Lumos! Illuminate the dark hacker attack trail

use Sigma rules to enhance threat hunting capabilities

TeamT5 Will

TEAMT5

Persistent Cyber Threat Hunters

AGENDA

TEAMT5

01 Introduction - Threat Detection with Sigma

02 Creating Sigma Rules

03 Windows APT Attack detection with Sigma

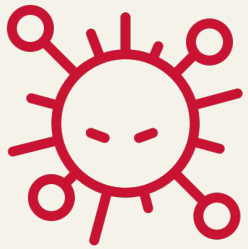
04 Conclusion and Next Steps

TASK

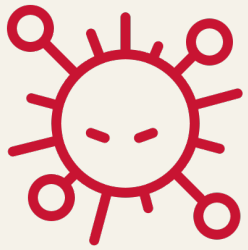
TEAMT5

- We’ll act as Threat Detection Team to defense three incident

Hunting - Mimikatz Credentials Dump



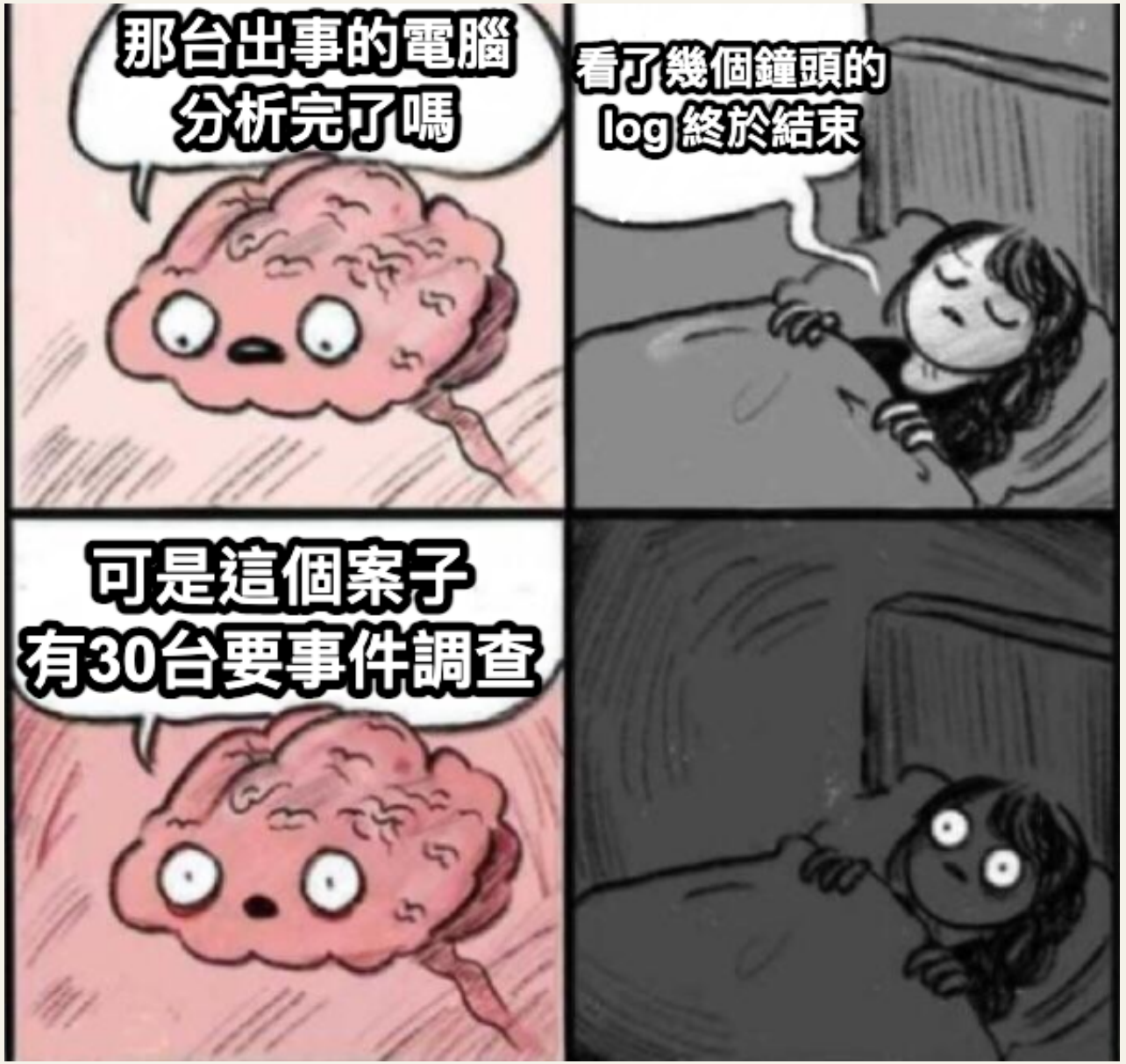
Hunting - PlugX RAT Infection Technique



Hunting - Higaisa APT - Shortcut-Based (Lnk) Attacks

Threat Hunting without Automation

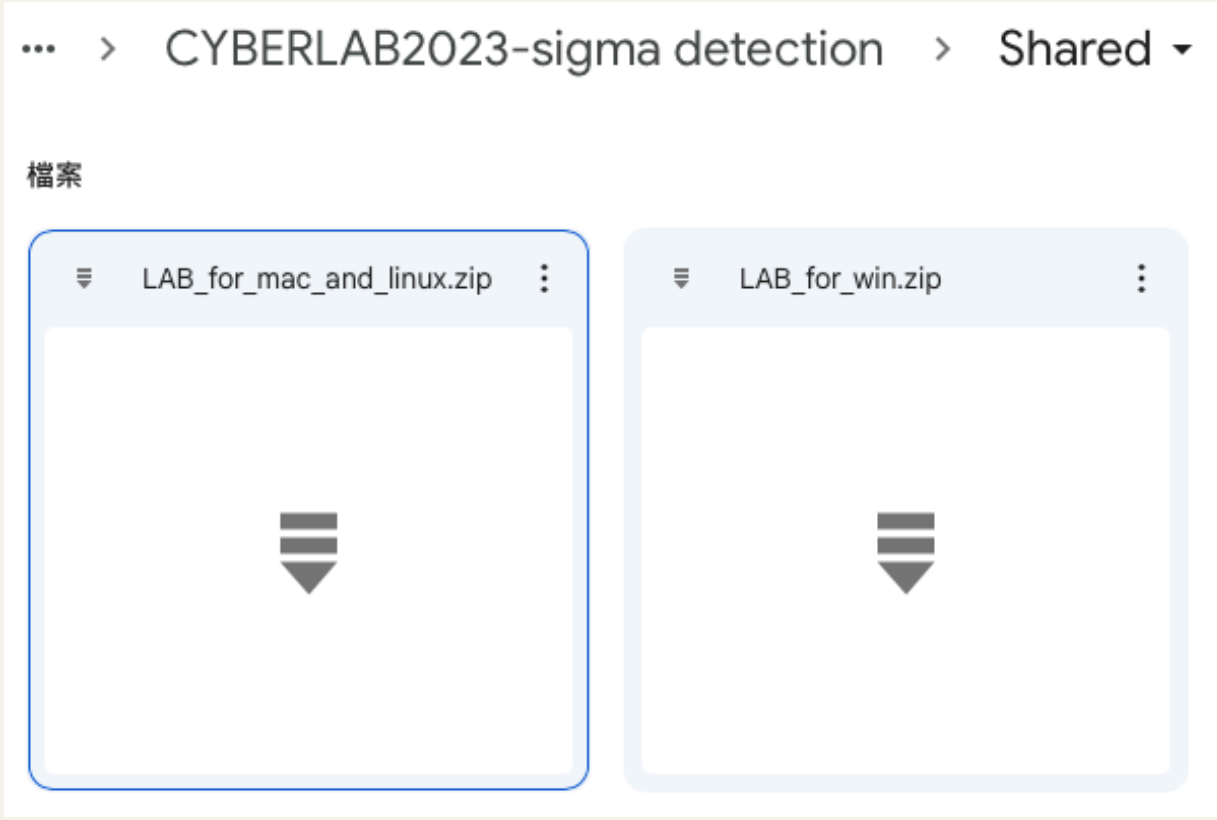
TEAMT5



Env Setup - Download LAB

TEAMT5

- 本課程可以透過任意系統來進行 (Windows/MacOS/Linux)，無需安裝虛擬機
- 從 這邊 下載 Lab 素材
  - 請根據自己的作業系統來選擇



Introduction
Threat Detection with Sigma

Threat Detection

TEAMT5

- IoC (Indicators of Compromise)
  - Record the adversary's information and use that information to detecting.
  - Info: C2 IP, domain, malware, fingerprints, signatures.
- IoA (Indicator of Attack)
  - Concern with the execution of behavior and step.
  - Gather the intent of the adversary.
  - Behavior: Process injection, data encrypted, lateral movement.

Threat Detection

TEAMT5

IoA:
Walk into

IoC:
Tom’s fingerprint

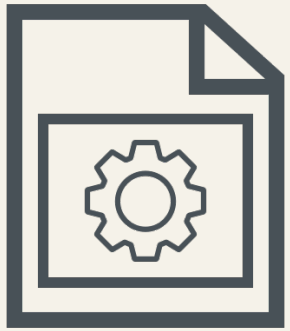
Threat Hunting

TEAMT5

Network Signature

Ex: 10.10.1.1 -> 10.10.1.223

Snort



File Signature

Ex: C File has RSA encryption patten

Yara

Process Signature

Ex: A process create B process

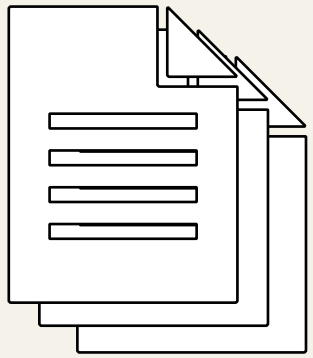
Sigma

Sigma Rule

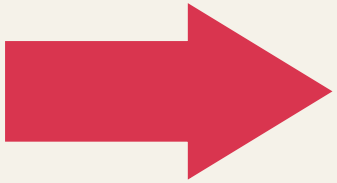
```yaml
title: Test
id: 89f75308-5b1b-4390-b2d8-d6b2340efaf8
status: test
description: Detects behavior for CybersecLab
references:
author: iThome Cybersec
date: 2023/04/14
tags:
    - attack.impact
logsource:
    category: process_creation
    product: windows
detection:
    Selection:
        - Image|endswith: '\run.exe'
        - CommandLine|contains: 'cybersec'
    condition: selection
falsepositives:
    - Unknown
level: high
```

Sigma Rule Cycle

TEAMT5

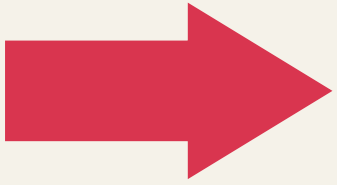


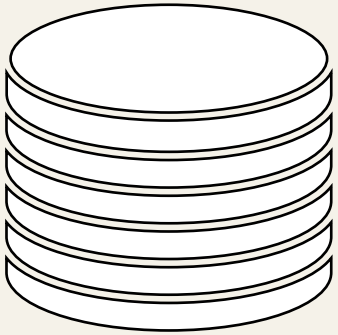
Convert



```
SELECT
 *
FROM
Info
WHERE
Image LIKE '/rm%'
```

