LightlessCan (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:28:13 UTC

LightlessCan is a complex HTTP(S) RAT, that is a successor of the Lazarus RAT named BlindingCan.

In Q2 2022 and Q1 2023, it was deployed in targeted attacks against an aerospace company in Spain and a technology company in India.

Besides the support for commands already present in BlindingCan, its most significant update is mimicked functionality of many native Windows commands:
• ipconfig
• net
• netsh advfirewall firewall
• netstat
• reg
• sc
• ping (for both IPv4 and IPv6 protocols)
• wmic process call create
• nslookup
• schstasks
• systeminfo
• arp

These native commands are often abused by the attackers after they have gotten a foothold in the target's system. Lightless is able to execute them discreetly within the RAT itself, rather than being executed visibly in the system console. This provides stealthiness, both in evading real-time monitoring solutions like EDRs, and postmortem digital forensic tools.

LightlessCan use RC6 for decryption of its configuration, and also for encryption and decryption of network traffic.

▶ [TLP:WHITE] win_lightlesscan_auto (20251219 | Detects win.lightlesscan.)
