Telos PRIMO PIANO SCADA/c
MAGGIO 2013 ANNO V NUMERO 5

Prima scena: Pechino, Autunno 2011. Il Terzo Dipartimento dell'Esercito popolare di liberazione, addetto alla sorveglianza del cyberspazio, sferra un attacco alla rete informatica italiana. L'Unità 61046 (Europa e Medio Oriente) viola la rete italiana dell'Università e della Ricerca, che collega 400 sedi tra Università, laboratori di ricerca, biblioteche e cliniche specializzate. Il bottino: centinaia di *password*, *email*, cartelle cliniche, studi scientifici e profili di docenti. L'FBI, analizzando l'attacco, lo metterà in relazione ad un'operazione di portata più vasta, che definirà *Byzantine foothold*, con vittime eccellenti come il *Massachussets Institute of Technology* e l'Università della California. Seconda scena: Mykolaïv, Ucraina meridionale, 28-31 Dicembre 2011. Un *hacker* penetra almeno sei volte nella rete del Consiglio Nazionale delle Ricerche di Genova, utilizzando un dispositivo portatile. Ogni volta rimane collegato per poco più di mezzo secondo, ma riesce ad inviare tramite i server del Cnr oltre 1 milione di *email*. Messaggi truffa, per lo più, sfruttando server considerati attendibili per aggirare le difese delle vittime e trafugare le loro *password*: una delle attività più redditizie delle mafie russe. Ma la rete del Cnr potrebbe essere stata utilizzata per riciclare denaro o per inviare messaggi riservati, anche a gruppi fondamentalisti in Cecenia. Terza scena: Dubai, Dicembre 2012. Si svolge la *World Conference on International Telecommunications*, che riunisce le Autorità regolatorie di 193 Paesi con l'ambizioso obiettivo di riformare le norme internazionali sulle comunicazioni. Ad organizzarla è un' Agenzia dell'ONU, la *International Telecommunication Union* (ITU). Ma sulla gestione delle risorse fondamentali per il funzionamento di Internet emerge uno scontro insanabile tra il blocco legato agli Stati Uniti, incline a tenere Internet fuori dall'ambito di applicazione del Trattato, e le potenze emergenti come Cina e Russia che rivendicano maggiore autonomia di regolamentazione e controllo della rete. Per rafforzare la censura, accusano gli occidentali. Ma la disputa che va in scena a Dubai è anche e soprattutto espressione di una nuova contesa geopolitica: in discussione è il monopolio dell'assegnazione degli indirizzi sul *web*, gestito da una *partnership* pubblico-privata (Icann – *Internet corporation for assigned names and numbers*) che risponde al Dipartimento del Commercio americano. Spionaggio, affari illeciti, terrorismo, contrapposizione politica esplicita: scenari che credevamo, con la caduta del Muro di Berlino, ormai consegnati alla Storia. Ma la Storia non finisce: l'antagonismo tra grandi potenze non si risolve una volta per tutte nella *pace perpetua*, semplicemente cambiano i protagonisti e i mezzi. La sensazione è che la natura immateriale del mezzo informatico ne moltiplichi la pericolosità per le infrastrutture critiche, militari e civili, cioè per la vita quotidiana di tutti noi. L'Italia e l'Europa sono pronte a raccogliere la sfida? Siamo solo alle prime battute.

l'editoriale *di Mariella Palazzolo*
@Telosaes

CHIESA

LA MINACCIA CHE VERRÀ? INVISIBILE, MA È GIÀ TRA NOI.

> *"Oggi abbiamo a tutti gli effetti una cyber-cortina di ferro: basta vedere cosa è successo a Dubai al forum mondiale dell'ITU, dove le nazioni si sono schierate o dalla parte dell'ICANN o dalla parte dell'ITU, schierandosi di fatto da uno o dall'altro lato di questa cortina invisibile, ma presente. La minaccia è costante, pericolosa, sottovalutata."*

Telos: Fino a pochi anni fa, parlare di *minacce alla sicurezza nazionale* significava evocare l'immagine del terrorista kamikaze, che con il fanatismo sopperisce alla penuria e alla rozzezza dei mezzi. Oggi apprendiamo con sgomento che la principale minaccia alle infrastrutture critiche, militari e civili, viene dalle violazioni dei sistemi informatici. Quale ruolo è destinato a giocare lo spionaggio informatico nelle relazioni internazionali? Sarà l'arma di una nuova, inedita *guerra fredda* tra Occidente e Paesi emergenti?

