German
Data
Security

G Data

マルウェアレポート

—2009年上半期—

G Dataセキュリティラボ

ラルフ・ベンツミュラー＆ヴェナー・クライアー

(岸本眞輔・瀧本往人 訳)

Go safe. Go safer. G Data.

概要

数字とデータ

G Data セキュリティラボの調べでは、2009年上半期のマルウェア発生数は、663,952種にのぼりました。2008年上半期と比較すると、2倍以上の伸びを見せました。2008年下半期と比較すると、約15%の増加でした。また、活動しているマルウェアの種類は、7%減少しました。

種別では、トロイの木馬、バックドア、ダウンローダーが多く現れました。トロイの木馬とダウンローダーは比率が上昇し、バックドアは下降しました。ルートキットに関しては、引き続き増え続け、2008年上半期と比較すると、8倍以上の増加となりました。

自己増殖型のマルウェアであるワームは、全体の4%ほどでした。

亜種の多いマルウェア種は、トロイの木馬やバックドアに属すもの、またはオンラインゲームのアカウントを盗みだすものが、上位を占めました。ワーム種のオートラン（Autorun）が大幅に増加し、2008年上半期と比較すると約5倍増、割合では1.6%を占めるに至りました。

全マルウェアの99.3%がウィンドウズを標的としていました。変わりなくウィンドウズが大きな標的とされ続けています。

モバイルプラットフォームの不正コードが、ついにトップ5に入りました。ただしその数は106種であり、全ての新種マルウェアの割合からみると、微々たるものでした。

MacOS Xユーザーも攻撃対象とされました。数は15種。4月には初のアップルのボットネットも確認されました。

結果とトレンド

SNS が、ますますスパムやマルウェアの拡散に悪用される傾向にありました。

コンフィッカー、別名USBウイルスが大流行し、数百万台のPCを感染させました。エイプリールフールの動向が注目されましたが、大事には至らず、その後、沈静化しました。

展望

インターネット上に仕掛けられた不正コードの数は、まだまだ減少する気配はありません。しかも感染方法が、より複雑化・巧妙化し、成熟してゆくでしょう。

当面マルウェアは増加するとはいえ、その増加率は以前よりも低くなるでしょう。活動するマルウェアの種類も、減少する傾向にあると予測されます。

今後マルウェア製造者は、MacOS Xやスマートフォンを標的とするおそれがあります。

目次

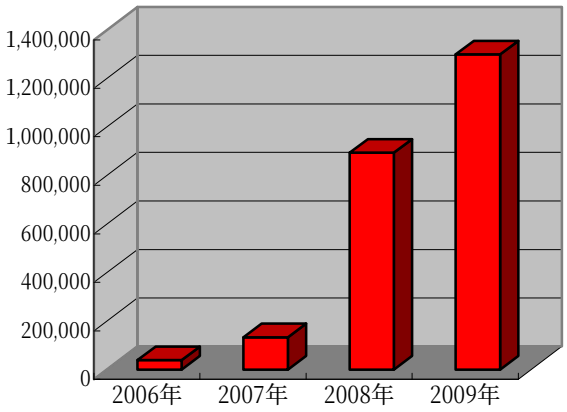
マルウェア状況：数字とデータ

マルウェアはまだ大量発生中も、伸びは鈍化

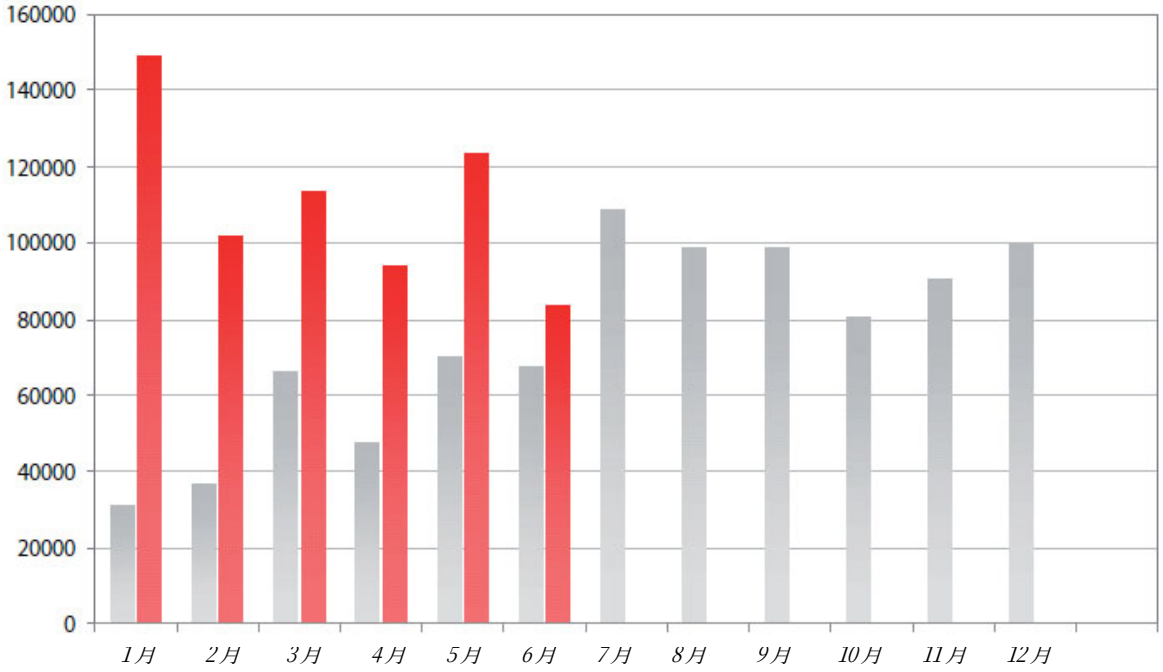
2009 年上半期の新種マルウェアの発生数は、G Data セキュリティラボの調べによれば、663,952 種にのぼりました*。まだ大量発生しているものの、伸び率で見るとやや鈍化し、2008 年下半と比べると 15%増にとどまりました。マルウェアの発生数は、ここ数年、異常な伸びを示してきたので、それと比べると、ようやくピークを迎えた可能性もあります。＊この総数の計算は、悪性コードを含むファイルを一つずつ数え上げたものではありません。あくまでもワクチン側から見たものです。

