



G Data

マルウェアレポート

—2010年下半期—

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

2010年下半期の動向

- ・2010年における新種マルウェアの活動はこれまでで最高数となり、計2,093,444件にのぼりました。
- ・しかしながら、マルウェア出現の増加率は緩やかになり、2010年上半期と比較して約5パーセント増にとどまりました。昨年同期と比較しても、約16パーセント増でした。
- ・カテゴリー分類で見ると、最も増加率が高かったのは、アドウェアで、上半期よりも66パーセント増となりました。アドウェアは、2010年上半期に一度大きく後退したあと、下半期になって再び増加に転じ、6番目に多いカテゴリーとなりました。
- ・オンラインゲームに関するマルウェアが減少しました。その代わりに、急激に増加しているのは、偽ウイルス対策ソフトや偽システムツールなどの、ソフトウェアを偽装したマルウェアでした。

2010年の傾向

- ・マルウェアのプログラムを書いている人間は、Javaのセキュリティホールに狙いを定めています。
- ・スタクスネット (Stuxnet) 事件が示しているように、セキュリティ問題は今や、デスクトップパソコンやサーバーに制限されなくなりました。産業設備が今後さらに、狙われるおそれがあります。

2010年のトピック

・2010年においては、裏市場で活動していたネット犯罪者たちが逮捕されたほか、いくつかの大きなボットネットが活動停止しました。インターネット時代における組織的犯罪は、大部分が国際的な協力によって成り立っているため、対抗する側も、国境をこえて協力しあう専門家たちの存在が不可欠となってきています。

2011年の展望

・2010年はアドビ製品における脆弱性を狙った攻撃が多数みられましたが、同じような脆弱性が発生しないのであれば、2011年はおそらく、Javaプラットフォームがネット犯罪におけるもっとも激しい攻撃ポイントとなるでしょう。さらに、ボットネットのような活動に対して法律上の制限が各国で進められているなかで、これまでのボットネットよりもっと巧妙な手口が登場するおそれがあります。

「ハクティビズム」(Hacktivism) という、ネットを通じて公的機関や国家、大企業などを狙う攻撃そして「祭り」や「炎上」のような、特定の標的を狙ったDoS攻撃的な活動もまた、2011年に数多く登場することが予期されます。しかもそれは、目立たないよう、こっそりと開始される可能性があります。したがって重要なポイントは、むしろ、私たちがいかにこういった攻撃に気づくことができるか、になります。

また、どんな場合であれ、SNS (ソーシャルネットワーク・サービス) を悪用した攻撃は数多く発見されるでしょう。位置情報確認やURL短縮サービスなどを通じてマルウェア感染する危険性は、今後大きくなる見込みです。また、個人ユーザーの個人情報漏洩に対する意識の薄さは、同時に個人情報の価値の高さ (それがクラウド上にある場合も含めて) と相まって、ネット犯罪者が機能を特化したマルウェアを使用して、世界中の各個人、各企業、各組織を標的にすることを可能にするでしょう。

目次

概要	2
2010 年下半期の概要	2
2010 年の傾向	2
2010 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	5
マルウェア種別状況	7
プラットフォーム別マルウェア発生状況	9
2011 年上半期の動向予測	10
2010 年下半期の注目ポイント	10
2010 年下半期の出来事とトレンド	13
2010 年 7 月	13
2010 年 8 月	14
2010 年 9 月	15
2010 年 10 月	16
2010 年 11 月	17
2010 年 12 月	18

マルウェア基本情報

ウイルス発生数の上昇傾向はストップ？

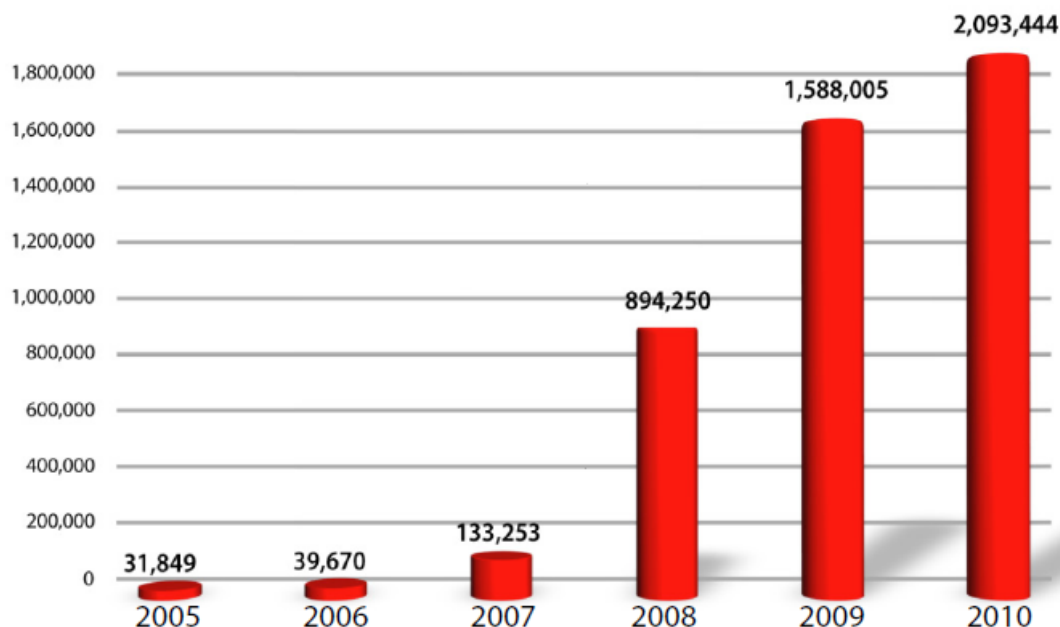
今から約25年前、1986年1月19日に、世界で最初のコンピュータウイルス「ブレイン」(Brain)が発見されました。このウイルスは、感染するとスクリーン上にメッセージを表示させるだけのものでした。今から見ると、詐欺や犯罪というよりも、悪戯に近いもので、技術的な能力の誇示程度のものにすぎませんでした。新種の数もまた、今からみると、きわめて少数の活動にとどまっていた。