Raoul Chiesa: La domanda è davvero corretta. Viviamo oramai in un mondo che dipende, quasi interamente, dalla c.d. *Tecnologia dell'Informazione*, altresì chiamata *Information Technology* o *Digital Society*. Senza l'ausilio di sistemi informatici e reti di comunicazione, oggigiorno non è possibile effettuare azioni anche banali, come prenotare un volo o un hotel, prelevare al Bancomat, fare una radiografia o viaggiare su autostrade o reti ferroviarie. La situazione peggiora poi drammaticamente laddove parliamo di centrali energetiche, acquedotti, sistemi di controllo del traffico aereo e così via. Infine, il vero potere di oggi – come scrissi nel lontano 1995 sui monitor di Bankitalia – è l'informazione. Lo spionaggio informatico è già la nuova frontiera dell'*Information Warfare*, anche se io preferisco il termine *Information Operations* (Info-Ops), che rende meglio l'idea. Si attaccano obiettivi strategici non per arrecare dei danni (come invece è successo per Stuxnet, la prima vera e propria *cyber weapon* della storia), bensì per acquisire informazioni a supporto di operazioni militari e di spionaggio. Siamo entrati in questa nuova era, ed oggi abbiamo a tutti gli effetti una cyber-cortina di ferro: basta vedere cosa è successo a Dubai al forum mondiale dell'ITU, dove le nazioni si sono schierate o dalla parte dell'ICANN o dalla parte dell'ITU, schierandosi di fatto da uno o dall'altro lato di questa cortina invisibile, ma presente.

Spionaggio militare, spionaggio industriale, attacco con motivazione ideologico/religiosa, sfida disinteressata, semplice divertimento… È possibile disegnare una mappa del *cybercrime* e dei suoi bersagli? E qual è la reale portata di questa minaccia alla nostra sicurezza?

Il *cybercrime* è il comun denominatore di differenti scenari, motivazioni ed obiettivi. Lo spionaggio militare, così come quello industriale, utilizza tecniche di attacco e strumenti propri del *cybercrime*, ma anche attacchi di *Spear Phishing* e tecniche di *Social Engineering*. Dall'altro lato troviamo invece gli hacktivisti, che sfruttano vulnerabilità abbastanza banali e pubblicamente note. Non si può parlare di *cybercrime* senza occuparsi di *underground economy*, quell'economia sotterranea che fattura, stando alle cifre ufficiali ed al bellissimo report 2012 della russa "Group IB", qualcosa come 12 miliardi di dollari all'anno; parliamo di introiti diretti, di utili insomma, e questa cifra è certamente solo la punta dell'iceberg di un mondo al quale è molto difficile fare i conti in tasca.

Raoul "Nobody" Chiesa è nato a Torino nel 1973. Dopo essere stato tra i primi *hacker* italiani a cavallo tra gli anni '80 e '90, Raoul decide nel 1997 di muoversi verso l'Information Security professionale: fonda @Mediaservice.net Srl, un'azienda di *security advisory vendor-neutral*, con sedi a Torino e Roma.
L'azienda, molto nota a livello nazionale, rappresenta dal 2003 la Training & Certification Authority italiana per l'ISECOM (Institute for Security and Open Methodologies, USA) e le certificazioni professionali OPST, OPSA, OPSE ed OWSE. Raoul è un socio fondatore dell'Associazione Italiana per la Sicurezza Informatica ed è membro, tra l'altro, del gruppo di lavoro Cyber World dell'Osservatorio Sicurezza Nazionale presso il Ministero della Difesa. Nel novembre del 2012 Raoul lascia la guida dell'azienda e fonda, insieme ad un nutrito gruppo di professionisti senior, *Security Brokers ScpA*, un *think-tank* altamente innovativo nel mondo dell'Information Security Consulting di alta fascia, una *cooperativa di cyber esperti* con storie professionali molto differenti e complementari. Dal 2003 Raoul collabora con l'Agenzia delle Nazioni Unite UNICRI, dove lavora all'Hackers Profiling Project ed oggi è *Senior Advisor on Cyber crime Issues*.
Infine, dal 2010 Raoul è membro del Permanent Stakeholders Group presso l'ENISA, European Network & Information Security Agency, sino al 2015. È autore di numerose pubblicazioni, tra cui *"I sistemi di controllo globale: un'analisi approfondita dei casi Echelon ed Enfopol"* (Apogeo 2000), *"Profilo Hacker"* (Apogeo 2007), *"11 Settembre 2021"* (Franco Angeli 2012).

I servizi del *cybercrime* sono noti. Cito i principali: *Phishing*, *Botnet* (per lanciare attacchi DDoS), furto di credenziali (la propria identità digitale, come l'account su Facebook o su Linkedin, ma anche le credenziali *e-banking*), il *carding* (furto di carte di credito e debito), l'*e-laundering* (il riciclaggio di denaro on-line), il gioco d'azzardo non autorizzato dall'autorità nazionale (AAMS), sempre a fini di riciclaggio di denaro sporco. E poi le tecniche di *cash-out*, per trasformare in denaro sonante quelle informazioni digitali che si sono rubate, la rivendita di exploit e di 0days, lo spionaggio elettronico, i siti porno ed il traffico pedopornografico. La minaccia è costante, pericolosa, sottovalutata. In Italia manca decisamente la cultura di base. C'è bisogno di educare, di sensibilizzare, e bisognerebbe iniziare proprio dai più giovani, dalle scuole elementari e superiori, dove studiano i nativi digitali italiani, i figli digitali della generazione Gutenberg, come li ha definiti pochi giorni fa su Repubblica Mariapia Veladiano. Tornando al *cybercrime*, è uscito da poco anche in Italia il libro *Kingpin* dai tipi di Hoepli, per i quali ho curato l'edizione italiana. È uno dei libri più belli che siano mai stati scritti sull'argomento: si legge come un romanzo, sembra un'opera di fantasia ma… è tutto tremendamente vero, a partire dalla rete criminale che ruba le carte di credito in Nord America ed acquista le macchine per stamparle dal lontano Oriente. Una lettura che aiuta a capire la complessità e la globalità di questo nuovo fenomeno e che narra, tra l'altro, la storia (vera) della rapina digitale più importante del ventunesimo secolo.

