

Stuxnet (Iran, 2009) – Il case study per disarticolare la Cyber War

La variabile che identifica l' "ora della morte di Stuxnet" è quella definita nel rettangolo rosso: "00 c0 45 4c 9c 51 cd 01" si traduce al 24 giugno 2012 nel formato standard di data e ora di Windows a 64 bit.

In linea con un mondo che continua ad essere sempre più interconnesso e dipendente dall'efficace funzionamento e dalla resilienza di reti, sistemi e dispositivi informatici – che conferiscono natura ubiquitaria ai contenuti da essi trasportati, elaborati e conservati – l'architettura nazionale cyber ha conosciuto, nel 2017, interventi di modifica miranti a razionalizzare e potenziare ulteriormente le capacità di difesa cibernetica del sistema – Paese. Tale riorganizzazione, in Italia, è stata formalmente declinata nel "Piano nazionale per la protezione cibernetica e la sicurezza informatica", che ha individuato, nell'annesso Piano d'Azione, le misure ritenute più urgenti per rafforzare gli assetti cibernetici del nostro Paese.

Numerosi, però, sono stati gli episodi di guerra cibernetica che si sono fatti spazio ben anche prima del 2017 sulla quarta dimensione, notoriamente indicata come "*spazio cibernetico*", ed intesa come nuova arena della rivalità multinazionale. Nel campo della guerra militare, la storia indicizza, almeno per quanto riguarda il primo millennio, una serie di episodi in cui si è fatto principalmente uso delle armi convenzionali. Con l'affacciarsi ad un mondo del tutto nuovo, dall'introduzione dell'uso di Internet ad oggi, si è progressivamente abbandonato il vecchio sistema per approdare ad uno scenario di guerra non convenzionale, che si avrà modo di disarticolare più avanti.

Dall'analisi di un professionista qual è Umberto Gori, professore Emerito di Relazioni Internazionali all'Università di Firenze, apprendiamo che il primo vero caso di "*cyber war*" e quindi di guerra cibernetica vera e propria, – che non va per ciò solo confusa con "*info war*", la cui traduzione è "guerra informatica" – è rappresentato dall'attacco sferrato attraverso **Stuxnet**: questo è il nome del virus letale iniettato negli impianti della nota centrale di Natanz (Iran, 2009).

Questa valutazione prende vita dal contesto strategico situazionale e parte dall'individuazione di alcuni fattori principali scaturiti dall'attacco subito dagli iraniani:

1. Il target scelto per l'attacco, elemento fondamentale per la realizzazione dell'attacco.
2. Il tipo di azione e gli effetti commisurati ai danni prodotti.
3. Occorre poi una motivazione importante. Sarà questa, insieme all'analisi della complessità dell'azione, che consentirà alla polizia giudiziaria, coadiuvata da un team di periti ed esperti, di pervenire anche ad una prima ipotesi di attribuzione. Saranno dunque le indagini di un Pubblico Ministero che permetteranno di giungere ad un capo d'imputazione. Non sono sempre alte le percentuali con cui viene annunciata una vittoria delle Autorità, ma quasi sempre si punta ad individuare, dopo una serie di accertamenti, l'autore del reato.

Osserviamo meglio quali elementi mette a disposizione l'analisi del caso Stuxnet.

La centrale nucleare è stata classificata dagli iraniani, con una certa facilità, quale target prescelto, cioè quale obiettivo materiale della spedizione militare.

L'azione è stata subito accertata, in quanto ha prodotto evidenti effetti e gravi danni a cose; nel caso di specie la

distruzione materiale delle centrifughe della centrale, anche se resta non accertata la presenza di eventuali vittime. La complessità per la pianificazione e l'esecuzione dell'azione hanno permesso di stabilire un enorme dispendio di risorse economiche e di intelligence, di conseguenza si ravvisa la partecipazione – anche se non dichiarata – di un'entità statale capace di supportarne i costi. Si comincia già da questo dettaglio a ventilare un'ipotesi di "attribuzione".

La motivazione politica è evidente, come si avrà modo di spiegare.

