Computer Security Symposium 2017
23 - 25 October 2017

Sysmon を用いた mimikatz の悪用の検知

松田 亘[†1]　藤本 万里子[†1]　満永 拓邦[†1]

概要：標的型攻撃において，組織に侵入した攻撃者は mimikatz という攻撃ツールを使って組織内で横展開を試みることが多い．mimikatz を使う攻撃では，正規ユーザか攻撃者によるアクセスかを判別するのが難しいという問題がある．そこで，Sysmon を使用して，コンピュータ上で mimikatz がロードした DLL を検知する研究が行われているが，特定の Windows や mimikatz のバージョンのみを対象としているため，実環境では誤検知が発生する可能性がある．本研究では，Windows や mimikatz のバージョンによってロードされる DLL の違いを網羅的に検証し，誤検知を軽減する手法について調査する．また，分析エンジンである Elasticsearch を用いてログを分析し，効率的に検知する方法についても述べる．

キーワード：mimikatz, Sysmon, 標的型攻撃, 横展開, Elasticsearch

Detecting mimikatz by Sysmon

Wataru Matsuda[†1]　Mariko Fujimoto[†1]　Takuho Mitsunaga[†1]

Abstract: In targeted attacks, attackers who have intruded into an office network often use a tool called “mimikatz” to steal credentials in order to attempt to perform lateral movement. It is difficult to judge whether an access is made by a legitimate user or an attacker when mimikatz used. As a breakthrough, some methods have been proposed which detect DLLs loaded by mimikatz using Sysmon. However, false detection can be caused because they are tested on the specific Windows and mimikatz versions. This presentation proposes methods to reduce false detection rate by investigating difference among Windows and mimikatz versions. Furthermore, a technique using Elasticsearch (an analysis engine) to effectively detect compromised machines will be introduced.

Keywords: mimikatz, Sysmon, APT, Lateral Movement, Elasticsearch

1. はじめに

標的型攻撃において，組織に侵入した攻撃者は効率的に組織を侵害するために，Active Directory（以下，AD）を狙う傾向にある[1]. AD を侵害するために，Windows 系 OS を攻撃するツールである mimikatz を使って他のコンピュータやドメインコントローラに対して横展開を試みることが多い．mimikatz を使った攻撃では，正規のアカウントが悪用されるため，システム管理者は正規ユーザか攻撃者によるアクセスなのかを判別するのが難しいという問題がある．そのような背景の中，mimikatz がロードする DLL に着目し，Sysmon[2]を使用して，コンピュータ上で mimikatz が使用された痕跡を検知する研究が行われている．

ただし，既存の研究で紹介されている検知手法は特定の DLL のロードを行っているかをもとに mimikatz の利用の有無を判断しているが，mimikatz を使用する環境(Windows や mimikatz のバージョン)よってロードする DLL が異なるため，誤検知が発生する可能性がある．そこで，本研究では，Windows のバージョンに依存して mimikatz がロードする DLL の違いを網羅的に調査して，検知すべき DLL の検証を行い，誤検知を軽減する手法について検証とその評価を行う．

また，ログ分析エンジンである Elasticsearch[3]を用いてログを集約し，分析することで，侵害されたコンピュータを効率的に検知する方法についても紹介する．

2. AD に対する攻撃手法

標的型攻撃において，攻撃対象の組織が AD を使っている場合，AD を侵害することにより，効率的に目的を達成しようとする．攻撃者が組織内に侵入すると，正規のドメインアカウントを悪用して，組織を横断的に侵害し（横断的侵害），最終的にドメイン管理者権限アカウントを侵害し，組織内の機密情報を窃取する．標的型攻撃では組織内への侵入自体を防ぐことは難しいが，侵入されても横断的侵害の時点で早期に気づくことができれば被害を最小限に抑えることも可能である．本章では，AD や標的型攻撃などの説明を交えながら，AD への攻撃を検知することの必要性について述べる．

