Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

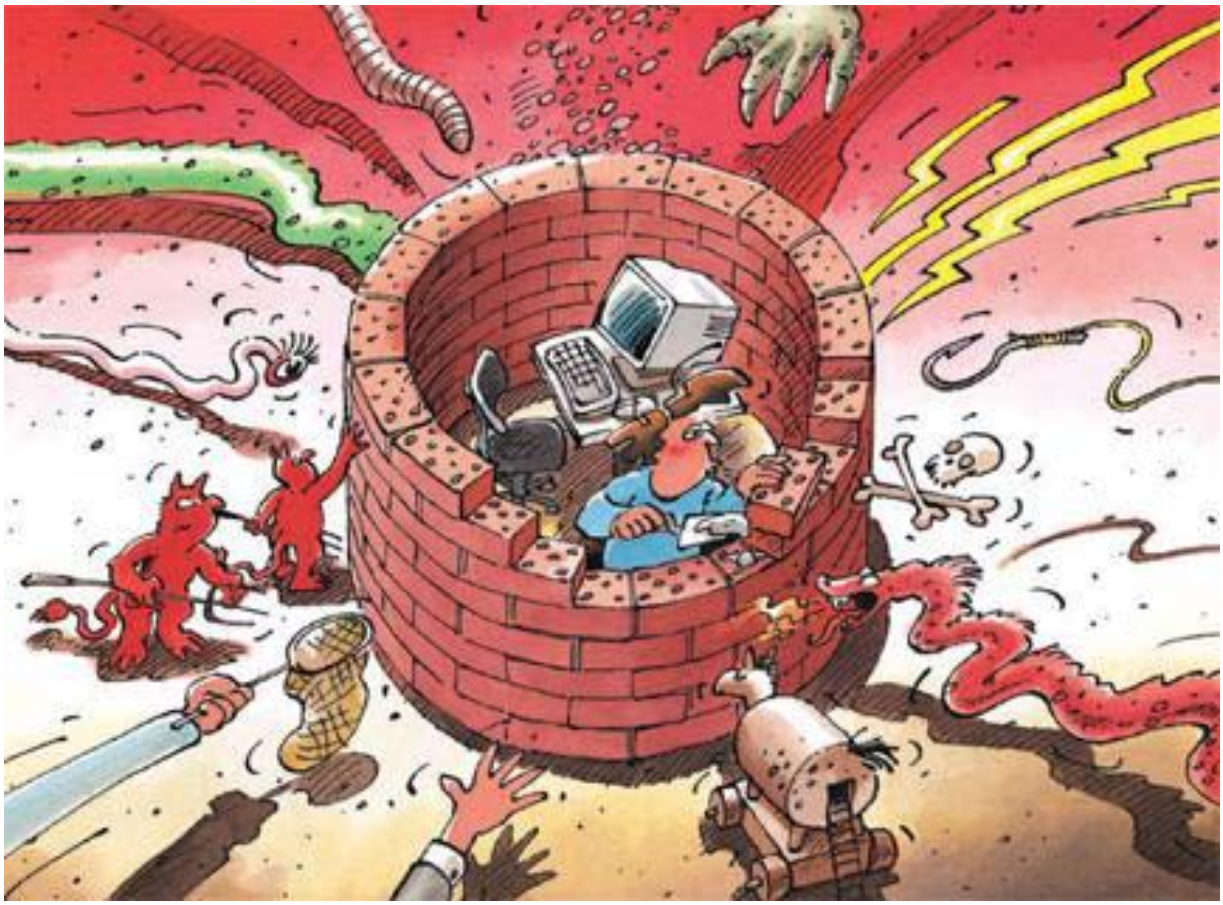
Organo strategia informatica della Confederazione OSIC
Servizio delle attività informative della Confederazione SIC

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI
www.melani.admin.ch

Sicurezza dell'informazione

Situazione in Svizzera e a livello internazionale

Rapporto semestrale 2010/II (luglio – dicembre)



Indice

1 Cardini dell'edizione 2010/II

- **Stuxnet – Attacco ai sistemi di controllo**
  Sull'esempio del verme informatico Stuxnet, nel corso dell'anno in rassegna i media hanno ampiamente riferito in merito alla problematica degli attacchi ai sistemi di controllo (SCADA), già discussa da lungo tempo dalle cerchie specializzate. Stuxnet è tuttavia il primo caso che ha suscitato grande attenzione a livello mondiale. In presenza di una motivazione altrettanto forte e di risorse sufficienti praticamente ogni sistema può prima o poi essere infiltrato o sabotato. Ci si deve aspettare che simili attacchi si ripetano in futuro.
  ► Situazione attuale a livello internazionale: capitolo 4.1
  ► Situazione attuale a livello internazionale: capitolo 4.6
  ► Tendenze / Prospettive: capitolo 5.1
- **Attacchi alla disponibilità – Attacchi di Distributed Denial of Service, DDoS**
  Gli attacchi alla disponibilità dei siti Web, i cosiddetti attacchi di Distributed Denial of Service (DDoS) sono sfruttati a diversi scopi nel ciberspazio. Inizialmente gli attacchi avevano il carattere di semplici atti di vandalismo. Nel frattempo ne sono mutate le motivazioni. Si osservano ad esempio attacchi DDoS come strumento di vendetta, per danneggiare la concorrenza, per il racket o per motivi politici.
  ► Situazione attuale a livello svizzero: capitolo 3.1
  ► Situazione attuale a livello svizzero: capitolo 3.2
  ► Tendenze / Prospettive: capitolo 5.2
  ► Allegato: capitolo 7.1
- **Sicurezza degli smartphone**
  Per lungo tempo si è ritenuto che il pericolo di virus per gli smartphone fosse esiguo perché gli smartphone non costituirebbero un obiettivo redditizio per l'industria del malware. Ne sarebbero motivo la molteplicità dei sistemi operativi, la difficile diffusione del malware e l'assenza di «modelli d'affari della criminalità informatica». La diffusione crescente degli smartphone e di telefoni mobili con funzionalità di tipo PC come pure la memorizzazione di dati sensibili su questi apparecchi li rende però maggiormente attraenti anche per i criminali.
  ► Tendenze / Prospettive: capitolo 5.3
- **Permangono elevate le infezioni di siti Web**
  Le infezioni di siti Web sono al momento il vettore più utilizzato per la diffusione di software nocivo. In questo contesto svolgono un ruolo primario i server centrali che mettono contenuti a disposizione di diversi siti Web. Nel caso soprattutto della pubblicità online, ma anche in quello dei servizi di statistica, una sola compromissione può vere ampie conseguenze.
  ► Situazione attuale a livello svizzero: capitolo 3.9
  ► Situazione attuale a livello svizzero: capitolo 3.13
- **Aumento del phishing ai danni dei servizi Internet**
  Sono particolarmente minacciati i servizi che sono unicamente protetti dal login e dalla password e tramite il cui accesso è possibile guadagnare direttamente o indirettamente denaro. Oltre al commercio di emissione ne sono soprattutto colpiti le carte di credito, i sistemi di pagamento online, le piattaforme di asta, i provider di e-mail e le reti sociali.
  ► Situazione attuale a livello svizzero: capitolo 3.5
  ► Situazione attuale a livello internazionale: capitolo 4.3
  ► Situazione attuale a livello internazionale: capitolo 4.4

2 Introduzione

Il dodicesimo rapporto semestrale (luglio – dicembre 2010) della Centrale d’annuncio e d’analisi per la sicurezza dell’informazione (MELANI) spiega le principali tendenze nel campo dei pericoli e dei rischi che accompagnano le tecnologie dell’informazione e della comunicazione (TIC). Esso presenta un compendio degli avvenimenti in Svizzera e all’estero, illustra i principali sviluppi in ambito di prevenzione e presenta in sintesi le attività più importanti degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (*termini in corsivo*) sono riunite in un **glossario** (**capitolo 6**) alla fine del presente rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate dal loro colore.

I temi scelti del presente rapporto semestrale sono accennati nel **capitolo 1**.

I **capitoli 3 e 4** abbordano le avarie e i crash, gli attacchi, la criminalità e il terrorismo che presentano relazioni con le infrastrutture TIC. Per il tramite di esempi scelti sono illustrati i principali avvenimenti della seconda metà del 2010. In merito il capitolo 3 tratta i temi nazionali, il capitolo 4 i temi internazionali.

Il **capitolo 5** presenta le tendenze e una prospettiva delle evoluzioni attese.

Il **capitolo 7** è un allegato contenente ampie spiegazioni e istruzioni tecniche su tematiche scelte del rapporto semestrale.

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Attacchi alla disponibilità delle pagine Web di PS, PPD, PLR e UDC

Nel corso di una settimana i siti Web dei quattro maggiori partiti politici svizzeri sono stati pregiudicati, rispettivamente paralizzati di volta in volta durante parecchie ore da un *attacco alla disponibilità* (DDoS). Nel caso del PS gli attacchi sono iniziati lunedì 8 novembre 2010, mentre il PPD ha registrato un attacco il giovedì successivo. Il venerdì sera è stata la volta del PLR e la domenica dell'UDC. Secondo quanto riferito dal PS il sito Web ha ricevuto richieste simultanee da fino a 200 computer, principalmente dalla Germania, dai Paesi Bassi e dagli USA. Nello spazio di quattro ore si sono sommati otto milioni di accessi. Il PPD ha riferito di 120 computer che inviavano richieste simultanee al proprio sito Web. Si ritiene che gli attacchi siano stati effettuati per il tramite di una *rete bot*.

Non si conoscono le motivazioni di questi attacchi, in particolare non è noto se gli attacchi fossero in relazione con le votazioni del 20 novembre 2010. Queste votazioni concernevano tra l'altro l'iniziativa espulsione. Oltre agli attacchi conosciuti si ritiene che si sia verificato un numero notevole di attacchi (diretti contro imprese di minori dimensioni, rispettivamente siti Web) che non sono stati comunicati al pubblico.

Anche chi non dispone di un grande know-how tecnico può commissionare in maniera relativamente semplice un attacco DDoS sul mercato clandestino. Il prezzo si orienta in merito sulla capacità del sito Web da attaccare. Normalmente siffatti attacchi possono essere prenotati per poche centinaia di dollari. Dato che nel caso dei computer che sferrano l'attacco si tratta di sistemi compromessi di utenti insospettati è estremamente difficile individuare con mezzi tecnici l'origine dell'attacco. A seconda del tipo di attacco anche l'indirizzo IP del mittente è falsificato.

3.2 Attacco dei sostenitori di Wikileaks

Il 5 dicembre 2010 il fornitore di servizi finanziari PostFinance ha bloccato il conto corrente di solidarietà di Julian Assange, fondatore di «Wikileaks», a motivo di false indicazioni sul suo presunto domicilio a Ginevra. Successivamente il sito Web di PostFinance è stato vittima di un *attacco alla disponibilità (DDoS)* da parte di presunti sostenitori di «Wikileaks». L'attacco ha pregiudicato il sito Web per circa 22 ore, rallentando o rendendo impossibile l'accesso ai quasi 1.2 milioni di conti e-banking di PostFinance. Gli attacchi sono manifestamente stati coordinati da un gruppo informale denominato «Anonymous», che dal dicembre del 2010 esegue attacchi di rivalsa nei confronti di coloro che considera oppositori di Wikileaks.
Il gruppo ha rivolto un appello al pubblico invitandolo a scaricare da Internet un programma in grado in inviare in grande massa richieste «insensate» a un qualsiasi indirizzo Internet. Quanto maggiore il numero di utenti che avrebbero utilizzato tale programma, tanto maggiore sarebbe stata la probabilità che a partire da un determinato momento il sito Internet prescelto sarebbe stato sovraccaricato e quindi non più raggiungibile. Oltre a PostFinance sono stati vittime di attacchi analoghi PayPal, società filiale di Ebay, come pure i siti Web di Mastercard, Visa, Interpol e delle autorità svedesi.

Nel contesto di questi attacchi le autorità di perseguimento penale hanno effettuato arresti in diversi Paesi. Negli USA l'FBI ha perquisito 40 case e appartamenti[1]. In Gran Bretagna la polizia ha proceduto all'arresto di cinque presunti hacker[2]. Nei Paesi Bassi è stato arrestato un sedicenne che aveva partecipato a questa azione.[3] Anche in Germania e in Francia le autorità hanno avviato delle inchieste[4].

Per sferrare questi attacchi ci si serve normalmente di reti bot. Nella fattispecie i simpatizzanti di «Wikileaks» hanno scaricato un programma denominato «Low Orbit Ion Canon» (LOIC) e quindi immesso manualmente l'URL oppure lasciato volontariamente comandare a distanza il proprio computer. L'appello è stato rivolto per il tramite dei media sociali come ad esempio Facebook e Twitter. Dato che nel caso di LOIC vi è anche una versione del programma che può essere eseguito nel browser, anche le persone con scarso know-how IT potevano partecipare a questo attacco. Visto che gli autori degli attacchi non avevano grandi conoscenze nel campo IT, è stato abbastanza facile per i diversi organi di polizia identificare le persone responsabili.

Gli attacchi DDoS non costituiscono una novità e sono frequentemente utilizzati a scopo di estorsione o per danneggiare imprese concorrenti. Si osservano però anche con maggiore frequenza attacchi dettati da motivazioni politiche, come va presunto nel caso descritto qui sopra. Oltre che con dimostrazioni sulla piazza pubblica le proteste si svolgono viepiù nello spazio virtuale.

3.3 Primo esercizio «Cyber Europe»

L'Unione europea ha effettuato per la prima volta il 4 novembre 2010 un esercizio esteso all'intera Europa per testare la capacità di reazione dell'UE e dei Paesi dell'AELS in caso di possibile ciberattacco. L'esercizio, della durata di un giorno, è stato organizzato dall'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA). Oggetto del test sono stati il settore della protezione delle infrastrutture critiche di informazione, il perseguimento penale in ambito di cibercriminalità, i GovCERTs e i regolatori. All'esercizio hanno partecipato complessivamente 22 Paesi dell'UE e dell'AELS, fra i quali anche la Svizzera. Altri 8 Paesi europei erano presenti come osservatori del centro di controllo dell'esercizio ad Atene. Oltre 150 esperti provenienti da 70 servizi pubblici di tutta l'Europa hanno partecipato all'esercizio. Per la Svizzera vi hanno partecipato la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI con il GovCERT.ch, la polizia criminale federale e l'Ufficio federale delle comunicazioni. Tutti i Paesi partecipanti sono stati confrontati a oltre 320 incidenti. L'esercizio era basato su uno scenario che vedeva i collegamenti Internet tra i Paesi europei partecipanti venire meno gradualmente o essere fortemente limitati. Nell'ambito dell'esercizio i Paesi membri dovevano collaborare per impedire ulteriori incidenti e ristabilire i collegamenti. Sono state testate la cooperazione internazionale, ma anche la collaborazione nazionale tra i singoli servizi responsabili della lotta contro i ciberattacchi. Si trattava soprattutto di verificare i canali di comunicazione e gli iter all'interno e tra i diversi Stati. Ulteriori obiettivi erano gli insegnamenti da trarre dalla gestione degli incidenti all'interno dell'Europa per migliorare gli iter di sostegno vicendevole in caso di incidenti o di ciberattacchi massici.

[1] http://www.tagesanzeiger.ch/digital/internet/FBIAktion-gegen-Anonymous/story/23000748 (stato: 10 gennaio 2011).

[2] http://cms.met.police.uk/news/arrests_and_charges/five_arrested_under_computer_misuse_act (stato: 10 gennaio 2011).

