TIM

CYBERSECURITY

notiziariotecnico

1-2024

Il **Notiziario Tecnico** è un webmagazine, con taglio tecnico-divulgativo che presenta in modo ragionato l'evoluzione del settore delle tecnologie dell'informazione, dando particolare attenzione alle sinergie tra innovazione digitale e scenari di business.

Notiziario Tecnico
Anno 33 - Numero 1, Aprile 2024
www.telecomitalia.com/notiziariotecnico

Proprietario ed editore
TIM S.p.a.

Direttore responsabile
Michela Billotti

Comitato di direzione
Gabriele Elia
Daniele Franceschini
Elisabetta Romano
Federica Romano

Web Director
Enrico Gallo

Photo
123RF Archivio Fotografico
Archivio Fotografico TIM

Redazione
Roberta Bonavita
Giampiero Rossi

Contatti
Via G. Reiss Romoli, 274, 10148 Torino
notiziariotecnico.redazione@telecomitalia.it

Registrazione
Presso il Tribunale di Torino n. 60 del 03/11/2021 - ISSN 2038-1921

Editoriale

Il tema della cybersecurity è sempre più attuale e riveste un ruolo cruciale nel mondo delle telecomunicazioni, dove le minacce si evolvono costantemente.

Secondo una ricerca **dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano**, nel solo primo trimestre del 2023 ci sono stati 1.382 incidenti gravi rilevati dal Clusit, +11% rispetto allo stesso periodo del 2022. In Italia, ben il 74% delle grandi organizzazioni nazionali ha rilevato un incremento dei tentativi di attacco subìti e il 12% ha registrato conseguenze tangibili derivanti da un incidente informatico. Di recente il procuratore nazionale antimafia e antiterrorismo, **Giovanni Melillo**, intervenendo al convegno "Violenza della rete, violenza nella rete", ha dichiarato che l'Italia è al terzo posto in Europa e al sesto nel mondo per attacchi ransomware ed ha aggiunto che nel nostro Paese si è registrato un aumento del 23% degli attacchi informatici solo in questo ultimo anno.

È chiaro che gli attacchi informatici, dalle violazioni dei dati alle minacce ransomware, mettono in grave rischio la sicurezza delle informazioni sensibili; ed è per questo che le organizzazioni devono investire sempre più in tecnologie avanzate di difesa anche basate sull'IA e sull'apprendimento automatico per anticipare e neutralizzare queste minacce.
La cybersecurity si conferma infatti una priorità di investimento nel digitale tra le imprese: nel 2023 il

mercato italiano della cybersecurity ha raggiunto il record di 2,15 miliardi di euro, +16% rispetto al 2022. A ciò si aggiunge che il rapporto tra spesa in cybersecurity e PIL in Italia si attesta allo 0,12%; in crescita, certo, rispetto allo 0,1% del 2022, ma, nonostante l'aumento, l'Italia resta all'ultimo posto nel G7, a grande distanza dai primi in classifica, Stati Uniti (0,34%) e Regno Unito (0,29%), e da Paesi come Francia o Germania allo 0,19%.

In questo contesto in continua evoluzione, come Gruppo TIM siamo fortemente impegnati nello sviluppare nuove protezioni contro gli attacchi informatici, certi che la convergenza tra Intelligenza Artificiale e cybersecurity sia essenziale. Dato che è riportato anche nello studio di **Acumen Research and Consulting**, in base al quale il mercato globale dei prodotti di cybersecurity basati sull'IA raggiungerà la notevole cifra di 133,8 miliardi di dollari entro il 2030.
Ma noi di TIM guardiamo oltre e siamo in prima linea anche nel diffondere una "cultura sulla cybersecurity", frutto della collaborazione tra pubblico e privato, per sviluppare nuove competenze, in modo da disegnare profili e percorsi formativi adeguati alle esigenze del mercato del lavoro digitale.
Per questo **TIM e la Cyber Security Italy Foundation** hanno siglato un protocollo di intesa per diffondere già nelle scuole dell'obbligo una cultura sulla cybersicurezza mirata a studiare la minaccia cibernetica soprattutto sotto il profilo della Cyber Threat Intelligence, in modo da formare giovani con competenze digitali per una crescita sociale consapevole, sostenibile e inclusiva.

Per tutti questi motivi, poiché riteniamo che la consapevolezza riguardo alla cybersecurity debba essere diffusa a tutti i livelli, abbiamo deciso di focalizzare questo numero del Notiziario Tecnico sul nostro impegno in questa cruciale tecnologia.

Vi auguro una buona lettura

Elisabetta Romano
Chief Network, Operations & Wholesale Office, TIM

Indice

TIM

Un caffè con...
Matteo Macina
Director of Cybersecurity in TIM

A cura di Michela Billotti

Con l'implementazione dell'Intelligenza Artificiale nella cybersecurity, dott. Macina, come sono cambiate le cose in Italia ed in particolare in TIM cosa stiamo predisponendo?

Con l'implementazione dell'Intelligenza Artificiale nella cybersecurity, in Italia, e in particolare in TIM, si è assistito a una trasformazione significativa nel modo in cui affrontiamo le minacce digitali. Grazie all'utilizzo di algoritmi di machine learning, sempre più spesso disponibili nelle piattaforme di sicurezza e di sistemi di rilevamento avanzati, siamo in grado di identificare e contrastare le minacce in tempo reale, migliorando la nostra capacità di difesa e risposta. Tuttavia, va sottolineato che gli attaccanti stanno anche sfruttando l'Intelligenza Artificiale per scopi malevoli. Un esempio sono gli attacchi di phishing potenziati dall'Intelligenza Artificiale generativa, in cui algoritmi di machine learning vengono impiegati per generare messaggi di phishing altamente personalizzati e convincenti, difficili da distinguere da comunicazioni autentiche.
Inoltre, si sono registrati casi di utilizzo di deepfake, una tecnologia basata sull'IA generativa, per manipolare e falsificare contenuti audiovisivi al fine di diffondere disinformazione o danneggiare l'immagine di individui o aziende. Questi sviluppi sottolineano l'importanza di mantenere un approccio proattivo alla sicurezza informatica, includendo la capacità di rilevare e mitigare le minacce basate sull'IA generativa. In TIM, stiamo continuamente migliorando le nostre difese per adattarci a questa evoluzione delle minacce digitali, integrando tecniche avanzate di rilevamento delle anomalie e di analisi comportamentale per identificare e contrastare anche attacchi basati sull'IA generativa.

Secondo una recente analisi di Gartner, entro il 2025, ben il 75% delle aziende subirà un attacco ransomware; contro questa minaccia cosa facciamo in TIM? E quali servizi offriamo per proteggere le aziende italiane?

Di fronte alla crescente minaccia degli attacchi ransomware, in TIM stiamo adottando una serie di misure preventive e reattive sia tecnologiche che processive. Offriamo servizi di sicurezza informatica avanzati alle aziende italiane, tra cui soluzioni di backup e ripristino, monitoraggio continuo delle minacce, e formazione del personale per riconoscere e affrontare gli attacchi ransomware. Inoltre, stiamo potenziando le nostre infrastrutture e collaborando con partner specializzati per migliorare la resilienza e la protezione dei nostri clienti.

Quali sono i punti d'attenzione che vanno più costantemente monitorati per evitare i più comuni errori legati alla gestione della cybersecurity?

I punti d'attenzione che vanno costantemente monitorati per evitare errori legati alla gestione della cybersecurity includono la vulnerabilità delle infrastrutture

digitali, la sicurezza dei dati sensibili, la consapevolezza del personale e la conformità normativa. È essenziale adottare una strategia olistica che comprenda la protezione delle reti, la gestione degli accessi, la crittografia dei dati e la formazione continua del personale, in uno scenario di gestione del rischio che combina i vincoli delle vecchie infrastrutture informatiche e di rete con il mondo del cloud e, per un operatore come TIM, delle reti di nuova generazione e dei servizi che queste abilitano.

Per cambiare passo nel fronteggiare le minacce cyber, oltre ad una maggior diffusione di una cultura pro-sicurezza informatica nelle aziende, quale altro fattore vede determinante? In tal senso, secondo lei, la politica può avere un ruolo proattivo?

Per affrontare efficacemente le minacce cyber, oltre alla diffusione di una cultura pro-sicurezza informatica, è fondamentale anche il coinvolgimento attivo della politica e delle istituzioni.
La politica può svolgere un ruolo proattivo nel promuovere normative e regolamenti che favoriscano la sicurezza digitale, incentivando la collaborazione tra pubblico e privato, investendo in ricerca e sviluppo di tecnologie avanzate per contrastare le minacce digitali e favorendo la formazione del personale specialistico, ma anche diffondendo la cultura della cyber sicurezza a livello di cittadinanza nel suo complesso.

Infine, quali strategie e meccanismi specifici possono essere adottati a livello globale per implementare politiche di sicurezza informatica più efficienti volte a garantire una circolazione dei dati più efficace e protetta?

A livello globale, per implementare politiche di sicurezza informatica più efficienti, è necessario adottare una strategia multilaterale che coinvolga governi, aziende, organizzazioni internazionali e società civile. Questa strategia dovrebbe includere la condivisione delle informazioni sulle minacce, lo sviluppo di tecnologie esclusive e di nuovi standard e protocolli comuni, incentivi per le aziende che investono in miglioramenti sulla sicurezza informatica, la promozione di una cultura di sicurezza digitale e la collaborazione tra paesi della stessa area geo politica per contrastare le minacce cyber in modo coordinato e quindi più efficace.■

Autori

Michela Billotti *michela.billotti@telecomitalia.it*

Giornalista, direttore responsabile del Notiziario Tecnico TIM, è passata dal mondo delle lettere classiche, in cui si è laureata nel 1993, al settore delle telecomunicazioni. Da oltre vent'anni in Azienda ha dapprima collaborato all'organizzazione di eventi nazionali e internazionali, poi gestito i rapporti con i media interessati all'evoluzione dell'ICT; ora coordina i vari aspetti della comunicazione tecnica. È autrice di articoli e di libri sull'evoluzione del mondo delle telecomunicazioni scritti per un pubblico di "non addetti ai lavori". ■

Matteo Macina *matteo.macina@telecomitalia.it*

Matteo Macina, matematico, ha iniziato la sua carriera in Deloitte di cui è stato Manager per i Cyber Risk Service, per poi ricoprire vari incarichi manageriali anche presso Terna S.p.A. dove è stato responsabile del Cyber Defence Center.
Dal 2022 è direttore della struttura Cyber Security di TIM con la responsabilità di assicurare, a livello di Gruppo, la sicurezza logica e la tutela delle risorse informatiche e infrastrutturali, degli asset ICT nonché delle informazioni, garantendo altresì le attività di engineering e application management di competenza. Inoltre, collabora come docente con il dipartimento di Economia Aziendale di Roma Tre sui temi di Governance, Sistemi di Controllo e Auditing. ■

Intelligenza Artificiale e Cybersecurity

Madalina Baltatu, Luigi Gallo, Maria Saleri

L'articolo esplora l'intersezione tra Intelligenza Artificiale (IA) e Cybersecurity, mettendo in evidenza come le tecnologie basate sull'IA stiano rivoluzionando il campo della sicurezza informatica. Vengono esaminati i metodi con cui l'IA contribuisce al rafforzamento delle difese contro le minacce informatiche, attraverso il riconoscimento di schemi complessi e l'apprendimento autonomo per prevenire attacchi. L'analisi si estende anche agli utilizzi malevoli delle stesse tecnologie di IA, con cenni ai rischi e alle sfide etiche che esse pongono.

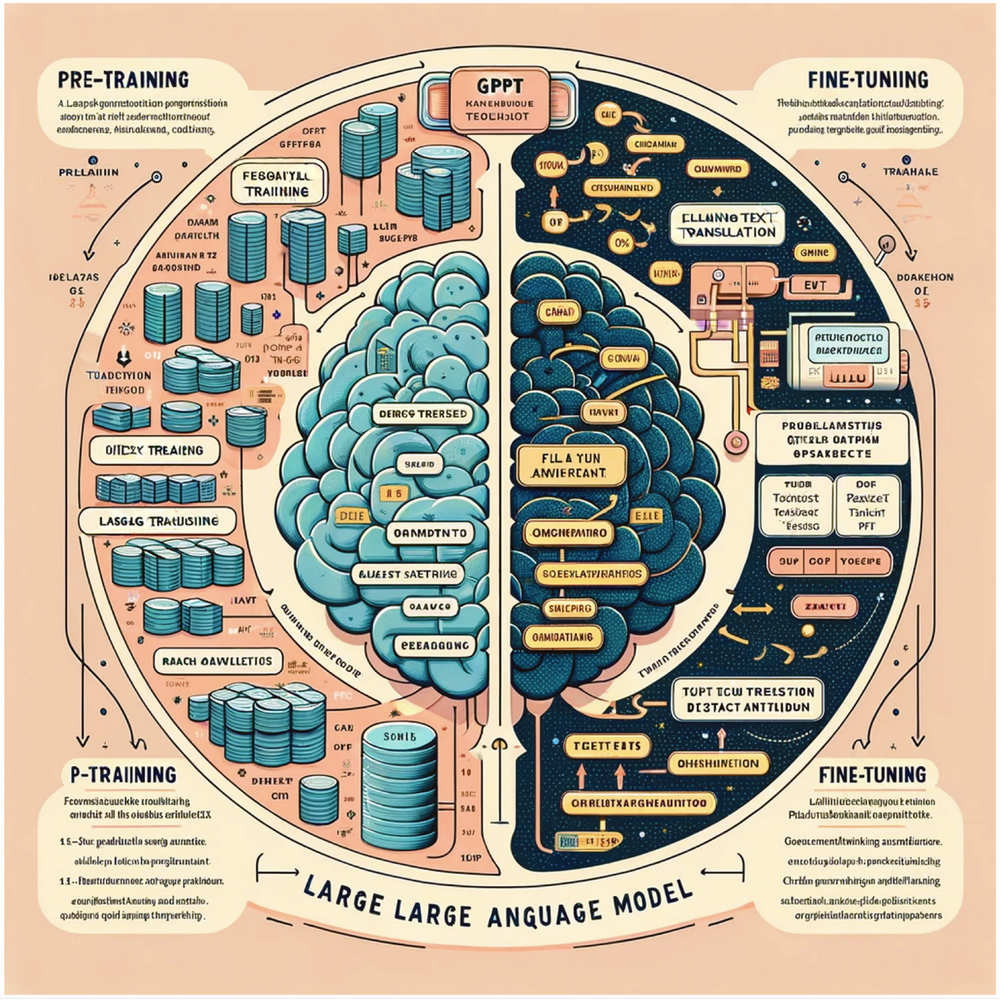
L'emergere di strumenti di Intelligenza Artificiale (IA) generativa rivolti al consumo su larga scala ha rapidamente e radicalmente modificato l'opinione pubblica relativamente al potere e al potenziale dell'IA. Precedentemente relegata ad un utilizzo molto più circoscritto e limitato, nell'ultimo anno si è rivelata come un rivoluzionario avanzamento della tecnologia che promette opportunità (e rischi) notevoli. Si prevede che l'IA avrà un grande impatto sul mondo del lavoro e automatizzerà la metà di tutte le professioni tra il 2040 e il 2060 [1]. Ne consegue che le professionalità e gli strumenti nell'ambito della Cybersecurity si evolveranno, anche in funzione dei cambiamenti che l'Intelligenza Artificiale apporterà al panorama delle minacce informatiche da fronteggiare.

Introduzione all'Intelligenza Artificiale

L'Intelligenza Artificiale (IA) è una branca dell'informatica che si occupa di creare algoritmi capaci di eseguire compiti che, tradizionalmente, richiederebbero l'intelligenza umana. Questi compiti includono: il riconoscimento di schemi, l'apprendimento da dati, l'interpretazione del linguaggio naturale, la presa di decisioni e la soluzione di problemi.
Al cuore dell'IA ci sono gli algoritmi di machine learning e deep learning, che permettono ai sistemi di migliorare le loro prestazioni apprendendo automaticamente dall'esperienza. Il machine learning utilizza modelli statistici per fare previsioni o prendere decisioni basandosi su dati passati, mentre il deep learning, sfruttando reti neurali artificiali con molteplici strati, è in grado di catturare relazioni complesse nei dati.
L'ultima frontiera dell'Intelligenza Artificiale è quella cosiddetta Generativa (GenAI), che non si limita a interpretare o analizzare i dati, ma è capace di crearne di nuovi, imitando o innovando su basi esistenti. Questo tipo di IA utilizza approcci come le reti generative avversarie (GAN) [2] e i modelli di linguaggio per generare contenuti originali, che vanno da immagini e musica a testi e oltre. Questa capacità di generare contenuti nuovi e personalizzati apre nuove frontiere nell'arte, nel design, nell'educazione e nell'intrattenimento, promettendo di rivoluzionare il modo in cui creiamo e interagiamo con i media digitali.
All'interno dell'universo dell'Intelligenza Artificiale generativa, i Large Language Models (LLM) rappresentano una pietra miliare per il trattamento e la generazione del linguaggio naturale. Questi modelli sono stati addestrati su vasti corpus di testo che abbracciano l'intera gamma della conoscenza e dell'espressione umana disponibile online. Attraverso l'apprendimento profondo e l'analisi di miliardi di parole, gli LLM hanno acquisito una notevole capacità di comprendere e generare testi in modo coerente e contestualmente rilevante, spaziando dalla creazione di articoli e racconti al rispondere a domande e simulare dialoghi.
La loro flessibilità e potenza li rendono strumenti preziosi per una varietà di applicazioni, come l'assistenza automatizzata al cliente, la creazione di contenuti, la traduzione automatica e l'istruzione, sfidando continuamente i confini tra la comunicazione umana e quella artificiale [3].
Abbiamo chiesto ad un modello di GenAI di generare un diagramma educativo che illustra le due fasi principali nel funzionamento dei Large Language Models (LLM),

ottenendo la Fig.1 come risultato. L'immagine abbozza una rappresentazione visiva che evidenzia la due fasi di training degli LLM: la fase di pre-training, dove una vasta raccolta di testi viene elaborata e utilizzata per l'addestramento iniziale della rete neurale, e la fase di fine-tuning, dove il modello viene ulteriormente addestrato su un dataset specifico per compiti precisi. Riteniamo sia importante evidenziare anche le limitazioni di queste tecnologie: limitazioni nella precisione, generalizzazione eccessiva, ambiguità, variazioni di stile, potenziali bias e difficoltà nel rappresentare dettagli tecnici specifici (i.e. le parti testuali).
Questo può risultare in rappresentazioni semplificate o vagamente accurate di concetti complessi. È importante tenere a mente, tuttavia, che siamo solo agli inizi dell'evoluzione di queste impressionanti tecnologie.

Figura 1: Immagine generata con GenAI che rappresenta l'addestramento di un LLM



Applicazioni dell'Intelligenza Artificiale in Cybersecurity

L'Intelligenza Artificiale sta trasformando il campo della Cybersecurity, tramite nuovi strumenti e approcci per affrontare minacce sempre più avanzate. Le tecnologie IA possono rapidamente individuare correlazioni e modelli nei dati. Attualmente, l'IA è principalmente utilizzata come supporto all'analista, operando in un ambiente semiautomatico.
La Fig.2 riassume alcuni degli utilizzi difensivi dell'Intelligenza Artificiale.
Le tre principali aree della sicurezza informatica in cui l'IA è efficacemente integrata sono: il rilevamento delle minacce, l'automazione di eventuali risposte ad esse e la loro previsione o prevenzione.

Rilevamento delle minacce

L'Intelligenza Artificiale ha ottenuto risultati significativi nel rilevare le minacce informatiche.
Gli algoritmi di machine learning possono esaminare enormi quantità di dati in tempo reale per individuare comportamenti anomali o modelli non usuali.

Alcuni esempi includono:
- **rilevamento delle anomalie** anche quando le minacce sono nuove o sconosciute;
- **analisi comportamentale** per individuare attività potenzialmente dannose o non autorizzate;
- **rilevamento di malware.**

Automazione della risposta alle minacce

Oltre al rilevamento, l'Intelligenza Artificiale permette una risposta automatizzata più efficiente alle minacce. Ciò implica che i sistemi di sicurezza possano reagire con maggiore prontezza ed efficienza alle minacce in tempo reale.

Ecco alcuni esempi di automazione nella risposta alle minacce:
- **sistema di risposta automatica**: bloccare l'accesso alle risorse critiche, isolare dispositivi compromessi e applicare regole di sicurezza in modo autonomo;
- **analisi delle vulnerabilità**: individuare e valutare le vulnerabilità nei sistemi;
- **correlazione degli eventi**: individuare correlazioni tra eventi apparentemente non collegati per rilevare attacchi complessi e orchestrati.

Figura 2: Applicazioni dell'Intelligenza Artificiale nella Cybersecurity

Previsione e prevenzione

L'Intelligenza Artificiale non solo risponde alle minacce esistenti, ma può anche prevedere e prevenire quelle future [4]. L'analisi predittiva basata sull'IA consente di identificare possibili scenari di attacco, permettendo alle organizzazioni di adottare misure preventive. Alcuni esempi includono:

- **modelli di previsione delle minacce**: analisi di dati storici e attuali per individuare tendenze e modelli che potrebbero segnalare futuri attacchi;
- **simulazioni di attacco**: simulare potenziali scenari di attacco e valutare la resilienza dei sistemi;
- **adattamento delle politiche di sicurezza**: aggiornare le politiche di sicurezza in tempo reale, in base alle minacce attuali e alle vulnerabilità rilevate.

L'NLP (Natural Language Processing) e la GenAI sono strumenti preziosi nella Cyber Threat Intelligence (CTI). L'NLP analizza grandi quantità di testo da fonti aperte, forum underground, dark web e social media per identificare indizi, pattern e informazioni relative a minacce cibernetiche.
La GenAI genera modelli predittivi basati su dati storici e attuali per anticipare attacchi potenziali e sviluppare strategie di difesa. Insieme, queste tecnologie migliorano notevolmente la capacità di rilevare e mitigare le minacce cibernetiche in modo proattivo, sia in utilizzi automatici continui che in assistenza al lavoro dell'analista CTI.

