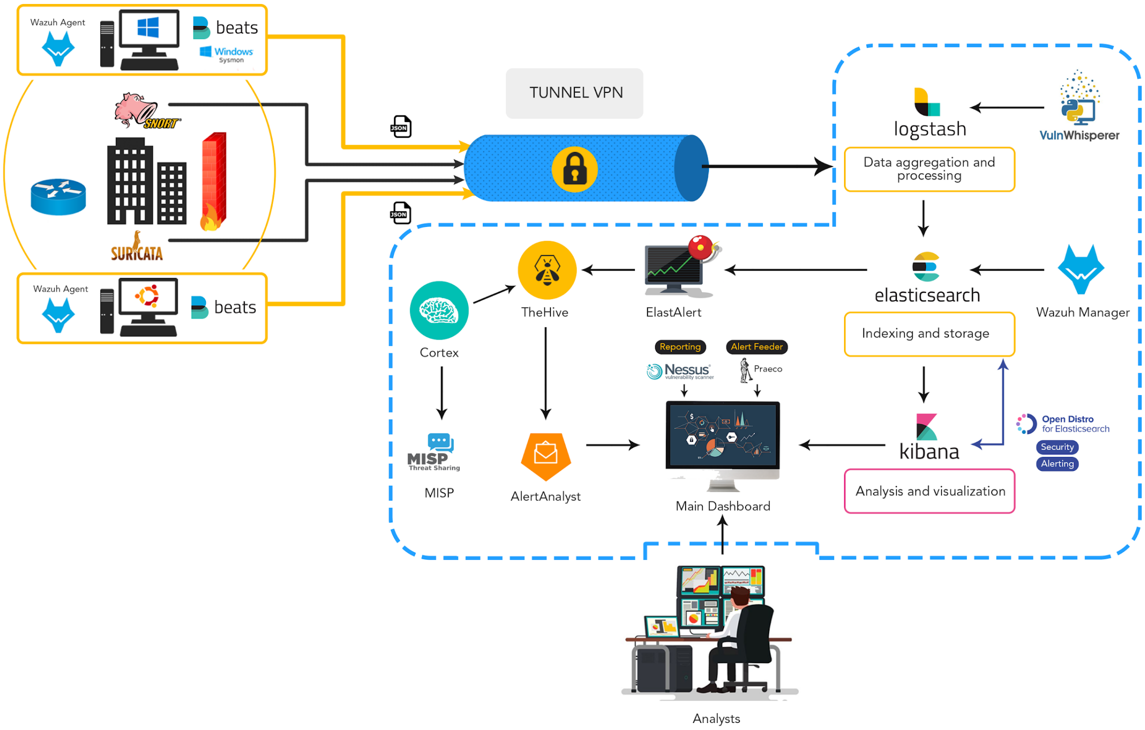
SCIENCES
SORBONNE
UNIVERSITÉ

Supervision Sécurité SIEM



Réalisé par : - **Yanis Alim**
- **Anastasia Cotorobai**

Dirigé par : **Tarek Radah**

Evaluation

1. **Citez la source de logs qui permet d'identifier les accès aux partages de fichiers.**

Microsoft-Windows-***Security***-Auditing est la source de logs qui permet d'identifier les accès aux partages de fichiers.

2. **Citez l'event id qui permet d'identifier les fichiers téléchargés depuis internet via un browser.**

Event id 15 (FileCreateStreamHash) : Cet événement est créé lorsqu'un flux de fichier est créé et génère des événements qui enregistrent le hachage du contenu du fichier auquel le flux est affecté (le flux sans nom), ainsi que le contenu du flux nommé. Il existe des variantes de logiciels malveillants qui suppriment leurs ***exécutables*** ou leurs paramètres de configuration via les ***téléchargements*** du ***navigateur***, et cet événement vise à capturer celui-ci en fonction du navigateur attachant un flux Zone.Identifier "mark of the web" stream.

