ホワイトペーパー

分析：Operation High Roller

McAfee Advanced Research および Threat Intelligence ディレクター、デイブ・マーカス（Dave Marcus）
Guardian Analytics 脅威研究者、ライアン・シェルストビトフ（Ryan Sherstobitoff）

ハイテク業界がマントラのように唱えている「自動化と革新」は残念ながら、グローバルに展開し、何層にも重なった構造を持つ詐欺集団が、企業や個人から高額を騙し取ることに役立ってしまっている。この詐欺集団は、「SpyEye」や「Zeus」といった確立した戦術をベースに、巧妙に進化させた新しい手口を数多く生み出している。たとえば、物理的な多要素認証の回避や、自動化されたミュールアカウント（不正口座）のデータベース、サーバーベースの不正決済、10 万ユーロ（13 万 US ドル）にものぼる金額の不正な企業口座への送金企てなどである。これまで、こうした金融詐欺集団のターゲットは主に欧州であったが、今回私たちの調査で米国やコロンビアをはじめとして欧州外にも広がっていることがわかった。

目次

概要

マカフィーとGuardian Analyticsは、非常に巧妙な金融サービス詐欺がグローバルな規模で展開されており、米国の金融機関システムにも到達していることを突き止めた。この報告書がメディアに届けられる間にも、私たちは国際的な法執行機関に積極的に協力して、これらの攻撃を阻止するよう努めている。

標準的な「SpyEye」や「Zeus」といった手動の攻撃とは異なり、サーバー側のコンポーネントとかなり徹底した自動化を利用しているグループを12件以上発見した。詐欺師たちは、大金を蓄えている口座から多額の金を吸い上げる。このことから、本調査のタイトルを「Operation High Roller[1]」とした。

人が介入する必要がないため、攻撃は迅速に進み、巧妙に拡散する。この手口は、金融機関の取引システムに対するインサイダーレベルの知識をベースに、カスタムメイドと既成の悪質なコードを組み合わせて攻撃を行うもので、「組織犯罪」という表現が適当だと思われる。

この調査では、多額の資金を蓄えている商用アカウントや個人富裕層を狙って金銭を引き出そうとする、なりすまし犯罪の処理を何千件と行っているサーバーが60台確認された。攻撃のターゲットが消費者から企業にシフトするに従って、不正な企業口座への不正送金額は平均で数千ユーロにものぼり、中には10万ユーロ（13万USドル）[2]もの大金が不正送金されるケースも現れるようになった。ターゲットが欧州連合（EU）、中南米、そして北米へと広がるにつれて、3つの攻撃の戦略が浮かび上がってきた。

本調査は、大きな銀行しか狙われないという世間一般の理解を覆し、信用金庫、グローバル規模の大手銀行、地方銀行を問わず、すべての規模の金融機関が攻撃の標的になることを示している。これまでで、少なくとも60以上の銀行から、最低額で6000万ユーロ（7800万USドル）の不正送金が企てられたと推計されている。仮にこういった詐欺行為がすべて本報告書に記載したオランダの例のように成功したとすると、企てられた不正送金の額は20億ユーロにも上ることになる[3]。

用語集

GIRO

欧州の標準的な支払い形態で、これを利用して支払者から受取人に金銭が送られる。米国も類似の振込モデルを使用しており、自動資金決済センター（Automated Clearing House）と呼ばれている。

IBAN

国境を越えて銀行口座を特定するための標準。

詐欺取引サーバー

金融機関のバンキングポータルにアクセスし、実際の取引を処理する（ここにはアカウントログインも含まれる）。

Web インジェクション

特別な HTML コードと JavaScript をブラウザーのウィンドウに挿入して行う攻撃。このコードは、テキストや画像を表示したり、フォームに欄を追加したりして、必要な認証情報の収集を可能にする。

ZEUS/SPYEYE

マルウェアのペイロードをインストールしてコンピューターやアプリケーションを制御することのできるツールキット。このツールキットによって Web インジェクションが配信されることも多く、ブラウザーベースのフォームを書き換えて、パスワードやログイン情報、その他のアカウント情報を攻撃者に転送するのに使われる。

ケーススタディの流れ

本調査では、複数の攻撃について検出と分析を行った。以下に、いくつか調査を行った具体例を詳述し、攻撃の裏側にある革新と自動化について議論を行っていきたいと思う。その後、私たちの調査でわかった3つのタイプの攻撃戦略を、ステップ・バイ・ステップ方式で説明していくものとする。

イタリアにおける自動化攻撃

今回の研究で見つかった一連の詐欺行為の最初のターゲットは、知名度の高いイタリアのある銀行と、その消費者および企業顧客のアカウントだった。その攻撃では、SpyEyeとZeusマルウェアを使用して、口座の金銭が個人名義のミュールアカウントあるいはプリペイドのデビットカードに金銭を送り、そこから犯罪者がすぐに匿名で引き出せるようになっていた。

一見、他のクライアントベースの攻撃と変わらないように思われるが、この攻撃はさらに自動化されている。データを収集して、別のコンピューターに手作業で送金するのではなく、iFRAMEタグをこっそりと挿入して被害者の口座を乗っ取るもので、攻撃者が積極的に介入することなく、送金はローカルで開始される。

このイタリアの例では、マルウェアに使用されているコードが被害者の最高額を探し出し、残高を確認して、一定のパーセンテージ（今回は3%などというように攻撃のたびごとに決定）もしくは比較的少額の、500ユーロほどの金額を、プリペイドのデビットカードまたは銀行口座に送る仕組みであった。

狙われた消費者の中には、いわゆる「High Roller（高額預金者）」と呼ばれる人もいて、平均で25万ユーロから50万ユーロを口座に貯えていた。送金先は、国内のこともあり、IBANコードを使用して国外へ送られることもあった。

この詐欺には、ほかにも革新的な要素が含まれている。スマートカードリーダー（ヨーロッパでは一般的）による物理的な認証（8ページ欄外）を必要とするところで、システムが必要な追加情報を入手して処理し、二要素認証形式を回避することに成功した初のケースとなったのだ。

60秒以内に、スクリプトがGIRO（振替処理のページ）へと誘導し、リモートのデータベースからミュールアカウントの情報を抽出して、送金を開始する。人手の介入はなく、遅延もなく、データ入力のエラーもない。

広がる攻撃の足跡

一度攻撃パターンがわかってからは、欧州や中南米の銀行でも同様の攻撃の証拠が見つかるようになった。これらの攻撃は、イタリアで見つかったものと同じコードを使い、それぞれの銀行に合わせて調整していた。ここではじめて、この詐欺が本質的にグローバルに展開されたものであることがわかり、私たちは、他の地域にも攻撃が広がっている可能性を疑い始めた。後にコロンビアと米国で積極的な攻撃活動の証拠が見つかり、私たちの推測が裏づけられた。

次に示す欧州の例では、企てられた詐欺活動の被害想定額を見積もっている。攻撃に関与したサーバーは60台見つかっており、以下の表と合わせると、犯罪者が企てた不正送金の合計額は、6,000万ユーロから20億ユーロと推計される。

ドイツにおける攻撃活動

2012年1月の終わり頃、私たちはドイツでまったく同じ攻撃を発見した。被害者のサーバー上のログデータを調べてみると、176の口座にアクセスし、100万ユーロ近い金額がポルトガル、ギリシャ、英国のミュールアカウントに送られていたことがわかった。口座の平均残高は約5万ユーロであり、富裕層に狙いが絞られていたことがわかる。平均送金額は約5,500ユーロにまで達していたが、国際送金では金額がさらに高くなり、1回のIBAN送金で、2万7,563ユーロから5万ユーロをはるかに超える金額が処理されている。

アクセスされた口座の合計額	8,339,981ユーロ
企てられたミュールへの送金額合計	962,335ユーロ
被害者の平均口座残高	47,657ユーロ
企てられたミュールへの送金額平均	5,499ユーロ

