25th Anniversary

Mimikatz実行痕跡の発見手法

IIJ
Internet Initiative Japan

株式会社インターネットイニシアティブ
セキュリティ本部 セキュリティ情報統括室
小林 稔

Ongoing Innovation

自己紹介

名前：小林 稔

所属：セキュリティ本部 セキュリティ情報統括室

2014年5月IIJ入社。

2015年8月より社会保障審議会年金事業管理部会運営担当参与。

Mauritius 2016 FIRST Technical Colloquium スピーカーおよびトレーニング講師。

2017年セキュリティキャンプ全国大会講師。

今日の内容

1. Mimikatzとは
2. Mimikatz実行痕跡の発見方法（デフォルト設定）
3. Mimikatz実行痕跡の発見方法（追加設定）
4. 検出のスクリプト化
5. まとめ

Mimikatzとは

Mimikatzとは

作者曰く…

mimikatz is a tool I've made to learn C and make somes experiments with Windows security.

実際のところは…

Windowsのメモリ上に保持されているアカウントの認証情報にアクセスし、管理者権限の取得や他のアカウントのなりすましを行うためのツール。

- Twitter
  - https://twitter.com/gentilkiwi
- Github
  - https://github.com/gentilkiwi/mimikatz

Mimikatzの実行痕跡を調査する意味

標的型攻撃でシステム内の横展開やGolden TicketやSilver Ticketによるなりすましのために頻繁に使用される。なお、Mimikatzを使用するためには管理者権限やSYSTEM権限が実質的に必要となるため、最低1台は特権が取られえていると考えた方が良い。

また、作者の対応スピードが早く、以前はMimikatz発見に使えたインジケータが現在は使えないこともある。このような情報を再整理しアップデートすることでインシデントレスポンスの品質向上を図ることができる。

Mimikatzの実装形態

- EXE版
  - 32bit
  - 64bit
- DLL版
  - 32bit
  - 64bit
- PowerShell版
  - ファイルレスで実行可能

- 重要な機能の実行には管理者権限またはSYSTEM権限が必要

Mimikatzでできること

- 認証情報ダンプ
  - プレーンパスワード
  - NTLMハッシュ
  - Kerberos Ticket Export
- Pass-the-Hash
- Pass-the-Ticket
- Golden Ticket/Silver Ticket生成
- DCSync
- Skeleton Key
- などなど

Mimikatzを実行した痕跡の発見方法（デフォルト設定）

検証環境

- 今回の検証環境
- Windows Server 2016
  - Active Directoryサーバ
  - ドメイン名：mylab.local
  - グループポリシーはデフォルトのまま
- Windows 10 Pro 1703
  - ドメイン参加

- Mimikatzが残す特徴的なログやファイルを探す。
- 多くの場合において、攻撃検出のための特別な設定は行われていないため、デフォルト設定で残る情報から実行痕跡を探し出す。

Mimikatzが残す痕跡 (1)

- OSに残る痕跡
  - Prefetch
    - クライアント系Windowsのみ
    - 実行日時と実行回数が分かる
  - Shimcache
  - Amcache

- 実行されたことは分かるが起動時のオプション等は分からない。
- ファイル名が変更された場合Mimikatzと判断できない。

Mimikatzが残す痕跡 (2)

WinPrefetchView

File Edit View Options Help

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run
MAKECAB.EXE-0F170...	10/20/2017 8:42:02 PM	10/23/2017 8:44:...	12,456	MAKECAB.EXE	C:\Windows\System32\makecab.exe	4	10/23/20
MANAGEMENTAGEN...	10/16/2017 4:27:36 PM	10/16/2017 4:27:...	9,203	MANAGEMENTAG...	C:\PROGRAM FILES\VMware\VMWARE TO...	1	10/16/20
MICROSOFT.PHOTOS....	10/20/2017 8:23:27 PM	11/1/2017 12:46:...	27,220	MICROSOFT.PHO...	C:\PROGRAM FILES\WINDOWSAPPS\MICR...	4	11/1/201
MICROSOFTEDGE.EXE...	10/23/2017 8:43:36 PM	10/23/2017 8:49:...	36,376	MICROSOFTEDGE....	C:\Windows\SYSTEMAPPS\MICROSOFT.MI...	2	10/23/20
MICROSOFTEDGECP....	10/23/2017 8:43:37 PM	10/23/2017 8:49:...	44,547	MICROSOFTEDGE...	C:\Windows\SYSTEMAPPS\MICROSOFT.MI...	10	10/23/20
MIMIKATZ.EXE-E6AD8...	10/23/2017 4:15:31 PM	11/6/2017 12:00:...	5,850	MIMIKATZ.EXE	C:\Users\USER01.MYLAB\Desktop\tools\MI...	15	11/6/201
MMC.EXE-31A29E87.pf	10/23/2017 4:23:21 PM	10/31/2017 7:20:...	38,695	MMC.EXE	C:\Windows\System32\mmc.exe	5	10/31/20
MMC.EXE-E5EE3A89.pf	10/23/2017 8:10:55 PM	11/6/2017 11:33:...	41,148	MMC.EXE	C:\Windows\System32\mmc.exe	5	11/6/201
MMC.EXE-F5DC4F82.pf	11/1/2017 12:39:54 AM	11/1/2017 1:10:4...	28,418	MMC.EXE	C:\Windows\System32\mmc.exe	5	11/1/201
MOBSYNC.EXE-C5E22...	10/16/2017 4:23:51 PM	11/6/2017 11:32:...	7,662	MOBSYNC.EXE	C:\Windows\System32\mobsync.exe	16	11/6/201
MORE.COM-6776F1D...	10/24/2017 3:22:20 PM	10/24/2017 7:04:...	1,906	MORE.COM	C:\Windows\System32\more.com	7	10/24/20
MPCMDRUN.EXE-F40...	10/20/2017 8:27:21 PM	11/6/2017 11:42:...	5,749	MPCMDRUN.EXE	C:\PROGRAM FILES\WINDOWS DEFENDER\...	45	11/6/201

Filename	Full Path	Device Path	Index
MIMIKATZ.EXE	C:\Users\USER01.MYLAB\Desktop\tools\MIMIKATZ_TRUNK_2.1.1 20170813\x64\mimikatz.exe	\VOLUME{01d346d82cb7b60c-6c2e9e...	4
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll	\VOLUME{01d346d82cb7b60c-6c2e9e...	5
BCRYPT.DLL	C:\Windows\System32\bcrypt.dll	\VOLUME{01d346d82cb7b60c-6c2e9e...	47
BCRYPTPRIMITIVES.DLL	C:\Windows\System32\BCRYPTPRIMITIVES.DLL	\VOLUME{01d346d82cb7b60c-6c2e9e...	14
CFGMGR32.DLL	C:\Windows\System32\cfgmgr32.dll	\VOLUME{01d346d82cb7b60c-6c2e9e...	23
COMBASE.DLL	C:\Windows\System32\combase.dll	\VOLUME{01d346d82cb7b60c-6c2e9e...	13
CRYPT32.DLL	C:\Windows\System32\crypt32.dll	\VOLUME{01d346d82cb7b60c-6c2e9e...	9
CRYPTBASE.DLL	C:\Windows\System32\CRYPTBASE.DLL	\VOLUME{01d346d82cb7b60c-6c2e9e...	42
CRYPTDLL.DLL	C:\Windows\System32\cryptdll.dll	\VOLUME{01d346d82cb7b60c-6c2e9e...	31
CRYPTSP.DLL	C:\Windows\System32\cryptsp.dll	\VOLUME{01d346d82cb7b60c-6c2e9e...	41
DEVOBJ.DLL	C:\Windows\System32\devobj.dll	\VOLUME{01d346d82cb7b60c-6c2e9e...	40
CONDRV.SYS	C:\Windows\System32\drivers\condrv.sys	\VOLUME{01d346d82cb7b60c-6c2e9e...	56
MOUCLASS.SYS	C:\Windows\System32\drivers\mouclass.sys	\VOLUME{01d346d82cb7b60c-6c2e9e...	55
GDI32.DLL	C:\Windows\System32\gdi32.dll	\VOLUME{01d346d82cb7b60c-6c2e9e...	15
GDI32FULL.DLL	C:\Windows\System32\GDI32FULL.DLL	\VOLUME{01d346d82cb7b60c-6c2e9e...	16

253 Files, 1 Selected

NirSoft Freeware. http://www.nirsoft.net

ENG 12:29 PM 11/6/2017

Mimikatzが残す痕跡 (3)

- PowerShell版Mimikatzの実行痕跡はPowerShell関連のイベントログに残る。
  - Windows PowerShell.evtx
  - Microsoft-Windows-PowerShell%4Operational.evtx
  - 起動時の引数やスクリプトブロックの内容は記録されるが、インタラクティブにどのような操作が行われたのか分からない。
- Mimikatzの操作に関連する痕跡はセキュリティイベントログに残る（EXE版、DLL版、PowerShell版共通）。
  - Security.evtx
- 今回はセキュリティイベントログを中心に解説する。

Mimikatzが残す痕跡 (4)

