



G DATA  
Whitepaper 2009  
On Conficker

ラルフ・ベントムラー (G DATA セキュリティラボ所長)

Go safe. Go safer. G DATA.

## コンフィッカーについて

G DATA Software 株式会社（代表取締役：Jag 山本、本社：東京都千代田区）は、ここ12か月において、最も巧妙で危険度が高く、かつ、世界中で注目を集めているマルウェア（ワーム）の一つである「コンフィッカー（Conficker）」について、以下、白書の形でレポートいたします。

他国と比べると日本ではまだ著しく目立つ動きにはなっていないものの、2009年1月22日には警視庁のオンラインシステムの端末に使用されているPCから発見されるなど、今後、更なる増加の恐れがありますので、十分な注意が必要です。

### コンフィッカーの現状

コンフィッカーとは、ワームの一種で、昨年10月にMicrosoftがパッチ提供をしたWindowsのRPC（＝リモート プロシージャ コール）サービスの脆弱性「MS08-067」を悪用するマルウェアです。別名として、ダウンロード（Downad）、ダウンロードアップ（Downadup）、キド（Kido）などがあります。

Microsoftがウイルス製造者の逮捕につながる情報提供者に懸賞金を出すという発表をしたことにより、一般的によく知られるウイルスとなりました。

類似したものに、2007年から2008年にかけて爆発的に拡散した「オートラン」と呼ばれるマルウェアがあります。今年に入ると、オートランよりもコンフィッカーが増加しています。

コンフィッカーはまず、細工されたクエリー（処理要求）をコンピュータに送信し、コンピュータに脆弱性があれば、不正コードをコンピュータに送りつけます。感染したコンピュータにはHTTPサーバがインストールされ、細工されたクエリー、場合によっては感染ファイルを、他のコンピュータに送ります。

偽メッセージで商品を買わせるようなスケアウェアなどもインストールされる場合があります。

コンフィッカーは、単純なパスワードでしか保護されていないローカルネットワーク内で拡散し、USBメモリ、外付けハードディスク、デジタルカメラなどのオートスタート機能を悪用します。

**甘いパスワードとオートスタート機能。この2つの特徴を活用してコンフィッカーは巧みに万延しているのです。**

EU諸国ではすでに、ドイツのケルンテルン州における3000台の感染を筆頭に、オーストリアやイギリスの病院、フランス海軍のコンピュータなど、数多くの場所で被害が起っています。

また、ボットネットサーバとの接続が途切れないよう、コンフィッカーは日付を使って、「ejzrcqw.net」「doxkknuq.org」「ytfvksowgul.org」といったようなドメイン名を日々250ほど作っています。

最近のこの感染の広がりを見ると、コンフィッカーの作者は、新たなボットネットの基礎を作りあげたと考えられます。ボットネットを操作する側にとって大量の感染したコンピュータの存在とは、攻撃準備が整った状態を意味するのです。

### 感染の規模

感染の規模については、現在、少なく見積もっても数十万台、多ければ数千万台のコンピュータが感染していると予想されます。しかし、これ以上の正確な数字の把握は困難です。なぜならば、多くの感染したコンピュータがコントロールサーバと接続され数倍に数えられていたり、会社のネットワーク内の複数台のコンピュータが1台と計算されることもあるからです。

正確な数字は出ないとしても、今回の拡散の仕方は、メールやインターネットを通じた感染だけではなく、USBメモリなどを介していることもあり、潜在的な感染数はもっと多い可能性もあります。

これは、USBメモリが、ネット犯罪者たちにとって、拡散のための有用な道具とみなされていることを意味しています。

### 対策方法

2008年10月に、Microsoftの発表によって、コンフィッカーがOS内の脆弱性を悪用するということが判明しました。それ以来Microsoftは、関連のアップデートを提供していますが、多くのネットワーク管理者は適切な対応をとることができず感染を許しています。

また、もう1つの重要な点は、ネットワークやアカウント用パスワードに「12345」や「admin」「zzzzz」といったような簡単なパスワードを設定している場合が、意外と多いということです。