ところが、その後、ワームやトロイの木馬、スパイウェア、キーロガーなど、多種多様なウイルスがこの世に登場し、しかも、大部分が金稼ぎを目的とした「ネット犯罪」の道具へと変わってゆきました。基本的な機能が次々と増えているというわけではありませんが、ネットの裏市場では、簡単にマルウェアを作成できるツールが売買され、それを悪用するネット犯罪者が攻撃道具として膨大な量のマルウェアをメールやネット、その他、あらゆる手段を使って拡散させています。その結果、2010年下半期にG Dataセキュリティラボが採集した新種マルウェアの数*は、約100万種、正確には、1,076,236に上りました。

*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。

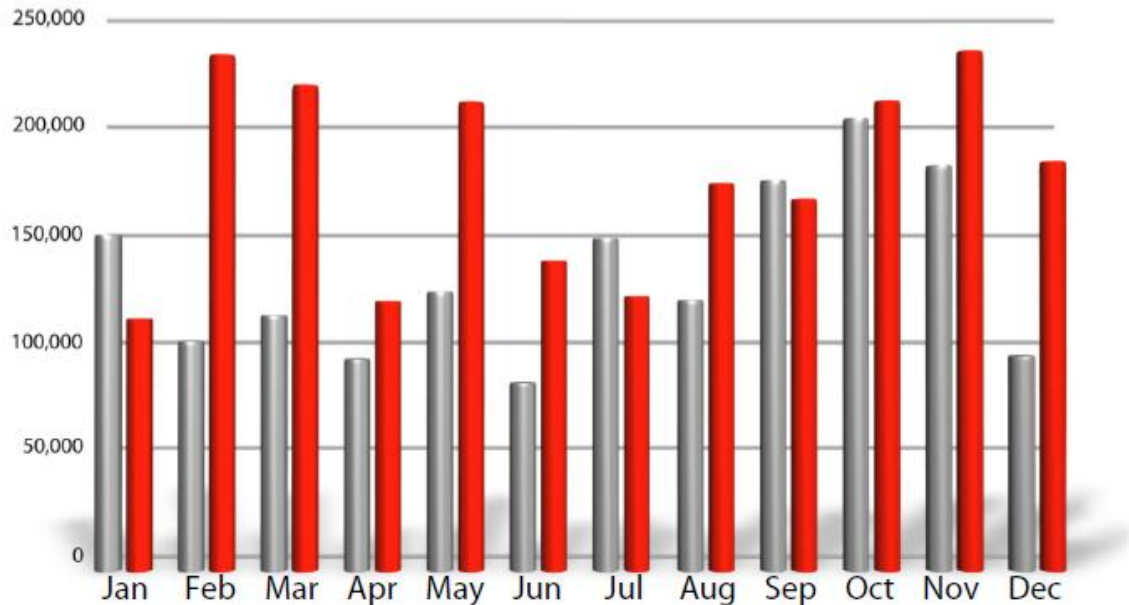
この数は、1日にすると、平均で5,849種が出現したことになります。つまり、15秒ごとに1種の新たなマルウェアが発生した計算になります。

グラフ1にあるように、2010年の1年間では、200万種以上のマルウェアが出現したことになります。確かに2009年からの増加は、それほど大きくなくなりました。しかし同時に、2006年と比べると、なんと52倍になっています。



グラフ1 新種マルウェア数の変遷 (2005~2010)

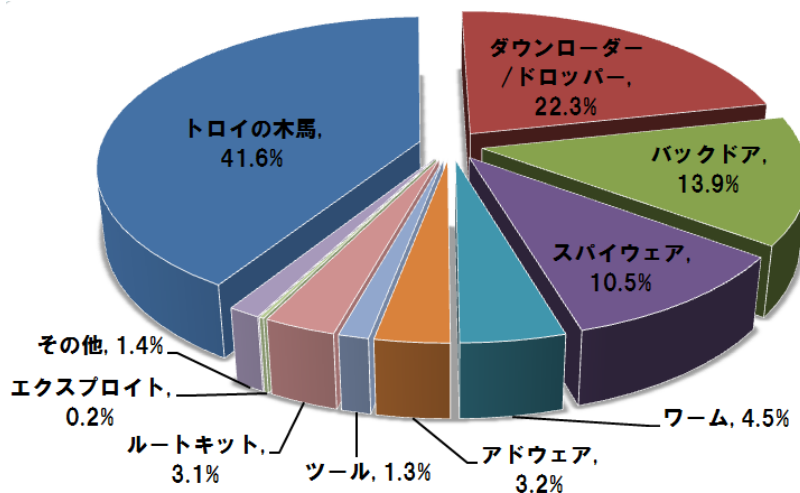
とはいえ、月別でみた場合、明らかに上昇度合いは落ち着いています。2010年2月、3月、5月は、昨年比でかなり多くなったものの、下半期には、8月、11月、12月が若干多いとしても16パーセント増程度であり、さらに上半期との比較においてはわずか6パーセント程度の増加にとどまりました。コンピュータにおけるウイルス、つまりマルウェアというものが登場して以来激増を続けてきたこれまでの経緯を考えると、これほどわずかな上昇にとどまった期は、今回が最初になります。



グラフ2 月別マルウェア数の変遷 (赤=2010年、グレー=2009年)

マルウェア カテゴリー別状況

マルウェアは、それぞれの活動の特性に基づいてカテゴリーごとに分けられています。2010年下半期に出現したマルウェアは、カテゴリー別にみると、次のような比率になります。



グラフ3 カテゴリー別マルウェア比率

このように、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」、複合的な機能を持ち強力な潜伏能力をもつ「ルートキット」、また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「ドロッパー」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90パーセント近くになります。

