

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:26:22 UTC

Tool: Pirpi

Names	Pirpi SHOTPUT Badey EXL CookieCutter Backdoor.APT.CookieCutter
Category	Malware
Type	Backdoor
Description	SHOTPUT is a custom backdoor used by APT3.
Information	< https://www.fireeye.com/blog/threat-research/2010/11/ie-0-day-hupigon-joins-the-party.html > < https://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/ >
MITRE ATT&CK	< https://attack.mitre.org/software/S0063/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.pirpi >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:Pirpi >

Last change to this tool card: 30 December 2022

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

All groups using tool Pirpi

Changed	Name	Country	Observed	
APT groups				
	APT 3, Gothic Panda, Buckeye		2007-Nov 2017	

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



Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=da701115-a28c-458d-8a72-3e1783fb6379>