04|2014

NEL PASSATO DELLA CYBER SECURITY

Parte I, 1990 - 2005

A cura di
Francesco Corona

CISINT Centro Italiano di Strategia e Intelligence

LIMITAZIONE DELLA RESPONSABILITÀ

Le opinioni espresse nel presente documento, rilasciato a scopo informativo, sono di responsabilità esclusiva dell'autore e non riflettono necessariamente la posizione ufficiale del CISINT - Centro Italiano di Strategia e Intelligence.

www.cisint.org **info@cisint.org**

Sommario

INTRODUZIONE

L'obsolescenza media dei numerosi avvenimenti globali riguardanti i fenomeni legati al Cyberspace ha raggiunto e forse superato quella delle stesse tecnologie infrastrutturali coinvolte al proprio mantenimento. In un processo temporale sempre più ridotto di svecchiamento delle componenti elettroniche e similmente comunicazionali, la percezione comune dei fenomeni avvenuti pochi anni or sono è quella di eventi appartenuti al nostro passato remoto. Non commettendo errori di valutazione, fisseremo in modo organico fatti e avvenimenti di qualche anno fa per meglio comprendere la situazione attuale sul fronte del fenomeno Hacking, ciò al fine di offrire alcune previsioni per il prossimo futuro. Concentreremo pertanto l'attenzione su quella particolare strategia di attacco che rappresenta de facto una seria minaccia per organizzazioni, enti, istituzioni pubbliche e private, lasciando al lettore una serie di riferimenti bibliografici per un quadro d'insieme dettagliato del fenomeno trattato.

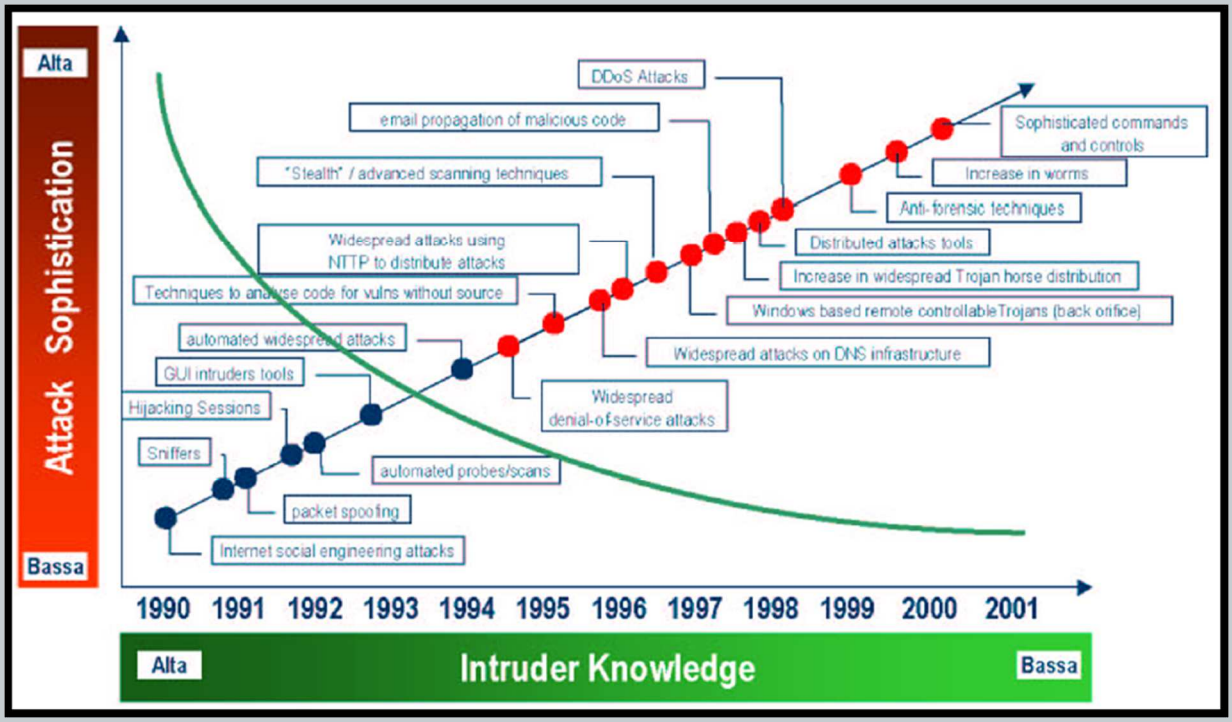

Fig.1.a - Evoluzione delle tipologie di attacco dal 1990 al 2001 - Fonte: CERT Carnegie Mellon University, 2004