2.1 典型的な標的型攻撃の流れ

典型的な標的型攻撃はサイバーキルチェーンと呼ばれ

†1 東京大学情報学環 セキュア情報化社会研究グループ, The University of Tokyo, Secure information society research group

る複数のステップに分けることができ，本研究では以下 4 つのプロセスに分類する．横断的侵害の時点で気づき，対処することで攻撃者が目的達成に到達することを防止することが可能となる．

準備：標的組織の情報を入念に調査し，攻撃ツールやマルウエアなど攻撃の準備を整える

潜入：不正な実行ファイルを添付した標的型メールの送付や不正な URL への誘導などにより，組織内のコンピュータをマルウエアに感染させる

横断的侵害：感染コンピュータを遠隔操作することで，組織内部のネットワーク情報の探索や感染の拡大を行い，目的を達成するまで組織内ネットワークを横断的に侵害する

目的達成：機密情報の窃盗など本来の目的を達成する

2.2 Active Directory の機能

AD は Microsoft 社が提供するディレクトリサービスで，ドメインと呼ばれる管理単位を持ち，ドメインに属するアカウントやコンピュータ，ファイルなどのリソースを集中的に管理することができる．AD では Kerberos 認証や NTLM 認証と呼ばれる認証方式が用いられ，Kerberos 認証であれば，認証チケットと呼ばれる認証情報を用いてアカウント認証などを行う．認証サーバとしてドメインコントローラが設置され，ドメインを管理したりするアカウントをドメイン管理者アカウントと呼ぶ．ドメイン管理者はドメインに所属するリソースを一元的に管理することができ，すべてのリソースにアクセスすることも可能であるなど，非常に強力な権限を有している．そのため，組織内に侵入した攻撃者もドメイン管理者権限を窃取しようと試みる．

2.3 mimikatz を悪用した AD に対する攻撃

組織内に侵入した攻撃者が AD を攻撃する場合，mimikatz と呼ばれる攻撃ツールが悪用されることが多い[1][4]．mimikatz にはコンピュータのメモリに保存されている認証情報を窃取したり，AD の脆弱性（MS14-068 など）を悪用して権限昇格を行ったり，バックドアである Golden Ticket を作成するなど，Windows 系 OS を侵害するための多くの機能を有している．図 1 は mimikatz によりコンピュータに保存された認証情報を窃取している画面である．

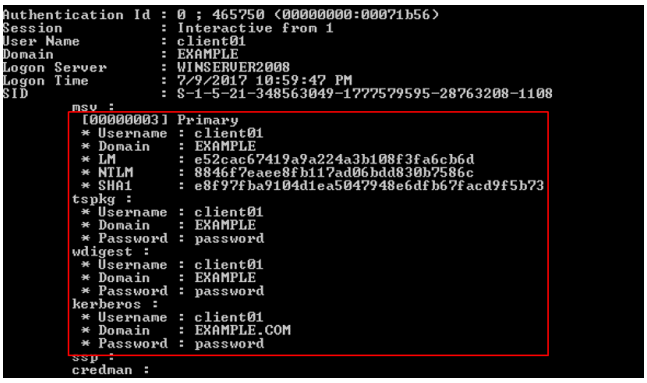

図 1　mimikatz による情報窃取

Figure 1　Stolen credentials by mimikatz.

以下に組織内に侵入した攻撃者の典型的な攻撃の例を紹介する（図 2）．前提として侵入に成功したコンピュータで使用されているアカウントはローカル管理者権限と一般ユーザ権限（Domain Users グループに所属しているユーザ）しか有しておらず，機密情報へのアクセス権限はないものとする．