年間ベースで見ると、下半期にほぼ同数程度発生すると考えると、年間で約 130 万種程度の発生となる勢いです。2006 年が 39,124 種、2007 年が 133,252 種、2008 年が 894,250 種でしたので、2009 年 1 年間の発生数は過去最高となる公算が大きいでしょう。

月別については、年初の 1 月で 14 万種を超えピークに達しましたが、その後の 5 ヶ月はやや減少傾向にありました。しかし、それでも結果的には、2008 年上半期の 318,248 種の発生数と比べると、2 倍以上の増加となりました。



年別マルウェア発生数（2009 年は推定値） G Data セキュリティラボ調べ

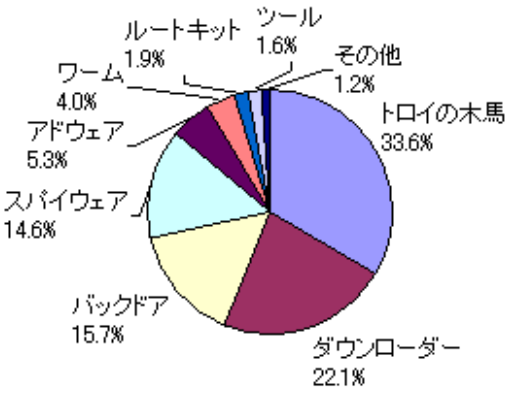


月別マルウェア発生数(赤＝2009 年、グレー＝2008 年) G Data セキュリティラボ調べ

マルウェアカテゴリー別状況

2008 年上半期のマルウェア発生状況において、カテゴリー別にみると、トロイの木馬型が 33.6%を占めトップとなりました。ダウンローダーが 2 位で 22.1%、続いて、バックドア、スパイウェア、アドウェアが 3～5 位となりました。

トロイの木馬とダウンローダーが伸びているのに対して、バックドア、スパイウェア、アドウェアの増加はやや鈍化している、というコントラストが発生しました。



ウイルス種別比率(2009 年上半期) G Data セキュリティラボ調べ

特にバックドアが今回はじめて減少に転じたのは、スパムを送って DoS（サービス不能）攻撃を行うボットネットの需要に、やや陰りが現れてきたことを意味するかもしれません。ただし、8 位のルートキットが割合こそ 1.9%ではあるものの、2008 年上半期との比較では 8 倍以上の増加が見られたので、バックドアが単体ではなく複合化して動き出している可能性もあります。

また、アドウェアが高い数字で推移していますが、飛躍的に増加していないということは、各機関による啓蒙活動が、何らかの効果を発揮している、という見方もできます。しかしながら、経済恐慌が長引くなかで、ネット犯罪に関与する人間たちでさえ、これまでのように闇雲にウイルス攻撃を行うのではなく、多少絞り込みを行っている、というのが実情かもしれません。

次に、スパイウェアはほんのわずか減少する一方で、キーロガーの数が倍増しました。また、オンラインバンキングやオンラインゲームのパスワードを盗み出すトロイの木馬は、それぞれ約 30%減少しました。銀行やネットゲーム企業は、セキュリティを強固にしたため、従来通りの手法ではデータを盗み出すことができなくなったことが、数字の低下につながったようです。今後もまた、データを窃取することを目的としたマルウェアは、より高性能のものが目指されるでしょう。

