3.1. IL *CYBER RISK* IN UN PANORAMA DELLE MINACCE IN CONTINUA EVOLUZIONE

In passato, la gestione del rischio informatico nel settore aziendale ha spesso adottato un approccio basato sull'eventualità di subire incidenti di sicurezza. Ciò ha relegato il concetto di *cyber risk* a una prospettiva puramente ipotetica, infondendo talvolta un falso senso di sicurezza e compromettendo l'incisività delle contromisure adottate. Nel contesto contemporaneo in cui tecnologia, società ed economia sono profondamente interconnessi, il *cyber risk* ha superato l'ambito della mera ipotesi, transitando dalla dimensione della possibilità a quella della pervasività e influenzando inevitabilmente ogni aspetto delle operazioni aziendali.

Questa realtà di rischio pervasivo è determinata da due principali fattori: da un lato, la rapida evoluzione del panorama delle minacce informatiche (*cyber threat landscape*), ovvero il quadro generale delle minacce potenziali e reali che interessano individui o gruppi, specifici settori o aree geografiche; dall'altro, le crescenti difficoltà che le aziende devono affrontare nel tentativo di mantenere processi e sistemi di sicurezza al passo con tale evoluzione.

A contribuire ai cambiamenti del *cyber threat landscape* sono, oltre all'alternarsi di **diversi tipi di minaccia** e alla loro **crescente sofisticazione**, anche l'altrettanto **rapido sviluppo tecnologico**, che ha visto in pochi anni l'emergere di nuove tecnologie come la Generative AI o la *blockchain*, e in generale la sempre più inevitabile interdipendenza tra tecnologia, società e impresa. Questi elementi aumentano l'entità e gli impatti del rischio informatico sulle aziende e sui singoli utenti. Come mostrano i dati relativi all'Italia nel 2023, nella prima metà dell'anno si è verificato il più alto numero di attacchi *malware* in Europa, per un totale di 174.608.112 rilevamenti di *malware* nel periodo di riferimento[1]. Solo l'anno precedente, l'Italia era il quarto Paese europeo per numero di attacchi informatici subiti, rivelando una tendenza in preoccupante crescita[2]. Tra le principali minacce, il *ransomware* è rimasto preponderante nel corso di tutto il 2023, con una crescita del 34,6% nel secondo trimestre dell'anno rispetto al primo. In particolare, le PMI sono bersaglio dell'80% degli attacchi *ransomware* rilevati e riscontrano grandi difficoltà ad applicare i protocolli di sicurezza adeguati e le più efficaci strategie preventive: il 77% delle aziende colpite ha meno di 50 dipendenti e il 91% è costituito da aziende con meno di 250 milioni di dollari di fatturato. I settori economici e produttivi più colpiti dal *ransomware* in Italia durante l'anno passato sono stati i servizi (54%), il manifatturiero (11%) e la sanità (9%)[3]. Nel 2024, la situazione non sembra accennare ad un miglioramento. Secondo i dati più recenti, si è verificato un **aumento del 30% degli attacchi su scala globale** nel secondo trimestre dell'anno rispetto allo stesso periodo di osservazione del 2023 – con picchi del 35% per l'area europea – anche a causa della trasformazione digitale in atto e dell'adozione dell'Intel-

[1] *Trend* Micro, *Stepping ahead of risk – Report Trend Micro sulle minacce di cybersecurity del primo semestre 2023*, 12 settembre 2023.
[2] IBM Security, *X-Force Threat Intelligence Index 2023*, 2023.
[3] Swascan, *Report Threatland Q2 – Trend e scenari del Cybercrime*, 2023.

ligenza Artificiale da parte di attaccanti che, grazie ad essa, sono in grado di perpetrare attacchi sempre più sofisticati[4].
In aggiunta, nei recenti conflitti in Ucraina e Medio Oriente, il cyberspazio è emerso come nuovo fronte di combattimento e l'***hacktivismo***, una minaccia in grado di sfruttare in modo efficace le risorse digitali per condurre operazioni di sabotaggio e propaganda, ha assunto una nuova rilevanza come attore di primo piano negli scenari geopolitici internazionali. I conflitti in corso sono anche il teatro di scontri tra attori sponsorizzati dai governi, dotati di capacità tecniche avanzate, che conducono regolarmente **campagne di disinformazione, spionaggio e sabotaggio di obiettivi sensibili**. Ciò rafforza la portata e gli effetti dei conflitti, con forti interconnessioni tra impatti virtuali e reali.
Inoltre, se da un lato continuano ad essere utilizzate **le più svariate forme di *malware* e le diverse tecniche di ingegneria sociale**, dall'altro si affacciano all'orizzonte e si perfezionano minacce nuove o emergenti, che spesso includono l'Intelligenza Artificiale nel proprio arsenale e che costituiscono un rischio anche per tecnologie sempre più diffuse ma generalmente meno sicure, come l'*Internet of Things* (IoT). Queste minacce si preparano a svolgere un ruolo determinante in un panorama globale in costante mutamento e rendono quanto mai urgente l'adozione di misure che gestiscano e contrastino efficacemente il *cyber risk*.
Le evoluzioni del *cyber threat landscape* non sono però la sola preoccupazione delle aziende che si trovano ad operare nel contesto contemporaneo. Altre sfide critiche sono costituite dalla crescente difficoltà nel mantenere aggiornati i sistemi di sicurezza, dalla cronica **carenza di personale esperto** e dall'imperativo che impone di adeguarsi a normative stringenti in tema di protezione dei dati. Questi fattori, se combinati all'evoluzione costante delle tecnologie e alla cruciale necessità di proteggere i dati aziendali e la proprietà intellettuale, rendono la gestione della sicurezza informatica un compito estremamente complesso e multidimensionale.
Per molte organizzazioni, mantenere i sistemi informatici aggiornati costituisce una vera e propria sfida nella sfida più ampia della sicurezza. L'evoluzione continua delle tecnologie e la necessità di applicare con frequenza aggiornamenti e patch rappresentano un fattore di complessità per le aziende, che si ritrovano a gestire una vasta gamma di *software* e dispositivi con il rischio che essi rimangano vulnerabili ad attacchi, compromettendo la sicurezza dei dati e delle infrastrutture. Si tratta di un compito difficile, poiché l'**aggiornamento dei sistemi**, per quanto urgente e imprescindibile, richiede un dispendio significativo di tempo, personale e costi, che finisce per ridurre nel complesso l'efficienza delle operazioni aziendali. Nel processo di aggiornamento, inoltre, le aziende devono tenere in considerazione la necessità di preservare la compatibilità tra le diverse versioni *software* e devono eseguire test di funzionamento approfonditi prima di implementare aggiornamenti critici che potrebbero compromettere il funzionamento dei sistemi. Non va tralasciata anche la disponibilità sul mercato di un numero crescente di

[4] Check Point Research, *Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks*, blog.checkpoint.com, 16 luglio 2024.

software e soluzioni specializzate per le diverse funzioni e operazioni della sicurezza informatica, che pur offrendo un supporto prezioso, ampliano inevitabilmente la confusione e l'incertezza delle aziende quando queste si trovano a dover scegliere le opzioni più adatte alle proprie esigenze, ed aumentano gli sforzi richiesti per la loro gestione.
L'insufficiente disponibilità di personale esperto in *cybersecurity* è ormai una costante degli ultimi anni e rappresenta un ulteriore problema critico, poiché il crescente rischio informatico a cui le aziende sono esposte e l'incremento del numero di attacchi ha aumentato la domanda di professionisti qualificati, senza che l'offerta di specialisti e nuovi laureati riesca a chiudere il divario. Nel 2023 si stimava che, solo in Europa, mancassero almeno 350.000 esperti (i posti vacanti a livello globale ammontavano a più di 3,4 milioni)[5], confermando una tendenza che vede le posizioni aperte superare costantemente il numero di candidati disponibili. Questo *gap* non solo mette a rischio la sicurezza delle infrastrutture critiche, ma rallenta anche l'innovazione tecnologica e la capacità delle organizzazioni di rispondere in maniera efficace alle minacce emergenti.
Infine, è diventato imperativo per le organizzazioni adeguarsi alle normative in materia di sicurezza informatica e protezione dei dati, con l'introduzione del Regolamento Generale sulla Protezione dei Dati (GDPR) in Europa e del *California Consumer Privacy Act* (CCPA) negli Stati Uniti, che obbligano le aziende a conformarsi e garantire *standard* elevati per le proprie pratiche di gestione dei dati. Al fine di garantire l'applicazione delle norme stringenti con cui **i dati personali devono essere raccolti, conservati e gestiti** ed evitare l'applicazione di pesanti **sanzioni in caso di violazione**, è spesso necessario compiere investimenti significativi in nuove tecnologie, piani di formazione del personale e consulenze legali, mantenendosi in un complesso equilibrio tra il necessario adeguamento a normative in continua evoluzione e la volontà di **proteggere la reputazione aziendale e la fiducia degli utenti.**
Monitorare l'evoluzione del panorama delle minacce informatiche è dunque un compito complesso. Le aziende, spesso impegnate in una corsa estenuante all'adozione dell'ultimo *software* di cybersicurezza avanzato, si trovano ad affrontare sfide come la carenza di personale specializzato, la gestione delle vulnerabilità di sicurezza e la necessità di rispettare le normative legali in continua evoluzione e non possono quindi dedicare le risorse necessarie a mantenere una visione completa e proattiva delle minacce che le circondano. Ciò spesso le porta a perdere di vista le minacce concrete che potrebbero avere un maggiore impatto sul loro *business*. Ciò è tanto più rischioso poiché affrontare la sfida della sicurezza informatica non significa agire alla cieca o reagire indiscriminatamente a ogni possibile rischio, ma piuttosto sviluppare una chiara comprensione di chi siano i potenziali avversari, quali siano le loro tattiche e strategie, e quali minacce rappresentino un pericolo reale per l'organizzazione. Solo con una visione strategica e mirata è possibile concentrare le risorse di difesa in modo efficace, proteggendo così ciò che conta davvero. Il presente capitolo ha lo scopo di fornire una panoramica dei principali rischi e minacce a livello globale, offrendo alcune informazioni essenziali per comprendere il complesso scenario delle minacce informatiche.

[5] ISC2, *Cybersecurity Workforce Study 2023*, 2023.

3.2. ATTORI MALEVOLI E I LORO OBIETTIVI

Il primo passo per orientarsi nella complessità del panorama delle minacce informatiche è riconoscere che non tutte le minacce perseguono gli stessi scopi o obiettivi. Gli attori malevoli si distinguono per le loro motivazioni, risorse e competenze, spaziando da coloro che mirano al guadagno economico, attraverso il furto di dati, a gruppi con finalità politiche o strategiche, come hacktivisti o attori sponsorizzati da Stati-nazione.
Con attori malevoli (*threat actor*) ci si riferisce ad entità rappresentate da un singolo individuo o da un gruppo che perpetrano azioni dannose nel contesto informatico contro altri soggetti e organizzazioni. Essi possiedono capacità, risorse e *background* differenti, e differenti sono anche le metodologie di attacco impiegate per i diversi scopi. Generalmente, essi si classificano in:

- cybercriminali: individui o gruppi che perseguono principalmente scopi finanziari, di sabotaggio o personali. Questi avversari costituiscono una categoria estremamente variegata, che comprende individui con diversi livelli di competenze e conoscenze tecniche. La sempre più facile reperibilità di strumenti in rete consente infatti anche a criminali privi di capacità avanzate di perpetrare attacchi e truffe *on line*, con potenziali danni anche significativi per i loro bersagli. Anche i metodi di attacco impiegati possono variare, spaziando dall'uso di *malware* sofisticati, al phishing, al *ransomware*. Gli scopi, infine, sono molteplici e possono comprendere la rivendita di dati e credenziali, la vendita di accessi a reti e sistemi ad altri criminali, l'estorsione di denaro alle vittime;
- attori *state-sponsored* e APT (*Advanced Persistent Threat*): avversari dotati di un livello di sofisticazione notevole, in grado di mantenere l'accesso alle reti delle vittime per lungo tempo senza essere individuati. Spesso, questi gruppi sono organizzati e finanziati da entità statali e ne perseguono gli scopi. Tra le attività principali vi sono il *cyber*-spionaggio e la raccolta di informazioni strategiche, l'interferenza o il sabotaggio delle infrastrutture critiche, la diffusione di propaganda e la manipolazione delle dinamiche geopolitiche per ottenere vantaggi politici, economici o militari;
- hacktivisti: individui o gruppi che sfruttano le proprie abilità informatiche per perpetrare cause ideologiche, sociali, politiche o religiose. Le loro azioni sono principalmente mirate ad ottenere visibilità o alla ritorsione e si configurano frequentemente come attacchi DDoS (*Distributed Denial of Service*), *defacement* di siti *web* e *leak* di informazioni sensibili.

I prossimi paragrafi illustrano le peculiari caratteristiche di ciascuna tipologia di avversario e, presentando alcuni casi di studio reali, cercano di mostrare la rilevanza nel panorama globale delle minacce, le potenzialità di attacco, i rischi derivanti e i possibili impatti sulle organizzazioni che ne restano vittime.