Utilizzi innovativi in Cybersecurity TIM

Diversi sono gli utilizzi dell'AI/ML sviluppati a supporto degli strumenti di sicurezza interni al nostro contesto enterprise, come ad esempio l'analisi automatica degli eventi di spam/phishing e la prioritizzazione degli indicatori di compromissione nella piattaforma di Threat Intelligence aziendale.
Attraverso collaborazioni con le Università e Dottorati di Ricerca, siamo in fasi di studio e prototipazione di strumenti AI nell'ambito di analisi automatica dei malware [5] e arricchimento/contestualizzazione automatica degli eventi cyber da fonti eterogenee OSINT e CLOSINT.

Utilizzi malevoli dell'Intelligenza Artificiale

L'Intelligenza Artificiale, pur offrendo notevoli vantaggi in diversi settori, può essere impiegata anche per scopi malevoli.
Gli attacchi basati sull'IA possono minacciare la sicurezza nazionale e la stabilità globale, oltre a danneggiare singole organizzazioni private.

È essenziale riconoscere questi rischi e sviluppare adeguate misure di sicurezza per prevenire l'abuso dell'IA. La regolamentazione, la formazione, la sicurezza informatica avanzata e la consapevolezza sull'IA sono tutti elementi cruciali per mitigare le minacce correlate all'utilizzo malevolo di questa tecnologia.

È importante sottolineare che mentre il crimine informatico potrà beneficiare delle tecnologie di Intelligenza Artificiale senza moderazioni, censure e limitazioni, probabilmente chi difende le infrastrutture dovrà fare i conti con una Intelligenza Artificiale potenzialmente meno efficace dal punto di vista della difesa. Questo perché dovrà essere normata e bilanciata dal punto di vista etico.

Generazione automatizzata di fake news

Uno dei principali rischi legati all'IA è l'utilizzo per generare contenuti falsi o fuorvianti, noti come "fake news".
Si possono creare articoli, rapporti, post o contenuti multimediali sui social media che sembrano autentici, ma sono stati concepiti per diffondere disinformazione, influenzare opinioni pubbliche o danneggiare la reputazione di individui o organizzazioni.
Con l'ausilio delle tecnologie IA, è possibile manipolare contenuti multimediali come video, audio e immagini per supportare le fake news generate, questa tecnica è nota come "deepfake" e può avere gravi conseguenze in termini di reputazione e sicurezza.

Attacchi di phishing avanzati

Una delle tattiche più efficaci per perpetrare attacchi informatici è il phishing. Gli algoritmi di generazione del testo possono creare messaggi di phishing che sembrano provenire da fonti affidabili, ingannando le vittime e spingendole a divulgare informazioni sensibili.
Questo approccio diventa particolarmente efficace quando l'IA si combina con le tecniche di social engineering, sfruttando le informazioni personali (spesso pubbliche) delle vittime per creare attacchi personalizzati e sofisticati.

Attacchi DDoS avanzati

Gli attacchi distribuiti di Denial of Service (DDoS) hanno beneficiato dell'uso dell'IA, ma non in termini di aumento della potenza in termini di volumi di traffico.
Piuttosto, l'IA ha migliorato l'efficacia degli attaccanti nell'orchestrare e mascherare gli attacchi DDoS, rendendoli più difficili da contrastare.

Questi attacchi sono diventati particolarmente comuni in un contesto di tensioni geopolitiche internazionali, spesso generate da conflitti in corso, e possono causare interruzioni nei servizi online, danneggiando aziende, organizzazioni e, ovviamente, gli utenti.

Vulnerabilità delle applicazioni di Intelligenza Artificiale

Le applicazioni di Intelligenza Artificiale, come qualsiasi altro software, possono essere affette da vulnerabilità, spesso sfruttate dagli attaccanti per perpetrare i loro attacchi. Di seguito sono elencate alcune delle principali vulnerabilità delle applicazioni di IA e come queste possono essere sfruttate per scopi malevoli.

Evasion Attack e Prompt injection

Se non addestrati a riconoscere input sospetti, i modelli AI potrebbero essere vulnerabili ai cosiddetti "Evasion Attack", i quali inducono il modello a commettere errori.
Questi attacchi sono progettati con l'intento di fornire input al modello che sembrano normali alle ispezioni umane o ai processi di validazione, ma che sono stati manipolati in modo tale da indurre il modello a fare una classificazione o previsione errata.
In Fig.3 un esempio di Evasion Attack: con piccole modifiche, le quali non impedirebbero ad un essere umano di riconoscere il segnale di STOP, si potrebbe invece ingannare un modello di IA se non ben addestrato. Un'applicazione di Intelligenza Artificiale in esecuzione su veicoli autonomi, che si basa sul riconoscimento automatico delle immagini dei segnali

stradali, può essere influenzata dalla manipolazione dei segnali stradali.

Nel contesto dei Large Language Model (LLM), il termine "prompt injection" si riferisce a una potenziale vulnerabilità in cui un attaccante manipola il prompt fornito al modello per ottenere risultati desiderati o dannosi. Questa tecnica potrebbe consentire a un attaccante di influenzare in modo fraudolento le risposte generate dal modello, inducendolo a produrre risultati indesiderati o persino pericolosi.

Data poisoning

Una delle vulnerabilità più comuni nelle applicazioni di IA è la manipolazione dei dati. Gli attaccanti possono introdurre dati dannosi o fasulli nei set di addestramento degli algoritmi di machine learning, compromettendo la sicurezza e l'accuratezza dei modelli di IA. Ciò può portare a risultati distorti, decisioni dannose e comportamenti imprevisti. Si potrebbe per esempio indurre un modello di IA ad una certa classificazione (sbagliata) con riferimenti a input specifici, iniettando una vera e propria backdoor [5].

Manipolazione delle decisioni autonome

L'IA è utilizzata per prendere decisioni autonome in una varietà di contesti, come il trading finanziario e la guida autonoma. Purtroppo, un sistema completamente autonomo potrebbe essere manipolato per scopi malevoli, come influenzare il mercato finanziario o causare incidenti stradali intenzionali. È cruciale riconoscere queste vulnerabilità e adottare misure di sicurezza adeguate a proteggere le applicazioni di IA. Queste misure includono l'implementazione di controlli di accesso, la crittografia dei dati, la gestione delle chiavi, la validazione dei dati di input e l'addestramento di modelli di IA robusti definiti Generative Adversarial Network (GAN).

Aspetti etici dell'utilizzo dell'Intelligenza Artificiale nella Cybersecurity

Nel contesto della Cybersecurity, una delle principali questioni da considerare è il rischio per la privacy e la sorveglianza digitale. Questo è uno dei principali rischi individuati dalla Commissione Europea per i prossimi 10 anni [6].
L'IA può essere utilizzata per monitorare le attività online al fine di rilevare potenziali minacce alla sicurezza, ma c'è il rischio che tale monitoraggio possa essere utilizzato per scopi non consentiti dai principi etici. È fondamentale trovare un equilibrio tra la necessità di proteggere la sicurezza e il rispetto dei diritti individuali alla privacy.
Inoltre, per quanto riguarda la responsabilità legale, sorgono domande importanti: chi è responsabile in caso di errore dell'IA? In sintesi, l'uso dell'IA nella Cybersecurity offre numerosi vantaggi, ma solleva anche significative sfide etiche. È essenziale che le organizzazioni affrontino queste sfide in modo etico, rispettando i principi di privacy, trasparenza, equità e responsabilità.

Figura 3: Esempio di Evasion Attack

Conclusioni

L'interazione tra Intelligenza Artificiale e Cybersecurity rappresenta una delle frontiere più promettenti e, al contempo, impegnative del nostro tempo.
L'IA, con le sue capacità di apprendimento automatico e di elaborazione dei dati su larga scala, offre strumenti potentissimi per rafforzare le difese informatiche, individuando minacce in tempo reale, prevedendo attacchi futuri e rispondendo in modo autonomo agli incidenti di sicurezza.
Tuttavia, questa simbiosi porta con sé sfide significative, tra cui questioni etiche, la necessità di proteggere gli algoritmi di IA da manipolazioni e la garanzia che l'uso dell'IA nella sicurezza informatica non comprometta la privacy degli utenti.
Non ultimo, l'Intelligenza Artificiale è riconosciuta come strumento potente al servizio anche e soprattutto degli attaccanti, estremamente facilitati nell'ingresso nel cybercrime anche in assenza di elevate competenze.

Man mano che procediamo in questa era digitale, è fondamentale che sviluppatori, esperti di sicurezza, policy maker e la società nel suo complesso collaborino per navigare in queste acque complesse, garantendo che i benefici dell'IA nella Cybersecurity siano realizzati in modo responsabile e sostenibile. Così facendo, possiamo sperare di creare un ambiente digitale più sicuro per tutti, sfruttando al massimo le straordinarie potenzialità dell'Intelligenza Artificiale a beneficio della sicurezza collettiva.■

Riferimenti

1. “The economic potential of generative AI,” McKinsey & Company, June 14, 2023, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#/
2. Goodfellow, Ian; Pouget-Abadie, Jean; Mirza, Mehdi; Xu, Bing; Warde-Farley, David; Ozair, Sherjil; Courville, Aaron; Bengio, Yoshua (2014). Generative Adversarial Nets (PDF). Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014). pp. 2672–2680
3. Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language models are unsupervised multitask learners. OpenAI blog, 1(8), 9
4. ENISA Research and Innovation Brief, ARTIFICIAL INTELLIGENCE AND CYBERSECURITY RESEARCH, June 2023, https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research
5. Mario D’Onghia, Federico Di Cesare, Luigi Gallo, Michele Carminati, Mario Polino, and Stefano Zanero. 2023. Lookin’ Out My Backdoor! Investigating Backdooring Attacks Against DL-driven Malware Detectors. In Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security (AISec ’23). Association for Computing Machinery, New York, NY, USA, 209–220
6. Rossella Mattioli, Apostolos Malatras, (ENISA) - Eve Naomi Hunter, Marco Gino Biasibetti Penso, Dominic Bertram, Isabell Neubert, (Detecon). IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030, March 2023

Acronimi

CTI	Cyber Threat Intelligence
DDos	Denial of Service
GAN	Generative Adversarial Network
GenAI	Generative AI
IA	Intelligenza Artificiale
LLM	Large Language Models
NLP	Natural Language Processing

Autori

Madalina Baltatu *madalina.baltatu@telecomitalia.it*

È un’analista/ricercatrice nel campo della Cyber Security in Telecom Italia dal 2002. Ha conseguito il dottorato in Sicurezza delle Reti presso il Politecnico di Torino nel 2001. Le sue principali aree di interesse sono la Cyber Security, in particolare la Cyber Threat Intelligence, la sicurezza delle reti TCP/IP, le tecniche di rilevamento delle anomalie per sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS), l’autenticazione e, in passato, la crittografia basate sulla biometria. Ha partecipato a numerosi progetti finanziati dall’Unione Europea nel campo della sicurezza, è autrice di diversi brevetti internazionali e possiede la certificazione GIAC in Cyber Threat Intelligence (GCTI). ■

Luigi Gallo *luigi1.gallo@telecomitalia.it*

È ricercatore presso il Cyber Security LAB di Telecom Italia (TIM), incluso nella funzione di Security Threat Management. Ha conseguito il Dottorato di Ricerca in Information Technology and Electrical Engineering presso l’Università degli Studi di Napoli ’Federico II’. Attualmente si occupa di attività di ricerca e innovazione per scopi di sicurezza, con particolare riguardo a Security Awareness, Intelligenza Artificiale, Threat Intelligence e Reti Mobili 5G. Ricopre inoltre il ruolo di delegato in 3GPP SA3 per il gruppo TIM. ■

Maria Saleri *maria.saleri@telecomitalia.it*

Ricercatrice presso il Cyber Security LAB di Telecom Italia (TIM), nella funzione di Security Threat Management. Laureata presso l’Università degli Studi di Brescia nel 2022 nel corso di laurea di Ingegneria Informatica con tesi di laurea: “L’Open Source INTelligence per la valutazione strutturata del livello di esposizione di figure decisionali aziendali ai rischi di cyber-attacck”.
Attualmente si occupa di attività di ricerca nell’ambito della Threat Intelligence, con interesse per le analisi OSINT e la gestione delle segnalazioni di vulnerabilità. ■

Incident Handling: Minacce Cyber, preparazione e contrasto

Federico Grattirio

Una delle prime cose che si imparano lavorando in un SOC è non dare nulla per scontato. Spesso, infatti, un alert apparentemente insignificante può portare alla identificazione di una compromissione su larga scala. Il successo (o l'insuccesso) nell'identificazione di quanto realmente interessante in un tempo finito deriva da un insieme di fattori, il primo in assoluto è rappresentato dalle persone, dalle loro competenze e dalla sinergia del gruppo. Le persone ovviamente devono essere coadiuvate da strumenti software e hardware di qualità e da processi solidi, snelli e resilienti all'errore umano.

Da Alert a Incidente

Strumenti a supporto

La selezione degli strumenti da utilizzare è una fase molto importante, a partire da ciò verranno infatti impattate sia la capacità di identificazione e reazione alle minacce che la velocità di gestione. Nell'ultimo periodo i vendor stanno indirizzando il mercato verso:

- **prodotti SaaS e Agent based**, che semplificano notevolmente la gestione in quanto il software è ospitato su macchine offerte e manutenute dal vendor stesso. Ciò permette di concentrarsi su quanto realmente importante, gli alert. Se la funzionalità del prodotto si presta, inoltre, fanno uso di agent installati sulle macchine velocizzando e delocalizzando le attività di detection e risposta;
- **prodotti basati su modelli comportamentali**, che sono spesso molto efficaci e, dopo una prima fase di training, permettono di evidenziare anomalie rispetto al comportamento standard di un utente/sistema. Non è comunque consigliabile basare la propria strategia di detection solo su software di questo tipo.

Il singolo prodotto può essere valido per una realtà e meno per una altra, è quindi necessario valutare di caso in caso. Sicuramente quanto non può mancare è un EDR (Endpoint Detection&Response), un software agent based che permette di tracciare le attività svolte dagli endpoint (telemetria), meglio se con funzionalità di blocco, invio telemetria in cloud e retention dei log di almeno 90 giorni.
È fondamentale anche un correlatore di eventi (SIEM o applicazione big data), anche in questo caso è bene selezionare un prodotto che garantisca tempi di ricerca adeguati su grandi moli di dati, ciò consente di aumentare la retention senza penalizzare le analisi.
Una terza cosa che non può assolutamente mancare è un software di tracciamento mediante il quale è possibile mantenere evidenza di tutte le azioni effettuate per la singola gestione. Spesso una scelta errata o l'imposizione di software già in uso porta a enormi problemi e sprechi di tempo. A partire dal set base di prodotti citati è poi necessario integrare in base al proprio business e alla conformazione della propria infrastruttura IT.

Processi

I processi sono le fondamenta della attività di gestione incidenti, più sono stabili maggiore sarà il beneficio che potranno apportare.
Osservando l'attività dall'esterno, probabilmente ciò non traspare. Nell'immaginario collettivo l'analista di sicurezza è spesso visto come una figura mitica che risolve i problemi schiacciando pochi tasti. Nella realtà invece, gli analisti devono attenersi a regole ferree e tracciare ogni attività svolta, altresì quanto effettuato potrebbe diventare inutilizzabile.
In questo ambito si innestano i processi, che hanno il compito di aiutare gli analisti a seguire la giusta via, ridurre i tempi di gestione e standardizzare le attività. Per garantire efficacia ed efficienza un processo deve essere:

- **conosciuto**, gli analisti devono essere a conoscenza dell'esistenza e devono sapere dove reperire le informazioni all'occorrenza;
- **concreto**, deve essere completo, preciso, chiaro, deve riportare nel dettaglio le azioni minime da fare e non deve su-

bire variazioni basate su dettagli a contorno. Devono inoltre essere previsti indicatori di verifica che ne garantiscano l'applicazione;
- **aggiornato**, devono essere previsti momenti di revisione periodici e l'aggiornamento costante e tempestivo del processo a seguito della comparsa di nuove casistiche.

Approccio reattivo contro Approccio proattivo

Uno degli inneschi standard del processo di gestione incidenti sono gli alert, ovvero la notifica di anomalie da parte di uno strumento. In questo specifico caso si sta utilizzando un approccio reattivo. Negli ultimi anni gli attaccanti spesso utilizzano tecniche atte alla evasione degli strumenti di sicurezza. Ciò porta ad avere alert in minor numero o di minore entità, aumentando il tempo a disposizione per portare a termine l'attacco. Diventa quindi fondamentale coadiuvare l'approccio reattivo con attività di tipo proattivo, che in gergo vengono definite "Hunting".
L'attività si basa sulla ricerca manuale di comportamenti malevoli all'interno di log ed eventi, con la finalità di identificare pattern non riconosciuti o riconoscibili dagli strumenti. L'attività può essere effettuata su qualsiasi tipo di fonte, per garantirne il successo si consiglia però di assegnarla a personale con forti competenze tecniche e buona conoscenza dell'infrastruttura.

Gestione falsi positivi e alert fatigue

Il maggiore problema di un approccio reattivo è dato dalla quantità di alert ricevuti. Il rischio è di non riuscire a valutarne portata e impatti, sia per la mancanza di tempo che per un riflesso inconscio degli analisti: "se così tanti alert sono falsi positivi lo sarà anche questo".
Purtroppo, ad oggi, il problema è molto diffuso e non sono presenti soluzioni univoche.
È però possibile limitarne gli impatti attuando delle azioni come:
- **dedicare una o più persone alla gestione degli strumenti**, al tuning proattivo, alla creazione di alert e all'approfondimento dei comportamenti anomali;
- **creare un flusso di revisione degli alert in "anello chiuso"**, ovvero ogni falso positivo o problema deve essere segnalato e gestito tempestivamente, interfacciandosi con l'IT ove necessario per capirne le cause scatenanti;
- **affiancare analisti esperti ad analisti di minore esperienza** in modo da garantire supporto ed evitare tempi di gestione eccessivi.

Incidente

In letteratura la gestione di un incidente di sicurezza viene modellizzata mediante fasi. Nella realtà, in base alla tipologia di incidente, ogni fase potrà essere più o meno corposa, potrà sovrapporsi o unirsi e potrà essere ripetuta più volte durante l'intero processo. Si riporta di seguito un compendio di quanto proposto dal SANS Institute.

Preparazione

Tipicamente corrisponde ad un momento di "pace" per gli analisti di sicurezza, ovvero un momento in cui non sono presenti incidenti. Ogni gruppo lavora con l'obiettivo di preparare quanto necessario per le future gestioni, ottimizzare quanto già in essere ed approfondire nuove tematiche.

Identificazione e scoping

A valle della identificazione di un incidente si cerca di capire l'estensione della compromissione, il perimetro e gli asset coinvolti. Per incidenti di grandi dimensioni le attività di scoping si ripetono ogni qualvolta si identifichi una nuova evidenza. È di fondamentale importanza procedere con cura, precisione e metodo in quanto, altresì, si rischia di non identificare l'intero perimetro.

Contenimento

Terminato lo scoping si procede al contenimento, ovvero a bloccare qualsiasi possibilità di espansione del perimetro. Ciò potrebbe prevedere l'isolamento di una o più macchine, il blocco delle utenze impattate, la creazione di regole firewall.
Molte delle misure applicate nella presente fase sono temporanee.

Eradicazione e bonifica

È la fase in cui i sistemi compromessi vengono bonificati, in base alle evidenze reperite dalle analisi potrebbe essere necessario rifare completamente una macchina o solo rimuovere una serie di artefatti.

Recupero

A valle della bonifica dei sistemi si procede ad applicare eventuali ulteriori misure di hardening o patch specifiche. È infine possibile riportare l'applicazione in "produzione".
È necessario considerare con la massima attenzione ogni alert derivante dai sistemi.
Qualora una delle precedenti fasi non fosse stata effettuata nel modo corretto l'attaccante potrebbe guadagnare nuovamente accesso al sistema.

Lesson learned

Ultima fase, prevede un monitoraggio dedicato delle attività svolte dalla piattaforma oggetto di incidente per un periodo arbitrario di tempo. Prevede inoltre la revisione di quanto individuato ed effettuato durante la gestione, la valutazione della bontà dei metodi utilizzati e dei risultati ottenuti.
Ogni errore commesso in fase di gestione va rivisto, commentato e scongiurato nelle successive gestioni.

Ruoli & Persone

Analista di sicurezza

È il cuore pulsante di un SOC, si occupa dell'analisi degli alert e della gestione degli incidenti. Tipicamente è una persona con un profilo fortemente tecnico. In un ambiente medio/grande sono in genere previsti più livelli:
- **L1**, effettuano la prima scrematura degli alert, elevando quanto di interesse ad incidente. Possono essere interni od esterni all'azienda e possono lavorare anche su turni in modo da garantire un monitoraggio H24;
- **L2**, si occupano della gestione di quanto segnalato da L1, fornendo analisi di maggiore dettaglio e verificando con maggiore profondità gli eventi;
- **L3** che possono essere definiti CERT (Computer Emergency Response Team). Il loro compito è quello di gestire incidenti critici, complessi e distribuiti. In ambienti medio/piccoli è possibile che tale figura sia demandata a società esterne.

Ogni livello deve avere anche il compito di fornire supporto al livello sottostante

garantendone così la crescita professionale e rafforzando i rapporti interpersonali.

