Stuxnet

Nicola Cufaro Petroni
USPID – Unione Scienziati Per Il Disarmo
CIRP – Centro Interdipartimentale di Ricerche sulla Pace, Università di Bari
cufaro@ba.infn.it

Stuxnet è un oggetto misterioso legato per due ragioni all'argomento di questa rubrica: infatti esso è da un lato uno dei primi esempi rilevanti di quelle che oggi si usa chiamare *armi cibernetiche*, e dall'altro sembra aver trovato la sua prima applicazione nella lotta che alcuni paesi stanno conducendo contro il programma iraniano di arricchimento dell'uranio e le sue eventuali implicazioni per la *proliferazione nucleare*.

Le armi cibernetiche sono ormai una realtà: il vice-Segretario US alla Difesa W.J. Lynn su *Foreign Affairs* di sett/ott 2010 ha esplicitamente citato il ciberspazio come *quinto dominio* della guerra assieme a terra, acqua, aria e spazio, e nel maggio 2010 il Pentagono ha istituito l'U.S. Cyber Command (USCYBERCOM) con lo scopo di difendere le reti militari americane e predisporre attacchi su quelle considerate ostili. Il presidente Obama ha dichiarato che l'infrastruttura digitale americana deve essere considerata come un valore strategico, ed è ormai opinione diffusa che numerosi settori chiave siano minacciati: banca, finanza, trasporti, manifattura, servizio sanitario, educazione, governo, per non parlare delle forniture energetiche e delle attività militari. *The Economist* dell'1 luglio 2010 stima che ormai da tempo molti paesi (in particolare Cina, Russia, Israele e Corea del Nord) si stanno attrezzando in questo settore, mentre secondo l'espressione dell'ex vice-direttore della intelligence USA M. Hayden alla conferenza per la sicurezza informatica di Black Hat di luglio 2010, "il ciberspazio assume sempre più il ruolo del Bassopiano settentrionale tedesco" celebre durante la Guerra Fredda per essere considerato come la via lungo la quale si sarebbe sviluppata un'ipotetica offensiva delle forze del Patto di Varsavia. E che queste non siano valutazioni pittoresche o esagerate lo mostra proprio il caso dell'attacco *Stuxnet* che R. Obermann della *Deutsche Telekom* ha paragonato sull'*International Herald Tribune* del 28 febbraio 2011 al cosiddetto "Sputnik shock" per aver messo in evidenza la vulnerabilità di tutte le strutture industriali.

Stuxnet, individuato nel giugno 2010 da *VirusBlokAda* (una ditta Bielorussa), è un computer *worm* progettato per attaccare software ed equipaggiamenti industriali. Un *malware* (*malicious software*) è un software programmato per entrare senza autorizzazione e con intenzioni ostili in un computer, e un *worm* è un *malware* autoreplicante che usa una rete per produrre sue copie su altri nodi senza interventi esterni. La prima variante di *Stuxnet* ha cominciato a diffondersi nel giugno 2009, ma la sua diffusione si è accelerata con le versioni successive del marzo-aprile 2010. Il nome è derivato da alcune *keywords* nascoste all'interno del software e trovate dagli analisti che lo hanno scoperto. *Stuxnet* include anche un *rootkit* (un software creato per avere il controllo completo di un sistema senza autorizzazioni) predisposto per un *Programmable Logic Controller*, cioè per computer specializzati nella gestione e controllo di processi industriali, ma in realtà studiato per colpire solo il sistema SCADA (*Supervisory Control And Data Acquisition*) della *Siemens* destinato a controllare processi industriali molto particolari. La *Symantec* che ha esaminato il caso ha dichiarato alla BBC il 15 febbraio 2011 che diverse varianti di *Stuxnet* hanno attaccato fra giugno 2009 e aprile 2010 cinque impianti iraniani con il probabile obiettivo di colpire l'infrastruttura per l'arricchimento dell'uranio che usa equipaggiamenti *Siemens* procurati clandestinamente. L'analisi suggerisce anche che i produttori del *worm* devono aver "infiltrato" le organizzazioni da colpire perché si tratta ovviamente di impianti non collegati a Internet per ragioni di sicurezza. Pertanto l'infezione è

avvenuta presumibilmente tramite chiavi USB inserite manualmente da qualcuno in maniera deliberata o accidentale.