Event Viewer

File Action View Help

Windows PowerShell Number of events: 95

Level	Date and Time	Source	Event ID	Task Category
Information	10/23/2017 5:47:58 PM	PowerShell (PowerShell)	403	Engine Lifecycle
Information	10/23/2017 5:47:58 PM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	10/23/2017 5:47:58 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	10/23/2017 5:47:58 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	10/23/2017 5:47:58 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	10/23/2017 5:47:58 PM	PowerShell (PowerShell)	600	Provider Lifecycle

Event 400, PowerShell (PowerShell)

General Details

```
HostName=ConsoleHost
HostVersion=5.1.15063.674
HostApplication=powershell.exe -exec bypass Invoke-Mimikatz.ps1;Invoke-Mimikatz
RunspaceId=469b3beb-5ecc-4535-bda6-9f42157ae357
PipelineId=
CommandName=
CommandType=
ScriptName=
```

Log Name:	Windows PowerShell		
Source:	PowerShell (PowerShell)	Logged:	10/23/2017 5:47:58 PM
Event ID:	400	Task Category:	Engine Lifecycle
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	WIN10.mylab.local
OpCode:			
More Information:	Event Log Online Help		

Actions

Windows PowerShell
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help

Event 400, PowerShell (Pow...
- Event Properties
- Attach Task To This Ev...
- Copy
- Save Selected Events...
- Refresh
- Help

Mimikatzが残す痕跡 (5)

Event Viewer

File Action View Help

Operational Number of events: 223

Level	Date and Time	Source	Eve...	Task Category
Warning	10/23/2017 5:48:58 PM	PowerShell (Micros...	4104	Execute a Remote Command
Warning	10/23/2017 5:48:58 PM	PowerShell (Micros...	4104	Execute a Remote Command
Information	10/23/2017 5:48:51 PM	PowerShell (Micros...	53504	PowerShell Named Pipe IPC
Information	10/23/2017 5:48:51 PM	PowerShell (Micros...	40961	PowerShell Console Startup

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

```
Creating Scriptblock text (1 of 145):
function Invoke-Mimikatz
{
<#
.SYNOPSIS

This script leverages Mimikatz 2.1.1 and Invoke-ReflectivePEInjection to reflectively load Mimikatz
completely in memory. This allows you to do things such as
dump credentials without ever writing the mimikatz binary to disk.
The script has a ComputerName parameter which allows it to be executed against multiple
computers.
```

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	10/23/2017 5:48:58 PM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Warning	Keywords:	None
User:	MYLAB\admin01	Computer:	WIN10.mylab.local
OpCode:	On create calls		
More Information:	Event Log Online Help		

Actions

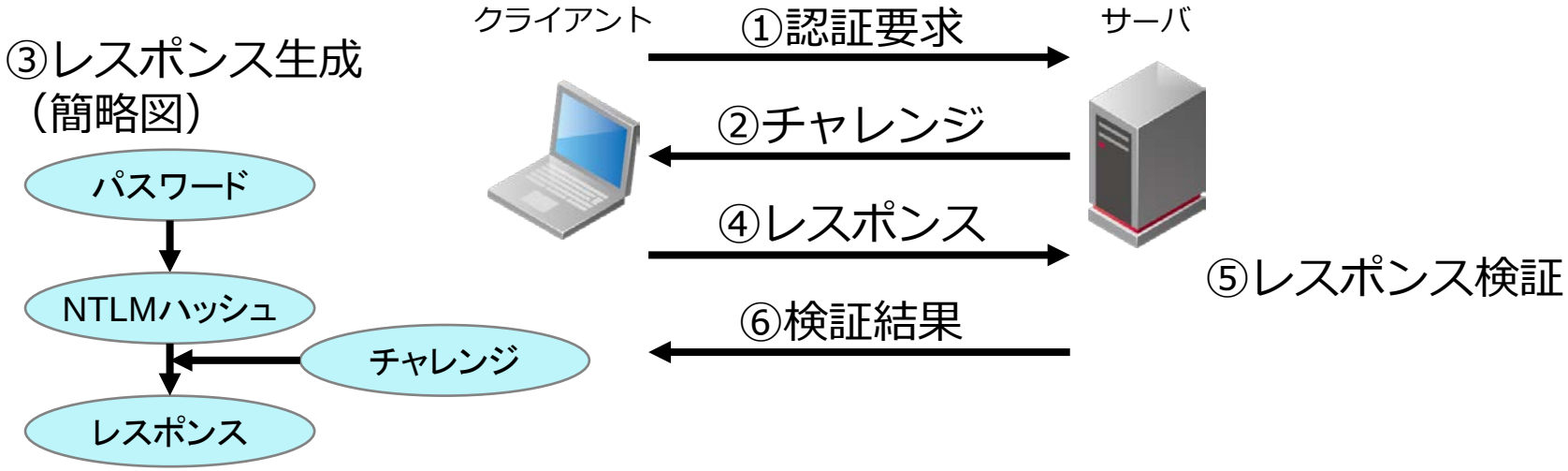
Operational
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Disable Log
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help

Event 4104, PowerShell (Mi...
- Event Properties
- Attach Task To This Ev...
- Copy
- Save Selected Events...
- Refresh
- Help

Pass-the-Hash
Pass-the-Ticket

Windowsの認証方式 (1)

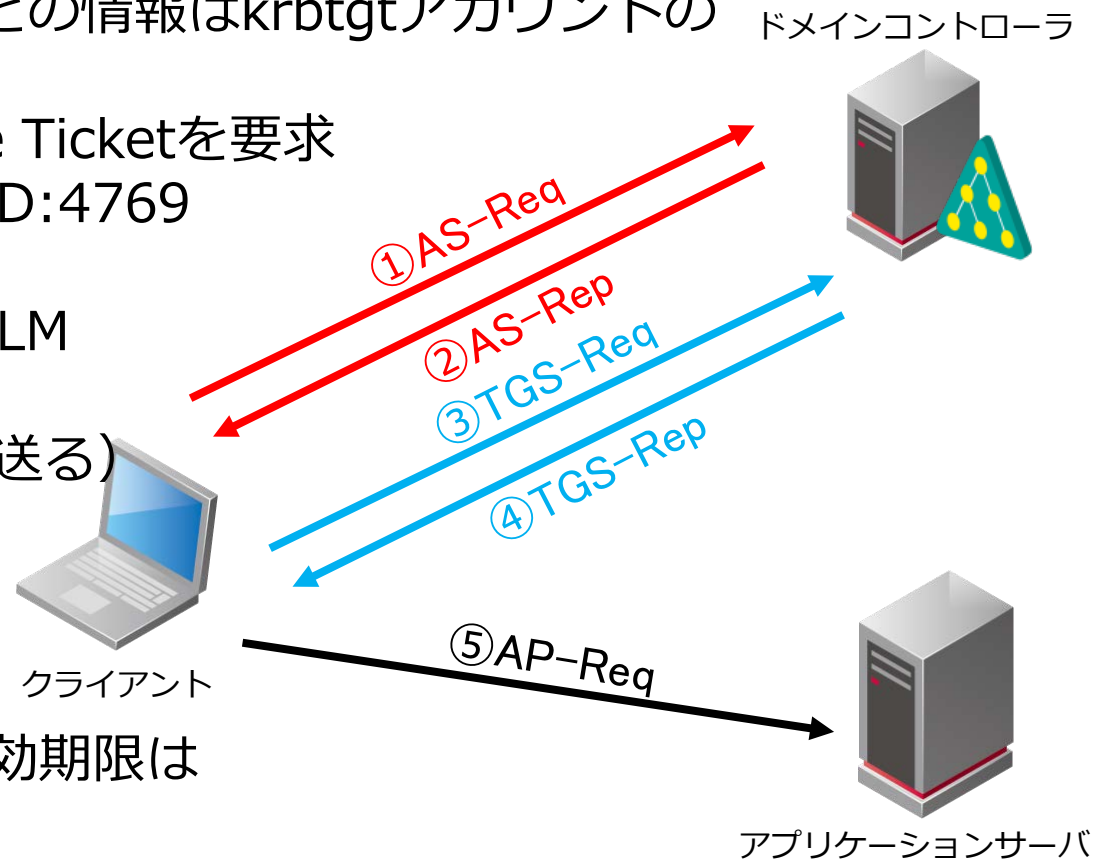
- NTLMv2認証
- チャレンジ・レスポンス方式



Windowsの認証方式 (2)

