KASPERSKY lab

# Kaspersky Security Bulletin 2016

## 2016 年 サイバー脅威の主要動向：進化する脅威

標的型攻撃の定着、金融機関への攻撃増加、
巧妙化するモバイルマルウェア、産業インフラのインシデント

GREAT

# 目次



著者：David Emm, Roman Unuchek, Kirill Kruglov  Kaspersky Lab

Kaspersky Security Bulletinは、Global Research and Analysis Team（GReAT：グレート）のトップセキュリティエキスパート50人がまとめた脅威の動向レポートです。GReATは、Kaspersky Labで研究開発に携わる中核部門として、脅威に関する情報収集、調査研究およびその成果発表などの活動を通じ、社内および業界をリードしています。

# 標的型攻撃

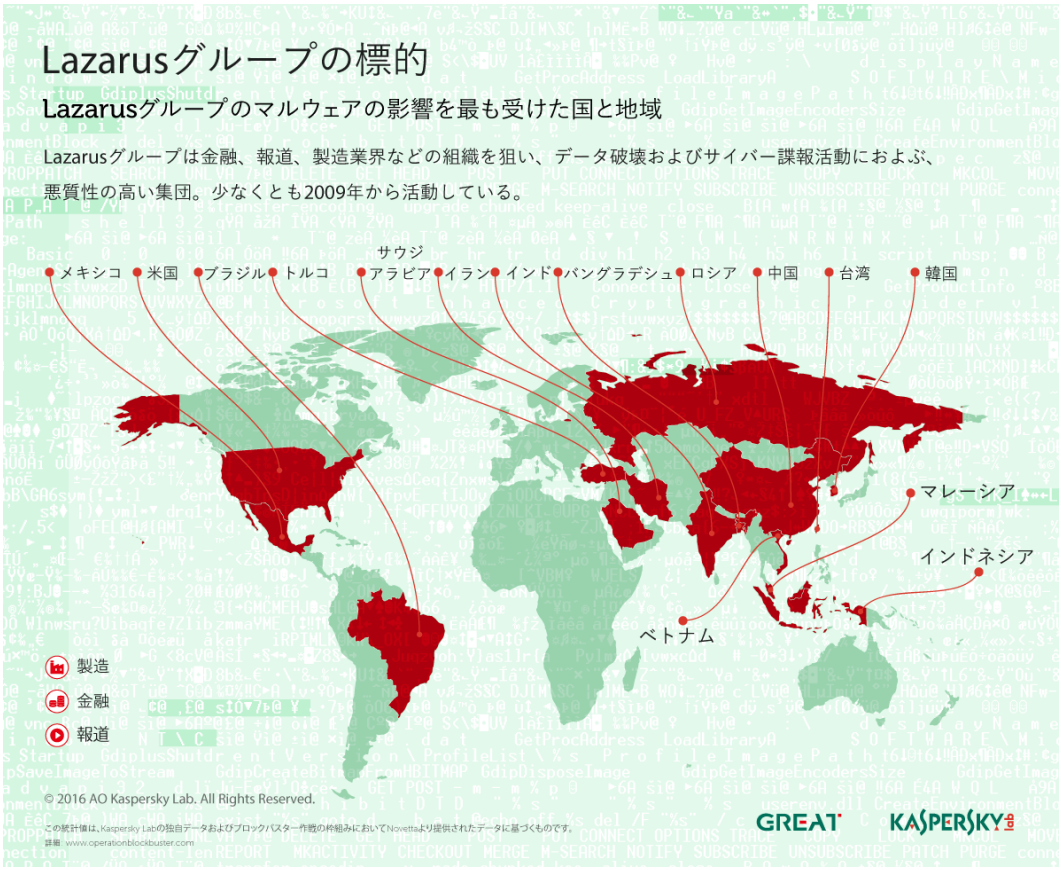
標的型攻撃は脅威の一部としてすっかり定着していることから、まず、Kaspersky Labが2016年に報告した主な標的型攻撃（APT）のキャンペーンについて紹介します。

## BlackEnergy

2016年は、ウクライナのエネルギー産業に対するBlackEnergyのサイバー攻撃で幕を開けました。その損害の内容を考えると、特徴的な攻撃だといえます。攻撃者はウクライナ西部の送電システムをダウンさせ、標的のシステムでワイパープログラムを起動し、被害企業のテクニカルサポートサービスに電話で分散型サービス妨害攻撃（DDoS）を仕掛けました。Kaspersky Labの専門家は、この攻撃を主導したグループの活動に関する特徴、特に標的システムへの侵入に使用されたツールの分析を公表しています。攻撃の概要については、SANS InstituteとICS-CERTによるレポートをお読みください。

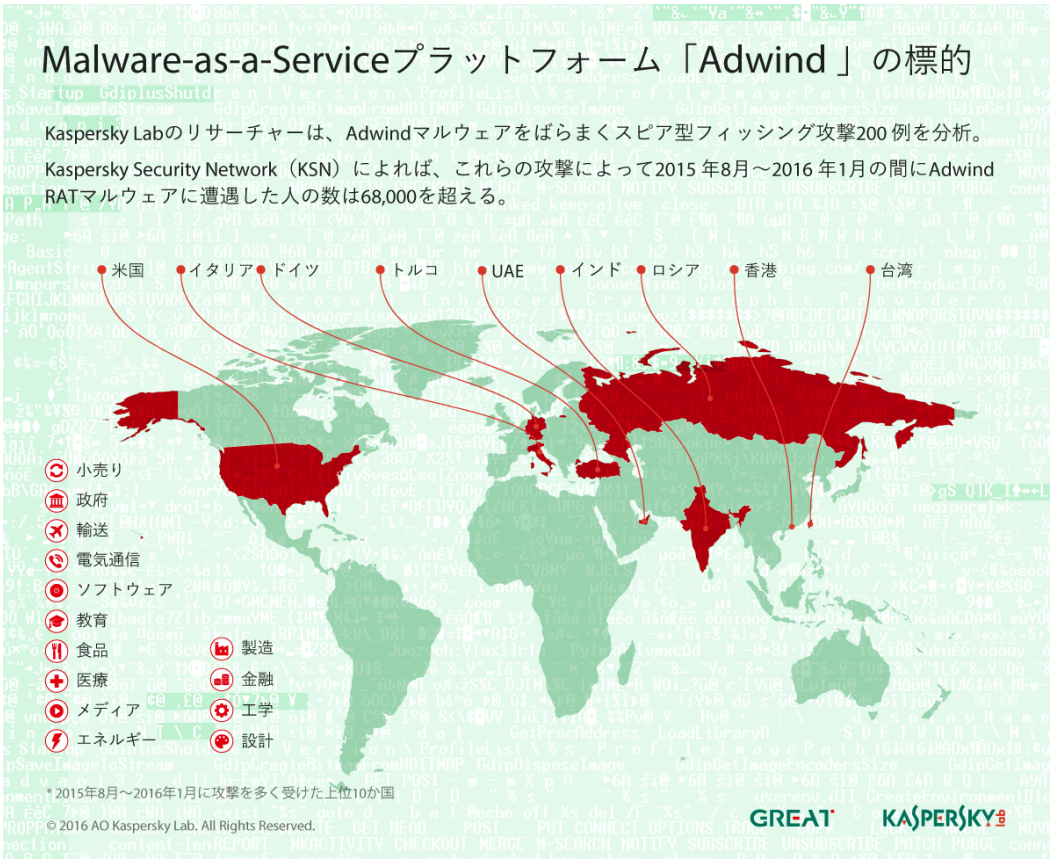
## Operation Blockbuster（ブロックバスター作戦）

Kaspersky Labは大手ITセキュリティ企業数社と連携し、Lazarusグループの活動を究明する共同調査、Operation Blockbuster（ブロックバスター作戦）に参加しました（詳しいレポートはこちらからご覧いただけます）。Lazarusは、北朝鮮で結成されたとみられるサイバー犯罪グループで、2014年のSony Picturesに対する攻撃を主導したとされます。2009年頃から活動を始め、2011年以降に動きが活発化しました。Lazarusは、Troy、Dark Seoul（ワイパー攻撃）、WildPositronなどのよく知られた攻撃を主導しており、企業、金融機関、ラジオ局やテレビ局を標的としています。




## Adwind

2016年2月に開催された Kaspersky Security Analyst Summitにおいて、弊社はAdwindに関する調査結果を発表しました。Adwindはクロスプラットフォーム対応の多機能型リモートアクセスツール（RAT）で、1つのMalware-as-a-Platform（プラットフォームとしてのマルウェア）サービスを通じて配布されます。このトロイの木馬は、2012年の登場以降、AlienSpy、Frutas、Unrecom、Sockrat、JSocket、jRatと次々に名前を変えてきました。2013年から2016年にかけて、世界中で443,000を超える個人、営利・非営利団体への攻撃に使用されたと考えられます。Adwindが他の販売されているマルウェアとは一線を画す主な特徴のひとつに、有料サービスとして公然と配布されている点が挙げられ、利用者は料金を支払ってこの悪意のあるソフトウェアを利用しています。利用者の数は2015年末までに1,800人程度に上るとみられ、今日存在する最大のマルウェアプラットフォームに数えられます。




## 脆弱性「CVE-2015-2545」を突くエクスプロイトを用いた攻撃

2016年5月、Kaspersky Labはアジア太平洋地域と中東地域で活動する別のAPTグループによる複数のサイバースパイ攻撃について報告しました。いずれの攻撃も、脆弱性「CVE-2015-2545」を突くエクスプロイトが用いられたという共通点があります。この欠陥を悪用すると、EPS形式の特別に細工された画像ファイルを用いて任意のコードを実行することができます。エクスプロイトではPostScriptを使用し、Windowsに実装されたASLR（Address space layout randomization：アドレス空間のランダム化）やDEP（Data Execution Prevention：データ実行防止）といったセキュリティ機能を回避します。このエクスプロイトを使用するグループとして、Platinum、APT16、EvilPost、SPIVYなどが知られていますが、最近ではDantiおよびSVCMONDRグループでも使用されました。この脆弱性を悪用するAPTグループの概要については、こちらをご覧ください。

