

RSA オンライン不正状況レポート

2009 年 6 月



RSA® AFCC (オンライン不正対策指令センター) マンスリー・インテリジェンス・レポート

オンライン詐欺は絶えず進化し、詐欺の実行者は組織も個人も無差別で攻撃しています。フィッシング、ファームング、トロイの木馬攻撃をはじめとしたオンライン攻撃は、世界中で急増している最も高度かつ組織的で革新的な技術犯罪です。詐欺の実行者は、アイデンティティ、クリデンシャル、その他の効率的に換金できる情報を盗み出そうと、昼夜を問わず休みなく活動し、あらゆる分野のオンライン・ビジネスを狙うだけでなく、職場や家庭で E コマース、ソーシャル・ネットワーク、E メールなどにインターネットを利用する個人をも標的にしています。

オンライン犯罪者は新しいツールを自在に使いこなし、高度なクラ임ウェアを用いて従来にも増して素早く適応する力を備え、ステルス・メカニズムを利用した急速な展開をみせています。またそのサプライ・チェーンは合法的ビジネスに匹敵する進化をとげ、RSA が「Fraud-as-a-Service」と名付けたものも提供できるようになっています。

このマンスリー・インテリジェンス・レポートは、RSA Anti-Fraud Command Center (AFCC: オンライン不正対策指令センター) の経験豊富な詐欺分析専門家チームが作成しているレポートです。RSA フィッシング・レポジトリのオンライン詐欺に関する統計値を示し、分析を加えていきます。

AFCC (RSA Anti-Fraud Command Center: オンライン不正対策指令センター) について

RSA AFCC は、世界 140 カ国以上でフィッシング、ファームング、トロイの木馬の攻撃を検知、監視、追跡して遮断する、24 時間 365 日稼働の対策センターです。AFCC は 320 を超える機関をオンライン攻撃から保護しており、これまでに 165,000 件以上のフィッシング攻撃を遮断し、新たに出現するオンライン上の脅威に関する、業界の主要な情報ソースを提供する役割を果たしています。

RSA AFCC に常駐する詐欺分析専門家チームは、不正な Web サイトの遮断、対策の展開、広範なフォレンジック分析の実施、オンライン犯罪の阻止、攻撃の事前防止に対して豊富な経験を持ち、オンライン攻撃の平均持続時間を中央値でわずか 5 時間に短縮しています。

RSA AFCC は、世界中の多数のインターネット・サービス・プロバイダーだけでなく、いくつかの CERT や法執行機関とも直接的でオープンなチャネルを確保しています。また、約 200 の言語による多言語翻訳サポートを提供し、グローバルな規模で不正 Web サイトの検出、ブロック、および遮断する機能をさらに強めています。



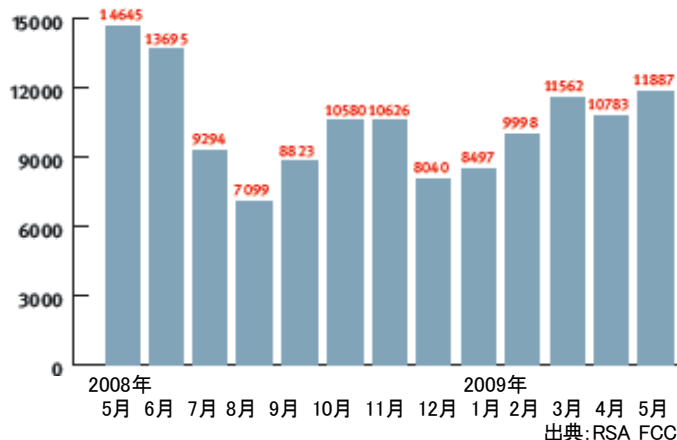
The Security Division of EMC

RSA AFCC が検知したフィッシング攻撃の総数

トレンド分析

2009年5月のフィッシング攻撃の総数は2009年4月に比べて10%増加し(攻撃総数は11,887件)、過去12カ月間の最高を記録しました。「夏にはフィッシング攻撃数が増加する」という年間を通じた傾向を反映したものと思われれます。

