ボットネットおよび
ボットコードセットの耐性解析

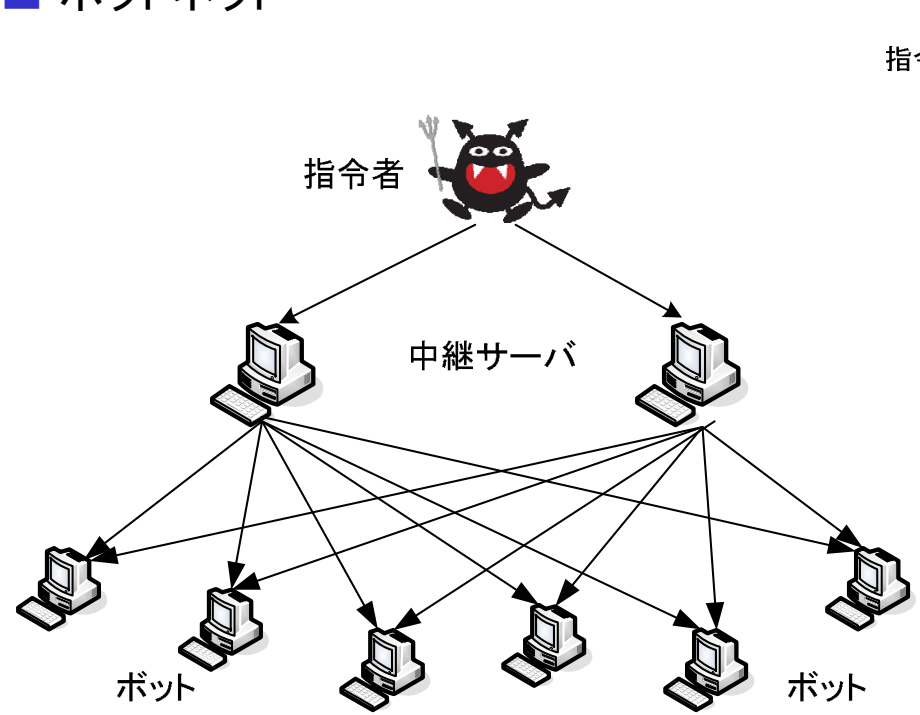
KDDI研究所　　静岡大学
竹森敬祐　磯原隆将　三宅優　西垣正勝

1. はじめに
2. 基本的な統計情報の調査
3. ネットワーク上でのボットネット耐性解析
4. PC上でのコードセット耐性解析
5. おわりに

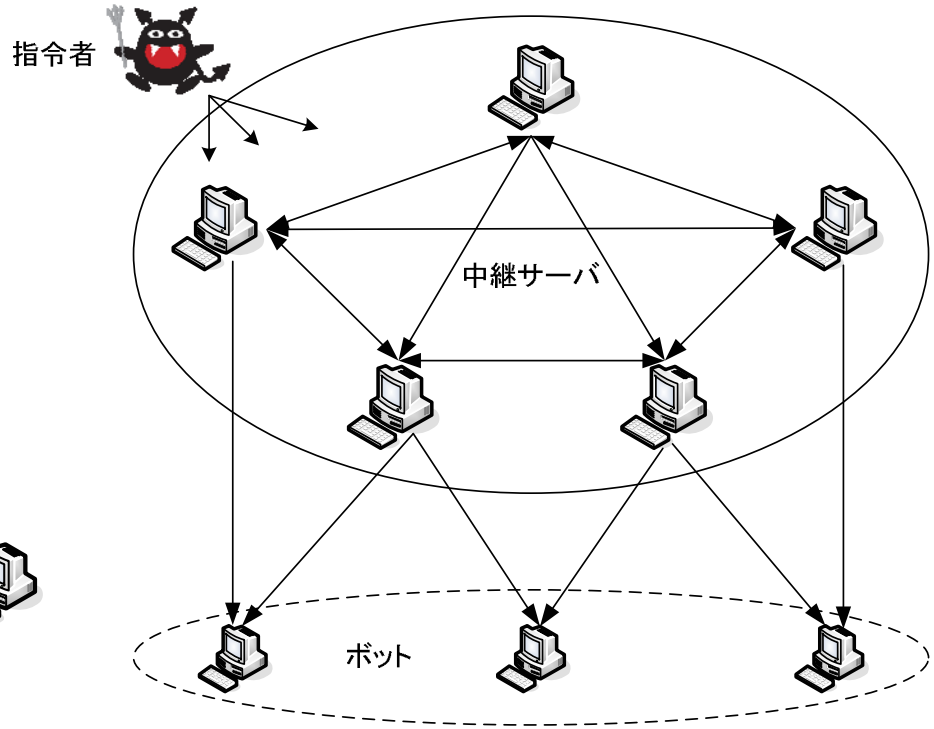
KDDI R&D LABS

1. はじめに

■ ボットネット



トップダウン型



P2P型

■ 課題

◆ 指令者は、効率的かつ安定的なボットネットの運用とボットの確保に努めている。

⇒ ボットネットおよびコードセットの耐性を把握することは、今後の対策として重要である。

KDDI R&D LABS

1. はじめに

【そこで本稿では】

■ ネットワーク上での耐性
- ◆ 中継サーバを並列化することで、ネットワーク上での生き残りを図っている。
  - (i) ボットネットの耐性解析
  - (ii) 並列管理されるコードの耐性解析

■ PC上での耐性
- ◆ 高機能を持った多数のコードをPCに送り込むことで、PC上での生き残りを図っている。
  - (iii) 送り込まれるコード数に着目した耐性解析
  - (iv) 単体のコードが持つ豊富な機能
  - (v) Anti Virus（AV）駆除後の残存コードのその後

