BlueShell (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:58:14 UTC

win.blueshell (Back to overview)

BlueShell

According to AhnLab, BlueShell is a backdoor malware developed in Go language, published on Github, and it supports Windows, Linux, and Mac operating systems. Currently, the original Github repository is presumed to have been deleted, but the BlueShell source code can still be obtained from other repositories. It features an explanatory ReadMe file in Chinese, indicating the possibility that the creator is a Chinese user.

References

2024-04-09 · Hunt.io · Hunt.io
BlueShell: Four Years On, Still A Formidable Threat
BlueShell

2023-09-11 · AhnLab · Sanseo
BlueShell Used in APT Attacks Against Korean and Thai Targets
BlueShell Sliver Dalbit

2023-09-05 · · AhnLab · Sanseo
BlueShell malware used in APT attacks targeting Korea and Thailand
BlueShell SparkRAT

2023-02-13 · AhnLab · kingkimgim
Dalbit (m00nlight): Chinese Hacker Group’s APT Attack Campaign
Godzilla Webshell ASPXSpy BlueShell CHINACHOPPER Cobalt Strike Ladon MimiKatz Dalbit

There is no Yara-Signature yet.
