Threat actors made in China

Focus sulle campagne di cyber spionaggio del governo cinese nei confronti delle aziende HiTech americane ed europee.

Con il processo di riforma iniziato negli anni ’70 e ’80 da Deng Xiaoping, la Cina ha compiuto progressivamente una trasformazione radicale che ha portato il Paese verso un futuro di grande crescita economica e di sviluppo industriale. Internet arriva in Cina negli anni ’90 e il governo di Pechino intravede immediatamente le sue grandi potenzialità, tanto da concentrare impressionanti risorse sullo sviluppo delle infrastrutture di telecomunicazione e tecnologiche del Paese.

Il 2015 è un anno molto particolare per la Cina: è l’anno in cui la Cina ha mostrato al mondo il suo piano.

Made in China 2025: la strategia di Cyber Espansione Globale

Rilasciato nel 2015, *“Made in China 2025”* è il piano decennale del governo cinese per sviluppare rapidamente una politica industriale mirata a rendere la Cina dominante nella produzione high-tech globale, in particolare dieci industrie high-tech, tra cui: auto elettriche, tecnologie dell’informazione (IT) e delle telecomunicazioni di prossima generazione, robotica avanzata, intelligenza artificiale, ingegneria aerospaziale, biomedicina avanzata e nuovi materiali sintetici.

Se consideriamo ciò che è scritto nel piano industriale del governo, risulta evidente che l’obiettivo strategico di Pechino è ridurre la dipendenza della Cina dalla tecnologia straniera e promuovere i produttori high-tech cinesi per conquistare la leadership tecnologica mondiale nel modo più rapido possibile. Il piano prevede un forte investimento del

governo in programmi per aumentare la posizione competitiva delle aziende cinesi sul mercato globale; e sicuramente anche l'impiego di operazioni di cyber spionaggio risulta determinante nel velocizzare il raggiungimento di tale scopo.

Lo spionaggio di segreti industriali e commerciali mira principalmente ad ottenere informazioni su come realizzare nuove tecnologie, processi industriali e commerciali in tempi brevi e con risorse proprie, saltando completamente la catena del valore, senza quindi dover investire in risorse economiche e umane necessarie a inventarle e progettarle: una pratica che nei fatti la Cina sta sempre più dimostrando di attuare, in particolar modo, attraverso il cyber spionaggio.

Threat Actors cinesi e operazioni di spionaggio internazionale

Il 6 luglio 2022 il direttore dell'FBI Christopher Wray e il capo dell'MI5 Ken McCallum, in una conferenza congiunta senza precedenti svoltasi nella sede dell'MI5 a Thames House (Londra), hanno evidenziato come le attività di contrasto di entrambi i governi, inglese e statunitense, alle azioni di spionaggio del governo cinese siano più che raddoppiate negli ultimi tre anni.

Wray ha affermato in particolare che la Cina ha sviluppato il più grande programma di cyber spionaggio per rubare know-how mai realizzato da qualsiasi altro paese; e McCallum ha reso note attività di contrasto a diverse cyber-minacce cinesi, come quella che nel maggio 2022 l'MI5 ha bloccato contro il settore aerospaziale.

Wray ha inoltre affermato che la Cina sta traendo molte informazioni dal conflitto tra Russia e Ucraina, dalla sperimentazione di nuove tecniche di cyber spionaggio alle strategie per evitare qualsiasi tipo di sanzione nel caso invadesse Taiwan: evento che causerebbe una crisi economica

molto più grave di quella avuta con la produzione dei chip nel 2022, sia per l'acquisizione indebita di know-how tecnologico sia perché causerebbe l'interruzione delle catene di approvvigionamento e gli investimenti occidentali in Cina verrebbero così trasformati in "ostaggi".

Wray ha infine affermato che il governo cinese "rappresenta la più grande minaccia a lungo termine" alla sicurezza economica e nazionale per il Regno Unito, gli USA e gli alleati europei.

Nei mesi successivi alla conferenza gli Stati Uniti hanno cominciato a rallentare i progressi della Cina nell'industria chiave dei semiconduttori, vietando ai cittadini statunitensi di lavorare per aziende di chip cinesi, incrementando i controlli sulle esportazioni nonché richiedendo licenze e autorizzazioni alle aziende che esportano chip in Cina e che utilizzano strumenti o software statunitensi, suscitando notevoli malumori da parte del governo cinese.

La particolarità di questa conferenza – oltre al fatto di essere stata indetta per la prima volta congiuntamente da Stati Uniti e Regno Unito – è di fatto un ultimatum ufficiale per richiamare la Cina all'accordo del 2015 (fatto proprio in concomitanza della presentazione del piano industriale cinese), in cui Stati Uniti e Cina si impegnavano comunemente a non effettuare "furti informatici di proprietà intellettuale, inclusi segreti commerciali o altre informazioni commerciali riservate per vantaggio commerciale". Accordo che, secondo gli Stati Uniti, ebbe fin da subito un risultato blando, in quanto gli attacchi di cyber spionaggio cinesi diminuirono in termini quantitativi, ma proseguirono invece quelli più sofisticati.

