BOLDMOVE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:40:27 UTC

elf.boldmove (Back to overview)

BOLDMOVE

According to Mandiant, this malware family is attributed to potential chinese background and directly related to observed exploitation of Fortinet's SSL-VPN (CVE-2022-42475). There is also a Windows variant.

References

2024-05-08 · Mandiant · Mandiant
M-Trends 2024 Special Report: Chinese Espionage Operations Targeting The Visibility Gap
BOLDMOVE WHIRLPOOL

2024-02-06 · NCSC NL · AIVD, MIVD
Ministry of Defense of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT
BOLDMOVE

2023-01-20 · The Hacker News · Ravie Lakshmanan
Chinese Hackers Exploited Recent Fortinet Flaw as 0-Day to Drop Malware
BOLDMOVE BOLDMOVE

2023-01-19 · Mandiant · Cristiana Kittner, Mark Lechtik, Sarah Hawley, Scott Henderson
Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475)
BOLDMOVE BOLDMOVE

There is no Yara-Signature yet.
