Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:28:05 UTC

Tool: PunchBuggy

Names	PunchBuggy ShellTea Powersniff
Category	Malware
Type	POS malware, Backdoor
Description	PUNCHBUGGY is a backdoor malware used by FIN8 that has been observed targeting POS networks in the hospitality industry.
Information	<https://blog.morphisec.com/security-alert-fin8-is-back> <https://www.thesecuritybuddy.com/malware-prevention/what-is-powersniff-malware/> <https://unit42.paloaltonetworks.com/powersniff-malware-used-in-macro-based-attacks/> <https://lokalhost.pl/gozi_tree.txt>
MITRE ATT&CK	<https://attack.mitre.org/software/S0196/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.powersniff>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PunchBuggy>

Last change to this tool card: 23 May 2020

Download this tool card in JSON format

All groups using tool PunchBuggy

Changed	Name	Country	Observed	
APT groups				
	FIN8	[Unknown]	2016-Dec 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e6081bfb-8593-4cc9-9f20-103980b059f9