3.2.1. Il *ransomware* come modello di *business cyber*-criminale

Nel panorama del *cybercrime*, il *ransomware* rappresenta una delle minacce più diffuse e in rapida evoluzione, caratterizzata da una costante crescita sia nel numero di incidenti

rilevati che negli impatti economici e sociali che è in grado di causare. Lo scopo principale del *ransomware* è la cifratura dei *file* presenti sui sistemi della vittima e la conseguente richiesta di un riscatto in cambio della chiave di decrittazione. Questa caratteristica strategia di attacco rende il *ransomware* responsabile di **perdite economiche** stimate nell'ordine delle centinaia di milioni di dollari ogni anno.
Noti sin dagli anni '80, gli attacchi di estorsione basata sulla cifratura o il furto di dati hanno subito un'evoluzione anche grazie al rapido svilupparsi e diffondersi di nuove risorse che ne facilitano le operazioni. Ad esempio, l'avvento del **Bitcoin** ha rivoluzionato il *ransomware* favorendo il trasferimento di denaro senza intermediari e introducendo l'anonimizzazione delle transazioni, che rende quasi impossibile per gli investigatori risalire all'identità degli attaccanti. Anche le cifre estorte alle vittime sono cresciute esponenzialmente nel tempo: se nei primi anni Duemila i *ransomware* richiedevano poche centinaia di dollari in riscatto per ottenere la **chiave di decrittazione**[6], oggi le cifre si aggirano sulle decine di milioni di dollari. Risale ai primi mesi del 2024, ad esempio, la più alta somma di denaro mai pagata per un riscatto che sia stata resa pubblica, la quale ammonta alla cifra record di 75 milioni di dollari. Il pagamento record è stato versato al gruppo Dark Angels da una società inclusa nella lista Fortune 50, la cui identità non è stata rivelata[7].
Il *ransomware* si è gradualmente evoluto assumendo nel tempo caratteristiche che lo rendono un vero e proprio *business* del *cybercrime*:

a) gli obiettivi sono selezionati preferendo sempre più spesso le aziende agli utenti privati e puntando ad **imprese di grandi dimensioni e dai fatturati più elevati**, potenzialmente più inclini a pagare grosse somme di denaro in riscatto. Tale strategia è nota come "*big game hunting*";
b) vi è un **alto livello di specializzazione** nello sviluppo di *malware* sofisticati e di varie forme di supporto tecnico offerto alle vittime durante la fase di trattativa;
c) il modello di *business* è sempre più simile a quello delle aziende tradizionali, basato sull'offerta di un servizio specializzato (*Ransomware-as-a-Service*) che comprende la fornitura del *software* malevolo e dell'infrastruttura necessaria ad altri criminali informatici, i quali operano come affiliati e condividono una percentuale dei ricavi con gli amministratori;
d) le notevoli capacità di adattamento ed evoluzione rispetto alle nuove misure di sicurezza si manifestano nella continua **ricerca di nuovi metodi di distribuzione del *ransomware* e nuove vulnerabilità da sfruttare**, ad esempio tramite l'acquisto di *exploit* per vulnerabilità *zero-day* – un tipo di vulnerabilità informatica che viene sfruttata dagli attaccanti prima che il produttore del *software* sia a conoscenza dell'esistenza della vulnerabilità stessa, senza quindi la possibilità di rilasciare patch in via preventiva – venduti ad un prezzo generalmente molto elevato negli ambienti underground.

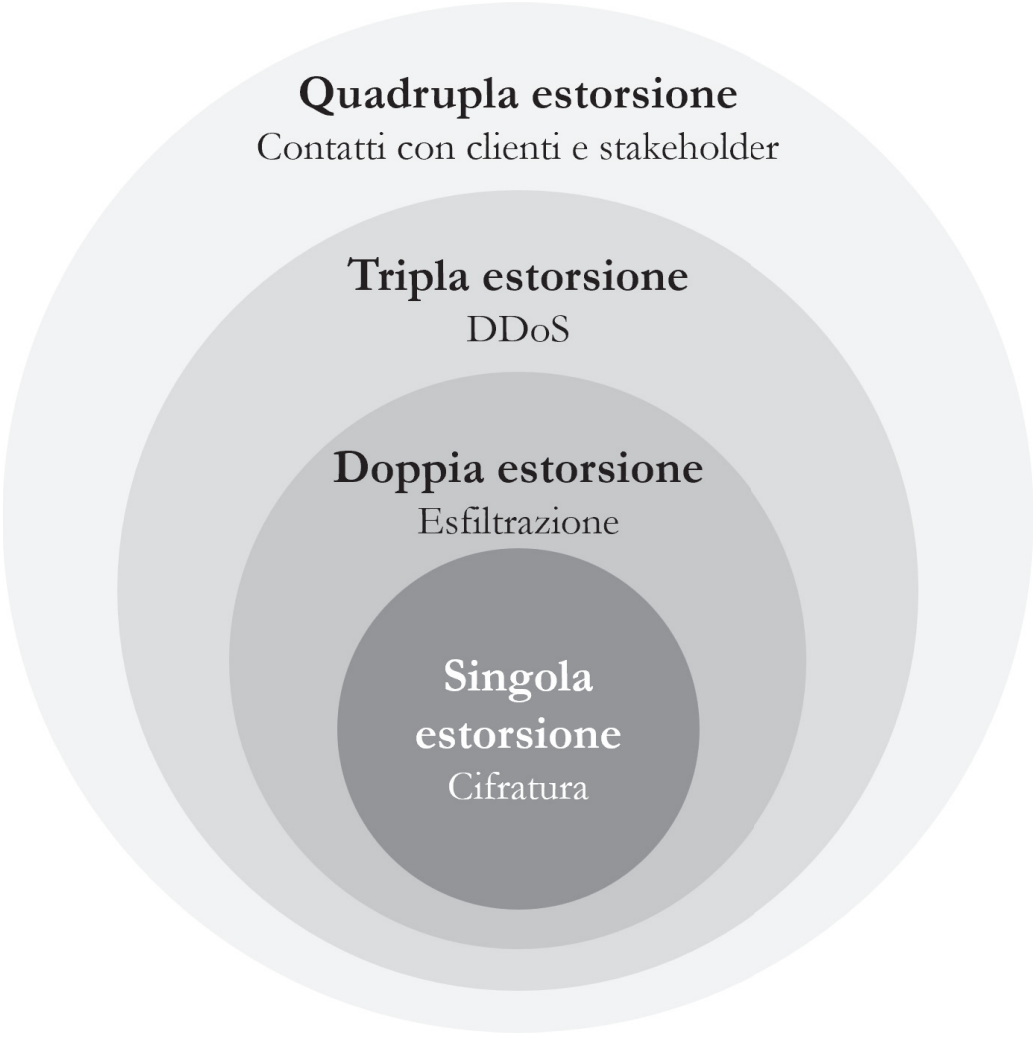
---

[6] R. Richardson and M. North, *Ransomware: Evolution, Mitigation and Prevention*, International *Management* Review Vol. 13 No. 1 2017, pag. 11-13.
[7] Zscaler ThreatLabz, *2024 Ransomware Report*, luglio 2024.

Un'ulteriore evoluzione dell'universo *ransomware* si è verificata nei metodi di estorsione impiegati. Negli anni è infatti avvenuto un cambiamento culturale nel modo in cui le aziende rispondono agli attacchi *ransomware*, che ha determinato una mentalità più proattiva e orientata alla resilienza e una crescente consapevolezza delle implicazioni etiche e sociali derivanti dal pagamento dei riscatti. In risposta a questo nuovo scenario, il *business* del *ransomware* ha saputo adattarsi ed evolversi, adottando la tecnica della multi-estorsione, ovvero l'utilizzo di molteplici livelli di estorsione per convincere le vittime a pagare il riscatto:

- **singola estorsione**: il *ransomware* crittografa i *file* presenti, rendendo i dati indisponibili e causando interruzioni delle operazioni aziendali e del funzionamento dei servizi. Viene richiesto un riscatto in cambio della chiave di decrittazione;
- **doppia estorsione**: il *ransomware* esfiltra i dati dai sistemi prima di eseguirne la crittografia. Gli attaccanti minacciano quindi la pubblicazione di tali dati *on line*, spesso avvalendosi di blog e siti *web* dedicati ospitati sulla rete Tor (*Data Leak Sites*);
- **tripla estorsione**: al fine di esercitare ulteriore pressione sulla vittima, gli attaccanti possono eseguire attacchi DDoS contro l'infrastruttura IT aziendale, rendendo irraggiungibili i servizi fino al pagamento del riscatto;
- **quadrupla estorsione**: per massimizzare i guadagni derivanti dall'attacco, gli avversari possono cercare di estorcere denaro anche a clienti e *stakeholder* della vittima stessa, che rischierebbero di subire ripercussioni derivanti da un'eventuale divulgazione dei dati. Talvolta, le *ransomware* gang minacciano anche di intraprendere azioni legali nei confronti delle loro vittime.

Tavola 3.1. – **Le quattro fasi dell'estorsione *ransomware***



Fonte dell'immagine: Palo Alto Networks, *What is Multi-Extortion Ransomware?*

I gruppi criminali coinvolti nelle attività *ransomware* mostrano spesso notevoli capacità di **resilienza**. Gli avversari solitamente pianificano risorse e contromisure alternative in caso di intervento delle forze dell'ordine, come siti *web* replicati su server di riserva (*mirror*), che consentono di tornare attivi in un tempo relativamente breve a seguito di un sequestro. In risposta alle azioni di contrasto, i gruppi *ransomware* tendono a raffor-

zare le misure di sicurezza adottate nelle proprie operazioni (la c.d. *OPSEC*), allo scopo di renderle più difficilmente individuabili. Inoltre, per ritorsione gli avversari possono intensificare i propri attacchi verso **obiettivi specifici** o **modificare le proprie regole di condotta**, eliminando alcune restrizioni e autorizzando gli affiliati a colpire indiscriminatamente qualsiasi entità, compresi obiettivi sensibili come ospedali e centrali nucleari, in precedenza spesso esclusi dagli attacchi.
Questo insieme di fattori rende il *ransomware* una delle minacce più sofisticate e complesse del panorama del *cybercrime*, in particolar modo nella sfera aziendale. La perdita di dati critici può comportare l'interruzione delle attività, con conseguenti **costi di ripristino elevati**, e la loro divulgazione può costituire una fonte di danno reputazionale, oltre a comportare sanzioni e conseguenze legali per l'organizzazione in caso di comprovata insufficienza delle misure di sicurezza adottate e di avvenuta violazione della *privacy*.

3.2.1.1. LockBit 3.0: l'*industry-leader del Ransomware-as-a-Service* (RaaS)

Il processo di trasformazione del *ransomware* verso un modello di *business* altamente organizzato e il suo impatto significativo sulle organizzazioni a livello globale sono caratteristiche ben evidenziate dalla parabola di LockBit, un'operazione *Ransomware-as-a-Service* che è stata a lungo considerata *leader* di questo settore.
Inizialmente noto come ABCD, il gruppo LockBit[8] ha avviato la propria attività all'interno del cartello *ransomware* Maze, staccandosene definitivamente nel 2019 e iniziando ad operare autonomamente. Dal febbraio 2020, il gruppo ha adottato un modello di *business* basato su affiliati, atto a massimizzare i profitti: LockBit fornisce il codice sorgente del *ransomware* e l'infrastruttura necessaria, mentre gli affiliati eseguono materialmente gli attacchi e ricevono una **quota dei riscatti**. Il modello prevede anche un *Data Leak Site* dedicato alla pubblicazione dei dati esfiltrati, l'approvvigionamento dell'accesso iniziale alle reti degli obiettivi acquistandolo dai c.d. *Initial Access Broker* (IAB) specializzati, la pubblicizzazione dell'operazione RaaS in diversi forum di *hacking* per il reclutamento di nuovi membri e l'ingaggio di ricercatori per un programma di *Bug Bounty* dedicato. Nel 2021, il gruppo adotta il nome di LockBit 2.0 e nel giugno 2022 diviene poi LockBit 3.0. A seguito della cessazione delle attività della nota *ransomware gang* Conti, LockBit diviene il gruppo *ransomware* più rilevante nel *cyber threat landscape*, rivendicando globalmente più di 2000 vittime sul proprio *Data Leak Site* e richiedendo estorsioni che ammontano complessivamente a centinaia di milioni di dollari[9].
In termini di vittimologia, LockBit colpisce in modo indiscriminato molteplici settori, con una preponderanza di vittime nel manifatturiero, nei servizi professionali e nell'assistenza sanitaria. L'area geografica maggiormente colpita risulta essere il Nord America, con circa metà delle vittime totali localizzate negli Stati Uniti. Seguono per numero di vittime Francia, Regno Unito, Canada e Italia. Il *ransomware* non colpisce i Paesi della

[8] SocRadar, *Dark Web Profile: LockBit 3.0 Ransomware*, socradar.io, 27 aprile 2023.
[9] Dati disponibili al mese di febbraio 2024.