Cyber espionage escalation

Da diversi anni ormai sempre più campagne di cyber spionaggio sono attribuite alla Cina, che sembra continuare le proprie operazioni in maniera sempre più "disinvolta". E mentre

l’abbattimento del sospetto pallone spia cinese, il 4 febbraio 2023, nello spazio aereo canadese, rimane ancora un mistero da svelare, l’India ha cautelativamente attivato il 6 marzo 2023 un protocollo operativo militare per abbattere ad alta quota eventuali palloni spia cinesi che dovessero sorvolare i propri cieli.

Un mese prima, nel gennaio 2023, Zheng Xiaoqing, un ex dipendente del conglomerato energetico General Electric Power (GE), è stato condannato dalla Corte di Giustizia americana a due anni di carcere per spionaggio di segreti industriali: Zheng inviava sui social foto di paesaggi naturalistici che in realtà contenevano all’interno file riservati rubati alla GE, attraverso una tecnica denominata steganografia[1].

Basta effettivamente verificare la cronaca degli ultimi anni, relativa alle operazioni di cyber spionaggio, per constatare la massiccia attività che la Cina sta sviluppando non solo verso gli Stati Uniti (dove l’attribuzione arriva al 90% dei casi totali) ma anche verso altri Paesi.

Ovviamente il settore delle telecomunicazioni risulta essere particolarmente esposto alle attenzioni delle campagne di cyber spionaggio cinesi, sia come target da colpire sia come vettore per le loro attività di spionaggio. A titolo di esempio vale la pena citare il caso del malware MESSAGETAP, sviluppato nel 2019 dal gruppo di spionaggio Wicked Panda (APT41), sponsorizzato dallo Stato cinese, che monitorava il traffico globale di messaggi SMS selezionando specifiche parole chiave, numeri di telefono e IMSI (*International Mobile Subscriber Identity*), relativamente a target operanti in settori come: difesa, governativo, energia, finanza, trasporti.

Spionaggio elevato a sistema

Un errore da non commettere è considerare il modello di spionaggio cinese simile a quello dei governi occidentali. La

cultura dello spionaggio in Cina ha origini antichissime, si ritrova nella dottrina di Confucio e negli scritti di Sun Tzu. Lo spionaggio è parte del sistema sociale cinese. Ogni cittadino cinese è tenuto a mantenere riservate le informazioni sulla propria attività lavorativa e contestualmente educato a riferire qualsiasi informazione possa essere di interesse per il governo di Pechino; e, nonostante i meccanismi di funzionamento dei servizi segreti cinesi siano noti, rimane ancora incomprensibile come una tale mole di informazioni fornita da miliardi di fonti possa essere vagliata e classificata.

Ancor prima dell'ambizioso piano "Made in China 2015", da oltre 50 anni l'autoritario governo della Repubblica Popolare Cinese ha fortemente investito nello sviluppo delle tecnologie digitali connesse ad Internet, sviluppo che non ha mai rallentato e che ha prodotto una capacità di spiare e applicare una sorveglianza di massa sempre maggiore, che oggi risulta tra le più avanzate del mondo.

Analizzando il tasso di penetrazione della connettività Internet sulle popolazioni degli Stati , notiamo che ad oggi la Cina, nonostante abbia un tasso del 64.1% – di molto inferiore a quello di altri Stati, come ad es. il Nord America con il 93.4% o l'Europa con l'88.4% (fonte Atlas VPN) – con il suo miliardo di utenti in rete è al primo posto in termini di utenti connessi ad Internet, seguita dall'India e con notevole distacco dall'Europa e dagli USA.

L'*e-commerce* nel Paese ha raggiunto un livello di maturità superiore a quello italiano e degli Stati europei. La sua politica autoritaria permette di controllare l'immenso mercato online da oltre 1 miliardo di persone: lo fa addirittura piegando i "modus operandi" dei mercati americani e occidentali, comprese le "Big Tech" GAFA (acronimo di Google, Apple, Facebook e Amazon), alle regole imposte dal governo di Pechino. Ad es. nel 2019 Google, pur di poter essere presente sul territorio cinese, è stato costretto a sviluppare una

versione riveduta e corretta del suo motore di ricerca (progetto Dragonfly) secondo i voleri del governo cinese.

Ma il governo di Pechino è andato oltre, sviluppando i suoi "Gafa" sotto l'acronimo di BAT (Baidu, Alibaba, Tencent). Per avere successo e competere nel mercato cinese si deve utilizzare il motore di ricerca Baidu, primo motore di ricerca in Cina e terzo tra i più usati nel mondo. Baidu è molto di più di un semplice motore di ricerca: è un'enorme realtà tecnologica specializzata in servizi e prodotti, che sta sempre più utilizzando l'intelligenza artificiale nelle proprie soluzioni, diventando di fatto una delle più grandi società mondiali di Internet e intelligenza artificiale.