- Kerberos認証：ドメイン環境の認証方式
- 2種類のチケットを使って認証や認可を行う

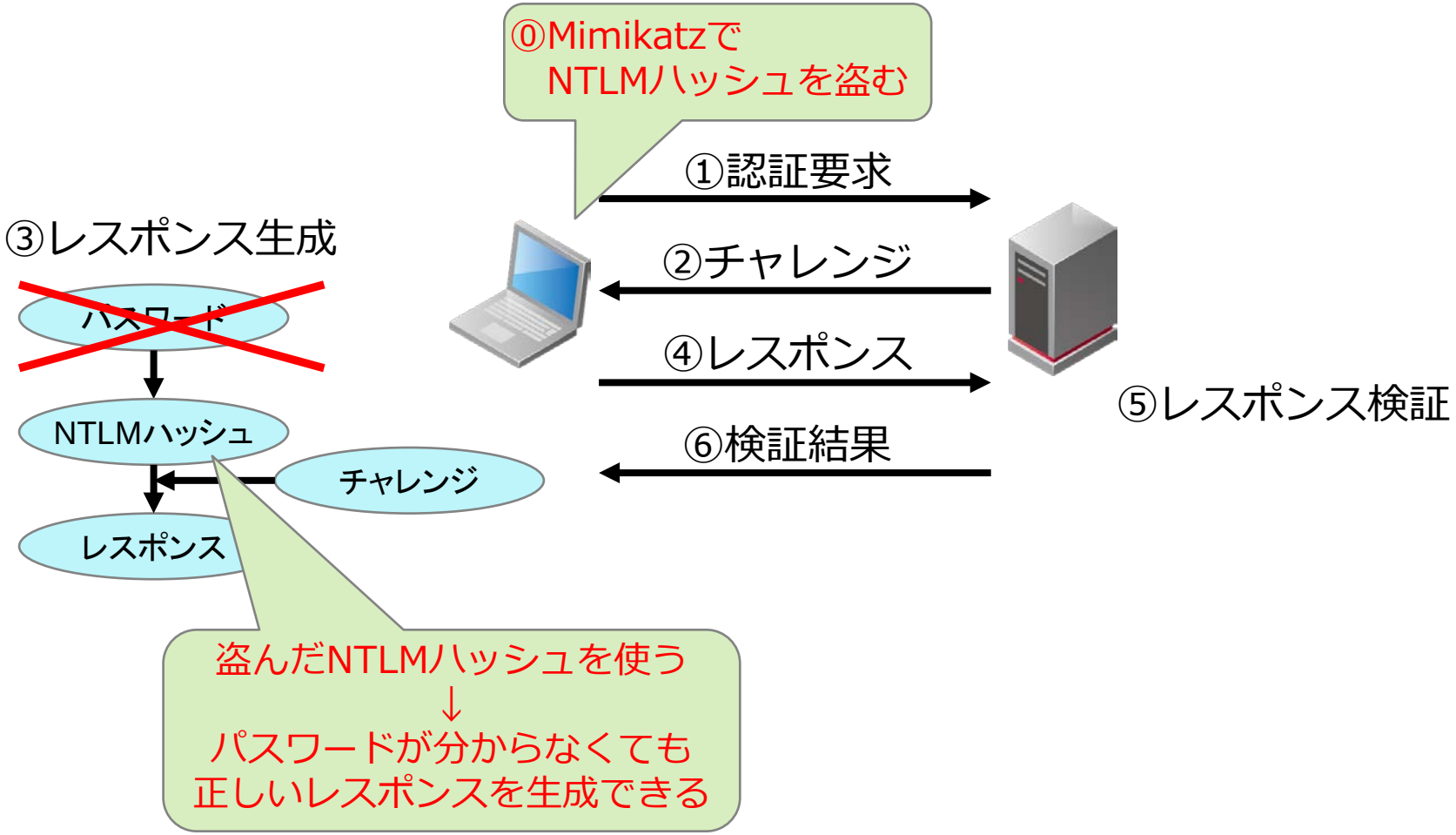
①Ticket-Granting Ticket (TGT)要求：イベントID:4768
②TGTを発行（ユーザ権限などの情報はkrbtgtアカウントのNTLMハッシュで暗号化）
③利用するサービスのService Ticketを要求（TGTも送る）：イベントID:4769
④Service Ticket (ST)を発行（サービスアカウントのNTLMハッシュで暗号化）
⑤サービスにアクセス（STも送る）：イベントID:4624, 4672



※TGTとService Ticketの有効期限はデフォルトで10時間

Pass-the-Hash (1)

- パスワードを入力せずに盗んだNTLMハッシュを利用して認証する。

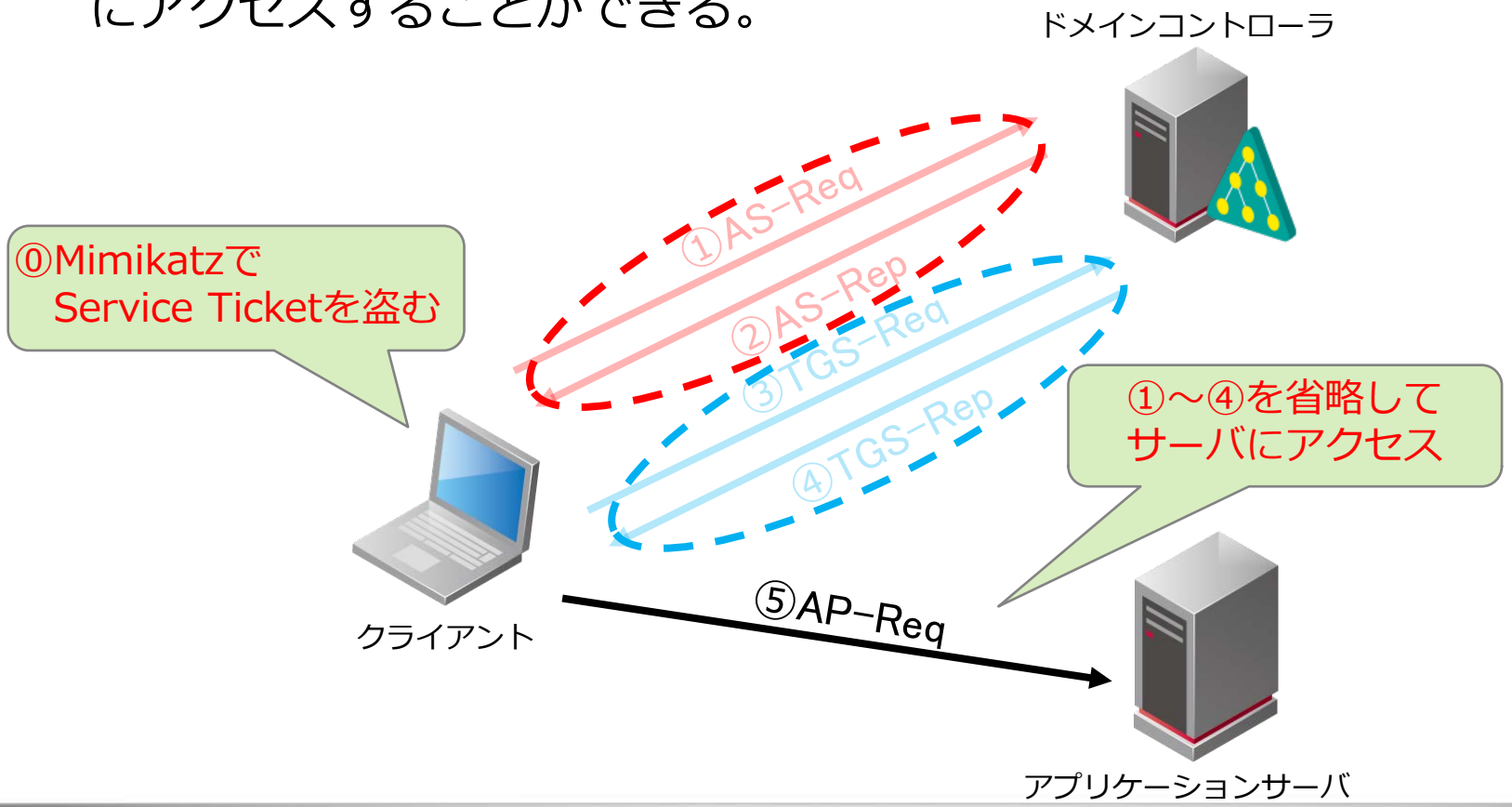


Pass-the-Hash (2)

- 検出方法：以下のログが記録される。
- イベントID: 4776：NTLM資格情報の確認
- イベントID: 4624：ログオン成功
  - ログオンタイプ：3
  - ログオンプロセス：NtLMSsp
  - 認証パッケージ：NTLM
  - パッケージ名 (NTLM のみ)：NTLM V2
- ドメイン環境では認証のほとんどはKerberos認証で行われるため、NTLM認証のログは注意すべき対象となる。

Pass-the-Ticket (1)

- Pass-the-Hashと同様に、パスワードを入力せずに盗んだまたは偽造したKerberos Ticketを利用する。
- 例）ファイルサーバ向けのService Ticketを入手した場合、①～④の処理を行わずにTicketのユーザ権限でファイルサーバのファイルにアクセスすることができる。