A questo punto, appare altrettanto evidente il valore fondamentale dell'analisi situazionale del contesto strategico nel quale avviene l'attacco cibernetico. La valutazione oggettiva del contesto serve a classificare un atto cibernetico nel suo sviluppo reale e nelle sue finalità. Vediamone alcuni casi, a mero titolo di esempio.

Se l'intento principale di un attacco informatico è la ricerca del guadagno finanziario tramite l'uso di mezzi criminali (come possono essere gli strumenti di phishing o le azioni di furto di identità e dati informatici), il fine ultimo è talmente chiaro che permette di classificare tale condotta come un atto di "cyber crime" o di "cyber espionage".

Se, invece, l'intento dell'attacco è esclusivamente la volontà di arrecare un danno significativo a una Nazione o ai suoi cittadini, l'intrusione informatica subita da infrastrutture civili e/o militari ricadrebbe invece con ogni probabilità nell'alveo di un classico "atto di guerra" disciplinato dallo *jus ad bellum*[1]. Quest'ultima fattispecie, quindi, non risponde alla voce "atti di cyber crime", ma ricade nel più ampio novero di episodi di "cyber war".

Il software dannoso, sviluppato dagli Stati Uniti presumibilmente nel 2010, in collaborazione con lo Stato di Israele, ha seguito uno schema inquadrabile in alcuni passaggi

definiti ed imprescindibili alla realizzazione del suo scopo ultimo.

Stuxnet, una volta iniettato attraverso un dispositivo USB all'interno di un device direttamente collegato alla centrale, rallento`ed accelero`di nascosto i motori delle centrifughe iraniane che venivano utilizzate per arricchire l'uranio, nonché le valvole che a loro volta collegavano sei cascate di centrifughe.

La dinamica è certamente ben più complessa di così e richiederebbe di essere meglio trattata in altra sede, ma fonti iraniane ci riferiscono che, alla fine, i motori si separarono e l'Iran dovette sostituire 1.000 macchine danneggiate. Un ulteriore passaggio risulta, ai nostri occhi, oltremodo fondamentale: mentre stava producendo il danno, Stuxnet, ha fornito un feedback falso agli operatori in modo che non avessero idea di cosa stesse succedendo: l'obiettivo era rendere i cambiamenti così`impercettibili che gli iraniani potessero pensare che la distruzione derivasse da parti del meccanismo guaste, ingegneria difettosa, incompetenza, o tutte e tre le cose. Ralph Langner, che è esperto in sicurezza informatica, è anche fra i primi analisti ad aver decodificato i bit di Stuxnet. Ha stimato che il 50% dei costi di sviluppo del malware sono stati impiegati per nascondere l'attacco.

Un funzionario del governo americano ha dichiarato al New York Times che Stuxnet mirava a "confondere le migliori menti scientifiche iraniane": sebbene gli iraniani avessero ammesso alcune infezioni nei loro sistemi informatici, l'effetto strategico ultimo del malware sul loro programma nucleare è rimasto tutt'oggi poco chiaro. Non di poco momento sono stati, infatti, gli orientamenti della dottrina sulle conseguenze dell'incidente.

Alcuni funzionari del governo degli Stati Uniti hanno affermato di aver rallentato il programma nucleare iraniano di un periodo compreso tra diciotto mesi e due anni. Altri

esperti americani hanno detto che l'attacco non ha contribuito a ritardare gli sforzi iraniani, ed in effetti potrebbe averli accelerati; gli scienziati iraniani hanno infatti lavorato per far funzionare correttamente le centrifughe, migliorandone le prestazioni ed il design, aumentandone la produzione. Il tempo guadagnato dagli attacchi potrebbe dunque essere stato un fattore importante per riportare l'Iran al tavolo dei negoziati e raggiungere un accordo sul suo programma nucleare previsto a luglio 2015.

Il ritardo, anche se pari a ben due anni, ha dato alle sanzioni economiche sul paese piu` tempo per realizzare un impatto notevole sotto diversi punti di vista.

Ed ecco che giungiamo, ora con una certa agilità, alla motivazione politica. A quanto pare la realizzazione del codice velenoso è stato anche un compromesso per convincere Israele a non condurre attacchi aerei contro le strutture iraniane. Nel 2008, Israele avrebbe chiesto all'amministrazione americana, durante il secondo mandato della presidenza di George W. Bush, di preparare bombe in grado di distruggere bunker, sperando di poterle usare nei siti di produzione e di ricerca nascosti nei fianchi delle montagne. Nel respingere la richiesta, il presidente Bush aveva placato gli israeliani dicendo loro che avrebbe autorizzato la missione "Giochi Olimpici" al fine di sabotare l'infrastruttura nucleare iraniana.