1. はじめに ～解析対象のデータ～

- CCC DATAset 2008 攻撃通信データ（以降、CCC2008攻撃通信データ）
  - ハニーポット（ボット感染PC）が送受信する通信パケット（**Pcapファイル**）
    - ⇒ 中継サーバとの通信パケット
    - ⇒ 攻撃通信パケット （ただし、FirewallでOutbound方向を棄却）

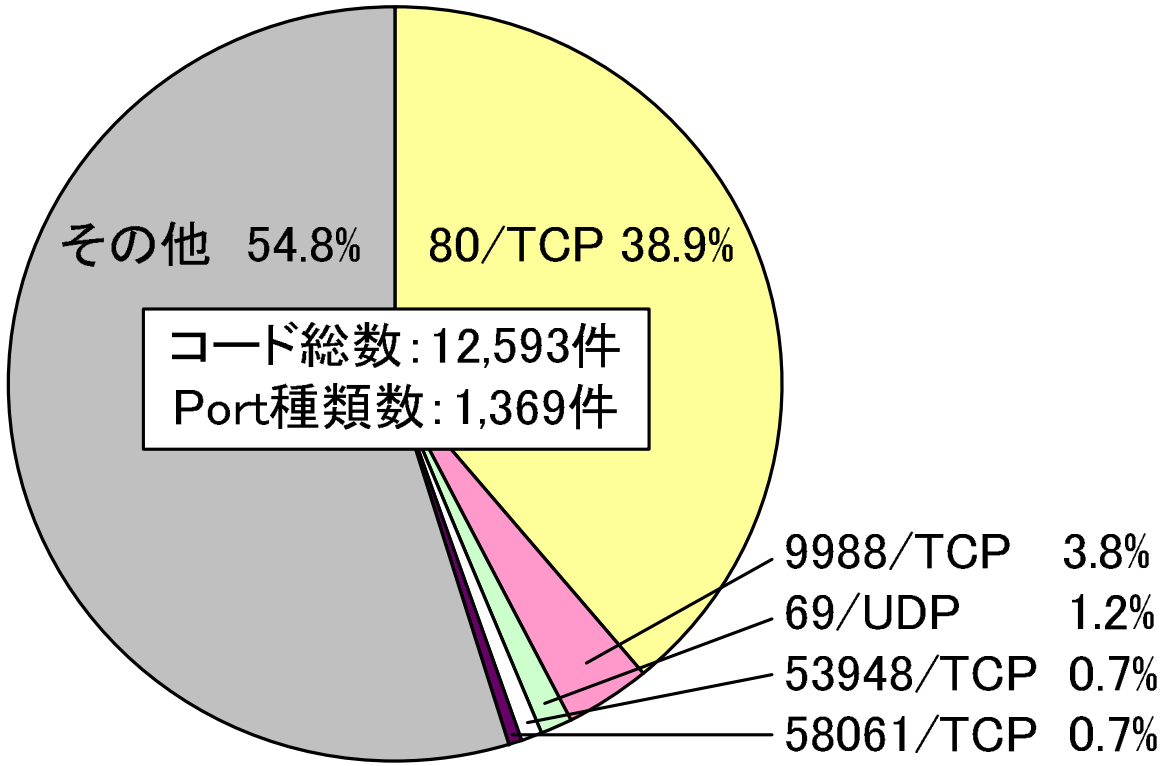
- CCC DATAset 2008 攻撃元データ（以降、CCC2008攻撃元データ）
  - ボットが中継サーバからコードを取得するときの**通信ログ**
    - ⇒ 中継サーバのIP：Port
    - ⇒ 取得されたコード名とハッシュ値

- 著者らが収集したコードから、、、
  - ハニーポットを運用しており、CCC攻撃元データに記録された同じコードを持っている。
    - ⇒ 同じコードをPCに感染させたときの**PCのファイル状態**
      （Outbound攻撃パケットの発信を棄却する安全な感染環境を構築している。）

2. 基本的な統計情報の調査 ～中継サーバ通信Portの分布～

■ 中継サーバ通信検知の難しさ
- ◆ IP変動の影響の小さな1日分：2008年4月30日のCCC2008攻撃元データに注目。
- ◆ 総コード数の38.9%は、80/TCPで配布されている。
- ◆ 他は様々な通信Portが利用されている。

