
black hat
USA 2019
AUGUST 3–8, 2019
MANDALAY BAY / LAS VEGAS
An easy ATT&CK-based Sysmon hunting tool
Bowen Pan
#BHUSA @BLACK HAT EVENTS

About me.

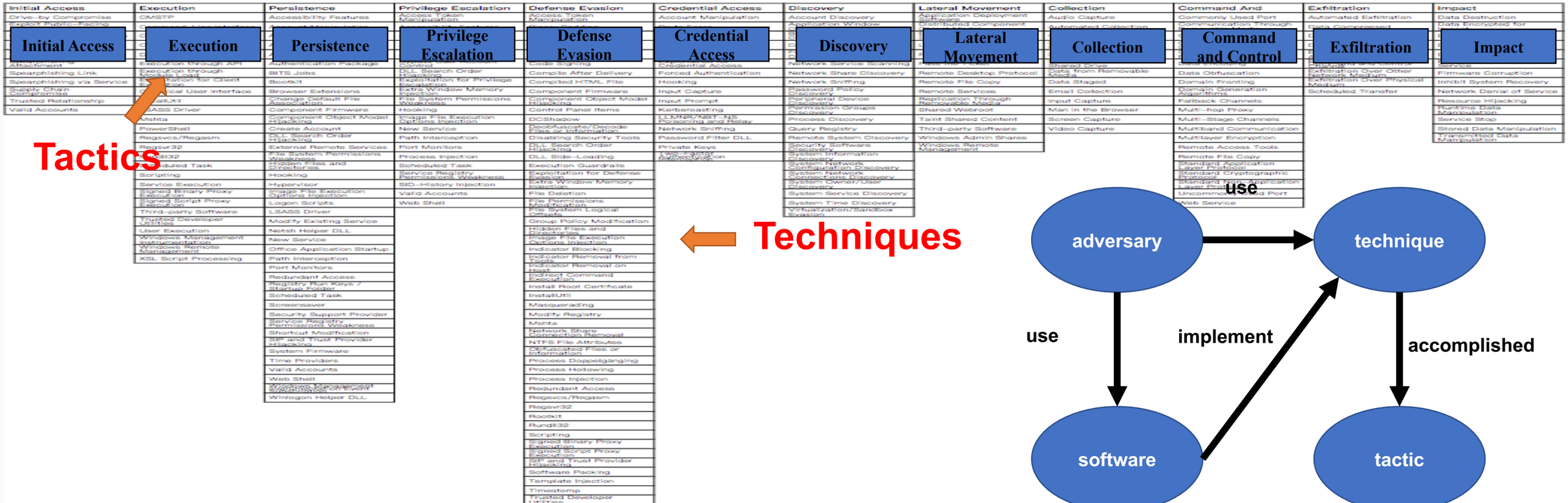
- **@baronpan**
- Senior threat analyst in **@RedDrip7** team.
- threat intelligence, APT/mobile threat analysis, etc.