La giornalista statunitense Kim Zetter, nel suo libro "Countdown to Zero Day", pubblicato nel novembre 2013, ha analizzato alcuni aspetti dell'attacco ancora poco conosciuti al grande pubblico, riferendosi soprattutto alle interazioni che hanno scatenato una serie d'infezioni tra il 2009 e il 2010. Riprodurre l'infezione, nel caso di Stuxnet, era piuttosto semplice per via di una caratteristica del malware, ovvero la sua capacita` di mantenere un resoconto dei dispositivi compromessi, compresi nome, nome di dominio e indirizzo IP.

Grazie alla particolarità di questi dati di poter essere continuamente aggiornati, è possibile risalire all'originale.

Successivamente, Symantec, leader globale della sicurezza informatica di nuova generazione, nel febbraio 2011 ha pubblicato il dossier "W32 Stuxnet", nel quale è arrivata alla conclusione che la diffusione del malware sia partita da cinque aziende (due sono state attaccate due volte, rispettivamente nel 2009 e nel 2010). Alla fine Kaspersky Lab, fra le più grandi società private di sicurezza informatica, se non prima in assoluto in Russia, è riuscita a risalire a queste aziende grazie all'analisi di 2.000 file in un arco di tempo di due anni.

La prima iterazione di Stuxnet 2009, chiamata anche "Stuxnet.a", venne creata il 22 giugno dello stesso anno. Poche ore dopo la compilazione, il malware aveva già infettato un PC del dominio ISIE. È improbabile quindi, secondo Zetter, che i cyber offensori avessero utilizzato un dispositivo Usb e, soprattutto, sarebbe stato molto difficile, in un lasso di tempo così breve, introdurre il malware nell'azienda colpita.

Sebbene fosse difficile pervenire ad un'identificazione, sospetti concreti suggerivano che si sarebbe potuto trattare di Foolad Technic Engineering Co (FIECO), azienda iraniana produttrice di sistemi automatizzati per l'industria pesante. Stuxnet era caratterizzato da un modulo spyware, per questo Fieco poteva essere un buon obiettivo. Probabilmente i cyber offensori avevano immaginato che potesse essere una scorciatoia per arrivare al vero obiettivo (il sabotaggio della centrale nucleare di Natanz) e dal quale si sarebbero compromessi dati importanti che riguardavano l'industria nucleare iraniana. Nel 2010, l'azienda è stata attaccata nuovamente dalla terza iterazione di Stuxnet.

La seconda vittima è stata attaccata per ben tre volte: a giugno 2009, poi a marzo, infine a maggio 2010.

Il secondo attacco ha scatenato l'epidemia globale Stuxnet 2010, anche nota come "Stuxnet.b".

Il dominio "Bepajoooh" ha permesso di identificare immediatamente la vittima: si trattava dell'azienda "Behpajoooh Co. Elec & Comp. Engineering". Coinvolta anche nell'automazione industriale, era per questo collegata a molte altre aziende. Il 24 aprile 2010, Stuxnet è passato dal dominio Behpajoooh al dominio Mscco. La candidata piu`probabile era l'azienda metallurgica iraniana Mabarakeh Steel Company (Msc). L'azienda utilizzava numerosi PC e ha tutt'oggi connessioni con molte aziende di tutto il mondo. Stuxnet, con tante opportunita`a disposizione, è stata in grado di scatenare una vera e propria epidemia globale: nell'estate del 2010, il worm ha raggiunto anche aziende in Russia e Bielorussia.

Il 7 luglio 2009, Stuxnet ha infettato il PC "appserver" del dominio Neda. In questo caso, non vi sono stati problemi a identificare la vittima: si trattava di Neda Industrial Group, dal 2008 nella lista nera del Ministero della Giustizia statunitense, poiché accusata di esportazione illegale di sostanze proibite in Iran. Oltre a Neda, un'altra organizzazione è stata infettata, la Control- Gostar Jahed Company, anch'essa con sede in Iran. Qui si è fermata la diffusione del malware, nonostante l'azienda avesse un buon portafoglio clienti ed una vasta portata.