Alibaba è una piattaforma che opera nel segmento dell'e-commerce, l'equivalente cinese di Amazon; mentre Tencent è il gruppo cinese che, tra le sue varie attività, ha sviluppato e gestisce app di messaggistica e comunicazione come QQ e WeChat, una piattaforma di instant messaging che unisce al suo interno funzioni per lo shopping, prenotazioni, pagamenti digitali, richiesta documenti, etc., estremamente più evoluta dell'americana WhatsApp o Messenger (di proprietà di Meta).

BAT rappresenta uno strumento di cyber spionaggio multifunzionale efficientissimo e sotto il completo controllo di Pechino, in grado di spiare tanto i cittadini cinesi quanto le attività delle aziende estere che commerciano con la Cina e di bloccare qualsiasi informazioni vada contro il pensiero del governo cinese.

La crescita del potere di mercato globale delle società tecnologiche cinesi attraverso le politiche di finanziamento del governo si trasforma in un vantaggio tecnologico anche a grazie ai prezzi particolarmente accessibili sul mercato estero; inoltre, l'applicazione di una politica interna preferenziale nel trattamento dei fornitori nazionali permette il controllo del mercato interno (oltre il 75%) e imbattibili economie di scala. L'influenza cinese nel mercato globale

delle tecnologie è cresciuta anche nelle organizzazioni per la normazione come ad es. ITU, 3G Partnership Project, etc. permettendogli di ricoprire, attraverso i suoi rappresentanti, posizioni decisionali chiave.

TikTok e Social Media: nuove frontiere dello Spionaggio Digitale

E se l'ex NSA Edward Snowden, nel 2019, aveva fatto delle rivelazioni riguardo le piattaforme social come Facebook e Instagram che spiavano gli utenti, anche la Cina sta dimostrando le sue capacità di spionaggio pervasivo di massa ben oltre i suoi confini, utilizzando sofisticate tecnologie di spionaggio cognitivo: in questo senso, uno dei migliori strumenti di *"story telling"* è senza dubbio TikTok.

Nel 2016 la società cinese ByteDance sviluppa l'app Douyin, una piattaforma social, per gli utenti cinesi. L'anno seguente l'app cambia nome in TikTok e la ByteDance acquista l'americana Musical.ly per entrare nel mercato americano, migrando così tutti gli account di Musical.ly su TikTok. L'app di TikTok ha la medesima versione software sia in Cina che nel resto del mondo ma i dati e i contenuti vengono mantenuti su reti separate, per rispettare le restrizioni alla censura dei diversi governi, in particolare quello cinese.

Nonostante questo, nel dicembre 2022 TikTok è arrivato all'attenzione della cronaca internazionale per aver spiato alcuni giornalisti di Forbes che stavano raccogliendo informazioni per degli articoli riguardanti proprio il social network. La vicenda ha poi acceso un riflettore su TikTok, facendo emergere successivamente ulteriori preoccupazioni e indizi di attività di spionaggio governative condotte attraverso la sede in Cina di TikTok, che avrebbe così avuto accesso ai dati degli utenti statunitensi (oltre 100 milioni) e di altri utenti stranieri.

La paura principale è che Pechino, supervisionando tutte le società tecnologiche nel suo Paese, possa richiedere a TikTok, essendo una società cinese, di trasferire all'intelligence nazionale tutti i dati richiesti, senza bisogno di un ordine del tribunale.

Sull'onda sensazionalistica delle vicende di spionaggio di TikTok da parte del governo cinese, a partire dalla metà di marzo 2023, funzionari e rappresentanti dell'UE (Parlamento e Commissione Europea) non potranno più utilizzare TikTok sui propri dispositivi di lavoro. Stessa sorte per i dipendenti del governo canadese (che ha già bandito l'app dai dispositivi mobili governativi) e degli Stati Uniti, dove il Congresso sta inoltre lavorando ad un disegno di legge che potrebbe portare al suo divieto totale entro il 2023.

Oggettivamente TikTok non rappresenta alcun rischio aggiuntivo rispetto ad altre piattaforme come Facebook, Instagram, etc.: TikTok è stata progettata prendendo spunto da quelle americane, migliorata e potenziata in termini cognitivi, cosa che l'ha resa molto più "avvincente" nell'utilizzo, più fluida nella comunicazione e nell'interazione.

Sicuramente anch'essa è in grado di spiare o veicolare disinformazione e probabilmente lo fa meglio delle sorelle americane ma – in questo specifico momento storico – il divieto dell'utilizzo di TikTok nelle istituzioni governative da parte degli USA e degli Stati occidentali ha soprattutto una lettura geopolitica: gli Stati Uniti e l'UE stanno cercando di limitare il potere tecnologico della Cina anche per paura di un suo coinvolgimento nella guerra in Ucraina. Ma questa tensione tecno-politica, soprattutto tra Washington e Pechino, potrebbe portare i governi stranieri a dover scegliere se commerciare con gli Stati Uniti o con la Cina, istituendo una sorta di nuova "cortina di ferro" tecnologica.

