L'INTELLIGENZA ARTIFICIALE E LA CYBER SECURITY

Brusotti Stefano
Caprella Ettore Elio
Francini Gianluca
Romagnoli Andrea

Lo sviluppo e l'applicazione dell'Intelligenza Artificiale sta progredendo in tutti i settori. Non fa eccezione quello della sicurezza delle informazioni e in particolare della Cyber Security che si occupa di rendere sicuro il cosiddetto cyberspazio, o spazio cibernetico, la quinta dimensione, dopo terra, acqua, aria e spazio in cui si sviluppano le attività e gli interessi di persone, imprese e stati. In TIM, a Torino, il Security Lab sta lavorando da alcuni anni allo studio e alla sperimentazione di queste tecnologie e in particolare all'applicazione pratica degli algoritmi di Machine Learning alle informazioni rilevanti per la sicurezza dei dati, delle reti e delle applicazioni.

Introduzione

Viviamo in un mondo in cui la tecnologia sta permeando le nostre case e le nostre aziende, con una rapidità di crescita ed evoluzione esponenziale. Ray Kurzweil, colui che sarebbe poi divenuto "*Director of Engineering*" di Google, nel 2001 formulò la legge dei ritorni acceleranti [**nota 1**], secondo la quale nel ventunesimo secolo non avremmo sperimentato 100 anni di progresso, bensì 20.000. Da quel momento abbiamo assistito alla diffusione degli *Smartphones*, alla nascita del *Cloud*, dell'*IoT*, delle *BlockChains*, e allo sviluppo dei Big Data solo per cita-

re alcuni esempi. Purtroppo l'evoluzione tecnologica non porta solo al progresso, ma anche alla crescita di tecniche d'attacco sempre più avanzate. Il caso più eclatante degli ultimi anni è stato sicuramente il *worm-ransomware WannaCry* di maggio 2017: se nel codice sorgente non fosse stato presente un grossolano kill-switch, ovvero un meccanismo per bloccarne la diffusione, le conseguenze sarebbero state ben più gravi [**nota 2**] rispetto ai centomila sistemi infettati in 105 diversi Paesi [**nota 3**]. Il modo più efficace per contrastare la sempre maggiore diffusione di tecniche d'attacco avanzate e innovative è quello di raccogliere e utilizzare un numero sempre maggiore di informazioni, per poter analizzare e prevedere le minacce ancor prima della loro diffusione massiva.

Volendo immaginare uno scenario futuribile, ma non troppo, pensiamo che non siano lontani i tempi in cui i *Security Operations Center* potranno avere a disposizione sistemi integrati per la raccolta, l'interpretazione e l'analisi di grandi moli dati, coadiuvati da soluzioni di *Artificial Intelligence* in grado di identificare sempre più autonomamente le minacce e capire come affrontarle, riducendo al minimo gli eventuali falsi positivi e permettendo una difesa sempre più efficace, proattiva e tempestiva delle risorse aziendali.

Per puntare a questo scenario è necessario costruire le condizioni per rendere efficace l'applicazione delle tecniche più avanzate di *Artificial Intelligence*. Prima condizione importante è il possesso di una grande mole di dati strutturati che forniscano un'adeguata Knowledge Base, essenziale per effettuare il training accurato degli algoritmi di ML (*Machine Learning*). Secondo elemento rilevante è l'estrazione di informazione dalla grande quantità di dati non strutturati fruibili da Internet affiancando, pertanto, agli strumenti di web crawling soluzioni di NLP (*Natural Language Processing*) in grado di interpretare e trasformare i dati in maniera sistematica, rendendoli fruibili a una fase successiva di elaborazione.

L'evoluzione del Machine Learning

L'obiettivo del *Machine Learning* è quello di estrarre informazioni significative da dati grezzi e più dati abbiamo a disposizione e più sarà sofisticato il sistema che potremo costruire. È un fatto che aumentando i dati processati è possibile ottenere sintetizzatori vocali sempre più simili alla voce umana, traduttori di lingue più precisi e auto a guida autonoma più affidabili.

La disponibilità di una vasta mole di dati e l'elevata capacità computazionale offerta dall'hardware moderno hanno consentito di realizzare i sofisticati sistemi di intelligenza artificiale che fino a qualche anno fa sembravano far parte più della fantascienza che della scienza.