オランダの金融機関を激しく攻撃した詐欺活動

2012年3月になると、ターゲットはオランダの金融機関システムに向けられ、攻撃は強化されて、サーバーサイドで攻撃を自動化するペイロードが採用されている。サーバーサイドで不正送金を実行することで、エンドポイントのセキュリティツールが回避でき、金融機関の詐欺監視チームが使用しているモニタリングツールを妨害できることに犯罪者は気づいたようだ。こういった取引を行ったサーバーは、カリフォルニア州サンノゼに位置されていた。

この攻撃では、オランダの2つの銀行の5,000を超える口座が狙われた。銀行の取引処理サーバーから被害者のログを引き出して調べてみたところ、企てられた詐欺被害額は全体で推定3,558万ユーロに上った。消費者からビジネスアカウントへとターゲットを移すことで、詐欺師は送金限度やマネーロンダリングの基準に制限されたり（たとえば米国では1万ドル以内に制限される）、怪しまれたりすることなく、さらに高額の送金ができるようになった。高額の電信送金はビジネス上ではよくあることで、そういった取引の頻度や送金額などから、詐欺取引は目立たなくなっていた。詐欺取引は、発見や法的な処置の適応を防ぐため、しばしば海外に送金されていた。国際送金には二つの利点がある。一つ目は詐欺行為が発見されたり、受け取り側で回収する可能性を軽減することで、二つ目は、規制、トラッキング、法の執行等が国ごとに異なり、追跡を困難にすることである。

アクセスされた口座の合計額	141,303,005ユーロ
企てられたミュールへの送金額合計	35,580,000ユーロ
被害者の平均口座額	28,170ユーロ
企てられたミュールへの送金額平均	2,500ユーロ

中南米への広がり

攻撃活動が欧州全体に広がると、活動は中南米にまで拡大した。2012年の3月3日、私たちは12以上のコロンビア企業がターゲットとされた攻撃を発見した。すべて同じ銀行に口座を持つ企業で、それぞれの口座残高は50万USドルから上は200万USドル近いものもあった。

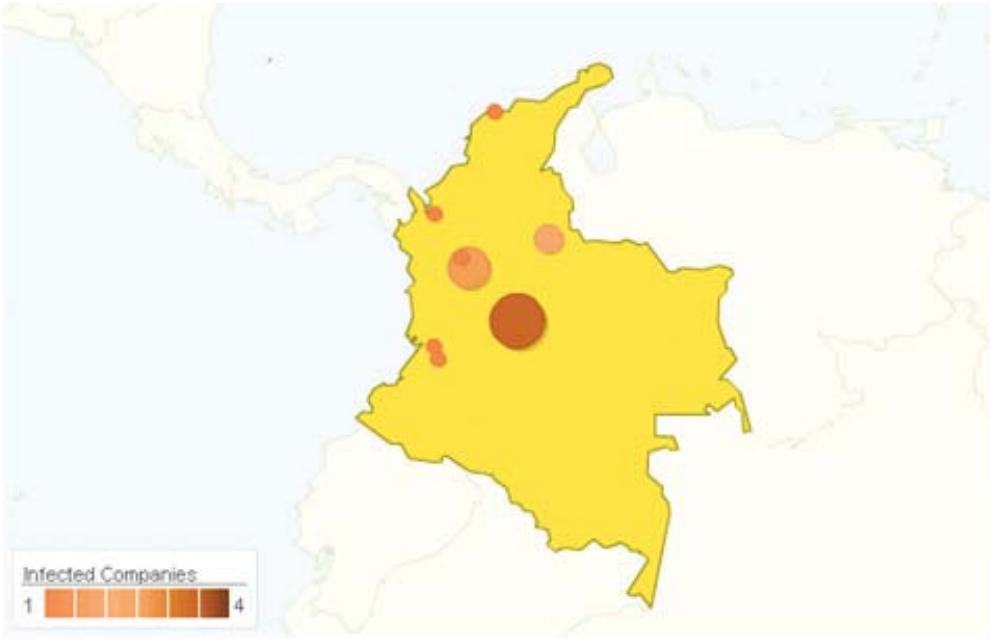


図 1. ボゴタ、 コロンビアが集中攻撃された

この攻撃活動に使用された不正送金サーバーがホスティングされていたのは、カリフォルニア州のブレアであった。攻撃の大半はこのサーバーによって自動化されていたが、詐欺師がロシアのモスクワから不正取引の一部を操作し、被害者の口座残高の50～80%を不正に引き出す企てをした証拠がログから突き止められた（以下の「戦略3」）。

米国に目を向けたオランダの詐欺師集団

同じく2012年の3月には、オランダの攻撃に使用されたカリフォルニア州サンノゼのプロバイダーが管理しているサーバーが、米国の銀行をターゲットとした詐欺行為に関与していることが確認された。このサーバーは、サーバーとクライアントの両サイドのコンポーネントを使用して、米国の金融機関に対する自動攻撃を仕掛けていた。これは、概して数千万ドルが置かれている特定の目的の商用または投資口座から電信送金を行うものである。北米の金融機関で攻撃が確認されたのはこれが初めてであり、109社が被害を受けている。この米国における攻撃の形跡から、米国の企業だけを狙ったマルウェアは8種類から10種類存在しており、ミュールアカウントへの不正送金をしていたことがわかった。

米国を狙った攻撃では1つの革新として、ターゲット企業の法人貯蓄から当座預金口座に自動振替する手口が使われている。当座預金口座に移された資金は、外部の口座に送金されるのがビジネスの手法として通常の流れと考えられる。ただこの場合は、送金先が国外のミュールアカウントであるということである。

60日間にわたる米国ターゲットの攻撃展開

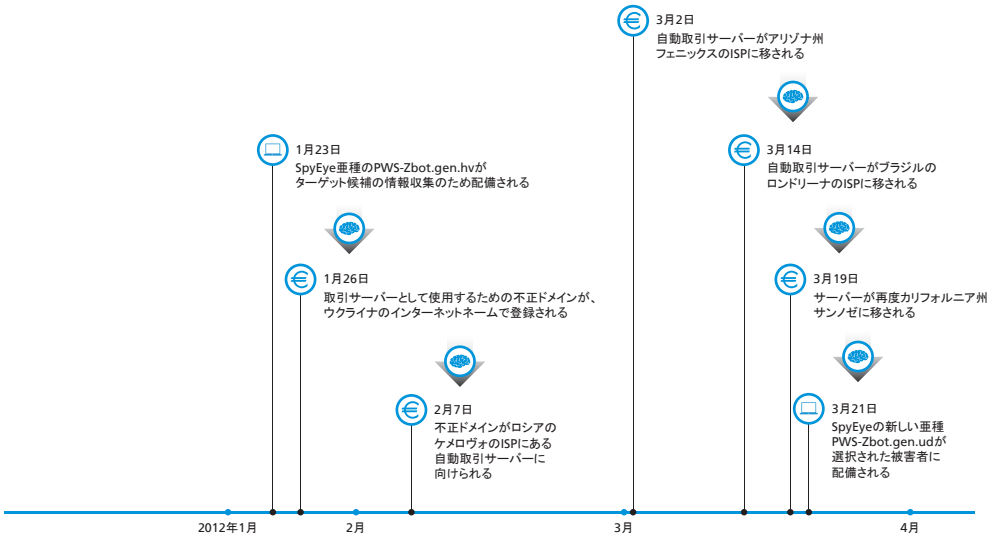


図 2. ある米国ターゲットの攻撃に関して、 世界中をわたって活動している様子を明らかにしたもの。サーバーがサンノゼに戻ってからは、 オランダと米国をターゲットとする新しい攻撃となった

二要素認証とは？

詐欺の手口が巧妙さを増すにつれて、金融機関はオンラインバンキングアプリケーションの認証を強化してきた。以下のカテゴリーの内いずれか2つを使用するものを、二要素認証という。