Huawei: “forza Cina”

La Cina ha da decenni capito che gestendo la produzione tecnologica del mondo occidentale, che gliel’ha delegata per via dei suoi bassi costi di produzione, poteva sfruttare questa sua posizione per sviluppare politiche di spionaggio su tutti i livelli dell’ambito ICT, dagli utenti finali alle grandi infrastrutture, fino ai governi stranieri.

Uno dei primi casi noti è quello di Huawei. In cinese antico, la parola Huawei significa “forza Cina”: e mai un nome è stato più adeguato a rappresentare un’azienda cinese. Huawei Technologies Co. Ltd è una multinazionale cinese che fornisce tecnologie dell’informazione e della comunicazione (ICT) a più di 3 miliardi di persone in tutto il mondo. Conta oltre 180.000 dipendenti in oltre 170 paesi e nel 2022 ha fatturato 91,53 miliardi di dollari.

Nonostante il successo a livello internazionale, Huawei ha incontrato difficoltà su alcuni mercati stranieri a causa del fin troppo evidente e indebito sostegno statale nonché per via dei suoi stretti collegamenti con il Ministero della sicurezza statale (MSS) cinese, che hanno generato preoccupazioni sul fatto che i dispositivi Huawei potessero consentire attività di spionaggio da parte del governo cinese.

Huawei non produce solamente dispositivi per il mercato *consumer* ma è il più grande produttore al mondo di apparecchiature per le telecomunicazioni di reti infrastrutturali come ad es. *router, switch,* centralini telefonici, etc., quindi sistemi progettati per essere installati anche su infrastrutture aziendali, governative e critiche di un Paese. Le reti di comunicazione di base costituiscono un’infrastruttura fondamentale, con evidenti implicazioni per la sicurezza nazionale. Il fatto che la tecnologia Huawei venga impiegata ad es. per le reti di comunicazione *backbone* implica che Huawei fornirebbe

componenti critici in sistemi di importanza strategica per la società di uno Stato, tra cui i servizi di sicurezza o le funzioni sociali ed economiche principali.

Huawei negli anni ha sollevato diversi sospetti casi di spionaggio: nel 2003 fu accusata dalla CISCO Systems di copia illegale della proprietà intellettuale, avendo immesso sul mercato apparati di *networking* simili a quelli della CISCO sia in termini di hardware che software. Nel 2018 è tornata alla ribalta delle cronache di spionaggio soprattutto per via della tecnologia 5G. Gli intrinseci aspetti tecnologici legati alle vulnerabilità del 5G e i dubbi sul fornitore della stessa, che si traducono nella stretta relazione con gli apparati di intelligence di Pechino, hanno spinto diversi governi a vietare l'utilizzo della tecnologia Huawei.

All'inizio del 2018 il governo australiano vietò a Huawei di prendere parte al lancio dell'infrastruttura mobile 5G per motivi di sicurezza nazionale, esempio seguito poi anche dall'agenzia per la sicurezza nazionale della Nuova Zelanda e dagli Stati Uniti. Nel 2020 il governo di Boris Johnson ha ordinato l'esclusione delle forniture 5G di Huawei in UK, con l'obiettivo di smantellare entro il 2027 l'esistente. Nello stesso periodo, anche l'Italia ha bloccato l'accordo in base al quale Fastweb avrebbe dovuto ricevere da Huawei apparecchiature per la sua rete *core* 5G.

The Big Hack: hardware backdoor nelle supply chain globali

Le posizioni di divieto imposte da diversi Stati nei confronti della tecnologia 5G della Huawei non sono frutto di particolari atteggiamenti paranoici da parte delle agenzie di *intelligence* o della propaganda politica dei governi . In realtà esistono fondate motivazioni per sospettare dei dispositivi realizzati dalle aziende cinesi: e più questi sistemi e dispositivi vanno a occupare ruoli strategici nella

riservatezza delle informazioni di una nazione, più è probabile che l'interesse del governo di Pechino "stimoli" le sue aziende ad operare in modo da acquisire quelle informazioni.

Nel 2018 Bloomberg pubblicò un'inchiesta relativa ad Amazon Inc. che nel 2015 aveva iniziato la valutazione di una startup chiamata Elemental Technologies per una potenziale acquisizione. L'Elemental aveva sviluppato un software di compressione e streaming video che interessava ad Amazon per un suo servizio di entertainment, oggi noto come Amazon Prime Video.

L'Elemental aveva utilizzato il suo software per trasmettere in streaming i Giochi Olimpici, per comunicare con la Stazione Spaziale Internazionale e grazie ad una partnership di sviluppo con In-Q-Tel Inc., società d'investimento della CIA, per la gestione di flussi video di droni alla Central Intelligence Agency. I contratti di sicurezza nazionale di Elemental erano un ulteriore valore aggiunto per le attività governative che Amazon stava implementando per la CIA attraverso la creazione di un cloud sicuro con Amazon Web Services (AWS). Durante l'attività di *due diligence* propedeutica all'acquisizione della Elemental, i consulenti preposti da AWS rilevarono delle anomalie sui server che Elemental aveva venduto ai suoi clienti e che utilizzavano il loro software di streaming video.