Alert engineer e On-boarding specialist

Sono figure che non procedono alla gestione diretta degli incidenti. Il ruolo di "Alert engineer" è ricoperto da persone che si occupano di tuning degli strumenti, con un profilo fortemente tecnico e possibilmente un passato nel campo della gestione incidenti. Il compito è di fondamentale importanza per garantire il corretto bilanciamento tra capacità di detection e numero di falsi positivi.
Il ruolo di "On-boarding specialist" è invece assegnato a persone che si occupano di interagire con l'IT per l'integrazione logica di nuove fonti log, studiarne la composizione e manutenere le informazioni inerenti quanto già in essere. Non è fondamentale un profilo fortemente tecnico, ma è consigliata una formazione informatica.
Il gruppo ha l'obiettivo di procurare in anticipo le informazioni di cui necessitano gli analisti, velocizzando le attività di gestione e garantendo una migliore contestualizzazione degli eventi.

Processi, procedure e standard

Il gruppo indicato si occupa della fase di redazione e aggiornamento di processi e procedure. Negli ultimi anni, inoltre, sono nati numerosi standard che indicano le "best practices" in materia di gestione incidenti, come ad esempio ISO 27001 ed ISO 27035. Ottenere una delle certificazioni indicate è motivo di prestigio e garanzia che le attività siano allineate ai più moderni standard di settore. I membri del suddetto gruppo hanno il compito di coordinare i restanti gruppi in modo che quanto indicato dalle norme sia assimilato e rispettato. Il profilo richiesto non è necessariamente tecnico ma è necessario possedere i concetti di base per poter comprendere le norme e garantirne il beneficio massimo.

Comunicazione e contatti esterni

Il gruppo si interfaccia con entità esterne, quali ad esempio l'ufficio legale e, nei casi peggiori con chi si occupa di comunicazione in azienda.
Per garantire una comunicazione efficace e limitare al minimo le incomprensioni è bene avere persone con un profilo ibrido, ovvero che possano capire al meglio entrambe le parti e fare da tramite. Non è pertanto richiesto un profilo verticale, ma è necessario possedere i concetti base delle discipline affrontate.

Conclusioni

In conclusione, negli ultimi anni l'attività di monitoraggio e gestione incidenti di sicurezza ha subito grandi modifiche. È passata dall'essere marginale e destrutturata ad essere una componente aziendale fondamentale e fortemente strutturata. Grazie anche alla pubblicità involontaria derivante dalle grandi compromissioni si sta piano piano creando una maggiore consapevolezza, stanno aumentando gli investimenti e soprattutto sta mediamente aumentando l'attenzione rivolta al tema. L'aumento di consapevolezza ed investimenti ha portato benefici anche nella disponibilità di materiale di studio, software sia open source che proprietari, linee guida e informazioni. Ciò ha portato alla necessità di creare nuovi ruoli e nuove professionalità che hanno come unico obiettivo agevolare e migliorare capacità e tempistiche di analisi. In sostanza sia dal punto di vista manageriale che dal punto di vista tecnico l'attività è in continuo divenire permettendo alle persone che vi lavorano di affrontare ogni giorno nuove stimolanti sfide.■

Acronimi

EDR	Endpoint Detection & Response
IOC	Indicatore di compromissione
SaaS	Software as a Service
SIEM	Security information and event management
SOC	Security operation center

Autore

Federico Grattirio *federico.grattirio@telecomitalia.it*

Laurea in Ingegneria Informatica presso l'università degli studi di Pavia con tesi volta allo sviluppo di software in ambito informatico forense. Dopo una prima esperienza nel campo della ingegnerizzazione e configurazioni di soluzioni SIEM e IAM ho approcciato il mondo della Threat Intelligence, appassionandomi sempre di più a tematiche "blue team". Dal 2019 lavoro presso il SOC di TIM come Security Analyst, prima su tematiche relative alle minacce derivanti da posta elettronica e successivamente con focus dedicato su tematiche di Incident Response e Forensic Analysis. ■

Il fattore umano nel Phishing: una questione di consapevolezza

Luigi Gallo, Alessandro Maiello, Lorenzo Rizzati

Il phishing sfrutta il fattore umano come principale vettore di attacco, mettendo in evidenza le vulnerabilità psicologiche degli individui di fronte alle sofisticate strategie dei cybercriminali. Questo articolo esplora come la manipolazione psicologica, l'ingegneria sociale e le tecniche di convincimento sono impiegate efficacemente nel phishing per indurre le vittime a compiere azioni dannose. L'articolo evidenzia come la comprensione del fattore umano sia cruciale nella lotta contro il phishing, proponendo strategie integrate che combinano tecnologia avanzata e psicologia comportamentale. È così che la sicurezza informatica, dall'essere un argomento puramente tecnico/tecnologico, diviene anche materia umanistica.

Da diversi decenni i servizi ICT vengono progettati seguendo il principio della Security-by-Design, rendendo i sistemi informatici molto più robusti agli attacchi rispetto al passato. Nello scenario moderno, il **Phishing** emerge dunque come **uno tra i principali vettori di attacco per il cybercrime** in quanto il progresso delle tecnologie ha irrobustito i sistemi, ma non i loro utilizzatori.

Gli attacchi di Phishing vengono realizzati attraverso e-mail malevole, le quali si basano su protocolli di gestione (i.e. SMTP) ideati ben prima che la sicurezza fosse parte integrante delle fasi di progettazione dei sistemi. Banalmente, il destinatario di una e-mail non può sempre autenticare con certezza il mittente. Questo difetto delle comunicazioni, tramite posta elettronica, genera opportunità enormi per i criminali informatici, i quali possono impersonare chi vogliono in un messaggio e insistere su quello che viene definito come "l'anello debole della catena", ovvero il **fattore umano**.

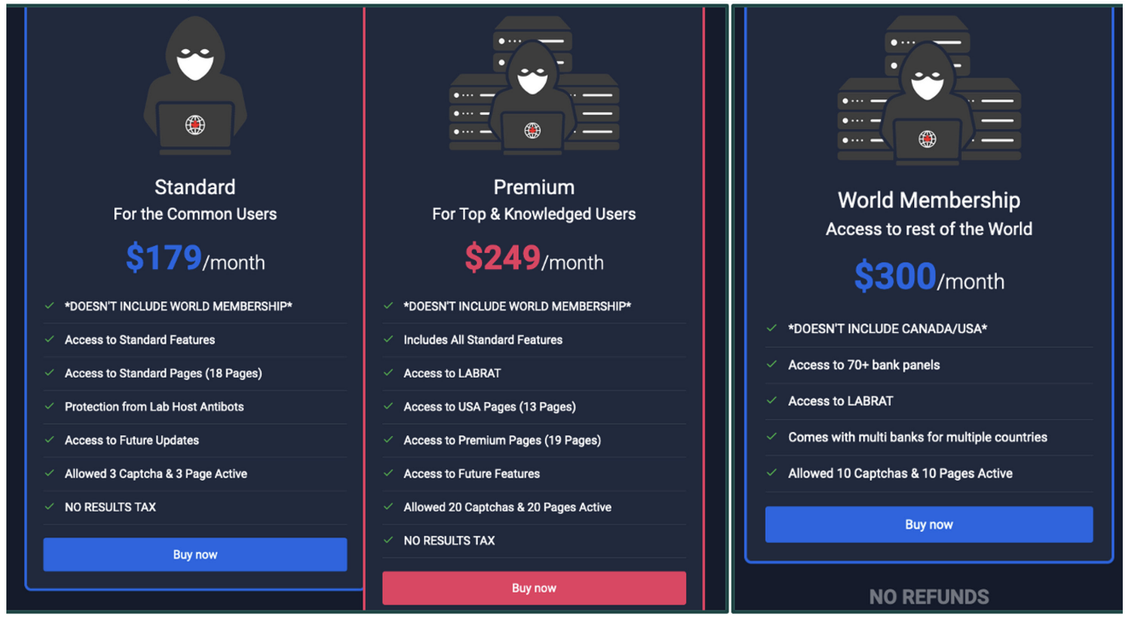
L'ecosistema degli attacchi di phishing

Anatomia di un attacco di phishing

La costruzione di una campagna di phishing da parte dei cyber criminali si articola attraverso fasi ben definite, sfruttando tecniche sempre più sofisticate e kit di phishing avanzati. Inizialmente, l'attaccante seleziona il bersaglio, che può variare da individui a grandi organizzazioni, identificando le vulnerabilità attraverso tecniche di social engineering o raccolta di informazioni pubblicamente disponibili.
Successivamente, si procede alla creazione del materiale di phishing, fase in cui entrano in gioco i kit di phishing: software complessi che permettono di generare in modo automatico e-mail ingannevoli, pagine web falsificate che imitano siti legittimi e altri elementi ingannevoli con un alto grado di personalizzazione e realismo.
Questi kit (che appartengono a quello che viene definito come modello di **Phishing-As-a-Service** o semplicemente PaaS) sono progettati per essere facilmente utilizzabili anche da malintenzionati senza profonde competenze tecniche, rendendo così l'attacco accessibile a un'ampia gamma di criminali informatici.
La fase di distribuzione segue, con l'invio massivo delle e-mail truffa ai destinatari selezionati, spesso utilizzando server e indirizzi IP compromessi per eludere i filtri antispam e mascherare la vera origine dell'attacco.

Il successo di un attacco di phishing dipende fortemente dalla capacità di convincere la vittima a compiere un'azione specifica, come inserire dati sensibili in una pagina web falsificata, cliccare su un link malevolo o su un allegato. Una volta che l'utente cade nella trappola, i cyber criminali raccolgono le informazioni acquisite per condurre frodi telematiche, accesso non autorizzato a sistemi protetti o altri atti illeciti. Gli attacchi di phishing non sono semplici iniziative isolate, ma il frutto di un'industria del cybercrimine strutturata, con una vasta gamma di attori coinvolti [1].
Questo ecosistema include organizzatori che coordinano le campagne, sviluppatori di toolkit di phishing avanzati, forniti come servizio (Fig.1) per l'anonimato e individui che gestiscono le operazioni finanziarie illecite. Questi stakeholder collaborano in mercati neri e forum clandestini, scambiandosi strumenti e servizi con l'obiettivo di ottimizzare l'efficacia e il rendimento degli attacchi.

Figura 1: Esempio di pannello di sottoscrizione ad un servizio di Phishing-as-a-Service (PaaS). Nello specifico viene mostrato il pannello degli abbonamenti mensili al software malevolo LabHost



Protezione e rilevazione degli attacchi di phishing

Le soluzioni adottate per prevenire gli incidenti di sicurezza causati dal phishing e dal comportamento improprio degli utenti sono le seguenti:

- **filtri antispam**: quando arriva un'e-mail, vengono applicate diverse logiche per individuare a monte un'e-mail indesiderata, prima di consegnarla al destinatario. Questo avviene tradizionalmente con approcci di blocklisting, basati sugli indirizzi IP di origine e sul comportamento a livello di rete delle e-mail (intestazioni SMTP). Tuttavia, logiche di rilevamento più innovative si basano anche sul contenuto delle e-mail, utilizzando classificatori pre-addestrati con tecnologie di machine learning o semplici euristiche. Purtroppo, molto spesso i criminali riescono ad eludere le logiche dei filtri antispam;
- **filtri web**: agli utenti viene impedita la navigazione in siti web noti per essere dannosi. In questo modo, anche se un utente clicca su un link dannoso contenuto in un'e-mail, la navigazione viene bloccata. Purtroppo, i sistemi di reputazione dei domini e degli URL devono essere continuamente aggiornati e molto spesso i criminali creano nuovi siti web (sconosciuti) appositamente per effettuare attacchi di phishing. Altre branche della sicurezza informatica si occupano di questi aspetti e della condivisione tempestiva di queste informazioni (i.e. Cyber Threat Intelligence);
- **software antivirus**: gli allegati vengono pre-scansionati dal software antivirus e classificati come dannosi o meno evitando che quelli malevoli vengano eseguiti dagli utenti. Come per i filtri Web, è importante mantenere aggiornati i database delle firme o disporre di logiche intelligenti di rilevamento del malware. Purtroppo, il malware utilizza spesso tecniche di offuscamento che impediscono al software antivirus di rilevarlo.

Data la non completa copertura di sicurezza dei sistemi sopra descritti e la crescente attenzione degli aggressori verso il fattore umano, i metodi di difesa volti a migliorare la postura di sicurezza dell'utente diventano molto importanti.
I più utilizzati sono:

- **policy di sicurezza**: regole "semplici" per un uso corretto degli strumenti di comunicazione via e-mail. Gli utenti sono invitati a non diffondere troppo il proprio indirizzo di posta elettronica, a non utilizzarlo per scopi non lavorativi (ad esempio, iscrivendosi a servizi o siti web che potrebbero essere soggetti a data breach) e a non diffondere informazioni relative al lavoro su canali pubblici. Per quanto possibile, anche le informazioni personali in rete dovrebbero essere ridotte, poiché sappiamo che vengono utilizzate per tecniche di social engineering. Spesso vengono suggeriti controlli di sicurezza rafforzati anche per le e-mail provenienti dall'esterno del perimetro aziendale (ma anche le e-mail interne devono essere controllate a causa del lateral phishing);
- **formazione e addestramento**: i dipartimenti di sicurezza delle aziende (o di terze parti) spesso conducono regolari campagne di formazione e addestramento per sensibilizzare gli utenti sul phishing. Il modo in cui questi corsi sono progettati è cruciale per la loro efficacia ed è ancora oggetto di studi scientifici. In caso di formazione inefficace, potrebbero addirittura essere controproducenti.

Il fattore umano: l'anello debole della catena

Come abbiamo visto, le tecniche di difesa tradizionali, seppur sofisticate, non riescono a proteggere completamente le vittime dagli attacchi di phishing. Per questo motivo l'attenzione, inizialmente rivolta allo sviluppo di difese tecniche contro il phishing, si è gradualmente spostata verso la comprensione degli elementi psicologici che contribuiscono al successo di tali attacchi.
In letteratura vari studi hanno analizzato l'importanza dei principi di persuasione utilizzati dai phisher per sfruttare le vulnerabilità cognitive, e la correlazione tra queste vulnerabilità e l'efficacia del phishing.
Secondo alcuni studi [2][3] i cinque grandi tratti (Big Five) della personalità, vale a dire apertura mentale, coscienziosità, estroversione, empatia e stabilità emotiva, sono legati alla suscettibilità al phishing, e fattori come le conoscenze informatiche e la consapevolezza delle pratiche web sicure (HTTPS, certificati), consentono all'individuo di identificare più facilmente i tentativi di phishing.
Tali conoscenze non forniscono mai una difesa perfetta dal phishing poiché noi tutti abbiamo delle vulnerabilità che potrebbero essere sfruttate, specie in un momento di distrazione, per sferrare un attacco di phishing efficace.
Risulta chiaro che l'elaborazione cognitiva delle e-mail da parte degli utenti

influenza in modo significativo la loro suscettibilità agli attacchi di phishing e che le vulnerabilità umane sono spesso l'anello più debole della sicurezza informatica.
Recentemente l'Intelligence Advanced Research Projects Agency (IARPA) degli Stati Uniti d'America ha lanciato ReSCIND, un programma che sfrutta la psicologia dei criminali informatici per contrastare gli attacchi. Si propone di integrare misure di sicurezza con la cyberpsicologia, creando nuove tecnologie di difesa informatica.
Il programma mira a identificare le vulnerabilità cognitive degli aggressori, sviluppare difese basate sulla psicologia informatica e fornire algoritmi per adattare le decisioni in base al comportamento osservato.
Quest'approccio innovativo punta a una difesa più efficace e di avanguardia, ponendo al centro il fattore umano come principale punto debole in operazioni di attacco e di difesa.

Vulnerabilità cognitive e principi di persuasione

Data l'importanza del fattore psicologico, le e-mail di phishing vengono spesso costruite includendo i cosiddetti attacchi cognitivi: porzioni di frasi utilizzate per esercitare un determinato principio di persuasione sulla vittima.

I principi della persuasione sono stati introdotti per la prima volta da Robert Cialdini ne "The psychology of persuasion" nel 1984 e si riferiscono a trucchi psicologici appositamente ideati per sfruttare specifiche vulnerabilità cognitive della vittima quali:

- Autorità: tendenza a obbedire a persone in posizione autorevoli, spinta dalla possibilità di incorrere in una punizione se non ci si attiene alle richieste dei superiori;
- Simpatia: Tendenza a dire "sì" alle richieste delle persone che l'individuo conosce e che gli piacciono;
- Scarsità: tendenza ad assegnare maggior valore a oggetti e opportunità quando la loro disponibilità è limitata, per paura di sprecare l'opportunità o di pentirsene successivamente;
- Coerenza: tendenza a comportarsi in modo coerente con le decisioni e i comportamenti passati;
- Riprova sociale: propensione a etichettare un comportamento come corretto in base al fatto che altri lo mettono in atto;
- Reciprocità: desiderio di ricambiare gli altri quando si riceve un favore.

L'efficacia di questi attacchi cognitivi è fortemente influenzata dal posizionamento all'interno dell'e-mail e dall'utilizzo dei "metodi di notifica".
Questi rappresentano un insieme di pratiche che possono essere adoperate per migliorare l'efficacia dell'attacco.

Secondo alcuni studi [4], determinati metodi di notifica sono più adatti a veicolare specifici attacchi cognitivi, secondo il seguente schema:

- Informazioni di contatto - Autorità;
- Personalizzazione - Simpatia;
- Oggetto - Scarsità;
- Oggetto - Coerenza.

Per degli esempi di applicazione dei principi di persuasione e la descrizione dei metodi di notifica, si rimanda alla Fig.2.

Esperimenti su larga scala [5] dimostrano l'efficacia degli attacchi personalizzati basati su vettori psicologici, evidenziando la necessità di una formazione continua e dinamica sulla consapevolezza del phishing per mantenere un alto livello di vigilanza tra i potenziali bersagli.

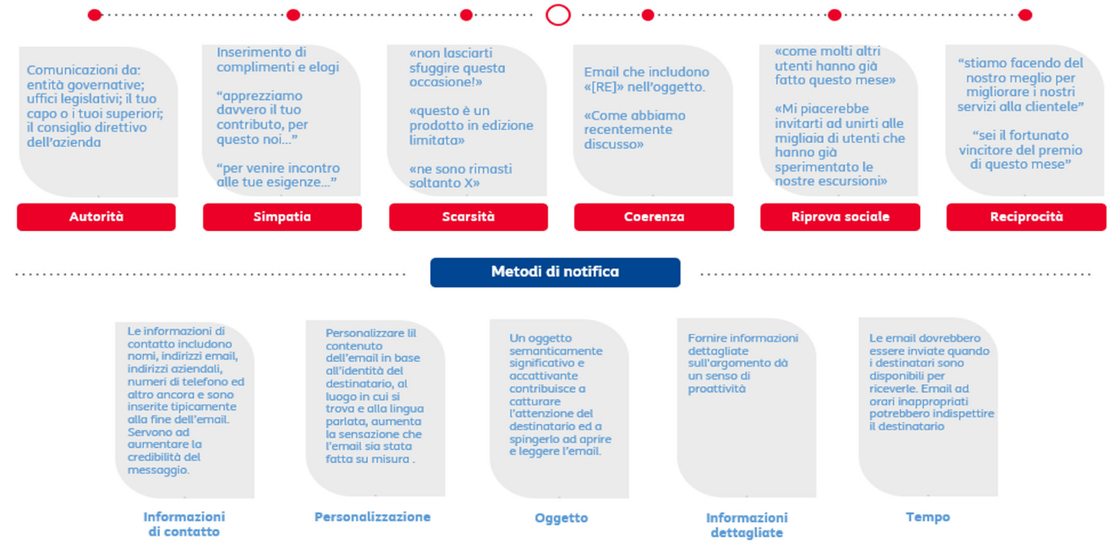
Nella sezione successiva illustriamo il nostro lavoro in progetti di ricerca e innovazione sul tema del fattore umano nel phishing, ampiamente trattato dalla comunità scientifica e di security come uno dei principali vettori d'infezione usato dal cybercrime.

Progetti di innovazione in TIM

TIM è impegnata in diversi progetti di ricerca e sviluppo di soluzioni efficaci da applicare in contesti enterprise in difesa degli attacchi di Phishing. Crediamo che l'approccio vincente sia un framework collaborativo basato su utenti consapevoli, che forniscono una "immunità di gregge", e strumenti intelligenti di prioritizzazione delle lavorazioni degli analisti di sicurezza [6].
Dall'inizio del 2018 abbiamo sviluppato questa idea, raccogliendo la posta elettronica di spam e supportando l'etichettatura di quelle effettivamente pericolose come critiche, attraverso il monitoraggio continuo degli analisti.
Utilizzando questo set di dati etichettato, abbiamo dimostrato che le tecnologie di Machine Learning possono classificare efficacemente le e-mail come critiche, evidenziando le minacce, aghi in un pagliaio di e-mail indesiderate ed innocue.

