Kaspersky Security Bulletin 2014:

マルウェアの進化

2014年のサイバー脅威を
象徴する10のケース

KASPERSKY lab

目次

デイヴィッド・エム（David Emm）
プリンシパルセキュリティリサーチャー
Global Research & Analysis Team

年の瀬は沈思黙考の時期。前途に待ち受けるものに思いを馳せる前に、来し方を振り返ります。ここでは例年どおり、セキュリティの脅威をめぐる2014年の主な動向を総括します。

標的型攻撃とマルウェアの活動

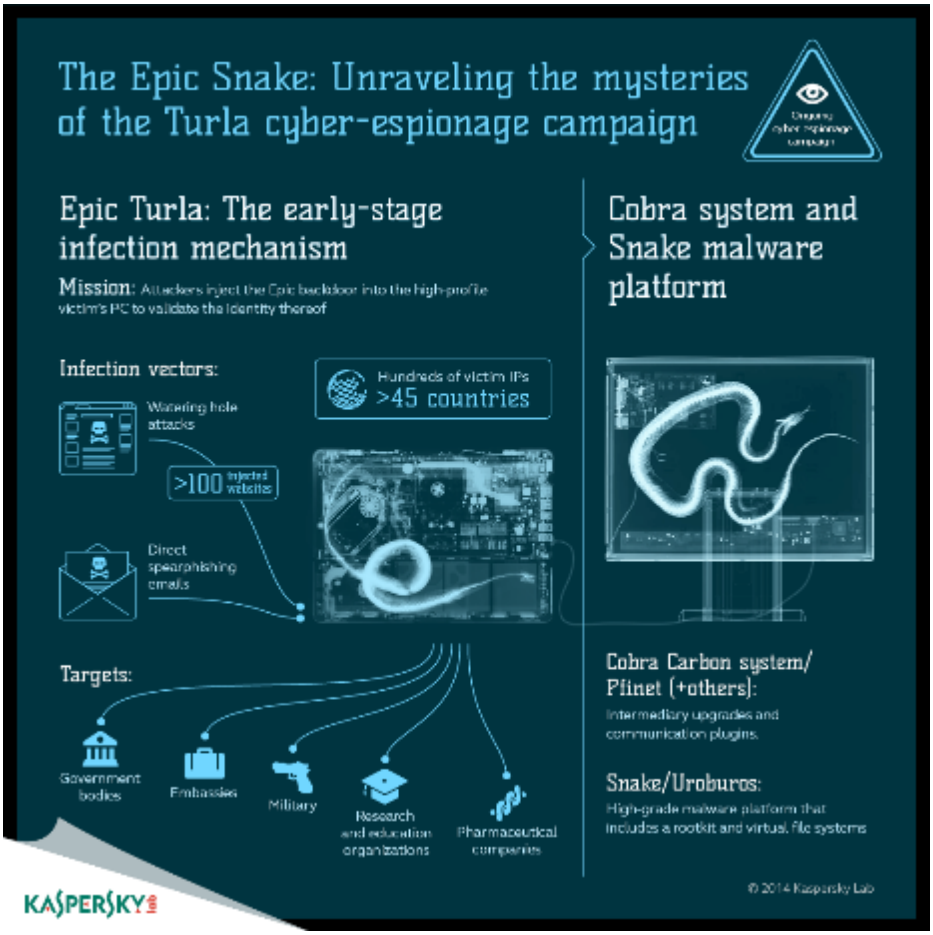
標的型攻撃は脅威の中で大きな位置を占めているため、この年次レポートでも詳しく取り上げます。

「Careto」または「The Mask」（Caretoはスペイン語で「醜い顔」「仮面」を意味する俗語）と呼ばれる複合的なサイバースパイ活動は、特定の組織から機密データを盗むように設計されていました。攻撃の標的は、世界31か国の政府機関、大使館、エネルギー企業、研究機関、未公開株式投資会社、活動家などです。Caretoには高度なバックドア型トロイの木馬が仕掛けられており、あらゆる通信チャネルを傍受し、感染したコンピューターからさまざまな情報を収集していました。盗まれた情報には、暗号鍵、VPN設定、SSH鍵、RDPファイルなどがあったほか、軍または政府レベルの特別な暗号化ツールとの関連が疑われる不明なファイルタイプもありました。コードは高度にモジュール化されており、攻撃者は自由に新機能を追加可能でした。バックドアにはWindows用とMac OS X用のバージョンがあり、一部のモジュールでは、Linux、iOS、Android向けバージョンの存在を示す要素も見つかりました。この種の高度な攻撃の例に漏れず、作成者の特定は困難です。コードにスペイン語が使われていましたが、大きな手がかりにはなりません。スペイン語は世界の多くの地域で使われているからです。撹乱のために意図的に使用された可能性もあります。しかし、この攻撃の背後には、サイバー犯罪者集団としてはまれな、非常に高い専門性を持つ集団の存在がうかがえます。これはCaretoが国家の後ろ盾のある活動である可能性を示しています。これまでの標的型攻撃と同様に、Caretoの起源は最初にこの脅威が明るみに出た時点よりはるか前にさかのぼります。弊社はこの攻撃者が2007年から活動していたと考えています。

3月初旬、セキュリティリサーチャーの間で、「Epic Turla」と呼ばれるサイバースパイ活動について広く議論されました。G-DATAのリサーチャーは、このマルウェアがロシアの特殊機関によって作成された可能性があると考えていました。一方、BAE Systemsの調査では、「Agent.btz」として識別されるマルウェアとの関連が指摘されました。これは2007年に開発されたマルウェアで、2008年に中東における米国の軍事作戦においてローカルネットワークを感染させるために使用されたものです。弊社によるEpic Turlaの最初の分析では、攻撃者がUSBメモリ使用して、盗難データ（インターネット経由でC&Cサーバーに直接送信できないデータ）を格納していたことに重点を置いています。このワームは、感染したコンピューターに接続されているすべてのUSBメモリに、「thumb.dll」という名前のファイルを書き込みます。メモリがその後、別のコンピューターに挿入されると、新しいコンピューターに「thumb.dll」ファイルがコピーされます。「thumb.dll」は、Red Octoberの「USB Stealer」モジュールにあるファイルの1つで、このファイルに対応しているマルウェアは、Epic Turlaだけではありません。過去にさかのぼると、GaussとminiFlameがthumb.dllに対応しており、USBメモリ上でこのファイルを検索していました。比較