Import



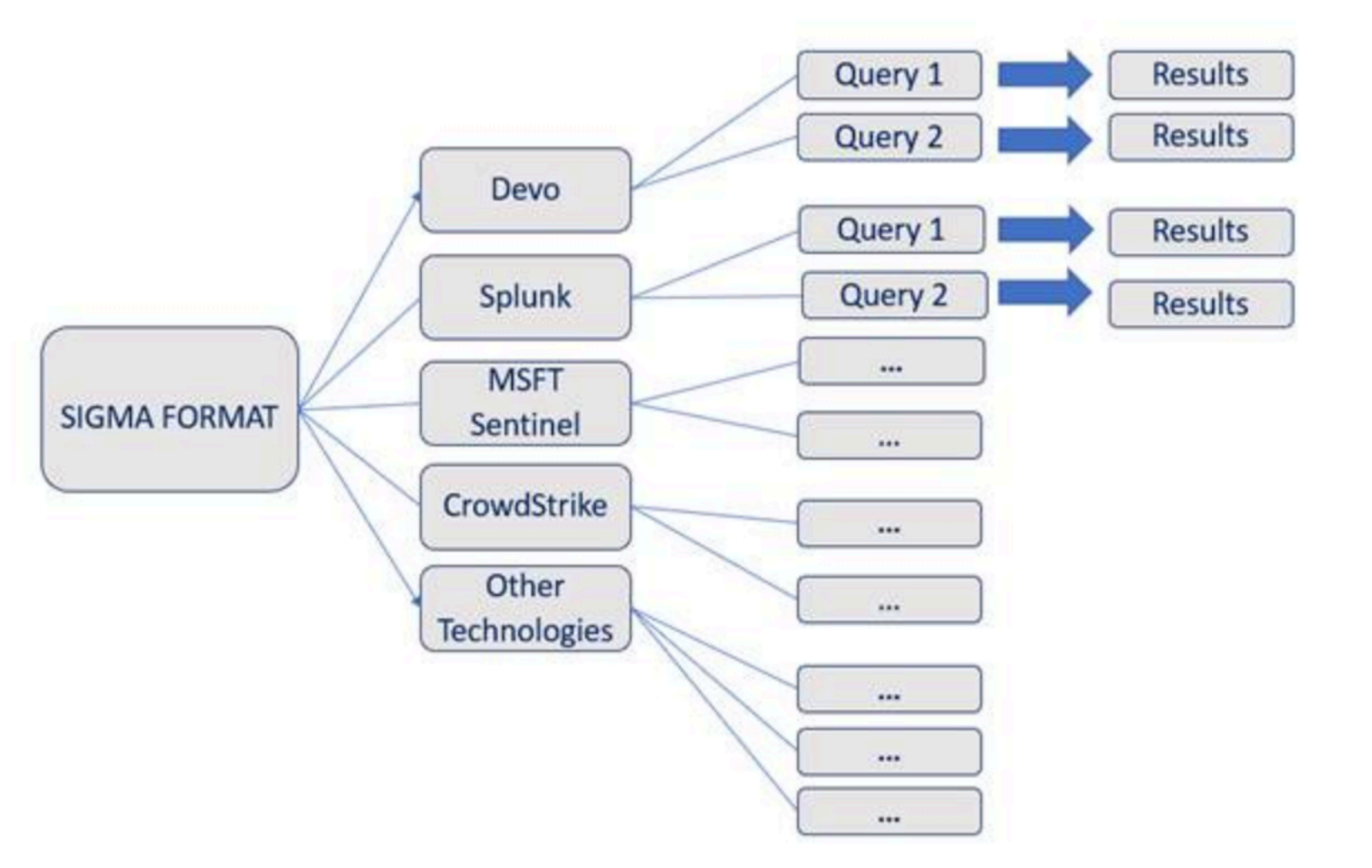


Sigma rules

Queries

EDR, SIEM product

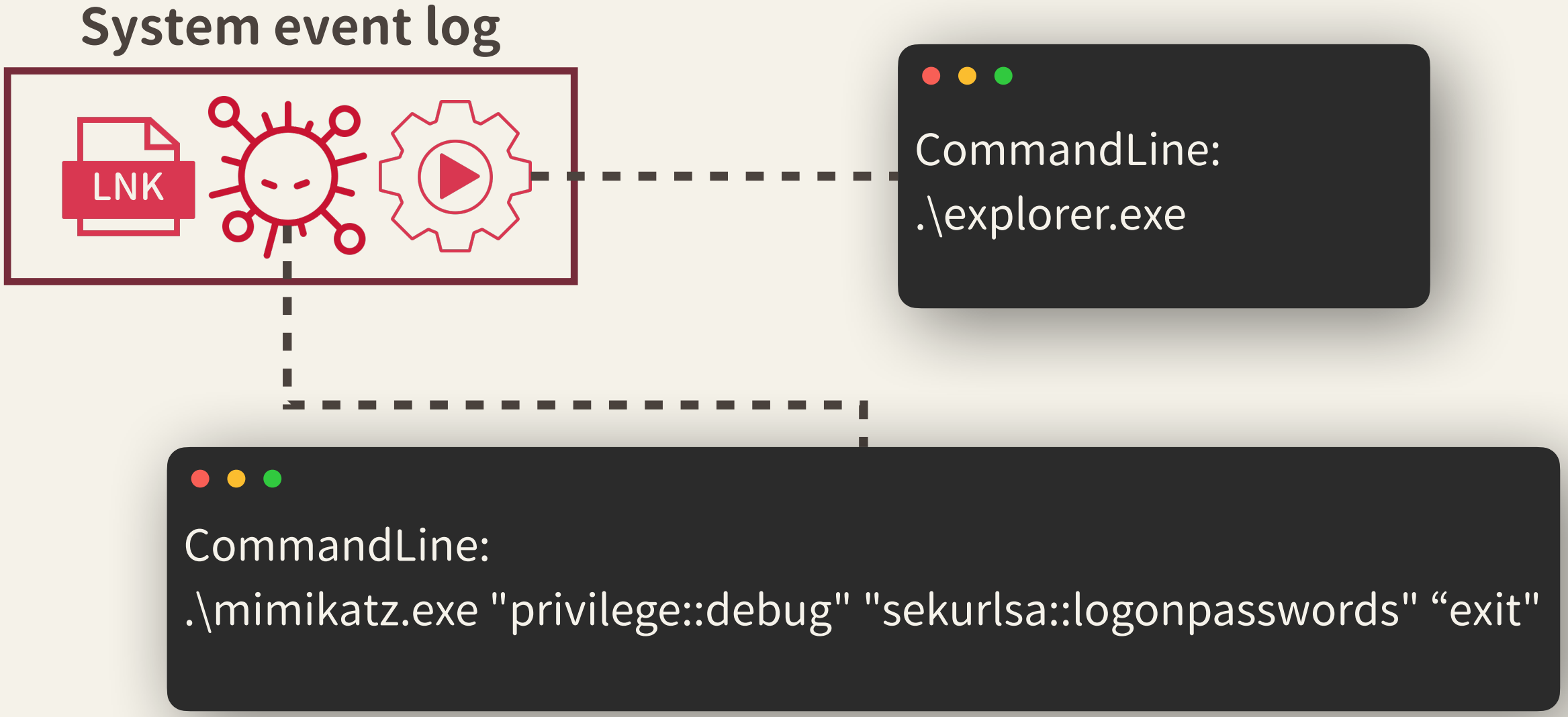
Sigma Rule Convert



https://www.optiv.com/insights/source-zero/blog/sigma-rule-translation-and-automatic-queries

Threat Hunting with Sigma

TEAMT5



Threat Hunting with Sigma

TEAMT5

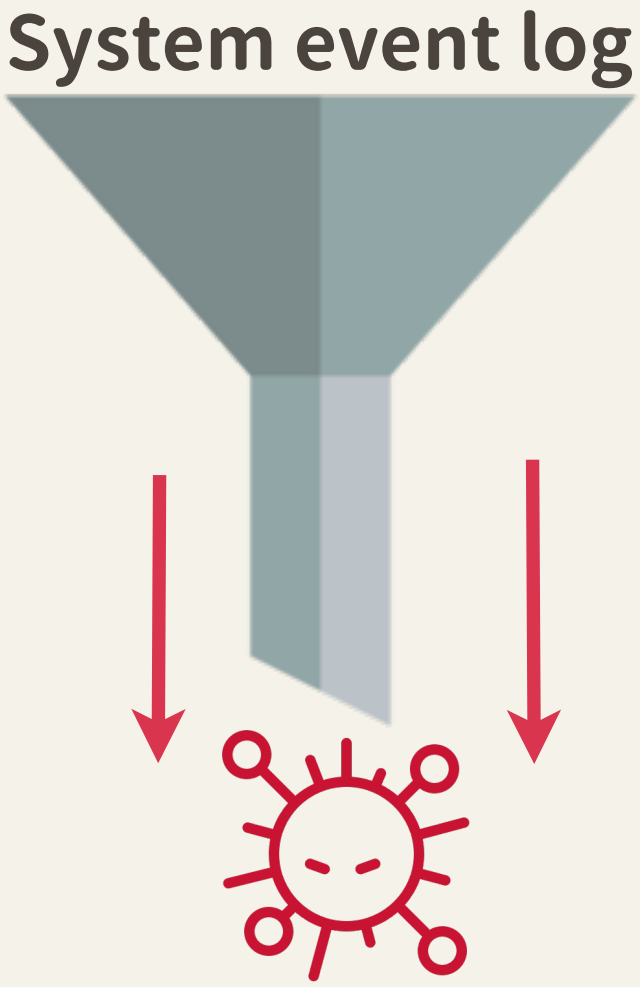
System event log

Sigma Ruleset

```
detection:
    selection:
        CommandLine|contains:
            - 'privilege::debug'
            - 'sekurlsa:logonpasswords'
        FileName: 'Mimikatz.exe'
    condition: selection and filter
```