Nella fig.1.a si evidenzia una escalation del genere e del livello di sofisticazione relativa alle tipologie di attacco su scala temporale, a partire dal 1990 sino al 2001. In realtà questi attacchi sono stati resi possibili dall'implementazione su vasta scala del protocollo TCP/IP che risultava e risulta tuttora essere lo standard per l'accesso a Internet.

Per una scelta di realizzazione, infatti, non è stata posta particolare sicurezza sull'identificazione del mittente di ogni pacchetto e se ciò da una parte consente di ottenere garanzie di anonimato, dall'altra può essere sfruttato con apposite tecniche per indurre a

credere che il pacchetto stesso provenga da sistemi differenti, rispetto a quello effettivo. Suddette limitazioni in parte sono state superate dalla ricerca attuale, in seguito all'adozione del protocollo IPv6.

EVENTI CORRELATI

Ciò che risulterà chiaro, dal presente studio, è che a partire dal 2000 i Cyber Attack hanno assunto connotazioni più sofisticate, crescendo di numero e portata. Inoltre è stata rilevata una correlazione, sostenibile con dati oggettivi, tra attacchi hacker di portata globale (Stati Uniti, Israele, India, Europa, Medio Oriente) come quelli verificatisi tra il 2000 e il 2001 e gli attacchi terroristici alle Torri Gemelle o i bombardamenti NATO in Serbia. Tali correlazioni viste alla luce di recenti valutazioni analitiche, non paiono più essere casuali ma inseribili in un quadro strategico ben preciso legato a obiettivi geopolitici e terroristici.

