Sign in

jsecurity101 / MSRPC-to-ATTACK Public

Notifications Fork 40 Star 307

Code Issues Pull requests Actions Projects Security Insights

MSRPC-to-ATTACK / documents / MS-WKST.md

58 lines (41 loc) · 2.21 KB

Preview Code Blame Raw

Protocol:

- Workstation Service Remote Protocol (MS-WKST)

Interface UUID:

- `6BFFD098-A112-3610-9833-46C3F87E345A`

Server Binary:

- `wkssvc.dll` (loads into) `svchost.exe`

Endpoint:

- ncacn_np: `\PIPE\wkssvc`

ATT&CK Relation:

- T1087 - Account Discovery

- User Logon Enumeration

Indicator of Activity (IOA):

- Network:
  - Inbound network connections to System over port 445
  - Methods:
    - `NetrWkstaGetInfo`
    - `NetrWkstaUserEnum`
  - Network connection to pipe `\pipe\wkssvc`
- Host:
  - 5145 (Detailed Network File Share) Event to
    - Share Name: `IPC$`
    - Relative Target - `\pipe\wkssvc`
    - Look at the user who made the connection
    - Access Request Information: Access Mask (`0x3` or higher) (`ReadData or ListDirectory + WriteData or AddFile`)
    - BH has been seen to have the hardcoded rights: `0x12019f` (`READ_CONTROL, SYNCHRONIZE,  ReadData (or ListDirectory), WriteData (or AddFile), AppendData (or AddSubdirectory or CreatePipeInstance), ReadEA, WriteEA , ReadAttributes, WriteAttributes`)

Prevention Opportunities:

- Prevent relay attacks by enabling SMB signing:
  - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters\RequireSecuritySignature = 1`
  - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters\EnableSecuritySignature = 1`
- MSFT link for guidance: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing

Notes:

- RPC filter doesn't exist for this interface due to the unknowings of other technologies that could be leveraging MS-WKST.
- Service Name: Lanman Workstation
- Often seen with BH activity for user enumeration.
- Look for connection to named pipe (both client and server)
- Protocol was built to facilitate remote tasks on a host, such as:
  - SMB network redirector configuration
  - Manage domain memberships
  - Return information related to user logins and enabled transports
- In order to run successfully - requester must have administrator rights

Useful Resources: