インシデント対応ハンズオン for ショーケース

2018年6月1日

JPCERT コーディネーションセンター
竹田春樹

自己紹介

- 分析センターに所属（2006年より）
  - 2016年4月より分析センター マネージャーに就任
- 主な業務
  - マルウエア分析（動的解析）などを中心に分析を実施
  - たまに講演活動なども行っています

「JPCERT/CCをご存知ですか？」

JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

脆弱性情報ハンドリング

- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

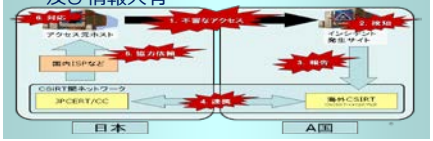
定点観測（TSUBAME）

- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供

インシデントハンドリング

（インシデント対応調整支援）

- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害の可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

トレーニングの概要（前半）

時間	内容
13:00 ～ 13:30	□ 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

トレーニングの概要（後半）

時間	内容
13:30 ～ 16:00	◘ ハンズオン ✓ ツールを使用したイベントログの抽出 ✓ ログ(イベントログ、Proxyサーバのログ)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
	◘ まとめ ◘ 質疑応答

注意事項 1

- **本ハンズオン受講用のPC**
  - キーボードを使用可能なWindows OSもしくはMacOS X、Linux OSを搭載した端末 ※タブレット端末は不可
    - 無線LANを使用可能なこと
  - ソフトウェア
    - Webブラウザ(ログのダウンロードに使用)CCleaner改ざん (2017/9)
    - zipファイルの展開ソフト
    - ログファイルを閲覧、検索する事が可能なソフトウエア

※ grepを推奨しますが、Excel、 その他大容量テキストを閲覧、 検索できるソフトでも代用可能です。

※ 以下のどちらかのソフトウェアをインストールすれば、Windows環境でもgrepを使用可能です。

- Cygwin
- GnuWin32のGrep for Windows

目次

1. ネットワーク内部に侵入した攻撃者の活動
2. 攻撃者が利用するコマンドおよびツール
3. コマンドおよびツール実行の痕跡
4. ハンズオン

1 ネットワーク内部に侵入した攻撃者の活動

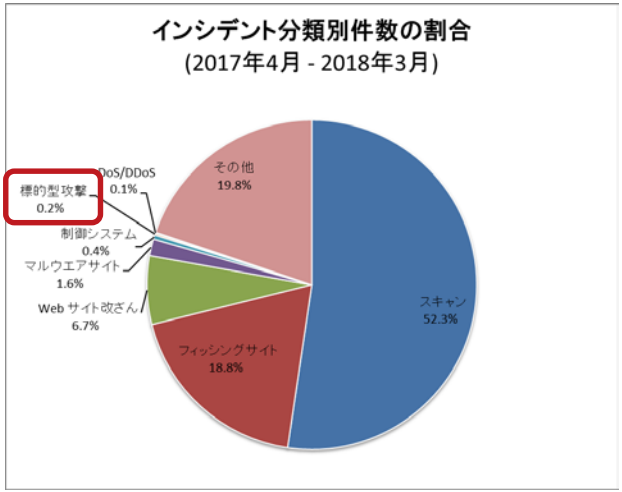
2 攻撃者が利用するコマンドおよびツール

3 コマンドおよびツール実行の痕跡

4 ハンズオン

高度サイバー攻撃（標的型攻撃）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**
  - 標的型攻撃、APTと呼ばれることも
  - 2015年以降、特にこのタイプの攻撃について、社会的に注目されるようになりました



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

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、様々な攻撃が発生している
    - 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
  - 目的を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

攻撃グループってどれくらいあるの？

- セキュリティベンダーにより命名されたもので攻撃の特徴毎に攻撃者グループの名称、オペレーション名がある
- 名称も命名した組織ごとに異なっており、把握するのは難しい

[名称（例）]

Mandiant	CrowdStrike	TrendMicro	Symantec
APT17	Aurora Panda	N/A	Hydden LYNX
APT27	Emissary Panda	N/A	N/A
APT28	Fancy Bear	Pawn Storm	N/A

参考: APT Groups and Operations
https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=361554658

