NanHaiShu (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:16:04 UTC

js.nanhaishu (Back to overview)

NanHaiShu

Actor(s): Leviathan

NanHaiShu is a remote access tool and JScript backdoor used by Leviathan. NanHaiShu has been used to target government and private-sector organizations that have relations to the South China Sea dispute.

References

2019-01-01 · MITRE · MITRE ATT&CK
Tool description: NanHaiShu
NanHaiShu

2017-10-16 · Proofpoint · Axel F, Pierre T
Leviathan: Espionage actor spearphishes maritime and defense targets
NanHaiShu SeDll APT40

2016-08-05 · F-Secure · F-Secure Labs
NANHAISHU: RATing the South China Sea
NanHaiShu

2015-06-24 · Spiceworks · Chris Miller
Stealthy Cyberespionage Campaign Attacks With Social Engineering
NanHaiShu

There is no Yara-Signature yet.