3. **Donnez les règles de détection qui correspondent aux TTP (SIGMA,ES Rules) :**

- ***Contournement de l'UAC avec l'Event Viewer***

Après avoir compris la technique de contournement de l'UAC avec l'Event Viewer, on peut faire une règle sigma qui regroupe les 2 comportements (au niveau de registre ***HKCU\Software\Classes\mscfile\shell\open\command*** ou bien au niveau de processus ***eventvwr.exe*** qui va faire une requête au Microsoft Management Console (***mmc.exe)***

```
title: Bypass UAC using event viewer
description: Detect when UAC is bypass through eventviewer.exe technique
logsource:
       product: windows
       category: registry_event
detection:
       methregistry:
       TargetObject: 'HKU\\*\mscfile\shell\open\command'
       condition: methregistry
logsource:
       category: process_creation
       product: windows
detection:
       methprocess:
       ParentImage: '*\eventvwr.exe'
       filterprocess:
       Image: '*\mmc.exe'
       condition: methprocess and not filterprocess
```

```
(winlog.channel:Microsoft-Windows-Sysmon/Operational AND
((winlog.event_id:13 AND
winlog.eventdata.TargetObject:*HKEY_USERS\\*\\mscfile\\shell\\open\\command
*) OR (winlog.channel:Microsoft-Windows-Sysmon/Operational AND
(winlog.event_id:1 AND process.parent.executable:*eventvwr.exe) AND (NOT
(process.executable:*mmc.exe*)))))
```

- ***Un Reverse Shell***

La détection d’un reverse shell va être basé sur des mot clés utilisés dans des commandes et leurs arguments :

```
title: Suspicious Reverse Shell Command Line
description: Detects suspicious shell commands or program code that may be exected or used
in command line to establish a reverse shell
logsource:
        product: linux
detection:
        keywords:
                - 'BEGIN {s = "/inet/tcp/0/'
                - 'bash -i >& /dev/tcp/'
                - 'bash -i >& /dev/udp/'
                - 'sh -i >$ /dev/udp/'
                - 'sh -i >$ /dev/tcp/'
                - '&& while read line 0<&5; do'
                - '/bin/bash -c exec 5<>/dev/tcp/'
                - '/bin/bash -c exec 5<>/dev/udp/'
                - 'nc -e /bin/sh '
                - '/bin/sh | nc'
                - 'rm -f backpipe; mknod /tmp/backpipe p && nc '
                -
        ';socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,ine
        t_aton($i))))'
                - ';STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>;'
                - '/bin/sh -i <&3 >&3 2>&3'
                - 'uname -a; w; id; /bin/bash -i'
                - '$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);
        $stream.Write($sendbyte,0,$sendbyte.Length); $stream.Flush()};'
                -
        ";os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);os.putenv('HISTFI
        LE','/dev/null');"
                - '.to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
                - ';while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print'
                - "socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:"
                - 'rm -f /tmp/p; mknod /tmp/p p &&'
                - ' | /bin/bash | telnet '
                - ',echo=0,raw tcp-listen:'
                - 'nc -lvvp '
                - 'xterm -display 1'
        condition: keywords
```

```
title: Possible Bind or Reverse Shell via NetCat (Auditbeat For Linux)
status: stable
description: Detects possible bind or reverse shell via "classic" netcat tool. For
rule usage, you must be install auditbeat.
logsource:
  product: linux
  service: auditbeat
detection:
  netcat_shell:
    process.name:
    - netcat
    - nc
    network.direction:
    - listening
    - outbound
    - outgoing
  netcat_shell_args:
    process.name:
    - netcat
    - nc
    process.args:
    - -e
    - /bin/bash
    - /bin/sh
    - -nv
  condition: netcat_shell or netcat_shell_args
```

```
(process.name:("netcat" OR "nc") AND (network.direction:("listening" OR
"outbound" OR "outgoing") OR process.args:("\-e" OR "\/bin\/bash" OR
"\/bin\/sh" OR "\-nv")))
```

product: Windows:

```
message: *whoami* or winlog.event_data.ParentCommandLine: *wmic* or
winlog.event_data.CommandLine: (*cmd.exe* and "*>*") or
winlog.event_data.ParentCommandLine: (*cmd.exe* and "*>*")
winlog.event_data.CommandLine: *powershell* and
(winlog.event_data.CommandLine:(*-enc* OR *-EncodedCommand*) AND
winlog.event_data.CommandLine:("*-w hidden*" OR "*-window hidden*" OR
"*-windowstyle hidden*")) AND winlog.event_data.CommandLine:(*-noni* OR
*-noninteractive*)
```