	2009 年上半期		2008 年下半期		前年下半期との差	2008 年上半期		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	221,610	33.60%	155,167	26.90%	143%	52,087	16.40%	425%
ダウンローダー/ドロッパー	147,942	22.10%	115,358	20.00%	128%	64,482	20.30%	229%
バックドア	104,224	15.70%	125,086	21.70%	83%	75,027	23.60%	139%
スパイウェア	97,011	14.60%	96,081	16.70%	101%	58,872	18.50%	165%
アドウェア	34,813	5.30%	40,680	7.10%	86%	32,068	10.10%	109%
ワーム	26,542	4.00%	17,504	3.00%	152%	10,227	3.20%	260%
ルートキット	12,229	1.90%	6,959	1.20%	176%	1,425	0.40%	858%
ツール	11,413	1.60%	7,727	1.30%	148%	12,203	3.80%	94%
エクスプロイット	2,279	0.30%	1,841	0.30%	124%	1,613	0.50%	141%
ダイアラー	1,153	0.20%	1,013	0.20%	114%	4,760	1.50%	24%
(狭義の) ウイルス	143	0.00%	167	0.00%	86%	327	0.10%	44%
その他	4,593	0.70%	8,419	1.50%	55%	5,170	1.60%	89%
計	663,952	100.00%	576,002	100.00%	115%	318248	100.00%	209%

マルウェア発生数と割合（2008年上半期、下半期、2009年上半期）G Dataセキュリティラボ調べ

ダイアラーは、2008年の上半期と比べると、約1/4ほどに下がりました。明らかにダイアラーは古いビジネスモデルとして古くなりました。

また、狭義のウイルス（ファイルインフェクターなど）の数も、2008年の上半期と比べると、かなり減少しています。

なお、ワームについては、今回はオートラン系統のものを数多く含むため、比率を4.0%まで増加させました。2008年の上半期と比べると2.6倍に、2008年の下半期と比べると1.5倍になりました。

マルウェア種別状況

使用されたプログラムコードの機能と特性に基づいて、マルウェアプログラムは種（ファミリー）に細分されます。2008 年上半期に発生したマルウェアを種別でみた場合、1 位はモンダー（Monder）でした。2 位はフピゴン(Hupigon)、3 位はゲノム(Genome)、4 位はブザス(Buzus)、5 位はオンラインゲームズ(Onlinegames)でした。

マルウェア種の数自体は、次第に減少しているのが現状です。2008年の上半期には2,395種発生しましたが、下半期には2,094種、そして2009年の上半期では、1,948種でした。つまり、種の数が減少する一方でマルウェアの発生数が増加しているということは、ある特定のマルウェアが集中して使用されているということを示します。

	2009 年上半期	ウイルス属	2008 年下半期	ウイルス属	2008 年上半期	ウイルス属
1	34,829	モンダー	45,407	フピゴン	32,383	フピゴン
2	26,879	フピゴン	35,361	オンラインゲーム	19,415	オンラインゲームズ
3	18,576	ゲノム	20,708	モンダー	13,922	バーチュモンド
4	16,719	ブザス	18,718	モンダーB	11,933	マガニア
5	16,675	オンラインゲームズ	15,937	シンマス	7,370	フェノメンゲーム
6	13,889	フラウドロード	13,133	ブザス	7,151	ブザス
7	13,104	ビフローズ	13,104	マガニア	6,779	ズィーロブ
8	11,106	ポイズン	12,805	ピーシークライアント	6,247	シンマス
9	10,322	マガニア	11,530	ズィーロブ	6,194	バンロード
10	10,312	インジェクト	10,412	バーチュモンド	5,433	ビフローズ

最も活動的なマルウェア種ベスト10（2008年上半期、下半期、2009年上半期） G Dataセキュリティラボ調べ

マルウェア種のなかには、亜種がそれほど多くないものもあれば、ものすごい勢いで増加しているものもあります。長年にわたってベスト10にランクインしているものもあれば、突発的に増加し消えてゆくものもあります。

バックドアに属するフピゴンとビフローズ、ネットゲームのデータを盗むオンラインゲームズとマガニア、トロイの木馬に属するブザスなどは、ここ数年、上位にランクインし続けているものです。ただしフピゴンは、2008年においては最上位にいましたが、今回、モンダーに首位を奪われました。モンダーは、バーチュモンドの後継的な存在として注目されているのです。

フラウドロードが新たにエントリーされたのは、偽ウイルス対策ソフトの挙動を伴うスケアウェアがサイバー犯罪者に絶大なる人気がある、ということを示すでしょう。

他に新たにエントリーされたのは、ゲノム、ポイズン、インジェクトでした。

上位マルウェア種の概要

1位　モンダー　（Monder）

トロイの木馬型で、感染したシステム上のセキュリティ設定を操作し侵入しやすくします。亜種が無数に発生しており、求められてもいない広告を表示するアドウェアを併用するものや、ウイルススキャンを偽装し、感染したとみせかけて完全版の購入を促し、クレジットカードで支払うよう誘導し、個人情報を盗み出すものがあります。また、別のマルウェアをダウンロードし、ユーザーに知られずにネット閲覧の履歴を攻撃者に転送するものもあります。

2位　フピゴン　（Hupigon）

バックドア型で、ウェブカムを利用してキー入力データを記録しスクリーンショットを撮ることができます。

3位　ゲノム　（Genome）

トロイの木馬型で、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。2009年1～2月に多く発生しました。

4位　ブザス　（Buzus）

改ざんされたサイトやメールの添付ファイルから感染し、脆弱性を狙ってセキュリティ設定を変えキーロガーなどを呼び込むトロイの木馬型ウイルスです。クレジットカードやオンラインバンキング、メールアドレス、FTPのIDとパスワードなどの個人情報を盗むのに用いられます。

