



G Data

マルウェアレポート

—2011年上半期 1-6月—

G Dataセキュリティラボ

ラルフ・ベンツミュラー & サブリナ・バーケンコフ

(瀧本往人・岸本真輔 訳)



Go safe. Go safer. G Data.

概要

2011年上半期の動向

- ・2011年上半期における新種マルウェアの活動は、計1,245,403件にのぼりました。2010年下半期と比べると、15.7%増でした。1日あたりの出現数は、平均で、6,881件でした。
- ・カテゴリ分類で見ると、トロイの木馬とアドウェアが平均以上の伸びを示しました。対比して、バックドア、ダウンローダーの数は、若干下がりました。新たなボットを増加させることよりも、コンピューターを感染させるエクスプロイト（攻撃）の方が、ネット犯罪者たちの関心事になっています。
- ・マルウェア・ファミリーは、2011年上半期においては、アクティブなもので、2,670種ありました。
- ・マルウェア全体におけるウィンドウズのマルウェアが占める割合は、増加して、99.6%にのぼりました。2010年下半期と比べて、ウィンドウズのプログラムファイル自体は、0.3%ほど下がったのですが、ドットネット（.NET）がこの減少分を埋める形になりました。
- ・ウェブ上で活動するマルウェア・プログラム、そして、モバイル端末のマルウェアが、上昇傾向にありました。

2011年上半期の傾向

- ・ハクティビズムは、次第に一般的になり、政治的発言をする一つの手法として定着しはじめています。
- ・モバイル端末のマルウェアの数が、急上昇しています。

2011年のトピック

- ・今年、マイクロソフトのデジタル犯罪ユニットとインターポール当局の間の緊密な協力によって、成功裡に、巨大なボットネットであるルストック（Rustock）を封鎖しました。3月には、1日に何十億通ものスパムメールを生成する原因だったコンピューター・ネットワークが活動停止に追い込まれました。
- ・4月から数カ月の間、ソニーグループに対する一連の激しいサイバー攻撃がありました。これらの攻撃は主にSPN(Sony Playstation Network)およびそのゲーマーに影響しました。アノニマスがこの攻撃の張本人と推定されたハッカー・グループでしたが、ラルズセック（LulzSec）が翌週以降何度も攻撃を行いました。

2011年下半期の展望

- ・マルウェア・プログラムの数は下半期に再び増加すると予測されます。1年間の出現数は、250万を超えるでしょう。
- ・下半期に、サイバー犯罪者は、ますますモバイル・プラットフォーム（特にアンドロイド）を攻撃する可能性があります。

目次

概要	2
2011 年上半期の概要	2
2011 年下半期の傾向	2
2011 年のトピック	2
マルウェア基本情報	4
全体	4
マルウェアカテゴリ別状況	4
マルウェア種別状況	5
プラットフォーム別マルウェア発生状況	8
2011 年下半期の動向予測	9
2011 年上半期の注目ポイント	10
モバイルマルウェアの増加	10
2011 年上半期の出来事	14
2011 年 1 月	16
2011 年 2 月	16
2011 年 3 月	17
2011 年 4 月	18
2011 年 5 月	19
2011 年 6 月	19

マルウェア基本情報

ウイルス発生数の上昇は止まらず

もうそろそろマルウェア数の増加が収まるのではないかと、という楽観的な見方も昨年末にはありましたが、2011年上半期の6ヶ月に出現したマルウェアの数をみると、それが誤りであったことが分かります。2011年の前半に新しく出現したマルウェア・プログラムの数は、1,245,403件で、昨年の下半期よりも15.7%増加しました。この数は、1日当たり平均で、6,881件の新しいマルウェア・プログラムが出現したことを意味します。この勢いが下半期も続くのであれば、2011年1年間で、約250万件のマルウェアを数えることでしょう。なお、250万件という数値は、2006年から2009年までの4年間に出現したマルウェア数とほぼ同じくらいです。

*この総数の計算は、悪性コードを含むファイルを一つずつ数え上げたものではありません。あくまでもワクチン側から見たものです。

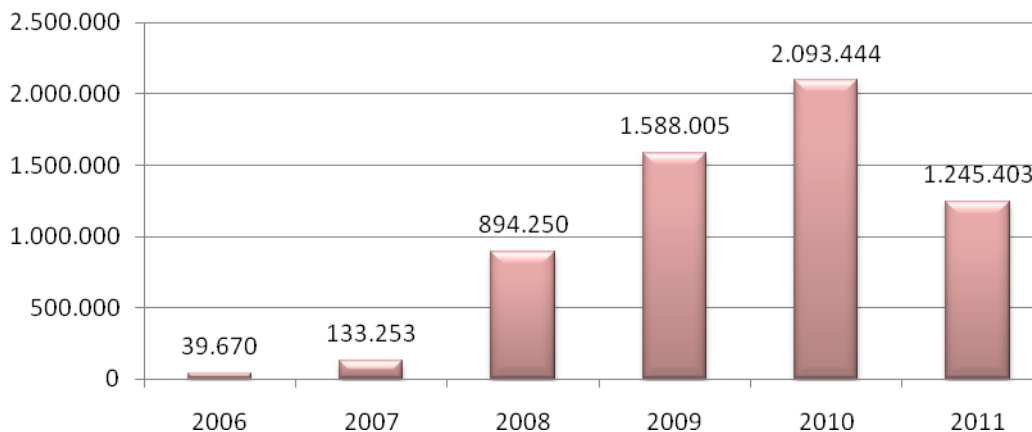


図1 新種マルウェア数の変遷 (2006～2011) (2011年は上半期のみ)

マルウェア カテゴリー別状況

マルウェアは、どのような悪意ある活動を行うのかに基づいて、カテゴリー分類されます。

現在では、寄生し次々と複製をつくりだし感染を増やすような、もともとの意味での「ウイルス」はほとんど姿を消しています。むしろ、寄生することなく独自に活動する「ワーム」や、侵入しそのコンピューターだけで活動する「トロイの木馬」が中心です。その他には、広告を表示させる「アドウェア」、複合的な機能をもち強力な潜伏能力をもつ「ルートキット」、さらには、OSやだれもがよく使うソフトの脆弱性を攻撃する「エクスプロイト」などが、活発に出現しています。

また、トロイの木馬に分類されるマルウェアがあまりにも多いため、もう少し細分化した分類を行っています。具体的には、外部との連絡や侵入ができるようにする「バックドア」、コンピューター内にある情報を盗み出す「スパイウェア」、外部から不正なプログラムを招き寄せる「ダウンローダー」、内部に忍ばせておきながら必要なときがくるまで凍結させておく「ドロップター」などに分けられます。これら、トロイの木馬系はすべて合わせると、出現したマルウェアの90パーセント近くになります。

図2は、2010年上半期から2011年上半期までの、直近の半期毎の期間の個々のカテゴリーの数を示しています(注:縦軸は対数)。見ての通り、「トロイの木馬」型が、ずっと1位でしたが、2011年上半期に、急激な増加を記録しました。「トロイの木馬」型は、何らかの悪意ある機能を実行するマルウェアをすべて含んでいます。ほとんどのトロイの木馬は、犯罪活動を行なうことを目的として、バックドア経由で感染したコンピューター上で走るプログラムを含んでいます。このグループは、スパム送信、サービス不能 (DoS)

攻撃、プロキシ・サービス、そして、サイバー犯罪市場に出回っているあらゆるサービスと同様の提供物を含んでいます。特にオンラインバンキングのトロイの木馬には多くの変種があり、ゼウス (Zeus) およびスパイアイ (SpyEye) が代表格です。このような、トロイの木馬が増加するというのは、地下ビジネスがうまくいっていることを示します。

