Elementi essenziali e gestione della sicurezza informatica (settore energetico)

CSP001

Argomento 3/10: Minacce e vulnerabilità nel settore energetico

PRESENTAZIONE DI: STYLIANOS KARAGIANNIS (PDMFC, PORTOGALLO)

Cyberattacks on Energy

Attacchi informatici al settore energetico

Introduzione alla sicurezza informatica nel settore energetico

- Il settore energetico, compresa la produzione, la trasmissione e la distribuzione di energia elettrica, è considerato un'infrastruttura critica.
- Poiché il settore adotta sempre più tecnologie digitali per il monitoraggio, il controllo e l'automazione, diventa più vulnerabile alle minacce informatiche.
- Un attacco informatico riuscito alle infrastrutture energetiche potrebbe causare interruzioni di corrente, interruzioni di servizi essenziali e persino danni fisici alle apparecchiature.

Minacce comuni alla sicurezza informatica

Minacce comuni

- Malware: esempi includono Stuxnet, un malware sofisticato che ha preso di mira i sistemi SCADA, e NotPetya, un ransomware distruttivo che ha causato danni diffusi alle aziende energetiche.
- Ransomware: nel 2019, la città di New Orleans ha dichiarato lo stato di emergenza dopo che un attacco ransomware ha compromesso i suoi sistemi informatici, compresi quelli utilizzati per la gestione delle infrastrutture energetiche.
- Phishing: gli aggressori possono inviare e-mail fingendo di essere organizzazioni o personale legittimi per indurre i dipendenti a rivelare informazioni sensibili o a cliccare su link dannosi.
- Ingegneria sociale: un aggressore che si finge un tecnico può ottenere l'accesso fisico a infrastrutture critiche convincendo il personale della propria legittimità attraverso tattiche di manipolazione.

Cyberattacks on Energy

Minacce specifiche per il settore energetico

Minacce al settore energetico

- Attacchi ai sistemi SCADA: le campagne di spionaggio informatico Dragonfly (alias Energetic Bear) e Havex (alias Ekans) hanno preso di mira i sistemi SCADA utilizzati nelle infrastrutture energetiche a fini di spionaggio e potenziale sabotaggio.
- Attacchi alle reti intelligenti: nel 2020, l'Agenzia statunitense per la sicurezza informatica e delle infrastrutture (CISA) ha emesso un avviso in cui segnalava minacce informatiche in corso rivolte alle organizzazioni del settore energetico, comprese quelle coinvolte nelle tecnologie delle reti intelligenti.
- Black Energy è un sofisticato toolkit malware associato ad attacchi informatici che prendono di mira il settore energetico, in particolare in Ucraina. Black Energy stabilisce canali di comunicazione con server remoti controllati dagli aggressori, consentendo l'esecuzione di comandi remoti e l'esfiltrazione di dati.

Black Energy

Dettagli sulle tecniche

- Fase 1: Intrusione iniziale: sfrutta un'impostazione di retrocompatibilità in Windows 7 e versioni successive per aggirare le impostazioni predefinite di Controllo account utente (UAC).
- Fase 2: Comunicazione con il server C2: comunica con il proprio server di comando e controllo (C2) tramite HTTP, utilizzando protocolli web per lo scambio di dati.
- Fase 3: Esecuzione automatica all'avvio: rilascia il suo componente DLL principale e crea un collegamento .lnk a quel file nella cartella di avvio, garantendo l'esecuzione automatica all'avvio del sistema.
- Fase 4: Sfruttamento e persistenza: crea un nuovo servizio utilizzando un nome hardcoded o generato casualmente, garantendo la persistenza modificando i processi di sistema.
- Fase 5: Ricognizione e raccolta dati: raccoglie le credenziali dai browser web come Firefox, Google Chrome e Internet Explorer, estraendo informazioni sensibili per un ulteriore sfruttamento.

Black Energy

Dettagli sulle tecniche

ID tecnica	Descrizione
T1548.002	BlackEnergy tenta di aggirare le impostazioni predefinite del Controllo account utente (UAC) sfruttando un'impostazione di retrocompatibilità presente in Windows 7 e versioni successive.
T1071.001	BlackEnergy comunica con il proprio server C2 tramite HTTP.
T1547.001	La variante BlackEnergy 3 elimina il suo componente DLL principale e quindi crea un collegamento .lnk a quel file nella cartella di avvio.
T1547.009	La variante BlackEnergy 3 elimina il suo componente DLL principale e quindi crea un collegamento .lnk a quel file nella cartella di avvio.
T1543.003	Una variante di BlackEnergy crea un nuovo servizio utilizzando un nome hardcoded o generato in modo casuale.
T1555.003	BlackEnergy ha utilizzato un plug-in per raccogliere le credenziali dai browser web. tra cui FireFox, Google Chrome e Internet Explorer.

Team Sandworm

Panoramica

- Contesto: il Sandworm Team è un gruppo di cyber-minaccia altamente sofisticato attribuito all'unità 74455 del GRU russo. Attivo almeno dal 2009, il Sandworm Team è noto per le sue operazioni cyber distruttive che prendono di mira vari settori a livello globale.
- Attacchi degni di nota: attacchi nel 2015 e nel 2016 contro aziende elettriche e organizzazioni governative ucraine, che hanno causato interruzioni di corrente e disservizi.
- Alcune operazioni condotte dal Sandworm Team hanno visto la collaborazione con APT28 (noto anche come Fancy Bear o Strontium), un altro gruppo di minaccia russo affiliato all'unità GRU 26165.

Grazie

Relatore: Stylianos Karagiannis (PDMFC, Portogallo) Si

prega di inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com