



AUGUST 3-8, 2019

MANDALAY BAY / LAS VEGAS

An easy ATT&CK-based Sysmon hunting tool

Bowen Pan

About me.

- **@baronpan**
- Senior threat analyst in **@RedDrip7** team.
- threat intelligence, APT/mobile threat analysis, etc.

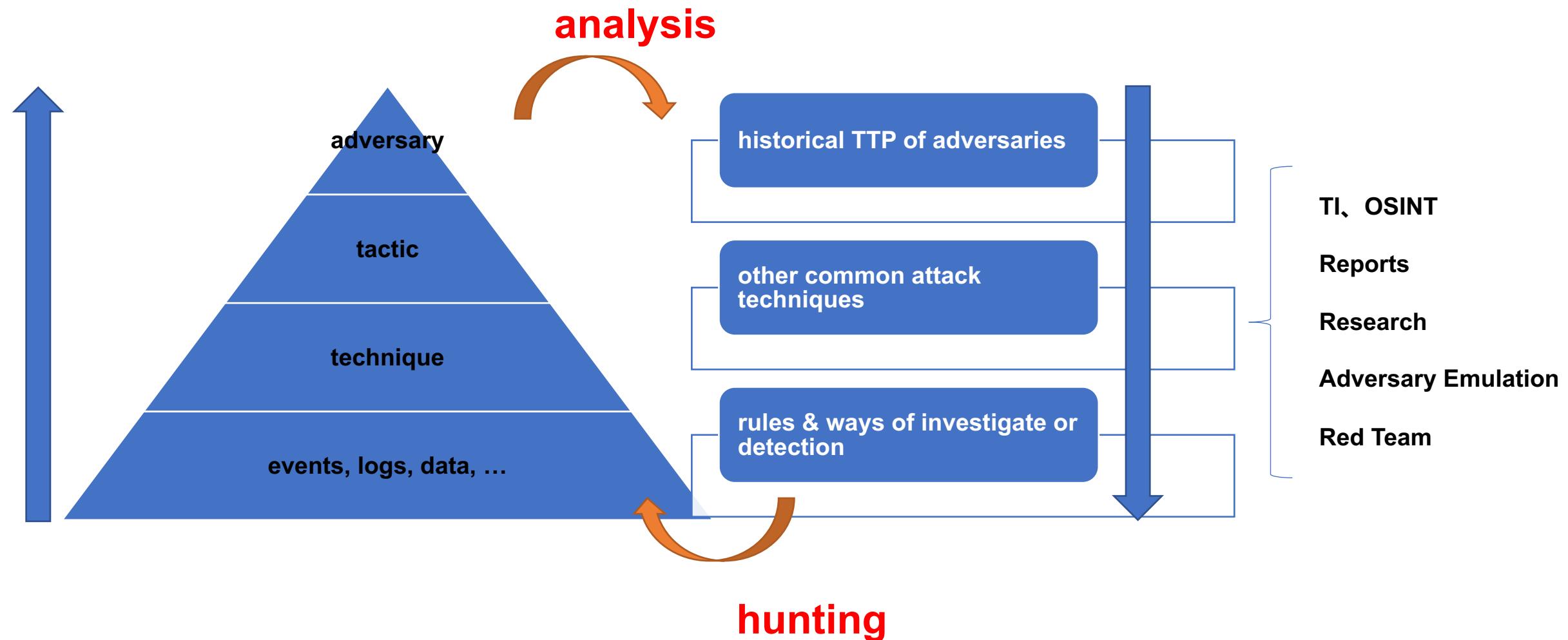
Motivation

- mid of 2018, interested in **MITRE ATT&CK**.
- how did ATT&CK can improve our analysis and hunting.
- some thoughts and ideas, start to implement...

MITRE ATT&CK (my view of.)