のポイントを紹介したチャートをこちらでご覧いただけます。このマルウェアによって作成された「thumb.dll」という名前のファイルを含むUSBメモリは、世界中に数万はあるものと見られます。

弊社はその後のEpic Turlaの分析で、攻撃者がソーシャルエンジニアリングを使用してマルウェアを拡散した手口を解明し、攻撃の全体像を明らかにしました。攻撃者は、スピア型フィッシングメールを使用して標的をだまし、コンピューターにバックドアをインストールさせます。その中にはゼロデイエクスプロイトが含まれており、1つはAdobe Acrobat Readerに影響する脆弱性、もう1つはWindows XPとWindows Server 2003における権限昇格の脆弱性を突くものでした。攻撃者は、Javaエクスプロイト、Adobe Flashエクスプロイト、Internet Explorerエクスプロイトを利用した水飲み場型攻撃を使用したり、標的をだまして偽の「Flash Player」マルウェアインストーラーを実行させたりします。標的のIPアドレスに応じて、攻撃者はJavaエクスプロイトやブラウザーエクスプロイト、署名された偽のAdobe Flash Playerソフトウェア、偽のMicrosoft Security Essentialsを使い分けます。当然ながら、選ばれるWebサイトには、攻撃者の特定の関心（そして標的の関心）が反映されています。しかし弊社の分析によって、Epic Turlaバックドアは感染の最初の段階にすぎないということが示されました。Epic Turlaは、「Cobra/Carbon」システム（一部のアンチマルウェア製品では「Pfinet」）というさらに高度なバックドアの展開に使用されるものです。Epic TurlaとCobra/Carbonの運用に関して独自の知識が用いられていることから、この2つのバックドアに直接的で明確な結びつきがあることがわかります。Epic Turlaは、足場を固めて標的を値踏みするために使用されます。標的が攻撃者の関心に見合うことがわかると、感染したコンピューターは完全なCarbonシステムにアップグレードされます。Epic Turlaの概要についてはこちらでご覧いただけます。



6月には、欧州の大手銀行の顧客に対する攻撃の調査結果を報告しました。この攻撃では、わずか1週間で500,000ユーロが盗まれています。弊社はこれを、C&Cサーバーで使用された管理パネルのパス名から「Luuuk」と名付けました。感染に使用されたマルウェアは入手できませんでしたが、犯罪者は「Man-in-the-Browser」攻撃を実行するバンキング型トロイの木馬を使用して、悪意あるWebインジェクションによって標的の認証情報を盗んだと考えられます。一部のログファイルにあった情報を確認したところ、このマルウェアはユーザー名、パスワード、ワンタイムパスコード（OTP）をリアルタイムで盗んでいました。攻撃者は、盗んだ認証情報を使用して標的の口座残高を確認し、悪意あるトランザクションを自動的に実行しました。おそらく、正規のバンキングセッションのバックグラウンドで動作していたと思われます。盗まれたお金は、事前に設定されたマネーミュールの口座に自動的に送金されました。事前に設定されたマネーミュールが分類されていたことは、非常に興味深いことです。マネーミュールのグループは4つあり、それぞれ受け取れる金額が異なっていました。これにはミュールの間での信用度が反映されているのでしょう。弊社は合計で190の標的を確認しました。大半の標的はイタリアとトルコに住んでいました。盗まれた金額は標的によって1,700ユーロから39,000ユーロまで幅があり、総計で500,000ユーロに達しました。

攻撃者は弊社が調査を開始した直後に、重要なコンポーネントをすべて削除しましたが、これは活動を完全に停止したためではなく、インフラストラクチャに変更があったためと考えられます。この攻撃の背後にいるサイバー犯罪者は、極めて高度な専門技術を持ち、非常に活動的です。また、予防的な安全対策を取っており、発見されるや戦術を変更し、痕跡を消していました。Luukに関する調査は、関係する銀行と然るべき警察機関に報告していますが、現在も継続中です。

6月末には、2013年前半に確認された「MiniDuke」と呼ばれる標的型攻撃が再び活発化しました。当初の攻撃には、いくつか際立った特徴がありました。たとえば、「昔ながらの」アセンブラ言語で書かれたカスタムバックドアが使用されていたことです。また、あまり一般的でないC&Cインフラストラクチャが攻撃の管理に使用されており、Twitterアカウントなど、複数の冗長パスが利用されていました。開発者は、更新された実行可能ファイルをGIFファイルの内部に隠して転送していました。

今回の「CosmicDuke」または「TinyBaron」と呼ばれる攻撃の標的は、政府、外交機関、エネルギー企業、軍、通信事業者などです。ただ、ステロイドやホルモンといった違法薬物の流通と販売に関係する組織も標的とされている点が他の攻撃とは異なります。その理由は判然としませんが、カスタマイズ可能なバックドアが、いわゆる「合法スパイウェア」として販売されたか、地下市場で販売され、それを製薬業界の企業が互いをスパイするために購入した、といったことが考えられます。

Victim geography (Miniduke and CosmicDuke)

このマルウェアは、バックグラウンドで動作するように設計された人気アプリケーションになりすましており、ファイル情報やアイコンはおろか、ファイルサイズまで本物に似せて設定されています。バックドア自体は「BotGenStudio」を使用してコンパイルされたものです。BotGenStudioはカスタマイズ可能なフレームワークで、攻撃者はボットを構成する際に、これを使用してコンポーネントを有効化または無効化します。このマルウェアは特定の拡張子を持つファイルを盗むだけでなく、パスワード、履歴、ネットワーク情報、アドレス帳、画面に表示される情報（5分おきにス

クリーンショットを撮影）など、他の機密データも収集します。各標的に一意のIDが割り当てられるため、固有のアップデートをそれぞれの標的に送り付けることができます。

このマルウェアは、難読化されたカスタムのローダーで保護されており、CPUリソースを3～5分間大量に消費してからペイロードに実行ファイルを渡すため、解析が困難です。また、セキュリティソフトウェアがマルウェアの実行をエミュレートするために必要なリソースまで消費します。独自の難読化ツールに加えて、RC4およびLZRWアルゴリズムに基づく暗号化と圧縮を多用します。実装は標準のバージョンとわずかに異なりますが、これはリサーチャーを欺くために故意に行われていると思われます。マルウェアの内部構成は、暗号化、圧縮、シリアライズが施され、複雑なレジストリのような構造となっており、文字列、整数、内部参照などさまざまなタイプのレコードがあります。盗んだデータは小さなチャンク（約3KB）に分割されて、圧縮、暗号化され、コンテナーに入れられてC&Cサーバーにアップロードされます。大容量のファイルは、数百のコンテナーに分けられて、個別にアップロードされる場合もあります。これらのデータチャンクは、攻撃者の側で解析、復号化、アンパック、抽出、再構築が行われるものと見られます。この方法ではオーバーヘッドが発生するものの、複数の処理工程が追加されるため、元のデータまで辿りつけるリサーチャーはほとんどいません。また、ネットワークエラーに対する耐性を強化するものでもあります。

