RDP forensic on src & dest

Remote Desktop Services: Source System Artifacts

If admins use remote desktop, expect attacker usage

- Most commonly Microsoft Remote Desktop (RDP)
- Also look for VNC, TeamViewer, etc. (if available in network)

EVENT LOGS

- `security.evtx`
  - **4648** – Logon specifying alternate credentials - if NLA enabled on destination
    - Current logged-on User Name
    - Alternate User Name
    - Destination Host Name/IP
    - Process Name
- `Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx`
  - **1024**
    - Destination Host Name
  - **1102**
    - Destination IP Address

REGISTRY

- Remote desktop destinations are tracked per-user
  - `NTUSER\Software\Microsoft\Terminal Server Client\Servers`
- ShimCache – `SYSTEM`
  - `mstsc.exe` Remote Desktop Client
- BAM/DAM – `SYSTEM` – Last Time Executed
  - `mstsc.exe` Remote Desktop Client
- `AmCache.hve` – First Time Executed
  - `mstsc.exe`
- UserAssist – `NTUSER.DAT`
  - `mstsc.exe` Remote Desktop Client execution
  - Last Time Executed
  - Number of Times Executed
- RecentApps – `NTUSER.DAT`
  - `mstsc.exe` Remote Desktop Client execution
  - Last Time Executed
  - Number of Times Executed
  - RecentItems subkey tracks connection destinations and times

FILE SYSTEM

- Jumplists – `C:\Users\<Username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\`
  - `{MSTSC-APPID}-automaticDestinations-ms`
  - Tracks remote desktop connection destination and times
- Prefetch – `C:\Windows\Prefetch\`
  - `mstsc.exe-{hash}.pf`
- Bitmap Cache – `C:\USERS\<USERNAME>\AppData\Local\Microsoft\Terminal Server Client\Cache`
  - `bcache##.bmc`
  - `cache####.bin`

Remote Desktop Services: Destination System Artifacts

Different artifacts on Source and Destination!

- Notice wealth of registry and file system info on Source
- Destination has more robust event log artifacts
  - * Event logs and IDs will be covered in more depth in next section

EVENT LOGS

- **Security Event Log** – `security.evtx`
  - **4624** Logon Type 10
    - Source IP/Logon User Name
  - **4778/4779**
    - IP Address of Source/Source System Name
    - Logon User Name
- `Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx`
  - **131** – Connection Attempts
    - Source IP
  - **98** – Successful Connections
- `Microsoft-Windows-Terminal Services-RemoteConnection Manager%4Operational.evtx`
  - **1149**
    - Source IP/Logon User Name
      - Blank user name may indicate use of Sticky Keys
- `Microsoft-Windows-Terminal Services-LocalSession Manager%4Operational.evtx`
  - **21, 22, 25**
    - Source IP/Logon User Name
  - **41**
    - Logon User Name

REGISTRY

- ShimCache – `SYSTEM`
  - `rdpclip.exe`
  - `tstheme.exe`
- `AmCache.hve` – First Time Executed
  - `rdpclip.exe`
  - `tstheme.exe`

FILE SYSTEM

- Prefetch – `C:\Windows\Prefetch\`
  - `rdpclip.exe-{hash}.pf`
  - `tstheme.exe-{hash}.pf`

Windows Admin Shares forensic on src & dest

Windows Admin Shares: Source System Artifacts

Mounting built-in shares is a simple and effective means of lateral movement: **C$** • **ADMIN$** • **IPC$**

```
net use z: \\host\c$ /user:domain\username <password>
```

EVENT LOGS

- **security.evtx**
  - **4648** – Logon specifying alternate credentials
    - Current logged-on User Name
    - Alternate User Name
    - Destination Host Name/IP
    - Process Name
- **Microsoft-Windows-SmbClient%4Security.evtx**
  - **31001** – Failed logon to destination
    - Destination Host Name
    - User Name for failed logon
    - Reason code for failed destination logon (e.g. bad password)

REGISTRY

- MountPoints2 – Remotely mapped shares
  - **NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2**
- Shellbags – **USRCLASS.DAT**
  - Remote folders accessed inside an interactive session via Explorer by attackers
- ShimCache – **SYSTEM**
  - **net.exe**
  - **net1.exe**
- BAM/DAM – **NTUSER.DAT** – Last Time Executed
  - **net.exe**
  - **net1.exe**
- **AmCache.hve** – First Time Executed
  - **net.exe**
  - **net1.exe**

FILE SYSTEM

- **Prefetch** – **C:\Windows\Prefetch**
  - **net.exe-{hash}.pf**
  - **net1.exe-{hash}.pf**
- User Profile Artifacts
  - Review shortcut files and jumplists for remote files accessed by attackers, if they had interactive access (RDP)

