Honeypot per Sistemi di Controllo Industriale (ICS)

Lorena Modica

Relatori:
Prof. Fabrizio Baiardi
Prof. Luca Deri

Università di Pisa
Dipartimento di Informatica

Pisa, 12 Aprile 2024

Tabella dei contenuti

Obiettivo

Per ragioni economiche e di efficienza negli ultimi anni i sistemi industriali , sono stati connessi alle reti aziendali e Internet. Questo se da una parte ha apportato enormi benefici, dall'altra ha esposto questi sistemi a dei seri rischi.

Uno degli esempi più rilevanti è **Modbus**, un protocollo industriale nato per ambienti isolati.

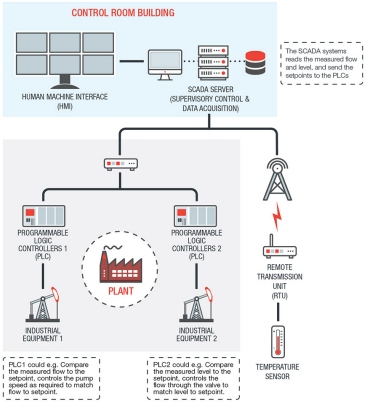
L' obiettivo della tesi è quello di profilare i possibili attacchi verso dispositivi che utilizzano il protocollo Modbus, raccogliendo informazioni per mezzo dell'honeypot **Conpot**.

ICS e SCADA

L'ICS-*Industrial Control System* è un sottoinsieme del settore dell'*Operational Technology* (OT) che comprende i sistemi utilizzati per monitorare e controllare i processi industriali.

Uno tra questi è il sistema SCADA (*Supervisory Control and Data Acquisition*).

Tra i tanti dispositivi, questi sistemi utilizzano anche **PLC** - Controllori Logici Programmabili:
dispositivi industriali che ricevono informazioni sulle condizioni di un processo e le inviano ai dispositivi di un sito di produzione per il controllo degli impianti.



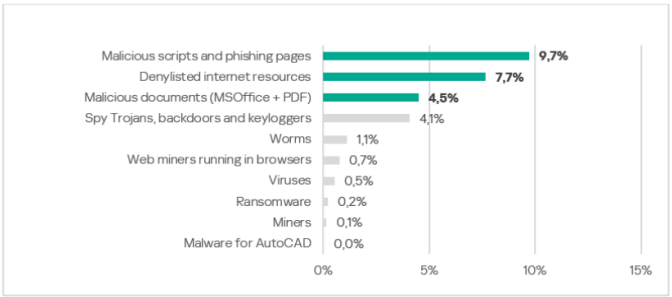
Modbus TCP

- Sfrutta il paradigma master-slave
- I dati vengono incapsulati in pacchetti TCP/IP
- Prevede operazioni di lettura, scrittura e diagnostica
- Ogni slave memorizza le informazioni in 4 tabelle:

Indirizzi dati	Offset	Numero consecutivo associato all'elemento analogico o discreto	Tipo	Nome tabella
0000h - 270Eh	00001	00001-09999	R/W	Discrete Output Coils
0000h - 270Eh	10001	10001-19999	Read-Only	Discrete Input Contacts
0000h - 270Eh	30001	30001-39999	Read-Only	Analog Input Registers
0000h - 270Eh	40001	40001-49999	R/W	Analog Output Holding Registers

Statistiche

Negli ultimi anni è aumentato il numero di attacchi rilevati in ambito ICS. Secondo il report ICS CERT di Kaspersky, in Italia, nel primo semestre del 2023, sono stati rilevati e bloccati oggetti malevoli sul 23,7% dei computer ICS.



Percentuale di computer ICS su cui sono stati bloccati malware di diverse categorie in Italia, H1 2023

Honeypot

- Un **honeypot** è un sistema informatico fittizio creato per attirare, rilevare e osservare il comportamento degli attaccanti.
- Gli honeypot essere classificati in:
  - ad **alta interazione**
  - a **bassa interazione** (e.g.**Conpot**).

	HoneyD	Capture-HPC	Honey PLC	LOGistICS	Conpot	GasPot	Gridpot
Versione Windows	✓	✓	✓	✓	✓	✓	X
Versione Linux	✓	✓	X	✓	✓	✓	✓
Lvl interazione	bassa	alta	media	media	bassa	bassa	media
Protocollo Modbus	X	X	X	✓	✓	X	✓
Open Source	✓	✓	✓	X	✓	✓	✓
Estensibilità	✓	X	✓	csv	xml	X	✓

Conpot

- Sviluppato dalla MushMushFoundation.
- Supporta la simulazione di diversi protocolli tra cui Modbus.
- Permette l'integrazione di controllori logici programmabili (PLC) e la loro personalizzazione tramite file XML.
- Registra gli eventi dei servizi con una precisione al millisecondo e offre informazioni di base sul tracciamento, come l'indirizzo di origine e il tipo di richiesta.

