
ITOCHU
Cyber &
Intelligence
Hack The Sandbox
Unveiling the Truth Behind Disappearing Artifacts

WHO ARE WE ?

ITOCHU Cyber & Intelligence Inc.

Yusuke Niwa

Lead Cybersecurity Researcher
JSAC, VB, Hitcon, Botconf Speaker

Satoshi Kamekawa

Cybersecurity Researcher
TAS Speaker

Shuhei Sasada

Cybersecurity Researcher
JSAC Speaker

Special Thanks ;)

Dominik Breitenbacher
ESET

J-CRAT
Cyber Rescue and Advice Team against targeted attack of Japan

Suguru Ishimaru
ITOCHU Cyber & Intelligence Inc.

Agenda

01 Introduction
02 About Windows Sandbox
03 Abusing with WSB Files
04 Emerging threats
05 Countermeasures
06 Conclusions

SECTION 01

Introduction

WINDOWS - EASY

50
Points

★ ★ ★ ★ ★
5.0 50 Reviewers

Breaking News January 8, 2025

- 警察庁による MirrorFace による攻撃キャンペーンについて注意喚起が公開
- Windows Sandbox を悪用した手口及び痕跡・検知策についても詳細に解説

MirrorFaceによるサイバー攻撃について（注意喚起）

警察庁及び内閣サイバーセキュリティセンターでは、2019年頃から現在に至るまで、日本国内の組織、事業者及び個人に対するサイバー攻撃キャンペーンが、「MirrorFace」（ミラーフェイス）（別名、「Earth Kasha」（アース カシャ））と呼ばれるサイバー攻撃グループによって実行されたと評価しています。

また、警察庁関東管区警察局サイバー特別捜査部及び警視庁ほか道府県警察による捜査等で判明した、攻撃対象、手口、攻撃インフラ等を分析した結果、「MirrorFace」による攻撃キャンペーンは、主に我が国の安全保障や先端技術に係る情報窃取を目的とした、中国の関与が疑われる組織的なサイバー攻撃であると評価しています。

この注意喚起は「MirrorFace」によるサイバー攻撃の手口を公表することで、標的となる組織、事業者及び個人に、直面するサイバー空間の脅威を認識してもらうとともに、サイバー攻撃の被害拡大防止及び被害の未然防止のための適切なセキュリティ対策を講じてもらうことを目的としています。

MirrorFaceによるサイバー攻撃について（注意喚起）

別添資料【Windows Sandbox を悪用した手口及び痕跡・検知策】

別添資料【VS Code を悪用した手口及び痕跡・検知策】

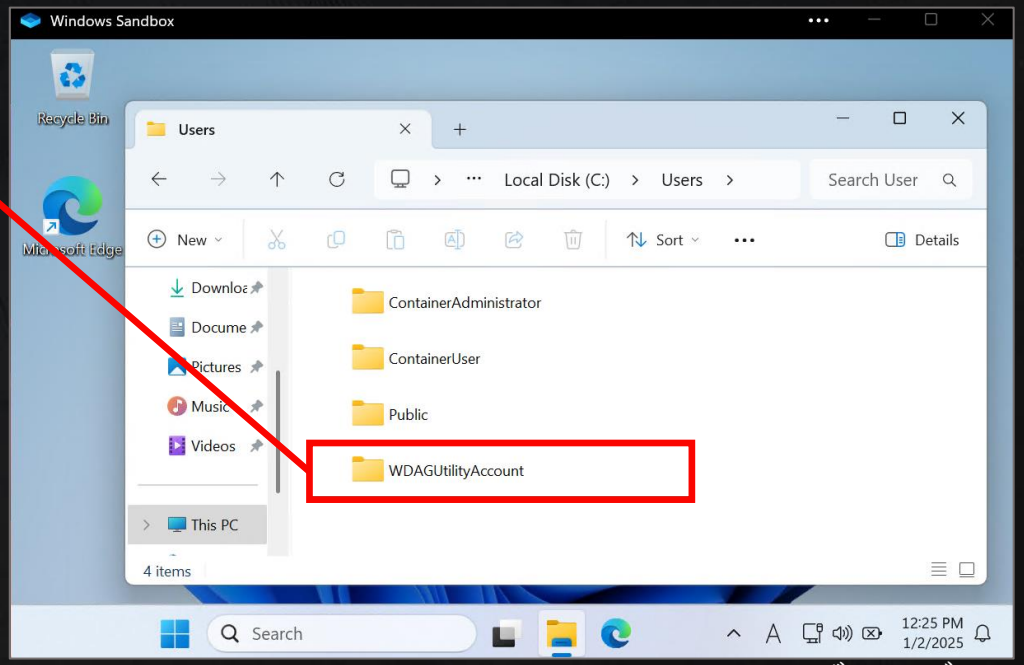
https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html

Windows Sandbox の悪用に関する重要な手がかり

- MirrorFace（APT10 傘下）による攻撃キャンペーンを観測
- OSS の Lilith RAT* をカスタマイズした LilimRAT が使用された
- LilimRAT は Windows Sandbox 内で実行されているかを確認するために、WDAGUtilityAccount フォルダを確認する機能が実装された
- WDAGUtilityAccount は Windows Sandbox のデフォルトユーザであると判明

```
29
30  FileAttributesA = GetFileAttributesA("C:\\Users\\WDAGUtilityAccount");
31  if ( FileAttributesA != -1 && (FileAttributesA & 0x10) != 0 )
32  {
33    c_GetModuleFileNameA();
34    c_WSAStartup();
35    v29 = 1;
36    Src = 0;
37    v13 = 0;
38    v14 = 0;
39    v24 = 0;
40    v25 = 15;
41    LOBYTE(v23[0]) = 0;
42    c_memmove(v23, &unk_440C40, 1u);
43    LOBYTE(v29) = 2;
44    v27 = 0;
```

ユーザフォルダを確認する機能が実装された LilimRAT



Windows Sandbox の WDAGUtilityAccount のユーザフォルダ

*Lilith RAT: https://github.com/werkamsus/Lilith/

APT アクターの攻撃手法の概要

- APT アクターは初期侵害を行い、対象ホストの Windows Sandbox を有効化
- OS の再起動後、APTアクターは WSB ファイルを悪用し、サンドボックスを起動
- セカンドペイロードマルウェアを実行して C2 サーバとの通信を開始

モチベーション

FACT

標的型攻撃者によって Windows Sandbox を悪用された事例が観測

ASSUMPTION

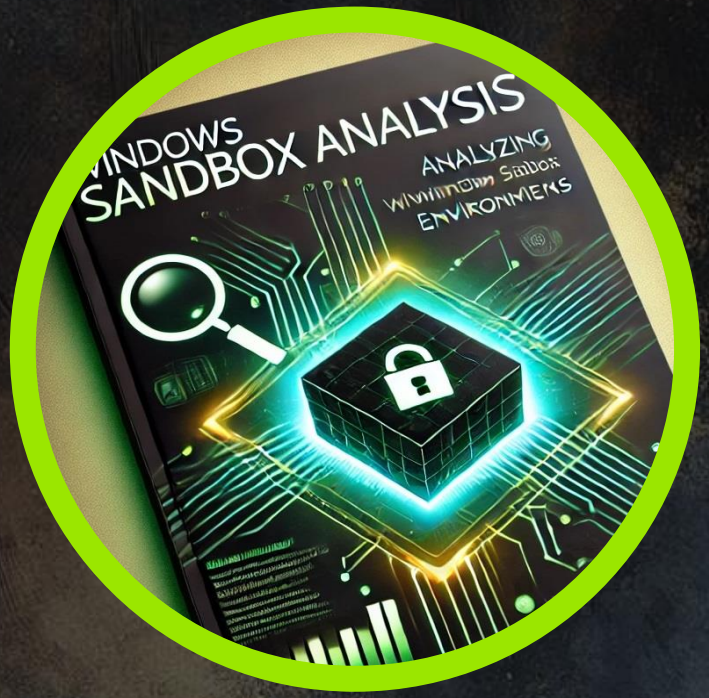
攻撃活動を
隠蔽するために悪用？

CONCERNs

- 全ての攻撃活動が隠蔽されてしまう？
- Windows Sandbox の仕様を理解することで対策につなげられる？
- 従来のアーティファクトでは太刀打ちできないのか？

