研究用データセット「動的活動観測 2016」

寺田真敏[†1]　佐藤隆行[†1]　堀健太郎[†1]
吉野龍平[†2]　萩原健太[†2]

概要：マルウェア検体の解析では，指令サーバ接続，情報窃取，バックドアなどの機能の存在や挙動把握に重点が置かれ，攻撃者の行動という視点で把握や解析することはなかった．しかし，組織内ネットワークへの侵害活動においては，攻撃者の存在，攻撃者のアトリビューションを意識する必要がある．本稿では，電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測とその研究用データセット「動的活動観測 2016 (BOS_2016)」について報告する．

キーワード：動的活動観測，マルウェア，指令サーバ

Overview of Research Data Set "Behavior Observable System 2016"

Masato Terada[†1], Takayuki Sato[†1], Kentaro Hori[†1],
Ryohei Yoshino[†2] and Kenta Hagihara[†2]

Abstract: Under the analysis of malware, mainly it focuses on the functions and behaviors of malware itself such as C&C server connection, information leak, backdoor and etc. The analysis of malware does not include the viewpoint of actions of threat actors. But under the targeted attack such as APT, we should focus on the actions of threat actor and attribution, too. In this paper, firstly we will describe the overview of our research data set "BOS_2016" for the countermeasures of targeted attack age. Secondly, we will introduce the typical case of targeted attack in BOS_2016.

Keywords: Behavior Observable System, Malware, C2 server

1. はじめに

マルウェアを用いたサイバー攻撃は技術を継承しつつ，活動形態を大きく変化させながら進化してきている．1999 年頃はウイルス添付型メール，2001 年頃は脆弱性を利用するネットワーク型ワーム，2004 年頃は遠隔操作可能なボットが流布した．2008 年頃からは，ブラウザが利用するプラグインやアプリケーションの脆弱性を利用した Web 感染型へと変遷してきた．2010 年に入ると，電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動である標的型攻撃へと進化し，APT(Advanced Persistent Threat)という名称で広く知れ渡るようになった．APT は，「特定組織を対象とし(標的型攻撃)，組織内ネットワークを活動基点とする(潜伏型手法の)侵害活動」の総称である．特に，侵入したシステムを遠隔から操作するためのプログラム，遠隔操作ツール(RAT: Remote Access Trojan/Remote Administration Tool)は，APT 世代の標的型攻撃において重要な役割を果たしている．

本研究の目的は，多様化と巧妙化するサイバー攻撃に対抗するため，攻撃者の行動観測を通したサイバー攻撃活動分析と共に，攻撃者のアトリビューションに着目した動的活動観測を進めることにある．本稿では，2015 年に実施した，電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測 BOS(Behavior Observable System)とその研究用データセット「動的活動観測 2016 (BOS_2016)」について報告する．

2. 関連研究

2.1 アトリビューション

サイバー攻撃の分野において,アトリビューションとは,攻撃者や攻撃仲介者の同一性や場所の特定を意味する[1].文献 1)では，アトリビューションのための技術として，トレースバック，モニタホストの導入，ハニーポット/ハニーネットの活用などを挙げている．文献2)では，マルウェアのメタデータ,埋め込みフォント,遠隔操作ツールの設定,攻撃者の行動パターンなどが利用できるとしている.また,脅威情報構造化記述形式 STIX(Structured Threat Information eXpression)[3]でも，サイバー攻撃で狙っているソフトウェア，システムや設定の弱点，攻撃を検知するための事象だけではなく，攻撃者の行動や手口，サイバー攻撃に関与している人／組織など，攻撃者の存在が意識したサイバー攻撃活動の構造化を試みている．

†1 (株)日立製作所, Hitachi Ltd.
†2 トレンドマイクロ(株), Trend Micro Incorporated.