- ***La technique T1170***

Mshta.exe est un utilitaire qui exécute les applications Microsoft HTML (HTA). Les TA sont des applications autonomes qui s'exécutent à l'aide des mêmes modèles et technologies d'Internet Explorer, mais en dehors du navigateur. Ce dernier va créer un ***processus (cmd.exe, wscript.exe, regsvr32.exe…***) qui vont donner main à l’attaquant pour exécuter des commandes sur le système de la victime.

```
title: MSHTA Spawning Windows Shell
description: Detects a Windows command line executable started from MSHTA

logsource:
       category: process_creation
       product: windows
detection:
       selection:
       ParentImage: '*\mshta.exe'
       Image:
                      - '*\cmd.exe'
                      - '*\powershell.exe'
                      - '*\wscript.exe'
                      - '*\cscript.exe'
                      - '*\sh.exe'
                      - '*\bash.exe'
                      - '*\reg.exe'
                      - '*\regsvr32.exe'
                      - '*\BITSADMIN*'
       condition: selection
```

```
winlog.event_data.Image: *mshta.exe and winlog.event_data.CommandLine:
mshta*
```

- ***La technique T1060***

Registry Run Keys / Startup Folder (T1060) : les clés d'exécution dans le registre et le dossier de démarrage dans le répertoire des utilisateurs sont des emplacements «old but gold» qui sont utilisés par les attaquants pour la persistance. L'ajout d'une entrée aux touches d'exécution ou la création d'un raccourci dans le dossier de démarrage suffit à exécuter du code malveillant lorsqu'un utilisateur se connecte.

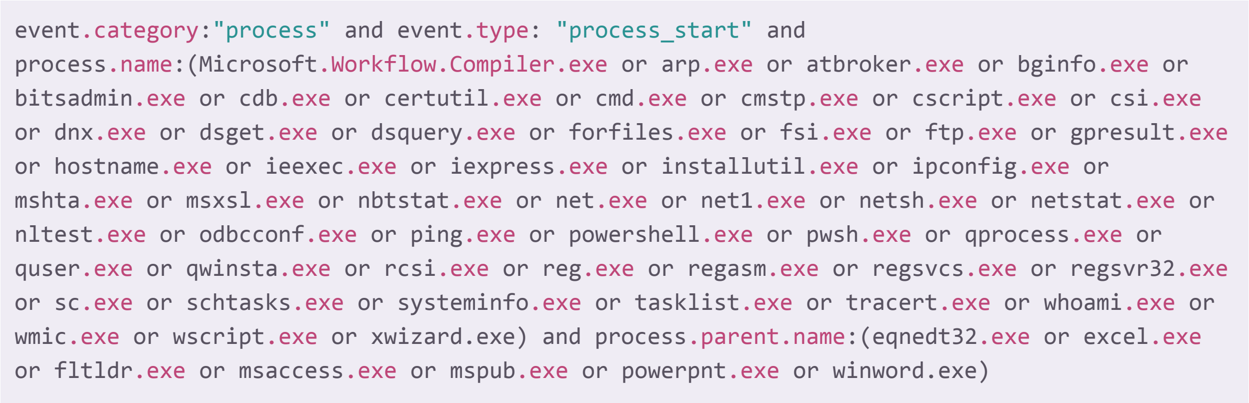
Soit-disons qu'il y a un malware qui veut ajouter un script (.exe, .vbs…) aux taches qui seront executés lors de la connexion de l'utilisateur :

```
title: Persistence via Windows Registry Run Keys with Visual Basic Scripting
status: experimental
description: Detects the addition of a visual basic script to the Windows Registry Run Key.
Adversaries may achieve persistence by adding a program to a Registry run key. Adding an
entry to the "run keys" in the Registry will cause the program referenced to be executed
when a user logs in.
logsource:
        product: windows
        service: security
detection:
        selection:
                EventID: 4688
                NewProcessName: '*\reg.exe'
                ProcessCommandLine|all:
                        - '*add*'
                        - '*.vbs*'
        selection1:
                ProcessCommandLine:
                        - '*\Software\Microsoft\Windows\CurrentVersion\Run*'
                        - '*\Software\Microsoft\Windows\CurrentVersion\RunOnce*'
                        - '*\Software\Microsoft\Windows\CurrentVersion\RunOnceEx*'
                        - '*\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce*'
                        - '*\Software\Microsoft\Windows\CurrentVersion\RunServices*'
                        - '*\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run*'
        condition: selection and selection1
```

```
winlog.event_data.RuleName: *RunKey* AND winlog.event_data.TargetObject:
(*\\Software\\Microsoft\\Windows\\CurrentVersion\\Run* OR
*\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\* OR
*\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\*)
```

