UNIVERSITÀ
DEGLI STUDI
FIRENZE

Scuola di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Triennale in Informatica

Tesi di Laurea

Stuxnet, Flame e Mydoom: analisi dei malware che hanno cambiato il volto della cybersecurity

Stuxnet, Flame and Mydoom: analysis of the malwares that changed the face of cybersecurity

Levi Camillo

Relatore: *Bondavalli Andrea*
Correlatore: *Pietropaoli Stefano*

Anno Accademico 2019-2020

Levi Camillo: *Stuxnet, Flame e Mydoom: analisi dei malware che hanno cambiato il volto della cybersecurity,* Corso di Laurea Triennale in Informatica, © Anno Accademico 2019-2020

Dedicato al nonno Mario, nonna Valeria, abuela Alicia e abuelo José.

"Questa parte della mia vita, questa piccola parte, si può chiamare felicità."
-La ricerca della felicità

INDICE

INTRODUZIONE

Un malware, in sicurezza informatica, è un particolare programma informatico progettato per arrecare danni o disturbare le operazioni che vengono svolte da un utente di un computer, e grazie al quale è possibile sferrare attacchi di varia natura. Col passare del tempo, e col conseguente sviluppo della tecnologia, questi attacchi sono diventati sempre più sofisticati, e sono arrivati ad essere in grado di colpire praticamente qualsiasi dispositivo tecnologico, sia informatico che, come vedremo, fisico. La componente di negligenza umana e la mancata sensibilizzazione in materia di difesa informatica hanno sicuramente giocato un ruolo fondamentale nella diffusione dei malware. La cyber security si trova quindi a dover affrontare attacchi informatici che generalmente possono anche arrivare a sfruttare debolezze non ancora scoperte all'interno dei

dispositivi, rendendo necessaria l'analisi dei malware che vengono man mano scoperti, al fine di trarne insegnamento da porre al servizio della prevenzione futura. In questa tesi ne vengono analizzati tre, grazie ai quali sono stati sferrati attacchi di grande spessore e che si differenziano per il loro fine, oltre che per il quantitativo di danni che sono riusciti a provocare a livello globale. Oltre ad un'analisi del codice e alla loro modalità di diffusione, dei malware in questione vengono affrontate anche le implicazioni giuridiche che questi hanno comportato, e le conseguenze che hanno avuto negli anni successivi alla loro scoperta. Software malevoli creati al fine di condurre un'operazione di spionaggio vengono affrontati in maniera giuridicamente differente da quelli creati per condurre un attacco di tipo denial-of-service, e gli aspetti della carente difesa sui quali inducono a porre l'attenzione le società di cyber sicurezza differiscono a seconda della debolezza sfruttata. La guerra cibernetica, essendo combattuta su un campo non visibile ai nostri occhi, è meno percepita a livello globale, nonostante in certi casi abbia avuto importanti conseguenze sotto vari aspetti, arrivando pure a far nascere il rischio di una vera e propria guerra nucleare.

1

STUXNET

1.1 VERSO STUXNET

Per poter comprendere a pieno l'obiettivo e le implicazioni di Stuxnet è utile inquadrarlo nel suo contesto storico e capire quali fatti portarono alla sua creazione, in particolare analizzando gli anni in cui prende forma il programma nucleare iraniano.

In seguito all'uso del 1945 delle bombe nucleari "Little Boy" e "Fat Man" sulle città giapponesi di Hiroshima e Nagasaki, rispettivamente, gli Stati Uniti lanciarono un programma noto come "Atoms for Peace" [1], un'iniziativa nata dal presidente Eisenhower. Uno dei tanti obiettivi del programma era quello di scoraggiare lo sviluppo e l'impiego di armi nucleari, rendendo al contempo gli Stati Uniti una potenza nucleare di prim'ordine. Il 5 marzo 1957 lo scià iraniano Mohammad Reza Shah Pahlavi stipulò un accordo con gli Stati Uniti nell'ambito di Atoms for Peace per la "proposta di accordo per la cooperazione nella ricerca sugli usi pacifici dell'energia atomica"[2].

Nel corso dei vent'anni successivi, l'Iran proseguì con l'obiettivo di creare centrali nucleari sempre più avanzate. Il Centro di ricerca nucleare di Teheran (TRNC) venne fondato nel 1967 e ebbe come suo fulcro principale di ricerca un reattore da 5 megawatt creato negli Stati Uniti. Il reattore era conosciuto come Tehran Research Reactor (TRR) e consumava uranio altamente arricchito

[1] "How Iran Went Nuclear," New Statesman, Giugno 22, 2009.
[2] Greg Bruno, "Iran's Nuclear Program," Council on Foreign Relations, Marzo 10, 2010.

come fonte di combustibile[3]. Una parte importante dell'accordo che permise all'Iran di ricevere il sostegno nucleare dagli Stati Uniti fu la firma del Trattato di non proliferazione delle armi nucleari (TNP). Questo venne firmato nel 1968, concedendo così agli Stati Uniti di tenere sotto osservazione il programma nucleare iraniano da parte dell'Agenzia Internazionale per l'Energia Atomica (AIEA)[4]. E' importante notare che questi passi avanti per l'Iran trasformarono la nazione in una potenza mondiale sotto questo aspetto, e tutto ciò fu fonte di grande orgoglio per il governo iraniano, a tal punto che lo scià volle espandere ulteriormente il programma facendo progetti per altre ventitré centrali nucleari. L'obiettivo fu quello di rendere operative queste stazioni aggiuntive entro il 2000, poiché si temeva che le riserve di petrolio sarebbero state molto limitate negli anni successivi[5]. Per raggiungere questo obiettivo, fu necessario stipulare accordi con importanti società.

Nel 1975 l'Iran firmò un contratto con la Kraftwerk Union, una compagnia che faceva da tramite tra la multinazionale Siemens AG e la Allgemeine Elektrizitäts-Gesellschaft(AEG), del valore di 4-6 miliardi di dollari. Il contratto descriveva i dettagli di un impianto nucleare che avrebbe ospitato due reattori ad acqua

[3] "Tehran Nuclear Research Center," The Institute for Science and International Security.
[4] 6. Greg Bruno, "Iran's Nuclear Program".
[5] Sam Sasan Shoamanesh, "History Brief: Timeline of US-Iran Relations until the Obama Administration," MIT International Review.

pressurizzata da 1.196 MW, da completare entro il 1981[6]. Il vicecapo dell'ambasciata americana a Teheran, Jack Miklos, evidenziò alcune preoccupazioni inerenti agli obiettivi inizialmente prefissati, a causa dell'incapacità dei funzionari iraniani di spiegare come l'Iran avrebbe utilizzato i 23.000MWe di potenza che si sarebbero aggiunti nei venti anni successivi: non vi era la necessità di possedere così tanta energia[7]. Le sue preoccupazioni si fecero più grandi quando lo Scià fece intendere che l'Iran sarebbe stato pronto a creare armi nucleari in caso le nazioni sprovviste avessero fatto lo stesso. Alle parole dello Scià seguì un test nucleare indiano nel 1974, noto come Operazione Buddha Sorridente: fu la prima esplosione dovuta a test nucleari condotta da una nazione che non faceva parte dei cinque membri permanenti del Consiglio di Sicurezza delle Nazioni Unite[8].

Gli Stati Uniti decisero che ulteriori accordi e vincoli per gli iraniani, riguardo il programma nucleare, erano necessari per poter gestire una rete multinazionale di impianti e di centrali. Conseguentemente l'Iran ritenne che la politica degli Stati Uniti fosse eccessivamente restrittiva, ed espresse una forte preoccupazione riguardo alla presenza di una sorveglianza estera segreta nelle proprie strutture. Nonostante questi attriti, nel marzo 1978, sotto la presidenza di Carter, fu firmato un accordo

---

[6] Henry U. Ufomba e Robert O. Dode, "Which Way to Tehran? Pre-emptive Air Strike Cumulative Diplomacy, Technical Isolation and the Iranian Nuclear Crises," Journal of Public Administration and Policy Research 2, (2010).
[7] William Burr, "A Brief History of US-Iranian Nuclear Negotiations," Bulletin of the Atomic Scientists.
[8] "Smiling Buddha: 1974,"
http://nuclearweaponarchive.org/India/IndiaSmiling.html.

che permise agli Stati Uniti di porre il veto al ritrattamento del combustibile nucleare esaurito[9]. L'accordo causò tensioni in Iran tra i funzionari del governo, che ritenevano che lo scià avesse soddisfatto in larga misura i desideri dell'Occidente.

Nel 1979 la situazione cambiò radicalmente: la rivoluzione iraniana dello stesso anno si concluse con il rovesciamento del potere e la sostituzione dello scià con l'Ayatollah Ruhollah Khomeini.

La nuova repubblica islamica causò ulteriori preoccupazioni per l'Occidente riguardo allo stato del programma nucleare iraniano. Negli anni successivi gli accordi tra l'Iran e varie società, tra cui la Kraftwerk Union AG, vennero in gran parte considerati nulli senza alcun rimborso di denaro versato al governo iraniano, e trovò molte difficoltà nell'ottenere il sostegno per la costruzione di nuove centrali nucleari. Eppure, negli anni '90 l'Iran stipulò un accordo con la Russia per acquisire esperti e tecnici russi, in aggiunta a informazioni riguardanti l'energia nucleare, e nel 1995 firmò un contratto con lo scopo di terminare l'impianto di Bushehr, dotato di un reattore ad acqua pressurizzata da 915 MWe[10].

Oltre all'impianto di Bushehr, l'Iran lavorò alla creazione di un accesso sotterraneo all'impianto di Natanz. Nel 2002, un gruppo dissidente noto come "Consiglio nazionale di resistenza dell'Iran"

[9] William Burr, "A Brief History of US-Iranian Nuclear Negotiations.".
[10] Adam Tarock, "Iran's Nuclear Programme and the West,".

rivelò l'esistenza dell'impianto di arricchimento dell'uranio a Natanz[11].

La tensione tra l'Iran e l'Occidente raggiunse il massimo storico nel 2006, quando il presidente iraniano Mahmoud Ahmadinejad confermò che l'Iran aveva completato il suo obiettivo di arricchimento dell'uranio. L'annuncio ebbe un impatto molto negativo su un grande numero di paesi, tra cui ovviamente gli Stati Uniti.

Il presidente George W. Bush dichiarò che la crescente minaccia del governo iraniano riguardo l'arricchimento dell'uranio doveva essere affrontata con forti conseguenze[12].

[11] Greg Bruno, "Iran's Nuclear program.".
[12] President George W. Bush, "President Bush Addresses American Legion National Convention," The White House, http://georgewbushwhitehouse.archives.gov/news/releases/2006/08/20060831-1.html .

Gli Stati Uniti, oltre a essere il paese che con maggior forza si oppose a queste dichiarazioni, fu anche l'unico ad avere la possibilità di osservare l'Iran da così vicino.

La risposta alle dichiarazioni iraniane venne creata segretamente, e uscì allo scoperto solamente nel giugno del 2010.

1. Centrale nucleare di Natanz, Iran.
https://www.bbc.com/news/world-middle-east-11927720

1.2 STUXNET E LE SUE VITTIME

Il 17 giugno 2010 i ricercatori della società di sicurezza informatica bielorussa VirusBlockAda ricevettero una segnalazione riguardo ad un nuovo malware da parte di un cliente iraniano, dopo che quest'ultimo aveva riscontrato involontari e continui riavvii su un server Simatic WINCC, programma creato dalla Siemens per sistema operativo Windows che fa da human-machine interface (HMI) per il funzionamento e la modifica di controllori logici programmabili (PLC), i quali sono ancora presenti in molti ambiti scientifici tra i quali reti di comunicazioni satellitari, impianti di raffinamento petroliferi e centrali di arricchimento nucleare[13].

Dopo un primo esame, i ricercatori della VirusBlockAda identificarono un potenziale malware zero-day, e decisero di informare la Microsoft, che analizzò 1 MB di codice binario (20 volte più grande di quello di qualsiasi altro malware mai esaminato fino ad allora), riconoscendone l'enorme complessità[14].

[13] 18. Joe Weiss (leading control systems cyber security expert), intervista telefonica, Giugno 2, 2012.
[14] 19. Bruce Dang, "Adventures in Analyzing Stuxnet," (presentation at 27th Chaos Communication Congress, Berlino, Germania, Dicembre 27-30, 2010).

Risultarono un totale di quattro vulnerabilità zero-day di Windows, un numero senza precedenti nella storia dell'analisi di un singolo malware, e il fatto che infettasse Windows XP, Vista e Windows 7 permise una rapida e subdola diffusione. Gli venne assegnato il nome Stuxnet, vista la frequente presenza delle keywords ".stub" e "mrxnet.says" [15].

Oltre agli zero-day exploits i ricercatori si accorsero che Stuxnet possedeva tante altre caratteristiche e funzionalità al suo interno, tra cui rootkit Windows, un network di controllo remoto, possibilità di aggiornamento peer-to-peer, certificati e licenze digitali, varie tecniche di elusione degli antivirus[16]. In particolare, il rootkit serviva a Stuxnet per poter introdursi nuovamente in un dispositivo che eventualmente fosse già stato ripulito dallo stesso. Il collegamento network dava la possibilità di poterlo controllare ed aggiornare da remoto, e in caso di assenza di rete avrebbe potuto comunque farlo grazie al sistema peer-to-peer installato al suo interno. I certificati e le licenze digitali permettevano l'installazione dei driver nei vari dispositivi, ed è proprio grazie a questa ultima caratteristica che Stuxnet era in grado di iniziare l'attacco ai sistemi, trasferendo il proprio codice all'interno di questi.

