アンラボ・セキュリティレター

Press Ahn

2014.1　Vol.01

終わりなきサイバー攻撃「多様化・高度化・加速化」

終わりなきサイバー攻撃「多様化・高度化・加速化」

2013年の情報通信環境はあまり安全とはいえなかった。特定の組織を標的に徹底的な分析と戦略的な侵入を試みる「APT(Advanced Persistent Threat)」攻撃が増加する一方、不特定多数に向けて無差別にマルウェアを配布したり、様々なタイプのモバイル端末に侵入を試みるマルウェアも増加している。金融情報を奪取して不正に金銭的な利益を得たり、会社の重要な機密情報や技術を流出し、国家の重要な人物に関する情報を監視する経済・政治的な行為も見られた。これら深刻化するインシデントの数々を見ると、侵入手法も技術的に高度化、緻密化していることがわかる。

個人と組織、国内外の地理的な要素、ソフトウェアやハードウェアなど、もはやマルウェアにとって侵入できない制約はないに等しい。特に昨年のセキュリティ市場では、これら制約の境界が崩れる様相を見せており、2014年にはこの傾向がさらに強くなると予想される。アンラボのセキュリティ専門家がセキュリティ脅威2014年の動向を展望した。

2014 年の脅威予測 : 攻撃には「境界なし」

1. APT攻撃手法の高度化、不特定多数向けの攻撃も拡大

昨年登場したマルウェアの多くは、ユーザーのシステム情報を変更した後、偽の金融サイトに誘導してユーザーの財務情報を奪取する手法を使用した。またオンラインゲームマネーを奪取するためのOnlineGameHackと、財務情報を抽出するためのBANKERの機能が区別できない程に似てきている。マルウェア感染が実際に金融業のインシデントに繋がるケースが増えており、マルウェア作成の目的が金銭的利益のための露骨な攻撃に変化していることがわかる。

上記二つのマルウェアタイプの変化を見ると、今後はAPT攻撃と区別がつかないほど類似していたり、複合的なタイプのマルウェアが登場するだろう。したがって2014年のAPT攻撃は、以前のように特定のターゲットを対象にした標的型攻撃と共に、不特定多数を対象とする広範囲な攻撃も行われると予想されている。また、従来のAPT攻撃と水飲み場型攻撃(Watering Hole)の境界も崩れていくだろう。特に金銭的利益のために無差別にマルウェアを配布してBitcoinマイニングを試みる可能性もある。

2. 電子金融詐欺とサイバー犯罪の産業化

昨年はマルウェアを利用した電子金融詐欺として、フィッシング、ファーミング、ボイスフィッシング、スミッシング、メモリハッキングなど様々な手法が使用された。これらの多様な攻撃手法は、ユーザーの金融情報と預金を奪取するためにますます高度化している。もはや、マルウェアは単に作成者の実力を見せ付けるための道具に留まらず、オンライン上で経済的な被害を与えるツールとしてサイバー犯罪の産業化に使用されている状況だ。2014年にも、マルウェア作成者はアプリケーションの脆弱性や通常プログラムの改ざん、USBなどの外部記憶装置の不正アクセスなど様々な手法でマルウェアを大量に配布し、オンライン金融サービスを対象にした攻撃も続けて増加するものと予想される。

3. マルウェアの配布方法が多様化・高度化

2014年にはマルウェアの配布手法も、より高度化されるだろう。これまではプログラム更新の際に発生する脆弱性やスピアフィッシングなどを通じて不特定多数を対象にマルウェアを配布し、目的に応じて亜種を拡散させる方式だった。今年は従来の手法に加えて、簡単に大量のマルウェアを配布する新たな手法が登場する可能性が高い。例えば多くのユーザーが接続するCDNやドメイン管理業者、ISP管理プロバイダを通じて多数のマルウェアを配布する方法も考えられる。このような大胆な攻撃を仕掛けるためには、まず攻撃者がVPNサービスや国内のドメインアドレスを申請する。

オンラインサービスの中には、別途の本人確認や認証なしに課金の有無だけでサービスの使用を許可するものもある。このため、国の主要システムや多数のシステムを攻撃する悪意ある目的で作成された有害サイトの活動を根本から遮断することは難しい。