Motivation

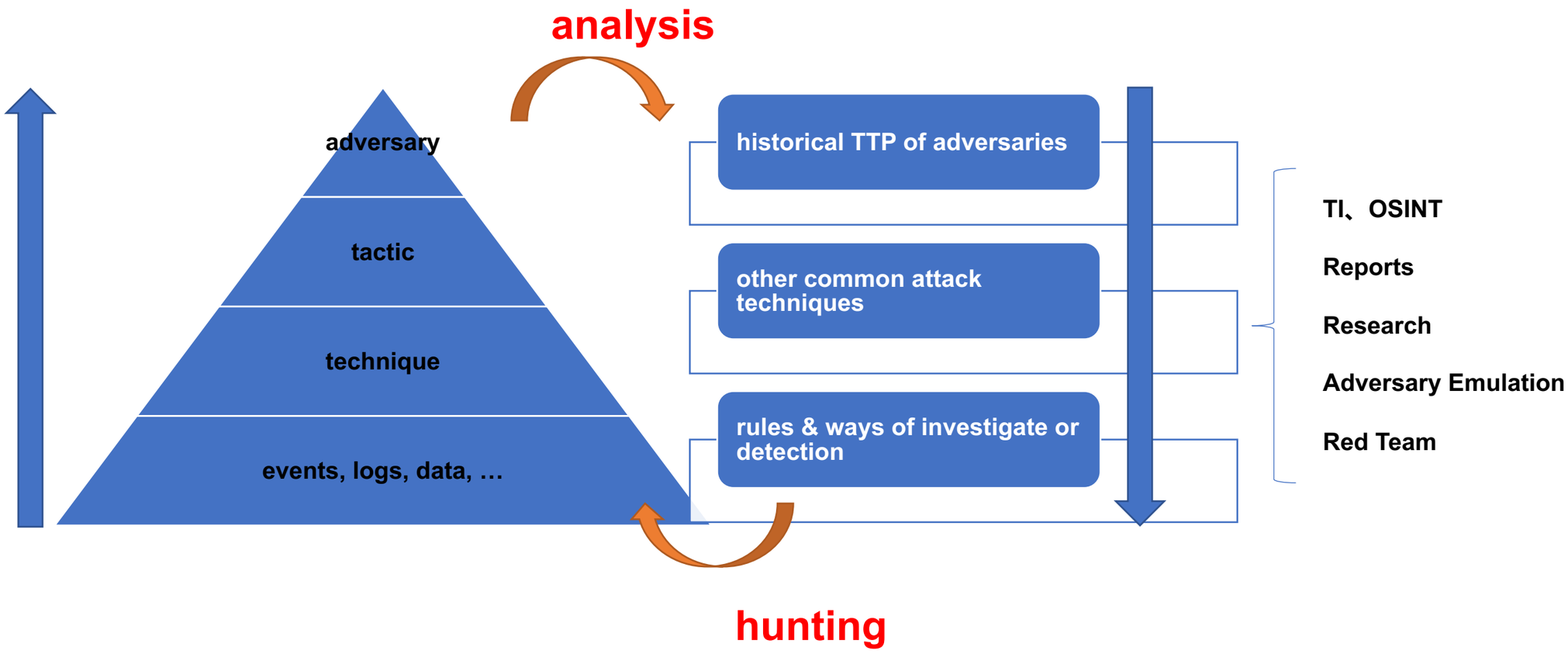
- mid of 2018, interested in **MITRE ATT&CK**.
- how did ATT&CK can improve our analysis and hunting.
- some thoughts and ideas, start to implement…

MITRE ATT&CK (my view of.)

- **A**dversarial **T**actics **T**echniques and **C**ommon **K**nowledge



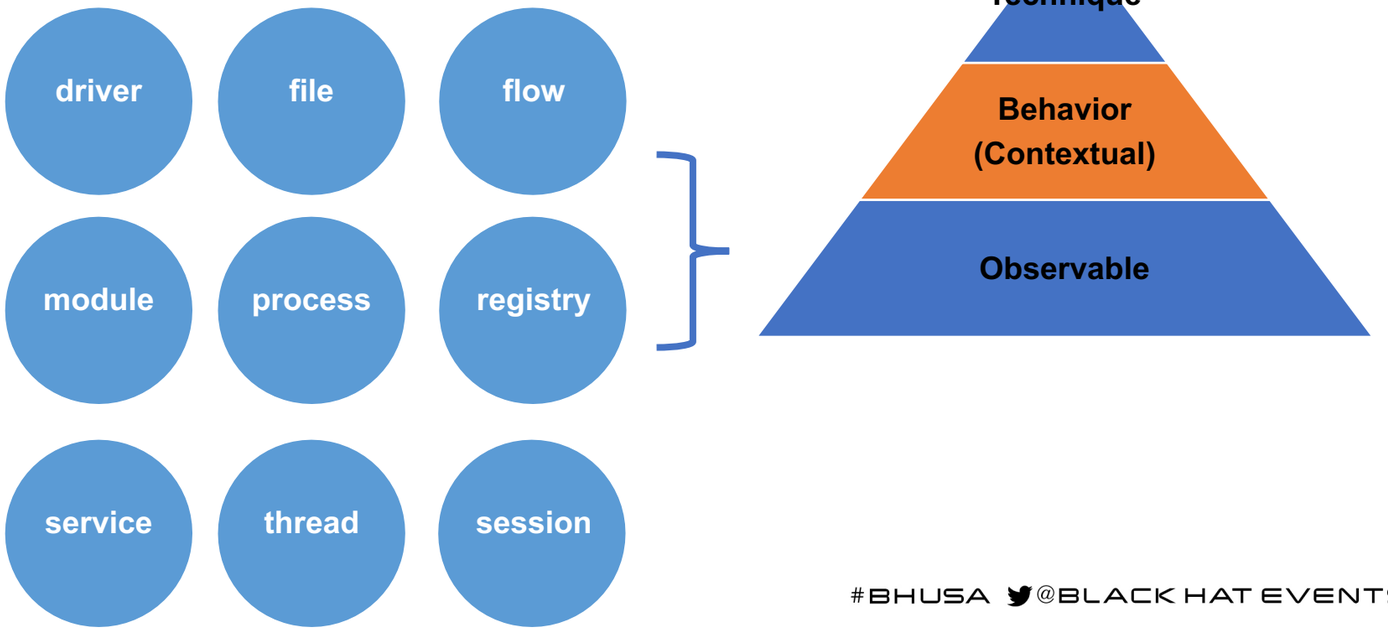
MITRE ATT&CK (my view of.)