2.2 情報活用によるサイバー攻撃への対応

(1) サイバー攻撃への早期対応

ばらまき型の標的型攻撃の場合，複数の組織が同様の手口で被害に合うことがあることから，脅威情報構造化記述形式 STIX などを用いた情報活用の適用分野となる．IPA を情報ハブとして，参加組織間で情報共有を行い，高度なサイバー攻撃対策に繋げていく取り組みであるサイバー情報共有イニシアティブ(J-CSIP)では，2016 年四半期の情報提供件数は 1,818 件で，そのうち，1,584 件が日本語のばらまき型メールの情報提供であったとしている[4]．また，文献[5]では，標的型攻撃を早期検知するための情報共有について検討している．この中で，早期検知のためには，共有する情報は「標的型攻撃そのものの有無を判定できる情報」として，メール送信元 IP アドレスやメールの件名，C&C 接続先 IP アドレス等を挙げ，標的型攻撃の侵害の進行の速さから，より早く共有すべきであるとしている．

(2) 情報活用基盤

サイバー攻撃活動の攻撃から対策までを構造化し記述する XML 仕様である脅威情報構造化記述形式 STIX，STIX などで記述した情報を交換するための検知指標情報自動交換手順 TAXII(Trusted Automated eXchange of Indicator Information)[6]を実装した情報活用基盤が普及しはじめている．米国では，サイバーセキュリティ法(Cybersecurity Act of 2015)の成立に伴い，2016 年 3 月，官民連携の一環の取り組みとして，STIX，TAXII を利用し観測事象の中から検知に有効なサイバー攻撃を特徴付ける指標を交換するための AIS(Automated Indicator Sharing)[7]が稼働し始めている．

3. 研究用データセット BOS_2016

本章では，研究用データセット「動的活動観測 2016 (BOS_2016)」の概要について述べる．

3.1 動的活動観測

(1) 目的

動的活動観測 BOS の目的は，攻撃者のアトリビューションの一部として，マルウェアの挙動に加えて，どのような操作をしたのか，どのようなファイルにアクセスしたのかなど攻撃者の行動と組合せていくことで，攻撃者行動視点で脅威の特徴付けを試みることにある．

(2) 観測環境

動的活動観測 BOS では，組織内ネットワーク自身を模擬した観測環境を構築している(図 1)．この環境は，組織内ネットワークのパソコンにおいてマルウェア感染が発生した以降を対象に，実インターネット上の攻撃者が組織内ネットワークで試みるサイバー攻撃活動を観測するシステムとなっている．クライアントは，標的型攻撃メールに添付されたマルウェア検体を実行するパソコンであり，プロキシ経由／プロキシ経由なしのいずれかの形態で，実インターネットへのアクセスが可能である．

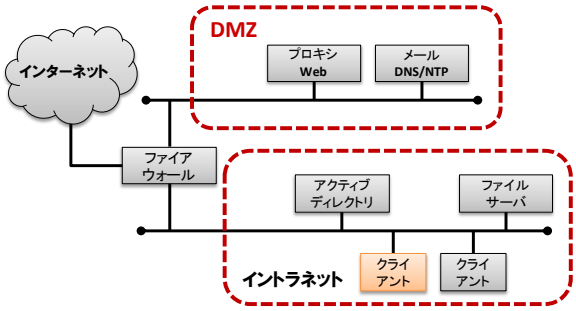

図 1：動的活動観測環境の概要図

3.2 観測事例

本節では，2015 年に実施した，電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測 BOS とその研究用データセット「動的活動観測 2016 (BOS_2016)」[8]について述べる(表 1)．

BOS_2016 では，新たに，表 2 に示す進行度という動的活動観測における攻撃活動の進み具合の区分を設け，標的型攻撃の段階に応じた研究用データセットとなるよう工夫をしている．

表 1：動的活動観測 2016(BOS_2016)の観測事例

#	観測期間		マルウェア検体名	進行度
	開始	終了		
e04	2015/08/06	2015/08/20	BKDR_EMDIVI.MSB	7
e12	2016/02/12	2016/02/16	BKDR_EMDIVI.L	5
e20	2016/02/15	2016/02/18	TROJ_PLUGX.AYM	5
e43	2016/02/12	2016/02/16	TROJ_EMDIVI.AE	1
e70	2016/02/15	2016/02/18	BKDR_PLUGX.DUKOA	4
e435	2016/03/28	2016/03/30	BKDR_PLUGX.DUKOQ	4

