
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

- The National Police Agency (NPA) has issued an advisory regarding an attack campaign by “MirrorFace”.
- Details regarding the attack method abusing Windows Sandbox, along with traces and detection measures, have also been made public.

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

Translated into English

Cyberattack Advisory Regarding "MirrorFace"

The National Police Agency (NPA) and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) have assessed that a cyberattack campaign targeting organizations, businesses, and individuals in Japan since around 2019 has been orchestrated by a cyberattack group known as "MirrorFace" (also referred to as "Earth Kasha").

Moreover, investigations and analyses conducted by the Cyber Affairs Bureau, the Tokyo Metropolitan Police Department, and other prefectural police departments have uncovered details about the targets, techniques, and infrastructure utilized in these attacks. Based on these findings, the "MirrorFace" campaign has been identified as an organized cyberattack, suspected to involve Chinese entities, primarily aiming to steal information related to Japan's national security and advanced technologies.

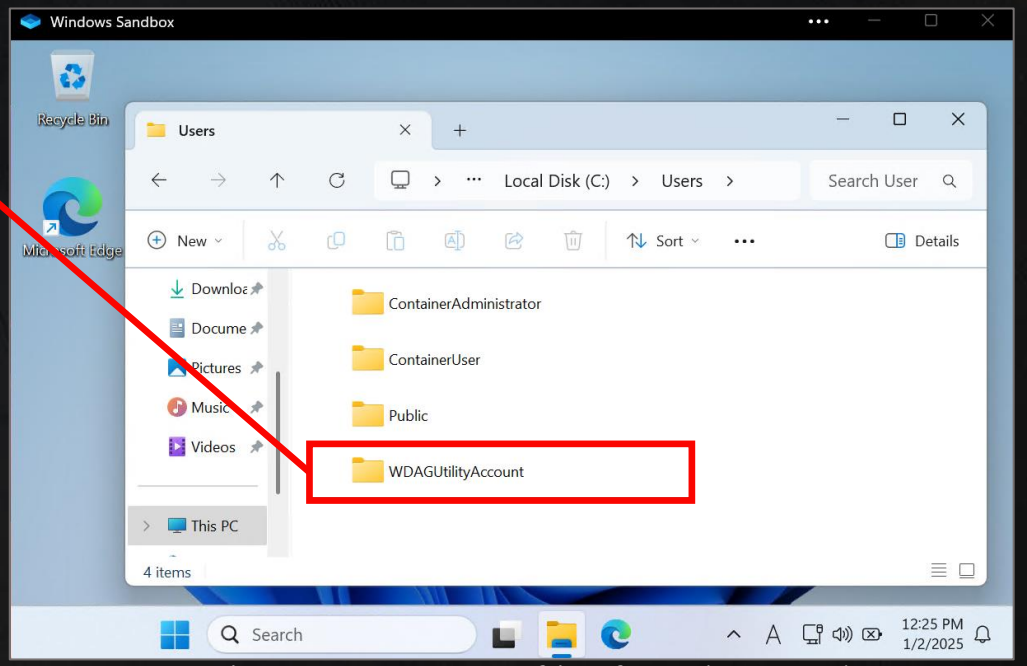
This advisory seeks to expose the tactics employed in "MirrorFace" cyberattacks to increase awareness among potential targets—organizations, businesses, and individuals regarding the threats they face in cyberspace. Additionally, it aims to encourage the adoption of appropriate security measures to mitigate the risk of further damage and prevent potential breaches.

Discovering Important Clues to Unlock Secrets

- Mirrorface (APT10 Umbrella) attack campaign utilizing LilimRAT, a customized version of open-sourse Lilith RAT*, was observed.
- LilimRAT checks WDAGUtilityAccount folder if it is running in a Windows Sandbox.
- The "WDAGUtilityAccount" is the fixed default username used by Windows Sandbox.

```
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;
```

User folder checking function implemented in LilimRAT

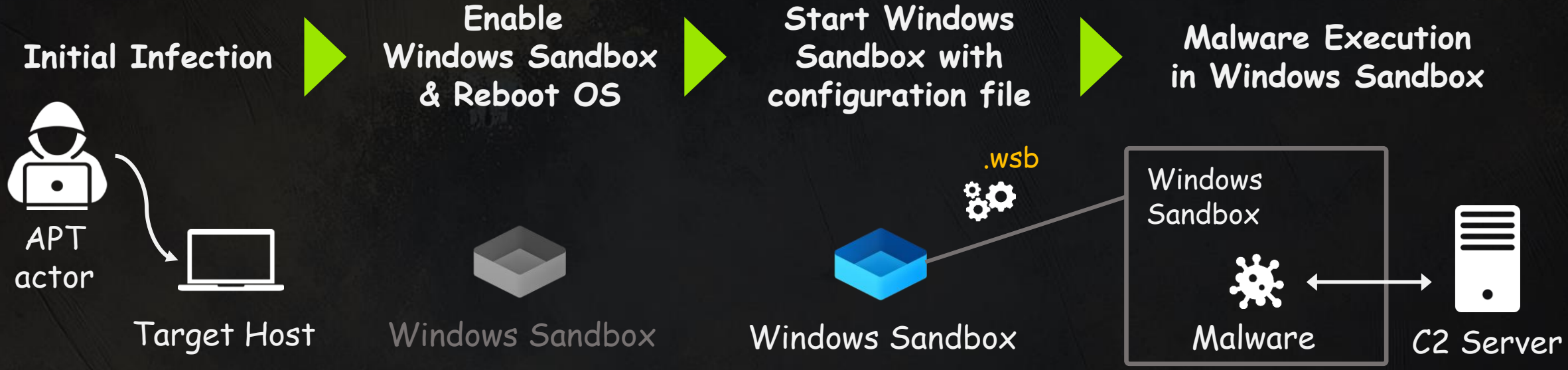


WDAGUtilityAccount Userprofile of Windows Sandbox

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

The APT Actor Methods Revealed

- The APT actor intrude into the system and enabled the Windows Sandbox.
- After reboot, they used the WSB file to launch the Sandbox.
- Executed the 2nd payload malware and initiated communication with C2 server.



Our Motivation

FACT

In this case, the APT actor abused Windows Sandbox.

