自己複製挙動に着目したワーム検知手法の提案

神谷 早紀 *，早川　顕太，鈴木　秀和，旭　健作，渡邊　晃 (名城大学)

Proposal of Worm Detection Method based on Self-Copy Behavior

Saki Kamiya, Kenta Hayakawa, Hidekazu Suzuki, Kensaku Asahi, Akira Watanabe(Meijo University)

1　はじめに

任意のターゲットに攻撃を行うボットと呼ばれるマルウェアが横行している．ボットに感染した PC 郡はボットネットを構成しており，命令に従って一斉に攻撃を行う．ボットはその性質上，ワームと同様に自分自身を複製して感染を拡大する．さらに，ボットを作成するキットが出回っており，日々亜種ボットが作成され，その被害は拡大している．

一般的にマルウェア検出は，マルウェア固有のパターンを記録した定義ファイルを用いたパターンマッチングで行われている．しかし，この手法では既知マルウェアしか検出出来ない．未知マルウェアを検出可能な手法としてビヘイビア法がある．リアルタイムにプロセスを監視し，マルウェアらしい挙動を行った時に，マルウェアとして検出する手法である．

本稿では，ビヘイビア法を用いて，ワーム特有の自己複製挙動に着目したワーム検出手法を提案する．

2　ビヘイビア法によるワーム検出の既存研究

ビヘイビア法を用いてワーム検出する既存研究として以下のようなものがある [1][2]．文献 [1] は，ワームが感染時に複製を作成するにあたって，自分自身のファイルを全て読み込むという挙動を検出する手法である．しかし，自己ファイル READ という挙動は正規インストーラでも起こる為，誤検知が発生する．文献 [2] は，ボット (ワーム) の侵入挙動の反復性を利用し検出する手法である．侵入挙動とは，ボットが未感染 PC 環境では自分自身を複製 (実行ファイル生成) して，自動起動されるようにレジストリなどに生成ファイルを登録するという挙動である．この挙動は正規インストーラにも見られるが，生成されたアプリケーションはインストール機能を持たない．侵入挙動を検知した時，未感染 PC 環境に復元して生成ファイルを実行する．再び侵入挙動が観測した時に検出することで正規プログラムと区別する．しかし，リムーバブルディスクへの自己複製などの自身を拡散する挙動は検出できない．

3　提案方式

一般的にワームは，未感染の PC に持ち込まれた時，PC 内に常駐するため，自身の複製を作成し自動実行リストへ登録する．また，感染拡大のため，リムーバブルディスクや共有フォルダに自分の複製を作成する．従って，ワームの特徴として実行中のワームのプロセスが自己複製を行うという挙動がある．

ワームの中には，ポリモーフィック技術を用いて，複製の度に暗号化の鍵を変えて暗号化し，自身を改変するタイプがある．しかし，実行ファイルのヘッダは変化すると実行不可能となるためヘッダは変化しないという特徴がある．よってヘッダを比較することにより自己複製挙動を検出できる．

Fig.1 に提案方式の概要を示す．提案方式では，実行中の全プロセスの処理を監視する．実行ファイル A のプロセスが実行ファイル B を生成した時に，実行ファイル A と B のヘッダを比較することにより自己複製挙動であるかどうかを判別する．

一部の正規アンインストーラでは，一時フォルダに自己複製することがある．しかし，一時フォルダ内のファイルは Windows 標準のディスククリーンアップ使用時などに削除されるため，マルウェアが自身の複製を一時フォルダに作成することは稀であると考えられる．提案方式では，一時フォルダへの自己複製を例外的に許可する事により，正規プログラムとワームを区別する．

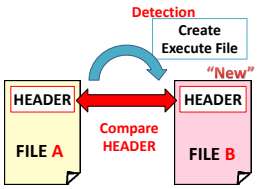


Fig. 1　Overview of the Proposed Method

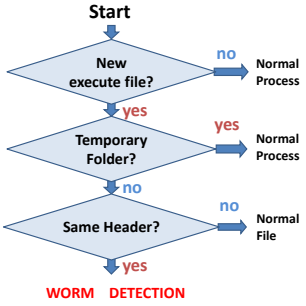


Fig. 2　Detection Flow of the Proposed Method

以上の条件を踏まえた提案方式の手順を Fig.2 に示す．全プロセスを監視し，実行ファイル作成を検出する．その実行ファイルが作成されたフォルダが，一時フォルダかどうか確認する．一時フォルダでなければ，実行ファイルを作成したプログラムと，作成された実行ファイルのヘッダを比較し，一致した場合にワームとして検出する．