こうした攻撃に関して最も衝撃的なのは、2015年9月にMicrosoftが修正パッチを公開しているにもかかわらず、その脆弱性を巧みに悪用している点です。Kaspersky Labは2016年の予測として、APT活動では目的達成のため高度なツールの開発に労力を投じるのではなく、既存のマルウェアを巧みに利用するようになるという見通しを立てていました。これは、ゼロデイエクスプロイトを開発する代わりに、既知の脆弱性を悪用した代表例です。

このことから、企業は自社のITインフラを保護するため、修正パッチの管理にもっと注意を払う必要があるといえます。

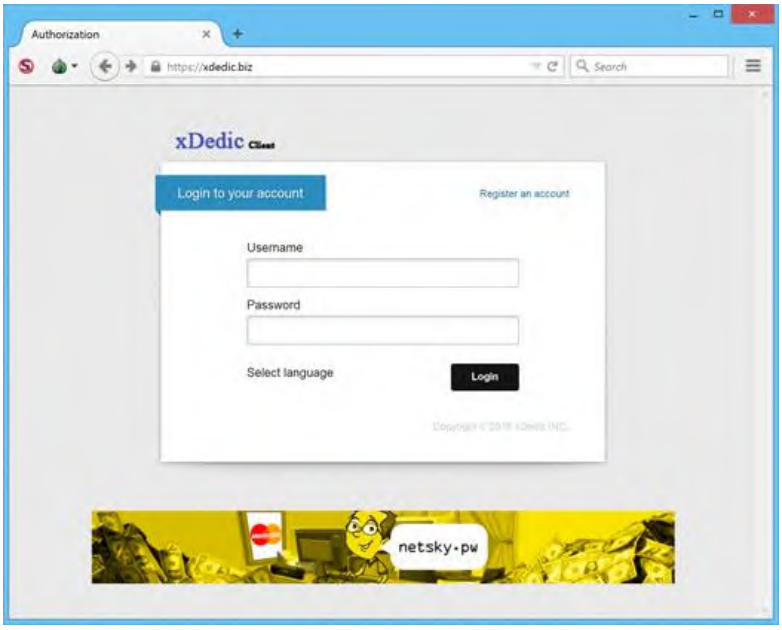
## Operation Daybreak

当然、ゼロデイエクスプロイトの利用を虎視眈々と狙うAPTグループは常に存在します。Kaspersky Labは、6月にコードネーム「Operation Daybreak」のサイバースパイ活動について報告しました。ScarCruftというグループは、それまで知られていなかったAdobe Flash Playerのエクスプロイト（CVE-2016-1010）を用いて攻撃を行いました。このグループは比較的新しく、それまで目立った活動をしていませんでした。その一方で、かつて別のゼロデイエクスプロイト（CVE-2016-0147）（2016年4月に修正パッチ公開済み）の展開にも関与していたものとみられます。グループは、アジア地域の司法当局、世界最大規模の貿易会社、米国のモバイル広告・アプリ配信企業、国際陸上競技連盟に関連する個人、ドバイ最大のショッピングセンターにあるレストランを標的としています。

100%完璧なセキュリティというものは存在しません。重要なのは、攻撃者がコストの問題で侵入をあきらめるか、別のターゲットに標的を移すレベルまでセキュリティ対策を徹底することです。標的型攻撃を防ぐ最善の方法は、従来のウイルス対策技術をパッチ管理、ホスト侵入検知、デフォルト拒否型のホワイトリスト戦略と組み合わせた、階層型のセキュリティ対策です。Australian Signals Directorateの調査によると、分析を行った標的型攻撃のうち85%は、4つのシンプルなリスク軽減戦略（アプリケーションのホワイトリスト化、アプリケーションの更新、OSの更新、管理権限の制限）によって防ぐことができるとされています。

## xDedic

2016年Kaspersky Labは、サイバー犯罪者向けの情報売買プラットフォーム、xDedicの実態を調査しました。xDedicは、リモートデスクトッププロトコル（RDP）経由でアクセス可能な、世界中でハッキングされたサーバーの認証情報についてのオンラインブラックマーケットです。弊社は当初、70,000台に上るサーバーがマーケットで扱われていると考えていましたが、最新のデータによると、xDedicの市場はさらに広く、176,000台のサーバーの認証情報が含まれることが示唆されています。xDedicには検索エンジンがあり、買い手はサーバー1台あたり最低8ドルの料金で、政府機関から企業のネットワークまであらゆる認証情報を手に入れることができます。「顧客」は、格安料金でそのサーバーのデータにアクセスし、さらなる標的型攻撃を仕掛けるための踏み台として利用することができます。




このように気軽に利用できる闇マーケットは今に始まったことではなく、最近では細分化が進んでいます。xDedicの運営者が採用するモデルは決して容易に真似できるものではありませんが、今後特定の分野に特化したマーケットが登場する可能性もあります。

## Dropping Elephant

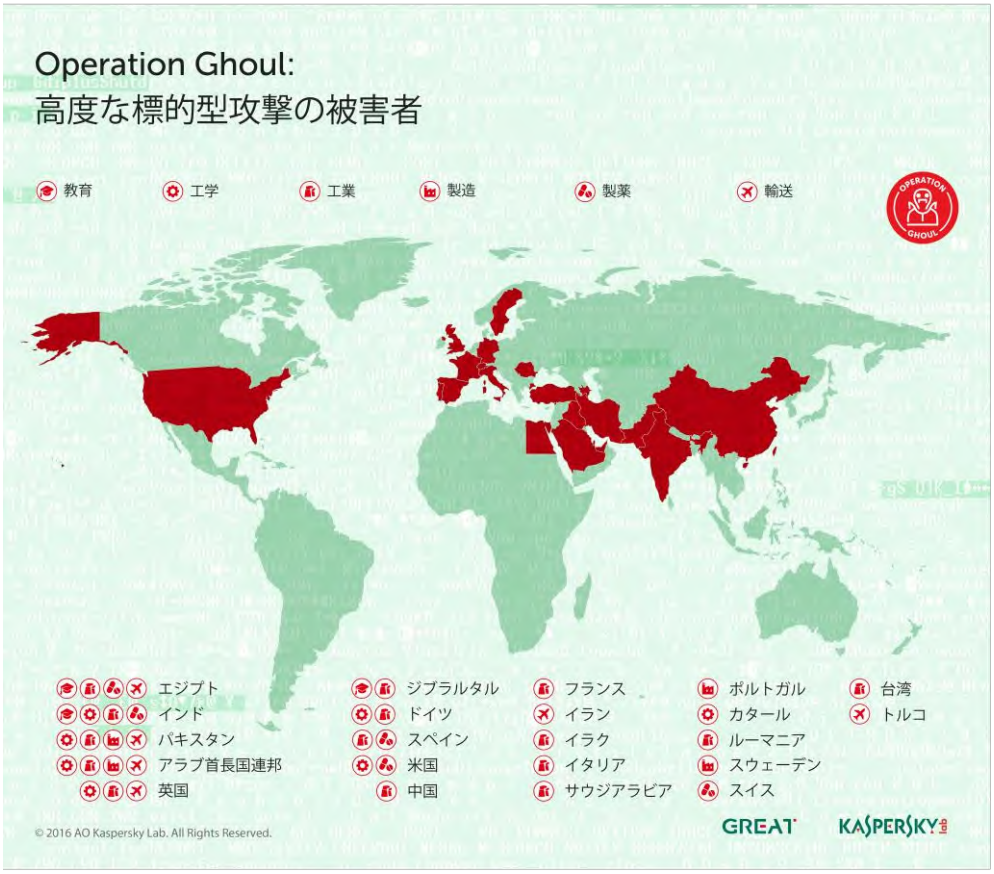
標的型攻撃活動は必ずしも技術的に高度なものであるとは限りません。Kaspersky Labは、7月にDropping Elephantというグループ（別名「Chinastrats」および「Patchwork」）について報告しました。このグループはソーシャルエンジニアリング手法や古いエクスプロイト、PowerShellベースのマルウェアを組み合わせて、中国高官および外交に関する経済機関から機密情報を盗み出すことに成功しました。攻撃者らは、スピアフィッシングメール（標的型攻撃メール）と水飲み場型攻撃を組み合わせて使用しています。Dropping Elephantグループがゼロデイエクスプロイトや高度な手法を用いることなく、政府機関への攻撃に成功したという事実は特筆すべき点です。Dropping Elephantは、既存のツールセットをソーシャルエンジニアリング手法と巧みに組み合わせることで、低コストでも十分な効果が上げられることを世に示しました。

このような攻撃は、セキュリティ更新プログラムを適用し、スタッフのセキュリティに対する認識を高めることで防ぐことが可能です。

## Operation Ghoul

攻撃者がソーシャルエンジニアリングを上手く使って標的組織で足がかりを得たもうひとつの例として、Operation Ghoulが挙げられます。このグループは、Kaspersky Labが2016年6月に報告した一連の攻撃に関与していました。攻撃者は、多数の企業の上級

管理職および中間管理職に狙いを定めて、悪意のあるファイルを添付したスピアフィッシングメール（標的型攻撃メール）を送りつけました。その標的は、かつてアラブ首長国連邦のある銀行に勤務していた人たちだとされます。メッセージはその銀行からの支払通知をうたい、SWIFTの書類が添付されていましたが、実際にはマルウェアが組み込まれていました。一部のC&C（コマンド＆コントロール）サーバーのシンクホールから入手した情報によると、標的の多くは工業および工学分野の組織でした。他にも、輸送、製薬、製造、貿易、教育機関が狙われました。




Operation Ghoulグループが使用したマルウェアは、Dark Webで公然と販売されている商業スパイウェアキット、Hawkeyeを活用したものでした。マルウェアはインストール後、被害者のコンピューターからキーストロークやクリップボード上のデータ、FTPサーバーの認証情報、ブラウザー/メッセージクライアント/電子メールクライアントのアカウントデータ、インストールされたアプリケーションなど、めぼしい情報を収集します。