MITRE ATT&CK (my view

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

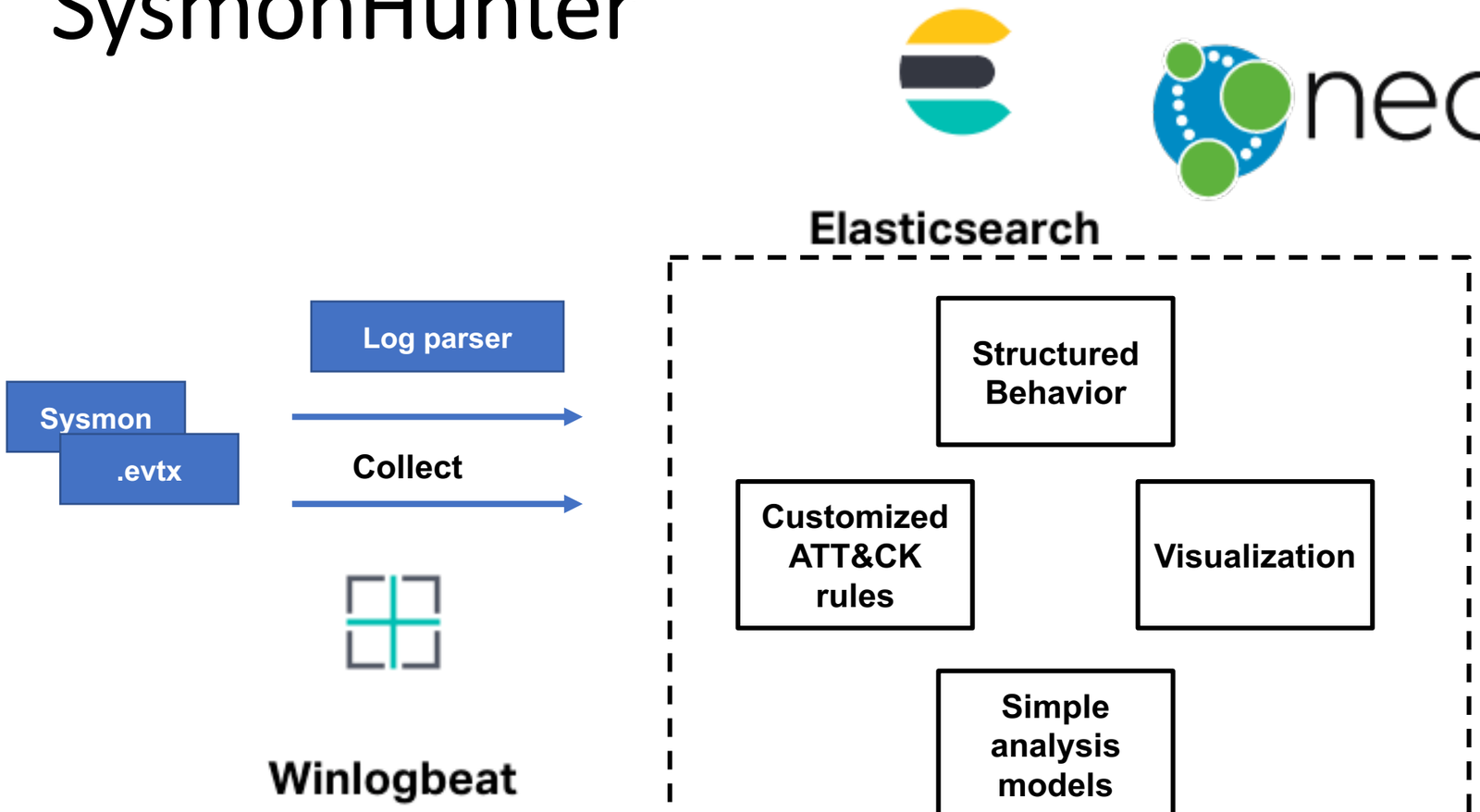
- Windows event logs
- Sysmon
- Autoruns
- Customized endpoint agent
  - network
  - other system logging