表 2：動的活動観測における進行度

進行度	区分		内容
1	通信発生なし		検体の実行が不可能 or マルウェアではない
2			検体実行するも，通信発生無し
3	検体が動作し，通信が発生	C2 サーバと攻撃通信成立せず	C2 サーバの名前解決不可
4			C2 サーバへ SYN パケット送信のみ
5			C2 サーバと通信成立しない (HTTP のステータスコード =403, 404, 503 など)
6		C2 サーバと攻撃通信成立	攻撃(活動/操作)観測できず．
7			攻撃(活動/操作)観測できた．
8			攻撃(活動/操作)観測でき，継続的に観測できた．

これまでの BOS_2014～BOS_2015 では，検体が動作し，指令サーバ(以降，C2 サーバ)との通信が発生した後，動的観測環境で攻撃者による活動を観測できた事例のみ(進行度 7 以上)を研究用データセットとしてきたのに比べてバリエーションを増やすことができている．

(1) Case e04

標的型攻撃において，組織内ネットワークでの一連の侵害活動を観測した事例である(表 3).

- メールサーバのアカウントとパスワード情報の窃取のために，PowerShell を使用している点に特徴がある．

(2) Case e12，e20

標的型攻撃において，組織内ネットワークでマルウェアが活動を開始し，C2 サーバとの TCP コネクションを確立できたが，HTTP のステータスコードが 403(Forbidden)，404(Not Found)，503(Service Unavailable)などで，C2 サーバとの攻撃通信が成立しない事例である．

(3) Case e70，e435

標的型攻撃において，組織内ネットワークでマルウェアが活動を開始し，TCP SYN パケットを送付するが，外部との TCP コネクションを確立できない事例である．

表 3：Case e04＜観測事象＞

Date	Time	Observable event
8/6	20:43	検体(.exe)を実行。C&Cサーバとの接続が確立。
8/7	10:43	**powershellの実行** powershell IEX (New-Object Net.WebClient). DownloadString('https://raw.githubusercontent. com/sakuramana/testpro/master/pass.ps1');[Program]::Ru n()
	10:43	**pass.ps1のダウンロード**
	10:43	**pass.ps1の実行**
	14:08	taskkillの実行失敗 (taskkill /pid 2492 /f) hostA%2A4292&1&dGFza2tpbGwgL3BpZCAyNDkyIC9m 30 ※プロセスIDが間違っているため、プロセス停止せず
	14:19	taskkillの実行 (taskkill /pid 4292 /f) hostA%2A4292&1&dGFza2tpbGwgL3BpZCA0MjkyIC9m 54

3.3 考察

本節では，研究用データセットとして，進行度 1～6 の事例を拡充していくにあたっての課題を明らかにしていくため，「動的活動観測 2016 (BOS_2016)」として用意した事例をトラフィックの視点から可視化する．

観測期間中にマルウェア感染端末から送出される TCP SYN パケット送出割合を，送信先 IP アドレス：ポート番号の組合せを見てみると，マルウェアが C2 サーバとの TCP コネクションを確立できた進行度 5(図 2，図 3)と，できない進行度 4(図 4，図 5)との間では，TCP SYN パケット送出割合の傾向に明らかな違いがある．進行度 4 の場合，送出割合から C2 サーバを特定可能である．一方，進行度 5 の場合，破線枠部分が C2 サーバとの通信にあたるが，送出割合から C2 サーバを特定しにくい．

また，特定の C2 サーバへの TCP SYN パケット送出件数を時間毎にみても，TCP SYN パケット送出割合と同様に，進行度 5(図 6，図 7)と進行度 4(図 8，図 9)とでは明らかな違いが見られる．

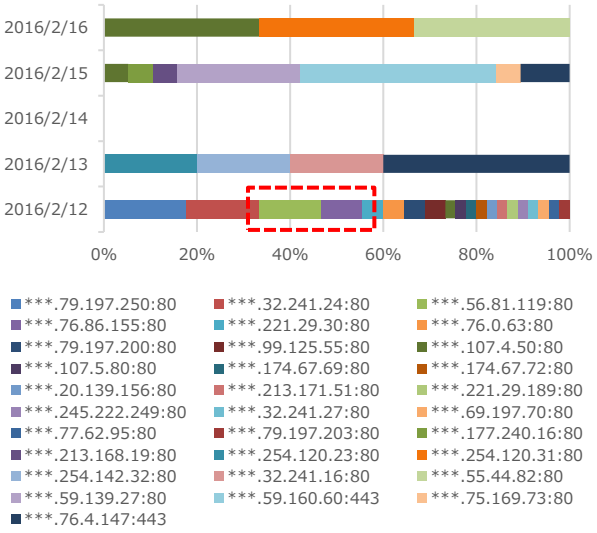

図 2：TCP SYN パケット送出割合(Case e12，進行度 5)

