Cina, Russia e USA. Il triangolo del Cyber spionaggio

di Mario Avantini

Il Cyber spionaggio e universalmente riconosciuta come una delle minacce informatiche ad opera di molti governi per rubare informazioni sensibili a Stati esteri e società private. Come afferma Luigi Sergio Germani in un recente contributo dedicato all'argomento: "Lo spionaggio industriale e scientifico è praticato sia da Stati che da attori non statali, esso viene condotto sempre più frequentemente nello spazio cibernetico e mediante le nuove tecniche intrusione informatiche (computer network exploitation o cyber exploitation), tra cui quelle più sofisticate, come APT (Advanced Persistent Threat)" (Germani, p. 19). Per spionaggio industriale si intende "la ricerca informativa occulta tesa all'acquisizione dei segreti industriali e proprietà intellettuali da imprese e centri di ricerca, un fenomeno in forte espansione in tutto il mondo" (Germani, p. 19). "I servizi di intelligence più agguerriti del mondo nel campo dello spionaggio industriale sono probabilmente quelli cinesi e russi. Entrambi stanno potenziando le proprie capacità offensive di cyber espionage al fine di carpire segreti industriali, scientifici e tecnologici in occidente. La Cina e la Russia che si considerano concorrenti strategici degli Stati Uniti e dell'Occidente, puntano ad acquisire (tramite intelligence) le più innovative tecnologie occidentali, allo scopo di modernizzare le proprie economie e apparati militari" (Germani, p. 28).

Bryan Underwood, un diplomatico americano che aveva lavorato presso il consolato degli Stati Uniti nella città di Guangzhou tra il 2009 e il 2011, ha confessato di aver cercato di vendere informazioni segrete al governo cinese. Ma già nel novembre 2011 gli americani accusarono Mosca e Pechino di rubare i loro segreti industriali**,** secondo uno studio intitolato "*Foreign spies stealing Us economic secrets in cyberspace*" presentato al Congresso da Robert Bryant capo dell'Office of the National Counterintelligence Executive. Lo studio presentato cita solo *Cina* e *Russia*, pur sostenendo che siano decine i servizi di intelligence, le aziende, le istituzioni accademiche e i privati cittadini che spiano i segreti americani sul web. **"***I cinesi sono i più attivi e accaniti autori di spionaggio economico"* secondo lo studio americano. Diverse aziende Usa hanno riferito di intrusioni nelle loro reti informatiche che hanno avuto origine in Cina, ma l'intelligence non riesce a risalire sempre ai diretti responsabili. Lo studio americano ammette la *difficoltà di capire chi veramente si celi dietro un cyber-attacco***.** Tuttavia, "Quando un attacco è molto sofisticato, noi presumiamo sempre che ci sia il coinvolgimento di un governo o di un servizio di spionaggio estero", questo e quanto dichiara Robert Bryant.

Ma anche la Russia rappresenta una temibile minaccia. "I servizi di intelligence russi stanno conducendo una serie di attività per raccogliere informazioni industriali e tecnologiche da obiettivi selezionati negli Stati Uniti, e quanto si legge nel report. Come rileva Germani nel succitato articolo: "Esperti di controintelligence da anni manifestano l'elevata aggressività e intensità delle attività informative condotte in tutti i Paesi Occidentali dai servizi d'intelligence russi…..Una delle massime priorità assegnata agli apparati informativi russi è l'acquisizione delle più innovative tecnologie segrete create in Occidente da industrie e istituti di ricerca, soprattutto nei settori indicati dal Cremlino come prioritari per la modernizzazione dell'economia: energia, information technology, telecomunicazioni, biotecnologie e nanotecnologie. Gli apparati informativi russi hanno potenti capacità di spionaggio industriale e scientifico-tecnologico, soprattutto tramite le tecniche di intrusione informatica, ad essi è stato affidato il compito di sostenere con ogni mezzo la modernizzazione economica e

tecnologica della Russia, senza la quale Mosca rischia di non poter mantenere lo status di grande potenza mondiale" (Germani, p. 29-30). Per questo Bryant ha definito il cyber-spionaggio una "minaccia silenziosa per la nostra economia con risultati enormi: segreti commerciali sviluppati dopo migliaia di ore di lavoro dalle nostre menti più brillanti sono rubati e trasferiti alla concorrenza nel giro di secondi".

