CLEANTOAD (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 12:51:26 UTC

win.cleantoad (Back to overview)

CLEANTOAD

Actor(s): Lazarus Group

CLEANTOAD is a disruption tool that will delete file system artifacts, including those related to BLINDTOAD, and will run after a date obtained from a configuration file. The malware injects shellcode into notepad.exe and it overwrites and deletes files, modifies registry keys, deletes services, and clears Windows event logs.

References

2018-01-01 · FireEye · FireEye
APT38
CHEESETRAY CLEANTOAD NACHOCHEESE

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.cleantoad