ASSUMPTION

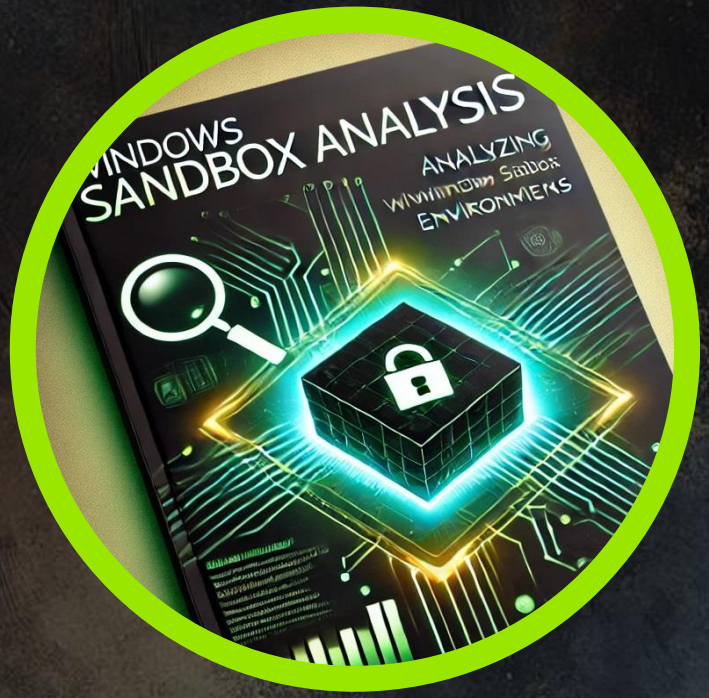
They may have used it to hide their activities?

CONCERNs

- ✓ Are all activities hidden?
- ✓ Can detailed Windows Sandbox specs counter this?
- ✓ Are conventional artifacts inadequate?

PURPOSE

As a Blue Team, we aim to address these concerns and provide actionable insights for countermeasures!



SECTION 02

About Windows Sandbox

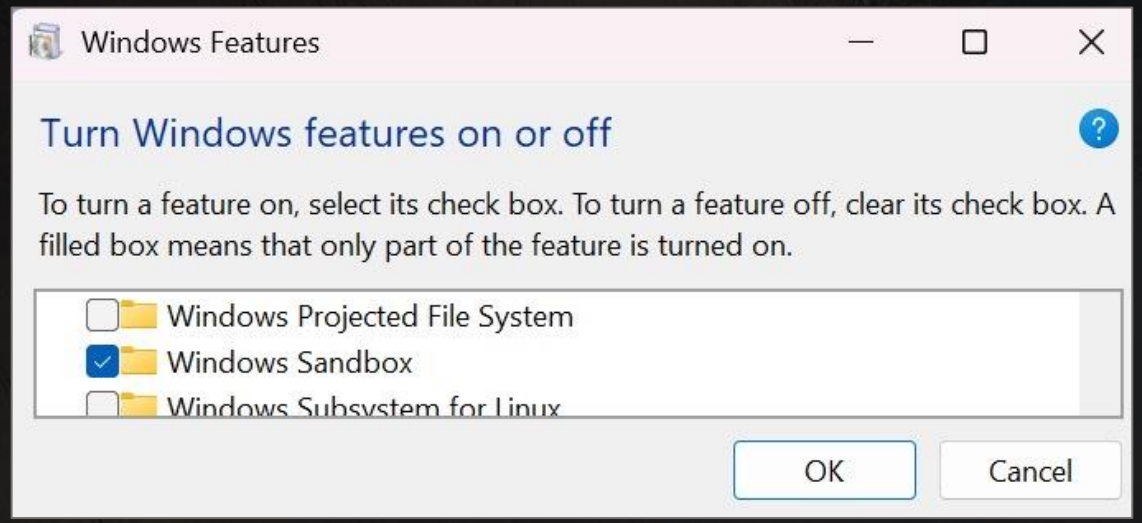
WINDOWS - EASY

50
Points

★ ★ ★ ★ ★
5.0 60 Reviewers

Environment and Conditions

- Windows Sandbox provides a secure and lightweight environment to run applications isolated from the host system, available from Windows 10 (build 18342) and Windows 11.
- By default, Windows Sandbox is disabled and must be manually enabled before use.



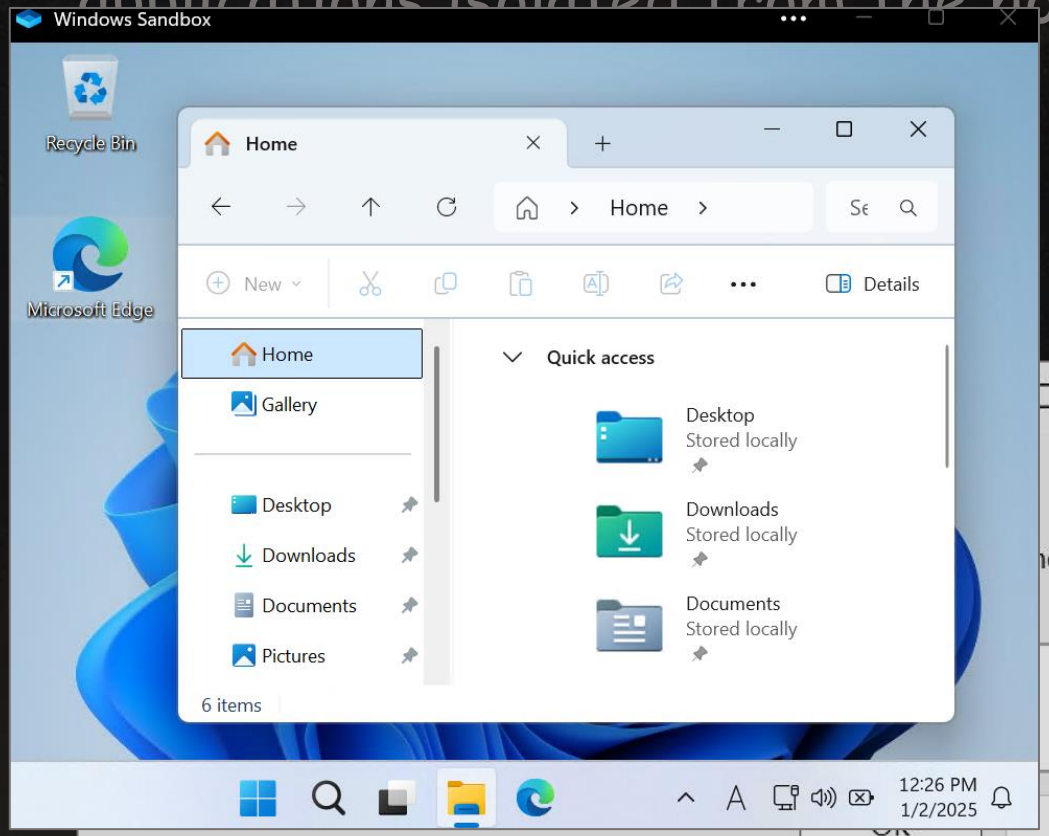
Windows Features GUI

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

PowerShell Command

Environment and Conditions

- Windows Sandbox provides a secure and lightweight environment to run applications isolated from the host system, available from Windows 10




```
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

Environment and Conditions

- The "WDAGUtilityAccount" is created in Windows Sandbox by default.
  - Additionally, this user is a member of the Administrators group.

