KASPERSKY lab

Kaspersky Security Bulletin 2015

2015年 サイバー脅威の主要動向

GREAT

目次

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2015年の主な動向を総括します。

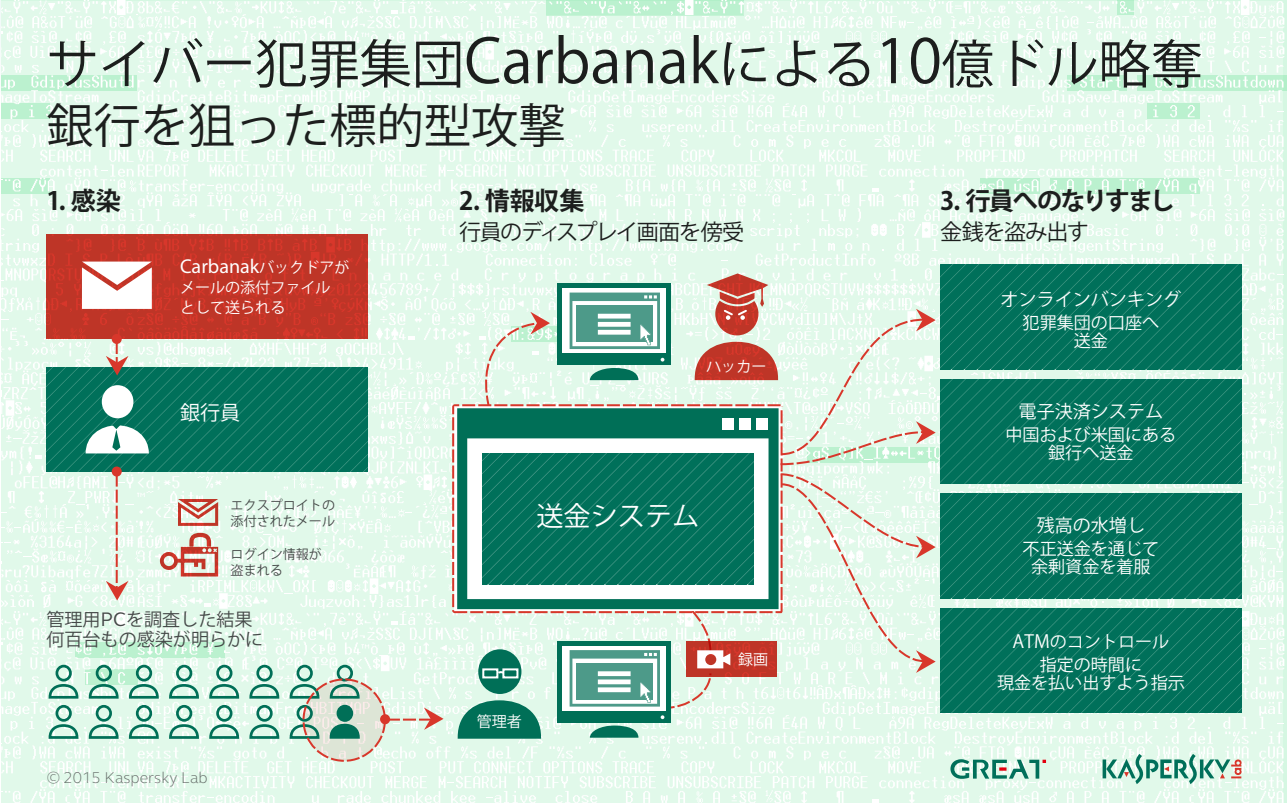
標的型攻撃とマルウェアの活動

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。Kaspersky Labが昨年発表した2015年のセキュリティ予測では、今後のAPTの進展について概要をまとめています。

- サイバー犯罪とAPTの融合
- 大規模なAPTグループの分裂
- マルウェア技術の進歩
- データ窃取の新たな手口
- APTの軍拡競争

弊社が今年報告した主なAPT活動について、以下にご紹介します。

Carbanakでは、サイバー犯罪（この事例では金融機関からの金銭窃取）と標的型攻撃に特有の侵入技術が融合されていました。この活動が発見されたのは2015年春です。ある銀行の一部のATMから現金が「無作為に」引き出されるようになったため、弊社に銀行システムのフォレンジック調査の依頼がありました。調査の結果、その銀行が感染していたことが判明します。Carbanakは、スパイ活動、データ窃取、感染コンピューターの遠隔操作を実行するバックドアです。攻撃者は標的への侵入にAPTの手法を用いていました。まず、銀行員にスピア型フィッシングメールを送信します。銀行のコンピューターにバックドアをインストールし、偵察活動によって処理、会計、ATMに関連するシステムを探し当てた後、正規の行員になりすまして活動します。Carbanakの金銭窃取の手口には、（1）ATMから現金を引き出す、（2）SWIFTネットワークを使ってサイバー犯罪者に送金する、（3）偽の口座を作成し、ミュール（出し子）に現金を回収させる、の3パターンがあります。およそ100の金融機関が標的となり、被害総額は約10億ドルに達しました。



2015年第1四半期に特に大きな話題となったのは、サイバースパイグループEquationに関するニュースでした。Equationの攻撃者は、イラン、ロシア、シリア、アフガニスタン、米国などで無数のコンピューターを感染させました。標的となった組織は、政府機関、外交機関、電気通信企業、エネルギー会社などです。Equationは史上最も高度なAPT活動の1つです。同グループは多数のモジュールを開発しており、その1つはハードドライブのファームウェアを改竄します。そのため、他の標的型攻撃よりも発見が困難で、長期にわたって活動が続きます。2001年以前にコードの開発が始まっていたことが明らかになっています。また、StuxnetやFlameといった悪名高い攻撃と繋がりがあり、たとえばEquationが悪用していた2件のゼロデイ脆弱性は、後にStuxnetでも利用されています。