5位　オンラインゲームズ　（OnlineGames）

トロイの木馬型で、ネットゲームのアクセスデータを盗み出します。ピークは2007年から2008年でしたが、ネットゲームは依然としてデータ窃盗の標的となっています。ゲームのキャラクターやアイテムなどのデータは多くのフォーラムにてRMT（リアルマネートレード）で取引されています。これがネット犯罪者たちをひきつけている理由です。

6位　フラウドロード　（Fraudload）

セキュリティソフトやシステムツールを偽装するスケアウェアを使ったもので、製品を購入させようと特設サイトに誘導しクレジットカード情報を入力させ盗み出します。一般に、OSのセキュリティホールにパッチをあてていない場合や、アプリケーション・ソフトに脆弱性があることで、感染が起こります。このフラウドロードは、アダルトや最新ニュース、ゴシップといった多くの人が関心を持ちそうなテーマの動画を用意し、その動画を再生するためにビデオコーデックをダウンロードしなければならない、と思わせて感染させるという手法をとっています。

7位　ビフローズ　（Bifrose）

バックドア型で、感染したPCにアクセスし、IRCサーバーに接続できるようにします。

8位　ポイズン　（Poison）

バックドア型で、認証されていなくともリモートでアクセスできるようになり、たとえば回線速度を遅くさせるなどのDDos攻撃に用いられます。

9位　マガニア　（Magania）

トロイの木馬型で、台湾のガマニア社のオンラインゲームのパスワードを盗むために用いられます。

メールの添付ファイル（.rar）に紛れて侵入し感染させ、バックドアを仕掛けると同時にインターネットエクスプローラーにDLLを登録し攻撃者がいつでもネット利用をモニタリングできるようにします。

10 位　インジェクト　（Inject）

実行プロセスを操作するタイプのトロイの木馬であり、多数の亜種があります。攻撃者が自由に、しかも、被害者に知られずに、プロセスを統御できるようにするものです。

USB ウイルスの流行

ワームのなかで最も活動的だったのは、オートランでした。トップ10には入りませんでしたが、9,689もの亜種があり、全体の1.6%を占めました。

オートランは、CDやDVDさらにはUSBメモリの自動実行ファイルを利用して感染させるものです。感染後にメディアにそれ自体をコピーして、「autorun.inf」と呼ばれるファイルを作成します。かなり広範囲にこのマルウェアが発生したため、ウィンドウズのオートラン機能を止めることが賢明な措置となり、マイクロソフトがパッチを用意することになりました。

PDF ウイルス

最も頻繁に起こったエクスプロイット攻撃は、PDF ウイルスによるものでした。ウィンドウズ・メタファイル（WMF）のセキュリティホールと PDF の脆弱性が利用されました。特に 2009 年 5 月から 6 月にかけてかなり多くの数が発生しました。これまでは多く利用されてきたセキュリティホールが多く狙われてきましたが、それだけではなく、PDF の JavaScript コードを実行する可能性が、マルウェア作者の中で注目されはじめています。

プラットフォーム別マルウェア発生状況

2009 年の前半のマルウェア状況について、プラットフォーム別にみると、ウィンドウズが圧倒的に多く、99.3%を占めました。マルウェア製造者は、攻撃先をあらためてウィンドウズに絞ったといえるでしょう。

したがって、他の OS の比率は極端に少なくなっています。5 位以下では、UNIX ベースのシステムでマルウェアは 66 種（昨年下半期は 16 種）、Mac OSX は 15 種（昨年下半期は 6 種）でした。Mac OS 以外にも、MSIL が 365 種（全体の 0.1%）、モバイルが 106 種（0.01%）と若干増加していますが、全体的には、引き続きウィンドウズを標的としたマルウェアが圧倒的多数であることに変わりはありません。

		2009 年上半期		2008 年下半期		2008 年上半期	
	プラットフォーム	発生数	構成比	発生数	構成比	発生数	構成比
1	Win32	659,009	99.3%	571,568	99.2%	312,656	98.2%
2	WebScript	3,301	0.5%	2,961	0.5%	3,849	1.4%
3	Script	924	0.1%	1,062	0.2%	1,155	0.3%
4	MSIL	365	0.1%	318	0.1%	252	0.1%
5	Mobile	106	0.0%	70	0.0%	41	0.0%

プラットフォーム別マルウェア発生数トップ５（2009年上半期、2008年下半期、上半期）

2位のWebScript はJavaScriptやHTML、Flash/Shockwave、PHPもしくはASP、さらにはブラウザ

の脆弱性などをもとにしたマルウェアを含みます。3位のScriptは、VBSやPerl、Python、Rubyといったスクリプト言語で書かれたバッチ、シェルスクリプト、またはプログラムを含みます。4位のMSILは、 .NETプログラムのバイトコードにストアされるマルウェアを含みます。5位のMobileは、J2MEやSymbian、Windows CEのマルウェアを含みます。