```
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
```

Anti-Virus within Windows Sandbox

- Regarding Anti-Virus feature, it is disabled by default and cannot be enabled through either GUI or PowerShell

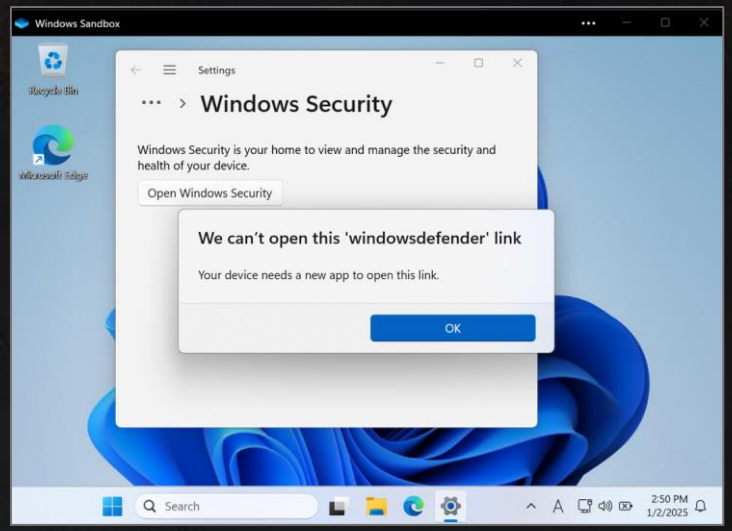
```
PS C:\Users\WDAGUtilityAccount> Get-MpComputerStatus


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

Configuration File(.wsb)

