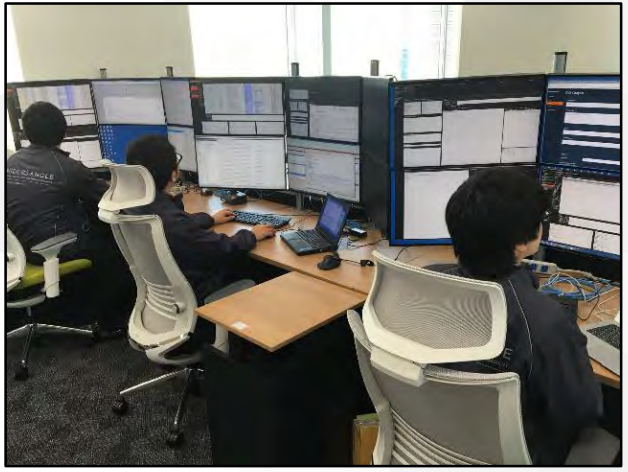
セキュリティログ分析のフィールドは エンドポイントへ
~Windows深層における攻防戦記~

NTTセキュリティ・ジャパン株式会社
林 匠悟

NTT Security

自己紹介

- 林　匠悟
  - NTTセキュリティ・ジャパンのSOCアナリスト
  - SOC歴 10年
  - 監視、デバイス設定変更、分析、製品検証、ホワイトペーパーの執筆、カスシグ作成、運用設計、サービス企画などを担当
  - 外部活動として日本SOCアナリスト情報共有会（SOCYETI）の立ち上げメンバーの一人として脅威動向や分析手法などの情報共有を行う



SOCYETI

目次

- エンドポイント分析の紹介
  - 監視の必要性
  - 分析における利点と課題点
  - 分析のコツ
  - カスタムシグネチャ運用
- EDRログから判明した攻撃事例の紹介
- 検知回避に対する対抗事例の紹介
- まとめ

エンドポイント分析の紹介

エンドポイントログとは

- プロセス情報（プロセスツリー、コマンドラインなど）
- ロードされたファイル
- ファイル操作（作成、削除、変更など）
- レジストリ操作（作成、削除、変更など）
- ネットワークアクセス
- DNSクエリ
- URLなど

※Sysmon [1], Process Monitor[2], EDR, 資産管理ツールなどを利用して監視・分析が可能。

なぜエンドポイントログの監視が必要か

- **攻撃手法が高度化され、これまでのネットワーク監視だけでは脅威を見つけることが困難**
  - マルウェアの通信先に改ざんされた正規サイトやファイル共有サイト、掲示板など正規のWebサービスが利用され、ネットワークログから正常通信か不正なものか判断が困難
  - ダウンロード時点では難読化、エンコード、暗号化などによって不正なファイルかどうか判断が困難

- **ネットワーク監視ポイント以外で外部と通信**
  - リモートワーク等によってProxyやIPS/IDSといった監視ポイントを通過しないため、気が付けない

SOCにおける検知状況

非公開

エンドポイントログ監視の利点と課題点

- **利点**
  - 端末特定が容易
  - ネットワーク上に特徴が現れない脅威を検知
  - より詳細に影響度の判断が可能

- **課題点**
  - ログ量が膨大
  - ネットワークとは異なるエンドポイント挙動の知識が必要

	攻撃プロセス	NW検知	ホスト検知
①	メール受信	○	
②	メール記載のURLへアクセス	○	
③	Zipファイルダウンロード	○	
④	Zipファイル展開		○
⑤	JavaScript実行		○
⑥	マルウェア生成		○
⑦	端末内の情報収集(ログイン、メールアドレス情報など)		○
⑧	ログオン時の自動起動設定		○
⑨	収集した情報のアップロード	△	○
⑩	C&Cサーバとの通信後のダウンロードや操作	△	○

エンドポイントログ分析の基本

- **プロセス毎に挙動を確認する**
  - 時系列だけで挙動を追うと混乱を招くため、プロセス単位でファイル、レジストリ、通信の挙動や親子プロセスの起動を追っていく
- **プロセス起動時のコマンドラインを確認する**
  - 起動したファイル名やコマンド内容を把握できる
- **プロセスの親子関係をチェックする**
  - 親子関係から感染源の特定や感染後の挙動を把握できる

エンドポイントログ分析の基本における注意点

- **プロセスを追うときはPIDと起動時間を確認する**
  - svchost.exeなど同じプロセス名で同時に複数起動している
  - PIDは使い回されているため、同じPIDでも起動時間で全く異なるプロセスを示す
- **起動したファイル名の確認はMRU、.lnkファイル、Prefetchでも確認できる**
  - Dynamic Data Exchange(DDE)によってコマンドラインに開いたファイル名が残らないなどがある
- **コードインジェクションの可能性を考慮する**
  - コードインジェクションが利用されているとプロセスの親子関係を追うだけでは挙動全体を把握できない