Kaspersky Labが中東でのインシデントを調査していたとき、新たな標的型攻撃グループの活動を発見しました。Desert Falconsは、アラビア語話者による初の本格的サイバースパイ活動グループであり、中東地域の政治的状況と関連があるものとみられています。活動の最初の兆候は2011年に認められました。最初の感染は2013年でしたが、活動のピークは2014年後半から2015年初頭でした。同グループは3,000を超える標的から100万以上のファイルを窃取しています。標的は、主にパレスチナ、エジプト、イスラエル、ヨルダンの政治活動家、政治指導者、政府機関、軍事組織、マスコミ、金融機関でした。Desert Falconsグループのメンバーが熟練の攻撃者であることは間違いありません。WindowsやAndroid向けのマルウェアをゼロから新規に開発しているほか、フィッシングメール、偽のWebサイト、SNSアカウントを駆使した高度な攻撃を計画しています。

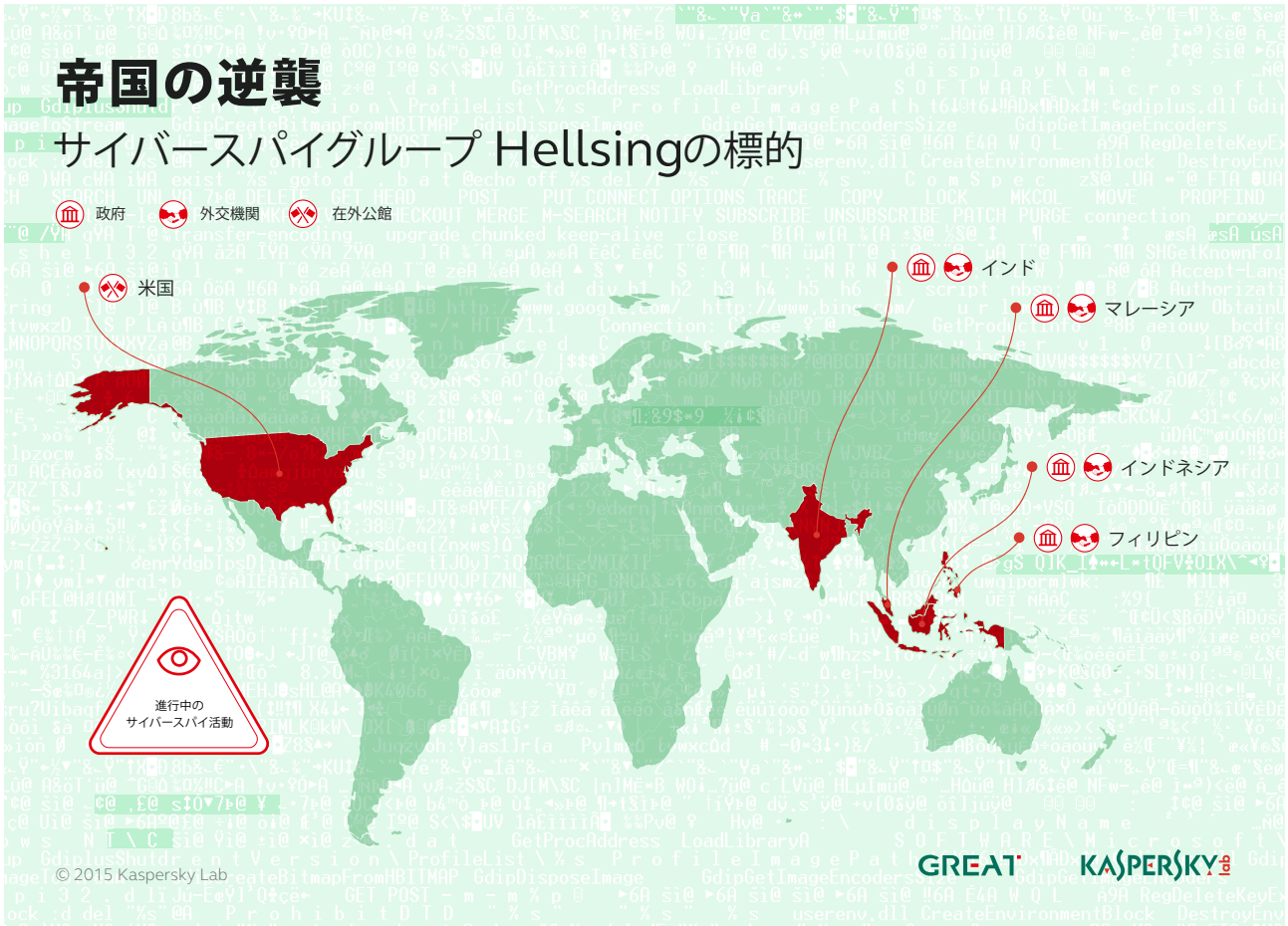
弊社がAnimal Farm APTに関するレポートを発表したのは2015年3月でしたが、この活動で使用されたツールに関する情報は、その前年から報道され始めていました。2014年3月、フランスのル・モンド紙は、カナダ通信安全保障部（CSEC）が発見したサイバースパイ活動用ツールセットに関する記事を掲載しました。このツールセットは、カナダ国内のフランス語メディアのほか、ギリシャ、フランス、ノルウェー、一部のアフリカ諸国を標的とした「Snowglobe」活動で使用されたものです。CSECは、フランスの諜報機関がこの作戦を開始した可能性があると考えていました。1年後、セキュリティリサーチャーは「Snowglobe」と共通点の多いマルウェアの解析結果（こちらとこちらとこちら）を発表しました。このリサーチで特筆すべきは、「Babar」のサンプルについて触れていたことです。「Babar」は内部の呼称であり、CSECが言及したプログラムと同じ名称です。これらのマルウェアの分析結果と、マルウェア間の関連性から、弊社は攻撃の背後にいるグループをAnimal Farm（動物飼育場）と命名しました。弊社は2014年、サイバー犯罪者に悪用されていた3件のゼロデイ脆弱性を発見しており、Animal Farmはそのうち2件を利用していました。たとえば、CVE-2014-0515エクスプロイトを使用してシリア法務省のWebサイトに侵入した攻撃では、Animal Farmの「Casper」というツールがダウンロードされていました。興味深いことに、同グループが使用するプログラムの1つ「NBOT」は、DDoS攻撃を実行するよう設計されており、これはAPTグループでは珍しいことです。この「飼育場」の悪意ある「動物」の1つには、「Tafacalou」という奇妙な名前がついており、これはおそらくオック語（フランスなどの一部地域で使われている言語）とみられています。