記憶しておくもの
- パスワード
- 4桁の個人識別番号（PIN）
- トランザクション認証番号（TAN）（リスト形式もしくはオンザフライで生成したものをSMS経由または別のセッションを通じてクライアントのコンピューターに送る形で、金融機関から提供される）

入手するもの
- 物理的なトークンまたは自分のデバイスにインストールされているソフトウェアトークンによる一度だけ有効なパスワード
- 認証とチップ付きのスマートカードとスマートカードリーダーといった物理的なデバイスの組み合わせにより生成したデジタルトークン

生体認証
- バイオメトリック指紋リーダー
- 虹彩スキャナー

新しい点：チップ、リーダー、PINによる物理的認証の自動回避

「Operation High Roller」のマルウェアは、はじめて「スマートカード＋物理的なリーダー＋PIN」の組み合わせを回避している。通常は被害者がチップ付きのスマートカードをカードリーダーに挿入し、PINを入力する。銀行のシステムが、物理的なスマートカードに含まれているデータをベースにデジタルトークンを生成し、トランザクションを承認する。

マルウェアは、ログイン時にこのプロセスのシミュレーションを正確に実行することで、認証をクリアする。疑惑を回避するために、スクリプトは送金認証プロセス中ではなく、ログイン時にそのトークンを収集する。そして、ユーザーに「しばらくお待ちください」というメッセージを表示して時間を稼ぎつつ、デジタルトークンを使用してトランザクションを有効にする。

新たな高みに達したサイバー窃盗団：「SpyEye」「Zeus」に比べて進化した点

攻撃は「SpyEye」および「Zeus」をベースにしているため、「Operation High Roller」は基本的に、Webインジェクションでよく見られるコード（口座利用者がブラウザーのセッションで目にする画面を改ざんするコード）と情報の傍受（口座から金銭を引き出す）、およびトランザクションを秘匿するアドオン[4]で成り立っている。しかし、一連の攻撃では、手口はこれらの基本を超えて巧妙になっており、「SpyEye」および「Zeus」攻撃の有名な中核部分に、ユニークなファクターを追加する3つの新たな戦略を組み合わせている。

さらに進んだ自動化

「SpyEye」「Zeus」攻撃は、大概手作業のコンポーネントをベースにしており、詐欺師自身が積極的に動かなければならない。彼らは、ソーシャルエンジニアリングと遠隔コードの実行により、ホストシステムとオンラインの銀行口座にそれぞれ攻撃を仕掛けている。マルウェアを仕掛け、Man-in-the-Browser攻撃によって認証情報を盗み出してデータを作成し、その後被害者のマシンから不正送金処理を行う。

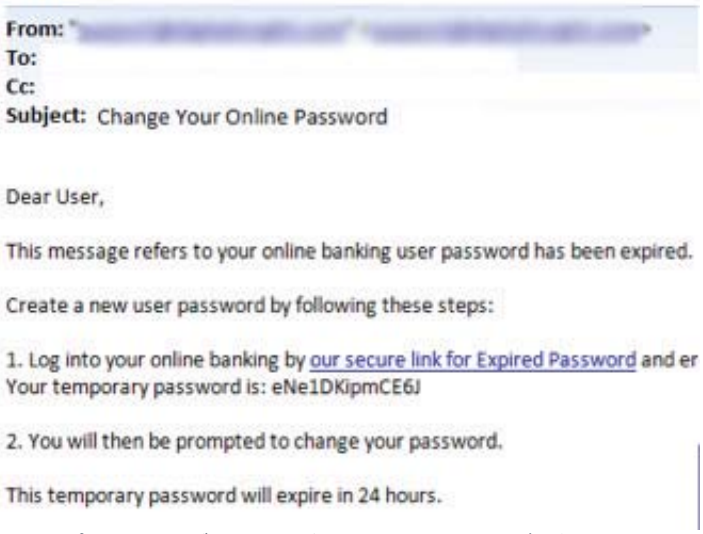
これに対して、相当な高額のトランザクションでは人手が入るケースがあるものの、ほとんどのHigh Rollerのプロセスは完全に自動化されており、ターゲットとする銀行や金融機関のオンラインプラットフォームに向けて、ひとたびシステムを稼働させてしまえば、何度でも自動的になりすまし犯罪を繰り返し行うことができる。たとえば「ドロップ」情報が常に最新になっているようにするために、送金を行う前に「アクティブなミュールアカウント」データベースに口座情報を照会する。自動化プロセスはさらに拡大されて、物理的な二要素認証の回避をはじめとして、以下の機能を含むようになってきている。

サーバーサイドの自動化

この攻撃では、システムと被害者のオンラインバンキングプラットフォームとの間でやり取りされる不正送金実行の方法について、実際の手口を隠すことを目的とした巧妙なサーバーサイドの自動化も行われている。私たちが最初にヨーロッパで発見したマルウェアと違い、オランダや米国で発見されたさらに巧妙化した攻撃は、不正な取引の処理をクライアントからサーバーへ移動させている。実際の口座へのログインも含めて、詐欺行為に関わるタスクは、「防弾」ISP（犯罪者に優しい利用規約のISP）に置かれた詐欺師のサーバーから行われ、変更されないようロックされ、検出を避けるために頻繁に移される。そしてプログラムを移すたびにWebインジェクションが更新されて、新たな拠点とのリンクが形成される。

富裕層のターゲット

北米で被害に遭ったのは皆、残高が少なくとも数百万ドルの商用口座を備えた企業だった。大概、標的はオンラインによる偵察とスピアフィッシングで見つけることができるが（図3）、中には既存の感染ホストを活用している攻撃者もいる。


From: [redacted]
To:
Cc:
Subject: Change Your Online Password

Dear User,

This message refers to your online banking user password has been expired.

Create a new user password by following these steps:

1. Log into your online banking by our secure link for Expired Password and er
Your temporary password is: eNe1DKipmCE6J

2. You will then be prompted to change your password.

This temporary password will expire in 24 hours.

図3. スピアフィッシングメールの一例。不正リンクはユーザーを不正サイトに誘導し、一連の感染プロセスを始める

ホストがすでにマルウェアに感染していた場合、「SpyEye」や「Zeus」を使用してホストをプロファイリングし、ユーザーが利用している金融機関のオンラインプラットフォームや、その他口座関連データといった情報を収集し、攻撃のカスタマイズに活用することができる。ペイロードを含むマルウェアをこれらの感染ホストにロードすると攻撃の準備が整い、ボットネットの管理者が、既存のボットネットから、さらに多くの利益を上げられるという仕組みである。

物理的な二要素認証の自動回避

「High Roller」を狙うマルウェアに関する例はすべて、複雑な複数段階の認証を回避することができる。シンプルの認証データ—セキュリティチャレンジ・クエスチョンやワンタイムトークン、またはPIN — を収集する最近の攻撃とは異なり、この攻撃は、カードをリーダーに通して、入力欄に情報を入力することで、拡張された(「ユーザーが入手するもの」を使った)物理認証を回避することができる。

この攻撃では、スマートカードリーダーとパッド・エントリーという物理的なコントロールを回避し、ワンタイムパスワード(またはデジタルトークン)を生成させるのに必要な情報の提供を被害者から引き出す。

公に議論されている他の攻撃と違う点は、詐欺師が物理的な二要素認証システムの回避に使用している複雑なプロセスである。通常のGIRO送金は2つのステップを必要とする。口座にログインして、次に送金(外部への支払い)を許可する、という手続きである。「High Roller」をターゲットとしたスキームでは、大がかりなJavaScriptでWebインジェクションを使用し、ログイン時のプロセスに手を加えて、2段階のログインステップで必要になる情報をすべて収集する。物理的な認証情報はログイン中に収集されるため、このトランザクションのコンテクストの外側にいる被害者はまったく疑いを持たず、ただログイン体験がアップグレードされたとしか思わない。

送金処理に必要な情報をすべて集めると、マルウェアがユーザーの注意をそらし、その間にバックグラウンドで合法的なデジタル トークンを使用して送金を実行する。詐欺師たちはすべての口座でこの自動化プロセスを複製することができ、複数のシステムで再利用できるため、規模がどんどん拡大していくという仕組みである。

物理的デバイスを使用した二要素認証システムの打破は詐欺師たちにとって飛躍的な進展であった。物理的なセキュリティデバイスにもこのテクニックが拡張する可能性を考えると、金融機関はこの革新を真剣に受けとめるべきであると考える。

標準的なセキュリティソフトウェアに対するテクニック

広範なカスタマイズにより、コードと攻撃インフラの安全性が確保される。ルートキットの使用により、クライアントサイドに置いたマルウェアをシステムの奥深くに潜伏させることができ、アンチウイルススキャンによる検出を逃れることができる。また実際のバイナリー(各銀行に合わせて調整し、ブラウザーに侵入させたペイロード)を、ごく少数の限られたターゲットにしか配布しないのも1つの巧妙な手段である。私たちの研究者がMcAfee® Global Threat Intelligence™ データベースを使用してバイナリーの追跡を開始したところ、感染システムの数は比較的少ないことがわかり、攻撃が検出システムのレーダーの下をかいくぐることができるよう、詐欺師たちが巧妙に策を講じていることが確認された。

リンクとコードは — エンコード、カプセル化、暗号化により — わかりにくくされており、Webインジェクションの内側に置かれて検出や検査を免れるようになっている。また、Webサーバーの中には動的な動きをするものもあり、その場合ブラックリストやレピュテーションベースのテクノロジーでは対抗できない。たとえばサーバーサイドのコンポーネント(コマンドとコントロールサーバー、および不正送金サーバーの両方)は巧妙に隠され、レピュテーションベースのシステムによる分類を回避できるよう仕組まれている。これによってサーバーが、より長くオンラインに留まることが可能になる。

分析の内情

このスキームは典型的な SpyEye や Zeus の使用法をとっていないため、検出は難しいものとなったが、 この調査は詐欺師たちによる重大なミスにより成功した。 それは被害者のログ、 送金データ、ミュール情報を格納するディレクトリーの構造が適切に保たれていなかったことである。このデータを元に手口のバーチャルマップを作成することが可能となった。

ログ情報のレビュー後、 調査チームはコードのバージョン、 日付、 標的となった被害者など、 法的に有効な重要な情報を発見した。

この調査で、 426 の未知の SpyEye および Zeus の亜種が確認された。

- 4 つのユニークな SpyEye バイナリーにパッシブトランザクションの操作が含まれていた
- 16 のユニークなバイナリーに一獲千金狙いの JavaScript コードが含まれていた
- 44 のユニークなバイナリーに EU スタイルの JavaScript コードの証拠が含まれていた

詐欺検出を避けるテクニック

詐欺師たちが金融業界について知識があるのは明らかである。慎重なナビゲーションで、銀行の詐欺検出プロセスのしきい値や規制トリガーを回避していることが見られる。たとえば、自動トランザクションで残高をチェックし、送金額が口座残高の一定のパーセンテージを超えないよう注意し、（ほとんどの場合）1口座につき2回以上の送金は避けている。また、攻撃アルゴリズムでもページナビゲーションのシミュレーションを行い、本当に人間が実行したように見せるために、送金のタイミングもそれぞれずらしている。さらに、Webインジェクションは金融機関の顧客の一般的な使用方法に合わせ、挿入するコンテンツもログイン画面、口座残高表示画面、トランザクション開始画面など、顧客の作業に従って見た目が変わるよう設定されている。

証拠隠しのテクニック

犯行後には、ユーザーからの送金の証拠を隠す複数の手順が取られる。たとえば、クライアントサイドに置いたマルウェアは、印刷可能なステートメントへのリンクを切断する。と同時に、確認のEメールおよびステートメントEメールのコピーを検索して、これらを消去する。最後に、被害者の画面に表示されるステートメントの送金額を変更し、不正送金が見えないようにする。こうした戦術は新しいものではないが、他の戦術と組み合わせて使っているところが非常に高い水準の専門技術を示すと言える。

3つの攻撃戦略

ターゲットが、最初に欧州で詐欺被害に遭った個人の資産家から、中南米や米国の資産価値の高い企業へとシフトする間に、攻撃を支えるテクノロジーが進化してきている。

戦略1：消費者に対する攻撃の自動化

最初に欧州で確認された感染パターンは「SpyEye」や「Zeus」を利用した他の詐欺活動とほとんど変わらないが、手動で行う代わりにトランザクションが自動化されている。

- フィッシング詐欺のEメールが、特定の金融機関に口座を持つ個人または企業に送られる。
- Eメールには偽のリンクが含まれており、ユーザーがこのリンクをクリックすると、不正なWebページに誘導され、悪質なシーケンスが開始される。
  - ページには「Blackhole Exploit Kit」や同様のフレームワークが含まれており、このキットが被害者のブラウザーに適当な脆弱性を検出して、エクスプロイトスクリプトをロードする。
  - エクスプロイトスクリプトが「Downloader Trojan」をインストールする。
  - そのあと「Downloader Trojan」が被害者のマシンに「SpyEye」または「Zeus」をインストールする。
  - 被害者がオンラインバンキングにログインすると、マルウェアがユーザーの口座の種類や残高といったパラメーターをチェックする。クライアントのパラメーターがマルウェアの基準に合致すると、トロイの木馬の「SpyEye」「Zeus」から詐欺師のコマンド＆コントロールサーバーに連絡が行き、銀行の適切なWebインジェクションを引き出す。そして、このWebインジェクションには、JavaScriptのペイロードが搭載されている。
- 詐欺のプロセスは、口座所有者であるユーザーが感染したコンピューターから正規の合法的な口座にログインしようとするのをきっかけにして開始される。
- ユーザーには標準的な本物の銀行のポータルが見えているが、実際にはユーザーの利用する銀行から必要な情報を入手するためのカスタムメイドのJavaScript Webインジェクションが表示されている。
- 挿入されていたスクリプトがセッションを制御し、具体的な指示を求めて詐欺師のサーバーに接続する。セッション内にトランザクション欄やエラーメッセージなどのコンテンツが挿入されている場合もある。たとえば、ユーザーがログインする際セキュリティ クエスチョンに答えることを求められ、そこでエラーが表示される。このエラーメッセージによって時間を稼ぎ、詐欺師のソフトウェアでトランザクションを完了することができるというわけである。
- ここでよく「お待ちください」のメッセージが表示され、ユーザーはその画面に60秒ほど引きとめられる。だが、実際には認証が行われていない。（図4）