Esiste però anche un terzo pilastro fondamentale alla base di questa rivoluzione: le reti neurali profonde. Nell'approccio tradizionale al *Machine Learning*, un esperto del dominio definisce quali sono le caratteristiche salienti da estrarre dai dati. Ad esempio, nel caso di un classificatore di immagini, gli elementi salienti possono essere i contorni degli oggetti o le variazioni locali di luminosità nella scena. Dopo aver definito manualmente queste caratteristiche, l'esperto stabilisce come aggregare le informazioni estratte in modo che siano sia compatte che facilmente confrontabili e infine esegue la vera e propria fase di *Machine Learning*, in cui il sistema apprende a eseguire una classificazione sulla base delle informazioni caratterizzanti l'immagine. Con le reti neurali profonde, queste operazioni sono completamente demandate alla fase di apprendimento. L'esperto definisce un'architettura, spesso piuttosto generica, del cervello artificiale ed è durante la fase di addestramento, basata sull'elaborazione dei dati grezzi, che la rete impara automaticamente a estrarre e aggregare le informazioni più significative. Questo approccio ha due vantaggi rilevanti: le caratteristiche salienti così determinate sono migliori di quelle che potrebbero essere stabilite manualmente da un essere umano e i dati eterogenei possono essere fusi insieme in modo efficace.

Questo secondo aspetto è particolarmente importante negli scenari

di applicazione per la *Cyber Security*, in cui si hanno a disposizione dati di natura molto differente, che vanno dai flussi di rete, ai log dei server fino alle informazioni più destrutturate come quelle relative all'interazione delle persone. Le reti neurali profonde riescono a unire insieme queste informazioni di natura ben diversa, dandone una rappresentazione omogenea e mantenendo gli elementi essenziali per rilevare i comportamenti anomali o fraudolenti.

Come è avvenuto in molti settori, l'intelligenza artificiale rappresenta un'arma fondamentale nella Cyber Security, ma occorre ricordarci che è a disposizione anche di chi vuole commettere atti criminali e quindi anche gli attacchi saranno destinati a essere sempre più sofisticati e richiederanno una risposta adeguata.

Applicazione dell'Intelligenza Artificiale per la Cyber Security in TIM

Le fondamenta per l'applicazione delle tecnologie di ML e AI sono state gettate, nell'ambito della *Cyber Security* in TIM, più di 4 anni fa quando abbiamo iniziato a progettare e a costruire la piattaforma di *Big Data di Security*.

Avevamo in mente uno strumento che dovesse essere flessibile, scalabile e che ci permettesse di aggiungere nel tempo nuove funzionalità per restare al passo con l'innovazione tecnologica.

Volevamo una piattaforma che consentisse di accedere rapidamente ai dati superando le problematiche relative alla loro interpretazione. Doveva pertanto essere in grado di indicizzare dati non strutturati e consentire ricerche di tipo text-based su centinaia di *terabyte*, con il fine di abbattere il tempo di ricerca per la gestione degli incidenti di *Cyber Security*. Tuttavia era anche ben chiara l'esigenza di dover e poter lavorare su dati strutturati per costruire analytics utili ai nostri analisti di sicurezza: obiettivo principale era, ed è tuttora, agevolare gli operatori del SOC fornendo automaticamente indicatori per l'individuazione di potenziali problemi di sicurezza e per rendere più semplice il processo di *incident-handling*.

Inoltre, durante la fase di progettazione del sistema, abbiamo ritenuto particolarmente importante garantire all'analista di sicurezza una semplice fruizione dell'informazione tramite la rappresentazione visuale dei dati, lasciando ad esso la scelta del miglior formato in funzione del contesto.

A tal riguardo, un paio di anni prima avevamo messo in campo la piattaforma VizSec che aveva proprio l'obiettivo di complementare l'approccio all'analisi degli eventi di sicurezza introducendo la componente visuale di esplorazione del dato. Crediamo fortemente in questo approccio innovativo alle analisi di sicurezza, tanto che la piattaforma VizSec è stata integrata nella soluzione di *Big Data di Security* ed è stata affiancata ad ulteriori strumenti di rappresentazione del dato.