Comunità degli Stati Indipendenti e i Paesi alleati della Federazione Russa, escludendo dai propri obiettivi i dispositivi che utilizzano specifiche lingue come lingua di sistema. LockBit 3.0, anche nota come LockBit Black, è l'ultima versione del *ransomware* e riflette perfettamente il modello di *business* adottato dai suoi operatori, in particolare nella possibilità di personalizzare le opzioni di compilazione ed esecuzione per configurarne il comportamento a discrezione del singolo affiliato. Gli sforzi di aggiornamento del codice del *ransomware* sono continui, ad esempio integrando strumenti utilizzati da altre famiglie di *ransomware*, come BlackCat, BlackMatter e Conti. Inoltre, il gruppo ha recentemente sviluppato una nuova variante atta a colpire una più ampia gamma di sistemi operativi, inclusi Linux, FreeBSD e macOS[10].
Tuttavia, negli ultimi anni la parabola ascendente di LockBit sembra aver subito una battuta di arresto. Nel corso del 2023 sono emersi elementi che suggerirebbero problemi operativi all'interno del gruppo, facendo ipotizzare una sua fase di declino[11]. Tra questi figurano incidenti di sicurezza interni dovuti alla struttura distribuita e semi-anonima del gruppo, che hanno portato a **fughe di informazioni**. Ad esempio, nel settembre 2022 è trapelato il *builder* di LockBit, ovvero lo strumento tramite il quale gli affiliati possono generare nuove versioni del *ransomware* con configurazioni personalizzate; esso è stato poi riutilizzato da altri cybercriminali e ciò ha determinato una maggior concorrenza nel mercato del *ransomware*. Questi leak hanno danneggiato anche le rivendicazioni degli attacchi, rendendo difficile dimostrarne la matrice, e hanno compromesso la fiducia nei confronti degli affiliati. La stabilità dell'infrastruttura del gruppo è stata messa in dubbio anche da problemi tecnici ricorrenti, come l'instabilità del *Data Leak Site* utilizzato per la pubblicazione dei dati delle vittime, spesso risultato irraggiungibile. Inoltre, l'introduzione di regole più restrittive e la percezione di una riduzione delle competenze all'interno del gruppo hanno determinato una generale perdita di fiducia da parte dei nuovi affiliati. Infine, alcuni scontri legati ad accordi sulle percentuali dei riscatti concesse agli affiliati sarebbero stati la causa del ban del creatore ed amministratore di LockBit, noto negli ambienti underground come "LockBitSupp", dai noti forum XSS ed Exploit, indebolendo la reputazione del gruppo e la sua posizione predominante nel panorama del cybercrime.
Le speculazioni e le indiscrezioni sono culminate, nel mese di febbraio 2024, con l'intervento del Dipartimento di Giustizia degli Stati Uniti che ha sequestrato e smantellato l'infrastruttura informatica del gruppo LockBit e ha incriminato due individui di nazionalità russa per crimini informatici contro vittime statunitensi ed internazionali[12]. L'operazione, denominata "*Operation Cronos*", ha coinvolto l'FBI, la National Crime Agency del Regno Unito e *partner* privati e ha consentito di ottenere il controllo dei server localizzati negli Stati Uniti utilizzati dagli amministratori di LockBit per trasferire i dati sottratti alle vittime, oltre a numerosi altri siti *web* malevoli. Inoltre, le forze dell'ordine hanno ottenuto migliaia di chiavi di decrittazione dei *file* delle vittime, che

[10] Kaspersky, *LockBit expands its reach, now targeting macOS*, kaspersky.com, 22 giugno 2023.
[11] *Trend* Micro, *LockBit Attempts to Stay Afloat With a New Version*, trendmicro.com, 22 febbraio 2024.
[12] Office of Public Affairs, U.S. Department of Justice, *U.S. and U.K. Disrupt LockBit Ransomware Variant*, 20 febbraio 2024.

sono dunque riuscite a recuperare l'accesso ai propri dati. Nel maggio 2024, il Dipartimento di Giustizia è giunto all'identificazione di un cittadino russo come "LockBitSupp", il creatore, sviluppatore ed amministratore del gruppo LockBit, e ne ha annunciato l'incriminazione per **26 capi d'accusa**[13].
Nonostante l'impatto significativo che Operation Cronos ha avuto sul gruppo LockBit, essa non ne avrebbe tuttavia determinato la completa eradicazione. Vi sono infatti diversi elementi[14] che suggeriscono che alcuni affiliati abbiano continuato ad operare a seguito dell'intervento delle forze dell'ordine e che siano tutt'ora in attività. Già pochi giorni dopo il primo annuncio del sequestro dell'infrastruttura IT e del *Data Leak Site*, gli operatori di LockBit hanno lanciato un nuovo sito sulla rete Tor in cui figuravano nuove presunte vittime, tra cui lo stesso FBI. Inoltre, il gruppo starebbe lavorando ad una nuova variante del *ransomware*, che potrebbe costituire la base per una futura versione LockBit 4.0. Attualmente, il sito Tor del gruppo è attivo e viene costantemente aggiornato con nuove vittime. L'operazione *ransomware* sembra dunque sopravvissuta, sebbene con capacità ridotte, e nonostante non sia al momento chiara l'identità e la composizione del gruppo di individui che continua a condurre gli attacchi e a manutenere l'infrastruttura.
La natura decentralizzata che caratterizza questo tipo di avversari rende estremamente complicato il completo smantellamento di un gruppo *ransomware* come LockBit, che continua dunque a costituire una minaccia, sebbene siano elevate le probabilità che perda il suo ruolo dominante nel panorama globale del *ransomware* nel prossimo futuro. La parabola di LockBit dimostra che, nonostante gli intensi sforzi delle forze dell'ordine, è oltremodo complesso e arduo eradicare completamente le operazioni *Ransomware-as-a-Service*, che si presentano spesso stratificate e ramificate, capaci di sopravvivere ai propri stessi creatori. Le organizzazioni hanno dunque la necessità cruciale di mantenere un elevato livello di attenzione e di implementare solide **misure di sicurezza** contro questo tipo di attacchi, che non solo persistono, ma continuano a evolversi, rappresentando un rischio significativo per la sicurezza dei dati e delle infrastrutture aziendali.

3.2.1.2. Scattered Spider e ALPHV: una nuova collaborazione tra avversari finanziariamente motivati

A fronte di una tradizionale tendenza dei gruppi *cyber*-criminali ad operare in modo isolato e competitivo, nel panorama delle minacce si osservano sempre più spesso forme di cooperazione tra *threat actor*. Questi gruppi sembrano infatti tendere sempre più frequentemente alla condivisione di risorse e allo scambio di tecniche e strategie di attacco. Tale cooperazione può assumere diverse forme e talvolta può culminare in vere e proprie *partnership* per il raggiungimento di obiettivi comuni, producendo impatti più significativi. Tale fenomeno aumenta la complessità delle minacce e ne complica la

[13] Office of Public Affairs, U.S. Department of Justice, *U.S. Charges Russian National with Developing and Operating LockBit Ransomware*, 7 maggio 2024.
[14] *Trend* Micro, *LockBit Attempts to Stay Afloat With a New Version*, trendmicro.com, 22 febbraio 2024.

prevenzione e la mitigazione, ostacolando le analisi a causa di una commistione di tecniche e strumenti utilizzati, che spesso impedisce la chiara identificazione di origini, motivazioni e obiettivi di cluster di attività malevola distinti, ma che tendono a sovrapporsi.
Uno dei più recenti esempi di questo fenomeno è emerso nel 2023, quando il *threat group* Scattered Spider ha avviato un rapporto di affiliazione con l'operazione *Ransomware-as-a-Service* di ALPHV/BlackCat. Scattered Spider è un appellativo che identifica un gruppo di cybercriminali finanziariamente motivato e specializzato nell'uso di tecniche di *social engineering*, in particolar modo di *smishing* e *SIM swapping*, per sottrarre credenziali valide ed ottenere l'accesso iniziale alle reti aziendali. Una volta ottenuto l'accesso alla rete della vittima, Scattered Spider concentra le proprie attività nella ricerca di dati sensibili e informazioni di valore, che vengono esfiltrati a scopo di estorsione o di rivendita in vari marketplace della Darknet. Emerso all'inizio del 2022, questo gruppo cybercriminale di lingua inglese ha colpito numerose organizzazioni di alto profilo in diversi settori, incluse organizzazioni dell'IT e delle telecomunicazioni, delle criptovalute e dei videogame.
A partire dal febbraio 2023, Scattered Spider ha modificato il proprio *modus operandi* includendovi la distribuzione di *ransomware* negli ambienti delle vittime per potenziare le proprie capacità di estorsione, scegliendo ALPHV quale *partner* atto allo scopo. Tale collaborazione sarebbe dimostrata dalla compatibilità tra le vittime attribuite a Scattered Spider e gli attacchi rivendicati da ALPHV/BlackCat, dall'utilizzo di medesimi tool e *file* malevoli nella catena di attacco e da un'elevata similitudine delle tattiche, tecniche e procedure impiegate dai due avversari[15]. Nella prima metà del 2024, inoltre, Scattered Spider ha ulteriormente espanso il proprio arsenale includendovi due nuovi payload *ransomware*: RansomHub e Qilin[16]. Ciò rafforza l'impressione che il gruppo sia particolarmente interessato a utilizzare e sfruttare strumenti di *ransomware* avanzati, con un approccio strategico orientato alla diversificazione e all'ottimizzazione dell'efficacia degli attacchi.

3.2.2. Gruppi *state-sponsored* e il *cyber*-spionaggio

Gli avversari *state-sponsored* o *nation-state* sono caratterizzati da livelli elevati di esperienza e sofisticazione nelle tecniche di attacco e negli strumenti impiegati, poiché generalmente godono di **finanziamenti statali, infrastruttura e strumentazione all'avanguardia e accesso a informazioni riservate o all'intelligence di Stato**. Gli avversari *state-sponsored* sono spesso identificati con i gruppi APT (*Advanced Persistent Threat*), ma più correttamente ne costituiscono un sottoinsieme, trattandosi di APT direttamente coinvolti nelle strategie geopolitiche dello Stato. Essi perseguono obiettivi

[15] *Cybersecurity* and Infrastructure Security Agency (CISA), *FBI and CISA Release Advisory on Scattered Spider Group*, cisa.gov, 16 novembre 2023.
[16] Microsoft Threat Intelligence (@MsftSecIntel), "*In the second quarter of 2024, financially motivated threat actor Octo Tempest, our most closely tracked ransomware threat actor, added RansomHub and Qilin to its ransomware payloads in campaigns.*", x.com, 15 luglio 2024.

politici, strategici o di sicurezza nazionale e conducono attività di *cyber*-spionaggio per l'acquisizione di informazioni sensibili, di sabotaggio, distruzione o destabilizzazione di infrastrutture e obiettivi critici di altre nazioni o organizzazioni, di propaganda al fine di influenzare le dinamiche geopolitiche e ottenere **vantaggi competitivi**. A questo scopo, gli avversari *state-sponsored* utilizzano tecniche avanzate per effettuare attacchi mirati, come ad esempio l'uso di *exploit zero-day* sviluppati in proprio o acquistati sul *Web*, *malware* creato *ad hoc* e tecniche sofisticate di ingegneria sociale.
La minaccia *state-sponsored* è intrinsecamente connessa al contesto geopolitico, all'evoluzione dei conflitti e alle relazioni tra nazioni, obiettivi politici e strategie nazionali. Di conseguenza, essa può subire cambiamenti di strategia condizionati da variazioni nelle agende politiche nazionali, dalla nascita di tensioni o accordi tra Stati, dalle relazioni diplomatiche e anche dall'evoluzione in campo tecnologico.
I più recenti sviluppi nella sfera degli avversari *state-sponsored* evidenziano come, nel corso del 2023, si sia verificato un cambiamento di rotta nell'attività *nation-state*, che dopo un periodo precedente focalizzato sulla distruzione di obiettivi critici e sul guadagno finanziario tramite *ransomware*, è tornata a concentrarsi principalmente su operazioni strategiche a lungo termine, come la **sottrazione di informazioni, l'intercettazione delle comunicazioni e il tentativo di manipolare l'opinione pubblica**. Gli attori che più spesso impiegavano tattiche distruttive, nel corso del 2023 hanno ridotto la frequenza di tali operazioni e si sono concentrati sul perfezionare le proprie capacità di collezionare informazioni strategiche. Ad esempio, le operazioni di *cyberwarfare* russe in Ucraina sono state incentrate su attacchi distruttivi principalmente nelle prime settimane del conflitto e successivamente sono virate verso lo **spionaggio, sottoforma di campagne di phishing ed esfiltrazione di dati**. Anche Cina, Corea del Nord e Iran hanno intensificato le proprie campagne di spionaggio verso i loro avversari geopolitici. Nel complesso, le attività *state-sponsored* osservate nell'ultimo anno hanno colpito obiettivi in più di 120 Paesi. Di queste, solo una piccola parte è costituita da attacchi distruttivi, mentre percentuali più significative sono rappresentate da intrusioni nelle reti ed esfiltrazione. Tali attività hanno anche registrato una più ampia gamma di obiettivi dal punto di vista geografico, con un'espansione verso i Paesi in via di sviluppo in America Latina e Africa Subsahariana. Gli obiettivi più colpiti restano comunque gli Stati Uniti, i Paesi europei, l'Ucraina e Israele, con una preponderanza di organizzazioni colpite nei settori governativo e della difesa, think tank, ONG e università[17]. Un'ulteriore tendenza in crescita è l'utilizzo sempre più frequente di operazioni di influenza coordinate con operazioni *cyber* al fine di diffondere propaganda e manipolare l'opinione pubblica. Ciò spesso avviene su due binari paralleli, allo scopo di minare le istituzioni democratiche dei Paesi avversari:

- *on line*, mediante operazioni coordinate che utilizzano bot automatizzati e gruppi istituzionalizzati di troll (*troll farm*) per generare e diffondere informazioni false o fuorvianti;

[17] Microsoft Threat Intelligence, *Microsoft Digital Defense Report 2023 (MDDR)*, ottobre 2023.

