Hunting Lateral Movement with Windows Events Logs

SANS Threat Hunting Summit 2018
Mauricio Velazco
@mvelazco
Peruvian

Recovering pentester, threat management lead

@mvelazco

Derbycon, Bsides, Defcon
1. Intro
Lateral Movement

Techniques that enable an adversary to access and control remote systems on a network.

https://attack.mitre.org/wiki/Lateral_Movement
Attackers are forced to move in the environment
How?

- Vulnerability Exploitation
- Logon Scripts
- Abusing application deployment software
- Removable media
- ……
- **Abusing Windows services/features**

“Out of all the incident response engagements that we conducted, 100% of them involved the threat actor compromising valid credentials during the attack.”

https://www.fireeye.com/blog/threat-research/2015/08/malware_lateral_move.html
Windows Services used for LM

- Server Message Block (SMB)
- Service Control Manager (SCM)
- Task Scheduler
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)
- Distributed Component Object Model (DCOM)
- Remote Desktop
<table>
<thead>
<tr>
<th>AppleScript</th>
<th>Application Deployment Software</th>
<th>DCOM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploitation</td>
<td>Logon Scripts</td>
<td>Pass the Hash</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote File Copy</td>
<td>Remote Services</td>
</tr>
<tr>
<td>Removable Media</td>
<td>SSH Hijacking</td>
<td>Shared WebRoot</td>
</tr>
<tr>
<td>Tainted Shared Content</td>
<td>Third party Software</td>
<td></td>
</tr>
<tr>
<td>Win RM</td>
<td>Windows Admin Shares (WMI, SCM, Task Sch)</td>
<td></td>
</tr>
</tbody>
</table>

https://attack.mitre.org/wiki/Lateral_Movement
2. The Events

KEEP CALM AND BELIEVE THAT BLUE TEAM ROCKS
**Authentication Events**

- Account Logon -> Credential validation
  Occurs on the host that is authoritative for the credentials

- Logon/Logoff -> Creation & Destruction of Sessions
  Occurs on the host being accessed

Kerberos

1. TGT Request
2. TGT
3. TGS Request
4. TGS

4768 - Authentication Ticket Requested
4769 - Service Ticket Requested
4624 - An account was successfully logged on
4625 - An account failed to log on
NTLM

1. Auth Request
2. Challenge
3. Response (Domain)
4. Response
5. Granted/denied

4624 - An account was successfully logged on
4625 - An account failed to log on
4776 - Credential Validation

Infected Host

Victim

DC

Account Logon
Logon/Logoff
Account Logon Events

4768: Auth Tkt Requested
- DC Name
- Account Name
- Source Ip
- Keywords

4769: Service Tkt Requested
- DC Name
- Account Name
- Service Name
- Client Address
- Keywords

4776: Credential Validation
- Computer Name
- Logon Account
- Source Workstation
- Error Code
Hunt Tip #1

✗ Source Ip requesting TGS for several computers \(\rightarrow\) Domain Controller Logs

\[
\text{Event}=4769 \text{ And } \\
\text{Service Name}=*\$
\text{group by (Client Address )} \\
\text{where unique(Service Name)} > [\text{Threshold}]
\]

✗ This behavior could represent

An adversary moving laterally ( or helpdesk deploying software) Host enumeration ( file share, PowerUp Sql, etc ) Bloodhound
Hunt Tip #2

✘ Possible Lateral Movement using NTLM → Domain Controller Logs

Event=4776 And (ComputerName=Dc1 Or …) group by (Source Workstation) Where unique(Computer Name) > [Threshold ]

✘ This behavior could represent:

An adversary moving laterally using NTLM based hacking tools like: metasploit, impacket, crackmapexec, smbexec, etc
Logon/Logoff Events

<table>
<thead>
<tr>
<th>4624</th>
<th>4625</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer Name</th>
<th>Account Name</th>
<th>Logon Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src Workstation Name</td>
<td>Src Network Address</td>
<td>Status</td>
</tr>
</tbody>
</table>

Sub Status
Hunt Tip #3:

❌ Possible Lateral Movement -> Computer Events

Event=4624 Or Event=4625 And
(Logon Type=3 Or Logon Type=10)
group by (Src Network Address)
Where unique(Computer Name) > [Threshold ]

❌ This behavior could represent:
An adversary moving laterally (or sysadmins working)
Password Spray / Brute Force Attack
BloodHound
Services and Tasks