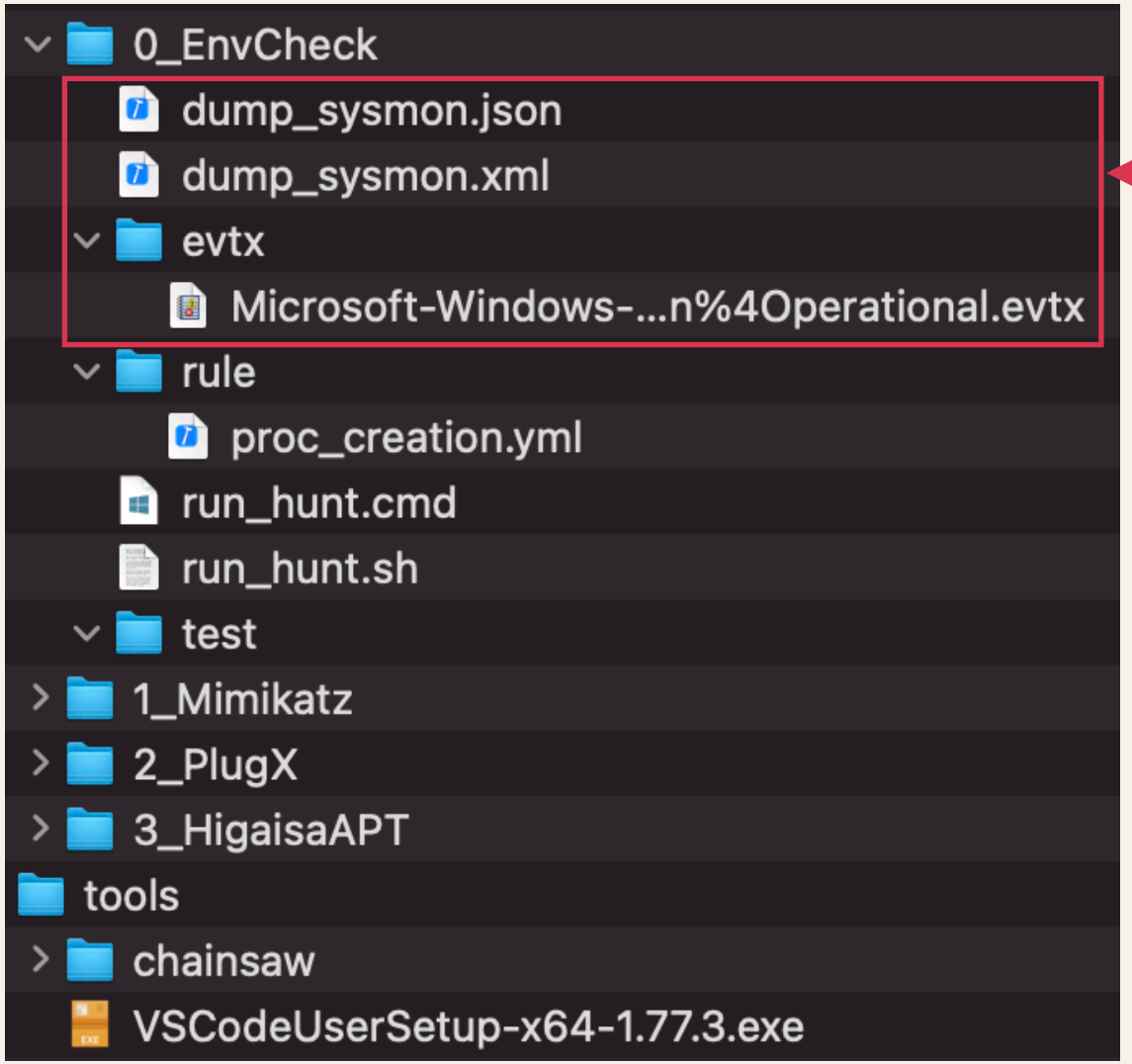
Threat Hunting with Sigma

TEAMT5



Env Setup

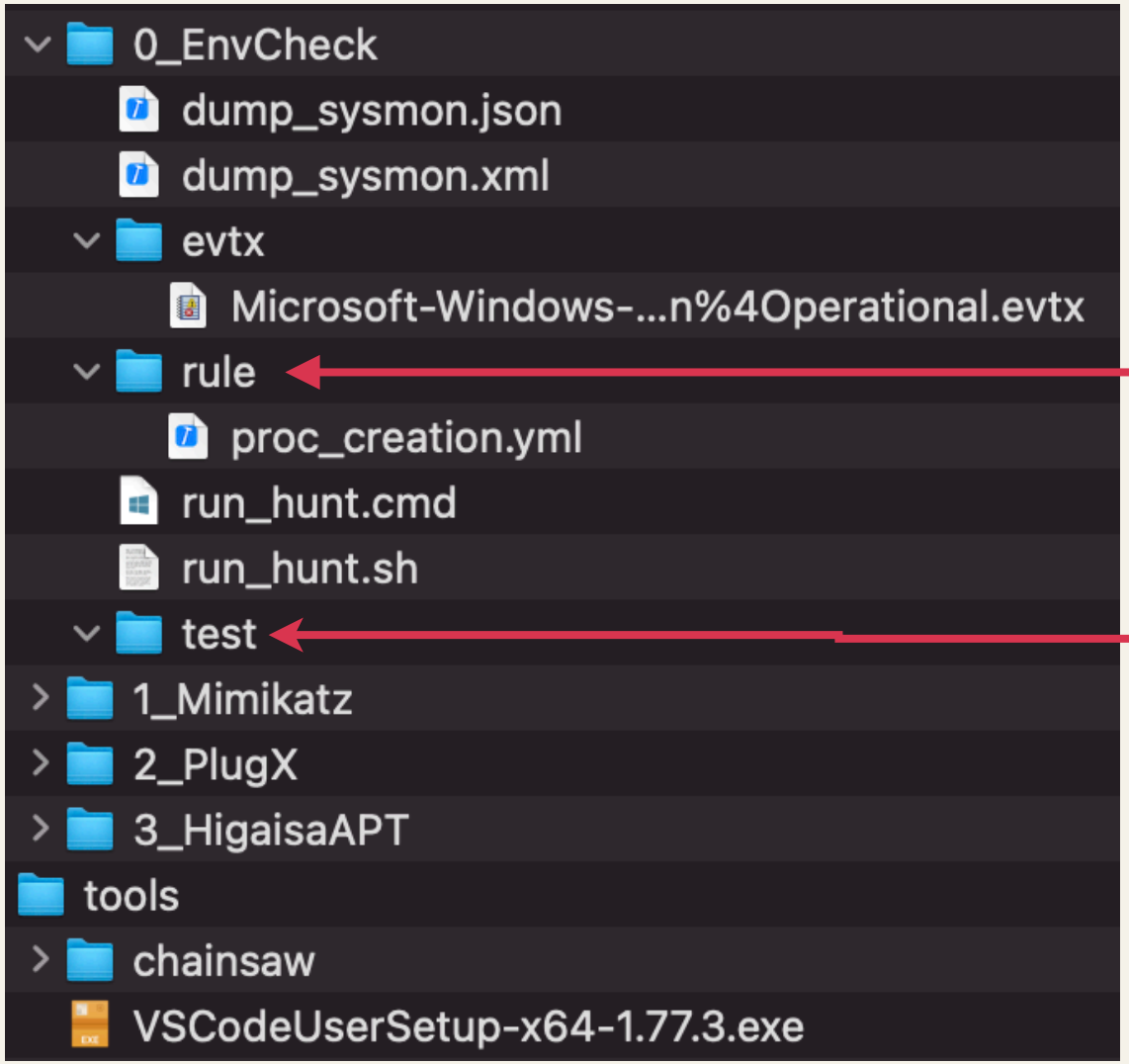
Env Setup - Lab 介紹



系統紀錄檔

TEAMT5

Env Setup - Lab 介紹

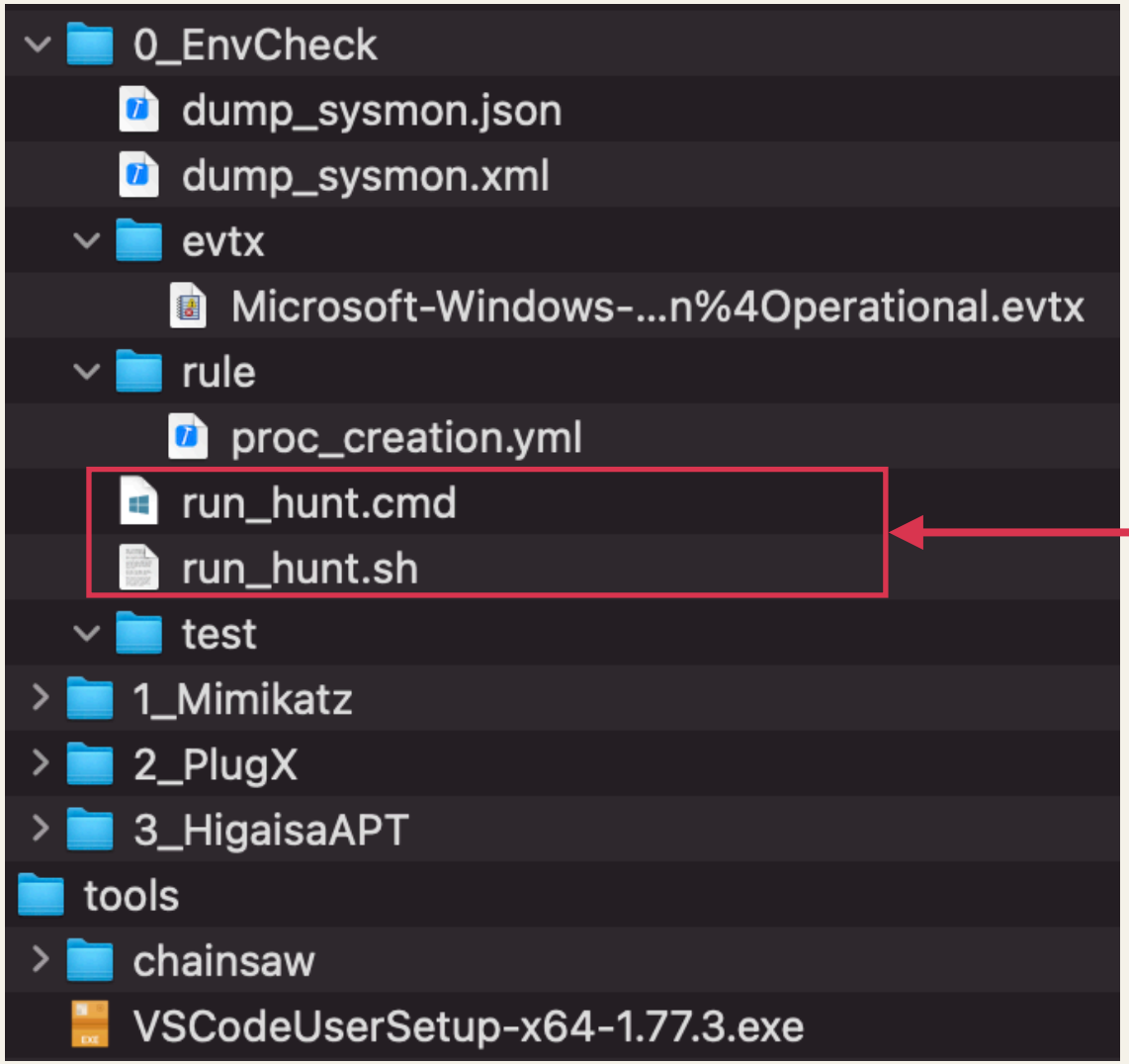


放置正在寫的規則

放置要測試的規則

TEAMT5

Env Setup - Lab 介紹



執行威脅獵捕

TEAMT5

Env Setup - Lab 介紹

- (Crtl+`) 打開 VScode 的終端機
- 根據系統輸入指令

```
> cd .\task\0_EnvCheck\
> ls
> .\run_hunt.cmd
```

Windows

```
> cd ./task/0_EnvCheck/
> ls
> ./run_hunt.sh
```

Mac/linux

TEAMT5

Env Setup - Hunting

- 由於現在還沒新增規則，因此工具會顯示沒有可以偵測的規則

```
PS C:\Users\user\Desktop\Lab> cd .\task\0_EnvCheck\
PS C:\Users\user\Desktop\Lab\task\0_EnvCheck> .\run_hunt.cmd

C:\Users\user\Desktop\Lab\task\0_EnvCheck>..\..\tools\chainsaw\chainsaw.exe hunt .\evtx\ -s .\test\ --mapping .
event-logs-all.yml
```

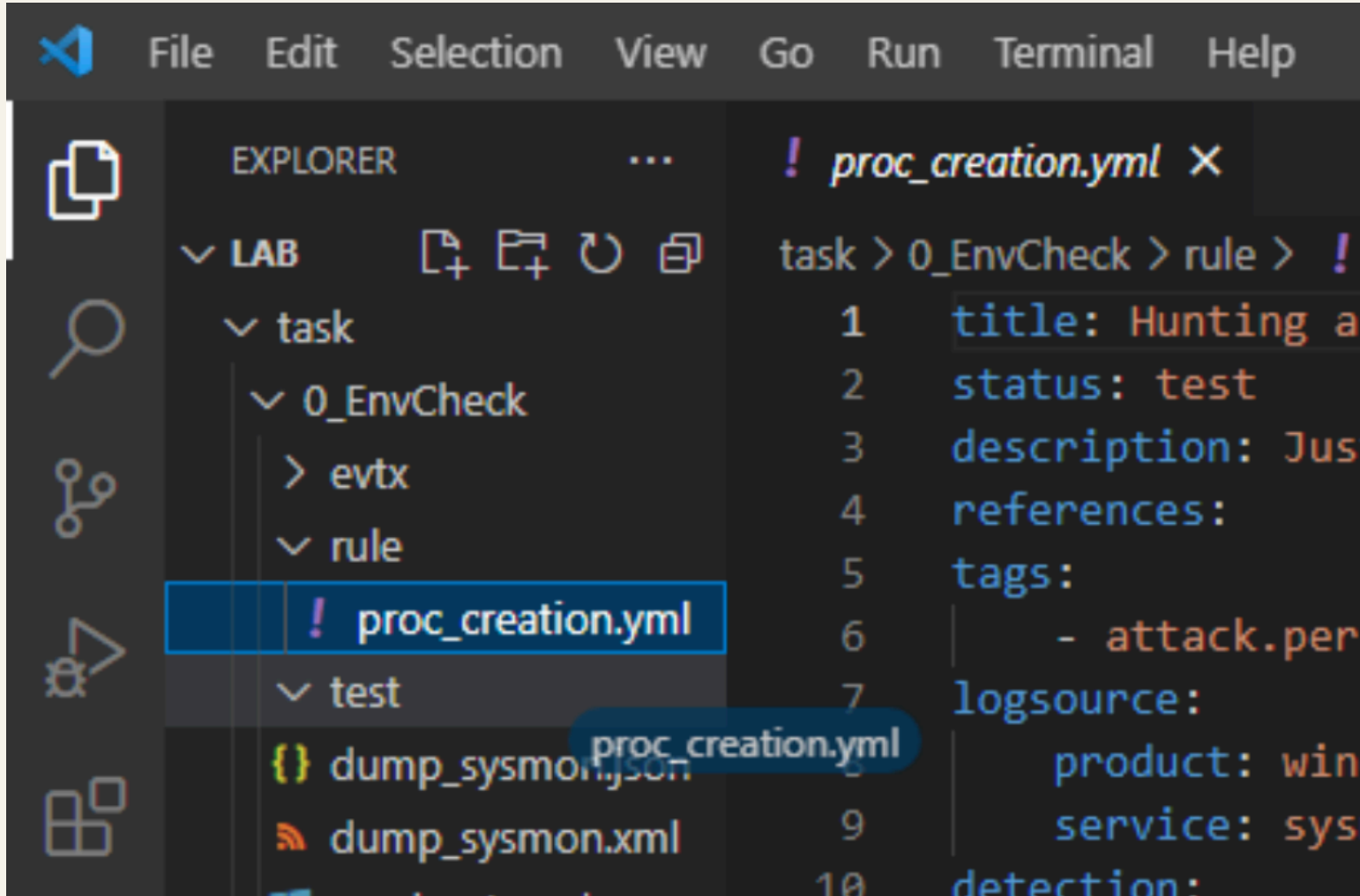

```
    By Countercept (@FranticTyping, @AlexKornitzer)

[+] Loading detection rules from: .\test\
[x] No valid detection rules were found in the provided paths
```