7月には「Crouching Yeti」と呼ばれる標的型攻撃についての詳細な分析を公開しました。CrowdStrikeのリサーチャーが攻撃元はロシアであるという可能性を示唆したため、「Energetic Bear」とも呼ばれますが、弊社はそれを裏付ける十分な証拠があるとは考えていません。この活動は2010年後半から続いており、これまでに標的となった業種には、工業/機械、製造、製薬、建築、教育、ITなどがあります。現在までに世界各国で2,800以上の標的が確認されており、弊社は101の標的組織を特定しました。大部分は米国、スペイン、日本、ドイツ、フランス、イタリア、トルコ、アイルランド、ポーランド、中国の組織です。

Crouching Yetiの背後にいる攻撃者は、さまざまなマルウェア（いずれもWindowsベースのシステムに感染）を使用して標的組織に侵入し、組織内部で活動範囲を拡大して、機密データ（知的財産などの戦略的な情報）を盗み出します。使用されるマルウェアには特別なモジュールが含まれており、特定の産業のIT環境からデータを収集します。感染したコンピューターは、ハッキングされたWebサイトで構成される大規模なネットワークに接続されます。このWebサイトはマルウェアモジュールをホスティングし、標的に関する情報を格納しているほか、感染したシステムにコマンドを送信します。攻撃者が標的を感染させる手口は、悪意あるDLLファイルを忍ばせて再パッケージした正規ソフトウェアのインストーラー、スピア型フィッシングメール、水飲み場型攻撃の3つです。

ITは私たちの生活に欠かせないものになりました。そのため、世界各地の紛争にサイバーの側面が見られることは当然と言えます。特に、地政学的な紛争が近年激化している中東で、この傾向が見られます。弊社は8月、2013年前半から続く、シリアでのマルウェア活動の増加を報告しました。こうした攻撃の標的はシリアだけでなく、トルコ、サウジアラビア、レバノン、パレスチナ、アラブ首長国連邦、イスラエル、モロッコ、フランス、米国でもマルウェアは確認されています。弊社は攻撃者のC&Cサーバーを、シリア、ロシア、レバノン、米国、ブラジルのIPアドレスまで追跡することができました。全体で、この攻撃に関連する110のファイル、20のドメイン、47のIPアドレスを発見しています。

攻撃に関わる集団が、統制の取れた組織であることは明白です。これまでのところは、マルウェアを独自に開発するのではなく、実証されたマルウェアツールを使用しています（ただし、単純なシグネチャベースの検知を回避するために、さまざまな難読化の手口を使用しています）。しかし、この地域で使用されるマルウェアは今後増加する可能性が高く、完成度も高まっていく傾向にあると見られます。

11月には「Darkhotel」APTに関する分析を公開しました。10年近くにわたり続いていた活動で、世界中の何千もの標的を攻撃していました。感染の90%は日本、台湾、中国、ロシア、香港で発生していますが、ドイツ、米国、インドネシア、インド、アイルランドでも感染が確認されています。

Darkhotelでは標的によってさまざまな手法が使用されています。第1に、スピア型フィッシングメールやゼロデイエクスプロイトによって、防衛産業基盤（DIB）、政府機関、非政府組織（NGO）など、さまざまな組織に侵入します。第2に、日本のP2P（ピアツーピア）ファイル共有サイトからマルウェアを無差別に拡散します。第3に、海外出張で多数の国のホテルに宿泊する企業の重役に狙いを定め、2段階の感染プロセスを実行します。攻撃者はまず標的の身元を特定してから、さらに重要度の高い標的のコンピューターに別のマルウェアをダウンロードし、機密データを盗みます。

家庭やその他の脆弱性

パッチが適用されていない脆弱性を利用する手口は、今もなお、標的のコンピューターに悪意あるコードをインストールする際に使用されています。こうした攻撃では、一般的なソフトウェアに脆弱性が存在し、個人や企業がアプリケーションにパッチを適用していないことが前提になります。

今年は、幅広く普及している2つのオープンソースプロトコルに脆弱性が発見され、それぞれ「Heartbleed」「Shellshock」と名付けられました。HeartbleedはOpenSSL暗号化プロトコルの欠陥であり、脆弱なバージョンを使用するシステム上でメモリの内容を読み取り、個人情報を窃取することが可能となります。OpenSSLはインターネットベースの通信（Web、メール、インスタントメッセージ、仮想プライベートネットワーク（VPN）など）の保護に広く使われているため、この脆弱性は極めて広い範囲に影響する可能性がありました。個人情報の漏えいのリスクが懸念される場合によくあることですが、各方面でパスワードを変更しようとする動きが見られました。当然ながら、オンラインプロバイダーがOpenSSLにパッチを適用するための対策を講じ、自社のシステムを保護しなければ、パスワードを変更しても効果はありません。新しいパスワードも、脆弱性を悪用しようとする攻撃者のリスクにさらされるだけです。発覚の2か月後、弊社はこの脆弱性の影響についての展望を発表しました。

情報セキュリティ業界は9月、Shellshock脆弱性（別名Bash）の発見を受けて、非常事態に直面しました。攻撃者はこの脆弱性を利用して、Bashコマンドインタープリターの起動時に呼び出される変数に、リモートから悪意あるファイルを追加することが可能になります（BashはLinuxとMac OS Xの既定のシェル）。この脆弱性は影響が大きく、エクスプロイトを容易に実行できることもあって、深刻な懸念が生じました。Heartbleedに並ぶものと評価する人も少なくありません。しかし、メモリからデータが盗まれるだけのHeartbleedと異なり、Shellshockを悪用すると、システムを完全に制御できます。攻撃者がこの脆弱性を利用しようとするまでに時間はかかりませんでした。弊社は発見の直後に、初期のサンプルをいくつかの話題で取り上げています。攻撃者がリモートから攻撃したWebサーバーのほとんどは、Bashで書かれているか、シェルスクリプトに値を渡すCGIスクリプトをホスティングするものでした。ただし、この脆弱性がWindowsベースのインフラストラクチャに影響を及ぼす可能性も残っています。不幸にして、この問題はWebサーバーだけに限定されるものではありません。Bashは、いまや日常生活の一部となったデバイスのファームウェアに広く使われています。ルーター、電化製品、ワイヤレスアクセスポイントなどがこれに当たりますが、中にはパッチの適用が困難なデバイスや、不可能なデバイスもあります。