L'ultima "vittima zero" va considerata per il grande numero di dispositivi infettati: l'11 maggio 2010, Stuxnet è uscita a entrare in tre computer del dominio "Kala". Si tratta di Kala Electric o anche Kalaye Electric Co. L'azienda è considerata la maggiore produttrice di centrifughe per l'arricchimento di uranio IR-1B nonché uno dei pilastri del programma nucleare iraniano.

In definitiva, di Stuxnet si puo`dire che si sia trattato di un malware incredibilmente produttivo: i suoi creatori hanno

eseguito la piu` grande operazione offensiva a livello mondiale, inaugurando una nuova era nel campo delle armi cibernetiche. Prima di esso, infatti, nessuno aveva pensato di mettere al sicuro le infrastrutture industriali. È risaputo che un metodo efficace è isolare completamente le apparecchiature dalle reti globali. Con la manomissione di dispositivi non connessi, i creatori del worm hanno dischiuso nuovi orizzonti all'Information Security, tanto che l'importanza di Stuxnet puo`essere comparata solo a quella di Great Worm, conosciuto anche come "Worm Morris", il primo malware della storia ad essersi guadagnato l'attenzione dei media e che risale al lontano 1988. Qualunque fosse stato l'impatto sul programma nucleare iraniano, Stuxnet è stato notevole su due fronti.

In primo luogo, era estremamente sofisticato, o, per citare una rivista tecnica, *"senza precedenti, magistrale e malevolo"*. Il malware ha fatto uso di cinque *"zero days"*, ovvero vulnerabilita`software sconosciute che consentono a un utente malintenzionato di accedere a un computer, un router o un server; non avendo mai rilevato prima questi difetti, gli sviluppatori avevano *"zero giorni"* per correggerli.

I giorni zero sono preziosi sia per gli attaccanti che per i difensori: si possono ottenere prezzi a sei cifre pur acquistandoli sul mercato nero e quindi anche un solo attacco particolarmente avanzato, ordinato da uno Stato – Nazione, puo` rivelarsi molto efficace. Inoltre, i computer che controllavano le centrifughe non erano collegati a Internet. Stuxnet ha dovuto saltare questo *"vuoto d'aria"* ed essere consegnato nel sistema, probabilmente tramite una pen – drive o un altro dispositivo portatile.

Il worm è stato anche configurato per funzionare su un sistema specifico: sebbene si diffondesse ampiamente – dati rilevano che il numero di infezioni avesse superato la cifra totale di 300 mila in piu`di cento paesi tra cui Australia, Brasile, Brunei, Cina, India, Indonesia, Paesi Bassi e persino Stati

Uniti – si attivava solo quando “vedeva” una configurazione di una linea di controllori logici programmabili Siemens, e avrebbe perciò distrutto le centrifughe solo dopo averne constatato l'impianto computer a Natanz, il principale impianto di arricchimento dell'Iran.

Stuxnet era solo uno degli strumenti più sofisticati a disposizione degli Stati Uniti e di Israele: altri due programmi, Flame e Duqu, progettati per raccogliere informazioni sulle reti di computer in Iran e in altri paesi del Medio Oriente, sembrano aver fatto anch'essi parte dell'Operazione Giochi Olimpici. Tuttavia, la complessità di Stuxnet va ben oltre la portata dei singoli hackers, in quanto ha indicato il coinvolgimento di interi Stato – Nazione che intendevano danneggiare fisicamente un obiettivo. La parentela con gli altri programmi è la seconda caratteristica degna di nota di Stuxnet e rappresenta un cambiamento epocale strategico.

Prima di Stuxnet, il codice informatico era servito principalmente a rubare o distruggere dati su altri computer; ora, causava il malfunzionamento dell'apparecchiatura. Stava creando risultati fisici prorompenti.

Tuttavia, a differenza di quanto capitava con le armi convenzionali o con quelle nucleari, gli effetti e le regole delle armi cibernetiche erano in gran parte sconosciuti. Non c'era alcuna comprensione delle conseguenze che Stuxnet avrebbe potuto scatenare, anche se c'era il timore che lo stesso tipo di armi avesse potuto, eventualmente, bersagliare gli Stati Uniti.

