Threat Category: State-Sponsored Threat ? Wiper Malware

Threat Name: HiddenCobra Wiper (Variant r4)

Threat Description: This rule detects a HiddenCobra (North Korean threat actor group) wiper malware variant. The malware targets system drives for destructive operations, utilizing direct physical drive access and BIOS extended write operations.

Indicators of Compromise (IoCs):

Two critical string indicators:

$PhysicalDriveSTR = "\\\\.\\PhysicalDrive" (wide string)

$ExtendedWrite = {B4 43 B0 00 CD 13} (hexadecimal pattern indicating BIOS interrupt 13h, used for disk writes)

Detection Mechanism:

File must satisfy both PE file structure validations:

uint16(0) == 0x5a4d (checks for "MZ" DOS header signature)

uint16(uint32(0x3c)) == 0x4550 (checks for "PE" NT header signature)

All specified strings must match (all of them condition).

Rule name must be: HiddenCobra_r4_wiper_2.

Reference:

US-CERT Malware Analysis Report (MAR): MAR-10135536.11

Author:

NCCIC Partner

Rule Metadata:

description: "Detects HiddenCobra Wiper"

date: "2017-12-12"

reference: "https://www.us-cert.gov/sites/default/files/publications/MAR-10135536.11.WHITE.pdf"

id: "75acc3cb-90dd-58e8-b094-ed3f28650b1b"