2015年4月には、拡大を続ける「Duke」ファミリーに新たなメンバーが加わったことを報告しました。このファミリーでは、すでにMiniDuke、CosmicDuke、OnionDukeなどが知られています。新メンバーのCozyDuke APT（別名「CozyBear」「CozyCat」「Office Monkeys」）は、米国、ドイツ、韓国、ウズベキスタンの政府組織や企業を標的としています。攻撃には高度な技術が多数使用されており、暗号化、検知対策機能のほか、「Duke」ファミリーの初期の脅威と構造的に類似する成熟したコンポーネントなどがあります。しかし、最も注目すべき特徴の1つはソーシャルエンジニアリングの利用です。CozyDukeの一部のスピア型フィッシングメールには、ハッキングされたWebサイト（中には知名度の高い正規サイトも）へのリンクが記載されており、そこにZIPアーカイブが置かれています。このアーカイブに潜むRAR SFXは、おとりとして空のPDFを表示している間にマルウェアをインストールします。また、偽のフラッシュ動画をメール添付で送りつけるという手口も使われています。よく知られた例（このマルウェアにつけられた別名の由来）が、「OfficeMonkeys LOL Video.zip」です。このファイルを実行すると、オフィスで働くサルの「楽しい」おとり動画が再生され、その間にCozyDuke実行可能ファイルがコンピューターにドロップされます。標的となった社員がこの面白い動画を同僚に転送し、オフィスのコンピューターが次々に感染していきます。CozyDukeをはじめ多数の標的型攻撃において、ソーシャルエンジニアリングで社員を欺き、企業セキュリティを危険にさらす行動に走らせる手口が成功しています。こうした現状から、社員教育をビジネスセキュリティ戦略の中心に据える必要性が浮き彫りになっています。

Naikon APTは、東南アジアと南シナ海沿岸地域の組織を主な標的としてきました。攻撃者は中国語話者のグループとみられており、活動期間は5年以上に及び、フィリピン、マレーシア、カンボジア、インドネシア、ベトナム、ミャンマー、シンガポール、ネパール、タイ、ラオス、中国の最高位の政府機関、民間団体、軍事組織を攻撃しています。標的型攻撃活動の例に漏れず、Naikonもソーシャルエンジニアリングを多用して標的組織の職員を欺き、マルウェアをインストールするように仕向けます。メインのモジュールはリモート管理ツールで、感染コンピューターを制御するための48種類のコマンドに対応しています。これらのコマンドには、システムファイルの完全なインベントリの取得、データ

のダウンロードとアップロード、アドオンモジュールのインストールを行うものや、キーロガーを使用して職員の認証情報を取得するものがあります。Naikonは標的国ごとにオペレーターを1人割り当て、その国の文化的特徴（個人のメールアカウントを業務に使用することが多い、など）をうまく利用していました。また、標的国内にある特定のプロキシサーバーを使用して、感染コンピューターへの接続を管理したり、攻撃者の指揮統制（C&C）サーバーにデータを転送したりしていました。メインのレポートとその続報は弊社のWebサイトをご覧ください。

弊社はNaikonの調査中に、Hellsing APTグループの活動も発見しました。同グループは主にアジアの政府機関や外交組織を攻撃対象としており、標的の大半はマレーシアとフィリピンに集中していましたが、インド、インドネシア、米国でも確認されています。Hellsingは小規模なサイバースパイグループであり、技術的に目立った特徴はありません（Hellsingの標的となった組織は約20）。興味深いのは、このグループがNaikonのスピア型フィッシング攻撃を受け、反撃に出た点です。スピア型フィッシングメールを受信したHellsingは、送信元に不審感を抱きました。その後、Naikonから返信を受け取りましたが、添付ファイルを開かず、その直後にHellsing独自のマルウェアを添付してNaikonにメールを送り返しました。自分たちが標的にされていることに気づいたHellsingグループが攻撃者の素性を突き止め、その活動に関する情報を収集しようとしていたことは明らかです。APTグループ同士が偶然対立することは以前にもありました（標的からアドレス帳を窃取し、そこに登録されていたすべての宛先にメールを一斉送信したケースなど）が、APTグループ同士の攻撃は例がありません。