エンドポイントログ分析の基本における注意点２

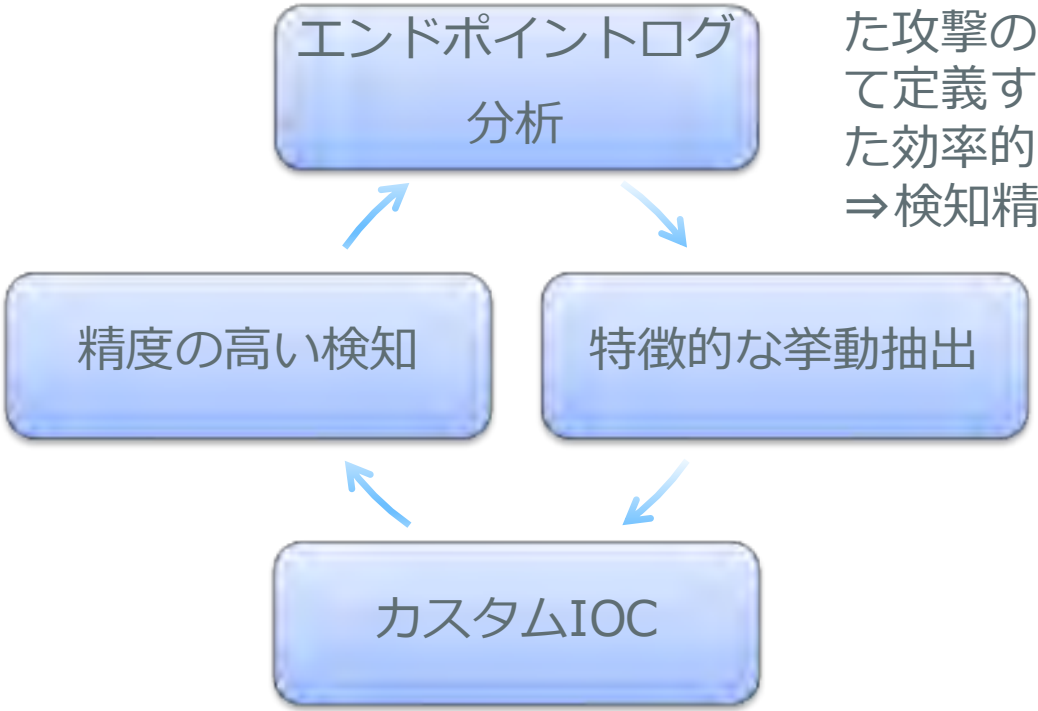
- **コードインジェクションが疑われる場合**
  - プロセスの親子関係が不自然に途切れている
  - 一連の親子関係のあるプロセスにおいて通信挙動が一つもない

- **コードインジェクションが疑われる場合の確認ポイント**
  - svchostやexplorerなどよくインジェクション対象として狙われるプロセスから不審な通信が出ていないか確認
  - svchostやexplorerなどよくインジェクション対象として狙われるプロセスから不審な子プロセスが起動していないか確認

基本的な不審ログの確認ポイント

- **正規プロセスにそっくりなプロセス名の起動**
  - scvhost.exe, dlhost.exe, explore.exeなどのプロセス起動
- **不審なプロセスの親子関係**
  - svchost.exeの親プロセスがservices.exe以外、lsass.exeから子プロセス起動など
- **ロードされるDLLファイルのファイルパスとコード署名**
  - ¥AppData¥配下にある署名のないDLLファイルのロード
- **自動起動設定された実行ファイルのパスとコード署名**
  - ¥AppData¥にある署名のない実行ファイルの登録
- **自動起動設定された長いコマンドライン**
  - Runキーに難読化されたスクリプトの登録
- **アンチウィルスの隔離ログ**
  - 隔離ログにあるファイル名やファイルハッシュ値など

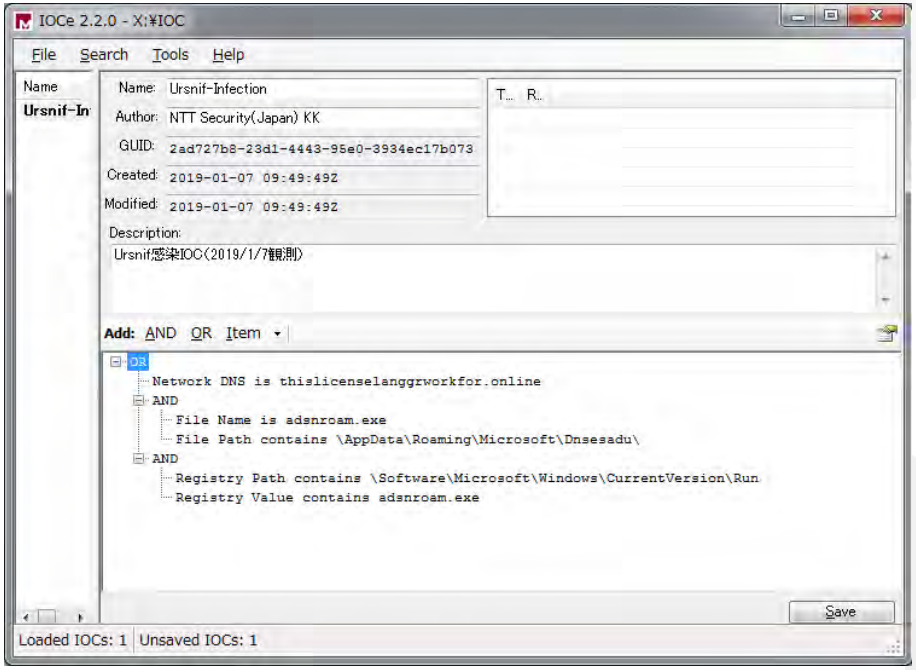
カスタムシグネチャ（カスタムIOC）運用



エンドポイントログを分析していく中で見つけた攻撃の特徴を検知できるようカスタムIOCとして定義することで、エンドポイントログを使った効率的な監視、分析を行うことができる。
⇒検知精度の向上、見逃しの防止