- Supports XML-based configuration files (.wsb) for customization

Sample.wsb

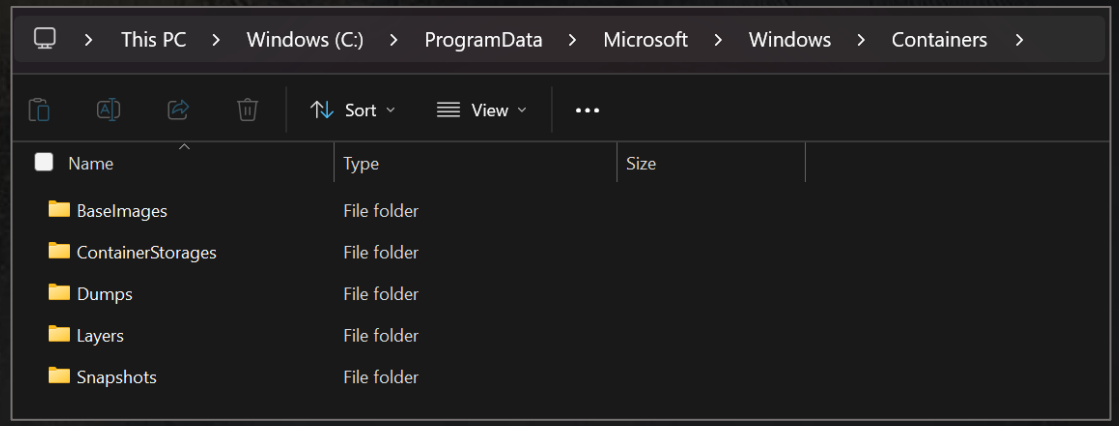
```
<Configuration>
 <Networking>Enable</Networking>
  <MappedFolders>
    <MappedFolder>
      <HostFolder>C:\Users\Public\Downloads</HostFolder>
      <SandboxFolder>C:\Users\WDAGUtilityAccount\Downloads</SandboxFolder>
      <ReadOnly>false</ReadOnly>
    </MappedFolder>
  </MappedFolders>
  <LogonCommand>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

Type of Configuration Item

Configuration item	Description
vGPU	Enables or disables GPU sharing.
Networking	Enables or disables networking in the sandbox.
Mapped folders	An array of folders, each representing a location on the host machine that is shared with the sandbox at the specified path.
Logon command	Specifies a single command that will be invoked automatically after the sandbox logs on.
Audio input	Shares the host's microphone input into the sandbox.
Video input	Shares the host's webcam input into the sandbox.
Protected client	Sandbox adds a new layer of security boundary by running inside an AppContainer Isolation execution environment.
Printer redirection	Enables or disables printer sharing from the host into the sandbox.
Clipboard redirection	Enables or disables sharing of the host clipboard with the sandbox.
Memory in MB	Specifies the amount of memory that the sandbox can use in MB.

Virtual Hard Disk(VHDX)

- Windows Sandbox is composed of a virtual disks called VHDXs, which have a parent virtual disk and a differential virtual disk.
- When the sandbox starts, the following folders are created.