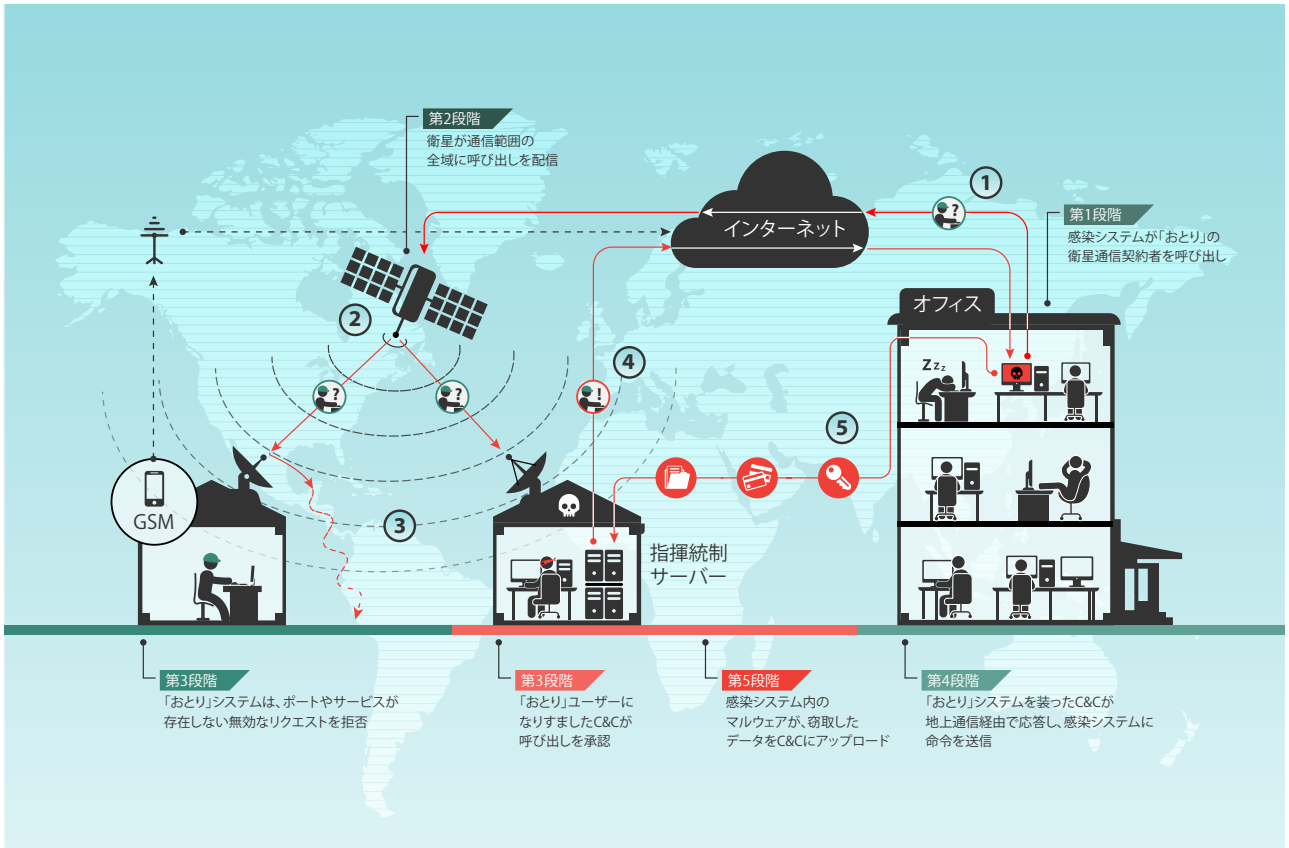


標的型攻撃の多くは、大企業や政府機関などの知名度の高い組織を狙っています。そのため、ニュースの見出しだけを読み、こうした組織だけが標的型攻撃を受けていると思いがちですが、前四半期に弊社が報告した活動の1つは、攻撃者の狙いが「大物」だけではないことをはっきりと示しています。サイバースパイ活動Grabitは主にタイやベトナム、インドに拠点を置く中堅中小企業からデータを窃取していますが、米国、UAE（アラブ首長国連邦）、トルコ、ロシア、中国、ドイツなどでも被害が報告されています。標的とされている業種は、化学、ナノテクノロジー、教育、農業、メディア、建設などで、攻撃の背後にいるグループは、約1万件のファイルを窃取したと推測されます。どんな企業も標的となる可能性があることは間違いありません。その企業の資産が狙われることもあれば、他の組織に侵入する手段として利用されることもあります。

