2008-10-09 (Thu) MWS2008-M4-1004

複数観測データを用いた ボットネットの活動分析に関する一考察

NTTコミュニケーションズ株式会社　畑田充弘
中央大学大学院　寺田真敏

もくじ

もくじ

はじめに

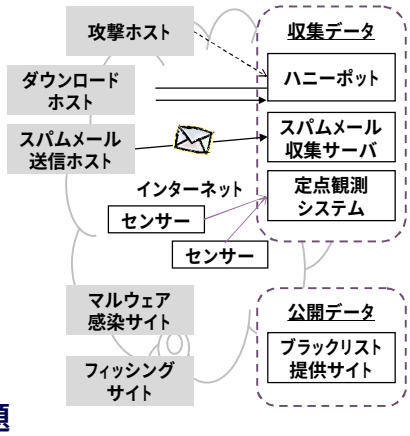
- ボットネットの活動
  - 様々な経路での感染活動
    - リモート攻撃、メール添付、Web受動的攻撃[4]、etc.
  - 大量のスパムメール送信
    - 広告インフラ、フィッシングやマルウェア感染サイトへの誘導、etc.
  - DDoS攻撃
    - 脅迫、大量トラフィック、etc.
  - フィッシングサイトやマルウェア感染サイトの開設
    - ID・PWD搾取、感染経路の開拓、金銭被害、構築ツール、etc.
  - DNSやWeb、IRCといったインターネットを支える各種機能を駆使した広範かつ巧妙な活動

- ボットを含むマルウェアの対策[1]
  - 感染検知
    - パターンマッチング、ヒューリスティック、ハニーポット、etc.
  - 動的／静的解析
    - 疑似環境での挙動解析、リバースエンジニアリング、etc.
  - 広域観測
    - FWやIDSの分散配置、マルチレイヤの観測情報の組合せ[2]、etc.
- 本稿では
  - ボットネットの活動の一端となる観測データを複数用いて、まずは活動傾向の分析例を示す

もくじ

観測データ

- 収集データ
  - 各観測環境で収集したデータ
  - 詳細なログ入手が可能
  - 収集環境の網羅性が課題
- 公開データ
  - ブラックリスト等として公開
  - 観測環境は不要、入手は容易
  - 網羅性や信憑性が課題
- 本稿では
  - 観測データの課題は今後の課題



観測データ

- No.1：感染活動ログ
  - 多数のハニーポットで収集したマルウェアダウンロード時の日時、ダウンロードホストIPアドレス、ウイルス名称、etc.（CCC DATAset 2008の攻撃元データ by CCC[3]）
- No.2：スパムメールログ
  - No.2-1：受信日時、発信元IPアドレス
  - No.2-2：本文中の誘導先URL、URL中FQDNのIPアドレス、クエリー日時
- No.3：マルウェア感染サイトのブラックリスト（BL）
  - Malware Block List[5] から日本時間0時と12時にURLリスト取得、URL中FQDNのIPアドレス、クエリ日時
- No.4：フィッシングサイトのBL
  - PhishTank[6]から日本時間6時と18時にVALIDかつONLINEの最新1,000件のURLリスト取得、URL中FQDNのIPアドレス、クエリ日時
- No.5：定点観測データ
  - JPCERT/CCが運用しているISDAS[7]のセンサーで検知した攻撃時のタイムスタンプ、発信元及び宛先のIPアドレス及びポート番号、etc.

もくじ

- 分析対象期間
  - 2008年4月1日～2008年4月30日の1ヶ月間
- 各観測データの件数
  - No.1：イベント数：406,555件
  - No.2：1,534,057通、ユニークなURL数：671,823件
  - No.3：ユニークなURL数：1,713件
  - No.4：ユニークなURL数：22,772件
  - No.5：イベント数：264,970件
- 分析方針
  - 下記の組合せにおいて、日時とIPアドレスを中心に分析
    - 感染活動ログ（No.1）と各観測データ
    - 感染活動ログ（No.1）と複数観測データ

感染活動ログ（No.1）と各観測データ

感染活動ログ（No.1）と各観測データ

- **ユニークIPアドレス**

No.	ユニークIPアドレス数
1	37,914
2-1	412,953
2-2	1,155
3	905
4	9,463
5	52,498

No.1：**感染活動**
No.2-1：**スパム発信元**
No.2-2：**スパム誘導先**
No.3：**マルウェア感染サイト**BL
No.4：**フィッシングサイトの**BL
No.5：**定点観測データ**