カスタムシグネチャ（カスタムIOC）の作成

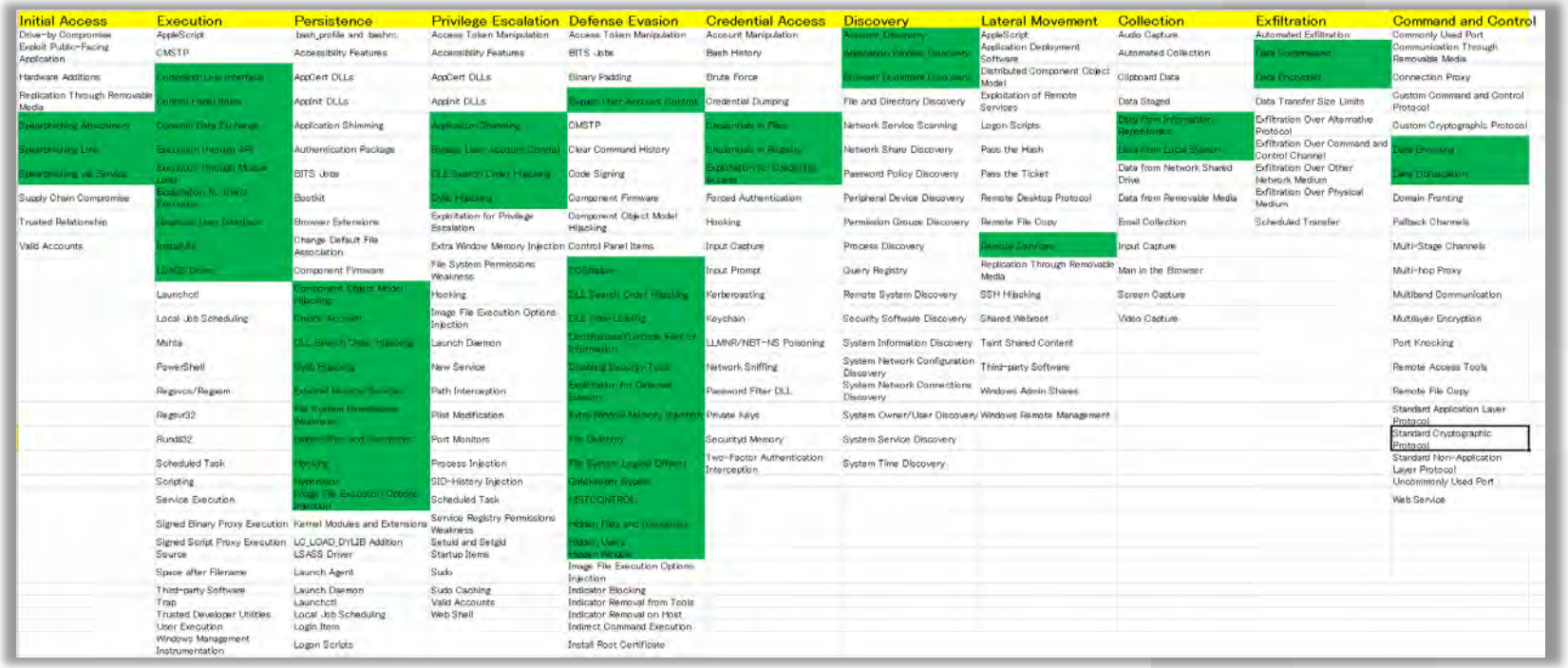
一般的にOpenIOC [3]やCybOX [4]などのフォーマットで定義することができる。



IOC Editorを利用したサンプルIOC [5]

ATT&CK(MITRE)の活用

作成したカスタムIOCをマッピングすることで検知した際の影響度をすぐに判断することができ、ブレない運用を実現できる。また、カスタムIOCによるカバー範囲の網羅性を向上することできる。



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	DYLIB Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Disabling Security Tools	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Securityd Memory	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Two-Factor Authentication Interception	System Time Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	SID-History Injection	Gatekeeper Bypass						Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Scheduled Task	HISTCONTROL						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Service Registry Permissions Weakness	Hidden Files and Directories						
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Setuid and Setgid	Hidden Users						
	Source	LSASS Driver	Startup Items	Hidden Window						
	Space after Filename	Launch Agent	Sudo	Image File Execution Options Injection						
	Third-party Software	Launch Daemon	Sudo Caching	Indicator Blocking						
	Trap	Launchctl	Valid Accounts	Indicator Removal from Tools						
	Trusted Developer Utilities	Local Job Scheduling	Web Shell	Indicator Removal on Host						
	User Execution	Login Item		Indirect Command Execution						
	Windows Management Instrumentation	Logon Scripts		Install Root Certificate						

ATT&CK Matrix for Enterprise [6]とのマッピング(活用例イメージ)

EDRログ分析から判明した攻撃事例の紹介

SOCにおける検知状況

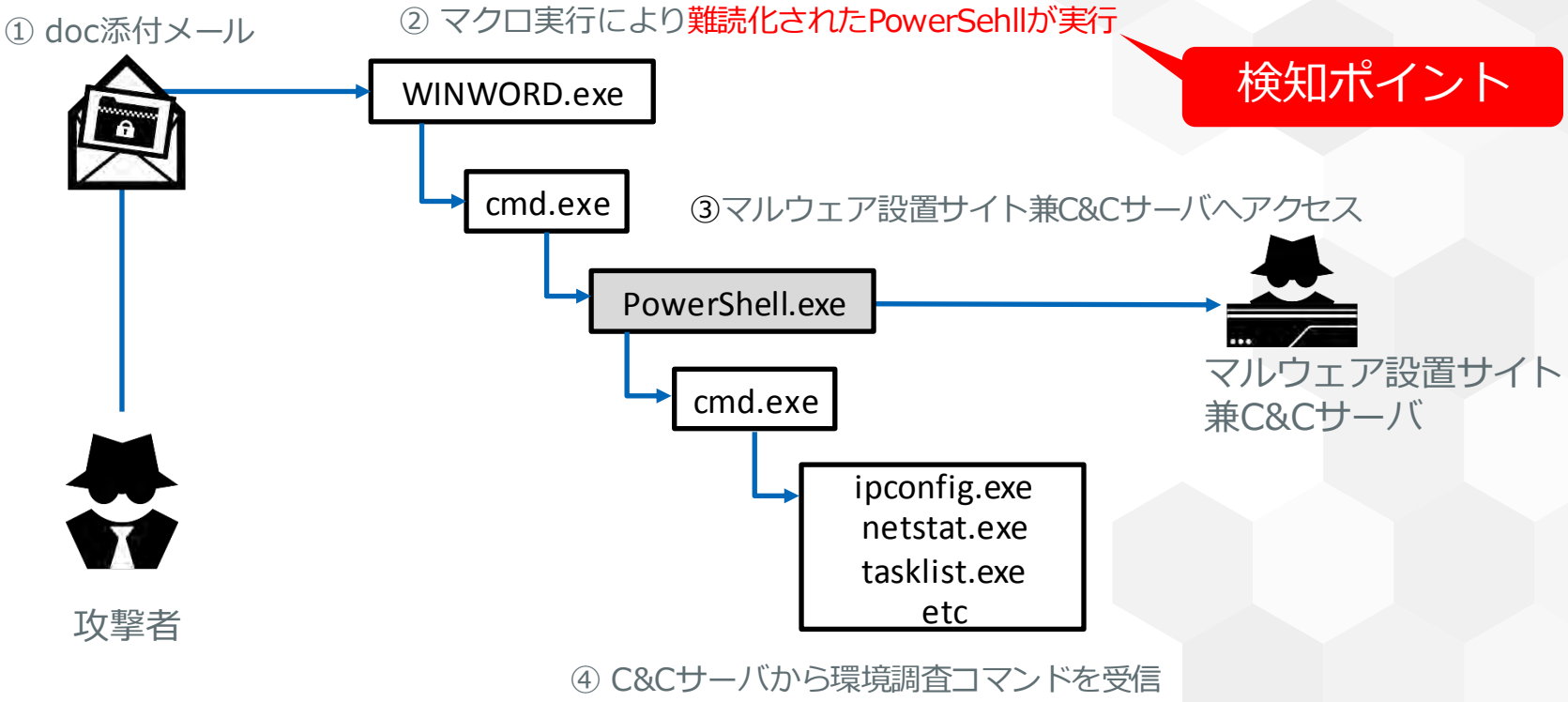
非公開

SOCで観測した事例から特徴的な事例を4つ紹介します。

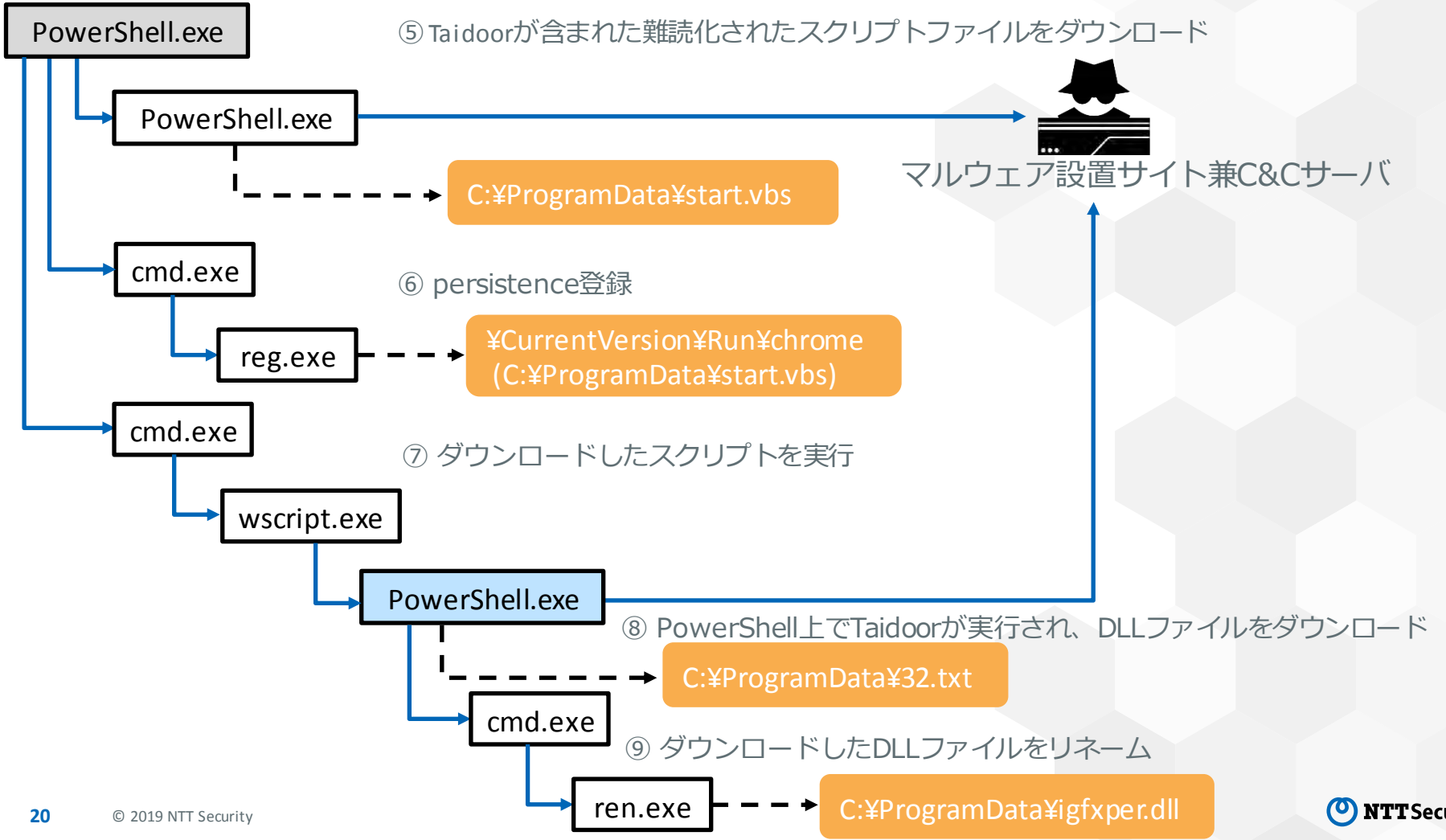
①2018年4月観測のTaidoor
②2018年5月観測のANEL
③2018年7月観測のANEL
④2018年10月観測のUnknownマルウェア