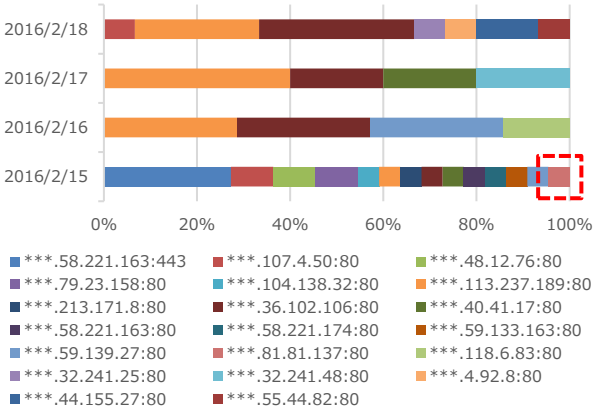

図 3：TCP SYN パケット送出割合(Case e20，進行度 5)

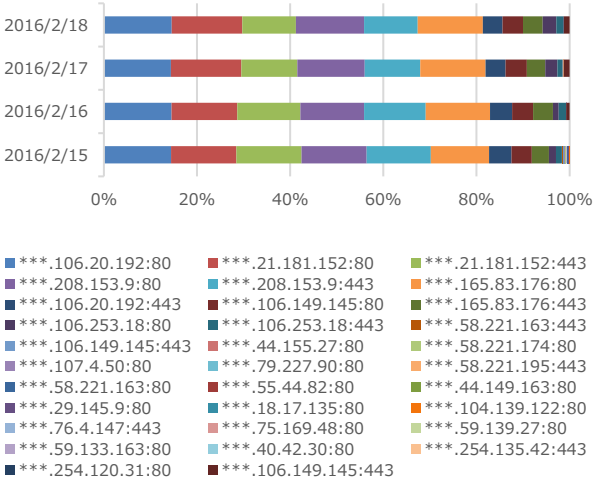

図 4：TCP SYN パケット送出割合(Case e70，進行度 4)

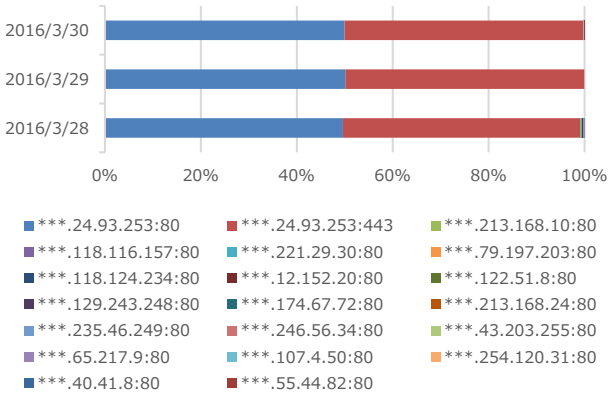

図 5：TCP SYN パケット送出割合(Case e435，進行度 4)

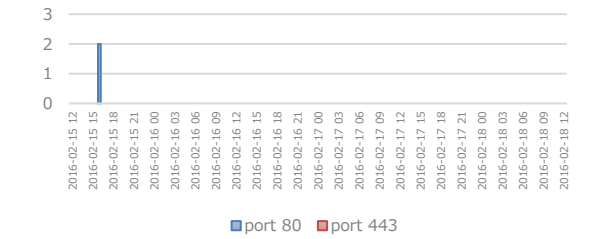

図 6：TCP SYN パケット送出件数(Case e12，進行度 5)

