トレンド

フォーティネットジャパン

2012年の上位8つのセキュリティ予測を公表

～モバイル ランサムウェア、Androidワームなど、増加するハクティビズム（社会的・政治的なハッキング行為）の脅威を予測

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、昨年末、脅威に関する統計およびトレンドを収集・集計しているFortiGuard Labsによる2012年の脅威予測を公表し、警戒すべき8つの脅威を指摘した。

【1】モバイル デバイスを人質にとるランサムウェア

「ランサムウェア」は「ランサム（身代金）」の支払いが完了するまでデバイスを「人質」に取るマルウェアだが、この脅威は長年にわたってパソコン上で発生してきた。感染したデバイスのルートアクセスを奪取するソーシャルエンジニアリング行為と一緒に、セキュリティ上の弱点を突くモバイル マルウェアも発見されてきた。ルート アクセスがより厳しくコントロールされアクセス権が制限されていることが、ランサムウェアのようなマルウェアにとって好ましいそうだ。FortiGuard Labsは、2012年にはモバイルデバイス上でランサムウェアの最初の発生を発見するだろうと予測している。

【2】Androidへのワーム攻撃

ワームはデバイスからデバイスへ素早く拡散するマルウェアだが、Android OS上にはこれまで存在していなかった。FortiGuard Labsは、2012年にこの状況は変わると予測している。2004年に発見された最初のSymbianワームであるCabirと違って、Androidマルウェアの開発者が、拡散方法に制限のあるBluetoothやコンピュータ同期を使う可能性はほとんどないと思われる。その代わり、SMSメッセージ内や、FacebookやTwitterなどのソーシャルネットワーク上にワームに感染したリンク先を通して、こうした脅威は入ってくるとFortiGuard Labsのチームは予測している。

【3】Polymorphismはクラッカーを望むか？

2010年、FortiGuard Labsは、Androidマルウェアが暗号を使用し、攻撃コードを組み込み、エミュレーターを検知し、ボットネットをインストールしていることを発見した。しかし、ポリモーフィズムの例はこれまで発見されていなかった。ポリモーフィズムは自動的に突然変異することができるマルウェアで、特定し駆除することを極度に難しくするものである。FortiGuard Labsのチームは以前、Windowsモバイルフォン上でポリモーフィズムに遭遇しており、このマルウェアがAndroidデバイス上に現れるのも時間の問題だと考えている。

【4】ネットワークベースのマネーロンダリングに対する取締り

匿名の送金サービス、人的ネットワークやペイメントプロセッサ（決済会社）の情報秘匿性を使用して、サイバー犯罪組織は長年にわたって、摘発されることなく自由に活動し続けてきた。FortiGuard Labsは、2012年には多くのサイバー犯罪者が追跡され、逮捕されると予測している。ChronoPayのCEOであるPavel Vrublevskyが、AerfolotのWebサイトをハッキングし、訪問者がチケットを買うのを妨害していた、まさにその時に逮捕された最近の事件は、FortiGuard Labsのチー

ムが予測している取締りの良い例であるそうだ。

【5】セキュリティ分野での官民の連携

2011年、FortiGuard Labsは、RustockやDNS Changerを含むグローバルに展開するボットネットの解体が増えていきていることを確認した。この解体と同時に、AnonymousやLulzSecという国際的なハッキング集団のメンバーが逮捕された。このような取締りは2012年においても継続すると予測されており、FortiGurard Labsのチームは、その多くが米政府直轄研究機関である国防高等研究計画局（DARPA）の公的防御イニシアティブの支援を受けて実施されるだろうと見ている。DARPAは、最近、18,800万米ドルの予算を確保しており、民間セクターでサイバー犯罪防御チームを立ち上げるイニシアティブにその予算の一部を投入することを計画している。2012年においても、引き続き、同様な官民の連帯が世界中で形成されると予測している。

【6】攻撃の視野に入ったSCADAの脅威

10年以上にわたって、SCADA（Supervisory Control And Data Acquisition）ベースの脅威は悩みの種であった。その理由は、多くの場合、電力や水道のグリッドなどのクリティカルなインフラに接続されているためだ。注意しなければならないことは、これらのインフラは常に閉ざされたネットワーク上で運用されているとは限らないことだそうだ。多くの新しいヒューマン・マシン・インタフェース（HMI）を持ったデバイスがこのようなインフラシステムと相互接続されており、ログインのためのWebインタフェースを利用している。バックエンドシステムに直接アクセスすることはできないが、Anonymousのような集団は、ターゲットを選びコードを調べることで、Webベースの脆弱性の組み合わせを既に発見していた。2012年内には、FortiGuard Labsは、潜在的な破壊結果を伴う、新しいSCADAの脆弱性が発見され、攻撃されるだろうと予測している。

【7】スポンサーによって支援された攻撃

FortiGuard Labsのチームでは、CaaS（サービスとしての犯罪）について頻繁に討議している。多くのコンピュータを感染させたり、スパムを送信したり、DDoS攻撃をしかけるなど、インターネットを通して不法で有害なサービスを犯罪組織がどのように提供しているのかを解明している。2012年、FortiGuard Labsは、国や企業レベルでの資金援助を含むCaaSが、企業や個人に対し、より戦略的かつ標的型の攻撃に悪用されるだろうと予測している。

【8】大義を一刀両断する

Anonymousは4Chan.org上に2003年に組織化されたが、2010年には、ゆるやかに組織されたアナーキスト達が彼らの力を利用して、ソニーのような大規模かつ高い注目を集めているターゲットを攻撃しはじめ、年末にかけて彼らの力を「慈善」のために使ってきている。この良い例としては、彼らは最近、メキシコの麻薬カルテルメンバーの正体を暴露すると脅迫したり、当局が子供のポルノ犯罪の一味を摘発するのを支援したりしている。ハッキング集団は、このような正義ラインのボーダーにのるか、これを超える攻撃を混在させているが、2012年には、ハッキング集団の正義が裁かれる事例が多く見られるだろうとFortiGuard Labsは予期している。

FortiGuard Labsについて（www.fortiguard.com）

FortiGuard Labsは、世界中で稼働しているFortiGateネットワーク セキュリティ アプライアンスおよびFortiGuard Labsの監視システムから収集したデータに基づいて、過去4週間の脅威に関する統計およびトレンドを収集・集計している。

●お問い合せ先●
フォーティネットジャパン㈱
URL：http://www.fortinet.co.jp/