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']
```

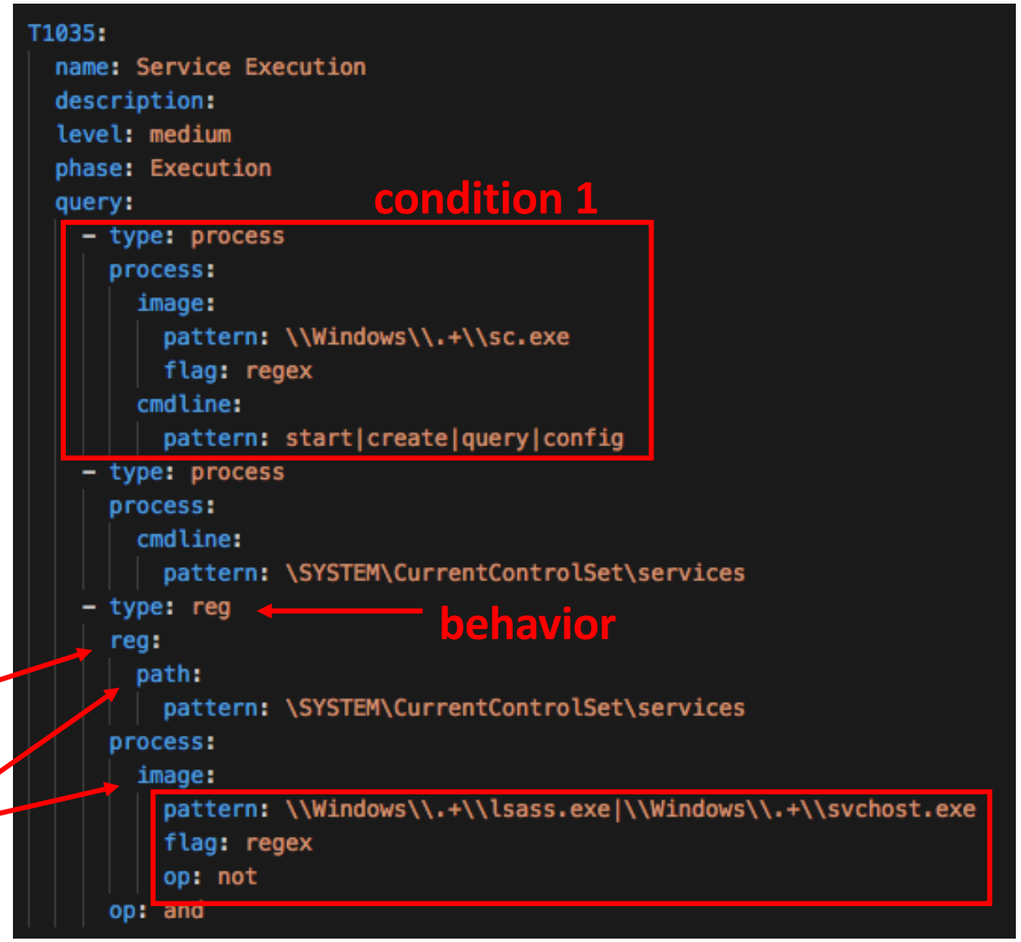
SysmonHunter – Event process

- 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

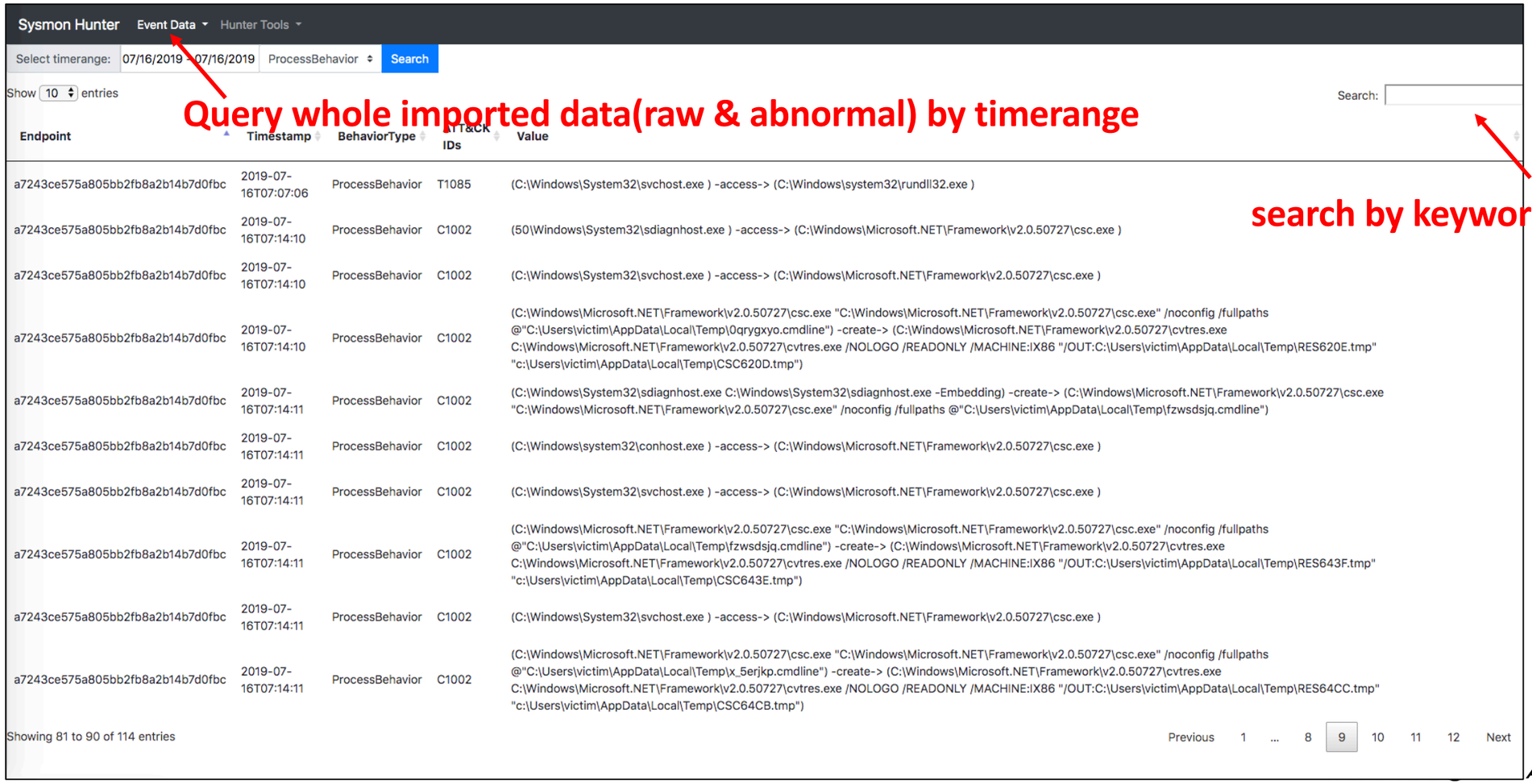
```
if __name__ == '__main__':
    parser = argparse.ArgumentParser()
    parser.add_argument('-c', help='conf file')
    parser.add_argument('-t', help='choose csv or winlogbeat')
    parser.add_argument('-i', help='csv file')
    parser.add_argument('-start', help='start date from winlogbeat, like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

