Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:44:40 UTC

Tool: Lurk

Names	Lurk
Category	Malware
Type	Downloader, Dropper
Description	(SecureWorks) Lurk is a malware downloader that uses digital steganography: the art of hiding secret information within a digital format, such as an image, audio, or video file. Lurk specifically uses an algorithm that can embed encrypted URLs into an image file by inconspicuously manipulating individual pixels. The resulting image contains additional data that is virtually invisible to an observer. Lurk's primary purpose is to download and execute secondary malware payloads. In particular, the Dell SecureWorks Counter Threat Unit (CTU) research team has observed Lurk dropping malware used to commit click fraud.
Information	<https://www.secureworks.com/research/malware-analysis-of-the-lurk-downloader> <https://securelist.com/the-hunt-for-lurk/75944/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.lurk>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:lurk>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Lurk

Changed	Name	Country	Observed	
APT groups				
	Lurk		2011-Jun 2016	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=da559a29-29ea-4956-8769-018b791db49a