In particolare, nei server che i clienti (Dipartimento della Difesa, NASA, CIA, etc.) avevano installato nelle loro reti e che erano stati assemblati per Elemental dalla Super Micro Computer Inc. (Supermicro), società con sede a San Jose in California e tra i maggiori fornitori al mondo di schede madri per server, fu individuato – proprio nelle schede madri – un minuscolo microchip, grande quanto la punta di una matita (Fig.1), che non faceva parte del design originario delle schede.

Amazon segnalò l'anomalia alle autorità, cosa che portò subito l'attenzione delle agenzie di *intelligence* statunitensi ai massimi livelli; FBI e CIA aprirono un'indagine top secret che durò oltre tre anni. Gli investigatori stabilirono che i chip consentivano agli aggressori di creare una backdoor per accedere in modalità *stealth* in qualsiasi rete che includesse le macchine alterate e, seguendo la catena di produzione, gli investigatori scoprirono inoltre che i chip erano stati inseriti in fabbriche gestite da subappaltatori di componenti di produzione in Cina.

Secondo Bloomberg gli investigatori arrivarono alla conclusione che un'unità militare cinese aveva progettato i microchip per assomigliare a comuni *transistor* ma che incorporavano all'interno componenti di memoria, capacità di rete e potenza di elaborazione sufficiente per un cyber attacco; inoltre piccole differenze nella dimensione dei chip "canaglia" rivelavano che la produzione degli stessi era stata fatta in aziende diverse. Il caso fece emergere tutti i timori ipotizzati, cioè che i server della Elemental erano solo alcuni rispetto alle migliaia di clienti che aveva Supermicro in tutto il mondo.

L'inchiesta di Bloomberg rivelò che questa attività di cyber spionaggio altamente sofisticata e orchestrata con successo aveva compromesso silenziosamente la catena di fornitura globale di hardware per computer, infiltrandosi in quasi 30 società statunitensi tra cui Amazon e Apple. Nei mesi successivi molte delle aziende coinvolte negarono i fatti descritti da Bloomberg, ma nessuno mosse mai alcuna azione legale nei confronti della testata .

Questo (presunto) attacco è stato più grave degli incidenti basati su malware e a cui siamo ormai abituati:, gli attacchi basati sull'hardware sono più difficili da realizzare, richiedono ingenti risorse, infrastrutture e soggetti "autorizzati" nella catena di produzione, sono potenzialmente più devastanti, producono effetti a lungo termine e qualsiasi

agenzia di spionaggio è disposta ad investire milioni di dollari pur di ottenere le informazioni a cui possono dare accesso.


Fig 1

Inoltre, a differenza dei software di spionaggio, la manipolazione dell'hardware richiede una pianificazione sofisticata, in quanto lascia tracce nel mondo reale. I componenti hardware hanno specifiche catene di approvvigionamento, bolle di spedizione, fatture, numeri di serie che identificano specifiche fabbriche. Per individuare la fonte dei chip "canaglia", le agenzie di *intelligence* statunitensi analizzarono l'intera *supply chain* di Supermicro fino ad appurare che i tre produttori principali che costruivano le sue schede madri, due con sede a Taiwan e una a Shanghai, avevano subappaltato le forniture a quattro fabbriche già da due anni prima dell'attacco.

Le agenzie di *intelligence* statunitensi, spiando le comunicazioni delle persone chiave delle varie aziende, identificarono quindi come responsabile un'unità dell'Esercito popolare di liberazione specializzata in attacchi hardware. I responsabili delle aziende sub-appaltanti erano contattati da persone che affermavano di rappresentare Supermicro o che ricoprivano posizioni che suggerivano un legame con il governo. Gli intermediari avrebbero richiesto le modifiche ai progetti originali delle schede madri, offrendo anche tangenti in caso di resistenza.

L'episodio causò un notevole imbarazzo diplomatico tra Stati Uniti e Cina, in quanto l'attribuzione dell'attacco, almeno per quanto riguardava la fonte geografica, risultava inequivocabile.

Il Ministero degli Affari Esteri cinese smentì fermamente le accuse di spionaggio e diffuse una dichiarazione che si concludeva in maniera evasiva:

> *“Speriamo che le parti facciano accuse e sospetti meno gratuiti, ma conducano colloqui e collaborazioni più costruttivi in modo da poter lavorare insieme alla costruzione di un cyberspazio pacifico, sicuro, aperto, cooperativo e ordinato”.*

La Cina e il “Cyber Superpower”

Nel recente congresso nazionale del Partito Comunista Cinese, il Segretario Generale Xi Jinping ha sottolineato che i funzionari del PCC che attuano le politiche cibernetiche devono avere una visione “corretta” del cyberspazio perché “le idee determinano le azioni” e che l’aspirazione della Cina è diventare una superpotenza cibernetica, nonché controllare il cyberspazio per proteggere la sicurezza nazionale e come luogo di competizione strategica internazionale.