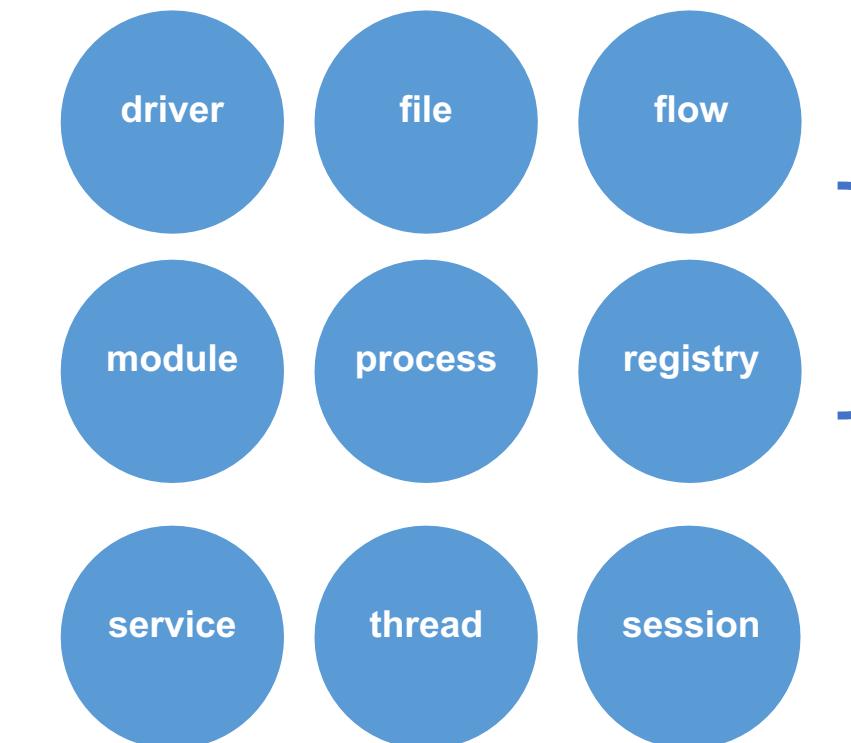
- Adversarial Tactics Techniques and Common Knowledge

MITRE ATT&CK (my view of.)

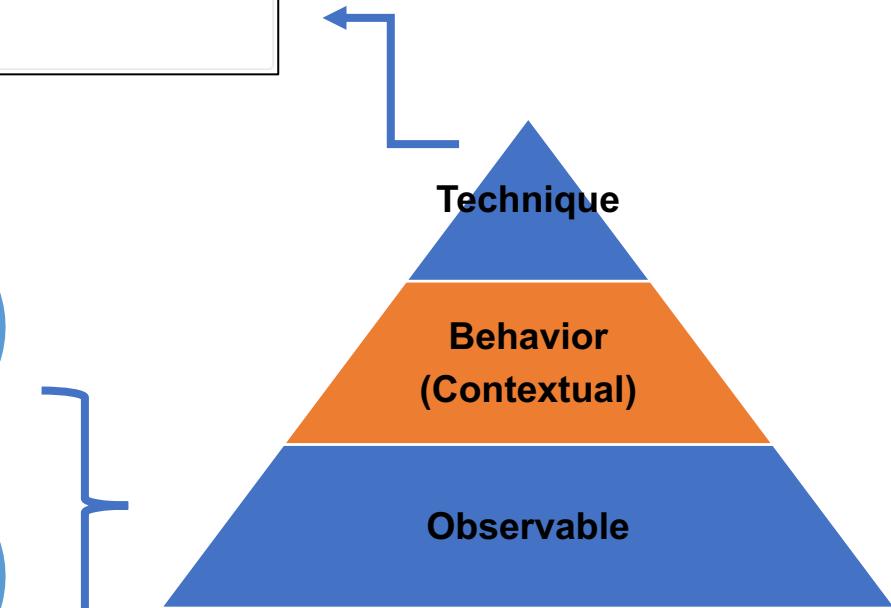


MITRE ATT&CK (my view)

- Windows event logs
- Sysmon
- Autoruns
- Customized endpoint agent
 - network
 - other system logging