PURPOSE

✓ 発見された端緒と兆候から悪用の事実を紐解き、手口を解明したい
✓ リサーチと技術検証で裏打ちされた実効性のある対策と調査方法をブルーチームとして共有したい



SECTION 02

About Windows Sandbox

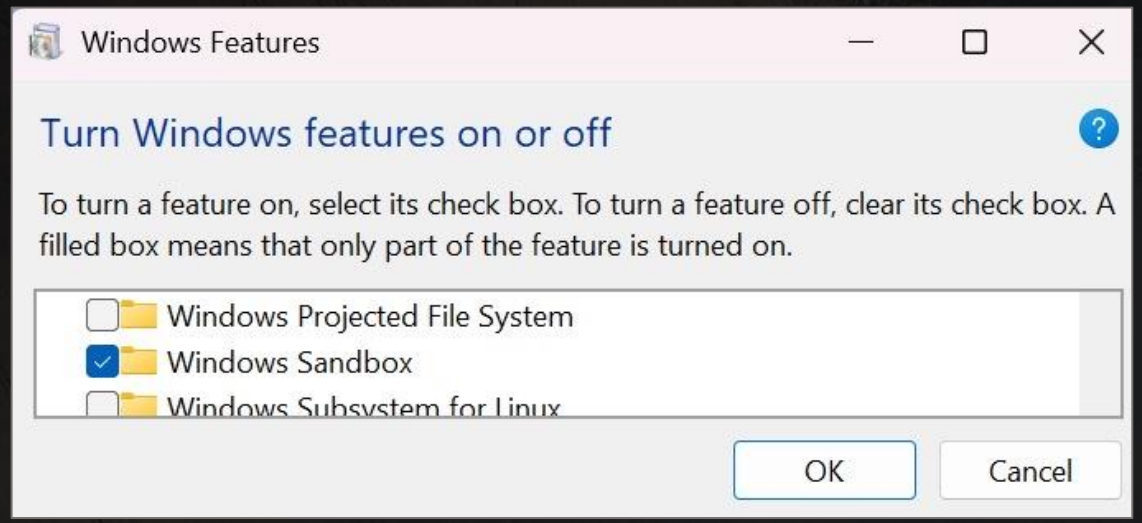
WINDOWS - EASY

50
Points

★ ★ ★ ★ ★
5.0 60 Reviewers

利用環境と条件

- Windows Sandbox はホストシステムと独立したアプリケーションを単独かつ安全に実行するための軽量のデスクトップ環境
- Windows 10 (build 18342) and Windows 11より提供開始
- デフォルトでは Windows Sandbox は無効化されており、手動での有効化が必要



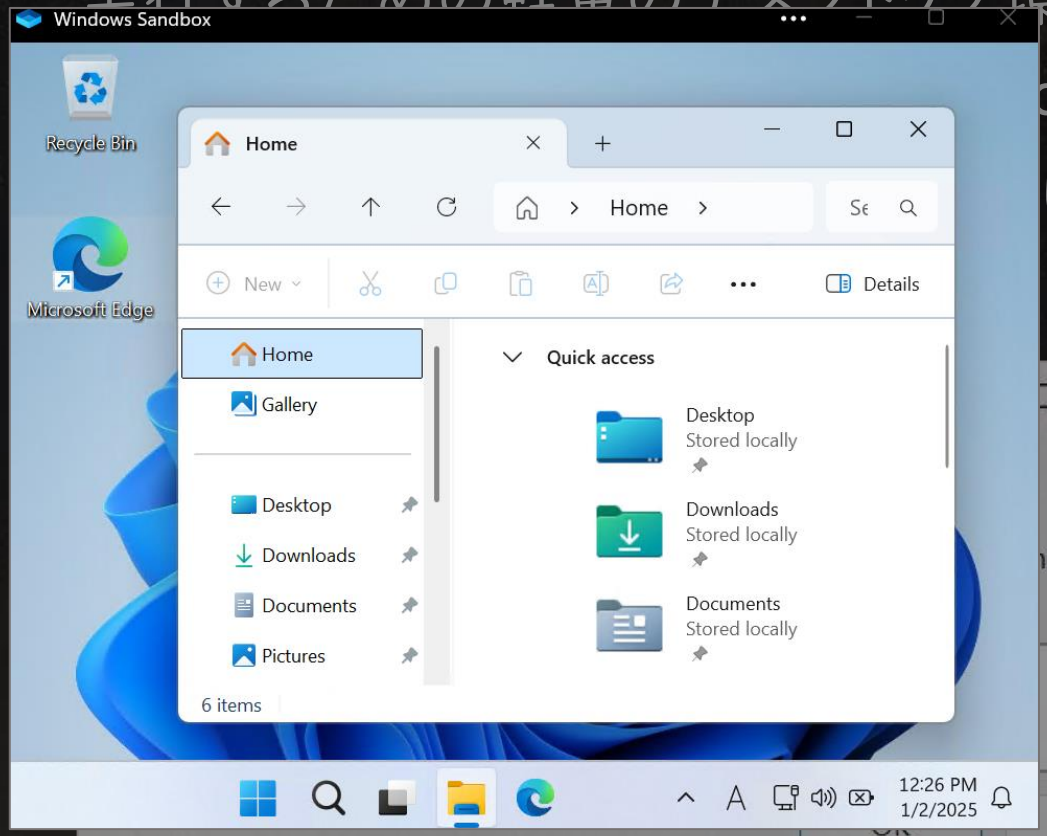
Windows Features GUI

```
Enable-WindowsOptionalFeature -FeatureName
"Containers-DisposableClientVM" -All -Online
```

PowerShell Command

利用環境と条件

- Windows Sandbox はホストシステムと独立したアプリケーションを単独かつ安全に実行するための軽量のデスクトップ環境




```
systeminfo
----
Host Name:                          1E65A2DC-B59B-4
OS Name:                            Microsoft Windows 11
Enterprise OS Version:              10.0.26100 N/A Build 26100
OS Manufacturer:                    Microsoft Corporation
~ Redacted ~
Total Physical Memory:              1,023 MB
Available Physical Memory:          42 MB
Virtual Memory: max Size:           2,751 MB
Virtual Memory : Available:         805 MB
Virtual Memory : In Use:            1,946 MB
Page File Location(s):              C:\pagefile.sys
Domain:                             WORKGROUP
Logon Server:                       \\1E65A2DC-B59B-4
~ Redacted ~
----
```

Windows Features GUI

利用環境と条件

- WDAGUtilityAccount はデフォルトユーザーとしてサンドボックス上に作成される
- Administrators グループに所属

```
C:\Users\WDAGUtilityAccount>net user WDAGUtilityAccount
User name                    WDAGUtilityAccount
Full Name
Comment                      Windows Defender Application Guard
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/8/2025 8:29:15 AM
Password expires             Never
Password changeable          1/8/2025 8:29:15 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/8/2025 9:11:44 PM

Logon hours allowed          All

Local Group Memberships      *Administrators *Remote Desktop Users *Users
Global Group memberships     *None
```

