マルウェア対策研究人材育成ワークショップ 2018(MWS2018)
意見交換会

HITACHI
Inspire the Next

研究用データセット「動的活動観測2018」

動的活動観測システム(BOS)
Behavior Observable System

2018/05/30
Masato Terada
Hitachi Incident Response Team
http://www.hitachi.com/hirt/

Opening

HITACHI
Inspire the Next

マルウェア検体の静的／動的解析では、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、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というのが実情である。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。

本データセットは、**「攻撃者行動視点で脅威の特徴情報」を明らかにしていくために、攻撃者の行動を記録する研究用データセットの作成**を目標としている。

BOS (Behavior Observable System)

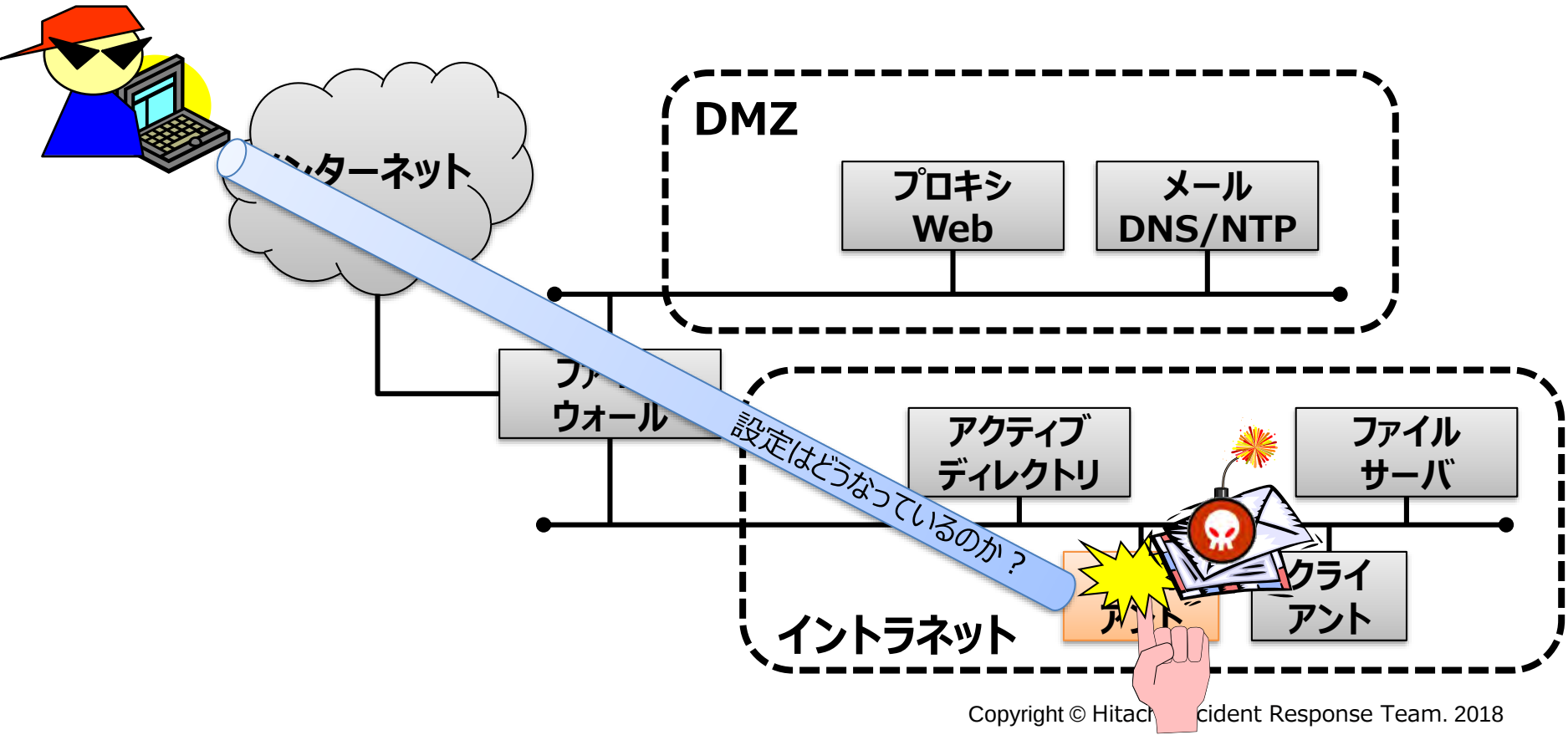
- **データセット概要**

(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。

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を特徴付けできる研究用データセット

BOS (Behavior Observable System)