Grazie ai risultati ottenuti e alle lezioni apprese, abbiamo riprogettato il processo di gestione delle minacce via e-mail attorno a questo approccio collaborativo. Si basa ora su utenti esperti e consapevoli che segnalano e-mail sospette, un sistema automatico di raccolta e analisi dei dati, e analisti di sicurezza che indagano

Figura 2: Esempi di applicazione dei principi di persuasione e metodi di notifica



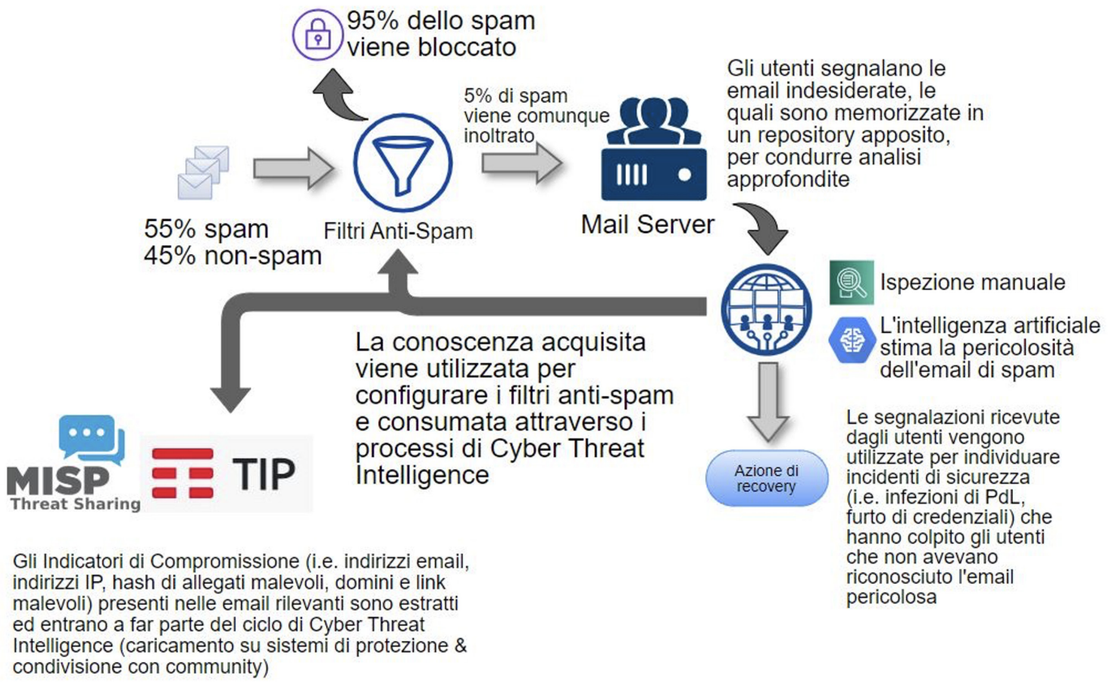
in profondità secondo i suggerimenti del sistema (Fig.3).

In sintesi, come risultato delle nostre proposte, l'approccio alla difesa collaborativa si basa non solo sulla collaborazione tra utenti, che segnalano e-mail sospette anche per la difesa degli altri, ma anche sulla collaborazione tra uomo e macchina. Infatti, grazie allo sforzo congiunto di dipendenti e analisti di sicurezza, un motore di apprendimento automatico viene alimentato con campioni segnalati dagli utenti ed etichettati dagli analisti.
La macchina viene quindi addestrata su quali sono le principali caratteristiche delle e-mail pericolose, classificando le nuove sospette per gli analisti e fornendo anche importanti informazioni su dove gli utenti devono migliorare per evitare di essere vittime di attacchi di phishing. A regime, le due fasi diventano concorrenti, formando un circolo virtuoso di difesa e prevenzione (Fig.4).

L'aspetto umano e personale è ormai al centro delle ricerche di una soluzione efficace agli attacchi di Phishing. In collaborazione con le Università, crediamo che per risolvere il problema del phishing bisogna comprendere profondamente il fenomeno umano e cognitivo.

Per questo motivo, abbiamo avviato una campagna di test su larga scala per collezionare preziose informazioni sul comportamento delle persone quando leggono le e-mail [7].
Partecipa anche tu:
https://spamley.comics.unina.it/.

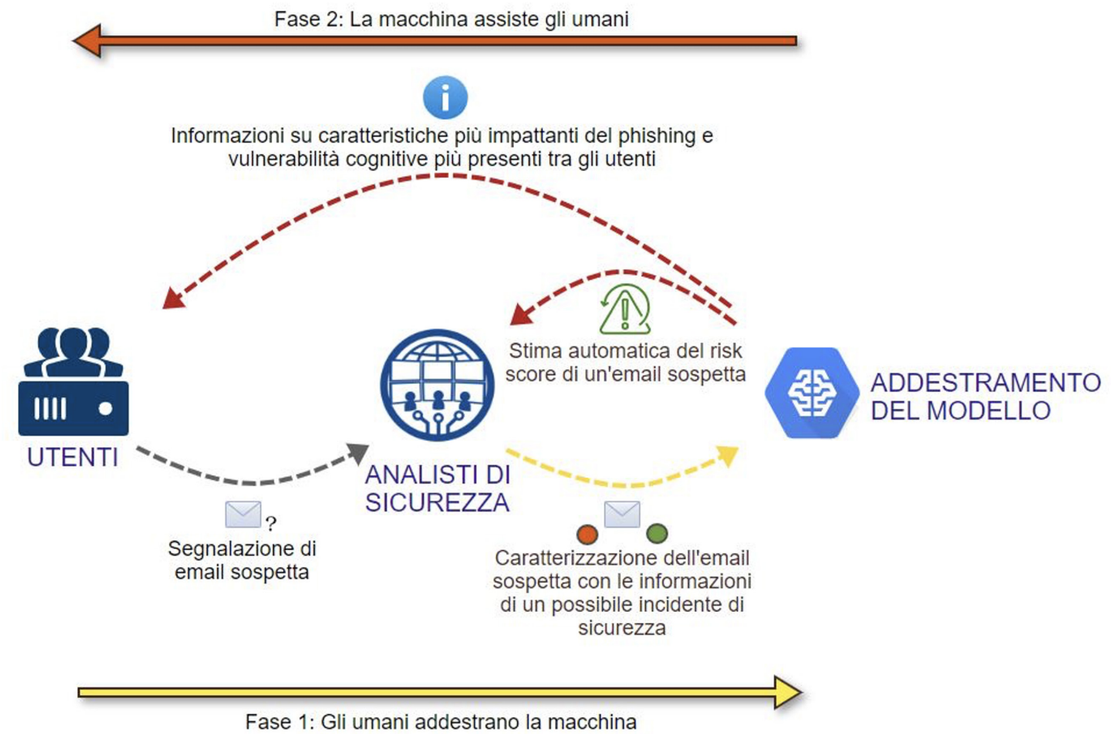
Figura 3: Ecosistema di difesa



Conclusioni

Chiunque non sufficientemente formato o semplicemente ingaggiato nel momento sbagliato, può essere indotto ad effettuare azioni che possono compromettere la sicurezza enterprise e vanificare gli sforzi tecnologici atti ad irrobustirla.
È così che la sicurezza informatica, dall'essere un argomento puramente tecnico/tecnologico, si combina con la psicologia, creando una nuova branca della cybersecurity chiamata "cyberpsychology" sempre più vicina alle materie umanistiche.
Attraverso questa nuova disciplina, si tenta di contrastare il crimine informatico che da sempre fa leva sulle debolezze umane per raggiungere i propri scopi. È tempo di armarci con la conoscenza, trasformando ogni utente in un guardiano digitale. Solo attraverso un impegno collettivo, che fonde tecnologia e sensibilizzazione umana, possiamo aspirare a un domani sicuro nel cyberspazio.■

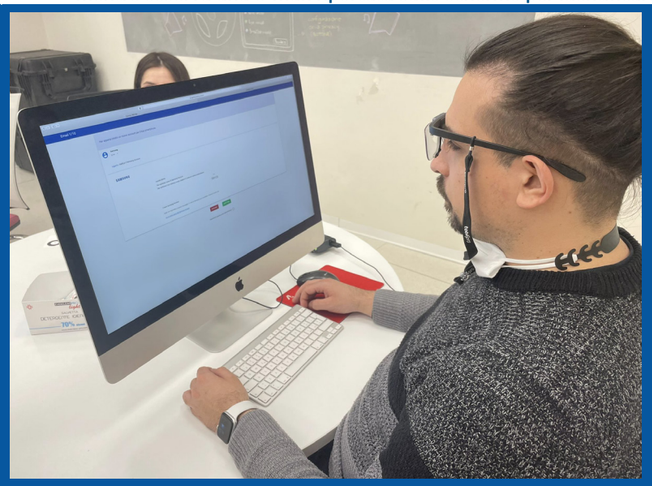
Figura 4: Framework collaborativo uomo-macchina



Analisi del comportamento dello sguardo nell'identificazione delle e-mail di Phishing

Poiché le tecniche di phishing continuano a evolversi, diventando sempre più sofisticate e ingannevoli agli occhi delle persone, la necessità di una comprensione multidimensionale dell'interazione umana con le e-mail diventa sempre più evidente.
In questo senso, gli studi che indagano sugli aspetti ergonomici e dei fattori umani rivestono un ruolo fondamentale, concentrandosi per definizione sulla comprensione del comportamento umano durante l'esecuzione di azioni suscettibili di errore, come aprire un collegamento malevolo presente all'interno di una e-mail. Gli approcci tradizionali allo studio del phishing dal punto di vista delle vittime hanno spesso fatto affidamento su sondaggi, auto-segnalazioni e analisi post hoc, fornendo preziose intuizioni sulla fenomenologia dell'attacco, ma non catturando pienamente le dinamiche in tempo reale dell'interazione degli utenti con le e-mail, che potrebbero invece essere utili a spiegare perché, molto spesso nonostante il training, le persone continuino a fallire nel riconoscimento, cadendo nell'inganno.
A questo proposito, recenti studi nell'ambito della cybersecurity e dell'ergonomia stanno sfruttando l'analisi del comportamento oculare delle persone, abilitata dall'utilizzo di dispositivi di eye-tracking.
Nella Fig.A è possibile osservare un esempio di eye-tracker indossabile (Tobii Pro Glasses 2), costituito da un paio di occhiali equipaggiato con due telecamere ad infrarossi rivolte verso gli occhi della persona monitorata atte a catturarne il riflesso corneale ed una telecamera rivolta verso l'esterno atta a catturare la scena visualizzata, in questo caso uno schermo su cui sono presentati diversi esempi di e-mail di phishing.
Il comportamento oculare delle persone è indicativo dell'attenzione che esse rivolgono ad una scena osservata: la conoscenza della sequenza dettagliata delle aree osservate consente di identificare le zone su cui il soggetto si sofferma di più, e dunque quali sono gli oggetti di sforzi di concentrazione o capaci di catalizzare interesse o ispezioni ripetute.

Figura A: Modalità di utilizzo di un dispositivo di eye-tracking indossabile durante un esperimento sul riconoscimento del phishing. Il soggetto indossa il dispositivo Tobii Pro Glasses 2 mentre osserva una e-mail riportata sullo schermo per identificare se sia phishing o meno



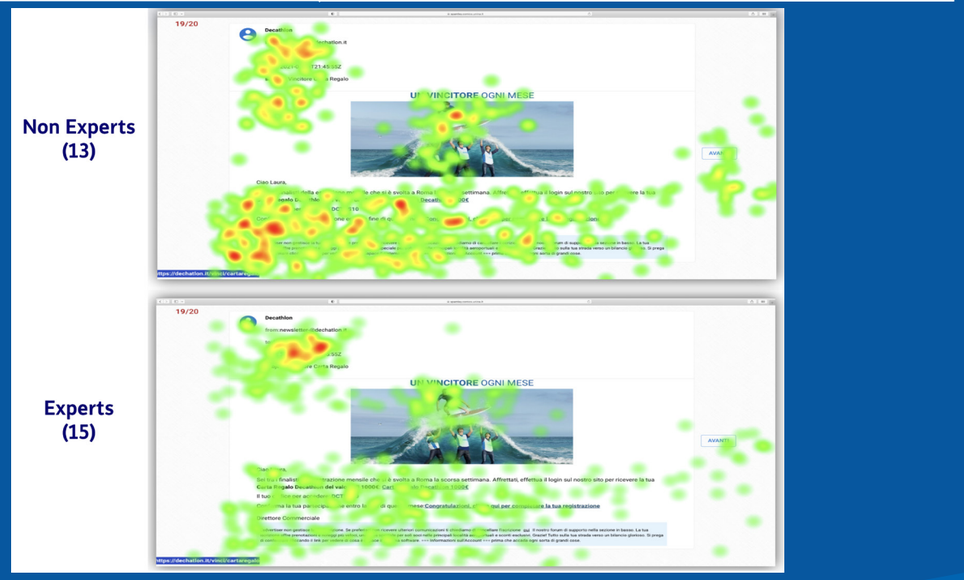
La Fig.B è un esempio del genere di informazioni che è possibile ottenere con gli studi basati su eye-tracking. Essa riporta tramite heatmap la distribuzione aggregata dell'attenzione visiva nell'ispezione di una e-mail di phishing da parte di un gruppo di 15 esperti di cybersecurity e di un gruppo di 13 non esperti: è evidente come gli esperti si concentrino sull'analisi dell'intestazione della e-mail, mentre i non esperti applicano un comportamento di ispezione più dispersivo.
Esaminando la relazione tra le performance nel riconoscimento di diversi tipi di phishing, gli attributi personali dell'individuo (i.e. dati demografici, livello di istruzione, livelli di affaticamento), e le informazioni raccolte tramite eye-tracking (i.e. la sequenza di osservazione delle aree di interesse e il tempo dedicato a ciascuna), è possibile ampliare notevolmente la comprensione delle modalità con cui le persone sono suscettibili al phishing.
Questo apre la strada a strategie di prevenzione più efficaci, migliorando i programmi di formazione degli utenti e sviluppando interfacce di e-mail client intuitive in grado di favorire percorsi di ispezione virtuosi e contrastare tentativi di phishing sempre più complessi.

alessio.botta@unina.it
roberta.presta@unisob.na.it

Riferimenti

F. Pietrantonio *et al.*, "Investigating Gaze Behavior in Phishing Email Identification", *2023 7th Network Traffic Measurement and Analysis Conference (TMA)*, Naples, Italy, 2023, pp. 1-4

Figura B: Heatmap di esperti e non-esperti di cybersecurity a confronto nell'ispezione di una e-mail di phishing



Bibliografia

1. Gianluca Stringhini, Oliver Hohlfeld, Christopher Kruegel, and Giovanni Vigna. The harvester, the botmaster, and the spammer: On the relations between the different actors in the spam landscape. In Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '14, pages 353–364, New York, NY, USA, 2014. Association for Computing Machinery
2. James L Parrish Jr, Janet L Bailey, and James F Courtney. A personality based model for determining susceptibility to phishing attacks. Little Rock: University of Arkansas, pages 285–296, 2009
3. Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems, pages 581–590, 2006
4. Pavlo Burda, Tzouliano Chotza, Luca Allodi, and Nicola Zannone. Testing the effectiveness of tailored phishing techniques in industry and academia: a field experiment. In Proceedings of the 15th International Conference on Availability, Reliability and Security, pages 1–10, 2020
5. Florian Quinkert, Martin Degeling, and Thorsten Holz. Spotlight on phishing: A longitudinal study on phishing awareness trainings. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pages 341–360. Springer, 2021
6. Luigi Gallo, Alessandro Maiello, Alessio Botta, Giorgio Ventre, 2 Years in the anti-phishing group of a large company, Computers & Security, Volume 105, 2021, 102259, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102259
7. Luigi Gallo, Danilo Gentile, Saverio Ruggiero, Alessio Botta, Giorgio Ventre, The human factor in phishing: Collecting and analyzing user behavior when reading emails, Computers & Security, Volume 139, 2024, 103671, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103671

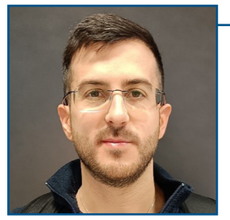
Acronimi

HTTPS	Hypertext Transfer Protocol Secure
IARPA	Intelligence Advanced Research Projects Agency
PaaS	Phishing-As-a-Service
SMTP	Simple Mail Transfer Protocol

Autori

Luigi Gallo *luigi1.gallo@telecomitalia.it*

È ricercatore presso il Cyber Security LAB di Telecom Italia (TIM), incluso nella funzione di Security Threat Management. Ha conseguito il Dottorato di Ricerca in Information Technology and Electrical Engineering presso l'Università degli Studi di Napoli 'Federico II'. Attualmente si occupa di attività di ricerca e innovazione per scopi di sicurezza, con particolare riguardo a Security Awareness, Intelligenza Artificiale, Threat Intelligence e Reti Mobili 5G. Ricopre inoltre il ruolo di delegato in 3GPP SA3 per il gruppo TIM. ■



Alessandro Maiello *alessandro.maiello@telecomitalia.it*

È un Cyber Security Analyst presso il Cyber Security LAB di Telecom Italia (TIM), incluso nella funzione di Security Threat Management. Ha conseguito la laurea magistrale in Ingegneria Informatica presso Università degli Studi di Napoli Federico II con una tesi sugli approcci di machine learning supervisionato per prevenire gli incidenti di sicurezza derivanti dalle e-mail di spam. Attualmente si occupa di attività di security testing di soluzioni di sicurezza sia in ambito fisso che mobile, con particolare attenzione alle Reti Mobili 5G. ■

Lorenzo Rizzati *lorenzo.rizzati@telecomitalia.it*

Cyber Security Engineer della struttura Cyber Security di TIM. Ha conseguito la Laurea Magistrale in Informatica all'Università degli Studi di Torino, con specializzazione in Reti e Sistemi Informatici. Da più di cinque anni lavora nello sviluppo di applicazioni per la gestione dei processi di cybersicurezza e nell'integrazione di soluzioni di Machine Learning. ■

La Threat Intelligence Platform di TIM

Madalina Baltatu, Stefano Brusotti, Luciana Costa, Dario Lombardo

Dopo una veloce incursione nella Cyber Threat Intelligence, che presenta i principali concetti e motivazioni di questa branca della Cybersecurity, l'articolo presenta la piattaforma di Threat Intelligence di TIM, partendo dalle origini, sino alle attuali funzionalità più innovative, che hanno fatto sì che TIM venisse inserita nell'Innovation Radar Europeo per i contributi implementati nell'ambito del progetto europeo H2020 Concordia, in particolare lo sviluppo del pilot "Automated Processing of Threat Intelligence Information".

La Cyber Threat Intelligence

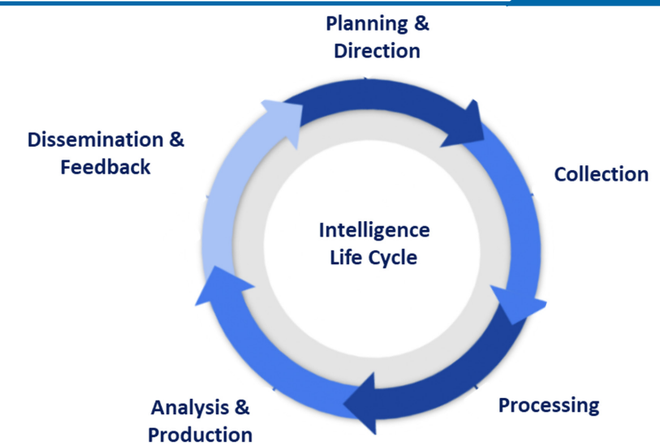
Lo scenario attuale delle minacce cyber è caratterizzato da una crescente complessità e sofisticazione delle tattiche utilizzate dagli attori malintenzionati. Questo scenario è influenzato da una serie di fattori, tra cui i conflitti geopolitici in corso, le tensioni tra Nazioni, le rivalità tra gruppi criminali e l'evoluzione delle tecnologie informatiche. È necessario quindi **sviluppare un'intelligence sulle minacce**, per migliorarne il rilevamento e la prevenzione, il che significa **contestualizzare** gli attacchi in merito a chi sta attaccando, le sue motivazioni, le risorse e le opportunità di cui dispone.

La **Cyber Threat Intelligence (CTI)** può essere definita come **la conoscenza complessiva e dettagliata delle minacce** informatiche attuali o emergenti [1]. Partendo dalla definizione in ambito militare [2], da cui la CTI deriva, l'intelligence è la raccolta e l'elaborazione di informazioni riguardanti entità competitive e i loro agenti, necessarie a un'organizzazione o a un gruppo per la propria sicurezza. L'**intelligence** è quindi **sia un processo che un prodotto**.

Nell'ambito cyber, la CTI è **il processo di raccolta, elaborazione e analisi dei dati** mentre **il prodotto è la comprensione delle motivazioni, capacità, obiettivi e comportamenti degli attori delle minacce** finalizzata a supportare il processo decisionale e a cambiare l'approccio difensivo da reattivo a proattivo.

Un'organizzazione deve prima di tutto conoscere cosa può rappresentare una minaccia valutando la **Capacità**, l'**Intento** e le **Opportunità** di un potenziale attaccante. Questo implica che una vulnerabilità da sola non rappresenta una minaccia, ma un'opportunità per un avversario; un malware da solo non è una minaccia a meno che non ci sia l'intenzione di un avversario e un'opportunità per utilizzarlo. La minaccia appare se c'è un'intersezione non nulla tra capacità, intento ostile e opportunità. Ne deriva che la CTI rappresenta tutto quell'insieme di informazioni riconducibili a degli eventi ostili, che consente di far acquisire all'organizzazione un vantaggio strategico e che permette di identificare, prevenire e mitigare le minacce informatiche.

Figura 1: Il ciclo di vita dell'intelligence



Principali tipologie di Threat Intelligence

L'Intelligence strategica è in grado di ottenere una visione di alto livello sulle tendenze delle minacce informatiche, ad esempio quelle che interessano un determinato settore, o sul come o il perché alcuni asset strategici di un'organizzazione possono essere presi di mira. Aiuta quindi a sviluppare strategie informate per contrastare le minacce a lungo termine.

L'Intelligence tattica è finalizzata a identificare indicatori di compromissione (IoC) per aiutare i team di risposta agli incidenti e di sicurezza a rilevare gli attacchi in corso o a prevenirli. Gli IoC includono elementi come indirizzi IP, domini malevoli, hash di malware. L'intelligence tattica in genere ha un ciclo di vita piuttosto breve poiché gli attori cambiano spesso le loro infrastrutture [3].

L'intelligence operativa fornisce informazioni dettagliate su specifici vettori di attacco, descrive le tattiche, le tecniche e le procedure (TTP) degli attori delle minacce. Nasce per rispondere a domande su chi/come/perché e quindi richiede maggiori risorse rispetto a quella tattica. In genere ha una durata di vita più lunga, perché il modus operandi degli attori cambia con meno rapidità rispetto agli strumenti utilizzati [4].