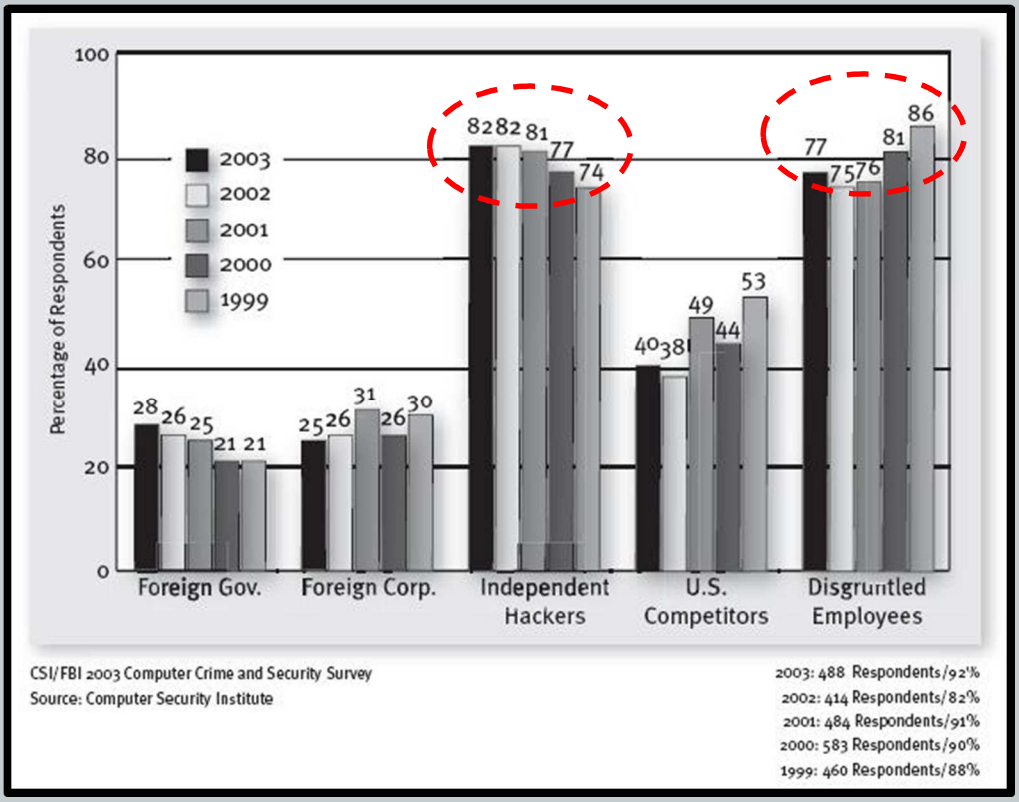

Fig.1.b – Provenienza di attacchi in % nel Cyberspace – Fonte: Computer Security Institute (CSI/FBI)

In figura 1.b presentiamo una proiezione di fonte FBI dalla quale risulta evidente come la più alta percentuale di attacchi compiuti dal 1990 al 2003 sul territorio degli Stati Uniti sia provenuta da hacker indipendenti e da impiegati con risentimenti verso le aziende di origine, seguite da attacchi pilotati da governi stranieri e/o da aziende competitrici a quelle statunitensi.

Da questo quadro risulta evidente come le tipologie di attacco attuate in quegli anni possono essere diversificate con scopi e modalità differenti.

Ricordiamo a tal proposito che nei primi mesi del 2000 sono stati rilevati i primi cambiamenti nel livello di sofisticazione degli attacchi nel Cyberspace, consistenti in sabotaggi effettuati contro siti Internet di importanti organizzazioni internazionali operanti in molteplici settori tecnologici e dei media.

Molti dei principali siti Internet sono stati resi inutilizzabili da quello che è apparso il più massiccio attacco DDoS[1] lanciato sulla rete. Il motore di ricerca Yahoo! è stato il primo a subire tale attacco, riportando un blackout di tre ore la domenica del 6 febbraio 2000. Ancora, il sito Buy.com non è risultato raggiungibile la mattina di lunedì 7 febbraio, i siti di CNN ed eBay non lo sono stati nel pomeriggio mentre quelli di Amazon e ZDNet sono rimasti isolati a lungo nelle ore notturne della medesima giornata.

Nello stesso periodo sono stati inoltre rilevati (in alcuni casi anche personalmente studiati) attacchi nei confronti di Università e Centri di Ricerca italiani. Nella primavera del 2000, è stato rilevato un poderoso cyber attack di tipo DDoS contro le infrastrutture NATO in Kosovo e Serbia, presumibilmente organizzato da gruppi ostili alla campagna di bombardamenti avviata dalla NATO contro la Serbia, confluiti nel nuovo esercito della già Repubblica Federale di Jugoslavia. Tale attacco è stato causa di numerosi danni a infrastrutture telematiche per le comunicazioni e ad alcuni servizi collegati. Nell'ottobre 2000 sono stati compiuti attacchi per fasi al Knesset (Israeli Parliament), all'IDF (Israeli Defence Forces), all'IMFA (Israeli Ministry of Foreign Affairs) e infine alla Banca di Israele con il Tel Aviv Stock Exchange, in una sorta di ***cyber jihad*** islamica che ha coinvolto tutti gli ISP (Internet Service Provider) israeliani.