---

[15] Zetter, Kim (11 July 2011). "How digital detective deciphered Stuxnet, the most menacing malware in history" arstechnica.com .

[16] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier,"Symantec Security Response.

Il complesso insieme delle caratteristiche di cui sopra è stato scoperto essere solo una parte del malware. Dall'analisi fatta al codice emerse infatti che poteva essere suddiviso in due parti fondamentali: il weapon system e il payload.

Il weapon system permetteva a Stuxnet di introdursi all'interno dei sistemi e di propagarsi attraverso la rete sfruttando le vulnerabilità zero-day, e una volta che il malware avesse infettato un dispositivo, era lui stesso a verificare che fossero presenti certi parametri prima di iniziare la fase di payload. In particolare, Stuxnet avrebbe iniziato questa fase solamente nel caso in cui si fosse trovato su un dispositivo di controllo dotato di un Siemens Process Control System 7 (PCS). In caso contrario, sarebbe rimasto semplicemente all'interno del dispositivo infettato, senza agire.

La parte di codice che rendeva Stuxnet una vera e propria arma cibernetica, e non un semplice malware avanzato, era quella riguardante il payload. Attraverso una complessa decodifica venne infatti scoperto che i dispositivi di controllo sui quali era previsto che Stuxnet iniziasse la fase di payload si trovavano nella centrale di arricchimento di uranio situata a Natanz, in Iran.

La conferma di questa ipotesi arrivò a seguito dell'analisi di una foto pubblicata sul sito del governo iraniano, che ritraeva il Presidente dell'Iran nella centrale di Natanz assieme ad alcuni ingegneri. Oltre ai soggetti immortalati, la foto comprendeva anche una parte di schermo di un calcolatore del laboratorio che in quel momento mostrava la disposizione delle centrifughe necessarie all'arricchimento nucleare[17].

L'esperto di Stuxnet Ralph Langner si accorse del dettaglio fotografico, e indagò sulla presenza di analogie tra il codice del malware, il modo in cui era previsto che attaccasse e le centrifughe rappresentate in foto. L'intuizione coincideva perfettamente con la strategia d'attacco del malware[18].

Inizialmente Stuxnet effettuava dei controlli per assicurarsi che si trovasse su un dispositivo di controllo delle centrifughe di gas di Natanz.

[17] "Visit to Natanz Facility," 2011 Presidency of the Islamic Republic of Iran, Aprile 8, 2008.
[18] Ralph Langner, "Stuxnet: A Deep Dive," (presentation at Digital Bond's SCADA Security Scientific Symposium, Miami, Florida,Gennaio 19-20, 2012).

Successivamente avviava parti di programma per capire se le condizioni fossero quelle previste per iniziare l'attacco; infine, se queste fossero state corrette, avrebbe fatto girare le centrifughe ad una velocità molto superiore rispetto a quella prevista, per poi farle rallentare di nuovo. La velocità di rotazione che Stuxnet prevedeva di far raggiungere corrispondeva a 1410 Hz, numero che coincideva precisamente con l'inizio del punto di rottura di quelle specifiche centrifughe, e ciò richiedeva una enorme competenza in materia da parte dei programmatori del malware. In più, Stuxnet faceva in modo che i display dei dispositivi di controllo non mostrassero nessuna anomalia agli occhi degli ingegneri.

2. Foto che ritrae il Presidente Ahmadinejad insieme agli ingegneri di Natanz, con relativi dispositivi per il controllo delle centrifughe.
https://www.infosecisland.com/blogview/18647-Photo-Shows-Stuxnet-as-Perfect-Match-to-Iranian-Network.html

Gli esperti convennero che i creatori di Stuxnet dovessero avere una conoscenza molto approfondita della struttura fisica di Natanz per riuscire a sferrare un attacco così mirato in assenza di ausilio di controlli da remoto e, soprattutto, di una connessione di rete, dal momento che l'obiettivo del malware si trovava una zona schermata e isolata. Che i programmatori di Stuxnet avessero un contatto all'interno della centrale o che fossero riusciti ad ottenere informazioni tramite dispositivi elettronici di qualche tipo, gli esperti concordarono sul fatto che in entrambi i casi si trovassero in presenza di un livello di dedizione e di spionaggio che fino a quel momento non erano mai stati visti.

In aggiunta, per sapere esattamente come i PLC avrebbero reagito ai codici e alle istruzioni di Stuxnet, i creatori dovevano essere tra i migliori programmatori di PLC al mondo: il payload era così dettagliato e preciso che richiedeva un livello di conoscenza del PLC superiore a quello che possedevano gli stessi ingegneri iraniani di Natanz[19].

[19] Ralph Langner (leading Stuxnet expert), discussion with author, 11th Control System Cyber Security Conference, Washington DC, Ottobre 17-21, 2011.

Le analisi degli exploits usati in Stuxnet mostrarono che l'infezione all'interno della centrale iniziò attraverso un dispositivo USB, e non si seppe mai se fosse stato utilizzato da un ignaro dipendente della struttura o se invece appartenesse ad una spia [20]. E' stato scoperto che, in ogni caso, il malware era all'interno della rete iraniana già da giugno 2009, e ciò risultò essere coerente con la routine di attacco di Stuxnet. Il payload era stato progettato per degradare lentamente le centrifughe durante un determinato lasso di tempo, e non per attaccarle e distruggerle istantaneamente, indice del fatto che si voleva tener nascosto il malware per la maggior quantità di tempo possibile[21].

[20] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet.Dossier.".
[21] Ralph Langner, "Stuxnet: A Deep Dive.".

3. Foto che ritrae il Presidente Ahmadinejad all'inaugurazione dell'apertura della centrale nucleare di Natanz, mentre cammina tra le centrifughe per l'arricchimento nucleare. https://www.voanews.com/middle-east/iran-plans-nuclear-equipment-upgrade

Gli esperti credettero che Stuxnet fosse in fase di sviluppo e di testing intorno al 2007, per poi aver colpito i suoi ultimi obiettivi nel 2009[22]. Inizialmente, il governo iraniano affermò che non erano presenti infezioni.

[22] Elizabeth Montalbano, "Stuxnet, Duqu Date Back to 2007, Research Says,".

Quando Stuxnet venne scoperto, lo stesso governo disse che non risultavano danni da parte del malware. Solo successivamente, il 29 novembre 2010, il Presidente dell'Iran Ahmadinejad ammise che Stuxnet aveva infettato le strutture nucleari iraniane e che aveva apportato danni al programma nucleare in generale prendendo di mira le centrifughe[23]. Le immagini satellitari e le indagini della Indian Exhibition Industry Association (IEIA) indicarono che almeno 1000 centrifughe delle 9000 presenti a Natanz vennero danneggiate da parte di Stuxnet[24].

L'attacco informatico Stuxnet non è stato solo uno dei più avanzati malware mai lanciato, ma anche il primo noto a provocare la distruzione di infrastrutture fisiche al di fuori di un ambiente di prova controllato. La protezione delle infrastrutture sensibili fu un argomento molto dibattuto a livello nazionale intorno al 22 maggio 1998, quando la Casa Bianca pubblicò direttive volte all'incremento della difesa delle suddette infrastrutture[25]. Fino alla scoperta di Stuxnet, una tipologia di attacco del genere non era mai stata resa pubblica, e le sue implicazioni furono molto importanti, spingendo ricercatori di cyber sicurezza e programmatori di sistema ad approfondire certi aspetti della difesa.

---

[23] William Yong and Robert F. Worth, "Bombing Hit Atomic Experts in Iran Streets," The New York Times, 29 Novembre 2010.
[24] David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Institute for Science and International Security, 22 Dicembre 2010.
[25] "Presidential Decision Directive/NSC-63," The White House, 22 Maggio 1998.

Stuxnet mostrò che attacchi all'interno del cyberspace potevano essere precisi e distruttivi tanto quanto quelli sferrati in veri e propri campi di guerra.

1.3 CONSEGUENZE DI STUXNET

Stuxnet è stato il primo esempio pubblicamente riconosciuto di cyber-arma utilizzata per attaccare macchinari industriali. Ha fornito ai ricercatori una strada da seguire per comprendere più dettagliatamente come può essere condotto un cyber-attacco mirato, e del tutto innovativo, contro un oggetto fisico sensibile[26]. Nello specifico, ha mostrato come poter infettare un dispositivo in tempo reale, sovrascriverne il codice in fase di esecuzione e mostrare all'esterno dei dati falsi che non destassero sospetti. Tutto ciò ha costituito un sostanzioso patrimonio di nuove conoscenze riguardanti la cyber-sicurezza, che oggi è consultabile e alla portata di tutti.

[26] Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security."

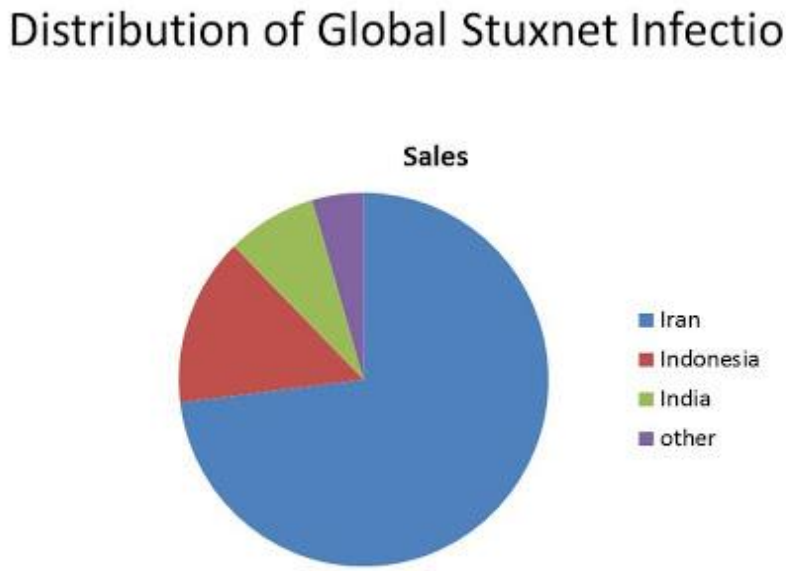
Le opinioni su come Stuxnet si sia diffuso, per arrivare a colpire la centrale di Natanz, sono contrastanti. L'autore David Sanger sostiene che un errore nel codice del malware stesso abbia permesso di infettare il computer di un ingegnere che lavorava all'interno dell'impianto iraniano, il quale, collegandolo alla rete internet, ha permesso al virus di replicarsi e diffondersi anche in altre località del mondo[27].

Il dossier della Symantec riguardante Stuxnet attribuisce invece la diffusione del malware ai suoi metodi programmati di replicazione, sostenendo che le macchine infettate all'esterno dell'impianto di Natanz fossero un effetto collaterale voluto dai programmatori stessi allo scopo di accertarsi che il virus arrivasse al suo obiettivo[28].

Il gruppo Langer teorizza che i creatori di Stuxnet avrebbero riconosciuto in precedenza i lati positivi dello smascheramento del malware, e che ciò fosse perfino compreso nella fase finale dell'intera operazione, al fine di mostrare al mondo intero le potenzialità di cyber-armi create e gestite da individui competenti[29].

---

[27] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."
[28] Falliere, Murchu and Chen, "W32.Stuxnet Dossier"
[29] Langer, "To Kill a Centrifuge"



4. Grafico che mostra la diffusione di Stuxnet a livello globale
http://www.berghel.com/col-edit/security_wise/su11/sw_su11.php

Indipendentemente dalla causa principale della diffusione di Stuxnet, risulta che ad oggi il codice è consultabile e disponibile pubblicamente, e conseguentemente può essere modificato e affinato per sferrare ulteriori attacchi informatici[30].

[30] Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security."