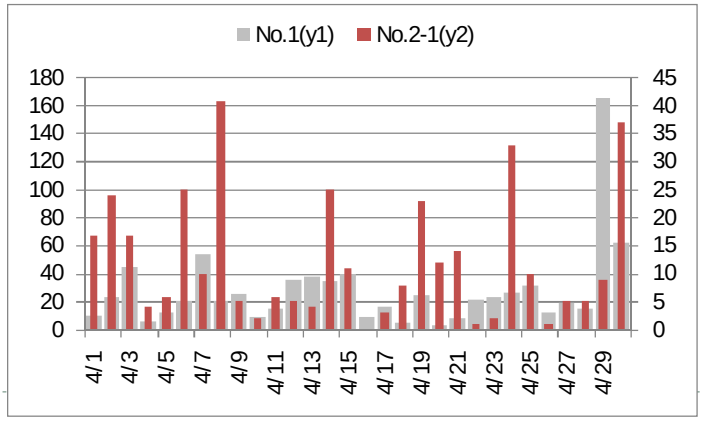
- **No.1との一致数及びドメイン別分布**

No.	一致数	ドメイン（数）
2-1	**75**	JP(26), US(6), RU(6), RO(5), MX(5), Other(27)
2-2	**7**	KR(5), CN(1), JP(1)
3	**1**	IL(1)
4	**7**	KR(4), CN(1), PH(1), US(1)
5	**3,690**	JP(3054), CN(153), TW(94), KR(58), US(53), Other(278)

No.1 & No.2-1

No.1：感染活動
No.2-1：スパム発信元

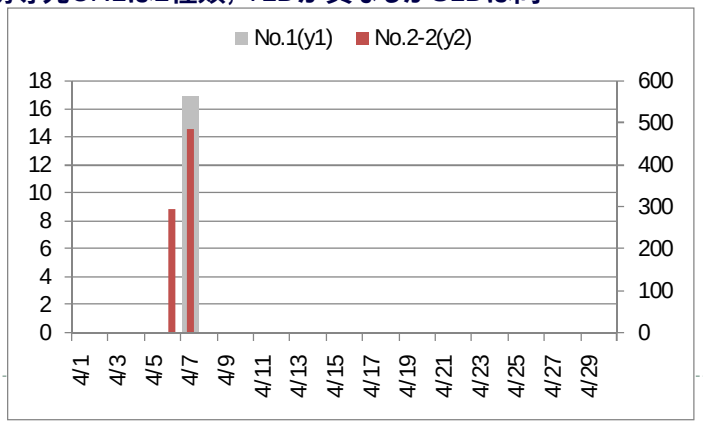
- 75個のIPアドレス
- 感染数とスパムメール受信数の推移
  - 増減の傾向に類似性が見える



No.1 & No.2-2

No.1：感染活動
No.2-2：スパム誘導先

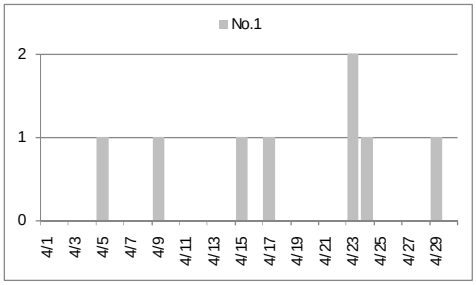
- 7個のIPアドレス。例として1個のIPアドレスについて。
- 感染数と誘導先URLが含まれるスパムメール受信数の推移
  - 感染活動と誘導先が短い期間においてのみ連動して利用
  - 誘導先URLは2種類，TLDが異なるがSLDは同一