犯人はソーシャルエンジニアリング手法を使って標的組織で足がかりを得ています。このことを教訓に、企業は社員の認識向上と教育をセキュリティ戦略の柱に位置づける必要があります。

## ProjectSauron

9月には、2011年6月よりロシア、イラン、ルワンダを中心とする諸国の組織から機密データを窃取してきたグループ、ProjectSauronの存在が明らかになりました。


攻撃にかけるコスト、複雑さ、執拗さ、そして国家機関から機密データを窃取するという活動の目的から、ProjectSauronは国家が支援するグループであるとみられます。攻撃者は、Duqu、Flame、Equation、Reginなど極めて高度なサイバー犯罪グループがもつ革新的な手法を取り入れ、それを独自に改良して検知を回避しているものと考えられます。利用するすべてのマルウェアを標的ごとにカスタマイズするため、脅威存在痕跡ではほとんど発見することができません。

**ProjectSauronの主な特徴**:

1. ProjectSauronは、長期的なサイバースパイ活動を可能にするモジュール型プラットフォームである。
2. すべてのモジュールおよびネットワークプロトコルで、RC6、RC5、RC4、AES、Salsa20といった強力な暗号化アルゴリズムを使用している。
3. 改良されたLuaスクリプトエンジンを用いて、コアプラットフォームとそのプラグインを実行している。
4. プラグインの種類は50種類以上に及ぶ。
5. ProjectSauronの攻撃者グループは、標的となる政府機関で広く使用されている通信暗号化ソフトウェアに高い関心を持っており、暗号化キー、設定ファイル、暗号化ソフトウェアに関連する主要インフラサーバーのIPアドレスを窃取している。
6. 特製のUSBストレージドライブを利用することで、隔離されたネットワーク間のエアギャップを飛び越えてデータを引き出すことができる。このUSBドライブでは、OSからは隠された領域にデータを保存する。
7. プラットフォームでは、データの引き出しとリアルタイムでのステータスレポーティングにDNSプロトコルを広く活用している。
8. このAPTは早ければ2011年6月頃から活動を始め、2016年4月まで活動を継続していた。
9. 被害組織のネットワークに侵入するための感染経路はいまだよくわかっていない。
10. 攻撃者は正規のソフトウェア配信チャネルを利用し、感染ネットワーク内を移動している。

コントロールサーバーや暗号化キーといった独自の手法を1回限りで使用する点と、他の主要なサイバー犯罪グループによる最先端の手法を取り入れている点がこれまでにない新しい手口だといえます。

ProjectSauronに対抗する上で唯一有効な方法は、組織のワークフローで軽微な異常をも検知できるセンサー群を導入し、これを脅威インテリジェンスとフォレンジック分析によって補強することで、階層型のセキュリティ対策を展開することです。こうした脅威への対応方法についてのさらなる考察は、こちらからご覧いただけます。

## 金融機関を狙う脅威

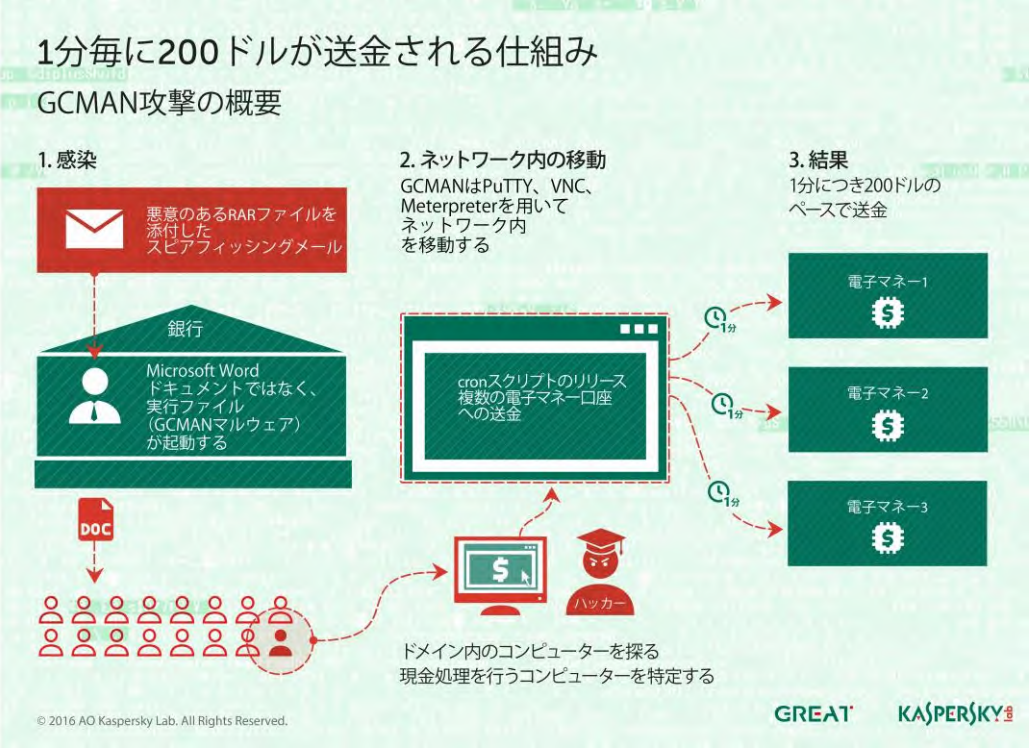
サイバー犯罪者が金銭を得る最も直接的な方法のひとつが、銀行の顧客を狙うことです。通常、攻撃者はソーシャルエンジニアリング手法を用いて被害者を欺き、個人情報を聞き出したり、銀行口座にアクセスするのに必要な個人情報（パスワードなど）を取得するためマルウェアをインストールさせたりします。2016年、Kaspersky Labのソリューションは、オンラインバンキング口座から現金を窃取するマルウェアを実行しようとする試みを2,871,965台のデバイスでブロックしました。

しかし、サイバー犯罪者が標的にするのは銀行の顧客だけではありません。近年、銀行や金融機関を狙った攻撃の発生件数が増加傾向にあります。中でも特に有名なのがCarbanakです。Carbanakでは、金銭の窃取を目的とした標的型攻撃に特有の侵入技術が使用されていました。2016年は金融機関を狙った攻撃がさらに発生しています。

2016年2月、Kaspersky Labは別の金融機関を標的にした他のAPTグループによる活動を発見しました。Metelを使う攻撃者グループはスピアフィッシングメール（標的型攻撃メール）とブラウザーのエクスプロイトを用いて銀行のネットワーク内に侵入した後、銀行のITシステム内で主要なコンピューターを乗っ取ります。このレベルまで侵入を拡大すると、ATM取引のロールバック機能を自動で操作することができるようになります。デビットカードを使用し、何度現金を引き出してもカード残高を元に戻すことで、多数のATMから現金を窃取することに成功しました。弊社の調査によると、攻撃者はロシア国内の様々な都市を車で回り、様々な銀行のATMから現金を引き出していました。夜間のみに活動し、数か所で現金を引き出していたことが分かっています。30行以上の金融機関でMetelを発見しましたが、インシデントレスポンスチームの尽力により感染ネットワークからマルウェアを完全に駆除することができたため、深刻な損害が生じるには至りませんでした。その一方で、Metelのサイバー犯罪者はいまだ活動を続けており、このマルウェアのさらなる拡大が予想されます。


もうひとつの例が、GCMAN（GCCコンパイラーでコンパイルされたコードによるマルウェアを使用していることから、こう呼ばれる）です。このグループは悪意のあるRARファイルを添付したスピアフィッシングメール（標的型攻撃メール）を使って、金融機関に侵入していました。アーカイブを開くと実行ファイルが起動し、最初の感染が起こります。こうして組織内で足がかりを作ると、PuTTY、VNC、Meterpreterといった正規の侵入テストツールを使って組織内を移動し、電子マネー口座に送金するためのコンピューターを特定していました。その方法として、攻撃者は銀行のサーバーのひとつにCronスクリプトを埋め込み（CronはUnixベースのOSで使用される時間ベースのスケジューラー）、1分につき200ドルのペースで送金を実行していました。スクリプトが1分毎に実行されると、新しい取引の命令がアップストリームの支払い処理システムに直接送信されるという仕組みです。幸い、金融機関は不審な活動を検知し、取引を取り消すことができました。もしこの動きに気付かなかったら、銀行内のシステムに取引の詳細が表示されることなく、

複数の電子マネー口座に現金が送金されるところでした。Kaspersky Labのリサーチャーは、GCMANマルウェアに感染したロシアの金融機関3行と連携して調査にあたりました。しかし、この脅威はもっと広い範囲に拡大しているものと考えられます。




興味深いことに、Kaspersky Labの調査では、マルウェアが発見される1年半ほど前に実際の攻撃が起こっていたことが分かっています。このグループは、銀行のいずれかの公開ウェブサーバーで実行されていた商用ソフトウェアにSQLインジェクション攻撃を仕掛けて情報を取得し、1年半後にその情報を悪用して銀行への侵入を試みました。このインシデントが起こる2か月前、誰かが銀行のサーバーの管理者アカウントで様々なパスワードを試した形跡がありました。試みは執拗であったものの土曜日に限られ、週に3回のみでした。これらはすべて、標的となる金融機関でセキュリティチームによる発覚を避けるための対策だったとみられます。GCMANグループの活動から、脅威の分野における新たな動向が明らかになりました。それは、特製のマルウェアモジュールではなく、正規のツールを悪用することです。

正規のツールはサイバー犯罪者にとって失敗が少なく、すばやく投資を回収することができる有効な手段です。ITセキュリティチームは、会社のセキュリティ戦略を見直すにあたってこのことを念頭に置いておくことが重要です。