サンドボックス内のアンチウィルス機能

- デフォルトでサンドボックスは無効化
- GUI、Powershell の双方においても有効化は不可

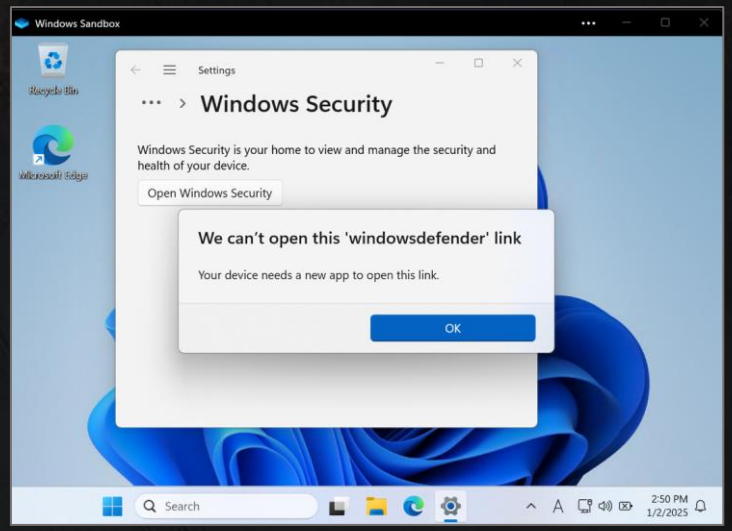
```
PS C:\Users\WDAGUtilityAccount> Get-MpComputerStatus


AMEngineVersion                 : 0.0.0.0
AMProductVersion                : 4.18.23110.3
AMRunningMode                   : Not running
AMServiceEnabled                : False
AMServiceVersion                : 0.0.0.0
AntispywareEnabled              : False
AntispywareSignatureAge         : 0
AntispywareSignatureLastUpdated :
AntispywareSignatureVersion     :
AntivirusEnabled                : False
AntivirusSignatureAge           : 65535
AntivirusSignatureLastUpdated   :
AntivirusSignatureVersion       :
BehaviorMonitorEnabled          : False
```

~ *Redacted* ~

```
OnAccessProtectionEnabled       : False
ProductStatus                   : 1
QuickScanAge                    : 4294967295
QuickScanEndTime                :
QuickScanOverdue                : False
QuickScanSignatureVersion       :
QuickScanStartTime              :
RealTimeProtectionEnabled       : False
RealTimeScanDirection           : 0
```

The Status of Windows Defender



Windows Defender GUI Settings

```
PS C:¥Users¥WDAGUtilityAccount¥Downloads> Set-MpPreference -DisableRealtimeMonitoring 0
Set-MpPreference : Operation failed with the following error: 0x800106ba. Operation: Set-M
pPreference. Target: DisableRealtimeMonitoring.
At line:1 char:1
+ Set-MpPreference -DisableRealtimeMonitoring 0
+
    + CategoryInfo          : NotSpecified: (MSFT_MpPreference:root¥Microsoft¥...FT_MpPre
   ference) [Set-MpPreference], CimException
    + FullyQualifiedErrorId : HRESULT 0x800106ba,Set-MpPreference
```

Disabling Windows Defender Using PowerShell Command

サンドボックスの構成ファイル(.wsb)

- サンドボックスのカスタマイズにおいて、
  XML ベースでの構成ファイル (.wsb) を使用することが可能

Sample.wsb

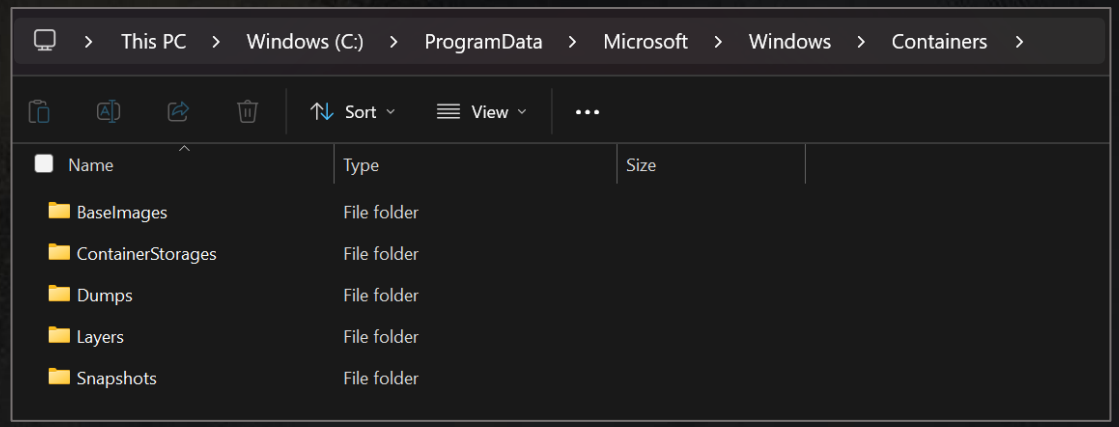
```
<Configuration>
 <Networking>Enable</Networking>
  <MappedFolders>
    <MappedFolder>
      <HostFolder>C:\Users\Public\Downloads</HostFolder>
      <SandboxFolder>C:\Users\WDAGUtilityAccount\Downloads</SandboxFolder>
      <ReadOnly>false</ReadOnly>
    </MappedFolder>
  </MappedFolders>
  <LogonCommand>
    <Command>explorer.exe</Command>
  </LogonCommand>
  <MemoryInMB>1024</MemoryInMB>
</Configuration>
```

WSB ファイルの設定項目

設定項目	概要
vGPU	GPU 共有の有効化/無効化
Networking	サンドボックス内の通信の有効化/無効化
Mapped folders	ホスト側とサンドボックス内のフォルダの共有設定 （絶対パス指定が必要）
Logon command	サンドボックスログオン後に自動実行されるコマンド
Audio input	サンドボックスへのオーディオ入力の有効化/無効化
Video input	サンドボックスへのビデオ入力の有効化/無効化
Protected client	AppContainer 分離実行環境内でサンドボックスを実行
Printer redirection	ホストからサンドボックスへのプリンター共有の有効化/無効化
Clipboard redirection	サンドボックスとのホスト クリップボードの共有
Memory in MB	サンドボックスが使用できるメモリの量（MB）の指定

Virtual Hard Disk(VHDX)

- Windows Sandbox は VHDX で構成されており、差分バックアップ方式が採用
- 以下フォルダ配下に VHDX 関連フォルダが格納
  - C:¥ProgramData¥Microsoft¥Windows¥Containers¥
- このフォルダは親子の複数の VHDX ファイルが保存されている



VHDX folders in Windows ＩＩ

- サンドボックスが終了すると差分バックアップが消失する

差分バックアップの関係性

- サンドボックスが起動すると Containers folder 配下に保存される

C:¥ProgramData¥Microsoft¥Windows¥Containers¥

* An example chain in Windows 11

<Parent>
.¥ContainerStorages¥fbd7ba93-6b62-44cb-a59e-0cc2c59b697a¥sandbox.vhdx

↑ Parent Path

<Differencing>
.¥ContainerStorages¥2a3c6d32-561c-4096-b099-73945cff9665¥sandbox.vhdx

↑ Parent Path

<Differencing>
.¥ContainerStorages¥a73d9514-1027-4ead-a3cb-6009ac2e8f3e¥sandbox.vhdx

- 親仮想ディスクと差分仮想ディスクがチェーン構成となる
- このチェーン構成を確認するためには、Hyper-V を有効化して Get-VHD コマンドを実行する必要がある