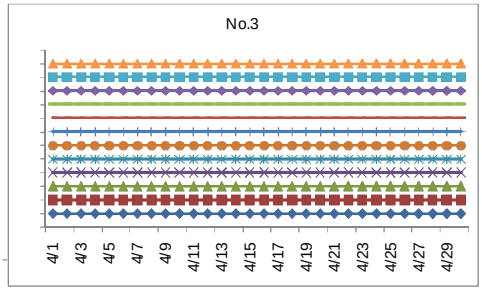


No.1＆No.3

No.1：感染活動
No.3：マルウェア感染サイトBL

- 1個のIPアドレス
- 感染数とBLにユニークなURLが登録されていた期間(BL登録期間)
- 感染数は少なく，12種類のURLのBL登録期間に対してまばら
- BLが公開されているため，攻撃者側もリストに基づく対策を回避？
- 12種類のURLはTLD，SLDが同一でありホスト部が異なるURL

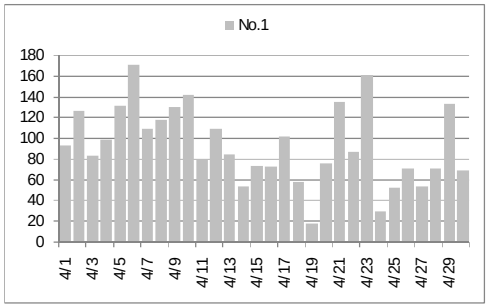


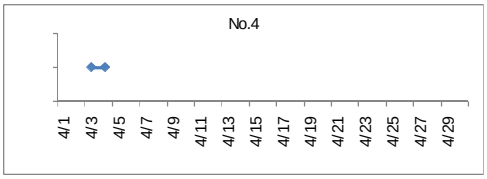


No.1＆No.4

No.1：感染活動
No.4：フィッシングサイトのBL

- 7個のIPアドレス。例として1個のIPアドレスについて。
- 感染数とBL登録期間
- フィッシングサイトとしてのBL登録期間は短期間ではあるが，分析対象期間を通して感染活動を確認

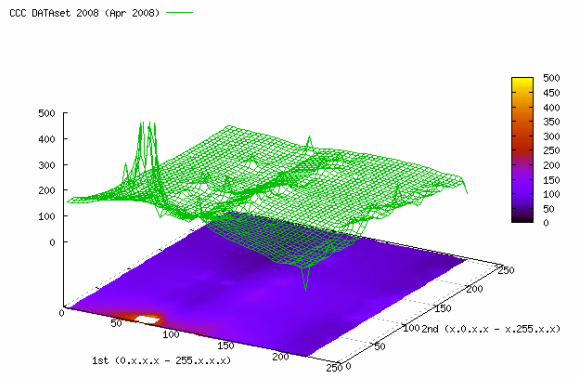




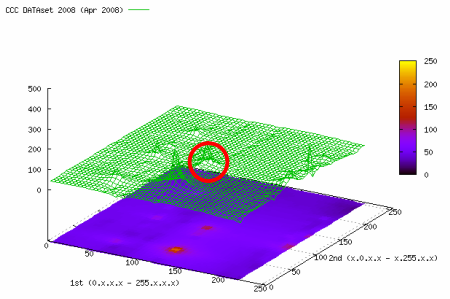
No.1＆No.5

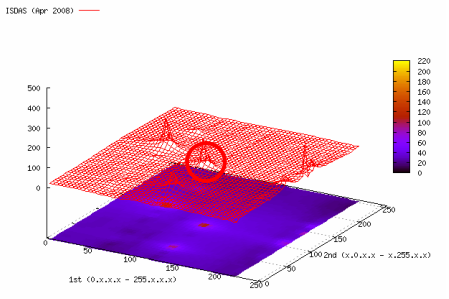
No.1：感染活動
No.5：定点観測データ

- 3690個のIPアドレス。
- まず、No.1についてIPアドレスの第1オクテットと第2オクテットによる頻度を算出



- “同一日に出現した”IPアドレスの第1オクテットと第2オクテットによる頻度をNo.1とNo.5について算出
- 12x.10x付近のホスト出現が共通して多い
- この出現頻度傾向は，No.1(前頁)だけの結果とは異な