I dati e le informazioni riportate in questo elaborato dimostrano come la distruzione della centrale nucleare di Natanz abbia rappresentato, per l'Iran in primo luogo, e subito dopo per l'intero asset mondiale, un esempio fortissimo di nuova rivalità: ad aggravare il controllo di un sistema minacciato da un'arma estremamente sofisticata, le cui

dinamiche operative sono ad oggi per alcuni aspetti ancora ignote, ha fatto da supporto un autore invisibile, che opera completamente nell'anonimato. Ciò non solo contribuisce ad aumentare la vulnerabilità della parte soccombente nella singola ipotesi, ma alimenta un clima di incertezza che si dovrebbe in qualsiasi modo evitare. L'obiettivo principe del cyber offensore è infatti quello di realizzare un contesto del genere: incerto, instabile e dove, di conseguenza, può muoversi con una certa disinvoltura.

Note:

[1] Nel diritto internazionale con il termine Jus ad bellum si fa riferimento all'uso legittimo della forza da parte degli Stati; mentre con Jus in bello si rinvia alle modalità con le quali tale uso della forza deve essere messo in atto; lo scontro, seppur legittimo, non deve mai contrastare con i diritti umani che determinano la condotta delle ostilità.

Bibliografia:

- GORI U. e GERMANI L. S., *"Information Warfare. Le nuove minacce provenienti dal cyber spazio alla sicurezza nazionale italiana"*, Franco Angeli, Milano, 2011
- GUASTELLA G., *Il dominio geopolitico dello spazio cibernetico*, Edizioni Ex Libris, Palermo, 2020
- KAPLAN F., *"Dark Territory, The secret history of cyber war"*, Simon e Schuster, 2016
- KISSINGER H., *"Ordine Mondiale"*, Mondadori, Milano, 2014;
- SANGER E. D., *"Confront and Conceal"*, Broadway Paperbacks, New York, 2013;
- SEGAL A., *"The Hacked World Order"*, Public Affairs, New York

Sitografia:

- Sistema di informazione per la sicurezza della Repubblica, *Documento di Sicurezza Nazionale*, Roma, 2017
- Presidenza del Consiglio dei Ministri, *Il linguaggio degli organismi informativi. Glossario intelligence, Sistema di informazione per la sicurezza della repubblica*, Quaderni di Intelligence Gnosis (2012)
- Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* (2013)
- Presidenza del Consiglio dei Ministri, *Piano nazionale per la protezione cibernetica e la sicurezza informatica* (2017)
- DPCM 2013 – Decreto del Presidente del Consiglio dei Ministri (24 gennaio 2013), “*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*”
- DPCM 2017 – Decreto del Presidente del Consiglio dei ministri (17 febbraio 2017), “*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*”

Articolo a cura di **Giulia Guastella**



Giulia Guastella è dottoressa in Relazioni Internazionali. Nel Luglio 2018 si specializza alla Luiss Guido Carli (Roma) con una tesi sperimentale in Studi Strategici, nella quale si approccia per la prima volta allo studio dell'ambiente digitale, tuttavia dando al suo lavoro un taglio internazionalistico che le permette di ricollegarsi al suo percorso universitario. Questo passo le fa da apripista a quello che, di lì a poco, sarebbe stato il suo vivo interesse per la cyber sicurezza e per i rami ad essa affini, muovendosi così tra le Relazioni Internazionali, il Diritto Penale e quello Privato nella tutela della privacy.

Da sempre affascinata dagli studi interdisciplinari, insieme ad un team di colleghi dà vita ad IMESI, un'associazione, nata a scopo benefico, che oggi funge da hub per la ricerca e la formazione post-universitaria. Giulia si interessa anche di Antimafia ed è impegnata nella causa del contrasto alla criminalità organizzata, ragione che l'ha spinta al prosieguo dei suoi studi presso la Facoltà di Giurisprudenza.

<https://www.ictsecuritymagazine.com/articoli/stuxnet-iran-2009-il-case-study-per-disarticolare-la-cyber-war/>