



A.A. 2022-2023



StealBot

Università degli studi di Napoli

Federico II



Valentino Bocchetti - N86003405



Valentina Annunziata - N86003280



Francesco Ciccarelli - N86003285

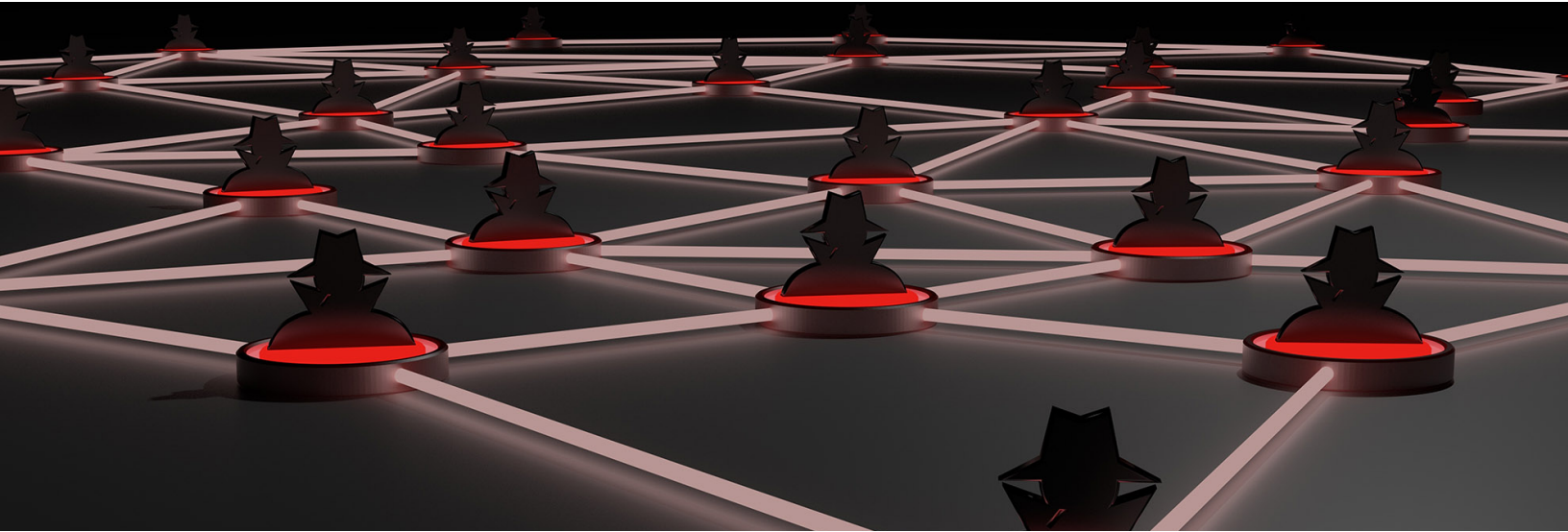


Giulia Caputo - N86003429

Indice

1	Presentazione	3
1.1	Descrizione della traccia	3
1.1.1	Tecnologie e linguaggi richiesti	3
1.2	Implementazione del sistema	3
1.3	Guida al Bot Master	4
1.3.1	Primo avvio	4
1.3.2	Analisi della struttura del progetto	4
1.3.3	Memorizzazione dei dati	4
1.4	Guida al Bot Slave	4
1.4.1	Analisi della struttura del progetto	4
1.4.2	Primo avvio	4
1.5	Report dei dati recuperati	4
2	Dettagli implementativi	4
2.1	Bot Master	4
2.2	Bot Slave	4
3	Codice sorgente sviluppato	4
4	Ringraziamenti	4

1 Presentazione



1.1 Descrizione della traccia

Si richiede la realizzazione di una **BotNET**¹ per il recupero di quante più informazioni possibili sulla dispositivo in cui una delle componenti della BotNET (a scelta dello studente) venga eseguito.

1.1.1 Tecnologie e linguaggi richiesti

Si richiede un applicativo scritto in **Python**² che utilizzi come strumento di comunicazione le **socket**³

1.2 Implementazione del sistema

Il progetto si concretizza in 2 componenti ben definite:

- ▶ Un **Bot Master** per la gestione dei dati ricevuti dal **bot slave** al quale inpartisce comandi sfruttando una connessione tramite socket asincrona;
- ▶ Il **Bot slave**, che ha il compito di ricavare quante più informazioni possibili sullo stato della macchina sul quale viene eseguito⁴.

¹ Per BotNET si intende una rete composta da dispositivi infettati da malware, detti bot o zombie, che agiscono tutti sotto lo stesso controllo di un unico dispositivo - detto botmaster - aumentando esponenzialmente le capacità dell'attaccante.

² Python è un linguaggio di programmazione di alto livello, orientato a oggetti, adatto, tra gli altri usi, a sviluppare applicazioni distribuite, scripting, computazione numerica e system testing.

³ Astrazione software progettata per utilizzare delle API standard e condivise per la trasmissione e la ricezione di dati attraverso una rete oppure come meccanismo di IPC..

⁴ Della quale non abbiamo nessun controllo diretto.

1.3 Guida al Bot Master

1.3.1 Primo avvio

DESCRIZIONE DELLE OPERAZIONI EFFETTUATE IN FASE DI AVVIO

1.3.2 Analisi della struttura del progetto

1.3.3 Memorizzazione dei dati

Il sistema permette inoltre utilizza un DBMS⁵ per il salvataggio dei dati ricavati dal *bot slave* durante la sua esecuzione.

1.4 Guida al Bot Slave

1.4.1 Analisi della struttura del progetto

1.4.2 Primo avvio

DESCRIZIONE DELLE OPERAZIONI EFFETTUATE IN FASE DI AVVIO

1.5 Report dei dati recuperati

TODO: Aggiungere screenshot/tabella dei record ottenuti mediante il bot

2 Dettagli implementativi

2.1 Bot Master

2.2 Bot Slave

3 Codice sorgente sviluppato

Il codice sorgente prodotto durante lo sviluppo di *StealBot*[®] è disponibile sulla piattaforma [GitHub](#), che ne ha permesso anche il versionamento.

Di seguito riportiamo un link per il [download](#)⁶

4 Ringraziamenti

Ringraziamo il professore [Alessio Botta](#) per lo splendido corso, che ci ha permesso di comprendere a pieno tecnologie di tutti fanno largo uso.

⁵Fa affidamento al DBMS (Database Management System) PostgreSQL.

⁶Potrebbe non essere accessibile a tutti (il repository è per privacy privato).