Se il 2000 si è concluso con attacchi di portata globale mai verificatisi prima, è pur vero che il successivo anno 2001 ha rappresentato l'apoteosi degli attacchi nel Cyberspace, molti dei quali ben occultati dalle stesse organizzazioni coinvolte tanto da far apparire il 2000 come un semplice test preliminare rispetto al 2001, in quella che potremo senza alcun dubbio definire un'annata di attacchi eccezionale. Infatti sono stati rilevati attacchi su scala globale concentrati nei mesi di aprile e luglio negli Stati Uniti, in Medio Oriente, in Europa e in India. Gli attacchi di aprile hanno coinvolto in special modo importanti enti governativi americani; sono stati isolati e analizzati, giungendo a comprendere che la Cina era il paese di provenienza. Presumibilmente essi rappresentavano un atto di rivendicazione patriottica, da parte di gruppi hacker rispettivamente denominati "Honkey Union of China" e "Chinese Red Guest"[2]. Ciò avveniva a seguito dell'incidente diplomatico risalente al 1° aprile 2001, avvenuto nei cieli del Mar della Cina. L'episodio si era concluso con la morte di un pilota militare cinese e l'atterraggio fortunoso di un Ercules C130 americano, all'interno del quale era installato un sofisticato apparato tecnologico ECHELON. L'equipaggio del velivolo americano sarebbe stato rilasciato a distanza di qualche giorno.

[1] DDoS - Distributed Denial of Service è una tipologia di attacco tramite il quale si attiva un numero elevatissimo di false richieste di servizio, provenienti da più computer e indirizzate al medesimo server, al fine di destabilizzarne la funzionalità e ottenere una negazione di servizio.
[2] Cyber Attack During The War on Terrorism: A Predictive Analysis, M.A.Vatis, Dartmouth College, Hanover, NH. Institute for Security Technology Studies - 2001

2001 - CYBER ATTACK CONCOMITANTI ALL'11/09

Gli attacchi del luglio - agosto 2001 hanno coinvolto numerose organizzazioni industriali e scientifiche europee e indiane. Analizzando un exploit di attacco per conto di un importante ente di ricerca italiano, è stato possibile costatarne la brillante strategia, organizzata in tre fasi distinte, messa in atto da hacker non certo sprovveduti e ben organizzati:

1. Sondaggio dell'infrastruttura con tecniche di scansione delle porte TCP/IP;
2. Attivazione di worm/file infector del tipo NIMDA e FUNLOVE con internal scanning delle porte precedentemente identificate, risultate libere per attuare una propagazione di attacco in rete su diverse dorsali[3];
3. Controllo remoto delle sotto-reti infestate da parte di un hacker esterno, il quale svolge attività di spionaggio e prelievo illecito di file.

