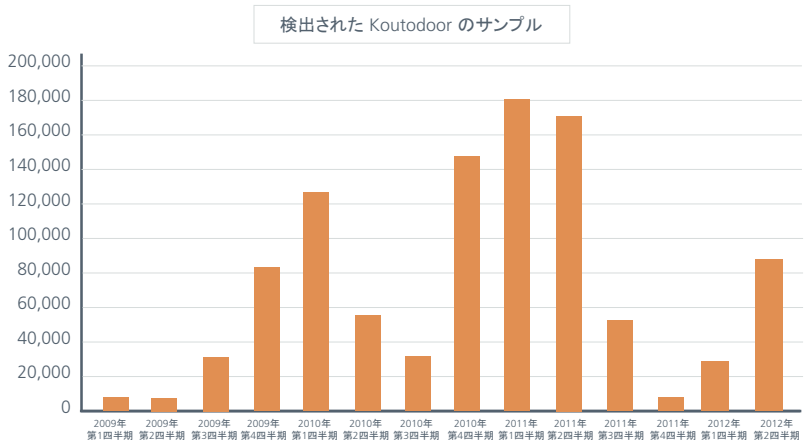
少なくとも、 岩がさらに重くなっていることは確かです。 ごくわずかな例外はありますが、 この四半期はマルウェアのすべての領域で前の四半期の数字を上回りました。 前の四半期に過去最高を記録した領域でも件数が増えています。 同じことを繰り返していたのではシーシュポス以上の徒労を永遠に強いられることになります。 今必要なことは、 この不条理を受け入れながらも、 新しい手法で対抗していくことでしょう。



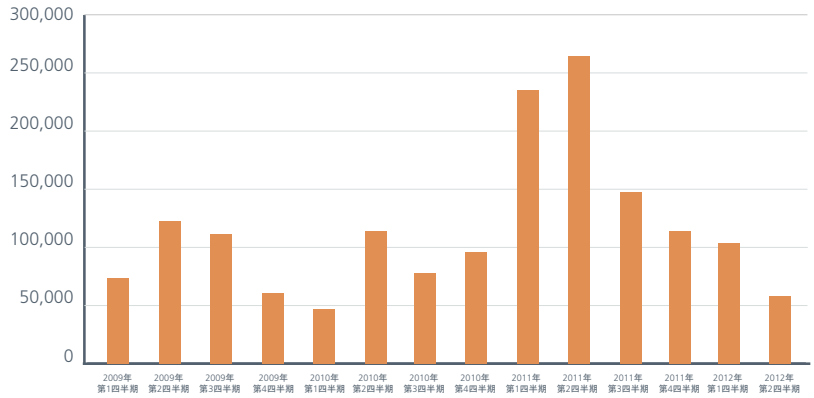


ルートキット全体で見ると、この四半期は若干の増加に止まりましたが、Koutodoor は著しく増えています。ZeroAccess と TDSS は前の四半期よりわずかに減少しましたが、 他のマルウェアへの影響は確実に見られます。ルートキット（ステルス性のあるマルウェア）はマルウェアの中で最も厄介な存在です。検出を回避し、システムに長期間潜伏するため、 他のマルウェアにも大きな影響を及ぼします。

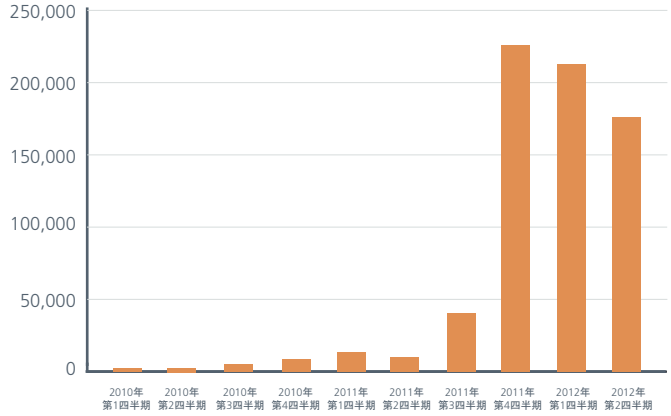




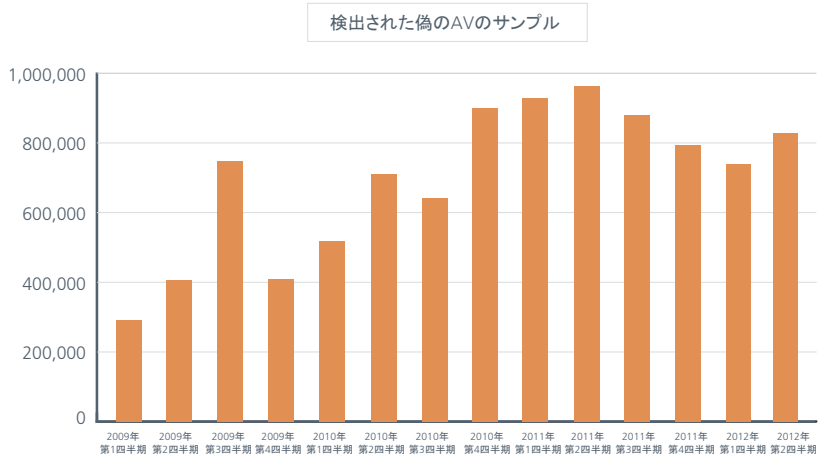
検出された TDSS のサンプル

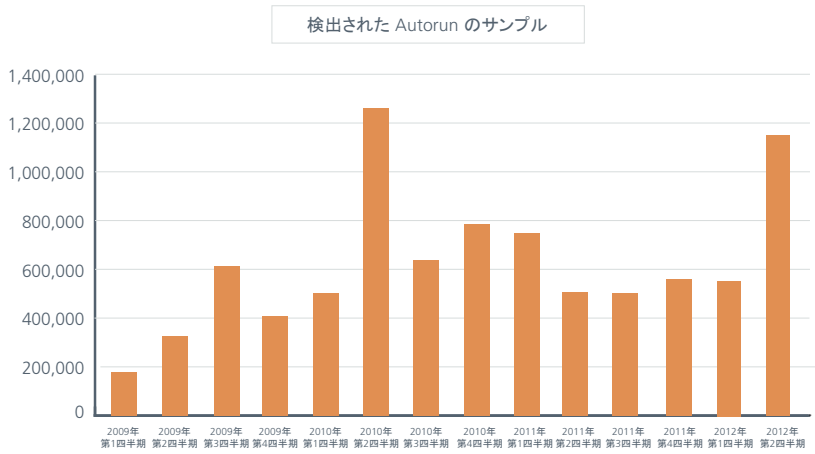


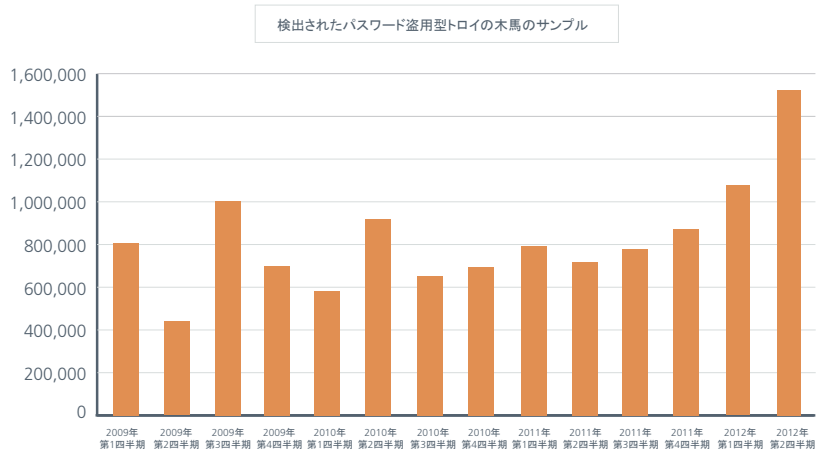
検出された ZeroAccess のサンプル



偽の AV（不正なセキュリティ ソフトウェア）、AutoRun、パスワード盗用型トロイの木馬は増加傾向を維持しています。 偽の AV はわずかな増加ですが、 AutoRun とパスワード盗用型トロイの木馬は大幅に増加しています。 全体的な傾向としては下降ぎみです。





