悪性プログラムの調査を目的とした通信データ解析ソフトウェアの実装

水谷 正慶† 武田 圭史† 村井 純‡

†慶應義塾大学大学院 政策・メディア研究科 ‡慶應義塾大学 環境情報学部

1 はじめに

近年，コンピュータウィルスやボット，スパイウェアなど悪意のあるプログラム (マルウェア) がインターネット上の脅威として深刻化している．特に組織的犯罪に利用されるボットなどでは，感染後にホスト上のセキュリティ対策ソフトの無効化や OS 機能の改変による隠蔽化が増加している．そのため，ネットワーク型侵入検知システム (IDS) を応用した感染ホストの検出 [1] やボットの活動モデルを利用した検知手法 [2] が運用，研究されている．しかし新しいマルウェアは次々に出現しており [3]，耐解析技術も実装されているため [4]，実験環境においてマルウェアを動作させることで活動形態や通信データを取得する動的解析が重要となる．

動的解析において得られたマルウェアの通信データを解析する際，特定のプログラムの動作解析を目的として作成されたソフトウェアは少なく，既存のソフトウェアを組み合わせた解析となる．しかし，各ソフトウェアの出力形式に互換性がないなどの問題から効率的な解析が難しい．本論文では動的解析によって得られたマルウェアの通信データ解析に着目し，解析に必要となる要件と，要件にもとづいた実装の機能について述べる．この実装は，ネットワークセキュリティ研究者がマルウェアの検知に必要となる情報の迅速な分析を支援を目的とする．

2 マルウェアの通信データの解析における要求事項と実装

本実装は筆者らの過去の実装 [5] を拡張した構成となっている．マルウェア解析における要求事項と，それに対応する実装についてまとめる．

2.1 通信の相関関係分析

マルウェアは複数の通信によって，感染の拡大や攻撃者との情報交換を実行する．特にボットはコマンド&コントロールサーバ (C&C サーバ) との通信によって攻撃者からの指示を受信するため，通信の相関関係に着目することで各通信の内容を推測できる．例えば，時系列にそって発生した通信を調査することで，命令コマンドの特定が容易になる．IRC のように長期的に接続する通信の場合はパケット単位で相関関係を調査するのが望ましいが，tcpdump[6] のように全ての通信をパケット単位で示すと全体像の把握が困難になる．しかし，一方で argus[7] のように全てをセッションで集約するとパケットに含まれるペイロードの発生時刻を把握するのが難しくなり，調査を妨げてしまう．

通信の相関関係を示すために，セッションごとに表示するプロトコルとパケットのペイロードを表示するプロトコルを選択可能とした．例えばボットの通信を解析する際，IRC のみをパケットとして表示することによって，マルウェアの転送や攻撃の指示のトリガとなるパケットを推測するのが容易となる．これによって，特定のペイロードやセッションの相関関係を特定するのが支援される．

2.2 通信の集約化

マルウェアは効率的に感染を拡大させるために，大量の外部ホストに対して調査，攻撃を実施する．そのため，感染活動中は大量のセッションが発生し，重要な通信の認識を困難にする．ただし，感染活動そのものは重要な活動の 1 つなので調査結果から除外するのも望ましくない．

感染活動やポートスキャンなどの際に発生する大量の通信を適切に扱うため，自動的に通信を集約化する機能を実装した．これは短期間に同一のポート番号に対して複数のアドレスに接続要求を送信する感染活動や，短期間に同一のアドレスに対して複数のポート番号へ接続要求を送信するポートスキャンを集約する．この機能は任意で有効化，無効化できるため，解析者が状況に応じて選択できる．

2.3 特定の通信の発見

既知のマルウェアに関連する通信内容の発見は，通信の解析において重要な手がかりとなる．例えば，既知の命令コマンドや Microsoft Windows の実行形式 [8] にもとづいたデータを含むセッションやペイロードの出現が挙げられる．これらの検知は一般的な IDS で実装されている機能だが，通信データ解析ソフトウェアの機能としても必要となる．

