エフセキュア 2010 年度セキュリティ総括レポート

（2011 年 1 月 18 日 ヘルシンキ発 － フィンランド本社発表資料抄訳）

2010 年のセキュリティ関連の大きな出来事のひとつとして、Wikileaks の台頭と Wikileaks に対する反対派と賛成派によるインターネット上での政略的な攻防がありました。これは理論上、サイバーサボタージュの脅威が証明されたことを意味しており、2010 年が IT セキュリティ史上に残る年になったといえます。

- **Wikileaks と DDos 攻撃の容易性**
- **Stuxnet ― IT セキュリティ史上最も重要なマルウェア**
- **サイバー犯罪検挙において最高の年**
- **未だに狙われている Windows XP**
- **モバイルセキュリティの進歩**

Wikileaks と DDos 攻撃の容易性

2010 年 12 月、セキュリティ関連の大きな出来事として、Wikileaks の台頭と Wikileaks に対する反対派と賛成派によるインターネット上での政略的な攻防がありました。しかし、IT セキュリティの専門家にとってこの攻撃手法は、特別なものではなく非常に身近なものでした。

エフセキュアのセキュリティ研究所で主席研究員 (CRO) を務める**ミッコ・ヒッポネン**は、次のように述べています。「Wikileaks と関係を絶った、Mastercard や Visa、Paypal のような企業を標的にしたサイバー攻撃は、新しいものではなく、従来の DDoS 攻撃でした。これは、昨今では誰でも簡単に参加できるようになり、とても単純な攻撃手法として知られているものです。」

2000 年に初めて DDos 攻撃が行われて以来、技術が進化、且つ簡略化することで、DDos 攻撃に参加する多くの Hacktivists (アクティビストとハッカーの混成語) と呼ばれる活動家は、違法行為の自覚のないまま一連の活動に参加している可能性があります。

ミッコ・ヒッポネンは、「実際、Wikileaks 賛成派による一連の DDos 攻撃のほとんどは、コンピュータのスペシャリストではなく、いわゆる有志の匿名団体、或いは個人でした。この DDos 攻撃は、自らのコンピュータを第三者が攻撃に利用できるようにするために、攻撃ツールをダウンロードするだけで参加できるという簡単なものでした。私は、これらの攻撃に参加した多くの人々は、犯罪に加担しているという認識を欠いていると確信しています。」と述べています。

この様な攻撃を阻止するには、複雑なプロセスと高額な費用がかさむため、企業の多くは実際に攻撃されない限り、具体的な対策を疎かにしがちです。

ミッコ・ヒッポネンは、「一連の DDos 攻撃により、Mastercard、Visa のどちらもオンライン決済に使用されるクレジットカード検証機能が一時停止を余儀なくされ、PayPal が提供するサービスも一部で混乱をきたしました。つまり攻撃者は、それらのクレジットカード会社に損害を与えるのに成功したのです。」と述べています。

ミッコ・ヒッポネンは、これらの一連のサイバー攻撃には、世界的、且つ政治的な意味があるのは認めながらも、"サイバー戦争"とは言えないとし、「組織や団体間における攻撃は戦争とはいいません。Wikileaksも然り、Mastercardも国ではありません。」と指摘しています。

Stuxnet — IT セキュリティ史上最も重要なマルウェア

Stuxnet はおそらく過去 10 年間において最も重要で、非常に洗練されたマルウェアと言っても良いでしょう。**ミッコ・ヒッポネン**は、「Stuxnet は、工場の制御システムに侵入し、オートメーションのプログラムを書き換えてしまうため、実際の社会に損害をもたらし、サイバーサボタージュを現実のものします。」と述べています。

Windows OS を狙うワームは USB フラッシュメモリを介して広がりますが、Stuxnet はシステムに感染し、ルートキットで身を隠しながら、感染したコンピュータが Siemens Simatic ファクトリシステムに接続しているかをチェックします。万一接続に成功した際は、Windows コンピュータから PLC (Programmable Logic Controllers) と呼ばれる工場のシステムを実際に制御する機械に、改ざんされたコマンドを送信します。PLC に感染すると、更に特定の工場環境を探そうとしますが、見つからない場合、或いは接続に失敗した場合は被害には繋がりません。

世界中の何十万台ものコンピュータが Stuxnet の標的になりました。Siemens は、少なくとも 15 の工場で感染を確認したと発表しましたが、Stuxnet は工場システムに限ったマルウェアではありません。感染したマシンの大部分は副次的な感染、すなわち SCADA システムに接続していない、一般家庭やオフィスのコンピュータでした。しかし、Stuxnet は特定の施設を狙うよう設計されたマルウェアであることから、IT セキュリティに革命的な脅威をもたらしたことになります。

