.. /rcsi.exe

Execute AWL bypass

Non-Interactive command line inerface included with Visual Studio.

Paths:
no default

Resources:

- https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/

Acknowledgements:

- Matt Nelson (@enigma0x3)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_csi_execution.yml
- Elastic: https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml
- Elastic: https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml
- BlockRule: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_csi_execution.yml

Execute

Use embedded C# within the csx script to execute the code.

```
rcsi.exe bypass.csx
```

Use case:	Local execution of arbitrary C# code stored in local CSX file.
Privileges required:	User
Operating systems:	Windows
ATT&CK® technique:	T1127

AWL bypass

Use embedded C# within the csx script to execute the code.

```
rcsi.exe bypass.csx
```

Use case: Local execution of arbitrary C# code stored in local CSX file.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1127