事例①

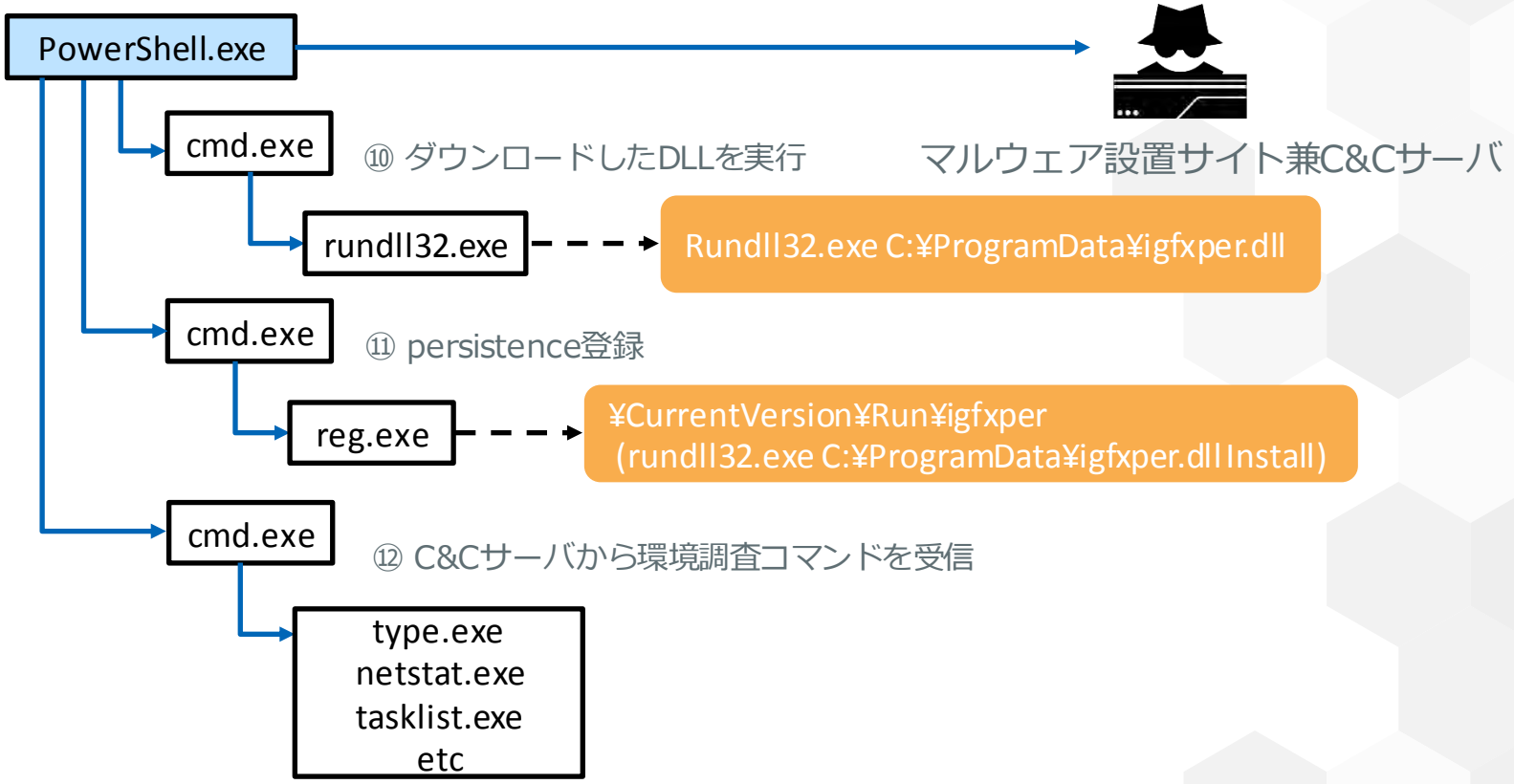
2018年4月に観測したTaidoorを利用した事例の概要



NTT Security



NTT Security



NTT Security

事例①における主な特徴

2018年4月に観測したTaidoorを利用した事例の特徴

- メールのFromはyahoo.co.jp
- メール本文や添付ファイルは全て日本語
- docファイルが添付されたメールがターゲット複数名に送信
- マルウェア設置サイトとC&Cサーバが同じ
- PowerShellのプロセス上でTaidoorを実行
- 複数のマルウェアをpersistence登録
- persistenceはRunキー
- 通信先はGoogleクラウドが利用され、直IPアドレスの443通信

事例①における主な検知回避テクニック

- **マルウェアの実行にPowerShell、Rundll32を利用**
  - 起動しているプロセス名は正規のものであるため、悪性には見えない

```
¥CurrentVersion¥Run¥igfxper
 (rundll32.exe C:¥ProgramData¥igfxper.dll Install)
```

Rundll32を利用したマルエアの起動

- **通信先にGoogleクラウド上のIPアドレスを利用**
  - レピュテーションサイトによるIPアドレスの評価は安全であり、IPアドレスに関する情報がほとんどないため、通信先のみでの悪性判定は難しい

事例②

2018年5月に観測したAPT10によるCobalt Strikeを利用した事例の概要

① rar添付メール

② マクロ実行によりマルウェア設置サイトへアクセスし、複数ファイルをダウンロード

EXCEL.exe

マルウェア設置サイト

C:¥Users¥a¥AppData¥Local¥Temp¥
gdi32.dll（ロードされる正規DLL）
CrashReport.dll（サイドロードされるマルウェアCobalt Strike）
memdefrag.exe（MemDefrag正規ファイル）
C:¥Users¥Public¥
web_lowtrust.config.uninstall(不正な実行ファイル)
System.Numerics.dll.manifest(不明)

攻撃者

③ persistence登録

¥CurrentVersion¥Run¥conhostdwm
(C:¥Users¥a¥AppData¥Local¥Temp¥memdefrag.exe)