インターネットは生活の一部に溶け込んでいます。文字どおり、日常的に利用する製品にネットワーク接続機能が埋め込まれていることもあります。この「Internet of Things:モノのインターネット」と呼ばれるトレンドは注目度がますます高まっており、遠い未来の技術のように思えたとしても、実際には想像以上に身近なものになっています。現代の多くの家庭では、従来型のコンピューター以外にも、ローカルネットワークに接続されるデバイスが使用されています。たとえば、スマートテレビ、プリンター、ゲーム機、ネットワーク接続ストレージ（NAS）デバイス、何らかのメディアプレーヤー、衛星受信機などです。

弊社のセキュリティリサーチャーの1人が、自宅のサイバーセキュリティが本当に万全かどうかを調査しました。NAS、スマートテレビ、ルーター、衛星受信機など、いくつかの電化製品について、攻撃に対して脆弱かどうか調べました。その結果は衝撃的でした。NASに14、スマートテレビに1つの脆弱性が見つかったほか、ルーターには遠隔制御が可能になる機能がいくつか隠されていました。詳細についてはこちらでご覧いただけます。ネットワークデバイスの使用には潜在的なリスクがつきまとうことを、誰もが理解することが重要です。これは個人にも企業にも当てはまります。また、強力なパスワードを設定し、悪意あるコードを防ぐソフトウェアを実行しているからといって、情報が安全とは限らないことを理解する必要があります。自分で制御できないものは数多くあり、情報の安全はある程度まで、ソフトウェアベンダーやハードウェアベンダー次第という部分もあります。たとえば、すべてのデバイスに自動でアップデートをチェックする機能が搭載されているわけではありません。消費者が新しいファームウェアのダウンロードとインストールを求められることもあります。これは必ずしも簡単な作業でありません。さらに悪いことに、デバイスのアップデートが常に可能とは限りません（この調査で対象となったデバイスの大半は、1年以上前に生産中止になっていました）。

3

モバイルマルウェアが引き続き爆発的に増加

近年、モバイルマルウェアの数は劇的に増大しました。2004年～2013年の期間に解析されたモバイルマルウェアのコードサンプルは、約200,000でしたが、2014年だけで新たに295,539のサンプルが解析されています。しかし、これがすべてではありません。コードサンプルは再利用され、パッケージしなおされます。2014年には、4,643,582のモバイルマルウェアインストールパックが確認されました（2004年～2013年に確認された10,000,000のインストールパックとは別です）。1か月あたりのモバイルマルウェア攻撃の数は10倍に増加しました。2013年8月は1か月に69,000件でしたが、2014年3月は644,000件となっています（2014年10月の『Mobile Cyber Threats, Kaspersky Lab and INTERPOL Joint Report』をご覧ください）。

今では、検知されたモバイルマルウェアの53%が、金銭を盗むマルウェアに関連しています。顕著な例の1つが、ロシアの大手銀行3行の顧客から金銭を盗んでいたSpvengです。このトロイの木馬は、顧客がオンラインバンキングアプリを開くまで待機し、それを独自のアプリに置き換えて、顧客の詳細なログイン情報を入手しようとします。また、Google Playアプリに重ねて独自のウィンドウを表示し、クレジットカード情報を入力するよう求めることによって、カードデータの窃盗を試みます。別の例にはWallerがあります。これは一般的なSMS型トロイの木馬と同様に動作するとともに、感染したデバイスのQIWIウォレットから金銭を盗み出します。

サイバー犯罪者は、デスクトップやラップトップで確立された手法を用いて、標的から金銭を盗む手段を多様化してきました。その1つにランサムウェア型トロイの木馬があります。確立された手法がモバイルデバイスに応用される例としては偽のアンチウイルスアプリもあります。また、今年は、Torネットワークにホスティングされたc&cサーバーを介して管理されるトロイの木馬が初めて出現しました。Torecバックドアは、広く普及しているTorクライアントOrbotを改変したものです。もちろん、犯罪者にとっての利点はc&cサーバーをシャットダウンできないことです。

最近まで、iOSを標的とするマルウェアの大半は、「脱獄した」デバイスを利用するものでした。

しかし、先ごろ確認された「WireLurker」マルウェアは、iOSといえども攻撃を免れないことを示しています。

いまやモバイルデバイスは生活の一部となっているため、モバイルマルウェアの開発が、マルウェア作成者、テスター、アプリデザイナー、Web開発者、ボットネット管理者などを包含するサイバー犯罪ビジネスによって支えられているのは、意外なことではありません。

