Threat Group Cards: A Threat Actor Encyclopedia

Tool: SNUGRIDE

Names	SNUGRIDE
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(FireEye) SNUGRIDE is a backdoor that communicates with its C2 server through HTTP requests. Messages are encrypted using AES with a static key. The malware's capabilities include taking a system survey, access to the filesystem, executing commands and a reverse shell. Persistence is maintained through a Run registry key.
Information	<https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0159/>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool SNUGRIDE

Changed	Name	Country	Observed	
APT groups				
	Stone Panda, APT 10, menuPass		2006-Mar 2025	

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