一方、アドウェアの急増は、2010年の後半以降は、やや落ち着きつつあります。しかしながら、14.6%の増加率を記録しており、アドウェアが引き続き、犯罪者たちにとっては、金儲けしやすく、ビジネス上大事なツールと受け止められていることがわかります。

また、ダウンローダー (ならびにドロップパー) は、わずかですが、減少がありました。バックドアの数もまた、わずかに減少しました。これらのマルウェア・プログラムはコンピューターを遠隔制御したり、ボットネットに組み込むことを可能とするので、その意味では、ボットネットの構築や維持・管理だけが、ネット犯罪者たちの優先事項というわけではなくなりました。

最後に、エクスプロイトの数は、長らくわずかずつ下降を続けてきましたが、今回初めて、再び増加しました。

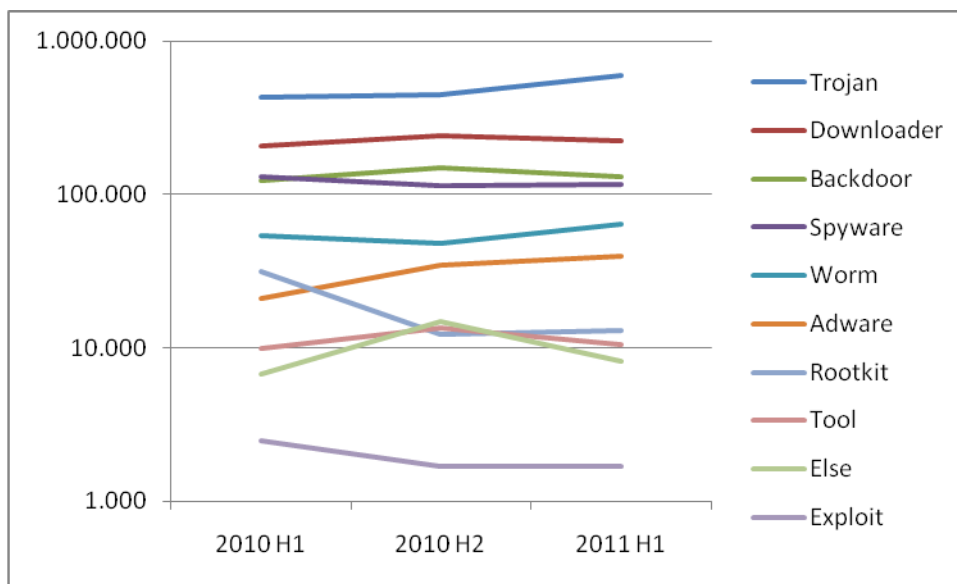


図2 カテゴリー別マルウェアの変動 (2010年上半期～2011年上半期)

マルウェア種別状況

マルウェアは、その機能と特性に従って、「種」 (=ファミリー) 別に分類できます。これらのいくつかの種については、たえず、新たな亜種が生み出され続けています。

マルウェア・ファミリーの総数は、2011年上半期は、2009年以降の微増傾向を踏襲し、2,670種を記録し、わずか2.4パーセントですが、増加しました。

近年は、新しいマルウェアの発生件数が著しく増加している一方で、「種」については、必ずしも増加しているわけではありませんでした。マルウェア種は、2008年の上半期には2,395種あり、それが下半期には2,094種となりました。さらに2009年の上半期には、1,948種にまで下がりました。しかし、この傾向は2009年下半期より、変化が生じました。2009年の下半期には2,200種に上昇し、2010年の上半期には2,262種、下半期には2,608種となり、今回、2,670種と、連続して微増しています。

次に、この1年半で最も多くの亜種を発生させたマルウェア種の上位を、図3で示します。

最も多く出現したマルウェア種は、3期とも変わらずゲノム (Genome) でした。これはトロイの木馬型で、さまざまな悪意ある機能を含んでいます。

2番目に多かったのは、フェイクAV (FakeAV) で、ウイルス対策ソフトやシステムツールを模造して金銭を奪うなどの被害をもたらすもので、この時期のネット犯罪市場においては、特に人気が高かったものです。

VB クリプト (VBKrypt) は、悪意のあるファイルを装い隠すための新しいプログラムで、今期は3番目に多く出現しましたが、前の期には登場していませんでした。

4番目が、TDSSで、ルートキットに属し、「TDL ルートキット」として知られています。強力なバージョンが登場したことにより、ネット犯罪者たちの利用が増えたと考えられます。

ワームのなかで急増したのが、パレボ (Palevo) で、5番目に出現が多く、ワーム自体の急増の理由になっています。

9番目には、今期はじめて登場したマルウェアであるメンチ (Menti) がランクインしましたが、これも1番目のゲノムと同様に、トロイの木馬型です。つまり、トロイの木馬は、ネット犯罪者たちにもっともよく利用されるマルウェアだということを示します。

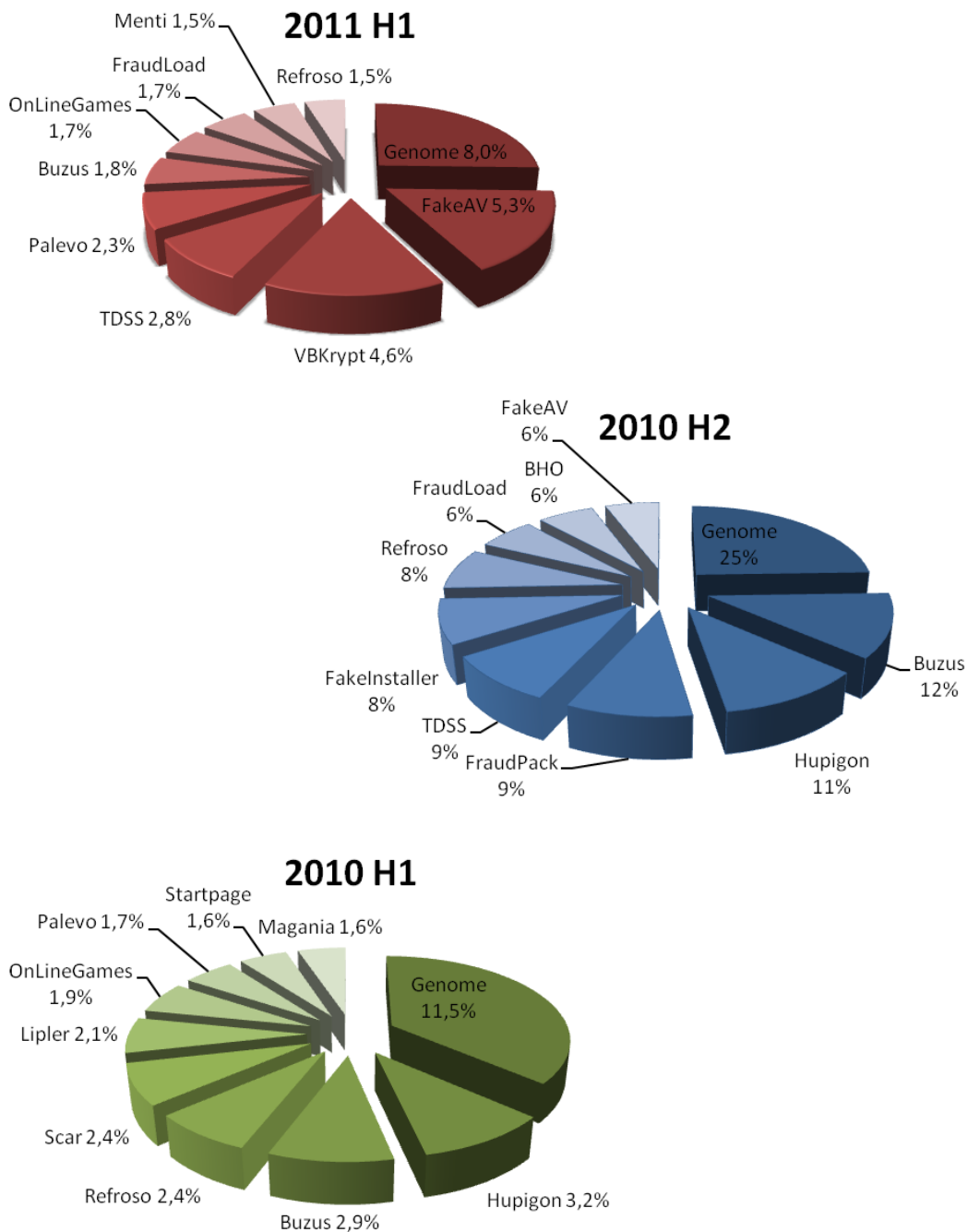


図3 活動が盛んだったマルウェア上位10種 (2010年上半期～2011年上半期)