Secondo gli esperti ed analisti , nel 2013 si moltiplicheranno notevolmente i casi di phishing nei confronti degli enti governativi nonché delle società private in varie sfere del settore imprenditoriale. Sempre più spesso saranno sottoposti a cyber-attacchi i siti di cruciale importanza, per esempio, i siti dell'infrastruttura di pubblica utilità o del sistema di trasporto, ovvero, "le infrastrutture critiche" di ogni Paese. Un report del National science foundation rivela che il governo, le università e le imprese americane hanno speso in ricerca e sviluppo 398 miliardi di dollari nel 2008. Ma non è possibile definire quanto di questo patrimonio sia rubato dalle cyber-spie**.** Da parte sua il Consiglio Nazionale degli USA per l'intelligence ritengono che i magnati di Internet del prossimo futuro accumuleranno nei loro sistemi volumi di informazioni superiori alle banche dati di tutti i governi del mondo. I web tycoon come Google e Facebook potranno controllare immense masse di informazioni in regime on-line. I governi nazionali avranno illimitate possibilità di controllare i cittadini. Ma anche i cittadini potranno lanciare sfide di risposta alle autorità.

Lo scorso dicembre la FireEye, nota società di sicurezza informatica aziendale, ha rivelato una campagna di spionaggio informatico, denominato "Sanny", attribuibile alla Corea del Nord contro obbiettivi Russi. Che dietro le operazioni informatiche della Corea del Nord ci sia qualche sostegno straniero non c'è dubbio, ma chi aiuta la Corea del Nord? La Cina naturalmente! Da indiscrezioni sembrerebbe che gli indirizzi IP (Internet Protocol) da cui sono partiti gli attacchi siano di proprietà della China Netcom, uno dei maggiori fornitori di servizi Internet della Cina. Forse gli hacker della Corea del Nord non sono abbastanza esperti da coprire le loro tracce, per cui gli indirizzi IP sorgente possono essere facilmente catturati, o forse la Corea del Nord è stata usata da hacker di altri paesi o dalla stessa Corea del Sud "ansiosa" di incolpare il suo vicino?

Hacker cinesi sono riusciti a sottrarre i progetti segreti del primo sommergibile nucleare indiano**,** l'INS Arihant. Secondo quanto riportato dal The Indian Express un gruppo di hacker si sarebbe infiltrato nei sistemi informatici del quartier generale del Comando Navale Orientale situato nei pressi di Visakhapatnam. L'INS Arihant rappresenta la punta di diamante della Marina Militare Indiana ed è attualmente in test nella acque circostanti. Ma come tutti ben sanno la missione del sommergibile, una volta entrato in servizio, sarà quella di condurre operazioni nel Mar Cinese Meridionale**.**

Le spie cinesi sono operative anche nella Russia di Putin. In luglio dello scorso anno Svyatoslav Bobyshev e Yevgeny Afanasyev, due professori universitari che lavoravano nel complesso militare-affiliato all'Università Statale Baltic Tecnologica a San Pietroburgo, sono stati condannati a 12 anni e mezzo di reclusione con l'accusa di aver fornito le specifiche di lancio dei Bulava subacquei (missile balistico lanciato dai sottomarini).

Anche qui, non si tratta del primo episodio. Nell'ottobre dello scorso anno, a una settimana esatta dalla visita a Pechino di Putin, il Servizio per la sicurezza statale (FSB, l'ex KGB) annunciò di aver catturato in flagrante una spia cinese mentre stava cercando di acquistare della documentazione top secret sulle tecnologie di produzione

dei sistemi missilistici terra-aria S-300. In realtà l'arresto era avvenuto un anno prima**,** ma venne reso noto solo in prossimità dell'incontro tra l'allora primo ministro russo e Hu Jintao, incentrato sulla questione delle esportazioni di gas verso la Cina.