Symbianで感染するSMSワーム

スマートフォンとポータブル・コンピュータのための新しいマルウェアプログラムは、数としては106種であり、全体の0.01%と微小ですが、昨年の上半期と比べると、倍にまで増加し、再びトップ5入りしました。しかもそのうち約90のプログラムは感染ルートを持っておらず、ロシアや中国の電話利用者にSMS（テキスト・メッセージ）が送られてくるだけのものでした。ただし、イクセ（Yxe）またの名をセクシー・スペース（SexySpace）だけは、ウェッブサイトへのリンクがあり、かつ、ネット犯罪者が、この流れの承認手続きをSymbianに対して行っていたため、危険性の高いものとなっていました。電話帳の番号を盗みメッセージを送りつけるため、大きな被害が出る恐れがありましたが、実際には中国もしくは中東でのみ発見され、それほどの被害は出ませんでした。今後の動きには十分な注意が必要でしょう。

2009年の展望

マルウェアは、まだしばらくのあいだは、膨大な利益を生むことでしょう。ネット犯罪の組織体制は、しっかりと確立され、スパム、スパイウェア、そしてアドウェアなどを使用した確固たるビジネスモデルができあがりました。マルウェアを製造する人間、マルウェアをまき散らす人間、そして、集金する人間、といったように、役割を分担しつつ、金儲けをすることが簡単になったのです。

もちろん時々は、警察などによるネット犯罪者の逮捕が報道されることもありますが、そのような一時的な成功は、このような体制を揺るがすことは難しいでしょう。

いずれにせよ、今後も相変わらずウィンドウズ・ユーザーが最も狙われることは間違いありません。そしてマルウェアの数も減ることはなく、あふれ続けることでしょう。しかしマルウェアの種はかなり絞り込まれ、増加率も、ここ数年の急な伸びと比べると、落ち着き気味となると予測されます。

地下経済とはいえ、専門的なアプローチを行っているので、OSやよく使われているアプリケーションにおけるセキュリティホールがリリースのほんの数日後にマルウェアによって利用されるのは、驚きではありません。

また、すぐに、マルウェアの作成を可能にするような使い易いツールが多数存在しているので、未経験のユーザーでもすぐさまマルウェアを利用可能です。現在最も弱い部分は、ブラウザとそのコンポーネントです。ほとんどのセキュリティホールが見つけられ、利用されます。このことは、コンピュータを最新の状態に保たないならば、ネット犯罪者にすぐにつけこまれるということを意味します。

もちろん他のプラットフォームへの攻撃の準備も続いています。特にアップル、ユニックス、携帯機器関連の数は増加することでしょう。とは言え、ただちに大規模な攻撃が起こるとは思えません。

マルウェア侵入経路の多くがセキュリティ技術で閉じられた今となっては、攻撃者は、数は少ないものの成功可能性の高い個所を狙おうとしています。そうすると現在最も勝算が高いのは、数多くのアプリケーションと関係しているウェブサイトということになります。

したがって今後は、より新しく、より巧妙な攻撃のシナリオが用意される可能性が高くなります。Flash

やPDFなど、現在の時点で過小評価されてきたメディアは、もっと頻繁に利用されることになるでしょう。また、ウェブ閲覧者がウェブページを訪れて、何らかのアクションをすることで感染するようなトリックは、確実に増えてゆくことでしょう。また、ソーシャルネットワークの関心が高まっているため、闇雲に攻撃が行われるおそれがあるでしょう。現在Twitterがこの点について最も注目されており、ユーザーからみると最も危険性があるところとなるでしょう。

2009年下半期の動向予測

2009年下半期のマルウェア動向について以下のようにまとめられます。急上昇するおそれのあるWebscriptsとMobileには特に注意が必要です。

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	↘
ツール	↗

カテゴリー	動向
ルートキット	↗
エクスプロイット	↗
Win32	↗
Web scripts	↑
Scripts	→
MSIL	→
Mobile	↑

2009年上半期の出来事とトレンド

ここでは、2009年上半期のマルウェア関連事件を以下に時系列順にまとめました。

最も際立った出来事は、2009年の最初の1カ月目から巨大な騒動を引き起こしたコンフィッカー関連のものです。また、Twitterや、LinkedInや、MySpaceやFacebookなどのSNS絡みの事件も目立ちました。差し当たり、マルウェア製造者は、すぐにそのような傾向を知り、それらが提供する機会を利用します。個々の思惑はいろいろとあると思いますが、SNSに強く関心を抱いていることは確かです。

フィッシング詐欺は1年前には銀行とeBayに主に制限されましたが、昨年末中にGoogle とSNS系のFacebook、SulakeおよびMySpaceがPhishTankのトップ10の常連になりました。しばらくSNSは、情報筋として狙っている攻撃の準備にサイバー犯罪者に役立っており、スパムをカスタマイズしています。SNSが、使用者を伸ばしているように、マルウェア製造者にとっても人気となっているのです。