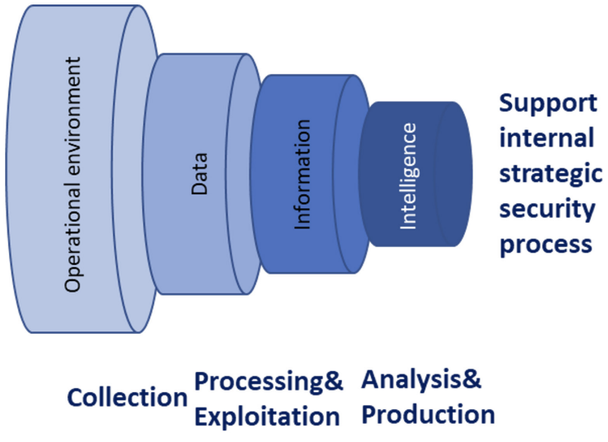
Il ciclo di vita dell'intelligence

L'acquisizione dell'intelligence scaturisce da un processo che prevede diverse fasi: la **pianificazione, raccolta, analisi, implementazione, diffusione**. Queste definiscono il ciclo di vita dell'intelligence (Fig.1).

Molto importante è la fase di **raccolta dei dati**, attraverso feed di intelligence che possono essere a pagamento o open source, sia in forma strutturata (indicatori di compromissione – machine readable) che in forma destrutturata (documenti, report – human readable). Qui gioca un ruolo fondamentale l'**affidabilità e credibilità delle fonti** e la capacità di identificare quelle più rilevanti per l'organizzazione. Se mentre da un lato più fonti di Threat Intelligence possono fornire maggiore visibilità, esiste il rischio di una sovrabbondanza di informazioni irrilevanti sulle minacce.

L'**analisi dei dati** raccolti permette l'arricchimento, la correlazione e contestualizzazione attraverso il lavoro degli analisti e l'uso di strumenti automatizzati (Fig.2).

Figura 2: Dai dati all'informazioni, all'intelligence



Il passaggio dai dati grezzi all'intelligence è essenziale: un indirizzo IP di destinazione raccolto dall'ambiente operativo è un dato, "questo indirizzo IP è il server di comando e controllo per questo determinato malware" è un'informazione, mentre "valutiamo che si tratti di un attacco mirato e un'infezione di un nostro sistema da parte di un determinato malware utilizzato da un determinato attore delle minacce" è effettivamente l'intelligence che deriva dall'analisi che correla dati e informazioni provenienti da diverse fonti per aggiungere contesto e per scoprire pattern [5].

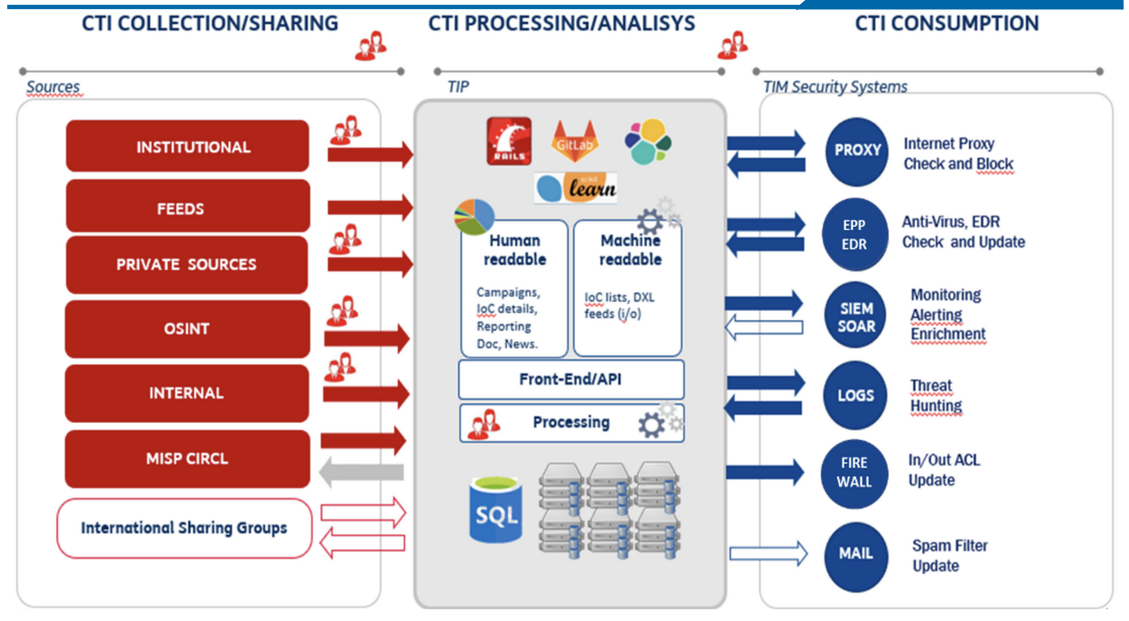
TIP – la piattaforma di Cyber Threat Intelligence di TIM

Il progetto di creare una piattaforma per gestire la Threat Intelligence nasce in TIM nel 2017, con l'intento di superare le limitazioni delle piattaforme commerciali esistenti e offrire maggiore flessibilità, focalizzandosi sui bisogni specifici del processo che andava nascendo. Molte volte, infatti, le piattaforme di security commerciali si erano dimostrate solo parzialmente adatte ai complessi processi di un'azienda come TIM, richiedendo sviluppi custom difficilmente implementabili. Il Security Lab aveva un'esperienza di sviluppo di piattaforme web basate su Ruby on Rails e quindi questa fu la scelta naturale. Sotto questa tecnologia furono fatte convogliare le altre tecnologie open source che ancora oggi sono in uso: MySQL (e poi PostgreSQL), Elasticsearch, Linux).

Inoltre, furono affiancate altre piattaforme che servivano a facilitare l'interconnessione verso altri ambienti, come MISP, Minemeld, TAXII in tutte le sue incarnazioni, e così via.

Tutte queste tecnologie dovevano collaborare per coprire i vari requisiti che via via emerge-

Figura 3: L'architettura della TIP



vano, che hanno poi portato ad una architettura ampia, complessa e scalabile (Fig.3).
Al momento dell'avvio del progetto, la Threat Intelligence gestiva alcune centinaia di indicatori di compromissione (IoC), principalmente lavorati manualmente. Con l'arrivo della TIP, 7 anni più tardi, i numeri sono cresciuti di molti ordini di grandezza. Uno su tutti: gli IoC attualmente presenti nella piattaforma sono **24 milioni** (Fig.4).
Grazie all'interfaccia web della TIP è possibile accedere e consultare le diverse informazioni, effettuare operazioni, richiedere azioni, comprendere lo stato di blocco/detection sui vari consumatori, eseguire ricerche Open Source Intelligence (OSINT).
Dietro a tutto questo c'è il backend, un potente sistema di elaborazione dati, composto da scheduler, processori, motori di indexing, che permette di fare tutte le elaborazioni automatiche al fine di alleviare gli analisti dal lavoro più routinario e massivo. Infine, ci sono le interconnessioni ovvero tutti quei connettori che, a vario titolo, parlano con i sistemi esterni, sia in lettura che in scrittura.
Queste parti lavorano insieme per implementare il ciclo di vita IoC, andando a ricalcare il tradizionale ciclo di vita della CTI. Le cinque fasi sono consecutive e inter-collegate, e l'output di ogni fase può diventare l'input di un'altra, secondo un tradizionale approccio di retroazione (Fig 5).

Le tipologie di dati

Per meglio rappresentare le peculiarità dei dati presenti, questi sono memorizzati in TIP secondo un modello relazionale che tiene conto delle diverse informazioni presenti. Elenchiamo qui alcuni dei modelli presenti e il loro ruolo nel ciclo di vita:

- **IoC**: è l'informazione base presente in TIP, oltre che la più importante. Si tratta principalmente di hash (di file di malware), IP (di attaccanti), domini/URL (di siti compromessi);
- **Campagne**: sono raggruppamenti di IoC e rappresentano eventi malevoli di varia natura. Possono riguardare singoli attacchi cyber, eventi persistenti, campagne di spam;
- **Threat Actor**: rappresentano i gruppi di avversari (nation-state, o cyber criminal) dietro agli attacchi. Questa informazione in TIP aiuta a caratterizzare le minacce e a comprendere i fenomeni.

Tali modelli sono interconnessi tra loro (relazioni da uno a molti), permettendo un'adeguata contestualizzazione e correlazione delle informazioni.
La TIP contiene molti altri modelli (Threat Type, Threat Name/Malware, Vulnerability, Target Sector, Target Technology, Target Country) che permettono di aggregare frammenti di informazioni per costruire uno scenario il più completo e approfondito possibile.
Le informazioni di contesto sono ora ricevute dalle varie sorgenti tramite API oppure inserite manualmente dagli analisti, mentre in futuro è prevista la possibilità di acquisizione, processamento e analisi dell'informazione tramite l'utilizzo di tecniche di Artificial Intelligence (AI), particolarmente Natural Language Processing (NLP), in grado di comprendere e identificare, in vari report, articoli, post su web e dark forum, i principali elementi della CTI insieme alle loro relazioni. Tali informazioni sono poi riportate sulla TIP in modo da completare e contestualizzare le informazioni già presenti e permettere un'analisi esaustiva dei fenomeni, come ad esempio la profilatura dei threat actor, delle campagne di attacco, statistiche e trend sulle tipologie di minacce, indagini su particolari indicatori.

TIP Innovation

La Threat Intelligence non può prescindere dall'avvalersi dell'uso di nuovi strumenti tecnologici come il Machine Learning (ML) e l'Intelligenza Artificiale (AI). Nell'ambito del progetto H2020 Concordia [6], a cui TIM

Figura 4: Alcuni dati significativi della TIP

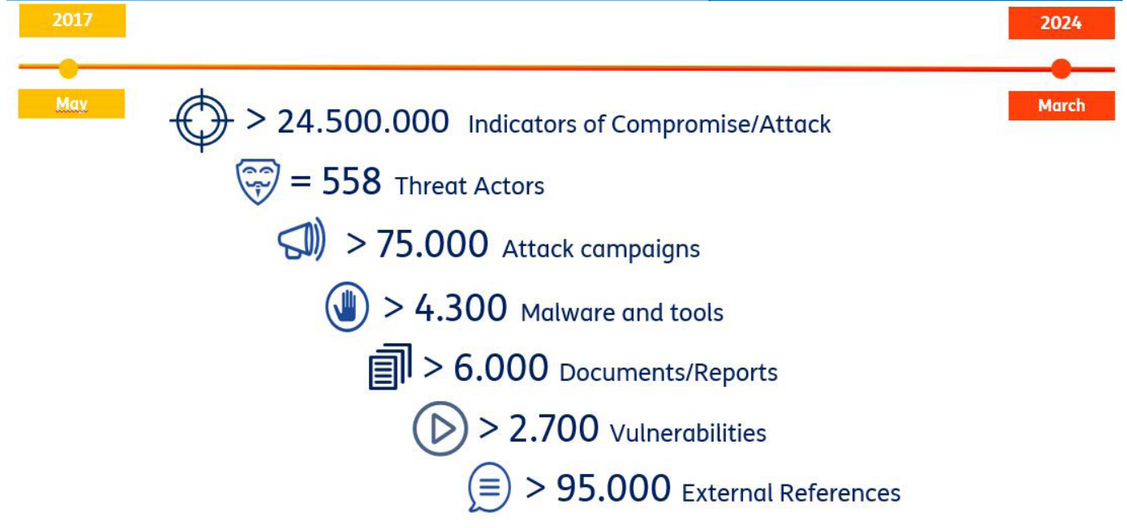
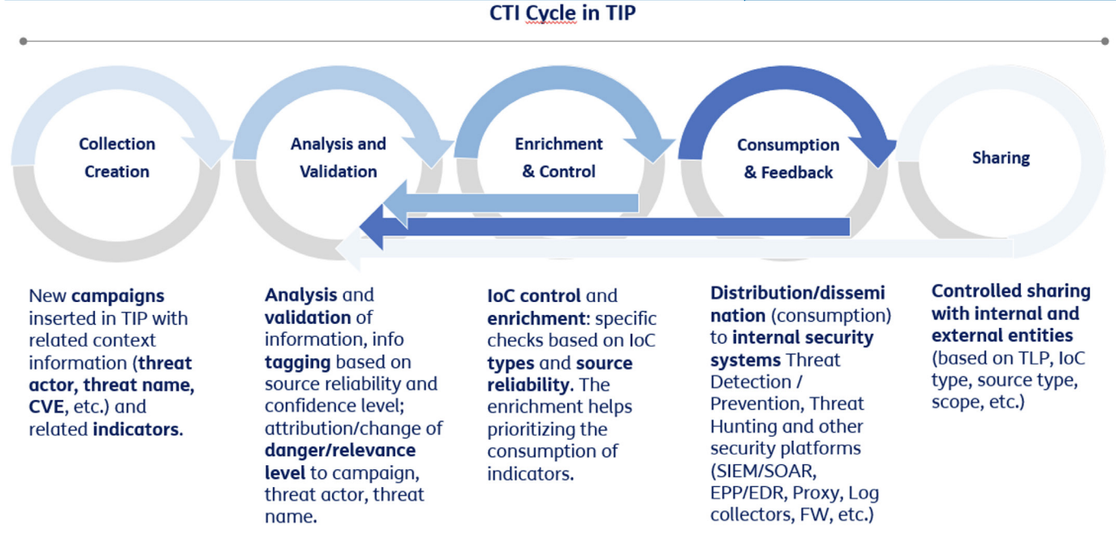


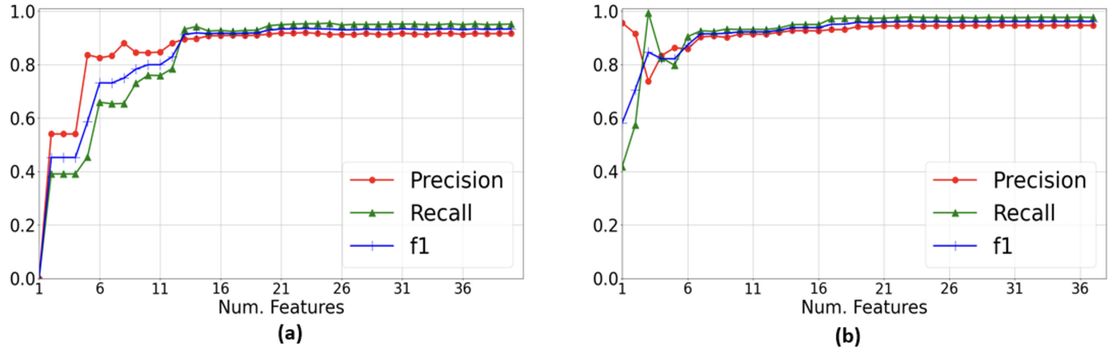
Figura 5: Il ciclo di vita della CTI in TIP



ha partecipato, è stato sviluppato un intero use case dedicato alla CTI per il settore delle telecomunicazioni, intitolato “Automated Processing of Threat Intelligence Information”, per il cui contributo TIM è stata inserita nel database EU dell’Innovation Radar Europeo (le aziende europee con il più alto potenziale di innovazione).
L'obiettivo principale è stato quello di progettare e implementare un metodo di automazione del consumo degli indicatori, con il requisito di poter gestire milioni di IoC al giorno, provenienti da sorgenti eterogenee con diversi livelli di contestualizzazione dell'informazione.
Dati questi requisiti, è stato definito un approccio automatico di analisi, validazione e prioritizzazione al consumo degli IoC, basato interamente sull’utilizzo di un insieme di algoritmi di Machine Learning. In una prima fase di training l’algoritmo impara il comportamento degli analisti per le principali macro-tipologie di indicatori (hash o network) e, in seguito, è in grado di assegnare uno score di priorità usabile ai fini del consumo dei nuovi IoC.

Per il training sono stati usati circa 1,2 milioni di indicatori raggruppati nei macrogruppi Hash (riguardanti file, eseguibili, malware) e Net (indirizzi IP, domini, URL dannosi) ed etichettati dagli analisti CTI. Quest’ultima operazione è un’eccellente base di conoscenze per la formazione sull’apprendimento automatico supervisionato dei motori che avranno poi il compito di classificare i nuovi IoC. Il modello e le feature utilizzate sono specifiche per ciascuno macrogruppo. Il set completo di feature estratte dai dati contiene 43 elementi. Tuttavia, il sistema ottiene un buon risultato di classificazione anche con sole 16 feature come illustrato in Fig.6.
Sono stati testati diversi algoritmi e loro combinazioni e il modello con le migliori prestazioni si è rivelato essere il Random Forest. Le prestazioni raggiungono rispettivamente il 92% e 95% dello score F1, che misura l’accuratezza del modello, sia per IoC di tipo Hash che per IoC di tipo Net.
Oltre all’algoritmo di prioritizzazione automatica degli indicatori di compromissione, nell’ambito del progetto si sono sviluppati anche strumenti per la condivisione delle informazioni di CTI, come il modulo MISP per la condivisione degli indicatori, estratti in tempo reale, relativi ad attacchi DDoS rilevati dagli strumenti di detection disponibili presso i vari partner del progetto (“DDoS Clearing House”).

Figura 6: Dati di performance



Prioritization algorithms’ performance on:
(a) hash indicators (md5, sha1, sha256) and
(b) network indicators (ip, domains, uri/url)

Conclusioni

A sette anni di distanza, la piattaforma per gestire la Threat Intelligence in TIM si trova al centro dei processi di Threat Management/Prevention e sta diventando sempre più importante per il Threat Hunting e l’Incident Handling. Sono state realizzate importanti integrazioni e sviluppi orientati sia alla fase di acquisizione dei dati, con l’integrazione di nuove sorgenti, che alla fase di analisi e consumo/condivisione per rendere la TIP uno strumento completo ed efficace nell’analisi delle minacce sempre più al supporto della security complessiva dell’azienda con la capacità di generare report strategici, tattici e operational. A tal punto è previsto in futuro l’utilizzo di strumenti di Artificial Intelligence a supporto degli analisti, tramite la ricerca e la sperimentazione delle tecnologie di Natural Language Processing in ambito CTI.■

Riferimenti

1. Definition: Threat Intelligence: https://www.gartner.com/en/documents/2487216
2. A Definition of Intelligence: https://www.cia.gov/resources/csi/static/Wanted-Definition-of-Intel.pdf
3. David Bianco “Pyramid of Pain”: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
4. Centre for Internet Security (CIS): https://www.cisecurity.org/what-is-cyber-threat-intelligence/ - defines strategic, operational, and tactical
5. The Data, Information, Knowledge, Wisdom Chain: The Metaphorical link, Michael Hey in 2004: https://www.jonohey.com/files/DIKW-chain-Hey-2004.pdf
6. Concordia – Cyber Security Competence for Research and Innovation: https://www.concordia-h2020.eu/

Acronimi

AI	Artificial Intelligence
CTI	Cyber Threat Intelligence
IoC	Indicator of Compromise
IP	Internet Protocol
MISP	Malware Information Sharing Platform
ML	Machine Learning
OSINT	Open Source Intelligence
SQL	Structured Query Language
TAXII	Trusted Automated Exchange of Intelligence Information
TIP	Threat Intelligence Platform
TTP	Tactics, Techniques and Procedures
URL	Uniform resource locator

Autori

Madalina Baltatu *madalina.baltatu@telecomitalia.it*

È un’analista/ricercatrice nel campo della Cyber Security in Telecom Italia dal 2002. Ha conseguito il dottorato in Sicurezza delle Reti presso il Politecnico di Torino nel 2001. Le sue principali aree di interesse sono la Cyber Security, in particolare la Cyber Threat Intelligence, la sicurezza delle reti TCP/IP, le tecniche di rilevamento delle anomalie per sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS), l’autenticazione e, in passato, la crittografia basate sulla biometria. Ha partecipato a numerosi progetti finanziati dall’Unione Europea nel campo della sicurezza, è autrice di diversi brevetti internazionali e possiede la certificazione GIAC in Cyber Threat Intelligence (GCTI). ■

Stefano Brusotti *stefano.brusotti@telecomitalia.it*

Dottore in Scienze dell’Informazione con master COREP in Telecomunicazioni è entrato nel Gruppo Telecom Italia nel 1996 occupandosi di moneta elettronica e micro pagamenti. Nel 2000 diventa responsabile del Centro di Competenza e Servizio “Security”. Dal 2001, in Telecom Italia Lab, è responsabile dell’Area di Ricerca ICT Security. Nel 2006, in Telecom Italia, della funzione Security Innovation, poi Security Lab, responsabile della prototipazione, scouting e testing di soluzioni di sicurezza e del presidio dell’evoluzione delle minacce. A partire dal 2017 aggiunge la responsabilità della Cyber Threat Intelligence di TIM. Da gennaio 2024 è responsabile della funzione Security Engineering e Threat Management di Cyber Security. ■

Luciana Costa *luciana.costa@telecomitalia.it*

Laureata in Ingegneria delle Telecomunicazioni presso il Politecnico di Torino nel 2000, entra in Telecom Italia nel 2001. A partire dal 2004 si occupa di sicurezza delle reti, in particolare delle problematiche di sicurezza relative al contesto mobile per le tecnologie 2G/3G/4G/5G. È oggi responsabile del gruppo della Cyber Threat Intelligence in TIM. E’ un membro della GSMA e la rappresentante di TIM nel gruppo FSAG. Ha partecipato a numerosi progetti finanziati dall’Unione Europea nel campo della sicurezza. È autrice di diversi brevetti internazionali e possiede la certificazione GIAC in Cyber Threat Intelligence (GCTI). ■

Dario Lombardo *dario.lombardo@telecomitalia.it*

Si laurea nel 2001 presso il Politecnico di Torino con una tesi sulla sicurezza delle reti IP. In TIM si è occupato di sicurezza delle reti e dei sistemi nel perimetro aziendale, per poi passare alla progettazione e realizzazione di piattaforme di security destinate alla sicurezza interna. Ha all’attivo numerosi paper su pubblicazioni scientifiche e un largo numero di contributi a software Open Source. Oggi lavora in Security Engineering con focus principale sullo sviluppo della piattaforma TIP, di cui è responsabile. ■

Il panorama degli zeroday e la ricerca svolta in TIM

Massimiliano Brolli, Elenia Cianfarani, Andrea Carlo Maria Dattola

Per vulnerabilità zeroday si intendono i bug di sicurezza di un prodotto non ancora conosciuti dal vendor, per i quali non è disponibile una patch correttiva. Oggi rappresentano uno dei rischi maggiori per la sicurezza informatica delle aziende e degli stati. Gli zeroday sono considerati dai cybercriminali e dalle entità governative delle risorse preziose, che consentono attraverso il loro sfruttamento di rubare dati, praticare attività di sorveglianza o spionaggio, oppure distruggere infrastrutture critiche. In questo articolo andremo ad analizzare queste "armi cibernetiche" andando ad esplorare cosa sono, i mercati che alimentano, il processo di divulgazione responsabile e le attività di ricerca che vengono svolte in TIM.