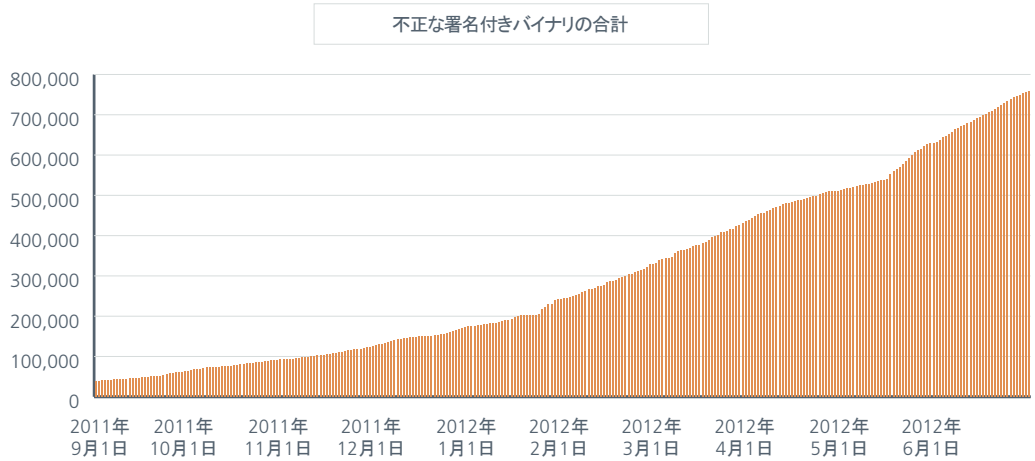


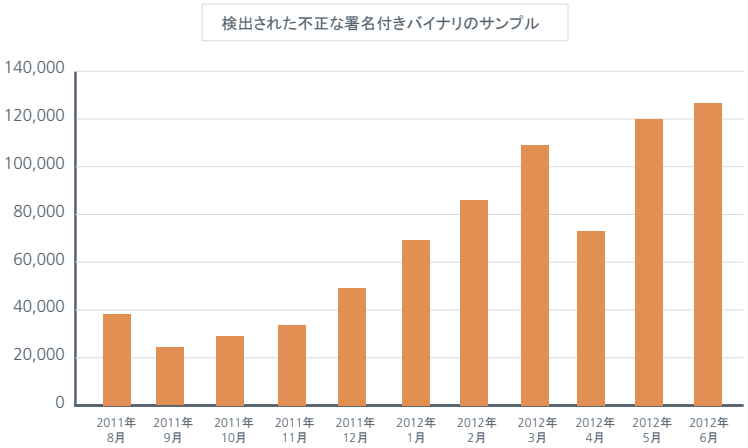
署名付きのマルウェア

McAfee Labs の上級研究員 Craig Schmugar のブログには非常に有益な情報が掲載されています。 そのブログの中に、 マルウェアの作成者がマルウェアにデジタル署名を付ける理由について次のような記述があります。

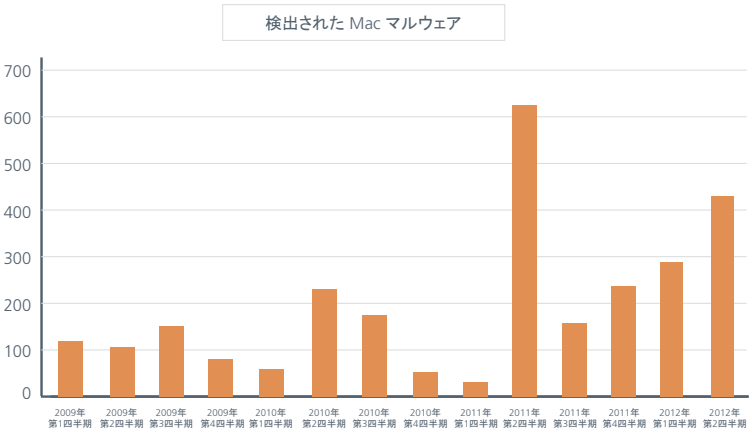
> 「攻撃者がマルウェアに署名を付けるのは、 ユーザーや管理者を騙してファイルを信用させるためだけではない。 セキュリティ ソフトウェアやシステム ポリシーによる検出を回避させる目的もある。 このようなマルウェアの大半は盗まれた証明書で署名されているが、 自己署名またはテスト署名の付いたバイナリも存在する。 テスト署名はソーシャル エンジニアリングでも利用されている。」[1]

この四半期も署名付きのマルウェアの数が増加しました。『2012 年の脅威予測』では、 Duqu や Stuxnet の成功に刺激を受けてこのようなマルウェアが増加すると予想しましたが[2]、 この予測は現実のものとなっています。

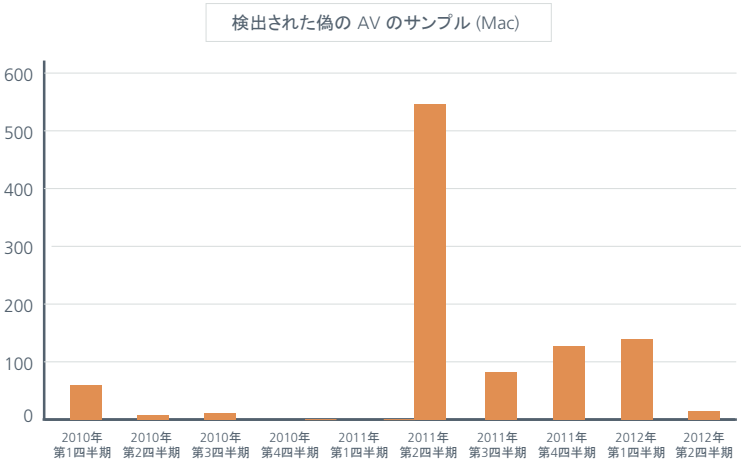




Mac の愛好家も警戒が必要です。 Mac を狙うマルウェアは確実に増えています。 Windows を攻撃するマルウェアに比べると、 数はそれほど多くありませんが、 この脅威は軽視できません。 Mac ユーザーも十分な対策を講じるべきです。マルウェアの作成者はすべてのオペレーティング システムやプラットフォームを攻撃対象と考えています。



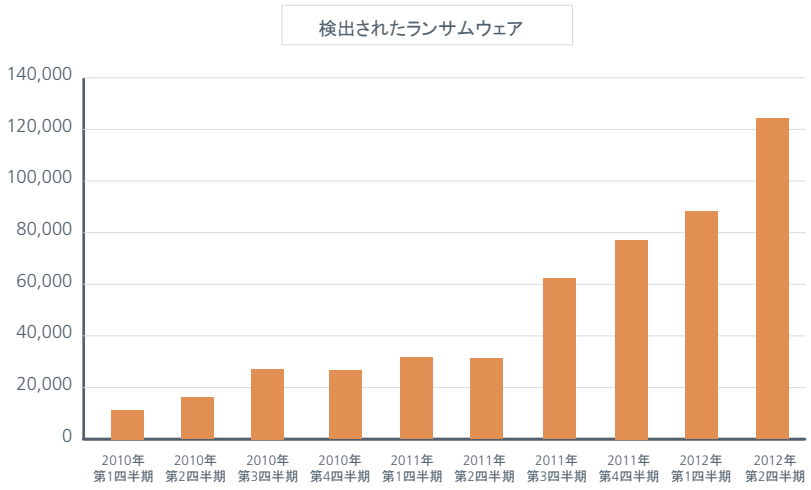
2011 年中頃に急増した Mac 用の偽の AV は急激に減少しています。



データを人質に取るランサムウェア

マルウェアにも流行があります。 サンプルと感染したコンピューター数の総数を見ると、偽のアラート / 偽の AV は 2011 年以降減少しています。 これにはいくつかの原因が考えられます。 当局の取り締まりが強化され、 盗み出したクレジットカードでの決済が難しくなったことも理由の一つでしょう。 しかし、 サイバー犯罪者も手を拱いているわけではありません。 一つのモデルが阻止されても、 別の方法を考え出し、 金銭を盗み出しています。 最近では、 ランサムウェアに関心を持つマルウェア作成者が増えています。

ランサムウェアは被害者のコンピューターやデータを人質に取ります。 このマルウェアは、 データまたはコンピューター全体を暗号化し、 データの復元費用を匿名の決済方法で払うように要求します。 サイバー犯罪者がクレジットカード決済を行う必要はありません。 この手口は目新しいものではありません。 この種のトロイの木馬が最初に出現したのは 1989 年です（PC を攻撃する AIDS-Trojan）。 その後、 このような攻撃は殆ど見られませんでしたが、 最近になって増え始めています。