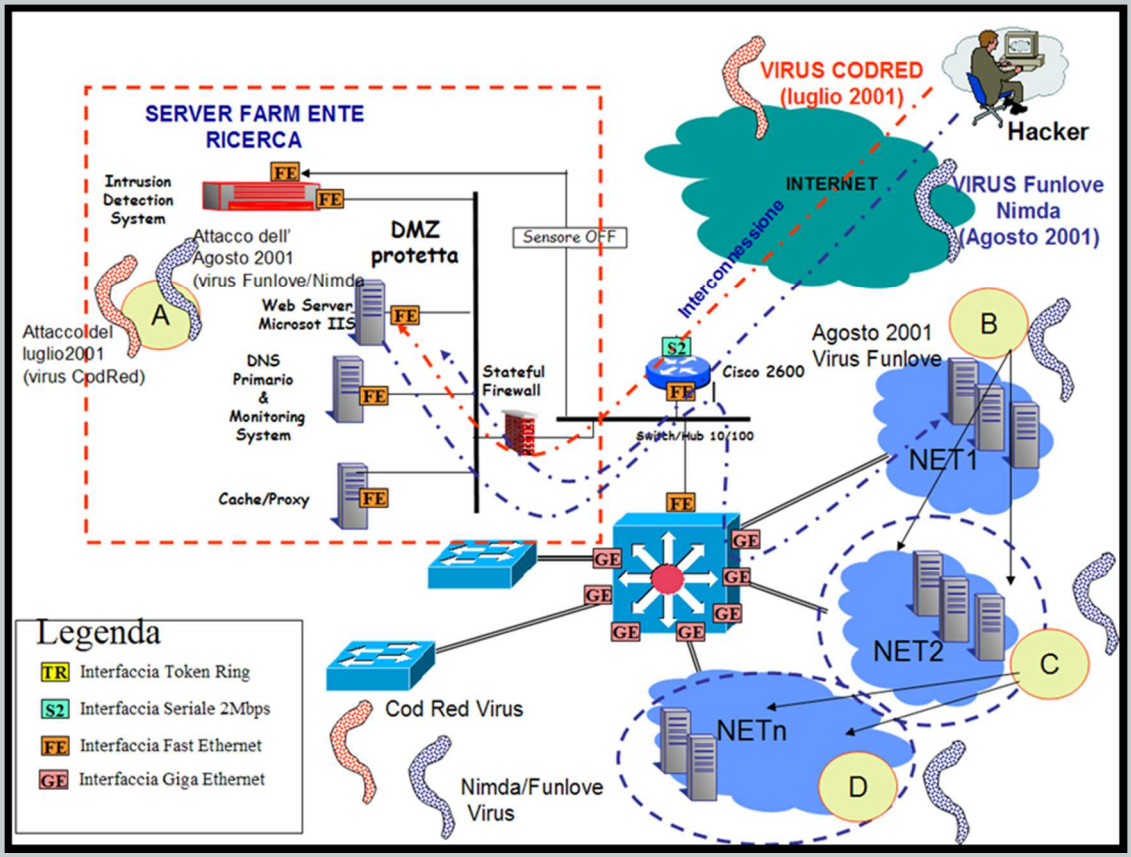

Fig.2 - Esempio di propagazione dell'attacco del luglio - agosto 2001

Tipicamente l'exploitation di un attacco è un evento anticipato da cali di performance su tutti i sistemi della rete per l'intensa attività di broadcast generata dal traffico di scansione o di saturazione prodotto dai worm o da tool specifici, a caccia di passaggi liberi tra i "gate" del

[3] Le dorsali o backbone sono reti fisiche di connessione e trasmissione ad alta velocità, estese centinaia di migliaia di chilometri, alle quali sono connessi i "rami" secondari, caratterizzati da una velocità di trasmissione inferiore.

protocollo TCP/IP (questi ultimi sono recuperabili anche su siti di download gratuiti dell'epoca, come ad esempio astalavista.com).

CYBER ATTACK DAL 2001 AL 2004

Le tensioni riscontrate nel 2001 tra Pakistan e India per la disputa territoriale del Kashmir, alla vigilia della caccia ai talebani in Afghanistan e nei territori di confine, hanno creato anche una situazione di diffusione di siti web Pro-Pakistan in India, consentendo la disseminazione di informazioni destabilizzanti. La vulnerabilità delle infrastrutture indiane come Zee Network TV, del Parliament of India, l'Indian Institute of Science e il Bhabha Atomic Research Center (BARC) è stata notata nell'immediato, allorché l'equivalente di 5 megabyte di dati sensibili sono stati sottratti dal BARC in uno degli attacchi informatici che si sono susseguiti in quei giorni. Tali attacchi sono stati condotti dal "PHG - Pakistan Hackerz Group", già conosciuto dalle autorità statunitensi per i tentativi di intrusione perpetrati nei confronti del DoE - Department of Energy e della sede centrale appartenente all'US Air Force. A distanza di circa tre anni gli attacchi, inquadrati principalmente nella categoria di sofisticati DDoS, si sono susseguiti senza interruzione nonostante le nuove contromisure adottate, basate prevalentemente su apparati di Intrution Detection (IDS), Firewall multilivello e sistemi di tracciamento HoneyPot[4], consentivano ai Security Manager di garantire maggiore sicurezza rispetto al 2001.