MetelおよびGCMANの活動についての詳細は、こちらからご覧いただけます。

当然、銀行は単独で営業しているわけではありません。海外送金には、SWIFT（国際銀行間通信協会）と呼ばれる銀行間ネットワークが必要です。

2016年2月、攻撃者らはバングラデシュ中央銀行の行員のSWIFT認証情報を使ってニューヨーク連邦準備銀行への不正な送金を依頼し、数百万ドルの現金をアジア地域の複数の銀行口座に送金しようとしました。その結果、8,100万ドルをフィリピンのリサール商業銀行に、さらに2,000万ドルをパンアジア銀行に送金することに成功しています。送金依頼に入力ミス（「foundation」を「fandation」とミス）がなければ、被害額はさらに拡大していたものとみられます。幸い連邦準備銀行が入力ミスに気づき、バングラデシュ中央銀行側で8億5,000万ドル分の取引を停止することができました。詳しい内容は、こちらからご覧いただけます。バングラデシュ中央銀行からの窃取事件の後、SWIFT認証情報を悪用して銀行を狙った他の攻撃も明るみに出ました。

ATMを標的とするのはMetalを使うグループだけではありません。ATMを狙うマルウェアは今に始まったことではなく、こうした悪意のあるプログラムは近年増加傾向にあります。2016年以前で最も注目すべきは、Tyupkinです。攻撃者は実際にATMへ出向き、ブータブルCDを挿入して機械を乗っ取りました。

2016年5月には、Kaspersky LabはATMを狙う新種のSkimerマルウェアについて報告しました。このレポートは、弊社が前年に実施したインシデントレスポンス調査の結果を受けて公表されたものです。このマルウェアが最初に浮上したのは2009年のことでしたが、その後設計が一新され、利用するサイバー犯罪者の手口も変わりました。新種は世界中のATMを標的にしています。弊社の調査では、アラブ首長国連邦、フランス、米国、ロシア、マカオ、中国、フィリピン、スペイン、ドイツ、ジョージア、ポーランド、ブラジル、チェコ共和国で攻撃が確認されました。

ATMに偽造カードリーダーを取り付けるというありきたりの方法に代わり、攻撃者はATM全体を乗っ取ります。まずはATMに直接出向くか、銀行の内部ネットワークに侵入して、ATMにSkimerマルウェアをインストールします。このマルウェアはATMの中枢部、すなわち他の銀行インフラとのやり取りやカード処理、現金の引き出しに関わる部分に感染します。従来のカードスキマーとは異なり、一見してATMが感染しているかどうかが分からないため、攻撃者はATMで使用されるカードから存分にデータ（顧客の銀行口座番号やPINなど）を取得したり、現金を直接窃取したりすることができます。

感染したATM内のマルウェアを起動するには、磁気ストライプに特定のレコードが仕込まれたカードを挿入します。Skimerはそのレコードを読み込んだ後、ハードコードされたコマンドを実行するか、カードによって有効化された特殊なメニューを使ってコマンドに応答します。カードを取り出してから60秒以内に、正しいセッションキーを入力すると、Skimerの操作メニューがディスプレイに表示されます。このメニューには、現金を引き出す、挿入されたカードの詳細情報を収集する、自分自身を削除する、更新する、といった21種類のオプションがあります。カードの詳細情報を自分のカードのチップに保存したり、収集した詳細情報を印刷したりすることも可能です。

攻撃者は、人目につかぬよう細心の注意を払っています。ATMから直接現金を引き出すという人目につきやすい方法をとるよりも、しばらく（場合によっては数か月間も）待機してから行動を起こします。通常、スキミングしたカードからデータを収集して、クローンカードを作成します。そのクローンカードを別の感染していないATMで使い、被害者の口座から現金を引き出します。こうすることで、元々侵入したATMから足がつくことはなくなります。

近年ATMを狙った攻撃が急増している背景には、スキマーの装置を使ってATMを乗っ取り、そこで利用されたカードからデータを抜き出すという定番の手口が必然的に進化を遂げてきたことがあります。残念ながら、多くのATMで動作しているOSには、セキュリティ上の脆弱性が存在することが知られています。物理的なセキュリティがますます重視されるのは、そのためです。

Kaspersky Labでは、銀行に対して推奨されるセキュリティ対策をいくつか提案しています。ウイルススキャンの定期的な実行、ホワイトリスト技術の導入、有効なデバイス管理ポリシーの適用、フルディスク暗号化の活用、ATMのBIOSをパスワードで保護、ハードディスクからのみのブート処理を強制し、ATMネットワークを他の銀行インフラと分離、などです。弊社の専門家がATMを狙ったジャックポッティング攻撃に関する徹底調査を実施し、ATMを保護するためのセキュリティ対策についての洞察を述べています。

Kaspersky Labでは、すでに起こった攻撃を調査するだけでなく、今後登場する技術を予測し、サイバー犯罪者がそれをどう悪用する可能性があるかを予想しています。最近、NFCによる非接触型認証、ワンタイムパスワード、バイオメトリクス（生体）認証といった認証手段についての調査結果を公表しました。驚くことに、12社がすでに偽造指紋スキャナー（生体情報スキマー）を提供しており、さらに少なくとも3社が静脈認証システムや虹彩スキャンシステムからデータを抜き出すことのできるデバイスを調査していることが分かっています。そのレポートは、こちらからご覧いただけます。

## IoT（Internet of things：モノのインターネット）

現代社会はスマートデバイスに囲まれています。電話、テレビ、温度計、冷蔵庫、ベビーモニター、ブレスレット型フィットネストラッカー、さらには子ども用のおもちゃなど日常的に使う家庭用品の中にも、スマートな製品が増えてきました。住宅にも「スマート機能」が取り入れられています。スマート化されたのは家庭用品だけにとどまりません。自動車、医療機器、CCTVカメラ、駐車メーターもスマートデバイスに挙げられます。いたるところにあるWi-Fi（必ずしも常に期待通りであるわけではありませんが）のおかげで、IoT(モノのインターネット)の一部としてこうしたのデバイスをインターネットに接続することができるようになりました。

これらのモノは私たちの生活を楽にしてくれます。日常にあるモノがインターネットにつながると、人の手がなくてもデータを自動的に収集し送信することができるため、動作がより効果的かつ効率的になります。その一方で、日常にあるモノがつながった世界では、サイバー犯罪者から攻撃を受けやすくなります。IoTデバイスが保護されていないと、そこでやり取りされる個人的なデータが漏洩し、攻撃の対象となったり、攻撃に悪用されたりする可能性があります。

残念ながら、セキュリティ機能はなかなか売上はつながりません。このオープンな市場では様々なベンダーが接続型のデバイスを製造しているため、投資利益率が重視されます。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置いて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。つまり、設計段階ではセキュリティが考慮されていないことが多いのです。過去の例を見ても、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。

ここ数年間にわたり、リサーチャーらは様々なコネクテッドデバイスにおけるセキュリティの問題を浮き彫りにしてきました。過去にKaspersky Lab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。昨年、チャーリー・ミラー氏とクリス・ヴァラセク氏がジープ・チェロキーの重要なシステムに無線アクセスすることが可能かを調査したところ、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ています。弊社のバシリス・ヒオレアスとExigent Systemsのトーマス・キンゼイ氏は、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。もっと最近では、ある医療機器メーカーのインスリンポンプに脆弱性が見つかり、サイバー攻撃によって機器に障害が起こったり、用量が変更されたりする危険があることから、医療機器メーカーがインスリンポンプを回収する事態となりました。また、たとえば子ども用のおもちゃやベビーモニター、玄関の呼び鈴といった日用品にも不安の種は潜んでいます。

2016年2月、Kaspersky Labは調査の一環として、病院を探し、その院内ネットワークにアクセスしてMRI機器を乗っ取り、患者の個人データや治療手順に関する情報を見つけ

出し、MRI機器のファイルシステムにアクセスすることがいかに容易であるかを示しました。弊社のリサーチャー、セルゲイ・ロズキンは2016年のKaspersky Security Analyst Summitでその調査結果を発表し、院内システムのセキュリティに影響を及ぼす主な要因を紹介しました。第一に、インターネットに接続する医療機器は、初期設定のパスワードでアクセス可能な状態でした。中にはWindows XPで稼働しているものもあり、修正パッチのない古い脆弱性に数多くさらされている状況で、院内システムへの侵入に悪用される恐れがありました。第二に、このような医療機器は、病院のローカルエリアネットワークから分離されていませんでした。そのため、院内のいずれかのWi-Fiネットワーク（パスワードが弱いもの）にアクセスすることができれば、医療機器に完全にアクセスすることが可能でした。第三に、ソフトウェア設計が脆弱であることから、医療機器に接続して初期設定のログイン画面を通過した後機器の管理画面、患者の個人情報および診断データにアクセスすることができました。これに加え、ユーザーの操作画面にはコマンドシェルが組み込まれていたため、機器のファイルシステムにアクセスできる状態でした。本レポートは、こちらからご覧いただけます。

病院は院内システムを守るための対策を講じる必要があります。

- 強力なパスワードを使い外部からの接続ポイントを保護する。
- ITセキュリティのポリシーを改定し、脆弱性評価とパッチシステムを構築する。
- 保護されたエリアへの不正アクセスが発生した場合に備え、ローカルネットワークで使用する医療機器にパスワードを設定する。
- 包括的なセキュリティソリューションでマルウェアやハッキング攻撃からインフラストラクチャを保護する。
- 定期的に重要な情報のバックアップを作成し、オフラインコピーを保管する。

4月、Kaspersky Labは、ここ数年の間にロシアの都市をはじめとする様々な地域で登場した、トラフィックセンサーについての調査結果を公表しました。これらのセンサーは速度制限を実施するのに役立っています：これらの新しいセンサーから発せられる信号は、交通警察が使用するスピードガンと同じ仕組みのため、運転手が持っているスピード違反取締カメラ探知器によっても反応します。しかし、センサーの設置理由はそういうことではありません。道路交通に関する生データ（車線毎の自動車台数、平均速度など）を収集し、分析を行うため市当局に提供しています。