Il generale statunitense Mike Hayden, ormai in pensione, durante un'intervista alla CBS News disse: "Siamo entrati in una nuova fase di conflitti, quella in cui creiamo e utilizziamo cyber-armi per recare danni fisici e, in questo caso, distruzione di infrastrutture critiche appartenenti ad altri paesi[31]". Il professor Paul Dorey, dell'Università di Londra, afferma che presumibilmente ogni forma di conflitto tra nazioni che si terrà in futuro includerà attacchi alla rete informatica del nemico, con l'obiettivo di inibire la difesa stessa[32]. Questo testimonia l'importanza delle partnerships tra settori informatici controllati privatamente e le agenzie governative di cyber-difesa. Il worm Stuxnet è stato la prima cyber-arma, pubblicamente riconosciuta, ad aver recato danni fisici ad una struttura attraverso l'uso della programmazione informatica, in una modalità che fino ad allora era possibile portare a compimento solamente tramite impiego di armi o sabotaggi manuali[33]. Ricercatori come il tedesco Ralph Langer credono che Stuxnet abbia aperto il "Vaso di Pandora" per i conflitti cyber, e che la sua influenza aumenterà col tempo, sostenendo inoltre che la futura generazione di malware, che con tutta probabilità si ispireranno al modello di Stuxnet,

[31] Kroft, "Stuxnet: Computer Worm Opens New Era of Warfare."
[32] "Cyber Terror Targets Utilities," May 31, 2012, http://www.news24.com/SciTech/News/Cyber-terror-targets-utilities-20120531
[33] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

sarà ancora più dannosa e complessa da neutralizzare[34]. Nel giugno 2012, il Presidente del Comitato di Intelligence della Camera dei Rappresentanti degli Stati Uniti Mike Rogers sostenne davanti alla CBS News: "Subiremo un attacco informatico catastrofico. Il tempo sta per scadere"[35]. Molte delle agenzie private di intelligence sono state costrette a rallentare il loro sviluppo in modo da poter aggiornare le misure di sicurezza del proprio settore informatico, alcune delle quali risalenti a trenta anni fa[36].Nonostante la sofisticatezza organizzativa di Stuxnet, l'attacco a Natanz non sarebbe stato possibile senza l'ingenuità di una componente umana[37]. Il primo fallimentare punto difensivo che ha portato alla diffusione del malware è stato l'accesso diretto all'interno della centrale iraniana tramite un dipendente. Stuxnet è stato progettato per essere trasportato a mano nell'impianto di Natanz, dal momento che i computer della struttura erano gestiti da un sistema chiuso, privo di connessione internet e non accessibile. Ciò richiedeva l'introduzione fisica tramite un dispositivo, un'unità removibile corrotta[38]. Gli esperti della Symantec ritengono che "ciò può essere

[34] Nakashima, "Stuxnet Malware Is Blueprint for Computer Attacks on U.S."
[35] Kroft, "Stuxnet: Computer Worm Opens New Era of Warfare."
[36] Kushner, "The Real Story of Stuxnet."
[37] Jim E. Crouch and Larry K. McKee Jr., "Cybersecurity: What Have We Learned?," National Security Cyberspace Institute, October 9, 2011, 1, http://www.nsci-va.org/WhitePapers/
2011-10-09-Cyber%20Lessons%20Learned-Crouch-McKee.pd
[38] Hosenball, "Experts Say Iran Has Neutralized Stuxnet Virus."

avvenuto grazie ad un volontario o a terzi inconsapevoli e ingenui" [39] .E' noto che gli attacchi provenienti da una fonte interna o dall'interno di una struttura possiedono un elevato potenziale di danno, in quanto gli addetti ai lavori hanno accesso diretto alle informazioni sensibili e ai dati. Possiedono inoltre le conoscenze necessarie e i mezzi per poter manipolare sistemi interni senza destare sospetti. In merito, un sondaggio del 2015 dell'istituto SANS condotto su 772 esperti di sicurezza informatica, appartenenti ai più svariati campi industriali, ha rivelato che il 69% di questi riponeva i motivi di una scarsa difesa informatica, all'interno di un impianto, nei dipendenti stessi[40]. Le minacce interne possono essere suddivise in due categorie. La prima comprende individui malintenzionati, che deliberatamente creano danni. La seconda comprende individui ingenui e negligenti, quindi persone con accesso a strutture o reti, che non hanno seguito pratiche di sicurezza prestabilite, generando vulnerabilità attraverso una impropria gestione dei dati, dei sistemi o delle reti[41].

[39] Falliere, Murchu, and Chen, "W32.Stuxnet Dossier,"
[40] Eric Cole, "Insider Threats and the Need for Fast and Directed Response," SANS Institute, Aprile 2015, 6, https://www.sans.org/reading-room
[41] Urrico, "Negating Cybersecurity Threats from Within."

Il sondaggio SANS evidenzia quindi un punto degno di nota: le minacce interne, e le vulnerabilità che queste generano, stanno diventando sempre più note tra i professionisti della sicurezza informatica. Non è tutt'oggi noto chi in particolare abbia infettato la centrale di Natanz, ma è chiaro che il ruolo di un dipendente interno è stato di fondamentale importanza per la riuscita dell'intero attacco. Il secondo fallimentare punto difensivo di Natanz è stata la diffusione di Stuxnet attraverso una rete air-gapped collegata ai PLC, i dispositivi che controllavano la velocità di rotazione delle centrifughe nucleari: una volta che il malware si fosse infiltrato nella rete della centrale, attraverso un dispositivo rimovibile, avrebbe dovuto diffondersi all'interno del sistema air-gapped per poter arrivare al proprio obiettivo. I sistemi isolati air-gapped, come quello presente a Natanz, presentano limitazioni quando si presenta la necessità di spostare dati da un elaboratore a un altro[42]. Stuxnet era stato programmato per copiare se stesso su unità rimovibili ogni qualvolta ne venisse utilizzata una: in questo modo, quando ne veniva fatto uso per spostare dati tra elaboratori, il malware veniva scaricato. Ciò rese molto

[42] Doug Niblick, "Protecting Critical Infrastructure against the Next Stuxnet," Davenport
University, Marzo 20, 2013, 19,
http://www.davenport.edu/system/files/Protecting_Critical_Infra
structure_Against_the_Next_Stuxnet.pdf.

più facile la diffusione di Stuxnet all'interno del sistema chiuso di Natanz. Inoltre, il worm possedeva l'abilità di auto-replicarsi e diffondersi all'interno di una rete dopo aver infettato il dispositivo che fungeva da host[43].

I primi due punti di debolezza della centrale nucleare iraniana possono essere considerati una diretta conseguenza del terzo: la policy interna. L'assenza di un appropriato e definito protocollo di sicurezza ha portato allo sfruttamento dei primi due punti da parte dei creatori di Stuxnet, e in generale sarebbe opportuno che fosse mirato alla protezione delle vulnerabilità interne di un sistema, oltre che a quelle esterne, dal momento che le minacce informatiche sono in continua evoluzione[44].

[43] Falliere, Murchu, and Chen, "W32.Stuxnet Dossier"
[44] Crouch and McKee Jr., "Cybersecurity: What Have We Learned?".

Il caso di Natanz è un esempio lampante di vulnerabilità interna dovuta ad uno scarso protocollo di sicurezza, a testimonianza del fatto che l'ingenuità umana può rappresentare una minaccia che spesso viene trascurata. In particolare, è noto che le infezioni tramite dispositivi rimovibili sono molto comuni: una politica riguardo le restrizioni sull'uso di questi avrebbe ridotto considerevolmente le vulnerabilità di Natanz [45]. Michael Davis, dell'Information Week Analytics, scrisse un articolo dal titolo "Stuxnet Reality Check: Are You Prepared for a Similar Attack?" dove asserì che i "removable storage device security software" sono la miglior tipologia di contromisura alle infezioni da dispositivi USB. Davis aggiunge che sono una prevenzione contro sconosciuti o non autorizzati dispositivi USB, CD/DVD, drives esterni, riproduttori di musica digitali e altri dispositivi che possono contenere infezioni, e che vengono inseriti e accettati dagli elaboratori senza criteri. Termina affermando che l'uso di questi strumenti dovrebbe essere regolato da permessi che garantiscano una garanzia sull'utente che effettivamente li utilizza, e su quali elaboratori questi possano essere inseriti [46]. Quindi, in generale, una struttura dovrebbe garantire un sistema di validazione

[45] Niblick, "Protecting Critical Infrastructure against the Next Stuxnet".
[46] Davis, "Stuxnet Reality Check: Are You Prepared for a Similar Attack?".

per i drives oltre che per chi ne fa uso [47], e ciò costituirebbe un accorgimento che rafforzerebbe il sistema di difesa di un obiettivo sensibile, come quello rappresentato da Natanz.

1.4 IMPLICAZIONI LEGALI DI STUXNET

Un cyber-attacco che sabotava il programma di arricchimento dell'uranio dell'Iran è stato un "atto di forza" ed era probabilmente illegale, secondo una ricerca commissionata da un centro di difesa della NATO. "Gli atti che uccidono o feriscono persone o distruggono o danneggiano oggetti sono inequivocabilmente usi di forza" e probabilmente violano il diritto internazionale, secondo il Manuale di Tallinn sul diritto internazionale applicabile alla guerra cibernetica, uno studio prodotto da un gruppo di esperti legali indipendenti su richiesta del Centro di eccellenza per la difesa cibernetica cooperativa della NATO in Estonia.

[47] Ibidem.

Gli atti di forza sono proibiti dalla Carta delle Nazioni Unite, tranne quando vengono compiuti per autodifesa, ha dichiarato al Washington Times Michael Schmitt, professore di diritto internazionale presso l'U.S. Naval War College di Rhode Island e autore principale dello studio.

I 20 esperti che hanno prodotto lo studio sono stati unanimi nel ritenere che Stuxnet sia stato un atto di forza, ma sono stati meno chiari sul fatto che il cyber sabotaggio contro il programma nucleare iraniano costituisse un "attacco armato", cosa che avrebbe autorizzato l'Iran a usare la controffensiva per autodifesa. Un attacco armato costituisce l'inizio di ostilità internazionali in base alle quali si applicherebbero le leggi di guerra della Convenzione di Ginevra.

Stuxnet è stato lanciato tra il 2009 e il 2010, e forse anche nel 2008, e ha preso di mira le centrifughe presso l'impianto di arricchimento dell'uranio di Natanz in Iran.

L'arma cibernetica sarebbe stata progettata da Israele e dagli Stati Uniti nel tentativo di ridurre la capacità dell'Iran di produrre un'arma nucleare, anche se gli Stati Uniti non hanno ufficialmente riconosciuto il loro ruolo nell'attacco. Fino a quando non sono avvenuti gli attacchi, le agenzie di intelligence hanno ipotizzato che l'Iran sarebbe stato in grado di produrre un'arma nucleare entro il 2010. Si ritiene che gli attacchi di Stuxnet abbiano rallentato il programma di circa tre anni.

Il manuale giuridico di 300 pagine è stato prodotto da 20 ricercatori, tra cui studiosi di diritto e avvocati militari senior dei paesi della NATO, con l'assistenza di analisti della sicurezza informatica.

"L'abbiamo scritto come una forma di aiuto per consulenti legali dei governi e dei militari, quasi come se fosse un libro di testo", ha detto Schmitt al Washington Times. "Volevamo creare un prodotto che fosse utile agli Stati, per aiutarli a decidere la loro posizione.

Non stavamo facendo raccomandazioni, non abbiamo definito le migliori pratiche da intraprendere, non volevamo entrare in politica", ha detto. Altri, tuttavia, non erano d'accordo con le conclusioni legali dei ricercatori. James A. Lewis, un ricercatore del Center for Strategic and International Studies, ha detto che i ricercatori stavano facendo progressi e che non c'erano ancora stati abbastanza incidenti di cyberconflitto per sviluppare una valida interpretazione della legge in questo senso. "Un cyber-attacco non è generalmente un atto di forza. Per questo motivo l'Estonia non ha fatto scattare l'articolo 5 nel 2007", ha affermato, facendo riferimento agli attacchi DDoS coordinati che hanno abbattuto le reti di computer di banche, agenzie governative e media in Estonia che sono stati attribuiti alla Russia o a hacker simpatizzanti per il governo russo. L'articolo 5 del trattato NATO impone agli Stati membri di aiutare gli altri membri in caso di attacco.

Stuxnet è l'esempio di come l'etica possa essere applicata alla guerra cibernetica. Vi è l'idea popolare che "tutto è giusto in amore e in guerra", ma la realtà è che ci sono una serie di rigide linee guida che si suppone che i comportamenti in guerra siano in grado di rispettare – quello che il filosofo legale del 1600 Hugo Grotius chiamava "jus in bello", o legge in tempo di guerra. Le sue rilevanti argomentazioni riguardavano la proporzionalità e la discriminazione. La legge di proporzionalità afferma che la sofferenza e la devastazione che una parte provoca ad un'altra, in particolare i danni collaterali ai bersagli non voluti, non possono superare il danno che ha causato il conflitto[48]. "In altre parole, se l'altra parte ha rubato la tua mucca, non puoi bombardare a buon diritto la loro città" [49]. La legge della discriminazione sostiene che tutte le parti belligeranti devono distinguere tra obiettivi legittimi (ad es. una postazione militare) e obiettivi non legittimi (ad es. civili o feriti), e fare il massimo per causare solo danni ai legittimi obiettivi previsti. Stuxnet si distingueva dal resto degli worm in quanto costituiva un nuovo tipo di arma, progettata per causare danni fisici tramite mezzi informatici. I suoi

[48]https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1009&context=jil

[49] Bruce Cronin, Reckless Endangerment Warfare: Civilian Casualties and the Collateral Damage Exception in International Humanitarian Law, 50 J. PEACE RES. 175, 176–77 (2013)

creatori volevano che danneggiasse gli obiettivi nel mondo reale, ma solo attraverso azione sulle reti digitali, e ciò costituì un approccio totalmente nuovo. Ma quello che veramente distingueva Stuxnet dalle armi tradizionali era quanto piccolo sia stato il suo impatto fisico, soprattutto alla luce della grande posta in gioco. L'obiettivo era un programma creato al fine di fabbricare bombe nucleari, che era già stato obiettivo di scontri diplomatici e sanzioni economiche.

Mentre è certamente discutibile se un'azione preventiva contro il programma iraniano fosse giustificabile, l'attacco di Stuxnet pone la rilevante questione di proporzionalità. Stuxnet ha rotto solo le centrifughe nucleari, che l'Iran aveva ottenuto illegalmente per condurre ricerche illecite.

Anche la discriminazione conta quando si giudica l'etica di questi attacchi. Stuxnet ha infettato non solo i bersagli in Iran ma migliaia di computer in tutto il mondo che non ricoprivano alcun ruolo nel programma di Natanz. Molti avvocati vedono questo aspetto delle cyber armi come prova della loro intrinseca violazione dei "codici prevalenti di leggi internazionali di conflitto, in quanto vanno oltre l'originale obiettivo dell'attacco, e prendono deliberatamente di mira il personale civile e le infrastrutture"[50]. A detta di esperti del settore, questa potrebbe essere un'interpretazione sbagliata, verosimile forse nel periodo antecedente alla ricostruzione della vicenda e dell'analisi dei danni provocati dal malware. Mentre Stuxnet mancava di discrezione secondo il vecchio modo di pensare, il suo stesso design ha impedito di infliggere danni a qualsiasi obiettivo sensibile che non fosse quello inizialmente prefissato.

