Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:24:06 UTC

Tool: Bateleur

Names	Bateleur
Category	Malware
Type	Backdoor
Description	(Proofpoint) Proofpoint researchers have uncovered that the threat actor commonly referred to as FIN7 has added a new JScript backdoor called Bateleur and updated macros to its toolkit. We have observed these new tools being used to target U.S.-based chain restaurants, although FIN7 has previously targeted hospitality organizations, retailers, merchant services, suppliers and others. The new macros and Bateleur backdoor use sophisticated anti-analysis and sandbox evasion techniques as they attempt to cloak their activities and expand their victim pool.
Information	<https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.bateleur>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Bateleur>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Bateleur

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	
	FIN7		2013-Jul 2024	

2 groups listed (2 APT, 0 other, 0 unknown)
