UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

DIPARTIMENTO DI INFORMATICA

CORSO DI LAUREA IN INFORMATICA

TESI DI LAUREA
IN
Vedi cosa fa Giacomo

APCMAM:
Inserisci un titolo Giacomo

RELATORE:
Prof.ssa Annalisa Appice

LAUREANDO:
Giacomo Gaudio

CORRELATORI:

Dott.ssa Giuseppina Andresini

ANNO ACCADEMICO 2024 2025

"Ad Oleg, a cui devo il 90% degli esami"
— Julius Robert Oppenheimer

Dedico questo lavoro ai miei cari

Indice

Disclaimer

Tutti i marchi, nomi commerciali, prodotti e loghi menzionati in questa tesi sono di proprietà dei rispettivi titolari. L'autore non rivendica alcun diritto di proprietà su tali marchi o nomi commerciali e li utilizza solo a scopo informativo e descrittivo, senza alcun intento di violazione.

Sommario

Questo è un abstract.

Capitolo 1

Introduzione

Con l'avvento dell'era digitale, sempre più attività e servizi sono migrati verso il mondo online: dall' e-commerce alla pubblica amministrazione, fino ai servizi finanziari e sanitari. In italia, secondo i dati ISTAT,l'86,2% delle famiglie italiane dispone di un accesso ad internet a testimonianza di un uso sempre più popolare [1].

Tuttavia, l'aumento della connettività comporta inevitabilmente anche una maggiore esposizione alle minacce informatiche. Nel 2024, l'Italia ha registrato il 10% degli attacchi informatici globali; secondo il rapporto Clusit, circa un terzo di tali attacchi è stato veicolato tramite l'utilizzo di malware[2].

Per malware si intende un istanza di un programma il cui intento sia malevole come carpire informazioni personali e/o arrecare danni ai dispositivi[3].

Per poter identificare i malware esistono due tipi di analisi: statica e dinamica. L'analisi statica prevede l'analisi del codice binario, analizzando ogni ramo di esecuzione possibile alla ricerca di codice malevolo. L'analisi dinamica invece prevede l'esecuzione del programma cercando di identificare un insieme di comportamenti noti tra i malware[4].

Per comportamenti intendiamo l'insieme (ordinato) delle chiamate Api al Kernel per permettere l'esecuzione dell'applicativo. Un singolo "comportamento" è effettivamente la singola chiamata Api prendendo il nome di "Api Call"; mentre la lista (ordinata) prende il nome "API call sequence"[5].

L'obbiettivo di questo caso di studio è di poter classificare un programma in base ai suoi comportamenti. Per raggiungere tale scopo sono stati raccolti diversi dataset di sequenza di chiamate api sul sistema operativo Windows ed è stato progettato e idealizzato un applicativo python (seguendo il paradigma OOP) che attraverso algoritmi di machine-learning riesca a classificare un programma in base alla sua sequenza di chiamate api.

1.1 Formato Windows PE malware

1.2 Categorie Malware

1.3 Chiamata Api Windows

1.4 Contributi

Bibliografia

[1] L. Zannella, M. Zanella, and M. Rizzo, "Report Cittadini E ICT," Istat, Report/Study, 2025. [Online]. Available: https://www.istat.it/wp-content/uploads/2025/04/REPORT_CITTADINI-E-ICT_2024.pdf

[2] C. , "© Clusit - Rapporto 2025 sulla Cybersecurity in Italia e nel mondo," Clusit, Tech. Rep., Mar. 2025. [Online]. Available: https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_03-2025_web.pdf

[3] N. Idika and A. P. Mathur, "A survey of malware detection techniques," *Purdue University*, vol. 48, no. 2, pp. 32–46, 2007. [Online]. Available: https://profsandhu.com/cs5323_s17/im_2007.pdf

[4] Y. Ki, E. Kim, and H. K. Kim, "A novel approach to detect malware based on api call sequence analysis," *International Journal of Distributed Sensor Networks*, vol. 11, no. 6, p. 659101, 2015. [Online]. Available: https://doi.org/10.1155/2015/659101

[5] Y. Qiao, Y. Yang, L. Ji, and J. He, "Analyzing malware by abstracting the frequent itemsets in api call sequences," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, July 2013, pp. 265–270. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6680850

Ringraziamenti