更に、多くの企業ではUSBメモリの利用などに関する規則がそれほど明確にとり決めていない、というのも拡散を助長させている理由の一つです。

オートスタートのメカニズムは、ほとんどのコンピュータにおいて有効に働き、コンフィッカーやUSBウイルスをはじめとした不正プログラムの拡散の原因となっています。メールやインターネットに関するセキュリティは一般的には強化されているので、使い勝手がよいためにデータの受け渡して利用されているUSBメモリを感染ルートに組み込んだと言えるでしょう。

また、OpenDNSは興味深いサービスを提供しています。OpenDNSは、ネットワーク内のコンフィッカーに感染したコンピュータを認識し、日々新しく発生するボットネットドメインへのアクセスをブロックするサービスを提供しています。このサービスによって、ゾンビPCは感染してしまったゾンビPCであっても、仕掛け人からの指示がなければ休止状態にすることができます。

#### コンフィッカーの検知方法

アンチウイルス製品のワクチンが最新の状態に更新されていれば、コンフィッカーは検出することが可能です。しかし、システム内にバックドアが潜んでいたり脆弱性が閉じられていなければ感染する危険があります。

コンフィッカーは「jwgkvsq.vmx」や「vfgthjki.rst」やといったような、ファイル名にランダムな文字の組み合わせが使われるので、検出は困難です。

レジストリが変更されるのは、以下の箇所です。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\ [Random name for the service]
Image Path = „%System Root%\system32\svchost.exe -k netsvcs“
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\ [Random name for the service] \Parameters
ServiceDll = „[Path and filename of the malware]“
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\SvcHost
```

下記のようなセキュリティサービスが機能しないことで、感染に気づくことがあります。

- Windows Security Center
- Windows AutoUpdate
- Windows Defender
- Error Reporting Service

「ウイルス」や「スパイウェア」といった文字列や「マイクロソフト」や「G DATA」をはじめとしたアンチウイルス製品の名前など、以下の文字列のあるウェブサイトへのアクセスができなくなります。

「virus」「spyware」「malware」「rootkit」「defender」「microsoft」「symantec」「norton」「mcafee」「trendmicro」「sophos」「panda」「etrust」「networkassociates」「computerassociates」「f-secure」「kaspersky」「jotti」「f-prot」「nod32」「eset」「grisoft」「drweb」「centralcommand」「ahnlab」「esafe」「avast」「avira」「quickheal」「comodo」「clamav」「ewido」「fortinet」「gdata」「hacksoft」

「hauri」「ikarus」「k7computing」「norman」「pctools」「prevx」「rising」「securecomputing」  
「sunbelt」「emsisoft」「arcabit」「cpsecure」「spamhaus」「castlecop」「threatexpert」  
「wilderssecurity」「windowsupdate」

ネットワーク管理者は、ポート番号 455 で増えるトラフィックで、感染コンピュータを見つけることができます。感染後は、コンフィッカーは感染したコンピュータの IP アドレスを以下のサイトの一つから呼び出し、調べます。

- <http://checkip.dyndns.org>
- <http://getmyip.co.uk>
- <http://www.getmyip.org>

アップデートのアドレスは、日付を使うことによって、以下のドメインから計算されます。

- ask.com
- baidu.com
- google.com
- msn.com
- www.w3.org
- yahoo.com

このドメインにアクセスするコンピュータは、感染の危険性があります。

コンフィッカーの除去方法

一旦コンフィッカーに感染したシステムをクリーンにする方法については、以下の Microsoft の URL を参照してください。

<http://www.microsoft.com/japan/protect/computer/viruses/worms/conficker.msp>

コンフィッカーは複雑な構成で、システム内の複数箇所を同時攻撃し、削除作業も手間がかかります。そこで、アンチウイルス製品をインストールしてスキャンをかけるか、もしくは、最新バージョンの MSRT (悪性ソフトウェア削除ツール) の利用をお勧めします。

<http://www.microsoft.com/japan/security/malwareremove/default.msp>

まとめ～コンフィッカーに感染しないために

- 1) Windows のアップデートを最新のものにする
- 2) ユーザーアカウントと共有ファイルのパスワードを複雑なものに変更する
- 3) G DATA 製品をはじめとしたウイルス対策ソフトを使用する  
(ワクチンを最新の状態にし、ハードディスク全体をウイルススキャンする)
- 4) USB メモリを使用する前にウイルススキャンをかける

G DATA Malware Whitepaper: Questions and Answers to Conficker  
Copyright © 2009 G DATA Software AG