・組織内に侵入した攻撃者は，mimikatz を用いてコンピュータのメモリに保存された認証情報を窃取する

・窃取した認証情報を悪用し，他コンピュータにアクセスしたり，不正な認証チケットを作成したりする

・mimikatz を用いて AD の脆弱性（MS14-068）などを悪用し，一般ユーザ権限からドメイン管理者に権限昇格する

・組織内の機密情報を窃取する

・mimikatz を用いて Golden Ticket とよばれるバックドアを作成し，別のコンピュータや次回の攻撃で悪用する

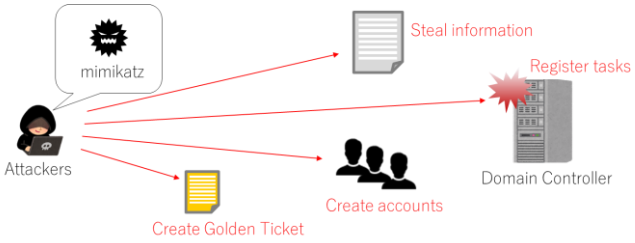

図 2　mimikatz による攻撃の例

Figure 2　An example of attacking by mimikatz.

このように攻撃者は侵害したコンピュータで mimikatz を悪用し，横断的侵害を試みる．そのため，mimikatz の悪用を早期に検知することが重要である．

2.4 攻撃検知のための Windows イベントログ

ドメインコントローラには認証に関するログなどが Windows イベントログという形で集約されているため，一元的に確認することができる．Sysmon と呼ばれる Microsoft 社が提供する無償のツールを使用することで，Windows プ

ロセスの起動やそのプロセスがロードした DLL，プロセス ID，起動したアカウント情報などの情報を Windows イベントログとして残すことができる．しかし，Sysmon ログについては，ドメインコントローラに集約されず，各コンピュータ内部に Windows イベントログとして保存される．図 3 のように Sysmon ログはイベント ID7 として記録され，プロセスに関する様々な情報が記録される．Image として記載されている箇所が親プロセスであり，図例では mimikatz.exe が親プロセスである．ImageLoaded として記載されている箇所がロードされた DLL を表している．図例では wintrust.dll がロードされた DLL であり，mimikatz.exe が wintrust.dll をロードしたことを表している．他にもプロセス ID やプロセスを起動したアカウントなどの情報が記載されている．

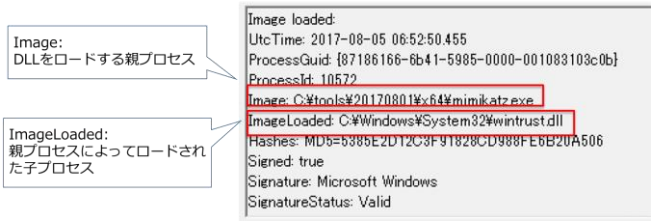

図 3　Sysmon ログの一例
Figure 3　Example of Sysmon log.

3. 関連研究

Jake Liefer は mimikatz がロードする DLL に着目して，mimikatz 悪用の検知手法を提案している[5]．Sysmon を用いて特徴的な DLL のロードを調査し，mimikatz がコンピュータ上で起動されたどうかを検知する．Roberto らは，より具体的に Sysmon のデータを ELK（Elasticsearch, Logstash, Kibana）に集約して可視化を使った検知手法を提案している[6].

また，Tom Ueltschi と Michael Haag はログ解析ツールである Splunk[7]と Sysmon を組み合わせることで，mimikatz の検出を試みている[8] [9].

ただし，これらの手法は技術的な検知可能性に言及した Proof of Concept であり，実際の環境での動作を深く検証したものではない．例えば，Windows や Mimikatz はバージョンによって，読み込む DLL が異なるが，それに対する調査は行っておらず，記載内容をそのまま適用すると False Negative が発生する（図 4）．これらの提案手法が実社会での利用に耐えうるためには，さらなる DLL の調査を通じた誤検知の低減と，効率的な検索手法が求められている．

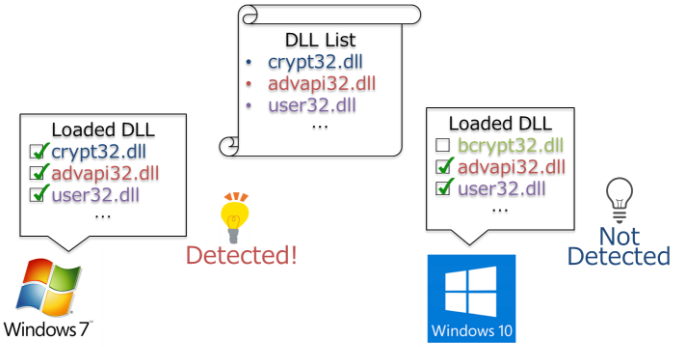

図 4　DLL リストによる mimikatz の検知
Figure 4　Detection of mimikatz activity using DLL list.