- ***Exécution de macro suspicieux***

```
title: Microsoft Office Product Spawning Windows Shell
description: Detects a Windows command line executable started from Microsoft Word, Excel,
Powerpoint, Publisher and Visio.
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        ParentImage:
            - '*\WINWORD.EXE'
            - '*\EXCEL.EXE'
            - '*\POWERPNT.exe'
            - '*\MSPUB.exe'
            - '*\VISIO.exe'
            - '*\OUTLOOK.EXE'
        Image:
            - '*\cmd.exe'
            - '*\powershell.exe'
            - '*\wscript.exe'
            - '*\cscript.exe'
            - '*\sh.exe'
            - '*\bash.exe'
            - '*\scrcons.exe'
            - '*\schtasks.exe'
            - '*\regsvr32.exe'
            - '*\hh.exe'
            - '*\wmic.exe'
            - '*\mshta.exe'
            - '*\rundll32.exe'
            - '*\msiexec.exe'
            - '*\forfiles.exe'
            - '*\scriptrunner.exe'
            - '*\mftrace.exe'
            - '*\AppVLP.exe'
            - '*\svchost.exe'
    condition: selection
```



```
event.category:"process" and event.type: "process_start" and
process.name:(Microsoft.Workflow.Compiler.exe or arp.exe or atbroker.exe or bginfo.exe or
bitsadmin.exe or cdb.exe or certutil.exe or cmd.exe or cmstp.exe or cscript.exe or csi.exe
or dnx.exe or dsget.exe or dsquery.exe or forfiles.exe or fsi.exe or ftp.exe or gpresult.exe
or hostname.exe or ieexec.exe or iexpress.exe or installutil.exe or ipconfig.exe or
mshta.exe or msxsl.exe or nbtstat.exe or net.exe or net1.exe or netsh.exe or netstat.exe or
nltest.exe or odbcconf.exe or ping.exe or powershell.exe or pwsh.exe or qprocess.exe or
quser.exe or qwinsta.exe or rcsi.exe or reg.exe or regasm.exe or regsvcs.exe or regsvr32.exe
or sc.exe or schtasks.exe or systeminfo.exe or tasklist.exe or tracert.exe or whoami.exe or
wmic.exe or wscript.exe or xwizard.exe) and process.parent.name:(eqnedt32.exe or excel.exe
or fltldr.exe or msaccess.exe or mspub.exe or powerpnt.exe or winword.exe)
```

- ***Dump de la NTDS***

```
title: Activity Related to NTDS.dit Domain Hash Retrieval
description: Detects suspicious commands that could be related to activity that
uses volume shadow copy to steal and retrieve hashes from the NTDS.dit file
remotely
logsource:
    product: windows
    service: sysmon
detection:
    selection:
        EventID: 1
        CommandLine:
            - 'vssadmin.exe Delete Shadows'
            - 'vssadmin create shadow /for=C:'
            - 'copy \\?\GLOBALROOT\Device\*\windows\ntds\ntds.dit'
            - 'copy \\?\GLOBALROOT\Device\*\config\SAM'
            - 'vssadmin delete shadows /for=C:'
            - 'reg SAVE HKLM\SYSTEM '
    condition: selection
```

```
winlog.event_data.CommandLine :(*vssadmin* or *secretsdump* or *ntdsutil*
or *Invoke-NinjaCopy* or *ntds* or *copy*)
```