  - C:\ProgramData\Microsoft\Windows\Containers\
- The created folder has multiple folders where the parent virtual disk and differential virtual disk are placed.



VHDX folders in Windows 11

- When the sandbox ends, the differential virtual disk disappears.

Relationship between Parent and Differential Backups

- During incident response, the Containers folder must be saved while the sandbox is running.

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

- The parent virtual disk and differential virtual disk are connected in a chain.
- To verify this chain configuration, Hyper-V must be enabled, and the Get-VHD command needs to be executed.

SECTION 03

Abusing with WSB Files

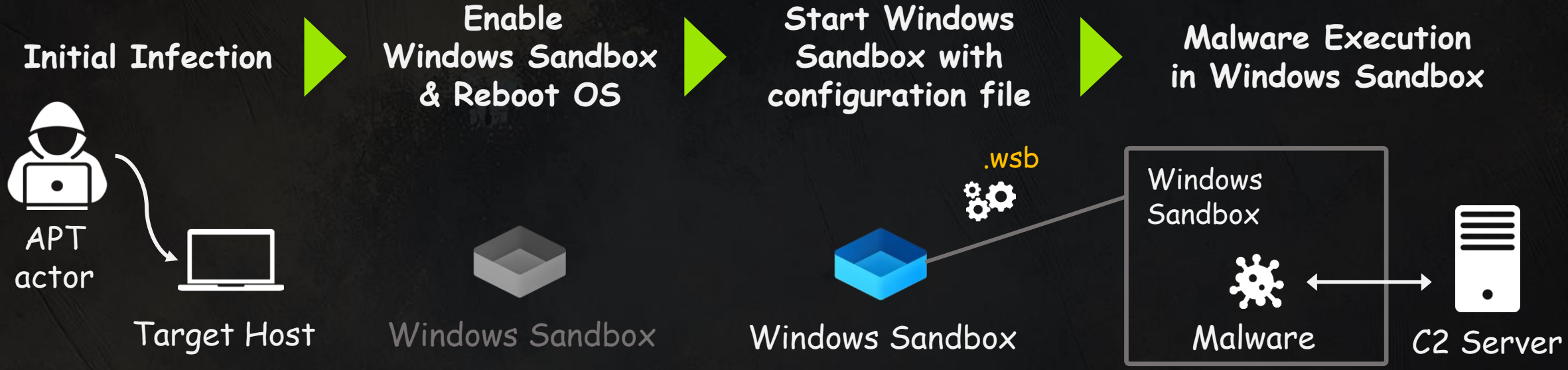
WINDOWS - EASY

100
Points

★ ★ ★ ★ ★
5.0 70 Reviewers

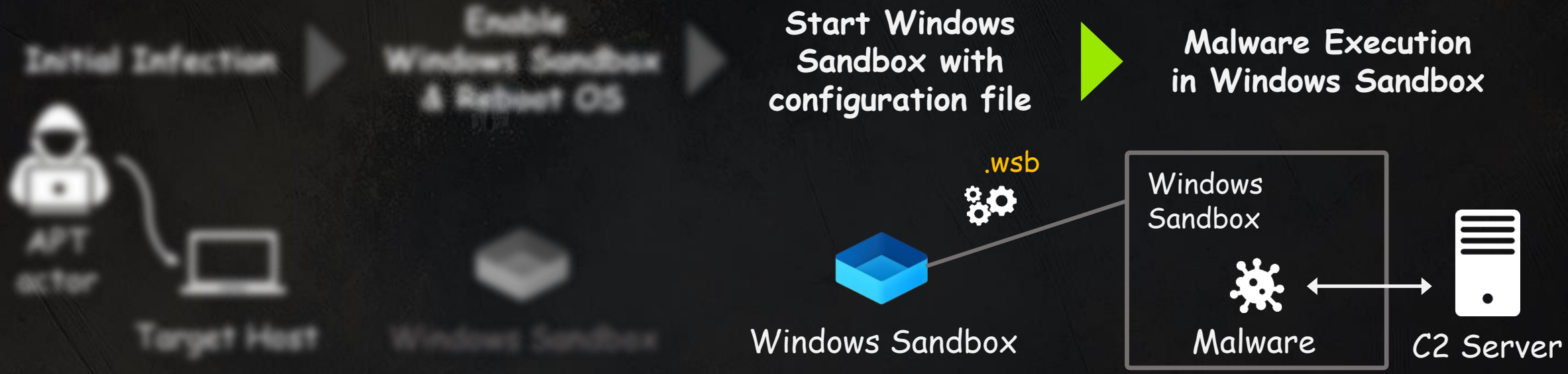
The APT Actor Methods Revealed

- The APT actor intrude into the system and enabled the Windows Sandbox.
- After reboot, they used the WSB file to launch the Sandbox.
- Executed the 2nd payload malware and initiated communication with C2 server.



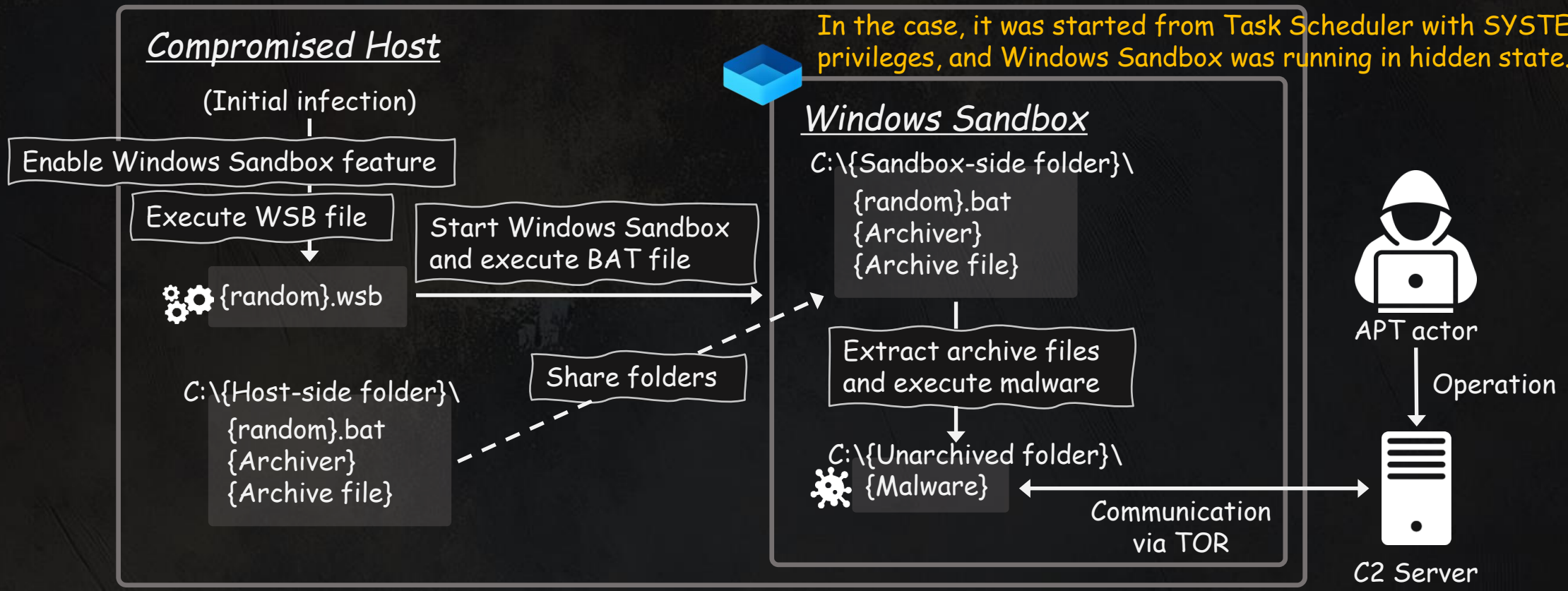
The APT Actor Methods Revealed

- The APT actor intrude into the system and enabled the Windows Sandbox.
- After reboot, they used the WSB file to launch the Sandbox.
- Executed the 2nd payload malware and initiated communication with C2 server.



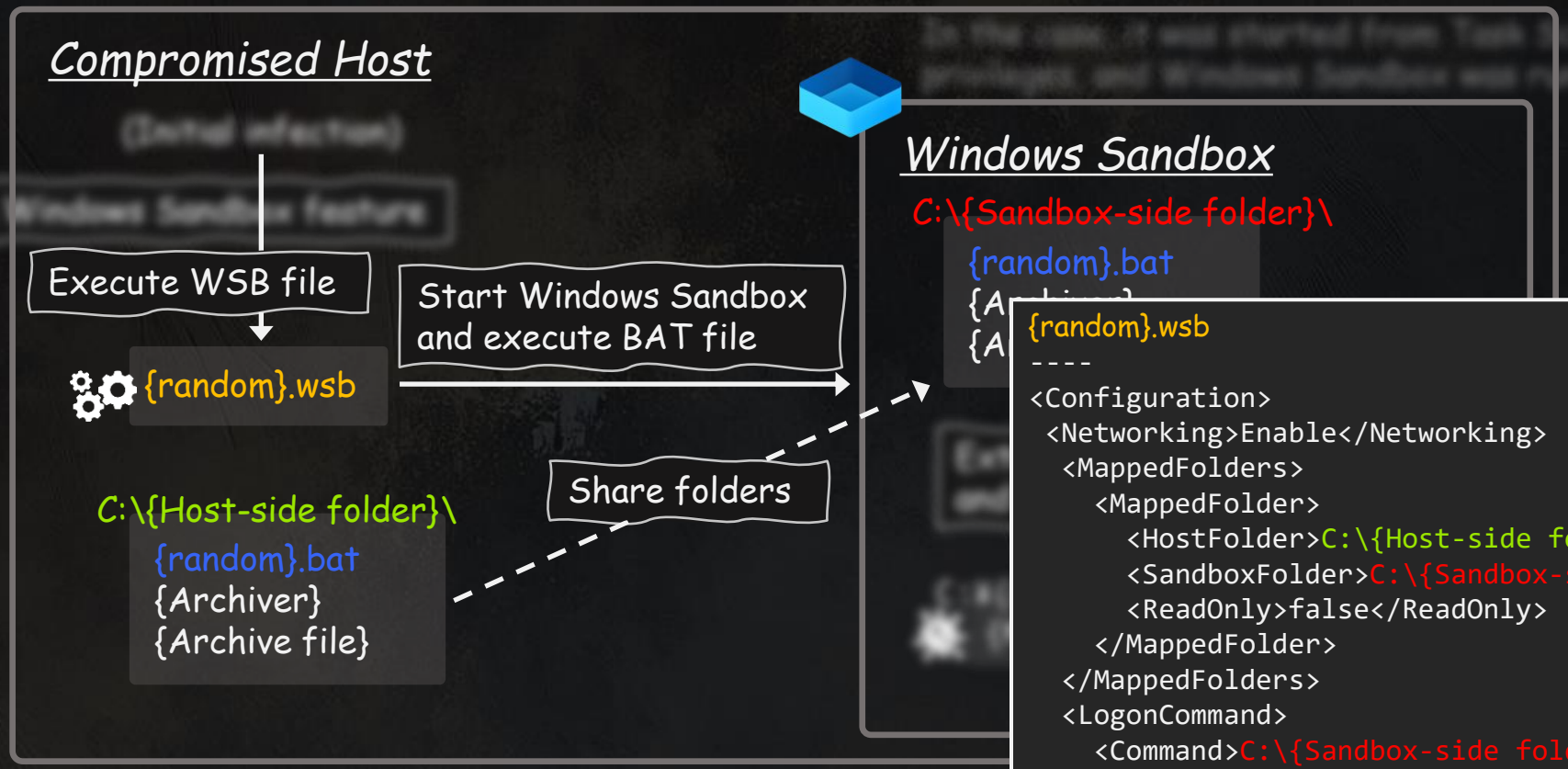
Unveiling the Attack Blueprint

- Stage 1: Persistence for malware execution



Unveiling the Attack Blueprint

- Stage 2: Folder sharing and bat file execution

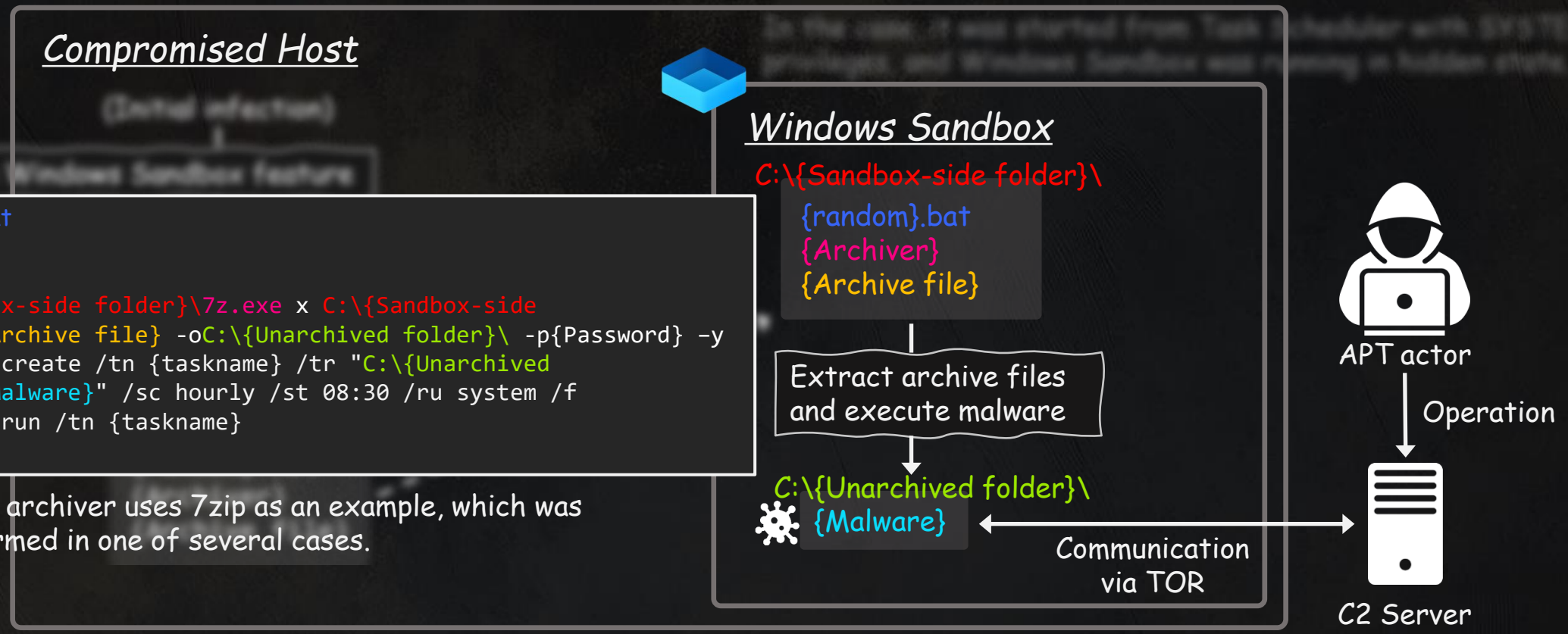


{random}.wsb