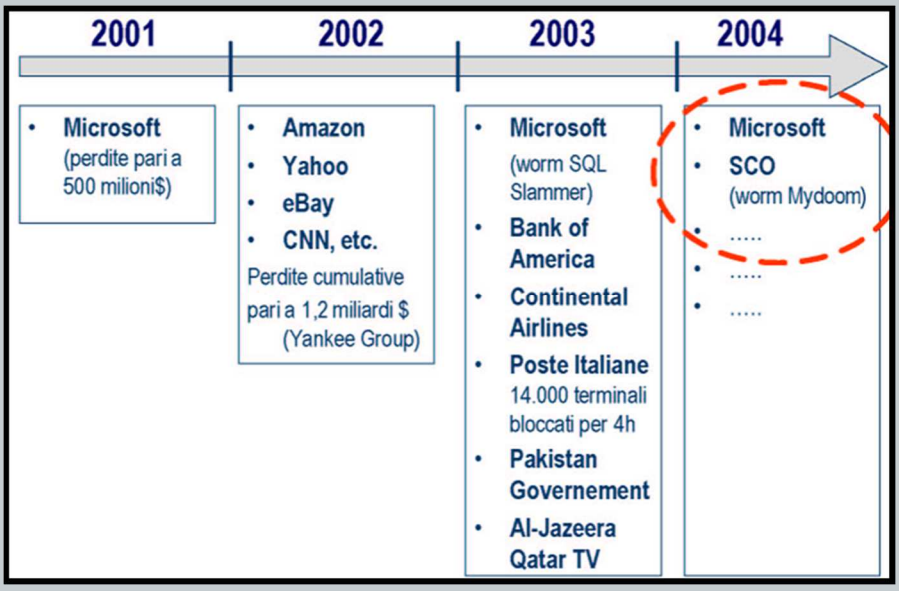

Fig. 3 Principali tipi di attacchi tra il 2001 e il 2004. - Fonte: Infosecurity Italia

[4] Il termine "HoneyPot" (letteralmente, barattolo di miele) identifica un sistema hardware o un'applicazione software utilizzata come "esca", ovvero una trappola contro eventuali attacchi informatici.

Gli attacchi più pericolosi appaiono essere quelli condotti all'interno delle reti intranet aziendali, tramite l'introduzione di ***trojan horse*** (Cavallo di Troia) a propagazione virale esponenziale.

Nel 2003 il worm SQL Slammer (conosciuto anche come W32.SQLExp.Worm) è stato il più dannoso mentre nel 2004 il worm Mydoom si è diffuso senza precedenti, tramite gli indirizzi email di circa un milione di utenti e infettandone i relativi computer. Detto ciò, gli attacchi più diffusi dal 2001 al 2005 sono inquadrabili nelle categorie:

- virus, worm e trojan horse;
- Packet Sniffing;
- IP spoofing;
- Mail spoofing;
- Mail bombing;
- DoS (Denial of Service);
- Telnet, FTP bounce;
- Exploit (bachi del software).

LIVELLI DI SOFISTICAZIONE - Distributed DoS (DDoS)

Uno dei più pericolosi attacchi, per la sua complessità strategica, risultava essere il DDoS. Esso consiste in una tipologia di attacco nel quale gli hacker attivano un numero elevatissimo di false richieste di servizio, provenienti in contemporanea da più macchine e rivolte al medesimo server, consumando le risorse di sistema e di rete del fornitore del servizio. In questo modo le strutture informatiche dell'azienda, dell'ente o del provider "affogano" letteralmente sotto le richieste incessanti, poiché non più in grado di erogare i servizi per i quali sono preposte, risultando quindi irraggiungibile.

In occasione di tali eventi, alcuni dei network provider coinvolti hanno dichiarato di essere stati sommersi da oltre 1 Gigabyte al secondo di traffico. In realtà, il più delle volte, questo tipo di attacco occulta un ben più serio pericolo: il controllo totale del/dei sistema/i sotto attacco da parte dell'hacker, il quale trasforma il sistema nel così detto "zombie" al proprio servizio, anch'esso pronto a sferrare attacchi su nuove direttrici di rete. Anche se questo genere di attacco non è affatto nuovo sulla rete, non ne erano mai stati rilevati su così vasta scala, e su così tanti obiettivi importanti quasi in contemporanea in quel particolare periodo storico.

