Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:21:39 UTC

Tool: STEELCORGI

Names	STEELCORGI
Category	Malware
Type	Dropper
Description	(FireEye) STEELCORGI is a packer for Linux ELF programs that uses key material from the executing environment to decrypt the payload. When first starting up, the malware expects to find up to four environment variables that contain numeric values. The malware uses the environment variable values as a key to decrypt additional data to be executed.
Information	<https://www.mandiant.com/resources/live-off-the-land-an-overview-of-unc1945> <https://yoroi.company/research/opening-steelcorgi-a-sophisticated-apt-swiss-army-knife/> <https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.steelcorgi>

Last change to this tool card: 05 April 2022

Download this tool card in JSON format

All groups using tool STEELCORGI

Changed	Name	Country	Observed	
APT groups				
	LightBasin		2016	
	UNC2891	[Unknown]	2020	

2 groups listed (2 APT, 0 other, 0 unknown)