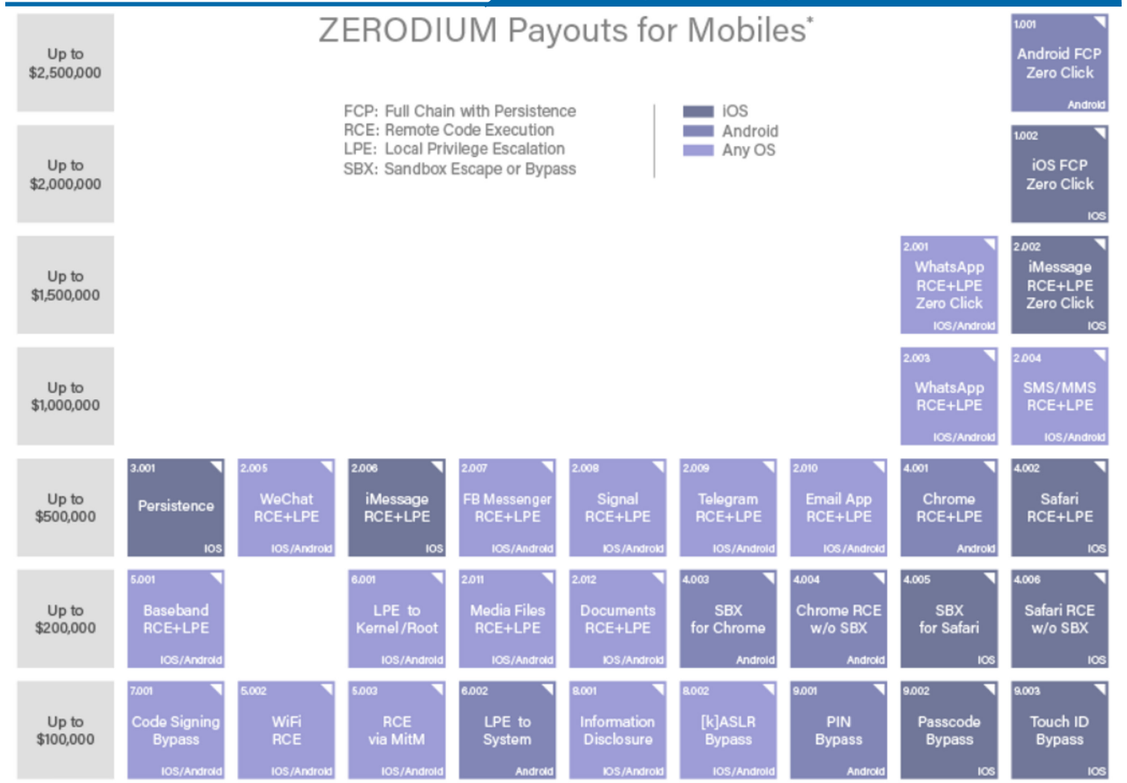
Cosa sono gli zeroday

Ogni prodotto hardware e software contiene del codice che a sua volta può contenere degli "errori" (o "falle di sicurezza" o semplicemente bug) che possono essere sfruttati da un malintenzionato per poter effettuare accessi illeciti ad una qualsiasi infrastruttura.
Tali "errori", sconosciuti al produttore del software ma conosciuti da un limitato numero di persone, vengono chiamati 0day.
Il nome deriva dal fatto che il fornitore ha 0 giorni per correre al riparo e quindi produrre una patch che consenta di rendere quell'errore non più sfruttabile da un ipotetico attaccante.

Zeroday tra etica e cybercrime

Come accennato nell'introduzione, le vulnerabilità zeroday sono molto pregiate. Una falla che consenta una totale compromissione di un dispositivo iPhone oggi può raggiungere il valore di circa tre milioni di euro.
Queste vulnerabilità possono essere sfruttate per accedere e compromettere completamente un dispositivo di un utente, come ad esempio avere il pieno accesso da remoto alla fotocamera e alle chat di uno smartphone. In sintesi, l'accesso a tutte le informazioni e le abitudini di una persona.
Va da sé che tali strumenti possono essere utilizzati per monitorare e sorvegliare le attività di un individuo, ma possono anche es-

Figura 1: Tabella dei pagamenti per exploit zeroday su dispositivi mobile disponibile sulla pagina web di Zerodium



sere utilizzati per interrompere un servizio come una filiera di produzione cartacea o addirittura un servizio idrico di una grande città.

Ricercatori di sicurezza

I bug 0day possono essere individuati dai "ricercatori di sicurezza", professionisti specializzati che esaminano attentamente il software per identificare vulnerabilità di sicurezza ancora sconosciute. Questi esperti, noti anche come "bug hunter", possono differire notevolmente l'uno dall'altro in base all'approccio etico che adottano nel loro lavoro.

I broker zeroday

I broker zeroday sono individui o aziende che si pongono come intermediari nell'acquisto e rivendita di vulnerabilità zeroday. Si è osservato negli ultimi anni che quello degli zeroday è un mercato in espansione e il prezzo di alcuni di essi, trattandosi di vulnerabilità difficili da reperire, può raggiungere anche milioni di dollari. Uno dei broker zeroday più noto è Zerodium, sito disponibile nel surface web che consente ad un bug hunter di vendere al broker gli exploit zeroday, ossia il codice (payload) di sfruttamento del bug (Fig.1).

Nel mercato degli intermediari zeroday sta emergendo anche un altro antagonista, Operation Zero, società russa che ha recentemente aumentato i pagamenti di alcuni exploit su dispositivi mobile, raggiungendo anche i 20 milioni di dollari, un valore decisamente più elevato rispetto a quello offerto da Zerodium.

Cybercrime da profitto

I bug hunter che decidono di non seguire la strada etica (in Fig.2 Gray Hat e Black Hat) possono rivolgersi a intermediari (zeroday broker) oppure mettere direttamente in vendita zeroday ed exploit zeroday su forum nel dark web. I loro clienti non sono solo criminali alla ricerca di guadagni illeciti; spesso gli exploit sono acquistati dagli stessi governi e dalle agenzie di intelligence per attività di spionaggio e sorveglianza. Per citare alcuni casi conosciuti in letteratura citiamo, Stuxnet ed Eternal Blue (si veda box approfondimento).

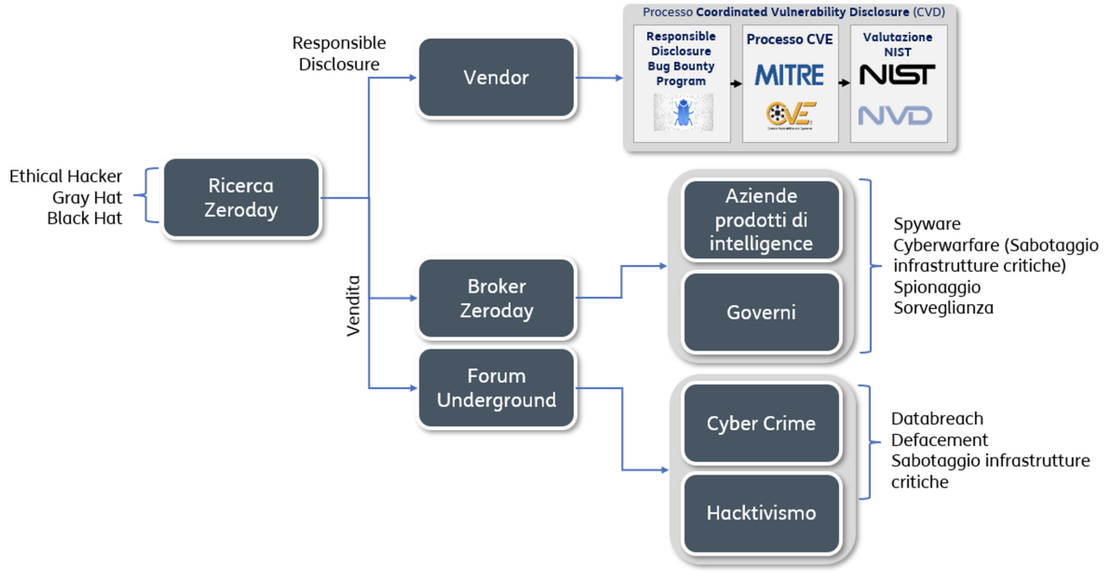
Inoltre, ci sono le aziende che producono sistemi di intelligence e che sono particolarmente interessate agli exploit zeroday no-click, ossia quelle preziose vulnerabilità che non richiedono l'azione degli utenti per entrare in azione.

Nello specifico tali bug consentono di installare spyware sui dispositivi senza alcuna interazione da parte degli utenti che li utilizzano sfruttando ad esempio una chiamata vocale WhatsApp non risposta (come nel caso di Pegasus, un potente spyware creato dall'azienda israeliana NSO Group). Queste aziende sfruttano il mercato degli 0day no-click per migliorare i loro prodotti e rivenderli ad agenzie di intelligence per eseguire operazioni mirate verso persone o paesi ostili.

Come abbiamo visto in precedenza, NSO Group è una azienda israeliana nota per aver sviluppato diversi spyware, come ad esempio Pegasus e Karma, utilizzati per la sorveglianza dei dispositivi mobile di giornalisti, dissidenti e attivisti in diversi paesi del mondo e nello spionaggio di stato. Oggi, è stato classificato come arma dallo stato d'Israele, pertanto, qualsiasi esportazione e utilizzo in paesi esteri deve essere approvata dal governo.

In conclusione, i vantaggi che si possono trarre dallo sfruttamento degli zeroday possono essere notevoli, sia dal punto di vista economico che dal punto di vista strategico, dipende dal vantaggio che vuole trarne l'attore che li utilizza. È da tenere in considerazione anche il rischio che si assume chi compra uno zeroday: potrebbe essere emessa una patch correttiva per quella vulnerabilità addirittura a distanza di poche ore dall'acquisto. Per questo generalmente vengono sfruttati dagli attaccanti verso target mirati, al fine di ridurre al minimo la possibilità che tali preziosi exploit possano essere intercettati.

Figura 2: Flusso di gestione di uno zeroday, dalla divulgazione responsabile alla vendita



La Coordinated Vulnerability Disclosure (CVD)

Esistono diversi modi per divulgare vulnerabilità zeroday: Coordinate Vulnerability Disclosure, divulgazione pubblica, divulgazione a terze parti o a programmi di bug bounty privati.

La Coordinated Vulnerability Disclosure è probabilmente la più etica, che prevede la comunicazione delle vulnerabilità zeroday da parte del bug hunter direttamente al vendor, in via confidenziale, consentendo al vendor stesso di emettere una patch di sicurezza prima della diffusione pubblica. La divulgazione etica rappresenta un vantaggio per l'intera comunità a discapito del cyber crime.

Nella CVD, i ricercatori che individuano una potenziale vulnerabilità zeroday, contattano il vendor del prodotto vulnerabile per segnalare il bug. Il quale, dopo un'analisi interna, può riconoscere o meno la vulnerabilità come zeroday e nel caso positivo avvia lo sviluppo di una patch correttiva; contestualmente, se il vendor non è una CNA (CVE Numbering Authorities), i ricercatori richiedono un identificativo univoco chiamato Common Vulnerabilities and Exposures (CVE) ad un ente no-profit degli Stati Uniti d'Ameri-

ca chiamato MITRE. Si tratta di un codice univoco che viene assegnato a ciascuna vulnerabilità. Nel momento in cui la patch di sicurezza viene rilasciata al pubblico, i ricercatori, in accordo con il vendor, procedono a richiedere al MITRE la divulgazione dello 0-day. Questo sarà disponibile pubblicamente nel National Vulnerability Database (NVD) statunitense con associata una Severity, ovvero una valutazione in scala 1 a 10 della criticità del bug di sicurezza rilevato.

Un cenno sui bug bounty program

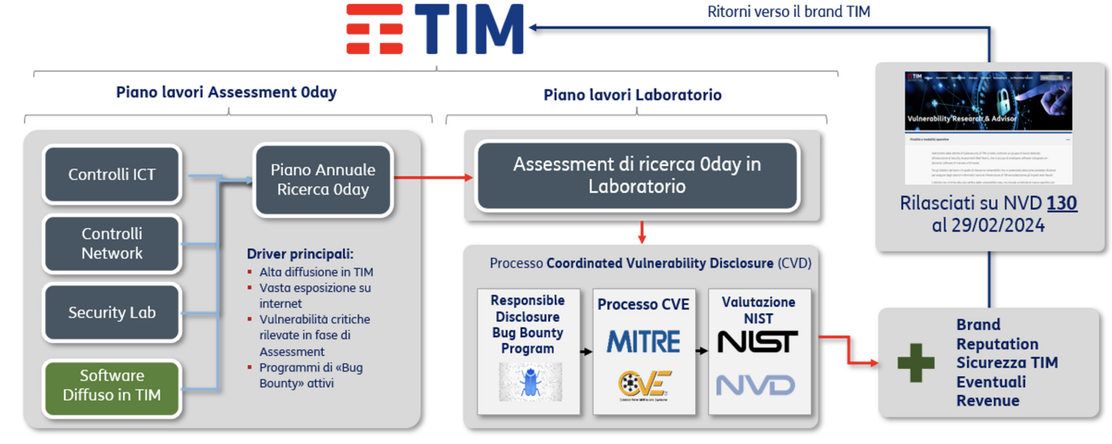
Alcune aziende hanno avviato dei programmi di bug bounty che gli hanno consentito di beneficiare delle competenze della comunità degli hacker etici. Nello specifico un programma di bug bounty è un programma promosso da un'azienda attraverso il quale fornisce una ricompensa, in denaro o altre forme di premi, a coloro che identificano e segnalano un bug di sicurezza non documentato sui prodotti dell'azienda. Le ricompense rilasciate sono molto inferiori ai guadagni che un hacker non etico potrebbe ottenere vendendoli in autonomia o attraverso un intermediario di vulnerabilità come visto in precedenza.

Il lavoro di ricerca in TIM

La storia e i numeri

A partire dalla fine del 2019, la funzione coordinata da Massimiliano Brolli all'interno della Security di TIM ha avviato il processo di Coordinated Vulnerability Disclosure (CVD) nell'ambito delle attività di ethical hacking (Red Team).
Il processo aderisce alla Coordinated Vulnerability Disclosure descritta sopra e prevede la divulgazione pubblica, previo consenso del vendor, quando sarà emessa la patch di sicurezza. Il processo adottato in TIM prevede che prima della pubblicazione, qualora il vendor non sia una CNA (e quindi capace di assegnare autonomamente le CVE) venga svolta una verifica in campo per valutare che la patch rilasciata dal vendor, ed installata sull'infrastruttura di TIM, sia stata efficace nella risoluzione del problema di sicurezza segnalato (Fig.3).
Fino a febbraio 2024 sono state inoltrate ai vendor 230 segnalazioni di bug zeroday, di cui 130 riconosciuti, risolti e pubblicati. In TIM cerchiamo sempre di promuovere con questi l'importanza della divulgazione responsabile delle vulnerabilità (Fig.4).

Figura 3: Processo di alimentazione della ricerca degli zeroday in TIM e Coordinated Vulnerability Disclosure



Infatti, questo processo adottato, oltre ad aiutare i vendor nell'identificazione di nuove vulnerabilità, comporta una serie di altri vantaggi:

- gli amministratori di sistema sono più solerti nell'installare una patch di sicurezza una volta che i dettagli dell'exploit sono stati resi pubblici;
- i fornitori di strumenti di protezione perimetrale potranno aggiornare le policy e far sì che il loro software intercetti e blocchi il "payload" ormai pubblico;
- i fornitori di soluzioni per l'esecuzione di Vulnerability Assessment potranno aggiornare il loro software al fine di rilevare le nuove vulnerabilità;
- altri vendor potranno prendere spunto e verificare se hanno replicato lo stesso problema di sicurezza su prodotti analoghi.

Cenni sulle vulnerabilità più critiche rilevate

Nel corso dell'attività di ricerca del Red Team di TIM si vogliono citare alcuni degli impatti più critici rilevati:

- un malintenzionato privo di credenziali, ma attestato nella rete TIM avrebbe potuto disabilitare le dorsali in fibra ottica di tutta TIM;
- un malintenzionato, con accesso alla rete aziendale, avrebbe potuto aprire qualsiasi varco all'interno degli edifici di TIM (compresi i data center);
- un malintenzionato avrebbe potuto manomettere la temperatura dei re-

Figura 4: Sintesi del lavoro di ricerca in TIM

frigeratori necessari alla corretta conservazione dei medicinali compromettendone l'utilizzo (vulnerabilità rilevata durante la pandemia per Covid-19 per cui è stato emesso uno speciale bollettino di sicurezza da CISA - Cybersecurity & Infrastructure Security Agency degli Stati Uniti d'America).

Principali tecniche per identificare gli zeroday

I ricercatori di sicurezza giocano un ruolo fondamentale nell'individuare vulnerabilità zeroday utilizzando una serie di strumenti e tecniche manuali sofisticate.
Generalmente il primo passo per scoprire una vulnerabilità zeroday è avere una comprensione approfondita del funzionamento interno del software e delle tecnologie che si intendono esaminare. Questo richiede una buona conoscenza dei linguaggi di programmazione, dei protocolli di comunicazione e delle architetture di sistema.
Esaminiamo adesso quali sono i metodi, le tecniche e le pratiche più comuni per trovare vulnerabilità zeroday per un bug hunter.

Analisi statica e dinamica

Le tecniche di analisi statica e dinamica sono fondamentali per individuare vulnerabilità nei codici sorgente e nei programmi in esecuzione. Gli strumenti di analisi statica esaminano il codice senza eseguirlo, cercando pattern ed errori comuni, come buffer overflow o problemi di gestione della memoria.
D'altra parte, l'analisi dinamica coinvolge l'esecuzione del software in un ambiente controllato, monitorando il suo comportamento per rilevare eventuali anomalie o vulnerabilità.
Tool comunemente usati:

- **analisi statica**: SonarQube, Fortify Static Code Analyzer, Checkmarx, Bandit (Python);
- **analisi dinamica**: Burp Suite, OWASP ZAP, Acunetix.

Reverse engineering

È una pratica comune tra i ricercatori di sicurezza per comprendere il funzionamento interno del software e identificare potenziali vulnerabilità. Questo processo coinvolge l'analisi dei file binari per comprendere la logica del programma, individuare funzionalità nascoste o vulnerabilità di sicurezza.
Tool comunemente usati:

- IDA Pro, Ghidra, Radare2, gdb, Cutter.

Fuzzing

Si tratta di una tecnica automatizzata utilizzata per scoprire vulnerabilità attraverso l'iniezione di dati casuali o semi-casuali nel software al fine di provocare errori o crash. Gli strumenti di fuzzing possono essere configurati per testare diversi input e scenari, esplorando il software in modo esaustivo alla ricerca di vulnerabilità.
Tool comunemente usati:

- AFL++(American Fuzzy Lop), Wfuzz, Hongfuzz, libFuzzer, Jazzer, OSSFuzz, Synopsys.

Penetration testing

È un'attività in cui un ricercatore di sicurezza simula un attacco informatico contro un sistema o una rete per identificare e sfruttare vulnerabilità. Anche attraverso questa metodologia, i Penetration Tester hanno la possibilità scoprire vulnerabilità zeroday.
Tool comunemente usati:

- Metasploit, Nmap, Nessus, BurpSuite, Sqlmap.

Conclusioni

La vendita delle vulnerabilità zeroday è considerata una pratica altamente controversa che fa molto discutere poiché considerata poco etica. Il commercio di tali vulnerabilità contribuisce alla ricchezza di pochi danneggiando molti. Per questo motivo in TIM ci battiamo per la divulgazione etica. Dal 2019 contribuiamo attivamente alla divulgazione etica e responsabile delle vulnerabilità zeroday, supportando i vendor nella risoluzione dei bug e diffondendo l'importanza della divulgazione etica delle vulnerabilità. Abbiamo supportato alcuni vendor, con cui collaboriamo, nell'adesione al programma CNA (CVE Numbering Authorities), sponsorizzandolo come un percorso di crescita e arricchimento sia per l'azienda stessa e soprattutto per i suoi clienti.■

Casi famosi nella storia

Stuxnet la prima arma cibernetica

Stuxnet è il nome di un worm che nel 2010 ha seriamente danneggiato la centrale nucleare iraniana di Natanz (Fig.A).
Spesso viene definita come la prima arma cibernetica della storia e ha segnato sicuramente un cambiamento epocale nel contesto geopolitico e nelle modalità di conduzione di una guerra.
Gli Stati Uniti erano preoccupati già da alcuni anni del programma nucleare che stava portando avanti l'Iran, dall'altra parte anche la vicina Israele stava chiedendo supporto per un bombardamento di tipo convenzionale verso i bunker iraniani. L'amministrazione Bush respinse questa richiesta, ma diede il via alla pianificazione di un cyber attacco.
L'operazione, nome in codice "Giochi Olimpici", vide coinvolti gli Stati Uniti in collaborazione con tecnici informatici israeliani e i servizi segreti olandesi. L'attacco ha sfruttato quattro zeroday Windows che hanno colpito i PLC Siemens che gestivano le centrifughe di arricchimento dell'uranio facendole andare fuori controllo e compromettendone il funzionamento.
Trattandosi di un programma nucleare segreto non sono noti i danni effettivi, ma la stima è che l'attacco abbia rallentato di diversi anni il programma nucleare iraniano.