上位マルウェア種の概要

ゲノム (Genome)

トロイの木馬型。ダウンローダー、キーロガー、ファイル暗号化の機能が統合されています。

偽AV (FakeAV)

トロイの木馬型。まるでウイルス対策ソフトや他のセキュリティ関連プログラムが画面上で起動しているかのように偽装するものです。亜種として、デフラグツールのようなシステム修復ツールの起動にみせかけるものもあります。実際には最初から用意されている「動画」が流れているだけで、本当にウイルスを検知したり除去したりしているわけではありません。にもかかわらずあたかもマルウェアが発見されたかのように見せかけてユーザーをだまし、料金を奪ったり、メールアドレスやオンラインバンクのアカウントやパスワードを奪うことを目的として仕掛けられます。

VBクリプト (VBKrypt)

VBクリプトは、ツール系で、悪意あるファイルを偽装するために使用されます。カモフラージュのルーティンが、Visual Basicで書かれています。偽装ファイルの内容は非常に多様で、ダウンローダー、バックドア、スパイウェア、そしてワームにまで及びます。

TDSS

ルートキットに分類されます。技術的にとても洗練したかたちでマルウェアファイルを偽装するため、ルートキットのなかでも主流となりました。バックドアやスパイウェア、アドウェアの機能が作動する際に、ファイルやレジストリを隠すために用いられます。

パレボ (Palevo)

ワームの一種で、P2Pのファイル共有ソフト (Bearshare、Kazza、Shareazaなど) の公開に乗じて自己複製を行いつつ、USBメモリの自動表示機能 (autorun.inf) を悪用し拡散します。また、インスタントメッセージング (MSNなど) を通じて、有害サイトへのリンクを拡散します。バックドア機能をエクスプローラーに仕掛け、特定のサーバー上にあるコマンドを探します。

ブザス (Buzus)

トロイの木馬型。個人情報 (クレジットカード、オンラインバンキング、EメールおよびFTPアカウント) を探し出し攻撃者にデータを転送します。そのうえ、より容易に攻撃できるように、侵入したコンピューターのセキュリティ設定を下げようと試みます。

オンラインゲームズ (OnLineGames)

トロイの木馬型。当初はネットゲームのアクセスデータを盗み出すために使用されました。実際には、多様なファイルやレジストリ・エントリが探索され、キーロガーがインストールされるので、ゲーム関連のデータ以外にも盗み出されます。中国や韓国、日本で多く発生しています。

フラウドロード (FraudLoad)

偽装ソフトの一種で、多数の亜種のバリエーションがあります。情報漏洩やシステムツールのふりをするものが大部分です。感染のためにシステムをスキャンするよう推奨されます。感染をすべてきれいにするためには、「有償完全バージョン」の購入を求められます。クリックするとダウンロード購入サイトに導かれ、クレジットカード情報を入力するよう、要請されます。一般的に感染は、OSにおけるふさがれていないセキュリティホールを使うか、よく使われているアプリケーションを狙います。しかしまた、アダルトコンテンツや最新ニュース、またはゴシップといったテーマを含む動画の視聴をコンテンツとしているサイトに誘い

出されるような攻撃メソッドもあります。この場合動画を見ようとすると、マルウェアを含む特殊なコーデックをインストールしなければなりません。

メンチ (Menti)

トロイの木馬型。感染したシステムに侵入しプログラムを埋め込み、サーバーと常に接触ができるようにします。コンピューターをボットネットに組み込んでしまいます。

リフロソ (Refroso)

トロイの木馬型。2009年6月の終わり頃に最初に発見されました。バックドアの機能を用い、ネットワーク内の他のコンピューターを攻撃します。

プラットフォーム別発生状況

ここ数年ウィンドウズを攻撃するマルウェアの激増が、続いてきました。2011年の上半期もまた、同じ傾向が見られました。もちろんプラットフォーム別においても、圧倒的な差で首位に立ち続けています。その比率は、250のマルウェアがあるとすると、そのうちの249がウィンドウズのプログラムファイルということになります。

しかしながら、厳密に言うと、ウィンドウズの32ビット版のみで作動するマルウェアの割合は微少しており、2010年上半期は98.5パーセントだったのが、下半期には98.1パーセントになり、2011年上半期には、97.8パーセントにまで下がりました。

ただし他方で、.NETの数が大きく上昇し比率を高めています。.NETは、.NET言語で書かれたプログラムをコンパイル変換したMSILなどを含み、プラットフォームやプログラミング言語に依存しないのですが、.NETアプリケーションの大部分は、ウィンドウズでホストされています。.NETとWin32と合わせると、最終的にはウィンドウズ関連のマルウェア・プログラムの比率は合計で、約99.5パーセントとなります。ウィンドウズが狙われなくなっているわけではなく、マルウェア作成者がこの.NET環境を悪用する機会が増えている、と考えるべきでしょう。

	プラットフォーム	2011 年上半期		2010 年下半期			2010 年上半期		
		発生数	構成比	発生数	構成比	当期比	発生数	構成比	当期比
1	Win32	1,218,138	97.8%	1,056,304	98.1%	15.3%	1,001,902	98.5%	21.6%
2	.NET	21,736	1.7%	15,475	1.4%	40.5%	9,383	0.9%	131.7%
3	WebScript	3,123	0.3%	2,237	0.2%	39.6%	3,942	0.4%	-20.8%
4	Scripts	832	0.1%	1,111	0.1%	-25.1%	922	0.1%	-9.8%
5	Mobile	803	0.1%	55	<0.1%	138.2%	212	<0.1%	273.1%
6	Java	313	<0.1%	517	<0.1%	-39.5%	225	<0.1%	39.1%
7	ix	233	<0.1%	382	<0.1%	-39.0%	226	<0.1%	3.1%
8	NSIS	131	<0.1%	130	<0.1%	0.8%	260	<0.1%	-49.6%

表3 プラットフォーム別マルウェア発生数上位8 (2011年上半期、2010年下半期、上半期)

* 「WebScript」は、JavaScript、HTML、Flash/Shockwave、PHPまたはASPに基づいているマルウェアを指します。通常はブラウザ経由で脆弱性を突くマルウェアを意味します。「Scripts」は、VBS、Perl、PythonまたはRubyといったスクリプト言語に書かれているバッチ、シェルスクリプトまたはプログラムです。「ix」は、LinuxやFreeBSD、SolarisなどのすべてのUNIX関連のものを含まれます。「NSIS」は、Winampによって使用されるインストールプラットフォームです。「Mobile」は、Android、J2ME、Symbian、およびWindows CEのためにマルウェアを含みます。