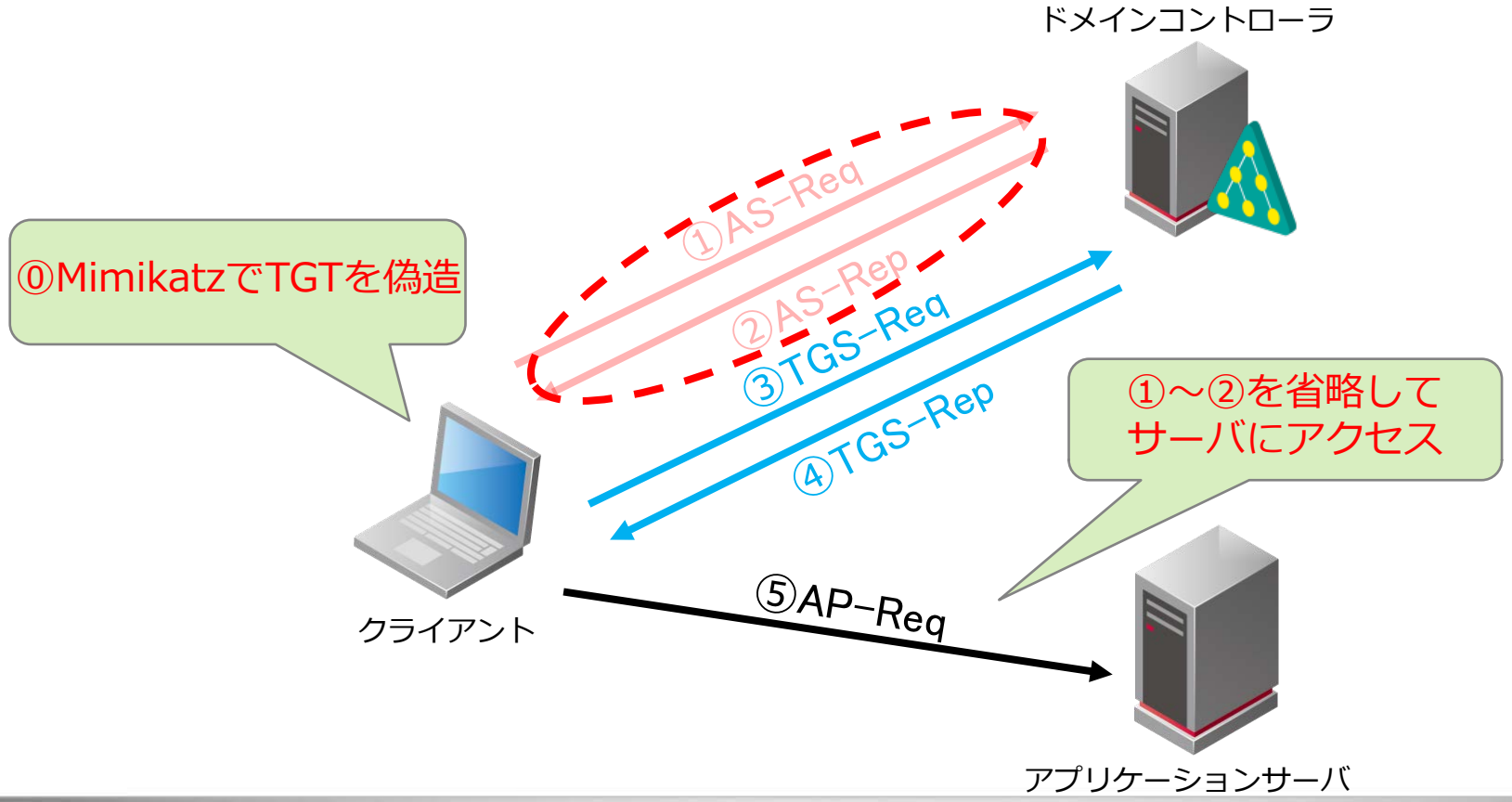
Pass-the-Ticket (2)

- 多くの場合、Pass-the-Ticketの手法で使用するチケットはGolden TicketやSilver Ticketであるため、検出方法の詳細はそれぞれの項目で記述する。

Golden Ticket

Golden Ticket (1)

- 偽造したTGTを送信して、Service Ticketを入手し、サービスにアクセスする攻撃手法。多くの場合、Domain Admins権限を持つようにTGTを偽造するので、任意のサービスにアクセス可能となる。



Golden Ticket (2)

- 偽造したTGTをドメインコントローラに送信して Service Ticketを発行させ、サービスを利用する。
- Golden Ticket作成に必要な情報
  - ドメイン名
  - ドメインSID
  - ドメインのkrbtgtアカウントのNTLMパスワードハッシュ
  - なりすましを行うユーザSID（とグループSID）
- Mimikatzで偽造したTGTの特徴
  - 有効期限：10年（Mimikatzデフォルト）
  - 任意のアカウント名（ドメイン内に存在しなくてもよい）

Golden Ticket (3)

- 検出方法：通常のKerberos認証で記録されるべきログが記録されない。
- Golden Ticket使用時に記録されないイベントID
  - イベントID: 4768：TGT要求
- 4769のログから10時間前までの間に4768が記録されていない場合、Golden Ticketが使われた可能性がある。
- 以下の特徴を持つ4769が記録される場合がある。
  - 「アカウント名」に存在しないユーザ名が入る。
  - 「アカウントドメイン」がすべて大文字になっていない。
- 誤検知となる要因
  - ログローテーションで4768のログが削除されてしまっている場合がある。
  - 通常の使い方をしていても、4768が記録されない場合がある。

Golden Ticket (4)

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
- Subscriptions

Security Number of events: 69,956 (!) New events available

Keywords	Date and Time	Source	Even...	Task Category
Audit Success	10/23/2017 4:52:45 P...	Microsoft Windows security a...	4624	Logon
Audit Success	10/23/2017 4:52:45 P...	Microsoft Windows security a...	4672	Special Logon
Audit Success	10/23/2017 4:52:45 P...	Microsoft Windows security a...	4769	Kerberos Service Ticket Op
Audit Success	10/23/2017 4:52:45 P...	Microsoft Windows security a...	4769	Kerberos Service Ticket Op
Audit Success	10/23/2017 4:52:33 P...	Microsoft Windows security a...	4634	Logoff
Audit Success	10/23/2017 4:52:33 P...	Microsoft Windows security a...	4624	Log

Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:
Account Name: hogehoge@mylab.local
Account Domain: mylab.local

Service Information:
Service Name: krbtgt
Service ID: MYLAB\krbtgt

Log Name: Security
Source: Microsoft Windows security Logged: 10/23/
Event ID: 4769 Task Category: Kerberos Service Ticket Operations

Actions
- Security
  - Open Saved Log...
  - Create Custom View...
  - Import Custom View...
  - Clear Log...
  - Filter Current Log...
  - Properties
  - Refresh
  - Help
- Event 4769, Microsoft Wind...
  - Event Properties

4769の前に4768がない

存在しないユーザ名
ドメイン名が大文字ではない

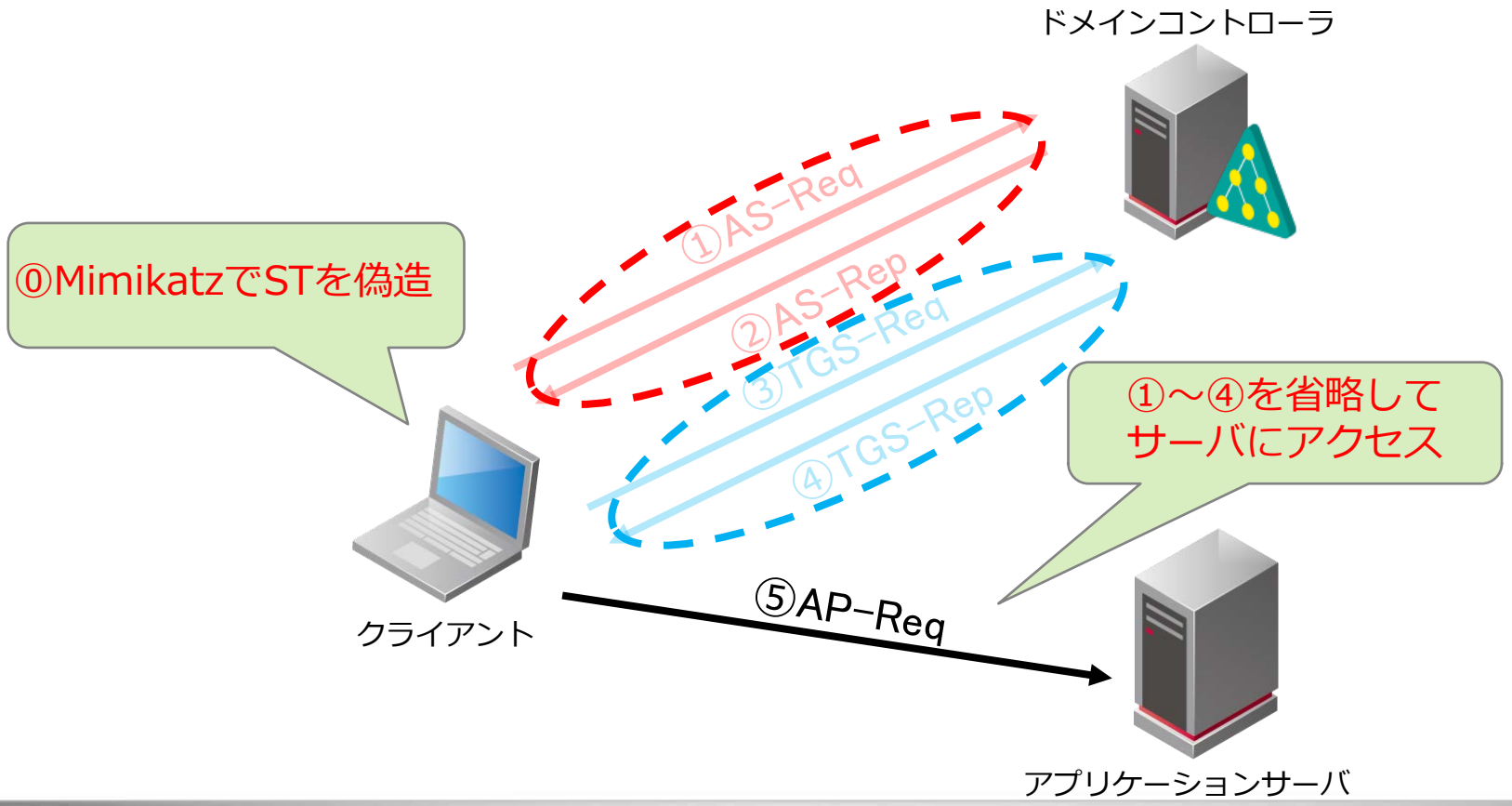
kerberos::golden /user:hogehoge /domain:mylab.local
/id:500 /sid:<DOMAIN_SID> /krbtgt:<NTLM_Hash> /ticket:hoge-golden.kirbi