- 動的活動観測環境
  - 企業のネットワークを模擬する小規模なネットワーク環境を構築
  - 標的型攻撃メールに添付されたウイルスなどを動的観測環境下で実行



BOS (Behavior Observable System)

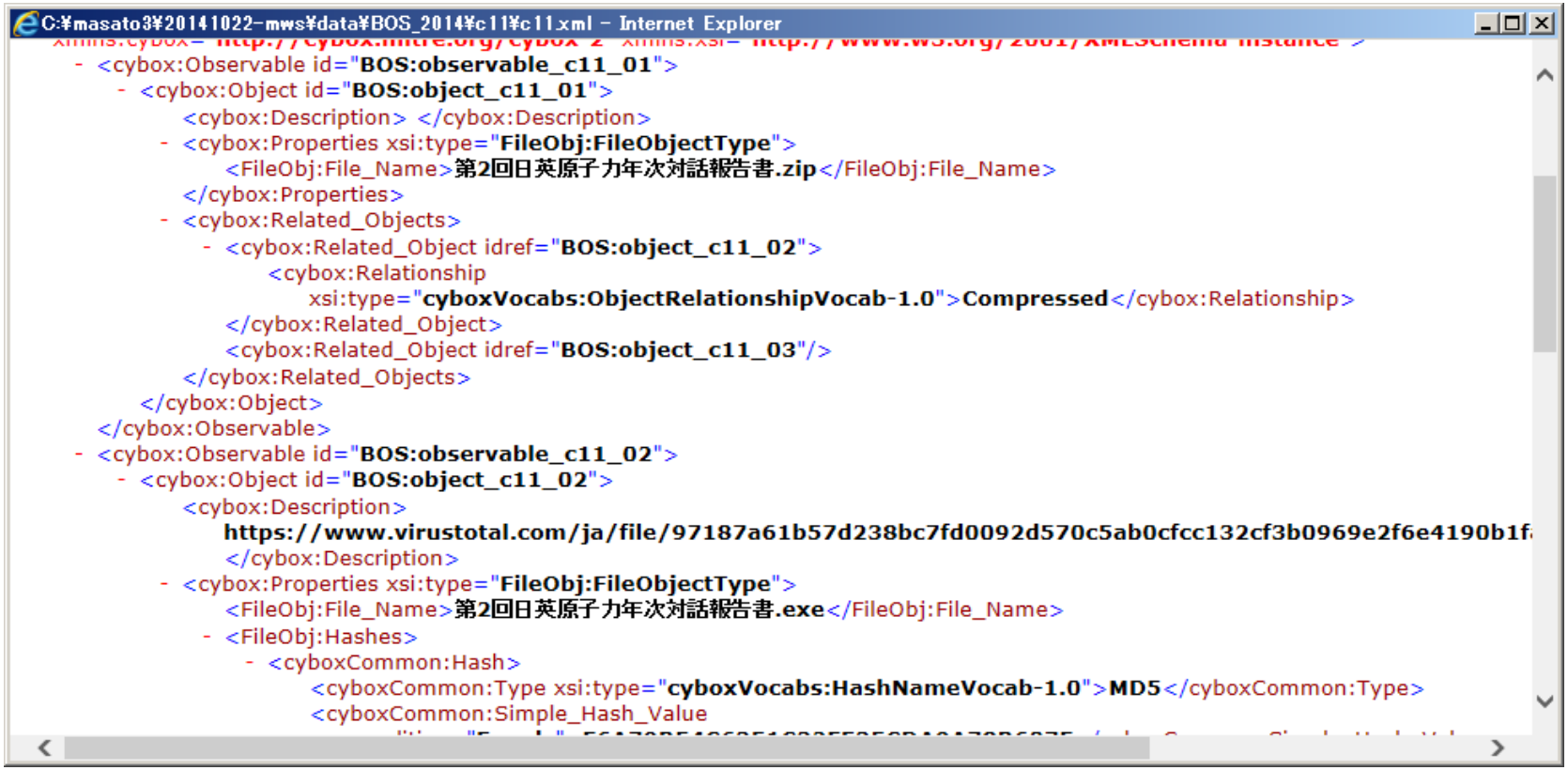
- **データセット構成**
  注：活動観測のケース毎に提供する観測データは異なる。