2009年下半年期からの、半期ごとの新種マルウェア発生のカテゴリー別推移については、表1で見ることができます。

カテゴリー	2010 年下半年期		2010 年上半年期		前年下半 期との差	2009 年下半年期		前年上半 期との差
	数	比率	数	比率	比率	数	比率	比率
トロイの木馬	447,644	41.6%	433,367	42.6%	3%	393,421	42.6%	14%
ダウンローダー /ドロッパー	240,124	22.3%	206,298	20.3%	16%	187,958	20.4%	28%
バックドア	149,723	13.9%	122,469	12.0%	22%	137,958	14.9%	9%
スパイウェア	113,117	10.5%	130,175	12.8%	13%	86,410	9.4%	31%
ワーム	48,324	4.5%	53,609	5.3%	10%	51,965	5.6%	-7%
アドウェア	34,882	3.2%	21,035	2.1%	66%	30,572	3.3%	14%
ツール	13,499	1.3%	9,849	1.0%	37%	14,516	1.6%	-7%
ルートキット	12,305	3.1%	31,160	3.1%	-61%	11,720	1.3%	5%
エクスプロイト	1,691	0.2%	2,495	0.2%	-32%	3,412	0.4%	-50%
その他	14,927	1.4%	6,751	0.7%	121%	6,595	0.6%	126%
計	1,076,236	100.0%	1,017,208	100.0%	6%	924,053	100.0%	16%

表1 マルウェア発生数と割合 (2010年下半年期、上半期、2009年下半年期)

このなかで、増減について、もっとも注目すべきカテゴリーは、アドウェアです。具体的には、ウイルス対策ソリューションやシステムツールを偽装したマルウェアが増えました。全体における比率は3.2パーセントにすぎませんが、前期比では66パーセントの増加となっています。

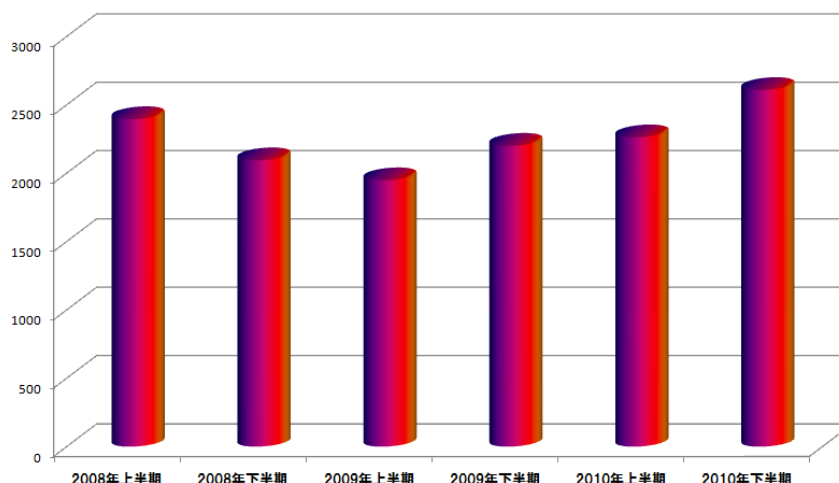
続いて顕著だったのは、ダウンローダーです。ダウンローダーは全体に占める割合も22.3パーセントと多いのですが、のみならず、前年同期比でも16パーセント増加となりました。バックドアも同様に上昇傾向が見られ、前年同期比で22パーセントとなりました。

一方、ルートキットは著しく減少し、前年同期比で61パーセントも落ち込みました。ただし前年上半期からの変化をみると、5パーセントの上昇であり、むしろ2010年上半年期が異常な伸びがあったといえます。

なお、エクスプロイトは連続して減少傾向にあります。

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。



グラフ4 マルウェア種の数の変動 (半期ごと)

ただし近年では、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（グラフ4参照）。

マルウェア種は、2008年の上半期には2,395あり、それが下半期には2,094となりました。さらに2009年の上半期には、1,948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種となり連続して微増しています。

これを年間での動向でみた場合も、同様の傾向が見られます。2009年のマルウェア種の数には3,267であるのに対して、2010年は3,313種のファミリーが出現しました。なお、年間ベースの場合出現した数は、上半期と下半期で重複しているものについてはカウントされないため、総数が減ります。

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上位10を、表2で示します。

	2010年 下半期	マルウェア種	2010年 上半期	マルウェア種	2009年 下半期	マルウェア種
1	70,570	ゲノム	116,469	ゲノム	67,249	ゲノム
2	34,412	ブザス	32,830	フピゴン	38,854	ピーシークライアント
3	31,834	フピゴン	30,055	ブザス	37,026	フピゴン
4	27,052	フラウドパック	25,071	レフレッソ	35,115	スカー
5	26,013	TDSS	24,961	スカー	24,164	ブザス
6	24,276	偽インストーラー	21,675	リプラー	20,581	リプラー
7	22,411	リフレッソ	19,835	オンラインゲーム	19,848	マガニア
8	17,535	フラウドロード	17,542	バヴェロ	18,645	レフレッソ
9	17,272	BHO	16,543	スターページ	16,271	サフィス
10	16,645	偽AV	16,517	マガニア	16,225	バスン

表2 最も活動的なマルウェア種ベスト10 (2010年下半期、上半期、2009年下半期)

上位は、大きく変わっていません。ゲノム (Genome)、ブザス (Buzas)、フピゴン (Hupigon) はほぼ常

連のものであり、順位が多少変わった程度です。

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たものです。

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、より容易に犠牲者のコンピュータを攻撃できるようにコンピュータのセキュリティ設定を下げようと試みます。

フピゴン (Hupigon)

バックドア型。攻撃者はコンピュータを遠隔操作します。キーボード入力の記録や、ファイルシステムへのアクセス、ウェブカメラへのアクセスを可能にします。

フラウドパック (FraudPack)

トロイの木馬型。本物らしく見せかけたセキュリティツールで攻撃します。あくまでも偽装ツールなので、このツールを使っても安全にはなりません。むしろ危険な状態のままにさせてしまうので、かえって注意が必要です。また、外部から新たなマルウェアを付加することも可能なので、ドロッパー型に含めることもできます。

TDSS

ルートキットに分類されます。とても技術的に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。外部からバックドアを作成したり、スパイウェアやアドウェアの機能も持っています。

偽インストーラー (FakeInstaller)

