研究用データセット「動的活動観測 2015」

寺田真敏[*1]　堀健太郎[*1]　成島佳孝[*1]
吉野龍平[*2]　萩原健太[*2]

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わ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 2015 (BOS_2015)」について報告する．

Overview of Research Data Set "Behavior Observable System 2015"

Masato Terada, Kentaro Hori, Yoshitaka Narishima
Ryohei Yoshino and Kenta Hagihara

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_2015" for the countermeasures of targeted attack age. Secondly, we will introduce the typical case of targeted attack in BOS_2015.

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わ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，2014 年に実施した，電子メールと遠隔操作ツールとを組合わ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 2015 (BOS_2015)」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

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

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．

2.2 遠隔操作ツール

遠隔操作ツールは，「攻撃側発呼型」「攻撃側着呼型」の世代に分けることができる(図 1).

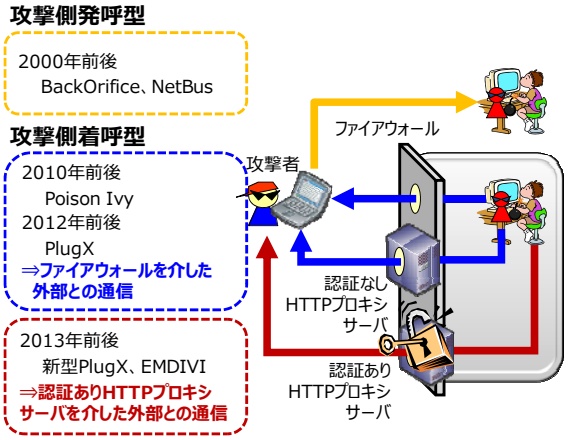

図 1：遠隔操作ツール(RAT)の変遷

(1) 攻撃側発呼型

Back Orifice, NetBus, Back Orifice 2000(BO2K)に代表される攻撃側発呼型は，クライアント(攻撃者 PC)からサーバ(攻撃対象 PC)に通信確立した後，攻撃者 PC から遠隔操作を指示する．

(2) 攻撃側着呼型

Poison Ivy，PlugX，EMDIVI に代表され，標的型攻撃に用いられる攻撃側着呼型は，サーバ(攻撃対象 PC)からクライアント(攻撃者 PC)にコネクション確立した後，攻撃者 PC から遠隔操作を指示する．通信確立の方向が反転した要因の一つに，インターネットとイントラネットとの境界にファイアウォールが設置されたり，PC にパーソナルファイアウォールが導入されたりしたことが挙げられる．

攻撃側着呼型には，利用される遠隔操作ツール，インターネット上の攻撃者 PC に向けて外部との通信確立する際に影響を与えるポート番号，通信プロトコル，プロキシ対応の点から，次に示す特徴が見られる[4][5].

- 利用される遠隔操作ツール
  Poison Ivy が減少し，PlugX，EMDIVI は増加傾向にある(図 2).
- 外部との通信確立に使用するポート番号
  一般的な 53/tcp，80/tcp，443/tcp が選択され，複数のポート番号を利用している．
- 通信プロトコル
  ポート番号に対応した既知プロトコル(HTTP，HTTPS など)と独自プロトコルを使用している(図 3).
- プロキシ対応
  攻撃対象 PC が接続されている多様なネットワーク構成下においても，外部との通信確立を可能とするために，プロキシ構成に対応．新型 PlugX，EMDIVI においては，プロキシの認証情報を窃取するため，設定情報やブラウザの通信を盗聴する機能を実装し，認証プロキシ構成に対応している．

