Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:59:24 UTC

Tool: BISCUIT

Names	BISCUIT zxdosml
Category	Malware
Type	Backdoor
Description	(FireEye) The BISCUIT backdoor (so named for the command “bdkzt”) is an illustrative example of the range of commands that APT1 has built into its “standard” backdoors. APT1 has used and steadily modified BISCUIT since as early as 2007 and continues to use it presently.
Information	<https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0017/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.biscuit>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool BISCUIT

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	

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