

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:19:08 UTC

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



Tool: LoJax

Names	LoJax
Category	Malware
Type	Backdoor , Rootkit
Description	(ESET) Starting in at least early 2017, trojanized versions of an older userland agent of the popular LoJack anti-theft software from Absolute Software were found in the wild. We call this trojanized LoJack agent LoJax. LoJack attracted a lot of attention in recent years as it implements a UEFI/BIOS module as a persistence mechanism.
Information	< https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf >
MITRE ATT&CK	< https://attack.mitre.org/software/S0397/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.lojax >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:lojax >

Last change to this tool card: 23 April 2020

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

All groups using tool LoJax

Changed	Name	Country	Observed	
APT groups				
	Sofacy , APT 28 , Fancy Bear , Sednit		2004-Apr 2025	

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