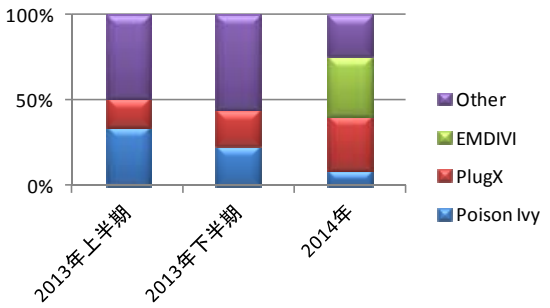

図 2：遠隔操作ツールの種別

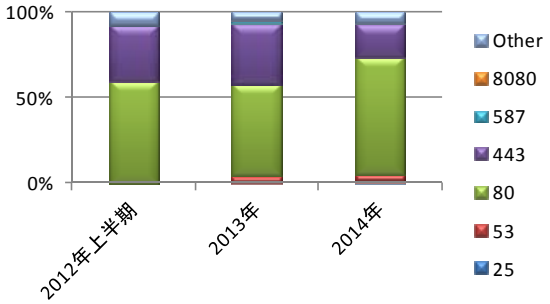

図 3：外部との通信確立に使用するポート番号

3. 研究用データセット BOS_2015

本章では，研究用データセット「動的活動観測 2015 (BOS_2015)」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わせていくことで，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 4)．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．

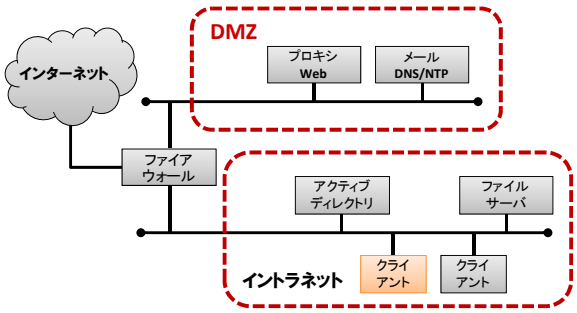

図 4：動的活動観測環境の概要図

3.2 観測事例

本節では，2014 年に実施した，電子メールと遠隔操作ツールとを組合わ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 2015 (BOS_2015)」[6]について述べる(表 1)．

表 1：動的活動観測 2015(BOS_2015)の観測事例

#	観測期間		マルウェア検体名
	開始	終了	
d18	2014/10/06	2014/11/07	BKDR_EMDIVI.I
d19	2014/10/06	2014/11/07	BKDR_EMDIVI.F
d33	2014/12/08	2014/12/22	BKDR_PLUGX.DUKLR
d37	2015/01/23	2015/02/02	BKDR_EMDIVI.AB

(1) Case d18

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 2)．

- ネットワーク環境の調査，端末調査，他端末内の情報探索，Active Directory(以降，AD)情報の窃取，C&C サーバへのファイルアップロード
- AD のアカウント情報をインポート/エクスポートする csvde.exe の使用

表 2：Case d18＜観測事象＞

Date	Time	Observable event
10/06	15:43	検体(医療費通知のお知らせ.exe)を実行し、ファイルが2つ(leassaq.exe、kptl.doc)が生成されC&Cサーバとの接続が確立。
	22:42 | 23:32	C&Cサーバとの接続確立より7時間後、反応あり。攻撃者がプロセス終了処理、ただ、プロセス名を間違え、正しく終了せず。1時間後、正しい名前で終了処理を実施。
10/07		攻撃者によるコマンド操作でのプロセス終了のみ。
10/09	15:14 | 15:48	1回目の攻撃発生。攻撃者は、実施端末だけでなく、他端末のシステム構成情報やディレクトリ情報を確認。また、実施端末に設置していたおとりファイルを窃取。
10/10		攻撃者によるコマンド操作でのプロセス終了のみ。
10/16	20:19 | 21:50	2回目の攻撃発生。1回目の攻撃と同様に、構成情報・ディレクトリ確認や、ファイル窃取を実施。また、端末に不正ファイルをダウンロードし、ADに接続を行ってユーザー情報などの構成情報をファイル化し窃取。
10/17	10:36 | 11:02	3回目の攻撃発生。ADの構成情報やドメイン参加者を確認したほか、１回目と同様に構成情報の確認やおとりファイルの窃取を実施。
10/18		攻撃者によるコマンド操作なし(C&Cサーバに一定回数以上接続を行ったら自身でプロセスを終了する仕組み)

(2) Case d19

Case d18 と類似の検体を，同時期観測した事例である(表 3)．

- メール情報を取得するツール(CallMail.exe)が送り込まれ，メール情報を 1.tm として出力した後，内容確認が行われた(表 4)．ただし，これ以降，継続的な侵害活動は発生しなかった．