⇒ **通信Portは広く薄く分布しており、通信Portに注目した検知やフィルタリングは難しい。**



中継サーバが利用するPortの分布

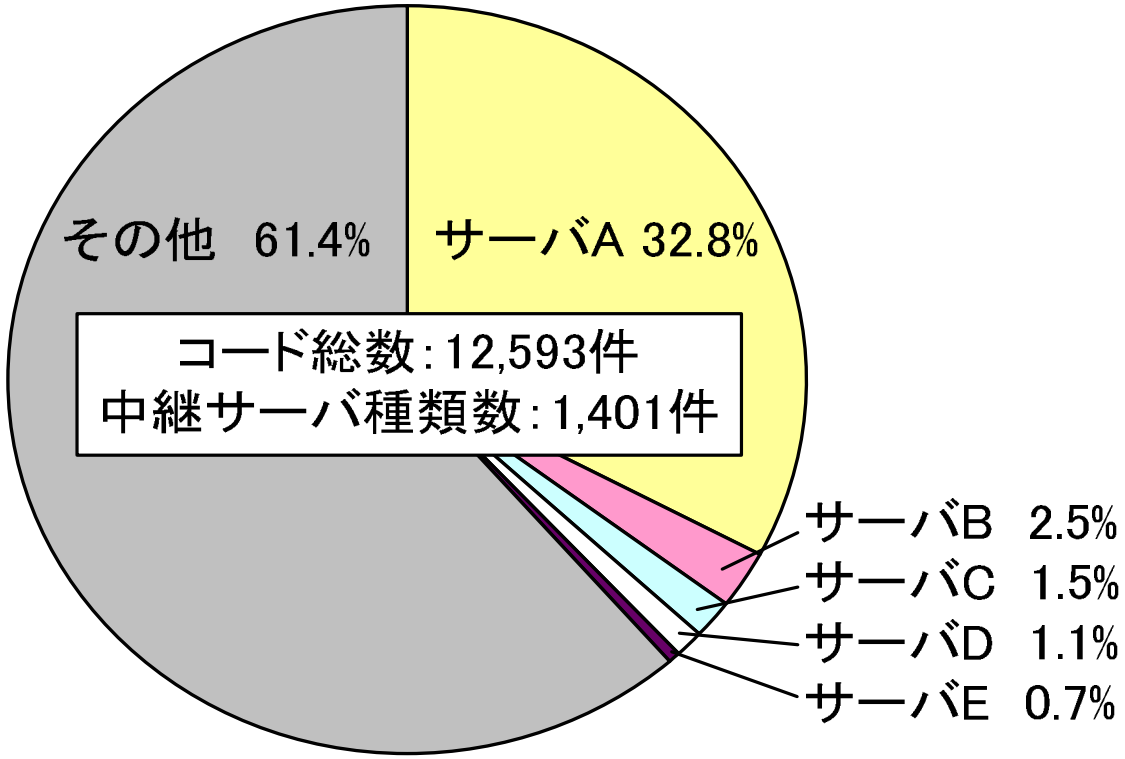
KDDI R&D LABS

2. 基本的な統計情報の調査 ～中継サーバIPの分布～

■ 中継サーバ駆除の難しさ

- ◆ IP変動の影響の小さな1日分：2008年4月30日のCCC2008攻撃元データに注目。
- ◆ 総コード数の32.8%のコードを配布した中継サーバが1つある。
- ◆ 他は多数の中継サーバが少しずつコードを配布している。

⇒ 中継サーバはインターネット上に広く薄く分布しており、ボットネットとして高い耐性あり。



コード配布を行う中継サーバIPの分布

KDDI R&D LABS

2. 基本的な統計情報の調査 ～未知のコード数～

■ 調査手順
- ◆ 2008年4月30日のCCC2008攻撃元データに注目。
- ◆ この時点でCCCが利用しているAVで判定できないUnknownコード数を調査した。
- ◆ コードの種別の判断は、ハッシュ値に注目した。

■ 未知のコード数
- ◆ 中継サーバから取得されたコード総数12,592件に対して、未知のコード総数は2,543件（**20.2%**）であった。

■ 未知のコード種類数
- ◆ 中継サーバから取得された総コード種類数817件に対して、未知のコード種類数は52件（**6.4%**）であった。

⇒ **未知のコードを積極的に配布している。**

3. ネットワーク上での耐性解析 ～概要～

■ 解析項目

(i) 中継サーバの並列化

⇒ CCC2008攻撃通信データからボットネットの構成を視覚化する。

(ii) コードの分散管理の様子

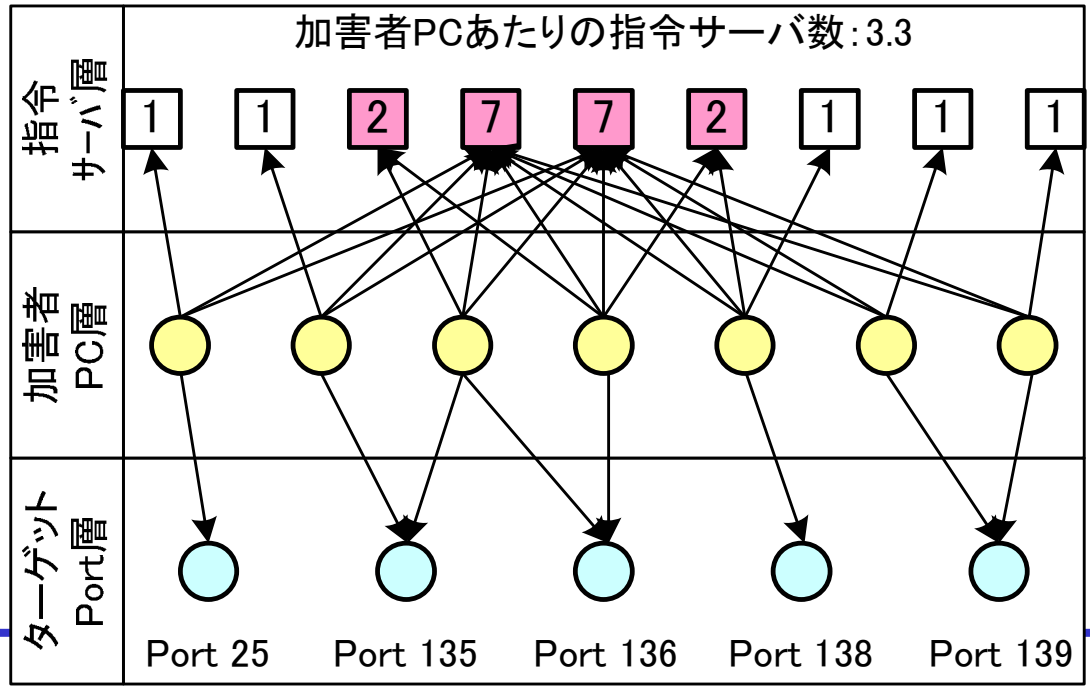
⇒ CCC2008攻撃元データからコード配布サーバの分散の様子を把握する。

3. ネットワーク上での耐性解析　～ボットネットの視覚化～

■ ボットネットのネットワーク上での耐性解析
- ◆ 数台の中継サーバが駆除されても、ネットワーク上でボットネットは生き残る。

■ ボットネットの視覚化ツールの提案 [DICOMO2008竹森、藤長、佐山、西垣]
- ◆ 本稿では、Pcapファイルから、ボットネットを視覚化するツールを実装した。