また攻撃者がCDNやドメイン業者、特定のISPで管理するサービスシステムに侵入して脆弱なコンテンツや製品のアップデートファイルを改ざんし、ドメインとサービスを介して同時にマルウェアを配布することも考えられる。2014年には、ドメイン登録や管理手順および管理者ネットワークのインシデント認知に関する注意が特に求められる。

4. Windows XP サポート終了によるセキュリティリスクの増加

2014年4月にはWindows XPのサポート終了が予定されている。その後は発見された脆弱性に対するセキュリティパッチも更新されることなく、ゼロデイ攻撃に対して無防備状態なることが予想される。このことから、サポート終了後のセキュリティリスク対する保護は、

PC用のセキュリティソリューションに完全に依存することになる。

現在Windows XPでは、IE9以上のバージョンがサポートされず、マルウェアに感染されやすいIE6～8バージョンが主に使用されている。日本では2013年時点でWindows XPのOSシェアが約2割だとされているため、ユーザーはサポート終了前にWindows 7または8に移行する必要がある。

5. 特定の標的を監視したり、情報を流出する「スパイアプリ」増加

2013年にはSMSやモバイルSNSを介して誕生日、結婚式などのイベント招待状や宅配便、銀行・企業のお知らせメッセージに偽装したスミッシング手法によるマルウェア感染が急増した。このマルウェアは多くのユーザーに配布するために作成され、公開的に配布されたために比較的容易に発見されたケースだった。しかし企業の機密漏えいや監視を目的に作成されたスミッシングマルウェアが、特定のユーザーを対象に配布される場合は、その存在を外部からは把握しにくい。

特にプライベートやビジネス的にも多くの情報が保存される携帯用のデバイスは使用率に比例して、ユーザーを監視したり必要な情報を盗むのに最適といえる。このことからもモバイル用のマルウェアを活用して特定の標的を監視したり、情報を奪取するスパイアプリが増加すると思われる。

6. サイバー情報に関する国家レベルのパラダイム変化

2013年にはアメリカ国家安全保障局(NSA)の広範囲な情報収集活動を暴露したエドワード・スノードンの秘密文書と、中国人民解放軍の組織がアメリカを拠点とする約141以上もの機関データを流出するなど、国家レベルの情報収集事件が発覚した。国を対象とした数多くの盗聴・監視の実態が明らかになり、国家間サイバー戦争はさらに激化していくものと予想される。

国家機関が敵・友好国を問わず情報収集活動を行うことは珍しくないかもしれないが、疑惑ではなくその実体が公けになってしまったことで、自国の利益を得るための国レベルの動きは加速していくだろう。また高度化された攻撃やデータ漏えいの被害を軽減するため、暗号化技術に加えてより進化したセキュリティ技術が求められている。

7. ハードウェアBIOSやファームウェア更新にマルウェアを挿入

2013年4月、某BIOS製造会社のソースコードが奪取される事件が発生した。同年10月には、ある会社のルーターのファームウェアにバックドアが含まれていたこともあった。またロシアに輸出された中国産アイロンとケトルがWi-Fi経由でスパム攻撃を実行した事件も話題になった。

このようにハードウェア内蔵型のソフトウェアを介したハッキング機能を実行する可能性も高まっている。タブレットPCなどの電子機器は、製造会社から配布されたファームウェアをダウンロードして更新するが、メーカーが開発からアップロードに至るまでの全過程を完璧に管理できているか保証できない状況だ。もちろんダウンロードパスに不正コードを挿入するには、メーカーが意図的に作成するか内部に共謀者がいてこそ可能だ。内部の協力なしに攻撃をするには、アタッカーが内部システムに侵入してコードを改ざんすることになるため、ハードウェアにマルウェアが挿入される可能性は低い。だが、機能レベルで悪意ある機能が挿入される場合は発見が難しい。そして国家間サイバー攻撃の存在が徐々に知られ、従来のサイバー犯罪者だけでなく国家機関でも情報収集のためにハードウェアのメーカーを利用することについて疑惑が広がっている。

マルウェアを挿入するためにはいくつかの段階を経る必要があり、実行はそう簡単ではない。

だが、2014年はハードウェアやファームウェアなどにマルウェアや不正機能を実行するコードが挿入される可能性も高い。

http://www.ahnlab.co.jp

http://global.ahnlab.com

http://www.ahnlab.com

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒101-002 東京都千代田区外神田4-14-1 秋葉原ＵＤＸ ８階北 | Tel：03-5209-8610 (代)