残りの0.5パーセントは、ウィンドウズ関連外のもので、ウェブ関連が中心です。その割合は全体的には微増しています。

ウェブサイトの不正コード、たとえば、JavaScript、PHP、ASP HTMLなどについては、0.3パーセントを占めます。これらにおいては新たな亜種の発生は減っています。ただし現存している亜種は、かなり活発な動きをしています。Javaマルウェアの割合が増加しているのは、ここ数カ月にウェブにおけるセキュリティホールを狙うマルウェア・プログラムが増加していることと連動しています。

他のプラットフォームのマルウェアは、全体から見れば、ごくわずかにしかすぎません。

注目は、モバイル関連のマルウェアで、さらに著しい増加を記録しました。しかもマルウェアの機能が狡猾になってきており、アンダーグラウンド市場で売買できるほどの地位に上がってきています。スマートフォンのマルウェアのうちの2/3は、高額な電話番号にSMSを送り、利益を得るというものです。また、スパイウェアとバックドアも顕著に増加しています。ネット犯罪者がもっとも注目しているプラットフォームと言えるでしょう。G Dataセキュリティラボでも監視の目を今まで以上に光らせています。

2011年上半期の動向予測

次に、2011年上半期のマルウェア動向ですが、マルウェアカテゴリーとしては、アドウェア以外は、ゆるやかな微増が予測されます。アドウェアは、今、上昇傾向が見られるので、注意が必要です。また、ウィンドウズOSを狙うマルウェアだけではなく、JavaやWeb Scripts、Mobileを狙うマルウェアの増加への注意も今後必要になってきます。特にそのなかでもアンドロイド端末への攻撃については、十分な警戒が必要です。

カテゴリー	動向
トロイの木馬	→
バックドア	→
ダウンローダー/ドロッパー	→
スパイウェア	→
アドウェア	↗
狭義のウイルス/ワーム	→
ルートキット	→

カテゴリー	動向
エクスプロイト	→
Win32	→
Web Scripts	↗
Java	→
MSIL	↗
Mobile	↗
ix	→

2011年上半期の注目ポイント

アンドロイド・マルウェアの増加

これまでマルウェアと言えば、ウィンドウズOSで動作するものが、大半を占めてきました。マルウェアもプログラムであることには変わりはないので、それぞれのOSで「悪さ」を行います。すると当然のことながら、利用者の多いOSが主に狙われることとなります。つまり、ウィンドウズOSが、第一のターゲットになります。もちろんマックやリナックスを攻撃するマルウェアも出現していますが、ウィンドウズと比べると、その割合は著しく低くなっています。

しかし、スマートフォンもしくはアンドロイド端末のマルウェアについては、大きく事情が異なります。2010年の後半より、急激にアンドロイド市場が成長してきたのに伴い、マルウェアを悪用する人間たちも利益目的に集まってきたために、マルウェア出現数も急増してきたのです。

実際には、ウィンドウズのマルウェアが2010年下半期と比べて2011年上半期は1.5倍の増加だったのに対して、アンドロイドを中心としたモバイルのマルウェアは、13.8倍の増加となりました。しかし「急増」と言っても、その数は、55件から803件に増えたにすぎず、ウィンドウズのマルウェア数と比べれば、その差は歴然としています。しかし今後もアンドロイドは、他のOSと比べてセキュリティ面でのリスクが、きわめて高くなるだろう、とG Dataセキュリティラボは予測しています。

というのは、マルウェア開発から実際の活用に至る流れは、すでにウィンドウズ関連のマルウェアを通じて地下経済にネットワークができあがっているため、アンドロイド関連のマルウェア開発は、PCマルウェアが出現しはじめた頃よりも、大幅に加速化されるおそれがあるからです。

したがって、現在、アンドロイドを取り巻くセキュリティ状況は、簡潔に、次のようにまとめられるでしょう。

- ・スマートフォンを利用する人々は、世界中で増加している。
- ・しかし、すでにメディアが盛んに報じているように、マルウェアに感染したアプリは、グーグルのアンドロイド・マーケットにおいてさえ、多数発見されている。
- ・アンドロイドへのマルウェア攻撃は、ユーザー数の増加とともに、激化している。

代表的なアンドロイド マルウェア

では、実際のところ、どのようなマルウェアがアンドロイド端末において発生してきたのでしょうか。以下では発生順に、代表的なものを挙げてみましょう。

フェイクプレイヤー、GPSスパイ

まず、「フェイクプレイヤー」(FakePlayer)と「GPSスパイ」(GPSSpy, Tap Snake)と呼ばれる2つのマルウェアが、2010年8月に発見されました。「フェイクプレイヤー」は、SMS送信を勝手に行おうとするトロイの木馬型、「GPSスパイ」は、GPS情報を外部に送ろうとするスパイウェアです。これらが、最初のアンドロイドのマルウェアと言われています。幸い、この時点ではプログラムがまだ十分には完成されておらず、本格的な攻撃というよりは、実験的要素が強かったようです。

ゲイニーミー

最初のアンドロイドマルウェアが登場してからわずか3ヶ月後の2010年11月には、大規模な感染騒動が中

国で起こります。「给你米」(Geinimi)という偽造アプリをインストールすることによって感染する「ゲイニーミー」(Geinimi)が発見されたのです。最初に偽造が発見されたアプリ名が「给你米」(Geinimi)だったことからゲイニーミーと名付けられたこのマルウェアは、外部から勝手に電話をかけたりメールの送受信をおこなったりできるボット機能をもっており、個人情報の漏洩や金銭被害などのおそれがありました。2011年1月までの約3ヶ月のあいだで、中国におけるアンドロイド約90万台が感染したのではないかと当初報道され、大騒ぎになりましたが、実質的には、数百~千台が感染被害を受けたと言われています。なお、感染元となった偽造アプリは、「Monkey Jump 2」「President vs. Aliens」「City Defense」「Baseball Superstars 2010」「入侵脳細胞」「植物大战僵尸」「超级猴子跳」などでした。

ゲイニーミー (日本語版)

続いて2011年2月には、このゲイニーミーが、日本語版のアプリにおいて発見されます。同じように非公式アプリサイトで配布されていた「いっしょにとれーにんぐ for Android」の無料海賊版をインストールすると感染する、というものでした。正規版では「ストレージ」だけがアプリ権限として許可を求められるのですが、海賊版では、個人情報など、さまざまな権限の許可が求められました。

ドロイドドリーム

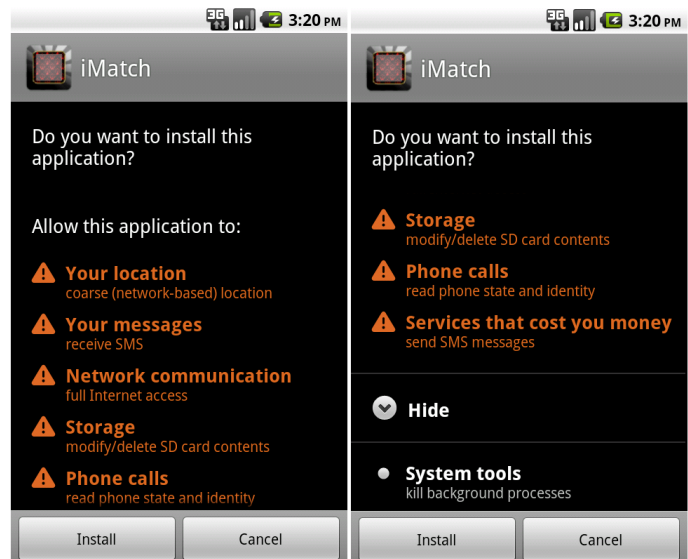
さらに2011年3月には、「ドロイドドリーム」(DroidDream)が登場します。管理者権限を奪い、個人情報をWebサイトに送るなどが可能とするもので、これもまた、海賊版アプリのインストールによって感染するものでした。「ドロイドドリーム」が話題になったのは、アンドロイド・マーケットからダウンロードされたものだったからです。しかも、ウイルス混入アプリは「掷骰子」「多彩绘画」「Advanced App to SD Version」「Magic Strobe Light」「Advanced Compass Leveler」など50種類以上(3つの公開者名)を数え、ダウンロード数も5~20万件と言われています。

