Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:43:19 UTC

Tool: BugSleep

Names	BugSleep MuddyRot
Category	Malware
Type	Backdoor
Description	(Check Point) BugSleep is a new tailor-made malware used in MuddyWater phishing lures since May 2024, partially replacing their use of legitimate RMM tools. We discovered several versions of the malware being distributed, with differences between each version showing improvements and bug fixes (and sometimes creating new bugs). These updates, occurring within short intervals between samples, suggest a trial-and-error approach. BugSleep main logic is similar in all versions, starting with many calls to the Sleep API to evade sandboxes and then it loads the APIs it needs to run properly. It then creates a mutex (we observed “PackageManager” and “DocumentUpdater” in our samples) and decrypts its configuration which includes the C&C IP address and port. All the configurations and strings are encrypted in the same way, where every byte is subtracted with the same hardcoded value. In most BugSleep samples, the malware then creates a scheduled task with the same name as the mutex and adds the comment 'sample comment' to it. The scheduled task, which ensures persistence for BugSleep, runs the malware and is triggered every 30 minutes on a daily basis.
Information	<https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bugsleep>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool BugSleep

Changed	Name	Country	Observed

APT groups

	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten		2017-Jul 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fd142e2a-1c90-4780-8eac-3319136a2f3f