SECTION 03

Abusing with WSB Files

WINDOWS - EASY

100
Points

★ ★ ★ ★ ★
5.0 70 Reviewers

APT アクターの攻撃手法の概要

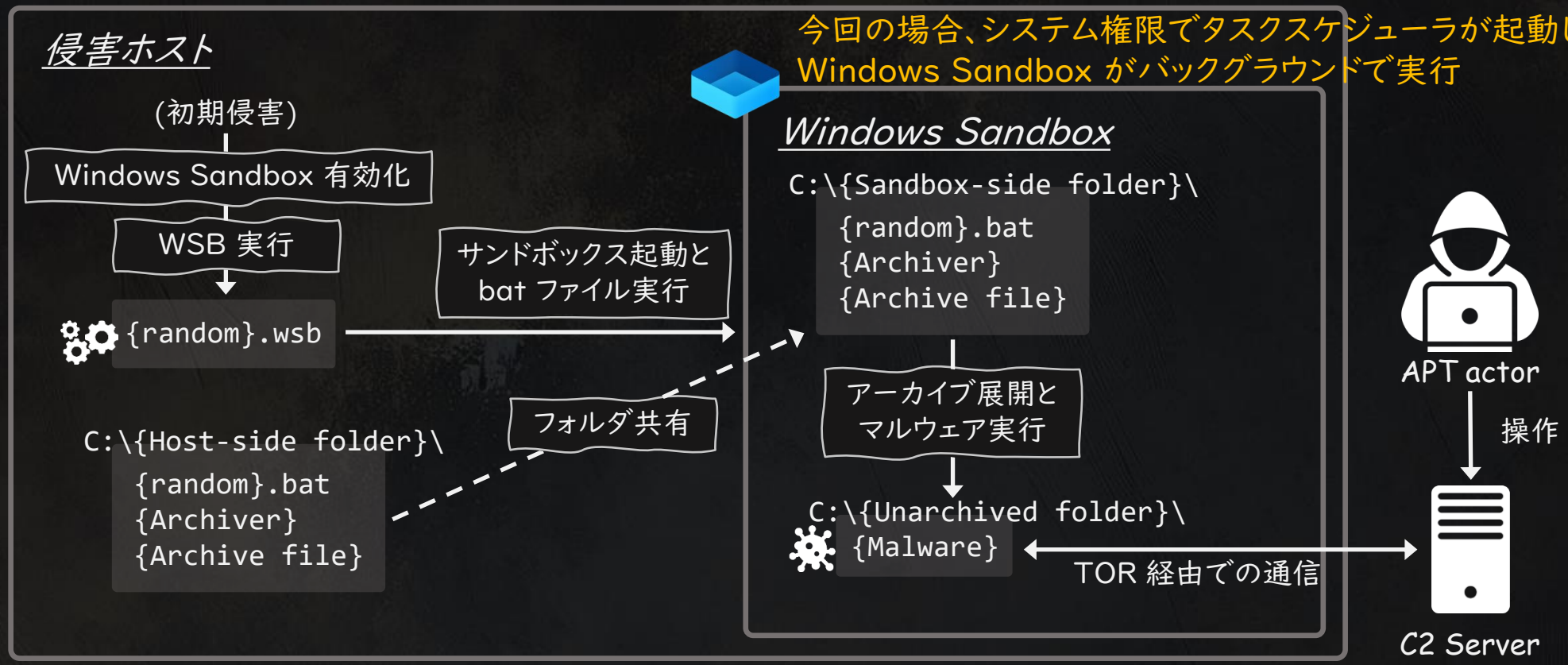
- APT アクターは初期侵害を行い、対象ホストの Windows Sandbox を有効化
- OS の再起動後、APT アクターは WSB ファイルを悪用し、サンドボックスを起動
- セカンドペイロードマルウェアを実行して C2 サーバとの通信を開始

サンドボックスを悪用した侵害ステップ

- APT アクターは初期侵害を行い、対象ホストのWindows Sandboxを有効化
- OS の再起動後、APT アクターは WSB ファイルを悪用し、サンドボックスを起動
- セカンドペイロードマルウェアを実行して C2 サーバとの通信を開始