4. 課題に対する解決策

本研究では，Windows や mimikatz のバージョンを網羅的に検証し，ロードされる DLL の違いについて検証を行う．検証結果から，Windows や mimikatz のバージョンに依存せず，共通的にロードされる DLL をまとめ，共通 DLL リストを作成する．共通 DLL リストに記述されている DLL を検知対象とすることで False Negative を抑止することが期待できる．

4.1 共通 DLL リストを作成するための環境

Windows や mimikatz のバージョンを組み合わせ，mimikatz を起動することでどのような DLL がロードされるか検証を行う．Windows については現在サポートされている以下のバージョンを使用する．

Windows Client OS
- Windows 7 64bit
- Windows 7 32bit
- Windows 8.1 64bit
- Windows 8.1 32bit
- Windows 10 64bit
- Windows 10 32bit

Windows Server OS
- Windows Server 2008 R2 64bit
- Windows Server 2012 R2 64bit
- Windows Server 2016 64bit

mimikatz については，頻繁にバージョンアップが行われるため全バージョンではなく，3 バージョンを選定し，検証を行う．

- mimikatz 2.1.1 (Aug 1 2017)

本稿執筆時点での最新版バージョン

- mimikatz 2.1 (May 1 2016)

[5]が公開された時期にリリースされたバージョン（ロー

ドされる DLL に変更があったと言及されている).

・mimikatz 2.0 alpha (May 2 2015)

日本で標的型攻撃が増加し始めた時期にリリースされたバージョン

Microsoft 社の公式 Web サイト[2]より Sysmonv6.02 をダウンロードし，各バージョンの Windows において，Sysmon のログを取得するように設定を行う.

4.2 共通 DLL リストの作成方法

4.1 節で述べた Windows 環境上で mimikatz（mimikatz.exe ファイル）を管理者権限で実行し，Sysmon ログからロードされる DLL（ImageLoaded）を抽出する．これを各バージョンの DLL リストと呼ぶことする.

さらに，各バージョンの DLL リスト全てにおいて共通的にロードされる DLL を共通 DLL リストとして抽出する（図 5）.

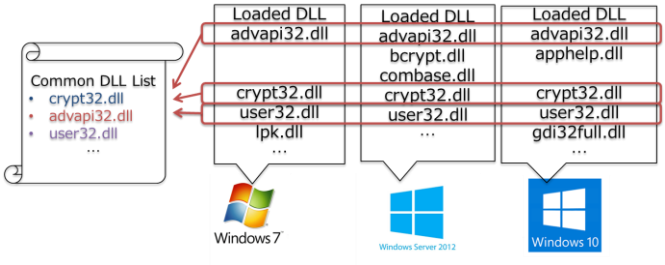

図 5　共通 DLL リストの作成

Figure 5　Creating of Common DLL list

4.3 共通 DLL リストの作成結果

作成した各バージョンの DLL リストの一例を示す．表 1 は Windows のバージョンを変えて mimikatz ver.2.1.1 (Aug 1 2017)を起動したときにロードされる DLL の一部である（Windows 7(x64), 8.1(x64), 10(x64)のみ抜粋）．網掛けしている DLL が共通的にロードされている DLL 名である．同様に表 2 は Windows 7(x64)上で mimikatz のバージョンを変えて起動したときにロードされる DLL の一部である.