✘ System Events
  7045: Service Installed

✘ Object Access
  4698: A scheduled task was created
TODO: WMI & WinRM

✗ WMI–Activity/Trace
  Event 1: Start of the event sequence
  Event 2: Actual Event
  Event 3: End of the event sequence

✗ Windows Remote Management
  Analytical
  Debug
  Operational
  169: User Authentication
Hunt Tip #4: EDR For The Win

✗ Services
  services.exe

✗ WMI
  wmiprsve.exe

✗ Windows Remote Management
  winrshost.exe
  wsmprovhost.exe

✗ DCOM – MMC20
  mmc.exe
Possible Lateral Movement execution → Sysmon Events

Event=1 And
(ParentImage=services.exe Or ParentImage=...) And
(Image=cmd.exe Or Image=powershell.exe OR
Image=mshta.exe Or Image=regsvr32.exe ...)

54 application whitelisting bypass techniques
https://github.com/api0cradle/UltimateAppLockerByPassList
3. Oriana
Oriana 1.0

Oriana is a threat hunting tool that leverages a subset of Windows events to run analytics and help defenders identify outliers and suspicious behavior in Windows environments.

- Get-WinEvent & Export-CSV
- Django Application, Python 2.7
- Bootstrap & DataTables
Hunt 1: Services and Tasks

- 7045 & 4698

- Frequency Analysis on
  - Unique Services
  - Unique Tasks

- Identify “Randomness” of
  - Service Name
  - Task Name
Hunt random: $N$-gram score

✗ Reg expressions are based on a sample and lack context
HunT 2: Possible Lateral Movement Event

4624
Type 3

4698

7045
Hunt 2: Possible Lateral Movement Session

✗ Assumption: Once access has been obtained, an attacker will profile or move laterally to more than one host.

Group possible lateral movement events based on time (X hour spans)
DEMO 2

NOT SURE IF TRICK
SHOW ME THE DEMO
Hunt 3: Outlier Users/Hosts

✘ User
  # of unique successful authentication events
  # of unique failed authentication events
  # of unique hosts a user has authenticated to locally
  # of unique hosts a user has authenticated to remotely
  # of unique hosts a user has remotely failed to authenticate
  # of unique hosts a user has RDP to

✘ Host
  # of unique users that authenticated to a host locally
  # of unique users that authenticated to a host remotely
DEMO 3

ENOUGH TALK
SHOW ME A DEMO!
Hunt 4: Suspicious User Behavior
<table>
<thead>
<tr>
<th>Status</th>
<th>SubStatus</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xC000006D</td>
<td>0xC000006A</td>
<td>Wrong password</td>
</tr>
<tr>
<td>0xc000015b</td>
<td>0x0</td>
<td>Acess denied</td>
</tr>
<tr>
<td>0xC000006D</td>
<td>0xC0000064</td>
<td>User does not exist</td>
</tr>
<tr>
<td>0xc000006e</td>
<td>0xc0000072</td>
<td>Account is disabled</td>
</tr>
</tbody>
</table>
SUB #1: PRIVILEGE ENUMERATION

✗ A user is failing to authenticate to a large number of hosts due to insufficient privileges for the requested logon type

✗ This behavior could represent
   - An adversary trying to execute remote commands (failing)
   - An adversary trying to mount an administrative share
   - An adversary enumerating privileges across the network
   - An adversary running BloodHound (with no admin privs)
SUB #2: HIGH NUMBER OF DESTINATIONS

✗ A user is successfully authenticating to a large number of hosts

✗ This behavior could represent:
  An adversary executing code remotely
  An adversary enumerating privileges across the network
  An adversary running BloodHound (with admin privs)
SUB #3 : Roaming User

✗ A user account is locally authenticating on several hosts

✗ This behavior could represent
   Compromised credentials usage
   Credential sharing
SUB #4: LOCAL ACCOUNT SPRAY

✘ A local user account is trying to authenticating to a large number of hosts.

✘ This behavior could represent
  An adversary moving laterally with a local account
  An adversary trying to brute force a local account
DEMO 4

ENOUGH TALK
SHOW ME THE DEMO!
Hunt 5: Suspicious Computer Behavior
https://github.com/mvelazc0/Oriana
Oriana 1.0

✘ https://github.com/mvelazco0/Oriana
   Standalone
   Docker!

✘ https://medium.com/@mvelazco/

✘ mauricio.velazco [at] gmail [dot] com

✘ @mvelazco
Hunting Lateral Movement with Windows Events Logs

SANS Threat Hunting Summit 2018
Mauricio Velazco
@mvelazco