検知ポイント

EXCEL.exe

cmd.exe

④ InstallUtilコマンドでマルウェアを起動し、C&Cサーバへアクセス

InstallUtil.exe

C&Cサーバ

C:¥Windows¥Microsoft.NET¥Framework¥v4.0.30319¥InstallUtil.exe /run= /logfile= /LogToConsole=false /u C:¥Users¥Public¥web_lowtrust.config.uninstall

cmd.exe

⑤ C&Cサーバから環境調査コマンドを受信

bitsadmin.exe
AdFind.exe
net.exe
findstr.exe
csvde.exe
etc

事例②における主な特徴

2018年5月に観測したAPT10によるCobalt Strikeを利用した事例の特徴

- メールのFromはyahoo.co.jp
- メール本文や添付ファイルは全て日本語
- rarファイルが添付されたメールがターゲット1名にのみ送信
- マクロ実行によりマルウェア設置サイトから複数のファイルをダウンロード
- DLLサイドロードを利用
- persistenceはRunキー
- アクセス先はクラウドサービス「OVH」が利用され、HTTPS通信

事例②における主な検知回避テクニック

- **マルウェアの実行に「InstallUtil」というマイクロソフト社の.NET Frameworkアプリケーション用のインストーラーツールを利用**
  - 起動しているプロセス名は正規のものであるため、悪性には見えない
  - コマンドラインから不審なものには見えない

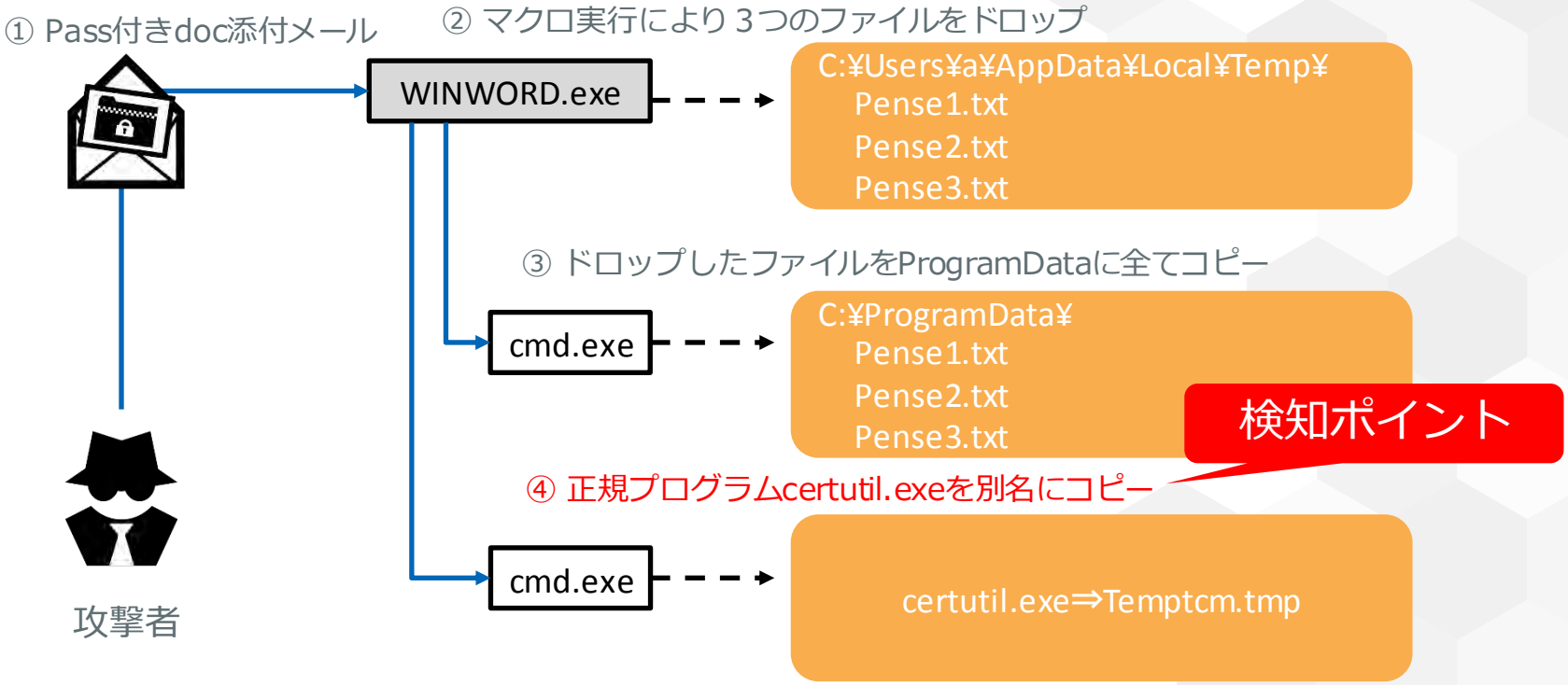
```
> C:¥Windows¥Microsoft.NET¥Framework¥v4.0.30319¥InstallUtil.exe /run=
/logfile= /LogToConsole=false /u C:¥Users¥Public¥web_lowtrust.config.uninstall
```

InstallUtilを利用したマルェアの起動

- **persistenceに「MemDefrag」という正規ツールを利用したDLLサイドロード**
  - 起動しているプロセス名は正規のものであるため、悪性には見えない
- **C&Cサーバへの通信にSSLを利用しているため、通信先のみでの悪性判定は難しい**

事例③

2018年7月に観測したAPT10によるANELを利用した事例の概要



NTT Security

検知ポイント

WINWORD.exe

⑤ コピーしたcertutilコマンドを利用してドロップしたファイルをそれぞれデコード

cmd.exe

Temptcm.tmp

Pense1.txt⇒GUP.txt(WinGUP正規ファイル)
Pense2.txt⇒libcurl.txt(サイドロードされる不正DLL)
Pense3.txt⇒c7583baa(暗号化されたマルウェアANEL)

cmd.exe

⑥ esentutilコマンドを利用してドロップしたファイルを別名にコピー

Temptcm.tmp

GUP.txt ⇒ GUP.exe(WinGUP正規ファイル)
libcurl.txt ⇒ libcurl.dll(ロードされるDLL)

⑦ libcurl.dllとc7583baaをロードして実行　⑧ persistence登録

GUP.exe

¥CurrentVersion¥Run¥GUP (C:¥ProgramData¥GUP.exe)