- offline, mediante l'organizzazione di proteste o provocazioni, l'attività dei media tradizionali e il supporto diretto ad esponenti o gruppi politici[18].

Le operazioni di influenza costituiscono una minaccia in crescita, sfruttata come elemento strategico a supporto di attacchi informatici e militari, che ne amplificano la portata e gli effetti sugli obiettivi.

3.2.2.1. Sandworm e gli attacchi alle infrastrutture critiche ucraine

Nell'ottobre 2022, un incidente di sicurezza distruttivo ha coinvolto un'infrastruttura critica ucraina. Si è trattato di un attacco multi-evento, che ha causato un'interruzione di energia elettrica coincisa con attacchi missilistici di massa ad altri obiettivi critici nel Paese. L'attacco è attribuito al *threat actor* noto come Sandworm, legato alla Military Unit 74455, il Centro principale per le Tecnologie Speciali della Direzione Generale per le Informazioni Militari della Russia (GRU). Si tratta di un avversario sofisticato, attivo dal 2009 con campagne di spionaggio, influenza e attacchi informatici distruttivi, mirati soprattutto contro entità ucraine. L'analisi di questo attacco[19] dimostra che l'avversario possiede elevate capacità tecniche, che lo rendono in grado di colpire efficacemente gli equipaggiamenti industriali dei propri obiettivi, costituiti da tecnologie ICS (*Industrial Control Systems*) e OT (*Operational Technology*). L'attacco in questione ha infatti permesso di scoprire l'impiego, in una prima fase, di una metodologia mai osservata prima per colpire sistemi OT basata su tecniche *Living-off-the-Land* (LotL), le quali consistono nello sfruttamento di risorse e funzionalità legittime già presenti nativamente in sistemi operativi, *software* o servizi di rete per condurre attività malevole, rendendo più difficile il rilevamento attraverso i tradizionali strumenti di sicurezza. In particolare, gli attaccanti avrebbero ottenuto l'accesso a un'istanza di gestione del controllo di supervisione e acquisizione dati (SCADA) di una sottostazione del sistema di distribuzione e trasmissione dell'energia elettrica, mantenendolo per circa 3 mesi. Al momento opportuno, coinciso con la data pianificata per l'esecuzione di un attacco missilistico da parte dell'esercito russo, Sandworm avrebbe sfruttato il sistema di controllo di supervisione MicroSCADA per inviare comandi alle unità terminali remote (RTU) della sottostazione affinché venisse interrotto il flusso di corrente elettrica. Nella seconda fase dell'attacco, l'avversario ha distribuito il *malware* CaddyWiper al fine di causare ulteriori malfunzionamenti e potenzialmente rimuovere le proprie tracce dall'ambiente compromesso.

Questo attacco dimostra il crescente interesse della Russia in investimenti per lo sviluppo di capacità offensive atte a colpite sistemi OT e ne ha studiato l'evoluzione più recente. L'utilizzo di tecniche LotL a livello OT da parte di Sandworm dimostra una crescente maturità dell'arsenale offensivo della Russia, evidenziata dalla capacità di individuare nuovi vettori di attacco alle infrastrutture OT, dallo sviluppo piuttosto rapido

[18] Ibid.

[19] K. Proska, J. Wolfram, J. Wilson, D. Black, K. Lunden, D. Kapellmann Zafra, N. Brubaker, T. Mclellan, C. Sistrunk, *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*, mandiant.com, 9 novembre 2023.

di nuove capacità e dallo sfruttamento di diverse tipologie di infrastruttura per l'esecuzione degli attacchi.
L'episodio ucraino è un esempio di come la sfera informatica sia divenuta cruciale nel contesto geopolitico e industriale odierno e di come il cyberspazio sia diventato un teatro di guerra a tutti gli effetti, estensione dei conflitti geopolitici e militari. Le ripercussioni di tali attacchi, che comprendono devastanti effetti a catena su un intero ecosistema economico e la **compromissione della pubblica sicurezza**, evidenziano la necessità di una preparazione e di una resilienza avanzate. Per le aziende dei settori critici, divenute bersagli allettanti nei conflitti moderni, è imperativo considerare la sicurezza informatica come una **priorità strategica**: a causa della loro rilevanza cruciale per l'intera società, ad esse è richiesto di contribuire alla difesa collettiva contro le minacce emergenti su scala globale. Eventuali gravi interruzioni dei servizi derivanti da attacchi informatici possono infatti portare non solo a perdite economiche significative, sanzioni regolamentari per violazione della *privacy* e danni reputazionali per l'organizzazione stessa, ma anche ad un concreto pericolo di danni fisici a persone e infrastrutture, con conseguenze potenzialmente drammatiche.

3.2.2.2. Le operazioni di influenza sulle elezioni politiche del 2024

Le operazioni di influenza condotte da attori *nation-state* sugli appuntamenti elettorali sono un fenomeno ormai frequentemente dibattuto anche dall'opinione pubblica generalista e rappresentano una minaccia crescente per la stabilità democratica, con particolare rilevanza in contesti globali altamente polarizzati. Il 2024 è un anno significativo per le operazioni di influenza, caratterizzato da numerose elezioni di rilievo a livello globale che coinvolgono miliardi di elettori, e che dunque costituiscono obiettivi sensibili: le elezioni presidenziali in Indonesia (febbraio 2024), le elezioni parlamentari in India (aprile-giugno 2024), le elezioni per il Parlamento europeo (giugno 2024), le elezioni legislative in Francia (giugno-luglio 2024) e le elezioni presidenziali negli Stati Uniti (novembre 2024), che complessivamente chiamano alle urne quasi la metà della popolazione mondiale. Tra queste, le elezioni europee e statunitensi sono tra gli appuntamenti che destano particolare preoccupazione negli analisti occidentali.
Ad esempio, nei mesi di maggio e giugno 2024 è stata identificata una campagna attribuita alla rete di disinformazione russa Pravda, con lo scopo di diffondere false informazioni e orientare l'opinione pubblica alla vigilia delle elezioni per il Parlamento Europeo. La campagna si è basata sulla creazione e distribuzione di contenuti generati mediante la Generative AI e di video *deep fake* in tutti i ventisette Stati membri dell'Unione Europea e in alcuni Paesi extra-UE[20]. Questa campagna ha destato particolare interesse poiché versioni dei siti *web* utilizzati per veicolare **fake news** erano disponibili in tutte le principali lingue dell'Unione, con un potenziale di diffusione molto significativo. Inoltre, è stato osservato che le capacità di traduzione automatica dei contenuti

[20] European Digital Media Observatory (EDMO), *Russian disinformation network "Pravda" tries a new route to influence EU public opinions few days ahead of the vote*, edmo.edu, 6 giugno 2024.

di questa campagna sono notevolmente migliorate rispetto alle precedenti dello stesso tipo.
Nello stesso contesto, nel mese di giugno è stata scoperta la creazione di "Euromore", un mezzo di informazione progettato dal governo russo per sostituire i canali mediatici statali RT e Sputnik, ormai vietati in Europa[21]. Il canale Euromore, nonostante si presenti come una piattaforma europea indipendente, è in realtà finanziato da organizzazioni strettamente legate all'intelligence russa, in particolare Pravfond e Rusfuture. Euromore diffonde narrazioni filorusse e tenta di contrastare i sentimenti antirussi nella popolazione europea, segnando un'evoluzione significativa nelle operazioni di informazione della Federazione Russa, soprattutto in risposta alle sanzioni imposte dall'Europa come conseguenza dell'aggressione all'Ucraina.
Gli analisti monitorano inoltre attentamente le elezioni presidenziali statunitensi ed hanno finora individuato intense attività di influenza da parte di attori russi, iraniani e cinesi a partire dall'inizio dell'anno.
Le operazioni di influenza di matrice russa si sono basate, nella prima metà del 2024, sulla diffusione di una narrativa anti-Ucraina allo scopo di minare il supporto militare e politico degli Stati Uniti a Kiev. Almeno settanta attori legati alla Russia hanno sinora diffuso contenuti ostili all'Ucraina attraverso i social *network* e i media tradizionali. Tra le principali operazioni russe attualmente note, gli analisti annoverano[22]:

- una campagna basata su contenuti video appositamente creati da presunti informatori o giornalisti, diffusi mediante siti *web* gestiti dagli avversari stessi e amplificati poi da espatriati o funzionari russi. I contenuti vengono infine ripubblicati da utenti statunitensi ignari della reale origine delle informazioni;
- una campagna ad opera di attori legati al collettivo militare russo di blogging e creazione di contenuti Rybar, basata sulla diffusione di contenuti legati al tema dell'immigrazione negli Stati Uniti. La campagna è veicolata da molteplici canali Telegram mirati a diffondere contenuti che fanno leva su sentimenti di odio e razzismo per incitare alla violenza e alla mobilitazione;
- un'operazione attiva dal 2022 e denominata "Doppelganger", con lo scopo di minare il sostegno all'Ucraina e la coesione tra le nazioni occidentali. L'operazione prevede la creazione di falsi siti *web* che imitano organi di informazione legittimi e agenzie governative per diffondere narrazioni anti-ucraine e filorusse.

La minaccia cinese alle elezioni americane è supportata da attori legati o supportati dal Partito Comunista Cinese e caratterizzata da un'evoluzione di tattiche e da un'espansione nelle piattaforme utilizzate. Tra questi attori vi sono gruppi specializzati nell'utilizzo di centinaia di account sui *social network* per diffondere contenuti ostili alle proteste studentesche pro-Palestina nelle università statunitensi, e gruppi mirati alla diffusione di video a sfondo politico atti a criticare l'amministrazione in carica e a veicolare un'immagine del Presidente Joe Biden come figura inadatta a ricoprire il proprio ruolo.

[21] L. Minisini, M. Vaudano, T. Eydoux, D. Leloup, *Euromore, Russia's new information warfare weapon*, lemonde.fr, 2 giugno 2024.
[22] Microsoft Threat Analysis Center (MTAC), *Nation-states engage in US-focused influence operations ahead of US presidential election*, 17 aprile 2024.

Ciò che emerge dalle analisi è però soprattutto una crescita significativa della matrice iraniana nelle operazioni di influenza *cyber* mirate alle elezioni statunitensi[23]. Già nel 2020 l'Iran aveva condotto campagne atte ad impersonare figure estremiste che incitassero alla violenza contro ufficiali del Governo americano. In vista dell'appuntamento elettorale del 2024, questi attori hanno utilizzato una combinazione di attacchi informatici e operazioni di influenza contro istituzioni e candidati, mirando allo stesso tempo a diffondere istanze divisive sui temi del razzismo, della disparità economica e dell'identità di genere. Tra gli esempi di tali campagne iraniane, tra cui alcune di matrice legata al Corpo delle Guardie Rivoluzionarie (IRGC), vi sono:

- una campagna mirata ad impersonare gruppi di attivisti politici allo scopo di diffondere *fake news* verso un pubblico mirato, per minare la fiducia nelle autorità e nell'integrità ed affidabilità dei processi elettorali;
- una serie di attacchi di phishing mirati contro alti funzionari politici e precedenti candidati, che potrebbero essere legati al tentativo di collezionare informazioni sensibili relative alle elezioni;
- la compromissione sospetta di un account appartenente al governo di un c.d. *swing State*, ovvero uno Stato in cui il risultato elettorale è incerto poiché il sostegno ai diversi candidati è relativamente equilibrato, e che costituisce dunque solitamente un obiettivo chiave delle campagne elettorali;
- una campagna basata su siti *web* malevoli apparentemente appartenenti ad organismi di informazione, i quali sono utilizzati in realtà per diffondere al pubblico statunitense messaggi polarizzanti su questioni particolarmente sensibili, come i candidati presidenziali, i diritti LGBTQ+ e il conflitto Israele-Hamas. Alla campagna sono connessi diversi siti *web* mirati a molteplici scopi, tra cui la diffusione di articoli relativi alle elezioni di metà mandato, di contenuti sul conflitto in corso a Gaza e sulle elezioni presidenziali.