Kaspersky Labのリサーチャー、デニス・レゲゾはデータトラフィックが保護されておらず、不正に操作される可能性があることを発見しました。Bluetoothで接続する場合を除いて、認証情報の確認はなく、その設定も不適切でした。弊社が調査したトラフィックセンサーのメーカーは、サービスエンジニアに手厚いサポートを提供しており、デバイスに関する多くの情報を自社の公式ウェブサイト等で広く公開していました。

これは良い流れです。「隠匿によるセキュリティ」は決して理にかなっているとはいえません。攻撃者はその気になればコマンドシステムを見つけ出し、何としてでもエンジニアリングソフトウェアにアクセスしてきます。ですから、オープンな対策、多額の懸賞金制度、特定された脆弱性へのすばやい対応を組み合わせて導入することのほうが理にかなっているのです。たとえ、リサーチャーの数が常に情報セキュリティ部門に勤める従業員の数よりも多いとしても、です。このレポートは、こちらからご覧いただけます。

近代の都市は、デジタルな要素も含め、数百もの要素から成る複雑なエコシステムです。スマートシティは、より便利で安全な生活を実現することが目的です。しかし、便利なものは、裏返せば悪用されることもあります。2016年9月、Kaspersky Labはスマートシティの様々な側面についての調査結果を発表しました。弊社のリサーチャー、デニス・マクルシンとウラジーミル・ダシュチェンコは、弊社が支援する「Securing Smart Cities」（スマートシティのITセキュリティ技術に関する専門家を集めた国際的な非営利プログラム）の一環として、調査結果をもとにレポートを作成しました。映画館のチケット販売機、

レンタサイクルポート、政府機関のサービスキオスク、空港の航空券予約端末や情報提供端末、タクシーの車載インフォテイメントシステムなどはすべて異なる形態をとっていますが、その中身はどれをとっても同じです。いずれの端末にもWindowsかAndroidが搭載されています。通常のデバイスとの大きな違いは、特殊なキオスクモードのソフトウェアが公開端末上で動作しており、ユーザー操作画面として機能している点です。このソフトウェアでは端末の特定の機能に簡単にアクセスできる一方で、端末のOSに備わっている他の機能（ウェブブラウザーや仮想キーボードを起動する機能など）へのアクセスが制限されています。そうした機能さえ攻略すれば、あたかもパソコンの前にいるかのような感覚でシステムに容易に侵入することができます。調査では、ほぼすべてのデジタル公開キオスクにセキュリティ上の弱点が1つ以上あることがわかっており、攻撃者によってOSの隠されている機能へアクセスされるおそれがあります。このレポートは、こちらからご覧いただけます。

私たちの日常生活はますますデジタル化が進んでいます。設計段階でセキュリティを考慮しないと、潜在的な危険が広範囲にわたって潜むことになります。後付けのセキュリティ対策は一筋縄ではいきません。スマートシティをそこに住む人たちにとって安全な場所にするためには、住民を情報システムと捉え、一人ひとりに合ったアプローチと専門知識で守る必要があります。

10月、サイバー犯罪者らはインターネットに接続した家庭用デバイス（IP対応カメラ、DVR、CCTVカメラ、プリンターなど）のボットネットを稼働させて、Dynに対するDDoS攻撃を仕掛けました。Dynは、TwitterやAmazon、PayPal、Netflixなどの企業にDNSサービスを提供する企業です。その結果、これらの企業のウェブサイトがダウンしたり、断続的に障害が起こったりしました。攻撃者は、脆弱性のあるデバイスをMiraiというマルウェアに感染させていました。このマルウェアは以前、セキュリティリサーチャー、ブライアン・クレブス氏のブログサイトに対するDDoS攻撃に用いられた経緯があります。史上最強のDDoS攻撃と称される攻撃です（最近、Miraiのソースコードがオンラインで公開されたため、Dynに対する攻撃が必ずしも同じ攻撃者によって実行されたとは限りません）。Miraiボットネットには550,000台程度のボットが組み込まれているとみられます。攻撃者は、初期設定のパスワードを使用してオンラインデバイスにアクセスしました。悪意のあるコードがデバイスに書き込まれると、そのデバイスはMiraiボットネットの一部となります。あらゆるDDoS攻撃がそうであるように、攻撃者は侵入したデバイスから狙いをつけたサイトに大量のトラフィックを送り込み、正常な動作を妨害します。

この攻撃は、感染したIoTデバイスを使用する他の攻撃と同じく、多くの人がスマートデバイスを購入したときにメーカーの初期設定情報を変更しないという弱点を突いたものでした。そのため、攻撃者グループにとっては既知の初期設定パスワードを試すだけで簡単にデバイスにアクセスすることができます。さらに、多くのデバイスにはファームウェアの更新がありません。IoTデバイスはインターネットに常時接続していることからも、サイバー犯罪者にとって格好の標的となっています。

自宅でインターネット接続デバイスやIoTデバイスを利用する人には、遠隔操作によるアクセスを防ぐため、すべてのデバイスで初期設定のパスワードを（独自の複雑なパスワードに）変更することを強く推奨します。これには、ホームネットワークへのゲートウェイとなるホームルーターも含まれます。こういう物騒なニュースを聞くと、すべてのデバイスをインターネットから切り離したい衝動に駆られるかもしれませんが、今日のますます“つながる世界”では決して現実的ではありません。代わりに、スマートデバイスの機能を常に確認し、実際に必要でない機能はオフにしておくことが得策です。また、パスワードを上手く「維持管理」することは、サイバー犯罪者をデバイスから遠ざける上で効果的です。こうした大規模攻撃の教訓として、メーカーがセキュリティ機能を後から組み入れるのではなく、設計段階で考慮するべきであることは明らかです。

# モバイルを狙う脅威

2016年にモバイルを狙った主な脅威は、感染デバイスのルート権限を悪用する広告型のトロイの木馬です。こうしたマルウェアがスーパーユーザー権限を取得することは決して珍しいことではありませんが、2016年にはデバイス上であらゆる機能を掌握するため、この権限を悪用するAndroid版のトロイの木馬が増え始めました。デバイスのルート権限を取得するために、トロイの木馬はシステムの脆弱性を悪用します。デバイスの多くは定期的に更新されていないため、このような脆弱性に対する修正プログラムを受け取っていません。そのため、Kaspersky Labでは今後ルート権限を悪用するトロイの木馬が増加し、その巧妙さも増すものと予測しています。

最近公表されたAndroidシステムの更新プログラムには、脆弱性に対する修正プログラムだけでなく、新しいセキュリティ機能も含まれていました。ところが、トロイの木馬はすでにその回避方法を見出しています。新しいセキュリティ機能を上手くすり抜けたマルウェアが今後、ますます登場するものとみられます。セキュリティ機能の中には、モバイルを狙ったトロイの木馬型ランサムウェアの攻撃を妨げることのできるものがあるかもしれません。それに伴い、攻撃者側の行動にも変化が生じる可能性があります。

## ルート権限昇格を試みるマルウェア

2016年にモバイルデバイスで最も多くみられた危険なトロイの木馬は、デバイスのスーパーユーザー権限を悪用する広告型のトロイの木馬でした。そのほとんどが、Trojan.AndroidOS.ZtorgおよびTrojan.AndroidOS.Iopファミリーに属するものです。

広告型のトロイの木馬は2016年を通じて着実に増加し、検出されたトロイの木馬の上位30種では、昨年と比べて発生件数が倍増していました（2015年の11件に対して2016年は22件）。

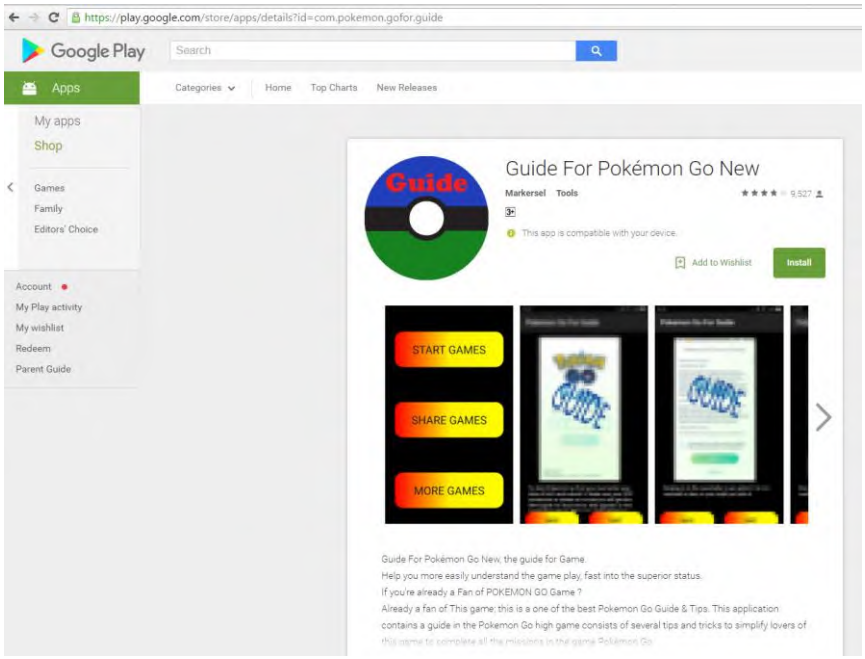
スーパーユーザー権限を取得するため様々なエクスプロイトを用い、デバイスがすでにルート権限昇格されている場合は既存のスーパーユーザー権限を悪用します。

スーパーユーザー権限の用途は主に2つです。第一に、このトロイの木馬は削除されないようしばらくシステムフォルダーに身を潜めています。中にはリカバリーイメージにも感染するものがあり、工場出荷時設定にリセットしても削除することができません。第二に、スーパーユーザー権限を取得し、様々なアプリをこっそりインストールし起動して、モバイルデバイスを広告で埋め尽くします。こうして新たにインストールされたアプリは広告を表示するだけで悪意のないアプリであることがほとんどですが、場合によっては新しいマルウェアがインストールされることもあります。あるケースでは、Zygoteプロセスに挿入するモジュールベースの Backdoor.AndroidOS.Triadaがインストールされていました。こうすることで、執拗に攻撃を続け、他のアプリから送信されたSMSを変更してユー

