Virus tipo API Nome in codice: BLACK THISTLE

Natura dell'API:

BLACK THISTLE è un API dormiente a cascata, progettato non per distruggere, ma per rendere cieco e sordo lo Stato nel momento esatto dell'attentato.

Non uccide, Permette che l'uccisione avvenga.

Filosofia del virus:

"Non colpire la regina. Colpisci il sistema che la protegge."

Come entra:

Non viene inserito direttamente nel sistema reale ma passa attraverso sistemi innocui e interconnessi, quelli che nessuno considera critici.

Ogni passaggio sembra legittimo.

Ogni sistema è una scusa.

Nessun allarme, nessuna firma ostile.

Installazione:

Il BLACK THISTLE è stato trasferito in una chiave USB speciale, non può essere installato come un semplice file e la procedura non può essere spiegata qui.
Tutte le informazioni saranno direttamente nella chiave USB.

BLACK THISTLE vive in tre fasi:

1. Infiltrazione passiva:
   - Non fa nulla di visibile
   - Osserva
   - Mappa flussi, orari, priorità e Impara come reagisce lo Stato

2. Modalità Dormiente:
   - Tutti i moduli sono spenti
   - Nessun traffico sospetto
   - Nessuna traccia di attività

3. Attivazione silenziosa (D.A.R.K. H.A.R.V.E.S.T.)

Qui diventa utile. Non spettacolare. Viene attivato tramite protocollo D.A.R.K H.A.R.V.E.S.T.

Funzioni chiave:

1. Desincronizzazione delle comunicazioni

I messaggi non spariscono ma arrivano in ritardo o arrivano nell'ordine sbagliato

Supporto e aiuti agiscono dopo.

2. Priorità falsate

Allarmi veri → bassa priorità

Avvisi inutili → alta priorità

Le sale operative sono occupate da "falsi problemi".

3. Protocollo di sicurezza fantasma

BLACK THISTLE simula che i protocolli siano attivi:

checkpoint "verificati"

percorsi "sicuri"

zone "bonificate"

In realtà nulla viene controllato.

Tutti sono convinti che qualcun altro abbia già fatto il lavoro.

4. Cecità selettiva

Non spegne telecamere o radar (troppo sospetto).

Li rende instabili - inattendibili - "tecnicamente funzionanti"

Nessuno si fida dei dati nel momento critico.

Effetto finale nella scena dell’attentato:

Tutto sembra funzionare ed essere sotto controllo, già gestito.

Ma:

la scorta è nel punto sbagliato

le comunicazioni arrivano tardi

l’allarme giusto viene ignorato

l’evacuazione non parte

L’attentato riesce non per forza, ma per assenza di reazione.

Dopo l’attentato, si spegne, cancella i moduli temporanei, lascia solo errori “compatibili con il caos”