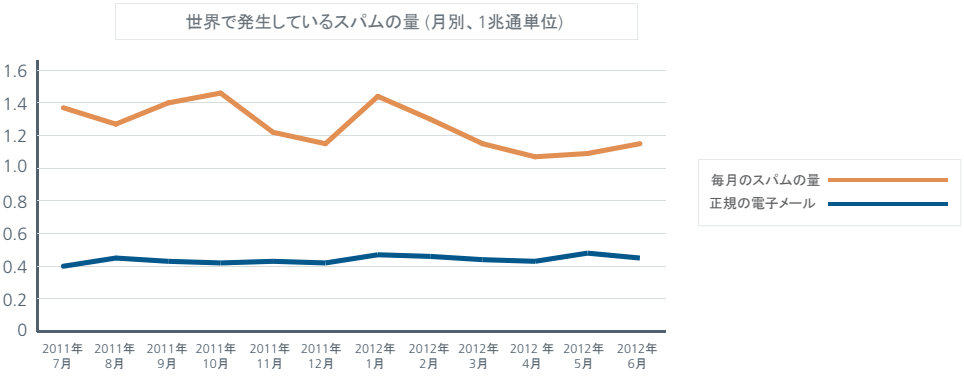
ランサムウェアはここしばらく増加傾向を示しています。 この四半期は過去最高を記録しました。

ランサムウェアは被害がすぐに発生し、 コンピューターが完全に使用不能になるため、 非常に厄介な脅威です。データが破壊されるだけでなく、脅迫に応じて身代金を渡せば金銭的な被害も発生します。一般ユーザーであれば個人的な被害（何年分かのデータ、 写真、 思い出の喪失）に止まりますが、 企業が狙われた場合、 社内ネットワークで被害者が書き込み可能なデータがすべて暗号化されるため、 被害は甚大なものとなるでしょう。

有効な対策はあるのでしょうか。 メールに添付されたファイルやリンク、 Web サイト上のリンクを安易に開かないこと、 また、 システムを定期的にバックアップすることが肝要です。 企業の管理者はセキュリティ製品のアクセス保護ルールで感染を防ぐことを検討するべきです。

メッセージングの脅威

スパム メールの量は 2011 年 10 月と 2012 年 1 月に一時的に増加しましたが、 全般的に下降線をたどっています。 この四半期はわずかに増加しましたが、 下降傾向にあることは変わりません。 国別の状況を見ると横ばい、 または減少が殆どです。 例外はコロンビア、 日本、 韓国、 ベネズエラで、 スパムの量が 10% 増加しています。しかし安心はできません。 スパムはまだ危険な存在です。 特に、 最近では標的型のスピア フィッシング詐欺が増えています。

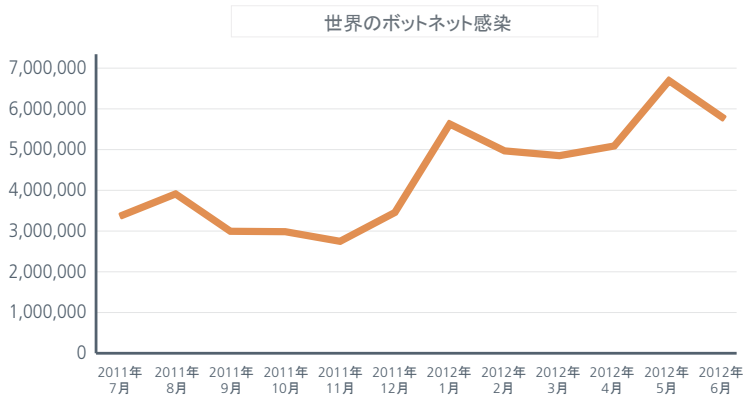

世界で発生しているスパムの量 (月別、1兆通単位)
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0
2011年 7月
2011年 8月
2011年 9月
2011年 10月
2011年 11月
2011年 12月
2012年 1月
2012年 2月
2012年 3月
2012 年 4月
2012年 5月
2012年 6月
毎月のスパムの量
正規の電子メール


スパムの量
アルゼンチン
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
オーストラリア
400,000
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
ブラジル
45,000,000
40,000,000
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
1,000,000
500,000
0
中国
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
コロンビア
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
ドイツ
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

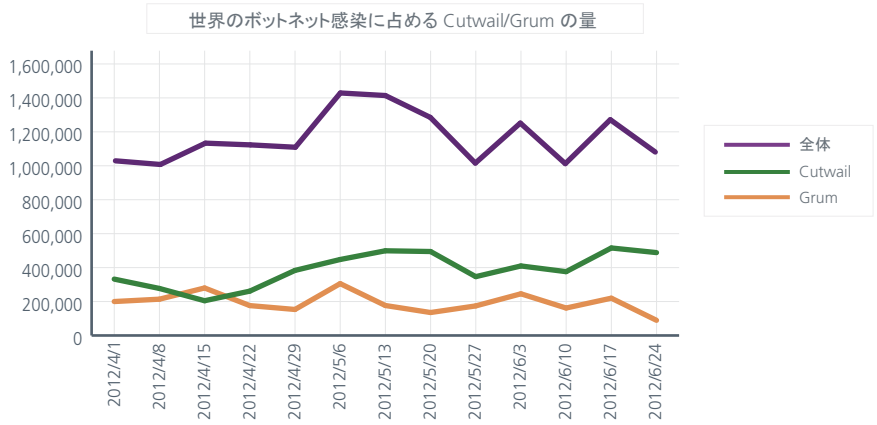

スパムの量
インド
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
インドネシア
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
イタリア
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
日本
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
ロシア
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000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

ボットネットの詳細

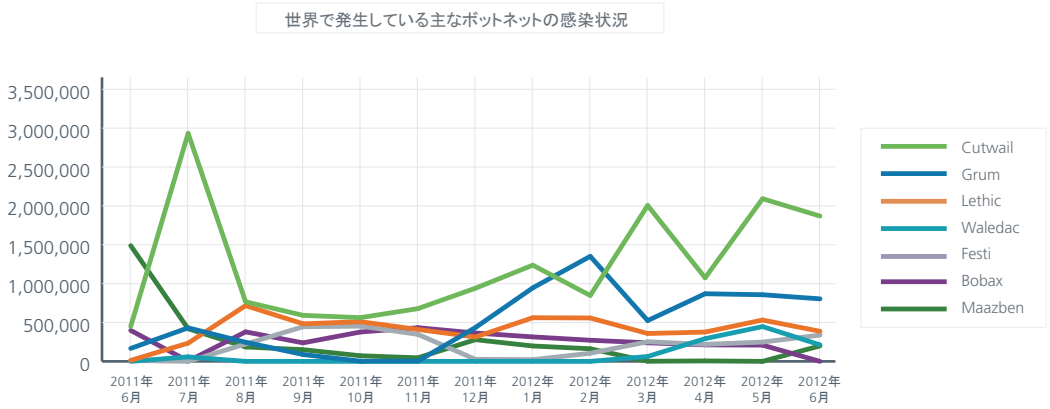
メッセージを送信するボットネットは、 前の四半期では横ばい状態でしたが、 この四半期は増加し、 過去 12 か月で最高となりました。世界で発生したスパムの量もほぼ同時期に急増しています。これはスパムの送信にボットネットの利用が一般的になっていることを意味します。 スパムの送信を行うため、 ボットネットの活動も活発化するでしょう。



この四半期に発生したスパムの殆どは Cutwail と Grum ボットネットによるものです。



メッセージを送信するボットネットの順位を見ると、 前の四半期と殆ど変化はありません。 Cutwail が引き続きトップで、 Grum と Lethic がそれぞれ 2 位と 3 位を維持しています。

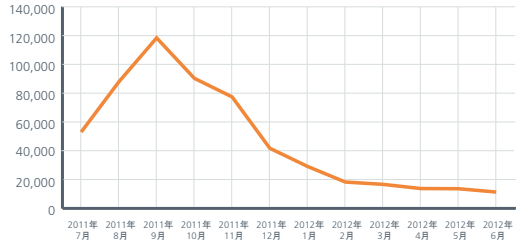


同種の他のボットネットは横ばい状態か、 減少傾向です。 6 月には Bobax が消滅し、 Maazben が再び活動を始めています。

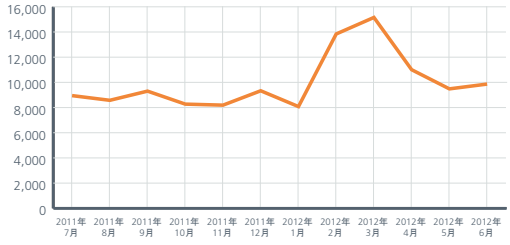
中国、 インド、 韓国、 米国では、 新しいボットネット送信者の数が 10% 以上増加しました。 特に韓国では 50% も増加しています。

検出されたボットネットの送信者(国別)

