Threat Group Cards: A Threat Actor Encyclopedia

Tool: Caterpillar

Names	Caterpillar
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader
Description	(ClearSky) Acting as a focal point, the group usually attacks webservers via a custom WebShell, namely Caterpillar – a variant of the open source WebShell 'ASPXSpy'. By using WebShell, the attackers leave their fingerprint on the web server and the internal network, move laterally, and deploy additional tools. On each compromised network the attacker installed one or more WebShell, supposedly to gain persistence and diversify the use of similar tools. The attackers use the WebShell to communicate with their C&C server for running commands and exfiltrating sensitive information. Connection to the WebShell is made using NordVPN or ExpressVPN services.
Information	<https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf>

Last change to this tool card: 19 April 2021

Download this tool card in JSON format

All groups using tool Caterpillar

Changed	Name	Country	Observed	
APT groups				
	Volatile Cedar		2012-Early 2020	

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