Questa rapida panoramica delle operazioni di influenza sulle elezioni globali mostra come esse siano utilizzate quali strumenti efficaci di destabilizzazione della democrazia e di alterazione degli equilibri politici internazionali, in grado di minare la fiducia nelle istituzioni democratiche e la sovranità degli Stati attraverso la manipolazione dei media e la disinformazione. Orientando la volontà popolare e favorendo candidati più affini ai propri interessi strategici, gli attori *nation-state* sono in grado di spostare gli equilibri di potere e di polarizzare la società, determinando instabilità politica e crisi a lungo termine. Per i governi e le istituzioni pubbliche, questi attacchi rappresentano una **minaccia diretta alla sicurezza nazionale** e possono compromettere le capacità di governo, poiché destabilizzano interi processi democratici e rendono difficile per i cittadini distinguere tra realtà e propaganda. Tuttavia, serie ripercussioni si verificano anche nel settore privato, in cui in particolare le aziende del settore IT, i media, le piattaforme social e i fornitori di infrastrutture critiche possono diventare bersagli o vettori involontari delle operazioni di influenza. Gli sforzi di manipolazione condotti dagli attori *na-*

[23] Microsoft Threat Analysis Center (MTAC), *Iran steps into US election 2024 with cyber-enabled influence operations*, 9 agosto 2024.

tion-state possono seriamente danneggiare la reputazione delle aziende coinvolte, ridurre la fiducia degli utenti e portare a severe conseguenze legali e regolamentari. Inoltre, le imprese possono subire danni economici diretti attraverso attacchi informatici, furto di proprietà intellettuale e sabotaggio digitale.
Con le loro gravi implicazioni, le campagne di influenza impongono alle organizzazioni e ai governi lo sviluppo di una maggiore resilienza dei processi democratici e la promozione di una collaborazione più stretta tra gli Stati e il settore privato per lo sviluppo di contromisure efficaci. È inoltre fondamentale che l'opinione pubblica e i cittadini vengano educati sui **rischi della circolazione incontrollata di contenuti non verificati**, per favorire lo sviluppo di consapevolezza e della capacità di riconoscere tentativi di disinformazione sempre più sofisticati.

3.2.3. ***Hacktivismo*: nuove frontiere dei conflitti nel cyberspazio**

L'evoluzione del contesto sociopolitico ha forti ripercussioni su un ulteriore tipo di minaccia, l'*hacktivismo*, la cui peculiarità risiede nel profondo legame che esso istituisce tra la sfera ideologica e il contesto informatico. Esso si muove in un'area ibrida complessa, che coinvolge le **dinamiche politiche e sociali**, e pertanto non semplice da indagare. Le motivazioni degli avversari della sfera hacktivista possono essere molteplici, legate alle più disparate visioni politiche e religiose, istanze culturali e ideologie nazionaliste, che possono talvolta sfociare nel terrorismo. Qualunque sia la ragione profonda delle azioni degli hacktivisti, la loro attività solleva interrogativi legali, morali ed etici di primaria rilevanza.
La storia dell'*hacktivismo* ha inizio negli anni '80 con il fenomeno del *phreaking*, una forma di *hacking* mirata ad effettuare chiamate gratuite manipolando le reti di telefonia. Tuttavia, è solo nel 1996 che il termine "*hacktivismo*" viene coniato fondendo i concetti di *hacking* e di attivismo, andando così a descrivere quel fenomeno di trasferimento delle proteste dal mondo offline all'universo di Internet. Se negli anni '90, con l'avvento dei primi PC e l'Internet sempre più accessibile, l'*hacktivismo* conosce una prima fase di crescita, è solo negli anni Duemila che il panorama hacktivista assume una dimensione più complessa e variegata. In questo periodo nascono i noti gruppi hacktivisti Anonymous e LulzSec, che iniziano a condurre **attacchi verso** obiettivi di alto profilo, come **governi e organizzazioni** percepiti come ostacoli o avversari di determinate istanze e princìpi morali. In particolare, è ben noto il coinvolgimento di Anonymous con le sue azioni di protesta e attivismo informatico nelle sollevazioni della Primavera Araba, tra il 2010 e il 2012. In questo contesto, il gruppo ha lanciato diversi attacchi DDoS verso i siti *web* del governo tunisino ("Operation Tunisia"), accusato di censurare l'ondata di proteste e dimostrazioni che prese il nome di Rivoluzione Tunisina, e contro il governo egiziano. Altre famose campagne hacktiviste furono, a titolo di esempio:

- Operation Payback (2010), condotta anch'essa da Anonymous contro una serie di entità coinvolte in attività di **antipirateria**;

- il *leak* di *Hacking* Team (2015), un'azienda italiana ritenuta colpevole di rivendere **strumenti di sorveglianza e intrusione** a clienti controversi e governi oppressivi;
- Panama Papers (2016), un *leak* di più di 11 milioni di documenti provenienti dallo studio legale panamense Mossack Fonseca, che fecero emergere un giro di evasione fiscale che coinvolgeva numerosi individui di alto profilo, tra cui *leader* politici, uomini d'affari e personaggi pubblici.

Negli ultimi anni, l'*hacktivismo* si è evoluto insieme ai cambiamenti del tessuto sociale e politico. I gruppi hacktivisti mostrano un crescente interesse per le questioni globali, come i cambiamenti climatici, i diritti umani e la libertà di espressione, concentrando molteplici azioni verso obiettivi percepiti come abusanti o irrispettosi di tali istanze. In particolare, è prevista un'ondata di *hacktivismo* climatico negli anni a venire, con il potenziale di causare ingenti danni mediante attacchi informatici rivolti ai **giganti dei combustibili fossili**[24]. Più in generale, la tendenza dell'*hacktivismo*, emersa soprattutto nei recenti conflitti in Ucraina e Medioriente, sembra essere quella di abbandonare attacchi su larga scala per concentrarsi su obiettivi mirati, costituiti da enti governativi e specifiche organizzazioni.

3.2.3.1. Nuovi sviluppi dell'*hacktivismo* nel conflitto Russo-Ucraino: un precedente per il futuro

I gruppi hacktivisti si inseriscono talvolta nelle dinamiche di tensione tra Stati e possono divenire elementi attivi di un conflitto armato, scatenando conseguenze imprevedibili che vanno oltre il controllo dei gruppi stessi. In una guerra fisica, l'inserimento dell'elemento informatico in dinamiche già complesse può influenzare le operazioni degli attori coinvolti, gli impatti sull'opinione pubblica e la narrazione del conflitto stesso. Ciò è tanto più preoccupante in quanto si tratta di un coinvolgimento non regolato di civili in un **conflitto armato tramite mezzi digitali**, i quali si cimentano nella conduzione in prima persona di operazioni contro il nemico (o qualunque entità sia percepita come tale). Considerando che un singolo gruppo può contare centinaia di hacker tra le proprie fila, l'*hacktivismo* ha portato la partecipazione di civili nei conflitti ad assumere proporzioni mai viste prima e ha spinto le istituzioni a prendere provvedimenti che ne regolino lo spazio d'azione, sia in termini di inquadramento nei "ranghi regolari", sia al contrario per limitarne il coinvolgimento. È il caso, ad esempio, del Ministro per la Trasformazione digitale ucraino Mykhailo Fedorov che, nell'immediatezza dello scoppio delle ostilità russe in Ucraina, ha indetto una "chiamata alle armi cibernetiche" allo scopo di costituire un **esercito di hacker attivi** a sostegno dell'Ucraina contro la Russia[25]. Le prime due operazioni, lanciate nel febbraio 2022, puntavano a colpire i principali siti *web* governativi e delle maggiori industrie russe con attacchi DDoS e a segnalare l'esistenza di canali YouTube mirati alla diffusione di disinformazione e propaganda russa sulla guerra in corso. Tra gli hacktivisti che hanno risposto

[24] DarkTrace, *AI Worms, Hallucinations and Climate Hacktivism: Darktrace Unveils Top Cybersecurity and AI Predictions for 2024*, darktrace.com, 14 dicembre 2023.
[25] J. Pearson, *Ukraine launches 'IT army,' takes aim at Russian cyberspace*, reuters.com, 27 febbraio 2022.

all'appello vi sono membri di Anonymous e la community di attivisti *Ukrainian Cyber Alliance* (UCA). Sul fronte russo del conflitto, invece, si sono dimostrati particolarmente attivi i gruppi nazionalisti KillNet e NoName057 (16), dediti in gran parte ad attacchi DDoS contro entità governative, infrastrutture critiche e organizzazioni occidentali e dei Paesi membri della NATO. In particolare, NoName057 (16)[26] ha dimostrato spiccate capacità organizzative e di orchestrazione dei propri membri e affiliati, dando vita al c.d. Progetto DDoSia, basato su un omonimo strumento che avvia attacchi DDoS contro i siti *web* catalogati come obiettivi, emettendo ripetutamente richieste di rete secondo un *file* di configurazione che specifica i percorsi URL di destinazione. Il progetto si avvale della **partecipazione volontaria di migliaia di utenti membri**, che installano e utilizzano lo strumento DDosia in cambio di una ricompensa monetaria che dipende dal numero di attacchi effettuati.
Altre istituzioni hanno invece tentato di limitare, o quantomeno regolamentare, l'intervento dei civili nei conflitti armati. Ad esempio, il Comitato Internazionale della Croce Rossa (ICRC) ha pubblicato alcune **regole di ingaggio per gli hacker civili**[27], incentrate principalmente sull'invito ad evitare di colpire obiettivi civili, strutture mediche e umanitarie. In particolare, l'IRCR sottolinea tre principali rischi derivanti dal coinvolgimento dei civili nella *cyberwarfare*:

a) l'*hacktivismo* può causare danni alla popolazione civile derivanti da attacchi specificamente diretti ad **obiettivi civili** (ospedali, banche, reti di trasporto, ecc.) o da danni collaterali;
b) gli hacktivisti rischiano di esporre se stessi e gli individui a loro vicini ad operazioni militari, poiché potrebbero essere considerati come direttamente partecipanti alle ostilità e dunque divenire **obiettivi militari**;
c) la partecipazione estesa di civili nelle operazioni militari sfuma il confine esistente tra chi è un civile e chi un combattente, con un conseguente rischio crescente di danni a civili inermi.

È indubbio che gli avvenimenti legati all'*hacktivismo* in Ucraina delineino una tendenza che avrà un seguito negli anni a venire, come sottolineato da alcuni analisti del settore[28]. Dinamiche molto simili sono state osservate, ad esempio, sin dall'inizio degli scontri tra Israele e Hamas in Palestina nell'ottobre 2023, anche da parte degli stessi avversari attivi nel conflitto Russo-Ucraino, che hanno ampliato il proprio raggio d'azione arrivando ad includere obiettivi Israeliani nei propri attacchi. L'interventismo dei gruppi hacktivisti è probabilmente determinato soprattutto da un desiderio di **attenzione**, ma quali che siano le reali motivazioni dietro le loro azioni, l'intreccio tra *hacktivismo* e *cyberwarfare* non sembra essere una tendenza destinata ad esaurirsi in breve tempo.

[26] D. Antoniuk, *What's in a NoName? Researchers see a lone-wolf DDoS group*, therecord.media, 4 settembre 2023.
[27] T. Rodenhauser, M. Vignati, *8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them*, blogs.icrc.org, 4 ottobre 2023.
[28] L. Hay Newman, M. Burgess, *La guerra in Medio Oriente*, wired.it, 14 ottobre 2023.

3.3. PRINCIPALI TECNICHE DI ATTACCO E VULNERABILITÀ

I prossimi paragrafi descrivono le principali tecniche di attacco e vulnerabilità che influiscono sull'attuale *cyber threat landscape*, illustrando alcune tendenze particolarmente significative che possono aiutare a comprendere le caratteristiche e gli obiettivi delle minacce e le direzioni in cui esse potranno evolversi nel prossimo futuro. Insieme ad altre problematiche di sicurezza generalmente diffuse, come l'uso di password deboli, l'assenza di metodi di autenticazione multi-fattore (MFA) e di crittografia delle comunicazioni, la presenza di configurazioni non corrette e di vulnerabilità di sicurezza non risolte in dispositivi e *software* obsoleti, questi elementi concorrono a minare significativamente la postura di sicurezza di aziende e individui, esponendoli a rischi informatici crescenti.