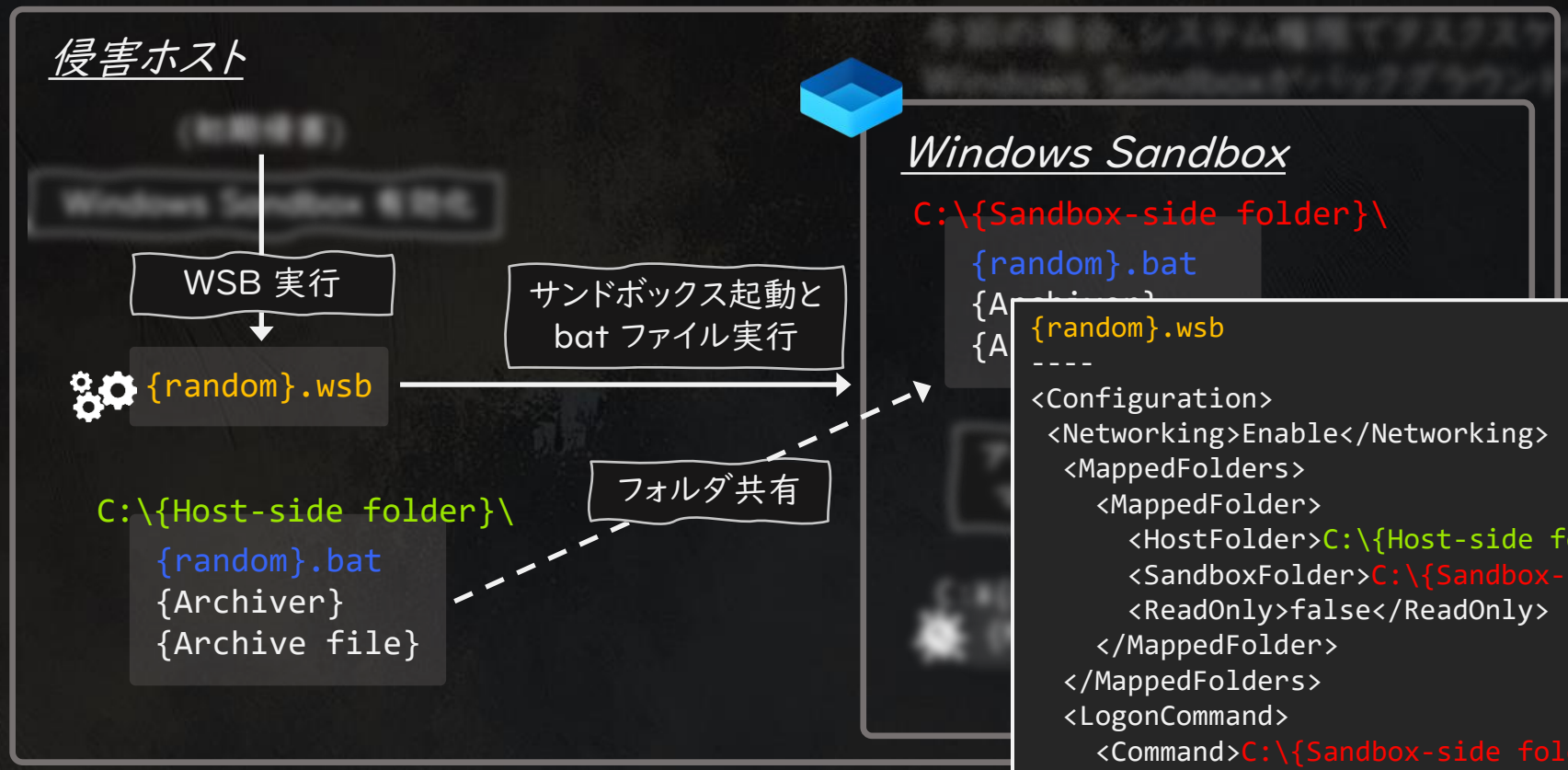
攻撃手法の詳細解説

- ステップ1：マルウェア実行の永続化



攻撃手法の詳細解説

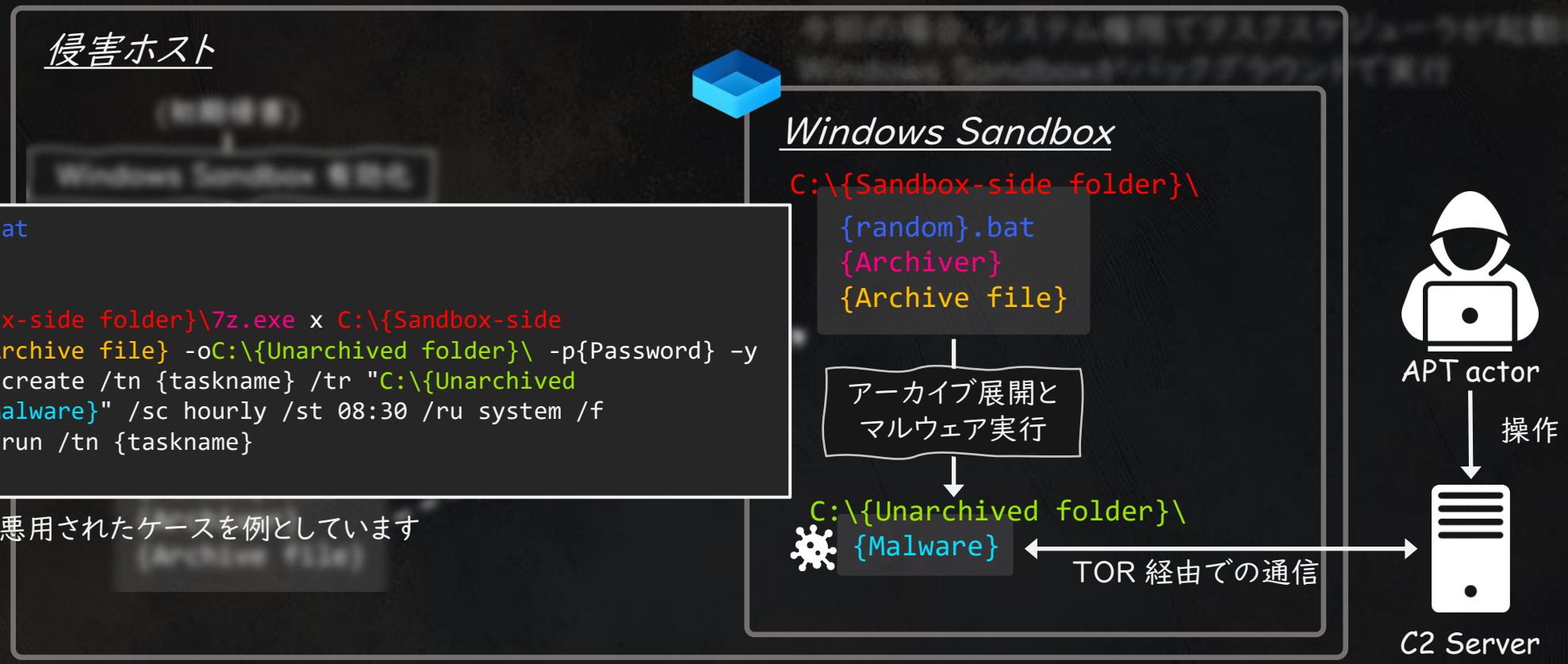
- ステップ2：フォルダ共有と bat ファイル実行




```
{random}.wsb
----
<Configuration>
 <Networking>Enable</Networking>
  <MappedFolders>
    <MappedFolder>
      <HostFolder>C:\{Host-side folder}</HostFolder>
      <SandboxFolder>C:\{Sandbox-side folder}</SandboxFolder>
      <ReadOnly>false</ReadOnly>
    </MappedFolder>
  </MappedFolders>
  <LogonCommand>
    <Command>C:\{Sandbox-side folder}\{random}.bat</Command>
  </LogonCommand>
  <MemoryInMB>1024</MemoryInMB>
</Configuration>
----
```

攻撃手法の詳細解説

- ステップ3：マルウェア展開と実行による C2 との通信




```
{random}.bat
---
@echo off
C:\{Sandbox-side folder}\7z.exe x C:\{Sandbox-side
folder}\{Archive file} -oC:\{Unarchived folder}\ -p{Password} -y
schtasks /create /tn {taskname} /tr "C:\{Unarchived
folder}\{Malware}" /sc hourly /st 08:30 /ru system /f
schtasks /run /tn {taskname}
----
```

* 7zip が悪用されたケースを例としています

SECTION 04

Emerging threats

WINDOWS - HARD

200
Points

★ ★ ★ ★ ★
5.0 80 Reviewers

Windows Sandbox Updates!

- 重要なアップデートが発生！
- Windows 11 の OS build preview のみ概要を言及されており、公式ドキュメントには記載がされていない

Learn / Windows / Security /

Windows Sandbox

Article • 07/20/2024 • 5 contributors • Applies to: ✅ Windows 11, ✅ Windows 10 Feedback

In this article

- Windows edition and licensing requirements
- Prerequisites
- Installation
- Usage

Undocumented

Windows Sandbox [illegible] desktop environment to safely run applications in isolation. [illegible] inside the Windows Sandbox environment remains "sandboxed" and runs separately from the host machine.

A sandbox is temporary. When it's closed, all the software and files and the state are deleted. You get a brand-new instance of the sandbox every time you open the application. Note, however, that as of Windows 11, version 22H2, your data persists through a restart initiated from inside the virtualized environment—useful for installing applications that require the OS to reboot.

https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-overview

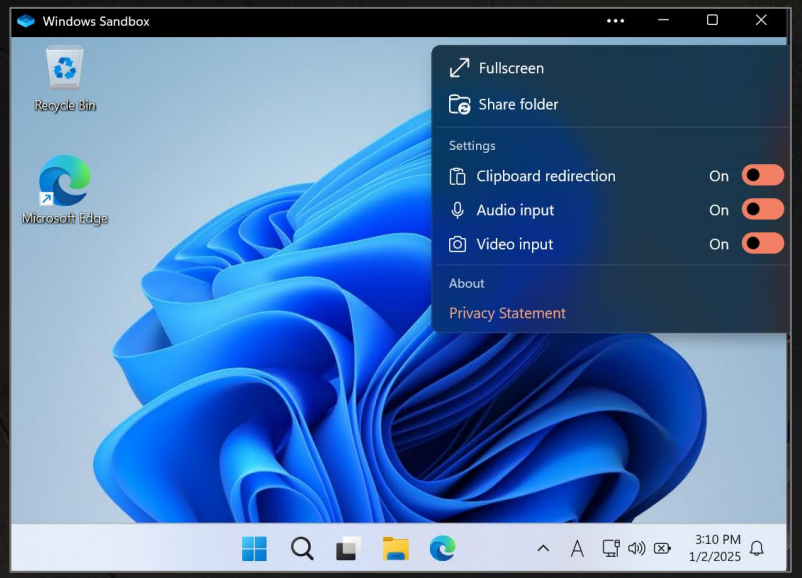
- **[Windows Sandbox Client Preview]** ***New!*** This update adds the Windows Sandbox Client Preview. It includes:
  - Runtime clipboard redirection
  - Audio and video input control
  - The sharing of folders with the host at runtime

  To access these, select the ellipses (...) at the upper right on the app. This preview also includes a version of command-line support. (The commands might change over time). To learn more, use the **wsb.exe–help** command. You can find new updates for this app in the Microsoft Store. This might not be available to all users because it will roll out gradually.