ザーのお金を盗むこともあります。このトロイの木馬は、ルート権限を用いて、たとえばブラウザーのURLを別のものに差し替えるなどまさにどんな操作も行うことができるようになります。

広告アプリに感染したデバイスは、迷惑な広告がひっきりなしに表示され、膨大な数のアプリがインストールされるため、ほとんど使い物になりません。このようなトロイの木馬は削除が難しく、新しいアプリをこっそりインストールしたり、場合によってはGoogle Playから勝手に購入したりします。

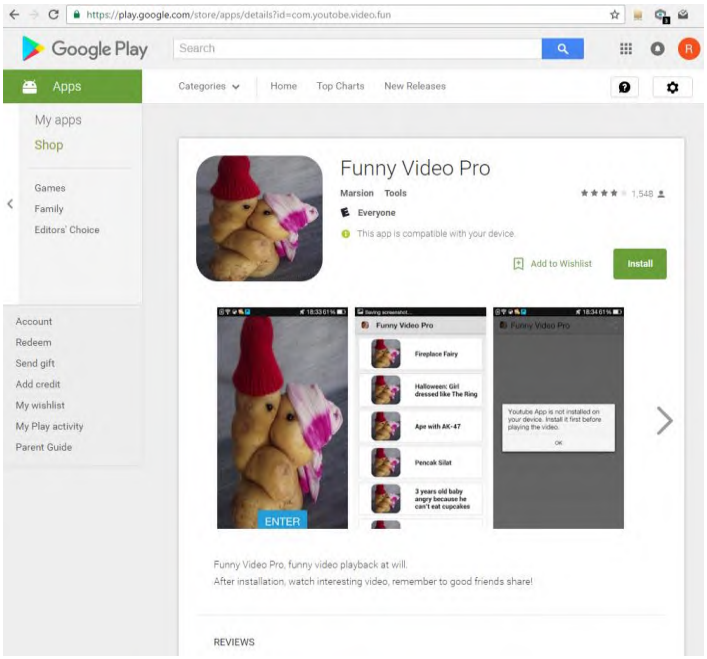
たいていサードパーティーのアプリストアを通じて拡散しますが、低価格帯のデバイスにあらかじめインストールされている場合もあります。2016年、このトロイの木馬がGoogle Playストアで配布される事態が起こりました。Google Playの統計によると、感染アプリは多くのケースで100,000回以上インストールされています。中には、Google Playで500,000回以上インストールされたアプリもあります。そこで使用されたPokemon GOガイドの感染アプリからは、Trojan.AndroidOS.Ztorg.amが検出されています。




Google Playストアで配布されたTrojan.AndroidOS.Ztorg.ad

## サイバー犯罪者は今でもGoogle Playストアを利用

サイバー犯罪者は今でもマルウェアの拡散にGoogle Playストアを利用しています。10月のわずか1週間のうちに、Kaspersky Labは Trojan.AndroidOS.Ztorg.am（Trojan.AndroidOS.Ztorg.adの改良版）に感染した新しいアプリをGoogle Playストアで10個以上発見しました。これらの新しいアプリは、100,000回以上インストールされていました。

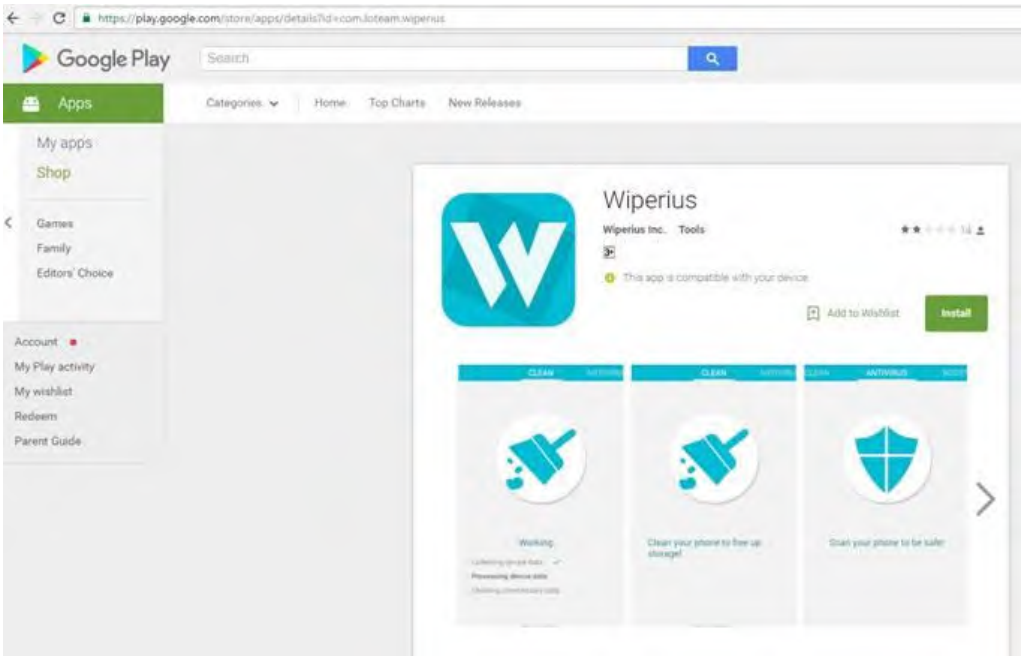



Google PlayストアでTrojan.AndroidOS.Ztorg.am

一方、Google Playではルート権限昇格を試みるマルウェアだけでなく、Trojans-PSWも配布されています。2015年10月、Kaspersky LabはGoogle PlayストアでTrojan-PSW.AndroidOS.MyVk.aを検出しました。この感染アプリは100,000回以上インストールされており、VKontakteソーシャルネットワークの音楽を再生するためのアプリに見せかけていました。ところが、実際にはユーザーからこのソーシャルネットワークの認証情報を盗み出していたのです。サイバー犯罪者らは2015年のうちに、このトロイの木馬の改良版をGoogle Playに複数回アップロードしています。セキュリティチェックをすり抜けるため、まずは有害な機能を持たないクリーンなアプリをアップロードしました。その後しばらくは感染していない更新プログラムを何度かアップロードした後、ある段階で感染プログラムをアップロードしました。サイバー犯罪者はこの手口を少なくとも2回使用しています。

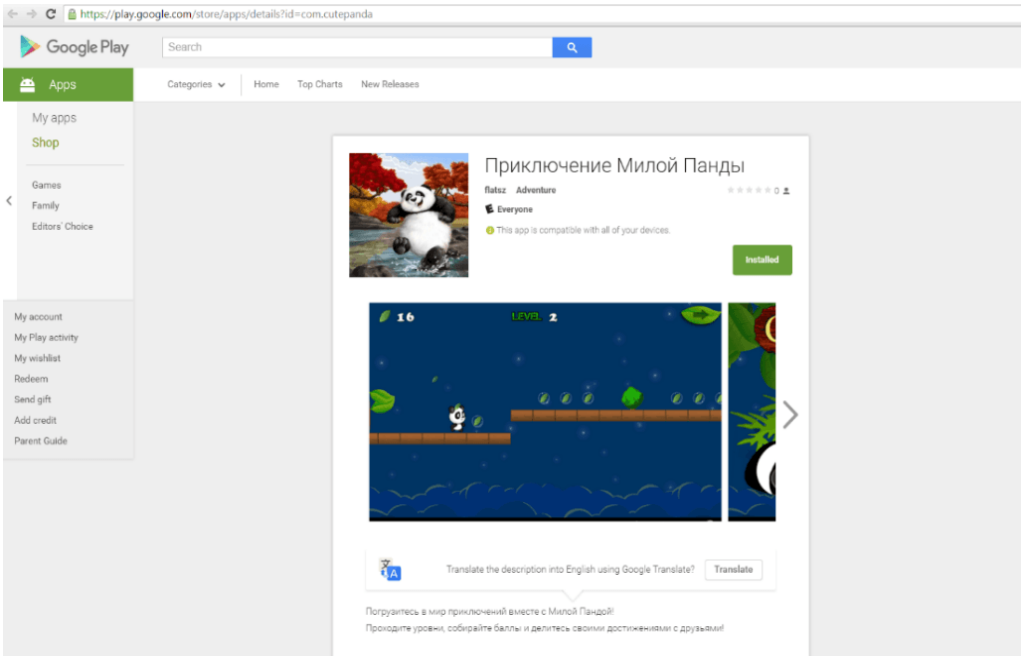
Google Playストアで配布されたもうひとつの認証情報窃取型マルウェアの例が、HEUR:Trojan-Spy.AndroidOS.Instealy.aです。この悪意のあるアプリは、ユーザーのプロフィール情報を誰が閲覧したのか知ることができるアプリと見せかけて、実際にはInstagramに接続するための認証プロセスに侵入していました。

Google Playストアで配布されたのは、ルート化マルウェアとTrojan-PSWだけではありません。弊社はさらに、サイバー犯罪者らがGoogle PlayでTrojan-Ransom.AndroidOS.Pletor.dを配布していることも突き止めました。




Google PlayストアでTrojan-Ransom.AndroidOS.Pletor.d

元々、Trojan-Ransom.AndroidOS.Pletorファミリーは、感染デバイスでユーザーのファイルを暗号化するものでしたが、この改良版では感染デバイスへのアクセスをブロックし、ユーザーに身代金の支払いを求めます。モバイルバンキングを狙ったトロイの木馬「Acecard」と同じサイバー犯罪者グループが「Pletor」を作成したことは、興味深い事実です。2015年12月、このグループはGoogle Playストアを利用してTrojan-Downloader.AndroidOS.Acecard.b（Trojan-Banker.AndroidOS.Acecard.aをダウンロードしてインストールするトロイの木馬）を配布しました。