C&Cサーバ

⑨ C&Cサーバへアクセス

cmd.exe

⑩ C:¥ProgramData¥のテキストファイルの削除

del.exe

del /f /s /q C:¥ProgramData¥*.txt

NTT Security

事例③における主な特徴

2018年7月に観測したAPT10によるANELを利用した事例の特徴

- メールのFromはyahoo.co.jp
- メール本文や添付ファイルは全て日本語（一部漢字の間違いあり）
- 本文にパスワードが記載され、docファイルが添付されたメールがターゲット1名にのみ送信
- マクロの実行により正規の実行ファイル、サイドロードされるDLL,暗号化されたANELがドロップ
- 複数のWindows標準コマンド利用
- DLLサイドロードの利用
- persistenceはRunキー
- アクセス先はクラウドサービス「DigitalOcean」が利用され、直IPアドレスのHTTP通信

事例③における主な検知回避テクニック１

- エンコードされたマルウェアをドロップ
- マルウェアのデコードに証明書サービスのインストールなどに利用するWindows標準コマンド「certutil」を利用
- 「certutil」の実行ファイルを別名にコピーして、コピーしたプロセスの起動
  - 別名でデコードを実行することで、certutilプロセス実行の検知を回避

```
> C:¥Windows¥System32¥cmd.exe /c copy C:¥Windows¥system32¥certutil.exe C:¥Users¥a¥AppData¥Local¥Temptcm.tmp
> C:¥Windows¥System32¥cmd.exe /c C:¥Users¥a¥AppData¥Local¥Temptcm.tmp –decode C:¥ProgramData¥pense1.txt C:¥ProgramData¥GUP.txt
```

コピーしたcertutilを利用したファイルのデコード

事例③における主な検知回避テクニック２

- **実行ファイルのリネームに証明機関のデータベース管理などに利用するWindows標準コマンド「esentutl」を利用**

```
> C:¥Windows¥System32¥esentutl.exe /y C:¥ProgramData¥GUP.txt C:¥ProgramData¥GUP.exe /o
```

esentutlを利用したマルウェアのコピー

- **persistenceに「WinGUP」という正規ツールを利用したDLLサイドロード**
  - 起動しているプロセス名は正規のものであるため、悪性には見えない

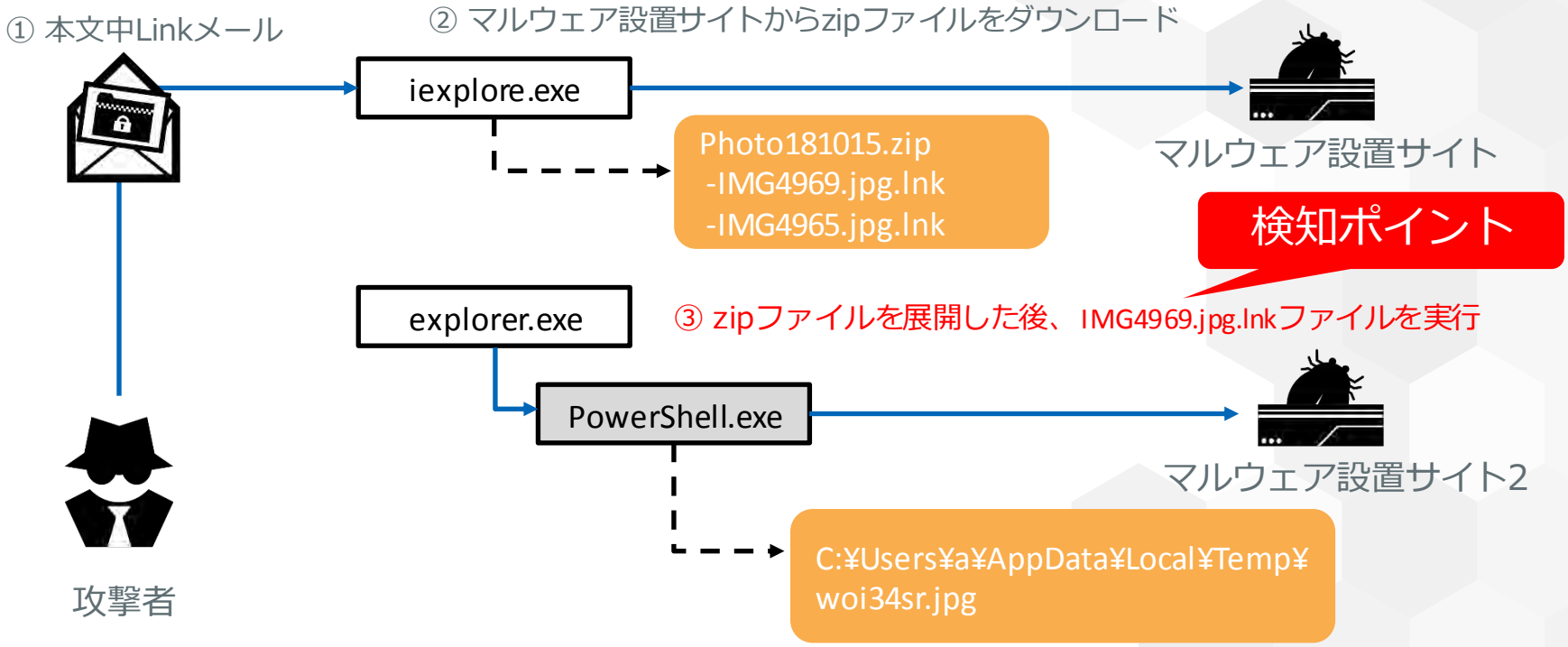
- **デコードやコピーで利用したファイルを削除**

```
> C:¥Windows¥System32¥cmd.exe /c del /f /s /q C:¥ProgramData¥*.txt
```