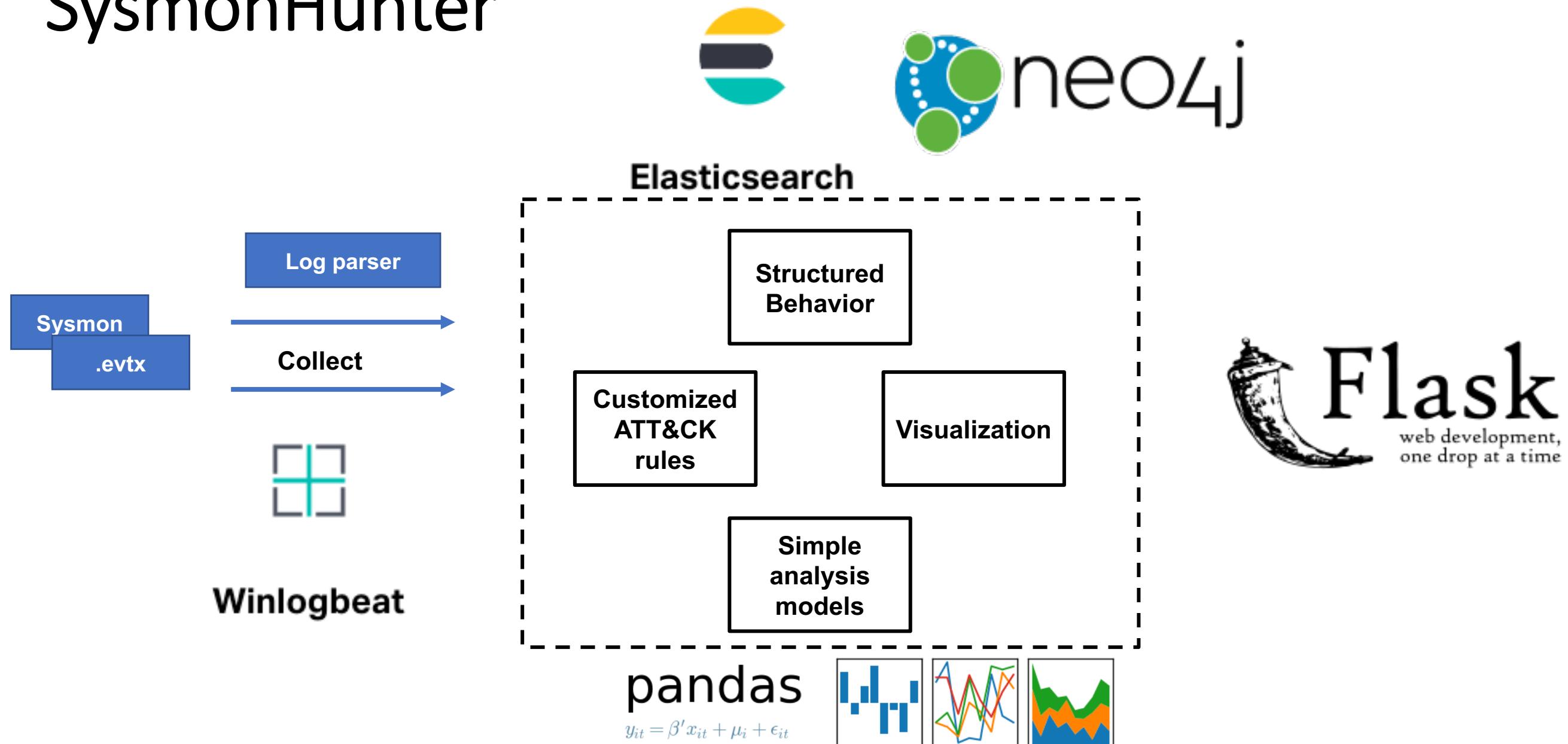
ID: T1086
Tactic: Execution
Platform: Windows
Permissions Required: User, Administrator
Data Sources: PowerShell logs, Loaded DLLs, DLL monitoring, Windows Registry, File monitoring, Process monitoring, Process command-line parameters
Supports Remote: Yes
Contributors: Praetorian
Version: 1.1



SysmonHunter

- structured observables with contextual and relation.
- support rules definition with simple logical expressions.
- some simple and visualize analysis models.

SysmonHunter



SysmonHunter – Data structured

- Entity – structured observables with properties
 - File
 - hash, path, name, signature, type
 - Process
 - pid, image path, cmdline, user, calltrace, guid
 - Network
 - remote ip, remote port, protocol, remote host
 - Registry
 - path, key, value
 - other entities
 - Endpoint, User, Service, ...