3.3.1. *Malware*

I *malware* sono *software* specificamente creati per scopi malevoli. Essi sono solitamente classificati per tipologia a seconda dei loro scopi e dei metodi di funzionamento:

- ***virus***: programma dannoso che si replica attaccandosi ad un altro eseguibile. Quando quest'ultimo viene eseguito, il virus si esegue a sua volta. Le azioni specifiche che il virus effettua sul sistema infetto dipendono dal particolare tipo di virus;
- ***worm***: programma dannoso che, una volta penetrato in un sistema o una rete, è in grado di autoreplicarsi creando nuove copie di se stesso, senza dipendere dall'attaccamento ad un altro eseguibile e dall'intervento *umano*;
- ***Trojan***: *software* che presenta funzionalità malevole nascoste, mentre *appare* come un programma innocuo. A differenza di *virus* e *worm*, un *Trojan* è un programma che necessita dell'intervento dell'utente per essere installato e avviato sul dispositivo. Di conseguenza, gli attaccanti cercano solitamente di convincere la vittima a scaricare e installare il *malware* tramite tecniche di ingegneria sociale, ad esempio promuovendo un videogame o uno strumento per la produttività;
- ***crypto-malware***: *malware* la cui funzione principale è la cifratura dei *file* presenti sul dispositivo allo scopo di renderli inutilizzabili. Un particolare tipo di *crypto-malware* è il *ransomware*, che chiede un riscatto all'utente in cambio della chiave di decrittazione;
- ***spyware***: *software* malevolo con la principale funzione di raccogliere informazioni sul dispositivo infetto e sulle azioni dell'utente. Questi *malware* sono solitamente dotati di numerose funzionalità, come la registrazione delle digitazioni dell'utente (*keylogging*), il monitoraggio delle attività di navigazione sul *Web*, la registrazione delle schermate visualizzate dall'utente e l'attivazione di periferiche quali fotocamera e microfono, la raccolta di dati bancari, la localizzazione del dispositivo. Talvolta, gli *spyware* sono utilizzati dagli attaccanti anche come mezzo per installare ulteriore *malware* sul sistema;
- ***adware***: *malware* progettato per visualizzare pubblicità indesiderata sul dispositivo dell'utente. Ciò può causare rallentamenti al sistema e determinarne un calo delle prestazioni, compromettendo le funzionalità del dispositivo.

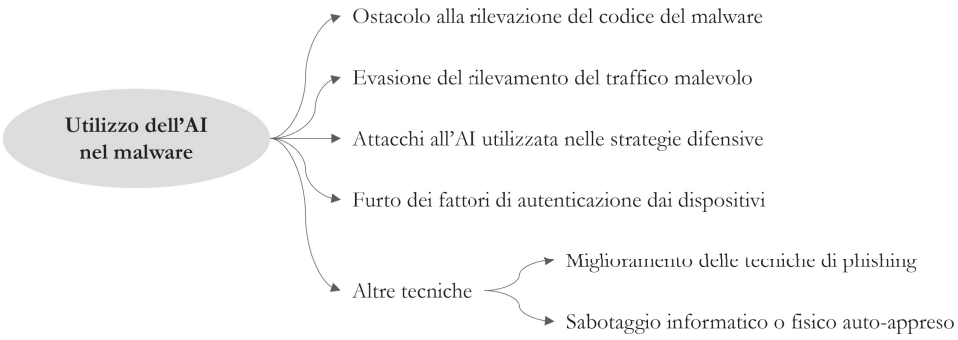
Ogni tipologia di *malware* presenta rischi specifici connessi alle singole funzionalità e può causare danni che spaziano dal furto di dati sensibili alle perdite finanziarie, al blocco delle operazioni aziendali. Anche le strategie di diffusione possono variare significativamente. Tra i metodi più utilizzati vi è ad esempio la distribuzione via e-mail, che mira a convincere il destinatario a scaricare un allegato contenente in realtà l'eseguibile malevolo. Gli avversari fanno uso, inoltre, di siti *web* creati appositamente per distribuire *malware* e di annunci *on line* che mirano a scaricare *software* malevolo sul dispositivo, anche ad insaputa dell'utente. Anche la distribuzione mediante driver USB infetti resta tra i metodi utilizzati dagli attaccanti, nonostante si tratti di una tecnica più datata: periodicamente se ne verificano picchi di utilizzo[29]. Non manca, infine, lo sfruttamento di popolari app store quale vettore di distribuzione, facilitata dalla capillare diffusione degli smartphone e dalla crescente disponibilità di applicazioni per i più diversi scopi, spesso di provenienza non facilmente verificabile.
La minaccia costituita dal *malware* è in costante evoluzione e presenta tendenze emergenti accanto ad altre ben consolidate:

a) il *malware* dimostra un crescente interesse per obiettivi rappresentati da aziende che fanno uso dell'OT (*Operational Technology*). Nel corso del 2022, questa tendenza si è consolidata mostrando una crescita del 27,5% rispetto all'anno precedente[30]. Anche le vulnerabilità che impattano i prodotti OT destano un sempre maggior interesse negli attaccanti intenzionati a sfruttarle come vettore di accesso iniziale;
b) come l'OT, anche l'infrastruttura IoT (*Internet of Things*) è stata negli ultimi anni soggetta al rischio crescente di attacchi *malware*. Generalmente, tali attacchi si configurano come il tentativo di creare una rete di *bot* o *zombie* (*botnet*), costituita da centinaia di migliaia di dispositivi infetti che agiscono sotto il controllo dell'attaccante e che a loro volta distribuiscono *malware* ad altri dispositivi IoT, ampliando esponenzialmente l'infrastruttura a disposizione per effettuare diversi attacchi, ad esempio di tipo DDoS;
c) gli sfruttamenti di vulnerabilità da parte dei *malware* quali punti di ingresso alle reti aziendali sono in costante aumento. Ciò dipende dal generale aumento del numero di vulnerabilità scoperte ogni anno, che inevitabilmente ampliano la superficie di attacco delle aziende. La crescente difficoltà nell'applicare tempestivamente le patch di sicurezza consente agli attaccanti di sfruttare queste vulnerabilità per ottenere l'accesso ed eseguire compromissioni;
d) le famiglie di *malware* utilizzano sempre più spesso la crittografia TLS (*Transport Layer Security*) per mimetizzare il traffico malevolo tra il traffico benigno[31]: ciò permette agli attaccanti di mantenere le proprie operazioni malevole nascoste più a lungo alle soluzioni di sicurezza, massimizzandone gli impatti;

[29] R. Joven, N. Choon Kiat, *The Spies Who Loved You: Infected USB Drives to Steal Secrets*, mandiant.com, 11 luglio 2023.
[30] Palo Alto Networks – Unit 42, *2023 Unit 42 Network Threat Trends Research Report*, 2023.
[31] S. Gallagher, *Nearly half of malware now use TLS to conceal communications*, sophos.com, 21 aprile 2021.

e) in generale, gli attacchi *malware* si dimostrano sempre più sofisticati grazie al diffuso utilizzo di strumenti avanzati, ideati per l'esecuzione di test di sicurezza legittimi, le cui potenti funzionalità sono però impiegate anche dagli avversari per effettuare campagne di social engineering e di phishing mirato e per condurre attività *post*-sfruttamento. Copie modificate o craccate di questi strumenti, utilizzate a scopo malevolo, consentono agli attaccanti di ottenere la persistenza sui sistemi e di muoversi lateralmente attraverso la rete aziendale;
f) la proliferazione di *malware* alimentati dall'Intelligenza Artificiale rappresenta una preoccupante minaccia emergente[32]. Essi utilizzano l'apprendimento automatico basato su pattern per adattarsi costantemente e sono in grado di utilizzare avanzate tecniche di elusione per infiltrarsi nei sistemi. Tali *malware* possono propagarsi autonomamente e in modo intelligence attraverso le reti e sono in grado di personalizzare le proprie strategie di attacco in base all'obiettivo.

Tavola 3.2. – **Utilizzo dell'Intelligenza Artificiale nel *malware***



Fonte dell'immagine: L. Fritsch, A. Jaber, A. Yazidi, *An Overview of Artificial Intelligence Used in Malware,* Nordic Artificial Intelligence Research and Development (NAIS 2022).

3.3.2. Ingegneria sociale (*Social engineering*)

Nel contesto della *cybersecurity*, la *social engineering* o ingegneria sociale è un insieme di tecniche psicologiche manipolatorie che mirano ad influenzare o ingannare una vittima allo scopo di perpetrare un'azione malevola, che può risultare nell'accesso non autorizzato ad un sistema informatico oppure nel furto di informazioni sensibili o finanziarie.

[32] L. Fritsch, A. Jaber, A. Yazidi, *An Overview of Artificial Intelligence Used in Malware*, Nordic Artificial Intelligence Research and Development (NAIS 2022), 1 giugno 2022.

La particolarità di questo tipo di minaccia sta nel suo sfruttamento dell'elemento umano. Tra le tecniche di ingegneria sociale più utilizzate vi sono:

- ***phishing***: invio di e-mail ingannevoli allo scopo di raccogliere informazioni, quali password e dati bancari. In questa casistica si possono annoverare anche lo *spear-phishing* (versione sofisticata del phishing mirato a specifici individui o organizzazioni), lo *smishing* (phishing effettuato mediante l'invio di SMS fraudolenti), il *vishing* (phishing effettuato mediante chiamate vocali).
- ***Business Email Compromise* (BEC)**: truffa sofisticata indirizzata ad impiegati o figure *executive* delle aziende, che mirano a convincere la vittima ad effettuare transazioni bancarie, oppure a compromettere l'account e-mail della vittima per distribuire *malware* ai suoi contatti aziendali;
- ***pretexting***: tecnica che si basa sulla creazione di un particolare contesto fraudolento atto a convincere la vittima a condividere informazioni sensibili che essa non condividerebbe al di fuori di tale contesto, ad esempio un finto colloquio di lavoro;
- ***baiting***: tentativo di truffa basato sull'offerta fraudolenta di un bene o servizio (ad esempio, contenuti audio o video piratati, videogiochi) in cambio di informazioni sensibili condivise dalla vittima;
- **impersonazione**: creazione di false identità, ad esempio mediante finti profili sui *social media*, a fine di beneficiare dell'esposizione mediatica o dei contatti del soggetto impersonato.

Le tecniche dell'ingegneria sociale sono largamente utilizzate come vettore di accesso iniziale alle reti: secondo l'FBI, il *phishing* è il crimine informatico maggiormente diffuso[33]. Inoltre, un recente *report* pubblicato dall'ENISA ha rilevato un significativo aumento di questi eventi nella prima metà del 2023[34]: i costi ridotti e la semplicità di esecuzione mantengono l'ingegneria sociale tra le tecniche di attacco preferite dagli avversari, soprattutto contro obiettivi dei Paesi dell'area EMEA. Ciò è favorito dal fatto che anche il phishing, come il *ransomware*, negli ultimi anni ha assunto le caratteristiche di un vero e proprio *business* del crimine informatico, con la disponibilità di soluzioni *Phishing-as-a-Service* (PhaaS) al **costo irrisorio di 15 dollari al giorno**, che consentono anche a malintenzionati con minime conoscenze informatiche di perpetrare truffe ed eseguire attacchi anche complessi. Inoltre, i recenti conflitti hanno fornito nuove esche ai cybercriminali, che a partire dal 2022 hanno ampiamente utilizzato il tema della guerra in Ucraina in attacchi di *spear-phishing* contro Paesi della NATO[35], in modo simile a come è stato per la pandemia di Covid-19 negli anni precedenti. Infine, non può ignorarsi il sempre più facile accesso all'Intelligenza Artificiale grazie a strumenti come ChatGPT, che consentono agli avversari di creare contenuti di phishing altamente credibili e convincenti.

[33] Federal Bureau of Investigation (FBI), *Internet Crime Report 2022*, 14 marzo 2023.
[34] European Union Agency for *Cybersecurity* (ENISA), *ENISA Threat Landscape 2023*, 19 ottobre 2023.
[35] S. Huntley, *Fog of war: how the Ukraine conflict transformed the cyber threat landscape*, blog.google, 16 febbraio 2023.

Nonostante i diversi tentativi di contrasto a tale minaccia, il *phishing* si dimostra resiliente nei confronti di misure di sicurezza quali **l'autenticazione multi-fattore** (MFA), le quali vengono aggirate dagli attaccanti mediante tecniche specifiche, come l'*MFA fatigue* – che prevede l'invio ripetitivo di richieste di autenticazione MFA alle vittime – o il *SIM swapping*.

3.3.3. Attacchi alla *Supply chain*

Con attacco alla *supply chain* si definisce un tipo di attacco complesso, costituito da due fasi interconnesse e di solito progressivamente orchestrate:

1. l'attaccante colpisce un fornitore o un *partner* commerciale che costituisce un **anello debole nella catena di approvvigionamento di un'organizzazione**;
2. i risultati della prima compromissione consentono all'attaccante di ottenere l'accesso a dati o sistemi dell'organizzazione che costituisce l'**obiettivo reale dell'operazione offensiva**.

