Gray Lambert - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:40:56 UTC

Tool: Gray Lambert

Names	Gray Lambert
Category	Malware
Type	Backdoor
Description	(Kaspersky) Gray Lambert is the most recent tool in the Lamberts' arsenal. It is a network-driven backdoor, similar in functionality to White Lambert. Unlike White Lambert, which runs in kernel mode, Gray Lambert is a user-mode implant. The compilation and coding style of Gray Lambert is similar to the Pink Lambert USB stealers. Gray Lambert initially appeared on the computers of victims infected by White Lambert, which could suggest the authors were upgrading White Lambert infections to Gray. This migration activity was last observed in October 2016. Some of the known filenames for Gray Lambert are mwapi32.dll and poolstr.dll – it should be pointed though that the filenames used by the Lamberts are generally unique and have never been used twice.
Information	<https://securelist.com/unraveling-the-lamberts-toolkit/77990/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Gray Lambert

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Longhorn, The Lamberts		2009	

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