Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:22:28 UTC

Tool: Brambul

Names	Brambul SierraBravo SORRYBRUTE
Category	Malware
Type	Worm, Backdoor
Description	(US-CERT) Brambul malware is a malicious Windows 32-bit SMB worm that functions as a service dynamic link library file or a portable executable file often dropped and installed onto victims' networks by dropper malware. When executed, the malware attempts to establish contact with victim systems and IP addresses on victims' local subnets. If successful, the application attempts to gain unauthorized access via the SMB protocol (ports 139 and 445) by launching brute-force password attacks using a list of embedded passwords. Additionally, the malware generates random IP addresses for further attacks.
Information	<https://www.us-cert.gov/ncas/alerts/TA18-149A> <https://www.us-cert.gov/ncas/analysis-reports/AR18-149A> <https://www.acalvio.com/lateral-movement-technique-employed-by-hidden-cobra/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.brambul>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Brambul

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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