Koobfaceによる被害が増加

これはKoobfaceワームの進化で明確に示されます。名前が示すように、初めに拡散させるプラットフォームとしてFacebookの上と、そして、MySpaceのその後すぐ上で集中していたなら、リストはこの数か月にhi5.comや、friendster.comや、myyearbook.comや、bebo.comや、tagged.comや、netlog.comや、fubar.comやlivejournal.comなどのソーシャルネットワーキングサイトによって広げられました。 そこで作成されたリンクが、ウェブサイトにどこを指すか、テンプレートをだまして奪いながら立証されて、「Schummel AntiVirus」や「コーデックまたはフラッシュのダウンロード」を抽出できます。

しかし、また、以下のテーブルが示すように、Koobfaceは増加しています。 6月に、亜種の数は約10倍にまで上昇しました。

	2009年1月	2月	3月	4月	5月	6月
クーブフェイス亜種発生数	18	14	23	50	56	541

2009年上半期におけるクーブフェイス亜種の発生数

今後もSNS関連の被害が増えると予想できます。利用者数の増加に応じて、マルウェアをまき散らしたがっている人々の関心も高まっているのです。

Jan 2009

1月5日　スパムメール配信に利用するための、Twitterユーザーを狙った偽ログインサイトへの誘導がみつかる。

1月6日　複数のアカウントがハックされたと、Twitterが警告。被害者の名でメッセージが送信され、被害者にはブリトニー・スピアーズ、バラク・オバマなども。

1月7日　SNSサービスの LinkedIn において、偽の有名人プロファイルの作成を確認。それらには偽ウイルススキャナやトロイの木馬に感染したウィンドウズ・メディア・プレイヤーのバージョンがダウンロードされるリンクが貼りつけられていた。有名人の被害者は、Victoria Beckham, Beyoncé Knowles, Salma Hayek など。

1月8日　オーストリアのケルンテルン州政府のPC 3,000台がコンフィッカーワームに感染。原因は2008年10月にMSから提供されているパッチを適応していなかったため。

1月12日　コンフィッカーがケルンテルン州で猛威をふるう。今回はケルンテルンの病院、KABEGにて。約3,000台のPCが被害に。

1月14日　コンフィッカー感染の推定数：250万件。コンフィッカーは特殊なアルゴリズムで常にドメイン名を作成し、そのドメイン名にランダムで接続することがわかる。攻撃者は事前にランダムドメインを登録し、不正コードを感染PCに次々ロードしたりするために悪用する。

1月21日　 コンフィッカーの流行が続く。英国軍にも被害が。

1月23日　トロイの木馬に感染したAppleのiWork 09がBitTorrentで流通。1月初旬より、約2万ものユーザーがこれをダウンロード。

1月25日　データ流出被害をリクルート系ポータルのMonster.comが発表。データベースへの不正アクセスで、アクセスデータ、名前、電話番号、メールアドレスなどのデータが盗みだされる。

Feb 2009

2月1日　Windows7ベータ版の脆弱性を悪用し、簡易スクリプトでUACが動作不能に。攻撃者はユーザーが気付かないように不正ソフトを忍び込ませることが可能。

2月2日　 Hamburger Abendblatt オンライン版が攻撃の対象に。訪問者はサイトに仕掛けられた不正プログラムにより感染。

2月4日. ドイツ人気ＴＶ局、RTL が運営するSNS（werkenntwen.de）の偽ログインサイトでユーザー多数がアクセスデータを詐取される

2月8日　DDoS攻撃で、セキュリティ検証の Metasploit, Milw0rm, Packetstormなどのサイトが一時ダウン。

2月10日　2日後に再びMetasploitへDDoS攻撃が確認される。攻撃者は何度も攻撃手法を変え攻撃。

2月11日　Typo 3のセキュリティホールを悪用した攻撃で、サイトが改ざん。被害者：ドイツブンデスリーガ１部のFC Schalke 04、ドイツ内相Wolfgang Schaeubleのサイトなど。

2月12日　マイクロソフトがコンフィッカーの作者の逮捕および訴追につながる情報に対し、25万ドルの

懸賞金を設定。同時に感染を抑止するため、ICANNやDNSサーバーの運営者との密な協業を発表。

2月14日　ドイツ連邦国防軍の数百台のコンピュータがコンフィッカーni感染。

2月17日　チェコのISPがルーターの設定ミスにより、地域的にデータ通信が不安定に。

2月23日 マルウェア研究者による分析の結果、コンフィッカー Worm B および B++はそのモジュール構成からコンフィッカー Aよりフレキシブルな振る舞いが可能とわかる。

2月25日 Flashバナーから、オンラインマガジン eWeek や Ziff-Davis-Netzwerkes オンライン版などのサイト上で、被害者のPCに偽ウイルス対策ソフトをインストールする不正PDFファイルを配布。

Mar 2009

3月1日　マルウェア研究者により、コンフィッカーがコントロールサーバーのドメイン名を作成するために使用するアルゴリズムを解読。コンフィッカーは既に利用されている名前も生成。3月に正規のドメイン jogli.com (音楽検索)、wnsux.com (サウスウェスト航空)、qhflh.com (中国の女性用ネットワーク)、praat.org (Audio分析)にて、コンフィッカー感染PCからの接続絡みで障害が発生した模様。