October 24, 2024—KB5044384 (OS Build 26100.2161) Preview

New Features

- Windows Sandbox にコンテナライクな CLI コマンドが実装
- Windows Sandbox はバックグラウンドで実行可能となる
- 簡単な設定変更が GUI を通して変更可能となる



Simple config change via GUI

```
> wsb.exe start
Windows Sandbox environment started successfully:
Id:  7f1397ca-3b46-416a-827a-a4a5b76e880e

> wsb.exe list
7f1397ca-3b46-416a-827a-a4a5b76e880e

> wsb.exe connect --id 7f1397ca-3b46-416a-827a-a4a5b76e880e
```

wsb command examples

WSB.exe Command Options

Commands, alias	Options	概要
StartSandbox, start	--id <id> -c, --config <config>	Windows Sandbox のインスタンス起動
ListRunningSandboxes, list	-	実行中のすべての Windows Sandbox 環境の ID を一覧表示
Execute, Exec	--id <id> (REQUIRED) -c, --command <command> (REQUIERED) -d, --working-directory <working-directory> -r, --run-as <ExistingLogin|System>(REQUIRED)	実行中の Windows Sandbox 環境でコマンドを実行
ShareFolder, share	--id <id> (REQUIRED) -f, --host-path <host-path>(REQUIRED) -s, --sandbox-path <sandbox-path> -w, --allow-write	ホストから Windows Sandbox セッションにフォルダを共有
StopSandbox, stop	-	実行中の Windows Sandbox の終了
ConnectToSandbox	--id <id>	Windows Sandbox 環境のリモートセッションの開始
GetIpAddress, ip	--id <id> (REQUIRED)	Windows Sandbox 環境の IP アドレスの取得

Windows Sandbox 新機能の悪用

- 新機能により WSB ファイルを利用することなく、サンドボックスが起動可能となる

例 ワンライナーでサンドボックスを起動

```
> wsb.exe start -c "<Configuration>
<Networking>Enable</Networking><MappedFolders><MappedFolder><HostFolder>C:\Users\Public\Downlo
ads</HostFolder><SandboxFolder>C:\Users\WDAGUtilityAccount\Desktop</SandboxFolder><ReadOnly>fa
lse</ReadOnly></MappedFolder></MappedFolders><LogonCommand><Command>C:\Users\WDAGUtilityAccoun
t\Desktop\a.bat</Command></LogonCommand><MemoryInMB>1024</MemoryInMB></Configuration>"
Windows Sandbox environment started successfully:
Id: c2d290db-5986-4c06-bd7b-05f35f091fa4
```

- 重要なアーティファクト「.wsb」が残らない
- 攻撃者の利便性が向上する恐れがある

Windows Sandbox 新機能の悪用

- 新機能に伴い、バックグラウンド実行と永続性に対するアップデートは、攻撃者の利便性を高める恐れがある

特徴	Windows 10	Windows 11
バックグラウンド実行	Not Available	Available by default
永続性	No *ウィンドウを閉じてサンドボックスを停止	Yes *サンドボックスの再起動後も残存 *明示的な wsb stop コマンド実行まで起動

*どちらの場合も、サンドボックスはプロセスが強制終了または再起動されると終了する

SECTION 05

Countermeasures

WINDOWS - HARD

200
Points

★ ★ ★ ★ ★
5.0 90 Reviewers

調査と監視

- ホスト側と Windows Sandbox 側の両方で、ある程度の監視と調査が可能

ホスト側

- クライアント端末の操作ログ、特徴的なプロセス、メモリの監視
- WSB ファイルに関連するアクティビティの監視
- 特徴的なイベントログの監視
- 一般的なフォレンジック調査のためのその他のアーティファクト

Windows Sandbox

- 操作ログやプロセスの監視や調査は困難
- ホスト側の親 VHDX と差分 VHDX を適切に保存することで、サンドボックス内の特定のアーティファクトを調査することが可能。

- Windows Sandbox からの通信は、ホストからの通信として監視可能

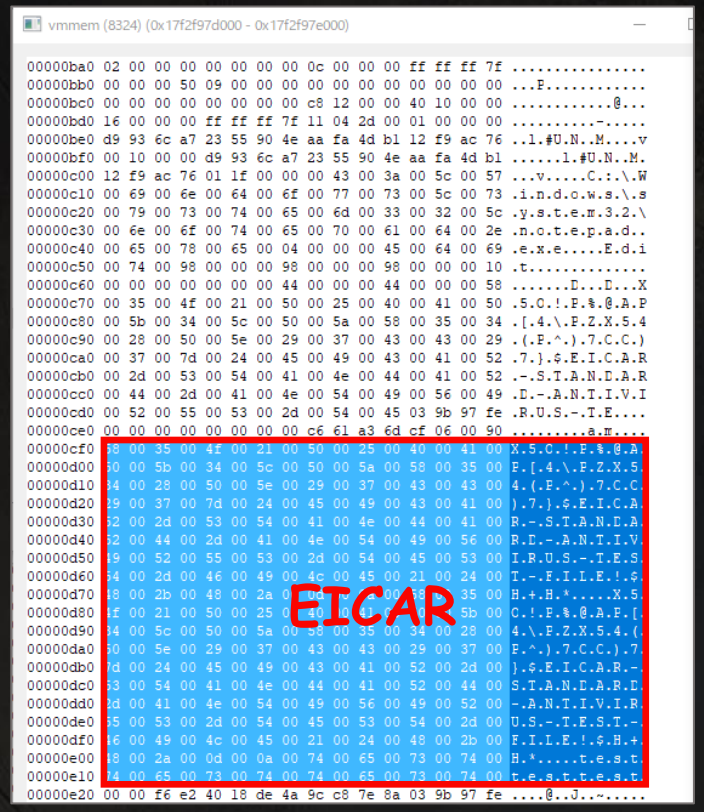
ホスト側のプロセス

- ホスト側でこれらのプロセス実行を優先的に監視することで、Windows Sandbox の起動を検出することが可能
- 実際には実行方法に応じて様々な引数が設定されることも注意が必要

プロセス名	パス	概要
WindowsSandbox.exe	C:¥Windows¥System32¥WindowsSandbox.exe	WSBファイル実行時と通常起動時
WindowsSandboxClient.exe	C:¥Windows¥system32¥WindowsSandboxClient.exe	
cmproxyd.exe	C:¥Windows¥system32¥cmproxyd.exe	
WindowsSandboxServer.exe	C:¥Program Files¥WindowsApps¥MicrosoftWindows.WindowsSandbox_0.3.1.0_x64__cw5n1h2txyewy	WSBファイル実行時、通常実行、wsb.exeによるコマンド実行(Windows 11ビルドプレビュー版0.3.1.0のみ)
WindowsSandboxRemoteSession.exe	C:¥Program Files¥WindowsApps¥MicrosoftWindows.WindowsSandbox_0.3.1.0_x64__cw5n1h2txyewy	
wsb.exe	C:¥Users¥{USERNAME}¥AppData¥Local¥Microsoft¥WindowsApps¥wsb.exe	wsb.exe を使用したコマンド発行時のみ（Windows 11ビルドプレビュー用）