Il principale scopo degli attacchi alla *supply chain* riguarda la raccolta di informazioni strategiche o sensibili; tuttavia, essi possono anche conformarsi come eventi distruttivi che mirano all'interruzione delle operazioni aziendali.
Gli attacchi alla *supply chain* sono stati definiti a più riprese come uno dei rischi informatici più pressanti degli ultimi anni e una forma di attacco in costante crescita: si prevede che, entro il 2025, il 45% delle aziende subirà un attacco alla propria *supply-chain* del *software*[36]. Tali attacchi avvengono in un contesto complesso, rappresentato dalle relazioni di fiducia tra le parti che costituiscono una **catena di approvvigionamento**, e mirano a colpire i punti deboli di tali relazioni. Questa complessità ostacola l'individuazione di attacchi che possono avvenire in qualsiasi fase della catena. L'impatto degli attacchi alla *supply chain* può inoltre avere un **effetto domino**, in quanto le conseguenze di un singolo attacco si diffondono rapidamente ad altre organizzazioni e mettono a rischio la produzione di beni e servizi. Di conseguenza, essi possono comportare danni alla reputazione aziendale e minare la fiducia di *partner*, clienti e consumatori finali. La loro natura interconnessa li rende particolarmente ardui da contrastare, soprattutto per la difficoltà nel mettere in campo strategie di difesa sinergiche tra le diverse parti in causa. Ne consegue che le organizzazioni più a rischio sono quelle operanti in settori produttivi caratterizzati da **catene di approvvigionamento complesse**, come la **produzione di energia, il settore farmaceutico e manifatturiero, i trasporti e i servizi finanziari**.
Trattandosi di operazioni complesse che spesso necessitano di un'accurata pianificazione, gli attacchi alla *supply chain* sono solitamente tipici di gruppi APT e attori *state-sponsored* dotati delle necessarie competenze e risorse. Ne è un esempio il noto attacco del 2020 alla *supply chain* di SolarWinds, azienda statunitense sviluppatrice di *software* di gestione, attribuito ad un avversario legato al governo russo e noto come Nobelium

[36] Gartner, *Gartner Identifies Top Security and Risk Management Trends for 2022*, gartner.com, 7 marzo 2022.

o APT29[37]. Il sofisticato attacco ha compromesso il *software* Orion, prodotto da SolarWinds, iniettandovi un *malware*; questa versione compromessa è stata poi distribuita e scaricata dalla piattaforma di SolarWinds da migliaia di clienti che utilizzavano Orion come strumento di monitoraggio di rete. Gli attaccanti hanno dunque ottenuto l'accesso ai sistemi di numerose vittime e hanno potuto sottrarre dati sensibili, con un impatto esteso su numerose organizzazioni, inclusi enti governativi e aziende private.
Inoltre, nel recente periodo gli attacchi alla *supply chain* hanno assunto una rilevanza dovuta al conflitto in Ucraina. Nel corso del 2023, avversari legati alla Russia hanno continuato a condurre questi attacchi per ostacolare la **catena di approvvigionamento umanitario e militare**, oppure per raccogliere informazioni su reti e sistemi e per eseguire il **furto di dati**. Anche il conflitto fra Israele e Hamas ha determinato, sin delle prime ostilità nell'ottobre 2023, impatti significativi alla *supply chain* di enti ed organizzazioni causati da attacchi informatici mirati al disturbo o all'interruzione delle attività di *partner* e fornitori.
Gli attacchi alla *supply chain* destano sempre più spesso anche l'interesse del cybercrime. In particolare, i gruppi *ransomware* hanno individuato in tali attacchi un metodo efficace per massimizzare gli impatti e i ricavi economici, come è evidente se si osserva da vicino uno dei maggiori eventi di questa tipologia degli ultimi anni: la scoperta – e il conseguente sfruttamento su larga scala – della vulnerabilità *zero day* nota come "Log4shell" e tracciata come CVE-2021-44228, presente nella libreria Java Log4j. Nel 26% dei casi, lo sfruttamento di questa vulnerabilità è stato eseguito come parte di un attacco *ransomware*[38].
Le tendenze emerse dall'analisi degli attacchi alla *supply chain* evidenziano la frequente inclusione di fornitori di soluzioni di Identity *Management* tra gli obiettivi di interesse, dal momento che un sempre maggior numero di organizzazioni sceglie di affidarsi a *identity provider* per le procedure di autenticazione. Inoltre, gli avversari si stanno concentrando sempre più spesso sull'eseguire attacchi altamente mirati contro il personale in possesso di privilegi elevati, come gli **amministratori o gli sviluppatori**, per ottenere l'accesso agli *asset* aziendali, come ad esempio *repository* di codice, che possono essere ulteriormente sfruttati per compromettere altre organizzazioni della *supply chain*.

3.3.4. Vulnerabilità di sicurezza

La gestione delle vulnerabilità è un aspetto particolarmente critico della sicurezza informatica, poiché esse sono spesso sfruttate dai cybercriminali per penetrare nei sistemi aziendali. Molte organizzazioni hanno difficoltà a mantenere i propri *software* e *hardware* aggiornati e, a causa di risorse limitate o della mancanza di consapevolezza dei potenziali rischi, tendono a trascurare la presenza di queste vulnerabilità e a non eseguire tempestivamente gli aggiornamenti critici, lasciando le reti e i sistemi esposti a tentativi di sfruttamento ed aumentando la probabilità di incidenti di sicurezza con

[37] Fireeye (Mandiant), *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*, mandiant.com, 13 dicembre 2020.
[38] Verizon, *2023 Data Breach Investigation Report*, 2023.

conseguenze disastrose. L'utilizzo di *software* obsoleto e la mancata disattivazione di applicazioni non più supportate, uniti talvolta all'uso di configurazioni di *default* e password predefinite, facilitano gli attacchi ed espongono le aziende a **potenziali violazioni**, **danni finanziari e reputazionali** e al rischio di incorrere in pesanti sanzioni.
Un esempio recente di quanto la presenza di una vulnerabilità possa determinare gravi compromissioni risale al maggio 2024, quando un settimanale tedesco ha rivelato che avversari ignoti avrebbero ottenuto l'accesso non autorizzato a video-riunioni riservate del Governo tedesco grazie allo sfruttamento di una vulnerabilità presente nel *software* per videoconferenze Cisco Webex[39], non ancora corretta dal produttore – si trattava dunque di una vulnerabilità *zero day*. Secondo quanto riportato dal giornale, il Governo utilizzava una versione *on-premise* di Webex e conservava i dati su un server locale. Tuttavia, la presenza di una vulnerabilità avrebbe consentito agli attaccanti di ottenere i *link* utilizzabili per accedere a migliaia di meeting interni. Inoltre, le *meeting room* personali degli alti ufficiali tedeschi coinvolti nell'incidente non erano protette da password, facilitando ulteriormente gli sforzi degli attaccanti, che sono così riusciti ad autenticarsi e ad assistere a riunioni riservate. La combinazione di **vulnerabilità e cattive pratiche di sicurezza** ha dunque causato l'esposizione dell'identità dei partecipanti e delle informazioni sensibili discusse, tra cui alcune relative ad attività militari. Nel mese di marzo 2024, la registrazione audio trapelata di un meeting dei vertici militari tedeschi tenutosi su Webex era stata diffusa da RT, un *network* televisivo controllato dal Cremlino. La responsabilità di attori russi nell'*hacking* delle riunioni del Governo tedesco non è stata tuttavia definitivamente confermata.
L'episodio tedesco dimostra inoltre che le vulnerabilità di cui doversi preoccupare non sono solamente quelle presenti in *software* e *hardware*, ma anche quelle derivanti dal comportamento degli utenti, il c.d. fattore umano. Per quanto le organizzazioni si sforzino di adottare le buone pratiche di sicurezza e di installare gli strumenti di monitoraggio più sofisticati disponibili sul mercato, possono ugualmente incorrere in gravi incidenti qualora dimentichino di considerare che l'**errore umano**, come l'utilizzo di una password debole, un semplice click sul *link* contenuto in un'e-mail di *phishing* o la condivisione inconsapevole di informazioni con i destinatari scorretti, può rendere vulnerabile anche la rete più fortificata. Tali errori non sono commessi solo dal personale più inesperto, ma possono essere commessi anche dai dirigenti, coloro che solitamente detengono l'accesso ai dati più sensibili e l'autorizzazione per avviare transazioni finanziarie. Ignorare il fattore umano può determinare ingenti perdite di denaro, danni alla reputazione e sanzioni normative. Per tale motivo, ogni organizzazione dovrebbe assicurarsi di adottare un approccio che includa le vulnerabilità umane nel proprio più ampio programma di gestione delle vulnerabilità di sicurezza.

3.3.5. Il potenziale dell'Intelligenza Artificiale: minaccia o soluzione?

A partire dal suo lancio nel novembre del 2022, ChatGPT ha avvicinato milioni di utenti all'Intelligenza Artificiale (AI) e ha determinato una maggiore familiarità con la

[39] E. Wolfangel, *Jeder konnte sie finden*, zeit.de, 4 maggio 2024.

Generative AI, un termine che definisce sistemi di intelligenza artificiale in grado di generare autonomamente e creativamente contenuti quali immagini, testi e suoni. ChatGPT, un chatbot basato su tecniche di apprendimento automatico, ha democratizzato l'accesso alla Generative AI senza richiedere pregresse competenze tecniche avanzate.
Dal punto di vista della *cybersecurity*, questa diffusione generalizzata della Generative AI e la sua semplicità di utilizzo portano all'insorgere di nuovi rischi e di nuovi interrogativi etici, ma possono anche rivelarsi una risorsa preziosa se applicata efficacemente al contrasto alle minacce[40].
Nel corso del 2023 sono emerse nuove tendenze nel *cyber threat landscape* che puntano a trarre vantaggio dall'AI[41]. Nell'ambito dell'ingegneria sociale, si prevede che la Generative AI e i *Large Language Model* (LLM) verranno sempre più spesso utilizzati per rendere più credibili gli attacchi di *phishing*, *smishing* e *vishing*, eliminando alcune barriere linguistiche e culturali che ancora persistono in questo genere di operazioni offensive, e consentendo agli attaccanti di mimetizzarsi maggiormente tra le comunicazioni legittime grazie alla capacità di imitare più accuratamente le interazioni umane. Le potenzialità della Generative AI rendono possibili attacchi che finora erano considerati estremamente difficili da realizzare, come ad esempio la clonazione della voce in attacchi di *vishing* altamente credibili[42]. Inoltre, i nuovi strumenti consentono anche di velocizzare la creazione di *phishing* mirato a diverse organizzazioni, riducendo il carico di lavoro necessario all'attaccante, e di determinare la tecnica più efficace di ingegneria sociale per ogni obiettivo, aumentando le probabilità di successo.
Grazie all'adozione dell'AI, le operazioni di influenza punteranno sempre più di frequente alla produzione di *fake news* e *deepfake* che si mimetizzino facilmente tra i contenuti mainstream e influenzino efficacemente l'opinione pubblica. Del resto, operazioni di questo tipo sono già realtà, come dimostrato dalla recente identificazione di una ***bot farm* potenziata dalla Generative AI**, utilizzata da affiliati di Russia Today per creare profili *on line* che riflettono persone di nazionalità diverse, con lo scopo di diffondere disinformazione in diversi Paesi, tra i quali Stati Uniti, Polonia, Germania e Paesi Bassi. La bot farm è stata creata utilizzando Meliorator, un pacchetto *software* potenziato dall'intelligenza artificiale generativa in grado di **creare profili di *social media* dall'aspetto autentico, imitare contenuti realistici dei *social media***, rispecchiare la disinformazione di altri bot, perpetuare automaticamente **false narrazioni e formulare messaggi** in base al tipo di bot che lo utilizza[43].
Da queste minacce sofisticate deriva un serio rischio per l'attendibilità delle informazioni e un generalizzato calo di fiducia negli organi informativi e nei governi. Come visto in precedenza, un livello di rischio particolarmente preoccupante è associato alle

[40] L. Fritsch, A. Jaber, A. Yazidi, *An Overview of Artificial Intelligence Used in Malware*, Nordic Artificial Intelligence Research and Development (NAIS 2022), 1 giugno 2022.
[41] Google Cloud, *Cybersecurity Forecast 2024 – Insights for future planning*, 9 novembre 2023.
[42] European Union Agency for *Cybersecurity* (ENISA), *ENISA Threat Landscape 2023*, 19 ottobre 2023.
[43] FBI, CNMF, AIVD, MIVD, DNP, CCCS, *State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity*, 9 luglio 2024.