```
<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>
```

Unveiling the Attack Blueprint

- Stage 3: Malware execution and C2 communication




```
{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}
----
```

* The archiver uses 7zip as an example, which was confirmed in one of several cases.

SECTION 04

Emerging threats

WINDOWS - HARD

200
Points

★ ★ ★ ★ ★
5.0 80 Reviewers

Windows Sandbox Updates!

- A significant update has been observed
- Although it is only mentioned in the OS build preview for Windows 11 and is not documented in the official documentation.

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 provides a lightweight desktop environment to safely run applications in isolation. Software installed 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.

- **[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

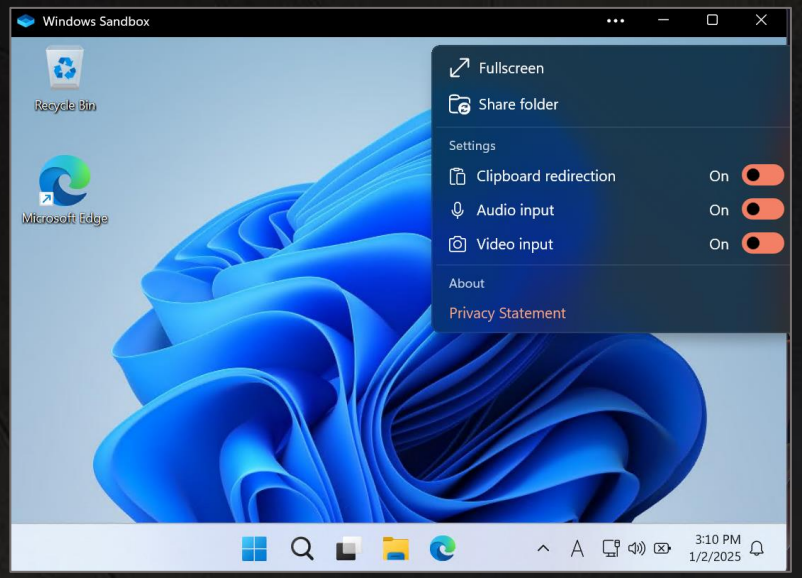
  To access these, select the ellipses (...) at the upper right on the app. This preview also includes a version of command-line support. (The commands might change over time). To learn more, use the **wsb.exe–help** command. You can find new updates for this app in the Microsoft Store. This might not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

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

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

New Features

- Container-like CLI commands have been implemented in Windows Sandbox.
- Windows Sandbox can be run in the background
- Simple configuration changes can be made through the GUI.



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	Description
StartSandbox, start	--id <id> -c, --config <config>	Starts an instance of Windows Sandbox.
ListRunningSandboxes, list	-	Lists the IDs of all running Windows Sandbox environments.
Execute, Exec	--id <id> (REQUIRED) -c, --command <command> (REQUIERED) -d, --working-directory <working-directory> -r, --run-as <ExistingLogin|System>(REQUIRED)	Executes a command in the running Windows Sandbox environments.
ShareFolder, share	--id <id> (REQUIRED) -f, --host-path <host-path>(REQUIRED) -s, --sandbox-path <sandbox-path> -w, --allow-write	Shares a folder from the host to the Windows Sandbox session.
StopSandbox, stop	-	Terminates a running Windows Sandbox.
ConnectToSandbox	--id <id>	Starts a remote session for a Windows Sandbox environment.
GetIpAddress, ip	--id <id> (REQUIRED)	Gets the IP address of the Windows Sandbox environment.

Abusing New Windows Sandbox Features

- Existing attack methods can be updated in the following ways…

E.g. Execute a single line command using config without .wsb file