- ***Injection de Processus par MSBUILD***

```
title: Process Injection through MSBUILD
description: Detects a possible remote threat creation with MSBUILD
logsource:
  product: windows
  service: sysmon
detection:
  selection:
    EventID: 8
    Image :
          - '*\msbuild.exe'
    CommandLine:
          - 'CreateRemoteThread'
  condition: selection
```

```
process.name: *msbuild* and event.action:"CreateRemoteThread detected
(rule: CreateRemoteThread)"
```

4. **Donnez les règles de détection qui correspondent aux outils (SIGMA,ES Rules) :**

- ***Mimikatz***

```
title: Mimikatz Use
description: This method detects mimikatz keywords in different Eventlogs (some of
them only appear in older Mimikatz version that are however still used by different
threat groups)
logsource:
    product: windows
detection:
    keywords:
        - mimikatz
        - mimilib
        - <3 eo.oe
        - eo.oe.kiwi
        - privilege::debug
        - sekurlsa::logonpasswords
        - lsadump::sam
        - mimidrv.sys
    condition: keywords
```

```
*.keyword:(*mimikatz* OR *mimilib* OR *3 eo.oe* OR *eo.oe.kiwi* OR
*privilege::debug* OR *sekurlsa::logonpasswords* OR *lsadump::sam* OR
*mimidrv.sys*)
```

- ***PowerShell Dnscat2***

```
title: DNSCat2 Powershell Implementation Detection Via Process Creation
id: b11d75d6-d7c1-11ea-87d0-0242ac130003
status: experimental
description: The PowerShell implementation of DNSCat2 calls nslookup to craft
queries. Counting nslookup processes spawned by PowerShell will show hundreds or
thousands of instances if PS DNSCat2 is active locally.
logsource:
       category: process_creation
       product: windows
detection:
       selection:
       ParentImage|endswith: '*\powershell.exe'
       Image|endswith: '*\nslookup.exe'
       CommandLine|endswith: '*\nslookup.exe'
       condition: selection | count(Image) by ParentImage > 100
fields:
       - Image
       - CommandLine
       - ParentImage
falsepositives:
       - Other powershell scripts that call nslookup.exe
```

5. **A partir de cet article d'analyse de l'un des malwares de l'APT Turla, proposer une règle pour la détection du malware analysé :** https://www.nccgroup.com/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/

```
title: Turla PNG Dropper Service.
description: This method detects malicious services mentioned in Turla PNG dropper
report by NCC Group in November 2018.
logsource:
  product: windows
  service: system
detection:
  selection:
       EventID: 7045
       ServiceName: WerFaultSvc
  condition: selection
```

```
(winlog.event_id:7045 AND
winlog.event_data.ServiceName:/[Ww][Ee][Rr][Ff][Aa][Uu][Ll][Tt][Ss][Vv][Cc]
/)
```

6. **Donnez les règles de détections pour la suite des techniques suivante (SIGMA,ES Rules) :**

1. *Initial foothold (Using MSHTA Stager) - T1170*

```
title: Mshta JavaScript Execution
description: Identifies suspicious mshta.exe commands
logsource:
       category: process_creation
       product: windows
detection:
       selection:
       Image|endswith: '\mshta.exe'
       CommandLine|contains: 'javascript'
       condition: selection
```

```
winlog.event_data.Image : *mshta.exe and winlog.event_data.CommandLine :
*javascript*
```

2. *Local Recon - T1087*

https://blog.menasec.net/2019/02/threat-hunting-5-detecting-enumeration.html

```
title: AD Privileged Users or Groups Reconnaissance
description: Detect priv users or groups recon based on 4661 eventid and known
logsource:
       product: windows
       service: security
       definition: 'Requirements: enable Object Access SAM on your Domain
Controllers'
detection:
       selection:
       EventID: 4661
       ObjectType:
       - 'SAM_USER'
       - 'SAM_GROUP'
       ObjectName:
       - '*-512'
       - '*-502'
       - '*-500'
       - '*-505'
       - '*-519'
       - '*-520'
       - '*-544'
       - '*-551'
       - '*-555'
       - '*admin*'
```

```
      condition: selection
```

```
winlog.event_id: 4661 and winlog.user.type: ('SAM_USER' or 'SAM_GROUP') and
winlog.user.name: ("*-512" or "*-502" or "*-500" or "*-505" or "*-519" or
"*-520" or "*-544" or "*-551" or "*-555" or "*admin*")
```