4　検知実験

提案方式により実際にワームの検出が可能か検証を行った．プロセスの処理を監視できる ProcessMonitor と，2 つのファイルを比較する CompFile を用いて実験を行った．実験環境は，仮想マシン VMware 上の WindowsXP SP3 で，ネットワーク環境はホストオンリーとした．使用した検体は，マルウェア配布サイト Offensive Computing[3] から独自に入手したマルウェアの内，Symantec 社の検出種別がワームである 18 体である．

実験の結果，18 体中 14 体の検体を検出できた．従って自己複製をワームの特有の挙動として検出する提案方式の有用性が示された．未検出の 4 体はそもそも実行ファイルを作成していなかったため，検出できなかった．この原因は，ワームではなかった，もしくはワームが仮想環境であることを検知し挙動が変化したためと推測される．

5　まとめ

本稿は，ワームが自己複製をした時にファイルのヘッダ部分は変更できない点に注目し，ワームを検出する方法を検討した．監視ツールを用いた基礎実験から提案方式の有用性が確認できた．

文　献

[1] 松本. 他：自己ファイル READ の検出による未知ワームの方式, 情報処理学会論文誌, Vol.48,No.9, pp.3174–3182,Sep2007.

[2] 酒井. 他：侵入挙動の反復性を用いたボット検知方式, 情報処理学会論文誌,Vol.51,No.9,pp.1591-1599,Sep2010.

[3] Offensive Computing,URL:http://www.offensivecomputing.net.

自己複製挙動に着目したワーム検知手法の提案

名城大学　理工学部
神谷早紀，早川顕太，鈴木秀和，旭健作，渡邊晃

Watanabe Lab.

研究背景

マルウェアによる攻撃が巧妙化し被害が深刻化

- ボット
  - 攻撃者の命令に従って，感染PC上で活動する
  - ボット作成キットにより日々大量の亜種ボットが増えている
  - ボットに感染したコンピュータ群によりボットネットを構成し，一斉に攻撃などを行う

  →ワームと同様の性質

- ワーム
  - 他のPCへ侵入し，自身を拡散する

ワームを検出する手法を提案する

従来のマルウェア検出手法

- パターンマッチング法
  - 個々のマルウェアそれぞれに特徴的なシグネチャを定義し，検査対象と比較し一致するものを検出
    - **利点：既知マルウェアは確実に検出できる**
    - **欠点：未知のマルウェアは検出不可**

- ビヘイビア法
  - 実行されているプログラムの動作を監視し，事前に定義したマルウェアらしい特有の挙動を検出
    - **利点：未知マルウェア検出可能**
    - **欠点：誤検知が起こりうる**
      （真にマルウェアらしい挙動の定義が重要）

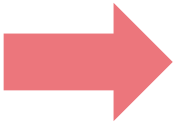
未知のワームも検出可能なビヘイビア法に着目

ビヘイビア法に関する既存研究

- 自己ファイルREADの検出による未知ワームの検知方式
  - **検出方法：「自身のファイルをREADする」挙動を検出**
    - ワームは拡散の性質上自身を複製するために自己ファイルREADする
  - **課題：誤検知が起こる**
    - 自己ファイルREADは正規プログラムでも起こるため
- 侵入挙動の反復性を用いたボット検知方式
  - **検出方法：侵入挙動が観測された場合に，PC環境を侵入挙動前に戻し再度実行する**
    - ボットは未感染環境では侵入挙動を行う性質（侵入挙動の反復性）
    - 侵入挙動：PC内に常駐するために，自動実行リストへ登録する
  - **課題：処理が重い**
    - 環境を復元する事と，再度実行する必要がある

ワームの挙動

- PC侵入時の挙動
  - PC内に常駐するために，自身を複製し，複製を自動実行リストへ登録する
- 他PCへ拡散時の挙動
  - リムーバルディスクや共有フォルダなどに自身の複製を作成する