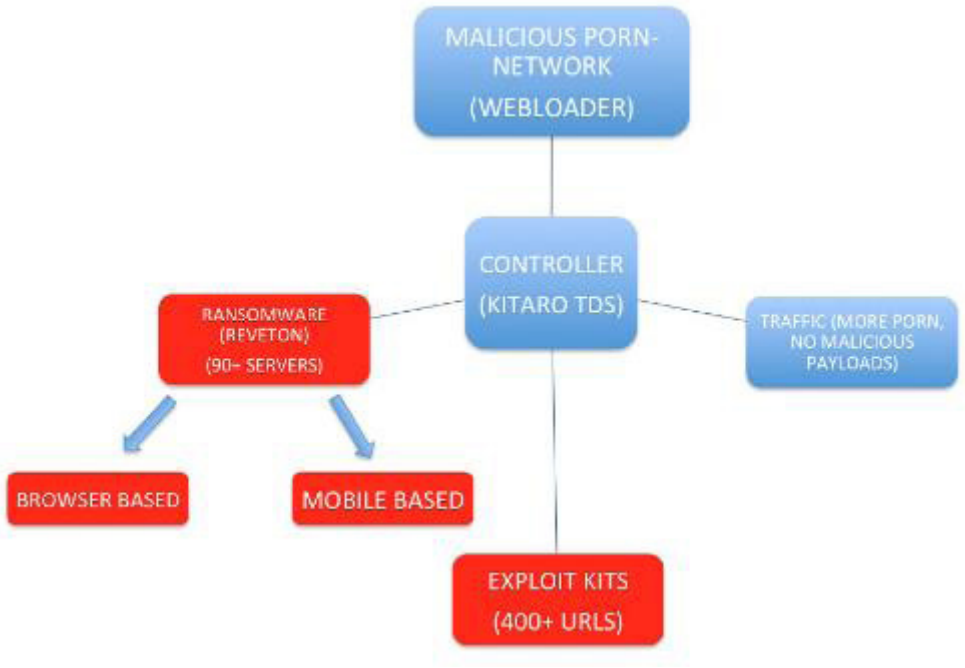
金銭かファイルか

ランサムウェアプログラムはこの数年で増加しています。標的のコンピューターへのアクセスをブロックして、通常のアクセスに戻す代わりに身代金の支払いを要求するだけのランサムウェアもありますが、さらに進んで、コンピューター上のデータを暗号化するものも数多くあります。最近の例としては「ZeroLocker」があります。ZeroLockerは標的のコンピューターのほぼすべてのファイルを暗号化し、暗号化したファイルに拡張子「.encrypt」を追加します（ただし、「Windows」「WINDOWS」「Program Files」「ZeroLocker」「Destroy」という単語を含むディレクトリにあるファイルや、サイズが20MBを超えるファイルは暗号化されません）。ファイルの暗号化には160ビットAES鍵が使用されます。暗号化が完了すると、「cipher.exe」ユーティリティが実行され、すべての未使用データがドライブから削除されます。この2つの機能のために、ファイルの復元は非常に困難になります。ZeroLockerを操るサイバー犯罪者は、ファイルの復号化と引き替えに、まず300ドル相当のBitcoinを要求します。すぐに支払わなかった場合、時間が経つにつれて、要求額が500ドル、1,000ドルと増えていきます。

Kaspersky Labが今年解析したランサムウェアプログラムには、Onionもあります。このトロイの木馬はTorネットワークを使用してC&Cサーバーを隠蔽するだけでなく、標的ユーザーによる入力がなくても、Torとの完全なインタラクションが可能となっています。類似の他のプログラムは、Torネットワークと通信するために、（場合によっては他のプロセスにコードを埋め込むことによって）正規の「tor.exe」ファイルを起動します。対照的に、Onionはこの通信をマルウェアコード自体の一部として実行します。Onionには特殊な暗号化アルゴリズムも使用されており、C&Cサーバーとの通信が傍受された場合でも、ファイルを復号化することはできません。このトロイの木馬は、非対称暗号化だけでなく、ECDH（楕円曲線ディフィー・ヘルマン鍵共有）と呼ばれる暗号プロトコルも使用します。そのため、マスター秘密鍵を使用しない限り復号化は不可能ですが、サイバー犯罪者が制御するサーバーの外部にこの鍵が出ることはありません。

今年は、ランサムウェアプログラムを使用した攻撃が、Android搭載デバイスにまで拡大しました。たとえば、2014年前半に発見されたSvpengの最初のバージョンは、スマートフォンをブロックし、児童ポルノを見ていたと言いがかりをつけ、ロック解除に500ドルの「罰金」を要求します。このマルウェアの改変版（2014年6月に発見）は、デバイスを完全にロックするため、「オフ」ボタンを長押ししなければ電源を切ることができません。しかし、もう一度デバイスの電源を入れると、トロイの木馬がすぐに再ロードされます。主に米国のユーザーを攻撃していましたが、英国、スイス、ドイツ、インド、ロシアでも被害が確認されました。このバージョンはスマートフォンのロック解除に200ドル、支払いにはMoneyPakバウチャーを使用するよう要求します。身代金を要求する画面には、デバイスの前面カメラで撮影されたユーザーの写真が表示されます。2014年5月に発見された「Koler」というトロイの木馬も同じ手口を使用しており、デバイスへのアクセスをブロックし、解除と引き替えに100～

300ドルの身代金の支払いを要求します。Svpengと同様、警察を名乗ってメッセージを表示するトロイの木馬で、世界の30以上の国のユーザーに各国の「警察」のメッセージを送りつけています。



Kolerの拡散インフラストラクチャ

データを暗号化する初のAndroidトロイの木馬「Pletor」が、2014年5月に出現しました。このトロイの木馬は、AES暗号化アルゴリズムを使用してスマートフォンのメモリカードのコンテンツを暗号化し、画面に身代金の要求を表示します。身代金は、ユーザーのQIWI Visaウォレット、MoneXy、電話番号への標準的な送金手段を使用して支払うよう要求されます。主な標的はロシアとウクライナのユーザーで（ただし、他の旧ソ連諸国の標的も確認されています）、300ドル相当の金額をルーブルまたはグリブナ（ウクライナの通貨単位）で要求します。

ランサムウェアは標的ユーザーが金銭を支払うことを前提としています。しかし、お金を払ってはいけません。そのかわり、データを定期的にバックアップしておけば、ランサムウェアの被害に遭っても（またはハードウェアが故障してファイルにアクセスできなくなっても）、データを失うことはありません。

5

ATMから現金を盗むマルウェア

ATM用のマルウェアは目新しいものではありません。この種のマルウェア「Skimer」は、2009年に初めて発見されています。その標的は、WindowsベースのOSが稼働する東欧のATMでした。Skimerは文書化されていない機能を使用して、感染マシンに挿入されたカードの詳細を出力し、マスターカードコマンドを使用して現金カセットを開いていました。ATMマルウェアは他にも2010年にブラジルで確認されています。この「SPSniffer」は、強固な暗号で保護されていない暗証番号入力パッドを使用する旧型のATMから、暗証番号を収集していました。また、昨年発見された新たなATMマルウェアファミリー「Atmer」は、メキシコのATMから現金を盗むものでした。

Kaspersky Labは今年、ある金融機関からの要請を受けて、アジア、欧州、中南米におけるATMへの新たな攻撃に関して、フォレンジック調査を実施しました。この攻撃は2つの段階で実行されていました。サイバー犯罪者はATMに物理的に近づき、ブータブルCDを使用して「Tyupkin」というマルウェアをインストールします。続いてマシンを再起動してマルウェアをロードし、ATMを制御下に置きます。次にマルウェアが無限ループで実行され、コマンドを待機します。