TEAMT5

Env Setup - Hunting

- 將 rule 底下的檔案移動至 test 底下



Env Setup - Hunting

- 再執行一次，檢查是否有事件被我們獵捕到

```
PS C:\Users\user\Desktop\Lab\task\0_EnvCheck> .\run_hunt.cmd

C:\Users\user\Desktop\Lab\task\0_EnvCheck>..\..\tools\chainsaw\chainsaw.exe hunt .\evtx\ -s .\test\ --mapping ..\..\tools\chainsaw\mappings\sigma-event-logs-all.yml
```


```
    By Countercept (@FranticTyping, @AlexKornitzer)

[+] Loading detection rules from: .\test\
[+] Loaded 1 detection rules
[+] Loading forensic artefacts from: .\evtx\ (extensions: .evt, .evtx)
[+] Loaded 1 forensic artefacts (69.6 KB)
[+] Hunting: [========================================] 1/1 -
[+] Group: Sigma
```

timestamp	detections	count	Event.System.Provider	Event ID	Record ID	Computer	Event Data
2023-05-03 07:54:03	+ Hunting all process creation	1	Microsoft-Windows-Sysmon	1	18356	WIN10-PRO-22H2-64	CommandLine: '"C:\Program Files\Notepad++ otepad++.exe" ' Company: Don HO don.h@free.fr CurrentDirectory: C:\Program Files\Notepad++\ Description: Notepad++ FileVersion: '8.49' Hashes: MD5=5BE76B396AF91837C038EF58CC3AB0C8,SHA256=DE844BAE026E847B6BF54582E3CA331AE3D47ABF6BD7729B174C921DEAED70AE,IMP HASH=F458F0F3EAD86F56BBB64D1C7

Creating Sigma Rules

https://sigmahq.github.io/sigma-specification/Sigma_specification.html

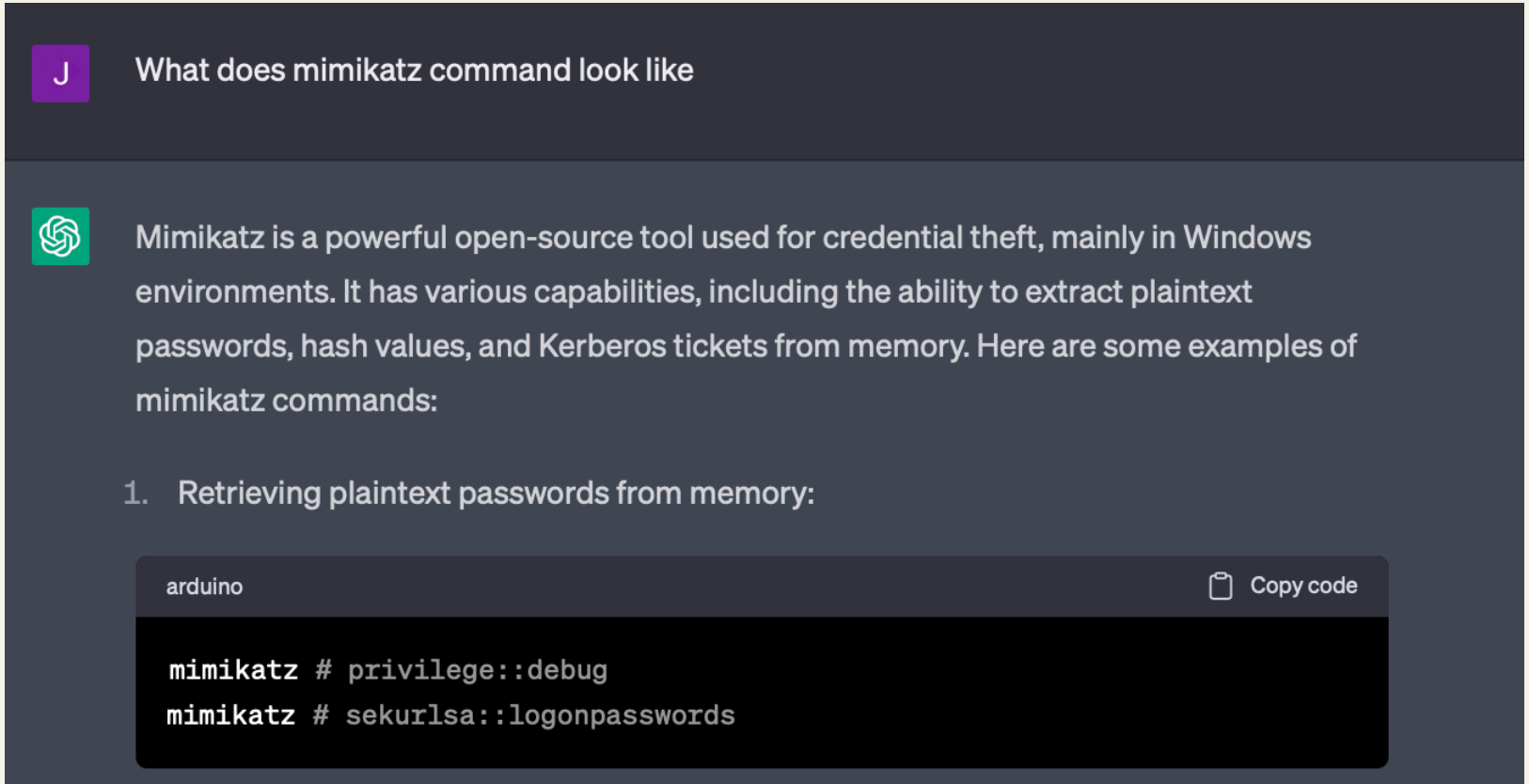
TEAMT5

Sigma Writing Steps

TEAMT5

1. information gathering

The first step to building a Sigma rule is deciding what activity you need to find



Sigma Writing Steps

TEAMT5

1. information gathering

The first step to building a Sigma rule is deciding what activity you need to find

2. Rule Creation

Compose Sigma rules based on events recorded in the system log

Find the Anomalous Behavior !!!

Sigma Writing Steps

TEAMT5

1. information gathering

The first step to building a Sigma rule is deciding what activity you need to find

2. Rule Creation

Compose Sigma rules based on events recorded in the system log

3. Detection testing and improvement

Perform testing of the rule for false positives in both standard and anomalous system environments

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_hktl_mimikatz_command_line.yml

Sigma

Rule Identification

- Rule should be identified

```yaml
title: Test
id: 89f75308-5b1b-4390-b2d8-d6b2340efaf8
status: test
description: Detects behavior for CybersecLab
references:
author: iThome Cybersec
date: 2023/04/14
tags:
    - attack.impact
logsource:
    category: process_creation
    product: windows
detection:
    Selection:
        - Image|endswith: '\run.exe'
        - CommandLine|contains: 'cybersec'
    condition: selection
falsepositives:
    - Unknown
level: high
```

Sigma

Rule Detail

- Status: Declares the status of the rule
- Description: A short description of the rule
- References: Ref to the source that the rule was derived from
- Date: Creation date of the rule

```yaml
title: Test
id: 89f75308-5b1b-4390-b2d8-d6b2340efaf8
status: test
description: Detects behavior for CybersecLab
references:
author: iThome Cybersec
date: 2023/04/14
tags:
    - attack.impact
logsource:
    category: process_creation
    product: windows
detection:
    Selection:
        - Image|endswith: '\run.exe'
        - CommandLine|contains: 'cybersec'
    condition: selection
falsepositives:
    - Unknown
level: high
```

Sigma

Detection Logic

- Log Source: describes the log data on which the detection is meant to be applied to.
  - category:
    - Ex: firewall, antivirus
  - product
    - Ex: win, apache
  - service
    - Ex: sushi, applocker

```yaml
title: Test
id: 89f75308-5b1b-4390-b2d8-d6b2340efaf8
status: test
description: Detects behavior for CybersecLab
references:
author: iThome Cybersec
date: 2023/04/14
tags:
    - attack.impact
logsource:
    category: process_creation
    product: windows
detection:
    Selection:
        - Image|endswith: '\run.exe'
        - CommandLine|contains: 'cybersec'
    condition: selection
falsepositives:
    - Unknown
level: high
```

Sigma

Detection Logic

- Detection: A set of search-identifiers that represent properties of searches on log data.
- List and maps

```yaml
title: Test
id: 89f75308-5b1b-4390-b2d8-d6b2340efaf8
status: test
description: Detects behavior for CybersecLab
references:
author: iThome Cybersec
date: 2023/04/14
tags:
    - attack.impact
logsource:
    category: process_creation
    product: windows
detection:
    Selection:
        - Image|endswith: '\run.exe'
        - CommandLine|contains: 'cybersec'
    condition: Selection
falsepositives:
    - Unknown
level: high
```

Detection Logic - List

TEAMT5

- Starting with a hyphen
- All items of a list are logically linked with ‘OR’

String

```
Selection:
   - '\run.exe'
   - 'cybersec'
```

Log contains ‘\run.exe’ OR ‘cybersec’

key-value pair

```
Selection:
   - Image: '\run.exe'
   - CommandLine: 'cybersec'
```

Image is ‘\run.exe’ OR CommandLine is ‘cybersec’

Detection Logic - Maps

TEAMT5

- Starting without a hyphen
- All elements of a map are joined with a logical ‘AND’

```
Selection:
   '\run.exe'
   'cybersec'
```

Log contains ‘\run.exe’ AND ‘cybersec’

```
Selection:
   Image: '\run.exe'
   CommandLine: 'cybersec'
```

Image is ‘\run.exe’ AND CommandLine is ‘cybersec’

Detection Logic - Modifiers

TEAMT5

- contains -> The sentence contains a certain keyword
- endswith -> Expect at the end of the field’s content
- startwith -> Expect at the beginning of the field’s content

```
Selection:
   Image|contains: '\run.exe'
   CommandLine|contains: 'cybersec'
```

Detection Logic - condition

TEAMT5

```
selection_a:
    - Image: '\run.exe'
    - CommandLine: ‘cybersec'
selection_b:
    - Image: '\good.exe'
    - CommandLine: ‘malware'
condition: 1 of selection*
```

Detection Logic - Examples

TEAMT5

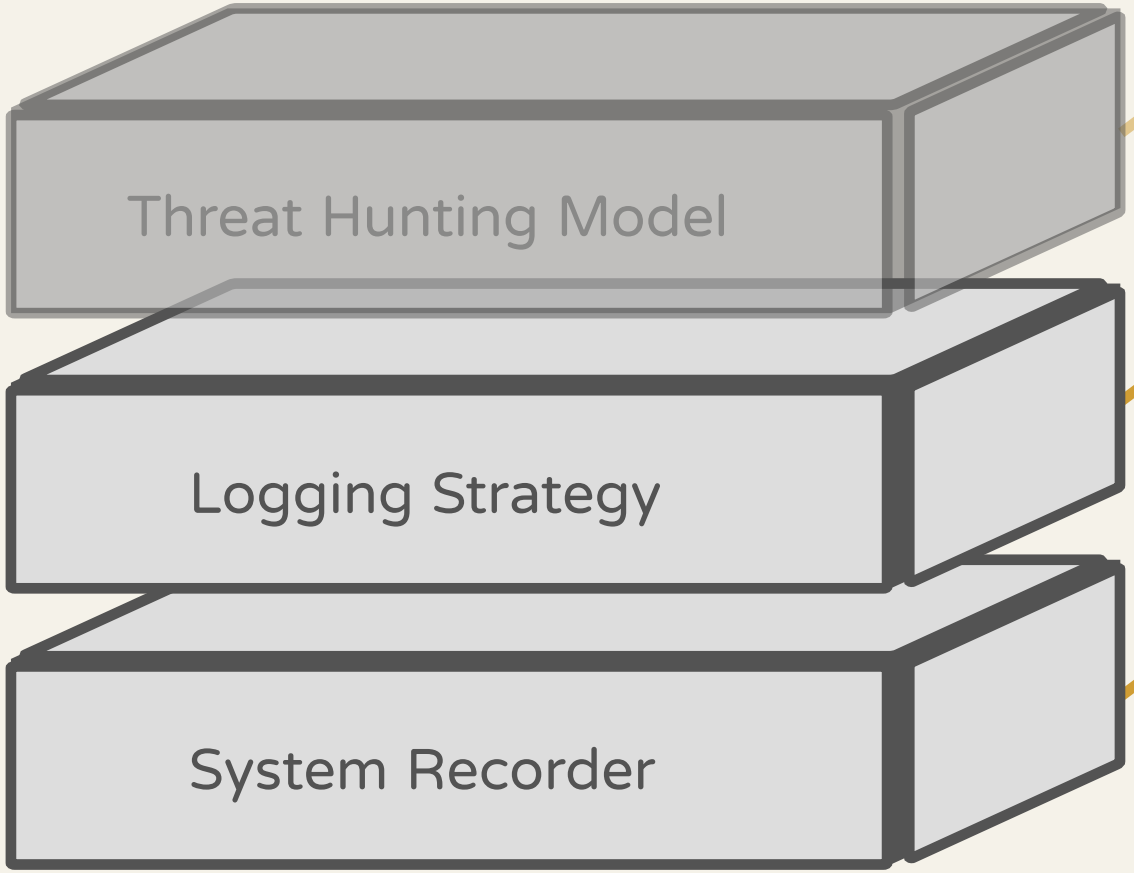
- What does this code aim to convey?

```
detection:
    selection_cscript:
        Image|endswith: '\cscript.exe'
        CommandLine|contains: '.vbs /shell '
    selection_csvde:
        CommandLine|contains:
            - 'csvde -f C:\windows\web\'
            - 'cscript.exe'
    condition: 1 of selection_*
```