L'Italia si è recentemente dotata di un nuovo modello organizzativo per la risposta al crimine informatico, che prevede, oltre alla rimodulazione delle competenze istituzionali, anche un maggiore coinvolgimento delle aziende che gestiscono reti strategiche. Quale contributo può dare la collaborazione pubblico-privato nel contrasto al *cyber threat* e quali ostacoli può incontrare?

La cosiddetta PPP è fortemente voluta e sostenuta dalla Commissione Europea, e la stessa ENISA (Agenzia Europea della sicurezza delle reti e dell'informazione) – di cui faccio parte come uno dei tre italiani membri del PSG, il *Permanent Stakeholders Group* – ne ha fatto un cavallo di battaglia. La collaborazione con il settore privato è essenziale: il *cybercrime* si combatte con lo scambio di informazioni, possibilmente in tempo reale, perché il crimine digitale di oggi è globale, non ha frontiere, corre veloce. La scelta italiana con il DPCM del 24 gennaio scorso mi ha lasciato però un po' perplesso. Da un lato, finalmente anche il nostro Paese si è mosso, e tutto fa ben sperare. Dall'altro canto, in certi ambienti questo decreto è già stato soprannominato *il riempi poltrone*. Come da abitudine tutta italiana, prevede la creazione di nuove agenzie, mentre sarebbe forse bastato utilizzare al meglio quello che già c'è, dato che le competenze ci sono, ma sono sparpagliate e mancano di coordinamento. Vedremo cosa accadrà, sono fiducioso.

Da *hacker* a consulente dell'UNICRI: la Sua vita ruota attorno alla sicurezza informatica. Potrebbe spiegarci in che cosa consiste il Suo lavoro e qual è il contributo dell'UNICRI allo sviluppo di una risposta globale alla minaccia cibernetica?

In UNICRI sono un consulente esterno e mi occupo di contrasto al *cybercrime*, insieme a Francesca Bosco, responsabile della *Emerging Crimes Unit (ECU)*. Ho accettato a condizione di lavorare *pro-bono*, esattamente come accade per le mie attività nel PSG dell'ENISA. Vede, quando la tua professione è quella di contrasto alla criminalità informatica, quello che deve guidarti è la passione. La mia vita è, come lei giustamente dice, la sicurezza informatica. In UNICRI iniziai circa nel 2003, quando fui chiamato come docente per un Master in legge, ed iniziai insegnando *electronic crime*. Nel 2004 diedi in dote all'Istituto un progetto *open source* che stavo portando avanti con l'ISECOM (Institute for Security and Open Methodologies) e che si chiama HPP, *Hacker's Profiling Project*. Quel progetto di ricerca, il cui *budget* è da allora pari a zero (!), è ancora attivo, è passato alla fase "*2.0*" e sta andando avanti, seppur con le difficoltà causate dalla mancanza cronica di fondi e di sponsor. Un vero peccato, se considera che il *profiling* nel mondo del *cybercrime* è una scienza completamente nuova: il nostro progetto ce lo invidia il mondo intero, le pubblicazioni ed i libri che abbiamo scritto con i colleghi sono studiate all'FBI Academy di Quantico! Tanto per darle un'idea, quando recentemente un importante dipartimento del Governo italiano ha pubblicato la sua visione sulla sicurezza cibernetica (che brutto termine!) le differenti categorie di *hacker*, i nomi dei profili e persino i testi provenivano proprio dal progetto HPP e dai nostri testi: peccato che nessuno abbia citato l'UNICRI, né fatto un cenno al bellissimo lavoro che portiamo avanti da quasi dieci anni…
In questo periodo in UNICRI ci stiamo occupando dei legami, spesso oscuri, tra il mondo del crimine organizzato, del *cybercrime*, dell'*hacktivism*, e del ruolo svolto da Governi, forze armate e servizi di intelligence. Sono scenari avvincenti, innovativi e di notevole stimolo per tutti i nostri colleghi; forniamo risultati che il mondo intero ci invidia e che saranno utili nel contrasto a nuove forme di criminalità. Spero che, leggendo questa intervista, qualche azienda ed ente di buon cuore, che qualche visionario (alla Steve Jobs) capisca il valore di quanto stiamo facendo e decida di darci una mano.

Telos Primo Piano Scala *c* - Direttore responsabile: Maria Palazzolo. Editore: Telos A&S srl Via del Plebiscito 107, 00186 Roma - Reg.: Trib. di Roma 295/2009 del 18 settembre 2009. Diffusione: protocolli Internet - Isp: Eurologon srl. www.telosaes.it - telos@telosaes.it