ドロイドドリーム・ライト

続いて2011年5月には、「ドリームドロイド・ライト」(亜種)が登場します。これもまた、アンドロイド・マーケットからの感染でした。ウイルス混入アプリは30種類以上、3~12万件がダウンロードされたとされています。ウイルス混入アプリの開発者名には、Magic Photo Studio、BeeGoo、Mango Studio、E. T. Tean、DroidPlus、GluMobiというクレジットがありました。

ズィーズワン

同じく2011年5月にもう一つ、「ズィーズワン」(Zsone)が現れました。これもトロイの木馬型で、SMSでの送信を行うところに特徴があります。「iCalender」「iMine」「iMatch」など、グーグルのアンドロイド・マーケットにアップされていたアプリの開発者の名称からとられたもので、やはり偽造アプリから感染するタイプのものでした。これをアンドロイドにインストールしてしまうと、中国の高額通信サービスにつながり、さらに、レジストレーションの確認が妨害されるため、請求をチェックする時点にならないと感染ユーザーは高額請求に気づかない、という仕掛けが施されていました。このマルウェアは今のところ、中国のアンドロイド・ユーザーだけを脅かすものです。



ズィーズワンによって感染したアプリは、モバイルフォンにある多数の権限に認可を与え、ユーザーに被害をもたらします。(右が感染アプリ) (出所:G Data セキュリティラボ)

スマートフォンはますます世界的な人気を誇っています。しかも、単に通話をするためだけではなく、支払いサービスなどにも利用されてきており、このことが、ネット犯罪者の注目を集めるきっかけになっています。

今のところ、すべてのモバイルのマルウェアの3分の2以上は、中国語環境のもので、高額請求サービス宛にSMSを送る手法で占められています。特に、中国では、高額なSMS番号に自動送信し、課金分をネット犯罪者が奪い取るというやり口が流行しています。

これは、かつてウィンドウズではダイヤラーと呼ばれたマルウェアと似たような攻撃です。当時はまだ、ユーザー数も少なく、軽い被害で済みましたが、現在のアンドロイド端末の場合、市場がそもそも大きく、しかも成長率が高いために、さらに広範囲に被害をもたらすおそれがあります。

ジットモ

しかし同時に、スマートフォンをボットネットに組み込もうとして使用されるバックドアの数も、増加しています。たとえば、銀行の取引をリモートで行う際に使用され、SMSで送られるワンタイムパスワードmTANを盗み出す、オンラインバンキング型（またはスパイウェア型）のトロイの木馬である「ジットモ」(ZitMo、ZeuS in the Mobile) も、アンドロイド版が登場しました。

これは、ウィンドウズOSを攻撃し個人情報盗み出しボットネットを構築することでよく知られる「ゼウス」(ZeuS)が、2010年秋にシンビアンOSを攻撃したことにより、「ジットモ」と呼ばれるようになったのですが、2011年6月には、ついにアンドロイド版も登場しました。

まだウィンドウズ版ほどは洗練されていないのですが、今後ウィンドウズで磨き上げられたマルウェアがアンドロイドに移植される動きはますます多くなると予測されます。「ジットモ」がSMSで送られるワンタイムパスワードを傍受できるならば、もはやアンドロイドでの操作は安全ではなくなります。明らかに、モバイルのマルウェアは、早くも実験段階から抜け出し、実行段階に移ろうとしているのです。

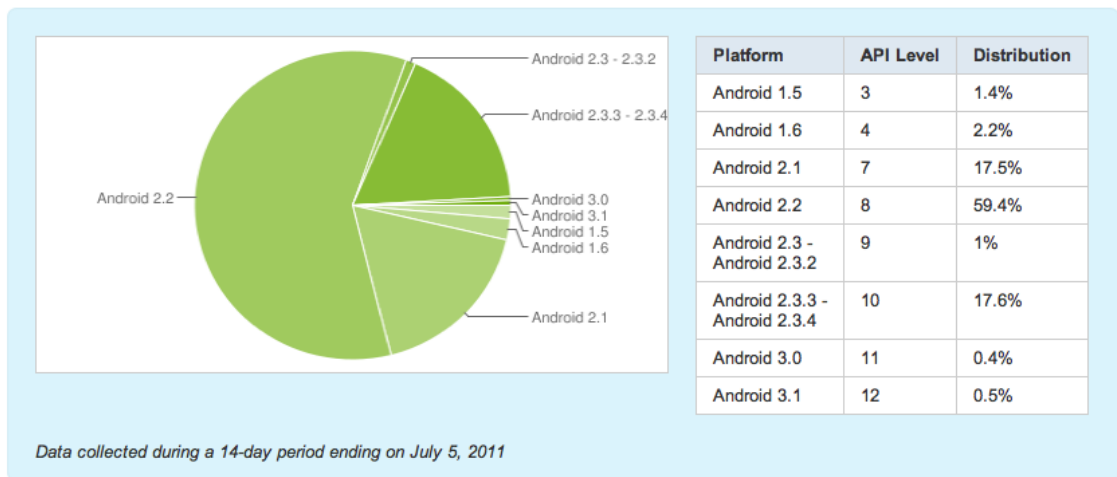
以上、いくつかの代表的なアンドロイドのマルウェアを挙げてみましたが、「感染」を考える際に無視できないのが、OSのバージョンアップと、権限許可という2つの問題点です。

狙われる旧バージョン

アンドロイドのプラットフォームは、今後もユーザーの人気を獲得し続けることと思われます。その第一の理由は、他の競合製品、たとえばiOSを搭載している端末よりも低価格であることが挙げられます。さらに、アンドロイドの場合、スマートフォンだけではなく、タブレット型のさまざまな端末が今後登場する可能性があるのも、市場を広げる原因になっています。しかしながら、このようなラインナップの広がりには、逆に著しく不利に働くこともあります。

つまり、内部の品質管理がうまくゆかず、さらには、適宜にユーザー全体に新しいバージョンを配布することが必ずしも可能だとは限らないからです。米国クパティーンに本拠地のあるコンペチターであるアップル社のiPhoneが、この好例です。しかも、電話の旧モデルをアップグレードすることは、多くの場合可能ではありません。たとえば、2011年7月の初めに、アンドロイド・マーケットを訪れたユーザーにおける旧バージョンOSの使用率は、かなり高い割合にある、という結果があります（図1を参照）。

新バージョンOSへの移行には、グーグルから端末メーカーへ、そしてサービス・プロバイダーを経由して、カスタマーへ、といったように、かなり長い過程を必要としますが、この長さが、ネット犯罪者たちに旧OSの脆弱性を開発する機会を与えています。これらは数日ではなく数ヶ月もの遅れを伴います。この問題点は、引き続きサイバー犯罪者が狙うところになるでしょう。



アンドロイド・マーケット訪問者におけるアンドロイドのプラットフォーム傾向

(出典: <http://developer.android.com/resources/dashboard/platform-versions.html>)

人的要因によるリスク

また、旧バージョンの脆弱性といった、ハードウェア関連のリスクに加えて、「人的要因」によるリスクもまた、過小評価されるべきでないでしょう。

アプリをインストールするあいだ、ユーザーは何も注意も払うことなく、表示されている権限の要求をそのまますんなりと認可してしまっている場合が少なくありません。海賊版アプリはもちろんですが、正規のアンドロイド・マーケットからダウンロードするアプリであってもです。