Stuxnet はこれまでのマルウェアからは考えられないほど大きいサイズで、1.5MB もあり、5 種の脆弱性が利用され、（そのうちの 4 種はゼロデイで、現在全ての脆弱性は Microsoft によって修正されています）盗まれた証明書によりドライバに署名されていました。エフセキュアのセキュリティ研究所では、Stuxnet は 10 人の研究者が 1 年以上かけて開発するくらいの複雑性を備えていると考えています。

未だに明らかになっていないものの、Stuxnet の複雑性、ウラン濃縮施設を狙った攻撃であること、そして金銭目的ではないことから、恐らく政府によって開発されたと憶測できます。

Stuxnet に関する詳しい情報は、下記のエフセキュアブログにてご覧いただけます。
http://blog.f-secure.jp/archives/50464996.html

サイバー犯罪検挙において最高の年

2010 年は、これまでで最も多くのサイバー犯罪が発生しただけでなく、同時にインターネット犯罪を犯して逮捕された人、有罪判決を受けた人の数が過去最高になった、素晴らしい年でした。

過去、マルウェアは趣味や好奇心によって作成されたものがほとんどでしたが、2003 年頃以降は、サイバー犯罪者によって利益を追求する組織により開発されるようになりました。

しかしながら、これまではオンラインでの迷惑行為から犯罪行為へのマルウェアの変遷が、犯罪加害者の逮捕や有罪判決の数に反映されていませんでした。万一逮捕、起訴されることがあっても、多くは懲罰的な罪状ではなかったのが実情でした。しかし 2010 年は、サイバー犯罪者を取り締まり、起訴するための法施行が活発化した年となったといえます。

その中でも画期的なのは 2010 年 3 月に起きた事件があります。TJ Maxx などの米国大手小売店のシステムをハッキングし、何千万ものクレジットカード情報を盗んだアルフレド・ゴンザレスは、20 年の実刑判決を受けました。これは、これまでのサイバー犯罪関連の事件で下された実刑の中では、最も重い判決です。ゴンザレスと彼の一味は、小売業者のレジ認証システムの Wi-Fi をハッキングし、クレジットカード情報へのアクセスに成功しました。その結果、被害に遭った何百万ものクレジットカードが再発行されるに至りました。

FBI が 10 月に明らかにしたのは、米国の銀行口座から約 7000 万ドル盗んだとして起訴された、国際的なサイバー犯罪組織のうち、90 人以上を逮捕したというものでした。

また、英国とウクライナでも多くのサイバー犯罪組織の幹部が逮捕されました。それらは、マルウェアを仕込んだスパムメッセージを送ることにより、オンラインバンクの詳細情報を盗み出すもので、FBI によれば、一連の逮捕は、彼らが今までに捜査してきた最も大きなサイバー犯罪の1件の一端であるとのことです。

7 月には、Register によって報告された興味深い事件がありました。それは、既成ソフトをスパイツールとして悪用し、配偶者やライバルなどの携帯端末の通信情報を盗聴したとして、ルーマニア当局が 50 人を逮捕したというものでした。

同じく Register によると、ルーマニアの対組織犯罪とテロ対策局 (The Romanian Directorate for Investigating Organized Crime and Terrorism) は、iPhone、Blackberry、Symbian、Windows Mobile などの携帯端末で利用可能な同ソフトを販売した容疑で、ダン・ニコラエ・オプロイユという 30 歳の IT スペシャリストを逮捕しました。

ミッコ・ヒッポネンは、「我々アンチウイルス ベンダは、警察が然るべき行動を執ることができるよう、研究成果や調査結果などの資料を司法当局に提供しています。この取り組みが功を奏し、サイバー犯罪に対する法的執行が活発化したということを非常に喜ばしく思っています。今後も一層サイバー犯罪の取り締まりが強化されることを願っています。」を述べています。

未だに狙われている Windows XP

Windows7 は、Windows Vista よりも安全な OS として、脚光を浴びました。今年、ついに Vista のシェアを追い抜くとされていますが、未だに Windows XP のシェアには全く及ばないのが実情です。つまり、Windows XP は最も利用者の多い OS であり、最も大きなマルウェアの標的になっていると言えます。

「サイバー犯罪者はいつも格好のターゲットを探しています。」と、**ミッコ・ヒッポネン**は続け、「今後も数年にわたり、Windows XP が標的にされる可能性が十分にあります。」と忠告しています。