```
> 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
```

- By abusing this method, the important artifact, ".wsb" file is lost
- Updates unintentionally may boost convenience for the threat actors

Abusing New Windows Sandbox Features

- Updates to background execution and persistence extended with new features may increase convenience for attackers.

Characteristics	Windows 10	Windows 11
Background execution	Not Available	Available by default
Persistence	No *Stop Sandbox by closing window.	Yes *Rebooted sandbox is still active. *Until explicit wsb "stop" command

*In both cases, the sandbox terminates when the process is killed or restarted.

SECTION 05

Countermeasures

WINDOWS - HARD

200
Points

★ ★ ★ ★ ★
5.0 90 Reviewers

Investigation and Monitoring

- Some monitoring and investigation is possible on both the host and Windows Sandbox sides.

Host-Side

- Monitoring client terminal operation logs, characteristic processes and memory
- Monitoring activities related to WSB files
- Monitoring characteristic event logs
- Other artifacts for general forensic investigation

Windows Sandbox

- Operation logs and processes are difficult to monitor and investigate.
- Proper preservation of the host-side parent and differential VHDX allows investigation of certain artifacts in the sandbox.

- Communications from the Windows Sandbox can be monitored as originating from the host.

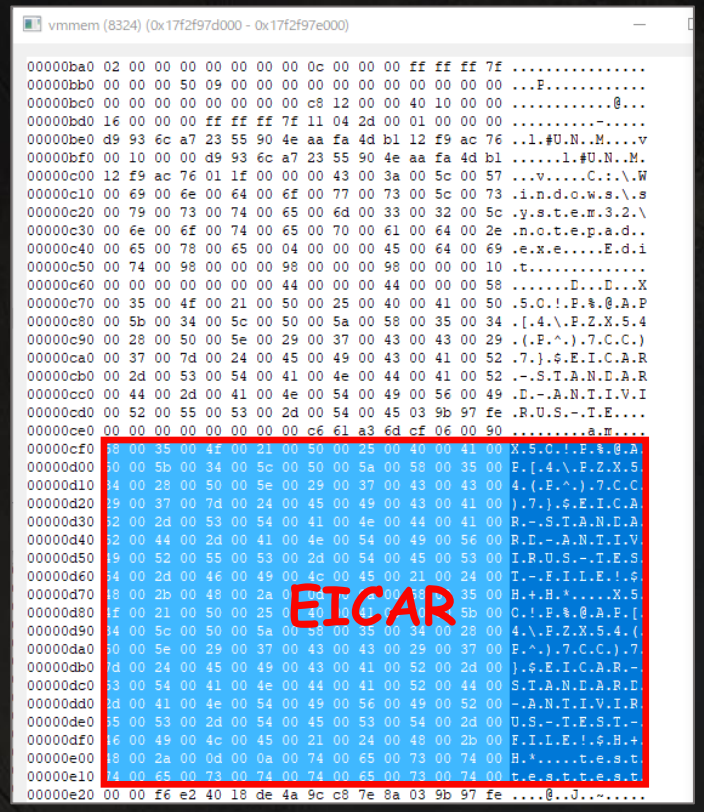
The Host-Side Process

- By preferentially monitoring these process executions on the host side, it is possible to detect Windows Sandbox invocations.
- It should also be noted that various arguments are actually set depending on the execution method.

Process Names	Paths	Descriptions
WindowsSandbox.exe	C:\Windows\System32\WindowsSandbox.exe	When execute WSB file and at normal startup.
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	When execute WSB files, normal execution, and command execution using wsb.exe. (Only for 0.3.1.0 version in Windows 11 build preview)
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	Only when issuing a command using wsb.exe. (For Windows 11 build preview)

The Host-Side Memory of Windows Sandbox

- The process running in Windows Sandbox can be detected in the vmmem process on the host side

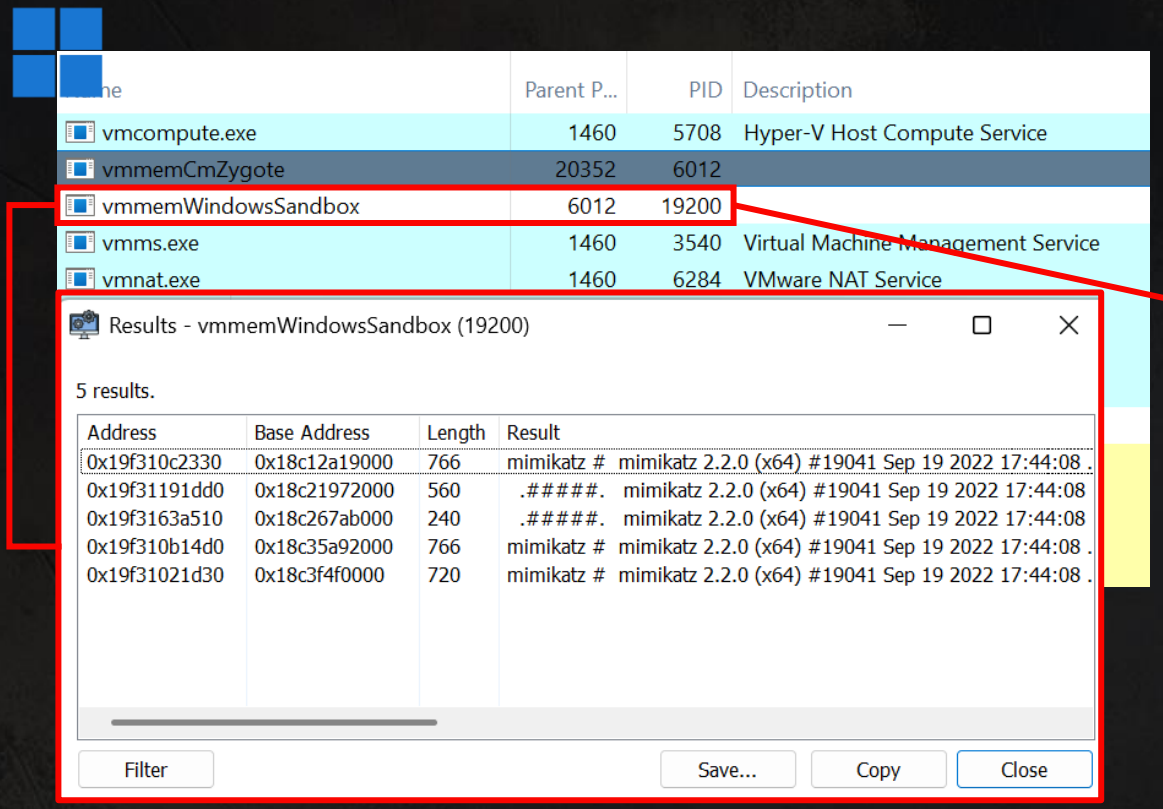


Exposed part of Windows Sandbox memory in host side

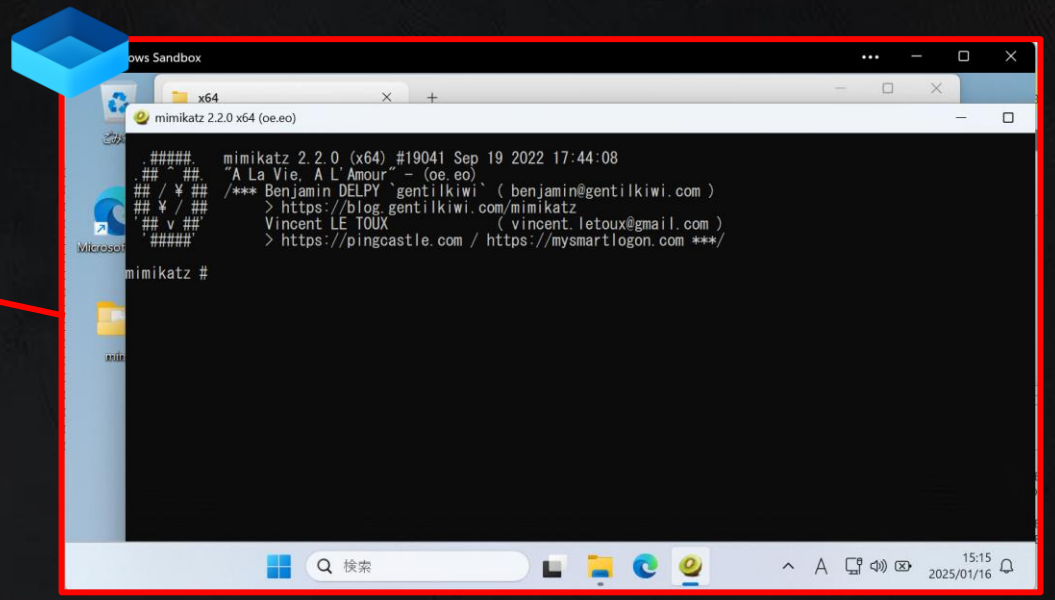
Process Name	OS
vmmem	Windows 10
vmmemWindowsSandbox	Windows 11

The Host-Side Memory of Windows Sandbox

- When Mimikatz is executed within Windows Sandbox, the memory on the host side is also exposed, allowing it to detect with memory scan such as Yara.



Exposed part of Windows Sandbox memory in host side



Execution of Mimikatz in Windows Sandbox

The Host-Side Important Artifacts

- Windows Sandbox operations leave no traces internally, but activation and startup traces may remain on the host.
- We recommend to focus on the following artifacts and investigate them for related signs.

Classification	Description
$MFT	The creation of the WSB file, the creation of the mount source folder and file, and the creation of the VHDX file are recorded.
$UsnJrnl	The creation of the WSB file, the creation of the mount source folder and file, and the creation of the VHDX file are recorded.
Prefetch	Loading of WSB and VDHX files may be recorded.
Registry	The application association is set. • HKLM\SOFTWARE\Classes\Applications\WindowsSandbox.exe • HKLM\SOFTWARE\Classes\Windows.Sandbox\shell\open\command • HKLM\SOFTWARE\Microsoft\Windows Sandbox\Capabilities\FileAssociations
Eventlog	* Described later

The Host-Side Important Artifacts: Event Log 1/2

Classification	Evtx	Source	Event ID	Description
Eventlog	System	Microsoft-Windows-Hyper-V-VmSwitch	102	Virtual machine network driver settings
			232	Virtual machine NIC port related information
			233	Virtual machine NIC related information

	Security	Microsoft-Windows-Security-Auditing	4624	• An account was successfully logged on.
				  • Account Domain : NT VIRTUAL MACHINE
				  • Process Name : C:\Windows\System32\vmcompute.exe

			4648	• A logon was attempted using explicit credentials.
				  • Account Domain : NT VIRTUAL MACHINE
				  • Process Name : C:\Windows\System32\vmcompute.exe

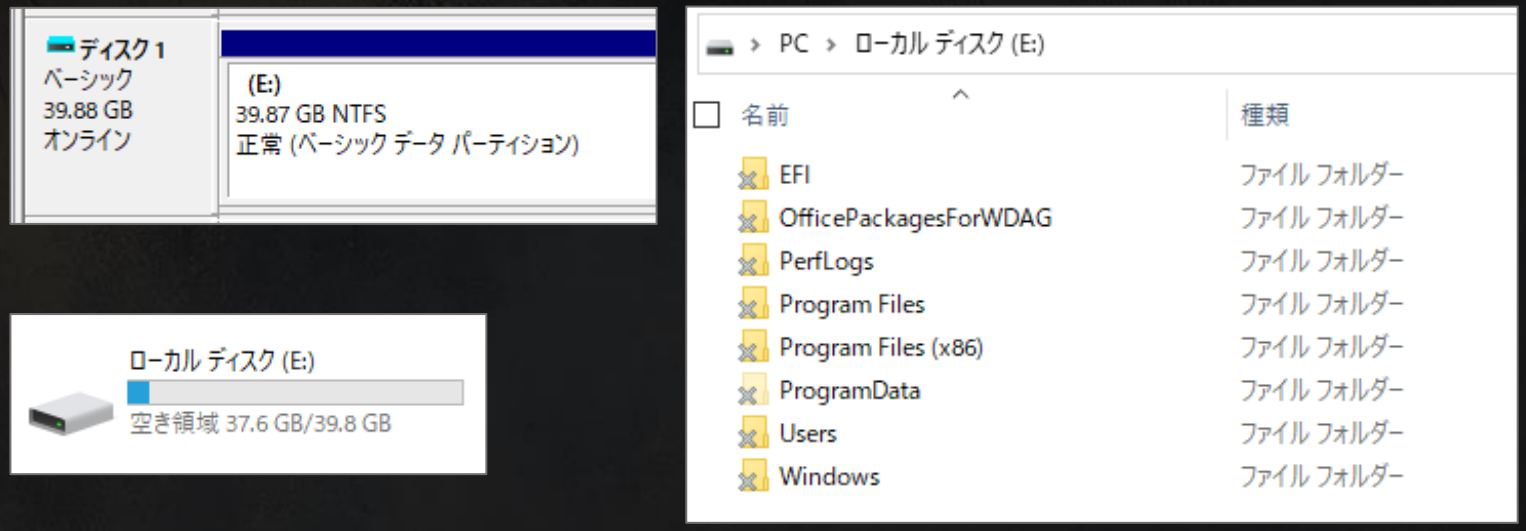
			4672	• Special privileges assigned to new logon. • Account Domain : NT VIRTUAL MACHINE
