STEELCORGI (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:17:35 UTC

STEELCORGI

According to FireEye, STEELCORGI is a packer for Linux ELF files that makes use of execution guardrails by sourcing decryption key material from environment variables.

References

2022-03-16 · Mandiant · Joshua Homan, Logeswaran Nadarajan, Martin Co, Mathew Potaczek, Sylvain Hirsch, Takahiro Sugiyama, Yu Nakamura
Have Your Cake and Eat it Too? An Overview of UNC2891
SLAPSTICK STEELCORGI LightBasin

2021-01-12 · Yoroi · Antonio Pirozzi, Luca Mella, Luigi Martire
Opening “STEELCORGI”: A Sophisticated APT Swiss Army Knife
STEELCORGI

2020-11-02 · FireEye · Adrian Pisarczyk, Antonio Monaca, Daniel Caban, Daniel Susin, Justin Moore, Luis Rocha, Sara Rincon, Wojciech Ledzion
Live off the Land? How About Bringing Your Own Island? An Overview of UNC1945
SLAPSTICK STEELCORGI

There is no Yara-Signature yet.