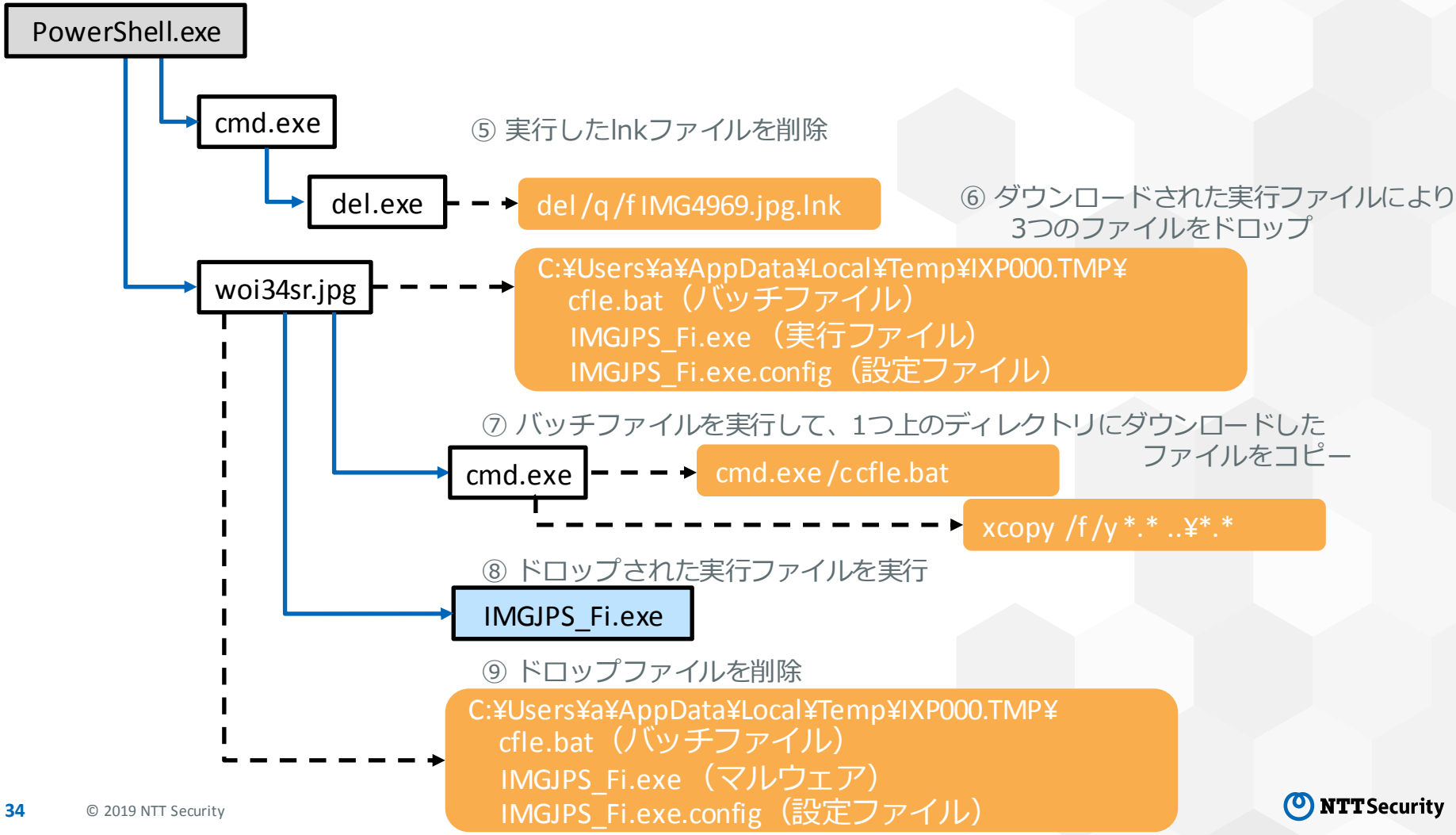
delを利用したファイルの削除

事例④

2018年10月に観測した事例の概要



NTT Security



⑨ persistence登録

IMGJPS_Fi.exe

タスク名：WinsUpdte-ub48572
実行ファイルパス：C:¥Users¥a¥AppData¥Local¥Temp¥IMGJPS_Fi.exe

svchost.exe

taskeng.exe

IMGJPS_Fi.exe

⑩ 再起動後にタスクスケジューラによってマルウェアが起動し、C&Cサーバへアクセス

C&Cサーバ

事例④における主な特徴

2018年10月に観測した事例の特徴

- メールのFromはyahoo.co.jp
- メール本文や添付ファイルは全て日本語
- 本文にリンクが含まれたメールがターゲット1名にのみ送信
- .NETマルウェアを利用
- persistenceはタスクスケジューラ
- タスクスケジューラによってマルウェアが起動されることでC＆Cサーバへ通信
- アクセス先はクラウドサービス「shinjiru」が利用され、10分間隔でHTTP通信
- アクセス先のドメインは評価なし

事例④における主な検知回避テクニック

- **マルウェアはタスクスケジューラによって起動されることでC&Cサーバへアクセス**
  - タスクスケジューラ以外での手法で起動すると外部への通信が発生しないため、悪性判定が難しい
- **ダウンローダーとして利用したファイル等を削除**

```
> C:¥Windows¥System32¥cmd.exe /c del /q /f IMG4969.jpg.lnk
```

ダウンローダーファイルの削除

- **C&Cサーバで利用したドメインは数カ月前に作成した新しいものを利用**
  - ドメインの評価結果がないため、通信先のみでの悪性判定が難しい

検知回避に対する対抗事例の紹介
～APT10によるANEL編～

非公開

まとめ

- 高度化する攻撃に対して従来のネットワークログを利用した監視・分析だけではなく、エンドポイントログを活用した監視・分析が必須
- エンドポイントログを活用することで検知力のアップと容易に影響範囲が特定
- 攻撃者はすでにエンドポイントログを意識して攻撃手法を変えてきているため、カスタムシグネチャで対抗

参考文献

[1] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

[2] https://technet.microsoft.com/ja-jp/sysinternals/processmonitor.aspx

[3] https://www.fireeye.com/blog/threat-research/2013/10/openioc-basics.html

[4] http://cyboxproject.github.io/

[5] https://www.fireeye.jp/services/freeware/ioc-editor.html

[6] https://attack.mitre.org/