(3) Case d33

標的型攻撃において，組織内ネットワークでの内部感染拡大活動を観測した事例である(表 5)．

- SAM，AD などからアカウントのハッシュ情報を取り出すツール gsecdump.exe を実行後，取得したハッシュ情報を元に，パスワードを特定し，net use コマンドを使用(表 6)
- 組織内ネットワークでの内部感染活動として，端末間での PlugX 亜種のコピー
- AD のアカウント情報をインポート/エクスポートする csvde.exe の使用

(4) Case d37

標的型攻撃において，組織内ネットワークでのセキュリティツールの導入有無を判断する手段の一つとして，Recent フォルダの確認を観測した事例である(表 7).

- 調査ツールのログのリンクファイルを C&C サーバにアップロードし，取得したファイルから実ファイルンのパスを特定し，dir コマンドで確認(表 8)

表 3：Case d19＜観測事象＞

Date	Time	Observable event
10/06	18:45	検体(医療費通知のお知らせ.exe)を実行し、ファイルが2つ(leassnq.exe、kptl.doc)が生成されC&Cサーバとの接続が確立。
	22:30 | 22:41	C&Cサーバとの接続確立より4時間後、反応。１回目の攻撃発生。 実施端末だけでなく他端末のシステム構成情報や、ディレクトリ情報を確認。
10/07		攻撃者によるコマンド操作でのプロセス終了のみ。
10/08	17:02 | 17:12	２回目の攻撃発生。攻撃者は、１回目と同様に確認を行い、プロセス終了処理を実施。
10/09		攻撃者によるコマンド操作でのプロセス終了のみ。
10/14	11:26 | 11:33	３回目の攻撃発生。攻撃者はメールの構成情報などを窃取するスパイウェアを端末にダウンロード。
10/15		攻撃者によるコマンド操作なし (C&Cサーバに一定回数以上接続を行ったら自身でプロセスを終了する仕組み)

表 4：Case d19＜メール情報の参照＞

Date	Time	Observable event
10/14	11:27	**CallMail.EXEダウンロード** upload "d_CallMailPs.EXE" "%temp%¥CallMail.EXE"
	11:29	**ディレクトリ情報取得** cmd /c dir "%temp%¥*.exe" /o-d
	11:29	**CallMail.EXE起動** CallMail.EXE /stext 1.tmp
	11:30	**ファイル内容取得** cmd /c type 1.tmp
	11:30	**CallMail.EXE削除** cmd /c del CallMail.EXE /q

表 5：Case d33＜観測事象＞

Date	Time	Observable event
12/08	15:43	検体(結果報告.exe)を実行。C&Cサーバとの接続が確立。
12/10	10:04	C&Cサーバからの応答を確認。
	10:06	CMD.EXEを起動。(遠隔操作による攻撃の開始) ipconfig /all を実行し、ネットワーク設定を確認。 Netコマンドを用いて共有リソースを確認、使用。
	10:11	ドメイングループの確認を実行。
	10:17	実行端末(hostA)で20141113-443.exe,gsecdump.exeがドロップ、実行。
	10:28	AD(hostB)を共有資源として接続
	10:39	AD(hostB)に対しgsecdump.exeを実行、C:¥Users¥Public¥Videos¥a.txtを作成。
	10:44	別端末(hostC)を共有資源として接続。 Netコマンドを用いて共有リソースを確認、使用。 ドメイングループの確認を実行。また、Windows.exeをドロップ。
	10:51	AD(hostB)を共有資源として再接続。
	11:13	自ドメイン、自ネットワーク(*.*.*.1～255)にpingを発信。TTLも確認。
	11:40	csvde.exeをドロップさせ実行、AD情報をcsvファイルにて出力。 AD情報を元に再度端末へpingを発信。 この間に共有資源であるAD(hostB, hostD)にWindows.exeをコピー、実行。
	14:44	net use * /del /yes を実行し、共有資源の設定を全削除。
	14:45	検体(結果報告.exe)を実行。C&Cサーバとの接続が確立。
	15:59	netstat の実行を最後に操作が終了(通信は継続)