Kaspersky Labは2015年春のセキュリティスイープ（検査）において、複数の社内システムに影響するサイバー侵入を検知しました。これを受けて実施された大規模な調査で、新たなマルウェアプラットフォームの開発が明らかになりました。それは、APTの中でも特に技術力が高く、正体が謎に包まれた有力グループであり、Stuxnetの兄弟とも言われるDuquです。弊社はこの新プラットフォームを「Duqu 2.0」と命名しました。弊社に対する攻撃では、Windowsカーネルのゼロデイ脆弱性（Microsoftが2015年6月9日に修正済）が悪用されていました。また、同じく当時はゼロデイだった脆弱性（現在は修正済み）が最大2件使われた可能性もあります。Duquの主な目的は、弊社の技術、進行中のリサーチ、内部プロセスをスパイすることでした。しかし、弊社だけが標的だったわけではありません。Duqu 2.0の感染者には、イランとの核関連協議であるP5+1の関係者が含まれており、攻撃者はこのような高官レベルの会議が行われる場所に攻撃を仕掛けようとしていたとみられます。さらに、同グループはアウシュビッツ=ビルケナウ強制収容所の解放70周年記念行事の出席者にも同様の攻撃を行っていました。Duqu 2.0最大の特徴は、永続性（persistence）がないことです。システムにほとんど痕跡を残さず、ディスクやシステム設定を一切変更しません。Duqu 2.0は、感染システムのメモリ内でしか存続しないように設計されていました。このことから、個々の標的のコンピューターが再起動され、マルウェアがメモリから消去されても、システム内に存続できるという攻撃者の自信が伺えます。Duqu 2.0に関する技術文書と永続モジュールの分析は、弊社のWebサイトをご覧ください。

8月には、Blue Termite APTについて報告しました。日本の組織から情報窃取することに重点を置いた標的型攻撃です。標的組織は、政府機関、地方自治体、公益団体、大学、銀行、金融機関、エネルギー、通信、重工業、化学、自動車、電気、ニュースメディア、情報サービス、医療、不動産、食品、半導体、ロボット工学、建設、保険、運輸などです。特に注目を集めた標的は日本年金機構でした。マルウェアは、標的に合わせてカスタマイズされます。Blue Termiteのバックドアには、C&C、API名、解析妨害用文字列、ミューテックスの値、バックドアコマンドのMD5チェックサム、内部プロキシ情報など、バックドア自体に関するデータが格納されています。このデータは暗号化形式で保存されており、サンプルごとに異なる復号鍵が必要になるため、解析は非常に困難です。他の多くの標的型攻撃と同様、主な感染手段としてスピア型フィッシングメールが使われますが、それ以外の手段も確認しています。その1つがHacking Teamに対するセキュリティ侵害で漏洩したエクスプロイトの1つ、Flashエクスプロイト（CVE-2015-5119）を使用したドライブバイダウンロードです。日本の複数のWebサイトがこの方法で侵入を受けました。また、水飲み場型攻撃も数例確認されています。この中には、著名な日本政府関係者のWebサイトも含まれていました。

サイバースパイ活動Turlaを展開するグループが活動を開始してから8年以上が経過し、世界45か国以上で無数のコンピューターが感染しています（弊社の最初のレポート、その後の分析はsecurelist.comをご覧ください）。Turlaは攻撃の初期段階で、水飲み場型攻撃によって標的をプロファイリングします。しかし、弊社の最新レポートにまとめられているとおり、それ以降の攻撃では衛星通信を使用して、C&Cトラフィックを管理しています。Turlaが衛星の下り回線の乗っ取りに使う手口では、衛星インターネットの正規契約は不要です。これには、匿名性という大きな利点があります。つまり、攻撃者の特定が極めて困難ということです。衛星の受信機は、その衛星の通信範囲内の地域（通常は広域）であればどこにでも設置できるうえ、C&Cサーバーの実際の所在地やハードウェアは、簡単には特定できず、物理的に押収することもできません。また、この手口は衛星ベースの回線を購入するよりも安価であり、標的と衛星事業者の通信を傍受して途中でパケットを挿入するよりも容易です。Turlaグループは、コンゴ、レバノン、リビア、ニジェール、ナイジェリア、ソマリア、UAEなど、中東とアフリカの衛星インターネットプロバイダーを悪用する傾向にあります。このような国からの衛星放送は通常、欧州や北米の国々を対象としていないため、セキュリティリサーチャーがこういった攻撃を調査することは非常に困難です。衛星ベースのインターネット回線を利用するのは、興味深い手法です。下り回線の帯域幅の乗っ取りは安価で（初期投資に約1,000ドル、保守費用が年間約1,000ドル）、手軽に実行できるほか、極めて高い匿名性を得られます。一方、この手法は必ずしも従来の手口（防弾ホスティング、複数のプロキシ階層、ハッキングされたWebサイト）ほどの信頼性があるわけではありません（Turlaは従来の手法も使用しています）。そのため、大規模ボットネットの管理に利用される可能性は低いとみられます。しかし、この手法がAPTグループやサイバー犯罪者の間に広がった場合は、ITセキュリティ業界と警察機関にとって深刻な問題となるでしょう。



2015年8月には、Darkhotel APTの最新情報を公開しました。この攻撃には当初、窃取した証明書を不正利用する、さまざまな手段でHTAファイルを配布する、ホテルのWi-Fiへ侵入して標的コンピューターにバックドアを仕掛ける、などの特徴がありました。

Darkhotel APTの背後にいる攻撃者は、こうした手口を使い続ける一方で、攻撃手段を拡充し、選定した標的に対するスピア型フィッシングに関心を移しています。HTAファイルを使用するほか、RTLO（Right-to-Left Override）を利用してファイルの実際の拡張子を隠し、感染したRARファイルを配布します。また、Hacking Teamに対するセキュリティ侵害で漏洩したゼロデイエクスプロイトなど、Flashエクスプロイトも使用しています。同グループは地理的な攻撃範囲も拡大しており、北朝鮮、ロシア、韓国、日本、バングラデシュ、タイ、インド、モザンビーク、ドイツなどの組織も標的となっています。

