

## 技術解説

# BotNetwork の学内における現状

総合情報基盤センター

助手 沖野 浩二

## 1. はじめに

今年度の学内ネットワークにおいての特質すべき事例として挙げられるのは、Virus 対策ソフトでは、検出も削除できない凶悪な Virus ソフトが複数検出されたということである。

今までの、Virus の場合には、パターンファイルを最新にすることなどで検出・削除が可能であった。しかし、今年度発見された Virus ソフトは、root kit と呼ばれる特殊ソフトと組み合わせることによって、Virus 対策ソフトの検出を回避し、Virus のような悪意あるソフトウェアの存在自体を隠蔽しますものである。

これらの Virus Soft を解析した所、WORM\_NUWAR(ヌーウォー)と呼ばれる種類だと確認された。また、この Virus を検出した PC を精査した所、他にも複数の Virus が検出された。

これらの Virus の蔓延には、BotNetwork と呼ばれる Virus の感染した PC をコントロールするための仕組みが、組織を含めて整備されて現状がある。

本解説では、学内における BotNetwork の蔓延現状と、今後の対策について説明する。

## 2. Virus 概論

### 2.1 Virus とは

一般に Virus とは、下記の要件をみたすものである。

- ・コンピュータに対して悪意ある動作（被害を発生する動作）を行うプログラム

- ・ユーザにインストールの確認をしないこれらの定義は昔からあるもので、フロッピーディスクなどによって Virus 付きのプログラムが伝播され、そのプログラムを実行することによって Virus が感染した時代のものである。現在では、ネットワークに接続された PC が多く、その感染経路も多様であり、当てはまらない Virus も多い。

### 2.2 マルウェアとは

現在は、これらの要件を満たさないソフトウェアも多いため、マルウェア（Malicious Software）と呼ばれる悪意あるソフトウェアという概念が示されている。マルウェアでは、

Virus:上記のプログラム

Worm : 自己増殖、拡散性を有するプログラム

Trojan(トロイ) : 利用者に知られずに別の機能が動いているもの

Spyware:PC 内の情報を外部に提供

Keylogger:入力内容を記録

Bot:外部からコントロール可能になっている PC

Browser Hijacker:ブラウザを乗っ取り、アダルトサイト等に強制的に誘導するソフトウェア

と呼ばれるソフトウェア等を示している。また、上記の悪意あるプログラム加えて、

単体では問題がないが

Root kit:OS 等を改変してソフトウェアの存在等を隠す機能を有するソフトウェア Downloader : Windows Update の様に、外部からソフトウェアを Download し、Update を行うソフトウェアと呼ばれる機能を持ったソフトウェアがマルウェアと組み合わせて利用されている。

### 2.3 マルウェアの現状

旧来の Virus ソフトでは、それぞれの機能しか装備されていない单機能型の Virus が主流であったが、現在には、複数の機能を持つた Virus や单機能の Virus を複数同時に感染してそれぞれの機能を補うものが主流となってきている。学内においても Virus に感染している PC からは同時に複数の Virus が検出されている。

また、ユーザのセキュリティ意識の向上やセキュリティ対策ソフトの普及により、マルウェアが導入されづらい状況から、長い契約書を示してユーザの誤認を狙うソフトウェアやソフトウェアの目的を偽装した Spyware 等も広く蔓延している。

具体的には、Virus 対策ソフトを模した WinFixer2005,WinAntiVirusPro が有名であるが、これらのソフトウェアが学内で導入されていた事例もある。

### 2.4 マルウェアの目的変化

現在では、さらに進化したマルウェアが発見されている。進化のキーワードとしては、2つあり、ひとつは、スピア型攻撃と呼ばれる進化であり、もうひとつは、BotNetwork と呼ばれるものである。

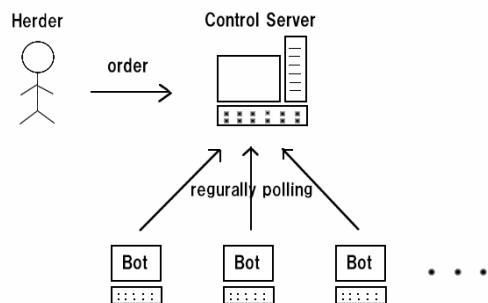
#### ・スピア型攻撃とは

スピア型攻撃とは、ある特定の組織や集団を狙ったものである。スピアとは槍(spear)を示したものであり、槍のように鋭く一点だけに攻撃が行われる点から名付けられた。有名なものとしては、2006年8月16日に Justsystem 社製ワープロソフト一太郎の脆弱性を利用した Virus メールが中央省庁に送付された事件などがあり、明らかに特定の集団とその特性を利用したものである。スピア型攻撃の増加理由については、攻撃相手の情報を元に攻撃を行うことでの成功率の向上、配布範囲の限定による Virus 対策ソフトウェアによる検出の回避、取得情報の価値向上があげられる。