3月4日　ドイツ Baden Württemberg州の州刑事局は、トロイの木馬、データ詐取方法やクレジットカード偽造方法に関する情報を販売していた、不法取引プラットフォームの codesoft.cc の営業を停止。

3月9日　コンフィッカーが新しいアルゴリズムを利用。1日あたりのドメイン数は、今までの250から一気に5万へ。さらに、ワームの分析ツール関連の特定ストリングに含まれるプロセスを感染PCで終了することにより、被害拡大の抑制に対しても対策が講じられる。

3月12日　英国のBBCが、22,000台もの規模を持つボットネットを入手。BBCが非難の対象に。BBCは、この活動は公共の利益で違法性なない、と主張。ただし、このボットネット入手費用については、BBCは未回答。

3月17日　正しいドメインと見せかけた、DHL-Packstation.info というドメインを使い、Packstation ユーザーのアクセスデータを詐取。Packstationとは、DHLがドイツで提供する、無人の小包受取/発送サービス。

3月23日 Typ Netcomm NB5のDSLルーターは、老朽化したファームウェアのため、ウェブインターフェースとSSHアクセスで不正操作が可能に。また、8〜10万ものルーターが感染したPsybotというボットネットを確認。

3月30日　専門家たちは、コンフィッカーは自身により作成された無数のドメインのアップデートを開始するとコメント。

3月31日 この便乗犯の犯罪手法は、PCの感染の偽情報でユーザーに警告を発し、クレジットカード情報を盗みだすタイプの偽ウイルス対策ソフトのインストール。メディアでのコンフィッカーに対する関心が高まり、コンフィッカー駆除ツールというおとりを使う便乗犯も登場。Googleの検索でも上位にランクインしていた。

Apr 2009

4月1日　コンフィッカーのアップデートはなし。この段階では、準備が整っていなかったと推測。

4月9日　大方の予想とは異なり、コンフィッカーのアップデートは、あるアルゴリズムで作成されたドメイン名経由でロードされなかったが、その代わりコンフィッカーはP2Pのメカニズムを使って、別の感染システムに接触。新種は、駆除ツールを提供するウイルス対策ソフトベンダーのウェブサイトへのアクセスをブロック。

4月12日　コンフィッカーは、ウクライナのサーバーからスケアウェアの「SpywareProtect2009」をロード。このスケアウェアは、偽のウイルス検出メッセージを出し、ユーザーに49.95ドルの支払いを求める。

4月18日　セキュリティ専門家は、初のアップルのコンピュータボットネットを発見。感染経路はビットトレントで流通する、トロイに感染したiWork 09やAdobe Photoshop CS4と推測。

4月22日　約2百万台ものゾンビPCを従えた、世界最大規模のボットネットが発見される。このボットネット運営者は、ウクライナで Command & Control Serverを運営する、6名からなるグループ。

4月23日　ユーザーをPCにログインできないようにし、それを解除するために支払いを要求するトロイの木馬がロシアで見つかる。被害にあったユーザーは、ある高額な有料の電話番号にSMSを送信すると、解除コードを入手できる仕組み。