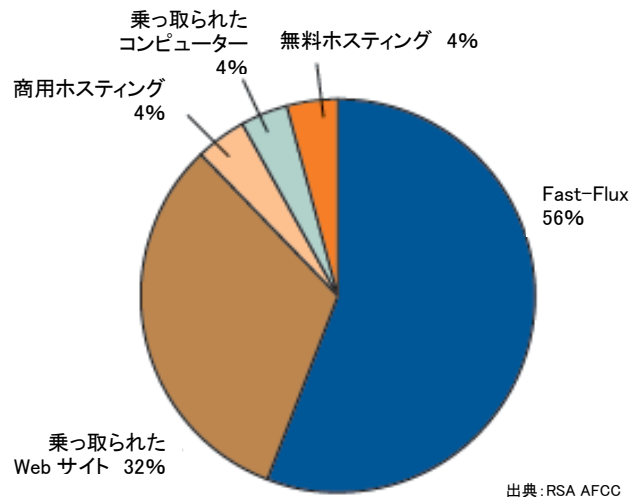
5月は標準的なフィッシング攻撃数が約7%減少した一方で、Fast-Flux 攻撃(ほとんどが Rock Phish 攻撃によるもの)が30%近く増加していました。



ホスティングの手法による攻撃の分類

トレンド分析

2009年5月の Rock Phish 攻撃の多さを考えると、Fast-Flux ネットワークが攻撃のホスティング手法として最も多く使用され続けているのは当然と言えます。Fast-Flux ネットワークでホスティングされた攻撃の割合(56%)は、2009年4月に比べてわずかに増加しました。乗っ取られた Web サイトを使用してホスティングされた攻撃は、2009年4月と同じ割合を保っています(32%)。商用ホスティングと乗っ取られたコンピューターの割合はわずかに減少してそれぞれ4パーセントでしたが、無料ホスティングはわずかに増加し、同様に4パーセントとなりました。



ホスティング手法の説明:

—Fast-Flux ネットワークは高度なサービス拒否(DNS)テクニックで、ボットネットと呼ばれる侵入されたコンピューターのネットワークを利用して、フィッシングやマルウェアのウェブサイトのホスティングと提供を行います。侵入されたコンピューターは、被害者と Web サイトとの間のプロキシ、またはミドルマンの役割を果たします。フィッシングやマルウェアの Web サイトを提供しているコンテンツ・サーバーは、多数の侵入されたマシンの背後に隠れます。それらのマシンのアドレスは検知を逃れるために頻繁に変化するので、Fast-Flux ネットワークを見つけ出し、遮断するのは難しくなります。

- 「乗っ取られた Web サイト」では、詐欺実行者が合法的な Web サイトのサブドメイン上で不法なコンテンツをホスティングすることができるため、フィッシング攻撃に用いる独自のドメインを登録せずに済むことになります。
- 「商用ホスティング」には、料金をとって他の詐欺実行者のために悪意ある Web サイトのホスティングを引き受ける詐欺実行者が含まれています。
- 乗っ取られたコンピューターでは、IP アドレスが特定のフィッシング・ドメインに割り当てられ、侵入を許したコンピューターで構成されます。
- 無料ホスティングは、無料ホスティング・サービスを利用する攻撃です。

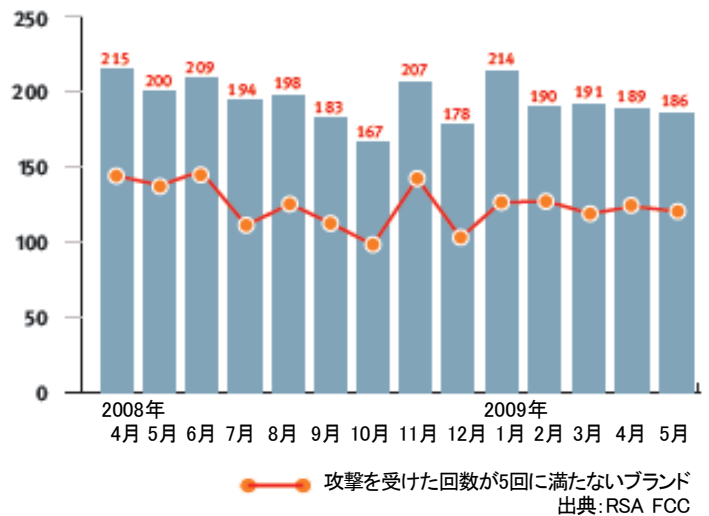


攻撃を受けたブランド総数

トレンド分析

2009年5月にフィッシング攻撃を受けたブランド数は、攻撃数が10%増加したのに対し、2009年4月に比べてわずかに減少しました。通常は攻撃を受けた回数が5回に満たないブランドの割合が60~65%の範囲になりますが、2009年5月は例外的で、攻撃を受けた回数が5回以下のブランドが85%以上にのぼっています。