Windows Admin Shares: Destination System Artifacts

- Easy way to stage malware or access sensitive files
- Pass-the-hash attacks are common
- Vista+ requires domain admin or built-in admin rights

EVENT LOGS

- **Security Event Log** – **security.evtx**
  - **4624** Logon Type 3
    - Source IP/Logon User Name
  - **4672**
    - Logon User Name
    - Logon by user with administrative rights
    - Requirement for accessing default shares such as **C$** and **ADMIN$**
  - **4776** – NTLM if authenticating to Local System
    - Source Host Name/Logon User Name
  - **4768** – TGT Granted
    - Source Host Name/Logon User Name
    - Available only on domain controller
  - **4769** – Service Ticket Granted if authenticating to Domain Controller
    - Destination Host Name/Logon User Name
    - Source IP
    - Available only on domain controller
  - **5140**
    - Share Access
  - **5145**
    - Auditing of shared files – NOISY!

REGISTRY

FILE SYSTEM

- File Creation
  - Attacker's files (malware) copied to destination system
  - Look for Modified Time before Creation Time
  - Creation Time is time of file copy

PsExec forensic on src & dest

PsExec: Source System Artifacts

- Lightweight, remote execution tool provided by Microsoft
  - PsExec is not a default application
- Often used for both legitimate and nefarious deeds (on same network)

```
psexec.exe \\host -accepteula -d -c c:\temp\evil.exe
```

EVENT LOGS

- **security.evtx**
  - **4648** – Logon specifying alternate credentials
    - Current logged-on User Name
    - Alternate User Name
    - Destination Host Name/IP
    - Process Name

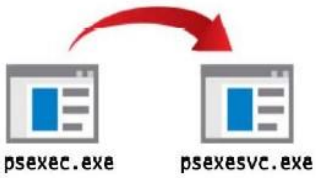
REGISTRY

- **NTUSER.DAT**
  - **Software\SysInternals\PsExec\EulaAccepted**
- ShimCache – **SYSTEM**
  - **psexec.exe**
- BAM/DAM – **SYSTEM** – Last Time Executed
  - **psexec.exe**
- **AmCache.hve** – First Time Executed
  - **psexec.exe**

FILE SYSTEM

- Prefetch – **C:\Windows\Prefetch**
  - **psexec.exe-{hash}.pf**
  - Possible references to other files accessed by psexec.exe, such as executables copied to target system with the "**-c**" option
- File Creation
  - **psexec.exe** file downloaded and created on local host as the file is not native to Windows

PsExec: Destination System Artifacts



- ✓ Authenticates to destination system
- ✓ Named pipes are used to communicate between source and target
- ✓ Mounts hidden **ADMIN$** share
- ✓ Copies **PsExeSvc.exe** and any other binaries to Windows folder
- ✓ Executes code via a service (**PSEXESVC**)

EVENT LOGS

- **security.evtx**
  - **4624** Logon Type 3 (and Type 2 if "**-u**" Alternate Credentials are used)
    - Source IP/Logon User Name
  - **4672**
    - Logon User Name
    - Logon by a user with administrative rights
    - Requirement for access default shares such as **C$** and **ADMIN$**
  - **5140** – Share Access
    - **ADMIN$** share used by PsExec
- **system.evtx**
  - **7045**
    - Service Install

REGISTRY

- New service creation configured in **SYSTEM\CurrentControlSet\Services\PSEXESVC**
  - "**-r**" option can allow attacker to rename service
- ShimCache – **SYSTEM**
  - **psexesvc.exe**
- **AmCache.hve**
  - **psexesvc.exe**

FILE SYSTEM

- Prefetch – **C:\Windows\Prefetch**
  - **psexesvc.exe-{hash}.pf**
  - **evil.exe-{hash}.pf**
- File Creation
  - User profile directory structure created unless "**-e**" option used
  - **psexesvc.exe** will be placed in ADMIN$ (\Windows) by default, as well as other executables (evil.exe) pushed by PsExec

Windows Remote Management Tools

Windows includes many tools capable of remote execution

- Create and start remote service

```
sc \\host create servicename binpath= "c:\temp\evil.exe"
sc \\host start servicename
```

- Remotely schedule tasks

```
at \\host 13:00 "c:\temp\evil.exe"
schtasks /CREATE /TN taskname /TR C:\evil.exe /SC once /RU "SYSTEM" /ST 13:00 /S host /U user
```

- Interact with remote registries

```
reg add \\host\HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v Data /t REG_SZ /d "C:\evil.exe"
```

- Execute any remote command

```
winrs -r:host -u:user command
```

Windows Remote Management Tools: Remote Services

Remote Services Source System Artifacts

EVENT LOGS	REGISTRY	FILE SYSTEM
	■ ShimCache – `SYSTEM` • `sc.exe` ■ BAM/DAM – `SYSTEM` – Last Time Executed • `sc.exe` ■ `AmCache.hve` – First Time Executed • `sc.exe`	■ Prefetch – `C:\Windows\Prefetch\` • `sc.exe-{hash}.pf`