[50] Singer & Allan Friedman, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW

Come ha scritto George Lucas, un filosofo dell'Accademia Navale degli Stati Uniti, in una valutazione sull'etica di Stuxnet, "A meno che non vi capiti di azionare una vasta gamma esattamente di 984 centrifughe Siemens contemporaneamente, non avete nulla da temere da questo worm"[51].

In effetti, il giudizio che è possibile dare riguardo l'etica di Stuxnet, e delle armi informatiche più in generale, dipende dal punto di vista dal quale viene analizzata la vicenda nella sua completezza. In ogni caso, forse solo la storia potrà rendere possibile la formulazione di un giudizio su Stuxnet. Come ha detto Ralph Langner, l'affascinante nuova arma che ha scoperto "potrebbe essere considerata un esempio da manuale di un approccio di 'guerra giusta'. Non ha ucciso nessuno. Questa è una buona cosa. Ma temo che questo sia solo un giudizio a breve termine. A lungo termine ha aperto un vero e proprio vaso di Pandora[52]".

---

[51] George R. Lucas, PERMISSIBLE PREVENTIVE CYBERWAR: RESTRICTING CYBER CONFLICT TO JUSTIFIED MILITARY TARGETS (2011);

[52] Mark Clayton, From the Man Who Discovered Stuxnet, Dire Warnings One Year Later, CHRISTIAN SCI. MONITOR (22 Settembre 2011), http://www.csmonitor.com/USA/2011/0922/From-the-man-who-discoveredStuxnet-dire-warnings-one-year-later.

2

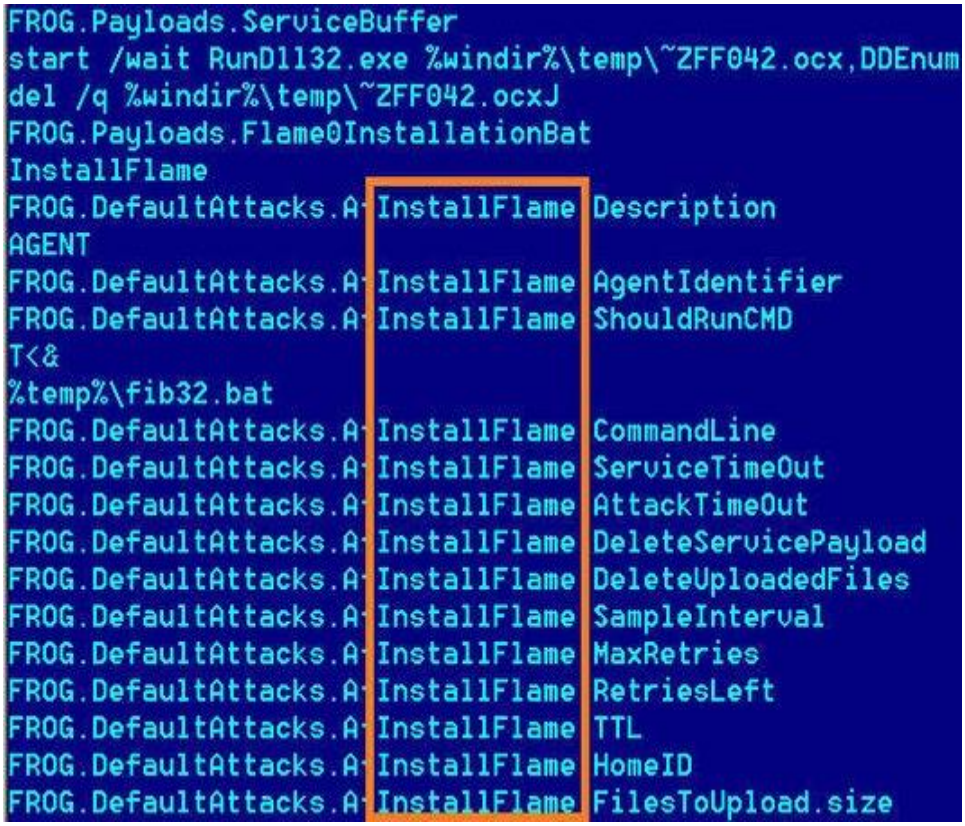
FLAME

2.1 La scoperta di Flame

Subito dopo l'evento Stuxnet, il mondo della sicurezza informatica comprese la potenziale pericolosità di una guerra cibernetica e gli effetti che certi livelli di trascuratezza dei protocolli di difesa potevano portare. Malware più complessi dello stesso Stuxnet vennero creati successivamente, che non prevedevano danni fisici a strutture sensibili. Uno tra questi fu Flame.

Flame (o DaFlame) venne identificato nel maggio del 2012 dal MAHER Centre of Iranian National CERT, Kaspersky Lab e CrySyS Lab (Laboratory of Cryptography and System Security) dell'Università di Tecnologia ed Economia di Budapest. In particolare, Kaspersky Lab venne incaricato dall'Unione Internazionale delle Telecomunicazioni delle Nazioni Unite di indagare sulle segnalazioni di un virus che colpiva i computer del Ministero del Petrolio iraniano[53]. Si trattava di un hash MD5 e di un filename che apparivano in calcolatori situati in Medio Oriente. Dopo alcune indagini, i ricercatori soprannominarono il programma "Flame" a seguito di una parola che compariva spesso nel codice stesso.

[53] Zetter, Kim (28 Maggio 2012) "Meet 'Flame': The Massive Spy Malware Infiltrating Iranian Computers".



5. Frammento di codice di Flame
https://www.wired.com/2012/05/flame/

Secondo Kaspersky, Flame operava almeno dal febbraio 2010 [54]. CrySyS Lab riferì che il nome del file del componente principale era già stato osservato nel dicembre 2007.

[54] Gostev, Alexander (Maggio 2012) "The Flame: Questions and answers".

Non è mai stato possibile determinarne direttamente la data di creazione, in quanto le date di creazione dei moduli del malware furono falsamente impostate a prima del 1994[55].

"Chiunque l'abbia creato è stato attento a cambiare le date di compilazione in ogni singolo modulo. I moduli sembrano essere stati compilati nel 1994 e nel 1995, ma stanno usando codice che è stato rilasciato solo nel 2010"[56].

Gli esperti considerarono Flame come la causa di un malfunzionamento che nell'aprile del 2012 costrinse i funzionari iraniani ad interrompere forzatamente la connessione a Internet dei dispositivi petroliferi [57]. All'epoca la Students News Agency iraniana si riferì al malware colpevole come "Wiper", un nome datogli dallo stesso creatore[58].

[55] Ibidem.
[56] Ibidem.
[57] Hopkins, Nick (28 Maggio 2012) "Computer worm the hit iran oil is more complex yet".
[58] Erdbrink, Thomas (23 Aprile 2012) "Facing Cyberattack, Iranian Officials Disconnect some Oil Terminals From Internet" New York Times.

Tuttavia, Kaspersky Lab ritenne che Flame potesse essere "un'infezione completamente separata" dal malware Wiper[59]. A causa delle dimensioni e della complessità del programma, descritto come "venti volte" più complicato di Stuxnet, il laboratorio dichiarò che un'analisi completa del codice avrebbe potuto impiegare fino a dieci anni[60].

Il 28 maggio, il CERT dell'Iran annunciò di aver sviluppato un programma di rilevamento e uno strumento di rimozione per Flame, e di averli distribuiti a "organizzazioni selezionate" per diverse settimane[61]. Dopo l'esposizione di Flame nei media, l'8 giugno Symantec riferì che alcuni computer di comando e controllo dello stesso malware (C&C) inviarono un comando "suicida" ai PC infetti per rimuoverne tutte le tracce[62]. Secondo le stime di Kaspersky, nel maggio 2012, inizialmente Flame infettò circa 1.000 macchine[63], con vittime tra cui organizzazioni governative, istituzioni educative e privati. All'epoca i paesi più colpiti erano l'Iran, Israele, i Territori Palestinesi, il Sudan, la Siria, il Libano, l'Arabia Saudita e l'Egitto[64].

---

[59] Zetter, Kim (28 Maggio 2012) "Meet 'Flame': The Massive Spy Malware Infiltrating Iranian Computers".
[60] Ibidem.
[61] Ibidem.
[62] "Flame malware makers send 'suicide' code" BBC News, 8 Giugno 2012.
[63] Zetter, Kim (28 Maggio 2012) "Meet 'Flame': The Massive Spy Malware Infiltrating Iranian Computers".
[64] Gostev, Alexander (Maggio 2012) "The Flame: Questions and answers".

2.2 FLAME E LA SUA DIFFUSIONE

Dalle varie analisi effettuate si comprese subito che non si trattava di un semplice worm, ma di qualcosa di molto più sofisticato e complesso. Flame presentava una struttura modulare e, per questo motivo, alcuni lo hanno paragonato a Duqu. In realtà Flame era un prodotto molto più articolato, pesava circa 20 MB e conteneva al suo interno un vero e proprio "arsenale" costituito da molte librerie (tra cui quelle necessarie alla compressione dei dati, come zlib, libbz2, ppmd), moduli per la manipolazione dei dati (sqlite3), DLLs, algoritmi di encryption, script e una macchina virtuale contenente un'implementazione Lua [65]. Lua è un linguaggio di programmazione facilmente interfacciabile a moduli scritti in C e in C++, tipicamente utilizzato per lo sviluppo di videogiochi.
Sembra che la logica seguita dagli sviluppatori sia stata quella di scrivere i moduli top-level in Lua e interfacciarli con librerie compilate in C++. Si tenga presente, per comprendere la complessità del sistema, che le sole righe di codice della porzione scritta in Lua ammontavano ad oltre 3000.

[65] Ibidem.

Flame presentava, in sintesi, le seguenti caratteristiche:

- si propagava attraverso supporti removibili o reti locali;
- effettuava attività di network sniffing, rilevando risorse di rete disponibili e collezionando liste di password vulnerabili;
- effettuava una scansione dei dischi dei sistemi infettati alla ricerca di specifici tipi di file;
- creava una serie di screenshots del desktop dell'utente quando erano in esecuzione determinati processi o finestre attive;
- interagiva anche con l'hardware della macchina pilotando il microfono per registrare suoni provenienti dall'ambiente circostante o registrando i keystroke della tastiera;
- trasferiva i dati raccolti ad una serie di C&C servers, utilizzando più di 10 domini e attraverso connessioni cifrate (via SSH e HTTPS);
- non veniva rilevato dalla maggior parte degli antivirus e antimalware (in realtà tutti i maggiori produttori stanno ora rilasciando removal tools e aggiornamenti);
- colpiva Windows Xp, Vista e Windows 7.

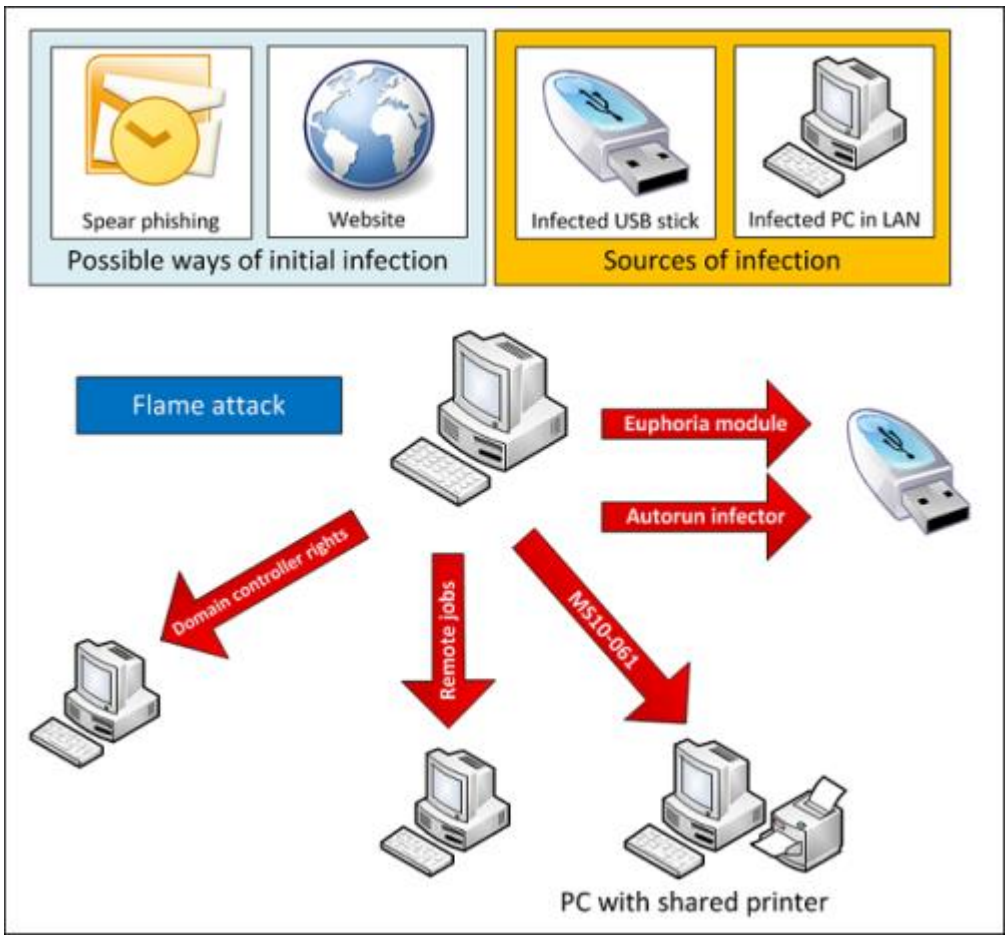
Flame utilizzava vari vettori di attacco per infettare i propri target: siti web (eventualmente compromessi), e-mail di phishing, drives USB, computer già infettati.

