AIRBREAK (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:27:50 UTC

js.airbreak (Back to overview)

AIRBREAK

aka: Orz

Actor(s): Leviathan

AIRBREAK, a JavaScript-based backdoor which retrieves commands from hidden strings in compromised webpages.

References

2020-01-01 · Secureworks · SecureWorks
BRONZE MOHAWK
AIRBREAK scanbox BLACKCOFFEE CHINACHOPPER Cobalt Strike Derusbi homefry murkytop SeDll APT40

2018-07-11 · FireEye · Ben Read, Ben Wilson, Dan Perez, Marcin Siedlarz, Scott Henderson, Steve Miller
Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally
AIRBREAK APT40

2018-03-30 · Kahu Security · Kahu Security
Reflow JavaScript Backdoor
AIRBREAK

There is no Yara-Signature yet.