JPCERT/CC が対応した標的型攻撃（2017年）

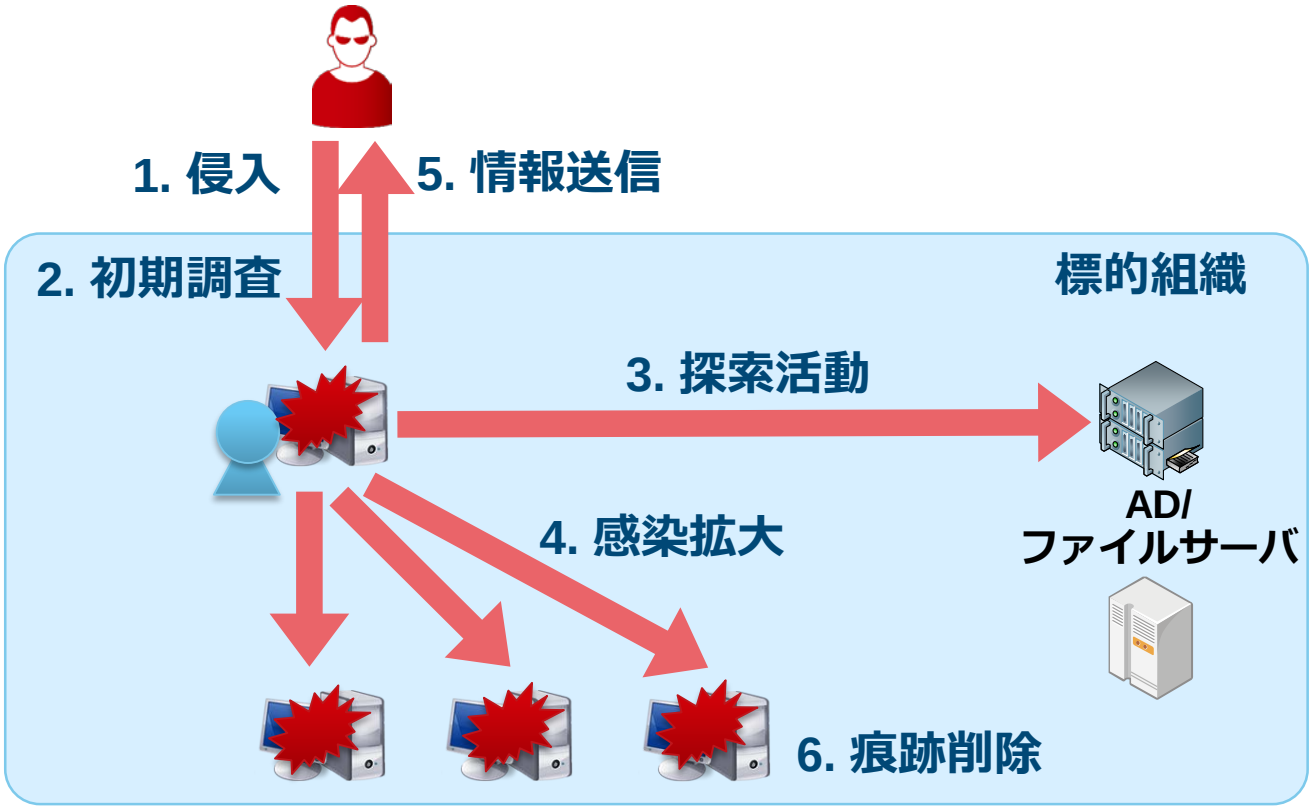
	1月-3月	4月-6月	7月-9月	10月-12月	備考
Daserf	→	→			BRONZE BUTLER, Tick などと命名される撃キャンペーンと関連
ChChes	→				国内組織を狙った標的型攻撃で確認
RedLeaves	→				APT10との関連性が疑われる
DragonOK		→			Paloalto Networksが命名した攻撃グループ。日本、台湾、チベット、ロシアなどがターゲット
Winnti				→	企業・組織のコードサイニング証明書を窃取し、マルウエアや攻撃ツールの署名に使用する攻撃グループ
CCleaner			→		APT17との関連性が疑われる

※ → 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

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	攻撃対象とする組織の関係者などを装いメールを送付し、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	攻撃対象とする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
アップデートハイジャック	攻撃対象とする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	攻撃対象とする組織が使用する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