Task Introduction

Threat Hunting with Sigma

TEAMT5



Sigma Rules

Hunting by chainsaw tool

Sysmon config

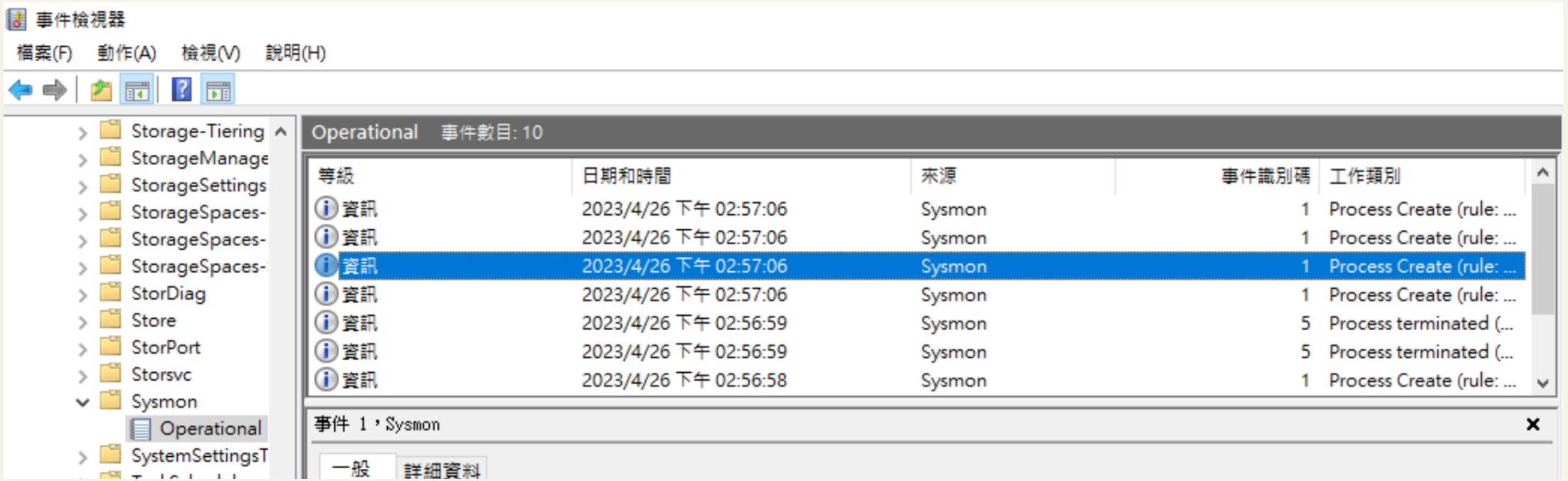
https://github.com/
SwiftOnSecurity/sysmon-config

Sysmon

Logs, Processes, Registry,
Filesystem

Sysmon

- Sysmon is a system monitoring tool developed by Microsoft that can record various events on Windows systems
- Uses Windows Event Tracing (ETW) to log events, ensuring that events are captured in a standardized format that can be easily parsed and analyzed



Sysmon Event ID

TEAMT5

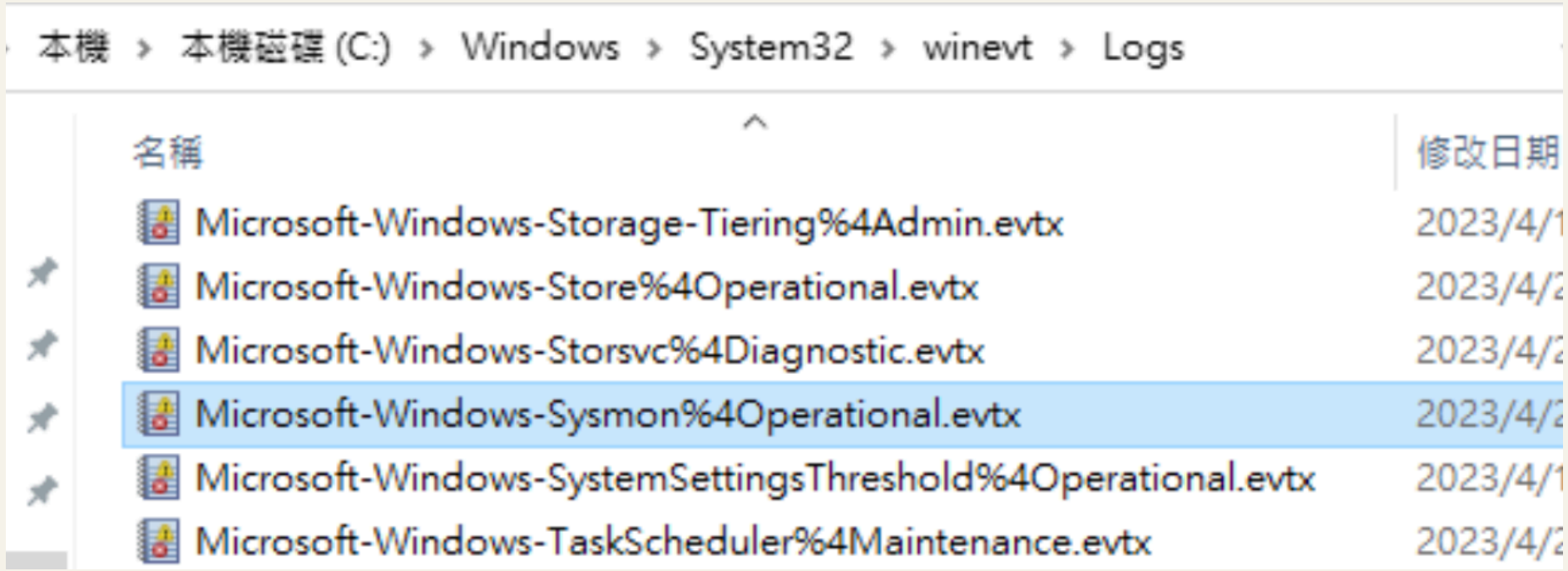
Event ID	Description
1	Process creation
2	A process changed a file creation time
3	Network connection
5	Process terminated
6	Driver loaded
7	Image loaded
8	CreateRemoteThread detected
9	RawAccessRead detected

Event ID	Description
10	Process Access
11	FileCreate
12	RegistryEvent (Object create and delete)
13	RegistryEvent (Value Set)
14	RegistryEvent (Key and Value Rename)
15	FileCreateStreamHash
16	Sysmon configuration change

Sysmon Log File

TEAMT5

- Path
  - C:\Windpws\System32\winevt\Logs



Threat Hunting with Sigma

TEAMT5

Sigma Rules

Hunting by chainsaw tool

Sysmon config

https://github.com/SwiftOnSecurity/sysmon-config

Sysmon

Logs, Processes, Filesystem, Packets, Devices

Chainsaw

TEAMT5

- Rapidly Search and Hunt through Windows Forensic Artefacts(.evtx)
- https://github.com/WithSecureLabs/chainsaw

By Countercept (@FranticTyping, @AlexKornitzer)

```
[+] Loading detection rules from: ./test/
[+] Loaded 1 detection rules
[+] Loading forensic artefacts from: ./evtx/ (extensions: .evt, .evtx)
[+] Loaded 1 forensic artefacts (1.1 MB)
[+] Hunting: [========================================] 1/1
[+] Group: Sigma
```

timestamp	detections	count	Event.System.Provider	Event ID	Record ID	Computer	Event Data
2023-04-29 04:39:33	‣ Potential HigaisaAPT behavior - system config read	1	Microsoft-Windows-Sysmon	1	14987	WIN10-PRO-22H2-64	CommandLine: '"C:\Windows\System32\cmd.exe" /c ipconfig>C:\Users\Public\Downloads\d3reEW.txt & copy C:\Users\user\AppData\Local\Temp\sychastd.exe "C:\

Task1: Mimikatz Dump Credentials

事件分析

TEAMT5

主旨	駭侵事件處理
事件描述	客戶 IT 人員發現 AD 有被遠端登入成功的紀錄，疑似密碼遭到盜走，並從記錄檔有發現 Mimikatz 的執行指令
處理方式	轉請 Threat Detection Team 透過提供的 syslog 設計 Sigma 規則，防止其他客戶遭受同樣攻擊
備註	提供 sysmon 的紀錄檔 (.evtx)

Mimikatz Credentials Dump

TEAMT5

- Dump plaintext password
- Dump NTLM hash

```
PS C:\Users\user\Desktop\x64> .\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 6491833 (00000000:00630eb9)
Session           : Interactive from 2
User Name         : user
Domain            : WIN10-PRO-22H2-
Logon Server      : WIN10-PRO-22H2-
Logon Time        : 2023/4/26 下午 03:19:21
SID               : S-1-5-21-1924812608-2403969082-1162371674-1001
```

(1) Study Sysmon Event Log

TEAMT5

- Process Creation: Dump plaintext password from lsass Process Memory


```
Record 1995
{
    "EventData": {
      "CommandLine": "\"C:\\Users\\user\\Desktop\\x64\\mimikatz.exe\"
privilege::debug sekurlsa::logonpasswords exit",
      "Image": "C:\\Users\\user\\Desktop\\x64\\mimikatz.exe",
      "OriginalFileName": "mimikatz.exe",
      "ParentCommandLine": "\"C:\\Windows\\System32\
\WindowsPowerShell\\v1.0\\powershell.exe\" ",
      "ParentImage": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\
\powershell.exe",
    },
    "System": {
      "EventID": 1,
```

(1) Study Sysmon Event Log

TEAMT5

- Process Creation: Dump plaintext password from lsass Process Memory

Commandline:
.\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" “exit"

(1) Study Sysmon Event Log

TEAMT5

- Save hklm\security hklm\sam registry

```
Record 2380
{
    "EventData": {
      "CommandLine": "\"C:\\Windows\\system32\\reg.exe\" save hklm\
\sam SamBkup.hiv",
      "Company": "Microsoft Corporation",
      "CurrentDirectory": "C:\\Users\\user\\Desktop\\x64\\",
      "Image": "C:\\Windows\\System32\\reg.exe",
      "OriginalFileName": "reg.exe",
      "User": "WIN10-PRO-22H2-\\user",
      "UtcTime": "2023-04-27 03:32:47.015"
    },
    "System": {
      "EventID": 1,
```

(1) Study Sysmon Event Log

TEAMT5

- Save hklm\security hklm\sam registry
  - \SAM contains local user account and local group membership information, including their passwords.
  - \SECURITY stores the Lsass policy database

```
reg save hklm\sam SamBkup.hiv

reg save hklm\security SystemBkup.hiv

 .\mimikatz.exe "privilege::debug" “token::elevate" "log hash.txt"
“lsadump::sam SamBkup.hiv SystemBkup.hiv" "exit"
```

(3) Writing Rule

TEAMT5

- Note:
  - Focus on interesting behavior
    - Process creation with abnormal string
    - Registry Save
    - …
  - Are there any unique characteristics specific behavior?