一般的によく知られているソフトウェア、もしくは違法ではないソフトウェアをインストールするふりをする詐欺プログラムです。インストールの手順が進むように見えていながら、何も行わず、プログレスバーを表示させ、終了後に、ある内容が記載されたSMSを送り、法外な金額を請求します。大部分はロシアで操作されています。

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を攻撃します。

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。

BHO

インターネットエクスプローラー (Internet Explorer) のプラグインとして作動します。スパイウェアのような動きをします。さまざまなサーバーに秘密裏に接続しようとしています。プラグイン自体はDLLファイルですが、プラグインをインストールし実行するドロッパーもまたこのファミリーに含まれています。

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。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。

プラットフォーム別発生状況

従来と同様、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。2010年の下半期もまた、同じ傾向が見られました。しかしながら、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減少し、2009年下半期は99.0パーセントだったのが2010年上半期には98.5パーセントとなり、さらに下半期には98.1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、Windowsでホストされています。.NETとWin32と合わせると、最終的にはWindows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。単純にウィンドウズが狙われなくなっているというよりも、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	2010年下半期		2010年上半期			2009年下半期		
		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	1,056,304	98.1%	1,001,902	98.5%	5%	915,197	99.0%	15%
2	.NET	15,475	1.4%	9,383	0.9%	65%	2,732	0.3%	466%
3	WebScript	2,237	0.2%	3,942	0.4%	-43%	4,371	0.5%	-49%
4	Scripts	1,111	0.1%	922	0.1%	20%	1,124	0.1%	-1%
5	Java	517	0.0%	225	0.0%	130%	229	0.0%	1568%
6	ix	382	0.0%	226	0.0%	69%	229	0.0%	932%
7	NSIS	130	0.0%	260	0.0%	-50%	229	0.0%	-43%
8	Mobile	55	0.0%	212	0.0%	-74%	120	0.0%	-54%

表3 プラットフォーム別マルウェア発生数トップ5 (2010年下半期、上半期、2009年下半期)

* 「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関連のものを含みます。「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、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、その割合は全体的には減少しています。ウェブサイトの不正コード(たとえば、JavaScript、PHP、ASP HTMLなど)であり、0.4%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。スマートフォンのマルウェアファミリーの数は全体的に減少している一方、UNIXベースのオペレーティングシステムのためのマルウェアプログラムの数の増加は、見逃すべきではないでしょう。

2011年上半期の動向予測

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	→
ツール	→

カテゴリー	動向
ルートキット	↗
エクスプロイト	→
Win32	↘
Web Scripts	↗
Java	↗
MSIL	↗
Mobile	↗
ix	→

次に、2011年上半期の動向ですが、マルウェアカテゴリーとしては、ルートキット以外は、ゆるやかな微増が予測されます。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。

注目すべき出来事

ウィキリークスとネット活動家

2010年下半期に起こった注目すべき出来事として、第一点目は、ウィキリークス (WikiLeaks) とその影響をとりあげます。非営利組織であるウィキリークスが極秘文書を含む公文書を次々とネット上に公開していったことによって、「機密」の情報の扱いに関して、公開することが是か非か、世界中で激しい論争が巻き起っています。

2010年7月25日に、ウィキリークスのサイトは、いわゆる「アフガン戦争機密文書」を公開しました。そしてさらに、2010年11月28日の「暴露」は、この7月の文書公開以上の衝撃力がありました。つまり、1966年から2010年に至る、計251,287件の米国の外交記録(=「公電」と呼ばれています)がネット上に置かれ、今や「ケーブルゲート」事件として知られるようになったのです。ウィキリークスによれば、彼らがこれらの公電を公表する直前に、ウィキリークスのサーバーは標的型攻撃(=DDoS攻撃)を仕掛けられました。情報をウィキリークスに提供した密通者であるブラッドリー・マニング (Bradely Manning、米陸軍情報担当兵)は、訴訟内容すべてが有罪であれば懲役52年相当となります。メディアの報道によると、米国国防総省では、スタッフがウィキリークスの文書を見るのを禁じるだけでなく、この文書について議論もしくは説明をしている約25のメディアサイトに対して、米空軍のネットワークへのアクセスをブロックしました。

この事件に関連して、いくつかのインターネット企業に公権力が発動されました。たとえばアマゾン、ウェブサーバーからウィキリークス関連の文書を削除しました。ペイパル (PayPal) やマスターカード (MasterCard) は、ウィキリークスの口座を凍結し取引停止に至らせました。しかし、そうすると今度は、このような処置をおこなった企業に対して、多数のウィキリークス支持者が報復を開始しました。賛同者たちは、スイス郵政公社やマスターカード、ビザ (Visa)、ペイパル、エブリディエヌエス (EveryDNS) およびアマゾンに対して「払い戻し作戦 (オペレーション・ペイバック)」を始めるとともに、DDoS攻撃を行いました。その結果、かかわったサイトはしばらくの間利用困難なほど通信回路を遮断されました。しかしながら、G Dataの調査によれば、攻撃は組織的な犯罪の体裁をもったものではなく、問い合わせを数多く投げかけ各サイトに負荷を与えるツールを使用した攻撃に終始しました。

こういった形式の抗議は、これまで一個人によって使用されることはほとんどありませんでした。しかも、DDoS攻撃に協力した若い男性たちは、素朴に、軽い気持ちで攻撃を行ったにすぎず、自分が法的に処罰されることになるとは、微塵にも思っていなかったことでしょう。実際にオランダでは、16歳と19歳の2人の男性が、これに関与した疑いで逮捕されました (オランダの法律ではDDoS攻撃は6年以内の懲役が科せられます)。

ウィキリークスのプラットフォームだけが、批判的ではありません。ウィキリークスのスポークスマンであり編集主幹であるオーストラリア出身のジュリアン・アサンジ (Julian Assange) 自身もまた、12月7日にロンドンにて身柄を拘束され、一度は保釈されたものの、身柄送還に関する聴取のため今なお軟禁状態にあります。

