Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor

By Author:

Archived: 2026-04-06 00:54:26 UTC

Color

Size

of 36

1BLACK BASTA RANSOMWARE | ATTACKS DEPLOY CUSTOM EDR EVASION TOOLS TIED TO FIN7 THREAT ACTOR
BLACK BASTA RANSOMWARE |
ATTACKS DEPLOY CUSTOM
EDR EVASION TOOLS TIED
TO FIN7 THREAT ACTOR
Authors: Antonio Cocomazzi, Antonio Pirozzi
November 2022
SentinelLABS

2BLACK BASTA RANSOMWARE | ATTACKS DEPLOY CUSTOM EDR EVASION TOOLS TIED TO FIN7 THREAT ACTOR
TABLE OF
CONTENTS
3 EXECUTIVE SUMMMARY
4 OVERVIEW
5 BLACK BASTA INITIAL
ACCESS ACTIVITY
6 ENTER THE BLACK
BASTA OPERATOR
8 BLACK BASTA PRIVILEGE
ESCALATION TECHNIQUES
9 REMOTE ADMIN TOOLS
12 BLACK BASTA
LATERAL MOVEMENT
13 IMPAIR DEFENSES
14 CUSTOM DEFENSE
IMPAIRMENT TOOL
18 UNCOVERING FURTHER TIES

BETWEEN BLACK BASTA AND FIN7
23 ATTRIBUTION OF THE
THREAT ACTOR: FIN7
24 CONCLUSION
25 INDICATORS OF COMPROMISE
36 ABOUT SENTINELLABS