Hunting: Process Create

TEAMT5

```
detection:
    filter:
        - EventID: 1
    selection:
        CommandLine|contains:
            - 'privilege::debug'
            - 'privilege::driver'
            - 'sekurlsa::'
            - ……
    condition: selection and filter
```

3 events hit

Hunting: Reg Save

TEAMT5

```
detection:
    filter:
        - EventID: 1
    selection:
        CommandLine|contains:
            - 'save hklm\sam'
            - 'save hklm\security'
        OriginalFileName|contains: 'reg.exe'
    condition: selection and filter
```

5 events hit

Hunting: Process Access

TEAMT5

```
detection:
    filter:
        - EventID: 10
    selection:
        TargetImage|contains: 'lsass.exe'
        GrantedAccess:
            - '0x1410'
            - '0x1010'
    condition: selection and filter
```

2 events hit

https://www.splunk.com/en_us/blog/security/you-bet-your-lsass-hunting-lsass-access.html
https://learn.microsoft.com/en-us/windows/win32/procthread/process-security-and-access-rights?redirectedfrom=MSDN

APT Attack detection with Sigma

Task2: Hunting PlugX RAT

事件分析

TEAMT5

主旨	駭侵事件處理
事件描述	MDR 團隊從定期掃描報告中發現有 PlugX 的 YARA 規則，以確定客戶受到 PlugX 的惡意程式感染
處理方式	轉請 Threat Detection Team 透過提供的 syslog 設計 Sigma 規則，防止其他客戶遭受同樣攻擊
備註	提供 sysmon 的紀錄檔 (.evtx)

https://www.trendmicro.com/en_us/research/23/b/investigating-the-plugx-trojan-disguised-as-a-legitimate-windows.html

PlugX

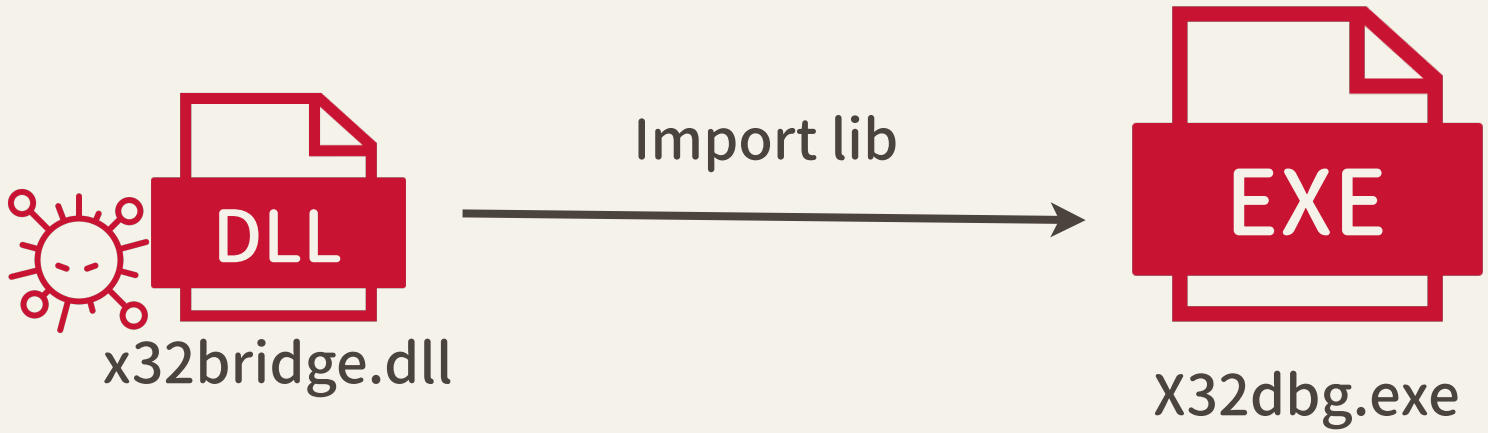
- First seen: 2008
- A RAT with modular plugins
- Used by many Chinese APT groups
  - APT41, APT27, DragonOK
- Various PlugX variants

https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

(1) Study Sysmon Event Log

TEAMT5

- Process Creation: DLL Sideload
  - DLL Search Order Hijacking T1574.001
  - DLL Sideload is a technique that involves loading and executing an external Dynamic Link Library (DLL) in a Windows application



(1) Study Sysmon Event Log

TEAMT5

- File Creation: move malware to three paths

```
Record 15317
{
    "EventData": {
      "CreationUtcTime": "2023-04-29 05:37:11.531",
      "Image": "C:\\Users\\user\\Desktop\\release\\x32\\x32dbg.exe",
      "ProcessGuid": "CAB8CBF0-AD07-644C-CD02-000000000F00",
      "ProcessId": 5256,
      "TargetFilename": "C:\\ProgramData\\UsersDate\\Windows_NT\
\Windows\\User\\Desktop\\x32dbg.exe",
    },
    "System": {
      "EventID": 11,
```

(1) Study Sysmon Event Log

TEAMT5

- File Creation: move malware to three paths
  - C:\ProgramData\UsersDate\Windows_NT\Windows\User\Desktop
  - C:\Users\Public\Public Mediae\
  - C:\Users\<username>\Users\

(1) Study Sysmon Event Log

TEAMT5

- Persistence: Scheduled Task

```
Record 15325
{
    "EventData": {
      "CommandLine": "schtasks  /create /sc minute /mo 5  /tn
LKUFORYOU_1  /tr C:\\ProgramData\\UsersDate\\Windows_NT\\Windows\\User\
\Desktop\\x32dbg.exe    /f",
      "Image": "C:\\Windows\\SysWOW64\\schtasks.exe",
      "OriginalFileName": "schtasks.exe",
      "ParentCommandLine": "C:\\ProgramData\\UsersDate\\Windows_NT\
\Windows\\User\\Desktop//x32dbg.exe",
     "UtcTime": "2023-04-29 05:37:11.653”
   }
    "System": {
    "EventID": 1,
```

(1) Study Sysmon Event Log

TEAMT5

- Persistence: Scheduled Task
  - T1053 Scheduled Task/Job
  - "schtasks" is a command-line tool used to config scheduled tasks
  - Scheduled Task allows the malware to continue running even after the system has been rebooted, making it more difficult to remove

```
`schtasks  /create /sc minute /mo 5  /tn  LKUFORYOU_1  /tr C:\\ProgramData\\UsersDate\\Windows_NT\
\Windows\\User\\Desktop\\x32dbg.exe    /f`
```

(1) Study Sysmon Event Log

TEAMT5

- Persistence: Registry Set


```
Record 15326
{
    "EventData": {
      "Details": "C:\\ProgramData\\UsersDate\\Windows_NT\\Windows\
\User\\Desktop\\x32dbg.exe",
      "EventType": "SetValue",
      "Image": "C:\\ProgramData\\UsersDate\\Windows_NT\\Windows\
\User\\Desktop\\x32dbg.exe",
      "TargetObject": "HKU\
\S-1-5-21-1924812608-2403969082-1162371674-1001\\SOFTWARE\\Microsoft\
\Windows\\CurrentVersion\\Run\\x32dbg",
   },
    "System": {
     "EventID": 13,
```

(1) Study Sysmon Event Log

TEAMT5

- Persistence: Registry Set
  - Windows Run keys
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  - `RUN` key allows the malware to continue running even after the system has been rebooted.

(1) Study Sysmon Event Log

TEAMT5

- System Binary Proxy Execution: Rundll32

```
Record 15324
{
    "EventData": {
      "CommandLine": "rundll32 SHELL32.DLL, ShellExec_RunDLL rundll32
C:\\ProgramData\\UsersDate\\Windows_NT\\Windows\\User\\Desktop\
\akm.dat,Start",
      "Image": "C:\\Windows\\SysWOW64\\rundll32.exe",
      "OriginalFileName": "RUNDLL32.EXE",
      "ParentCommandLine": "C:\\ProgramData\\UsersDate\\Windows_NT\
\Windows\\User\\Desktop//x32dbg.exe",
     "UtcTime": "2023-04-29 05:37:11.645"
    },
    “System": {
      "EventID": 1,
```

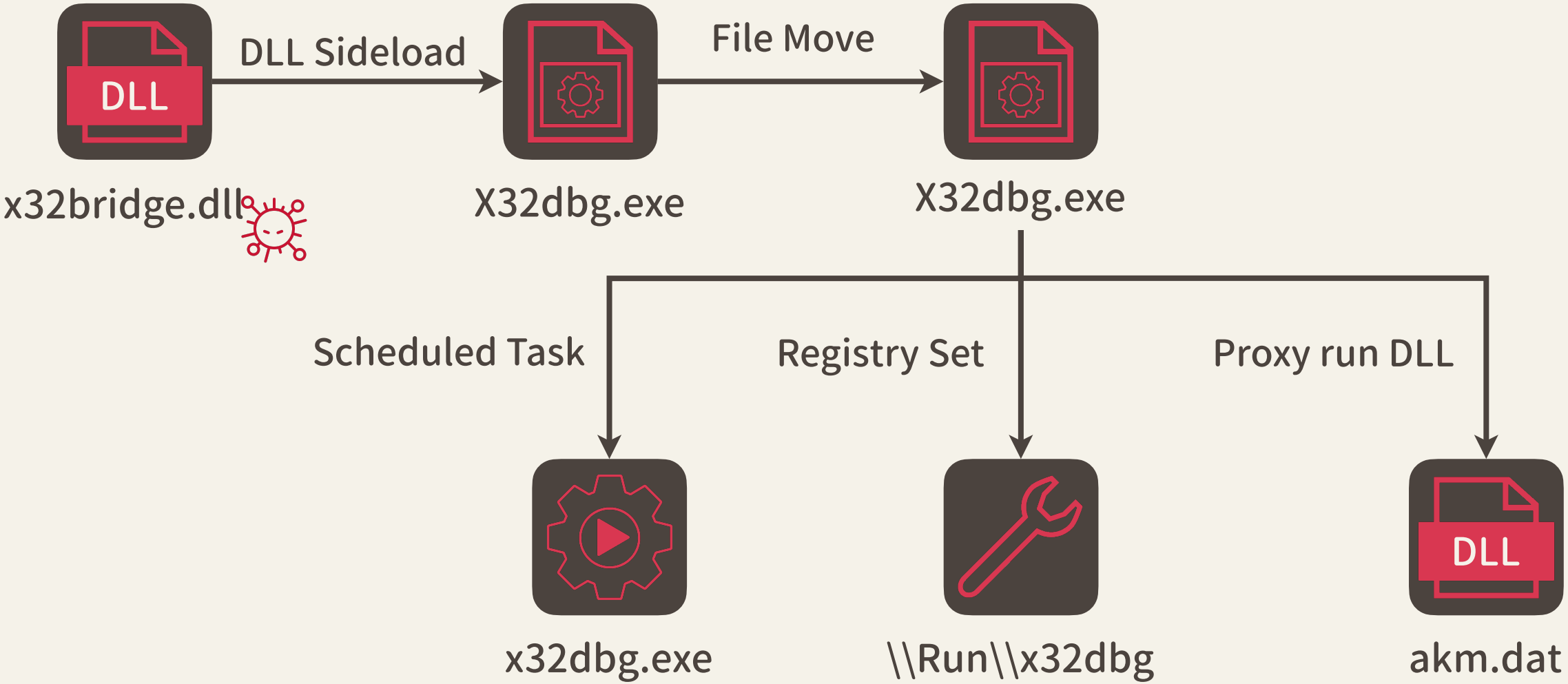
(1) Study Sysmon Event Log

- System Binary Proxy Execution: Rundll32
  - Attackers often use Rundll32 to execute malicious code by creating a DLL with a specific exported function
  - With rundll32, the attacker can execute their malicious code using a trusted system binary, making it more difficult to detect and block

"rundll32 SHELL32.DLL, ShellExec_RunDLL rundll32 C:\\ProgramData\\UsersDate\\Windows_NT\\Windows\
\User\\Desktop\\akm.dat,Start",

(2) Attack Summary

TEAMT5



(3) Writing Rule

TEAMT5

- Note:
  - The file x32dbg.exe is a legitimate executable of a debugging software
  - Focus on interesting behavior
    - Scheduled Task
    - Registry Set
    - Rundll32
    - …
  - Are there any unique characteristics specific behavior?