情報漏洩

今年もセキュリティ侵害が絶え間なく報告されました。個人情報は正規の企業だけでなく、サイバー犯罪者にとっても価値があるため、このような事件が繰り返し発生しても驚くようなことではありません。今年の特に大きな情報漏洩事件には、Anthem、LastPass、Hacking Team、米政府人事管理局、Ashley Madison、Carphone Warehouse、Experian、TalkTalkなどへの攻撃がありました。これらの攻撃の中には大量のデータ盗難につながったものもあり、多くの企業が自社を守るための適切な対策を講じていないという事実が浮き彫りになっています。これは企業の境界だけを保護するという単純な問題ではありません。100%完璧なセキュリティというものは存在しないため、システムが侵害されないことを保証するのは不可能です。まして、内部の人間が唆されて企業のセキュリティを危険にさらす行動をとった場合には、安全の保証など到底できないでしょう。しかし、どのような組織であっても、個人情報を保有している限りは、データを効果的に保護する注意義務を負っています。これには、顧客パスワードのハッシュとソルト、機密情報の暗号化などの方法があります。

一方、個人は、他にはない複雑なパスワードを選択することで、セキュリティ侵害の被害をオンラインプロバイダーで食い止めることができます。理想的なパスワードは、長さが15文字以上で、キーボード上のさまざまな文字、数字、記号で構成されたものです。代替策として、こういった作業をパスワード管理アプリケーションで自動的に処理することもできます。

パスワードの問題は繰り返し発生しています。あまりにも簡単に推測できるパスワードを選べば、なりすまし攻撃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、問題がさらに深刻化します。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てしまいます。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したり、アカウントの設定を変更したりする際、ハードウェアトークンで生成されたコードか、モバイルデバイスに送信されたコードを入力する必要があります。確かに2段階認証によってセキュリティは強化されます。ただし、それは2段階認証が任意の場合ではなく、必須の場合だけです。

個人情報の盗難は、盗まれた側に深刻な結果をもたらす可能性がありますが、時には重大な連鎖反応を起こすこともあります。Hacking Teamに対するセキュリティ侵害によって、400GBのデータが公開される結果となりました。これには、Hacking Team社が自社の監視ソフトウェアに使用していたエクスプロイトも含まれます。流出したエクスプロイトには、DarkhotelやBlue TermiteといったAPT攻撃で使われたものもありました。当然ながら、この漏洩事件の後、攻撃者によって暴露された脆弱性に対して緊急パッチが作成されています。

スマート（であっても安全とは限らない）デバイス

インターネットはすでに私たちの生活の一部となり、スマートテレビ、スマートメーター、ベビーモニター、電気ポットなど、現代の家庭にはインターネットに接続できる日用品が増え続けています。昨年、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。この調査の続報はこちらでご覧いただけます。しかし、「モノのインターネット（IoT）」は家庭用品だけにとどまりません。

リサーチャーは過去数年にわたり、コネクテッドカーに関連する潜在的なセキュリティリスクを研究してきました。2014年7月、Kaspersky LabとIABは、コネクテッドカーにおける潜在的な問題点について研究結果を発表しました。今年までは、自動車と物理的に接続することで車載システムにアクセスする方法が主流でした。しかし、この状況はリサーチャーのチャーリー・ミラー（Charlie Miller）氏とクリス・ヴァラセク（Chris Valasek）氏がジープ・チェロキーの重要なシステムに無線アクセスする方法を発見した時点で一変しました。両氏はジープを乗っ取り、道路を脱線して走行させることに成功したのです（詳細についてはこちらをご覧ください）。

この研究は、自動車業界だけにとどまらず、あらゆるコネクテッドデバイスに関連する問題を浮き彫りにしています。残念ながら、セキュリティ機能はなかなか販売に結び付きません。競争の激しい市場では、消費者の生活を楽にするモノが優先される傾向にあります。さらに、接続機能は多くの場合、セキュリティを念頭に作られていない既存の通信ネットワークに追加されています。そして、これまでの歴史が示しているように、何か悪いことが起きて、セキュリティの弱点による影響が露呈するまで、セキュリティ機能は組み込まれません。こういった問題の詳細については、前述の研究後に公開されたユージン・カスペルスキー（Eugene Kaspersky）のブログ記事をご覧ください。

こうした問題は「スマートシティ」にもあてはまります。たとえば近年、政府組織や警察機関がCCTVシステムを利用して、公共の場を監視するケースが大幅に増加しています。多数のCCTVカメラがインターネットに無線接続され、警察が遠隔地から監視できるようになっていますが、これらのシステムは必ずしも安全ではありません。サイバー犯罪者が密かに監視カメラのフィードを傍受し、ネットワークにコードを挿入して、カメラのフィードを偽の画像と置き換えたり、システムをオフラインにしたりする可能性があります。先日、弊社のセキュリティリサーチャーであるバシリス・ヒオレアス（Vasilios Hioureas）とExigent Systemsのリサーチャーのトーマス・キンゼイ（Thomas Kinsey）氏が、ある都市に設置されたCCTVシステムの潜在的なセキュリティ脆弱性を調査しました（ヒオレアスのレポートは弊社Webサイトに掲載されています）。

カメラは隠されていなかったため、使用されているカメラのメーカーや型式はすぐに判明し、仕様を調べてラボ環境で縮小モデルを作成することができました。使用されている装置は効果的なセキュリティコントロール機能を搭載していましたが、実際には使われていませんでした。メッシュネットワークを行き来するデータパケットは暗号化されていなかったため、攻撃者が独自のソフトウェアを作成し、このネットワークを通るデータを操作することができました。これを悪用すれば、たとえば警察署に偽の映像を送信し、ある場所で事件が発生しているかのように見せかけ、その都市のどこか別の場所で実際に行われている攻撃から警察の目をそらすことができた可能性があります。