この統計値から、2009年5月には詐欺実行者らが少数のブランドを集中的に攻撃したことがわかります。初めてターゲットとなったブランド数は2009年4月とほとんど変わらず、2009年5月に初めてフィッシング攻撃を受けたブランドは16でした。



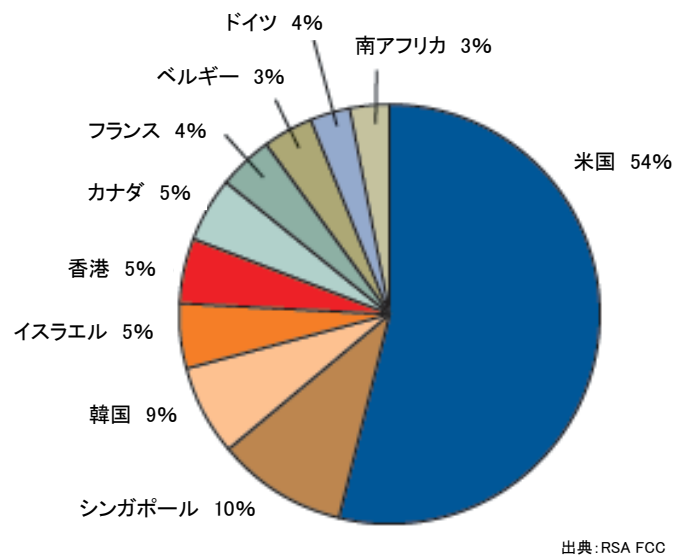
フィッシング攻撃のホスト元となった上位10カ国

トレンド分析

最も多くのフィッシング攻撃をホスティングする国(ISPまたはホスト元となった企業の所在地によります)として常にトップの位置を保ってきた米国は、先月は首位でなかったものの、2009年5月には再び上位10カ国の首位となりました。2009年4月に米国がホスティングした攻撃の割合は全体の32%にすぎませんでしたが、2009年5月には全体の54%へと急増しています。

2009年4月にはスペインが全体の33%で最上位を占めました。2009年5月には激減しており、リストから姿を消しました。2009年5月には実際、フィッシング攻撃をホスティングした割合の高い国の顔ぶれが大きく変化しています。こうした移り変わりがあったのは、米国、シンガポール、韓国、香港、カナダ、イスラエルなどの国でRock Phish集団が登録したドメインが多数にのぼった結果です。

シンガポールは全攻撃の10%をホスティングして、突然2位に登場しています。2009年5月にはノルウェーのほか、南アフリカとオーストラリアが上位10カ国から姿を消しました。リスト初登場のイスラエルは、香港、カナダと共に全体の5%と同率4位となっています。



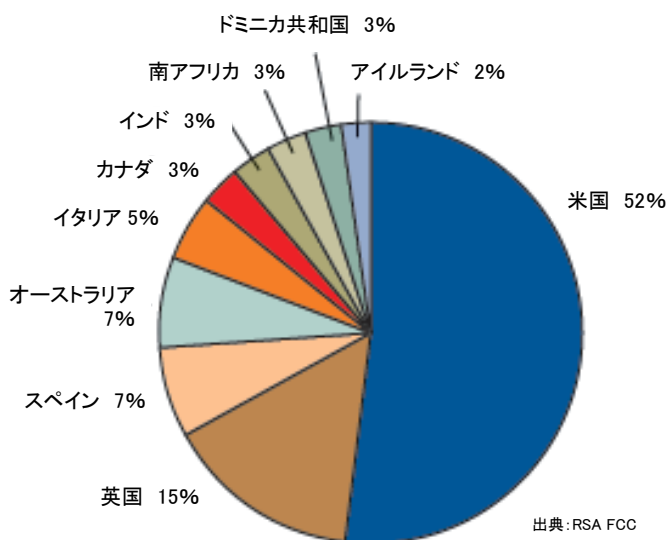


攻撃を受けたブランドが多い上位 10 カ国

トレンド分析

2009 年 5 月に攻撃を受けたブランドが最も多かった国は前月と同じ米国で、全体の 52%を占めました。2 位も依然として英国で、全体の 15%でした。

ドミニカ共和国とアイルランドが 2009 年 5 月に上位 10 カ国に初登場しました。一方で、オランダとブラジルがリストから姿を消しました。スペイン、オーストラリア、イタリア、カナダ、インド、南アフリカのブランドは、2009 年 4 月と変わらない割合で攻撃を受けています。