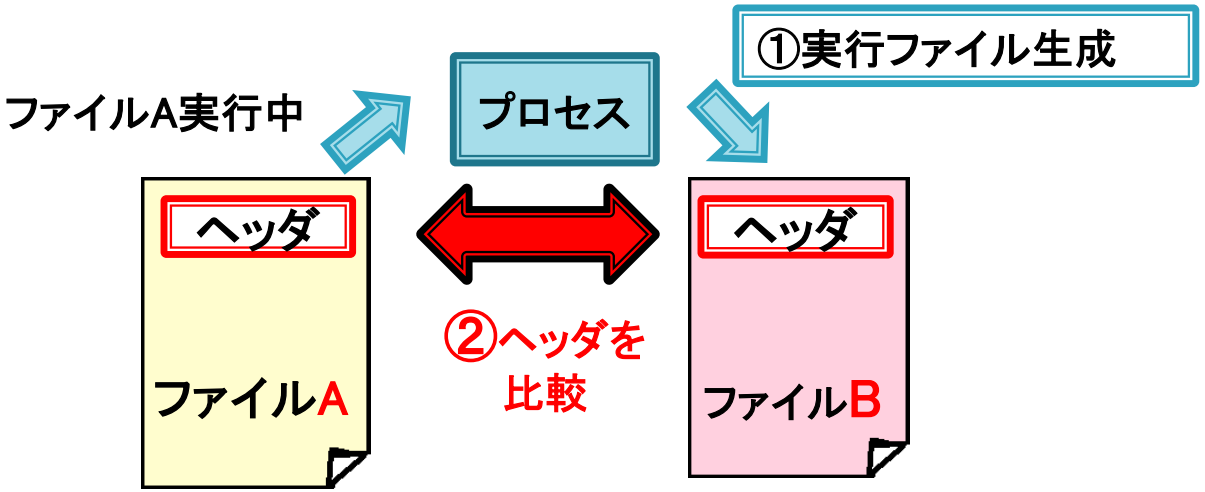


自己複製挙動を検知することでワームを検出できる

提案方式

- ワーム特有の挙動：自己複製挙動
  - 自己複製挙動の検出方法

① 実行中のプログラムのプロセスにおいて，実行ファイルを生成
② 生成された実行ファイルBと，生成したプログラムAのヘッダは一致



ポリモーフィック型

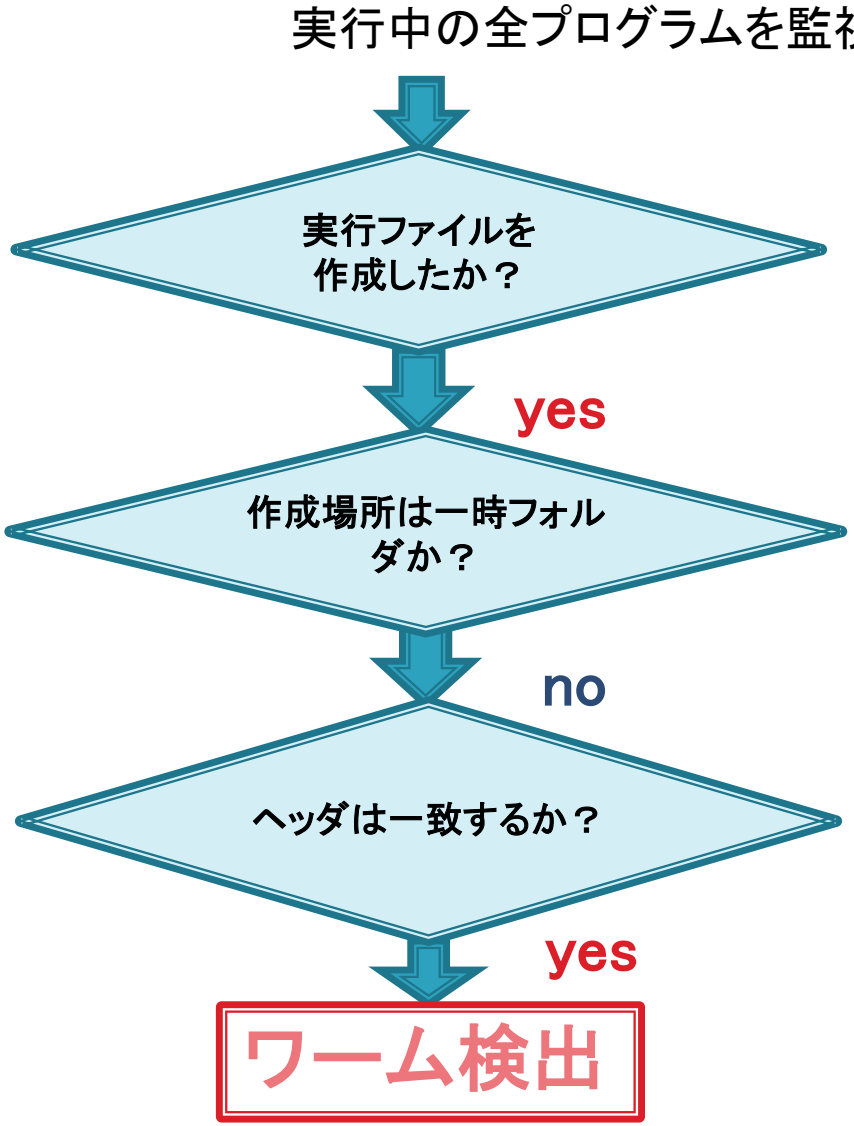
複製のたびに暗号化の鍵を変え，自己改変する
→ヘッダは改変が難しく変化しない
→ヘッダを比較することで自己複製を検出する