2人は実際の都市監視システムの管理担当者にこの問題を報告しました。現在は担当者によってセキュリティ問題の修正が行われているところです。一般に、このようなネットワークで重要なのは、強力なパスワードで保護されたWPA暗号化を実装すること、ハードウェアからラベルを除去して攻撃者に機器の仕組みを突き止められないようにすること、ネットワーク内を流れる映像を暗号化することです。

ここでさらに大きな問題となるのは、日常生活のさまざまな面でデジタル化が急速に進んでいる点です。設計の時点でセキュリティを考慮しなければ、潜在的な危険が先々まで付きまとう可能性があります。セキュリティの後付けはそう簡単にはいかないでしょう。弊社はSecuring Smart Citiesイニシアチブを通じて、スマートシティの開発担当者がサイバーセキュリティを考慮して設計するよう支援しています。

国際協力によるサイバー犯罪者対策

オンライン活動がかつてないペースで活発化していく中、その裏でサイバー犯罪はもはや日常の一部となっています。今ではこれが公式な統計にも表れています。たとえば、英国の国家統計局は、社会において犯罪の性質が変化しているという事実を踏まえ、犯罪規模の推定値にサイバー犯罪を盛り込むようになりました。サイバー犯罪が大きな利益を生むことは間違いありませんが、サイバー犯罪者は必ずしも罰せられないわけではなく、世界の警察機関の活動が大きな影響を及ぼしています。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。今年は警察機関による捜査に、いくつか目立った成果がありました。

Kaspersky Labは4月、国際刑事警察機構（インターポール）の指揮によるSimdaボットネットの壊滅作戦に協力しました。この捜査はMicrosoftが開始し、その後次第に規模が拡大し、Trend Micro、サイバーディフェンス研究所、オランダ国家ハイテク犯罪ユニット（NHTCU）の捜査員、FBI、ルクセンブルクのPolice Grand-Ducale Section Nouvelles Technologies（大公国警察新技術セクション）、国際刑事警察機構モスクワ本部の支援を受けたロシア内務省のサイバー犯罪部門「K」から派遣された捜査員が参加しました。その結果、オランダ、米国、ルクセンブルク、ポーランド、ロシアにあった14台のサーバーを停止させました。シンクホールサーバーのログの一部を予備解析したところ、このボットネットによる影響を受けた国は190か国に及ぶことが判明しました。

オランダ警察は9月、Kaspersky Lab、Panda Security、オランダ国家ハイテク犯罪ユニット（NHTCU）との共同捜査によって、CoinVaultランサムウェア攻撃に関与した疑いで2人の男を逮捕しました。2014年5月に始まったこのマルウェア攻撃は今年に入っても続き、標的は20か国以上にのぼり、特にオランダ、ドイツ、米国、フランス、英国に集中していました。攻撃者は1,500台以上のWindowsコンピューターでファイルを暗号化し、データの復号と引き換えに、Bitcoinでの身代金支払いを要求しました。このランサムウェア攻撃を実行したサイバー犯罪者は、マルウェアを数回にわたって改造し、新たな標的を常に追い続けました。2014年11月、弊社とオランダのNHTCUは、復号鍵を提供するWebサイトを立ち上げました。また、復号ツールをオンラインで公開し、身代金を支払わなくてもデータを復元できるようにしました。CoinVaultの作成者が使用したさまざまな手法の分析はこちらでご覧いただけます。ランサムウェアは、サイバー脅威の重要な一角を占めるまでになりました。このケースはリサーチャーと警察機関の連携が好ましい結果につながりましたが、消費者や企業も、この種のマルウェアのリスクを軽減するための対策を講じることが極めて重要です。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。9月には、あるFBI捜査官が、ランサムウェアの被害者はデータを取りかえすために身代金を支払うべきであると提案して、物議を醸しました。これは現実的な解決策のようですが（特に、データを復元できない場合もあるため）、危険な戦略です。まず、サイバー犯罪者がデータの復号に必要な手段を提供してくれる保証はありません。また、犯罪者のビジネスモデルが強化され、ランサムウェアの開発が一段と進められる可能性があります。こうした不愉快な状況に陥らないためにも、企業も個人ユーザーもデータを定期的にバックアップすることをお勧めします。

産業インフラに対する攻撃

産業インフラでは、サイバーセキュリティの問題に起因するインシデントが、頻繁に発生しています。たとえばUS ICS CERTのデータによると、米国でのこのようなインシデントは2014年度に245件、2015年の7月と8月に22件記録されました。しかし、この件数は実状を反映しておらず、実際のサイバーインシデントの件数はこれよりも多いと考えられます。また、企業経営者や所有者がこのようなインシデントを隠蔽したり、単に気づいていないこともあります。

以下に、2015年に弊社が注目した2件のケースを紹介します。

1件はドイツの製鋼所で発生したインシデントです。ドイツ連邦情報技術安全局（Bundesamt für Sicherheit in der Informationstechnik:BSI）は2014年の暮れに公開したレポートの中で、ドイツのある製鋼所でサイバーインシデントが発生し、その結果、溶鉱炉に物理的な損傷を受けていたことを明らかにしました。

弊社が把握している限り、産業用設備に物理的な損傷を与えたサイバー攻撃は、Stuxnetに続きこれが2例目です。BSIによると、攻撃者はまず、フィッシングメールを使用してこの会社のオフィスネットワークを感染させた後で、SCADAコンピューターを感染させ、物理機器を攻撃しました。しかし、BSIはこれ以上の情報を提供しておらず、使用されたマルウェアやその仕組みについては明らかになっていません。