Le componenti tecnologiche alla base della soluzione Big Data di Security sono al momento:

- Elasticsearch [nota 4]
- Hadoop nella distribuzione HDP di Hortonworks [nota 5]
- SAS Visual Analytics [nota 6]

La scelta di adottare tecnologie abilitanti l'utilizzo delle tecniche di ML è stata frutto di un'attenta valutazione. Nel corso di questi anni abbiamo infatti potuto osservare come l'evoluzione tecnologica e degli algoritmi basata su logiche di ML fosse dirompente ed eravamo sicuri che prima o poi il fenomeno avrebbe interessato il contesto *Cyber Security*. Era quindi necessario raccogliere la sfida e prepararsi al futuro: avere cioè a disposizione dati, capacità computazionale e framework software da utilizzare al fine di integrare soluzioni basate su AI e verificarne l'efficacia all'ambito *Cyber Security*.

Ad oggi la piattaforma di Big Data di Security è a regime per quel che riguarda la raccolta di dati e la rappresentazione di *analytics*, ed è in continua evoluzione anche al fine di integrare nuove fonti. Negli ultimi tempi abbiamo iniziato ad esplorare e a provare le soluzioni di AI che venivano messe a disposizione dai *framework* in nostro possesso. In particolare abbiamo iniziato ad utilizzare la nuova feature Machine Learning di Elasticsearch. Si tratta di un sistema per l'individuazione di

L'ESPERIENZA DAL CAMPO

Il punto di vista di Marco Gazza

(SEC.CS SECURITY OPERATIONS CENTER DI TIM)

Dal punto di vista dell'utilizzo on field, l'introduzione di strumenti di *Analytics e Machine Learning* ha permesso di gestire problematiche che richiedono analisi estremamente complesse. Nell'*Incident Handling* le analisi visuali permettono di velocizzare i tempi di risposta, di valutare al volo scenari alternativi, di filtrare e restringere velocemente il campo di analisi fino al dettaglio di interesse. È di interesse per esempio capire il primo, nella serie storica, degli eventi che ha dato origine ad un *data breach*, valutare che non ci siano stati accessi non autorizzati a risorse, oppure che non si nascondano eventi malevoli nella immensa quantità di log di accesso ad un portale, quando i sistemi "classici" di difesa del perimetro come firewall, IDS (*Intrusion Detection System*), e sonde non rilevano nulla di malevolo. Inoltre, alcune "*query*" banali dal punto di vista concettuale, tipo "quanti eventi di log ci sono con codice di risposta KO per questa URL?" non lo sono affatto dal punto di vista pratico quando la mole di dati in gioco rende giustizia al concetto di *Big Data*. In fase di *Hunting*, la predisposizione di *Report* con *Analytics* mirati ad aspetti di sicurezza consente di osservare l'occorrenza di fenomeni malevoli altrimenti difficilmente rilevabili ed inoltre ci sono grandi aspettative per il ML, che è in fase di valutazione. In questo ambito, gli algoritmi di *Machine Learning* non supervisionato sembrano essere la prima opzione, infatti sia il ML di Elasticsearch che la soluzione *Cyber* di SAS sfruttano questo tipo di approccio. Questo è piuttosto coerente rispetto alla estrema difficoltà di definire cosa è anomalo e cosa è normale nell'ambito *security*. Per dirla con le parole di Heather Adkins (*Google, Director of Information Security & Privacy): "...we just don't have a sense of what is good and bad from a security security perspective...*" [*https://www.youtube.com/watch?v=9y2JBsNFHcw*]. Questo comporta però di dover gestire l'effetto collaterale di un grande numero di falsi positivi.

In ambito TIM gli scenari di *Machine Learning* che stanno funzionando meglio sono quelli dove il "campo d'azione" degli algoritmi è stato ristretto a priori: se sparare nel mucchio (tutti i log di una certa sorgente come i portali) al momento non sembra particolarmente efficace e produce un numero eccezionalmente elevato di falsi positivi, restringere il campo a priori, ovvero tecnicamente eseguire un campionamento estremamente "biased" su condizioni specifiche di comportamento (ad esempio solo una porzione di sito web) è stato decisamente più utile ■

marco.gazza@telecomitalia.it

anomalie all'interno di serie temporali che utilizza tecniche di *Machine Learning* con apprendimento non supervisionato.

Più nel dettaglio consente il riconoscimento di anomalie associate alla deviazione temporale di valori, conteggi o frequenze. Permette inoltre l'identificazione di comportamenti anomali di un elemento all'interno di una popolazione e infine segnala eventi statisticamente rari.

Abbiamo deciso di mettere alla prova la soluzione utilizzando gli access log di alcuni dei portali web di TIM.