E' notizia recente che il team di esperti di Kaspersky Lab ad ottobre 2012 ha avviato un'inchiesta a seguito di una serie di attacchi effettuati contro le reti informatiche delle agenzie internazionali, di servizi diplomatici oltre ad istituti di ricerca, società operanti nel settore dell'energia e del nucleare, obiettivi commerciali e aerospaziali, di molti Paesi (tra cui quelle di Stati Uniti, Germania, Israele e Italia). Durante l'indagine sono emerse attività di spionaggio informatico su larga scala. Secondo il rapporto di analisi di Kaspersky Lab, (l'Operazione Ottobre Rosso, chiamata "Rocra") questo sistema di spionaggio era già attivo almeno dal 2007, nel gennaio 2013 sembra ancora attivo. Al momento sono state scoperte 300 vittime, ma si stima che moltissime ancora si aggiungeranno. Non è stato ancora scoperto il server madre, ma la rete Red October si serviva 60 domini diversi. I trojan hanno colpito sia Microsoft Office sia Excel. Sono stati diffusi attraverso delle semplici e-mail. I dati sensibili, poi, una volta rubati vengono criptati e successivamente trasferiti attraverso dei server localizzati in Germania e in Russia. Russa sembra anche l'identità degli hacker. Secondo gli analisti di Kaspersky dietro a quest'attacco informatico potrebbe esserci un governo. E si fa il nome di quello cinese.

Come ha affermato Germani: "I servizi di Intelligence cinesi considerano qualsiasi cittadino cinese residente all'estero come un loro potenziale collaboratore occulto. Si ritiene, inoltre, che i servizi cinesi utilizzino per finalità informative un numero considerevole di connazionali che ogni anno si recano nei paesi occidentali per motivi di studio, per affari o per partecipare a programmi di cooperazione scientifica. Un altro modus operandi è l'utilizzo di migliaia di aziende di copertura aventi sede in Occidente e negli USA, molte delle quali controllate dai militari cinesi, costituite allo scopo di acquisire clandestinamente tecnologie avanzate e segreti industriali. Infine, molto spesso il servizi cinesi mettono sotto sorveglianza molti stranieri che si recano in Cina per motivi professionali (uomini d'affari, scienziati, professori universitari e funzionari governativi), per intraprendere nei loro confronti operazioni di reclutamento. Gli apparati cinesi impiegano le sopra descritte metodologie tradizionali di spionaggio insieme alle tecniche della Cyber-exploitation, al fine di potenziare maggiormente quest'ultime." (Germani, p. 28-29)

Gli apparati informativi cinesi devono stabilire priorità e accettare i rischi sulla scelta di amici e partner, accettando il rischio che siano infedeli, per concentrarsi sugli avversari interni ed esterni; deve decidere cosa fare con amici scomodi come Iran, Corea del Nord, Siria, Pakistan, Venezuela e Sudan. Devono prepararsi all'eventualità che l'enorme potenziale di cyber warfare di cui oggi dispongono in maniera caotica e discontinua non gli sfugga di mano. La Cina deve essere pronta ad uno slittamento da guerra informatica nel campo commerciale e delle informazione a militare.

Akamai Technologies ha pubblicato il Rapporto sullo Stato di Internet relativo al secondo trimestre 2012 (disponibile all'indirizzo www.akamai.com/stateoftheinternet). Basato sulle informazioni raccolte dalla Akamai Intelligent Platform il rapporto offre un'analisi approfondita di dati quali penetrazione di Internet. Attraverso i rilevamenti di un set distribuito di agenti attivi su internet, Akamai è in grado di monitorare il traffico legato agli attacchi informatici e individuare sia i Paesi origine del maggior numero di attacchi sia le porte loro obiettivo. Con il 16% degli attacchi osservati, è la Cina la maggiore fonte per il secondo trimestre 2012, seguita da USA (12%) Turchia (7,6%) e Russia (6,3%). L'Europa è stata responsabile di oltre il 36% del traffico

legato agli attacchi. Mentre lo scorso trimestre il 77% delle azioni malevole si dirigeva su dieci porte in particolare, in questo trimestre la concentrazione di traffico è scesa al 62%, probabilmente a causa di una diminuzione di attacchi alla Porta 445. L'Italia entra al nono posto nella top ten delle nazioni che generano il maggior numero di attacchi informatici, essendo responsabile del 2.1% degli attacchi, in crescita dell'1,9% rispetto al trimestre precedente.