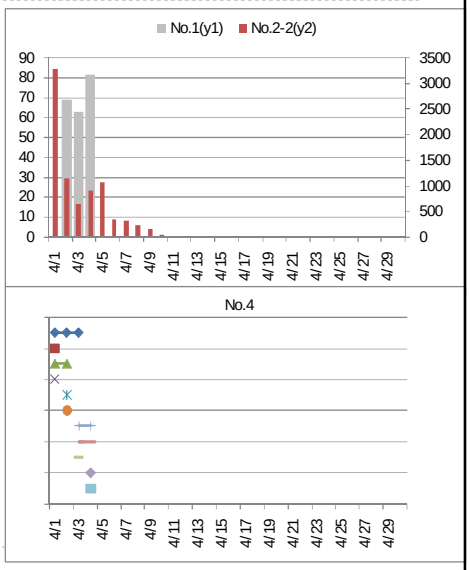


感染活動ログ（No.1）と複数観測データ

No.1、No.2-2＆No.4

No.1：感染活動
No.2-2：スパム誘導先
No.4：フィッシングサイトのBL

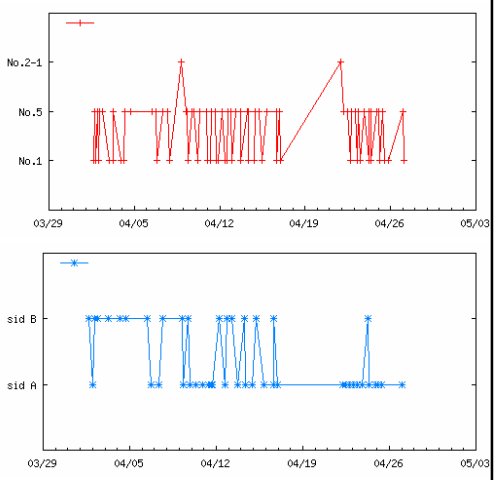
- 5個のIPアドレス（4個のIPアドレスはKRの同一netname、1個のIPアドレスはCN。感染検体は全て同一ハッシュ値のトロイの木馬）。1個のIPアドレスについて
- 感染数と誘導先URLが含まれるスパムメール受信数の推移，及びURLがフィッシングサイトのBL登録期間
- 4月前半のみに分布
- 誘導先URLの31種類はフィッシングサイトのBL登録のURLとの一致は無し
  - 21種類は1日のみ誘導先URLとして用いられていた．



No.1、No.2-1＆No.5

No.1：感染活動
No.2-1：スパム発信元
No.5：定点観測データ

- 7個のIPアドレス。例として1個のIPアドレスについて
- 各観測データの検知状況、No.5の各センサーの検知状況
- スパム発信元としての利用に比べ、マルウェアのダウンロードや感染に至る攻撃元としての利用頻度が高い
  - スパム送信依頼：受動的活動
  - 支配下に置く：ホスト拡大：能動的活動
- イベント検知はsid A及びsid Bの2センサーのみ
  - 攻撃活動自体はある程度局所的なものと推定



デモ

もくじ

おわりに

- ボットネットの活動の一端と考えられるインターネット上の実観測データを複数用いて、日時とIPアドレスを中心に分析を行い、連動を示すことができた。
- バーチャルドメインのホスティングサーバ、DNSにより負荷分散されたサーバ群、DynamicDNSなど、ボットネットの運用に適した攻撃対象は従来と同様に警戒が必要と考える。
- URL短縮サービスや検索エンジンを利用したWebページのリダイレクト等を含むURLの多段リンク構造も、追跡を困難にしている。
- 観測データの拡充、網羅性・信憑性・即時性の評価、複数の観測データに基づいたURLやURI、IPアドレスでのブラックリストのリアルタイム管理、フィルタ等の適用など仕組みの検討が課題。

謝辞

- 本研究の遂行にあたって、ISDASの定点観測データならびに研究用データセット“CCC DATAset 2008”を提供頂いたJPCERT/CC とサイバークリーンセンターに感謝する

参考文献

- [1] 藤原将志，他：マルウェアの感染方式に基づく分類に関する検討，情報処理学会CSEC研究報告 No.21 p177-182(2008年3月)
- [2] 鬼頭哲郎，他：マルチレイヤ型広域モニタリングに関する検討，情報処理学会CSEC研究報告 No.16 p279-284(2007年3月)
- [3] サイバークリーンセンター，https://www.ccc.go.jp/
- [4] 秋山満昭，他：クライアントハニーポットを用いたWeb感染型マルウェアの実態調査，CSS2008(2008年10月)
- [5] Malware Block List，http://www.malware.com.br/index.shtml
- [6] PhishTank，http://www.phishtank.com/
- [7] ISDAS，http://www.jpcert.or.jp/isdas/