Remote Services Destination System Artifacts

EVENT LOGS		REGISTRY	FILE SYSTEM
■ `security.evtx` • **4624** Logon Type 3 – Source IP/Logon User Name • **4697** – Security records service install, if enabled – Enabling non-default Security events such as ID 4697 are particularly useful if only the Security logs are forwarded to a centralized log server	■ `system.evtx` • **7034** – Service crashed unexpectedly • **7035** – Service sent a Start/Stop control • **7036** – Service started or stopped • **7040** – Start type changed (`Boot | On Request | Disabled`) • **7045** – A service was installed on the system	■ `SYSTEM` • `\CurrentControlSet\Services\` • New service creation ■ ShimCache – `SYSTEM` • `evil.exe` • ShimCache records existence of malicious service executable, unless implemented as a service DLL ■ `AmCache.hve` – First Time Executed • `evil.exe`	■ File Creation • `evil.exe` or `evil.dll` malicious service executable or service DLL ■ Prefetch – `C:\Windows\Prefetch\` • `evil.exe-{hash}.pf`

Windows Remote Management Tools: Scheduled Tasks

Scheduled Task Source System Artifacts

EVENT LOGS

- `security.evtx`
  - **4648** – Logon specifying alternate credentials
    - Current logged-on User Name
    - Alternate User Name
    - Destination Host Name/IP
    - Process Name

REGISTRY

- ShimCache – `SYSTEM`
  - `at.exe`
  - `schtasks.exe`
- BAM/DAM – `SYSTEM` – Last Time Executed
  - `at.exe`
  - `schtasks.exe`
- `AmCache.hve` - First Time Executed
  - `at.exe`
  - `schtasks.exe`

FILE SYSTEM

- Prefetch – `C:\Windows\Prefetch\`
  - `at.exe-{hash}.pf`
  - `schtasks.exe-{hash}.pf`

Scheduled Task Destination System Artifacts

EVENT LOGS

- `security.evtx`
  - **4624** Logon Type 3
    - Source IP/Logon User Name
  - **4672**
    - Logon User Name
    - Logon by a user with administrative rights
    - Requirement for accessing default shares such as `C$` and `ADMIN$`
  - **4698** – Scheduled task created
  - **4702** – Scheduled task updated
  - **4699** – Scheduled task deleted
  - **4700/4701** – Scheduled task enabled/disabled
- `Microsoft-Windows-TaskScheduler%4Operational.evtx`
  - **106** – Scheduled task created
  - **140** – Scheduled task updated
  - **141** – Scheduled task deleted
  - **200/201** – Scheduled task executed/completed

REGISTRY

- `SOFTWARE`
  - `Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks`
  - `Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\`
- ShimCache – `SYSTEM`
  - `evil.exe`
- `AmCache.hve` – First Time Executed
  - `evil.exe`

FILE SYSTEM

- File Creation
  - `evil.exe`
  - Job files created in `C:\Windows\Tasks`
  - XML task files created in `C:\Windows\System32\Tasks`
    - Author tag under "RegistrationInfo" can identify:
      - Source system name
      - Creator username
- Prefetch – `C:\Windows\Prefetch\`
  - `evil.exe-{hash}.pf`

WMI forensic on src & dest

WMI: Source System Artifacts

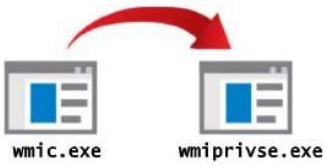
```
wmic /node:host /user:user process call create "c:\temp\evil.exe"
Invoke-WmiMethod - Computer host -Class Win32_Process -Name create - Argument "C:\evil.exe"
```

- One of the most powerful lateral movement options and one of the most difficult to investigate
- WMI is native to every modern Windows system
  *PowerShell will be covered separately
- Source system artifacts are sparse

EVENT LOGS	REGISTRY	FILE SYSTEM
■ `security.evtx` • **4648** – Logon specifying alternate credentials - Current logged-on User Name - Alternate User Name - Destination Host Name/IP - Process Name	■ ShimCache – `SYSTEM` • `wmic.exe` ■ BAM/DAM – `SYSTEM` – Last Time Executed • `wmic.exe` ■ `AmCache.hve` – First Time Executed • `wmic.exe`	■ Prefetch – `C:\Windows\Prefetch\` • `wmic.exe-{hash}.pf`

WMI: Destination System Artifacts

- WMI activity has long been a blind spot
  - **`wmiprvse.exe`** is a strong indication
  - The new **`Microsoft-Windows-WMI-Activity/Operational`** log is a game changer
  - Look for residue left from WMI event consumers



