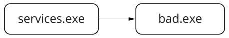
LATERAL MOVEMENT ANALYSIS CHEAT SHEET v1.0 by Huntsman

Lateral Movement Analysis Cheat Sheet for DFIR Team to analysis, investigation and response.

github.com/WirapongP   huntsman-dfir.medium.com

SERVICES

Detection



Investigation

Source Host & Compromised Account Name

Windows Event Logs (Security.evtx) - Event ID 4624
Logon Type == 3

- Network Information\Source Network Address
- New Logon\Account Name

Service Name & Service File Name

Windows Event Logs (System.evtx) - Event ID 7045

- Service Name
- Service File Name

Process Name & Process Command Line

Windows Event Logs (Security.evtx) - Event ID 4688
Creator Process Name == "Services.exe"

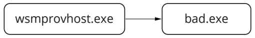
- Process Information\New Process Name
- Process Information\Process Commane Line

Eradication/Action

1. **Change Password of Compromised Account**
2. **Delete Service >sc delete [Service Name]**
   - SYSTEM\CurrentControlSet\Services\[Service Name]
3. **Kill Malware Process**
4. **Delete Malware File**
5. **Malware Analysis**
6. **Investigate at Source Host**

Powershell

Detection



Investigation

Source Host & Compromised Account Name

Windows Event Logs (Security.evtx) - Event ID 4624
Logon Type == 3

- Network Information\Source Network Address
- New Logon\Account Name

Process Name & Process Command Line

Windows Event Logs (Security.evtx) - Event ID 4688
Creator Process Name == "wsmprovhost.exe"

- Process Information\New Process Name
- Process Information\Process Commane Line

Scriptblock

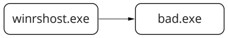
Windows Event Logs (Microsoft-Windows-PowerShell%4Operational.evtx) - Event ID 4103,4104

Eradication/Action

1. **Change Password of Compromised Account**
2. **Kill Malware Process**
3. **Delete Malware File**
4. **Malware Analysis**
5. **Investigate at Source Host**

WinRS

Detection



Investigation

Source Host & Compromised Account Name

Windows Event Logs (Security.evtx) - Event ID 4624
Logon Type == 3

- Network Information\Source Network Address
- New Logon\Account Name

Process Name & Process Command Line

Windows Event Logs (Security.evtx) - Event ID 4688
Creator Process Name == "winrshost.exe"

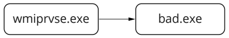
- Process Information\New Process Name
- Process Information\Process Commane Line

Eradication/Action

1. **Change Password of Compromised Account**
2. **Kill Malware Process**
3. **Delete Malware File**
4. **Malware Analysis**
5. **Investigate at Source Host**

WMI/WMIC

Detection



Investigation

Source Host & Compromised Account Name

Windows Event Logs (Security.evtx) - Event ID 4624
Logon Type == 3

- Network Information\Source Network Address
- New Logon\Account Name

Process Name & Process Command Line

Windows Event Logs (Security.evtx) - Event ID 4688
Creator Process Name == "wmiprvse.exe

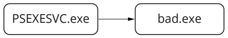
- Process Information\New Process Name
- Process Information\Process Commane Line

Eradication/Action

1. **Change Password of Compromised Account**
2. **Kill Malware Process**
3. **Delete Malware File**
4. **Malware Analysis**
5. **Investigate at Source Host**

PSExec

Detection



Investigation

Source Host & Compromised Account Name

Windows Event Logs (Security.evtx) - Event ID 4624
Logon Type == 3

- Network Information\Source Network Address
- New Logon\Account Name

Process Name & Process Command Line

Windows Event Logs (Security.evtx) - Event ID 4688
Creator Process Name == "PSEXESVC.exe"

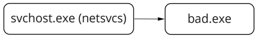
- Process Information\New Process Name
- Process Information\Process Commane Line

Eradication/Action

1. **Change Password of Compromised Account**
2. **Kill Malware Process**
3. **Delete Malware File**
4. **Malware Analysis**
5. **Investigate at Source Host**

Scheduled Tasks

Detection



Investigation

Source Host & Compromised Account Name

Windows Event Logs (Security.evtx) - Event ID 4624
Logon Type == 3

- Network Information\Source Network Address
- New Logon\Account Name

Process Name & Process Command Line

Windows Event Logs (Security.evtx) - Event ID 4688
Creator Process ID == [Process ID of svchost.exe -k netsvcs]

- Process Information\New Process Name
- Process Information\Process Commane Line

Task Name & Author

Windows Event Logs (Security.evtx) - Event ID 4698

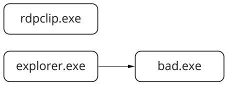
- Task Information\Task name
- RegistrationInfo\Author

Eradication/Action

1. **Change Password of Compromised Account**
2. **Delete task >schtasks /delete /tn [Task Name]**
   - C:\Windows\System32\Tasks
3. **Kill Malware Process**
4. **Delete Malware File**
5. **Malware Analysis**
6. **Investigate at Source Host**

RDP

Detection



Investigation

Source Host & Compromised Account Name

Windows Event Logs (Security.evtx) - Event ID 4624
Logon Type == 10

- Network Information\Source Network Address
- New Logon\Account Name

Process Name & Process Command Line

Windows Event Logs (Security.evtx) - Event ID 4688
Creator Process Name == "explorer.exe"

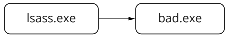
- Process Information\New Process Name
- Process Information\Process Commane Line

Eradication/Action

1. **Change Password of Compromised Account**
2. **Kill Malware Process**
3. **Delete Malware File**
4. **Malware Analysis**
5. **Investigate at Source Host**

Exploitation of Remote Services

Detection



Abnormal child/parent relationships
(Hunts evil poster - SANS)

Investigation

Process Name & Process Command Line

Windows Event Logs (Security.evtx) - Event ID 4688
Creator Process Name == "lsass.exe" OR [process of vuln. service]

- Process Information\New Process Name
- Process Information\Process Commane Line

Eradication/Action

1. **Change Password of Compromised Account**
2. **Kill Malware Process**
3. **Delete Malware File**
4. **Malware Analysis**
5. **Patch**
6. **Investigate at Source Host**