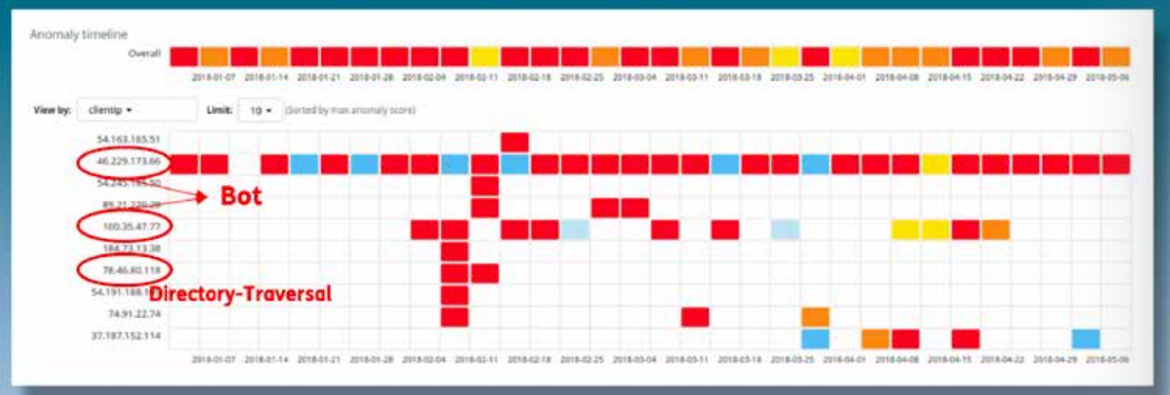
I risultati li possiamo definire promettenti in quanto il sistema è stato in grado di elaborare centinaia di milioni di righe di log in breve tempo, fornendo indicazioni puntuali sulle anomalie riscontrate. Tuttavia è evidente che siamo solo all'inizio di un lungo percorso: le anomalie sono sicuramente tali dal punto di vista statistico e dal punto di vista degli algoritmi di *Machine Learning* ma non è assolutamente detto che un'anomalia statistica sia sempre sintomo di un problema di sicurezza. Come spesso accade nei sistemi di *Machine Learning*, uno degli obiettivi è quello di minimizzare il FPR (*False Positive Rate*). Avendo una piattaforma contenente miliardi di righe di log, anche un FPR molto basso si tradurrebbe in valore assoluto in un numero molto significativo di segnalazioni [**nota 7**].

Si deve pertanto ancora lavorare molto focalizzando l'attenzione sull'arricchimento dei dati, sull'individuazione delle features più significative e sulla scelta degli algoritmi da utilizzare.

Conclusioni

L'aspettativa per i vantaggi che l'applicazione dell'Intelligenza Artificiale potrà portare alla *Cyber Security* è molto alta. Le prospettive sono buo-

1
Individuare un inusuale numero di request da parte di un client ip



2
Individuare IP che frequentemente accedono a uri_path rari

ne e ci si sta muovendo sempre più rapidamente in una direzione che apparare molto promettente.

È tuttavia importante ricordare che esistono criticità e specificità legate al dominio della sicurezza. Ad esempio i log applicativi, una delle fonti primarie di dati per le analisi di sicurezza, sono tipicamente strutturati in modo da fornire informazioni utili per le operations oppure per il *troubleshooting* ma molto meno per la security. Migliorare all'origine la qualità dell'informazione in ottica sicurezza è un obiettivo che tutti si dovrebbero dare. Anche solo inserire nei tracciati informazioni utili per analizzare problematiche di sicurezza connesse alla AAA (*Authorization, Authentication, Accounting*) e soprattutto generare i log in formati "standard" come ad esempio il formato CSV o il formato JSON permetterebbe di fare un bel passo avanti. Altro aspetto da non trascurare è l'impatto che i vincoli normativi e di privacy posso determinare all'applicazione di queste tecnologie in certi domini. In questo ambito lo sforzo di tutti deve essere volto a trovare il miglior compromesso tra le esigenze di *Cyber Defense* e privacy, ricordando l'asimmetria che nel mondo cyber da sempre esiste tra attaccanti, che tutto possono, e i difensori. Le stesse tecnologie dell'Intelligenza Artificiale sono utilizzabili e utilizzate dagli attaccanti. Recentemente ad esempio usando algoritmi di ML è stato creato un chatbot per phishing mirato su twitter [**nota 8**] finalizzato al furto di informazioni che ha avuto quasi il 100% di successo! ■