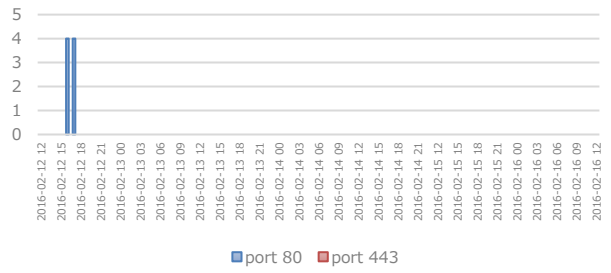

図 7：TCP SYN パケット送出件数(Case e20，進行度 5)

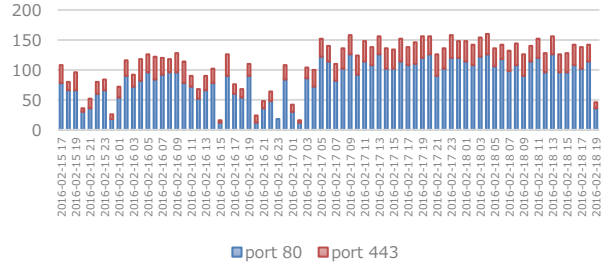

図 8：TCP SYN パケット送出件数(Case e70，進行度 4)

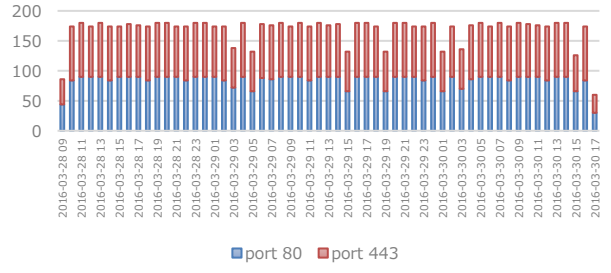

図 9：TCP SYN パケット送出件数(Case e435，進行度 4)

BOS_2016 から，研究用データセットの環境情報として，検体実行機器の IP アドレスを付記しているが，どこまで分析した結果を添付しておくと良いのかは，拡充にあたっての継続的な課題である．

4. おわりに

本稿では，電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測 BOS(Behavior Observable System)とその研究用データセット「動的活動観測 2016 (BOS_2016)」について報告した．

研究用データセット「動的活動観測 2016 (BOS_2016)」は，攻撃者の行動観測を通したサイバー攻撃活動分析と共に，攻撃者のアトリビューションに着目したデータセットである．「動的活動観測 2016 (BOS_2016)」では，攻撃者行動視点での特徴付けとして，標的型攻撃において，組織内ネットワークでの一連の侵害活動を観測した事例だけではなく，進行度という動的活動観測における攻撃活動の進み具合の区分を設け，標的型攻撃の段階に応じた事例を含んでいる．

今後の課題は，研究用データセット「動的活動観測」として，各進行度の事例拡充など，サイバー攻撃に関する脅威情報データベースと連携した「動的活動観測」の推進を検討していきたいと考えている．

謝辞

本研究は総務省実証事業「サイバー攻撃解析・防御モデル実践演習の実証実験の請負」で実施したものである．本研究を進めるにあたって有益な助言と協力を頂いた関係各位に深く感謝申し上げる．

参考文献

1) David A. Wheeler, et.al.：Techniques for Cyber Attack Attribution (Institute for Defense Analysis, IDA Paper)(2003.10)
2) FireEye：高度なサイバー攻撃の痕跡 ～攻撃者の素性を特定する 7 つの手がかり～(2013)
3) Structured Threat Information eXpression (STIX), http://stix.mitre.org/
4) サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2016 年 4 月～6 月], https://www.ipa.go.jp/security/J-CSIP/
5) 岡田周平，後藤厚宏．標的型攻撃の早期検知に向けた STIX/TAXII の活用に関する検討．情報処理学会第 78 回全国大会 6V-02
6) Trusted Automated eXchange of Indicator Information (TAXII), http://taxii.mitre.org/
7) Automated Indicator Sharing (AIS), https://www.us-cert.gov/ais
8) 高田、寺田、村上、笠間、吉岡、畑田：マルウェア対策のための研究用データセット ～MWS Datasets 2015～，情報処理学会 CSEC/SPT 合同研究発表会(2016.07)