Step 1) 正常な宛先IPを除外する。
Step 2) ボットにみられる特徴的なパケットのSource IPをボット層に描画する。
Step 3) 攻撃拡散に利用されるPort25, 53, 135-139, 445などを、ターゲット層に描画する。
Step 4) 上記以外のDestination IPを中継サーバ層に描画する。

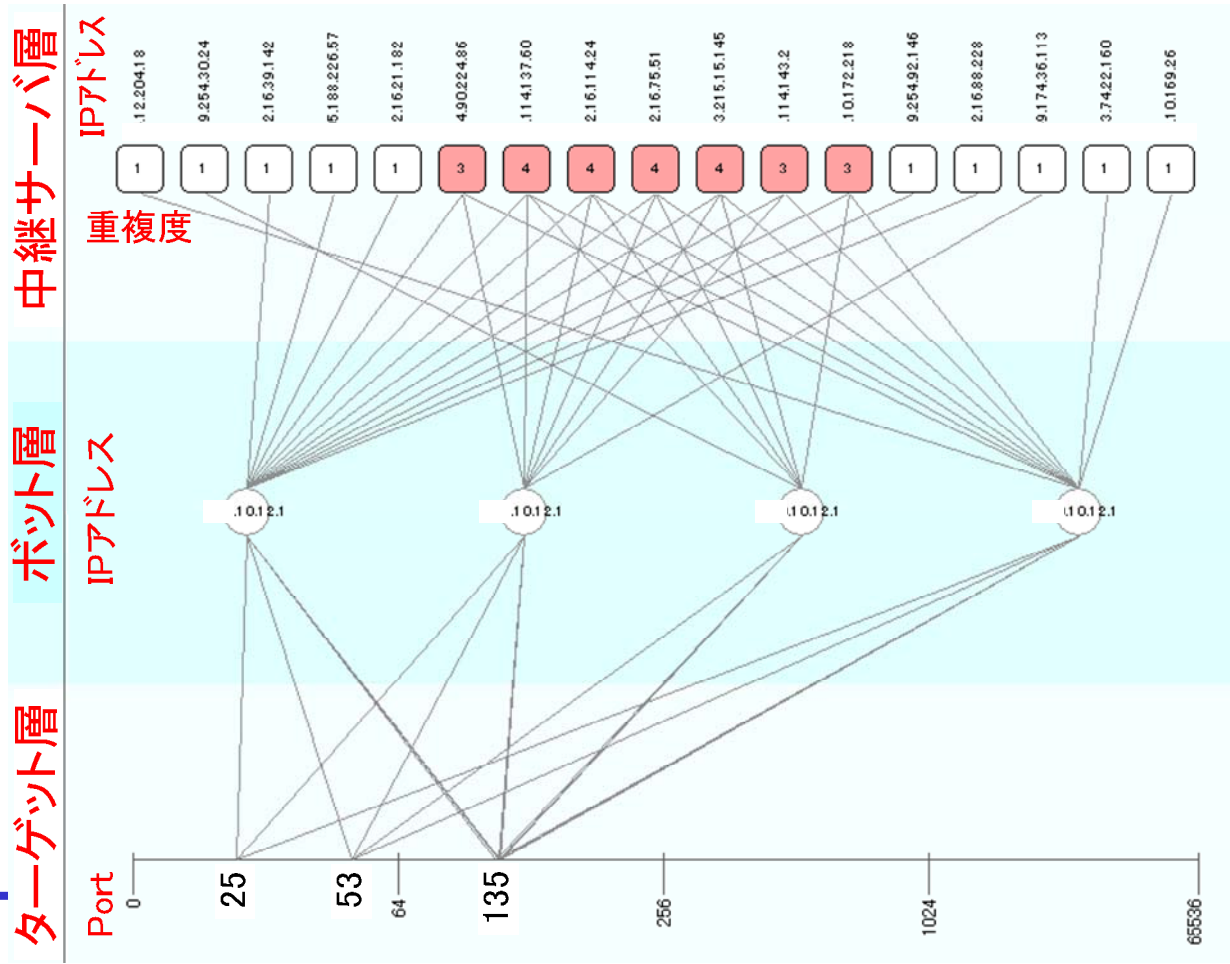


KDDI R&D LABS

3. ネットワーク上での耐性解析 ～(i)中継サーバの並列化～

■ 視覚化の効果

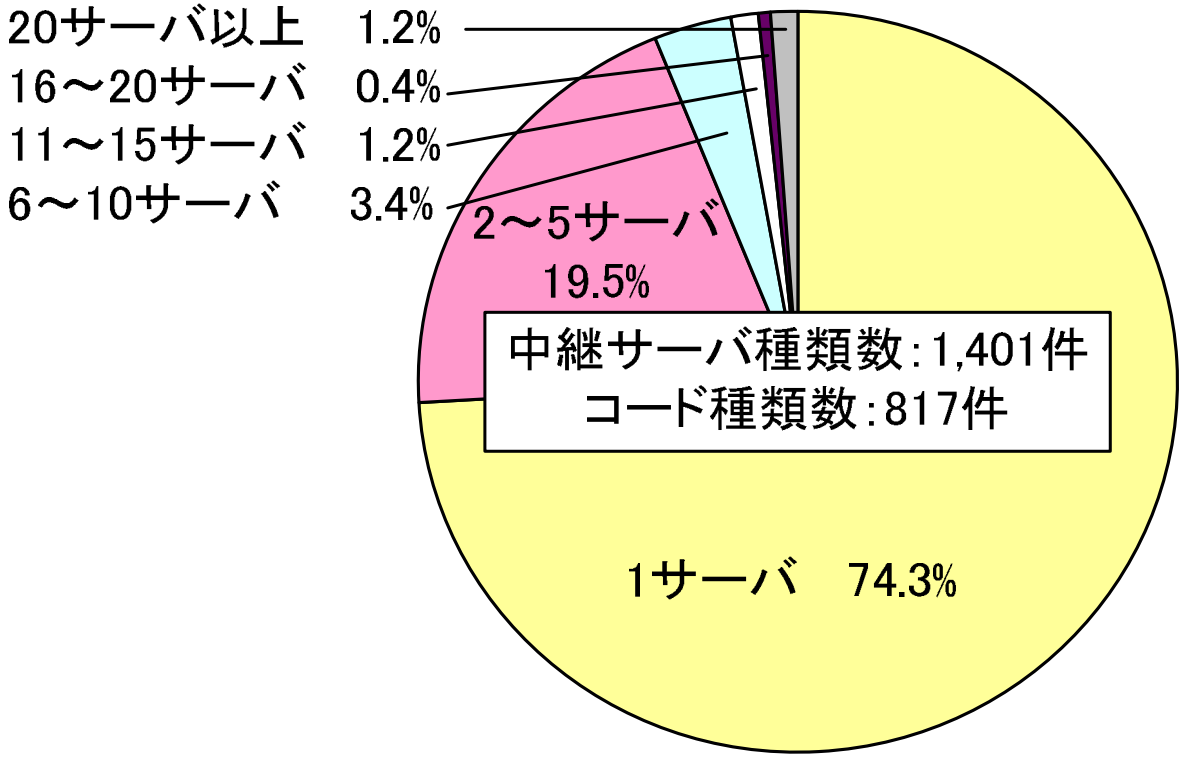
- ◆ あるボットネットを視覚化した。活発な中継サーバ7台を含む、合計17台の中継サーバで制御されている様子がわかる。
- ◆ Pcapファイルのオフライン解析として、ボットネット構成を自動描画できる。
- ◆ ボットネットが狙うターゲットPortを把握できる。
- ◆ 活発な中継サーバを把握できる。



3. ネットワーク上での耐性解析 ～(ii)コード管理の並列化～

■ コードのネットワーク上での耐性解析

- ◆ コードを複数の中継サーバで管理・配布することで、中継サーバが駆除された場合でも、ネットワーク上でコードが生き残ることができる。
- ◆ CCC2008攻撃元データに記録されているコードのハッシュ値に注目して、各々のコードがいくつの中継サーバから配布されているかを調査した。
- ◆ 25.7%のコードが複数台の中継サーバから配布されていた。多いものは、69、40、34台。



KDDI R&D LABS

4. PC上での耐性解析 ～解析対象のコードセット～