8:41 PM
11/7/2017

Silver Ticket

Silver Ticket (1)

- 偽造したService Ticketを送信して、サービスにアクセスする。多くの場合、Domain Admins権限を持つようにService Ticketを偽造するので、任意のサービスにアクセス可能となる。



Silver Ticket (2)

- 偽造したService Ticketを使用してサービスを利用する。
- Silver Ticket作成に必要な情報
  - ドメイン名
  - ドメインSID
  - アプリケーションサーバのFQDN
  - サービスのNTLMハッシュ
  - なりすましを行うユーザSID（とグループSID）
  - サービス名(SPN)
- Mimikatzで偽造したService Ticketの特徴
  - 有効期限：10年（Mimikatzデフォルト）
  - 任意のアカウント名（ドメイン内に存在しなくてもよい）

Silver Ticket (3)

- 検出方法：通常のKerberos認証で記録されるべきログが記録されない。
- Silver Ticket使用時に記録されないイベントID
  - イベントID: 4768：TGT要求
  - イベントID: 4769：Service Ticketの要求
- 以下の条件を満たす場合、Silver Ticketが使われた可能性がある。
  - イベントID:4624（ログオン成功）から10時間前までの間に4769が記録されていない。
  - 4769のログから10時間前までの間に4768が記録されていない。

Silver Ticket (4)

- 誤検知となる要因
  - ログローテーションで4768, 4769のログが削除されてしまっている場合がある。
  - 通常の使い方をしていても、4768, 4769が記録されない場合がある。

Silver Ticket (5)

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
- Subscriptions

Security Number of events: 69,956 (!) New events available

Keywords	Date and Time	Source	Even...	Task Category
Audit Success	10/24/2017 8:16:11 P...	Microsoft Windows security a...	4634	Logoff
Audit Success	10/24/2017 8:16:04 P...	Microsoft Windows security a...	4624	Logon
Audit Success	10/24/2017 8:16:04 P...	Microsoft Windows security a...	4672	Special Logon
Audit Success	10/24/2017 8:16:03 P...	Microsoft Windows security a...	4634	Logoff
Audit Success	10/24/2017 8:16:03 P...	Microsoft Windows security a...	4624	Logon
Audit Success	10/24/2017 8:16:03 P...	Microsoft Windows security a...	4672	Special Logon

Event 4624, Microsoft Windows security auditing.

General Details

New Logon:
Account Name: fuga-cifs
Account Domain: mylab.local
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {f98a4731-f5aa-651f-6f1

Log Name: Security
Source: Microsoft Windows security Logged: 10/24/2017 8:16:04 PM
Event ID: 4624 Task Category: Logon

Actions
- Security
  - Open Saved Log...
  - Create Custom View...
  - Import Custom View...
  - Clear Log...
  - Filter Current Log...
  - Properties
  - Refresh
  - Help
- Event 4624, Microsoft Wind...
  - Properties
  - Task To This Ev...
  - Refresh

4768, 4769がない

存在しないユーザ名
ドメイン名が大文字ではない

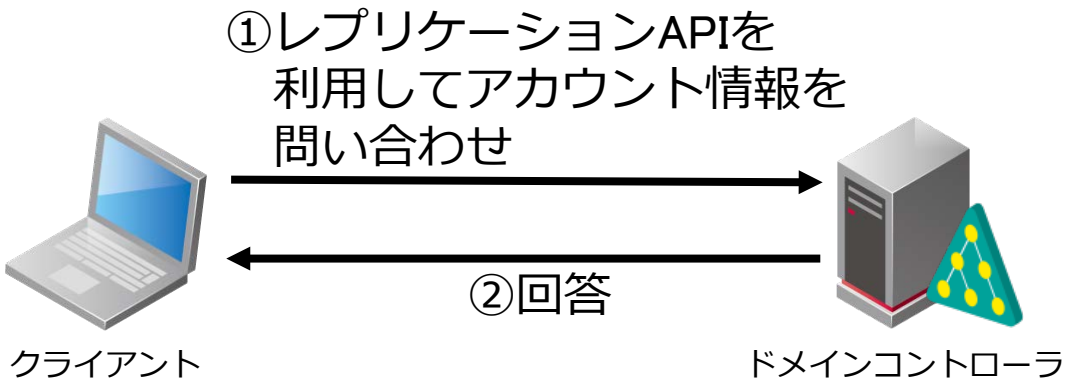
```
kerberos::golden /user:fuga-cifs /domain:mylab.local /id:500 /sid:<DOMAIN_SID>
    /ticket:fuga-silver-ad01-cifs.kirbi /target:ad01.mylab.local /service:cifs
    /rc4:<SERVICE_NTLM_Hash>
```

9:23 PM
11/7/2017

DCSync

DCSync (1)

- ドメインコントローラのレプリケーションAPIを使用して、任意のActive Directoryアカウントの情報をネットワーク経由で問い合わせる。
- ドメインコントローラを複数台で構成する場合に使用されるAPI。
- Mimikatzはドメインコントローラ上で動作する必要はない。



DCSync (2)

mimikatz 2.1.1 x64 (oe.eo)

```
mimikatz # lsadump::dcsync /user:krbtgt /domain:mylab.local
[DC] 'mylab.local' will be the domain
[DC] 'AD01.mylab.local' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 10/23/2017 11:37:34 AM
Object Security ID   : S-1-5-21-180789512-3239218266-3690940378-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 053dfd3a23f0578c6e558d55fd54ad3f
    ntlm- 0: 053dfd3a23f0578c6e558d55fd54ad3f
    lm  - 0: f876e010dbd289d74c5ed4099f35da6c

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 2f2a280cdfd6b6d9352c12407bfbfed7

* Primary:Kerberos-Newer-Keys *
    Default Salt : MYLAB.LOCALkrbtgt
    Default Iterations : 4096
```

DCSync (3)

- 検出方法：以下のログが記録される。
- イベントID: 4662が3回連続で記録される。
- Mimikatzを実行したアカウントが、4662のログの「セキュリティID」と「アカウント名」に入っている。
  - 通常、セキュリティIDはSYSTEMが、アカウント名はコンピュータアカウント（アカウント名の最後に「$」が最後に入る）が入る。
- どのクライアントからリクエストがあったのか記録されていないため、ファイアウォールなどのログと突き合わせる必要がある。

DCSync (4)

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
- Subscriptions

Security Number of events: 63,839 (!) New events available

Keywords	Date and Time	Source	Even...	Task Category
Audit Success	11/7/2017 1:26:00 AM	Microsoft Windows security a...	4672	Special Logon
Audit Success	11/7/2017 1:25:03 AM	Microsoft Windows security a...	4662	Directory Service Access
Audit Success	11/7/2017 1:25:03 AM	Microsoft Windows security a...	4662	Directory Service Access
Audit Success	11/7/2017 1:25:03 AM	Microsoft Windows security a...	4662	Directory Service Access
Audit Success	11/7/2017 1:25:00 AM	Microsoft Windows security a...	4634	Logoff
Audit Success	11/7/2017 1:25:00 AM	Microsoft Windows security a...	4624	Log
Audit Success	11/7/2017 1:25:00 AM	Microsoft Windows security a...	4672	Special Lo

Event 4662, Microsoft Windows security auditing.

General Details

An operation was performed on an object.

