Rule Info Winnti_APT_Hdump_Tool - Valhalla

Archived: 2026-04-05 16:15:09 UTC

Name

Winnti_APT_Hdump_Tool

Description

Password dumper used by Winnti group - file pn.exe

Reference

Internal Research

Rule Hash

b7bc4234f427f855d3ef2a2bcf743735

Tags

['FILE', 'EXE', 'G0044', 'T1003', 'APT', 'CHINA']

Antivirus Verdicts

Malicious (>= 10 engines)

5

Suspicious (< 10 engines)

3

Rule Matches

Timestamp

Positives

Total

Hash

VT

2025-06-25 19:34:32

33

72

85eada3b4af6e9bd6ee17a068bb6d74717ad1f541d1a5eef09d74557abdbf778

2024-05-23 04:38:23

8

74

cf5739ac59dac84d94aa95123a18ed0cdeb58fbd3a42645580485808f6692a59

2024-03-16 01:05:11

4

71

48bdb774ad21b97a9a09f1ba3ba2daac5b6b5d765e7ac6324e485ab7312e99a0

2023-05-16 04:12:48

29

70

3fc6b07ab22dc5c7732b491418ca395dbe819423bda2b61b946013278a41df54

2023-02-21 19:44:47

17

70

64ab1c1b19682026900d060b969ab3c3ab860988733b7e7bf3ba78a4ea0340b9

2023-02-17 16:45:23

6

69

b4f2dd50bf5a65a71b89d490fc5e83aa60af5d4f62f451b7b5de58d152c838d6

2021-11-09 07:44:38

10

62

c17eda56d9a48bcb1beb20f47065da93c765dcb29b4f7f389d172f50292d0e4d

2021-04-11 11:11:34

27

70

724d0be8e7a56efca098e6e93aa8604b0df2b41a8a1569d9872bf9a043520f68