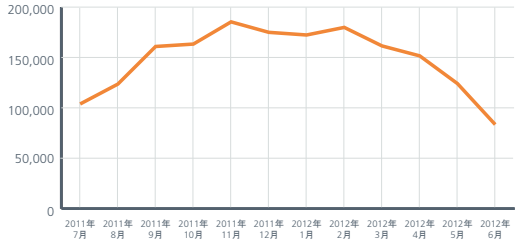
インドネシア



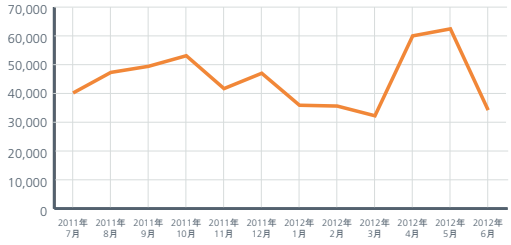
日本



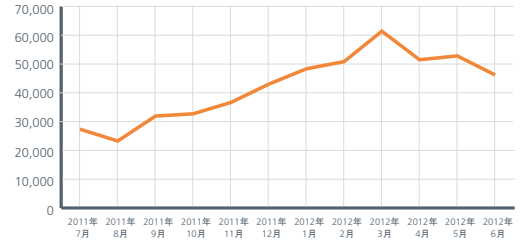
ロシア



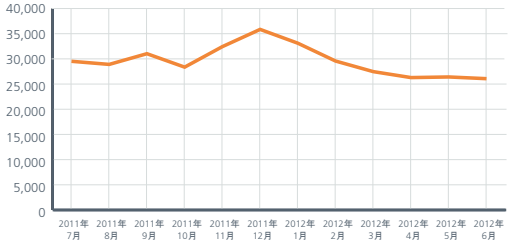
韓国



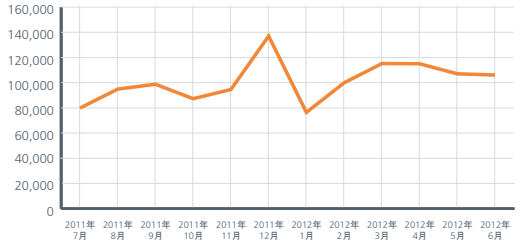
スペイン



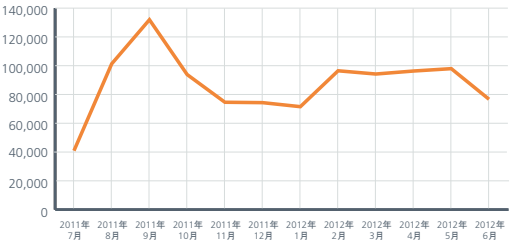
英国



米国



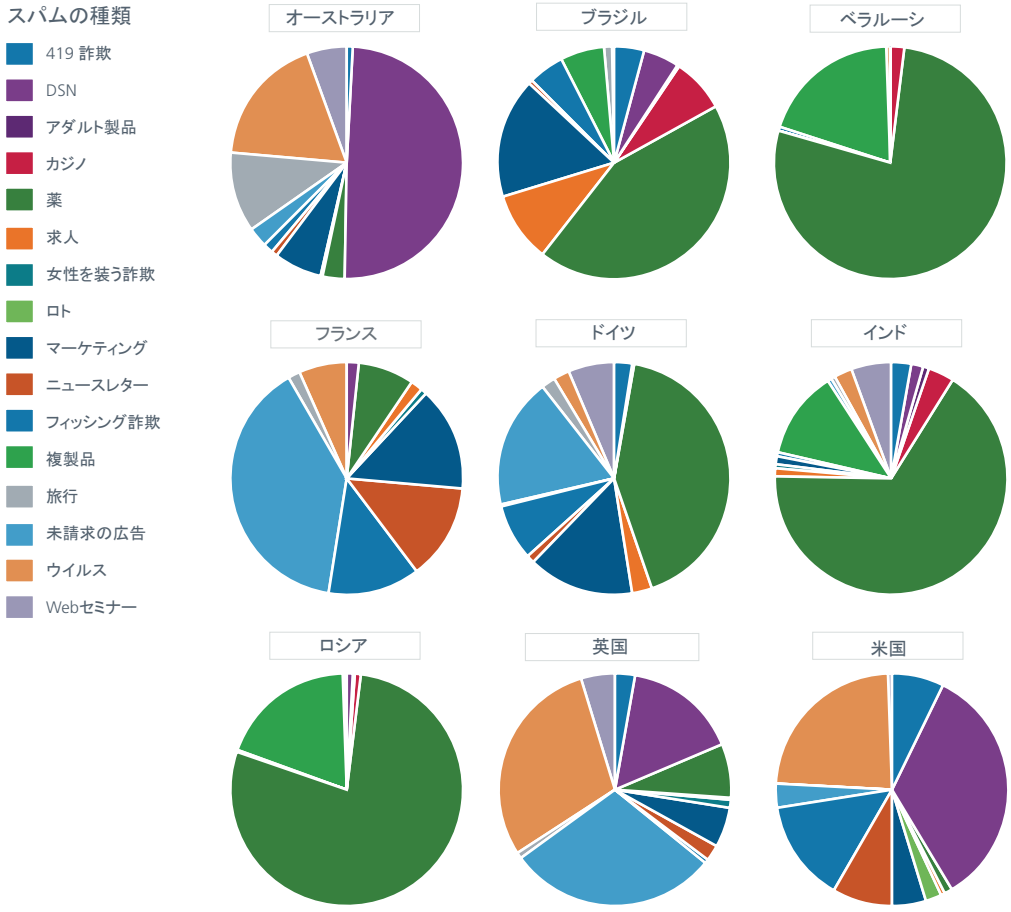
ベネズエラ



新しい感染数が減少していても、 現在の脅威がなくなったわけではありません。 国別にボットネットの詳細を見ると、 多くのボットネットが世界中で活発に活動しています。 Cutwail は、 新たな感染数だけでなく、 インド、 パキスタン、 ベネズエラを除く各国で最も蔓延しているボットネットになっています（この 3 つの国では Grum がトップです）。

ソーシャル エンジニアリングを駆使するスパム

スパムの件名は国や地域によって大きく異なります。 スパム送信者は、国、文化、宗教などによってソーシャル エンジニアリングの効果が異なることを熟知しています。 世界で最も多いスパムの種類は配信状況通知（DSN）で、ドラッグ関連のものもよく使われています。



ネットワークの脅威

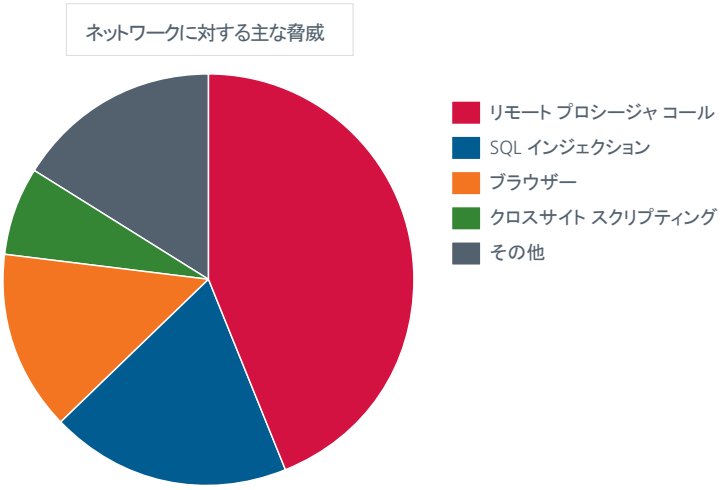
前回のレポートでも報告したように、 マカフィーではネットワーク ベースの分析に力を入れています。 このデータを分析すると分かりますが、 攻撃元とその関係者を特定するのは簡単な作業ではありません。 「この攻撃の発生源はどこか」、「この攻撃の首謀者は誰か」という質問に対して正確に答えるのは至難の業です。 コードを解析しても作成者までは特定できないことが殆どです。 ネットワーク攻撃の分析も同様です。 分析は順調に進んでいますが、 攻撃者を特定する段階には至っていません。 コードの振る舞いや攻撃内容、 攻撃元と思われる場所については情報を提供できても、 それ以上のことを明言することはできません。 オスカー ワイルドの作品に次のような一節があります。

> あらゆる芸術は表面であるとともにまた象徴でもあるのだ。
> 表面の下をさぐろうとするものは危険を覚悟すべきである。
> 象徴を読みとろうとするものもまた危険を覚悟すべきである。
> 芸術が真に映しだすのは人生を観る者であって、人生ではない。
> ある芸術作品に関する意見の相違はその作品が斬新で、 複雑で、 生命力に満ちていることを示すものである。
> ―『ドリアン・グレイの画像』岩波文庫 西村孝次訳

