Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:37:53 UTC

Tool: BendyBear

Names	BendyBear Waterbear Deuterbear
Category	Malware
Type	Backdoor
Description	(Palo Alto) The BendyBear sample was determined to be x64 shellcode for a stage-zero implant whose sole function is to download a more robust implant from a command and control (C2) server. Shellcode, despite its name, is used to describe the small piece of code loaded onto the target immediately following exploitation, regardless of whether or not it actually spawns a command shell. At 10,000+ bytes, BendyBear is noticeably larger than most, and uses its size to implement advanced features and anti-analysis techniques, such as modified RC4 encryption, signature block verification, and polymorphic code.
Information	<https://unit42.paloaltonetworks.com/bendybear-shellcode-blacktech/> <https://www.trendmicro.com/en_us/research/24/d/earth-hundun-waterbear-deuterbear.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0574/>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=bendybear>

Last change to this tool card: 22 April 2024

Download this tool card in JSON format

All groups using tool BendyBear

Changed	Name	Country	Observed
APT groups			

	BlackTech, Circuit Panda, Radio Panda		2010-Oct 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8a45f278-6be3-4157-896d-9af9ec672f29