In particolare sono stati individuati due moduli, denominati "Autorun Infector" ed "Euphoria", che sarebbero stati responsabili dell'infezione via USB. Per quanto riguardava invece la diffusione nelle LAN, Flame avrebbe sfruttato la vulnerabilità del print spooler di Microsoft, classificata con il codice MS10-061. Questa vulnerabilità, che consente la remote code execution, era già stata sfruttata da Stuxnet nel 2010. In sostanza, quando veniva eseguito da utente con privilegi di amministratore su un domain controller, Flame attaccava gli altri host della rete creando degli user accounts backdoor con una password predefinita, che veniva utilizzata per autocopiarsi sulle macchine da infettare[66].

A differenza di Stuxnet, Flame non si replicava automaticamente. I meccanismi di diffusione venivano disattivati di default e dovevano essere attivati dagli aggressori prima che il malware si diffondesse. Una volta che infettava una chiavetta USB inserita in una macchina infetta, l'exploit USB veniva immediatamente disattivato[67].

[66] Zetter, Kim (28 Maggio 2012) "Meet 'Flame': The Massive Spy Malware Infiltrating Iranian Computers".
[67] Gostev, Alexander (Maggio 2012) "The Flame: Questions and answers".

In questo modo si intendeva probabilmente controllare la diffusione del malware e ridurre la probabilità che venisse rilevato. Questa potrebbe costituire la risposta degli aggressori alla diffusione fuori controllo che si verificò con Stuxnet, e che conseguentemente accelerò la sua rilevazione.



6. Schema raffigurante il meccanismo di diffusione di Flame
https://www.html.it/articoli/flame-malware-o-cyber-weapon/

È possibile che gli exploit siano stati abilitati nelle prime versioni del malware per consentire la diffusione automatica del malware, per poi venire disabilitati dopo che Stuxnet diventò pubblico nel luglio 2010, e dopo che le vulnerabilità .lnk e print spooler furono patchate. Infatti, Flame è stato lanciato prima della scoperta di Stuxnet, e Microsoft applicò una patch alle vulnerabilità .lnk e allo spooler di stampa ad agosto e settembre 2010. Qualsiasi malware che tentasse di utilizzare le vulnerabilità sopracitate, attualmente verrebbe rilevato se le macchine infette eseguissero versioni aggiornate dei programmi antivirus. Flame, infatti, verificava la presenza di versioni aggiornate di questi programmi su una macchina e, in base a ciò che trovava, determinava se l'ambiente fosse favorevole o meno all'utilizzo degli exploit da diffondere [68]. I ricercatori dicono di non sapere ancora come si verifica un'infezione iniziale di Flame su una macchina prima della sua effettiva diffusione [69]. Il malware ha tutt'ora la capacità di infettare un dispositivo con Windows 7 completamente patchato, il che suggerisce che potrebbe esserci un

[68] Zetter, Kim (28 Maggio 2012) "Meet 'Flame': The Massive Spy Malware Infiltrating Iranian Computers".
[69] Ibidem.

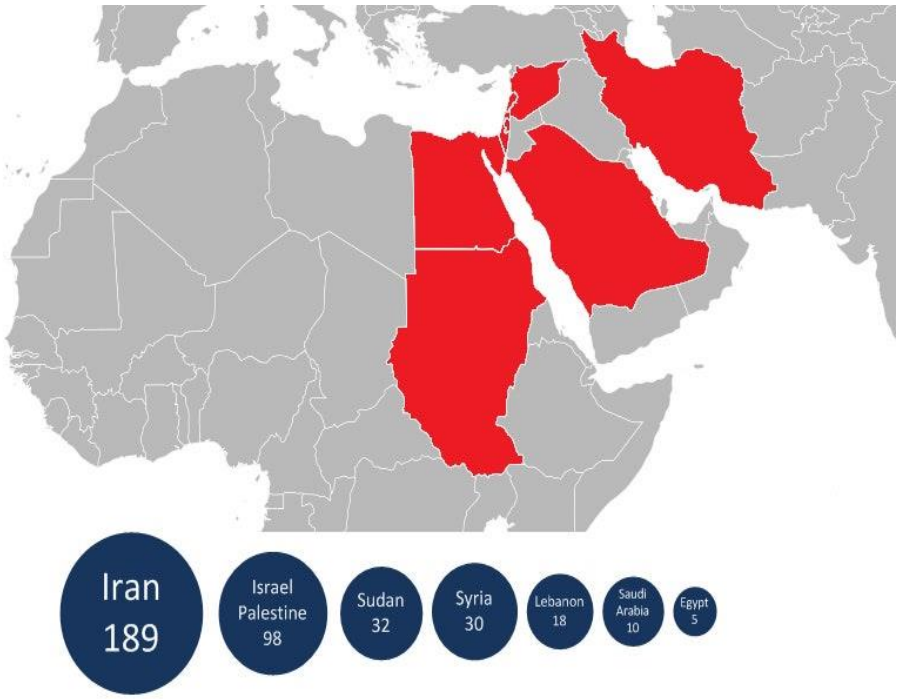
exploit zero-day nel codice che i ricercatori non hanno ancora trovato[70].

2.3 CONSEGUENZE DI FLAME

Flame è un enorme programma da 20 megabyte, grande come un file video, e 40 volte più grande di Stuxnet. Ma Flame non è solo un'altra arma cibernetica: potrebbe espandere notevolmente il raggio d'azione delle nazioni in grado di effettuare attacchi cibernetici. Flame presenta molte somiglianze con Stuxnet. Entrambi sono esempi di programmazione altamente avanzata e di competenza dettagliata in molti settori specializzati. Scott Borg, capo della U.S. Cyber Consequences Unit riferì che "solo una manciata di nazioni ha la capacità tecnica per fare questo tipo di lavoro. L'elenco comprende gli Stati Uniti, il Regno Unito, la Germania, la Cina, la Russia, Israele e Taiwan".

[70] Ibidem.

Ma Flame si differenzia da Stuxnet per molti aspetti importanti. Mentre Stuxnet è stato progettato per uno scopo specifico, cioè quello di infiltrarsi e distruggere le centrifughe utilizzate nell'impianto iraniano di arricchimento del combustibile nucleare di Natanz, Flame sembra essere uno strumento di spionaggio di uso generale. Ha un'ampia capacità di raccogliere dati da schermate o attraverso connessioni Bluetooth con altri dispositivi. Una volta che Flame si collega a un computer, inizia a "controllare il traffico di rete, a fare screenshot, a registrare le conversazioni audio, a intercettare cosa viene digitato sulla tastiera e così via", come è scritto in un rapporto del 28 maggio della società di sicurezza Kaspersky. È in grado di comprimere e criptare le informazioni catturate e di trattenerle fino a quando non dispone di una connessione Internet affidabile per inviarle. Flame aveva come obiettivo i Paesi del Medio Oriente: si è manifestato soprattutto in Iran, con infezioni anche in Israele, nei territori palestinesi, in Sudan e in Siria.



7. Grafico che mostra la diffusione di Flame
https://www.wired.com/2012/05/flame/

"I programmatori che hanno progettato Flame non hanno cercato di mascherare il codice in modo da rendere difficile il reverse engineering. La pratica, nota come 'offuscamento del codice', è comune tra gli sviluppatori di software commerciale, e costituisce un modo per impedire ai concorrenti di capire come vengono progettati i prodotti software. I programmatori di Flame apparentemente non hanno preso tali misure, il che significa che un programmatore esperto non avrebbe troppi problemi ad estrarre la progettazione pertinente di Flame e ad utilizzarla.

Questo non vuol dire che chiunque possa scaricare Flame e iniziare a usarlo, naturalmente. La mancanza di offuscamento del codice aggiunge decine di stati alla lista di quelli in grado di effettuare sofisticati attacchi informatici" sostiene Scott Borg, "e tra questi potrebbe benissimo esserci l'Iran, i cui programmatori stanno continuando a studiare Flame. L'incapacità di proteggere il codice di Flame dall'ingegneria inversa potrebbe rivelarsi un errore monumentale".

Quali sono le implicazioni di tutto questo?
I maggiori rappresentanti di cyber security sostengono che Flame sia la testimonianza di come le moderne tecnologie di sicurezza non stiano più svolgendo il proprio lavoro in maniera soddisfacente.
"Negli ultimi 18-24 mesi, tutto ciò che abbiamo conosciuto sulla sicurezza è cambiato. La sicurezza perimetrale come la conoscevamo è morta", ha detto Adam Bosnian nel 2012, vicepresidente esecutivo della società di gestione delle identità privilegiate Cyber-Ark.

“Alla luce del fatto che chiunque può infettare una rete indipendentemente dai protocolli di sicurezza perimetrale di un'organizzazione, vi è la necessità di cambiare rapidamente il modo di pensare, e di concentrarsi sulla protezione dall'interno verso l'esterno. Flame fornisce anche un buon esempio di come gli aggressori stiano sfruttando account privilegiati come metodo di attacco primario per gli attacchi alla sicurezza informatica delle imprese. Questi account fungono da gateway verso i dati più sensibili di un'organizzazione, che sono accessibili attraverso sistemi, applicazioni e server" continua Bosnian.

Mentre Flame sembra avere a disposizione diversi metodi di infezione, si è scoperto che si propaga attraverso reti che sfruttano lo stesso exploit privilegiato utilizzato da Stuxnet: la vulnerabilità della MS10-061. Lo sfruttamento di questo punto di accesso privilegiato permette al virus di attaccare altre macchine su una stessa rete.

Sempre Bosnian sostiene :“I punti di accesso privilegiati esistono in quasi tutti i dispositivi dotati di microprocessore, ma spesso sono protetti con password deboli o predefinite, e una volta dentro, gli aggressori utilizzano l'account privilegiato, o elevano i privilegi associati all'account, per accedere ad altri server, database e altri sistemi di alto valore a cui solo poche persone selezionate hanno effettivamente il permesso di accedere.

Il risultato è un facile accesso a milioni di record sensibili, il che significa che a un certo punto le aziende e le organizzazioni governative devono svegliarsi e capire che gli account e le password privilegiate sono l'obiettivo numero uno per gli hacker".

2.4 IMPLICAZIONI LEGALI DI FLAME

Flame è stata un'arma di cyber spionaggio di cui tutt'ora è ignoto l'autore. A volte chiamata "la seconda professione più antica"[71], lo spionaggio affonda le sue radici nell'antico Egitto, in Grecia,
Roma e Cina[72]. Infatti, il grande studioso di diritto del XVII secolo Hugo Grotius osservò che "non c'è dubbio, ma la legge delle nazioni permette a chiunque di mandare spie, come fece Mosè nella terra promessa[73]". La legge sullo spionaggio è rimasta però relativamente sottosviluppata. Gli studiosi sono infatti tutt'oggi divisi in maniera netta sulla legalità dello spionaggio in tempo di pace. La maggior parte degli studiosi affermano che è legale, affermando che una migliore informazione su ciò che gli altri paesi stanno facendo promuove la stabilità ed è implicita nel diritto di autodifesa preventiva[74].

---

[71] Michael N. Schmitt, The Tallinn Manual on the International Law Applicable to Cyber Warfare (New York:
Cambridge University Press, 2013)
[72] Ibidem.
[73] Ibidem.
[74] Julius Stone, "Legal Problems of Espionage in Conditions of Modern Conflict"

Altri non sono d'accordo, condannandola come una violazione imprescibile dell'integrità territoriale del paese spiato[75]. Altri ancora affermano che lo status giuridico dello spionaggio rimane ambiguo, e il diritto internazionale non lo condanna né lo giustifica[76]. In assenza di principi chiari, fatta eccezione per sottopunti quali l'interferenza con i comunicati diplomatici, lo spionaggio resta la provincia di diritto interno e cade al di fuori dei punti fondamentali dello jus in bello.

Solo negli ultimi anni sta venendo alla luce una letteratura in materia di cyber spionaggio[77]. Vi sono aspetti dello spionaggio informatico che potrebbero cambiare il risultato delle leggi in divenire. Da un lato, come nel caso della sorveglianza satellitare[78], la mancanza di invasione del territorio rende la cyber-sorveglianza meno invasiva e meno problematica[79]. Alcuni lo considerano un vantaggio, in quanto gli aspetti non-letali delle capacità informatiche li rendono

[75] Quincy Wright, "Espionage and the Doctrine of Noninterference in Internal Affairs"
[76] Christopher D Baker, "Tolerance of International Espionage: A Functional Approach,"
[77] Sean P Kanuck, "Information Warfare: New Challenges for Public International Law,"
[78] Christopher D Baker, "Tolerance of International Espionage: A Functional Approach,"
[79] Ibidem.

preferibili ad altri mezzi [80]. Altri sostengono il contrario,poiché lo spionaggio cibernetico aumenta significativamente la scala della capacità di raccolta di informazioni, che dovrebbe essere frenata e trattata in maniera più seria rispetto allo spionaggio tradizionale [81]. In ogni caso, non è mai emerso un accordo generale rispetto alle pratiche tradizionali di spionaggio, e non sembra esserci motivo di aspettarsi che il consenso sia più probabile nel contesto informatico.