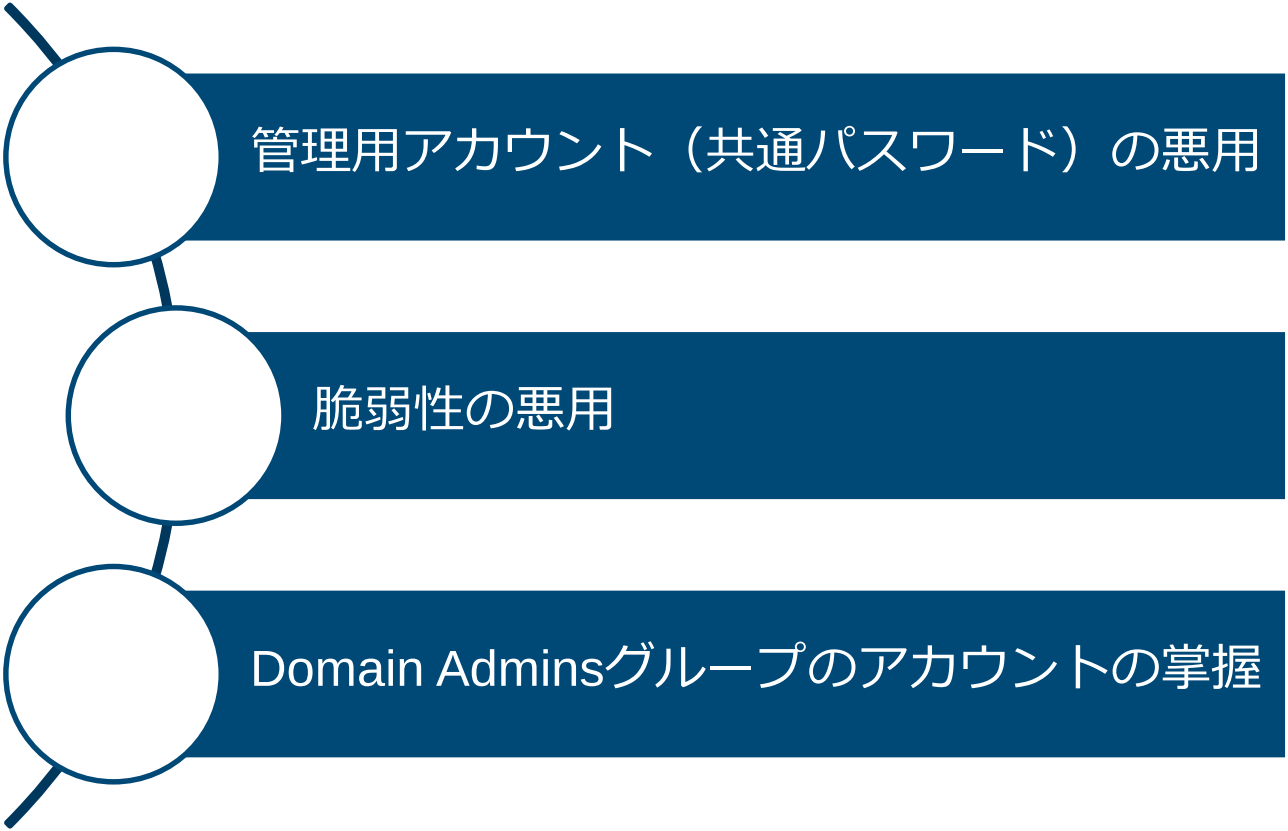
ネットワーク内部に侵入した攻撃者の活動



ネットワーク内部に侵入した攻撃者の活動

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	• 感染した端末を別のマルウエアにも感染させる、または別の端末にアクセスを試みる
痕跡削除	• 攻撃者の使用したファイルおよびログの削除