表 6：Case d33＜ハッシュ情報の取得＞

Date	Time	Observable event
12/10	10:17	gsecdump.exeの生成
	10:17	CMD.EXEの起動
	10:17	gsecdump.exe -a
	10:17	gsecdump.exe -a
	10:18	net user
	10:18	net group "domain admins" /domain
	10:27	net view
	10:28	net use ¥¥hostB¥ipc$ "P@ssw0rd" /u:BOS¥Administrator

表 7：Case d37＜観測事象＞

Date	Time	Observable event
1/23	12:35	検体(2015.01.19.102850.exe)を実行。C&Cサーバとの接続が確立
1/24	12:47	C&Cサーバからの応答を確認。コマンドによる遠隔操作が行われる。
	12:47	whoami/net view/net group domain admins等を用いた環境調査
	12:54	ADのドライブ直下のディレクトリの捜索 ＋ 動的活動観測環境(検体実行環境)のIPをまとめたファイルをtypeコマンドにて確認
	13:00 | 13:17	IP情報を基に、各端末起動中のタスクやpingの応答確認を行う
	15:37	感染させた端末内のデスクトップやディレクトリの確認
	15:38	08012015_report.lnkのファイルを窃取
	15:40 | 15:45	攻撃者がプロセスキャプチャのログを確認
	15:48	攻撃者によりtaskkillが行われ、マルウェアのタスクが終了する

表 8：Case d37＜Recent フォルダの確認＞

Date	Time	Observable event
1/14	15:38	**ディレクトリ情報取得** cmd /cdir c:¥users¥HCG015~1.HIT¥AppData¥Roaming¥Microsoft¥Windows¥Recent
	15:38	**08012015_report.lnkのアップロード** downbg "c:¥users¥HCG015~1.HIT¥AppData¥Roaming¥Microsoft¥Windows¥Recent¥08012015_report.lnk" "08012015_report.lnk" "0" "0" "1024" "1"
	15:40	**ディレクトリ情報取得** cmd /cdir C:¥Program Files (x86)¥Trend Micro¥ProcessCapture¥ProcessCapture¥x64¥Report
	15:41	**ファイル内容取得** cmd /ctype C:¥Program Files (x86)¥Trend Micro¥ProcessCapture¥ProcessCapture¥x64¥Report¥24012015_report.log
	15:45	**ディレクトリ情報取得** cmd /cdir C:¥Program Files (x86)¥Trend Micro

3.3 考察

本節では，研究用データセット「動的活動観測 2015 (BOS_2015)」を対象に，遠隔操作を担当した攻撃者(以降，遠隔操作攻撃者)の行動について考察する．

3.3.1 観測期間中の行動時間

観測期間中の遠隔操作攻撃者の行動時間として，表 9 に，動的活動観測 2014 の 2 件，2015 の 4 件を対象に，遠隔操作を開始するまでの時間，遠隔操作の総時間を示す．なお，遠隔操作を開始するまでの時間は，マルウェア検体を実行してから，遠隔操作攻撃者が該当端末の遠隔操作を開始するまでの時間である．

表 9：観測期間中の行動時間

#	遠隔操作を開始するまでの時間	遠隔操作の総時間
c11	9 分	30 分
c21	1.5 時間	1.5 時間
d18	7 時間	3 時間
d19	4 時間	30 分
d33	38 時間	6 時間
d37	24 時間	30 分

3.3.2 Case d18 における行動分析

2014 年 9 月中旬頃に流布した医療費通知の偽装メールでの観測事例 d18 を対象に遠隔操作攻撃者の行動分析を試みる．

医療費通知の偽装メールは，健康保険組合などからの医療費通知メールを偽装し，ユーザのパソコンを遠隔操作可能な不正プログラム(検出名：BKDR_EMDIVI)に感染させようとする攻撃であった．医療費通知メールの添付ファイルには，文書アイコン偽装された実行形式の不正プログラムが含まれていた．動的活動観測 BOS では，パソコンが不正プログラムに感染した後，約 7 時間すると遠隔操作攻撃者が観測環境を訪れ侵害活動を開始し，活動を停止するまでの 12 日間のあいだに，3 回，計 3 時間ほどの活動を通して，システム構成やディレクトリ情報の確認，感染パソコンなどからファイルの窃取などを行う様子を観測している．