SysmonHunter – Data structured

- Behavior – Set of entities and relationship
 - Process/Network/File/Registry

More contextual:

**PARENT PROCESS - execute -> CHILD
PROCESS with related FILE on ENDPOINT
at DATETIME**

```
class ProcessBehavior(BaseBehavior):
    CONTEXT = ['parent', 'current', 'file', 'endpoint']
    def __init__(self, _raw):
        super(ProcessBehavior, self).__init__(_raw)

        self.parent = ProcessEntity(_raw['parent'])
        self.current = ProcessEntity(_raw['current'])
        self.file = FileEntity(_raw['file'])
        self.date = _raw['datetime']
        self.endpoint = EndPointEntity(_raw['endpoint'])
        self.relation = _raw['relation']
```

SysmonHunter – Event process

- Event data process
 - manually
 - logparser.exe -i:evt -o:csv "select TimeGenerated, SourceName, ComputerName, SID, EventID, Strings from Microsoft-Windows-Sysmon%4Operational.evtx"
 - winlogbeat
- Process agent
 - agent.py
 - raw event -> structured data

```
if __name__ == '__main__':
    parser = argparse.ArgumentParser()
    parser.add_argument('-c', help='conf file')
    parser.add_argument('-t', help='choose csv or winlogbeat')
    parser.add_argument('-i', help='csv file')
    parser.add_argument('-start', help='start date from winlogbeat, like 2019-07-19')
    parser.add_argument('-end', help='end date from winlogbeat, like 2019-07-19')
    args = parser.parse_args()
```

SysmonHunter – Rule definition

- YAML format
- logical expression
 - and, or, not
- match pattern
 - nocase/case, regex
- Format
 - Technique id
 - name, description, alert level, attack phase
 - query conditions

```
T1035:  
  name: Service Execution  
  description:  
  level: medium  
  phase: Execution  
  query:  
    - type: process  
      process:  
        image:  
          pattern: \Windows\.\+\sc.exe  
          flag: regex  
        cmdline:  
          pattern: start|create|query|config  
    - type: process  
      process:  
        cmdline:  
          pattern: \SYSTEM\CurrentControlSet\services  
    - type: reg ← behavior  
      reg:  
        path:  
          pattern: \SYSTEM\CurrentControlSet\services  
      process:  
        image:  
          pattern: \Windows\.\+\lsass.exe|\Windows\.\+\svchost.exe  
          flag: regex  
          op: not  
      op: and
```

condition 1

entity

property

SysmonHunter

Sysmon Hunter Event Data ▾ Hunter Tools ▾

Select timerange: 07/16/2019 - 07/16/2019 ProcessBehavior ▾ Search

Show 10 entries Search:

Query whole imported data(raw & abnormal) by timerange

search by keyword, support regex.

Endpoint	Timestamp	BehaviorType	MT&CK IDs	Value
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:07:06	ProcessBehavior	T1085	(C:\Windows\System32\svchost.exe) -access-> (C:\Windows\system32\rundll32.exe)
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:14:10	ProcessBehavior	C1002	(50 Windows\System32\sdiaignhost.exe) -access-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe)
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:14:10	ProcessBehavior	C1002	(C:\Windows\System32\svchost.exe) -access-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe)
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:14:10	ProcessBehavior	C1002	(C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe "C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe" /noconfig /fullpaths @"C:\Users\victim\AppData\Local\Temp\0qrygxyo.cmdline") -create-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\victim\AppData\Local\Temp\RES620E.tmp" "c:\Users\victim\AppData\Local\Temp\CSC620D.tmp")
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:14:11	ProcessBehavior	C1002	(C:\Windows\System32\sdiaignhost.exe C:\Windows\System32\sdiaignhost.exe -Embedding) -create-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe "C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe" /noconfig /fullpaths @"C:\Users\victim\AppData\Local\Temp\fzwsdsjq.cmdline")
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:14:11	ProcessBehavior	C1002	(C:\Windows\system32\conhost.exe) -access-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe)
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:14:11	ProcessBehavior	C1002	(C:\Windows\System32\svchost.exe) -access-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe)
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:14:11	ProcessBehavior	C1002	(C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe "C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe" /noconfig /fullpaths @"C:\Users\victim\AppData\Local\Temp\fzwsdsjq.cmdline") -create-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\victim\AppData\Local\Temp\RES643F.tmp" "c:\Users\victim\AppData\Local\Temp\CSC643E.tmp")
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:14:11	ProcessBehavior	C1002	(C:\Windows\System32\svchost.exe) -access-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe)
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-16T07:14:11	ProcessBehavior	C1002	(C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe "C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe" /noconfig /fullpaths @"C:\Users\victim\AppData\Local\Temp\x_5erjkp.cmdline") -create-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\victim\AppData\Local\Temp\RES64CC.tmp" "c:\Users\victim\AppData\Local\Temp\CSC64CB.tmp")

