Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:33:54 UTC

Tool: Flashflood

Names	Flashflood
Category	Malware
Type	Loader
Description	(Kaspersky) FLASHFLOOD is responsible for copying files from an inserted removable drive to the hard drive of an infected computer, presumably to remove files transferred from the air-gapped system to an Internet-connected machine for removal from the victim network. FLASHFLOOD will scan both the infected system and any inserted removable drive for specific files (based on file extension or last modified time) and copy them to a specified location, using the same compression and encoding method as SPACESHIP. FLASHFLOOD may also log additional information about the victim host, including system information and data from the user's Windows Address Book.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0036/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.flashflood>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:flashflood>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Flashflood

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)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e2853862-6433-4ecc-82d3-9f5205197047