L'abuso dei file MSC da parte degli Advanced Persistent Threat (APT)

Gianfranco Tonello - *CEO di TG Soft Cyber Security Specialist*

L'intervento mostrerà le tecniche di abuso documentate, le campagne reali e la vulnerabilità GrimResource, con casi concreti tratti dagli scenari geopolitici più caldi degli ultimi due anni.

Un talk tecnico, concreto, con casi reali sul tavolo. Per chi vuole capire come si muovono gli attori più sofisticati, prima di trovarli nella propria rete.

Un file Windows legittimo. Un vettore APT invisibile. Da Kimsuky in poi, i file MSC sono diventati una delle tecniche preferite dai gruppi di cyber-spionaggio state-sponsored, nei conflitti tra Cina e Taiwan, Russia e Ucraina e non solo.

Attacchi di cifratura e Business Continuity

Enrico Tonello – *Co-fondatore di TG Soft Cyber Security Specialist*

L'intervento verterà su cosa sia un attacco Ransomware di cifratura e quali canali vengano comunemente utilizzati per infiltrarsi sulle macchine (PC e Server).

Si procederà ad illustrare alcune delle tecnologie, tra le più efficaci ed efficienti, per bloccare la cifratura nella fase iniziale dell'attacco e rendere minimi i danni da questa provocati e le tecniche di ripristino e di rimessa in produzione delle macchine.

Al termine dello speech, allo stand di TG Soft, sarà possibile assistere ad una **dimostrazione di un attacco Ransomware reale** utilizzando un sample recente che mostrerà un tipico HumanOperatedRansomwareAttack, dal vivo nelle due modalità: attacco su una macchina SENZA sistemi di protezione specifici; attacco su una macchina CON SISTEMA DI PROTEZIONE ATTIVO.