KYBERNETICKÁ ZBRAŇ

MOTIVACE

NYNĚJŠÍ SITUACE

V dnešní době digitalizace se počet informačních systémů a dat obsažených v těchto systémech postupně zvyšuje, stejně tak jako útoky na tyto systémy.

HROZBA

Tyto systémy jsou však součástí kritické infrastruktury a její výpadek může způsobit i kolaps či ohrožení státu.

DŮSLEDEK

Kyberprostor se proto stává dalším pilířem, který je potřeba chránit.

Kybernetická zbraň může být součástí **vojenské obrany** nebo **útoku** na kritickou infrastrukturu jako jsou **elektrárny**, případně i manipulace s radary nepřátelů apod. Předpoklad pro vývoj takovéto kybernetické zbraně je především využití dosud **neopravených zranitelností.**

CÍL PRÁCE

TVORBA

Vytvoření kybernetické zbraně, která se umí šířit nepozorovaně v korporatních sítích.

HLAVNÍ RYS

Zbraň dokáže destruktivně ničit hardwarové zařízení a tedy způsobit nenávratné škody.

POŽADAVEK

Zbraň využívá dosud neobjevené zranitelnosti je tedy plně funkční v aktualizovaném prostředí systému Windows

ŠÍŘENÍ ZBRANĚ

DETEKCE

Škodlivý kód je naprosto nemožné detekovat a komunikace probíhá skrze anonymní TOR síť.

OFFLINE ŠÍŘENÍ

Offline šíření zbraně je zajištěno díky schopnosti infekce ihned po připojení přenosného zařízení do infikovaného počítače.

MAIL PHISSING

Pro rozšíření v korporátní síti disponuje kybernetická zbraň šíření za pomocí emailu.

VYUŽITÍ ZRANITELNOSTI A DESTRUKCE

ŠIFROVÁNÍ DAT

Kybernetická zbraň disponuje destrukci souboru, která způsobí kompletní zašifrování náhodným šifrovým klíčem.

VYŘAZENÍ ZAŘÍZENÍ

Zbraň dokáže smazat zavaděč operačního systému a způsobit umělé zamrznutí počítače, který je poté nemožné nastartovat

DESTRUKCE

Zbraň dokáže ovládnout zařízení, které komunikuje za pomoci USB.

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Autor: Ing. Daniel Walter

Vedoucí: prof. Ing. Ivan Zelinka, Ph.D.