.. /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: proc_creation_win_csi_execution.yml
- Elastic: defense_evasion_unusual_process_network_connection.toml
- Elastic: defense_evasion_network_connection_from_windows_binary.toml
- BlockRule: 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: Trusted Developer Utilities Proxy Execution

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: Trusted Developer Utilities Proxy Execution