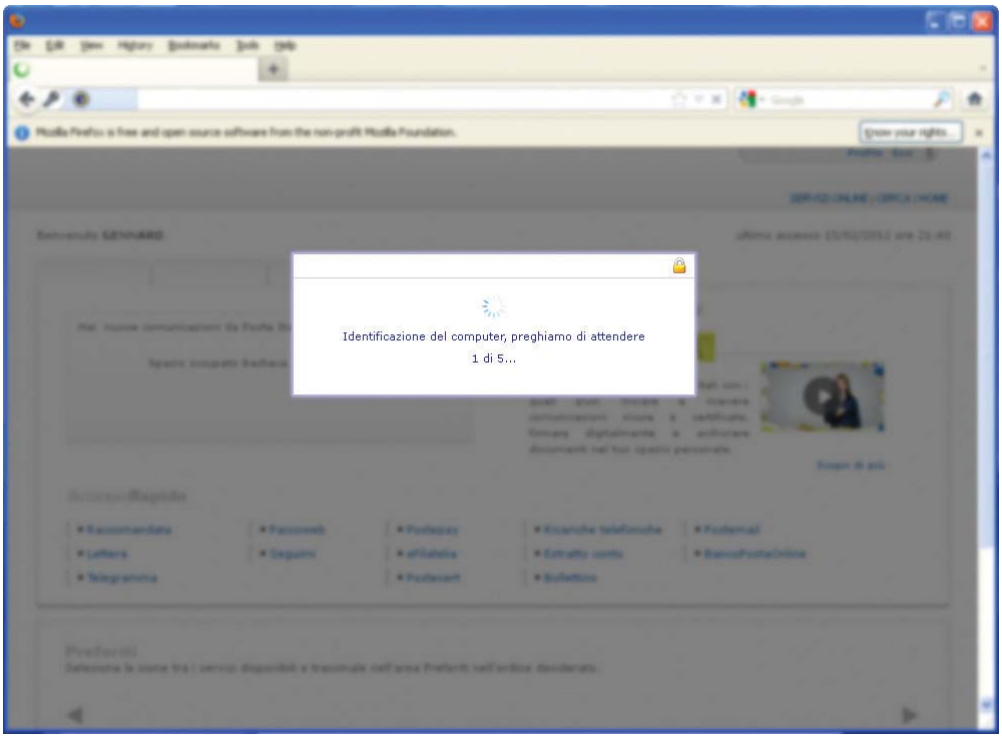


図 4. 消費者が自分の口座にログインすると、「しばらくお待ちください」という偽のメッセージが画面に表示されることがある

- 自動攻撃中に金融機関からトランザクション認証番号（TAN）の入力が求められた場合、クライアントサイドのWebインジェクションが偽のTANページをユーザーに表示される。マルウェアは以下のようにプロセスを進行する。
  - マルウェアが被害者の画面からTANを収集し、不正送金ができるよう本物のTANを金融機関に提出する一方で、被害者の口座へのアクセスを遅らせる。
  - マルウェアは傍受した認証情報を利用して、密かに（個人または企業の）ミュールアカウントへ送金を開始する。あるケースでは、送金先がプリペイドのデビットカードの例もあった。
  - マルウェアは、別のデータベースから有効なミュールアカウントを探し出す。これは従来手動で行われていたプロセス中のステップを自動化したものだ。クライアント上のバックグラウンドで行われるオンラインバンキングのセッションと並行して、隠されたiFrame内でトランザクションが行われる。コードがトランザクションページへと誘導し、自動のフォーム送信機能が作動し、出し子の情報を追加する。
- のち、ユーザーはセッションを進めることができる。
- 出し子が金を引き出し、それをウエスタンユニオンまたはリバティリザーブのペイメントに転換して、詐欺師に支払う。出し子は騙し取った金額のごく一部を取り、数日後にはすでに金の追跡ができなくなる。
- 窃盗を隠すために、マルウェアは被害者のコンピューターのメモリー内に留まり、偽の残高を示すように、ユーザーの銀行のステートメントを改ざんして、トランザクションに関する行項目を削除し、本当の口座残高およびトランザクションシーケンスを示しそうなステートメントの印刷を阻止する。

戦略2：自動化されたサーバーベースの攻撃

攻撃の2つ目のタイプは、詐欺のロジックをサーバーサイドへと移し、詐欺師のロジックをさらにわかりづらくしている。米国を狙うケースの中には、特定のインターネットバンキングプラットフォームを通して攻撃を仕掛けるものがあり、これによっていかなる規模の金融機関に対しても自動化された攻撃をすることが可能となっている。詐欺師は、特定のインターネットバンキングプラットフォームを使用している金融機関を特定し、その金融機関のクライアントを検出することに時間を費やす。その後マルウェアがサーバーサイドのWebインジェクションを利用した不正送金を自動で実行する。以下に一般的な流れを示す。

- 戦略1のときと同様に、クライアントの感染と情報漏えいが起こり、カスタムメイドのWebインジェクションが、マルウェアとともにダウンロードされる。
- 戦略1ではユーザーは60秒ほどで先に進み、目的のトランザクションを実行できた。しかしこのバージョンにおいて、ビジネスユーザーには「システムメンテナンス中」または「しばらくお待ちください」といったメッセージがよく表示され（図5）、長い時間その状態で足止めされる。12時間後、あるいは2日後に再度試すようになどと表示され、被害者に怪しまれることなくその間に送金が完了するのである。
- この攻撃では、不正送金は被害者のコンピューターからではなくサーバーから実行される。サーバーから金融機関のオンラインバンキングポータルに接続し、トランザクションを行うが、実は被害者は認証を行っていない。
- トランザクションが完了すると、「システムメンテナンス中」のメッセージが消え、被害者自身も認証が可能になる。この際彼ら被害者はログインデータを再入力することになる。
- 戦略1のときと同様に、金はミュールアカウントに送付され、引き出し可能となってから2から3時間以内に引き出される。プロセス全体の完了には、1～3日ほどかかる。

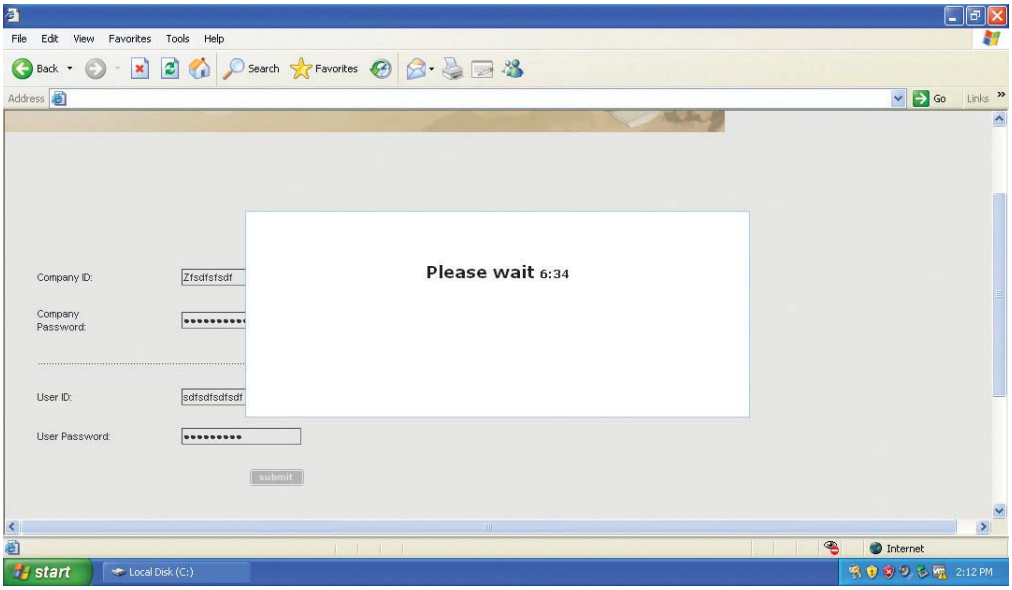


図 5. 企業を狙った詐欺では、 ユーザーは長時間待つよう求められる。（この場合は 6 時間以上）この間に送金が完了し、 ユーザーは残高が予定外に変わっているのに気づかない。

さらに、知名度の高いオンラインエスクロー（第三者預託）企業を狙う、トランザクションポイズニングと呼ばれるスキームも確認された。これは、感染被害者に代わって新しく電信送金を開始するのではなく、正当な口座名義人が始めたトランザクションを変更するものである。もともとのトランザクションは、北米の口座から英国のエスクロー口座にオークションで購入した車両の代金を送金するというものだったが、その代金がミュールアカウントに送金されていた。（図6、7）

この攻撃は、合法的なデータの裏側に必要な情報を埋め込むリモートスクリプトを使用する。その結果、口座所有者には不正送金が見えないという仕組みだ。スクリプトは以下のフィールド情報を書き換える。