■ コードのPC上での耐性解析
- ◆ ここでは、(iii)送り込まれるコード数、(iv)コードの多機能性、(v) 残存コードの挙動、(vi) AV処理の妨害について紹介する。

■ 8つのコードセット
- ◆ 我々が独自に収集したコードのうち、CCC2008攻撃元データと一致するものに注目。
- ◆ ボットに感染すると、中継サーバから複数のコードを取得して、以下の処理を行う。
  - ⇒ 自身のコードを削除するもの
  - ⇒ HDDにそのまま保存されるもの
  - ⇒ 複数のコードに変態してHDDに保存されるもの
  - ⇒ 元からあるファイルに感染するもの
  - ⇒ レジストリや設定ファイルを改変するもの

4. PC上での耐性解析 ～(iii)PCに送り込まれるコード数～

■ 8つのコードセット
- ◆ 各コードに感染して10分後の、コードと設定の追加・変更・削除の様子をTripwireで確認。

■ 解説
- ◆ 複数のコードを取得して、多数のコードを書き込み、多数の設定を改ざんする。

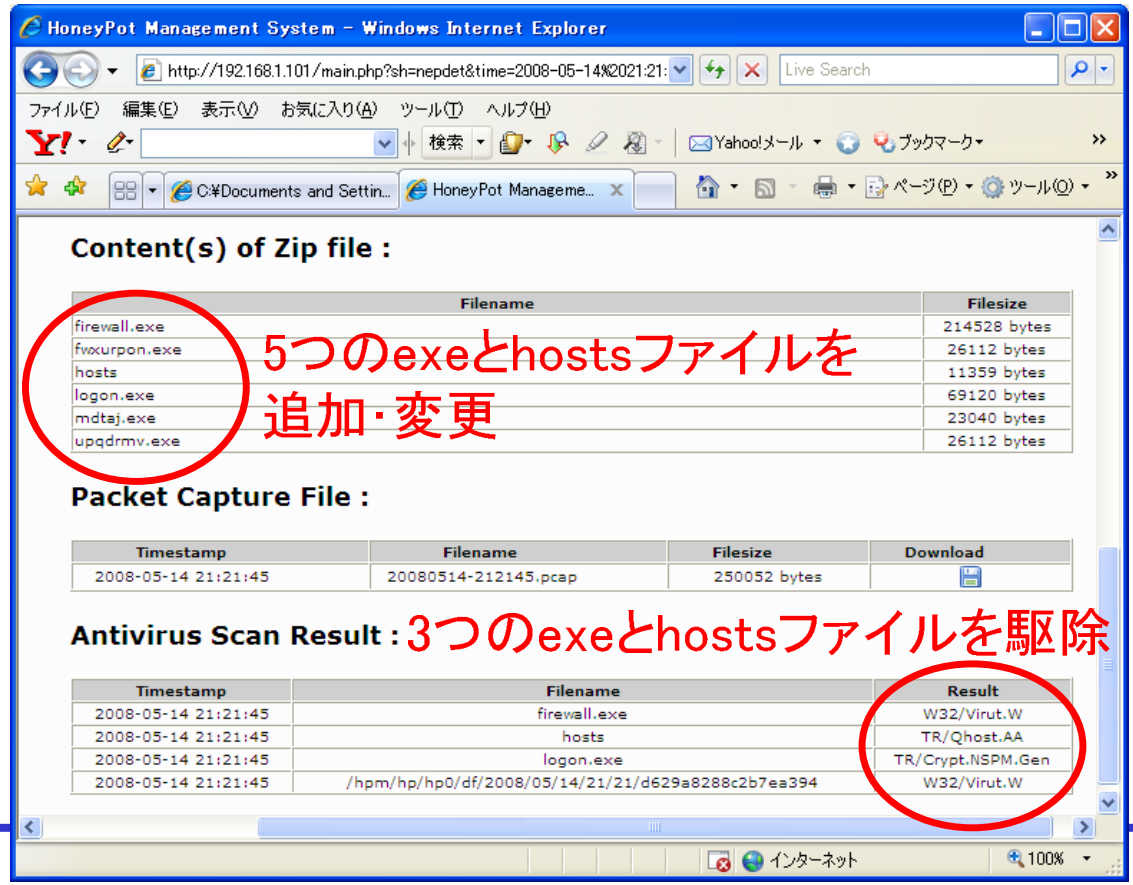
セット	コード		設定の追加・変更・削除	
	追加	変更	レジストリ	hosts
1	4 (exe)	527(exe,htm,scr)	305	有(127型)
2	3 (exe)	422 (exe,scr)	311	有(255型)
3	107(exe)	106 (htm)	15	無
4	5 (exe)	0	3	有(255型)
5	6 (exe)	0	3	有(127型)
6	6 (dll,exe)	3 (ini,sys)	115	無
7	5 (exe)	0	4	有(127型)
8	4 (dll,exe)	1 (ini)	7	有(255型)