Note

1. http://www.kurzweilai.net/the-law-of-accelerating-returns
2. https://www.financialexpress.com/industry/technology/major-cyber-attacks-over-the-past-10-years/667347/
3. http://www.repubblica.it/tecnologia/sicurezza/2017/05/12/news/maxi_attacco_hacker_mondiale_virus_chiede_riscatto_colpita_anche_l_italia_-165285797/
4. https://www.elastic.co/
5. https://hortonworks.com/products/data-platforms/hdp/
6. https://www.sas.com/en_us/software/visual-analytics.html
7. Ad esempio su 1 miliardo di righe di log, circa 3 mesi dei log dei portali web, e un FPR dello 0,01%, cioè molto basso, si avrebbero comunque 100.000 segnalazioni in 3 mesi da gestire e verificare.
8. https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter.pdf

Stefano Brusotti *stefano.brusotti@telecomitalia.it*

responsabile del Security Lab di TIM, si occupa dei processi di threat intelligence management e delle attività di presidio dell'evoluzione delle minacce cyber, dell'ideazione e dello sviluppo di piattaforme innovative per la cyber security, delle attività di scouting per l'identificazione delle nuove soluzioni di sicurezza e dell'erogazione dei servizi di security testing per le diverse esigenze interne. Laureato in Scienze dell'Informazione con master COREP in Telecomunicazioni, ha iniziato a lavorare nel Centro Ricerche del Gruppo Telecom Italia nel 1996 occupandosi da subito di sicurezza delle informazioni e delle reti. ■

Ettore Elio Caprella *ettoreelio.caprella@telecomitalia.it*

laureato in Ingegneria Informatica e in Economia e gestione delle imprese, ha iniziato a lavorare nel 2000 presso Telecom Italia. Ha sempre lavorato nell'ambito della Sicurezza Informatica occupandosi principalmente dello sviluppo prototipale di soluzioni innovative di sicurezza. Nel 2013 ha conseguito la certificazione PMP del Project Management Institute. Dal 2015 si occupa di Big Data ed è responsabile della piattaforma BigData4Security (aka SODS) che raccoglie e indicizza log applicativi e di sicurezza utili alla costruzioni di analytics funzionali ai processi di Cyber Security. È co-inventore di 7 brevetti nel campo dei sistemi di autenticazione SIM-based e dei metodi per il controllo non ripudiabile delle transazioni. Attualmente è responsabile del team di Security Prototyping nella funzione Security Lab. ■

Gianluca Francini *gianluca.francini@telecomitalia.it*

laureato in Scienze dell'Informazione, ha iniziato al sua attività lavorativa nel campo avionico, passando nel 1996 al settore delle telecomunicazioni come ricercatore del gruppo Multimedia del Centro Studi e Laboratori Telecomunicazioni (CSELT). Nel gruppo Multimedia ha lavorato su temi di computer vision, in particolare sulle applicazioni di teleconferenza tridimensionale, sui sistemi di ricostruzione 3D e sulla codifica video scalabile. Nel 2006 è entrato a far parte della struttura Research Project, lavorando su tecniche di raccomandazione di contenuti e sulla ricerca visuale, sviluppando tecnologie che sono diventate parte dello Standard Internazionale MPEG Compact Descriptors for Visual Search. È attualmente responsabile del Joint Open Lab Cognitive Computing TIM/Politecnico di Torino, laboratorio in cui si sviluppano algoritmi di analisi dei dati aziendali mediante l'adozione di tecniche di machine learning. È co-inventore di 19 brevetti nel campo dell'analisi delle immagini e del Deep Learning. ■

Andrea Romagnoli *andrea.romagnoli@telecomitalia.it*

Laureato Magistrale in Informatica presso l'Università degli Studi di Torino, nel 2016 ha iniziato il suo percorso lavorativo in TIM. Inizialmente si è occupato di scouting e testing di soluzioni IDS/IPS open source, per poi lavorare nel campo della Log Analysis con tecnologie Big Data come ElasticSearch e Hadoop, applicate alla Cyber Security. Durante gli studi universitari ha potuto approfondire tematiche legate all'Intelligenza Artificiale, laureandosi nel 2015 con il massimo dei voti con la tesi "Animazione facciale non rigida basata su deformazione di mesh poligonali", frutto di un anno di lavoro presso il Centro Ricerche e Innovazione Tecnologica RAI.
La sua formazione in ambito tecnologico è accompagnata da una formazione prettamente artistica, coronata nel 2012 dal conseguimento del Diploma di violino presso il Conservatorio di Musica di Trento, con il massimo dei voti ■