Windows Sandbox のホスト側メモリ

- Windows Sandbox で実行されているプロセスは、ホスト側の vmmem プロセスで検出可能

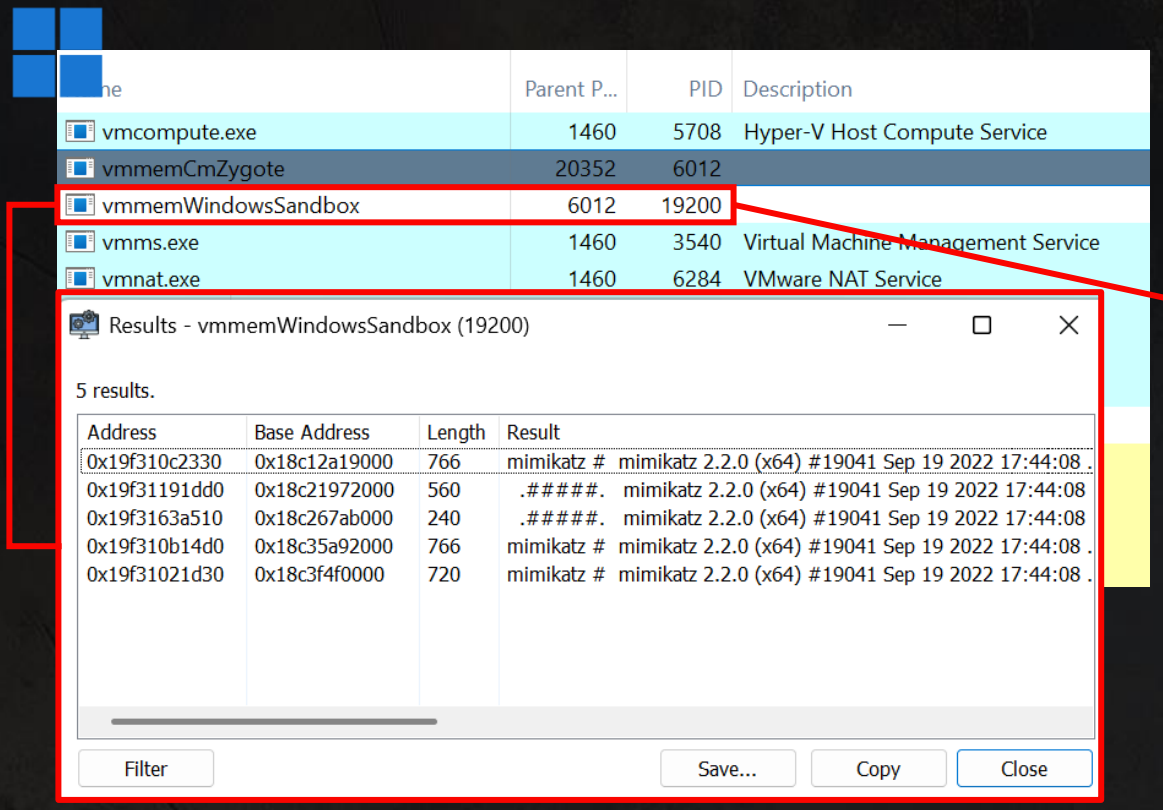


ホスト側で露呈した Windows Sandbox のメモリ

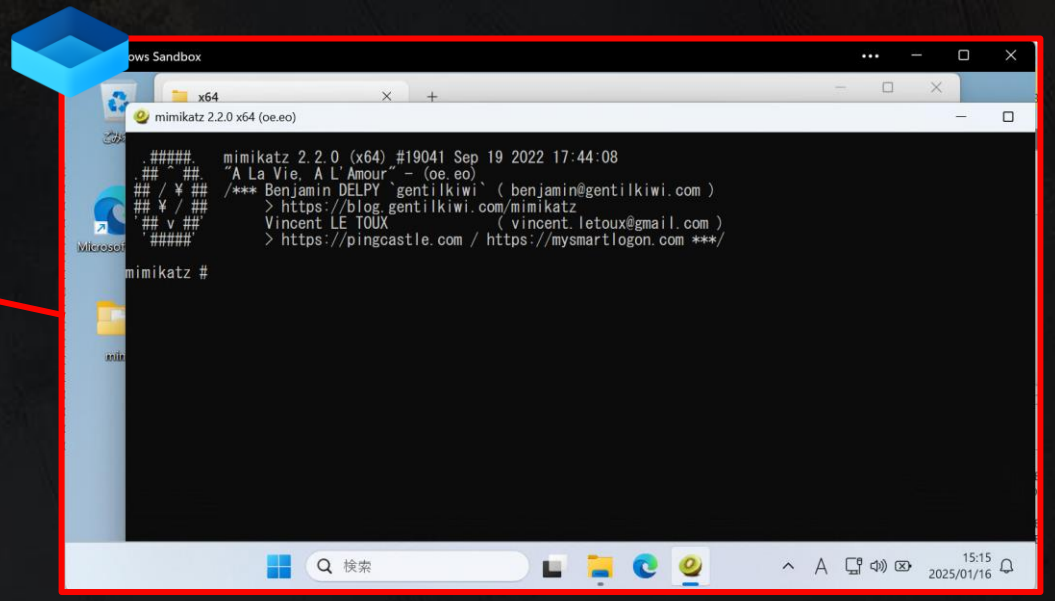
プロセス名	OS
vmmem	Windows 10
vmmemWindowsSandbox	Windows 11

Windows Sandbox のホスト側メモリ

- Windows Sandbox 内で Mimikatz を実行すると、ホスト側のメモリも露出されるため、Yara などのメモリスキャンで検出可能



ホスト側で露呈した Windows Sandbox のメモリ



Windows Sandbox で実行した Mimikatz

ホスト側の重要なアーティファクト

- Windows Sandbox の内部動作の痕跡は記録されないが、ホスト側にはサンドボックスの有効化と起動関連の痕跡は残存する場合がある
- 以下アーティファクトに注目し、関連する兆候を調査することを推奨

アーティファクト	概要
$MFT	WSB ファイルの作成、マウントソースフォルダとファイルの作成、VHDX ファイルの作成が記録
$UsnJrnl	WSB ファイルの作成、マウントソースフォルダとファイルの作成、VHDX ファイルの作成が記録
Prefetch	WSB と VDHX ファイルのロードが記録されることがある。
Registry	以下が設定 • HKLM¥SOFTWARE¥Classes¥Applications¥WindowsSandbox.exe • HKLM¥SOFTWARE¥Classes¥Windows.Sandbox¥shell¥open¥command • HKLM¥SOFTWARE¥Microsoft¥Windows Sandbox¥Capabilities¥FileAssociations
Eventlog	* 次ページ記載

ホスト側の重要なアーティファクト: Event Log 1/2

Classification	Evtx	Source	Event ID	概要
Eventlog	System	Microsoft-Windows-Hyper-V-VmSwitch	102	仮想マシンのネットワークドライバー設定
			232	仮想マシンの NIC ポートに関する情報
			233	仮想マシンの NIC に関する情報

	Security	Microsoft-Windows-Security-Auditing	4624	• アカウントの正常なログオン
				  • Account Domain : NT VIRTUAL MACHINE
				  • Process Name : C:¥Windows¥System32¥vmcompute.exe

			4648	• 明示的な認証情報を使用したログオン試行
				  • Account Domain : NT VIRTUAL MACHINE
				  • Process Name : C:¥Windows¥System32¥vmcompute.exe