elezioni politiche, che costituiscono solitamente un potenziale obiettivo primario per gli attori interessati a manipolare o minare la democrazia in determinati Paesi. La generazione di materiale di propaganda mediante Generative AI è ormai estremamente accessibile e potrebbe mettere a rischio l'affidabilità dei media informativi a cui solitamente gli elettori si affidano per orientare la propria scelta di voto[44].
Inoltre, nell'ambiente underground ha riscosso un significativo successo la disponibilità di servizi a pagamento che offrono agli attaccanti la possibilità di ottimizzare costi e infrastrutture e al contempo consentono di condurre attacchi avanzati, come il *Ransomware-as-a-Service* e il *Phishing-as-a-Service*. Nel prossimo futuro è plausibile la diffusione di strumenti di Generative AI offerti *as-a-service* in forum di *hacking* specializzati, che aumenteranno esponenzialmente l'incidenza di attacchi più efficaci, come **campagne di phishing sofisticate** e altamente mirate.
Le possibilità di sfruttamento malevolo dell'AI sono numerose e definirne una lista esaustiva è complicato dal fatto che si tratta di una tecnologia in divenire, di cui ancora non sono completamente chiare le enormi potenzialità. Non vi è tuttavia dubbio che l'adozione dell'intelligenza artificiale offra vantaggi ad ogni tipologia di *threat actor*, supportando la conduzione di attacchi più efficaci, la scoperta di nuove vulnerabilità, la creazione di nuovi *malware* sofisticati, le operazioni di spionaggio digitale e il miglioramento della precisione dei tentativi di compromissione.
L'AI può inoltre divenire essa stessa oggetto di attacchi che mirano a sfruttarne il funzionamento. Poiché i modelli di linguaggio come ChatGPT funzionano rispondendo a richieste o istruzioni degli utenti (*prompt*), sono vulnerabili a tecniche di attacco che mirano a manipolare o ingannare il modello attraverso l'iniezione di prompt specificamente creati per causarne un comportamento indesiderato o dannoso. Questi attacchi sono detti **attacchi di *prompt injection*** e possono consentire di ottenere risposte che il modello non dovrebbe poter dare, come ad esempio informazioni sensibili o l'esecuzione di istruzioni non previste o vietate dalle norme del modello stesso. Sono inoltre studiate con sempre maggiore attenzione le diverse tipologie di attacco che si possono perpetrare nei confronti del Machine Learning, uno degli strumenti principali utilizzati dall'AI per apprendere dai dati, riconoscere schemi ed effettuare previsioni. Nel complesso, questa tipologia di attacchi è definita *Adversarial Machine Learning* ed include molteplici tecniche, tra cui:

- **attacchi di evasione (*evasion*)**: questa tipologia di attacco tenta di eludere i sistemi di AI, manipolando i dati in input così da ingannare il sistema e fare in modo che dati malevoli o fraudolenti non siano riconosciuti come tali e considerati legittimi;
- **avvelenamento dei dati (*data poisoning*)**: questo attacco ha l'obiettivo di inquinare o alterare il dataset utilizzato per addestrare il modello di AI, ad esempio allo scopo di far apprendere comportamenti pericolosi, che violino le regole del modello o che introducano vulnerabilità nel modello stesso;

[44] Darktrace, *AI Worms, Hallucinations and Climate Hacktivism: Darktrace Unveils Top Cybersecurity and AI Predictions for 2024*, darktrace.com, 14 dicembre 2023.

- **inversione del modello (*model inversion*)**: con questo attacco, gli avversari mirano a ricostruire ed ottenere informazioni personali o sensibili contenute nel dataset utilizzato per addestrare il modello di AI. Questo tipo di attacco sofisticato viene eseguito interrogando il modello e sottoponendo dei set di dati per capire se questi siano stati utilizzati per l'addestramento;
- **estrazione del modello (*model extraction*)**: questo tipo di attacco ha lo scopo di ricostruire il modello di AI di un'organizzazione mediante l'analisi dei suoi output per replicarne il comportamento e violarne quindi la confidenzialità. In questo caso, l'attaccante può ottenere informazioni sulla struttura del modello stesso e può verificarsi una violazione della proprietà intellettuale.

D'altra parte, le tecnologie dell'intelligenza artificiale possono costituire una preziosa risorsa per il fronte difensivo della *cybersecurity*, soprattutto per il supporto all'analisi di grandi quantità di dati e alle operazioni di contestualizzazione dei dati stessi, che attualmente comportano un significativo dispendio di tempo e risorse e sono rese difficoltose dai **costi elevati** e dalla insufficiente disponibilità di personale esperto. Nello scenario contemporaneo, in cui le quantità di dati da analizzare crescono in modo esponenziale e il loro trattamento diviene sempre più complesso, l'utilizzo dell'AI offre un supporto fondamentale attraverso strumenti capaci di gestire ed elaborare grandi volumi di informazioni in modo efficiente e tempestivo. Grazie all'aumento delle capacità analitiche, i team di sicurezza potranno produrre analisi approfondite e tempestive ed applicare strategie di individuazione, contenimento e mitigazione più efficaci, quali ad esempio:

a) l'utilizzo del machine learning per l'individuazione di **anomalie nel comportamento dei sistemi** e l'adozione di misure preventive guidate dall'analisi predittiva delle minacce;
b) l'utilizzo di strumenti di sicurezza per endpoint basati su AI che rilevino e blocchino *malware* e attività dannose;
c) l'analisi di log e dati mediante algoritmi di machine learning per l'identificazione di tendenze e modelli;
d) l'automatizzazione della **risposta agli incidenti** per una migliore coordinazione delle contromisure (come l'isolamento dei sistemi compromessi o di segmenti di rete);
e) la simulazione efficace di scenari di attacco per la valutazione del **livello di resilienza** dell'organizzazione.

Pur offrendo vantaggi significativi in termini di efficienza e innovazione, l'adozione dell'AI solleva anche una serie di implicazioni etiche e ambientali da cui le organizzazioni e i governi non dovrebbero prescindere. Sul fronte etico, essa determina problemi di *privacy*, dovuti alla necessità di garantire trasparenza ed equità nell'uso dei dati e il rispetto dei diritti degli individui, evitando discriminazioni o distorsioni nei processi decisionali. A livello ambientale, i processi di addestramento e l'esecuzione dei modelli di AI comportano una serie di problemi legati alla notevole richiesta di risorse computazionali, con conseguenti elevati consumi energetici e un impatto ambientale significativo in termini di emissioni e consumo energetico.

Per tutte le ragioni finora discusse, un'adozione sostenibile dell'AI richiede che questa tecnologia sia trattata come una **scelta strategica**, che richiede un approccio responsabile e una valutazione approfondita dei rischi informatici, dei benefici apportati alle operazioni aziendali, delle implicazioni etiche e dell'impatto ambientale.

3.4. NUOVE FRONTIERE E SFIDE EMERGENTI: ULTERIORI SVILUPPI TECNOLOGICI E POSSIBILI NUOVE MINACCE

Come finora sottolineato, il *cyber risk* pervasivo impone l'adozione di una strategia dinamica nell'affrontare le minacce del *cyber threat landscape*, e richiede di privilegiare un approccio proattivo, anticipando nuove sfide e sviluppi futuri. Ciò include anche l'identificazione dei potenziali rischi derivanti da tecnologie emergenti o in fase di espansione, come ad esempio l'IoT, la blockchain e il *quantum* computing, e implica una continua revisione delle strategie di sicurezza, l'adozione di soluzioni avanzate e un'attenzione alla formazione e ritenzione dei talenti per preservare l'integrità e la resilienza dei sistemi informatici di fronte alla mutevolezza del panorama della *cybersecurity*.

Internet of Things

Con *Internet of Things* (IoT) ci si riferisce ad una rete di dispositivi fisici interconnessi che si scambiano dati attraverso Internet e che vengono utilizzati per diversi scopi, come l'automazione e il monitoraggio nei settori della domotica, dell'assistenza sanitaria, dei trasporti, dell'energia, della difesa e in svariati settori industriali. Anche a causa della loro sempre più capillare adozione, questi dispositivi sono particolarmente presi di mira dagli attaccanti. Tra i motivi principali di questo interesse si possono annoverare le misure di sicurezza ridotte generalmente adottate, come:

1. l'assenza di **procedure di autenticazione robuste**, l'uso di **password deboli** o di *default* e la **mancanza di crittografia** per la protezione dei dati trasmessi;
2. la scarsa disponibilità o la mancata applicazione regolare di **aggiornamenti *software***;
3. l'assenza di **isolamento** tra i dispositivi IoT e altri dispositivi sulla rete;
4. l'ampia diffusione dell'IoT in molteplici ambiti, che ne ostacola la gestione centralizzata.

Gli avversari sfruttano frequentemente le vulnerabilità presenti o gli insufficienti meccanismi di sicurezza per compromettere i dispositivi IoT ed ottenere più facilmente l'accesso alla rete aziendale per ulteriori operazioni malevole. Una volta compromessi, questi dispositivi possono anche essere inclusi in una *botnet* e consentire all'attaccante di ampliare la portata dei propri attacchi, quali ad esempio DDoS, *spam* e *phishing*, *mining* di criptovaluta, attacchi di forza bruta contro altri dispositivi. A seconda dell'ambito specifico di impiego della tecnologia IoT, gli attacchi possono generare conseguenze anche gravi, incluso il rischio di danni fisici a persone o infrastrutture.

Blockchain

Il termine *blockchain* definisce una struttura di dati costituita da una catena di record, anche detti "blocchi", i quali contengono un insieme di dati o transazioni e sono collegati tra loro da funzioni crittografiche. Poiché ogni blocco contiene un identificatore univoco del blocco precedente (in forma di *hash*), la catena costituisce una sequenza cronologica immutabile e può essere utilizzata per immagazzinare, gestire e trasmettere dati in modo sicuro e trasparente. Inizialmente introdotta come infrastruttura per la criptovaluta Bitcoin, oggi la *blockchain* è utilizzata in diversi ambiti, come la ***supply chain***, la **gestione dei dati in ambito sanitario** e **l'identità digitale**. Nonostante la sua sicurezza intrinseca, la tecnologia *blockchain* è suscettibile a diversi attacchi informatici[45] che mirano a colpire protocolli e *software* utilizzati dalle blockchain e che coinvolgono, ad esempio, i nodi della rete, i protocolli di consenso, i portafogli digitali. Alcuni di essi possono mettere a rischio l'integrità della *blockchain* stessa e consentire la manipolazione delle transazioni. Inoltre, i contratti intelligenti, i protocolli crittografici e le librerie utilizzate per lo sviluppo di criptovaluta non sono immuni ad attacchi che mirano a sfruttarne le vulnerabilità, allo stesso modo dei protocolli di consenso e dei portafogli digitali, che possono essere presi di mira da *malware* o tentativi di phishing per comprometterne la sicurezza e sottrarre informazioni.

Quantum Computing

Il *quantum computing* è un tipo avanzato di computing basato sui principi della **meccanica quantistica**, ed è dunque contraddistinto da capacità di calcolo molto superiori a quelle dei computer classici. Esso utilizza i *qubit* (*quantum bits*) al posto dei bit binari come unità fondamentale di informazione. A differenza di un bit classico, che può trovarsi solo in uno stato alla volta (o 1 o 0), un *qubit* può esistere in una superposizione di entrambi gli stati contemporaneamente. Ciò conferisce ai computer quantistici una potenza di calcolo e una velocità ineguagliati. Nonostante il calcolo quantistico sia ancora nelle fasi iniziali di sviluppo e non siano previste sue applicazioni pratiche a breve termine, esso potrebbe ricoprire un ruolo significativo in diversi ambiti scientifici e industriali. I computer quantistici potranno utilizzare la fisica quantistica per elaborare informazioni e risolvere in modo efficiente problemi troppo complessi per le attuali capacità di calcolo dei computer classici. Le sperimentazioni hanno infatti dimostrato che un processore quantistico potrebbe completare una computazione mirata in 200 secondi, mentre un supercomputer impiegherebbe migliaia di anni per lo stesso compito.

Le principali implicazioni per la sicurezza derivanti dal *quantum computing* sono relative al suo potenziale impatto sugli attuali algoritmi crittografici utilizzati per la protezione di dati e comunicazioni, che potrebbero essere violati in tempi molto ridotti rispetto agli attuali e dunque risultare **vulnerabili e obsoleti**[46]. La crittografia a chiave pubblica attuale si basa sulla difficoltà di risolvere alcuni problemi matematici com-

[45] IBM, *What is blockchain security?*, ibm.com.
[46] I. Barmes, *The Quantum threat to Cryptography*, deloitte.com.

plessi per generare le chiavi di cifratura e decifratura. Anche se i computer tradizionali non sono in grado di effettuare i complessi calcoli necessari per rompere i moderni algoritmi crittografici, i computer quantistici potrebbero riuscirci in pochi minuti.
Allo stato attuale, questa tecnologia non è sufficientemente sviluppata per violare la crittografia che viene correntemente utilizzata, ma secondo gli esperti i continui e rapidi progressi potrebbero renderlo possibile entro il 2030. Tale rischio potrebbe compromettere significativamente la sicurezza e l'affidabilità delle comunicazioni, delle firme digitali e della protezione della proprietà intellettuale. Per questo motivo, diverse istituzioni hanno sollecitato le organizzazioni a prepararsi all'adozione di metodi di crittografia in grado di resistere ad attacchi da parte di computer quantistici[47]. Nel mese di agosto 2024, il *National Institute of Standards and Technology* (NIST) degli Stati Uniti ha pubblicato i propri *standard* crittografici *post-quantum*[48], ideati per resistere agli attacchi informatici basati sul *quantum computing* e basati su **tre algoritmi crittografici**, di cui uno utilizzabile per la crittografia generica e due ideati specificamente per le firme digitali.

[47] *Cybersecurity* and Infrastructure Security Agency (CISA), *Preparing Critical Infrastructure for Post-Quantum Cryptography*, agosto 2022.
[48] National Institute of Standards and Technology (NIST), *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*, nist.gov, 13 agosto 2024.