PROGETTO DI RICERCA Ce.Mi.S.S. ANNO 2020

Codice AP-SMD-05

1. TITOLO

Un supporto al Dominio Cyber: *AI and Deep Learning*.

2. SCOPO

L'obiettivo prefisso, nel dominio della sicurezza informatica, è il raggiungimento dell'automazione del rilevamento, dell'analisi e della classificazione tramite efficaci tecniche di apprendimento automatico valutate con dovuta scrupolosità. Pertanto, bisogna identificare e mappare le classi di algoritmi in cui è attualmente applicato l'apprendimento automatico e l'apprendimento profondo: analisi di *malware,* rilevamento di intrusioni, rilevamento di *spam, phishing* e certificazione del *software*. Inoltre, bisogna analizzare i principali limiti degli approcci esistenti e valutare la maturità delle soluzioni attuali e degli schemi di rilevamento.

3. QUADRO DI RIFERIMENTO

Nell'attuale contesto mondiale, una delle sfide significative che i ricercatori, le industrie e i governi devono affrontare nell'ambito della sicurezza informatica è la classificazione e l'individuazione dei *malware* e delle minacce. Attualmente, non è facile identificare i programmi dannosi in quanto gli aggressori utilizzano tecniche complicate come il polimorfismo, la rappresentazione, la compressione e l'offuscamento per eludere il rilevamento. Un valido supporto a tale sfida lo si può trovare nel *Deep Learning*. Difatti, l'apprendimento automatico viene adottato in una vasta gamma di domini in cui viene mostrata la superiorità rispetto agli algoritmi tradizionali basati su regole. L'apprendimento profondo, invece, si basa su una rappresentazione a più livelli dei dati di input e può eseguire la selezione delle funzioni in modo autonomo attraverso un processo apprendimento della rappresentazione definito. Questi metodi vengono integrati nei sistemi di *cyber detection* con l'obiettivo di supportare o addirittura sostituire il primo livello di analisti della sicurezza.

4. CONTENUTI

Il progetto di ricerca dovrà, di massima, analizzare i punti di seguito riportati:

- Supporto alle procedure attuali di sicurezza informatica utili per la scansione e analisi dei *malware*, rilevamento di intrusioni, rilevamento di *spam, phishing* certificazione del software;
- Supporto alle procedure di classificazione ed individuazione dei *malware;*
- Supporto o complementarità alle soluzioni di prevenzione, evitando l'esecuzione involontaria di *malware*, non noti, mediante un meccanismo di ricerca che, a partire da ipotesi, produce previsioni da sottoporre a successiva valutazione.

5. MODALITA' DI ESECUZIONE

Ricerca da fonti aperte.

6. COMPENSO

A titolo gratuito

7. PUNTO DI CONTATTO DEL COMMITTENTE

CIOC
Capo Reparto Operativo
Col. ing. SM Emanuele SCANO 202 5041
crop@cioc.difesa.it

7. PUNTO DI CONTATTO DEL RESPONSABILE DELLA RICERCA

Col. c.(li.) s.SM. Andrea CARRINO
Dipartimento Ricerche – Vice Direttore e Capo Dipartimento
Tel. 06 4691 3203 – mil. 23203/23218
caporicerche.cemiss@casd.difesa.it; ricerche.cemiss@casd.difesa.it