(4) Writing Rule: Scheduled Task

```
eventid:
    EventID: 1
selection_sch_name:
    - Image|endswith: 'schtasks.exe'
selection_sch_command:
    - Commandline|contains:
        - /create
        - /sc
        - /mo
selection_plugx_signature:
    - CommandLine|contains:
        - 'LKUFORYOU_1'
        - 'x32dbg.exe'
        - ‘C:\\ProgramData\\UsersDate\\Windows_NT\\Windows'
condition: 1 of selection_sch* and selection_plugx_signature and eventid
```

Hunting: Scheduled Task

2023-04-29 05:38:40	+ Potential PlugX Persistence - Scheduled Task	1	Microsoft-Windows-Sysmon	1	15411	WIN10-PRO-22H2-64	CommandLine: schtasks /create /sc minute /mo 5 /tn LKUFORYOU_1 /tr C:\ProgramData\UsersDate\Windows_NT\Windows\User\Desktop\x32dbg.exe /f Company: Microsoft Corporation CurrentDirectory: C:\Users\user\Desktop\release\x32\ Description: Task Scheduler Configuration Tool FileVersion: 10.0.19041.1503 (WinBuild.160101.0800) Hashes: MD5=48C2FE20575769DE916F48EF0676A965,SHA256=ABCD98A854E034F464DB23A8954208B52A6FD15E6F94B8593004E7932E8F3CFC,IMPHASH=918DBB01101BFA7F1042CCA9520D2A05 Image: C:\Windows\SysWOW64\schtasks.exe IntegrityLevel: Medium

23 events hit

(4) Writing Rule: Registry Set

```
eventid:
    EventID: 13
    EventType: 'SetValue'
selection_reg:
    - TargetObject|contains:
          '\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\'
    - TargetObject|endswith: 'x32dbg'
selection_file:
    - Image|startswith:
          'C:\\ProgramData\\UsersDate\\Windows_NT\\Windows'
    - Image|contains: 'x32dbg'
condition: 1 of selection* and eventid
```

Hunting: Registry Set

```
[+] Loaded 1 forensic artefacts (1.1 MB)
```

timestamp	detections	count	Event.System.Provider	Event ID	Record ID	Computer	Event Data
2023-04-29 05:37:11	+ Potential PlugX Persistence - Registry Key Set	1	Microsoft-Windows-Sysmon	13	15326	WIN10-PRO-22H2-64	Details: C:\ProgramData\UsersDate\Windows_NT\Windows\User\Desktop\x32dbg.exe EventType: SetValue Image: C:\ProgramData\UsersDate\Windows_NT\Windows\User\Desktop\x32dbg.exe ProcessGuid: CAB8CBF0-AD07-644C-CE02-000000000F00 ProcessId: 4528 RuleName: T1060,RunKey TargetObject: HKU\S-1-5-21-1924812608-2403969082-1162371674-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\x32dbg User: WIN10-PRO-22H2-\user UtcTime: 2023-04-29 05:37:11.656

```
[+] 1 Detections found on 1 documents
```

1 events hit

(4) Writing Rule: rundll32


```yaml
eventid:
    EventID: 1
selection_rundll32_name:
    - Image|endswith: 'rundll32.exe'
selection_rundll32_command:
    - Commandline|contains|all:
        - 'ShellExec_RunDLL'
        - 'SHELL32.DLL'
selection_plugx_signature:
    - CommandLine|contains:
        - 'Start'
    - ParentImage|contains:
        - 'x32dbg.exe'
        - 'C:\\ProgramData\\UsersDate\\Windows_NT\\Windows'
condition: 1 of selection_rundll32* and selection_plugx_signature
```

Hunting: rundll32

timestamp	detections	count	Event.System.Provider	Event ID	Record ID	Computer	Event Data
2023-04-29 05:37:11	+ Potential PlugX Execution - rundll32	1	Microsoft-Windows-Sysmon	1	15324	WIN10-PRO-22H2-64	CommandLine: rundll32 SHELL32.DLL, ShellExec_RunDLL rundll32 C:\ProgramData\UsersDate\Windows_NT\Windows\User\Desktop\akm.dat,Start Company: Microsoft Corporation CurrentDirectory: C:\Users\user\Desktop\release\x32\ Description: Windows host process (Rundll32) FileVersion: 10.0.19041.746 (WinBuild.160101.0800) Hashes: MD5=889B99C52A60DD49227C5E485A016679,SHA256=6CBE0E1F046B13B29BFA26F8B368281D2DDA7EB9B718651D5856F22CC3E02910,IMP

2 events hit

Task3: Hunting Higaisa APT - Shortcut-Based (Lnk) Attacks

TEAMT5

事件分析

TEAMT5

主旨	駭侵事件處理
事件描述	MDR 團隊發現系統有可疑lnk指令產生並且連線到惡意 C2 Server 的跡象
處理方式	轉請 Threat Detection Team 透過提供的 syslog 設計 Sigma 規則，防止其他客戶遭受同樣攻擊
備註	提供 sysmon 的紀錄檔 (.evtx)

https://www.malwarebytes.com/blog/news/2020/06/higaisa

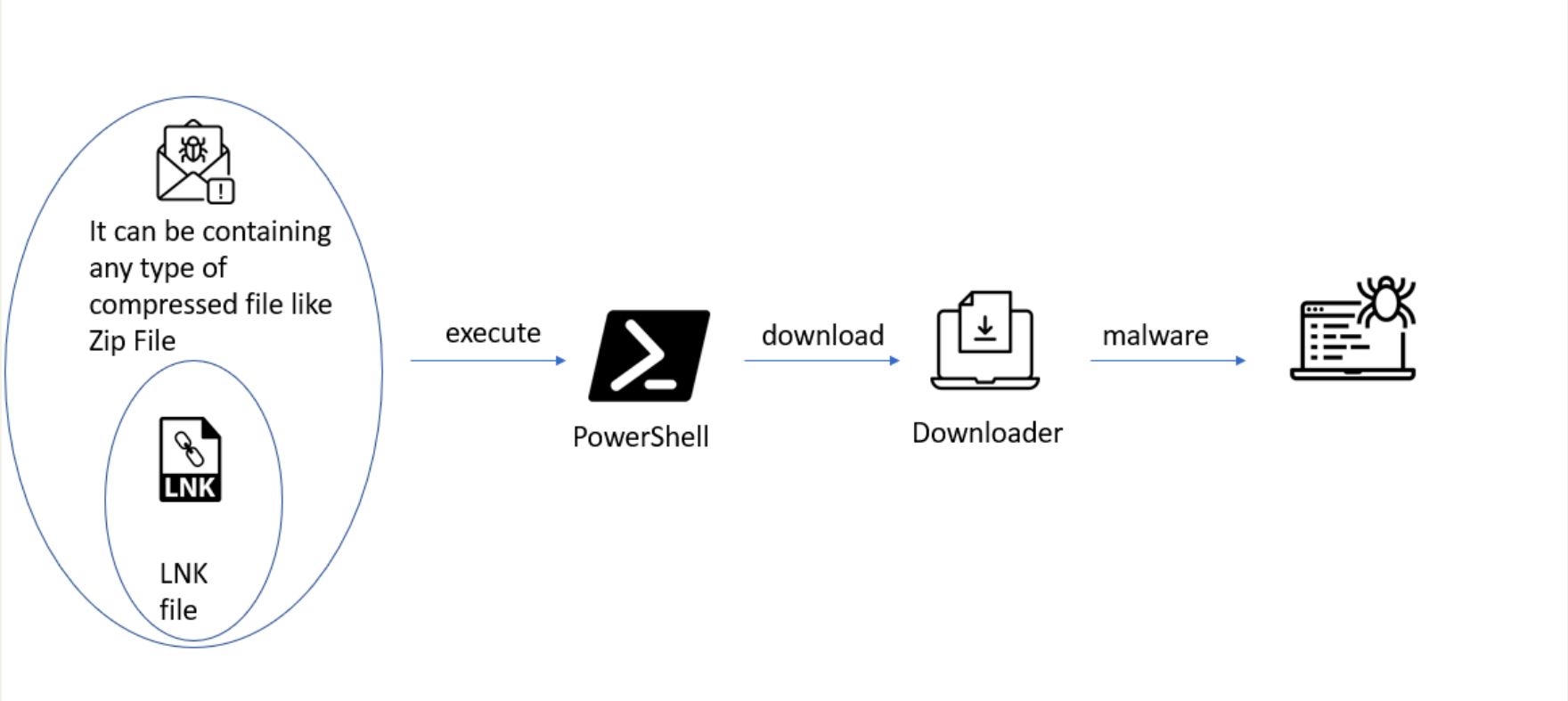
LNK File

- Shell Link Binary File Format (.LNK) contain metadata about the executable file, including the original path to the target application

https://www.resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise

LNK File

- LNK files typically look legitimate, and may have an icon the same as an existing application or document.

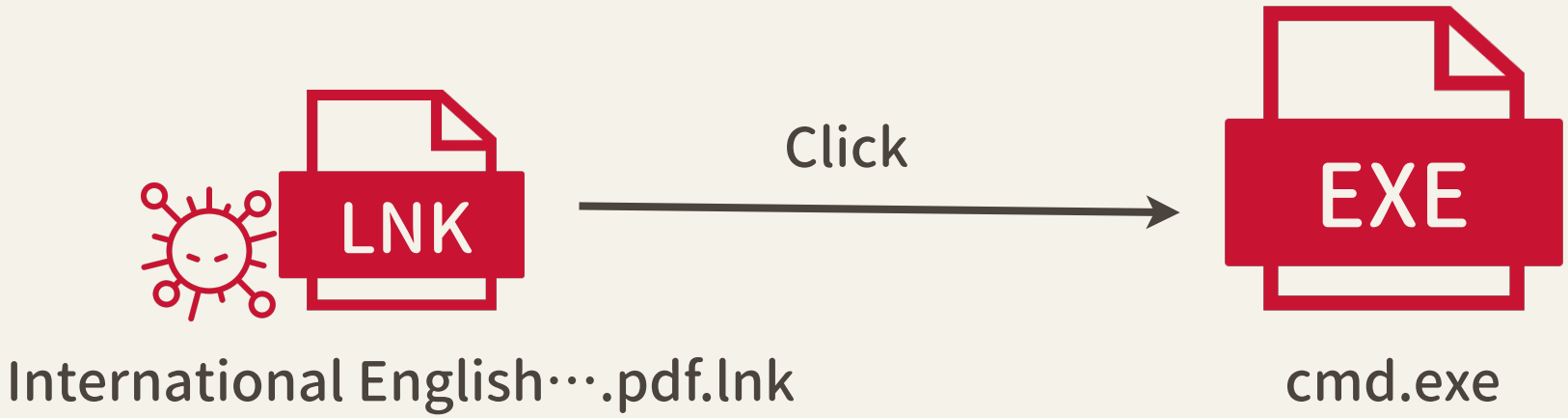


https://www.resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise

(1) Study Sysmon Event Log

TEAMT5

- User Execution: Malicious File
  - Rely upon a user opening a malicious file in order to gain execution
  - Determine which commands are executed behind the lnk file



(1) Study Sysmon Event Log

TEAMT5

- User Execution: Malicious File

```
Record 14978
{
    "EventData": {
      "CommandLine": “\”C:\\windows\\System32\\cmd.exe\" ... ... ”,
      "Company": "Microsoft Corporation",
      "CurrentDirectory": "C:\\Users\\user\\Desktop\\mal\\",
      "Image": "C:\\Windows\\System32\\cmd.exe",
      "OriginalFileName": "Cmd.Exe",
      "ParentCommandLine": "C:\\Windows\\Explorer.EXE",
      "ParentImage": "C:\\Windows\\explorer.exe",
      "UtcTime": "2023-04-29 04:39:33.239"
    },
    "System": {
     "EventID": 1,
```

(1) Study Sysmon Event Log

TEAMT5

- User Execution: Malicious File
  - LNK Commandline analysis
    - Copy decoy ink file to tmp folder and rename to “g4ZokyumB2DC4.tmp”
    - Find file *ertu*.exe and copy to tmp folder and rename to “gosia.exe”

```
copy "International English Language Testing System certificate.pdf.lnk"
     C:\\Users\\user\\AppData\\Local\\Temp\\g4ZokyumB2DC4.tmp /y

for /r C:\\Windows\\System32\\ %%i in (*ertu*.exe) do copy %%i C:\
\Users\\user\\AppData\\Local\\Temp\\gosia.exe /y
```

(1) Study Sysmon Event Log

TEAMT5

- User Execution: Malicious File
  - LNK Commandline analysis
    - Copy decoy ink file to tmp folder and rename to “g4ZokyumB2DC4.tmp”
    - Find file *ertu*.exe and copy to tmp folder and rename to “gosia.exe”

certutil.exe

Decode

https://lolbas-project.github.io/lolbas/Binaries/Certutil/

Command to decode a Base64 encoded file.

```
certutil -decode encodedInputFileName decodedOutputFileName
```

Usecase: Decode files to evade defensive measures
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
MITRE ATT&CK®: T1140: Deobfuscate/Decode Files or Information

(1) Study Sysmon Event Log

TEAMT5

- LNK Commandline analysis
  - Deobfuscate/Decode Files or Information
    - Search for file contents starting with the string “TVNDRgA\”, then save the str
    - Use gosia.exe (certutil.exe) decode the new file then store into “o423DFDS4.tmp”

```
findstr.exe /b \"TVNDRgA\" C:\\Users\\user\\AppData\\Local\\Temp\
\g4ZokyumB2DC4.tmp>C:\\Users\\user\\AppData\\Local\\Temp\\cSi1rouy4.tmp

C:\\Users\\user\\AppData\\Local\\Temp\\gosia.exe -decode C:\\Users\
\user\\AppData\\Local\\Temp\\cSi1rouy4.tmp C:\\Users\\user\\AppData\
\Local\\Temp\\o423DFDS4.tmp
```

(1) Study Sysmon Event Log

TEAMT5

- LNK Commandline analysis
  - Deobfuscate/Decode Files or Information
    - Extract the file “o423DFDS4.tmp”
    - Open the decoy pdf

```
&
expand C:\\Users\\user\\AppData\\Local\\Temp\\o423DFDS4.tmp -F:* C:\
\Users\\user\\AppData\\Local\\Temp
&
"C:\\Users\\user\\AppData\\Local\\Temp\\International English Language
Testing System certificate.pdf"
```