2010 年 7 月に Microsoft は、Windows XP Service Pack2 のサポートを終了しました。我々はその時点で、未だに Windows XP SP2 を使用し、それらの脆弱性が放置されたままになっている顧客は、およそ 10%に上ると推測していました。

サポートがすでに終了しているような古い OS を使用するということは、セキュリティに問題が発生しうるといえます。たとえば、メキシコ湾における重油流出事件の原因のひとつに、未だに 1996 年の Windows NT4 を使用していたことが起因しているという報告があります。

ミッコ・ヒッポネンは、「10 億ドルもかけて行う石油ビジネスであるにも関わらず、最新のコンピュータ、OS を使用していなかったせいで、多くの被害をもたらした罪は重い。」と締め括っています。

モバイルセキュリティの進歩

2010 年は、携帯電話を狙うマルウェアの数は劇的な増加を見せませんでしたが、将来の動向のヒントとなるいくつかの進歩が見られました。

2010 年初頭、Android マーケットからいくつかのオンラインバンキング用のアプリケーションが削除されました。それらのアプリケーションは、銀行から正式に認可されたアプリケーションではないどころか、実際にオンラインバンキングに全く対応しておらず、ユーザの銀行情報を盗むために、オンラインバンクのウェブインタフェースを開いていただけでした。

4 月に、一部の Window Mobile ユーザが、高額な通信料金がかかる国際電話をかける、「3D Anti-terrorist action」というトロイの木馬に感染しました。これはロシア人のハッカーが、「3D Anti-terrorist action」というアクションゲームから複製を防止するコピーガード機能を外し、代わりにトロイの木馬を仕込んだゲームをダウンロードさせるサイトに置くことで、無料ゲームを探している人々に偽のゲームをダウンロードさせるという攻撃手法です。

悪意のあるアプリケーションは、8 月にも Android マーケットで発見されました。「Tap Snake」と呼ばれるゲームの正体は、スパイ用のクライアントとして商用目的で開発された「GPS SPY」というアプリケーションでした。「Tap Snake」は、「Snake」という普通のゲームのように見えるものの、2 つの隠された機能がありました。このゲームは終了することがなく、一旦インストールされるとバックグラウンドで永遠に動作し、仮に携帯電話をリスタートしたとしても再起動してしまいます。また、ユーザに気付かれぬよう 15 分おきに端末の GPS 情報を攻撃者のサーバに送り続けるという特徴がありました。

エフセキュアのセキュリティ研究所は以前より、スマートフォン上のオンラインバンキングを狙うトロイの木馬が出現するのは時間の問題だと予測していました。実際、携帯電話のトランザクション認証番号 (mTAN) を盗み出す Zeus の亜種が、Symbian (.sis) と Blackberry (.jad) で発見されました。mTAN は、SMS で送信され、オンライントランザクションの認証にワンタイムパスワードとして使用され、オンラインバンキングなどの決済取引の際に使用する使い捨てパスワードとして利用している銀行もあります。

エフセキュアのセキュリティ研究所の分析によれば、それら一連のサイバー攻撃は、好奇心ではなく、モバイルアプリケーションとソーシャルエンジニアリングに関する専門的な知識を持ちわせたスペシャリストによるものでした。今後、モバイルバンキングを狙う攻撃手法は一層複雑化すると見られています。

エフセキュア株式会社 会社概要

http://www.f-secure.co.jp/

エフセキュアは、IT 先進国フィンランドで 1988 年に設立されて以来、23 年にわたりセキュリティ製品に取り組んでいる業界の老舗で、世界規模でセキュリティサービスを提供しています。1999 年に OMX ヘルシンキ証券取引所に上場し、以来、順調に成長を続けている株式公開企業のひとつです。
エフセキュア株式会社は、エフセキュア社 100%出資の現地法人として設立され、以降、増収を続けながら順調に企業規模を拡大しており、2009 年 5 月に日本法人設立満 10 周年を迎えました。

会 社 名: エフセキュア株式会社
代 表 者: 日本法人代表 桜田 仁隆
所 在 地: 〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F
設 立: 1999 年 5 月
事業内容: セキュリティ関連製品・サービスの販売およびサポート

本件に関するお問合せ先
エフセキュア株式会社
担当: 尾崎 risa.ozaki@f-secure.com
TEL: 03-5545-8942 FAX: 03-5545-8945
〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F
URL: http://www.f-secure.co.jp
Blog: http://blog.f-secure.jp/