KDDI R&D LABS

4. PC上での耐性解析 ～(iii)送り込まれるコード数～

■ 未知コードの様子
- ◆ 我々が運用しているハニーポットで判定された未知／既知コードの様子を示す。

■ 解説
- ◆ 初期コードが削除され、5つのexeコードが追加され、hostsが改竄された。
- ◆ AVで初期コード、2つのexeコード、hostsが検知され、**2つのexeコードが残っている**。

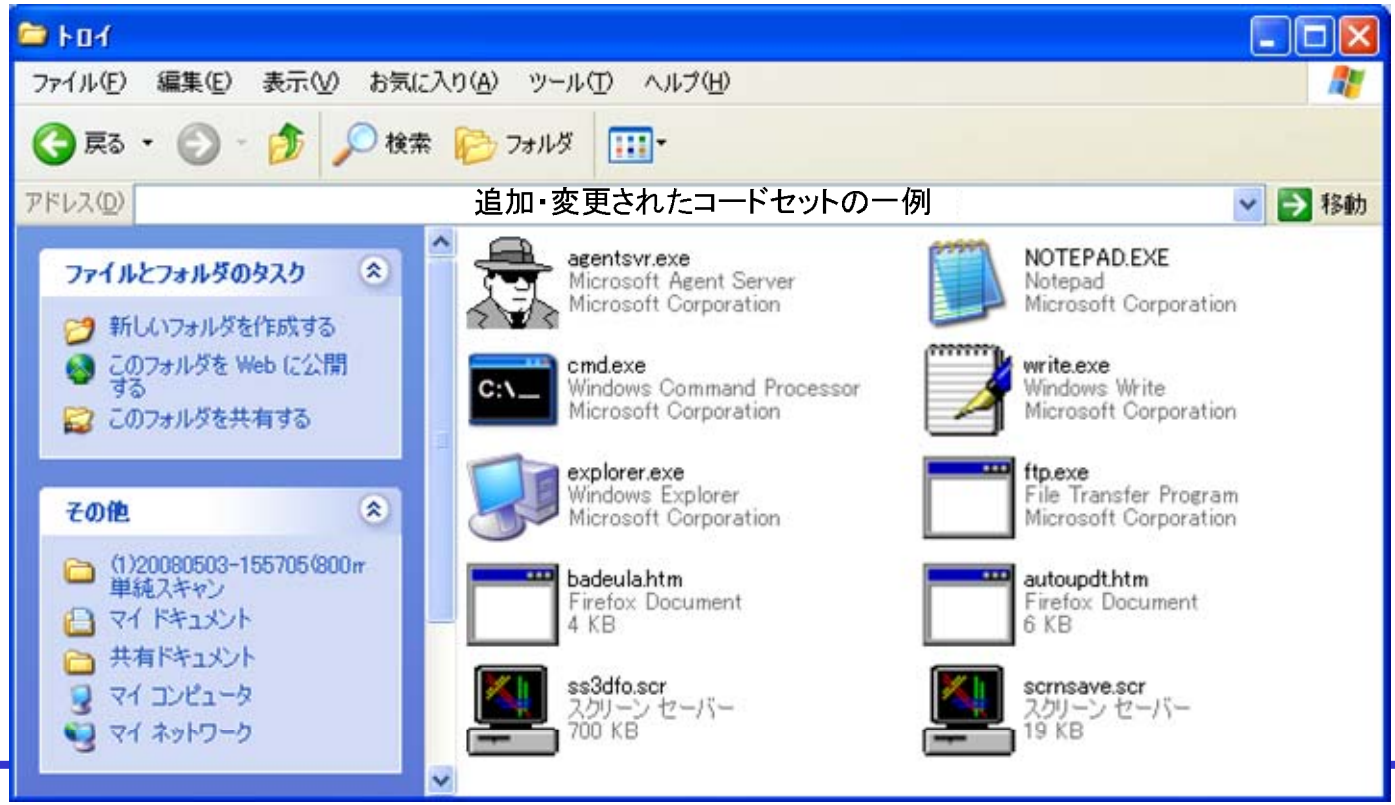


KDDI R&D LABS

