

# Purple Lambert - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:19:10 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Purple Lambert

## Tool: Purple Lambert

Names	Purple Lambert
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	<p>(<a href="#">Kaspersky</a>) The samples were compiled in 2014 and, accordingly, were likely deployed in 2014 and possibly as late as 2015. Although we have not found any shared code with any other known malware, the samples have intersections of coding patterns, style and techniques that have been seen in various Lambert families. We therefore named this malware Purple Lambert. Purple Lambert is composed of several modules, with its network module passively listening for a magic packet. It is capable of providing an attacker with basic information about the infected system and executing a received payload. Its functionality reminds us of <a href="#">Gray Lambert</a>, another user-mode passive listener. Gray Lambert turned out to be a replacement of the kernel-mode passive-listener <a href="#">White Lambert</a> implant in multiple incidents. In addition, Purple Lambert implements functionality similar to, but in different ways, both Gray Lambert and White Lambert.</p>
Information	< <a href="https://securelist.com/apt-trends-report-q1-2021/101967/">https://securelist.com/apt-trends-report-q1-2021/101967/</a> >

Last change to this tool card: 16 May 2021

Download this tool card in [JSON](#) format

## All groups using tool Purple Lambert

Changed	Name	Country	Observed
<b>APT groups</b>			
	↳ <a href="#">Subgroup: Longhorn, The Lamberts</a>		2009

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

---

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=6b947f53-6e78-45e6-a1b7-bed678f998ff>