犯行の発覚を防ぐため、マルウェアは日曜日と月曜日の夜の特定の時刻にのみコマンドを受け入れます。攻撃者はATMのキーボードで数字の組み合わせを入力し、マルウェアのオペレーターに電話をかけ、さらに別の数字の組み合わせを入力して、ATMから出てくる現金を回収します。

感染したATMの監視カメラのビデオ映像に、ATMから現金を引き出す手口が映っていました。数字の組み合わせキーは乱数に基づいてセッションごとに生成されるため、犯罪者集団のメンバー以外の人物が、偶然現金を手にすることはありません。アルゴリズムを知っており、表示される数字に基づいてセッションキーを生成できる別のメンバーが、オペレーターに電話で指示を出します。これは、回収担当のメンバーが1人で現金を盗めないようにするためです。正しいキーが入力されると、各現金カセットに保管されている金額がATMに表示され、オペレーターがどのカセットから奪うかを選択します。これで、選択されたカセットから一度に40枚の紙幣が引き出されます。

近年ATMに対する攻撃が急増しているのは、自然な流れと言えます。物理的にスキミング装置を取り付けたATMでカードのデータを読み取る手口は以前からありますが、ATMに対する攻撃は、この手口をさらに発展させたものです。残念ながら、既知の脆弱性を抱えるOSが多くのATMで稼働しています。そのため、物理的なセキュリティがいっそう重要になります。Kaspersky Labはすべての銀行に対し、ATMの物理面のセキュリティを見直すよう呼びかけています。

忘れ去られても使用が続くWindows XP

Windows XPのサポートは4月8日に終了しました。これは、新しいセキュリティ更新もホットフィックスも提供されず、無償有償を問わずサポートオプションも終了し、オンライン技術文書の更新もないことを意味します。しかし、今も多くの人がWindows XPを使用しています。弊社のデータでは、感染の原因の約18%がWindows XPであることを示しています。セキュリティパッチの提供が終了した今、多くのユーザーが攻撃に対して無防備になっているということです。4月以降に発見されたほぼすべての脆弱性はゼロデイ脆弱性、つまりパッチが作成されていない脆弱性でした。アプリケーションベンダーがWindows XP向け更新プログラムの開発を終了するなか、この問題はさらに深刻化するでしょう。パッチ未適用のアプリケーションが別の侵入口となり、攻撃対象範囲がさらに拡大する恐れがあります。この流れはすでに始まっており、Javaの最新版ではWindows XPがサポートされていません。

新しいOSへのアップグレードが、シンプルで明白な解決策のように思えます。しかし、Microsoftがサポート終了の予告に力を入れていたとはいえ、一部の企業にとって新OSへの移行が困難である理由は容易に理解できます。切り替えの費用以外に、新しいハードウェアへの投資が必要になることもあり、さらには、新しいOSでは動作しない自社専用のカスタムアプリケーションの変更が必要になる場合もあります。そのため、一部の組織がXPのサポート継続に料金を支払っていることも当然といえます。

もちろん、アンチウイルス製品によって保護することはできるでしょう。ただし、ここで言う「アンチウイルス」とは、総合的なインターネットセキュリティ製品のことです。プロアクティブ技術によって、新しい未知の脅威を防げる製品でなければ意味はありません。特に、エクスプロイトの使用に対処できる機能が重要です。シグネチャによって既知のマルウェアをスキャンするといった程度の機能しかない簡単なアンチウイルス製品では不十分です。また、セキュリティベンダーが今後開発する保護技術は、いずれWindows XPに対応しなくなるでしょう。

現在もWindows XPを使用しているユーザーは、移行戦略を決定するまでの暫定措置と考える必要があります。多数のユーザーがWindows XPを使い続けている限り、間違いなくマルウェア作成者の標的となります。パッチ未適用のOSの方が、犯罪者にとってチャンスがはるかに大きいからです。ネットワーク上のWindows XPベースのコンピューターは、企業に対する標的型攻撃に利用される可能性があり、弱点となります。犯罪者はこうしたコンピューターを足がかりに、より広いネットワークへの侵入を試みます。

当然ながら、個人にとっても企業にとっても、新しいOSへの移行には不便が伴い、費用もかかります。しかし、危険が増大する一方のOSを使用するリスクは、不便さと費用を上回るはずです。

オニオンの皮に隠れて

Tor(The Onion Routerの略)は、インターネットにアクセスするユーザーが匿名性を確保するためのソフトウェアです。Torが登場してしばらく経ちますが、長年にわたり、専門家や熱心な愛好家を中心に使用されていました。しかし、主にプライバシーに関する懸念の増大から、Torネットワークの利用が今年急増しました。Torは、何らかの理由で監視と機密情報の漏えいを恐れる人々にとって、有益なソリューションとなっています。その一方で、Torの匿名性がサイバー犯罪者にとっても魅力的であるという事実が、弊社の調査から明らかになりました。

Torを積極的に利用して悪意あるインフラストラクチャをホスティングするサイバー犯罪者は、2013年に出現しました。マルウェアに加え、C&Cサーバーや管理パネルなど、関連するリソースが数多く発見されています。Torネットワークにサーバーをホスティングするサイバー犯罪者を特定し、ブラックリストに登録し、排除することは困難です。マルウェアや盗まれた個人情報の売買が行われるTorベースの地下市場も存在します。通常、こうした市場では、追跡を逃れるためにBitcoinで支払いが行われます。サイバー犯罪者はTorを利用することで、マルウェアの活動の隠蔽、サイバー犯罪サービスの取引、違法に得た利益のマネーロンダリングを行っています。

Kaspersky Labは7月、新たな方法でTorを利用したランサムウェア型トロイの木馬、「Onion」の解析結果を公開しました。

Androidベースのマルウェアの開発者も、Torを使用するようになりました。人気のTorクライアントOrbotのマルウェアバージョンであるTorecというトロイの木馬は、.onion疑似ゾーン内のドメインをC&Cサーバーとして使用します。ランサムウェア型トロイの木馬Pletorの一部の亜種でも、詐欺を管理するサイバー犯罪者との通信にTorネットワークが使用されています。

Torを使用しても、サイバー犯罪者が罰から逃れられるとは限りません。このことは、先ごろ世界の警察機関が多数のTorベースのサイバー犯罪サービスに対して実行した「Onymous作戦」によって証明されました。