感染アプリは、個人情報の窃取、ボット化、高額請求サービス宛にSMSが送られてしまうなど、さまざまな被害を与えるきっかけとなります。

実際、市販のアプリにおいても、GPS情報などが本人に気づかれずに取得されるなど、スパイウェア的な機能を商品化する側も無自覚な場合もあり、今後も、注意が必要です。

まとめ

サイバー犯罪者は、これからも、さらにモバイル端末、特にアンドロイド端末をターゲットにすることでしよう。したがって、マルウェア開発に占めるアンドロイド関連の割合も、攻撃者によって得られる利益が多いため、まだまだ加速することでしょう。アンドロイド端末の売上高が上昇するのに応じて、地下経済もまた、もっと富んでゆくのです。

さらに言えば、スマートフォンを攻撃する機会が減少するどころか増加する方向性をもつなかで、新たな技術や機能が登場するにしたがって、それ以上に攻撃の幅も増えていくことになるでしょう。近い将来の一つの可能性の例としては、アンドロイド2.3以降移植された近距離無線通信 (NFC) 機能によってスマートフォンでの支払いが簡単にできる、という機能が付加されれば、確実に、金銭被害に至るようなマルウェア攻撃が起こりえます。アプリや新機能は、高性能化、多機能化する際のおもしろさがありますが、セキュリティの面から何が行われているのか、こういった危険性があるのか、ていねいに確認してゆくべきであると、G Dataは考えます。

2011年上半期の出来事

2011年上半期におけるネット犯罪とマルウェアの動向を振り返る

2010年におけるネット犯罪とマルウェアの動向について振り返り、来年ならびに将来へのパソコンやネットへの更なる安全対策を呼びかけます。

注：この項目のみ、マルウェアを含まないネット犯罪全般を含みます。

▼ネット犯罪・マルウェア事件 2011 上半期 ダイジェスト

1 【情報流出】 ソニーグループへの不正アクセスによる1億件以上もの個人情報の漏洩 (4-6月)

PSN、Qriocityのサーバーが不正アクセスされるなど、延べ1億件以上の個人情報が流出
AnonymousとLulzSecが連携したと言われ、一味の一部は逮捕されたが、真相は闇の中

2 【詐欺】 震災に乗じて日本赤十字を名乗る募金詐欺が横行 (フィッシング) (3-5月)

手口は古典的だが、改めてこういった未曾有の大災害時に「火事泥棒」のような輩がいることが残念
別件だが、体から放射能を消すサプリをネット販売した業者も、便乗商法の一つ。

3 【拡散】 アンドロイドマルウェアの日本語版が登場 (2月)

アンドロイド・ユーザーの急増に伴い、ロシア、中国、に続いて日本でもマルウェアが出現
海賊版アプリのインストール時の権限許可を悪用し、個人情報の送信などを実行する攻撃が登場

4 【犯罪】 サイバー刑法成立 (6月)

ウイルスの作成、提供、共用、取得、保管で罪に問われる「ウイルス作成罪」新設
ほか、わいせつ物頒布等の処罰対象も改正、新たに、電子データが追加された

5 【偽装】 ネット上でスキャン画面を突然表示させ偽ウイルス対策ソフトを導入させる攻撃 (5月)

新種SQLインジェクション攻撃である「ライザムーン」(LizaMoon)が再び活発に
市販ソフトを巧妙に模造しており、気づかれずに支払・カード情報が窃取される被害

6 【拡散】 大手出会い系スパム業者逮捕 (1月)

出会い系サイト宣伝目的で大量にスパムメールを送った大手業者、1年半で5億の売上
日本データ通信協会には24万件の相談、「特定電子メール法」違反で逮捕

7 【詐欺】 改正薬事法、ネットでの偽回春薬が摘発 (4月)

ネットで個人輸入したED治療薬「シアリス」の模造品を服用し、意識障害
個人輸入代行業者のサイトから購入した製品の約6割が偽物と言われている

8 【不正】 ケータイとQ&Aサイトを使って入試カンニング (2月)

4つの大学の入試問題が試験中にQ&Aサイトに投稿され、そこから回答を得ていたかどで予備校生が逮捕
結局は単純な犯行だったが、当初は高度なサイバー犯罪の可能性をマスコミが騒ぎたてた

9【犯罪】ファイル共有ソフト利用者の著作権法違反、18人を逮捕（1月）

23都道府県警察がファイル共有ソフトを利用した著作権法違反事件の一斉取締りを実施、18人を逮捕
ファイル共有ソフトのShareを利用し、アニメ、コミック、ゲームなどの違法アップロードを対象

10【予告】ネットにおける犯罪予告、逮捕が増加（1-6月）

秋葉原無差別殺傷事件後、取り締まりが厳しくなっているにもかかわらず、その後多数発生
「2月11日午後9時にJR新宿駅で通り魔を起こす」という掲示板書き込みがあり騒ぎになるなど

未曾有の災害・事故が起こったなかでも、ネットの裏市場は無関係に、むしろそれさえも悪用して好況を呈しています。すでに、しっかりとしたインフラができあがっており、ネット犯罪者たちは、いともたやすく仲間を見つけ、ツールを買い求め、私たちを罠に陥れようと狙っています。今や愉快犯などほとんど存在しません。みな、最終的には、金銭目的なのです。

ネット犯罪者は、まず、数千万台のパソコンをネットワークし、自在に操ることのできる「ボットネット」を構築します。これによって、大量にスパムメールを送ることも、特定の標的へのサイバーテロを仕掛けることも、もちろんそれぞれのボット化したパソコンの個人情報も奪うことも、さらには、奪った個人情報から金銭を盗み出すこともできるようになります。

その意味では、一番重要なのは、ボットネットに組み込まれないことです。知らない間に自分のパソコンが犯罪に加担し、さらに、知人にも迷惑をかけることにもなります。

ネット犯罪者は、ボット化させるために、マルウェアを仕込みます。主に、以下の方法を利用します。

- ・スパムメール（主に添付ファイルの開封から感染）
- ・ウェブサイト（閲覧だけで感染するものやフィッシング詐欺など）
- ・USBメモリ（オートラン機能でネット無接続でも感染）
- ・ファイル共有ネットワーク（ファイル名につられてダウンロード後に感染）

ファイル共有ネットワーク以外はいずれも、大部分のんびとが日常的に利用しているものです。つまり、日常のなかに悪質な罠が紛れ込んでいるのです。この事実には私たちはもっと気づくべきです。

しかも、このようなネット犯罪が、国境に縛られず世界中でまん延しており、日本のユーザーもすでに彼らのボットネットに組み込まれつつあるのが現状です。もちろんネット犯罪は、英語がもっとも使われているため、日本語環境にある私たちは、若干、危険な度合いが下がるともいえます。しかし、今年のネット犯罪状況をみると、そろそろ他人事では済まされない状態になっている、と言っても過言ではありません。

また、昨年より急増しているアンドロイド端末の利用に伴い、ネット犯罪者も、アンドロイドOSで起動するマルウェアの開発に向かいはじめました。ネットワークは今までウィンドウズで培ってきたものを使いながら、活発に攻撃を仕掛けています。今後は、iPhoneをはじめ他の端末も含めて、注意すべきです。

こういったネット犯罪から自分の身を守り、知人に迷惑をかけないようにするためには、まずは、ご自身のパソコンや携帯端末の安全性を高めることが、第一です。年間で200万以上の新種ウイルスが発生するご時世、ネット犯罪の脅威が日常化しつつある今、マルウェア対策、ネット犯罪対策は、これまで以上に、もっと真剣に、もっと慎重になる必要があるのではないのでしょうか。

2011年1月

1月9日 オーストラリアのメディア大手の Fairfax Media は、Vodafoneのデータベースに納められている顧客データの保護が不十分であるとして、Vodafoneを非難。SMSや電話履歴などの個人情報も「ペーパービュー」プロセスで第三者も閲覧可能であった。

