Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:06:34 UTC

Tool: VEILEDSIGNAL

Names	VEILEDSIGNAL
Category	Malware
Type	Backdoor
Description	(Mandiant) SIGFLIP and DAVESHELL extract and execute a modular backdoor, VEILEDSIGNAL, and two corresponding modules. VEILEDSIGNAL relies on the two extracted modules for process injection and communications with the Command and Control (C2) server. VEILEDSIGNAL and the accompanying two components provide the following functionality: • The VEILEDSIGNAL backdoor supports three commands: send implant data, execute shellcode, and terminate itself. • The process injection module injects the C2 module in the first found process instance of Chrome, Firefox, or Edge. It also monitors the named pipe and reinjects the communication module if necessary. • The C2 module creates a Windows named pipe and listens for incoming communications, which it then sends to the C2 server encrypted with AES-256 in Galois Counter Mode (GCM).
Information	<https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.veiledsignal>

Last change to this tool card: 13 October 2023

Download this tool card in JSON format

All groups using tool VEILEDSIGNAL

Changed	Name	Country	Observed
APT groups			

	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a459f3f3-ccd1-40f9-96b3-f15763d2051e