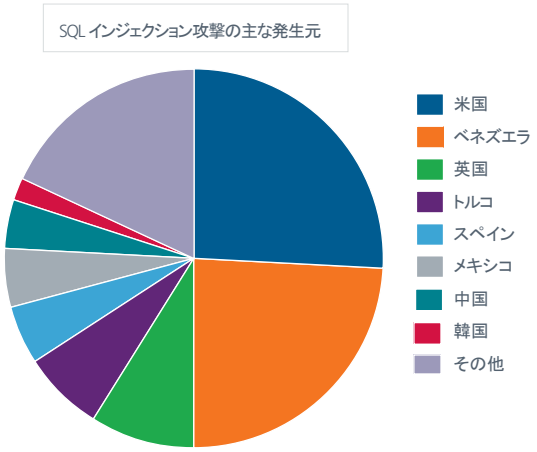
セキュリティの世界でも帰属について様々な意見があります。 大半はアナリストの先入観を反映していますが、この多様性自体が、帰属の調査がまだ始まったばかりであることを表しています。 データを分析しても、表面的なことしか言えない場合もあります。

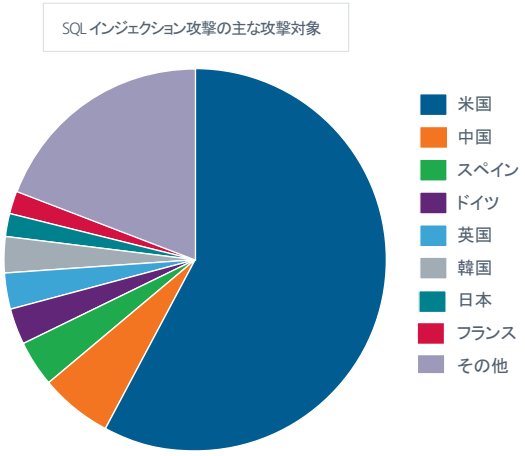
最も多くのサイバー攻撃が発生し、攻撃を受けているのが米国です。 McAfee Global Threat Intelligence™ ネットワークの収集・分析結果に基づいて、 いくつかの攻撃について詳しく見てみましょう。

種類別に見ると、上位の脅威は前の四半期と同じですが、円グラフのスライスの大きさは異なります。 今回はリモート プロシージャ コールの数が増えています。 これに伴って他の攻撃のスライスは小さくなっていますが、 順位に変動はありません。

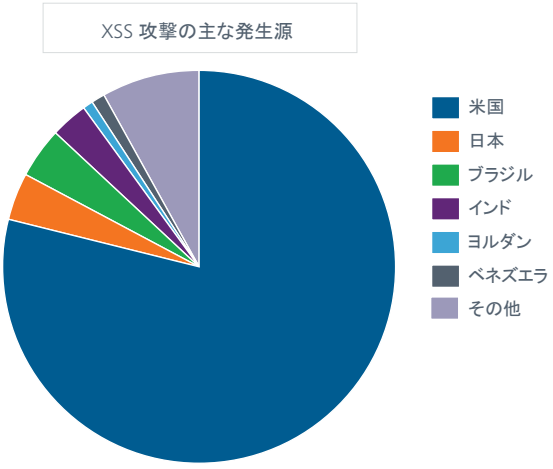


攻撃者の数が最も多かったのは米国ですが、 2 位のベネズエラとあまり差はありません。 攻撃の被害者数をみると、 米国が他を大きく引き離しています。

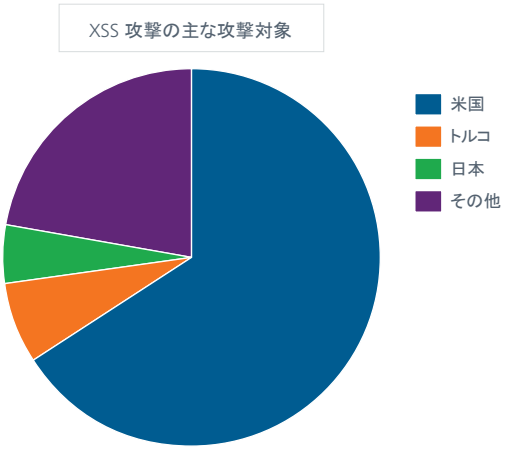




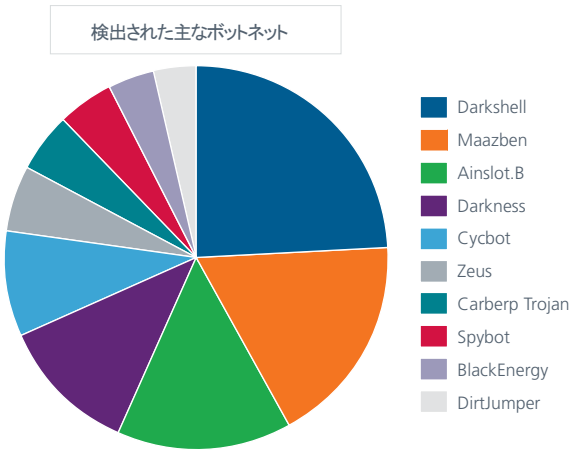
クロスサイト スクリプティング（XSS）攻撃の発生元では、 前の四半期と同様に米国が圧倒的に多く、2 位以下とかなり差が付いています。



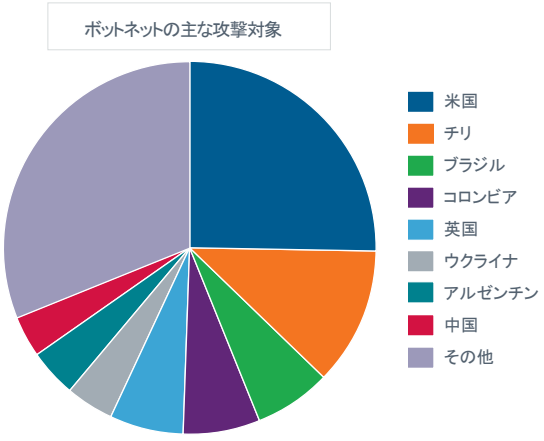
XSS の攻撃対象でも米国が 1 位ですが、 2 位にトルコが入っています。トップとの開きはかなりあります。



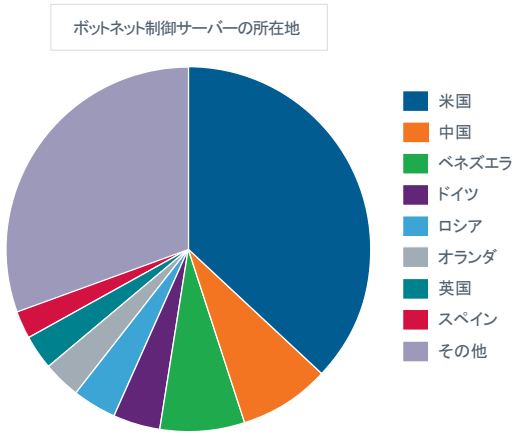
前の四半期は Mariposa と Pushdo（Cutwail）が上位を占めていましたが、この四半期は Darkshell と Maazben が 1 位と 2 位になっています。



攻撃対象を見ると、トップがベネズエラから米国に代わり、 中国が 2 位に入っていますが、 感染数は約半分です。



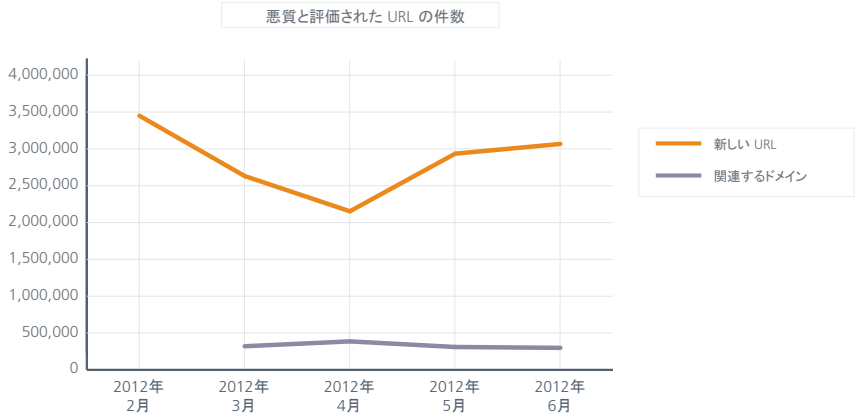
ボットネット制御サーバーが存在する国では、 引き続き米国がトップですが、 サーバーの数は 10% 減少しています。 米国に次いで多い国は中国とベネズエラです。