L’espressione “superpotenza cibernetica” è sia uno slogan politico che un concetto strategico fondamentale in ambito di *cyber warfare* e di guerra asimmetrica [2], ambito in cui la Cina sta focalizzando sempre maggiori risorse. Parte integrante di questa strategia è la costituzione di gruppi di hacker apparentemente indipendenti, ma che spesso rivelano collegamenti con l’Esercito di liberazione cinese (PLA), la Forza di supporto strategico (SSF) e l’*intelligence* cinese.

Ad avvalorare l’ipotesi di forti legami tra questi gruppi e il governo cinese è l’utilizzo delle risorse durante gli attacchi, la collaborazione tra gruppi e i Paesi target, che rivelano un unico profilo comune come attore di minaccia.

Questi gruppi si concentrano quasi esclusivamente su Stati che hanno legami conflittuali con il governo cinese: Paesi occidentali (ad es. Stati Uniti) e asiatici (ad es. Taiwan, Giappone) che sono percepiti come una minaccia politica e industriale per la Cina.

Un’altra caratteristica è che tali gruppi spesso operano congiuntamente e quando un gruppo viene individuato, spesso si ferma e cambia alias (cosa piuttosto inconsueta per gruppi hacker che perseguono un ideologia) e i membri non attivi si spostano ad operare in altri gruppi: questo denota un’organizzazione centrale che dirige le risorse di tutti i gruppi.

Uno studio dell’International Institute for counter terrorism IDC HERZLIYA ha effettuato una classificazione dei gruppi hacker cinesi in base al livello di priorità delle loro attività. Di seguito i principali gruppi operativi in Cina per azioni di cyber spionaggio con evidenti collegamenti all’*intelligence* nazionale cinese.

APT1 aka Unit 61398, Comment Crew: il gruppo, ritenuto collegato al PLA e più specificamente al General Staff Department’s (GSD) 3rd Department, ha capacità che denotano un gruppo numeroso, focalizzato principalmente su obiettivi di tecnologia di difesa e di alta tecnologia, compreso il sistema israeliano Iron Dome, situati in particolare negli Stati Uniti, a Taiwan e in Giappone.

APT3 aka Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110: è considerato uno dei più sofisticati gruppi di hacker cinesi ed è collegato al gigante tecnologico Huawei. Il gruppo, i cui obiettivi includono un’ampia gamma di Paesi e industrie bersaglio, è sospettato di essere finanziato dallo Stato e conduce attività di spionaggio informatico.

APT12 aka Calc Team, DynCalc, DNSCALC, Numbered Panda: il gruppo è focalizzato su varie organizzazioni governative, dei media e dell’alta tecnologia. Nel 2013 APT12 è stato responsabile di una serie di attacchi al New York Times: il gruppo si è infiltrato nelle reti e nei sistemi informatici della testata, esfiltrando dati dei giornalisti e di altri dipendenti. Il mandante fu associato al governo cinese in quanto all’epoca un’inchiesta del New York Times riguardava la

raccolta di miliardi di dollari da parte dei parenti dell'allora primo ministro cinese Wen Jiabao.

APT18 aka DYNAMITE PANDA, TG-0416, SCANDIUM, PLA Navy, Wekby, G0026: gruppo attivo da diversi anni che si rivolge a vari settori come le telecomunicazioni, l'aerospaziale, la difesa, l'alta tecnologia e la biotecnologia. Noto per sfruttare gli exploit zero-day, come nel caso dell'exploit Flash di HackingTeams, è anche sospettato di aver preso di mira il gruppo terroristico Daesh in Iraq nel 2014 per proteggere gli interessi petroliferi nella regione.

APT27 aka GreedyTaotie, TG-3390, EMISSARY PANDA, TEMP.Hippo, Red Phoenix, Budworm, Gruppo 35, ZipToken, Iron Tiger, BRONZE UNION, Lucky Mouse, G0027, Iron Taurus: gruppo cinese finanziato dallo stato, altamente sofisticato, prende di mira gli Stati Uniti, i sistemi di difesa dei Paesi asiatici e la tecnologia dei droni europea.

APT41 aka WINNTI UMBRELLA: gruppo identificato come divisione dell'intelligence cinese. È attivo da molto tempo e i suoi obiettivi principali sono politici di vari Paesi, inclusi Stati Uniti, Tibet, Giappone e Corea del Sud. Il nome Umbrella identifica una raccolta di gruppi di hacker sponsorizzati dallo Stato cinese che include un certo numero di singoli gruppi (tra cui LEAD, BARIUM, Wicked Panda, GREF, PassCV e altri).

ELDERWOOD aka Beijing Group, Sneaky Panda: è un gruppo di spionaggio informatico cinese che sarebbe stato responsabile dell'intrusione di Google del 2009 nota come Operazione Aurora[3]. Il gruppo ha preso di mira organizzazioni di difesa, produttori di catene di approvvigionamento, organizzazioni per i diritti umani non governative (ONG) e fornitori di servizi IT.