感染拡大パターン



管理用アカウント（共通パスワード）の悪用

すべての端末に準備されている共通アカウントを悪用

端末のセットアップ、メンテナンス目的で社内の全端末に共通するアカウントを設定している

共通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

脆弱性の悪用

**Windowsの脆弱性を利用して
ドメイン管理者権限に昇格する**

Domain Controllerのサーバにパッチを適用していない場合

脆弱性が悪用されてドメインの管理者権限を悪用される

MS14-068は特に注意が必要

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

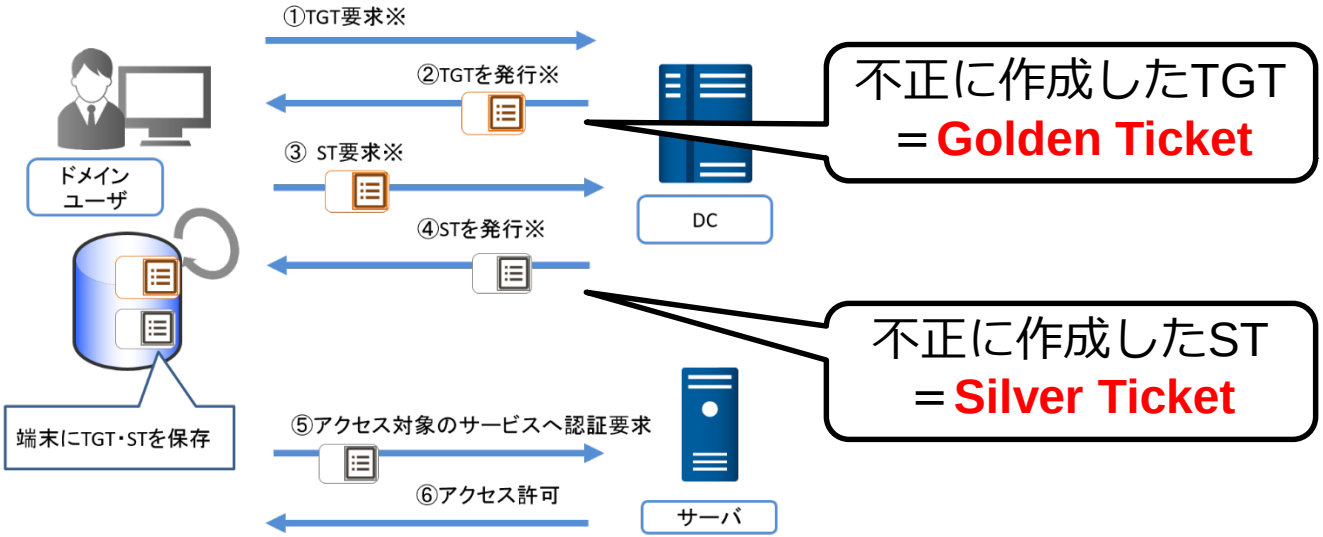
不正ログインを行う攻撃手法

- 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 最近使われる手法	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	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

FYI: 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 : 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

