FORUMECCATRONICA

STORMSHIELD

Cybersecurity in ambito ICS - Come un ransomware può compromettere la linea di produzione

STORMSHIELD

Davide Pala

Presales Engineer

ANIE AUTOMAZIONE

messe frankfurt

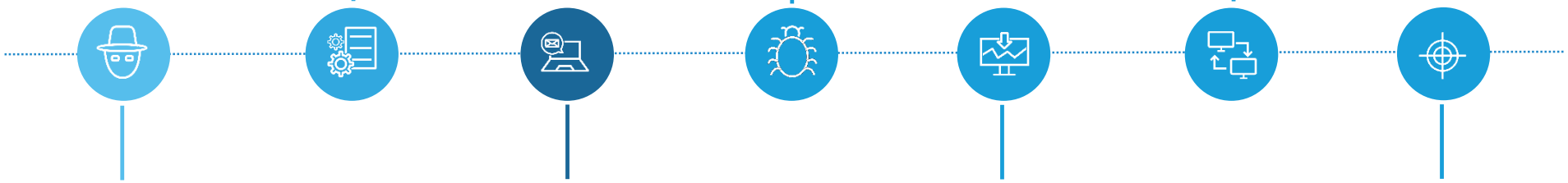
Davide Pala

Presales italy

Cybersecurity specialist

davide.pala@stormshield.eu

La cyber kill chain e le sue fasi



RECONNAISANCE

Ricerca delle informazioni sull'obbiettivo

WEAPONIZATION

Creazione di un malware utilizzabile sull'obbiettivo

DELIVERY

Invio del malware alla vittima tramite sistemi di comunicazione o scambio dati

EXPLOITATION

Sfruttamento di una o più vulnerabilità presenti sull'obbiettivo

INSTALLATION

Installazione sull'obbiettivo di un RAT che funga da backdoor

COMMAND AND CONTROL

Viene instaurata una comunicazione con il server di controllo dell'attaccante

ACTIONS ON OBJECTIVES

Esecuzione dell'attacco vero e proprio.

Fase uno: preparazione dell’attacco.

RECONNAISANCE

La ricerca di informazioni sull’obbiettivo vede coinvolte tutte quelle risorse che normalmente sono usate dai dipendenti per scopi diversi.

Anche i social network rappresentano una sorgente di informazioni.

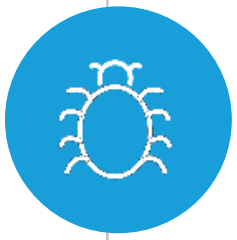
WEAPONIZATION

Tenendo a mente le informazioni ottenute nella fase di reconnaisance l’attaccante nasconde il dropper in un documento «attendibile».

Fase 2: primo approccio all’obbiettivo

A questo punto l’attaccante deve recapitare il DROPPER. Una mail di phishing, un sito compromesso possono andar bene …. Ma anche una chiavetta USB abbandonata nel parcheggio aziendale non è male.

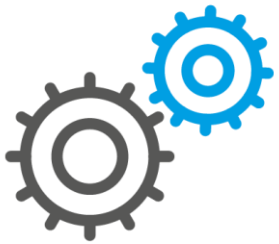
DELIVERY



EXPLOITATION

Eseguire il dropper è il primo ostacolo, un’exploit è l’atto di sfruttare una vulnerabilità software o una misconfigurazione …

Fase 3: Aggiungi un posto a tavola, hai un’ospite …

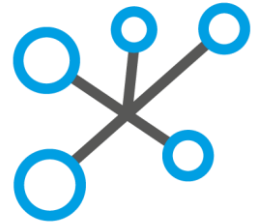


INSTALLATION

Una volta compromessa la macchina si deve capitalizzare il risultato: Occorre creare un sistema che consenta di mantenere l’accesso alla macchina della vittima, la così detta **persistenza**

COMMAND AND CONTROL

La Command and Control, abbreviata C2, è la creazione di un sistema di comunicazione che permette all’attaccante di inviare comandi e ricevere feedback dall’infrastruttura vittima. Fase cruciale per i **lateral movement**



Fase 4: All in …

ATTACK

La fase finale della cyber kill chain, l'attacco vero e proprio. In generale l'attacco è l'azione per raggiungere il risultato desiderato dall'attaccante, maggiore è l'interesse verso il risultato e maggiore sarà l'effort dedicato a tutte le fasi viste fino ad ora. Funziona?

Questione di ….

PROFITTO

RISORSE COMPETENTI

RISORSE HARDWARE

EFFORT DI GESTIONE DEL TEAM

TEMPO DEDICATO

UBI MAIOR … MINOR CESSAT

TEMPO DI RIPRISTINO

EVITARE IL PAGAMENTO

FORUMECCATRONICA

STORMSHIELD

GRAZIE PER L'ATTENZIONE!

ANIE AUTOMAZIONE

messe frankfurt