Green Lambert - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:51:48 UTC

Tool: Green Lambert

Names	Green Lambert
Category	Malware
Type	Loader
Description	(Kaspersky) Looking further for malware similar to Blue Lambert, we came by another family of malware we called Green Lambert. Green Lambert is a lighter, more reliable, but older version of Blue Lambert. Interestingly, while most Blue Lambert variants have version numbers in the range of 2.x, Green Lambert is mostly in 3.x versions. This stands in opposition to the data gathered from export timestamps and C&C domain activity that points to Green Lambert being considerably older than the Blue variant. Perhaps both Blue and Green Lamberts have been developed in parallel by two different teams working under the same umbrella, as normal software version iterations, with one seeing earlier deployment than the other. Signatures created for Green Lambert (Windows) have also triggered on an OS X variant of Green Lambert, with a very low version number: 1.2.0. This was uploaded to a multiscanner service in September 2014. The OS X variant of Green Lambert is in many regards functionally identical to the Windows version, however it misses certain functionality such as running plugins directly in memory.
Information	<https://securelist.com/unraveling-the-lamberts-toolkit/77990/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0690/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Green Lambert

Changed	Name	Country	Observed

APT groups

	↳ Subgroup: Longhorn, The Lamberts		2009	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ca7ec4d8-ddd5-4a6a-a1ef-891f53ce52be