Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:25:00 UTC

Tool: Spaceship

Names	Spaceship
Category	Malware
Type	Exfiltration
Description	(FireEye) SPACESHIP searches for files with a specified set of file extensions and copies them to a removable drive. FireEye believes that SHIPSHAPE is used to copy SPACESHIP to a removable drive, which could be used to infect another victim computer, including an air-gapped computer. SPACESHIP is then used to steal documents from the air-gapped system, copying them to a removable drive inserted into the SPACESHIP-infected system.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0035/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.spaceship>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:spaceship>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Spaceship

Changed	Name	Country	Observed	
APT groups				
	APT 30, Override Panda		2005	
	Naikon, Lotus Panda		2010-Apr 2022	

2 groups listed (2 APT, 0 other, 0 unknown)