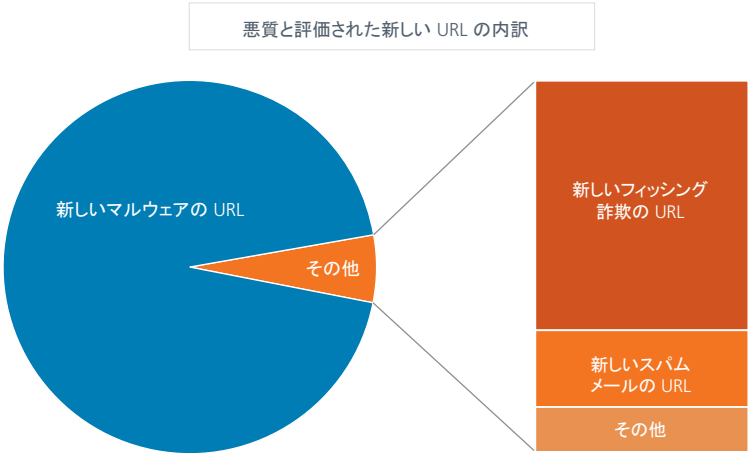
Web 脅威

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、 振る舞い自体の怪しいサイトもあります。 サイトの評価には、 いくつかの要因が考慮されます。

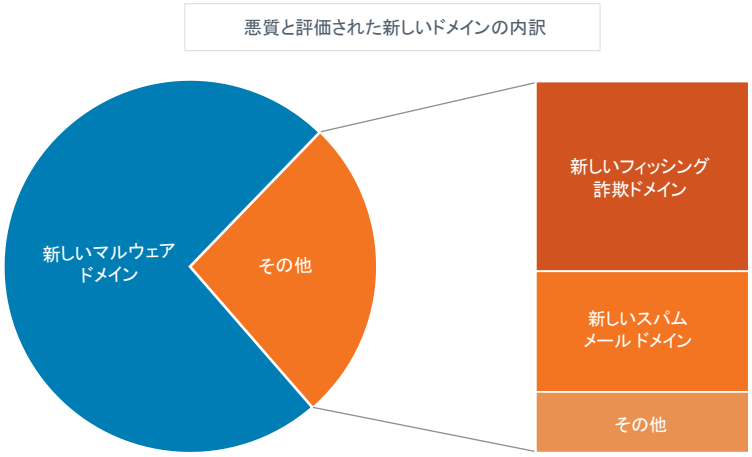
マカフィーのラボで 6 月末までに確認した悪質な URL の合計数は 3,600 万を超えました。 これは 2,260 万個のドメイン名に相当します。 この四半期に確認した悪質な URL は毎月平均で 270 万件になります。 6 月に新たに確認した URL は約 300,000 の悪質なドメインに関係していました。 1 日当たりで約 10,000 件で、 この数は前の四半期よりも若干増加しています。 ちなみに、 Google が 6 月にブログで発表した悪質なサイトの数は 9,500 でした [3]。

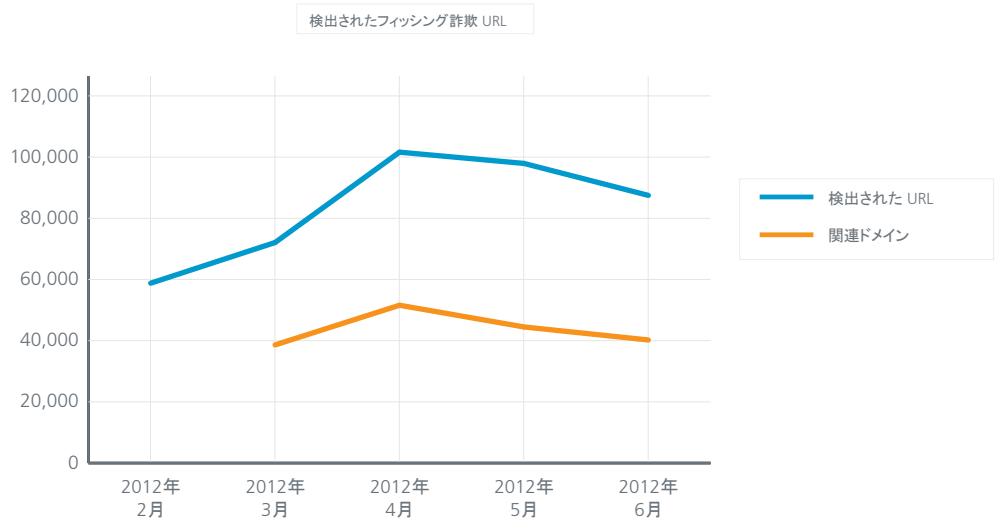


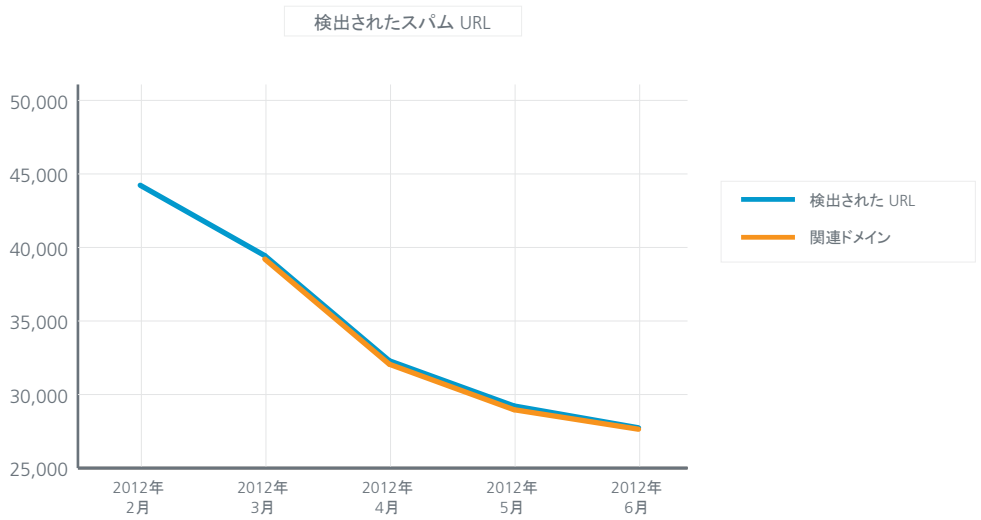
これらの URL の大半（94.2%）には、マルウェア、エクスプロイト、コンピューターの乗っ取りに使用するコードが存在しています。 フィッシング詐欺とスパムの URL はそれぞれ 4%、 1% です。



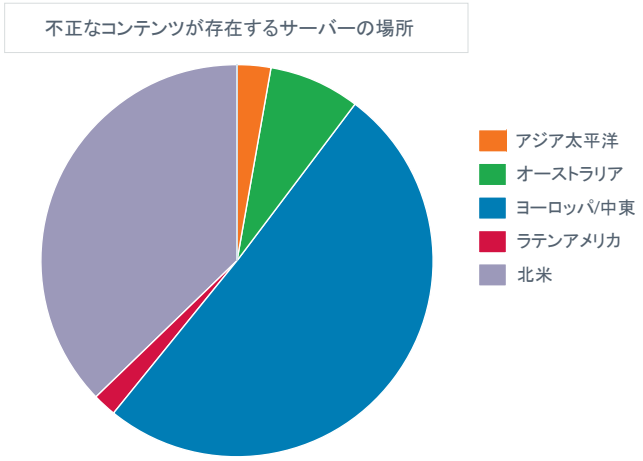
ドメインの分布も若干異なります。







この四半期は不正なサーバーの所在地に変動がありました。 前の四半期は不正なサーバーの 92% が北米にありましたが、この四半期はヨーロッパ / 中東がトップになっています。 各地域を詳しくみると、さらに変化が見られます。 この四半期に最も多くの不正コンテンツが見つかったのはオランダでした。



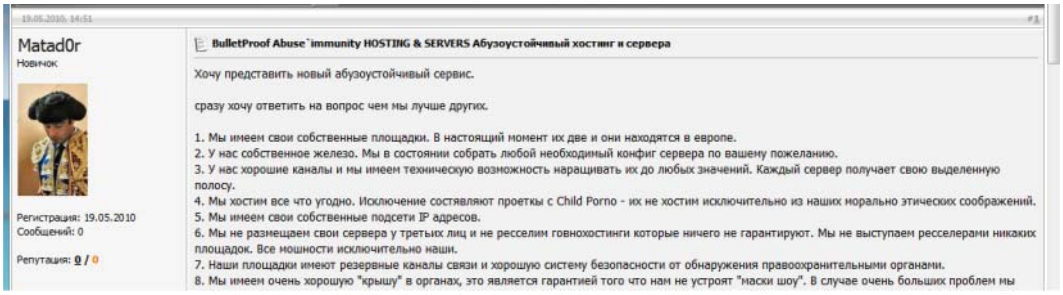

不正なコンテンツが存在するサーバーの場所
アフリカ
南アフリカ
セネガル
セイシェル
チュニジア
その他
アジア太平洋
韓国
日本
中国
香港
インドネシア
その他
オーストラリア/ニュージーランド
オーストラリア
ニュージーランド
ヨーロッパ/中東
オランダ
スイス
ドイツ
英国
イタリア
その他
ラテンアメリカ
バハマ
英領バージン諸島
ブラジル
その他
北米
米国
カナダ