Gli antenati degli attacchi attuali si manifestavano esaurendo le risorse hardware della vittima, quali lo spazio su disco, la memoria e la CPU: ciò era ottenibile spedendo pochi pacchetti malformati che mandavano in crash il sistema remoto. La più nota tra le utility di questo genere è stata Nuke mentre il sistema più utilizzato è stato il WinNuke, in grado di mandare in crash molti computer desktop. Il primo (e il più abusato) prodotto di DoS che ha acquisito notorietà è stato lo Smurf Attack che tutt'oggi è in grado di paralizzare reti con tecnologie non aggiornate (generalmente piccole/medie aziende e ISP locali). In seguito è stato utilizzato The LowDown, conosciuto anche come **Network Saturation Attack** o **Bandwidth**

Consumption Attack: un nuovo attacco DoS in grado di inondare un network con un numero impressionante di pacchetti. I router e i server che subiscono l'attacco, nel tentativo di gestire correttamente il traffico, subiscono un eccessivo carico di lavoro a causa del quale interrompono la propria funzionalità. Ovviamente l'eccesso di traffico ostile rende impossibile anche il traffico lecito (posta, web, file transfer ecc.) bloccando intere reti in pochi minuti.

La generazione successiva, attualmente impiegata, è appunto quella degli attacchi di tipo **Distributed Denial of Service (DDoS)** e **Distributed Reflection Denial of Service (DRDoS)**. Spingendo all'eccesso l'idea del network saturation attack, il DDoS ripete lo stesso approccio utilizzando però diversi punti d'ingresso contemporanei: in questo modo un *cracker*[5] è in grado di mettere in ginocchio sistemi più grandi che sarebbero indifferenti a un singolo flood. Per effettuare questo genere di operazione si deve poter installare un proprio agente sui sistemi da cui si vuole scatenare l'attacco stesso. È quindi una tecnica che viene preparata per tempo, attrezzandosi con un pool di macchine compromesse da poter scagliare contro il sistema vittima. Il DRDoS consiste invece nell'attuazione di un DDoS con ulteriore moltiplicazione delle fonti di attacco. Ciò avviene mediante il reclutamento di server operanti su larga banda (ISP Server o DSL Bandwith Server) innescati da delle SYN request (richieste di connessione) che propagano i pacchetti SYN/ACK in modalità esponenziale.

[5] Il cracker è un individuo in grado di effettuare azioni di *crash* di sistemi telematici, alterandone il codice di funzionamento.

BIBLIOGRAFIA

[01] L.J. jr. Hughes – Tecniche di sicurezza in Internet, Jackson Libri - 1996

[02] F. Corona - Web Intelligence, dispense corso Techno-Intelligence del Master in Sicurezza e Intelligence (MAINS) Link Campus Università di Malta – Roma, 2004

[03] R. Shea - L2TP - Addison Wesley

[04] R. MansField – Hacker Attack! – SYBEX

[05] M. Strebe, C.Pekins – Firewalls – SYBEX

[06] P.E. Proctor – Intrusion Detection HandBook – PH PTR

[07] Mel Baker – Cryptology/Decryptology – Addison Wesley

[08] M.A. Vatis, Cyber Attacks During the War on Terrorism: A Perspective Analysis - Istitute for Security Technology Studies, Dartmouth College - 2001

[09] MIS Training Istitute, Infosecurity University Book - Las Vegas - 2002

[10] Nina Hachigian, China's Cyber-Strategy, 2003

[11] Dispense sessione di conferenze del Clusit, www.infosecurity.it - 2004

[12] Silverman R., Intrusion Detection Systems Sniff Out Digital Attack, The Wall Street Journal, pg. B6 - February 4, 1999

[13] Bass T., Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness, Communications of the ACM (to appear) - 1999

[14] de Bony E., NATO Reinforces against Net Attack from Serbs, InfoWorld Electric, Posted at 9:40 AM PT - Apr 2, 1999

[15] Bass T., Freyre A., Gruber D. and Watt. G., E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Brand Integrity, IEEE Network, pp. 10-17, Vol. 12, No. 2 - March/April 1998

[16] Denning D.,An Intrusion-Detection Model, IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp. 222-232 - February 1987