Subject:
Security ID: MYLAB\admin02
Account Name: admin02
Account Domain: MYLAB
Logon ID: 0x648EF0

Object:
Object Server: DS

Log Name: Security
Source: Microsoft Windows security
Logged:
Event ID: 4662
Task Cat
Level: Information
Keyword
User: N/A
Compute
OpCode: Info
More Information: Event Log Online Help

Actions
- Security
  - Open Saved Log...
  - Create Custom View...
  - Import Custom View...
  - Clear Log...
  - Filter Current Log...
  - Properties
  - Refresh
  - Help
- Event 4662, Microsoft Wind...
  - Event Properties
  - Attach Task To This Ev...
  - py
  - e Selected Events...
  - resh
  - lp

3回連続で4662

自然に発生するログ
セキュリティID：SYSTEM
アカウント名：AD01$

1:35 AM
11/7/2017

Skeleton Key

Skeleton Key (1)

- ドメインコントローラのlsass.exeプロセスにパッチを当てて、全てのアカウントを本来のパスワードとは異なるパスワードでも認証できるようにしてしまう。
- 元々はマルウェアが使用していた技術
  - Skeleton Key Malware Analysis
    - https://www.secureworks.com/research/skeleton-key-malware-analysis
- メモリパッチなので再起動すると効果はなくなる。

Skeleton Key (2)

- 検出方法：イベントID: 4769の「チケット暗号化の種類」が0x17 (RC4)になっている。
- バックドアパスワードでログオンすると、4769で記録される暗号化方式が0x17になる。
- 通常、4769の「チケット暗号化の種類」は0x12 (AES256)になっている。

- 暗号の種類は以下を参照。
  - 4768(S, F): A Kerberos authentication ticket (TGT) was requested.
  - https://docs.microsoft.com/en-us/windows/device-security/auditing/event-4768#table-4-kerberos-encryption-types

Skeleton Key (3)

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
- Subscriptions

Security Number of events: 63,839 (!) New events available

Keywords	Date and Time	Source	Even...	Task Category
Audit Success	11/1/2017 9:39:36 PM	Microsoft Windows security a...	4624	Logon
Audit Success	11/1/2017 9:39:36 PM	Microsoft Windows security a...	4648	Logon
Audit Success	11/1/2017 9:39:36 PM	Microsoft Windows security a...	4769	Kerberos Service Ticket Op
Audit Success	11/1/2017 9:39:35 PM	Microsoft Windows security a...	4634	Logoff
Audit Success	11/1/2017 9:39:35 PM	Microsoft Windows security a...	4634	Logoff

Event 4769, Microsoft Windows security auditing.

General Details

Additional Information:

Ticket Encryption Type: 0x17

Transited Services: -

This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	11/1/2017 9:39:36 PM
Event ID:	4769	Task Category:	Kerberos Service Ticket Operations
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	AD01.mylab.local
OpCode:	Info		
More Information:	Event Log Online Help		

Actions

Security
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help

Event 4769, Microsoft Wind...
- Event Properties
- Attach Task To This Ev...
- Copy
- Save Selected Events...
- Refresh
- Help

1:49 AM
11/7/2017

Mimikatzを実行した痕跡の発見方法（追加設定）

認証情報ダンプ

認証情報ダンプ (1)

- lsass.exeプロセスに保持されている認証情報を抽出する。

mimikatz 2.1.1 x64 (oe.eo)

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1201563 (00000000:0012559b)
Session           : CachedInteractive from 1
User Name         : admin01
Domain            : MYLAB
Logon Server      : AD01
Logon Time        : 11/6/2017 11:33:54 AM
SID               : S-1-5-21-180789512-3239218266-3690940378-1104
        msv :
         [00000003] Primary
         * Username : admin01
         * Domain   : MYLAB
         * NTLM     : 4daf37a50ea3d37e28d9017b9ee8bbb6
         * SHA1     : 498783e74aa1c2ec08c279372253334747112cbf3
         * DPAPI    : 53a6c332387e6fe0531fbfe155788857
        tspkg :
        wdigest :
         * Username : admin01
         * Domain   : MYLAB
         * Password : (null)
        kerberos :
         * Username : admin01
         * Domain   : MYLAB.LOCAL
         * Password : secret#secret0
        ssp :
        credman :

Authentication Id : 0 ; 671616 (00000000:000a3f80)
```

認証情報ダンプ (2)

- 検出方法：
- ダンプコマンドに対応するイベントログは残らない。
- ダンプコマンド実行にSeDebugPrivilege権限が必要であるため、セキュリティイベントログにイベントID: 4672（特殊なログオン）が記録されるが、これだけでは判断不可能。
- Sysmonを使用してイベントログに残す方法がある。

認証情報ダンプ (3)

- Sysmon：Windowsのシステムアクティビティを記録するツール
  - プロセス生成・停止・プロセスに対するアクセス
  - ネットワーク接続
  - WMI登録 など
- 認証情報ダンプの時、Mimikatzは特定のアクセスマスクでlsass.exeプロセスにアクセスする。
- Sysmonでlsass.exeプロセスにアクセスするプロセスを記録しておくことでMimikatzを見つけられる可能性がある。

認証情報ダンプ (4)

- Hunting mimikatz with sysmon: monitoring OpenProcess()
  - https://blog.3or.de/hunting-mimikatz-with-sysmon-monitoring-openprocess.html

sekurlsa::*	kuhl_m_sekurlsa_acquireLSA()	lsass.exe	PROCESS_VM_READ | PROCESS_QUERY_INFORMATION	0x1410	for Windows Version < 5
sekurlsa::*	kuhl_m_sekurlsa_acquireLSA()	lsass.exe	PROCESS_VM_READ | PROCESS_QUERY_LIMITED_INFORMATIO	0x1010	for Windows Version >= 6

認証情報ダンプ (5)

- Sysmonコンフィグ例

```
<Sysmon schemaversion="3.40">
  <!-- Capture all hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
      <Signature condition="contains">microsoft</Signature>
      <Signature condition="contains">windows</Signature>
    </DriverLoad>
    <!-- Do not log process termination -->
    <ProcessTerminate onmatch="include" />
    <!-- Log network connection if the destination port equal 443 -->
    <!-- or 80, and process isn't InternetExplorer -->
    <NetworkConnect onmatch="include">
      <DestinationPort>443</DestinationPort>
      <DestinationPort>80</DestinationPort>
    </NetworkConnect>
    <NetworkConnect onmatch="exclude">
      <Image condition="end with">iexplore.exe</Image>
      <Image condition="end with">MicrosoftEdge.exe</Image>
    </NetworkConnect>
    <ProcessAccess onmatch="include">
      <TargetImage condition="end with">lsass.exe</TargetImage>
    </ProcessAccess>
  </EventFiltering>
</Sysmon>
```

認証情報ダンプ (6)

Event Viewer

File Action View Help

Operational Number of events: 16,074 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	11/1/2017 7:01:46 PM	Sysmon	10	Process accessed (rule: ProcessAccess)
Information	11/1/2017 6:56:55 PM	Sysmon	10	Process accessed (rule: ProcessAccess)
Information	11/1/2017 6:56:23 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	11/1/2017 6:55:32 PM	Sysmon	3	Network connection detected (rule: ...
Information	11/1/2017 6:55:32 PM	Sysmon	3	Network connection detected (rule: ...

Event 10, Sysmon

General Details

SourceProcessGUID: {8dedbc91-9a47-59f9-0000-0010b96fa000}
SourceProcessId: 2740
SourceImage: C:\Users\user01.MYLAB\Desktop\tools\mimikatz_trunk_2.1.1 20170813\x64\mimikatz.exe
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1010
...|C:\Windows\System32\KERNELBASE.dll+3b51d|C:\Users\user01.MYLAB\Desktop\tools\mimikatz_trunk_2.1.1 20170813\x64\mimikatz.exe+6dc6c|C:

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	11/1/2017 6:56:55 PM
Event ID:	10	Task Category:	Process accessed (rule: ProcessAccess)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WIN10.mylab.local
OpCode:	Info		
More Information:	Event Log Online Help		

Actions

Operational
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Disable Log
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help

Event 10, Sysmon
- Event Properties
- Attach Task To This Ev...
- Copy
- Save Selected Events...
- Refresh
- Help

認証情報ダンプ (7)

- svchost.exeやMsMpEng.exe(Windows Defender)など、mimikatz.exe以外のプロセスも同じアクセスマスクでアクセスする場合があるため、確実にMimikatzのみを記録することはできない。
- Sysmonイベントログから、lsass.exeへのアクセスを抽出するPowerShellスクリプト

```
$events = Get-WinEvent -Path C:¥Windows¥System32¥winevt¥Logs¥Microsoft-Windows-Sysmon%4Operational.evtx -FilterXPath "Event[System[(EventID=10)]] and Event[EventData[(Data[@Name='SourceImage']!='C:¥Windows¥System32¥svchost.exe' and Data[@Name='SourceImage']!='C:¥Program Files¥Windows Defender¥MsMpEng.exe') and Data[@Name='TargetImage']='C:¥Windows¥system32¥lsass.exe' and (Data[@Name='GrantedAccess']='0x1410' or Data[@Name='GrantedAccess']='0x1010')]]"

foreach($event in $events){
    $xml = [xml]$event.ToXml()
    $xml.Event.EventData.Data | Format-Table -AutoSize -Wrap
}
```

認証情報ダンプ (8)

Administrator: Command Prompt