FYI: Golden Ticket / Silver Ticket の怖さ

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

1 ネットワーク内部に侵入した攻撃者の活動

2 攻撃者が利用するコマンドおよびツール

3 コマンドおよびツール実行の痕跡

4 ハンズオン

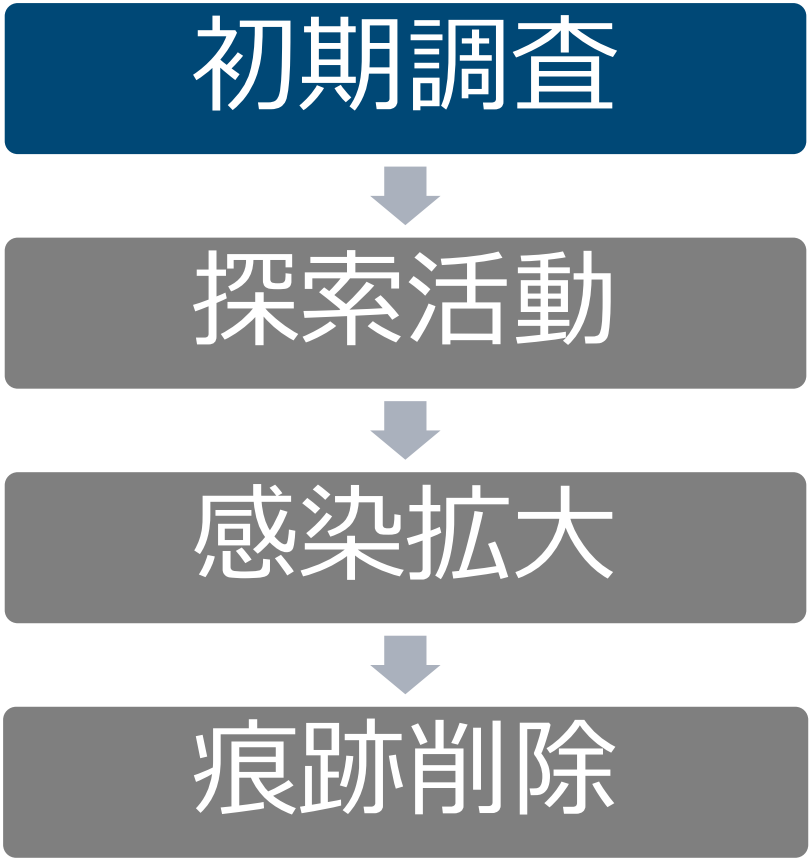
攻撃者が利用するコマンドおよびツール

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

攻撃者の活動：初期調査



初期調査

初期調査

- 感染した端末の情報を収集する

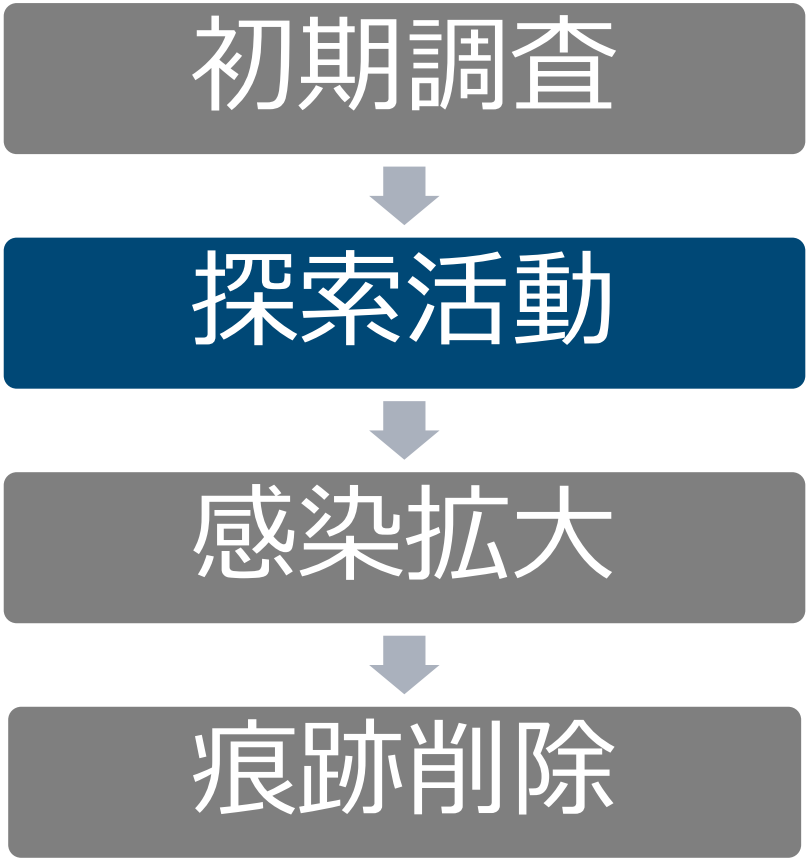
- マルウエアの機能を利用して収集
- Windowsコマンドを利用して収集

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3つの異なる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