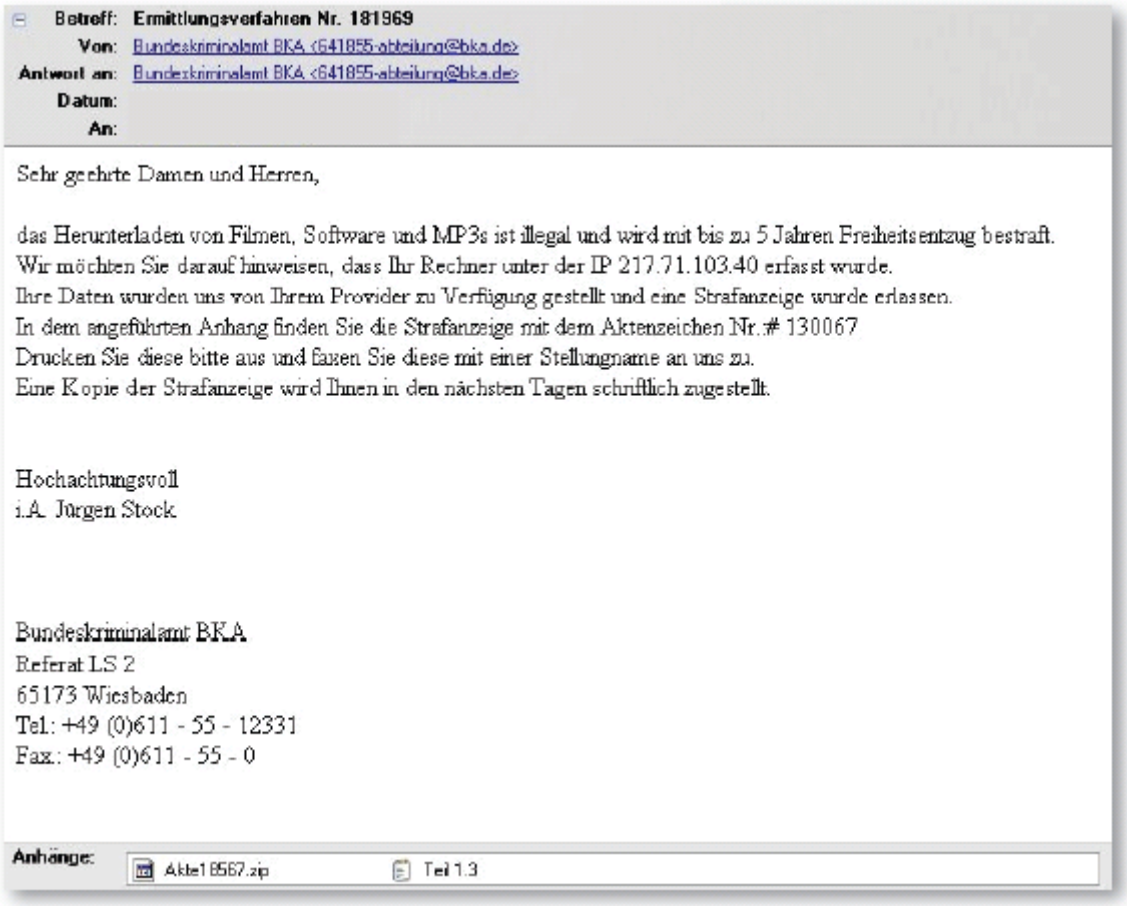
May 2009

5月7日　テレコミュニケーション企業BTの研究によると、取引される使用済みハードディスクの中には、多くの場合、データが完全に消去されていない模様。同研究では、約300個のハードディスクを入手し、検証。その中には、米軍のロケット防衛システムやLockheed Martin社の設計図などが見つかる。

5月8日　米連邦航空局、FAAは、ここ数年何度もハッカーが航空機監視システム内に侵入した、と発表。従業員5万人の個人情報、重要なサーバーの電源を切られる被害など。

5月9日トロイの木馬が仕込まれた、Windows7のRC版と謳った偽インストールパックが見つかる。セットアップ実行中に感染する。

5月24日　ドイツ連邦検事局は、当局の名前を騙った偽メールが確認されたことを発表し、警告した。そのメールでは、音楽・動画・ソフトなどの違法ダウンロードによる罰金支払いがメール受信者に要求されている。


Betreff: Ermittlungsverfahren Nr. 181969
Von: Bundeskriminalamt BKA <641855-abteilung@bka.de>
Antwort an: Bundeskriminalamt BKA <641855-abteilung@bka.de>
Datum:
An:

Sehr geehrte Damen und Herren,

das Herunterladen von Filmen, Software und MP3s ist illegal und wird mit bis zu 5 Jahren Freiheitsentzug bestraft.
Wir möchten Sie darauf hinweisen, dass Ihr Rechner unter der IP 217.71.103.40 erfasst wurde.
Ihre Daten wurden uns von Ihrem Provider zu Verfügung gestellt und eine Strafanzeige wurde erlassen.
In dem angeführten Anhang finden Sie die Strafanzeige mit dem Aktenzeichen Nr.:# 130067
Drucken Sie diese bitte aus und faxen Sie diese mit einer Stellungname an uns zu.
Eine Kopie der Strafanzeige wird Ihnen in den nächsten Tagen schriftlich zugestellt.

Hochachtungsvoll
i.A. Jürgen Stock

Bundeskriminalamt BKA
Referat LS 2
65173 Wiesbaden
Tel.: +49 (0)611 - 55 - 12331
Fax.: +49 (0)611 - 55 - 0

Anhänge: Akte18567.zip Teil 1.3

5月30日　新聞「InformationWeek」の記事によると、トルコの活動家が数度に渡り米軍のウェブサーバーを乗っ取り、被害にあった当該サイトにアクセスすると、同活動家の政治声明関連のサイトへリダイレクトされる。

Jun 2009

6月3日　数万ものウェブサイトがハッキングの被害にあう。改ざんされたウェブサイトの訪問者は、Internet Explorer、Firefox、QuickTime用のエクスプロイットが配布される、ウクライナのサーバーに転送される。

6月5日　カリフォルニアのISPであるPricewert LLC (3FNまたはAPS Telecom)は、米連邦取引委員会の

圧力により、ネットワークから排除。同ISPは4,500ものスパイウェアのCommand & Control Serverを制御しながら、サイバー犯罪用人員を積極的にリクルーティングし、違法コンテンツの追跡を阻害、かく乱。2008年11月のMcColo営業停止と異なり、スパムやマルウェアの送信の観点からは、効果は薄いと考えられる。

6月9日　イギリスのウェブホスト、Vaservのシステムに何者かが侵入。同社がホスティングする10万ものウェブサイトのデータが改ざんおよび削除。

6月17日　URL短縮サービス提供のcli.gsの約220万ものURLが改ざん、別のURLへ転送。

6月24日　ペンタゴンは、米国防総省の指示により、サイバー戦争用特殊部隊を編成。

6月26日　ハノーバー検察は、多くのPCユーザーを騙したとして、mega-downloads.net を捜索。消費者センターは、毎月約2万人のユーザーがサブスクリプション詐欺の被害にあっていたと推定。