La legge in materia di guerra, quindi, ha poco da dire riguardo a queste tipologie di sorveglianza. Ecco perché la regola 66(a) del Manuale di Tallinn afferma esplicitamente: "Cyber spionaggio e altre forme di raccolta di informazioni dirette ad un avversario durante un'azione armata non violano le leggi del conflitto armato" [82].

[80] Jeffrey TG Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality
in the Age of Cyber Warfare"
[81] Anna Wartham, "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate
UN Charter Provisions Prohibiting the Threat or Use of Force?"
[82] Michael N. Schmitt, The Tallinn Manual on the International Law Applicable to Cyber Warfare (New York:
Cambridge University Press, 2013)

Il commento rileva analogamente che il cyber spionaggio non costituisce un uso della forza o un attacco armato a scopo di danno, o una violazione del principio di non intervento[83]. Spiega anche perché la legge non affronta lo spionaggio di per sé e che, in quanto tale, la condotta connessa allo spionaggio è presuntivamente legale come questione di diritto internazionale[84].

Ancora più significativa è la parte del Manuale di Tallinn che distingue tra il cyber spionaggio, che avviene necessariamente in territorio controllato da una delle parti armate del conflitto, e lo sfruttamento delle reti informatiche e dalla ricognizione informatica, che possono essere condotte dall'esterno del territorio controllato dal nemico.

Per i suddetti motivi, quindi, eventi come quello di Flame, o il tipo di attività descritte nei documenti segreti divulgati da Edward Snowdene o l'attacco DDoS contro l'Estonia non sono affrontati adeguatamente dalle leggi del diritto internazionale. Di conseguenza, la legalità di tali comportamenti è generalmente affidata e gestita dalle leggi nazionali degli stati coinvolti.

[83] Ibidem.
[84] Ibidem.

3

MYDOOM

3.1 L'ARRIVO DI MYDOOM

Non tutti i malware che sono passati alla storia sono stati creati da team di programmatori scelti appartenenti a qualche azienda segreta di un particolare paese, e non tutti avevano lo scopo di recare danni fisici o di fungere da mezzi di spionaggio. Ci sono stati pericolosi malware che hanno creato molto scalpore anche solamente per aver detenuto un record per un consistente quantitativo di tempo, mantenendo una certa pericolosità e portando a termine un attacco di grosse dimensoni. E' il caso di Mydoom.

Mydoom venne rilevato per la prima volta nel 26 gennaio 2004, e passò alla storia come il worm che più velocemente riuscì a propagarsi via e-mail, rimanendo imbattuto fino al 2016[85].
E' conosciuto anche come W32.MyDoom@mm, Novarg, MiMail.R o Shimgapi, e i sistemi operativi che colpiva variavano da Windows 95 a Windows XP.

[85] CNN.com – Security Firm: Mydoom worm fastest yet, 2004

La mattina del 26 gennaio 2004 vennero intercettate numerose segnalazioni riguardanti malfunzionamenti di dispositivi informatici negli Stati Uniti, a seguito di una massiva ricezione di messaggi di posta elettronica provenienti dalla Russia, e nel corso della giornata le prestazioni di internet rallentarono del 10%. Il tempo medio di caricamento di una pagina web aumentò del 50%[86].

Le indagini condotte portarono alla formulazione di diverse tesi, di cui una delle più avvalorate riguardante la società SCO Group[87], il cui sito andò offline per qualche ora proprio la mattina del 26 gennaio 2004.

La SCO Group (nota precedentemente con il nome di Caldera International), a partire dal 1998, sviluppò distribuzioni GNU/Linux per workstation e server, ed era riconosciuta per essere una società associata al movimento open source.

[86] 'MORE DOOM?' europe.newsweek.com
[87] Ibidem

Dopo aver acquistato alcuni diritti sul marchio registrato UNIX, il 7 marzo 2003 SCO Group aprì una causa legale contro la IBM, accusandola di aver contribuito allo sviluppo del kernel Linux utilizzando codice sorgente di sua proprietà. In particolare, SCO Group citò IBM per la supposta svalutazione della sua versione del sistema UNIX, dichiarando danni per 1 miliardo di dollari. SCO Group sosteneva la tesi secondo cui IBM avrebbe aggiunto nel kernel Unix-like e open source Linux delle parti di codice la cui proprietà intellettuale apparteneneva a SCO [88] , avvisando le aziende delle liste di Fortune 1000 e Global 500 che sarebbero state considerate responsabili nel caso in cui avessero usato Linux stesso. La causa si concluse il 30 marzo 2010 con la decisione della Corte Distrettuale dello Utah, la quale respinse tutte le richieste di SCO Group.

Il 27 gennaio 2004, giorno successivo alla scoperta di Mydoom, SCO Group, ritenendo di essere l'obiettivo di un attacco DoS, decise di offrire una ricompensa di 250000 dollari in cambio di informazioni che avrebbero portato all'arresto del creatore del worm[89], mobilitando FBI e Servizi Segreti degli Stati Uniti.

[88] 'Causa Caldera – Microsoft' - digitalresearch.biz
[89] 'Mydoom virus starts to fizzle out' - news.bbc.co.uk

Nei giorni immediamente successivi, venne scoperta una seconda versione di Mydoom, che includeva sia l'attacco originale a SCO Group che un attacco identico rivolto a Microsoft.com e ai siti di oltre 60 società di sicurezza informatica, con inizio programmato il 3 febbraio 2004[90]. Ciò portò a una conseguente offerta di 250000 dollari anche da parte di Microsoft in cambio di informazioni. Giunti al 1° febbraio, SCO rimosse il proprio sito dal DNS a seguito di un attacco DoS da parte di circa un milione di dispositivi infetti, ritenuto tra i più grandi attacchi DoS fino ad oggi[91]. Il 3 febbraio l'attacco nei confronti di Microsoft iniziò, mentre la stessa società si tutelò offrendo un sito web non influenzato dal worm, information.microsoft.com [92] . Tuttavia, l'impatto dell'attacco risultò minimo ed il sito ufficiale rimase funzionante. Ciò venne attribuito alla relativamente scarsa distribuzione della seconda versione di Mydoom, alla tolleranza elevata dei server e alle precauzioni prese dalla società. Alcuni esperti sottolinearono che il peso del worm, in termini di byte, fosse inferiore a quello degli aggiornamenti software e altri servizi web comunemente offerti da Microsoft[93].

---

[90] 'What You Should Know About the Mydoom Worm Variants: Mydoom.A and Mydoom.B' - information.microsoft.com
[91] Ibidem.
[92] Ibidem
[93] Ibidem.

3.2 DENTRO MYDOOM

Le tipologie di Mydoom scoperte fino ad oggi, in particolare le due versioni più conosciute Mydoom.A e Mydoom.B, utilizzavano le e-mail come principale canale di propagazione insieme a Kazaa.Kazaa Media Desktop client (o KMD) è un'applicazione Peer-To-Peer (P2P) utilizzata per consentire a più utenti di condividere file a distanza.

Spesso utilizzata per condividere file multimediali .mp3 o .mpeg attraverso altri file (.jpeg, .doc, .pdf, ecc.), durante il periodo di massima attività di Mydoom si stimava che gli utenti di KMD fossero 4.000.000[94].

MyDoom.A si copiava da solo nella directory condivisa predefinita dalla KMD , utilizzando un falso nome. Gli utenti che scaricavano il file corrotto lo eseguivano pensando fosse un normale file, e il virus veniva automaticamente copiato e condiviso con altri utenti.

[94] https://www.giac.org/paper/gcih/568/mydoom-dom-anlysis-mydoom-virus/106069

La diffusione del virus nella rete Kazaa non solo occupava molta banda e spazio su disco rigido, ma provocava nuovi exploit di sicurezza su ogni computer infetto, sotto forma di porta aperta[95] utile a controllare il dispositivo da remoto. Ciò non solo dimostra l'importanza degli attuali anti-virus, ma dimostra anche come i programmi P2P come il KMD possano risultare rischiosi per la sicurezza di un dispositivo, attraverso lo scambio costante di dati non esaminati correttamente.

Il diffuso utilizzo di KMD da parte di MyDoom.A è stato parte del motivo per cui MyDoom e le sue varianti si sono propagate così velocemente.

Per propagare se stesso, MyDoom.B copiava un file contenente se stesso nella cartella predefinita di KMD, esattamente come Mydoom.A .

Mydoom.A e Mydoom.B erano stati programmati per non diffondersi attraverso domini che generalmente venivano utilizzati da persone più competenti quali panda, .gov e hotmail, e non infettava account comunemente associati a tecnici, come “admin”, “support” o “root”.

[95] Ibidem.

La versione originale di Mydoom.A è descritta come esecutrice di due payload; inizialmente veniva installata una backdoor sulla porta 3127/TCP per consentire il controllo remoto del PC infetto (mettendo il proprio file SHIMGAPI.DLL nella directory system32 ed eseguendolo come un processo figlio di Windows Explorer). Successivamente veniva sferrato l'attacco a SCO Group, nel caso di Mydoom.A, o a SCO Group e a Microsoft nel caso di Mydoom.B[96] . In particolare, il virus apriva una backdoor TCP per permettere ad altre varianti di Mydoom di infettare il dispositivo.

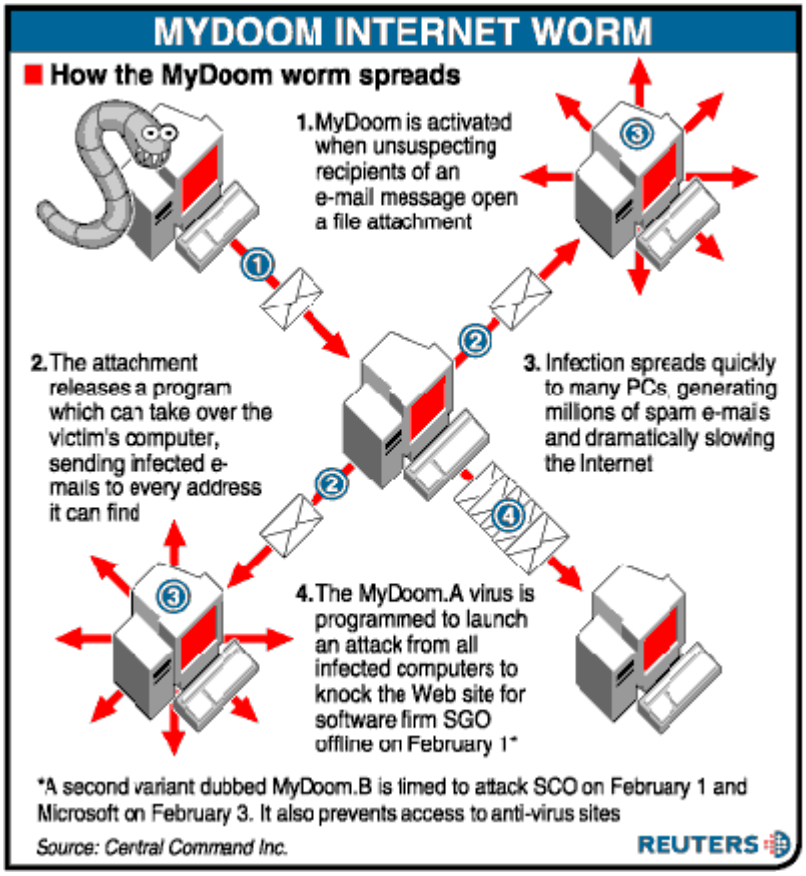
La diffusione via e-mail di Mydoom consisteva nella scansione del dispositivo infetto da parte del worm stesso, con lo scopo di rintracciare file che contenessero indirizzi e-mail.

Gli indirizzi e-mail venivano così raccolti, e ad ognuno di questi veniva inviato un file contente Mydoom.

La scansione prevedeva anche il controllo delle cache, il che permetteva al worm di raccogliere una grande quantità di obiettivi.

[96] 'What You Should Know About the Mydoom Worm Variants: Mydoom.A and Mydoom.B' - information.microsoft.com

Un file infetto veniva quindi inserito nella directory condivisa sulla rete Kazaa, la cui esistenza veniva preventivamente determinata esaminando proprio il registro di Kazaa. Il worm procedeva con ridenominazione del file e col suo conseguente inserimento nella directory condivisa, alla quale gli altri clienti della rete Kazaa potevano accedere.



8.Metodo di propagazione di Mydoom
https://blog.knowbe4.com/15-year-old-mydoom-remains-a-common-phish-hook

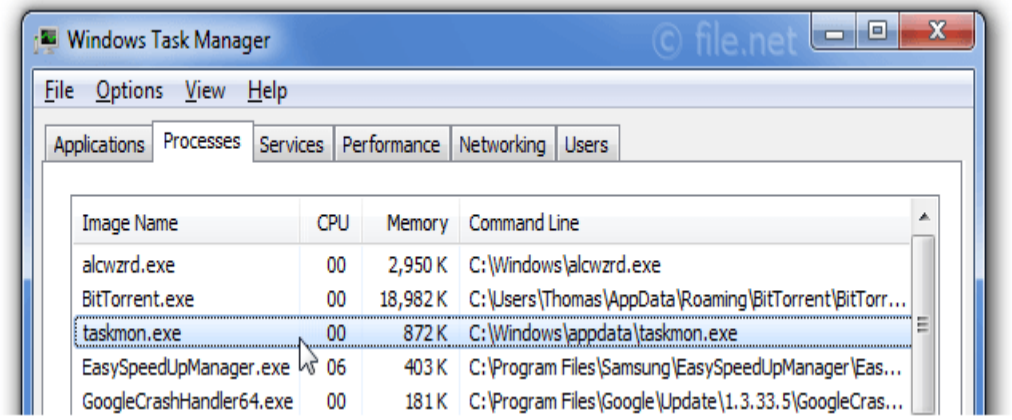
L'exploit di sicurezza di MyDoom.A, e similmente di MyDoom.B, iniziava quindi con l'esecuzione di un file, mascherato da un altro file eseguibile. Una volta che il file infetto veniva eseguito, i seguenti registri di sistema subivano delle modifiche:

·HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run

·HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

In particolare, al loro interno veniva installato un file eseguibile chiamato taskmon.exe. Le suddette modifiche del registro di sistema comportavano ,di conseguenza, un avvio mascherato del virus ad ogni reboot del sistema stesso.