攻撃者の活動：探索活動



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

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コマンドが多用されている

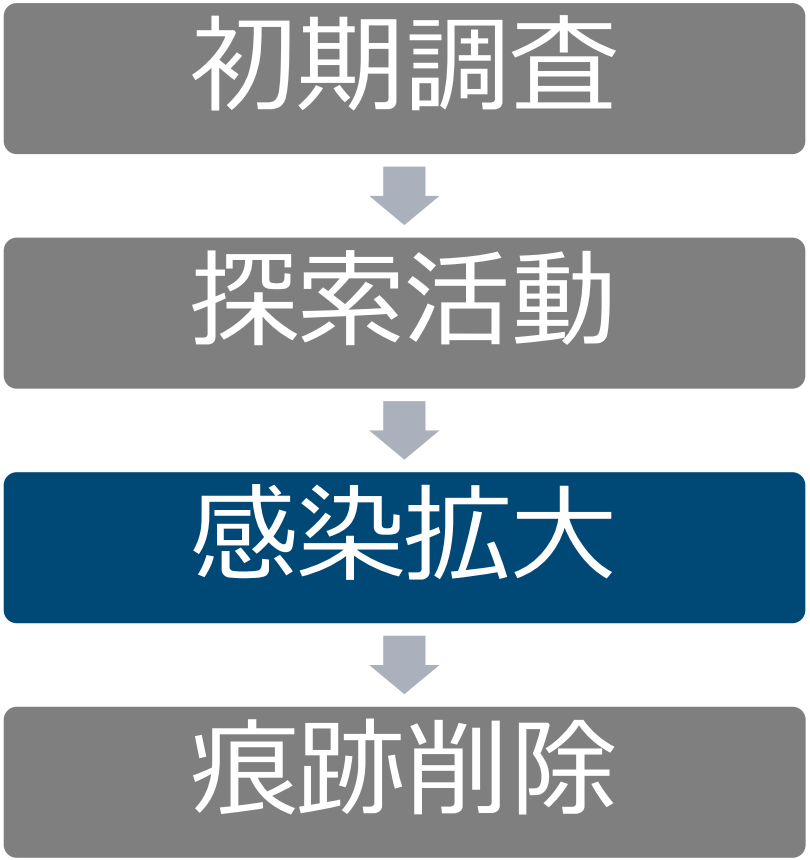
その他のツール

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

攻撃者の活動：感染拡大



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

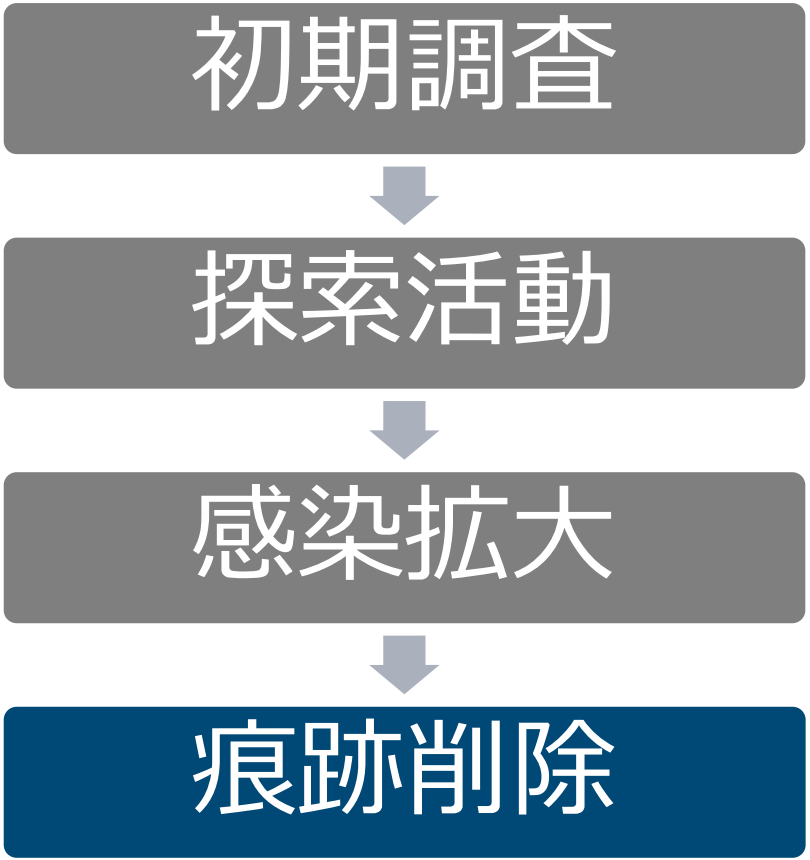
- パスワード、ハッシュダンプツールを使用
- Windowsコマンドを利用して感染拡大

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

攻撃者の活動：痕跡削除



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

情報の送信

1 ネットワーク内部に侵入した攻撃者の活動

2 攻撃者が利用するコマンドおよびツール

3 コマンドおよびツール実行の痕跡

4 ハンズオン

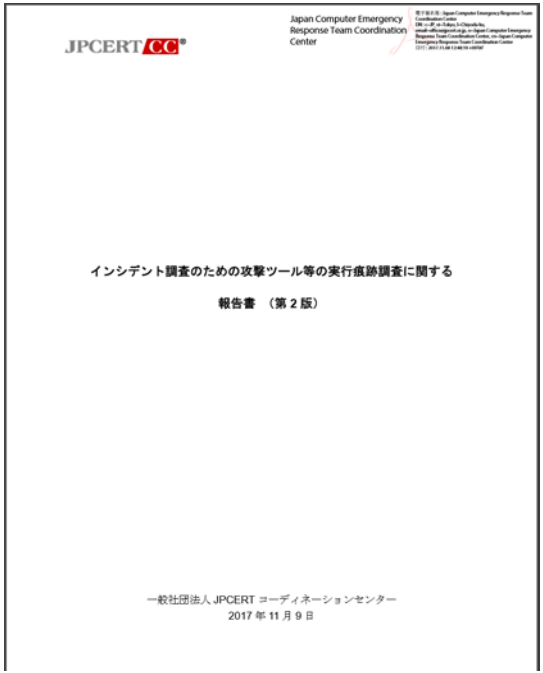
JPCERT/CCの調査で確認している事実と問題

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

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
https://www.jpcert.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