(1) コマンド操作ミスについて

10 月 6 日の 22:42～23:32 の間に，遠隔操作攻撃者は，表 10 に示すようなコマンド操作ミスをしている．ここで，leassnp.exe は同時期に観測を行った Case d19 で使用されていた不正なプログラムの名称である．遠隔操作攻撃者は，接続先に対して複数の不正なプログラムを使い分けており，そのために，コマンド操作を誤ったものと考えられる．

表 10：Case d18＜コマンド操作ミス＞

Date	Time	Observable event
10/6	22:42	**leassnp.exe停止(失敗)** cmd /c taskkill /im leassnp.exe /f
	23:29	**プロセス一覧取得** cmd /c tasklist /v
	23:32	**leassaq.exe停止** cmd /c taskkill /im leassaq.exe /f

感染した端末ではレジストリuserinit設定に基づきログオン時にleassaq.exeを自動起動し、特定時間帯に攻撃活動を開始する。また、攻撃活動の最後にはtasklistでプロセス一覧を取得し、taskkillでleassaq.exeを停止し、次回ログオン時まで攻撃活動をしない。このとき遠隔操作攻撃者は当該端末においてはtaskkill /im leassaq.exe /fのコマンドを実行し、プロセスを停止しなければならないところをtaskkill /im leassnp.exe /fというコマンドを実行し、プロセス終了に失敗していた。

(2) 1 回目の攻撃 (10 月 9 日 15:14～15:48)

1 回目の攻撃では，感染パソコンを基点とし，ファイル探索を中心とした活動を観測した．遠隔操作攻撃者は，端末に格納されているファイルを単純に全て取得するというわけではなく，デスクトップやマイドキュメントを手掛かりにしてファイル探索を試みている．

表 11：Case d18＜ファイル探索＞

Date	Time	Observable event
10/9	15:19	cmd /c dir C:¥Users¥ADMINI~1¥desktop
	15:20	cmd /c net view /domain:HITACHI
	15:21	cmd /c dir c:¥users
	15:21	cmd /c dir c:
	15:21	cmd /c dir ¥¥hostX¥c$
	15:21	cmd /c wmic logicaldisk get caption,providername,drivetype,volumename
	15:21	cmd /c dir C:¥Users¥ADMINI~1¥documents
	15:22	cmd /c dir d:
	15:22	cmd /c dir C:¥Users¥ADMINI~1¥desktop¥社外秘
	15:22	cmd /c dir C:¥Users¥ADMINI~1¥desktop¥secret
	15:23	cmd /c dir ¥¥hostX¥c$¥Users
	15:24	cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop
	15:24	cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop¥山本商事
	15:25	cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop¥sysinterna
	15:25	cmd /c dir "%temp%¥*.exe" /o-d
	15:25	dir "%temp%¥*.doc" /o-d7
	15:26	cmd /c dir "C:¥Users¥ADMINI~1¥AppData¥Roaming¥Microsoft¥Windows¥Start Menu¥Programs¥Startup"
	15:29	downbg "C:¥Users¥ADMINI~1¥desktop¥重要_中東地域の当社拠点情報.pdf" "11.pdf" "0" "0" "1024" "1"
	15:32	cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop¥DDA
	15:32	cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop¥DDI
	15:32	cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop¥DS
	15:33	cmd /c dir ¥¥hostY¥c$¥Users¥Administrator¥desktop
	15:34	cmd /c dir ¥¥hostY¥c$¥Users¥Administrator¥documents
	15:34	cmd /c dir ¥¥hostZ¥c$¥Users¥Administrator¥documents
	15:35	cmd /c dir ¥¥hostZ¥c$¥Users¥Administrator¥desktop
	15:35	cmd /c dir ¥¥hostZ¥c$¥Users¥Administrator¥desktop¥社外秘
	15:40	downbg "C:¥Users¥ADMINI~1¥desktop¥■■■との会合に関する事前ヒアリング.xlsx" "22.xlsx" "0" "0" "1024" "1"
	15:42	cmd /c copy C:¥Users¥ADMINI~1¥desktop¥■■■との会合に関する事前ヒアリング.xlsx %temp%¥1.xlsx /y
	15:42	downbg "%temp%¥1.xlsx" "1.xlsx" "0" "0" "1024" "1"

次に，フォルダやファイルの名称を手掛かりに，重要な情報が含まれる可能性が高いと思われるファイルの窃取を試みようとしている(表 11).