Il travestimento dei file installati rendeva più facile per MyDoom evitare di essere scoperto, e di mantenere l'accesso al sistema, rendendo così possibili ulteriori attacchi DoS e infezioni da parte di altre tipologie del virus stesso attraverso la porta aperta.



9.Il processo taskmon.exe nel Windows Task Manager

https://www.file.net/process/taskmon.exe.html

Inoltre, Mydoom rilasciava un ulteriore file dal nome %sysdir%\shimgapi.dll , il quale apriva sequenzialmente le porte TPC dalla 3127 alla 3198.

Il punto di forza di Mydoom era la sua capacità di auto copiarsi all'interno della cartella condivisa di KMD. I file che più comunemente utilizzava per agire erano: nuke2004, winamp5, icq2004-final, office_crack, rootkitXP, activation_crack e strip-girl-2.0bdcom_patches, ai quali venivano aggiunte estensioni scelte casualmente tra .pif, .exe, .src, .bat .

Il nome del file veniva quindi scelto tra i più ricercati su KMD, e veniva inserito all'interno del percorso %root directory\Program Files\Kazaa\My Shared Directory\ .

Come detto in precedenza, la cartella condivisa di Kazaa era visualizzabile da qualunque utente, e di conseguenza i suoi file interni erano scaricabili ed eseguibili da terzi. I downloads quindi non erano in nessun modo scansionati da Kaaza stesso, consentendo al virus di diffondersi tra i diversi client della Kaaza Network.

3.3 CONSEGUENZE DI MYDOOM

Mydoom è stato un worm che si è diffuso grazie a principi di ingegneria sociale, oltre che alla negligenza di svariati utenti.
La mancata osservazione di principi di prevenzione e di accorgimenti sul piano informatico, e la mancanza di un vero e proprio controllo delle operazioni dei sistemi P2P, hanno portato ad una repentina diffusione di Mydoom.

Un punto che si può apprendere è che da parte degli utenti è necessaria una corretta gestione delle mail sconosciute e dei file che queste possono contenere. E' risaputo che mail inaspettate arrivate da utenti sconosciuti generalmente non contengono benefici per chi effettivamente le apre[97].

Altro punto fondamentale dal punto di vista dell'utenza è legato alla rete P2P e le capacità di condivisione che possiede. E' necessario un periodico controllo dei file che vengono condivisi su una rete, come quella di Kazaa. Spesso un utente condivide file di cui non è conoscenza proprio per un mancato preventivo e periodico controllo[98].

Il traffico causato dalla rete P2P in generale occupa molta banda; di conseguenza un limite all'uso di questa, ed in particolare a quella occupata da KMD, potrebbe prevenire il download di file non desiderati da parte degli utenti[99], come è successo nel caso di Mydoom. Sarebbe quindi importante implementare un limite ai pacchetti condivisi.

E' quindi importante capire che l'ingegneria sociale ha fornito a Mydoom un ottimo metodo di propagazione, e costituisce un mezzo che sta prendendo piede nel mondo della sicurezza informatica.

---

[97] https://antivirus.comodo.com/blog/comodo-news/mydoom-virus/
[98] Ibidem
[99] Ibidem

Il social engineering si basa sull'acquisizione della fiducia da parte dell'utente nei confronti del sistema; normalmente avviene
attraverso un approccio stile Trojan, che consiste nel nascondere un file maligno all'interno di uno apparentemente innocuo e proveniente da una fonte a prima vista sicura, camuffandolo a tal punto da indurre l'utente a fidarsi e ad aprirlo.
I metodi più comuni usati dai virus come Mydoom, e che fanno uso dei principi dell'ingegneria sociale, si basano sull'invio di mail con titoli che generalmente attirano l'attenzione. L'apertura di una mail "innocua" generalmente non costituisce un problema, al contrario dell'esecuzione di un file sconosciuto che essa può contiene[100].

Interessante è analizzare anche l'attacco che è stato portato a termine.
Affrontare un attacco di denial-of-service distribuito come quello che ha abbattuto il sito web di SCO Group continua ad essere una grande sfida per le aziende. Un attacco DDoS tipicamente coinvolge migliaia di sistemi "zombie" compromessi, che inviano flussi di dati inutili o richieste di dati a server o reti mirate.

---

[100] 'The Seattle Times: Business & Technology: E-mail viruses blamed as spam rises sharply' - seattletimes.nwsource.com

L'attacco a SCO, ad esempio, è stato lanciato utilizzando sistemi precedentemente infettati da Mydoom. Il virus conteneva un codice che ordinava a migliaia di computer infetti di accedere contemporaneamente al sito web di SCO, rendendolo inaccessibile agli utenti legittimi.

“Fermare il flusso di traffico può essere molto difficile perché proviene da così tante fonti” sostiene Bruce Schneier, presidente di Counterpane Internet Security Inc. .

“Ci sono diversi approcci che le aziende possono adottare per prepararsi ad attacchi come questo” ha detto Paul Mockapetris, inventore del Domain Name System (DNS). “Uno è quello di mettere a disposizione una banda di rete extra e una maggiore capacità di elaborazione dei server per resistere a improvvisi picchi di traffico, continua Mockapetris. “Un altro è quello di ‘ritirarsi’ dal proprio dominio ed essenzialmente trasferire il proprio sito web ad un altro indirizzo mentre l'attacco si svolge”, come è stato il caso di Microsoft all’inizio dell’attacco di Mydoom.B .

“La distribuzione geografica dei server Web è un altro approccio che vale la pena di considerare” sostiene Schneier, “in questo modo, anche se un server o un segmento di rete viene abbattuto da un attacco, il normale traffico può essere reindirizzato verso altri server”.

Ma mettere in atto una capacità di elaborazione supplementare dei server per gestire gli attacchi DDoS può essere costoso ed è probabile che abbia senso solo per le imprese più grandi. "C'è un certo divario digitale quando si tratta della capacità delle imprese di difendersi da questi attacchi", sostiene Mockapetris.
"La risposta a lungo termine alla protezione DDoS deve arrivare dai server providers", ha detto John Pescatore, un analista di Stamford, "questo perché i service providers sono in una posizione migliore per riuscire a rilevare e bloccare il traffico diretto a uno specifico indirizzo IP[101]". Di conseguenza, è una buona idea richiedere ai service providers di offrire una sorta di garanzia contro gli attacchi DDoS. Pescatore, infatti, sostiene questo principio da oltre due anni, esortando gli utenti a includere un mezzo di protezione DDoS nei loro accordi con i fornitori di servizi Internet e le società di hosting dei data center[102].

Ma meno dell'1% delle aziende nel complesso acquista tali servizi, ha dichiarato Pescatore, "La maggior parte delle aziende dice: 'Non sta piovendo, quindi il tetto non perde. Perché ripararlo?[103]".

---

[101] https://blogs.gartner.com/john_pescatore/2010/01/04/internet-weather-partly-available-with-gusts-of-ddos/
[102] https://searchsecurity.techtarget.com/ehandbook/DDoS-prevention-The-latest-means-and-methods
[103] Ibidem.

3.4 IMPLICAZIONI LEGALI DI MYDOOM

Mydoom è stato un worm che si è servito degli utenti della rete Kaaza per poter mettere a segno un attacco DDoS contro il sito di SCO Group e, nella sua seconda versione, il sito di Microsoft. Gli attacchi DDoS sono una tipologia diffusa di attacco informatico, particolarmente utilizzato al fine di mettere in atto una protesta contro siti di aziende, di organizzazioni o governativi.

Considerato nel contesto delle relazioni e delle norme internazionali, gli attacchi DDoS non possono violare il divieto dell'uso della forza (articolo 2(4) della Carta delle Nazioni Unite) - "è improbabile che un rifiuto temporaneo di servizio sia classificato come uso della forza" (Tallinn Manual, 2012, RULE 11, par. 10) - tuttavia, tale atto può costituire una violazione della legge consuetudinaria di non intervento e dell'immunità e inviolabilità sovrana ("... un attacco di diniego di servizio contro il satellite militare di uno Stato costituirebbe una violazione della sua immunità sovrana" (Manuale di Tallinn, 2012, Regola 4, par. 4)).

Dal punto di vista ambientale, il DDoS può rientrare in termini come "inquinamento" o "emissioni" transfrontaliere[104].

In materia di attacchi DDoS, le norme variano a seconda degli stati.

In Australia, un DDoS, come qualsiasi altro reato digitale, è regolato dalla legislazione del Commonwealth nell'ambito della Parte 10.7 - Reati informatici, come codificato nel Criminal Code Act del 1995. In generale, queste questioni sono sotto la giurisdizione della polizia australiana quando il computer, il sistema o il server interessato si trova in Australia, o vi è un cittadino australiano tra le persone coinvolte[105].

Il Comitato della Convenzione sulla criminalità informatica dell'Unione europea accusa e gestisce legalmente gli attacchi DDoS nella nota guida n. 5 di T-CY, articolo 2, 4, 5, 5, 11, 13.

Il sistema legale del Regno Unito, e più specificamente il Computer Misuse Act del 1990, vieta il DDoS e gli individui coinvolti nell'attacco rischiano fino a 10 anni di carcere[106].

---

[104] Healey & Pitts, 2012
[105] http://www.afp.gov.au/policing/cybercrime/hightech-crime.aspx
[106] http://legalpiracy.wordpress.com, 2011

Negli Stati Uniti le persone che prendono parte ad attacchi DDoS corrono il rischio di essere accusate di reati legali a livello federale, sia a livello penale che civile. Il Computer Fraud and Abuse Act (CFAA) è la legge applicabile in questi casi. Affinché una persona violi il CFAA, deve intenzionalmente causare danni a un sistema informatico facente parte del commercio interstatale o estero[107]. Anche i tentativi di attacchi DDoS possono essere perseguiti[108].

Anche i privati che svolgono il ruolo di intermediario lungo il vettore dell'attacco DDoS, come ad esempio gli Internet Server Providers, possono sporgere un'accusa civile per recuperare le perdite finanziarie subite a causa di una violazione dell'accordo sulle "condizioni di servizio", che tra l'altro ha una validità pari a quella di un contratto legale. Gravi violazioni possono portare a un'azione legale per violazione del contratto e persino alla violazione di beni mobili[109].

[107] Ibidem.
[108] http://users.atw.hu/denialofservice/ch08lev1sec2.html
[109] http://www.technicallylegal.org/the-legality-of-denial-of-service-attacks/, 2010

Nonostante la corrente di pensiero secondo la quale gli attacchi DDoS dovrebbero essere visti come una forma di protesta legale, come fecero comprendere i componenti di Anonymous nel 2013 quando postarono una petizione sul sito della Casa Bianca al fine di ridimensionare il suddetto reato, questa tipologia di attacco informatico è tutt'oggi considerata illegale in tutte le sue forme.

CONCLUSIONI

Lo sviluppo tecnologico globale ha subito una crescita innegabilmente vertiginosa negli ultimi anni, che ha portato ad una serie di conseguenze nell'ambito della sicurezza e della prevenzione informatica. Il mondo si sta digitalizzando sempre di più, siamo circondati dalla tecnologia, e lo sviluppo di software e dispositivi che possano migliorarci la vita è sempre in crescita. Questo porta inevitabilmente ad un aumento del numero dei potenziali obiettivi che un attacco informatico può avere. Da Stuxnet, in particolare, abbiamo imparato che il target di alcuni attacchi si può potenzialmente spostare su oggetti fisici con componenti elettroniche, e che ciò costituisce sicuramente un cambiamento che può portare a conseguenze molto drammatiche. Basti pensare a tutti i sistemi informatici sensibili che troviamo nella vita di tutti i giorni: sistemi ferroviari, ospedalieri, aerei ecc. e tutti questi costituiscono

potenziali obiettivi nel futuro. E' chiaro quindi che con l'aumento della digitalizzazione dei vari ambiti della società si aumentino conseguentemente anche i rischi ai quali ci esponiamo. Un proporzionale aumento degli investimenti nel campo della sicurezza informatica risulta perciò doveroso. E' lecito pensare che in futuro le guerre si combatteranno prevalentemente nel cyber spazio, e che i danni saranno ancora più devastanti di quelli a cui siamo abituati per mezzo di armi o bombe. E' necessario quindi anche sensibilizzare la popolazione mondiale in questo senso, evitando di compiere ingenuità come quelle che hanno portato alla diffusione incontrollata dei malware analizzati in precedenza. Oltre a questo, con il vertiginoso sviluppo tecnologico degli ultimi anni, è necessario che anche il sistema giudiziaro vada di pari passo con le nuove tecnologie informatiche, e che riesca ad occuparsi in maniera più mirata dei reati informatici di tutti i tipi. E' altresì vero che, così come l'antidoping sarà sempre un passo indietro rispetto alla scoperta di nuove sostanze dopanti, anche la prevenzione e la difesa dagli attacchi informatici si troveranno a dover fronteggiare malware che sfrutteranno sempre nuove debolezze non scoperte in precedenza. Quindi, se da una parte la velocità dello sviluppo tecnologico ha permesso e permette tutt'ora di migliorare le nostre vite e il modo in cui possiamo risolvere problemi di qualsiasi tipo,

dall'altra ci espone a rischi di cui potenzialmente non possiamo conoscere né l'entità né gli eventuali danni, impedendoci inoltre di poterli gestire dal punto di vista giuridico, preparando quello che probabilmente sarà il terreno di guerra di un futuro non troppo lontano.