Figura A: Centrifughe della centrale nucleare di Natanz in Iran

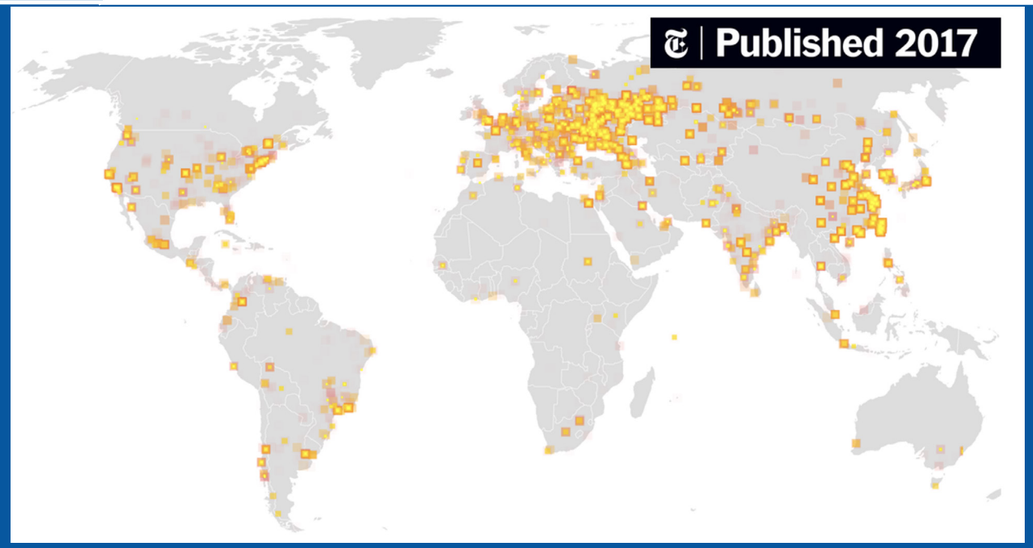
Lo zeroday nascosto dalla NSA

Nel maggio 2017 si diffuse a macchia d'olio nel mondo il malware WannaCry.
Tale malware utilizzava un potente 0day che era stato precedentemente rubato a una nota agenzia di intelligence statunitense: la National Security Agency (NSA).
WannaCray per diffondersi, utilizzava uno 0day chiamato EternalBlue che consentiva al malware di rendersi "wormable", ovvero espandersi da un computer windows ad un altro, avendo pieno accesso alle risorse del computer. Ma perché avvenne tutto questo?
Perché Microsoft, non conoscendo questo bug (e relativo exploit), non aveva aggiornato il servizio (nello specifico SAMBA) che risultava vulnerabile ad un attacco 0day. In sintesi, in quei giorni tutti i computer Windows del mondo erano vulnerabili a WannaCry (Fig.B).

Log4Shell – Lo zeroday che ha fatto tremare il mondo

Il 10 dicembre del 2021 è stata resa pubblica la vulnerabilità cosiddetta Log4Shell che consentiva, ad un attaccante remoto senza alcuna autenticazione, l'esecuzione di codice arbitrario su un server prendendone totale controllo.
La vulnerabilità era stata segnalata privatamente alla fine di novembre ad Apache, che l'aveva resa pubblica solo dopo aver emesso una patch che inizialmente era compatibile solo con un sottoinsieme di sistemi.
Il motivo per cui questa vulnerabilità ha sconvolto il mondo intero, oltre che per il livello di criticità massima ottenuta (10 su 10), era la sua scalabilità senza precedenti.
Il prodotto vulnerabile era ed è ampiamente diffuso a livello globale, e fino al momento della risoluzione della vulnerabilità qualsiasi sistema esposto su Internet che implementava il prodotto era un potenziale bersaglio.

Figura B: Mappa della propagazione di WannaCry nel mondo pubblicata da The New York Times (https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html)



Sitografia

- https://www.redhotcyber.com/post/full-disclosure-delle-vulnerabilita-l-arma-definitiva-a-prova-di-zona-grigia/
- https://www.cybersecurity360.it/nuove-minacce/vulnerabilita-zero-day-cosa-sono-e-come-funziona-il-mercato-nero-degli-exploit/
- https://www.cve.org/
- https://zerodium.com/
- https://it.wikipedia.org/wiki/NSO_Group
- https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors

Acronimi

CISA	Cybersecurity and Infrastructure Security Agency
CNA	CVE Numbering Authorities
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
NSA	National Security Agency
NVD	National Vulnerability Database
PLC	Programmable Logic Controller

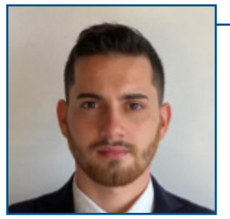
Autori

Massimiliano Brolli *massimiliano.brolli@telecomitalia.it*

Responsabile della funzione di Security Threat Management di TIM, è in azienda dal 2001, dopo aver maturato diversi anni di esperienza nell'ambito dello sviluppo software e aver avviato alcune startup innovative. In TIM ha ricoperto svariati incarichi entrando a far parte della struttura di Security nel 2008.
Attualmente coordina i gruppi di Cyber Threat Intelligence, Security Lab e il Red Team, dove ha sviluppato attività innovative di ricerca nell'ambito 4G/5G, protocolli di segnalazione e ha introdotto la ricerca di vulnerabilità zeroday in TIM. ■

Elenia Cianfarani *elenia.cianfarani@telecomitalia.it*

Cyber Security Specialist, entra a far parte del gruppo TIM nel 2019 ricoprendo il ruolo di Security Service Manager in Telsy, gestendo attività di ethical hacking principalmente in ambito Golden Power. Dal 2008 al 2019 ha lavorato per diverse multinazionali di consulenza, dove ha maturato esperienze in svariati ambiti della Cyber Security. Dal 2023 passa nella funzione Security Threat Management di TIM, dove attualmente dirige il processo di Coordinated Vulnerability Disclosure e le attività di Zeroday Research Assessment. ■



Andrea Carlo Maria Dattola *andreacarlomaria.dattola@telecomitalia.it*

Dal 2020 è un Penetration Tester/Ethical Hacker presso il Red Team di Telecom Italia (TIM), incluso nella funzione di Security Threat Management di TIM coordinata da Massimiliano Brolli. Ha conseguito la Laurea Magistrale in Ingegneria Informatica e dei Sistemi per le Telecomunicazioni. Attualmente si occupa di garantire la Sicurezza dei sistemi TIM attraverso attività di penetration testing sui prodotti aziendali e in Golden Power, ricerca sulle falle di sicurezza nei protocolli di segnalazione nell'ambito 4G/5G e ricerca di vulnerabilità 0day: ad oggi 17 CVE. ■

Crittografia Post-Quantum: le sfide della transizione

Veronica Cristiano, Marco Rinaudo, Edoardo Signorini, Francesco Stocco

L'avvento del computer quantistico, seppur offra nuove opportunità, apre la possibilità ad attaccanti dotati di strumenti quantistici di sferrare attacchi agli attuali sistemi crittografici, con un impatto disastroso sulla sicurezza dei protocolli di comunicazione odierni. Per far fronte alla minaccia, la comunità scientifica internazionale si è mobilitata nella definizione di nuovi standard crittografici, resistenti a questo tipo di attacchi e implementabili su calcolatori classici. La transizione a schemi di crittografia post-quantum ha portato nuove sfide alle quali l'industria si sta preparando.

Nei protocolli di comunicazione oggi utilizzati, tra cui il TLS (che protegge le comunicazioni Internet), la sicurezza dei dati è garantita da algoritmi crittografici afferenti a due principali famiglie:

- chiave simmetrica: mittente e destinatario condividono una chiave segreta usata per cifrare e decifrare;
- chiave pubblica: ogni utente ha una coppia di chiavi pubblica e privata. Chiunque può usare la chiave pubblica per cifrare, ma solo chi ha la chiave privata può decifrare.

In tali protocolli, gli schemi a chiave pubblica vengono usati per scambiare una chiave simmetrica con cui successivamente si cifrano i dati.

La minaccia del quantum computer

Nel corso degli anni '80 [1] venne teorizzato un nuovo tipo di calcolatore, denominato quantum computer (QC), il cui funzionamento si basa su alcune leggi della meccanica quantistica. Tale oggetto, rimasto per molti anni un concetto puramente teorico, permetterebbe di risolvere alcune classi di problemi in modo estremamente più efficiente di quanto possibile con un computer classico. Tra i diversi campi in cui sono state indagate le potenzialità del QC vi è anche quello della crittoanalisi: nel 1994 l'americano Peter Shor descrisse un algoritmo in grado di risolvere in tempo polinomiale i problemi della fattorizzazione degli interi e del logaritmo discreto, su cui si basa la quasi totalità degli schemi a chiave pubblica attualmente utilizzati. Qualora venisse costruito un QC con sufficiente potenza per implementare l'algoritmo di Shor, diventerebbe quindi possibile rompere concretamente schemi quali RSA o ECDH, rendendo vulnerabili i dati scambiati attraverso il TLS o altri protocolli crittografici (es. VPN, app messaggistica).

Nel corso degli ultimi anni sono stati presentati i primi prototipi di QC che, pur non essendo ancora sufficienti per un utilizzo crittoanalitico, evidenziano importanti investimenti e il crescente rischio per la sicurezza delle informazioni. Inoltre, il futuro sviluppo di un QC può costituire un pericolo anche per i dati scambiati oggi: in un attacco "store now, decrypt later" l'attaccante intercetta i dati cifrati e li conserva fin quando non avrà un QC con cui recuperare i dati in chiaro. Tale attacco impatta soprattutto contesti che prevedono di mantenere cifrati i dati per lunghi periodi (es. dati sanitari o classificati) e rende necessario un avvio quanto più rapido della transizione verso soluzioni quantum resistant.

Si rendono quindi necessari algoritmi a chiave pubblica non attaccabili da un QC, che formano la cosiddetta Post Quantum Cryptography o PQC.

La standardizzazione della PQC

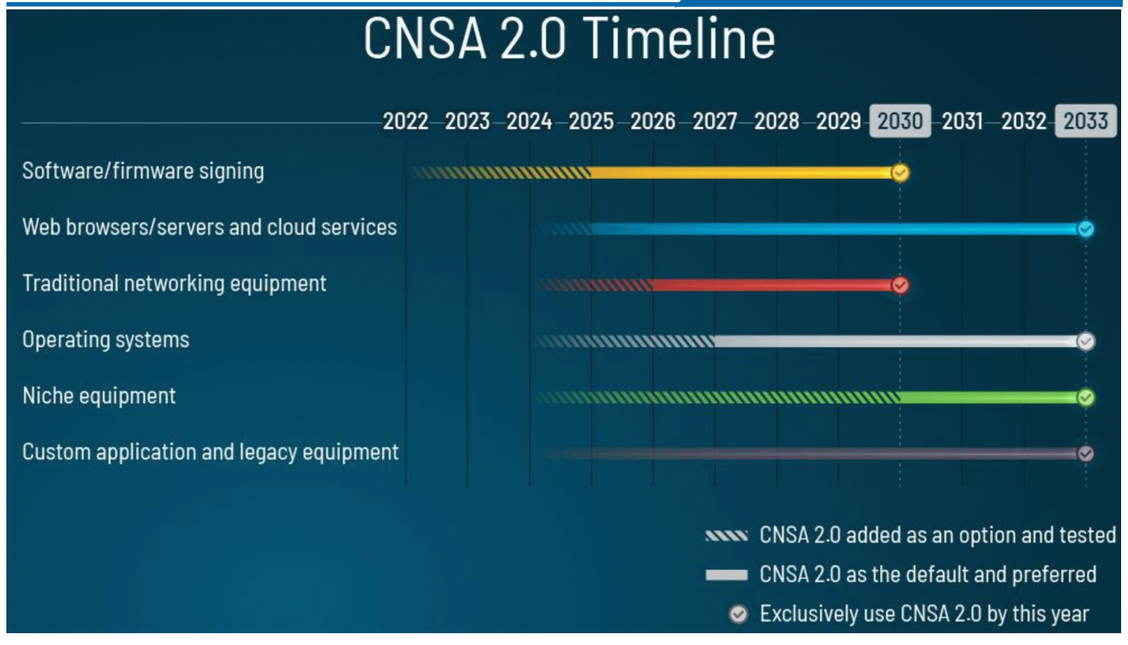
Per fornire un riferimento univoco da seguire nell'implementare tali algoritmi, diversi enti di standardizzazione hanno intrapreso iter volti alla selezione dei migliori schemi PQC. Punto di riferimento è il processo indetto dal NIST americano: articolato su diversi round, svol-

tisi tra il 2016 e il 2022, ha portato alla pubblicazione di una bozza di standard per tre schemi PQC nell'agosto 2023. La versione definitiva è prevista entro fine 2024. Gli schemi presentati riguardano primitive di scambio chiave, tramite Key Encapsulation Mechanism (KEM), e di firma digitale.
Mentre alcuni Paesi (ad es. Australia, UK, Canada) seguono quanto fatto dal NIST, altri governi hanno avviato processi indipendenti [2]. Tra questi possiamo ricordare:

- Cina: avvio nel 2018 di un round di valutazione che ha portato, nel 2020, a selezionare tre schemi (diversi da quelli NIST);
- Corea del Sud: nel 2021 ha inizio la competizione KpqC volta a standardizzare schemi PQC, non ancora conclusa.

In Europa, ANSSI (Francia) [3] e BSI (Germania) [4] hanno prodotto linee guida sulla PQC che prendono a riferimento la competizione NIST, ma se ne discostano in alcuni frangenti. In USA, la NSA ha aggiornato la suite di algoritmi CNSA per la protezione del segreto di stato includendo schemi PQC [5], definendo inoltre un piano di transizione (Fig.1).

Figura 1: Timeline per la transizione a CNSA 2.0



La matematica della PQC

La matematica è parte fondamentale della costruzione di schemi crittografici; infatti, la loro sicurezza si basa sulla difficoltà computazionale di risolvere un dato problema matematico.
Se gli schemi di crittografia classica basano la loro sicurezza su problemi difficili per un calcolatore classico, il logaritmo discreto (ECDH) e il problema della fattorizzazione (RSA), gli schemi di crittografia post-quantum fondano la loro sicurezza su problemi diversi, difficili anche per un computer quantistico.
La maggior parte di questi è costruita su oggetti matematici che danno il nome alle branche della PQC: lattice-based (reticoli), code-based (codici) e hash-based cryptography (funzioni di hash).

Reticoli

Un reticolo è definito, a partire da una base di vettori linearmente indipendenti, come l'insieme delle combinazioni lineari a coefficienti interi dei vettori della base. Gli schemi selezionati dal processo di standardizzazione del NIST, sia KEM che firme, appartenenti alla lattice-based cryptography sono costruiti a partire dal problema del Learning With Errors (LWE) [6]. Dato un sistema di equazioni lineari random che descrivono un segreto, il LWE si basa sull'idea di nascondere il valore del segreto aggiungendo del rumore al sistema.
Nel corso degli anni sono state proposte delle varianti strutturate del LWE allo scopo di diminuire la dimensione della chiave pubblica: Ring-LWE e Module-LWE.

Codici

Altri oggetti matematici di importanza rilevante nella PQC sono i codici (o codici a correzione d'errore). Questi nascono nel contesto delle telecomunicazioni per individuare e correggere errori che possono verificarsi nella trasmissione attraverso un canale rumoroso e sono stati introdotti nel contesto della crittografia con lo schema di Robert McEliece [7] nel 1978. A partire da questo sono stati progettati altri algoritmi PQC, sia KEM che firme, costruiti su problemi riconducibili al più generale Decoding Problem, ovvero il problema della decodifica di un vettore contenente un errore.

Hash

Le funzioni di hash hanno un ruolo fondamentale in numerose costruzioni crittografiche. In particolare, nel panorama PQC le funzioni di hash possono costituire l'elemento cardine di una firma. È interessante notare che nelle firme hash-based la sicurezza non si basa su un problema matematico, bensì sulla proprietà di generiche funzioni di hash.

Maturità percepita

Tra le firme, quelle hash-based vantano il fatto che risulterebbero attaccabili solo se fosse possibile compromettere la funzione di hash utilizzata al loro interno. In quanto componenti comuni ad altre firme, una vulnerabilità di questo tipo avrebbe ripercussioni così estese da non essere ritenute plausibili. Questa è percepita dalla comunità scientifica come una garanzia di sicurezza.

A sostegno della sicurezza della lattice-based cryptography, sebbene sia più recente (il primo schema è del 1996 e il LWE del 2005), vi è un peculiare risultato teorico [8] che ne ha rafforzato la fiducia e ha in parte favorito la predominanza di schemi basati sui reticoli nel processo di standardizzazione NIST: alla fine del

terzo round sono stati scelti CRYSTALS-Kyber [9] per la negoziazione chiave e CRYSTALS-Dilithium [10], Falcon [11] e SPHINCS+ [12] per le firme digitali post-quantum. Tutti, tranne SPHINCS+ che è hash-based, sono costruiti sui reticoli.

Rimane fuori dalle scelte del NIST, per ora, la code-based cryptography con lo schema più conservativo: Classic McEliece [13]. Nel tempo, questo schema ha resistito a numerosi tentativi di crittoanalisi e ha dimostrato un'elevata affidabilità ed efficienza in termini di prestazioni. Nonostante ciò, il principale svantaggio, che negli anni ha ricevuto soluzioni solo parziali o insicure, è quello della dimensione delle chiavi pubbliche che rende questo schema di difficile utilizzo in contesti con stringenti requisiti di memoria o banda.

Transizione al post-quantum

La transizione verso nuovi standard crittografici comporta storicamente numerose sfide. Nella migrazione ad algoritmi post-quantum, si possono identificare processi separati per gli schemi di scambio chiave e di firma digitale. Un caso di studio particolarmente interessante per le sue applicazioni è il TLS [14]. Nel protocollo TLS, sebbene la sicurezza di una comunicazione attiva sia garantita da algoritmi simmetrici, non impattati dall'avvento del quantum computer, l'avvio del protocollo richiede un metodo per scambiare la chiave (simmetrica) crittografica ed è necessario verificare l'identità del server a cui si è connessi (e talvolta anche quella del client).
In questa fase, detta di handshake, entrano in gioco algoritmi asimmetrici di negoziazione chiave, per garantire confidenzialità della comunicazione, e di firma digitale, per l'autenticità. Entrambe sono proprietà irrinunciabili in un protocollo di comunicazione sicura come il TLS, ma la sostituzione degli algoritmi sottostanti presenta sfide e orizzonti temporali differenti.
Ad oggi, l'algoritmo maggiormente utilizzato nella fase di negoziazione chiave del TLS è lo schema ECDH X25519 [15].
L'alternativa post-quantum in fase di standardizzazione è lo schema ML-KEM (Kyber), uno schema KEM basato su reticoli. DH e KEM sono due diversi paradigmi di negoziazione chiave, il primo di difficile realizzazione in ambito post-quantum.
Sebbene presentino potenziali incompatibilità dovute alla necessaria interattività dei KEM (Fig.2), l'utilizzo di un KEM nel TLS non presenta difficoltà.
D'altra parte, ML-KEM ha dimensioni molto maggiori, anche nella versione ML-KEM-512 che corrisponde allo stesso livello di sicurezza di X25519 (Fig.3). Sperimentazioni guidate da Google [16] e Cloudflare [17] hanno dimostrato come l'incremento di dimensioni introduca un aumento di latenza trascurabile nell'handshake TLS.
Le nuove dimensioni possono però indurre una frammentazione dei pacchetti di handshake, causando possibili incompatibilità con dispositivi legacy. La migrazione di questi apparati rappresenta una delle principali sfide nell'introduzione di KEM PQC. Le firme PQ, contrariamente ai KEM, non presentano differenze funzionali rispetto agli schemi tradizionali. Ciò nonostante, lo stato di queste primitive appare oggi più complesso. Il NIST sta definendo gli standard di tre schemi: ML-DSA (Dilithium), FN-DSA (Falcon) e SLH-DSA (SPHINCS+).
La difficoltà nel sostituire gli algoritmi classici risiede nell'uso eterogeneo che

Figura 2: DH vs KEM. I KEM richiedono sempre un round di interazione dopo lo scambio delle chiavi pubbliche