	Country	Q2 '12 % Traffic	Q1 '12 %
1	China	16%	16%
2	United States	12%	11%
3	Turkey	7.6%	5.7%
4	Russia	6.3%	7.0%
5	Taiwan	5.4%	5.3%
6	Brazil	4.6%	4.0%
7	Romania	3.5%	3.0%
8	India	2.9%	3.0%
9	Italy	2.1%	1.9%
10	South Korea	2.1%	4.3%
–	Other	37%	39%

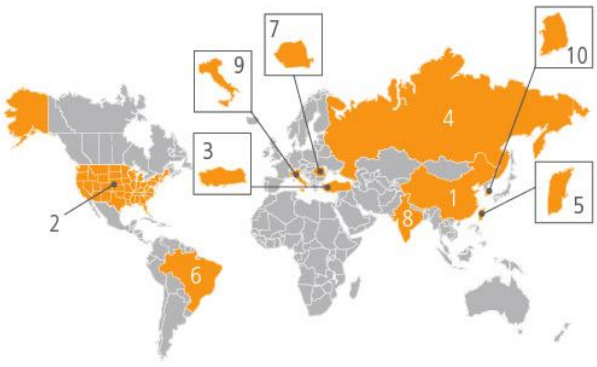

Figure 1: Attack Traffic, Top Originating Countries

Fonte Akamai Technologies

Sono dati rilevati dalla società che attraverso i suoi server gestisce un quinto del traffico globale su internet. E permettono di costruire una mappa che rivela la geografia del web criminale: il 60% degli assalti elettronici parte dalle prime dieci nazioni nell'elenco redatto dall'azienda del Massachusetts.

Concludendo, appare evidente che la rete si presta ad un utilizzo strumentale da parte di attori statuali, terroristici e criminali che potrebbero avere come obbiettivi finali interessi nazionali di rilevanza strategica. Come ha sottolineato Germani nel succitato articolo (p.31-32), per rilanciare la crescita economica di un Paese, occorrerà aumentare in misura consistente il livello di investimento pubblico e privato in ricerca scientifica e tecnologica. Ogni Paese dovrà essere sempre più in grado di rispondere alla domanda di prodotti High-Tech nel mercato internazionale. Di conseguenza nei prossimi anni, è destinata ad assumere una maggiore rilevanza la protezione del patrimonio scientifico, tecnologico e industriale nazionale nei confronti di attività ostili di intelligence specie nelle intrusioni informatiche, non sarà, quindi, più possibile affidarsi alle sole difese di tipo passivo ma occorrerà dotarsi di capacità pro-attive per la condotta di Cyber operation offensive a similitudine di quanto già fatto da altri Paesi, primi tra tutti USA, Cina, Iran ed Israele.

<u>Riferimenti:</u>

http://italian.ruvr.ru/2012_08_31/86767827/

http://news.nationalpost.com/2012/10/04/texas-businessman-charged-with-being-russian-spy-conspiracy-to-steal-u-s-weapons-technology/

http://intelnews.org/2012/10/05/01-1103/

http://www.corrierecomunicazioni.it/tlc/12637_gli-usa-cina-e-russia-rubano-i-nostri-segreti-industriali.htm

http://geopoliticamente.wordpress.com/category/cindia/

Luigi Sergio GERMANI, "Verso una nuova forma di guerra economica: il cyber-spionaggio industriale pilotato da servizi d'intelligence" , pubblicato nel volume *Information Warfare 2011: la sfida della cyber-intelligence al sistema-Italia*, a cura di Umberto Gori e L.S. Germani (Franco Angeli, Milano, 2012)

Report Kaspersky Lab 2013

ONCIX - Office of the National Counterintelligence Executive "Foreign spies stealing Us economic secrets in cyberspace"

Rapporto Akamai – secondo semestre 2012

Fredrik Westerlund , " Russian Intelligence Gathering for domestic R&D – Short Cut of Dead End for Modernization"