BIBLIOGRAFIA

1. "How Iran Went Nuclear," New Statesman, Giugno 22, 2009.
2. Greg Bruno, "Iran's Nuclear Program," Council on Foreign Relations, Marzo 10, 2010.
3. "Tehran Nuclear Research Center," The Institute for Science and International Security.
4. Greg Bruno, "Iran's Nuclear Program".
5. Sam Sasan Shoamanesh, "History Brief: Timeline of US-Iran Relations until the Obama Administration," MIT International Review.
6. Henry U. Ufomba e Robert O. Dode, "Which Way to Tehran? Pre-emptive Air Strike Cumulative Diplomacy, Technical Isolation and the Iranian Nuclear Crises," Journal of Public Administration and Policy Research 2, (2010).
7. William Burr, "A Brief History of US-Iranian Nuclear Negotiations," Bulletin of the Atomic Scientists.
8. "Smiling Buddha: 1974," http://nuclearweaponarchive.org/India/IndiaSmiling.html.
9. Adam Tarock, "Iran's Nuclear Programme and the West,".
10. President George W. Bush, "President Bush Addresses American Legion National Convention," The White House, http://georgewbushwhitehouse.archives.gov/news/releases/2006/08/20060831-1.html
11. Joe Weiss (leading control systems cyber security expert), intervista telefonica, Giugno 2, 2012.

12. Bruce Dang, “Adventures in Analyzing Stuxnet,” (presentation at 27th Chaos Communication Congress, Berlino, Germania, Dicembre 27-30, 2010).
13. Zetter, Kim (11 July 2011). “How digital detective deciphered Stuxnet, the most menacing malware in history” arstechnica.com .
14. Nicolas Falliere, Liam O Murchu, and Eric Chien, “W32.Stuxnet Dossier,”Symantec Security Response.
15. “Visit to Natanz Facility,” 2011 Presidency of the Islamic Republic of Iran, Aprile 8, 2008.
16. Ralph Langner, “Stuxnet: A Deep Dive,” (presentation at Digital Bond’s SCADA Security Scientific Symposium, Miami, Florida,Gennaio 19-20, 2012).
17. Ralph Langner (leading Stuxnet expert), discussion with author, 11th Control System Cyber Security Conference, Washington DC, Ottobre 17-21, 2011.
18. Nicolas Falliere, Liam O Murchu, and Eric Chien, “W32.Stuxnet.Dossier.”.
19. Elizabeth Montalbano, “Stuxnet, Duqu Date Back to 2007, Research Says,”.
20. William Yong and Robert F. Worth, “Bombing Hit Atomic Experts in Iran Streets,” The New York Times, 29 Novembre 2010.
21. David Albright, Paul Brannan, and Christina Walrond, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” Institute for Science and International Security, 22 Dicembre 2010.
22. “Presidential Decision Directive/NSC-63,” The White House, 22 Maggio 1998.
23. Karnouskos, “Stuxnet Worm Impact on Industrial Cyber-Physical System Security.”
24. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran.”
25. Falliere, Murchu and Chen, “W32.Stuxnet Dossier”
26. Langer, “To Kill a Centrifuge”
27. Karnouskos, “Stuxnet Worm Impact on Industrial Cyber-Physical System Security.”
28. Kroft, “Stuxnet: Computer Worm Opens New Era of Warfare.”
29. “Cyber Terror Targets Utilities,” May 31, 2012,

30. http://www.news24.com/SciTech/News/Cyber-terror-targets-utilities-20120531
31. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran.”
32. Nakashima, “Stuxnet Malware Is Blueprint for Computer Attacks on U.S.”
33. Kroft, “Stuxnet: Computer Worm Opens New Era of Warfare.”
34. Kushner, “The Real Story of Stuxnet.”
35. Jim E. Crouch and Larry K. McKee Jr., “Cybersecurity: What Have We Learned?,”
36. National Security Cyberspace Institute, October 9, 2011, 1, http://www.nsci-va.org/WhitePapers/
37. 2011-10-09-Cyber%20Lessons%20Learned-Crouch-McKee.pd
38. Hosenball, “Experts Say Iran Has Neutralized Stuxnet Virus.”
39. Eric Cole, “Insider Threats and the Need for Fast and Directed Response,” SANS
40. Institute, Aprile 2015, 6, https://www.sans.org/reading-room
41. Urrico, “Negating Cybersecurity Threats from Within.”
42. Doug Niblick, “Protecting Critical Infrastructure against the Next Stuxnet,” Davenport
43. University, Marzo 20, 2013, 19, http://www.davenport.edu/system/files/Protecting_Critical_Infra
44. structure_Against_the_Next_Stuxnet.pdf.
45. Falliere, Murchu, and Chen, “W32.Stuxnet Dossier”
46. Crouch and McKee Jr., “Cybersecurity: What Have We Learned?”.
47. Niblick, “Protecting Critical Infrastructure against the Next Stuxnet”.
48. Davis, “Stuxnet Reality Check: Are You Prepared for a Similar Attack?”.
49. https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1009&context=jil
50. Bruce Cronin, Reckless Endangerment Warfare: Civilian Casualties and the Collateral Damage Exception in International Humanitarian Law, 50 J. PEACE RES. 175, 176–77 (2013)
51. Singer & Allan Friedman, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW

52. George R. Lucas, PERMISSIBLE PREVENTIVE CYBERWAR: RESTRICTING CYBER CONFLICT TO JUSTIFIED MILITARY TARGETS (2011);
53. Mark Clayton, From the Man Who Discovered Stuxnet, Dire Warnings One Year Later, CHRISTIAN SCI. MONITOR (22 Settembre 2011), http://www.csmonitor.com/USA/2011/0922/From-the-man-who-discoveredStuxnet-dire-warnings-one-year-later.
54. Zetter, Kim (28 Maggio 2012) "Meet 'Flame': The Massive Spy Malware Infiltrating Iranian Computers".
55. Gostev, Alexander (Maggio 2012) "The Flame: Questions and answers".
56. Hopkins, Nick (28 Maggio 2012) "Computer worm the hit iran oil is more complex yet".
57. Erdbrink, Thomas (23 Aprile 2012) "Facing Cyberattack, Iranian Officials Disconnect some Oil Terminals From Internet" New York Times.
58. "Flame malware makers send 'suicide' code" BBC News, 8 Giugno 2012.
59. Michael N. Schmitt, The Tallinn Manual on the International Law Applicable to Cyber Warfare (New York:
60. Cambridge University Press, 2013)
61. Julius Stone, "Legal Problems of Espionage in Conditions of Modern Conflict"
62. Quincy Wright, "Espionage and the Doctrine of Noninterference in Internal Affairs"
63. Christopher D Baker, "Tolerance of International Espionage: A Functional Approach,"
64. Sean P Kanuck, "Information Warfare: New Challenges for Public International Law,"
65. Jeffrey TG Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare"
66. Anna Wartham, "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate
67. UN Charter Provisions Prohibiting the Threat or Use of Force?"
68. Michael N. Schmitt, The Tallinn Manual on the International Law Applicable to Cyber Warfare (New York:
69. Cambridge University Press, 2013)
70. CNN.com – Security Firm: Mydoom worm fastest yet, 2004

71. 'MORE DOOM?' europe.newsweek.com
72. 'Causa Caldera – Microsoft' - digitalresearch.biz
73. 'Mydoom virus starts to fizzle out' - news.bbc.co.uk
74. 'What You Should Know About the Mydoom Worm Variants: Mydoom.A and Mydoom.B' - information.microsoft.com
75. https://www.giac.org/paper/gcih/568/mydoom-dom-anlysis-mydoom-virus/106069
76. https://antivirus.comodo.com/blog/comodo-news/mydoom-virus/
77. 'The Seattle Times: Business & Technology: E-mail viruses blamed as spam rises sharply' - seattletimes.nwsource.com
78. https://blogs.gartner.com/john_pescatore/2010/01/04/internet-weather-partly-available-with-gusts-of-ddos/
79. https://searchsecurity.techtarget.com/ehandbook/DDoS-prevention-The-latest-means-and-methods
80. Healey & Pitts, 2012
81. http://www.afp.gov.au/policing/cybercrime/hightech-crime.aspx
82. http://legalpiracy.wordpress.com, 2011
83. http://users.atw.hu/denialofservice/ch08lev1sec2.html
84. http://www.technicallylegal.org/the-legality-of-denial-of-service-attacks/, 2010

Ringraziamenti

In poche righe riuscire a ringraziare adeguatamente tutte le persone che sono state fondamentali durante questa parte della mia vita lo trovo estremamente difficile, ma provarci è il minimo che possa fare.
Anzitutto desidero ringraziare il professor Stefano Pietropaoli, che con grande attenzione, precisione e disponibilità mi ha aiutato a svolgere il presente elaborato.
Grazie ai ragazzi della Comunità Ebraica, in particolare a Jacopo, Federico, Andrea e Noemi, che dall'inizio di questo percorso mi hanno sostenuto nei momenti difficili, e hanno saputo darmi conforto quando ne ho avuto più bisogno. Quando l'intenzione era di lasciar perdere tutto, siete sempre stati lì a dirmi che dovevo continuare. Da voi ho imparato quanto le amicizie di vecchia data possano costituire un punto di riferimento nella vita.
Grazie ai Chewbacca, nonché i miei ex compagni di liceo, che mi hanno sempre saputo dare consigli quando mi stavo perdendo d'animo, e la cui leggerezza e simpatia hanno costituito uno strumento che mi ha aiutato a ridimensionare molte preoccupazioni che ho avuto, talvolta banali. Vedere i vostri successi mi ha sempre dato una grande carica, e poter contare ancora su di voi dopo tutto questo tempo è stato fondamentale. Un ringraziamento particolare va a Sofia: il terrore di vedere una chiamata da parte sua quando si è in ritardo la mattina per andare in biblioteca vi assicuro fa aprire gli occhi dieci minuti prima della sveglia. Un'amica che non solo mi ha fatto ritrovare un ordine nel momento più buio della mia carriera universitaria, ma che mi ha anche fatto da spalla nella vita di tutti i giorni, senza mai pretendere nulla in cambio. Da tutti voi del liceo ho imparato che a certi episodi della vita si dà un'importanza eccessiva, e che una cena in compagnia prendendosi un po' in giro può davvero risollevare l'animo quando se ne ha bisogno.
Grazie al Team105, i miei compagni di università, senza i quali non sarei letteralmente riuscito a passare certi esami. Ma l'amicizia che si è formata in questi anni, al di là di quella dovuta alla frequentazione della stessa facoltà, è stata ancora più fondamentale. Bocciare tutti insieme un esame, passarlo tutti insieme, aiutare chi rimaneva indietro, la pastina al bar, i viaggi, le passeggiatine, l'acquina, i caffè (sospesi), le cene e i pranzi, i sushi, i lampredotti, gli sporadici discorsi seri e tutto quello che c'era intorno è sempre stato sintomo della presenza di qualcosa che andava al di là del legame scolastico. Da voi ho imparato l'importanza di avere a fianco a sé delle persone fidate durante il raggiungimento di uno scopo comune, e a quello per voi accosto un sentito ringraziamento al Dipa, compagno di merende e di esami. Colgo l'occasione per ringraziare tutta la Oneplus e i suoi dipendenti: ottimo lavoro ragazzi.
Grazie a Piero, Andry e Ema, i castruviddari coi quali ho convissuto durante l'ultimo periodo della mia carriera universitaria, e che mi hanno sostenuto nella spinta finale. In particolar modo ringrazio Piero, per tutto quello che ha fatto per me, e per avermi fatto capire che non siamo fuorilegge ma abbiamo necessità. Da voi ho imparato che certe volte non bisogna prendersi troppo seriamente, e che è importante dare il giusto peso agli avvenimenti della propria vita.
Grazie a Romina, un'amica sulla quale ho sempre potuto contare fin dalle medie.
Grazie a mia zia Leda, che per me ha sempre avuto una buona parola o un consiglio nelle situazioni di difficoltà.
I ringraziamenti più importanti vanno a mia sorella, mia madre e mio padre.
Se state tenendo in mano la mia tesi di laurea è perché ho avuto la fortuna di avere due genitori che hanno fatto sacrifici immensi per potermi rendere ciò che sono, e una sorella senza la quale non avrei saputo affrontare certi momenti della mia vita. Mamma, babbo, Adele: se state leggendo queste righe è perché non mi avete mai fatto mancare nulla, e di questo vi sarò sempre grato. Mi avete sempre sostenuto in tutto quello che ho fatto, e senza di voi non ci sarebbe stato niente di tutto questo. La felicità che provo scrivendo queste righe la devo a voi.
Vi ringrazio di essere quello che siete per me.