EVENT LOGS		REGISTRY	FILE SYSTEM
■ `security.evtx` • **4624** Logon Type 3 - Source IP/Logon User Name • **4672** - Logon User Name - Logon by an a user with administrative rights	■ `Microsoft-Windows-WMI-Activity%4Operational.evtx` • **5857** - Indicates time of wmiprvse execution and path to provider DLL – attackers sometimes install malicious WMI provider DLLs • **5860, 5861** - Registration of Temporary (5860) and Permanent (5861) Event Consumers. Typically used for persistence, but can be used for remote execution.	■ ShimCache – `SYSTEM` • `scrcons.exe` • `mofcomp.exe` • `wmiprvse.exe` • `evil.exe` ■ `AmCache.hve` – First Time Executed • `scrcons.exe` • `mofcomp.exe` • `wmiprvse.exe` • `evil.exe`	■ File Creation • `evil.exe` • `evil.mof` – .mof files can be used to manage the WMI Repository ■ Prefetch – `C:\Windows\Prefetch\` • `scrcons.exe-{hash}.pf` • `mofcomp.exe-{hash}.pf` • `wmiprvse.exe-{hash}.pf` • `evil.exe-{hash}.pf` ■ Unauthorized changes to the WMI Repository in `C:\Windows\System32\wbem\Repository`

PowerShell forensic

PowerShell Remoting: Source System Artifacts

- Look for evidence of **`powershell.exe`** execution
- PowerShell v5 (Win10) introduced improved logging

```
Enter-PSSession -ComputerName host
Invoke-Command -ComputerName host -ScriptBlock {Start-Process c:\temp\evil.exe}
```

EVENT LOGS

- `security.evtx`
  - **4648** – Logon specifying alternate credentials
    - Current logged-on User Name
    - Alternate User Name
    - Destination Host Name/IP
    - Process Name
- `Microsoft-Windows-WinRM%4Operational.evtx`
  - **6** – WSMan Session initialize
    - Session created
    - Destination Host Name or IP
    - Current logged-on User Name
  - **8, 15, 16, 33** – WSMan Session deinitialization
    - Closing of WSMan session
    - Current logged-on User Name
- `Microsoft-Windows-PowerShell%4Operational.evtx`
  - **40691, 40692**
    - Records the local initiation of powershell.exe and associated user account
  - **8193** & **8194**
    - Session created
  - **8197** - Connect
    - Session closed

REGISTRY

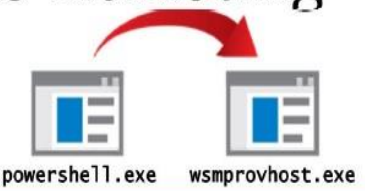
- ShimCache – `SYSTEM`
  - `powershell.exe`
- BAM/DAM – `SYSTEM` – Last Time Executed
  - `powershell.exe`
- `AmCache.hve` – First Time Executed
  - `powershell.exe`

FILE SYSTEM

- Prefetch – `C:\Windows\Prefetch\`
  - `powershell.exe-{hash}.pf`
  - PowerShell scripts (.ps1 files) that run within 10 seconds of powershell.exe launching will be tracked in powershell.exe prefetch file
- Command history `C:\USERS\<USERNAME>\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt`
  - With PS v5+, a history file with previous 4096 commands is maintained per user

PowerShell Remoting: Destination System Artifacts

- **`wsmprovhost.exe`** is good indicator of PS Remoting
- Full script logging is available in PSv5
  - Blocklisted cmdlets are logged by default



EVENT LOGS

- `security.evtx`
  - **4624** Logon Type 3
    - Source IP/Logon User Name
  - **4672**
    - Logon User Name
    - Logon by an a user with administrative rights
- `Microsoft-Windows-PowerShell%4Operational.evtx`
  - **4103, 4104** – Script Block logging
    - Logs suspicious scripts by default in PS v5
    - Logs all scripts if configured
  - **53504** Records the authenticating user
- `Windows PowerShell.evtx`
  - **400/403** "ServerRemoteHost" indicates start/end of Remoting session
  - **800** Includes partial script code
- `Microsoft-Windows-WinRM%4Operational.evtx`
  - **91** Session creation
  - **168** Records the authenticating user

REGISTRY

- ShimCache – `SYSTEM`
  - `wsmprovhost.exe`
  - `evil.exe`
- `SOFTWARE`
  - `Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy`
    - Attacker may change execution policy to a less restrictive setting, such as "bypass"
- `AmCache.hve` – First Time Executed
  - `wsmprovhost.exe`
  - `evil.exe`

FILE SYSTEM

- File Creation
  - `evil.exe`
  - With `Enter-PSSession`, a user profile directory may be created
- Prefetch – `C:\Windows\Prefetch\`
  - `evil.exe-{hash].pf`
  - `wsmprovhost.exe-{hash].pf`