表 1　各 Windows バージョンにおけるロードされた DLL の違い

Table 1　The difference of loaded DLLs on each Windows versions

	Win7x64	Win8.1x64	Win10x64
C:¥Windows¥System32¥gdi32full.dll	-	-	○
C:¥Windows¥System32¥hid.dll	○	○	○
C:¥Windows¥System32¥imm32.dll	○	○	○
C:¥Windows¥System32¥kernel.appcore.dll	-	○	○
C:¥Windows¥System32¥kernel32.dll	○	○	○
C:¥Windows¥System32¥KernelBase.dll	○	○	○
C:¥Windows¥System32¥logoncli.dll	○	○	○
C:¥Windows¥System32¥lpk.dll	○	-	-

表 2　各 mimikatz バージョンにおけるロードされた DLL の違い

Table 2　The difference of loaded DLLs on each mimikatz versions

	mimikatz 2.0 (May 2 2015)	mimikatz 2.1 (May 1 2016)	mimikatz 2.1.1 (Aug 1 2017)
C:¥Windows¥System32¥advapi32.dll	○	○	○
C:¥Windows¥System32¥apphelp.dll	-	-	-
C:¥Windows¥System32¥bcrypt.dll	○	○	-
C:¥Windows¥System32¥bcryptprimitives.dll	-	-	-
C:¥Windows¥System32¥cfgmgr32.dll	-	○	○
C:¥Windows¥System32¥combase.dll	-	-	-
C:¥Windows¥System32¥crypt32.dll	○	○	○
C:¥Windows¥System32¥cryptbase.dll	-	-	○
C:¥Windows¥System32¥cryptdll.dll	○	○	○

さらに各バージョンの DLL リスト全てにおいて共通的にロードされている DLL を抽出した結果，合計 20 の DLL が共通的にロードされることがわかった．共通 DLL リストは付録 A-1 に掲載した.

全ての DLL リスト（各バージョンの DLL リスト，共通 DLL リスト）は以下に掲載している.

https://github.com/sisoc-tokyo/mimikatz_detection

5. 解決策の評価

検証結果より得られた共通 DLL リストを評価するため，実際のエンタープライズ環境で実施すると想定した作業を行い，その中で mimikatz を起動した．起動した mimikatz の挙動について，共通 DLL リストを用いて検知できるか，検知率の評価を行った.

5.1 評価環境

共通 DLL リストを用いた検知の正確性を評価するため，以下の評価環境を用いた.

・クライアント端末：Windows7(x64)，Windows10(x64)

・ドメインコントローラ：Windows Server 2008 R2

・mimikatz：4.1 節で述べたバージョンの mimikatz

通常のエンタープライズ環境で実施されるような以下のような作業を数日行い，ランダムなタイミングで mimikatz を複数回起動した.

・電源オフ，電源オン

・ログオン，ログオフ

・Outlook の起動と使用（E-mail の送信）

・Microsoft Word の起動と使用

・Microsoft Excel の起動と使用

・Microsoft PowerPoint の起動と使用

・ファイルサーバへのアクセス

・コマンドプロンプトの起動と使用

・Power shell の起動と使用
・Windows Update

5.2 評価方法

以下のような方法で評価を行った．

・Sysmon ログから，ロードされた DLL（ImageLoaded）を抽出
・共通 DLL リストに含まれる全ての DLL をロードしており，かつ同一のプロセス ID であるものを抽出
・ロード元のプログラム名（Image）が mimikatz.exe であれば，検知成功
・ロード元のプログラム名が mimikatz.exe でなければ False Positive と判定
・mimikatz.exe を実行したにもかかわらず，それを検知できなければ False Negative と判定

5.3 評価結果

最終的には mimikatz の実行を含む正規のプロセスを合計 3,408 プロセス起動したが，表 3 に示すように False Positive，False Negative 共に 0%であった．ただし，本研究では業務で使用すると想定した典型的な環境や作業のみを評価しているため，環境や操作によっては誤検知が発生する可能性もあると考えている．そのため，より長い評価期間を設け，さらに多様な検証を実施する必要があると考えている．