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

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

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/

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

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

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

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

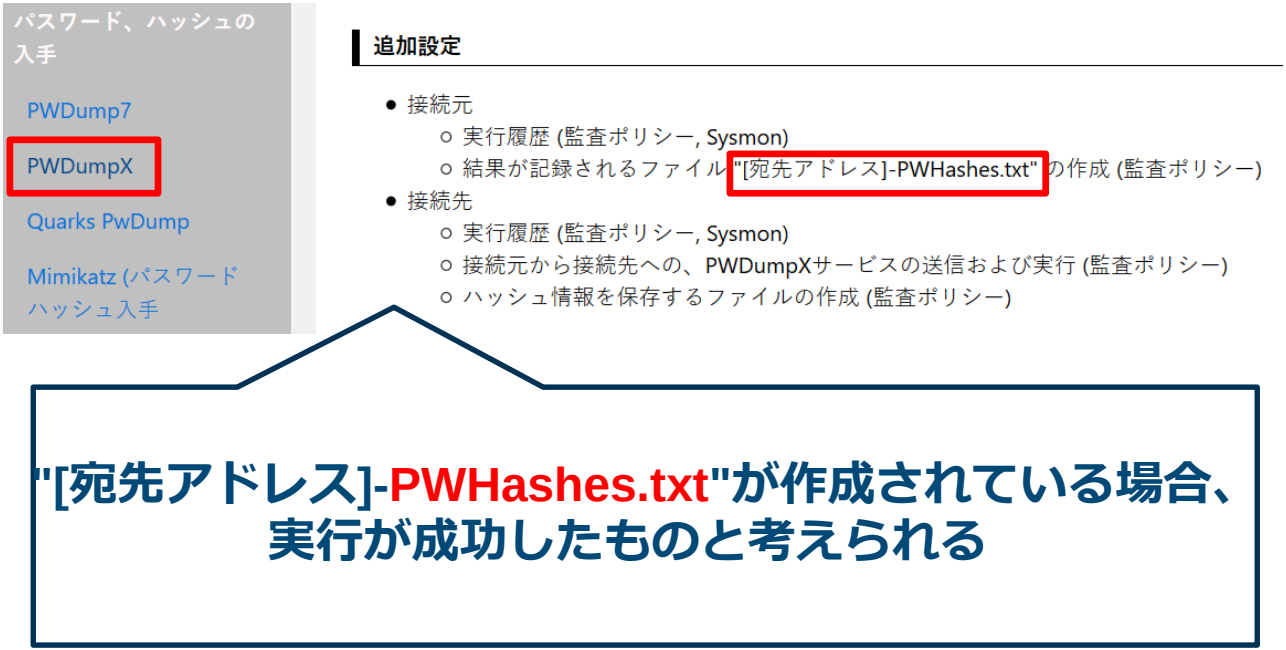
- 他のホストに、リアルタイムにログを転送
  - イベント サブスクリプション
  - Syslog形式などで送信
  - 定期的なログファイルのバックアップ

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

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



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

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

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

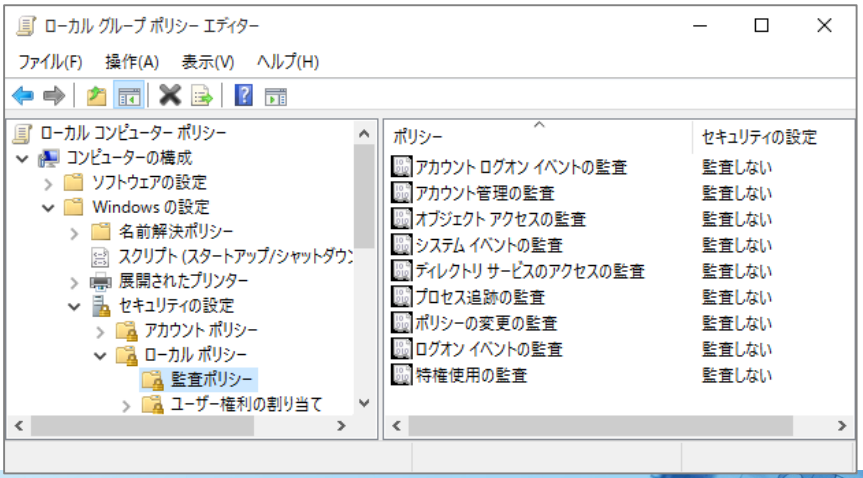
- 監査ソフトウエア（資産管理ソフトなど）でも同様のログを取得可能な場合がある
  - プロセスの実行
  - ファイルの書込み