4. PC上での耐性解析 ～(iv)コードの多機能性～

■ コードの生き残りの工夫
- ◆ 追加・変更されたコードの一例を示す。

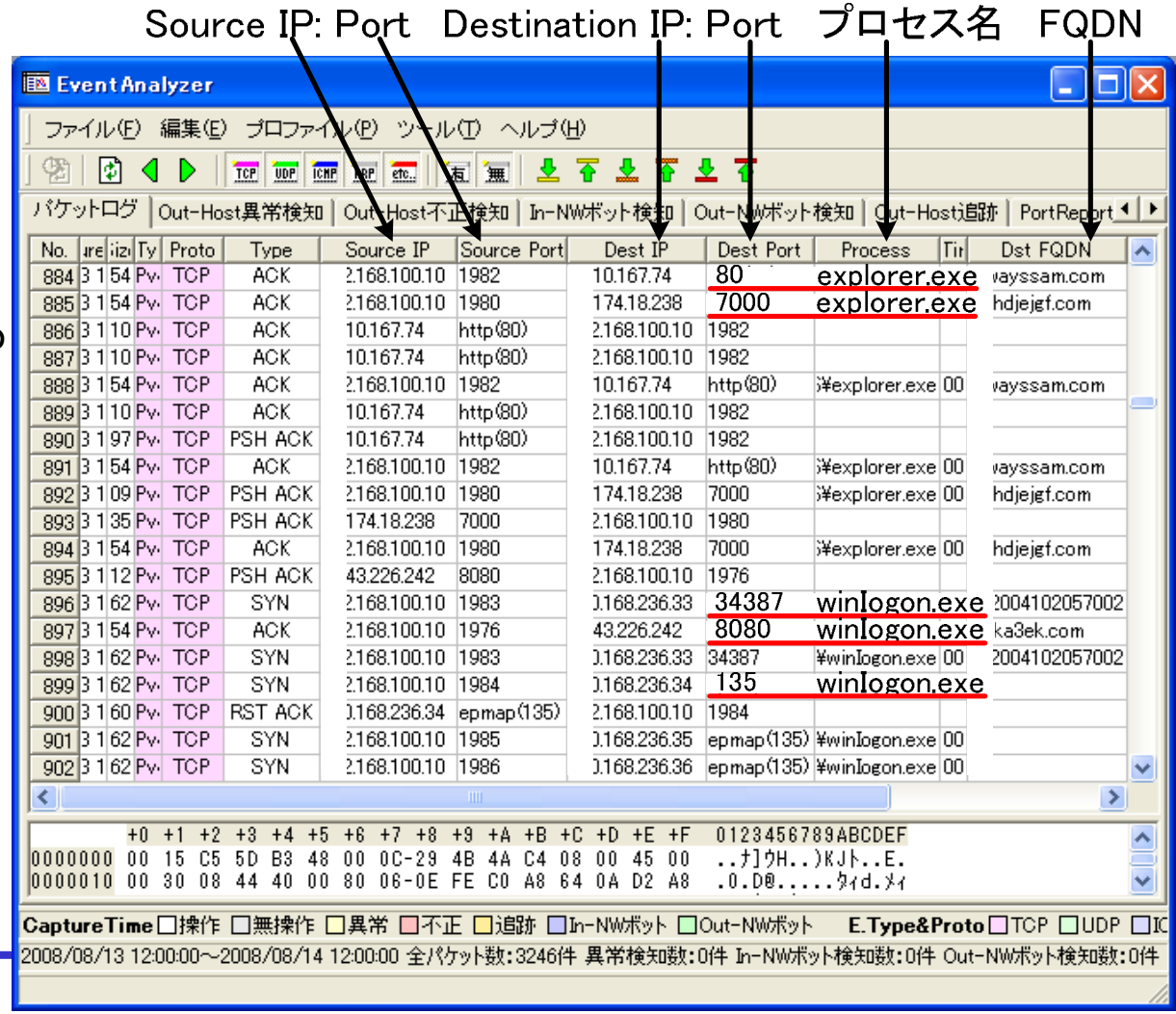
■ 解説
- ◆ これらの殆どが起動されることなく、HDDに保存されたままである。しかし、cmd.exeやexplorer.exe、bedaula.htm、などは，Windows PCが元々持つプログラムに感染しており、ユーザ操作の中で起動が期待されるトロイの木馬である。