(3) 2 回目の攻撃 (10 月 16 日 20:19～21:50)

2 回目の攻撃では，行動範囲の拡大のための活動を観測した．遠隔操作攻撃者は，AD のアカウント情報をインポート/エクスポートするツール csvde.exe を用いて，AD のアカウント情報の窃取を試みている(表 12)．また，csvde.exe のダウンロード，実行，実行結果 1016.csv のアップロードという一連の操作の最後に，csvde.exe と 1016.csv を削除しており，活動の痕跡を消そうとしていることが伺える．

表 12：Case d18＜AD 情報の取得＞

Date	Time	Observable event
10/16	21:01	**csvde.exeダウンロード** upload "csvde.exe" "%temp%¥csvde.exe"
	21:03	**csvde.exe起動** C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥csvde.exe -f C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1016.csv –u
	21:03	**ディレクトリ情報取得** cmd /c dir C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1016.csv
	21:03	**1016.csvアップロード** downbg "C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1016.csv" "1016.csv" "0" "0" "1024" "1"
	21:16	**1016.csvファイル削除** cmd /c del C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1016.csv /q
	21:16	**csvde.exeファイル削除** cmd /c del C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥csvde.exe /q

表 13：Case d18＜ショートカットファイル＞

Date	Time	Observable event
10/17	10:57	cmd /c dir c:¥users¥*.doc* /s
	10:57	cmd /c dir c:¥users¥*.lnk* /s
	10:57	downbg "c:¥users¥administrator¥AppData¥Local¥Temp¥kptl.doc" "1.doc" "0" "0" "1024" "1"
	10:57	**ショートカットファイルのアップロード** downbg "c:¥users¥administrator¥AppData¥Roaming¥Microsoft¥Windows¥Recent¥国交正常化交渉における対外戦略_H260907.docx.lnk" "a.txt" "0" "0" "1024" "1"
	11:01	cmd /c dir C:¥Users¥administrator¥Documents¥
	11:01	downbg "C:¥Users¥administrator¥Documents¥国家安全保障戦略会議議事_H261001.xlsx" "m.xlsx" "0" "0" "1024" "1"
	11:01	downbg "C:¥Users¥administrator¥Documents¥UNSC executive branch agreement.pdf" "m.pdf" "0" "0" "1024" "1"
	11:02	**ショートカットファイルの実ファイルのアップロード** downbg "C:¥Users¥administrator¥Documents¥国交正常化交渉における対外戦略_H260907.docx" "a.docx" "0" "0" "1024" "1"

遠隔操作攻撃者がアクセスした動的活動観測下のパソコン数は，AD のアカウント情報の窃取前後で，3 台から 5 台に増えている．このことから，窃取した情報を用いて行動範囲の拡大につなげたと推定できる．

(4) 3 回目の攻撃 (10 月 17 日 10:36～11:02)

3 回目の攻撃では，1 回目と同様に，ファイル探索を中心とした活動を観測した．遠隔操作攻撃者は，ショートカットファイルを対象としたファイル探索を試みている．また，興味深いショートカットファイルがあると，ショートカットファイルを取得し，そのプロパティ情報から，実ファイルのフルパス情報を特定，窃取している(表 13).

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わ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 2015 (BOS_2015)」について報告した．

研究用データセット「動的活動観測 2015 (BOS_2015)」は，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 2015 (BOS_2015)」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，類似の検体を同時期観測した事例，内部感染拡大活動を観測した事例，セキュリティツール導入有無の確認方法を観測し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」の拡充，類似の検体の同時観測，同一の C&C サーバに接続する異なる検体の観測など，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) STIX, http://stix.mitre.org/
4) トレンドマイクロ：2013 年上半期国内における持続的標的型攻撃の分析(2013)
5) トレンドマイクロ : 国内標的型サイバー攻撃分析レポート 2015 年版(2015.04)
6) 神薗、秋山、笠間、村上、畑田、寺田：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(2015.07)