# C8 インターネット定点観測に基づくマルウェア平均感染期間の推定

松尾峻治

## 1. はじめに

現在の多くのセキュリティソフトでは定義ファイルの更新によって、多種にわたるマルウェアに適応してきた。この定義ファイルの更新の頻度はウィルスの発生率や感染潜伏期間に大きく依存する。[1]によると、2004 年のウィルスの感染期間は 32 日と報告されている。本研究では、2004 年から 4 年間に渡るマルウェアの感染期間を求め、その推移を求めることを目的とする。

## 2. 感染期間の算出方法

### 2.1 インターネット定点観測

インターネット上のパケットを観測する方法に定点観測システムがある。本研究では、JPCERT/CC が運用している定点観測システム ISDAS[2]のセンサで観測されたデータを元に解析した。

### 2.2 適応閾値の算出方法

パケットの到着間隔は不正ホスト毎に異なり、感染・駆除のサイクルを決める閾値Tは一意に決まらない。その到着間隔はポアソン分布に従うことを仮定し、期間 $T$ でパケットが届かない確率を同定する。$\lambda$ はパケットの到着率とし、$\lambda = c/d_0$ と定義する。$c$ は各送信元アドレスの総パケット数とし、$d_0$ は最初と最後のパケットの観測時間差である。この時パケットが到着しない確率が 1%となる閾値は $T = -ln(0.01)/\lambda$ で求められる。

### 2.3 解析システム

ISDASより入手した不正IPアドレス、日時、センサ番号、送信元 port、宛先 port から成るテキストを入力データとする。不正ホストのアドレス毎に日時順にソートし、パケットの到着間隔を適応閾値 $T$、感染期間 $d$ を求めるプログラムを Java を用いて開発した。補助出力として、ユニークセンサ数がある。

## 3. 調査結果

2004 年 9 月 1 日から 2008 年 4 月 30 日に独立したセンサ 50 台で観測されたデータを半年毎に分割($P_1$～$P_7$)し、各々に2.2の方式を適用して、マルウェアの感染期間を同定した。この結果を表 1 に示す。ここで $U_i$ を期間 $P_i$ユニークホスト数、$d_i$ を平均感染期間,$\sigma_i$ を平均感染期間の標準偏差とする。また、感染機関の推移を図1に示す。

表 1:各観測期間の平均感染期間

| 観測期間 | | $U_i$[address] | $d_i$[day] | $\sigma_i$ |
|---|---|---|---|---|
| $P_1$ | 2004/9 | 1535990 | 11.52 | 25.37 |
| $P_2$ | 2005/3 | 1503238 | 11.34 | 26.14 |
| $P_3$ | 2005/9 | 950645 | 10.38 | 25.19 |
| $P_4$ | 2006/3 | 733038 | 8.20 | 21.54 |
| $P_5$ | 2006/9 | 790350 | 6.03 | 18.13 |
| $P_6$ | 2007/3 | 727947 | 5.97 | 17.96 |
| $P_7$ | 2007/9 | 552289 | 6.23 | 18.11 |

感染期間 $d_i$ をグラフに直すと図 1 のようになる。

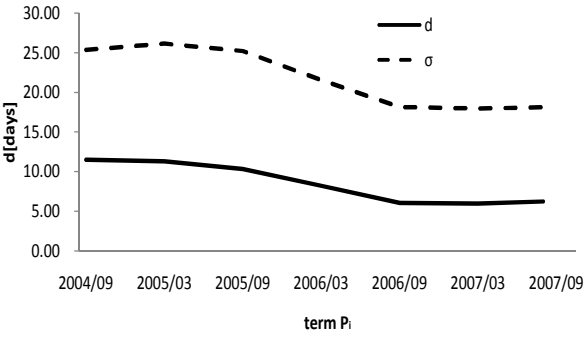


図 1:平均感染期間の推移介

図 1 から、平均感染期間が緩やかに減少しているのが見える。3 年半で約 5.29 日、年間約 1.51 日減少している。また、標準偏差は年間で 2.07 減少している。

## 4. おわりに

感染期間は年間で約 1.51 日減少していることがわかった。セキュリティ対策が進んできている理由が考えられる。今後、がどのように変化するか興味が尽きない。

## 参考文献

[1] 小堀，他，ISDAS 分散観測:ウィルスの平均寿命はいくらか？，情報処理学会，CSS2006，pp.519-524，2006.

[2] 戸田，他，ISDAS: Internet Scan Data Acquisition System，情報処理学会，CSS 2004， pp.199-204 ,2004.