- 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

FYI: 監査ポリシーの有効化方法

設定方法 ①

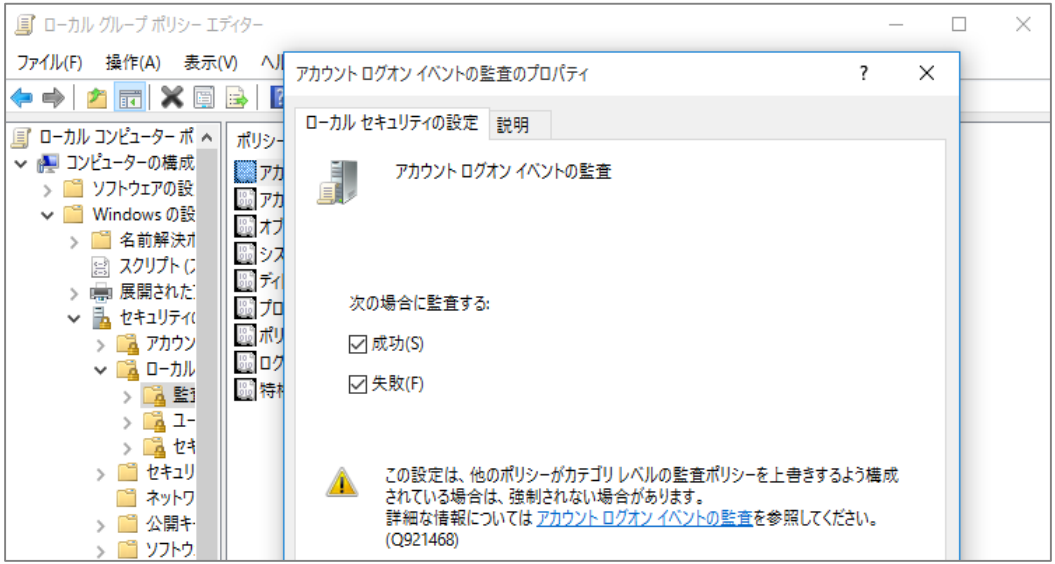
- ローカル グループ ポリシーの編集
  - [コンピューターの構成]→[Windowsの設定]→[セキュリティの設定] →[ローカル ポリシー]→[監査ポリシー]



FYI: 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



FYI: 監査ポリシーの有効化方法

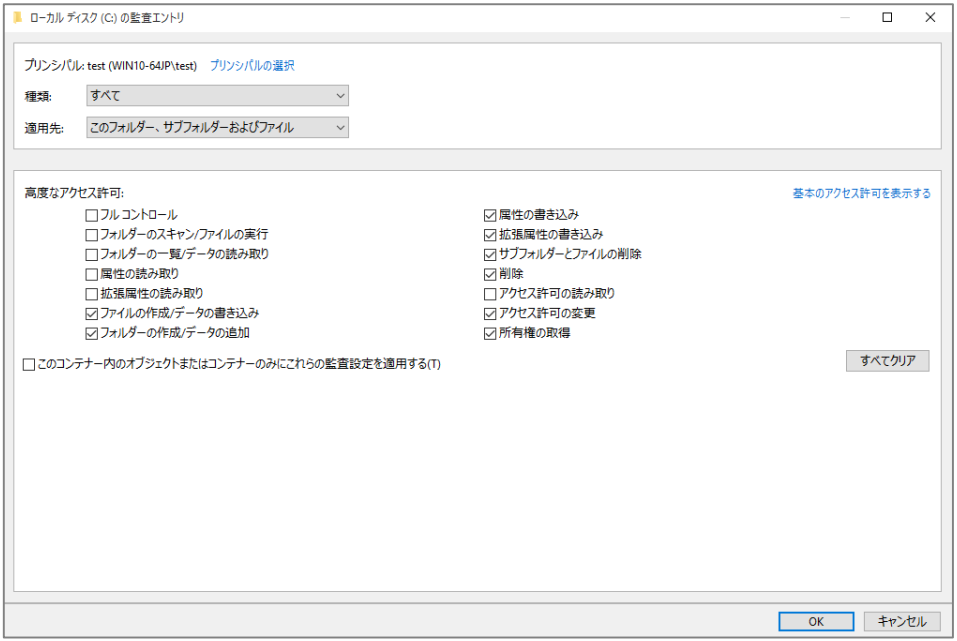
設定方法 ③

- 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

FYI: 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



FYI: 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

FYI: Sysmonのインストール方法

ダウンロードURL

- https://technet.microsoft.com/ja-jp/sysinternals/dn798348

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

目次

1. ネットワーク内部に侵入した攻撃者の活動
2. 攻撃者が利用するコマンドおよびツール
3. コマンドおよびツール実行の痕跡
4. ハンズオン

ハンズオンの内容は別紙に記載します

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html