[17] Mukherjee B., Heberlein L., and Levitt K., Network Intrusion Detection, IEEE Network Magazine, Vol. 8. No. 3, pp. 26-41 - May/June 1994

[18] Denning D. et al., A Prototype IDES: A Real Time Intrusion Detection Expert System, Computer Science Laboratory, SRI International - August 1987

[19] Snapp S. et al., A System for Distributed Intrusion Detection, Proceedings of IEEE COMPCON, pp. 170-176 - March 1991

[20] Bauer D. and Koblentz M., NDIX - An Expert System for Real-Time Network Intrusion Detection, Proceedings of the IEEE Computer Networking Symposium, pp. 98-106 - April 1988

[21] Hochberg et al., NADIR: An Automated System for Detecting Network Intrusion and Misuse, Computers & Security, Elsevier Science Publishers, pp. 235-248 - 1993

[22] Heberlein L. et al., A Network Security Monitor, Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, pp. 296-303 - May 1990

[23] Waltz E. and Llinas, J., Multisensor Data Fusion, Artech House, Boston, MA - 1990

[24] Waltz E., Information Warfare Principles and Operations, Artech House, Boston, MA - 1998

[25] Hall D., Mathematical Techniques in Multisensor Data Fusion, Artech House, Boston, MA - 1992

[26] Varshney P., Distributed Detection and Data Fusion, Springer-Verlag, New York, NY - 1996

[27] Antony R., Principles of Data Fusion Automation, Artech House, Boston, MA - 1995

[28] Rose M., The Simple Book, Prentice-Hall, Englewood Cliffs, NJ -1994

[29]Stevens R., TCP/IP Illustrated, Volume 1: The Protocols, Addison-Wesley, Reading, MA - 1994

[30] Bass T., Cyberspace Situational Awareness and Cyber Rules for Engagement, Silk Road - December 8, 1998.

[31] Graham B., Cyberwar: A New Weapon Awaits a Set of Rules, The Washington Post, pp. A1, A10 - July 8, 1998

[32] Schultz G., Chairman, Detection of Malicious Code, Intrusions, and Anomalous Activity Workshop, Department of Energy, National Security Council & Office of Science and Technology Policy - February 22-23, 1999

L'AUTORE

Francesco Corona

È Consigliere e membro fondatore del CISINT, Direttore Programmi di Ricerca e Sviluppo e del Comitato Scientifico appartenenti all'Associazione. Autore di numerose pubblicazioni di carattere scientifico, relatore e conferenziere, è laureato in Scienze dell'Informazione presso la Facoltà di Scienze Matematiche, Fisiche e Naturali dell'Università di Bari. Ha conseguito il Master in Marketing presso l'Università LUISS "Guido Carli" di Roma. Ha ricevuto incarichi di ricerca al CNR - IASI di Roma, come specialista in Tecniche di Simulazione e Intelligenza Artificiale, oltre a ricoprire il ruolo di Senior Consultant presso importanti aziende private, lavorando in team internazionali. Nell'ambito della sicurezza informatica ha partecipato, per oltre un ventennio, a numerosi progetti con i principali player in ambito internazionale. Per diversi anni è stato docente di tecniche di Cybersecurity e contro-sabotaggio telematico presso la Scuola di Addestramento del Ministero dell'Interno. Dal 2000 al 2012 è stato professore a contratto presso la Facoltà di Ingegneria Gestionale dell'Università Roma2 "Tor Vergata", oltre che titolare di corsi universitari integrativi. Possiede vari depositi SIAE per opere di ingegno in ambito di Intelligence Ambientale, Sicurezza nelle Telecomunicazioni Mobili e Ottimizzazione Logistica. Nel 2013 ha ottenuto il prestigioso Premio Nazionale per l'Innovazione, conferito dal Presidente della Repubblica, oltre al Premio Confindustria "Convergenza - TLC driven".

CISINT
Centro Italiano di Strategia e Intelligence

Via Clelia 45, 00181 - Roma

Tel/Fax: (+39) 06 7808035

Email: info@cisint.org

www.cisint.org