しかもスウェーデンでは、アサンジに対して性的暴行の告発が行われましたが、彼は本件の容疑を否定しました。こじつけや虚偽であり、告発内容が、あくまでも政治的な動機によって企てられたものであると述べています。

米国では、アサンジに対する合法的な処置が可能かどうかを調査しています。しかし、どういった理由で裁かれねばならないのか、まだ明確な説明は現れていません。

メディアでは本件に関して、「謀略」や「諜報活動取締法もしくは諜報法」(米国で1917年に国防への違反を罰するために成立した法律で反戦活動や左翼取り締まりなどに適用された)という言葉が用いられますが、言論の自由への権利を前にして、どこまでそのような法を適用できるのか、疑わしい点があります。また、ネット活動家 (Hacktivist) は今後さらに無視できない「勢力」となることでしょう。

産業設備のウイルス感染～スタクスネット

スタクスネット (Stuxnet) と呼ばれるコンピュータワームは、2010年7月に最初に報告されました。その仕組みや特性への調査結果が次第に増えてゆく一方で、分析は今一歩本質に踏み込めず、なかなか全体像がつかみきれませんでした。当初注目された、いわゆる「LNKセキュリティホール」(CVE-2010-2568)は、全体からみると、氷山の一角にすぎませんでした。

CVE-2010-2568は、ウィンドウズ シェルの脆弱性によって、リモートでコードが実行されてしまうもので、USBメモリなどをパソコンに装着することによって拡散し、たとえオートラン機能を無効にしていたとしても感染をもたらしてしまうものでした。このマルウェアに関する詳細が、徐々に明るみになってきたのは、このセキュリティホールが、スタクスネット環境から悪性コードを非制御で拡散を行うということによります。最終的には、これまで知られていないセキュリティホールが合計で4件、マルウェアを拡散させるのに用いられ、かつ、必要な権利を使用して目標システムにおいて悪性コードを実行するのに使用されていたのです。

これが問題なのは、ウィンドウズ システムだけにかかわるものではなかったからです。

ルートキットがインストールされ、盗まれた認証情報が、悪意あるファイルを隠すのに用いられました。攻撃の目標は、シーメンス社の工程制御システム (SCADA) のための管理ソフトウェアパッケージでした。このソフトウェアには、エンジニアリングツールとして「ステップ7」という自身のプログラミング言語が用いられており、これによって産業設備を制御できるプログラムを生成します。悪意がある機能自体は、制御プログラムに至り、機械の制御コードがコンパイルされたあとに、生成されます。長い間、実際の攻撃目的が何であったのかは、不明瞭なままでした。最終的には、目標はイランの核再処理工場であり、ウラン遠心分離機が一時的に制御不能になっていたことが判明しました。わずかな時間でも遠心分離機が制御できない状態になっていたことによって、同位元素はうまく分離できず、その結果精製の質が下がってしまいました。この、スタクスネットと呼ばれるマルウェアプログラムを構成するコードの開発には、かなりの資金援助と、多数の専門家の共同作業を必要とし、かなりの時間を要したはずですが。開発の背景に誰がいたのかは明らかではなく、さまざまな憶測が出回っています。

このスタクスネット事件が示しているのは、たとえそれが重要インフラであっても、攻撃目標とされる産業設備を操作するという目的のために、資金援助を行う人々とそれに応じて悪性コードを開発する人々とのネットワークがあるということです。スタクスネットのような事件から私たちが分かるのは、セキュリティの問題が、ただデスクトップパソコンやサーバーに制限されない、ということです。原則として、IPアドレスが割り振られている制御装置ならばなんでも利用できる、ということを考えるべきです。

セキュリティは長い間、多くの産業設備では特に注意されていませんでした。しかしながら、スタクスネットでは明らかになったのは、これまで重要であると指定されたインフラストラクチャの部門だけではなく、産業設備に対しても同様に注意しなければならないということです。

PDFを凌駕するJavaへの攻撃

2010年の後半になって、マルウェア脅威の状況 (G Dataによる月次マルウェア発生統計データ) に大きな変化が見られました。それは、Javaベースのマルウェアの急増です。ネット犯罪者は、10月頃より、マルウェア拡散にJavaのセキュリティホールを攻撃しはじめています。実際のところ、2010年10月には、頻出するマルウェア種の最高位は、2月以来初めて、「JS Pdfka-OE Exp1」から「Java. Trojan. Exploit. Bytverify. NJ」に変化しました。12月にも再び、「Java. Trojan. Downloader. OpenConnection. AI」という別のJavaベースの脅威が1上位に入りしました。

「JS:Downloader」のようなJavaScriptベースのダウンローダーもまた、現在、非常に活動的であり、恒常的にマルウェア作者によって亜種が作られています。2011年1月に至るまで毎月、Top10でこのマルウェアの亜種を見つけることができます。

Javaにおけるセキュリティホールは、技術的にさまざまな可能性を攻撃者に提供することになります。ま

た、他の形式の感染と比べると、悪性コードの作成と拡散はとても簡単です。そして容易に、攻撃の構成要素をいわゆる 익스プロイトキット内に組み込むことができます。Javaは家庭用でもビジネス用でも、いずれのPCにおいても膨大な量のパソコンで使用されています。2010年下半期では、すべてのPCのうち、平均79%が、Javaプラグインをインストールしていました。

そのうえまた、PDFの脆弱性に関する警告が最近多く発せられたことにより、この危険性の認知率が上昇しました。さらに、PDFリーダーの製造元による多くのセキュリティアップデートのおかげで、マルウェアプログラムの開発がかなり阻害されました。特に、Adobe Readerのバージョン10における大幅な改良によって悪性コードを実行するのは、はるかに困難になりました。