サイバー犯罪

防弾ホスティング

この四半期も引き続き「サービスとしてのクライムウェア」について調査を行いました。 今回は、防弾ホスティングについて詳しく見てみましょう。 前回報告したように、 米財務省検察局が実施した「Open Market」作戦で犯罪集団 Carder.su のメンバーや関係者など 50 人が摘発されました。

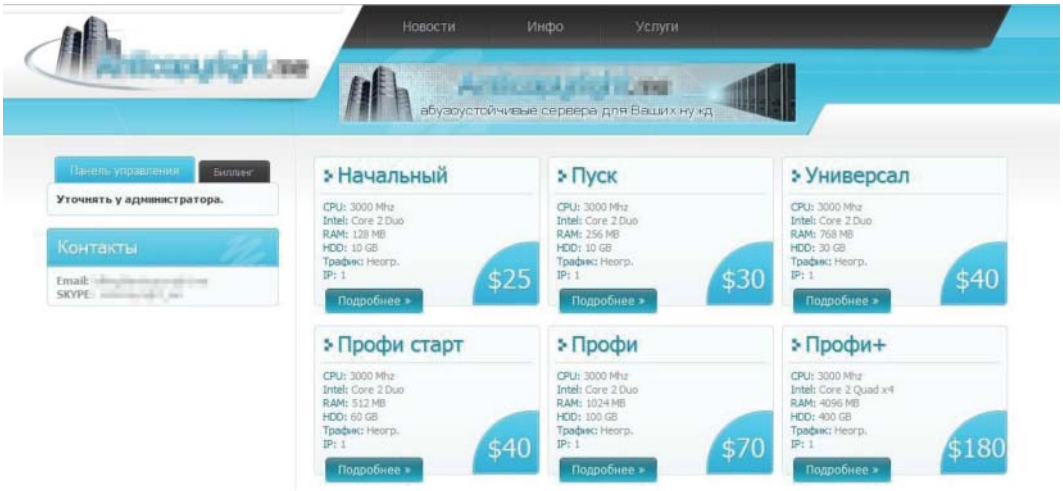
この容疑者の中で Dorbik や Matad0r は防弾ホスティング サービスを提供していました。 2010 年に行われた専門家向けのいくつかのフォーラムで、 そのサービスの内容が紹介されています。



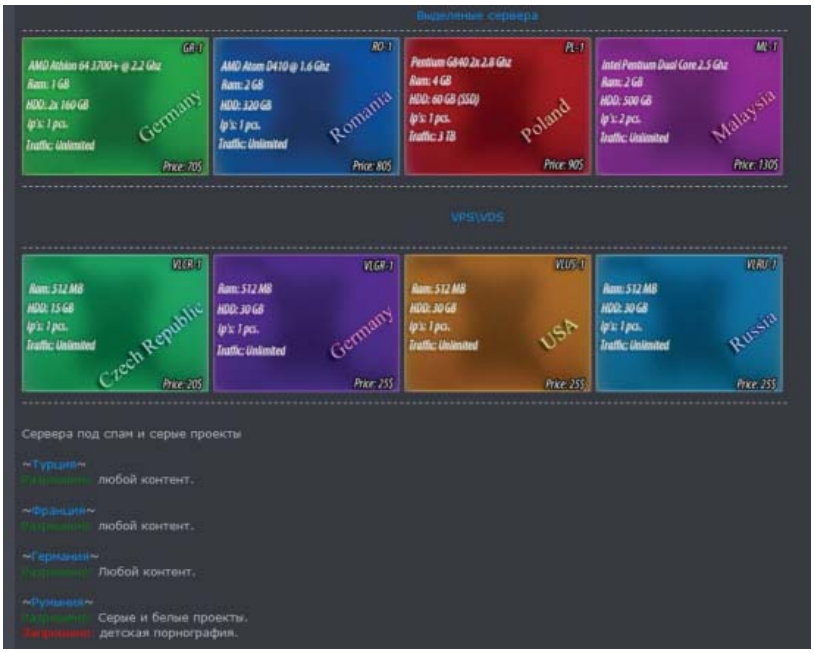
Matad0r の料金表 :

ホスティング	プライベートまたは専用の仮想サーバー	専用サーバー
• サーバー上に 2GB の領域 • 最大 10 個までのパークドメイン • 専用の DNS サーバー • ホスティングのコントロールパネル • トラフィック無制限 • 必要なモジュールとソフトウェアを無料で提供 • 月額 $ 50	• VMware 技術 • root 権限でのサーバーに対するフルアクセス • 最大 25% までの Xeon CPU • RAM: 1GB ～ • ストレージ : 30GB ～ • トラフィック無制限 • セットアップ / 再セットアップは無料 • 完全なソフトウェアセット • IP アドレスの追加（必要な場合） • 月額 $ 150	• 複数の構成 • 24 時間でのセットアップ • トラフィック無制限 • セットアップ / 再セットアップは無料 • 任意の OS を無料で提供（Windows を含む） • IP アドレスの追加（必要な場合） • 月額 $ 400

現在、 インターネット上に類似したサービスが数多く見られます。 また、 このようなサービスの利用者も確実に存在します。 ロシア語のサービスの例をいくつか紹介しましょう。



次のサービスは、専用サーバー（上）とプライベート / 専用の仮想サーバーを特別価格で提供しています。



ロシア語の内容は次のとおりです。

スパムとグレーハット

~ トルコ ~
許可 : 任意のコンテンツ

~ フランス ~
許可 : 任意のコンテンツ

~ ドイツ ~
許可 : 任意のコンテンツ

~ ルーマニア ~
許可 : グレーハットとホワイトハット。 禁止 : 児童ポルノ

このショップがリンクしているサイトを見ると、さらに別のサービスを提供していました。たとえば、フランスの顧客向けには次のようなメニューが用意されています。

このスクリーンショットには決済方法も表示されています。

サイバー犯罪に対する取締り

この四半期は、警察による取り締まりが成功裏に行われました。

- 匿名の Tor ネットワーク経由でのみアクセス可能なサイトで麻薬を販売していたとして、米国などで 8 人の容疑者が逮捕されました。この容疑者は The Farmer's Market というサイトを運営し、LSD、エクスタシー、マリファナなどの薬物を販売していました。2007 年 1 月から 2009 年 10 月までに約 5,256 件のオンライン注文を処理し、34 か国に 3,000 人ほどの顧客を抱え、100 万ドル以上の利益を上げていました [4]。2010 年に Tor に移行する前は、暗号化されたメールサービスである Hushmail で注文に対応していました。
- 4 月 26 日、英国重大組織犯罪庁（SOCA）が FBI、米司法省との合同捜査の完了を発表しました。この捜査では、盗まれたクレジットカードやオンラインバンキングのアカウント情報を扱う 36 の犯罪サイトが摘発の対象になりました [5]。これらのサイトでは、盗み出した大量のデータを迅速に販売するため AVC（Automated Vending Carts）という電子商取引用のプラットフォームが使用されていました。
- 5 月 3 日、米ニュージャージー州の弁護士が、2011 年 12 月に逮捕された 7 人の容疑者がインターネット詐欺グループへの関与を認めたと発表しました。この詐欺グループは、フィッシング詐欺を実行してインターネット ユーザーからアカウント情報を収集し、130 万ドル以上の金を盗み出しています。「運び屋」の写真を付けて運転免許証を偽造し、被害者になりすまして口座から金を引き出していました [6]。