Showing 81 to 90 of 114 entries

Previous 1 ... 8 9 10 11 12 Next

SysmonHunter – Statistic analysis

Sysmon Hunter Event Data ▾ Hunter Tools ▾

Select timerange: 07/16/2019 - 07/17/2019

Selected Behavior Details Show 10

Search:

Parent Image Path	Child Image Path	Occurs
C:\Windows\System32\svchost.exe	Graphic Manage	15
C:\Windows\Microsoft.NET\Framework	Graphic Search	8
C:\Windows\System32\svchost.exe	Endpoint	8
C:\Windows\System32\svchost.exe		7
50\Windows\System32\sdianghost.exe		4
C:\Windows\System32\cmd.exe		4
C:\Windows\system32\conhost.exe		4
C:\Windows\system32\lsass.exe		4
C:\Windows\System32\sdianghost.exe		4
C:\Windows\System32\svchost.exe		4

Statistic behaviors on frequency.

Showing 1 to 10 of 41 entries

Previous 1 2 3 4 5 Next

SysmonHunter – Graphic analysis

- Nodes in/out degrees

Sysmon Hunter Event Data ▾ Hunter Tools ▾

Select Node type : ProcessBehavior RegistryBehavior FileBehavior NetworkBehavior

Delete selected node

Node value

Domain

Query

InDegree OutDegree

	InDegree	OutDegree
(50\Windows\System32\cmd.exe) -access-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe)	0	3
(C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe) -access-> (C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe)	0	3
(C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe) -access-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe)	0	3
(C:\Windows\System32\cmd.exe) -access-> (c:\Users\victim\Desktop\Sysmon.exe)	0	3
(C:\Windows\system32\conhost.exe) -access-> (C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe)	0	3
(C:\Windows\system32\conhost.exe) -access-> (C:\Windows\system32\scrtasks.exe)	0	3
(C:\Windows\system32\conhost.exe) -access-> (C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe)	0	3
(C:\Windows\system32\csrss.exe) -access-> (C:\Windows\System32\cmd.exe)	0	3
(C:\Windows\system32\csrss.exe) -access-> (C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe)	0	3
(C:\Windows\System32\csrss.exe) -inject-> (C:\Windows\System32\cmd.exe)	0	3

Showing 1 to 10 of 58 entries

Previous 1 2 3 4 5 6 Next

HAT EVENTS

SysmonHunter – Graphic analysis

Sysmon Hunter Event Data ▾ Hunter Tools ▾

Query: (keyword per line)

```
powershell
```

Query

Selected Node: (C:\Windows\System32\wbem\WmiPrvSE.exe C:\Windows\system32\wbem\wmiprvse.exe -Embedding) -create-> (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -enc

```
SQBmACgAJABQAFMAvgBFAHIAUwBpAG8ATgBUAGEAYgBsAEUALgBQAFMAvgBFAFIAcwBpAG8ATgAuAE0AQBqAG8AchgAgAC0ARwBFACAAMwApAHsAJBHFAARgA9AfSAcgBiAGYAXQAUAEAcwBzAEUATQBiAGwAeQAUAEcAZQBUAFQAWQBwAGUAKAAnAFMAeQBzAHQAZQ
```

Test case 1

- Empire post-exploitation tool
 - stager: windows/macro
 - listener: http
 - bypassuac and use mimikatz dump credentials.