#### ・BotNetwork とは

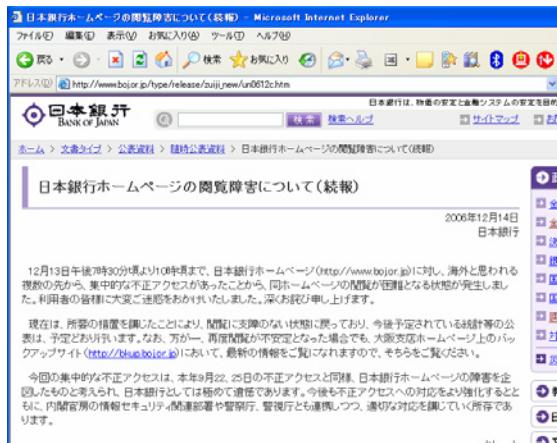
近年、Virus の目的が、感染を広げることよりも、感染したパソコンを利用するのを主目的としたマルウェアが多く発見されている。これが Bot(ボット)と呼ばれものである。Bot に感染されたパソコンは、外部からコントロールが可能になっている。このため、Bot に感染した場合には、Virus に感染した被害者になるだけでなく、他の PC を攻撃する加害者ともなる。Bot という言葉は、外部からの命令を受けて行動を行うことから、Robot が語源である。この Bot は、定期的に指定されてサイトに接続し、攻撃者からの命令を待つ。一般に複数の bot が特定のサーバに接続しており、一回の命令で、それらすべてに同じ動作をさせることができる。この bot を操る攻撃者を herder(ハーダー：羊飼い)とよび、サイトに接続している bot の集合を BotNetwork と呼ぶ。

BotNetwork を構築することで、一台あたりの能力が低くても、多数の台数からの強調した攻撃が可能になり、大きな攻撃能力を持つことが可能になる。



## 2.5 BotNetwork の利用対象

実際に BotNetwork を利用した事例としては、フィッシングメール等の SPAM メールの配信や特定サイトへの攻撃等に利用されている。具体例としては、社会的に大きなものとしては、国内においては、2006 年 12 月に日本銀行の Web ページへのアクセス不能攻撃に利用されている。



また、学内においても Bot に感染したマシンから多量の Spam メールが発信され、学外の機関からのクレームを受けている。

## 2.6 学内においての現状

学内においても、これら Bot に感染してい

る PC が多数発見されている。特に感染している PC の特徴としては、Virus 対策ソフトの未導入および Windows Update 等の日常的なセキュリティ対策がなされていない点が上げられる。また、Mail や HTTP などの通信に関しては総合情報基盤センターのセキュリティ機器により Virus Check をしているので、一般的な経路による感染確率はかなり低いといえる。これらのことにより感染経路として想定されるのは、学内における感染であり、原因としては、

- ・学外で感染したマシンの持ち込みの持込

- ・他の Bot に感染しているマシンからの感染

- ・Virus 感染しているソフトウェアの実行

があげられる。Bot に感染した場合には、ある種、特殊な通信パターンが発生する。これらの通信パターンを利用し、学内の通信状態から類推すると、学内には少なくとも 10 台以上の Bot に感染したマシンがあると思われる。センターもこれらの通信を発見するたびに利用者への連絡を行っているが、Bot の数はなかなか減らないのが現状である。

## 3. 問題点の整理

### 3.1 Bot に感染することの問題

Bot に感染することによる問題の本質は、攻撃者が Bot に感染している PC を自由に利用できるということである。自由に利用できるということは、PC の操作だけでなく、PC 内部に格納された情報も含む。実際に Bot を利用した事案では、

- ・ 内部情報の漏洩
  - 研究データ
  - 成績データ
  - メールアドレス
  - Web 等のアクセスデータ
  - Keylogger
- ・ 外部への攻撃
  - SPAM メールの発送
  - Worm の発生元
  - フィッシングサイトの構築

が発生している。

現在の学内での利用状況を考えた場合には、PC からの情報漏洩は、本人のアクセス履歴や ID, Password、場合によっては金融機関等の情報までも流出するだけでなく、メールの交換をしている相手の情報や成績などの、その PC で作成した情報はもちろんのこと、講座等の共有している FileServer の情報までも流出している可能性があります。

これらの事案で、情報の漏洩が発生した場合には、裁判等で情報の管理義務が果たしていないと認定されれば、個人および法人に損害賠償が発生します。さらに共同研究等で別の契約を結んでいた場合等には、漏洩していないことまでを証明しなければならない場合があります。

また、SPAM メールやフィッシングに利用された場合や、自分の金融口座が利用された場合には、犯罪に加担することになりますので、警察等の司法機関からの事情聴取等が考えられます。

実際に Spam メールの情報収集や配達には、BotNetwork が大いに利用されています。学内に一台でも、Bot があれば、そのマシンから情報が漏洩し、Spam メールが

来る可能性が拡大すると考えられます。Bot に感染してからの対応では、遅いというのが実際なのです。

### 3.2 Bot に感染しないためには

Bot に感染しないためには、いくつかの基本的なことを守ることが重要です。

- ・ Windows Update 等のセキュリティ Paeth の適用する
- ・ Virus 対策ソフトの導入する
- ・ 添付ファイルは中身を確認する
- ・ 正規なソフトウェアを利用する
  - ・ ソフトウェアは正規版 CDROM から導入する
  - ・ Copy されたソフトは利用しない
  - ・ Internet からのソフトウェア DownLoad には注意する

実際には、これらの基本的なことを守っていても感染する可能性を 0 にすることはできないが、これらのこと気につけることで感染の可能性はかなり低くすることになる。

### 3.4 センターの対応

総合情報基盤センターでは、Bot の蔓延を防ぐためにいくつかの手段を用いている。

- ・ センター広報等でのアナウンス
- ・ 講演会の開催
- ・ Virus 対策ソフトの提供
- ・ FireWall の監視強化

これらの対策を行っても最終的には、利用者の心がけがなければ、Bot はなくなりません。利用者の方々は、必ず前節のことを行ってください。これはあなたが被害者にならないためには、必ず必要なことです。