Backdoor:Win64/KnuckleTouch.A!dha threat description - Microsoft Security Intelligence

By Microsoft Corporation

Archived: 2026-04-06 03:26:51 UTC

Published Feb 14, 2024 | Updated Feb 14, 2024

Summary

Backdoor:Win64/KnuckleTouch.A!dha is the detection for a custom backdoor used since at least early to mid-2022 by the threat actor Microsoft tracks as Seashell Blizzard.

This trojan has been involved in multiple campaigns distributing ransomware. Once installed, attackers can use the trojan to perform various tasks, such as stealing credentials or other information, additional destructive attacks, and giving attackers remote access to your device.

Seashell Blizzard is a high-impact threat actor linked to the Russian Federation and conducts global activities on behalf of Russian Military Intelligence Unit 74455 (GRU). Active since at least 2013, Seashell Blizzard's prolific operations have led to high-profile destructive attacks, such as KillDisk (2015) and FoxBlade (2022).