```
Name              #text
----              -----
UtcTime           2017-10-23 11:25:23.362
SourceProcessGUID {8DEDBC91-ACF3-59ED-0000-00103A57A400}
SourceProcessId   1716
SourceThreadId    2268
SourceImage       C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetProcessGUID {8DEDBC91-9012-59ED-0000-00108D8B0000}
TargetProcessId   812
TargetImage       C:\Windows\system32\lsass.exe
GrantedAccess     0x1010
CallTrace         C:\Windows\SYSTEM32\ntdll.dll+a5864|C:\Windows\System32\KERNELBASE.dll+3b51d|UNKNOWN(0000028EAA77BA3C
                  )


Name              #text
----              -----
UtcTime           2017-10-23 11:13:45.529
SourceProcessGUID {8DEDBC91-CEC1-59ED-0000-001046C5CB00}
SourceProcessId   4744
SourceThreadId    228
SourceImage       C:\Users\user01.MYLAB\Desktop\tools\mimikatz_trunk_2.1.1 20170813\x64\mimikatz.exe
TargetProcessGUID {8DEDBC91-9012-59ED-0000-00108D8B0000}
TargetProcessId   812
TargetImage       C:\Windows\system32\lsass.exe
GrantedAccess     0x1010
CallTrace         C:\Windows\SYSTEM32\ntdll.dll+a5864|C:\Windows\System32\KERNELBASE.dll+3b51d|C:\Users\user01.MYLAB\De
                  sktop\tools\mimikatz_trunk_2.1.1
```

Kerberos Ticketファイル

Kerberos Ticketファイル (1)

- MimikatzはKerberos Ticketをファイルとして保存することができる。
- ファイル保存の操作はイベントログに残らない。
- 認証情報ダンプと同様にSysmonを使用してイベントログに残す方法が使えるが、Mimikatzのアクセスマスクが同じであるため、Sysmonログだけではどちらの機能を使用したのか区別することはできない。
- 通常は存在しないファイルであるため、ファイルが存在すること自体が（またはその形跡があれば）、Pass-the-TicketやGolden Ticket/Silver Ticketが実行された可能性を示唆している。

Kerberos Ticketファイル (2)

- 検出方法：通常は存在しないKerberos Ticketのファイルを検出する。
- Ticketファイルを検知するためのYaraルール
  - https://blog.didierstevens.com/2016/08/12/mimikatz-golden-ticket-dcsync/

```
rule mimikatz_kirbi_ticket
{
    meta:
        description     = "KiRBi ticket for mimikatz"
        author          = "Benjamin DELPY (gentilkiwi); Didier Stevens"

    strings:
        $asn1           = { 76 82 ?? ?? 30 82 ?? ?? a0 03 02 01 05 a1 03 02 01 16 }
        $asn1_84        = { 76 84 ?? ?? ?? ?? 30 84 ?? ?? ?? ?? a0 84 00 00 00 03 02 01 05
a1 84 00 00 00 03 02 01 16 }

    condition:
        $asn1 at 0 or $asn1_84 at 0
}
```

イベントログで検知できること

Mimikatz機能	デフォルト設定で検知可能	追加設定で検知可能
認証情報ダンプ	×	○
Pass-the-Hash	○	–
Pass-the-Ticket	○	–
Golden Ticket/Silver Ticket	○	–
Kerberos Ticketファイル	×	○
DCSync	○	–
Skeleton Key	○	–

検出のスクリプト化

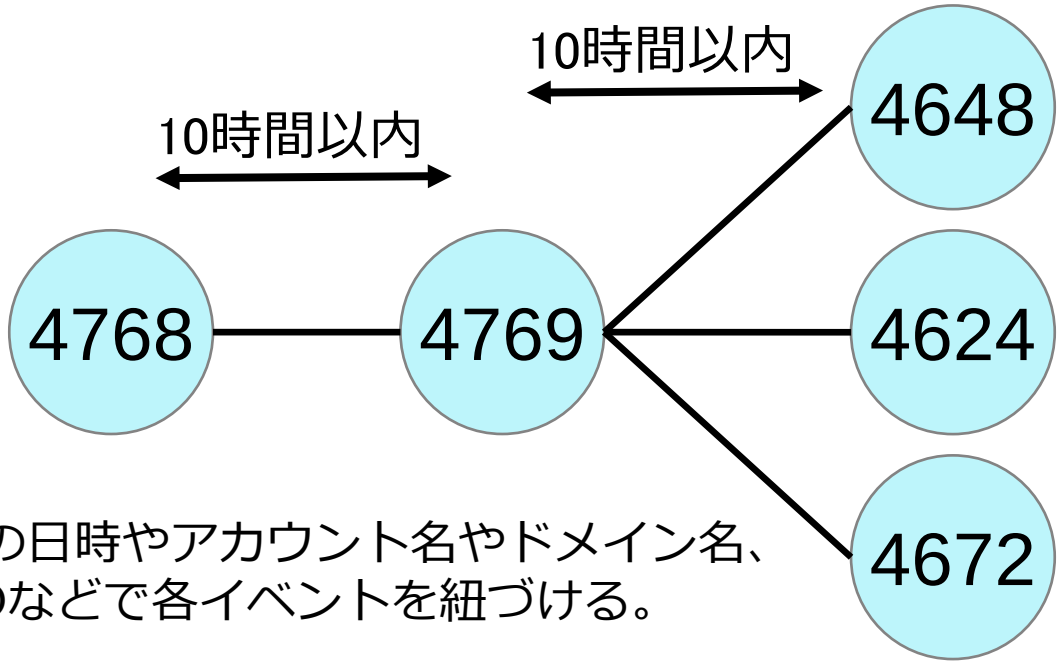
スクリプト化

- イベントビューワを使って手動で検出することも不可能ではないが、Golden TicketやSilver Ticketは複数のイベントを紐づけて読み解く必要があるため、解析はスクリプト化を検討した方が良い。

- イベントログを読み込むためのライブラリ
- python-evtx
  - https://github.com/williballenthin/python-evtx
- libevtx
  - https://github.com/libyal/libevtx

スクリプト実装例 (1)

- python-evtxを利用して、Golden TicketとSilver Ticketの使用を検出するPoCを作成した。
- 基本的な考え方：イベントID: 4768をルートとするKerberos認証のイベントツリーを作成し、不完全なツリーを疑わしい認証ログとして出力する。



ログの日時やアカウント名やドメイン名、GUIDなどで各イベントを紐づける。

スクリプト実装例 (2)

- サンプルのセキュリティイベントログ件数

```
Security    イベント数: 37,981
```

- スクリプトで処理

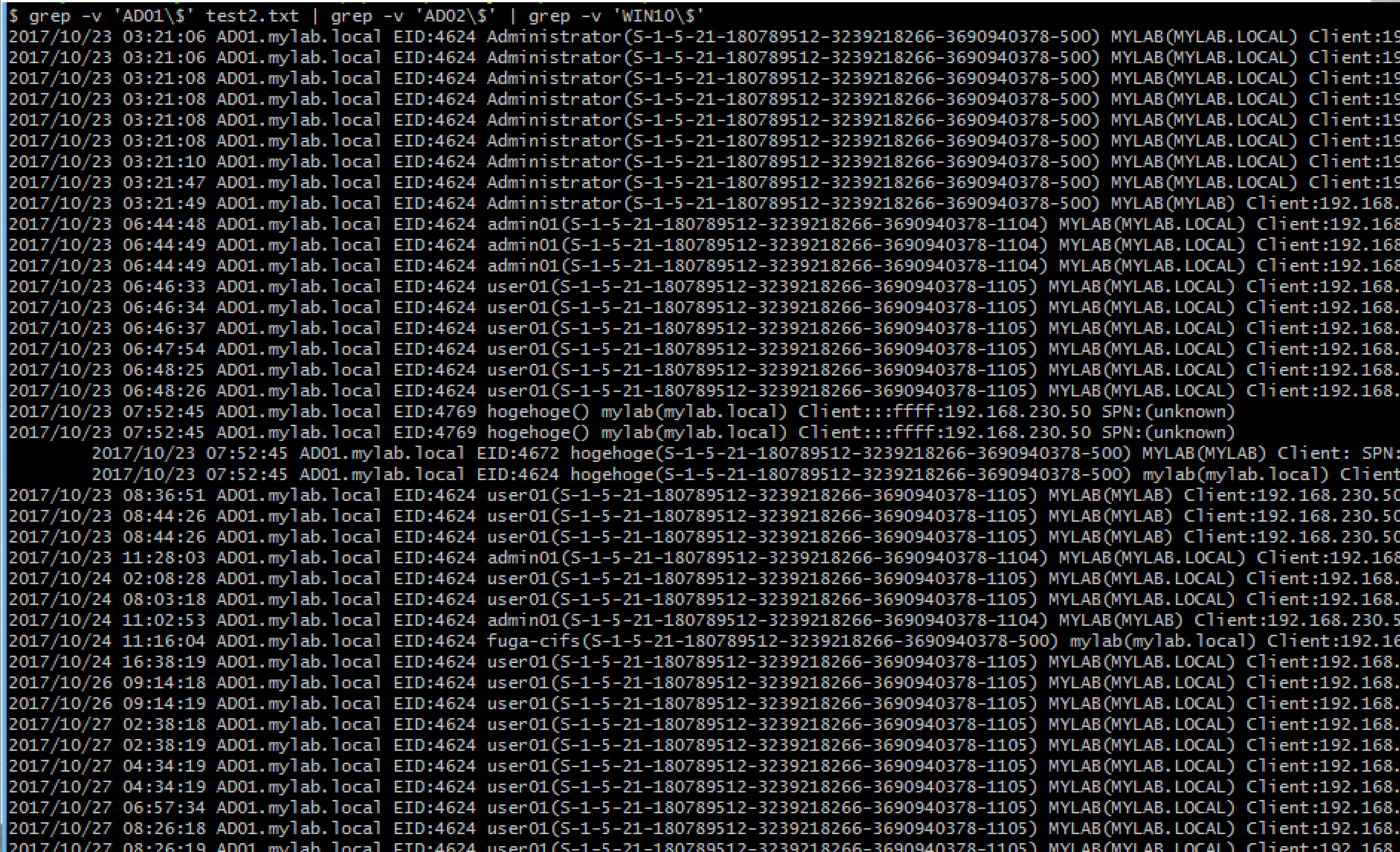
```
¥TechnicalWEEK>python ticket_tree.py Security.evtx > test.txt
```

- スクリプトで処理した後の件数