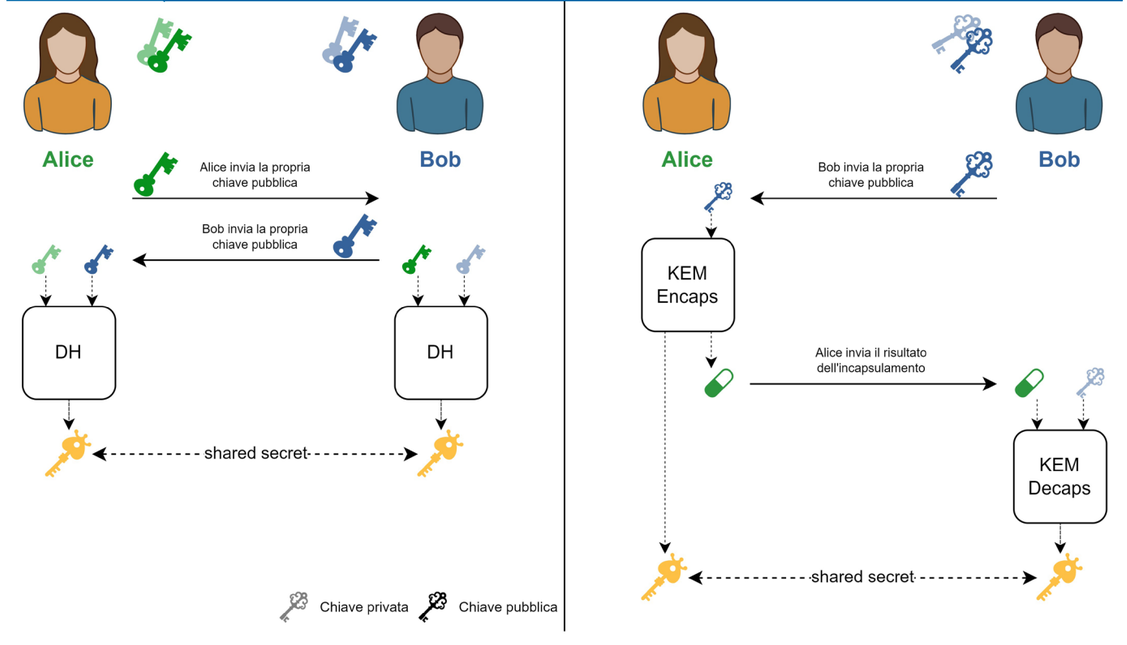
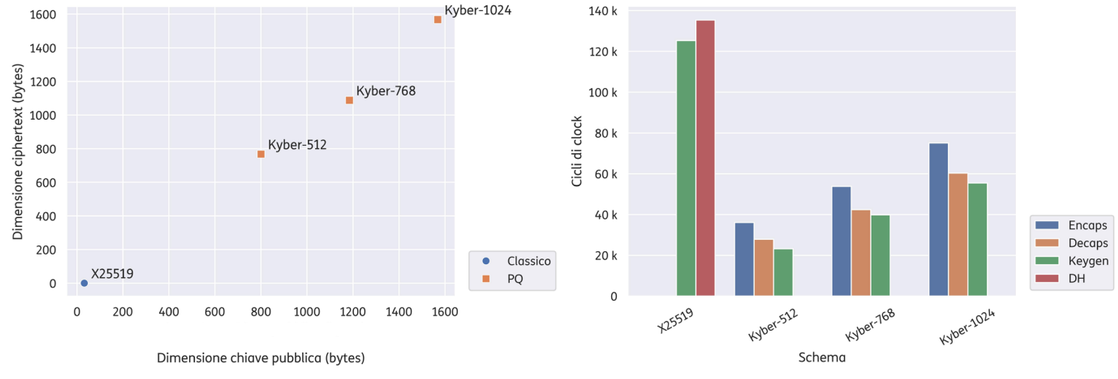


Figura 3: Confronto tra ECDH X25519 e KEM PQC Kyber, nelle sue tre versioni di sicurezza



viene fatto di questa primitiva. Nel TLS, ad esempio, le firme hanno ruoli e requisiti diversi a seconda che vengano utilizzate durante l'handshake o nella verifica dei certificati.
Nessuno degli schemi PQ attualmente proposti risulta particolarmente indicato per tutti i ruoli, d'altra parte utilizzare schemi multipli aumenta gli sforzi implementativi e la superficie di attacco. Ad oggi, solo la versione più compatta di ML-DSA (Dilithium-2) ha una combinazione di dimensioni e prestazioni compatibili con i tradizionali Ed25519 e RSA (Fig.4); essa, tuttavia, introduce 17 KB di overhead rispetto agli algoritmi tradizionali, con conseguenze più marcate rispetto all'uso dei KEM PQC. Lo stato parzialmente insoddisfacente delle firme digitali ha portato il NIST ad avviare nel 2023 un ulteriore processo dedicato [18].

Protocolli ibridi

Per facilitare la migrazione e ridurre l'impatto di possibili vulnerabilità negli algoritmi PQC, è possibile combinare la crittografia tradizionale e quella PQ tramite un approccio ibrido (Fig.5) nel quale la componente PQC difende da un attacco quantistico, mentre quella classica da una vulnerabilità dell'algoritmo PQC. Tale approccio rappresenta un passaggio intermedio importante nella transizione completa alla PQC, poiché di facile realizzazione e con immediati benefici di sicurezza.

Conclusioni

Il processo di standardizzazione delle tecnologie post-quantum si trova nelle fasi conclusive e l'industria si sta preparando alla transizione. Nel contesto delle comunicazioni web, l'integrazione di algoritmi PQC nel protocollo TLS garantirà già nel breve termine la confidenzialità dei dati rispetto ad avversari quantistici. Oltre al TLS, la migrazione alla PQC riguarda numerosi altri protocolli che impiegano la crittografia a chiave pubblica. Alcuni, come SSH o i protocolli VPN come IPSec e WireGuard, condividono le caratteristiche e le sfide evidenziate per il TLS. Altri, come DNSSEC o protocolli basati su primitive più avanzate, non presentano ad oggi alternative PQ praticabili e rappresentano interessanti direzioni di ricerca.

Nonostante i processi ancora in corso, l'industria ha oggi gli strumenti per avviare la transizione a tecnologie post-quantum, valutandone l'impatto sui processi e selezionando gli algoritmi migliori per i casi d'uso specifici. Una preparazione attenta è oggi fondamentale per mitigare la minaccia del QC, così da garantire la sicurezza delle informazioni a lungo termine.■

Figura 4: Confronto tra firme digitali tradizionali e PQ

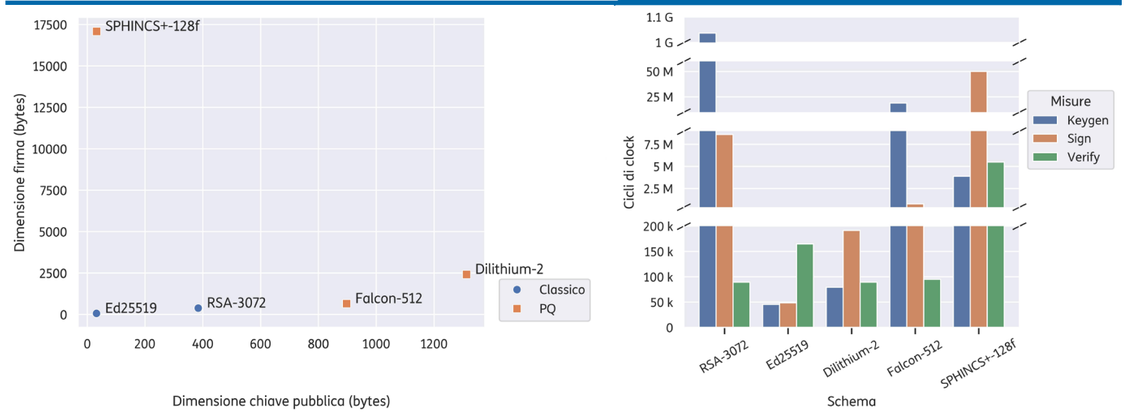
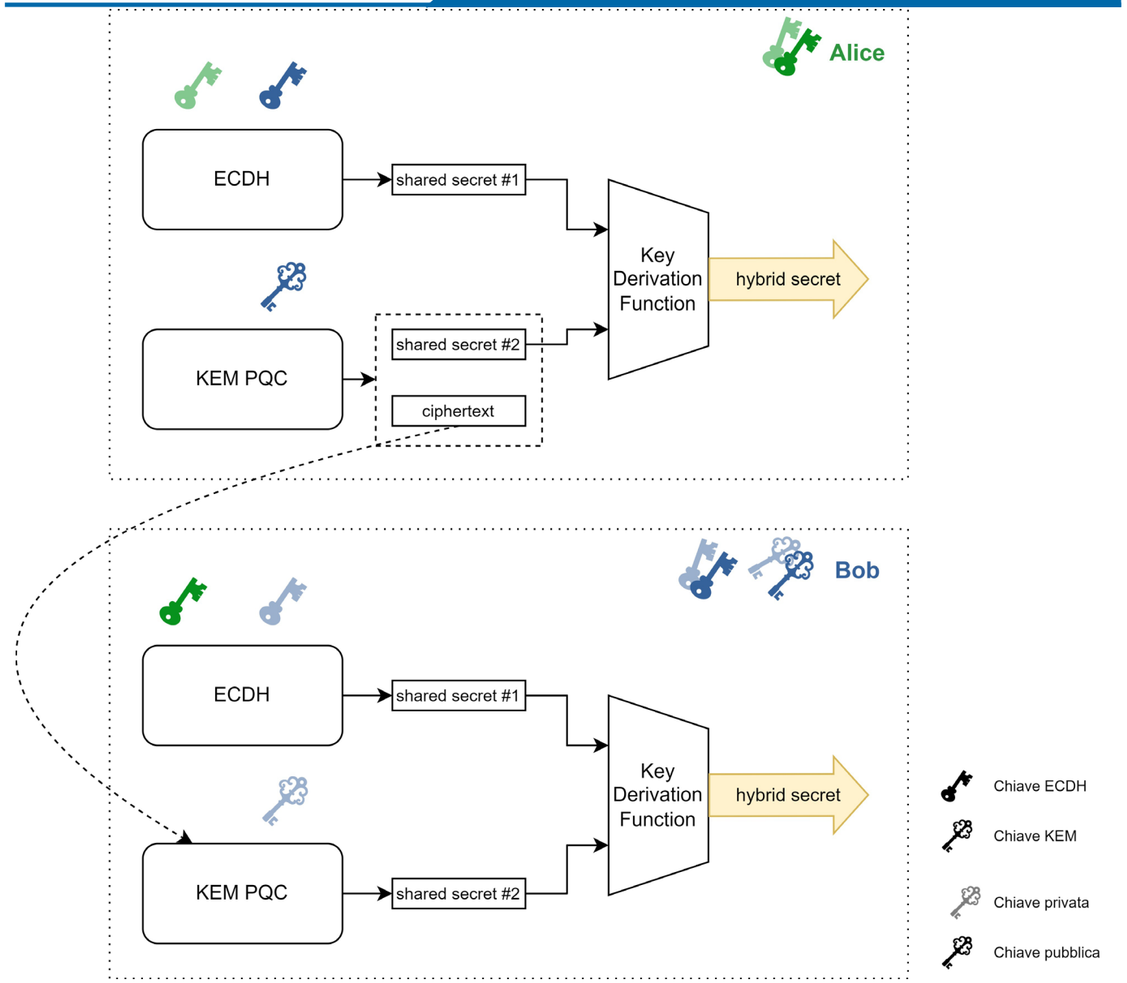


Figura 5: Negoziazione chiave ibrida tramite combinazione DH e KEM PQC

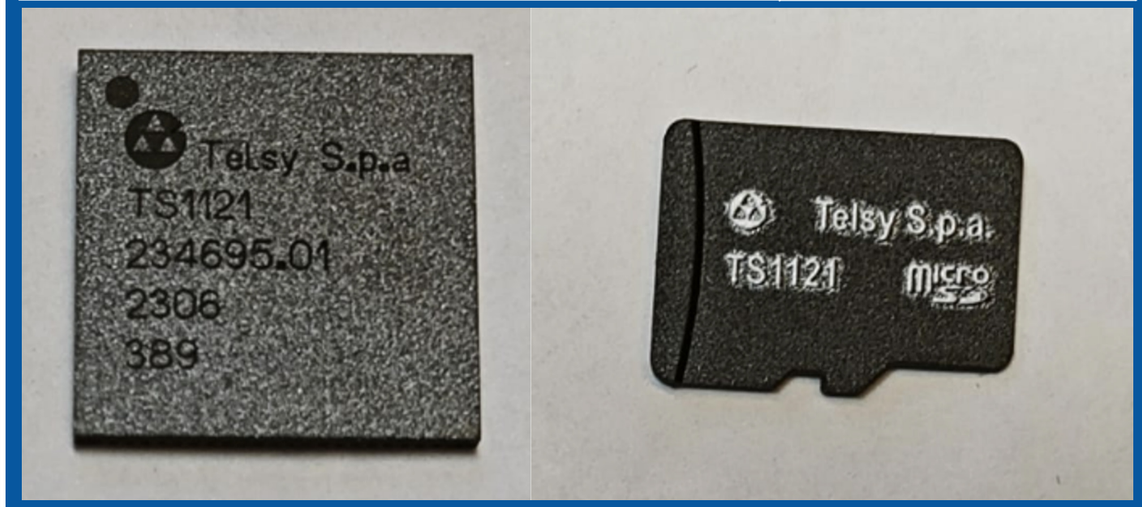


Telsy Secure Microchip

Il progetto “Telsy Secure Microchip” nasce nel 2020 allo scopo di realizzare un microcontrollore italiano per applicazioni di sicurezza.
L’obiettivo principale è la realizzazione di un dispositivo che agisca da Root of Trust tecnologica italiana per garantire la sicurezza informatica di sistemi complessi la cui supply chain è necessariamente eterogenea e globale.

Telsy Secure Microchip è una micro-piattaforma programmabile e sicura by design (secure element crittografico) che permette la realizzazione di soluzioni di sicurezza alla base di diverse applicazioni e servizi tecnologici. Esso garantisce la sicurezza logica e fisica delle operazioni crittografiche alla base delle architetture di sicurezza di un qualsiasi sistema che tratta informazioni sensibili.
Recentemente il Secure Microchip è stato selezionato tra le migliori innovazioni tecnologiche nel mondo delle telecomunicazioni da GSMA, l’associazione mondiale degli operatori TLC, certificando la grande portata innovativa e capacità tecnologica dimostrata dal Gruppo TIM.
Il Telsy Secure Microchip è adatto all’innalzamento delle misure di sicurezza in termini di confidenzialità, integrità e autenticazione, sia per quanto attiene il dominio cyber sia per quello relativo alla sicurezza fisica. L’utilizzo di algoritmi PQC all’interno di questo secure element garantisce inoltre tali proprietà anche nei confronti di avversari quantistici.

Figura A: Telsy Secure Microchip



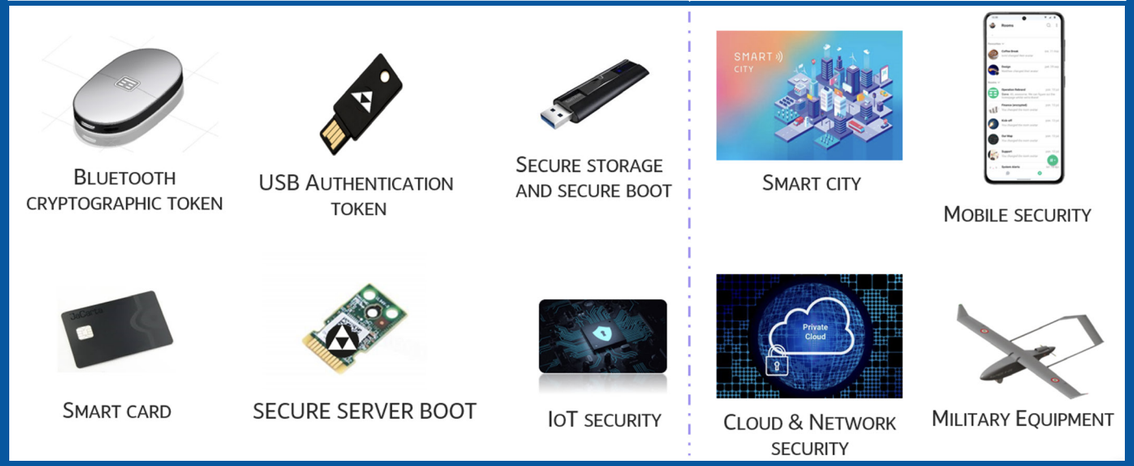
Infatti, queste soluzioni sono trasversali alla tecnologia che le ospitano, potendo essere applicate in fase di design del prodotto o post-produzione mediante un’applicazione “plug in” customizzata in relazione alla funzione di sicurezza richiesta.

Di seguito alcuni ambiti di applicazione distinti per tipologie di tecnologie:
- Information Technology – Cloud & Network Security;
- Operational Technology - Infrastrutture critiche, SCADA;
- Internet of Things - IoT (smart city, military wearable device);
- mezzi militari e sistemi d’arma (sistemi d’arma digitalizzati, droni).

Caratteristiche tecniche:
- completamente progettato in Italia e prodotto in Europa;
- elemento di sicurezza hardware che garantisce la compartimentazione dei dati sensibili rispetto all’applicazione;
- forti meccanismi fisici e logici di protezione delle chiavi applicative;
- anti-tampering e sensori per l’identificazione di attacchi fisici sul dispositivo;
- progettato con forti contromisure rispetto ai Side Channel Attacks;
- supporto di primitive crittografiche, incluse quelle Post Quantum
  - CRYSTALS-KYBER e CRYSTALS-DILITHIUM;
- ciclo di vita crittografico con forti meccanismi di ownership e Secure Boot.

davide.bellizia@telsy.it
riccardo.parisi@telsy.it
giuseppe.valente@telsy.it

Figura B: Telsy Secure Microchip Use Cases



Riferimenti

1. Feynman, R.P.: Simulating physics with computers. Int J Theor Phys. 21, 467–488 (1982). https://doi.org/10.1007/BF02650179
2. GSM Association: Post Quantum Telco Network Impact Assessment. GSM Association (2023)
3. Agence Nationale de la Sécurité des Système d'Information (ANSSI): ANSSI views on the Post-Quantum Cryptography transition (2023 follow up). ANSSI (2023)
4. Bundesamt für Sicherheit in der Informationstechnik (BSI): Cryptographic Mechanisms: Recommendations and Key Lengths. BSI (2024)
5. NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Sy, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FPress-Releases-Statements%2FPress-Release-View%2FArticle%2F3148990%2Fnsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se%2F
6. Regev, O.: On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. JACM. 56, 84–93 (2005)
7. McEliece, R.J.: A Public-Key Cryptosystem based on Algebraic Coding Theory. DSN Progress Report. 44, 114–116 (1978)
8. Ajtai, M.: Generating hard instances of lattice problems. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. pp. 99–108 (1996)
9. Schwabe, P., Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Seiler, G., Stehlé, D., Ding, J.: CRYSTALS-KYBER. National Institute of Standards and Technology (2022)
10. Lyubashevsky, V., Ducas, L., Kiltz, E., Lepoint, T., Schwabe, P. r, Seiler, G., Stehlé, D., Bai, S.: CRYSTALS-DILITHIUM. National Institute of Standards and Technology (2022)
11. Prest, T., Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: FALCON. National Institute of Standards and Technology (2022)
12. Hülsing, A., Bernstein, D.J., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S.-L., Kampanakis, P., Kölbl, S., Lange, T., Lauridsen, M.M., Mendel, F., Niederhagen, R., Rechberger, C., Rijneveld, J., Schwabe, P., Aumasson, J.-P., Westerbaan, B., Beullens, W.: SPHINCS+. National Institute of Standards and Technology (2022)
13. Albrecht, M.R., Bernstein, D.J., Chou, T., Cid, C., Gilcher, J., Lange, T., Maram, V., von Maurich, I., Misoczki, R., Niederhagen, R., Paterson, K.G., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Tjhai, C.J., Tomlinson, M., Wang, W.: Classic McEliece. National Institute of Standards and Technology (2022)
14. Rescorla, E.: The transport layer security (TLS) protocol version 1.3. RFC Editor (2018)
15. Langley, A., Hamburg, M., Turner, S.: Elliptic Curves for Security. RFC Editor (2016)
16. Experimenting with Post-Quantum Cryptography, https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html
17. The TLS Post-Quantum Experiment, https://blog.cloudflare.com/the-tls-post-quantum-experiment
18. Computer Security Division, I.T.L.: Call for Proposals - Post-Quantum Cryptography: Digital Signature Schemes | CSRC | CSRC, https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals

Acronimi

ANSSI	Agence Nationale de la Sécurité des Système d'Information (National Cybersecurity Agency of France)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office of Information Security)
CNSA	Commercial National Security Algorithm Suite
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman
KEM	Key Encapsulation Mechanism
LWE	Learning With Errors
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PQC	Post Quantum Cryptography
QC	Quantum Computer
SSH	Secure Shell
TLS	Transport Layer Security
VPN	Virtual Private Network

Autori

Veronica Cristiano *veronica.cristiano@telsy.it*

Crittografa in Telsy. Ha conseguito la laurea triennale in Matematica presso l'Università di Pisa e la laurea magistrale in Matematica con specializzazione in Crittografia presso l'Università di Trento con una tesi sulla gestione delle chiavi crittografiche. Dal 2021 fa parte del gruppo di Ricerca in Crittografia di Telsy, con cui si occupa di Post Quantum Cryptography e Homomorphic Encryption. ■

Marco Rinaudo *marco.rinaudo@telsy.it*

Laureato triennale in Matematica presso l'Università degli Studi di Torino e laureato magistrale con specializzazione in Crittografia presso l'Università di Trento con una tesi sulla cifratura omomorfa. Da gennaio 2023 è parte del Gruppo di Ricerca in Crittografia di Telsy, con cui partecipa a progetti finanziati sul tema della Post Quantum Cryptography. ■

Edoardo Signorini *edoardo.signorini@telsy.it*

Crittografo in Telsy, dove dal 2020 fa parte del Gruppo di Ricerca in Crittografia. Ha conseguito la Laurea Magistrale in Matematica presso l'Università di Trento nel 2020. Attualmente svolge un Dottorato di ricerca industriale in Matematica Pura e Applicata presso il Politecnico di Torino ed è parte del gruppo di ricerca di Crittografia e Teoria dei Numeri del Politecnico. La sua attività di ricerca si concentra sull'aggregazione l'ottimizzazione di firme digitali Post-Quantum e sull'analisi e lo sviluppo di protocolli crittografici. ■

Francesco Stocco *francesco.stocco@telsy.it*

Membro del Gruppo di Ricerca in Crittografia di Telsy. Nel 2020 ha conseguito la laurea magistrale in Matematica seguendo il programma di studi "Algebra Geometry And Number Theory" (ALGANT) presso le università di Padova e Bordeaux. Nello stesso anno è entrato in Telsy come ricercatore in crittoanalisi quantistica. Le sue attività attuali riguardano le tecniche crittografiche moderne, incluse Post-Quantum Cryptography e aspetti classici della Quantum Key Distribution. ■


TIM