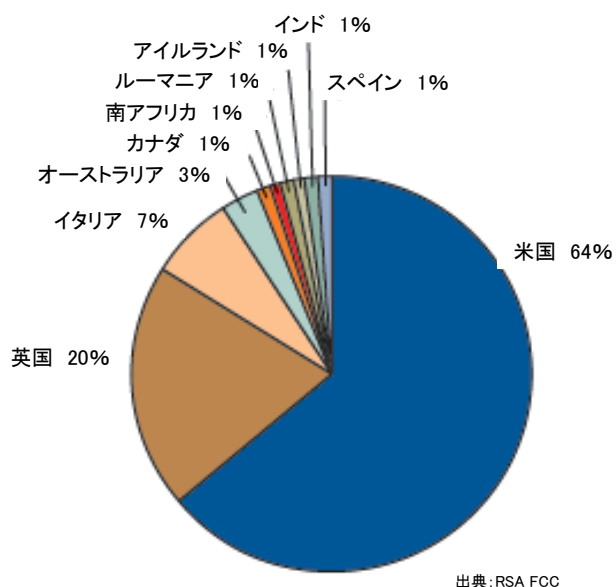
攻撃総数が多い上位 10 カ国

トレンド分析

2009 年 5 月に攻撃総数が多かった上位 3 カ国の順序を見ると、1 位米国(64%)、2 位英国(20%)、3 位イタリア(7%)で、典型的な結果となっています。

2009 年 5 月にはアイルランドとスペインがリストに登場し、マレーシアとギリシャが姿を消しました。オーストラリアの攻撃の割合がわずかながら増加し、2009 年 4 月には 1%でしたが、2009 年 5 月には 3%になっています。5 位は 6 カ国が同率で、カナダ、南アフリカ、ルーマニア、アイルランド、インド、スペインがいずれも全体の 1%の攻撃を占めました。

過去 1 年間に攻撃総数が多い上位 10 カ国に常に姿を見せたのは、米国、英国、イタリア、カナダ、スペイン、南アフリカの 6 カ国です。

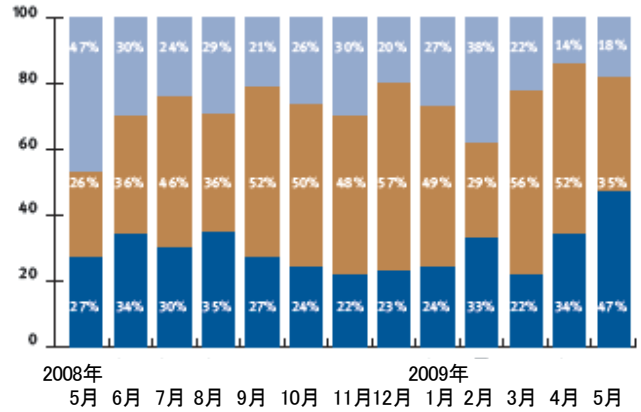




米国内でフィッシング攻撃を受けた金融機関の分類

トレンド分析

2009年5月には、全米規模の銀行への攻撃の割合(47%)が過去12カ月間で最大となりました。これまでほとんどの月で、地方銀行に対する攻撃が最も多くなっていましたが、今月は全米規模の銀行への攻撃が最も多くなりました。2009年5月には、これら3つの分類の中で全米規模の銀行への攻撃の割合がほぼ40%増加した一方、米国地方銀行に対する攻撃は33%減少しました。さらに、米国信用組合への攻撃の割合は、2009年5月におよそ30%増加しています。



出典: RSA FCC

■ 全米規模の銀行 ■ 米国地方銀行 ■ 米国信用組合



The Security Division of EMC

RSA セキュリティ株式会社
<http://japan.rsa.com>

RSA、RSAロゴはRSA Security Inc.の米国およびその他の国における商標もしくは登録商標です。EMCはEMC Corporationの登録商標です。本書に記載されているその他すべての商標は、それぞれの所有者に帰属します。