表 3　評価結果
Table 3　Test result

OS	Total amount of processes	False positive rate(%)	False negative rate(%)
Windows 7(x64)	1102	0	0
Windows Server 2008 R2	2016	0	0
Windows 10(x64)	290	0	0

6. 実環境への活用

本研究で得られた結果を実環境で活用するための具体的な手法について紹介する．

6.1 共通 DLL リストの活用方法

ロードされる DLL は Windows のバージョンなどの環境によって異なるため，共通 DLL リストを用いることで False Negative を抑止することができる．もし False Positive が起こる場合には，さらに各バージョンの DLL リストを用いて詳細調査することで False Positive を抑止することができる．2 種類の DLL リストを組み合わせ，2 段階で調査することで高い精度で，かつ効率的に mimikatz を検知できると考えている．

Step1　各コンピュータの Sysmon ログに記録されているロードされた DLL（ImageLoaded）をプロセス ID 毎に抽出し，共通 DLL リストに記述されている DLL と突き合わせる．全て合致すれば，そのプロセス ID のプロセス（Image）は mimikatz が起動された可能性がある．このプロセスを起動したコンピュータを詳細調査するため，Step2 へ進む

Step2　mimikatz が起動された可能性のあるコンピュータに対して，そのコンピュータに合ったバージョンの DLL リストと突き合わせる

6.2 Elasticsearch によるログの集約と分析

2.4 節で述べたように，Sysmon のログは各コンピュータに保存される．より効率的な検知のためには，ログを集約し，分析できる環境が望ましい．Elasticsearch 社よりオープンソースのログ分析エンジン，分析結果の可視化，ログの加工のソフトウエアとして，それぞれ Elasticsearch，Kibana，Logstash が公開されており，これらを組み合わせてログ分析するサーバを ELK サーバと呼ぶ．本研究ではこれらを用いてログの集約と分析を行う．ログ転送エージェントとして Winlogbeat と呼ばれるソフトウエアを Windows 系コンピュータにインストールすることで Windows イベントログを ELK サーバに集約し，分析することが可能である．

図 6 は ELK サーバを用いたログ集約の概念図である．Elasticsearch は REST API インタフェースを提供しているため，JSON 形式でクエリを記述でき，検知ツールとしての実装は比較的容易である．一例として，Python3 系で記述したサンプルコードを以下に掲載している．

https://github.com/sisoc-tokyo/mimikatz_detection/tree/master/pythonTool

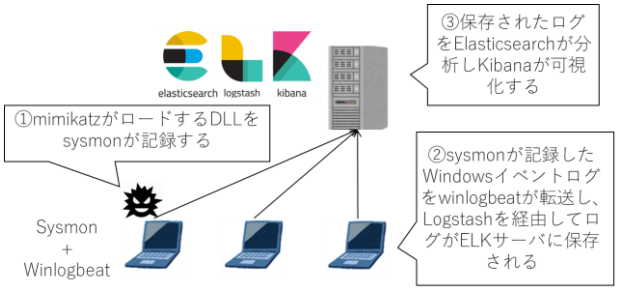

図 6　ELK によるログ集約と検知の概念図
Figure 6　Concept of centralized detection using ELK

6.3 共通 DLL リスト作成サンプルコード

mimikatz などのプロセスがロードする DLL は環境によって変化するため，自組織の環境で独自 DLL を作成することも有効である．Windows イベントログを CSV 形式で出力したデータを元に共通 DLL リストを作成したり，ログの

集約が難しい場合に，個々のコンピュータに保存された CSV 形式の Windows イベントログから mimikatz の起動を検知したりする Java コードも以下に掲載している．本ツールを用いた検知の概念図を図 7 に示す．
https://github.com/sisoc-tokyo/mimikatz_detection/tree/master/javaTool