1. 銀行名
2. 分類コード
3. スウィフトコード
4. IBANコード
5. 口座番号
6. 受取人のアドレス

このメソッドでは、「コールバック」を使ってトランザクションの正当性を確認する銀行のコントロールを回避することが可能になる。コールバックで金額の確認は行われるが、受取人の確認は行わないので、トランザクションが乗っ取られても見逃される。

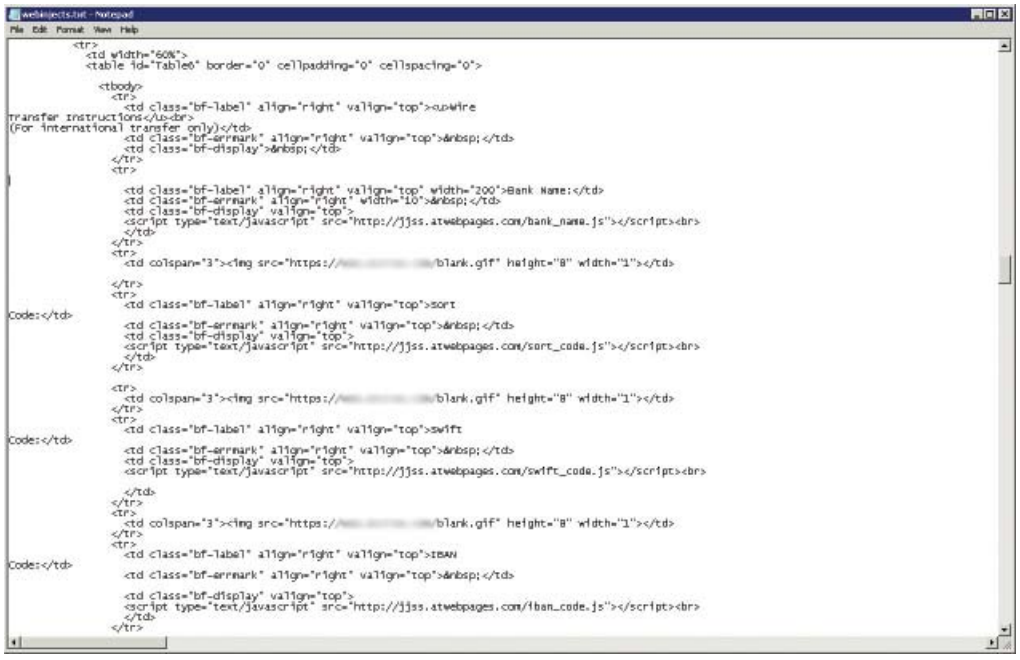


図 6.「SpyEye」 Web インジェクションが、 英国のミュールドロップポイントのミュールアドレス情報を挿入

図 7. 挿入されたミュールのアドレス情報

戦略3：人気の企業アカウントを狙う自動化／手動ハイブリッド攻撃

資産価値の高い企業アカウントやきわめて裕福な個人にサービスを提供しているブティック型銀行など、いわゆる世の中のトップクラスの企業がターゲットの場合は、詐欺師も他の攻撃よりアクティブにアプローチし、たびたび自動攻撃と平行して手動でセッションに参加することが私たちの研究でわかった。これにより、銀行専用のテクノロジーやシステム、ポリシーといった強化されたセキュリティ回避を可能にしている。また詐欺師が自ら定めた制約を無効にすることができるため、それぞれの口座からより高額を盗み取ることができる。

通常の流れは以下のようになる：

- 被害者のコンピューターが、これまでの例と同じ方法で危険に晒される。
- 詐欺師はマシンの前で、詐欺の被害となりそうなアカウント全体のイベントをモニターする。
- ユーザーがログインを試みると、マルウェアから詐欺師にセッション乗っ取りの通知が送付される（クライアントから JabberのインスタントメッセージもしくはSMSメッセージが送信される）。
- クライアントサイドのマルウェアがユーザーの認証を阻止し、詐欺師がバックグラウンドで、セキュリティクエスチョンを実行してトランザクションを処理する。
- 追加情報が要求される場合、詐欺師はそのデータを被害者のセッションに投入する。
- マルウェアに組み込まれた固定額、または口座残高の固定パーセンテージよりも高額を盗もうとする場合、ここで手動で取引額を調整する。
- サーバーが不正送金を処理し、その後、戦略2同様に「システムメンテナンス中」のメッセージを表示して被害者を足止めし、その間に送金を実行して、ミュールアカウントから金銭を引き出す。
- また、一企業に対して複数回の攻撃を企てることもある。その場合、クライアントのWebインジェクションスクリプトに変更を加えて異なるサーバーに向け、ブラックリスト型のソフトによる検出を免れる。また、被害者を新しいサーバーにリダイレクトすることも、新たな機能でアップグレードすることも可能である。こうした介入を通じて攻撃を継続して行うことができるのである。

障害回復および復旧の取り組み

2012年3月、詐欺活動の範囲が明らかになったことから、調査チームは積極的に法執行機関に協力し、米国内で検出された犯罪者が制御しているサーバーの所在の報告と、攻撃に関する情報提供を行った。

またマカフィーおよびGuardian Analyticsそれぞれの金融系顧客について、防御の検証および改善に着手した。多層管理や検出ソフトを正しく配備していれば、この攻撃は成功しないはずである。私たちは適切なセキュリティ構成を綿密に検討し、リアルタイムの脅威インテリジェンスをクライアントのホスト上でアクティベートし、ハードウェア併用のセキュリティで、捕捉の困難なマルウェアに対抗するなどの手段を講じている。

しかしOperation High Rollerが成功していることを考えると、金融機関、消費者、企業のすべてがそれぞれセキュリティコントロールや前提を見直すべきではないだろうか。

- アノマリ検出ソフトを備えていない地方銀行や信用金庫が多数存在し、この攻撃に対して完全に無防備な状態にある。
- 企業は、クライアントを危険に晒すソーシャルエンジニアリングおよびフィッシング詐欺攻撃に対するセキュリティコントロールと、特権ユーザーの教育の両方を強化する必要がある。
- 消費者は第一の標的ではないが、エンドポイントの制御を強化し、オンラインバンキングで取引を行う時は、不審な変更等がないか十分に注意すべきである。

基本的にセキュリティソフトウェアは、アクセスの検査、異常の検出、攻撃者のブロック等、何を目的とするものであっても、資産の周囲に階層的に配備してシステムを強化するべきである。Operation High Rollerのような攻撃は、複数の戦術と広範な自動化を用いるため、多様な防御を複数配備して、攻撃のさまざまな側面を検出し、妨害できるようにしておく必要がある。万能のツールというものは一つも存在しない。効果的にリスクを軽減するには、最低2層以上が必要であり、防御も自動化しておくと、攻撃の自動化に遅れず対抗できる。

たとえば、不正なサーバーを取り押さえ、ブラックリストを作成すれば、この種のリスクに対する効果的な緩衝材になると考えている銀行は多い。しかし、分析を見ると、こうしたサーバーサイドのシステムは、ダイナミックに移動を繰り返し、ブラックリスト技術による避けられない遅延を利用して、その裏をかいている。また、物理的な認証の回避やリンクを難読化するエンコーディング等の技術的進展は、詐欺師たちがマルウェア開発の最先端にあることを示すものとなっている。

教訓

大手金融機関において、詐欺検出部門のリソースは充実しているが、リソースが安全だという保証はない。今回の調査では、最も評判の高い金融機関でも、小さな信用金庫や地方銀行でも、攻撃が成功していたことがわかった。小規模なところは、規模が小さいため詐欺犯罪者のターゲットにはならないと考えていたかもしれない。しかし、金融機関が効率のよいオンラインプラットフォームを利用するようになったために、攻撃者は規模の大小にかかわらず、どの銀行に対しても詐欺行為を仕掛けることができるのである。

