Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:05:23 UTC

APT group: Antlion

Names	Antlion *(?)*
Country	China
Motivation	Information theft and espionage
First seen	2011
Description	(Symantec) Antlion is believed to have been involved in espionage activities since at least 2011, and this recent activity shows that it is still an actor to be aware of more than 10 years after it first appeared. The length of time that Antlion was able to spend on victim networks is notable, with the group able to spend several months on victim networks, affording plenty of time to seek out and exfiltrate potentially sensitive information from infected organizations. The targeting of Taiwan is perhaps unsurprising given we know Chinese state-backed groups tend to be interested in organizations in that region.
Observed	Sectors: Financial, Manufacturing. Countries: Taiwan.
Tools used	CheckID, EHAGBPSL, ENCODE MMC, JpgRun, NetSessionEnum, ProcDump, PsExec, xPack, WinRAR, Living off the Land.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/china-apt-antlion-taiwan-financial-attacks>

Last change to this card: 04 February 2022

Download this actor card in PDF or JSON format