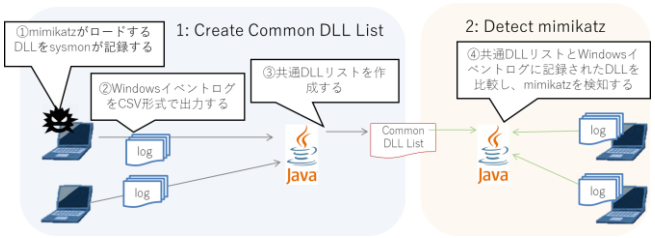

図 7　共通 DLL リストの作成と検知の概念図
Figure 7　Concept of creating common DLL list and detection

7. おわりに

横断的侵害の早期検知のため，Sysmon のログを用いて mimikatz の起動を検知することは有効である．ロードされる DLL は環境によって異なるため，共通 DLL リストを作成し，これを用いることで現在のところ高い確率で検知できることがわかった．

提案手法の利用により，効率的に mimikatz の悪用を検知することができようになり，標的型攻撃の被害軽減に貢献すると考えられる．

参考文献

[1] Shingo Abe. “Detecting Lateral Movement in APTs -Analysis Approach on Windows Event Logs-“.
https://www.first.org/resources/papers/conf2016/FIRST-2016-105.pdf
[2] Microsoft. “Sysmon v6.02”.
https://docs.microsoft.com/en-us/sysinternals/downloads/Sysmon
[3] Elasticsearch.
https://www.elastic.co/products/elasticsearch
[4] JPCERT/CC. “ログを活用した Active Directory に対する攻撃の検知と対策”.
https://www.jpcert.or.jp/research/AD.html
[5] Jake Liefer. “Detecting In-Memory mimikatz”
https://securityriskadvisors.com/blog/post/detecting-in-memory-mimikatz/
[6] Roberto Rodriguez. “Chronicles of a Threat Hunter: Hunting for In-Memory mimikatz with Sysmon and ELK - Part I (Event ID 7)”
https://cyberwardog.blogspot.jp/2017/03/chronicles-of-threat-hunter-hunting-for.html
[7] Splunk Inc.
https://www.splunk.com/ja_jp
[8] Tom Ueltschi, Swiss Post CERT “Advanced Incident Detection and Threat Hunting using Sysmon (and Splunk)”
https://www.first.org/resources/papers/conf2017/Advanced-Incident-Detection-and-Threat-Hunting-using-Sysmon-and-Splunk.pdf
[9] Michael Haag. “Splunking the Endpoint: Threat Hunting with Sysmon”
https://medium.com/@haggis_m/splunking-the-endpoint-threat-hunting-with-sysmon-9dd956e3e1bd

付録

付録 A.1 共通 DLL リスト

4.1 節で記述した Windows と Mimikatz のバージョンで共通的にロードされる DLL を共通 DLL リストとし，表 4 に示す．

表 4　共通 DLL リスト
Table 4　Common DLL list

No	Common DLLs
1	C:¥Windows¥System32¥advapi32.dll
2	C:¥Windows¥System32¥crypt32.dll
3	C:¥Windows¥System32¥cryptdll.dll
4	C:¥Windows¥System32¥gdi32.dll
5	C:¥Windows¥System32¥imm32.dll
6	C:¥Windows¥System32¥kernel32.dll
7	C:¥Windows¥System32¥KernelBase.dll
8	C:¥Windows¥System32¥msasn1.dll
9	C:¥Windows¥System32¥msvcrt.dll
10	C:¥Windows¥System32¥ntdll.dll
11	C:¥Windows¥System32¥rpcrt4.dll
12	C:¥Windows¥System32¥rsaenh.dll
13	C:¥Windows¥System32¥samlib.dll
14	C:¥Windows¥System32¥sechost.dll
15	C:¥Windows¥System32¥secur32.dll
16	C:¥Windows¥System32¥shell32.dll
17	C:¥Windows¥System32¥shlwapi.dll
18	C:¥Windows¥System32¥sspicli.dll
19	C:¥Windows¥System32¥user32.dll
20	C:¥Windows¥System32¥vaultcli.dll