2010年下半期の出来事

2010年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。

▼ネット犯罪・マルウェア事件 2010 ダイジェスト

- 1【情報流出】尖閣諸島中国漁船衝突ビデオの公開（9月）**
デジタルな「ネット情報」の可能性と危険性の両面を広く認知させ、マルウェアやネット犯罪への注意を高める契機にも。
- 2【社会的影響】ガンブラー攻撃（～2010年8月頃まで）**
大手企業をはじめ200以上のサイトが被害、国内最大規模。感染サイトへの訪問者のパソコンも感染し、個人情報盗まれる。
- 3【社会的影響】大手ニュースサイトの広告感染（9月）**
広告配信会社のサーバーを攻撃し、ネット広告を通じ感染拡大を狙う。偽ウイルス対策ソフトを購入させ、個人情報をも盗む手口。
- 4【犯罪】金銭獲得を目的としたロマンス詐欺犯の逮捕（5月）**
ファイル共有ネットワークにマルウェアを仕掛け、金銭をだまし取る。ウイルスを利用した金銭横領詐欺での摘発として、国内初となる。
- 5【犯罪】イカタコウイルス作者の（再）逮捕（8月）**
「著作権侵害」でかつて逮捕されたことのあるマルウェア作者が、今度はオリジナルイラストと使うも「器物破損罪」で2度目の逮捕。
- 6【犯罪】オンラインゲームのパスワード窃盗ウイルス犯の逮捕（11月）**
マルウェアを仕込んだサイトにゲーマーを呼び込み、ID/PWを窃取、アイテムをRMT転売で利益も、不正アクセス禁止法違反で逮捕。
- 7【海外】巨大ボットネット犯ブレードラボの逮捕（オランダ、10月）**
悪質なボットネットを構築していた主犯が産官協力により逮捕。警察も同じ仕組みを使い感染ユーザーに警告も、手法に課題を残す。
- 8【海外】スタクスネットによるサイバーテロ（イラン、11月）**
4つのMSの脆弱性を悪用した高度なマルウェアを使用した集中攻撃、狙いはイラン核施設、しかも後日イランのセキュリティ専門家が暗殺。

9 【海外】 内部告発サイト「ウィキリークス」主宰者の逮捕（英、12月）

尖閣ビデオ流出事件と同様、世界的に機密情報のネット暴露が問われる。ジャーナリストとの連携が鍵、手法として別件逮捕（暴行容疑）は課題。

10 【世界】 年間新種マルウェア発生数が200万を超える（1月～12月）

5年前＝数万、2007年＝10万、2008年＝90万、昨年＝150万。
2010年は200万超、15秒に1つの新種マルウェアが活動という現実。

世界的に景気が冷え込んでいるのとは裏腹に、ネット裏市場では、かつてないほど、好況を呈しています。私たちが思っている以上に、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みつけ、ツールを買い求め、私たちを畏にはめ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、大部分の人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畏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はないでしょうか。

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。

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、ご自身のパソコンの安全性を高めることが、第一です。年間で200万も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。

2010年7月

7月13日 マイクロソフトは、Windows XP 32bit Service Pack 2のサポートを終了。該当するユーザーは、Windows VistaまたはWindows 7へのアップグレード、もしくはWindows XP Service Pack 3（2014年4月までのサポート）のインストールが必要。Windows XPを使用し続けるユーザーは、サイバー犯罪者の危険に晒される可能性が高まる。

7月15日 通称「ゼウス」（Zeus banking Trojan）と呼ばれるトロイの木馬型マルウェアが「Visaによる認証」（Verified by Visa）や「セキュアコードプロテクション」（SecureCodeProtection）などのクレジットカードセキュリティ技術をターゲットにした攻撃を行う。オンラインバンキングのユーザーは、ブラウザの偽ウィンドウに、実際の銀行による処理では必要とされないような社会保障番号やクレジットカード情報の入力并要求される。米国の主要銀行15行がこの攻撃の対象とされる。

7月28日 マリポーザボットネットの作成者をFBIが突き止め、逮捕。同ボットネット作成者は、23歳のスロベニア人男性で、「Iserdo」というニックネームで活動。スロベニア警察によって逮捕された。スペイン、アメリカ、スロベニアの当局による「バタフライボットネット（Butterfly Botnet）」の捜査は開始から二年で実を結んだ。

2010年8月

8月5日 日本の警視庁は、PC上の全データを削除してタコヤイカのイメージに置き換えるコンピュータウイルス「タコイカウイルス」を頒布していた会社員の中辻正人容疑者（27）を逮捕。「タコイカウイルス」に感染したファイルは、削除前にWebサーバーに送信。警察の発表によると、被害者は20,000人にもものぼると特定。中辻容疑者は2008年にもウイルス作成していたがその際は著作権法違反の判決を受け、執行猶予中だった。今回は著作権法違反を回避するためか、自身でタコヤイカのイメージを用意していた。

8月16日 スケープゲーミング社（Scapegaming）が不法に独自のWOW用のゲームサーバを設置して運営していたことに対する裁判で、ブリザード社（Blizzard）が勝訴。カリフォルニア地方裁判所は、著作権侵害と判断し、8,800万USドルの損害賠償の支払いをスケープゲーミング側に命じた。スケープゲーミングが過去3年間で運営で売り上げた額は、約300万USドル。

8月19日 半導体メーカー最大手のインテル社（Intel）が、セキュリティソフトベンダー大手のマカフィー社（McAfee）の買収を発表。買収額は76億8000万USドルで、マカフィーはインテルの100%子会社となる予定。

8月23日 マイクロソフトがプログラムライブラリに関連付けられた脆弱性で、DLLスプーフィングの危険性について警告。リスクを軽減すると考えられる現在の唯一の方法は、WebDAVサービスとSMBファイル共有プロトコルの無効化。デンマークのセキュリティーベンダーであるセキュニア社（Secunia）が発表した160のリスクプログラムのリスト（2010年6月12日時点）によると、22のプログラムだけがセキュリティリスクに対応。

8月28日 ドイツのディスカウントチェーンであるシュレッカー（Schlecker）でデータ漏洩が発生。対象となったのは約15万人の顧客データ、および710万人分のニュースレター登録者のメールアドレス。

2010年9月

9月6日 ドイツ連邦刑事警察署とIT関連業界団体Bitkomは、2010年にドイツ国内でのインターネット犯罪による被害総額を17万ユーロと推定する調査報告を発表。同調査によると、ドイツ人の約43%が「自身のPCがマルウェアに感染している、もしくは感染したことがある」と回答。また、インターネットユーザーの5%が、データ盗難やマルウェアが起因なる金銭的損失を被っている。