HIDDEN LYNX: è stato collegato al Gruppo di Elderwood con una serie di importanti attacchi, inclusa l'Operazione Aurora e

gli attacchi “VOHO” a banche e siti web di servizi, istruzione e politiche pubbliche nel 2012.

DRAGONOK: gruppo di minaccia specializzato nelle organizzazioni giapponesi, noto per gli attacchi con e-mail di *phishing* e l’utilizzo di malware come Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog e NewCT, è stato associato anche al gruppo Moafee con cui condivide stesse tecniche e target.

I limiti del diritto internazionale in tema di spionaggio

L’influenza esercitata sulle aziende cinesi dal governo di Pechino pone la problematica di dover limitare il comportamento della Cina in attività di carattere spionistico anche attraverso la normativa internazionale, al fine di offrire maggiori garanzie di sicurezza ai governi occidentali.

Gli atti di spionaggio all’interno di un Paese in cui si opera sono normalmente puniti in base alla relativa legge nazionale e lo spionaggio in quanto tale non è direttamente disciplinato dal diritto internazionale. Questo, in generale, limita significativamente le azioni legali da Stato a Stato: uno Stato esercita in modo esclusivo la sua sovranità all’interno del proprio territorio e questo include la sua autorità su infrastrutture informatiche, persone e attività informatiche nel suddetto territorio, nel rispetto dei suoi obblighi giuridici internazionali. Di conseguenza, le azioni di uno Stato che ignorano od ostacolano l’esercizio della sovranità di un altro Stato costituiscono una violazione del diritto internazionale.

Affinché una particolare operazione cibernetica di spionaggio venga identificata come violazione della sovranità è però necessario valutare il grado di violazione dell’integrità territoriale dello Stato vittima, nonché il grado di

coinvolgimento dello Stato attaccante nell'operazione di spionaggio: elementi, questi, decisivi per determinare se l'attività costituisca una violazione del diritto internazionale.

La presenza di vulnerabilità (come ad es. backdoor) all'interno di prodotti di aziende cinesi avrebbe quindi poco significato dal punto di vista del diritto internazionale; l'autorità cinese, sui propri affari interni, può imporre obblighi alla propria industria anche a fini di collaborazione con l'intelligence nazionale. Viceversa la sovranità degli Stati occidentali può vietare la vendita e l'utilizzo dei prodotti cinesi sul proprio territorio, rispettando i loro obblighi nell'ambito degli accordi commerciali internazionali, in particolare l'Accordo generale sulle tariffe e il commercio (GATT) dell'OMC che riguarda il commercio internazionale di beni. L'articolo XXI del GATT contiene infatti un'eccezione che consente a una parte di adottare le azioni o le misure *"che ritiene necessarie per la sicurezza".*

Conclusioni

Le notizie sulle cyber minacce rappresentate dalla Cina appaiono regolarmente. La comunità dell'*intelligence* statunitense (IC) ha recentemente presentato la sua nuova valutazione annuale delle minacce 2023[4], identificando come principali minacce informatiche predominanti alla sicurezza nazionale la Cina, la Russia, l'Iran e la Corea del Nord.

Per quanto riguarda la Cina, ancora una volta il rapporto dell'IC conferma che Pechino utilizza una serie di strumenti – dagli investimenti pubblici allo spionaggio – per cercare di far progredire le proprie capacità tecnologiche, proteggere le imprese nazionali dalla concorrenza straniera e facilitare la loro tecnologia per facilitarne l'espansione sul mercato globale . La volontà di Pechino è di utilizzare lo spionaggio, i sussidi e la politica commerciale per cercare di dare un

vantaggio competitivo alle proprie imprese tale da assumere la *leadership* del progresso tecnologico e degli standard mondiali.

Il sospetto sulle capacità e le intenzioni delle cyber minacce cinesi potrebbe portare a un conflitto tra Stati, in particolare tra Cina e Stati Uniti, a causa del ruolo che gli strumenti informatici possono svolgere nelle operazioni militari. Per questo è necessario approfondire alcuni aspetti delle strategie cinesi sulla guerra informatica da una prospettiva diversa rispetto alla narrazione secondo cui la Cina starebbe usando il potere informatico per crescere e infine conquistare il dominio globale.

La Cina di oggi è difficile da definire: ha il capitalismo senza la democrazia, lo sviluppo economico senza libertà politiche, fonde la modernizzazione cosmopolita con il nazionalismo. La più grande economia di mercato a livello mondiale, governata da un regime autoritario che limita la libertà di espressione e non ammette opposizioni.

Questa situazione permette di avere però una guida stabile e di definire strategie economiche e politiche a lungo termine, a differenza degli Stati occidentali dove ormai, da circa 40 anni, assistiamo al continuo avvicendamento delle forze politiche al governo che operano strategie di "sopravvivenza" a brevissimo termine e che, soprattutto, lasciano il completo controllo delle politiche del Paese alle influenze delle lobbies economiche e della finanza, che spesso sono manifestazioni dell'influenza di Super potenze straniere.