本実装の元となった実装 [5] はシグネチャを元にしたイベント検知の機能を有する．そのため，パケットに

Implementing traffic analysis software for studying malware

Masayoshi MIZUTANI†, Keiji TAKEDA†and Jun MURAI‡
†Graduate School of Media and Governance, Keio University 252-8520, Kanagawa, Japan
‡Faculty of Environment and Information Studies, Keio University 252-8520, Kanagawa, Japan
{mizutani, keiji, jun}@sfc.wide.ad.jp

```
[ 4 | 0.357 | 60:38.33] 192.168.0.101:1031 -> 115.126.2.121:65520 (TCP:IRC) [359 byte (104 pkt) <-> 706 byte (71 pkt)]
[ 4 | 0.557 |PACKET] (IRC) To >> NICK aihrwcjh.USER r020501 . . :-
[ 4 | 0.858 |PACKET] (IRC) To >> .JOIN \&virtu.
[ 4 | 1.607 |PACKET] (IRC) To << :* PRIVMSG aihrwcjh :!get http://ntkrnlpa.cn/wr.jpg..
[ 5 | 2.375 |  0:00.48] 192.168.0.101:1030 -> 10.0.0.2:53 (UDP:DNS) DNS: ntkrnlpa.cn. (115.126.2.120)
[ 6 | 2.780 | 59:42.51] 192.168.0.101:1032 -> 63.173.172.98:6668 (TCP:IRC) [1485 byte (42 pkt) <-> 529 byte (26 pkt)]
[ 7 | 2.858 |  0:01.75] 192.168.0.101:1033 -> 115.126.2.120:80 (TCP:HTTP) HTTP: GET ntkrnlpa.cn/wr.jpg (200 image/jpeg,
                        37974 byte) *** Detect Windows Executable File ***
[ 6 | 3.067 |PACKET] (IRC) To >> NICK SR1-114487528..USER vkrngphfu 0 0 :SR1-114487528..
[ 8 | 3.097 |  0:00.00] 192.168.0.101:1028 -> 239.255.255.250:1900 (UDP:UPNP) [0 byte (0 pkt) <-> 133 byte (1 pkt)]
[ 6 | 3.359 |PACKET] (IRC) To << :ns1.xxx.us 001 SR1-114487528 :Cisco          ..:ns1.xxx.us 005 SR1-114487528
[ 6 | 3.359 |PACKET] (IRC) To >> USERHOST SR1-114487528..
[ 6 | 3.651 |PACKET] (IRC) To << :ns1.xxx.us 302 SR1-114487528 :SR1-114487528=+vkrngphfu@60-62-214-163.rev.home.ne.jp    ..
[ 6 | 3.651 |PACKET] (IRC) To >> MODE SR1-114487528 +x+i..JOIN #cc dcpass..USERHOST SR1-114487528..MODE SR1-114487528 +x+i..
                        JOIN #cc dcpass..
[ 6 | 3.940 |PACKET] (IRC) To << :SR1-114487528!vkrngphfu@60-62-214-163.rev.home.ne.jp JOIN :#cc..:ns1.xxx.us 332 SR1-114487
                        528 #cc :xvv asn139 150 0 0 -b -r -s.
[ 9 | 4.039 | 59:41.13] 192.168.0.101:1034 -> 192.168.231.125:139 (TCP:TCP)  === Aggregated Session: 168426 (Spread Scan) ===
[19 | 4.518 |  0:00.33] 192.168.0.101:1030 -> 10.0.0.2:53 (UDP:DNS) DNS: wrsnav.wwlax.com. (62.90.134.24)
```

図 1: 本実装によるマルウェアの通信データ解析結果例

含まれるヘッダ情報やペイロード部分のパターンマッチによって，指定した条件に一致するセッションやペイロードを示す機能を実装した．

3 本実装の有効性

図 1 に本実装による解析結果例を示す．図中の解析結果は AVG[9] によって Win32/Virut と判定された検体を動的解析した際の通信データである．本ソフトウェアはテキスト形式と HTML 形式の出力に対応しているが，今回はテキスト形式で出力している．各行がセッションもしくはパケットのデータを示しており，左からセッション ID，観測時刻，セッション継続時間もしくはパケットのペイロードデータを示す *PACKET* の表示，送信元，送信先 IP アドレスとポート番号，プロトコル情報となっている．パケットのデータは">>"がサーバへの送信，"<<"がクライアントへの送信を表している．

本解析では IRC はセッションだけではなくパケットのペイロード情報も表示しており，これによって C&C サーバから送信される命令と他のセッションとの相関関係が明確になる．まず上から 4 行目の IRC パケットは，サーバからクライアントに対して URL を含むメッセージを送信している．この直後，5 行目の HTTP セッションによって指定された URL のファイルをダウンロードしており，!get というメッセージがファイルのダウンロードを指示するコマンドであるとわかる．また，7 行目には Microsoft Windows の実行形式ファイルが含まれていることを示すイベントとして，*Detect Windows Executable File* という検知結果が示されている．URL の拡張子は jpg となっているが，パターンマッチによってファイル形式を判定しており，実際には Windows の実行ファイルであるマルウェア本体がダウンロードされているとわかる．さらに，下から 2 行目の *Aggregated Session...* というメッセージは，直前の行の `asn139` というコマンドによって実行されていると予想されるスキャン行為を集約して表示している．この集約化によって 168,426 件のセッションが 59 分 41 秒の間に発生していることを示しつつ，他のセッションを調査するための妨げになっていないことがわかる．

4 まとめ

本稿はマルウェアの動的解析によって得られた通信データを効率的に解析するソフトウェアの要求と実装について述べた．また，実際の通信データの解析結果を示し有効性を示した．現在は解析結果を表示できる形式が限定されているため，よりユーザビリティを考慮したユーザインターフェースの設計，実装が必要であると考える．

参考文献

[1] Richard Bejtlich. *EXTRUSION DETECTION*, chapter 1-10. Addison-Wesley, 2005.

[2] Guofei Gu, Phillip Porras, Vinod Yegneswaran, Martin Fong, Wenke Lee. BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. *Usenix Security Symposium 2007*, 2007.

[3] Cyber Clean Center. 2008 年 08 月度　サイバークリーンセンター活動実績, Aug 2008. `https://www.ccc.go.jp/report/200808/0808monthly.html`.

[4] 鵜飼裕司, 小林偉昭, 中野学. 脆弱性を利用した標的型攻撃のための解析ツール. **マルウェア対策研究人材育成ワークショップ** *2008*, Oct 2008.

[5] Masayoshi Mizutani, Shin Shirahata, Masaki Minami, Jun Murai. ROOK: Multi-Session based Network Security Event Detector. *SAINT 2008*, Jul 2008. `http://rook.sourceforge.net/`.

[6] LBNL's Network Research Group. TCPDUMP. `http://www.tcpdump.org/`.

[7] LLC QoSient. Argus, 2000. `http://qosient.com/argus/`.

[8] Eelco Visser. PC Executable Format. Program-Transformation.Org: The Program Transformation Wiki, Apr 2000. `http://www.program-transformation.org/Transform/PcExeFormat`.

[9] Grisoft. AVG Free Edition. `http://free.grisoft.com/`.