Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:42:43 UTC

Tool: EVILSUN

Names	EVILSUN
Category	Exploits
Description	(FireEye) EVILSUN is a remote exploitation tool that gains access to Solaris 10 and 11 systems of SPARC or i386 architecture using a vulnerability (CVE-2020-14871) exposed by SSH keyboard-interactive authentication. The remote exploitation tool makes SSH connections to hosts passed on the command line. The default port is the normal SSH port (22), but this may be overridden. EVILSUN passes the banner string SSH-2.0-Sun_SSH_1.1.3 over the connection in clear text as part of handshaking.
Information	<https://www.mandiant.com/resources/live-off-the-land-an-overview-of-unc1945>

Last change to this tool card: 03 April 2022

Download this tool card in JSON format

All groups using tool EVILSUN

Changed	Name	Country	Observed	
APT groups				
	LightBasin		2016	

1 group listed (1 APT, 0 other, 0 unknown)