Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:58:35 UTC

Tool: Bemstour

Names	Bemstour
Category	Malware
Type	Backdoor
Description	(Symantec) Bemstour exploits two Windows vulnerabilities in order to achieve remote kernel code execution on targeted computers. One vulnerability is a Windows zero-day vulnerability (CVE-2019-0703) discovered by Symantec. The second Windows vulnerability (CVE-2017-0143) was patched in March 2017 after it was discovered to have been used by two exploit tools—EternalRomance and EternalSynergy—that were also released as part of the Shadow Brokers leak.
Information	<https://symantec-blogs.broadcom.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Bemstour>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Bemstour

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

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