3. *SAM Database dump – T1003*

```
title: SAM Dump to AppData
description: Detects suspicious SAM dump activity as cause by QuarksPwDump and
other password dumpers
logsource:
  product: windows
  service: system
  description: The source of this type of event is Kernel-General
detection:
  selection:
       EventID: 16
  keywords:
  - '*\AppData\Local\Temp\SAM-*.dmp *'
  condition: selection or keywords
```

```
 (winlog.event_id:16 AND "*\AppData\Local\Temp\SAM\-*.dmp\ *")
```

4. Pass-The-Hash - T1075

```
title: Pass the Hash Activity
description: 'Detects the attack technique pass the hash which is used to move
laterally inside the network'
logsource:
    product: windows
    service: security
    description: The successful use of PtH for lateral movement between
workstations would trigger event ID 4624, a failed logon attempt would trigger an
event ID 4625
detection:
    selection:
        - EventID: 4624
                LogonType: '3'
                LogonProcessName: 'NtLmSsp'
                WorkstationName: '%Workstations%'
                ComputerName: '%Workstations%'
        - EventID: 4625
                LogonType: '3'
                LogonProcessName: 'NtLmSsp'
                WorkstationName: '%Workstations%'
                ComputerName: '%Workstations%'
    filter:
        AccountName: 'ANONYMOUS LOGON'
    condition: selection and not filter
```

```
(winlog.channel:"Security" AND (winlog.event_data.LogonType:"3" AND
winlog.event_data.LogonProcessName:"NtLmSsp" AND
source.domain:"%Workstations%" AND winlog.ComputerName:"%Workstations%" AND
(winlog.event_id:"4624" OR winlog.event_id:"4625")) AND (NOT
(winlog.event_data.AccountName:"ANONYMOUS\ LOGON")))
```

5. LSASS memory dump – T1003

```
title: LSASS Memory Dump
description: Detects process LSASS memory dump using procdump or taskmgr based on
the CallTrace pointing to dbghelp.dll or dbgcore.dll for win10
logsource:
       category: process_access
       product: windows
detection:
       selection:
        EventID: 4656
       TargetImage: 'C:\windows\system32\lsass.exe'
       GrantedAccess: '0x1fffff'
       CallTrace:
       - '*dbghelp.dll*'
       - '*dbgcore.dll*'
       condition: selection
```

```
(winlog.channel:"Security" AND winlog.event_id:"4656" AND
process.executable:"C\:\Windows\System32\lsass.exe" AND
winlog.event_data.AccessMask:"0x1fffff" AND
winlog.event_data.ObjectType:"SAM_DOMAIN")
```

6. *Getting a domain admin account and attacking DC with PTH attack–T1075*

```
title: Pass the Hash Activity 2
description: Detects the attack technique pass the hash which is used to move
laterally inside the network
logsource:
       product: windows
       service: security
       definition: The successful use of PtH for lateral movement between
workstations would trigger event ID 4624
detection:
       selection:
              - EventID: 4624
                     SubjectUserSid: 'S-1-0-0'
                     LogonType: '3'
                     LogonProcessName: 'NtLmSsp'
                     KeyLength: '0'
              - EventID: 4624
                     LogonType: '9'
                     LogonProcessName: 'seclogo'
                     filter:
                     AccountName: 'ANONYMOUS LOGON'
       condition: selection and not filter
```

```
(winlog.channel:Security AND (winlog.event_id:4624 AND ((user.id:S\-1\-0\-0
AND winlog.event_data.LogonType:3 AND
winlog.event_data.LogonProcessName:/[Nn][Tt][Ll][Mm][Ss][Ss][Pp]/ AND
winlog.event_data.KeyLength:0) OR (winlog.event_data.LogonType:9 AND
winlog.event_data.LogonProcessName:/[Ss][Ee][Cc][Ll][Oo][Gg][Oo]/))) AND
(NOT (winlog.event_data.AccountName:/[Aa][Nn][Oo][Nn][Yy][Mm][Oo][Uu][Ss]\
[Ll][Oo][Gg][Oo][Nn]/)))
```