SysmonHunter – Rule definition

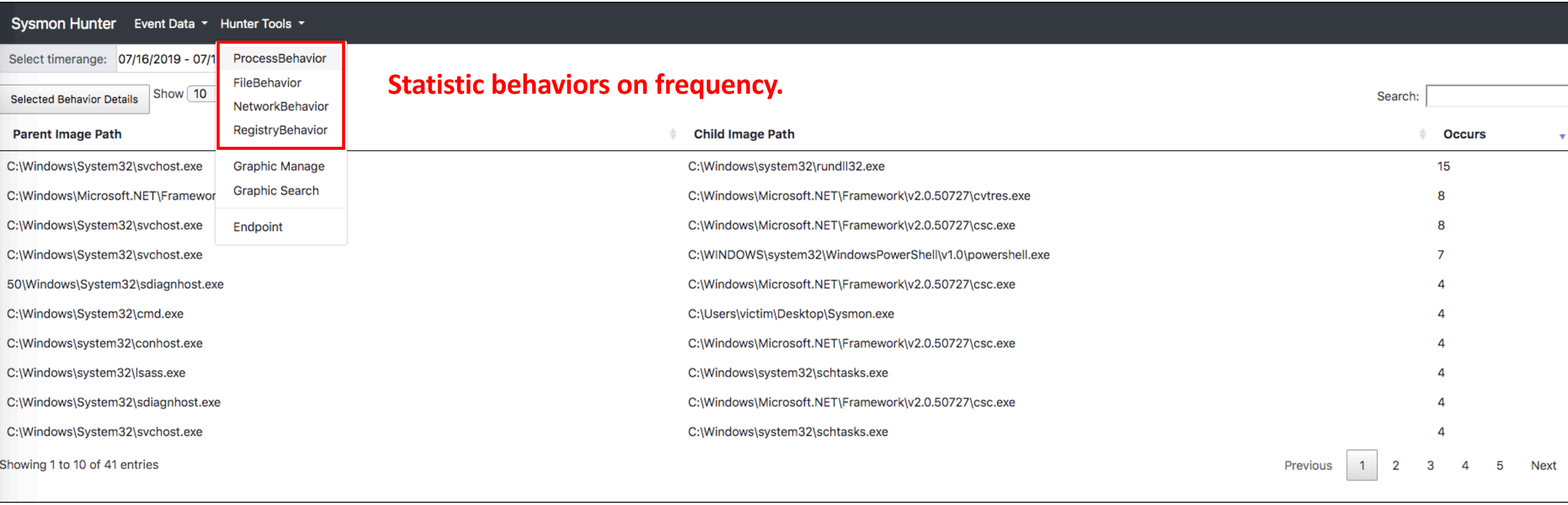
- YAML format
- logical expression
  - and, or, not
- match pattern
  - nocase/case, regex
- Format
  - Technique id
  - name, description, alert level, attack phase
  - query conditions