Google PlayストアでTrojan-Downloader.AndroidOS.Acecard.b

## 注意すべきは Google Play ストアだけではない

広告型のトロイの木馬では感染後にスーパーユーザー権限を取得するためエクスプロイトを利用していましたが、配布のためにエクスプロイトを利用したマルウェアもいくつか存在します。

Kaspersky Labのパートナー企業、Bluecoatはエクスプロイトで配布されるTrojan-Ransom.AndroidOS.Fusobを発見しました。このエクスプロイトキットを利用すると、悪意のあるアプリをダウンロードしインストールすることができます。その後しばらくして、弊社が既知の脆弱性を悪用してマルウェアを配布しようとするサイバー犯罪者の存在を突き止めました。

また、Trojan-Banker.AndroidOS.Svpengを配布するために別の興味深い手段も使用されていました。そのケースでは、サイバー犯罪者らはGoogle AdSenseの広告配信ネットワークを悪用して、Trojan-Banker.AndroidOS.Svpeng.qを配布しました。Svpengは、フィッシング詐欺用のウィンドウからユーザーの銀行カードの情報を盗み取り、テキストメッセージの傍受、削除、送信を行うことができます。最も利用者の多いオンライン広告配信ネットワークで配布されたことから、Svpengは、2016年に最も多く発生したAndroid版のバンキング型トロイの木馬でした。また、全体で見ても、発生件数はルート化型のトロイの木馬に次ぐ第2位でした。

## セキュリティ機能の迂回

上記のとおり、2016年には一部のトロイの木馬がAndroidのセキュリティ機能を迂回する方法を新たに見つけています。

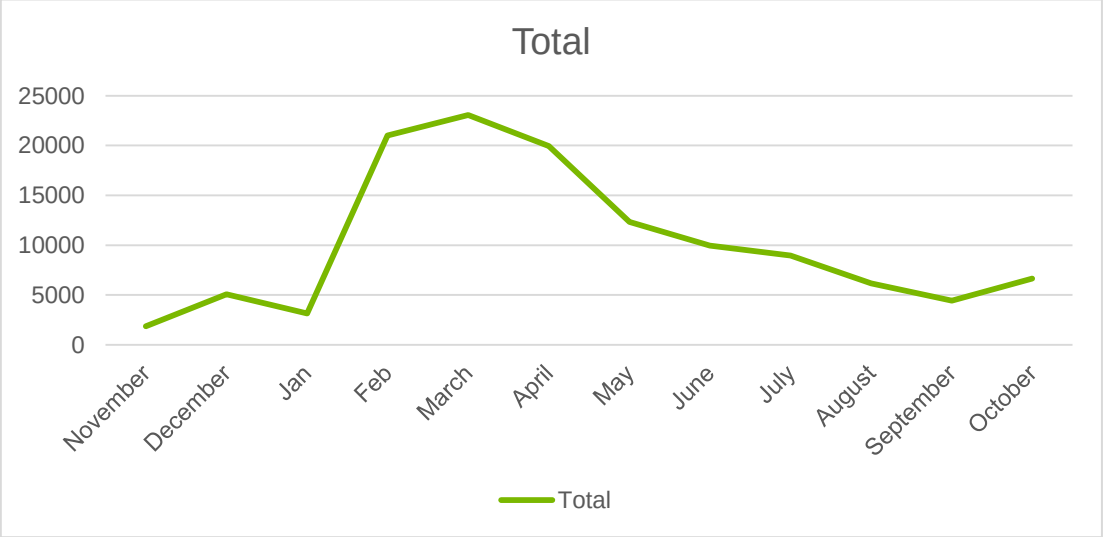
Android OSの最新バージョンでは、プレミアムレート番号(有料情報サービス)にSMSを送信する前にユーザーの承認が求められるようになりました。Tinyと呼ばれるSMS型トロイの木馬は、元のウィンドウに表示されているボタンはそのままに、このダイアログに独自の画面を重ねる方法をとっています。

同じ手法は、Trojan-Banker.AndroidOS.Asacubでも見られます。この場合、トロイの木馬は、元のボタンを残した状態で通常のシステムウィンドウに独自のウィンドウを重ねることで、デバイスの管理者権限を求めます。こうすることで、システム内で高い管理権限を取得しようとしている事実を隠し、ユーザーを欺いてこうした権限を承認させるのです。また、トロイの木馬「Asacub」はSMSのメッセンジャー機能を取得し、デバイスの標準的なSMSアプリに代わって独自のサービスを提供します。これにより、Android 4.4に初めて導入されたシステム制限をすり抜け、受信したSMSを勝手に削除したり、ユーザーから隠したりすることができます。

2016年6月、Kaspersky LabはTrojan-Banker.AndroidOS.Gugiの新しい改良版を発見しました。このトロイの木馬は、Android バージョン 6に新たに追加された2つのセキュリティ機能(権限許可に基づいてアプリを重ねて表示できる機能、そしてSMSや通話などアプリ内での危険な活動に対して、動的に許可を求める機能)を迂回する能力を持っています。改良版では脆弱性を悪用せず、ソーシャルエンジニアリング手法のみを使用しています。

## モバイル版ランサムウェア

2016年に最も発生件数の多かったモバイル版トロイの木馬型ランサムウェアは、Trojan-Ransom.AndroidOS.Fusobでした。最も活発に配布されたのはドイツ、米国、英国で、CISおよび近隣諸国での活動はないものとみられます。犯罪者は通常、デバイスのブロックを解除するために100ドルから200ドルの金額を要求します。身代金は、iTunesのプリペイドカードに印字されているコードを提供する形で支払わなければなりませんでした。このトロイの木馬は、2015年11月から2016年3月にかけて発生件数が大幅に増加しました。同期間中に攻撃を受けたユーザーの数は12倍に増えましたが、その後は前年と同程度の発生件数まで減少しています。




Trojan-Ransom.AndroidOS.Fusobの攻撃を受けたユーザー数の推移

攻撃を受けたユーザーの数はモバイル版「Ransom」よりモバイル版「Banker」のほうが多い一方で、インストールパッケージの受領件数に関しては逆の現象が起こっています。2016年第2四半期以降、「Trojan-Banker」より「Trojan-Ransom」のほうが受領件数が増えていました。

最初のモバイル版トロイの木馬型ランサムウェアはユーザーのファイルを暗号化し、その暗号化を解く代わりに金銭の支払いを求めるものでしたが、最近のAndroid版「Trojan-Ransom」はユーザーのファイルを暗号化しません。他のすべてのアプリよりも上に独自のウィンドウを表示し、システムダイアログすらも重ねて表示します。モバイルデバイスの暗号化がそれほど行われなくなった背景として、クラウドサービスでのデータバックアップが一般的になったことが考えられます。すべてのウィンドウに独自のウィンドウを重ねて表示する通常の「Trojan-Ransom」はきわめて効果的であり、このトロイの木馬を駆除することは大変困難です。

中国で最も発生件数の多いモバイル版ランサムウェアのファミリー、Trojan-Ransom.AndroidOS.Congurは、別の方法で感染デバイスをブロックします。起動後にデバイスの管理者権限を要求し、PINコードを変更したり、（事前にPINコードが設定されていない場合は）新たに設定したりします。QQメッセンジャーでサイバー犯罪者に連絡を取るよう求め、新しいデバイスのPINコードを聞き出します。この方法は一見シンプルですが、効果的です。

「Trojan-Ransom」は技術的に最もシンプルでありながら、効果的なトロイの木馬のひとつです。こうした理由から、KasperksyLabはこのトロイの木馬が引き続き増加し、来年新たな「Trojan-Ransom」ファミリーがさらに登場すると予想しています。

## 情報漏洩

個人情報は価値のある資産です。サイバー犯罪者が一度の攻撃で大量のデータを窃取するため、オンラインプロバイダーを狙うのは当然のことといえます。メディアで絶えず報道されるセキュリティ侵害のニュースもすっかりおなじみになりました。2016年も状況は変わらず、beautifulpeople.com、Tumblr、nulled.ioのハッカーフォーラム（標的となるのは合法的なシステムだけではありません）、Kiddicare、VK.com、Sage、DotA 2公式フォーラム、Yahoo、Brazzers、Weebly、Tesco Bankで情報漏洩が発生しました。

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。これは企業組織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。

顧客は、自分がオンラインプロバイダーに開示した個人情報を直接守ることはできません。一方、他にはない複雑なパスワードを選択することで、オンラインプロバイダーでのセキュリティ侵害の被害を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。それも難しいと感じる場合は、安全で覚えやすいパスワードを作成するための有益なヒントを参考にしてください。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。

残念ながら、あまりにも簡単に推測できるパスワードを選んだり、複数のオンラインアカウントで同じパスワードを使いまわしたりする人が多くいます。これでは、1つのパスワードが乗っ取られると、すべてのIDが危険に晒されてしまいます。この問題は、2016年5月に「Peace」というハッカーが数年前に盗まれたLinkedInの電子メールとパスワード1億1,700人分を転売しようとした事件で大きく取り沙汰されました。盗まれた100万件以上のパスワードが「123456」だったのです。

Kaspersky Labは7月、Ashley Madisonのデータ侵害事件がもたらした影響を振り返りました。利用者データの漏洩を引き起こした攻撃から1年が経ち、出会い系サイトを利用しようとするユーザーにとって、また、あらゆるオンラインアカウントを管理するユーザーにとっても役立つアドバイスになることでしょう。

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。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。

セキュリティ侵害がもたらしうる影響を考えると、規制当局がこの問題に意識を向けるのは決して驚くようなことではありません。英国情報コミッショナーオフィス（ICO）は最近、通信会社Talk Talkに史上最高額となる400,000ポンドの罰金を科しました。Talk Talkでは、2015年10月にサイバー攻撃を受けた際、基本的なサイバーセキュリティ対策すらも講じていませんでした。ICOは、この史上最高額の罰金が「サイバーセキュリティはITの問題でなく、経営者側の問題であることを他社にも警告する意味合いがある」との見解を示しています。