7. *NTDS Database dump – T1003*

```
title: Activity Related to NTDS.dit Domain Hash Retrieval
description: Detects suspicious commands that could be related to activity that
uses volume shadow copy to steal and retrieve hashes from the NTDS.dit file
remotely
logsource:
    product: windows
    service: sysmon
detection:
    selection:
        EventID: 1
        CommandLine:
            - 'vssadmin.exe Delete Shadows'
            - 'vssadmin create shadow /for=C:'
            - 'copy \\?\GLOBALROOT\Device\*\windows\ntds\ntds.dit'
            - 'copy \\?\GLOBALROOT\Device\*\config\SAM'
            - 'vssadmin delete shadows /for=C:'
            - 'reg SAVE HKLM\SYSTEM '
    condition: selection
fields:
    - CommandLine
    - ParentCommandLine
```

```
winlog.event_data.CommandLine :(*vssadmin* or *secretsdump* or *ntdsutil*
or *Invoke-NinjaCopy* or *ntds* or *copy*)
```

8. *Adding a user to domain admin group to achieve domain persistence - T1078*

```
title: User Added to Local Administrators
description: This rule triggers on user accounts that are added to the local
Administrators group, which could be legitimate activity or a sign of privilege
escalation
logsource:
      product: windows
      service: security
detection:
      selection:
      EventID: 4732
      selection_group1:
      GroupName: 'Administrators'
      selection_group2:
      GroupSid: 'S-1-5-32-544'
      filter:
      SubjectUserName: '*$'
      condition: selection and (1 of selection_group*) and not filter
```

```
(winlog.channel:Security AND (winlog.event_id:4732 AND
winlog.channel:Security AND (group.name:Administrators OR
winlog.event_data.GroupName:/[Aa][Dd][Mm][Ii][Nn][Ii][Ss][Tt][Rr][Aa][Tt][O
o][Rr][Ss]/ OR group.id:S-1-5-32-544 OR
winlog.event_data.GroupSid:S-1-5-32-544)) AND (NOT (user.name:*$)))
```

9. *Harvesting SSH credentials and connecting to a Linux server- T1005 + T1021*

```
title: Mimikatz Command Line
description: Detection of credential harvester using mimikatz
logsource:
       category: process_creation
       product: windows
detection:
       selection_1:
       CommandLine|contains:
              - DumpCreds
       selection_2:
       CommandLine|contains:
              - token
              - crypto
              - dpapi
              - sekurlsa
              - kerberos
              - lsadump
       selection_3:
       CommandLine|contains:
              - '::'
       condition: selection_1 or selection_2 and selection_3
```

```
(process.args:(/.*[Dd][Uu][Mm][Pp][Cc][Rr][Ee][Dd][Ss].*/) OR
(process.args:(/.*[Tt][Oo][Kk][Ee][Nn].*/ OR /.*[Cc][Rr][Yy][Pp][Tt][Oo].*/
OR /.*[Dd][Pp][Aa][Pp][Ii].*/ OR /.*[Ss][Ee][Kk][Uu][Rr][Ll][Ss][Aa].*/ OR
/.*[Kk][Ee][Rr][Bb][Ee][Rr][Oo][Ss].*/ OR
/.*[Ll][Ss][Aa][Dd][Uu][Mm][Pp].*/) AND process.args:(/.*\:\:.*/)))
```

```
title: Successful ssh
description: Detects a valid login in ssh service (password or publickey)
logsource:
       product: linux
       service: sshd
detection:
       keywords:
              - '*Accepted password for*'
              - '*Accepted publickey for*'
       condition: keywords
```

```
process.name: sshd and \*.keywords:("*Accepted\ password\ for*" OR
"*Accepted\ publickey\ for*")
```