L'assoluta centralità che riveste la stabilità nella politica di Pechino si palesa ad esempio in ambito di controllo del cyber spazio. Da quando, negli anni '90, la Cina è rimasta stupita dall'applicazione delle tecnologie delle forze armate statunitensi nella Guerra del Golfo e nelle successive operazioni in Kosovo, Afghanistan e Iraq, ha sviluppato una precisa strategia riguardo l'uso delle tecnologie

dell'informazione nei ruoli più critici, strategia che ha poi per la prima volta esposto pubblicamente nel 2013 con uno studio dell'Accademia delle scienze militari, "*The Science of Military Strategy*".

Uno studio dove veniva affrontata la guerra cibernetica da un punto di vista olistico, dove il cyberspazio diventava un nuovo ed essenziale dominio militare nel mondo moderno. Visione rafforzata nel documento del Ministero della Difesa Nazionale del 2015 intitolato *"China's Military Strategy"* proprio in concomitanza con della pubblicazione del piano decennale *"Made in China 2025"*.

La *"China's Military Strategy"* affrontava per la prima volta il tema della sicurezza informatica in un documento militare ufficiale, definendo il cyberspazio come nuovo pilastro dello sviluppo economico e sociale e nuovo dominio della sicurezza nazionale, dichiarando apertamente che la sicurezza dell'infrastruttura cibernetica cinese era a rischio, poiché la concorrenza internazionale nel cyberspazio stava sviluppando forze militari cibernetiche.

Un altro aspetto fondamentale è che le infrastrutture critiche della Cina, comprese quelle della Difesa, come in tutti gli Stati sono sempre più dipendenti dalle infrastrutture informatiche . Nonostante disponga di un'industria tecnologica su larga scala, potenzialmente in grado di competere con gli Stati Uniti in alcuni settori, la maggior parte delle tecnologie cinesi sono ancora fornite da società statunitensi. Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle e Qualcomm sono le principali aziende da cui la Cina è fortemente dipendente e che cerca di superare con lo sviluppo dell'industria tecnologica nazionale, al fine di rendere più sicura l'infrastruttura Internet interna del Paese: cosa che fa pensare che il suo obiettivo principale nel cyberspazio sia difensivo e non offensivo.

Nei fatti, ad oggi, non esistono prove inconfutabili che

dimostrino che la Cina sia stata coinvolta in cyber attacchi mirati a distruggere altri Stati; mentre lo spionaggio informatico a scopo economico è un'accusa a cui il governo cinese ha spesso risposto motivando le relative attività come rientranti nella sicurezza nazionale, un'azione comunemente condotta anche dalla maggior parte degli altri Paesi.

Come descritto nel documento *"China's Military Strategy*" del 2015, la Cina ha sviluppato una linea guida strategica nel cyberspazio mirata alla difesa attiva e questo comprende anche campagne di cyber spionaggio. La strategia ha quindi come obiettivo principale, nella guerra informatica, quello di migliorare le capacità di difesa per sopravvivere e contrastare un attacco cibernetico offensivo. Nel cyberspazio il principio secondo cui la migliore difesa è l'attacco non è applicabile: infatti nella prima fase di un attacco cibernetico la parte attaccata potrà rispondere con un preciso contrattacco solo se dispone di una forte difesa e l'attaccante, a sua volta, subirà esiti sfavorevoli se la sua difesa non sarà sufficientemente robusta.

Note

[1] Steganografia: evoluzione digitale dell'antica arte di occultare le informazioni, da strumento di riservatezza a strumento di offesa per dispositivi mobili, Francesco Arruzzoli, settembre 2017 (https://www.ictsecuritymagazine.com/articoli/steganografia-evoluzione-digitale-dellantica-arte-occultare-le-informazioni-strumento-riservatezza-strumento-offesa-dispositivi-mobili/)

[2] CYBER-ENABLED INFORMATION WARFARE, Francesco Arruzzoli, aprile 2022, pag. 48 (https://www.ictsecuritymagazine.com/pubblicazioni/quaderni-di-cyber-intelligence-1/)

[3] OPERAZIONE AURORA. STORIA, ANALISI ATTACCO, OBIETTIVI, PERPETRATORI

(https://italiawiki.com/pages/virus-informatico/operazione-aurora-storia-analisi-attacco-obiettivi-perpetratori.html)

[4] ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY, February 6, 2023 (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf)

Profilo Autore

Con oltre 25 anni di esperienza nell’ambito della sicurezza delle informazioni Francesco Arruzzoli è Senior Cyber Security Threat Intelligence Architect presso la Winitalia srl di cui è cofondatore. Si occupa di progettare infrastrutture e soluzioni per la Cyber Security di aziende ed enti governativi. In passato ha lavorato per multinazionali, aziende della sanità italiana, enti governativi e militari. Esperto di Cyber Intelligence e contromisure digitali svolge inoltre attività di docenza presso alcune università italiane.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/threat-actors-made-in-china/