KDDI R&D LABS

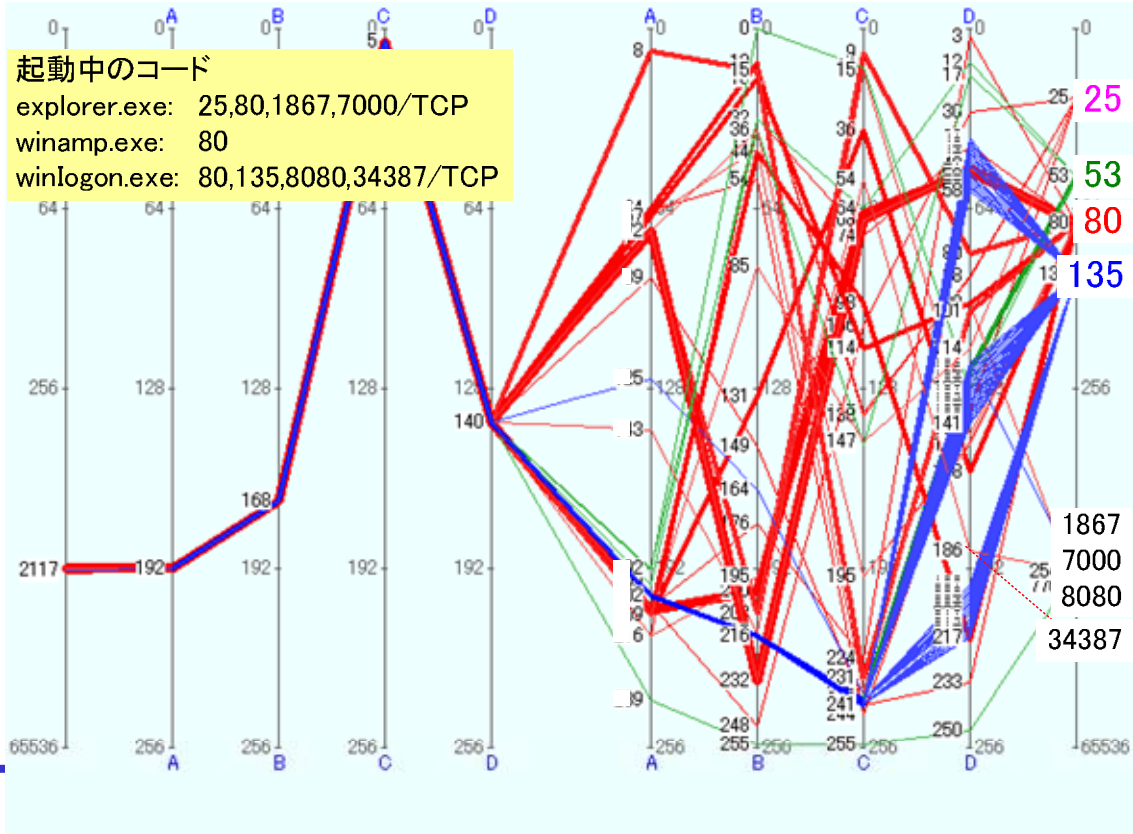
4. PC上での耐性解析 ～(iv)コードの多機能性～

- プロセス通信モニタ
  - 著者らが開発したホスト型の通信プロセスモニタ[4]を用いて視覚化した様子を示す。
- 解説
  - exploere.exe, winamp.exe, winlogon.exeの3つのコードが起動して外部のPCと通信している。
  - 3つのコード は独立動作しており、様々なIP:Portに向かって通信している。



4. PC上での耐性解析 ～(iv)コードの多機能性～

- 通信パターンモニタ
  - 著者らが開発した通信パターンモニタで先ほどの通信を視覚化した様子を示す。
- 解説
  - PCの送受信パケットを観測しただけでは、ユーザ操作による通信と、ボットの通信を見分けることはできない。
  - 起動中のボットプロセス数を推定することもできない.



KDDI R&D LABS

4. PC上での耐性解析 ～(iv)コードの多機能性～

■ 通信挙動の解析
- ◆ 3つのボットプロセスが10分間で通信したDestination Portと、正常なアプリケーションを特別な設定や操作を行うことなく利用したときのDestination Portについて示す。

■ 解説
- ◆ ボットのプロセスは，2つのHigh Portを含む4つのPortを利用している。
- ◆ 正常なアプリケーションは1つもしくは2つのWell-known Portを利用している。
- ◆ 3つのボットプロセスとも、80/TCPの通信を行っている。よって、1台のボット感染PCから発信される80/TCPの通信は、複数のボットプロセスから発信される複合パケットである。

アプリケーション	プロセス名	Destination Port
Outlook Express	msimn.exe	25,110/TCP
Internet Exproler	iexproler.exe	80,443/TCP
Acrobat Pro.	AcroRd32.exe	80/TCP
ボット	explorer.exe	25,80,1867,7000/TCP
	winamp.exe	80/TCP
	winlogon.exe	80,135,8080,34387/TCP

4. PC上での耐性解析 ～(iv)コードの多機能性～

■ 7KBのコードの脅威
- ◆ 数十～数百KBのサイズのコードが多い中、コードセット6では7KBのコードが追加された。
- ◆ このコードについて挙動解析を行ったところ、80/TCPによる指令の取得と、25/TCPによるスパムメールの送信を行った。

■ 解説
- ◆ 小さなコードでも豊富な機能を持つ。
- ◆ 今回の8つのコードセットでは、指令の受信や攻撃の発信をコード間で分担するような協調処理はみられず、個々のコードで処理が完結していた。

⇒ 一部のコードを駆除することで、コードセットを機能不全にすることはできない。

4. PC上での耐性解析 ～(v)残存コードのその後～

■ AV駆除後の残存コード
- ◆ コードセット7では、AVで駆除できずに未知コードとして残ったものがある。
- ◆ このコードを10分間活動させたときの様子をモニタした。

■ 解説
- ◆ 135/TCPへの攻撃を拡散する。
- ◆ 新たに80/TCPで2つのコードを取得して、これらを起動した。
- ◆ さらに3つのコードを作成して、HDDに保存した。これらは、起動されていない。

⇒ **駆除漏れのコードが残ることで、感染状態に戻ってしまう。**

- ◆ AVやIDSをインストールしてあるPCの場合、残ったコードが既知のコードを自動取得することで、身に覚えの無いAVアラームが次々と出ることになる。

⇒ **残存コードの有無を確認できる。**

5. おわりに

■ ネットワーク上での耐性解析
- ◆ 多数の中継サーバが並列化されていること
- ◆ コードを複数の中継サーバから配布していること

⇒ ネットワーク上でのボットネットの耐性が明らかになった。

■ PC上での耐性解析
- ◆ 多数のコードをHDDに作成すること
- ◆ トロイの木馬型コード、複数Port通信コード、多機能搭載のスモールコードであること
- ◆ 残存コードから復元されること
- ◆ AVのパターンファイルの更新を妨げること

⇒ PC上でのコードの耐性が明らかになった。

■ 著者からの提言
- ◆ AVは初期の感染予防には役立つが、感染後は、完全な駆除や修復は望めない。
- ◆ 身に覚えのないAVアラームが出るような場合には、残存コードが疑われる。

⇒ ユーザファイルのバックアップを取った後に、OSの再インストールを行う。