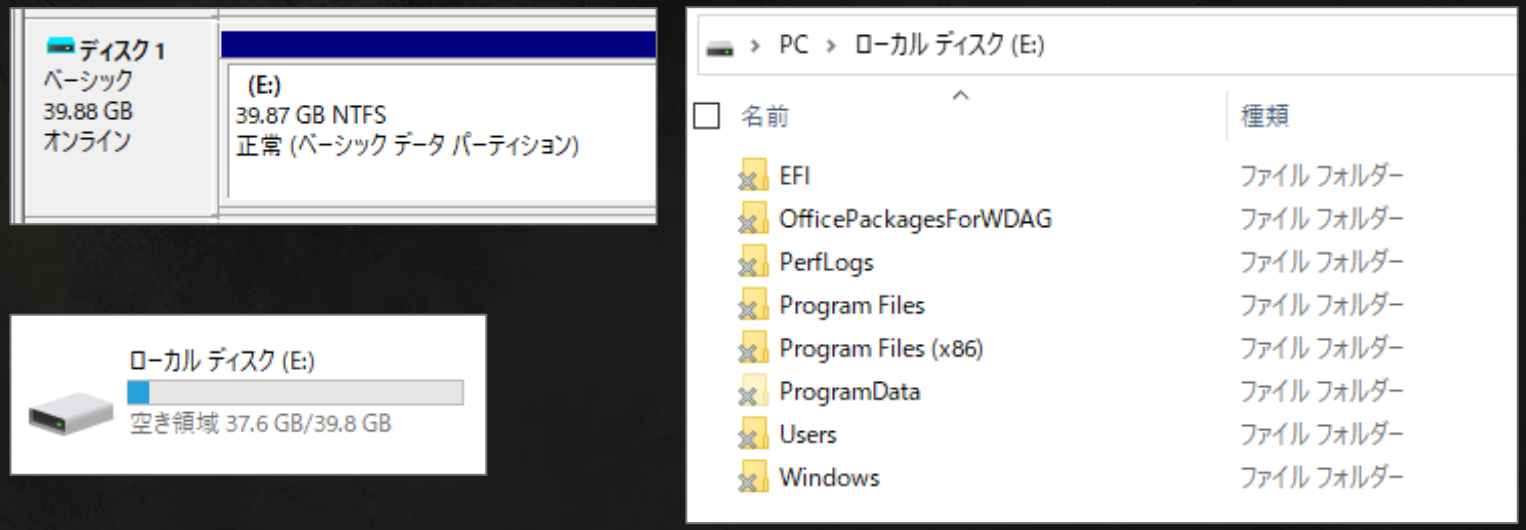
			4672	• 新しいログオンへの特別な権限割り当て • Account Domain : NT VIRTUAL MACHINE
	Microsoft-Windows-Hyper-V-Worker-Admin	• Microsoft-Windows-Hyper-V-SynthStor • Microsoft-Windows-Hyper-V-Worker	12148	仮想マシンの起動に関する情報
			12582	
			12597	仮想ネットワーク接続情報
			18500	仮想マシンの起動情報
			18502	仮想マシンの電源オフに関する情報
			18516	仮想マシンの中断に関する情報
			18596	仮想マシンの復元に関する情報
			18601	仮想マシンの起動情報
			18609	仮想マシンの初期化に関する情報

ホスト側の重要なアーティファクト: Event Log 2/2

Classification	Evtx	Source	Event ID	概要
Eventlog	Microsoft-Windows-Hyper-V-Worker-Operational	Microsoft-Windows-Hyper-V-VSmb	301	仮想マシンをマウントするフォルダに関する情報
	Microsoft-Windows-Hyper-V-Compute-Operational	Microsoft-Windows-Hyper-V-Compute	2500	プロセスの作成およびコマンド実行に関する情報
	Setup	Microsoft-Windows-Servicing	9	「Microsoft-Windows-Containers-OptionalFeatures」の「Containers-DisposableClientVM」の選択可能な更新が正常に有効化された
			13	「Microsoft-Windows-Containers-OptionalFeatures」の「Containers-DisposableClientVM」の選択可能な更新を有効化するには、再起動が必要
	Microsoft-Windows-VHDMP-Operational	Microsoft-Windows-VHDMP-Operational	1	仮想ディスクに関する情報（マウント/アンマウント、オンライン/オフラインなど）
			2	
			12	
			17,18	
			22~28	
			31~34	
			50,51	

Windows Sandbox Disk Image Forensics(VHDX)

- 親仮想ディスクと差分仮想ディスクのチェーンが維持されていれば、正しく保存された VHDX をマウントすることが可能
- したがって、一般的なフォレンジック調査が可能
- Windows Sandbox のプロセスが発見された場合、VHDXに関連するフォルダ全てを揮発性データとして保全する必要がある



VHDX mounted and drive assigned

Windows Sandbox 収集可能なアーティファクト

- フォレンジックで一般的に有用とされるアーティファクトの残存状況を検証した結果を示す
- 無効になっているものや完全でないアーティファクトもあるが、フォレンジック調査に極めて有用なアーティファクトも残存している

* Windows 10 / Windows 11

アーティファクト	利用可否	特記事項
$MFT	可	ホストからの共有フォルダに対する操作は記録されていない
$UsnJrnl	可	ホストからの共有フォルダに対する操作は記録されていない
Prefetch	否	記録なし
Registry	可	我々の検証では、Amcache のアップデートは確認できず
Browser History	可	デフォルトでインストールされたEdge のアクセス履歴は記録された ユーザによってインストールされたブラウザの履歴も記録された
SRUM	否	記録なし
Evtx	可	デフォルトのログストレージサイズは 20,480KB いくつかの有用なイベント（タスクスケジュールなど）は記録されない 成功したログオン（イベント ID 4624）、失敗したログオン（イベント ID 4625）、明示的な認証情報によるログオン（イベント ID 4648）、およびサービスのインストール（イベント ID 7045）などのログオンは記録される

ホスト側管理策

- Windows Sandbox の無効化状態を維持し続けることが望ましい
  - 意図しないサンドボックスの有効化を検出する必要がある

例: AppLocker ポリシーの適用

- AppLocker は Windows Sandbox の実行をコントロール可能
  AppLocker が Windows Sandbox をブロックした場合、イベントログに記録される

Evtx	Source	Event ID	概要
Microsoft-Windows-AppLocker/EXE and DLL	Microsoft-Windows-AppLocker	8002	AppLocker ルールが .exe または .dll ファイルを許可したことを記録
		8003	AppLocker ポリシーにリストされている .exe または .dll ファイルを AppLocker が記録したことを記録 監査のみの実施モードが有効な場合にのみ表示
		8004	AppLocker が指定された EXE または DLL ファイルをブロックしたことを記録（ルール強制モードが有効な場合にのみ表示）

ユーザーに管理者権限を与えないこと

SECTION 06

Conclusions

WINDOWS - HARD

200
Points

★ ★ ★ ★ ★
5.0 100 Reviewers

Conclusions

- 2024年、MirrorFace（別名 APT10）による Windows Sandbox の悪用が観測された
- ホスト上の EDR や AV での検出が難しい場合、監視の強化、徹底的な調査、効果的な管理といったプロアクティブな防御対策がリスクの最小化には不可欠である
- 利便性向上を目的とした新機能の開発が、意図せず攻撃者に有利に働く危険性も考えられる
- 攻撃者は往々にして我々の予想の範疇を超え、盲点や隙を巧みに突いてくるため、予想外の事態を予測可能にする努力を続け、脅威に対抗していくことが重要である


ITOCHU
Cyber &
Intelligence
Thanks for Listening ;)

References

- https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html
- https://blogs.jpcert.or.jp/en/2024/07/mirrorface-attack-against-japanese-organisations.html
- https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/
- https://www.thomasmaurer.ch/2019/05/how-to-configure-windows-sandbox/
- https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-overview
- https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-architecture
- https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-configure-using-wsb-file
- https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-windowssandbox
- https://dspace.cvut.cz/bitstream/handle/10467/114685/F8-DP-2024-Strom-Jakub-thesis.pdf
- https://research.checkpoint.com/2021/playing-in-the-windows-sandbox/
- https://support.microsoft.com/en-us/topic/october-24-2024-kb5044384-os-build-26100-2161-preview-5a4ac390-7c7b-4f7f-81c2-c2b329ac86ab
- https://techcommunity.microsoft.com/blog/windows-itpro-blog/windows-news-you-can-use-november-2024/4336665

Japanese sources

- https://answers.microsoft.com/ja-jp/windows/forum/all/windows-sandbox-%E3%81%AE%E7%B4%B9%E4%BB%8B/1660e8da-9a61-4273-afd5-dc9688e84e11
- https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html
- https://www.npa.go.jp/bureau/cyber/pdf/20250108_caution.pdf
- https://www.npa.go.jp/bureau/cyber/pdf/20250108_windowssandbox.pdf

Appendix – 検証環境情報

- 検証した OS バージョン

Host OS version	Windows Sandbox version	wsb version
Microsoft Windows 10 Enterprise 10.0.19045	Microsoft Windows 10 Enterprise 10.0.19041	N/A
Microsoft Windows 10 Enterprise 10.0.19045	Microsoft Windows 10 Enterprise 10.0.19045	N/A
Microsoft Windows 11 Pro 10.0.26100	Microsoft Windows 11 Enterprise 10.0.26100	0.3.1.0