Test case 1

order by timestamp

Show 100 entries

UAC bypass Search:

Endpoint	Timestamp	BehaviorType	ATT&CK IDs	Value
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T08:24:06	RegistryBehavior	T1088	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -open-> HKU\S-1-5-21-3583514301-2682539595-3720967138-1000_CLASSES\mscfile\shell\open\command
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T08:24:06	RegistryBehavior	T1088	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -update-> HKU\S-1-5-21-3583514301-2682539595-3720967138-1000_CLASSES\mscfile\shell\open\command\ (Default)
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T08:24:11	RegistryBehavior	T1088	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -open-> HKU\S-1-5-21-3583514301-2682539595-3720967138-1000_CLASSES\mscfile\shell\open\command
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T09:29:44	RegistryBehavior	T1088	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -update-> HKU\S-1-5-21-3583514301-2682539595-3720967138-1000_CLASSES\mscfile\shell\open\command\ (Default)
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T09:29:44	RegistryBehavior	T1088	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -open-> HKU\S-1-5-21-3583514301-2682539595-3720967138-1000_CLASSES\mscfile\shell\open\command
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T09:29:49	RegistryBehavior	T1088	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -open-> HKU\S-1-5-21-3583514301-2682539595-3720967138-1000_CLASSES\mscfile\shell\open\command

Showing 1 to 6 of 6 entries (filtered from 605 total entries)

Previous 1 Next

EVENTS

Test case 2

- Empire post-exploitation tool
 - stager: windows/hta
 - listener: http_com
 - bypassuac and use mimikatz dump credentials.

Test case 2

Endpoint	Timestamp	BehaviorType	ATT&CK IDs	Value	mshta execution
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T09:28:50	ProcessBehavior	T1170	(C:\Windows\explorer.exe C:\Windows\Explorer.EXE) -create-> (C:\Windows\System32\mshta.exe "C:\Windows\System32\mshta.exe" "C:\Users\victim\Desktop\http_com.hta")	SQBGACgAJABQAFMAVgBFAHIAUwBpAG8ATgBUAEAYgBsAGUALgBQAFMAVgBIAHIAUwBJAG8ATgAuAE0AQQBqAG8AcgAgAC0AZwBFACAAMwApAHsAJABHAF
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T09:28:50	ProcessBehavior	T1086	(C:\Windows\System32\svchost.exe) -access-> (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe)	
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T09:28:50	ProcessBehavior	T1170	(C:\Windows\System32\svchost.exe) -access-> (C:\Windows\System32\mshta.exe)	
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T09:28:50	ProcessBehavior	T1170, T1086	(C:\Windows\System32\mshta.exe "C:\Windows\System32\mshta.exe" "C:\Users\victim\Desktop\http_com.hta") -create-> (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe)	SQBGACgAJABQAFMAVgBFAHIAUwBpAG8ATgBUAEAYgBsAGUALgBQAFMAVgBIAHIAUwBJAG8ATgAuAE0AQQBqAG8AcgAgAC0AZwBFACAAMwApAHsAJABHAF
	2019-07-				

Show 100 entries

Search: embedd

Endpoint	Timestamp	BehaviorType	ATT&CK IDs	Value	IE Dcom launch
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T08:20:48	ProcessBehavior	T1086	(C:\Windows\System32\wbem\WmiPrvSE.exe C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding) -create-> (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe)	SQBGACgAJABQAFMAVgBIAHIAcwbJAE8AbgBUAGEAQgBMAEUALgBQAFMAVgBIAFIAUwBpAG8ATgAuAE0AQQBKAG8AcgAgAC0ARwBIACAAMwApAHsAJABHAF
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T08:20:48	ProcessBehavior	T1086	(C:\Windows\System32\wbem\WmiPrvSE.exe C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding) -create-> (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe)	SQBGACgAJABQAFMAVgBIAHIAcwbJAE8AbgBUAGEAQgBMAEUALgBQAFMAVgBIAFIAUwBpAG8ATgAuAE0AQQBKAG8AcgAgAC0ARwBIACAAMwApAHsAJABHAF
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T09:28:52	ProcessBehavior	C1005	(C:\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch) -create-> (C:\Program Files\Internet Explorer\iexplore.exe "C:\Program Files\Internet Explorer\iexplore.exe")	
a7243ce575a805bb2fb8a2b14b7d0fbc	2019-07-31T09:29:45	ProcessBehavior	C1005	(C:\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch) -create-> (C:\Program Files\Internet Explorer\iexplore.exe "C:\Program Files\Internet Explorer\iexplore.exe")	

Future work

- Rule list.
- Extend the data sources(other evtx, osquery).
- Extend behavior types.
- Extend analysis model.

- demo time!
- source code:
<https://github.com/baronpan/SysmonHunter>