	Microsoft-Windows-Hyper-V-Worker-Admin	• Microsoft-Windows-Hyper-V-SynthStor • Microsoft-Windows-Hyper-V-Worker	12148	Virtual machine startup information
			12582	
			12597	Virtual network connection information
			18500	Virtual machine startup information
			18502	Information about powering down virtual machines
			18516	Virtual machine suspension information
			18596	Virtual machine restore information
			18601	Virtual machine startup information
			18609	Virtual machine initialization information

The Host-Side Important Artifacts: Event Log 2/2

Classification	Evtx	Source	Event ID	Description
Eventlog	Microsoft-Windows-Hyper-V-Worker-Operational	Microsoft-Windows-Hyper-V-VSmb	301	Information about the folder from which to mount the virtual machine
	Microsoft-Windows-Hyper-V-Compute-Operational	Microsoft-Windows-Hyper-V-Compute	2500	Process creation and command execution related information
	Setup	Microsoft-Windows-Servicing	9	Selectable update Containers-DisposableClientVM of package Microsoft-Windows-Containers-OptionalFeatures was successfully turned on.
			13	A reboot is necessary before the selectable update Containers-DisposableClientVM of package Microsoft-Windows-Containers-OptionalFeatures can be turned on.
	Microsoft-Windows-VHDMP-Operational	Microsoft-Windows-VHDMP-Operational	1	Information about virtual disks (mount/unmount/online/offline, etc.)
			2	
			12	
			17,18	
			22~28	
			31~34	
			50,51	

Windows Sandbox Disk Image Forensics(VHDX)

- A VHDX can be mounted if the chain between its parent and differential disks is intact.
- Therefore, general forensic investigations are possible.
- If the Windows Sandbox process is discovered, the entire folder related to the VHDX must be preserved as volatile data.



VHDX mounted and drive assigned

Windows Sandbox Collectable Artifacts

- This shows the results of verifying artifacts useful in forensics.
- Although some are incomplete or disabled, certain artifacts remain highly useful for forensic investigations.

*** Windows 10 / Windows 11**

Classification	Available	Description
$MFT	Yes	No operations on shared folders from the host were recorded.
$UsnJrnl	Yes	No operations on shared folders from the host were recorded.
Prefetch	No	Not recorded.
Registry	Yes	We were unable to confirm any Amcache updates during our test.
Browser History	Yes	The browsing history of the pre-installed Edge was confirmed. The browsing history was also retained for browsers installed by the user.
SRUM	No	Not recorded.
Evtx	Yes	The default log storage size is 20,480 KB, and some useful events (such as task schedules) are not recorded. We observed logons such as successful logon (Event ID 4624), failed logon (Event ID 4625), logon with explicit credentials (Event ID 4648), and service installation (Event ID 7045).

The Host-Side Control Measures

- Maintain the disabled state of Windows Sandbox
  - It is necessary to detect unintended activation of the sandbox and disable it.

E.g. Apply AppLocker policy

- AppLocker can control the execution of the Windows Sandbox
- If AppLocker blocked the Windows Sandbox, it will be recorded in the event log.

Evtx	Source	Event ID	Description
Microsoft-Windows-AppLocker/EXE and DLL	Microsoft-Windows-AppLocker	8002	Indicates an AppLocker rule allowed the .exe or .dll file.
		8003	Indicates that AppLocker recorded the .exe or .dll file listed on an AppLocker policy. Shown only when **Audit** only enforcement mode is enabled.
		8004	AppLocker blocked the named EXE or DLL file. Shown only when the **Enforce rules** enforcement mode is enabled.

Don't grant administrator privilege to users

SECTION 06

Conclusions

WINDOWS - HARD

200
Points

★ ★ ★ ★ ★
5.0 100 Reviewers

Conclusions

- In 2024, abuse of Windows Sandbox by MirrorFace (APT10 Umbrella) has been observed.
- As EDR and AV on the host may not detect threats, proactive measures like enhanced monitoring, thorough investigations, and effective management are essential to minimize risks.
- Developers must prioritize user experience while recognizing their innovations may unintentionally aid attackers and reduce security barriers.
- Attackers often exceed our expectations, exploiting blind spots and gaps. To counter this, we must anticipate the unexpected and turn them into predictable!


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 - Test environment

- OS version of test environment

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