こうした隠蔽は誰の得にもなりません。同種の企業経営者は（おそらくドイツ企業を除き）、攻撃を分析して、対抗策を講じることができません。また、サイバーセキュリティの専門家も詳しい状況がまったくわからないため、顧客にセキュリティ対策を提案できません。

もう1件の興味深いインシデントは、2015年6月にワルシャワで発生したフレデリック・ショパン空港に対する攻撃でした。ある日曜日、ポーランドの国営航空会社LOTの飛行計画準備を処理するコンピューターシステムが、約5時間にわたってダウンしました。ロイターによると、この影響で数十本のフライトに遅延が発生しました。

空港の管理側が詳細を明らかにしていないため、専門家は経験をもとに見解をまとめざるを得ませんでした。IOActiveの主席セキュリティコンサルタント、ルーベン・サンタマルタ（Ruben Santamarta）氏は、以前から航空業界のITセキュリティの問題に対する注意を喚起していました。サンタマルタ氏は、LOT関係者の発言を分析し、同社が標的型攻撃を受けた可能性を示唆しました。システムが飛行計画を生成できなかったのは、バックオフィスの重要ノードが侵害されたか、地上通信装置を狙った攻撃が行われ、飛行機データ（飛行計画を含む）のロードや検証ができなくなったためとみられています。

弊社のエキスパートもこのインシデントに対応し、考えられるシナリオを2つ提示しました。1つは、人為的なミス、もしくは機器の不具合が原因という可能性です。もう1つの可能性として、ワルシャワの比較的小さな空港で発生したこのインシデントは、より大規模な空港でさらに大きな攻撃を実行するためのリハーサルだったとも考えられます。

その後、DDoS攻撃が行われていたこと、実際の侵入はなかったことが発表されました。このインシデントでも詳しい情報は一切開示されていないため、公式発表を信じるか、攻撃の真の理由と目的を推測することしかできません。

こうしたインシデントは、攻撃の背後に潜むのが誰であれ、その目的が何であれ、コンピューターが近年の生活の中でどれほど大きな部分を占めるようになったか、インフラストラクチャの構成要素がどれほど攻撃されやすくなったかを明確に物語っています。

残念ながら、現在は多くの政府機関や規制当局が秘密主義のポリシーを貫いています。弊社は、産業インフラを適切に保護する上で、サイバー攻撃に関する透明性と情報交換が重要であると考えています。この知識なしには、産業インフラを将来の脅威から保護することは極めて困難です。

最後にもう1つ、すでに現実の問題に直結し、今後数年にわたって私たちに影響を与え続けるであろうトレンドをご紹介したいと思います。すなわち、産業界の企業で使用されるハードウェアのインターネット接続が積極的に進められている点です。インターネットの普及はかなり前のことだとしても、産業プロセスに導入されたのはつい最近です。これが新たな産業革命を象徴していると言っても過言ではありません。現在は、「産業用モノのインターネット」、つまりEnterprise 4.0が誕生しつつある時代と言えます。これにより、企業はさまざまな付加的恩恵を受け、製造効率を向上させることができます。

機器メーカーはこのトレンドについていくために、もともと「オフライン」の世界向けに開発された機器（安全性、信頼性が高く、実績がある機器）にセンサーとコントローラーを追加し、インターネットに接続できるようにしただけで、「新しい機器」として顧客に提供しています。しかし、デバイスにオンライン機能を追加した時点で、サイバーセキュリティ関連のリスクや脅威が生まれることは考慮されていません。これはもはや「物理」デバイスではなく、「サイバーフィジカル」デバイスなのです。

物理デバイスの世界では、どの産業用デバイス、機器、通信プロトコルも安全性を念頭に置いて設計されていました。いわば、100%安全な設計です。つまり、デバイスが機能上の安全要件を満たすように設計されており、なおかつ安全規則に違反しないように操作していれば、人体や環境に対する不具合や害も発生しないということです。

Enterprise 4.0はセキュリティに「外部からの意図的な操作に対抗するITセキュリティまたは保護」という新たな次元をもたらします。インターネットがなかった時代に作られたモノや装置をそのままインターネットにつなぐことはできません。そんなことをすれば、壊滅的な被害を招く可能性があり、実際に多くの場合そうなっています。

「革命前」の古い設計方針をかたくなに守るエンジニアにとって、デバイスを「操作」する人物は許される行為とそうでない行為をわきまえたエンジニアだけであり、ハッカーがリモートからオブジェクトを操作するという許されない行為に及ぶことなど気づいてもいません。これが、長い歴史を持つ大手企業の一部が、機能上の安全性の面では信頼できてもサイバーセキュリティのレベルは不十分なハードウェアを提供している主な理由の1つです。

サイバーフィジカルデバイスの世界では、物理コンポーネントとサイバーコンポーネントは密接に統合されています。サイバー攻撃が産業プロセスを妨害し、機器に損傷を与えることもあれば、テクノロジーに起因する災害を引き起こす可能性もあります。ハッカーは実在する脅威であり、インターネットに接続されているものをすべて攻撃の対象にしています。だからこそ、機器メーカーはインターネット接続機能を備えた新たな産業用機器を設計する際、機能的に安全な設計をするときと同じくらい慎重に、サイバー脅威に対抗するための保護を実装しなければなりません。

株式会社カスペルスキー
PR-1020-201512