Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:10:13 UTC

Tool: HiddenLotus

Names	HiddenLotus
Category	Malware
Type	Backdoor
Description	(Malwarebytes) So HiddenLotus didn't seem all that interesting at first, other than as a new variant of the OceanLotus backdoor first seen being used to attack numerous facets of Chinese infrastructure. OceanLotus was last seen earlier this summer, disguised as a Microsoft Word document and targeting victims in Vietnam. But there was something strange about HiddenLotus. Unlike past malware, this one didn't have a hidden .app extension to indicate that it was an application. Instead, it actually had a .pdf extension. Yet the Finder somehow identified it as an application anyway.
Information	<https://blog.malwarebytes.com/threat-analysis/2017/12/interesting-disguise-employed-by-new-mac-malware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.hiddenlotus>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool HiddenLotus

Changed	Name	Country	Observed	
APT groups				
	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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