  (a) マルウェア検体ハッシュ値情報
  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 (Structured Threat Information eXpression；脅威情報構造化記述形式)形式で記載したファイルである。
  (b) 通信観測データ
  マルウェア検体を実行した際の通信のフルキャプチャデータであり、攻撃者の行動に関する解析が可能である。
  (c) プロセス観測データ
  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であり、攻撃者の行動に関する解析が可能である。
  (d) その他
  Windowsイベントログ、プロキシログ

2. 研究用データセット「動的活動観測」

BOS_20XX

- **データセット構成**
  (a) マルウェア検体ハッシュ値情報

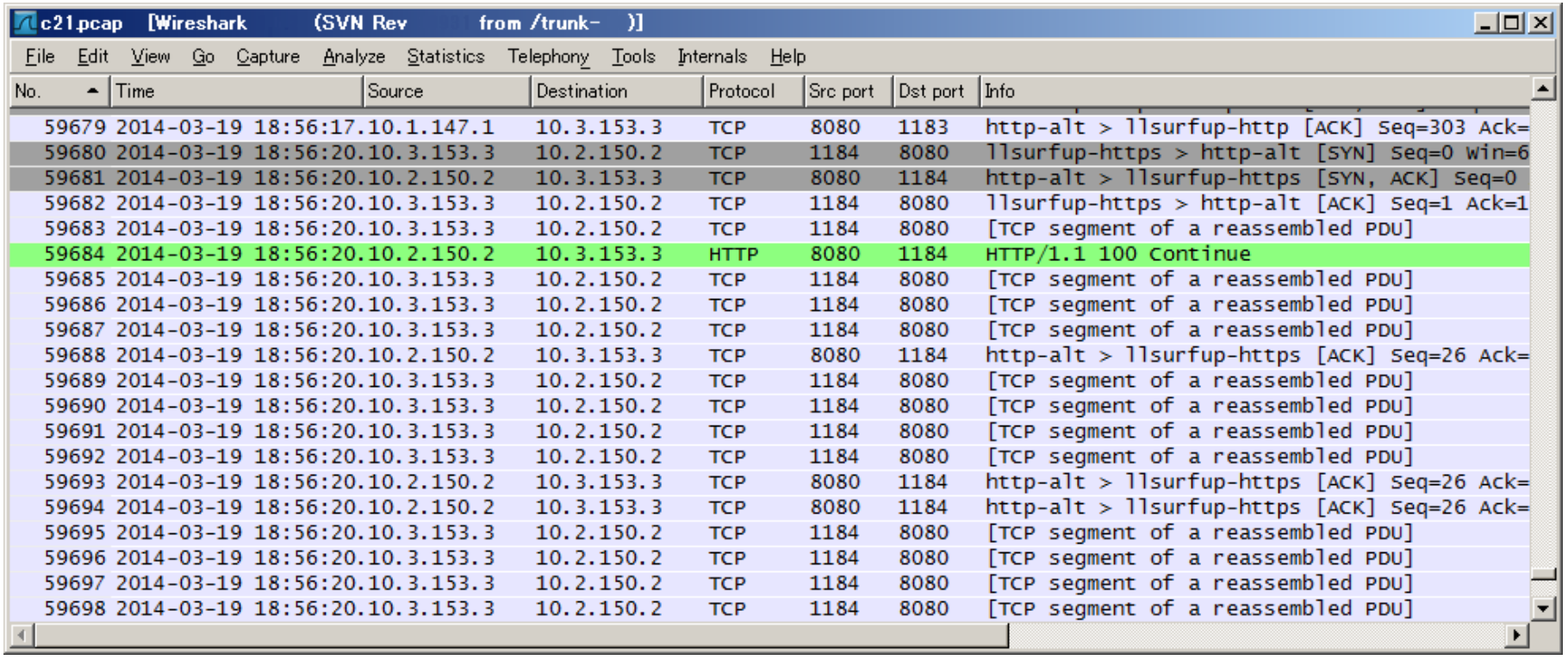


研究用データセット「動的活動観測」

Hitachi Incident Response Team

BOS_20XX

- **データセット構成**
  (b) 通信観測データ



No.	Time	Source	Destination	Protocol	Src port	Dst port	Info
59679	2014-03-19 18:56:17.10.1.147.1	10.3.153.3	TCP	8080	1183	http-alt > llsurfup-http [ACK] Seq=303 Ack=
59680	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	llsurfup-https > http-alt [SYN] Seq=0 Win=6
59681	2014-03-19 18:56:20.10.2.150.2	10.3.153.3	TCP	8080	1184	http-alt > llsurfup-https [SYN, ACK] Seq=0
59682	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	llsurfup-https > http-alt [ACK] Seq=1 Ack=1
59683	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59684	2014-03-19 18:56:20.10.2.150.2	10.3.153.3	HTTP	8080	1184	HTTP/1.1 100 Continue
59685	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59686	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59687	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59688	2014-03-19 18:56:20.10.2.150.2	10.3.153.3	TCP	8080	1184	http-alt > llsurfup-https [ACK] Seq=26 Ack=
59689	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59690	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59691	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59692	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59693	2014-03-19 18:56:20.10.2.150.2	10.3.153.3	TCP	8080	1184	http-alt > llsurfup-https [ACK] Seq=26 Ack=
59694	2014-03-19 18:56:20.10.2.150.2	10.3.153.3	TCP	8080	1184	http-alt > llsurfup-https [ACK] Seq=26 Ack=
59695	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59696	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59697	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]
59698	2014-03-19 18:56:20.10.3.153.3	10.2.150.2	TCP	1184	8080	[TCP segment of a reassembled PDU]

研究用データセット「動的活動観測」

Hitachi Incident Response Team

BOS_20XX

- **データセット構成**
  (c) プロセス観測データ

c21_process.log - メモ帳

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

```