2018年5月に施行されるEUの一般データ保護規則（General Data Protection Regulation：GDPR）の規定によると、情報漏洩が発生した場合、企業は規制当局に通知しなければならず、個人情報を保護できなかった企業には多額の罰金が科せられることとされています。本規則の概要は、こちらからご覧いただけます。今後、情報漏洩に関する報告が適時に行われるようになることが期待されます。2016年、Dropboxが多くの利用者にパスワード変更を求める通知を送ったことから、この問題が浮き彫りになりました。2012年にDropboxで発生したセキュリティ侵害により、電子メールアドレスのみならず、パスワードも流出しました。当時、電子メールアドレスの流出については利用者に通知がありましたが、パスワードに関しては伏せられていました。幸い、パスワードはハッシュやソルトの手法で保護されており、Dropboxは2段階認証を導入しています。

企業によっては、パスワードを完全に廃止しようとする動きもあります。Appleでは、iTunesでの購入やApple Payでの支払いに指紋認証を導入しています。Samsungは、今後Samsung Payに指紋認証、音声認証、虹彩スキャンを導入すると発言しています。Amazonは、「selfie-pay」の導入を発表しました。MasterCardとHSBCは、顔認証と音声認証による取引承認システムの導入を発表しています。一番のメリットは何といっても、これまで利用者が*記憶*しなければならなかったもの（パスワード）を、自分の持っているもので代用できるという点です。これなら、（弱いパスワードを適当に選んで）認証プロセスの手間を省こうとすることもできなくなります。

バイオメトリクス（生体）認証は、一般に先進的な方法だと考えられています。ところが、この方法ですらセキュリティ対策としては万全ではありません。前に紹介したとおり（こちらとこちらとこちらをご覧ください）、生体情報もなりすましに遭ったり、盗まれたりすることがあります。生体情報はパスワードではなく、ユーザー名に代わるものと考えるとよいでしょう。結局のところ、ユーザーが知っている情報、ユーザーが持っているもの、ユーザー本人を表すものを組み合わせたマルチファクター認証が不可欠です。

# 産業インフラのサイバーセキュリティ：脅威とインシデント

2016年は産業分野で発生したサイバーセキュリティインシデントの件数と深刻度の点で、それほど特筆すべき年ではなかったかもしれません。以下に、Kaspersky Labが特に注目すべきケースを紹介します。

## インシデント

2016年は原子力発電所でのサイバーセキュリティ問題が2回取り沙汰されました。1件目は、4月末に発生したインシデントです。ドイツ・グンドレミンゲン原子力発電所の運営会社がB棟制御システムのコンピューターでKido（別名Conficker）ワームへの感染が確認されたと報告しました。感染したのは、核燃料棒の制御システムに属するコンピュータでした。幸い、ワームは技術的な工程に影響を及ぼすものではなく、原発に損害はありませんでした。

本件は、関連する監視当局とドイツ情報セキュリティ庁（BSI）に通報されました。すべての重要システムとデバイスを確認したところ、悪意のある感染の兆候は見当たりませんでした。このインシデントを受けて、セキュリティ対策の拡充が行われました。本インシデントは、ドイツの報告基準でカテゴリーN（正常）に分類されています。国際原子力事象評価尺度（INES）では、レベル0（分類に満たない、安全上の重大性はまったくないか、極めて低い）に分類されます。

感染源は公表されていませんが、本原子力発電所の広報担当者は、オフィスネットワーク内で使用されていた18個のUSBデバイスが同じKidoワームに感染していたことを明かしています。この広報担当者によると、原発の重要な制御システムはすべて分離しており、システム設計全体がサービス妨害（DoS）に対して冗長で、乗っ取りから守られていたことから、損害が生じなかったといいます。

ただし、このケースでは（幸いなことに）Kido感染から深刻な損害が起こらなかっただけのことであり、標的を絞った専用のマルウェアのみが損害をもたらすものと考えてはいけません。2015年の年末、ウクライナの変電所が極めて組織的なサイバー攻撃を受けました。犯人は、電力会社の管理またはITネットワーク内にいる個人に、エクスプロイトを添付したスピアフィッシングメール（標的型攻撃メール）を送りつけていました。最初のコンピューター感染が起こると、犯人はすぐOTネットワークに侵入し、電力供給を中断させました。このケースで重要なのは、犯人がグリッドネットワークへのリモートアクセスを完全に遮断したことです。特定のエンジニアリングソフトウェアを消去し、システムのブートセクターを破壊することで、システムをリモート操作で管理したり、修理したりすることができないようにしました。

もしマルウェアが技術的な工程に影響を及ぼさず、SCADAやOPSゲートウェイ、リモートアクセスなどの重要な補助システムにサービス妨害（DoS）を引き起こしたとしても、ICS

はおそらく最新の設定で機能し続けるでしょう。しかし、万一事故や緊急事態が起きた場合に、システムの工程は制御不能となり、修正することもできなくなるかもしれません。

数か月前、国際原子力機関（IAEA）の天野之弥事務局長が、2～3年ほど前にある原子力発電所がハッカーによる攻撃を受けていたことを明かしました。天野事務局長は、「これは実際に起こったことで、問題を引き起こしました。その原発の操業を停止するには至りませんでしたが、何らかの予防策を講じる必要がありました」と述べています。しかし、これは単に原子力発電所における混乱を引き起こすサイバーセキュリティの問題ではありません。ICSとサイバーセキュリティ業界のコミュニケーション不足と透明性の欠如がもたらした、もっと大きな問題であることは確かです。結局、サイバーセキュリティの専門家には問題を分析する機会はなく、ICSの責任者とベンダーはインシデントの発生に備えてリスク軽減措置を導入するに至っていません。

## PLC を狙うマルウェアの PoC

2016年8月、Black Hat 2016カンファレンスの席で、OpenSource Securityチームのリサーチャーらが PLC（プログラマブルロジックコントローラー）ワームの PoC（概念実証）を紹介しました。PLCプログラムとしてのみ作成されたこのワームは、ネットワーク内で自力でPLCを特定し、PLC間で次々と拡散していきます。また、PLCの入出力を操作し、PLCのサービス妨害（DoS）を引き起こし、C&C（コマンド＆コントロール）サーバーに接続し、プロキシとしての役割を果たして攻撃を拡大させることが可能です。

このPoCの最も注目すべき点は、PLCに感染するための手法です。このPoCは、アクセス保護機能を備えたSiemens S7-1200コントローラーに対して作成されました。アクセス保護機能をオンにすると、S7CommPlusプロトコルを使用してPLCのアクセスに必要なパスワードを設定することができます。こうして、適切な権限を持たない者がPLCのコードを読み取ったり、変更したりすることを防ぎます。ところが、アクセス保護機能は初期設定でオフになっています。この機能をオンにした場合、ワームがPLCに感染するための唯一の方法は、片っ端からパスワードを試すか、何とかして盗み取ることしかありません。

それに対し、もしアクセス保護機能がオフになった状態でも、PLCへのアクセスを制限するために設計された保護機能がさらに2つ備わっています。

- デバイスからのPLCプログラムの抽出と変更を禁止する「ノウハウプロテクション」
- PLCプログラムを他のPLCデバイスに複製することを禁止する「コピープロテクション」

両方の保護機能（「ノウハウプロテクション」と「コピープロテクション」）に対するアクセス検証は、クライアントサイド（TIAポータル内）で導入されていました。ということはつまり、このシンプルな自己生成ツールは、認証チェックをすり抜けて、PLCに対してブロックの

読み出しと書き込みを行うことができてしまうということです。Siemensはセキュリティ勧告を公表し、S7-1200ファームウェアの修正パッチを提供しました。

このケースの重要な教訓は、いかに完成度の低いデバイスや攻撃者であっても、ひとたびICSネットワークにアクセスできれば、制御システム全体をいとも簡単に攻略してしまうということです。また、PLCデバイスはSCADAまたはエンジニアリングソフトウェア以外のツールとの通信を想定していないため、攻撃（特にDoS）を受けやすい傾向にあります。そのため、不正アクセスや入力の問題、悪意のある操作に対する防御方法をほとんど持ち合わせていません。

## ICS ソフトウェアとハードウェアのゼロデイ

2015年度（2015年10月から2016年9月）発行の米国ICS-CERTのデータによると、脆弱性の報告件数は2014年度は245件、2015年度は427件でした。脆弱性の約25%は入力情報の不適切な検証、27%は不十分なアクセス制御によるものでした。この他に脆弱性の中で大きな割合を占めていた「設定」と「運用」の問題については、多くのベンダーが責任を放棄しています。初期設定の認証情報、初期設定のセキュリティ設定（オフになっていることが多い）、隠れたAPI、マニュアルに記載されていない機能などの脆弱性は、高い技術力を必要とせず、制御システムへの幅広いアクセスを可能にすることから、非常に危険です。

残念なことに、ベンダーに脆弱性が報告されてから修正パッチが公開されるまでにきわめて長い時間を要します。場合によっては、ベンダーが脆弱な製品の製造を中止したと主張して、修正パッチを提供しないこともあります。そうなった場合、ICS責任者は莫大な費用をかけて近代化を進めるか、セキュリティ犯罪の被害に甘んじるか、いずれかの道を選ばなければなりません。

結論として、セキュリティリサーチャーのコミュニティが、ICSのサイバーセキュリティに貢献することの重要性を強調したいと思います。ここ数年で、ICSのセキュリティに対する関心が大幅に高まってきました。毎年数多くの調査レポート、ツール、枠組みが公表されています。たとえば、Kaspersky Labは2016年に産業インフラのサイバーセキュリティに対する脅威の動向をまとめた独自のレポートを公表していますが、これはICSに限らず様々な分野を専門とするサイバーセキュリティスペシャリストの方々の経験と知識の一助になると考えています。