- 5 月には、カナダ・ケベック州の警察が英国、ニュージーランド、マレーシア、チュニジアで活動中の国際的な詐欺グループのメンバーを 45 人逮捕し、12,000 枚以上の偽造キャッシュカードを押収しました。当局によると、この詐欺グループはキャッシュカードの所有者に気付かれずに 1 億ドルに上る金銭の引き出しに成功しています。手口としては、ATM 機の取り扱いに慣れた詐欺師が暗証番号を盗み出したり、店舗の端末に侵入し、偽造カードを使って口座引き出しを行いました。また、Bluetooth 経由で会社やレストランの POS 端末に侵入し、端末内のクレジットカードやデビットカードの情報を盗み出したケースもあります [7]。
- 6 月、ロシアの捜査当局が Carberp の別のグループを摘発しました。このグループは、以前使用したマルウェアの名前から The Hodprot とも呼ばれていましたが、4 年以上も活動を継続し、銀行口座を狙うマルウェアを使用してオンライン バンキングの口座から金を盗み出していました。このグループによるオンライン バンキングの被害額は 1 億 2,500 万ルーブル（約 370 万ドル）に上ります [8]。
- 英国の SOCA は、t0pp8uzz、GM というハンドル ネームを使用していた 2 人の詐欺師に対する禁固刑の判決を発表しました。この詐欺師達は詐欺サイトを運営し、2,690 万ポンド（4,100 万ドルまたは 3,320 万ユーロ）も稼いでいました。2011 年に逮捕されるまでは、Freshshop というサイトを運営し、盗み出した口座情報を転売していました [9]。
- 米連邦当局は、ネット上における盗難クレジットカードの売買を取り締まるため、過去最大規模のおとり捜査を行い、米国で 24 人、その他の国で 12 人を逮捕しました。2010 年 6 月、FBI が捜査員がカード情報の売買を監視するために Carder Profit というフォーラムを立ち上げました。FBI はこのフォーラムで 411,000 枚の架空のカード情報を流しました。この分量の情報が実際に悪用された場合、2 億 500 万ドルもの被害額になります [10]。この捜査で、Twitter と Google に攻撃を行ったと主張する UGNazi グループのリーダーも逮捕されました。

ハクティビズム

この四半期はハクティビストが数名逮捕されています。

- 4 月、Anonymous に関係する CabinCr3w グループのメンバーが逮捕されました。逮捕されたのは Kahuna と w0rmer で、容疑は 2 月に発生した警察関連の Web サイトに対するハッキングへの関与です [11]。
- ハクティビストの集団であり、サイバー軍の性格も持つ TeaMp0isoN グループが再び注目を集めました。4 月 11 日、このグループは英国の諜報機関 MI6 に電話を使ったサービス拒否（DoS）攻撃を仕掛けました。この攻撃を 24 時間継続した後、グループのリーダーと見られる TriCk がロンドンの MI6 の本部に電話をかけ、犯行声明を行いました。犯行の動機は、英国に関係するテロの容疑者を米国に引き渡すことを認めた欧州人権裁判所の決定に対する抗議だとしています [12]。この声明の 2 日後、TriCk（17 歳）はロンドン警視庁に逮捕されました [13]。この逮捕がグループの崩壊につながったようです。5 月までに TeaMp0isoN のメンバーである MLT（17 歳）と Phantom（28 歳）がそれぞれ英国とロシアで逮捕されました。
- メディアでは大きく報じられませんでしたが、6 月にはフランス、ベルギー、ケベックで Anonymous のメンバーが逮捕されています。

Anonymous の動きにも変化が見られます。多くの作戦を行っていますが、ごく小数の例外を除けば、その影響力は低下しているようです。しかし、活動を停止したと見るのは早計でしょう。この四半期の Anonymous の主な活動を見てみましょう。

- 4 月、Anonymous は Defense 作戦の中で、Cyber Intelligence Sharing and Protection Act を支持した政府関係者と業界関係者に DDoS 攻撃を実行しました [14]。

- 5 月、 Anonymous はカナダで 78 号法案が成立したことに抗議し、 Québec 作戦を実行しました。 この法律は学生の抗議活動を制限するものです [15]。 この作戦で、 モントリオールの F1 レースのサイトをハッキングし、 チケットを購入した個人の名前、 電話番号、 メール アドレスを公開しました。 また、 ケベックの政府機関や警察関連の Web サイト（公共安全省、自由党、検視官の事務所、警察倫理委員会など）を攻撃しました。
- 6 月、 Anonymous は強化される政府のインターネット検閲に抗議し、 #OpIndia を実行しました。 特に、 Torrentz や Vimeo などのサイトの閉鎖命令に強く抗議しています。 6 月 9 日、 Anonymous の訴えに共感したインドの活動家がインドの複数の都市で抗議デモを行いました。 参加者は少なかったものの、 Anonymous の仮面を被った若い活動家がムンバイ、 プネ、 バンガロールなどの 16 の都市で抗議活動を行いました。 Anonymous は cert-in.org.in や india.gov.in のサイトにも攻撃を行い、 機能停止に追い込んでいます [16]。
- 日本では、 著作権法が改正され、 DVD やブルーレイ ディスクなどの海賊版のダウンロードに対する罰則が強化されました。 これに抗議し、 #OpJapan タグで日本のサイトに対する攻撃を呼びかけました [17]。

Anonymous は、引き続き警察関連のサイトを標的にしています。

- 4 月、F**K FBI Friday で Anonymous のハッカーが Lake County、フロリダ州、郡保安官事務所のサイトを攻撃しました。 また、 International Police Association のサイトを改ざんしました [18]。
- ケベックでは、Anonymous の支持者が SPVM（モントリオール警察）のサイトから数千人分のユーザー名、氏名、メール アドレス、住所などの個人情報を盗み出し、公開しました [19]。 opQuebec では、モントリオール警察職員信用組合のサイトも攻撃し、 ウェルカム画面を黒いテンプレートで置き換え、 Anonymous のリソースへのリンクを追加しました。 この画面には銀行の顧客と従業員と見られる名前とメール アドレスも表示されました [20]。

筆者について

本レポートは、 McAfee Labs の Zheng Bu、 Toralv Dirro、 Paula Greve、 Yichong Lin、 David Marcus、 François Paget、 Vadim Pogulievsky、 Craig Schmugar、 Jimmy Shah、 Dan Sommer、 Peter Szor、 Adam Wosotowsky が準備し、 作成しました。

McAfee Labs について

McAfee Labs は、 世界各地に存在する McAfee の研究機関で、 マルウェア、 Web、 電子メール、 ネットワークなどに対する脅威を研究・調査し、 脆弱性の報告を行っています。 McAfee Labs は、 世界各地に数百万台のセンサーを配備し、 クラウド型サービスの McAfee Global Threat Intelligence™により情報収集を行っています。 世界 30 か国に存在する McAfee Labs には、 様々な分野を専門とする 350 名の研究者が在籍し、 企業や一般のユーザーを保護するため、 リアルタイムの脅威検出、 アプリケーションの脆弱性特定、 リスクの相関分析、 迅速な問題解決に努めています。

マカフィーについて

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

[1] http://blogs.mcafee.com/mcafee-labs/signed-malware-you-can-runbut-you-cant-hide
[2] http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf
[3] http://googleonlinesecurity.blogspot.co.uk/2012/06/safe-browsing-protecting-web-users-for.html
[4] http://www.wired.com/threatlevel/2012/04/online-drug-market-takedown/
[5] http://www.soca.gov.uk/news/446-web-domains-seized-in-international-operation-to-target-online-fraudsters
[6] http://www.ahherald.com/newsbrief-mainmenu-2/law-and-order/13094-man-admits-role-in-13-million-phishing-fraud-scheme
[7] http://www.cbc.ca/news/canada/montreal/story/2012/05/09/international-fraud-ring-montreal.html
[8] http://www.group-ib.com/index.php/7-novosti/633-group-ib-aided-russian-law-enforcement-agents-in-arresting-yet-another-cybercriminal-group%22
[9] http://www.infosecurity-magazine.com/view/26219/soca-announces-jailing-of-two-uk-credit-card-crooks/
[10] http://www.infosecurity-magazine.com/view/26608/fbi-arrests-was-ugnazi-a-target-or-an-instrument/
[11] http://blogs.mcafee.com/mcafee-labs/hacker-leaves-online-trail-loses-anonymity
[12] http://news.softpedia.com/news/TeaMp0isoN-Phone-Bombs-UK-Foreign-Intelligence-Agency-MI6-264125.shtml
[13] http://news.softpedia.com/news/TeaMp0isoN-Confirm-TriCk-s-Arrest-Operation-Retaliation-Starts-264663.shtml
[14] http://www.securityweek.com/anonymous-launches-attacks-against-trade-associations-and-boeing
[15] http://www.msnbc.msn.com/id/47620087/ns/technology_and_science-security/t/anonymous-threatens-montreal-grand-prix-over-anti-protest-law/#.T-r5_8XnNhw
[16] http://globalvoicesonline.org/2012/06/09/india-netizens-respond-to-anonymous-indias-protests/
[17] http://securityaffairs.co/wordpress/6829/hacking/opjapan-anonymous-against-japan-and-its-war-to-piracy.html
[18] http://news.softpedia.com/news/AntiSec-Hackers-Leak-40-GB-of-Data-from-Lake-County-Sheriff-s-Office-266784.shtml
[19] http://www.cyberwarnews.info/2012/06/02/canadian-police-server-hacked-lots-of-personal-information-leaked-by-anonymous/
[20] http://www.canada.com/health/Police+credit+union+site+hacked+Anonymous/6765994/story.html

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

48400rpt_quarterly-threat-q2_0812_fnl_ETMG