```
$ wc -l test2.txt
7497 test2.txt
```

スクリプト実装例 (3)

- 不要なログを除外（43件まで絞り込み）



```
$ grep -v 'AD01\$' test2.txt | grep -v 'AD02\$' | grep -v 'WIN10\$'
2017/10/23 03:21:06 AD01.mylab.local EID:4624 Administrator(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB.LOCAL) Client:19
2017/10/23 03:21:06 AD01.mylab.local EID:4624 Administrator(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB.LOCAL) Client:19
2017/10/23 03:21:08 AD01.mylab.local EID:4624 Administrator(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB.LOCAL) Client:19
2017/10/23 03:21:08 AD01.mylab.local EID:4624 Administrator(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB.LOCAL) Client:19
2017/10/23 03:21:08 AD01.mylab.local EID:4624 Administrator(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB.LOCAL) Client:19
2017/10/23 03:21:08 AD01.mylab.local EID:4624 Administrator(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB.LOCAL) Client:19
2017/10/23 03:21:10 AD01.mylab.local EID:4624 Administrator(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB.LOCAL) Client:19
2017/10/23 03:21:47 AD01.mylab.local EID:4624 Administrator(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB.LOCAL) Client:19
2017/10/23 03:21:49 AD01.mylab.local EID:4624 Administrator(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB) Client:192.168.
2017/10/23 06:44:48 AD01.mylab.local EID:4624 admin01(S-1-5-21-180789512-3239218266-3690940378-1104) MYLAB(MYLAB.LOCAL) Client:192.168
2017/10/23 06:44:49 AD01.mylab.local EID:4624 admin01(S-1-5-21-180789512-3239218266-3690940378-1104) MYLAB(MYLAB.LOCAL) Client:192.168
2017/10/23 06:44:49 AD01.mylab.local EID:4624 admin01(S-1-5-21-180789512-3239218266-3690940378-1104) MYLAB(MYLAB.LOCAL) Client:192.168
2017/10/23 06:46:33 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/23 06:46:34 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/23 06:46:37 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/23 06:47:54 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/23 06:48:25 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/23 06:48:26 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/23 07:52:45 AD01.mylab.local EID:4769 hogehoge() mylab(mylab.local) Client:::ffff:192.168.230.50 SPN:(unknown)
2017/10/23 07:52:45 AD01.mylab.local EID:4769 hogehoge() mylab(mylab.local) Client:::ffff:192.168.230.50 SPN:(unknown)
        2017/10/23 07:52:45 AD01.mylab.local EID:4672 hogehoge(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB(MYLAB) Client: SPN:
        2017/10/23 07:52:45 AD01.mylab.local EID:4624 hogehoge(S-1-5-21-180789512-3239218266-3690940378-500) mylab(mylab.local) Client
2017/10/23 08:36:51 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB) Client:192.168.230.50
2017/10/23 08:44:26 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB) Client:192.168.230.50
2017/10/23 08:44:26 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB) Client:192.168.230.50
2017/10/23 11:28:03 AD01.mylab.local EID:4624 admin01(S-1-5-21-180789512-3239218266-3690940378-1104) MYLAB(MYLAB.LOCAL) Client:192.168
2017/10/24 02:08:28 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/24 08:03:18 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/24 11:02:53 AD01.mylab.local EID:4624 admin01(S-1-5-21-180789512-3239218266-3690940378-1104) MYLAB(MYLAB) Client:192.168.230.5
2017/10/24 11:16:04 AD01.mylab.local EID:4624 fuga-cifs(S-1-5-21-180789512-3239218266-3690940378-500) mylab(mylab.local) Client:192.16
2017/10/24 16:38:19 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/26 09:14:18 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/26 09:14:19 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/27 02:38:18 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/27 02:38:19 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/27 04:34:19 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/27 04:34:19 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/27 06:57:34 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/27 08:26:18 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
2017/10/27 08:26:19 AD01.mylab.local EID:4624 user01(S-1-5-21-180789512-3239218266-3690940378-1105) MYLAB(MYLAB.LOCAL) Client:192.168.
```

スクリプト実装例 (4)

- アカウント名を絞り込み

```
$ grep -v 'AD01\$' test2.txt | grep -v 'AD02\$' | grep -v 'WIN10\$' | cut -d' ' -f5 | sort | uniq
admin01(S-1-5-21-180789512-3239218266-3690940378-1104)
Administrator(S-1-5-21-180789512-3239218266-3690940378-500)
ANONYMOUS
fuga-cifs(S-1-5-21-180789512-3239218266-3690940378-500)
hogehoge()
hogehoge(S-1-5-21-180789512-3239218266-3690940378-500)
user01(S-1-5-21-180789512-3239218266-3690940378-1105)
```

- この中で疑わしいアカウント
  - fuga-cifs
  - hogehoge
  - Administratorと同じSIDを持っている

スクリプト実装例 (5)

- 疑わしいアカウント名で絞り込み

```
$ grep -P "(fuga|hoge)" test2.txt
2017/10/23 07:52:45 AD01.mylab.local EID:4769 hoge                    local) Client:::ffff:192.168.230.50 SPN:(unkn
2017/10/23 07:52:45 AD01.mylab.local EID:4769 hogehoge() mylab(mylab.local) Client:::ffff:192.168.230.50 SPN:(unkn
        2017/10/23 07:52:45 AD01.mylab.local EID:4672 hogehoge(S-1-5-21-180789512-3239218266-3690940378-500) MYLAB
        2017/10/23 07:52:45 AD01.mylab.local EID:4624 hogehoge(S-1-5-21-180789512-3239218266-3690940378-500) mylab
2017/10/24 11:16:04 AD01.mylab.local EID:4624 fuga-cifs(S-1-5-21-180789512-3239218266-3690940378-500) mylab(mylab.
```

4768がない

4768, 4769がない

- 通常のKerberos認証のログ

```
2017/10/23 03:19:38 AD01.mylab.local EID:4768 admin01(S-1-5-21                    940378-1104) mylab(mylab)
        2017/10/23 03:19:38 AD01.mylab.local EID:4769 admin01() MYLAB(MYLAB.LOCAL) Client:::ffff:192.168.230.11 SP
        2017/10/23 03:19:38 AD01.mylab.local EID:4769 admin01() MYLAB(MYLAB.LOCAL) Client:::ffff:192.168.230.11 SP
                2017/10/23 03:19:38 AD01.mylab.local EID:4672 admin01(S-1-5-21-180789512-3239218266-3690940378-110
                2017/10/23 03:19:38 AD01.mylab.local EID:4624 admin01(S-1-5-21-180789512-3239218266-3690940378-110
```

4768, 4769, 4624, 4672が揃っている

- 以上より、hogehogeがGolden Ticketを使用し、fuga-cifsがSilver Ticketを使用していたことが分かる。

まとめ

まとめ (1)

- 起動の日時や回数はPrefetchやPowerShellのログから参照できる。
  - ファイル名が変更されるとMimikatzとは判別できない。
- セキュリティイベントログを解析してMimikatzの攻撃を検出できる。
  - 解析作業効率化のためスクリプト化を検討。
- セキュリティイベントログに残らない攻撃手法はSysmonでログに記録する。
  - ホスト上で常に動作させる必要がある。
  - 無駄なログを削減するため、設定ファイルのチューニングが必要。

まとめ (2)

- AppLocker/ソフトウェア制限ポリシー
  - プログラムのホワイトリスト運用も視野に入れる。
- LSA保護モード(Win8.1+)
  - 認証情報ダンプやSkeleton Keyを防ぐことができる。
  - https://msdn.microsoft.com/ja-jp/library/dn408187(v=ws.11).aspx
- Protected Usersグループ(Win8.1+)
  - http://go.microsoft.com/fwlink/?LinkId=298939
- Credential Guard/Remote Credential Guard(Win10)
  - https://docs.microsoft.com/ja-jp/windows/access-protection/credential-guard/credential-guard
  - https://docs.microsoft.com/ja-jp/windows/access-protection/remote-credential-guard

IIJ Internet Initiative Japan

ご清聴ありがとうございました

Ongoing Innovation