Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:49:42 UTC

Tool: Cryptmerlin

Names	Cryptmerlin
Category	Malware
Type	Backdoor
Description	(Trend Micro) Attackers used the DLL sideloading technique on the target machine to launch Cryptmerlin, a customized backdoor based on an open-source malware, Merlin Agent, written in Golang. Unlike the original Merlin Agent, Cryptmerlin currently only implements the ExecuteCommand function, which will communicate to the C&C server via HTTP/HTTPS request. To lower the security warning on the infected machine, Cryptmerlin can also communicate with the C&C server over proxy server, with the information of the victim's internal proxy also embedded in the config.
Information	<https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html>

Last change to this tool card: 26 December 2024

Download this tool card in JSON format

All groups using tool Cryptmerlin

Changed	Name	Country	Observed	
APT groups				
	Salt Typhoon, GhostEmperor		2020-Feb 2025	

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