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥WINDOWS¥WindowsShell.Manifest(0,0x001200a9,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥WINDOWS¥WindowsShell.Config(0,0x001200a9,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥windows¥debug¥rar.lng(0,0x00120089,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥WINDOWS¥system32¥rpcss.dll(0,0x00100020,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥WINDOWS¥system32¥uxtheme.dll(0,0x00100020,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥WINDOWS¥system32¥uxtheme.dll(0,0x00100020,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥WINDOWS¥system32¥MSCTF.dll(0,0x00100020,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥WINDOWS¥system32¥MSCTF.dll(0,0x00100020,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥WINDOWS¥system32¥setupapi.dll(0,0x00100020,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥Documents and Settings¥Administrator.vlanex¥Application D
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥Documents and Settings¥Administrator.vlanex¥Application D
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥Documents and Settings¥Administrator.vlanex¥Application D
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥windows¥debug¥rar.ini(0,0x00120089,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥windows¥config¥wininit.log(0,0x0012019f,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[C:¥windows¥config¥wininit.log(0,0x0012019f,)]
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[¥¥10.2.149.1¥public¥mail¥testMail - コピー2.vbs(0,0x00120089
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[¥¥10.2.149.1¥public¥mail¥testMail - コピー.vbs(0,0x00120089,
Access File: [C:¥WINDOWS¥Debug¥Rar.exe (0x00000e20)]->[¥¥10.2.149.1¥public¥mail¥testMail.vbs(0,0x00120089,)]
Terminate Process: [(0x00000990)]->[C:¥WINDOWS¥Debug¥Rar.exe(0x00000e20)]
Terminate Process: [(0x000001f8)]->[C:¥WINDOWS¥system32¥cmd.exe(0x00000990)]
Launch Process: [ (0x000001f8)]->[C:¥WINDOWS¥system32¥cmd.exe (0x00000f3c)]
```

BOS_20XX

- **BOS_20XX**
  - 進行度：動的活動観測における攻撃活動の進み具合の区分

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(403、404、503)
6		C2サーバと通信成立	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。

Ending

HITACHI
Inspire the Next

- **BOS2014～2018**
  組織内ネットワークへの侵害活動を想定した研究用データセット「動的活動観測2013～2017」

- 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、攻撃者行動視点で脅威を特徴付けできるようにするため、マルウェア検体(ハッシュ値)、通信観測データ、プロセス観測データなどから構成