9月8日 インターネット上での著作権侵害に対し、全欧規模の活動が欧州刑事警察機構（=ユーロポール）によって行われていることをベルギー警察が認める。欧州14カ国で、様々な調査、没収の執行（50件）、容疑者の逮捕などが行われた。リリースグループと呼ばれる組織が、オランダで行われていた約80%の新作映画の違法アップロードに関与していた模様。また、同組織が行っていた著作権で保護された音楽、ソフトウェア、PCゲームなどの配布についても告訴されている。

9月14日 ドイツのソーシャルネットワークであるロカリステン（Lokalisten.de）の運営者は、特殊なテキストを利用することでプラットフォーム上でクロスサイトスクリプティングの実行できるセキュリティホールを閉じた。ロカリステンが実装していたテキストのフィルタリングは、不正なJavaScriptコードは削除できていなかった。

9月14日 OpenX Ad Serverのビデオプラグインのセキュリティホールを悪用し、Webサイトへと配信されたバナー広告に悪意のあるコードを忍ばせることが可能に。感染したバナーは、The Pirate Bay、esarcasmとAfterDawnなどのサイトに掲載。

9月15日 ドイツの情報セキュリティ庁（BSI）とデジタル経済協会（eco）がアンチボットネット相談センターを設立。ボットネット対策の情報、アドバイス、ソフトウェアなどを提供。

9月20日 ゾーンアラーム（ZoneAlarm）の開発元であるチェックポイント社（Check Point）が、コンシューマーに向けたプロモーションを無料版製品に実装し、批判の対象に。ゾーンアラームの無料版ユーザーは、ポップアップで有料版のセキュリティスイート購入を促されるのだが、プロモーション方法はスクリーンウェアを彷彿とさせるものであった。

9月22日 アメリカの裁判所がブルース・レイズレリ（Bruce Raisley）（49）に有罪判決を言い渡した。レイズレリはマルウェアをプログラムし、10万台のPCを感染させてそれらでボットネットを構成。このボットネットを利用して、自身に関する記事を公開していた雑誌のWebサーバに対するDDoS攻撃を実施。レイズレリの復讐で生じた損害推定額は約10万USドル。

9月23日 ドイツのECカード決済処理会社であるイージーキャッシュ（Easycash GmbH）は、連邦データ保護法で求められているチェックアウトプロセス中に生成されるデータを使用していないことを、ドイツ公共放送のNDRが指摘。

9月24日 ユニセフは、2009年に実施した「プレゼントの分を寄付金に」（donate instead of sending presents）キャンペーンに関与した147の企業データを誤ってインターネット上に掲載。公開されたデータはグーグル（Google）の検索でアクセス可能で、今回の事故原因は、サーバーの移行におけるセキュリティの誤設定。

9月27日 オンライン決済サービスのペイパル（Paypal）では、未登録の第三者のクレジットカード情報を使用して、容易に最大1500ユーロまでの取引できることが明らかになった。ペイパルの広報担当者によると、

顧客データの検証は時間がかかるが、この間に 送金や受信などにリミットがないとコメント。

9月30日 ブリザードは、将来的に同社が提供するフォーラム内のすべての寄稿者をゲーマーの実名（実際のID）で表示すると、7月に発表した。ブリザード側は、この種の変更で、ゲームのよりソーシャルネットワーク化を目的としていたが、ゲームコミュニティはこれに反対。あるユーザーは、インターネット上で見つけたブリザードの従業員の個人情報の範囲を自分のブログに公表。これを受け、ブリザードは当初の計画を変更し、現在のフォーラムへの寄稿者が今後も匿名性を保持、またゲーム内でのリアルIDの機能はオプション提供のみ、と方向転換。

2010年10月

10月1日 FBIが18ヶ月前に開始したサイバー犯罪者（主にゼウスボットネット）に対する大規模な捜査、「トライデント・ブリーチ作戦」（Operation Trident Breach）を完了した。米国、オランダ、ウクライナ、イギリスで、少なくとも16搜索令状が執行され、39人の逮捕者が出た。犯罪の合計金額は2億2000万USドルにも上る。

10月9日 メディアの報道によると、ドイツの税関職員は司法当局の許可があればVoIP電話での通話を傍受でき、連邦憲法裁判所による判決の権限内でのオンライン調査が許可されている。調査員は容疑者のコンピュータに密かにアクセスし、データが暗号化される前に言語データとして抜き出す。

10月17日 ウイルス対策ソフトメーカーのカスペルスキー（Kaspersky）が、4時間にわたり同社の米国サイト上でスケアウェアを配布。攻撃者は、サードパーティプロバイダのアプリケーションが持つ脆弱性を悪用し、カスペルスキー製品をダウンロードしようとする顧客を偽ウイルス対策感染サイトに転送。

10月22日 5月に発足した米国政府サイバー軍の活動内容詳細は依然不明。当時、オバマ大統領は、「サイバー脅威が、現在私達の国家が直面する最も深刻な経済と国家安全保障上の課題の一つである。しかし、同国サイバー軍は、個人のネットワークやメールアドレスを監視することはない」とも主張していた。

10月27日 Firefox 3.5および3.6で深刻な脆弱性をモジラ（Mozilla）が報告。ノーベル平和賞のウェブサイトを経由したトロイの木馬のドライブバイダウンロードが確認された。この脆弱性は3.6.12の更新で対応し、48時間以内に閉じたこととなる。発表によると、今回の脆弱性はWindows 2000およびWindows XPが対象となっていた。

10月29日 ロシアの捜査組織「カツシャ（Katusha）」は、は、大規模なオンラインバンキングの不正取引を行っていた国際的なグループへの侵入に成功。この捜査は、エストニアと英国当局との共同調査で実施。260件を超える不正取引で少なくとも1.65万ユーロを不正取得していた模様。被害者のパソコンへの感染手口は、不正なPDFファイルやドライブバイダウンロードによる感染。