Risultati Principali

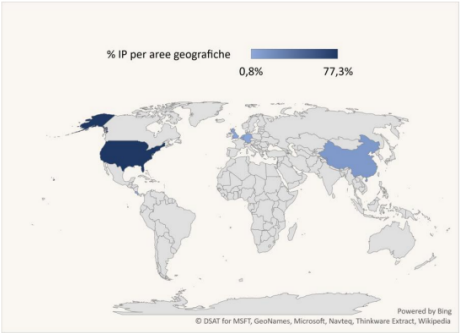
Utilizzando 3 honeypot con caratteristiche diverse:

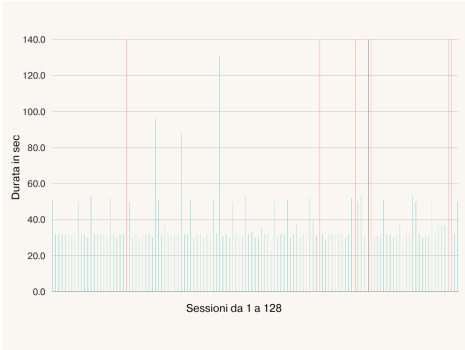
- Sono state raccolte informazioni sugli attaccanti e sulla natura degli IP collezionati.
- Sono stati confrontati i dati sulle modalità di interazione degli attaccanti con l'honeypot.
- I dati raccolti dimostrano che gli eventi che si verificano con maggiore frequenza sono errori o eccezioni:
  - Operazioni non valide
  - Connessioni interrotte improvvisamente
  - Pacchetti malformati
- Spesso gli attaccanti fanno operazioni di ricognizione anziché sfruttare direttamente le vulnerabilità di Modbus.

Dati Honeypot_1

- Raccolti tramite un honeypot su cloud ubicato in Italia che simula un PLC S7-200
- Periodo di riferimento: dal 21-02-2024 al 13-03-2024
- Maggiore presenza di IP malevoli
- I grafici rappresentano la distribuzione geografica degli IP e la durata delle sessioni per IP
- Anomalie:
  - Attacchi *Denial-of-Service*

Paese	% IP per aree geografiche
Stati Uniti	77,3%
Cina	11,8%
Regno Unito	4,2%
Germania	3,4%
Belgio	1,7%
Olanda	0,8%
Costa Rica	0,8%

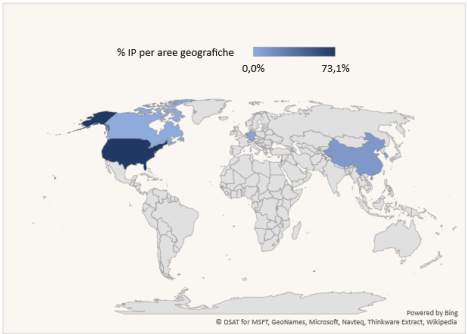




Dati Honeypot_2

- Raccolti tramite honeypot in ambiente casalingo ubicato in Italia che simula un PLC S7-200
- Periodo di riferimento: dall' 11-03-2024 al 18-03-2024
- In questo caso non vengono considerati gli IP benigni
- Anomalie:
  - Richiesta di operazioni a slave inesistenti

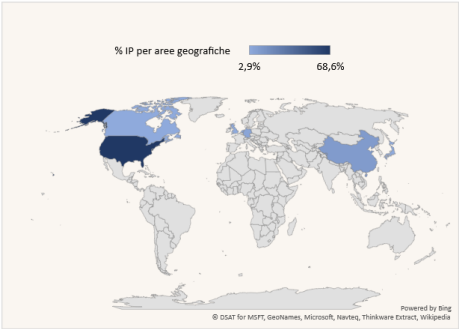
Paese	% IP per aree geografiche
Stati Uniti	73,1%
Cina	11,5%
Germania	3,8%
Olanda	3.8%
Canada	3.8%
Corea	3,8%



Dati Honeypot_3

- Raccolti tramite honeypot su cloud ubicato in Svizzera che simula un PLC S7-1500
- Periodo di riferimento: dal 16-03-2024 al 23-03-2024
- In questo caso non vengono considerati gli IP benigni
- Anomalie:
  - Malfunzionamento causato da un IP con una bassa probabilità di essere malevolo
  - Sessione di durata 6 min e 56 secondi con presenza di *Exception Code 1 : Illegal Function Exception*

Paese	% IP per aree geografiche
Stati Uniti	68,6%
Cina	11,4%
Olanda	5,7%
Germania	5,7%
Regno Unito	2,9%
Giappone	2,9%
Canada	2,9%



Confronti con altri lavori

Rispetto a lavori precedenti, l'analisi di dati raccolti in questa tesi si focalizza sul protocollo Modbus e non sugli altri protocolli supportati da Conpot.
Inoltre vengono:

- Confrontati dati raccolti da honeypot con caratteristiche differenti utilizzando sempre *template* personalizzati
- Catalogati esplicitamente gli eventi che si verificano con alta densità
- Analizzati comportamenti osservando le sessioni più significative

Conclusioni e sviluppi futuri

Conclusioni:

- Conpot è uno strumento valido in ambito ICS ma deve essere affiancato ad altri tool.
- Gli honeypot risultano essere degli ottimi alleati per comprendere e contrastare le interazioni malevole in ambito OT, ma è necessario specializzarli maggiormente per operare nel campo industriale.
- Oltre agli honeypot e ad altri strumenti per la sicurezza bisognerebbe avere anche una maggiore consapevolezza riguardo ai rischi che corrono questi sistemi.

I possibili sviluppi futuri, oltre all'approfondimento dei comportamenti degli attaccanti, sono:

- Fornire ulteriori dati sulle tipologie di interazione con i dispositivi Modbus.
- Analisi per affinare tecniche di *finger-printing* specifiche per gli attacchi al protocollo Modbus in ambito industriale.

Grazie per la vostra attenzione!