作戦に参加した警察機関は、どのようにして「侵入不可能」とされるネットワークを攻略できたのでしょうか。少なくとも理論的には、誰かが訪問する隠しサービスを支えるWebサーバーの物理的な場所を知る方法はありません。しかし、こちらで紹介したように、Torアーキテクチャそのものを攻撃せずに、隠しサービスを攻略する方法は存在します。Torベースのサービスが安全でいられるのは、正しく設定され、脆弱性や設定エラーがなく、Webアプリケーションにいかなる欠陥もない場合だけです。

8

善きもの、悪しきもの、そして醜きもの

残念ながら、ソフトウェアを善いプログラムと悪いプログラムに明確に分けることはできません。正当な目的で開発されたソフトウェアが、サイバー犯罪者によって悪用されるリスクは常に存在します。2月のKaspersky Security Analyst Summit 2014では、一般的なラップトップと一部のデスクトップコンピューターのファームウェアに、盗難対策技術の不適切な実装が存在し、これがサイバー犯罪者の強力な武器になりかねないことを説明しました。調査のきっかけはKaspersky Lab社員の私用ラップトップでした。Absolute Softwareが開発したComputraceソフトウェアのモジュールの不安定性に関連して、システムプロセスが何度もクラッシュしていたのです。この社員はComputraceをインストールしておらず、ラップトップ内に存在することさえ知りませんでした。この点から懸念が生じます。Absolute Softwareのホワイトペーパーによれば、インストールはコンピューターの所有者または同社のITサービスによって行われるからです。さらに、コンピューターにプレインストールされたソフトウェアの大半は、ユーザーが永久に削除または無効化できますが、Computraceは、専門家によるシステムのクリーンアップやハードディスク交換の後にも残るように設計されています。また、弊社のリサーチャー数名のコンピューターと一部の企業コンピューターでも、Computraceソフトウェアが実行されていることを示す類似の徴候が見られたため、これを単に一回限りの事象として片付けることはできませんでした。結果として、詳細な分析を実行することになりました。

Computraceを初めて調べたとき、現在のマルウェアでよく使われるトリックを数多く使用しているため、誤って、悪意あるソフトウェアだと考えました。実際、過去には、このソフトウェアはマルウェアとして検知されていましたが、現在では、大部分のアンチマルウェア企業がComputraceの実行可能ファイルをホワイトリストに登録しています。

弊社はComputraceが善意で開発されたソフトウェアであると考えています。しかし、弊社の調査が示すところでは、このソフトウェアに潜む脆弱性のために、サイバー犯罪者に悪用される恐れがあります。弊社の見解では、このような強力なツールには、強固な認証と暗号化を組み込む必要があります。分析対象となったコンピューターには、Computraceモジュールがひそかに有効化された証拠は見つかりませんでした。しかし、Computraceエージェントが有効になっているコンピューターが数多くあることは明白です。メーカーとAbsolute Softwareには、このことをユーザーに知らせ、使用を望まないユーザーには無効化する方法を説明する責任があると考えます。無効にしなければ、見捨てられたComputraceエージェントは気づかれずに実行され続け、リモートからエクスプロイトに利用される恐れがあります。

弊社は6月、イタリア企業HackingTeamが開発したRemote Control System（RCS）という「合法」ソフトウェアについての研究結果を発表しました。このソフトウェアには、C&Cサーバーの特定に使用できる機能が見つかりました。それによってIPv4空間の全体をスキャンし、世界各地のRCS C&Cサーバーのすべてのipアドレスを発見することができました。見つかったサーバーは計326台で、特に多かった国は米国、カザフスタン、エクアドルでした。一部のIPは「政府」関連機関のものであることが

WHOIS情報から判明しました。もちろん、特定の国にあるサーバーがその国の警察機関によって使用されている保証はありませんが、こう考えるとつじつまが合います。結局のところ、これは国家間の法的問題と、サーバーを他者に確保されるリスクを回避することになるのでしょう。また、HackingTeam社製の多数のモバイルマルウェアモジュールも発見されており、Android、iOS、Windows Mobile、BlackBerry向けのものがありました。いずれも同じタイプの構成を使用して制御されます。これは、互いに関連し、同じ製品ファミリーに属していることを示す有力な材料です。当然ながら、弊社が特に注目したのは、人気のプラットフォームであるAndroidとiOSに関連するバージョンでした。

モジュールはインフェクターを使用してインストールされます。インフェクターは、すでに感染したコンピューター上で稼働しているWindowsまたはMac OS用の特別な実行可能ファイルです。iOS用のモジュールは「脱獄した」デバイスだけをサポートします。これは感染能力を限定しますが、RCSで使用されている感染方法からすると、デバイスがロックされていなければ、接続先の感染コンピューターから、脱獄ツール（EvasiOnなど）を実行できる可能性があります。このiOSモジュールには、デバイス上のデータ（メール、連絡先、通話履歴、キャッシュされたWebページなど）にアクセスする機能のほか、ひそかにマイクを起動する機能や、カメラで通常の撮影を行う機能があります。これにより、標的のコンピューター内とその周辺で、環境全体を完全に制御することが可能になります。

AndroidモジュールはDexGuardオプティマイザー/難読化ツールによって保護されているため、解析は難航しました。しかし、Androidモジュールの機能がiOSモジュールの機能と一致しており、以下のアプリケーションから情報を乗っ取るためのサポートも追加されていると判断できました。「com.tencent.mm」「com,google,android,gm」「android,calendar」「com,facebook」「jp,naver,line,android」「com,google.android,talk」

この新しいデータは、こうした監視ツールの洗練度を強調するものでした。そのようなツールに関する弊社のポリシーは非常に明確です。弊社は起源や目的に関係なく、あらゆるマルウェア攻撃を検知し、修復に努めます。弊社にとっては「正しい」マルウェアも「悪い」マルウェアもありません。いわゆる「合法」スパイウェアのリスクについては、過去に公式の警告を発表しました。これらの監視ツールが悪の手に落ちないことが重要です。だからこそ、ITセキュリティ業界はマルウェアの検知に例外を作ることができないのです。