2010年11月

11月4日 メガディー・ボットネット（Mega D Botnet）を運営していたロシア人容疑者、オレグ・ニコラエenko（23）をFBIがラスベガスで逮捕。全世界で送信されているスパムの19%（デンマークのスパム対策ソフト開発会社であるスパムファイター（SPAMfighter）によると、2008年にMega Dのアカウントからのスパム送信が全世界で32%）の送信量を誇るメガディー・ボットネットが単独人物によって運営されていたかは、いままで定かではなかった。同容疑者はアメリカの迷惑メール規制法であるCAN-SPAM法（Controlling the

Assault of Non-Solicited Pornography and Marketing Act)違反容疑で告発。

11月5日 オリガミ・トロイというマルウェアが、ロシアやウクライナで主に蔓延中。個人情報盗む非常に強力で、主に銀行関連データが中心。ロシアやウクライナのユーザーがマルウェアの攻撃対象となっているのは極めて異例。

11月8日 泥棒に入った先のコンピュータでマイスペース (MySpace) を利用し、ログアウトしわすれたことで足が付き、逮捕される事件がフロリダで発生。

11月9日 ドイツの新たな電子IDカード用ソフトウェアが発売されてから24時間以内に脆弱性が発見された。

11月12日 2008年のアメリカ副大統領候補、サラ・ペイリンの個人メールアカウントをハッキングしたとするデビッド・カーネル (22) に、懲役1年と1日を言い渡された。米司法省の裁判官はカーネルの行為について「政治キャンペーンの頓挫を目的とした、政治的動機を背景とすると政治的な行為」と判断。カーネルは、ペイリン氏のプライベート画像やメールを誰でも見れるように、ネット上に公表していた。

11月18日 グーグルがグーグルストリートビューのサービスをスタート。2010年の初頭、多くの方面から非難されたが、ドイツ国内20都市のイメージが閲覧可能に。メディアの報道によると、25万人がサービス開始前にグーグルに対し自宅や自身の画像削除を依頼。グーグル側は、車のナンバープレートや人物の顔が認識できないよう加工することを約束。

11月18日 ジーデータのセキュリティラボ (G Data SecurityLabs) 研究員がゼウスの後継マルウェアを発見。マルウェア作成者は、フォーラムで近いうちのリリースを予告。このマルウェアの概要説明で、作成者は多数の亜種を約束し、あらゆる種類の攻撃に利用できると謳っている。なお、スターターパックは\$ 850。

11月23日 スコット・マシュー・アンダーソン (33) は、母親のリビングルームからボットネットを運営。何百万通ものスパムメール送信、ボットに感染したコンピュータから個人情報を不正に盗み出し、更にウェブカメラを通して被害者をスパイしていた容疑で、禁固18ヶ月と罰金5,000ポンドの刑を言い渡された。5児の父であるアンダーソン自身の家には、ブロードバンド環境が整備されていなかった。

11月24日 フランス政府は、「オンライン広告サービス購入」税を2011年1月1日から施行。この税 (通称「グーグル税」 (Google Tax)) を納める義務があるのは、オンライン広告を利用するフランスに所在する企業。フランス政府は、グーグル税によって年間10億~20億ユーロの歳入を見込む。

11月28日 ウィキリークス (Wikileaks) は、アメリカの外交機密文書約25万点を公開。これに関連して、16歳と19歳の男性2人がオランダで拘留された。この後、ウィキリークスのスポークスマンのジュリアン・アサンジも拘留され、保釈後も監視下におかれる。

2010年12月

12月1日 ドイツのノルトライン・ヴェストファーレン州の男性2人が音楽著作権侵害の容疑で起訴されています。二人は、トロイの木馬を使って音楽業界関係者のメールアドレスを不正に獲得し、コンピュータにアクセスするなどして、未発表曲を盗みだしていた。

12月3日 スイス議会で、通信とデータネットワークの保全に対する取り組みがテーマに上がり、アクティブおよびパッシブなセキュリティに関する法整備について話合われている。国防相はサイバー戦争やサイバ

一犯罪分野に関連する対策の必要性を主張。

12月10日 ドイツ西部のデュルメンでは、44歳の男性がトロイの木馬を利用し、約100台もの個人のコンピュータにアクセス。コンピュータに接続されているウェブカメラを使用して所有者を監視していた容疑で、1年10ヶ月の禁固（執行猶予付き）の判決が下された。最年少の被害者は13歳の少女で、ウェブカメラのランプが消灯しないのを不審に思い、それを報告して事態が判明。

12月14日 アメリカ・コロラド州保安官事務所で、大規模なデータ漏洩が発生。保存されていた容疑者、被害者、通報者などのデータ、20万セットがインターネットに流出。同年4月に同所のメンバーが自身のコンピュータにデータをコピー、その後、コンピュータの感染によりデータが流出した模様。

12月18日 ツイッター (Twitter) が2010年の年次統計を発表。話題トップ10の1位は、「メキシコ湾の原油流出事故」、続いて2位は「FIFAワールドカップ」、そして3位は「映画インセプション」。「タコのパウル君」はトップ10に掲載。「Most Powerful Tweet」の4位は、BPの偽アカウントからツイートされたつぶやき。

12月25日 米国タイム (Time) 誌は、フェイスブック (Facebook) 創設者であるマーク・ズッカーバーグ (Mark Zuckerberg) 氏を 2010年の「パーソン・オブ・ジ・イヤー」 (Person of the Year) に選んだ。選出理由は、ズッカーバーグ氏が創設したフェイスブックによる社会への変革と、5億5,000万人以上の世界中の人々（うち、約70%は米国外の居住者）を結びつけたことへの貢献。一方、英国の新聞フィナンシャルタイムズ (Financial Times) は、アップル (Apple) のCEOであるスティーブ・ジョブズ氏を2010年の「パーソン・オブ・ジ・イヤー」とした。

12月28日 オランダ、Zuidwest Drentheの警察署長が、同警察署が調査にあたっていた女性2人の死因に関する信頼性の低い情報をツイッター (Twitter) 経由で流し、被害者側の人権を侵害。