L'attacco *Stuxnet* ha avuto inoltre delle caratteristiche molto particolari discusse in un articolo pubblicato il 17 gennaio 2011 sulla prima pagina dell'*International Herald Tribune*. Da due anni infatti i laboratori di Dimona in Israele sembrano essere diventati la base di un progetto congiunto americano-israeliano inteso a sabotare il programma nucleare iraniano. In particolare essi ospiterebbero numerose centrifughe come quelle di Natanz in Iran, montate allo scopo di collaudare l'azione di *Stuxnet*, e si stima che la ragione dell'efficacia del sabotaggio stia proprio in questi controlli preliminari. Tutto suggerisce che il virus sia stato addirittura prodotto da USA e Israele per sabotare il programma iraniano. Ufficialmente l'autore resta misterioso, ma ci sono molti indizi. All'inizio del 2008 la *Siemens* ha collaborato con *Idaho National Laboratory* (sezione dell'Energy Department responsabile delle armi nucleari USA) per identificare le vulnerabilità del *Process Control System 7*, cioè dei computer di controllo che la *Siemens* vende assieme alle sue macchine industriali. Queste ultime erano state individuate dai servizi segreti americani come parti essenziali proprio del programma iraniano. La *Siemens* afferma che la collaborazione si inquadrava in un lavoro di routine per rendere sicuri i propri prodotti contro attacchi informatici, ma questa esperienza sembra aver dato ai laboratori americani la possibilità di identificare le ben nascoste falle del *PCL-7* che sono state sfruttate da *Stuxnet* l'anno dopo. La parte più segreta del progetto riguardava poi il collaudo del *worm* direttamente su macchine di arricchimento per essere sicuri che producesse l'effetto desiderato. Gli iraniani usano centrifughe *P-1* di provenienza pakistana, e gli israeliani sono riusciti a procurarsene un numero considerevole: la conoscenza della maniera di operare di tali macchine è stata critica per il progetto *Stuxnet*.

Alcuni indizi sembrano suggerire che il *worm* sia stato progettato addirittura solo per Natanz. Nel tentativo di sviluppare un software protettivo R. Langner, di una ditta di Amburgo, ha scoperto ad esempio che *Stuxnet* colpisce solo quando i sistemi di controllo *Siemens* sono in una particolare configurazione che sembra esistere solo per le centrifughe degli impianti di arricchimento. Il *worm* ha due componenti principali: la prima è progettata per far ruotare le centrifughe fuori controllo; la seconda registra segretamente le normali operazioni e le riesegue poi per l'operatore dell'impianto in modo che tutto appaia normale mentre le centrifughe si autodistruggono. Gli attacchi hanno bloccato alcune parti del progetto iraniano, mentre altre hanno superato la prova: non si sa però se ci saranno nuove versioni e nuovi attacchi.

Ovviamente USA e Israele negano recisamente di aver avuto un ruolo nella produzione di *Stuxnet*, ma le loro reazioni danno l'impressione di una grande soddisfazione. Recentemente l'ex-capo del Mossad M. Dagan – contraddicendo recenti posizioni israeliane che davano per imminente la realizzazione di una bomba – ha dichiarato che difficoltà tecniche sembrano aver ritardato il progetto iraniano fino al 2015, e il fattore più importante in questo esito sembra essere stato proprio *Stuxnet*. D'altra parte Israele era alla ricerca di un mezzo che permettesse di bloccare il progetto nucleare iraniano senza ricorrere ad un attacco aperto come in Iraq nel 1981 e in Siria nel 2007. Quando due anni fa gli israeliani pensavano ad una soluzione militare e richiesero agli USA le armi necessarie per un simile attacco aereo che nei loro progetti avrebbe ritardato il programma di tre anni, la Casa Bianca rifiutò. Gli oppositori del programma iraniano concordano ora sul valutare che con *Stuxnet* è stato raggiunto lo stesso risultato di un intervento militare. In novembre 2010 anche M. Ahmadinejad ha ammesso l'attacco affermando che il *worm* è stato scoperto e che i danni sono stati limitati. Un report su *Stuxnet* dell'*Institute for Science and International Security* (Washington) afferma comunque che dalla seconda metà del 2009 a Natanz sono state fermate 984 centrifughe.

Al di là dei commenti più interessati, però, molti analisti hanno comprensibilmente espresso la preoccupazione che queste operazioni possano legittimare una nuova forma di guerra industriale

indiscriminata. Nella sessione speciale sulla cibersicurezza alla 47ª Conferenza sulla Sicurezza di Monaco del 2011 è stato osservato che l'esplosione dell'uso del web negli ultimi 20 anni crea opportunità e rischi. Questo è già successo altre volte nella storia, ma con alcune importanti differenze: entrare in un settore militare come la marina o l'aeronautica costa molto e pone barriere contro i nuovi arrivati. Non succede invece così nel ciberspazio: non solo questo non è dominio esclusivo delle grandi potenze come nel caso di mare, terra, aria e spazio, ma sono proprio i grandi stati che mostrano grosse vulnerabilità a causa della loro dipendenza da sistemi militari ed economici complessi. Per anni gli USA hanno rifiutato di accettare una proposta Russa per qualche tipo di trattato sul controllo degli armamenti nel ciberspazio sostenendo che era necessario interessarsi prioritariamente di cibercrimine. Ora invece il *Wall Street Journal* del 4 giugno 2010 riporta che il generale K. Alexander, capo dell'appena istituito USCYBERCOM ha accettato di aprire trattative con la Russia su una proposta per limitare attacchi militari nel cibespazio: il momento sembra arrivato anche per un trattato in questo settore.

_____

Nicola Cufaro Petroni è un fisico teorico. È stato Segretario Nazionale dell'Unione Scienziati Per Il Disarmo (USPID) ed è attualmente membro del suo Consiglio Scientifico. Aderisce al Centro Interdipartimentale di Ricerche sulla Pace dell'Università *Aldo Moro* di Bari.