プライバシーとセキュリティ

プライバシーとセキュリティの緊張関係は今なお続いており、さまざまなニュースで取り上げられています。

今年も例年どおり多数のセキュリティ侵害が発生しました。その中で特に注目を集めた事件が、さまざまなハリウッドセレブの露骨な写真が盗まれて公開された事件だったことは、さほど意外ではありません。このニュースによって、プロバイダーと個人の両方が、オンラインに保存されたデータを保護する上での責任について注目が集まりました。写真の窃盗はiCloudのセキュリティの抜け穴により可能になったと見られます。「iPhoneを探す」のインターフェイスには、パスワードの試行回数に制限がなかったため、パスワードを総当たり攻撃で特定することが可能になっていました。Appleはすぐにこの抜け穴を塞いでいます。しかし、標的が脆弱なパスワードを使用していなければ、攻撃は不可能だったでしょう。現代人はオンラインで過ごす時間が増えています。しかし、多くの人は、個人情報をオンラインに保存することの意味を考えません。クラウドサービスのセキュリティはプロバイダー次第です。私たちはデータをサードパーティサービスに預けた瞬間に、データの管理権の一部を自動的に失うことになります。クラウドに保存するデータを入念に選択し、どのデータをデバイスからクラウドに自動的に転送するかを決定することが重要です。

パスワードの問題は引き続き発生しています。あまりに簡単に推測できるパスワードを選べば、なりすましの脅威に対して無防備になってしまいます。複数のオンラインアカウントで同じパスワードを使い回すと、さらに深刻な問題が発生します。1つのアカウントが乗っ取られると、すべてが危険にさらされます。そのため、Apple、Google、Microsoftなど、多くのプロバイダーが2段階認証を導入しました。2段階認証では、ユーザーがサイトにアクセスする際や、アカウントの設定を変更する際に、ハードウェアトークンによって生成されるコードか、モバイルデバイスに送信されるコードの入力が求められます。確かに2段階認証はセキュリティを強化しますが、それは任意で使用する場合ではなく、必須で使用する場合だけです。

セキュリティと使いやすさには常にトレードオフがあります。それらを両立する取り組みとして、Twitterは先ごろDigitsサービスを開始しました。アプリにサインインするために、ユーザー名とパスワードの組み合わせを作成する必要はもうありません。電話番号を入力するだけでよいというサービスです。ユーザーは各トランザクションを確認するワンタイムパスコードを受信し、このコードがアプリによって自動的に読み取られます。Twitterは事実上の仲介役となり、アプリプロバイダーに代わってユーザーの身元を確認します。これにはいくつかメリットがあります。消費者はもはや、アプリプロバイダーのアカウントを設定するためにログインとパスワードの組み合わせを作成する必要はありません。メールアドレスも不要です。開発者は、ログインを検証するための独自のフレームワークを作成する必要がなくなります。メールを使用しない潜在顧客を失うこともないでしょう。Twitterはユーザーの関心事項を把握しやすくなります。また、アプリプロバイダーのサーバーにパスワードが保存されないことも利点です。アプリプロバイダーのサーバーに不正アクセスがあっても、顧客の個人情報が盗まれることはありません。ただし、デバイスの紛

失や盗難があった場合も番号の検証は機能し続けるため、デバイスに触ることができれば誰でも本来の所有者と同じ方法でアプリにアクセスできてしまいます。それでも、従来のユーザー名とパスワードの方法と比較して、セキュリティ面で後退したことにはなりません。今のところ、モバイルアプリを実行するたびにログインが強制されるわけではないため、スマートフォンを盗まれた場合に、暗証番号、パスコード、指紋を設定していなければ、メール、SNS、アプリなど、すべてにアクセスされてしまいます。言い換えると、セキュリティは、デバイス自体へのアクセスに使用される暗証番号、パスコード、指紋という単一障害点に依存しているのです。

プライバシーに関する懸念の増大を受けて、「pwnedlist.com」Webサイトの開発者は、メールアドレスとパスワードが盗まれてオンラインで公開されているかどうかを確認できる使いやすいインターフェイスを作成しました。今年はそれが有料サービスになりました。

AppleとGoogleは、プライバシー情報の流出に関する懸念への対応として、iOSデバイスとAndroidデバイスのデータの既定での暗号化を有効にしました。しかし、一部の警察機関は、この対策によって検知の回避が容易になり、サイバー犯罪者を利することになると考えています。

10

警察機関の国際協力の成果

一般ユーザーのオンラインでの活動の増加を背景に、サイバー犯罪は日常生活と切り離せないものになっています。サイバー犯罪者は罰を受けることなく活動しているというイメージを持たれがちですが、警察機関の対処は犯罪者の活動に重大な影響を及ぼします。サイバー犯罪のグローバルな性質を考えると、国際協力は極めて重要です。今年は警察が大きな成功を収めています。

2014年6月、英国のNCA（国家犯罪対策庁）や米国のFBIをはじめ、複数の国の警察機関が参加した作戦により、「GameoverZeus」ボットネットを管理する世界規模のコンピューターネットワークが閉鎖されました。この「Tovar作戦」では、ボットネットの基盤となる通信を遮断し、サイバー犯罪者が制御できないようにしました。GameoverZeusは、当時稼動していたボットネットとしては最大級の規模を誇り、バンキング型トロイの木馬Zeusのコードをベースとしていました。このボットネットは、コンピューターをトロイの木馬Zeusに感染させ、オンラインメールアカウント、SNS、オンラインバンキング、その他のオンラインバンキングサービスのログイン情報を盗んでいたほか、「Cryptolocker」ランサムウェアを拡散していました。この警察の作戦により、標的ユーザーは時間の余裕ができ、コンピューターから不要なものを削除することができました。

Kaspersky Labは今年、警察機関と業界組織の共同作戦に貢献しました。これはNCAが指揮を取ったもので、トロイの木馬「Shylock」の背後にあるインフラストラクチャを破壊しました。バンキング型トロイの木馬Shylockは、シェイクスピアの『ヴェニスの商人』の抜粋がコードに含まれていたために命名されたもので、2011年に最初に発見されました。他の有名なバンキング型トロイの木馬と同様に、Shylockは「Man-in-the-Browser」攻撃であり、バンキングサービスのログイン情報を銀行の顧客のコンピューターから盗んでいました。このトロイの木馬は、標的となる世界各国の銀行が記載された設定済みのリストを使用します。

11月のOnymous作戦では、Torネットワーク内で運営されていた闇市場が閉鎖されました。

Securelist
Kaspersky Lab エキスパートの
テクニカルリサーチ、分析を主とした
ブログ

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

株式会社カスペルスキー
PR-1007-201501