トレンド

フォーティネット

2013年の脅威予測をFortiGuard Labsが発表

～モバイル端末を狙うAPT攻撃、IPv6によるセキュリティ確保、マシン間通信を介したエクスプロイトなどの傾向を予測～

ネットワークセキュリティのリーディングプロバイダーであり、UTM（Unified Threat Management：統合脅威管理）ソリューションの世界的リーダーである、フォーティネット（Fortinet,Inc.本社：米国カリフォルニア州サニーベール）は、2012年12月に、FortiGuard Labsの2013年における脅威予測を発表し、来年警戒すべき6つの脅威を指摘した。

【1】APT攻撃、モバイルプラットフォーム経由で個人を攻撃　APT攻撃とは高度かつ継続的脅威と定義されており、高度な技術と複数の手法を使って、センシティブな情報や極秘情報を入手するために特定の標的を攻撃するのが特徴だ。最近の例では、StuxnetやFlame、Gaussなどがある。2013年にはCEO、有名人、政界実力者を含む、一般市民を標的にしたAPTの出現が予測される。しかし、アタッカーは求めていた情報を入手後、攻撃があったことを被害者が気づく前に、標的にした機器からマルウェアをひそかに消してしまうことができるため、この予測が正しいと証明するのは困難だ。さらに、APT攻撃の被害にあったことに気づいた被害者がいたとしても、メディアにその情報を伝えない可能性が高いと思われる。こうした攻撃は重要なインフラストラクチャや政府、上場企業を直接狙うのではなく、まず個人を狙うため、標的となる情報の種類が異なる。アタッカーは支払いがなければ情報をリークすると恐喝するなど、犯罪行為に使う情報を狙っている。

【2】二要素認証が単一パスワード式サインオンのセキュリティモデルに取って代わる　パスワードのみのセキュリティモデルはもう終わりに来ている。最近では簡単にダウンロード可能なツールを使えば、4～5文字のシンプルなパスワードなら数分で解読できてしまう。クラウドベースの新たなパスワードクラッキングツールを使えば、アタッカーは20米ドル未満のコストで、たった20分以内に3億通りのパスワードを試みることができるのだ。破られにくい記号と英数字を組み合わせたパスワードでさえ、昼休みの間に解読することが可能だ。こうしたクラウドサービスを使ったクラッキングの一般的な標的となるのは、データベース（WebポータルやSQLインジェクションを介した不正アクセスがよくある）に暗号化して保管されている認証情報だろう。2013年は従業員や顧客に対して何らかの二要素認証を採用する企業が増加すると予測される。二要素認証とはパスワードが必要となるWebベースのログインと、ユーザーのモバイル端末か独立型のセキュリティトークンを介して入力される二次パスワードが必要となる認証方式だ。最近、AndroidデバイスのRSAのSecurID認証トークンがボットネットのZitmoにクラックされたのは確かだが、このタイプの二段階方式がいまだにオンラインでの活動を保護する最も有効的な手法だ。

【3】マシン間（M2M）通信を標的とするエクスプロイト　マシン間（M2M）通信とは、ワイヤレスシステムと有線システムが、同等の機能を持つ他のデバイスと通信を行えるようにする技術を指す。ホームサーバと通信して牛乳や卵を購入するタイミングを住人に知らせる冷蔵庫であったり、顔写真を撮ってその画像をテロリストのデータベースと照合する空港のスキャナーだったり、事故の犠牲者への酸素供給量を調整し、その人の心拍数が特定のしきい値を下回ると病院のスタッフに警告する医療機器のような技術だ。

M2Mは多くの場面において人的ミスを取り除ける可能性を有しているため、その実用技術の可能性には魅力があるが、技術を最も効果的に保護する方法についてはいまだ多くの疑問がある。まだ攻撃を受けていないM2Mが、2013年はおそらく初めて攻撃を受けることになると予測される。兵器開発施設のような、国の安全保障に関連するプラットフォームで行われる可能性が高い。これにはおそらく、M2Mのチャンネルを横断する情報の流れを汚染させる方法が用いられるだろう。つまり、1つのマシンに汚染情報を誤処理させることで脆弱性をつくり出し、アタッカーがこの脆弱なポイントからアクセスできるようにする手法だ。

【4】エクスプロイト、サンドボックスを迂回　サンドボックス化とは不正なコードが1つのプロセス（例えば、ドキュメントリーダー）から別のプロセス（例えば、オペレーティングシステム）へ移動できないようにするため、実行中のプログラムとアプリケーションを分けるセキュリティ対策技術だ。AdobeやAppleなどのベンダーはこのアプローチを採用しており、今後さらに多くの企業がそれに続く可能性が高い。導入が進むにつれ、アタッカーは当然この技術の迂回を試みる。FortiGuard Labsではすでに、Adobe Reader Xの脆弱性など、仮想マシン（VM）とサンドボックス環境を迂回することのできるエクスプロイトをいくつか確認している。最近のサンドボックスのエクスプロイトでは、ステルスモードのままとどまっていたものか（マルウェアコードがまだ開発中かテスト中であることを示している）、どちらの技術をも迂回しようと積極的な試みを行ったものがあった。2013年は、特にセキュリティ装置やモバイル端末が使用するサンドボックス環境を迂回するよう設計された、革新的なエクスプロイトコードが登場するだろう。

【5】クロスプラットフォームなボットネット　2012年、FortiGuard LabsではZitmoなどのモバイルボットネットの分析を行い、従来のPCボットネットと同様の特徴や機能を数多く発見した。異なるプラットフォーム間に見られるこうした特徴の類似性から、2013年にはPCとモバイル端末に同時に影響を及ぼす、新型のサービス妨害（DoS）攻撃が登場することになるだろうと予測される。例えば、感染したモバイル端末とPCが同じコマンドアンドコントロール（C&C）サーバや攻撃の手順を共有し、同じコマンドで同時に実行され、ボットネットの威力を増大させるというものだ。PCとAndroidのようなモバイルのオペレーションシステム上で別々に実行されていた2つのボットネットが、複数種類のエンドポイントで活動する単一のボットネットになるということだ。

【6】モバイルマルウェアの成長、ラップトップやデスクトップPCに迫る　現在はモバイル端末を狙うマルウェア、ノートブック／デスクトップPCを狙うマルウェアのどちらもが存在している。しかし、PCは数多く流通しており、また登場してからの期間がはるかに長いため、歴史的にはマルウェアの大部分がPC向けに開発されてきた。FortiGuard Labsの研究者たちは、現在、何百万というPCのマルウェアサンプルを監視しているが、モバイルマルウェアに関しては、監視しているサンプルの数は約50,000となっている。研究者たちはすでにモバイルマルウェアの数の大幅な増加を観測しており、現在ではノートブックやデスクトップPCよりも多くの携帯電話が市場に出回っており、さらにはユーザーがより新しい、より小さなタブレット端末を好んで従来型のPCを選ばなくなっていることから、この差は2013年以降さらに劇的に変化するだろうと考えられる。PCのマルウェアサンプルの数にモバイルマルウェアのサンプルの数が追いつくまでに数年はかかるとFortiGuard Labsの研究者たちは考えているが、今日のモバイル端末を保護するのは従来のPCを保護するよりも複雑であることをマルウェア作成者たちはわかっており、そのためモバイル端末に対するマルウェアの増加が加速するだろうと予測している。

●お問い合せ先●
フォーティネットジャパン㈱
TEL：03-6434-8542
E-mail：mktg_jp@fortinet.com
URL　http://www.fortinet.co.jp/