SysmonHunter

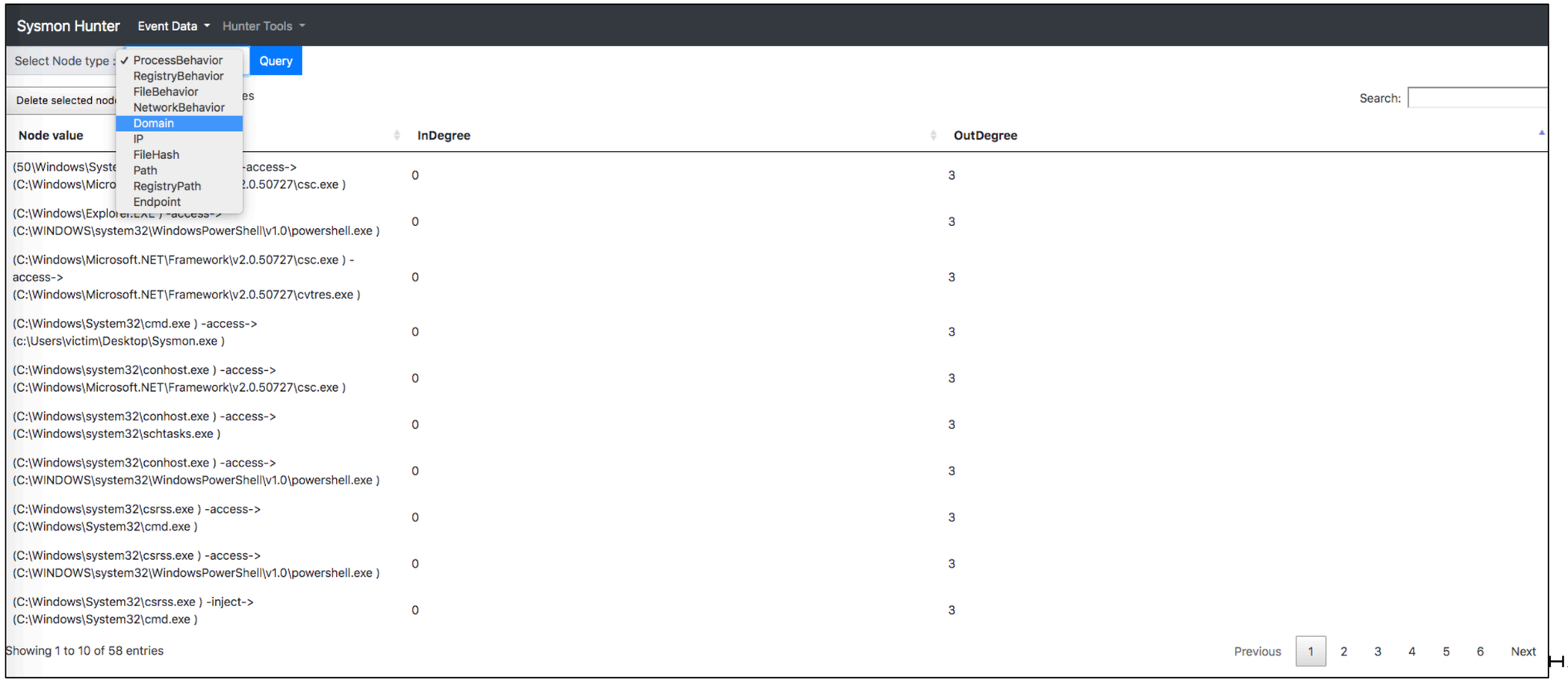


SysmonHunter – Statistic analysis

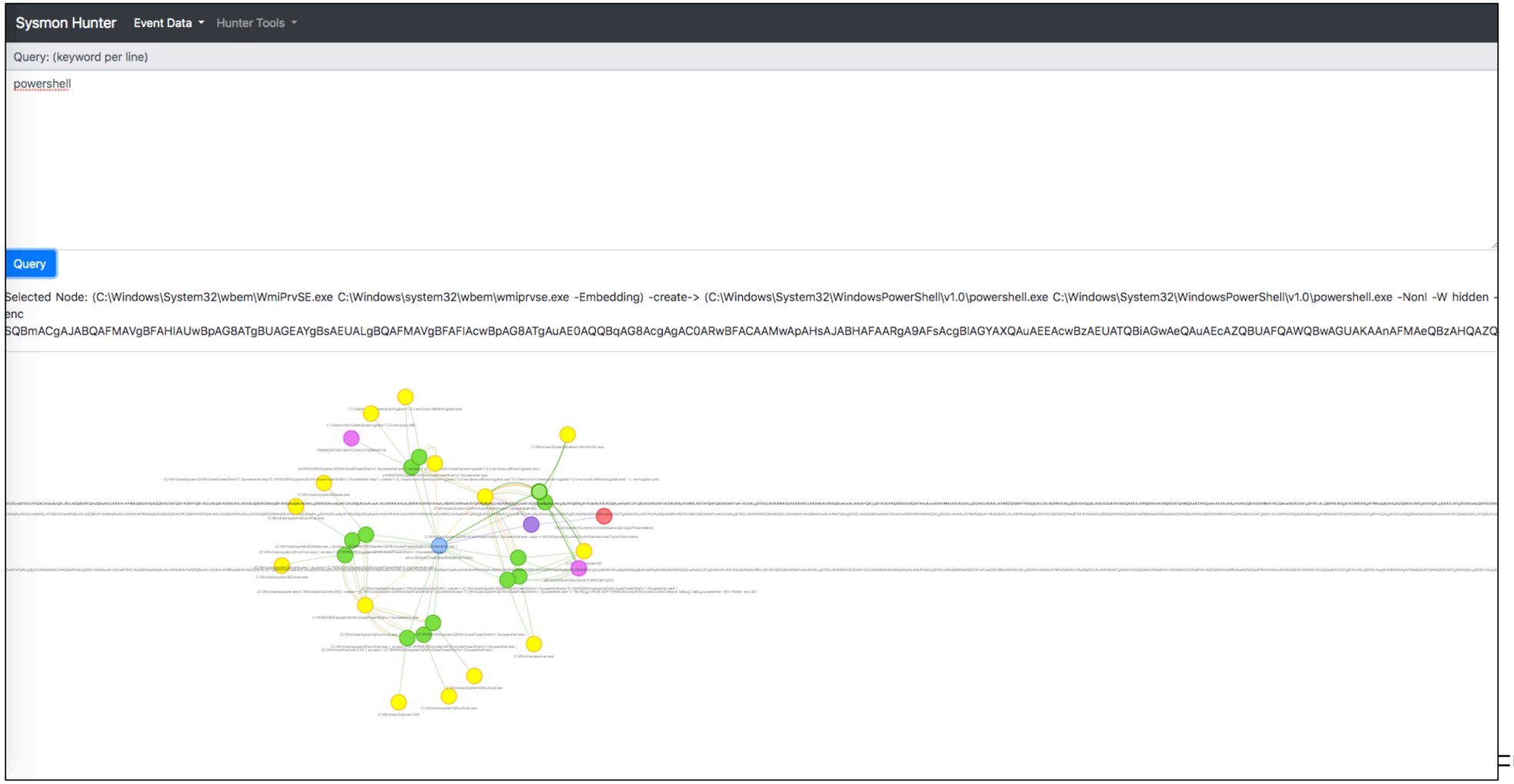


SysmonHunter – Graphic analysis

- Nodes in/out degrees



SysmonHunter – Graphic analysis



Test case 1

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

Test case 1

order by timestamp

UAC bypass

Show 100 entries Search: msc

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) C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -c $x=$((gp HKCU:Software\Microsoft\Windows Update).Update); powershell -NoP -NonI -W Hidden -enc $x
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) C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -c $x=$((gp HKCU:Software\Microsoft\Windows Update).Update); powershell -NoP -NonI -W Hidden -enc $x
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

Test case 2

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

Test case 2

mshta execution

Endpoint	Timestamp	BehaviorType	ATT&CK IDs	Value
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
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\WindowsPc SQBGACgAJABQAFMAVgBFAHIAUwBpAG8ATgBUAEEAYgBsAGUALgBQAFMAVgBlAHIAUwBJAG8ATgAuAE0AQQBqAG8AcgAgAC0AZwBFACAAMwApAHsAJAB
2019-07-				

Show 100 entries

Search: embedd

IE Dcom launch

Endpoint	Timestamp	BehaviorType	ATT&CK IDs	Value
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\WindowsPowe SQBGACgAJABQAFMAVgBlAHIAcwBJAE8AbgBUAGEAQgBMAEUALgBQAFMAVgBlAFIAUwBpAG8ATgAuAE0AQQBKAG8AcgAgAC0ARwBlACAAMwApAHsAJABHAF
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\WindowsPowe SQBGACgAJABQAFMAVgBlAHIAcwBJAE8AbgBUAGEAQgBMAEUALgBQAFMAVgBlAFIAUwBpAG8ATgAuAE0AQQBKAG8AcgAgAC0ARwBlACAAMwApAHsAJABHAF
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 Fi
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 Fi

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