CACTUSTORCH (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:04:54 UTC

js.cactustorch (Back to overview)

CACTUSTORCH

Actor(s): APT32, Leviathan

According to the GitHub repo, CACTUSTORCH is a JavaScript and VBScript shellcode launcher. It will spawn a 32 bit version of the binary specified and inject shellcode into it.

References

2022-01-16 · forensicitguy · Tony Lambert
Analyzing a CACTUSTORCH HTA Leading to Cobalt Strike
CACTUSTORCH Cobalt Strike

2020-09-24 · Microsoft · Ben Koehl, Joe Hannon, Microsoft Identity Security Team
Microsoft Security—detecting empires in the cloud
CACTUSTORCH LazyCat APT40

2020-09-23 · Seqrite · Goutam Tripathy, Kalpesh Mantri, Pawan CHaudhari
Operation SideCopy: An insight into Transparent Tribe’s sub-division which has been incorrectly attributed for years
CACTUSTORCH AllaKore

2019-04-01 · · Macnica Networks · Macnica Networks
OceanLotus Attack on Southeast Asian Automotive Industry
CACTUSTORCH Cobalt Strike

2018-12-20 · · Codercto · Codercto
Analysis of the attack activities of Hailian Lotus APT group against large domestic investment companies
CACTUSTORCH

2017-11-16 · Github (mdsecactivebreach) · Vincent Yiu

CACTUSTORCH: Payload Generation for Adversary Simulations

CACTUSTORCH

There is no Yara-Signature yet.