提案方式のフローチャート

- 誤検知回避について
  - 一部の正規プログラムが一時フォルダに自己複製を行うことがある
  - 一時フォルダ内のファイル
    - 通常アプリケーション終了時に削除される
    - ディスククリーンアップを行った時，削除される

  →ワームが一時フォルダに複製することは稀であり，検知結果に大きな影響はないと考えられる．

一時フォルダへの自己複製は
例外的に許可し，
誤検知のない方式とする



検知実験

提案方式が実際に有用であるか検知実験を行い検証

- 使用したワーム検体
  - 「Offencive　Computing」から独自に入手したマルウェアの内，Symantec社の種別がワームであるもの
- 実行環境
  - 仮想環境VMware上，「Windows7」（管理者権限で実行）

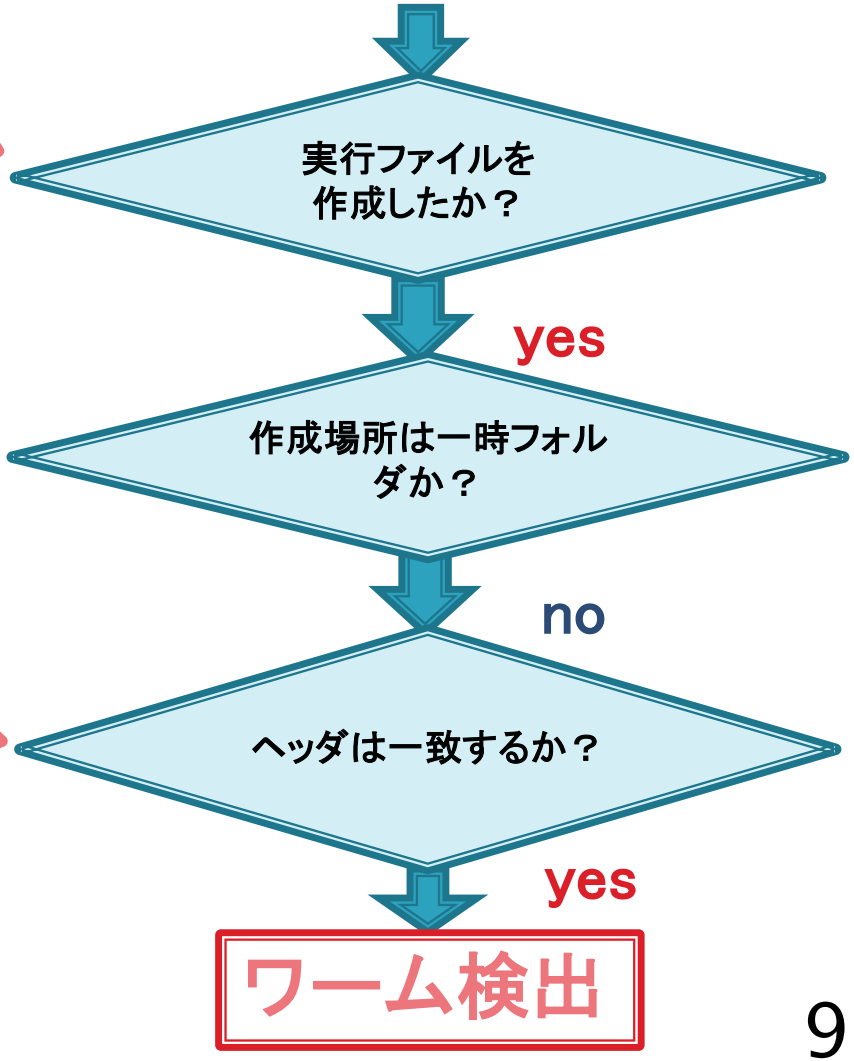
実験方法

ProcessMonitor
(プロセスの行った処理をリアルタイムで監視できるツール)で監視
→実行ファイル生成を検知

生成された実行ファイルのパスを確認
→一時フォルダかどうか確認

CompFile(2つのファイルを比較できるツール)を用いて,
実行ファイルを生成した側と,
生成された側の
ヘッダの一致を確認

実行中の全プログラムを監視



実験結果

	Symantec 社 マルウェア名	Symantec社 発見日	検出
1	W32.Disttrack	2012/8/16	×
2	W32.Cridex	2012/1/20	○
3	W32.IRCBot.NG	2011/4/7	△
4	W32.Pilleuz!gen2	2010/2/25	○
5	W32.Waledac	2008/12/23	×
6	W32.Downadup	2008/11/21	×
7	W32.Koobface	2008/8/3	○
8	W32.Koobface.B	2008/8/3	○
9	W32.Ircbrute	2008/6/20	×
10	W32.Badday.A	2007/10/3	○
11	W32.Fubalca.E	2007/4/1	△
12	W32.SillyFDC	2007/2/27	○
13	W32.SillyDC	2006/10/4	○
14	W32.Feebs.J@mm	2006/1/16	○
15	W32.Mytob.BE@mm	2005/4/21	○
16	W32.Mydoom.F@mm	2004/2/20	○
17	W32.Klez.gen@mm	2004/2/18	○
18	W32.Mimail.Q@mm	2004/1/7	○

- 12/18体検出（○）
  - 提案方式の有用性を確認
- 4/18体は自己複製をしなかった（×）
  - 仮想環境を検知された可能性
  - ワームではなかった可能性
- 2/18体は他プロセスに複製を委託（△）
  - 手法が巧妙であり，対策を検討中

まとめ

- ワーム検出の手法を提案した
  - ワームの本質的な挙動を考察し，自己複製挙動に着目
  - 検知実験を行い，提案方式の有用性を確認，課題を考察

- 今後の予定
  - 正規プログラムで誤検知が起きないか誤検知実験を行う
  - 課題を克服するため提案方式の改善方法について考え，実装を行う

参考文献