金融機関は、ますます自動化が進み、捉えづらく巧妙な詐欺行為を予期するべきである。ボットマスターは、既存の「SpyEye」「Zeus」感染マシン網をアップグレードして、より自動化が進められるよう進化する可能性が高い。また決済モデルも、自動資金決済センター（ACH）や送金決済をはじめ、さまざまなモデルが標的にされてくるだろう。本報告書で示した通り、攻撃はクライアントサイドからサーバーサイドに移行しているため、詐欺師たちはモデルを進化させて、詐欺ロジックの大半をサーバーに移していくものと思われる。そうなれば、セキュリティ責任者にとって防御戦略の開発は著しく困難になる。

しかしながら、本報告書に記された高度かつ自動化された攻撃に対しても、効果を発揮する詐欺防止ソリューションが存在する。口座名義人はそれぞれが特有であるため、詐欺師たちは、正規のプロセスと比較すると何か変ったこと、何か怪しい動きを見せるものである。アノマリ検出のソリューションは手動、自動を問わず、また既存の技術や新しく出てきたものにかかわらず、最も広範に詐欺攻撃を検出することが証明されている。アノマリ検出ソリューションは、ログインからログアウトを通して、オンライン／モバイルバンキング上で口座名義人の活動を監視し、正当なパターンと比較する。アノマリ検出について、米国連邦金融機関検査協議会（Federal Financial Institutions Examination Council = FFIEC）は、2011年の手引き補足（Guidance Supplement）において、金融詐欺の予防のための多層型セキュリティソリューションにおける最低限期待されるものであるという見解を強めている。

今回の調査では、攻撃者は、遅くて連携のない「ホワイトハット」的な検出システムを推定して金融詐欺を働いていたと結論づけられる。しかし、Operation High Rollerの解析、追跡に使用されたモデルは、詐欺に関する業界協力の効果を示すものと言える。Guardian Analyticsとマカフィーは、調査のために技術やデータリソースを提供し合い、相互補完的な見解、顧客ベース、スキルセットから、事件の全体像を導き出した。

こうしたパートナーシップを通じて、調査研究コミュニティは、金銭を辿って攻撃元をより効率よく突き止めることができる。業界は、以下のような質問に即答できるようにならなければならない。

- トランザクションの行先は？
- 送金サーバーはどこにあるのか？
- 法執行機関とはどのように連携すべきか？
- 標的とされているブランド（業界ソフトウェアベンダーを含む）への脅威に対抗するインテリジェンスは、どうすれば得られるか？
- どうすれば 、攻撃の複雑な挙動の特徴をより的確に捉えて、そのエコシステムを開発できるか？

セキュリティ研究者のなかには、今でも「SpyEye」といった悪質なバイナリをただ監視している人もいる。また、ポリモーフィックなマルウェアの挙動分析および検出に人生を賭けている研究者もいる。しかし、マルウェアは問題のほんの一部にすぎない。私たちは、犯罪活動の各段階で、システムを完全に機能停止に追い込む必要がある。マカフィーはすでに、以下の分野への投資を行っているが、マカフィーの研究者をはじめ、セキュリティ業界は、さらに先へと、迅速に進まなければならない。

- フィッシング詐欺 — 怪しいEメールおよび悪質な送信者のフィルタリング。
- Webサーバー — 月単位ではなく、分単位で自動送金の処理が行われているWebサーバーを検出し、遮断する。
- ネットワーク — ネットワークフロー、およびサーバーへの通信に使用されているプロトコルならびにパターン（バイナリーに限らず）から引き出した挙動情報を分類する。
- エンドポイント—ブートプロセス前のコードの挙動を調査し、ルートキットやメモリー操作を突き止めて、攻撃者にエントリーポイントを提供する脆弱性の存在するブラウザーやソフトウェアを検出して閉鎖し、攻撃可能な領域を縮小するためにホワイトリストの適用を実行する。

私たちには可能である。マシンも揃っている。たとえば、McAfee Global Threat Intelligenceは、クラウドから何十億というデータポイントを集めて検出を行っている。マカフィーのシステムは、悪質なサイトにレピュテーションを割り当てている。このシステムで、危険に晒されているトランザクションサーバーを特定し、アクセスをブロックすることもできる。これが新しいレピュテーションベースのブロッキングアプリケーションである。

Operation High Rollerを通して収集した情報は、金融犯罪における革新の戦略や範囲を明らかにする上で有用であった。他のセキュリティベンダーやグローバル銀行の業界に対して、この急増する詐欺の一団や来たるべく同様の攻撃に対して、検知や情報共有によって行動を起すことを推奨したい。この報告書が、現在も口座から金を盗まれている高い資産を持つ企業や個人に対して刺激となり、感度や警戒を高めることを願っている。

付録

以下のヒートマップでは、地球上で今回の詐欺師による活動が認められた場所を示している。不正サーバーは、高い密度で東ヨーロッパに見られ、また他の国にも戦略的に設置されていた。米国をターゲットとした攻撃における被害者マップは、この報告書以前に議論された同様の攻撃を除いて記載したことを考えると、予想を相当上回る大きな攻撃の形跡を示している。