1月10日 北朝鮮政府のTwitterおよびYouTubeアカウントが攻撃され、不正に利用される。北朝鮮の最高指導者金正日の後継者と目されている金正恩の誕生日に、ハッキングされたアカウントを使用して同政権に対する批判的なメッセージが流された。更に、金正恩がスポーツカーに乗って貧民を轆き殺すアニメなど、北朝鮮政府に対する皮肉がこめられた動画も公開された。韓国のインターネットフォーラムDC Insideのメンバーらが自身による攻撃だと認めた。



スクリーンショット 金正恩のアニメ（出典：YouTube.com）

1月16日 ドイツ連邦刑事局（BKA）は、ドイツ東部ドレスデンの銀行ATMを不正操作するブルガリア系のスキミング団を逮捕。銀行の支店でスキミング装置を取り付けていた3人が現行犯で逮捕された。このスキミング団による被害総額は不明。

1月23日 フランス大統領サルコジ氏のFacebookと、Facebook CEOのザッカーバーグ氏のFacebookファンページにおいて、本人のものと思わせるコメントが不正に書き込まれた。実行者がどのように書き込みアクセスを得たのかは不明。

1月24日 イランが、反政府主義者間のコミュニケーション（特にSNS）を防ぐ目的で、サイバー警察を形成。現大統領アフマディーネジャード氏の2009年の再選に対する抗議について、警察署長エスマエル・アハマディ・モガダム氏は、「反革命グループと反政府主義者は、SNSを利用して同調者や新たな仲間を探し出している。また、SNSは、彼らが諸外国とコンタクトをとるためのツールとして使われており、イラン国民を扇動する恐れがある」と説明。



1月31日 アメリカで盗難されたノートPCが、自動的にメールを送信。盗難されていたPCは内蔵カメラで写真を撮影し、それをPCの元々の所有者にメールで送信。警察は写真に写っていた2人の人物を手がかりに、捜査を行っている。

スクリーンショット2：盗まれたノートPCの内蔵カメラによって撮影された写真（出典：wavy.com）

2011年2月

2月5日 セキュリティ会社HGGary Federalの社員のAaron Barr氏は、Anonymousによる広範囲にわたった攻撃があったことを認めた。Barr氏は、以前、Operation Paybackを実行したAnonymousのメンバーを特定したと自慢気に話していた。これをNew York Times 誌も記事にしたため、AnonymousがHGGary Federalに対し反撃を行った。このAnonymousによる攻撃によって、HBGary社社員のパスワードやGreg Hoglund（共同創設者兼技術責任者）のGmailアカウントのハッキングなど、セキュリティ企業では起こらざるべき事件が引き起こ

された。ハッキングされた情報には、様々な受注案件やHoglundのサイトrootkit.comのアクセスデータが含まれていた。AnonymousはHoglundのメールと様々なデータを公開。攻撃の引き金となったAaron Barr氏は退社に追い込まれた。

2月7日 ドイツのハンブルク警察は、購読詐欺を仕掛けたウェブサイトの運営者と思われる人物2名を逮捕した。2008年の年末以降、この2人は、6万5000人もウェブサイトを訪問者に対し購読詐欺を実行し、約500万ユーロの利益を不正に得ていた。この詐欺では、まずユーザーにフリーソフト（もしくは体験版を無料で利用できるソフト）をダウンロードさせ、ダウンロードしたユーザーが気付かないように購買契約を締結させていた。

2月9日 Tinie Appというツールキットが闇マーケットにおいて、25USドルで販売。このツールは、Profile Creeps や Creeper Trackerのような Facebook用の不正アプリケーションを誰でも簡単に作成できるもので、多くのFacebookユーザーは未だにこのアプリケーションをクリックする（アフィリエイトで開発者に利益が生じる仕組み）。

2月12日 8万4000ものドメインで、児童ポルノ法に抵触するサイトに適用されるメッセージが誤って表示された。これはデータ転送時のエラーが引き起こした問題で、FreeDNS（DNSプロバイダ）のすべてのドメインでこの問題が発生した。

2月13日 Pixmania、Eidos、eHarmonyや diversitybusinessなどの顧客データの闇マーケットでの取引が確認された。データがセットで2000~3000USドルで取引され、アルゼンチン人のクリス・ルッソがデータを盗んでいた模様。eHarmonyの事例では、SQLインジェクションが使用された。



スクリーンショット3: 84,000のドメインに誤って表示されたバナー(出典: torrentfreak.com)

2月15日 脆弱なウェブサイトの大量感染の結果、BBC 6 Music websiteとBBC Radio 1extraにも不正コードが埋め込まれた。このコードは、ウェブサイトからファイルをダウンロードし、ウェブサイトの閲覧者に気付かれずに（drive by infection）感染させる。攻撃者はPhoenix exploit kitを使用し、コンピューター内の脆弱性をつく。

2月17日 UKの調査報告によると、UKにおけるサイバー犯罪の被害額は、年間307億EUR。知的財産の盗難が大部分を占め、続いて産業スパイとブラックメールに続く。

2月28日 イリノイ州ネイパービル在住の男性（48）が出会い系サイトでの詐欺被害に。インターネットで知り合った女性のため、ブラジル、USA、マレーシア、ナイジェリアなどの口座に、2年間で合計20万USドルを送金。女性と連絡が取れなくなった時、彼は彼女が誘拐されたと思い、警察に通報。そこで、ようやく詐欺の被害にあっていたことに気付く。

2011年3月

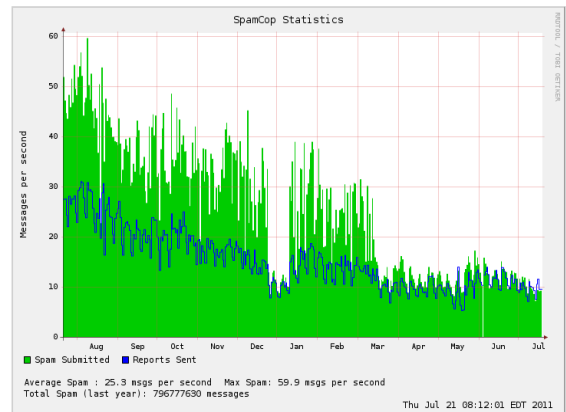
3月5日 3月1日に特定のアプリケーションをアンドロイド・マーケットから削除したことをGoogleが公表。対象のアプリケーションは、ルート権限を不正に獲得するなどの機能を持つDroidDreamに感染していたアプリケーション。Googleは、リモートアクセスを使用し、当該マルウェアに感染したデバイスのインストールを行った。また、Googleは、Android Market Security Tool March 2011をリリース。しかし、程なくして、トロイの木馬型マルウェアがアンドロイド・マーケットに出回った。



スクリーンショット4: アンドロイドロボット (出典: android.com)

3月6日 エジプトの国家セキュリティーサービスへの攻撃の間、政府反対者が英国企業Gamma InternationalがFinFisherと呼ばれるスパイソフトの購入をエジプト政府にオファーする書類を発見。このマルウェアを使うと、スパイ、盗聴、あるいは反政府主義者のコンピューターを不正に制御でき、購入費用(トレーニング込み)は52万5000USドルと言われる。

3月16日 Waledac botnetがシャットダウンされてから約1年が経過、Microsoftは更なるボットネットの解体を公表した。今回解体されたのは、Rustockと呼ばれるボットネットで、Microsoft Digital Crimes Unit (DCU)によると、100万台のコンピューターがこれに感染、毎日約10億通ものスパムメールの送信元であった。



図表3: 3月中旬より1秒あたりのスパムが画期的に減少 (出典: Spamcop.net)

