Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:49:23 UTC

Tool: LOWBALL

Names	LOWBALL
Category	Malware
Type	Backdoor, Exfiltration
Description	(FireEye) This backdoor, known as LOWBALL, uses the legitimate Dropbox cloud-storage service to act as the CnC server. It uses the Dropbox API with a hardcoded bearer access token and has the ability to download, upload, and execute files. The communication occurs via HTTPS over port 443.
Information	<https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0042/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.lowball>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:lowball>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool LOWBALL

Changed	Name	Country	Observed	
APT groups				
	Temper Panda, admin@338		2014	

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