- 松本. 他：自己ファイルREAD の検出による未知ワームの方式, 情報処理学会論文誌, Vol.48,No.9, pp.3174-3182,Sep2007.

- 酒井. 他：侵入挙動の反復性を用いたボット検知方式, 情報処理学会論文誌,Vol.51,No.9,pp.1591-1599,Sep2010.

- マルウェア配布サイト「Offensive」 Computing,URL:http://www.offensivecomputing.net.

補足資料

PEヘッダ

Windowsの実行ファイルはPE（Portable Executable）フォーマットに従っている

- Address Of EntryPoint
  - プログラムの開始位置を示す値
- Size Of Image
  - イメージファイルをメモリにロードするために必要なサイズ
- Import table
  - インポートセクションのサイズとアドレス

これらは実行ファイル各々に固有の値で，かつ変更が難しい

実験結果

	Symantec 社 マルウェア名	Symantec社 発見日	WindowsXP	Windows7
1	W32.Disttrack	2012/8/16	×	×
2	W32.Cridex	2012/1/20	○	○
3	W32.IRCBot.NG	2011/4/7	○	△
4	W32.Pilleuz!gen2	2010/2/25	○	○
5	W32.Waledac	2008/12/23	×	×
6	W32.Downadup	2008/11/21	×	×
7	W32.Koobface	2008/8/3	○	○
8	W32.Koobface.B	2008/8/3	○	○
9	W32.Ircbrute	2008/6/20	○	×
10	W32.Badday.A	2007/10/3	○	○
11	W32.Fubalca.E	2007/4/1	○	△
12	W32.SillyFDC	2007/2/27	○	○
13	W32.SillyDC	2006/10/4	○	○
14	W32.Feebs.J@mm	2006/1/16	×	○
15	W32.Mytob.BE@mm	2005/4/21	○	○
16	W32.Mydoom.F@mm	2004/2/20	○	○
17	W32.Klez.gen@mm	2004/2/18	○	○
18	W32.Mimail.Q@mm	2004/1/7	○	○

- WindowsXP
  - 14/18体を検出
  - 4/18体は実行ファイルを作成していなかった

既存研究①~自己ファイルREAD~

- 検出方法

  ワームは自身を拡散する性質がある

  →他のコンピュータに感染時，自身の複製を作成する

  →自分自身のファイルを全てREADする

  自身のファイルを全てREADするという挙動を検出する

- **課題**
  - 自己ファイルREADという挙動は，正規プログラム(正規のアンインストーラ)でも起こるため誤検知が起こる.

既存研究②~侵入挙動の反復性~

- **検出方法**
  - ワーム（ボット）はPC内に常駐するために，
    自己複製をし，自動実行リストへ登録するという侵入挙動を行う
    →PC環境を未感染状態に復元すると，再び侵入挙動を行う

侵入挙動後のワームβ　を，侵入前の環境に戻し（γ），γを実行する
→侵入挙動が反復された時　α，　β　を検出する

- 課題：拡散挙動は検出不可