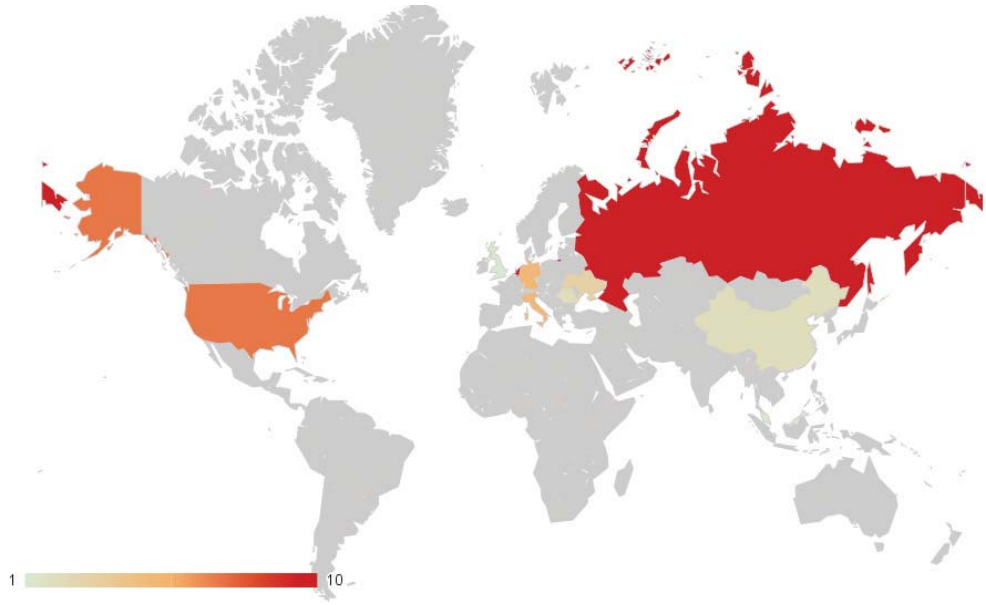


図 8. 不正送金実行サーバーがホスティングされている場所

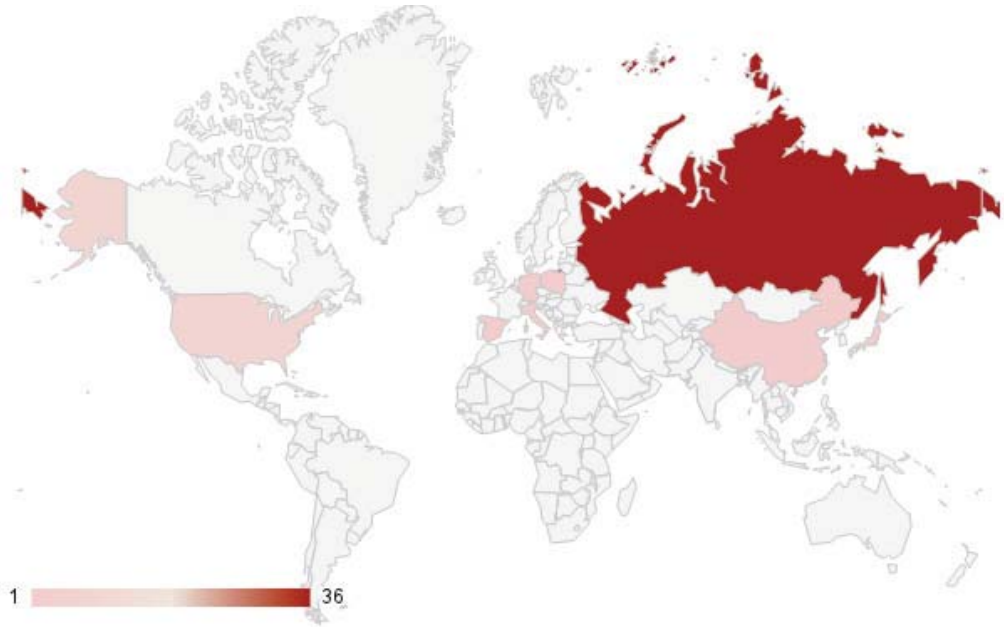


図 9. 米国のバンキングシステムを狙ったサーバーサイド自動化攻撃に使用された、 コマンドおよびコントロールサーバーの分布（16 亜種について分析）

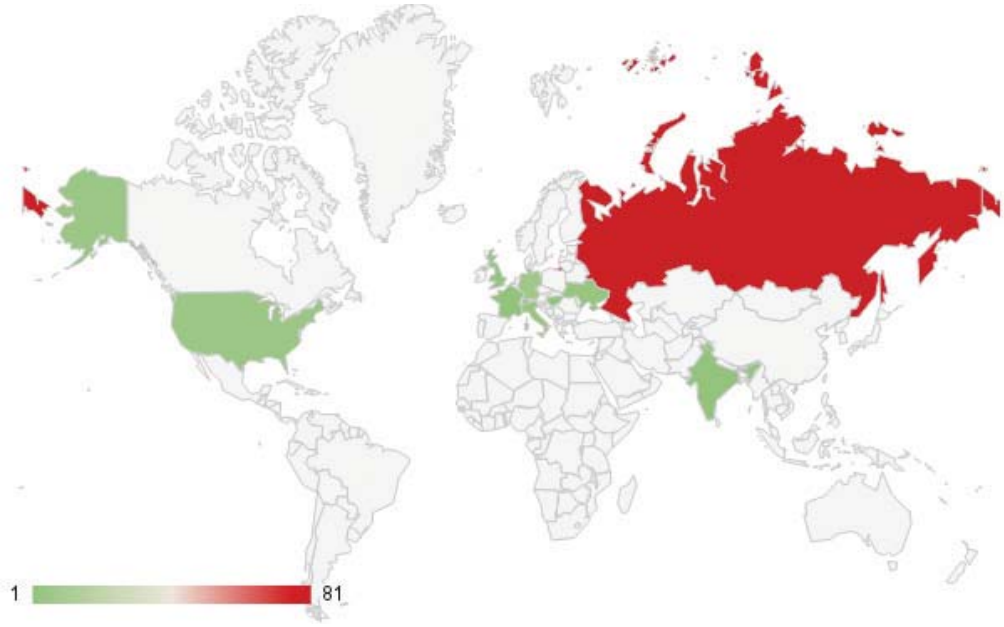


図 10. EU のバンキングシステムを狙ったサーバーサイド自動化攻撃に使用された、コマンドおよびコントロールサーバーの分布（44 亜種について分析）

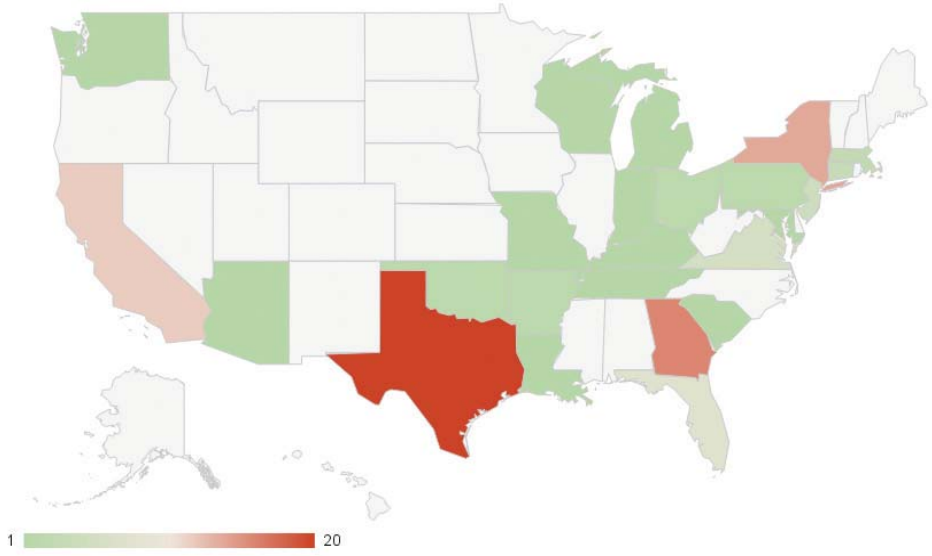


図 11. 攻撃中被害に遭った米国企業の所在地

著者について

デイブ・マーカスは、McAfee Labs™のAdvanced ResearchおよびThreat Intelligenceディレクターです。オープンソースやソーシャルメディアインテリジェンス、SCADAやICSシステムなどを注力分野とし、シリコン併用のテクノロジーを使った脅威検出の研究にも力を注いでいます。メディアを含む業界でのソートリーダーシップという面でも、ソーシャルメディア技術分野における重要な役割を果たしています。

ライアン・シェルストビトフは脅威研究者であり、前職においてPanda Securityの最高セキュリティストラテジストを務めました。Panda Securityでは、新興の脅威に対する米国の戦略的レスポンスを統括していました。セキュリティやクラウドコンピューティングのエキスパートとして広く知られています。

マカフィーについて

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

Guardian Analyticsについて

Guardian Analyticsは、金融機関の詐欺防止に完全特化しており、銀行や信用金庫などがプロアクティブに詐欺防止対策をとるためのお手伝いをします。金融機関にとって、詐欺行為から自身と口座所有者を防御することは、ブランド、評価、コミットメントを表す本質的な要素であり、セキュリティの保障は深刻な問題としてとらえられています。当社のビヘイビア・ベースのアノマリ検出ソリューション FraudMAPは、長年当社が知的財産分野に広範に投資する中で、実際に詐欺行為を解決した経験の蓄積や、オンラインバンキング詐欺防止の専門技術をもとに開発されています。

1 High Rollerとは、「大金を使う人」を意味する。
2 本報告書では、€1.0 ＝ $1.3の換算レートを使用する。
3 私たちは、様々な銀行における60台のサーバーログを調査した。この報告書では、調査結果から上限と下限の数字を引き出し、詐欺犯罪全体の推計として使用している。ログにはミュールアカウントに送られた送金額が示されているが、最終的に詐欺行為が成功した金額を把握することはできない。
4 http://threatpost.com/en_us/blogs/ramnit-worm-evolves-financial-malware-082311およびhttp://www.trusteer.com/blog/gift-wrapped-attacks-concealed-online-banking-fraud-during-2011-holiday-season を参照。

McAfee
An Intel Company

マカフィー株式会社
www.mcafee.com/jp

●製品、サービスに関するお問い合わせは下記へ

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

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

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

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

MCAWP-OHR-1207-MC