Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:28:13 UTC

Tool: SprySOCKS

Names	SprySOCKS
Category	Malware
Type	Backdoor
Description	(Trend Micro) Analysis of the SprySOCKS backdoor reveals some interesting findings. The backdoor contains a marker that refers to the backdoor's version number. We have identified two SprySOCKS payloads that contain two different version numbers, indicating that the backdoor is still under development. In addition, we noticed that the implementation of the interactive shell is likely inspired from the Linux variant of the Derusbi malware. Meanwhile, the structure of SprySOCKS's command-and-control (C&C) protocol is similar to one used by the RedLeaves backdoor, a remote access trojan (RAT) reported to be infecting Windows machines. It consists of two components, the loader and the encrypted main payload. The loader is responsible for reading, decrypting, and running the main payload.
Information	<https://www.trendmicro.com/en_us/research/23/i/earth-lusca-employs-new-linux-backdoor.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.spry_socks>

Last change to this tool card: 13 October 2023

Download this tool card in JSON format

All groups using tool SprySOCKS

Changed	Name	Country	Observed	
APT groups				
	Earth Lusca		2019-Sep 2024	

	RedHotel, TAG-22		2021-2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=13243f5b-af8f-4cca-92d0-fda5be8c437a