3月17日 セキュリティ企業RSAのサーバーが狙われ、二要素認証SecurIDの情報が盗まれる。攻撃方法は、Advanced Persistent Threatと呼ばれるもので、不正なExcelファイルをRSAの特定従業員に送信されるスパイ型の攻撃。Excelファイルを開くと、ゼロデイ脆弱性を悪用し、対象のコンピューターが乗っ取られる。

3月18日 アシュリー・ミッチェル (29) は、4000億分の仮想ポーカーチップ (1200万USドル) をアメリカのZynga社から盗んだとして、2年の禁固刑に処された。Zyngaは、オンラインゲームFarmvilleを運営。ミッチェルは盗み出したチップの一部を5万3000EURで闇マーケットで売り払っていた。

3月20日 大手旅行系ウェブサイトのTripAdvisorからデータ漏洩。データベースから登録者のメールアドレスが盗まれた。TripAdvisorは、漏洩原因を特定し、問題を修正。甚大なダメージはなかったと発表した。登録者への通知には、「今回の件で、登録者はスパムメールを受信する可能性がある」と記載されていた。

3月23日 ComodoのCA (認証局) が侵入され、不正なSSL証明書が発行された。認証は、3月15日に盗まれた。Comodoの発表では、複数のIPアドレスから攻撃され、大部分がイランからのものであったことが明らかに。

2011年4月

4月4日 大規模なSQLインジェクション攻撃の詳細が判明。Lizymoon攻撃と呼ばれるこの攻撃で、不正コードが何百ものウェブサイトに埋め込まれた。感染サイトのクリーンアップは、長期に及ぶ自体に。これ

により、当該ウェブサイトの訪問者は、偽のウイルス対策のウェブサイトへリダイレクトされ、そこで偽のウイルス対策ソフトを購入させられる。

4月8日 あるソフトウェア会社が女性プログラマーとセールスアシスタントの求人広告を掲載。応募条件における年齢制限は20～39歳、全裸で勤務ができること。

4月20日 アメリカ国土安全保障省は、ナショナルワイドのテロ警告を将来的に自身のホームページに限らず、テレビ、ラジオ、SNSでも公表する計画を発表。空港でのアナウンスや政府関連サイトでの告知は外れている模様。

4月24日 セキュリティメーカー、カスペルスキー社のCEO、ユージン・カスペルスキー氏の実息が誘拐されたが、ロシア保安局に無事保護される。発表によると、誘拐犯は300万ユーロを要求していたが、身代金の支払いは行われなかった模様。

4月27日 個人情報の保護が不適切だったとし、PlayStationユーザーによるSony Corpを相手取った初の訴えが起こる。4月17日から19日にかけて、SonyのPlayStationNetwork (PSN) およびQriocityはハッカーから攻撃を受け、7700万件ものユーザーデータが漏洩していた。

2011年5月

5月10日 フィンランド警察は、オンラインバンキングの詐欺団を分解、容疑者17人の身柄を確保。同国のNordea銀行の顧客がターゲットとなる。100回の取引で不正操作が行われ、被害額は約120万ユーロに上った。その後、被害額のうち、17万8000ユーロが被害者のもとに戻った。

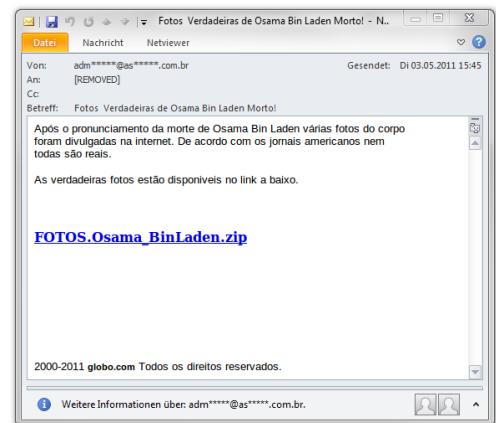
5月11日 ビン・ラディン死亡の報道がマルウェア作者をインスパイア。ビン・ラディン死亡の証拠写真へのリンクや、ワードの脆弱性 (CVE-2010-3333) を狙うワードファイルを含むメールが発見される。

5月11日 ロシアのメディアエージェンシーPravdaのウェブサイトがハッキングされ、ユーザー（閲覧者）を攻撃。Pravdaはこれを認識していなかった。犯罪者は、埋め込み型 exploit スクリプトを使用し、閲覧者のコンピュータ上のJavaの脆弱性を攻撃。

5月20日 ソフトウェア研究者のロサリオ氏は、Facebookなどログインが必要なウェブサイトへのアクセスを可能にするMicrosoft Internet ExplorerのExploitを発表。ログイン情報を入力すると、ウェブサイトがデジタルキーとしてクッキーを生成。このクッキーが盗まれると、通常なら保護されるべきウェブサイトへ第三者がアクセスできるようになる。この攻撃は、cookiejackingと呼ばれる。

5月23日 バンキング系トロイの木馬、Zeusの完全なソースコードが公表される。Zeusは、ここ数年において最も強力なバンキング系トロイの木馬として知られている。

5月25日 アムステルダム大学の博士号を持つ学生が、Google プロフィールのデータ記録3500万件をデータベースにロード。このデータには、名前、メールアドレス、経歴などのデータが含まれる。この情報の取



スクリーンショット5: オサマ・ビンラディン関連のメール例

集は、私立探偵やフィッシング犯罪者などが、いかに早く個人情報を入手できるか、実験する目的で行われていた。

5月26日 中国軍が同国におけるエリートサーバー団の存在を認める。この特殊部隊は「サイバーブルーチーム」として知られ、防衛目的か、はたして攻撃目的に組織されたかは不明。

2011年6月

6月3日 Sony PSN および Qriocityへの攻撃に続き、今度はSony Picturesがハッキングの被害に。後に、LulzSecurity (略:LulzSec) がこの攻撃を認め、100万件以上ものユーザーの個人情報が盗み出したと発表。

6月4日 MicrosoftのDCUは、3月に解体したRustock botnetの背景に潜む人物の特定作業を続ける。DCUの考察によると、ロシアから操作されていた（もしくは依然操作され続けている）。DCUは、無効化されたIPアドレスとドメインの所有者と接触するため、ロシアの重要紙に30日に渡る広告を掲載した。

6月7日 アメリカの航空機・宇宙船・武器メーカー、ロッキード・マーティン社は、3月に盗難されたと思われるRSA SecurID tokenを悪用され、同社のウェブサイトが攻撃されたことを公表。データ漏洩は素早い対策により回避された模様。同社は現在4万5000個の SecurID tokenを交換中。

6月20日 仮想通貨Bitcoinが一瞬にして大暴落。何者かがBitcoinのアカウント（全Bitcoinの7.7%）をハッキングし、交換所サイトのMt. GoxでUSドルに換金、その直後に、買い戻しを行った。これにより、1 Bitcoinあたりの価格は、一時、17.50USドルから1セントに落ちた。

6月26日 わずか50日後に、LulzSecが活動停止を発表。警察から捜査されているLulzSecは、ここ数週間、数々のハッカー攻撃とDDoS攻撃を行った。また、LulzSecは、ハッキングで入手した大量のデータをインターネット上で公開していた。

6月29日 MySpaceがカリフォルニアの広告会社に身売り。買収価格は約3500万USドル。メディア王のルパート・マードック氏が、2005年、5億8000万USドルで買収していたが、その後、Facebookの成長でユーザー数は大幅に減少していた。

6月30日 ドイツ連邦捜査局（BKA）は、ドイツ犯罪白書2010を公表。2010年におけるインターネット関連犯罪発生件数は、25万件。前年に比べ約2割増。被害額は、6150万ユーロに上る。