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/expand

(1) Study Sysmon Event Log

TEAMT5

- LNK Commandline analysis
  - Scripting Interpreter: JavaScript
    - Copy “66DF3DFG.tmp” to Download folder
    - Use Wscript run “34fDFkfSD38.js”

```
copy C:\\Users\\user\\AppData\\Local\\Temp\\66DF3DFG.tmp C:\\Users\
\Public\\Downloads\\66DF3DFG.tmp

Wscript C:\\Users\\user\\AppData\\Local\\Temp\\34fDFkfSD38.js

exit
```

(1) Study Sysmon Event Log

TEAMT5

- Process Creation: Wscript execute cmd.exe

```
Record 14987
{
    "EventData": {
      "CommandLine": "\"C:\\Windows\\System32\\cmd.exe\"  /c ipconfig>C:\
\Users\\Public\\Downloads\\d3reEW.txt & copy C:\\Users\\user\\AppData\
\Local\\Temp\\svchastd.exe \"C:\\Users\\user\\AppData\\Roaming\\Microsoft\
\Windows\\Start Menu\\Programs\\Startup\\Officeupdated.exe\"  ... ...",
      "ParentCommandLine": "Wscript  C:\\Users\\user\\AppData\\Local\\Temp\
\34fDFkfSD38.js",
      "ParentImage": "C:\\Windows\\System32\\wscript.exe",
      "UtcTime": "2023-04-29 04:39:33.818"
    },
    "System": {
      "EventID": 1,
```

(1) Study Sysmon Event Log

TEAMT5

- JS Commandline analysis
  - System Network Configuration Discovery: ipconfig
    - Save the system’s network information to ‘d3reEW.txt’

```
ipconfig>C:\\Users\\Public\\Downloads\\d3reEW.txt
```

(1) Study Sysmon Event Log

TEAMT5

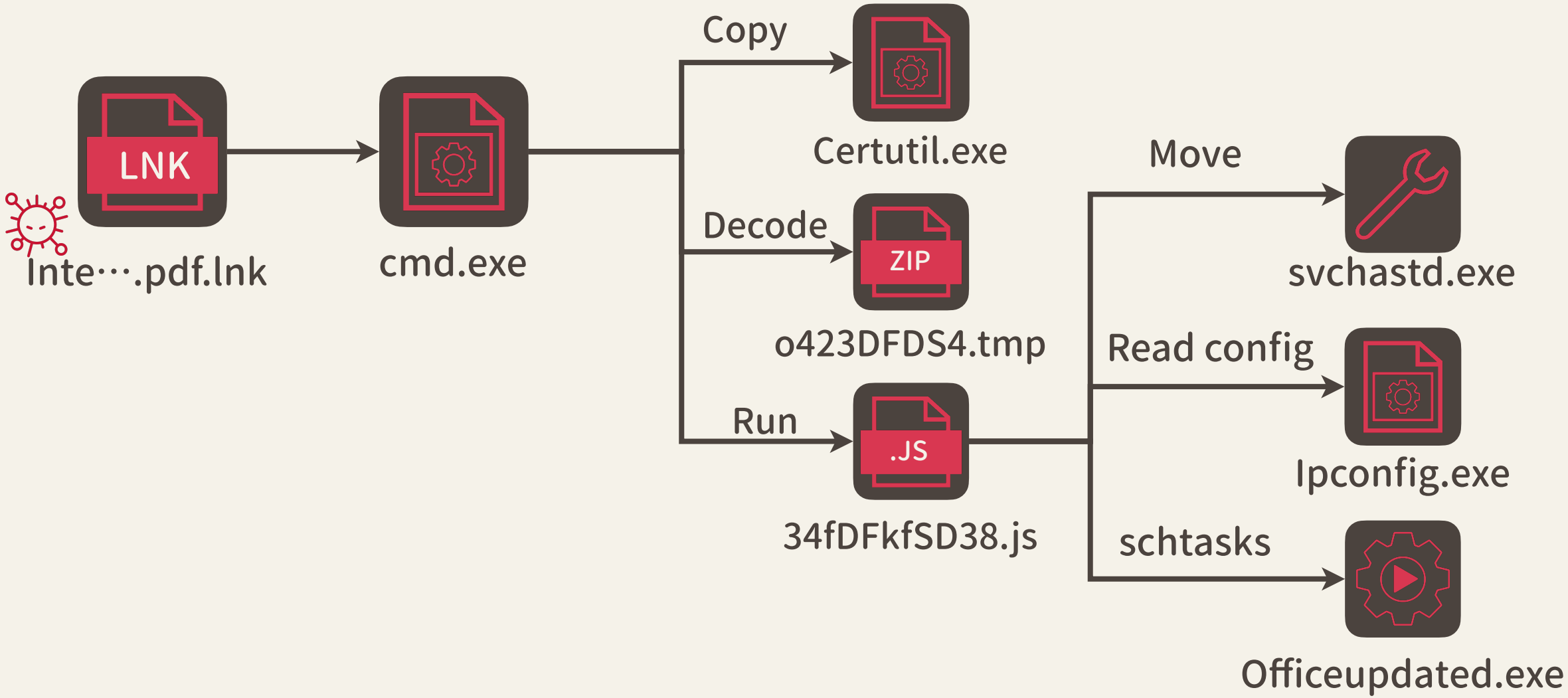
- JS Commandline analysis
  - Persistence: schtasks
    - Copy the file 'svchostd.exe' that was just extracted to this directory
    - Use schtasks to set autorun

```
copy C:\\Users\\user\\AppData\\Local\\Temp\\svchastd.exe \"C:\\Users\
\Public\\Downloads\\Officeupdated.exe\"

schtasks /create /SC minute /MO 120 /TN \"Office update task\"  /TR "C:\
\Users\\Public\\Downloads\\Officeupdated.exe"
```

(2) Attack Summary

TEAMT5



(3) Writing Rule

TEAMT5

- Note:
  - Focus on interesting behavior
    - Process creation with LNK file
    - certutil.exe, svchastd.exe copy and use
    - Process creation with JS file
    - System config read

(3) Writing Rule: LNK file execution


```
detection:
    eventid:
        EventID: 1
    lnk_behavior:
        CommandLine|contains: '.lnk'
        ParentImage: 'C:\Windows\explorer.exe'
        Image|contains:
            - 'cmd.exe'
            - 'powershell.exe'
    selection_HigaisaAPT_signature:
        - CommandLine|contains:
            - 'gosia.exe'
            - 'svchastd'
            - 'Officeupdated'
```

(3) Hunting: LNK file execution

[+] Group: Sigma

timestamp	detections	count	Event.System.Provider	Event ID	Record ID	Computer	Event Data
2023-04-29 04:39:33	+ Potential HigaisaAPT behavior - lnk execution	1	Microsoft-Windows-Sysmon	1	14978	WIN10-PRO-22H2-64	CommandLine: '"C:\windows\System32\cmd.exe" C:\Windows\System32\cmd.exe /c copy "International English Language Testing System certificate.pdf.lnk" C:\Users\user\AppData\Local\Temp\g4ZokyumB2DC4.tmp /y& for /r C:\Windows\System32\ %%i in (*ertu*.exe) do copy %%i C:\Users\user\AppData\Local\Temp\gosia.exe /y& findstr.exe /b "TVNDRgA" C:\Users\user\AppData\Local\Temp\g4ZokyumB2DC4.tmp>C:\Users\user\AppData\Local\Temp\cSi1rouy4.tmp&C:\Users\user\AppData\Local\Temp\gosia.exe -dec ... (use --full to show all content) Company: Microsoft Corporation CurrentDirectory: C:\Users\user\Desktop\mal\ Description: Windows Command Processor

1 event hit

(4) Writing Rule: Script Execution


```
    eventid:
        EventID: 1
    script_image:
        Image|endswith:
            - '\wscript.exe'
            - '\cscript.exe'
    selection_file_extenstion:
        CommandLine|contains:
            - '.jse'
            - '.vbe'
            - '.js'
    falsepositive:
        ParentImage|contains: '\winzip'
    condition: eventid and script_image and 1 of selection* and not
falsepositive
```

(4) Writing Rule: Script Execution

[+] Group: Sigma

timestamp	detections	count	Event.System.Provider	Event ID	Record ID	Computer	Event Data
2023-04-29 04:39:33	+ Potential HigaisaAPT behavior - javascript execution	1	Microsoft-Windows-Sysmon	1	14986	WIN10-PRO-22H2-64	CommandLine: Wscript C:\Users\user\AppData\Local\Temp\34fDFkfSD38.js Company: Microsoft Corporation CurrentDirectory: C:\Users\user\Desktop\mal\ Description: Microsoft ® Windows Based Script Host FileVersion: 5.812.10240.16384 Hashes: MD5=A47CBE969EA935BDD3AB568BB126BC80,SHA256=34008E2057DF8842DF2102469953 85A0441DC1E081D60AD15BD481E062E7F100,IMPHASH=0F71D5F6F4CBB935CE1B09754102419C Image: C:\Windows\System32\wscript.exe

1 event hit

(4) Writing Rule: decode payload


```
eventid:
    EventID: 1
certutil_copy_behavior:
    CommandLine|contains:
        - 'certutil.exe'
        - 'copy '
    OriginalFileName:
        - 'cmd.exe'
certutil_behavior:
    - OriginalFileName:
        - 'certutil.exe'
    - CommandLine|contains:
        - '-decode '
        - '/decode '
        - '-decodehex '
        - '/decodehex '
selection_HigaisaAPT_signature:
    - CommandLine|contains:
```

(4) Writing Rule: decode payload

[+] Group: Sigma

timestamp	detections	count	Event.System.Provider	Event ID	Record ID	Computer	Event Data
2023-04-29 04:39:33	+ Potential HigaisaAPT behavior - payload decode	1	Microsoft-Windows-Sysmon	1	14978	WIN10-PRO-22H2-64	CommandLine: '"C:\windows\System32\cmd.exe" C:\Windows\System32\cmd.exe /c copy "International English Language Testing System certificate.pdf.lnk" C:\Users\user\AppData\Local\Temp\g4ZokyumB2DC4.tmp /y& for /r C:\Windows\System32\ %%i in (*ertu*.exe) do copy %%i C:\Users\user\AppData\Local\Temp\gosia.exe /y& findstr.exe /b "TVNDRgA" C:\Users\user\AppData\Local\Temp\g4ZokyumB2DC4.tmp>C:\Users\user\AppData\Local\Temp\cSi1rouy4.tmp&C:\Users\user\AppData\Local\Temp\gosia.exe -dec

2 events hit

(4) Writing Rule: System config read


```
eventid:
    EventID: 1
ipconfig_binary:
    - OriginalFileName|contains:
        - 'ipconfig'
ipconfig_behavior:
    CommandLine|contains|all:
        - 'ipconfig'
        - '>'
    Image|contains: 'cmd.exe'
selection_HigaisaAPT_signature:
    - CommandLine|contains:
        - 'gosia.exe'
        - 'svchastd'
        - 'Officeupdated'
    - ParentCommandLine|contains:
        - '.js'
condition: eventid and 1 of ipconfig*
```

(4) Writing Rule: System config read

[+] Group: Sigma

timestamp	detections	count	Event.System.Provider	Event ID	Record ID	Computer	Event Data
2023-04-29 04:39:33	+ Potential HigaisaAPT behavior - system config read	1	Microsoft-Windows-Sysmon	1	14987	WIN10-PRO-22H2-64	CommandLine: '"C:\Windows\System32\cmd.exe" /c ipconfig>C:\Users\Public\Downloads\d3reEW.txt & copy C:\Users\user\AppData\Local\Temp\svchastd.exe "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Officeupdated.exe" & copy C:\Users\user\AppData\Local\Temp\svchastd.exe "C:\Users\Public\Downloads\Officeupdated.exe" & schtasks /create /SC minute /MO 120 /TN "Office update task" /TR "C:\Users\Public\Downloads\Officeupdated.exe"'

1 events hit

Conclusion

TEAMT5

- Provide a detailed explanation of how to use Sigma rules
- Understand the role of Sigma rules in threat hunting
- Practically integrate sysmon and sigma to hunt for various attack methods
- Simulated three threat scenarios and attempted to detect these attacks

Take Away

TEAMT5

- The content of the command line is rich in information but also very cluttered
- The act of deobfuscation is often more apparent to blue team
- Detection methods always depend on the event logging mechanism
- Sigma rules are widely used and powerful in the field of threat hunting.

Similar rules

TEAMT5

- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_certutil_decode.yml
- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_lolbin_rundll32_installscreensaver.yml
- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_findstr_lnk.yml

THANK YOU!

Will

Will@teamt5.org

TEAMT5
杜浦數位安全

主題攤位 R103

特調您的端點威脅防護

攤位現場
或 按讚
即可換特調

瞭解更多