[3] http://www.n-tv.de/politik/Hacker-rufen-zum-Cyber-Krieg-article2110826.html (stato: 10 gennaio 2011).

[4] http://www.spiegel.de/netzwelt/netzpolitik/0,1518,742298,00.html (stato: 10 gennaio 2011).

L'esercizio «Cyber Europe 2010» ha costituito un primo importante passo per rafforzare la prontezza di difesa dell'Europa contro i ciberattacchi e va considerato nel contesto del più forte impegno dell'UE nel settore della *protezione delle infrastrutture critiche di informazione (CIIP)*. Nella primavera del 2009 era stata riconosciuta a Tallinn, alla conferenza ministeriale CIIP degli Stati membri dell'UE, la necessità urgente di accrescere le possibilità di difesa, la sicurezza e la stabilità delle infrastrutture critiche di informazione in seno all'UE.

Nel suo genere questo esercizio è stato il primo in Europa. Il solo fatto che vi abbiano partecipato 22 Paesi europei va considerato un successo. È tuttavia ancora troppo presto per un'analisi dettagliata. Si può nondimeno affermare fin d'ora che la comunicazione ha ben funzionato, soprattutto tra i CERTs nazionali. Sia a livello europeo che a livello mondiale esistono già elenchi affermati di contatti od organizzazioni, come ad esempio l'unione dei CERT governativi europei (European Government CERTs - EGC), che vengono utilizzati quotidianamente. I gestori privati di infrastrutture di informazione non sono stati integrati in questo primo esercizio. Se ne prevede comunque la partecipazione ai futuri esercizi.

3.4 «Storie di Internet» per una maggiore sicurezza della società dell'informazione

Diversi servizi della Confederazione e dei Cantoni hanno pubblicato un opuscolo comune intitolato «Storie di Internet…che nessuno vorrebbe vivere». Con l'ausilio di fumetti l'opuscolo illustra situazioni pericolose sul Web, le modalità per individuarle, per reagire nei loro confronti o per evitarle. I fumetti trattano della trasmissione di dati personali, delle attività criminali in Internet, dell'insufficiente protezione dei bambini e dei giovani, dell'abbindolamento di consumatori, dei computer non protetti e delle *reti WLAN* non cifrate. Ogni storia è corredata di link a organizzazioni che offrono approfondimenti informativi. L'obiettivo è di rafforzare la sicurezza e la fiducia della popolazione nell'impiego delle tecnologie dell'informazione e della comunicazione (TIC).

I fumetti si rivolgono all'intera popolazione in tedesco, francese, italiano, reto-romancio e inglese. Essi possono essere scaricati da Internet oppure ordinati in forma stampata[5]. Su richiesta le storie possono essere ottenute in appositi formati di file per pubblicazione (con indicazione della fonte).

L'opuscolo costituisce una misura di attuazione del concetto «Sicurezza e fiducia», del quale il Consiglio federale ha preso atto l'11 giugno 2010[6]. Questo concetto presenta misure destinate a sostenere la popolazione e le PMI nell'utilizzo in maniera consapevole e conforme al diritto le tecnologie dell'informazione e della comunicazione (TIC). Per il loro tramite si intende inoltre rafforzare la fiducia nella TIC. Le misure sono attuate sotto la direzione del Servizio di coordinamento società dell'informazione dell'UFCOM, unitamente a diverse organizzazioni specializzate.

Internet, il computer e il cellulare fanno nel frattempo parte della vita quotidiana delle persone in Svizzera. I vantaggi dell'uso di Internet sono però sempre anche vincolati a pericoli. Diversamente da una passeggiata lungo le strade, i lati oscuri di Internet non sono sempre percettibili a prima vista. L'opuscolo aiuta a individuare i pericoli in Internet ed è stato bene accolto della popolazione. Esso è utilizzato con successo nell'insegnamento scolastico, nella formazione dei genitori, nella sensibilizzazione delle imprese, presso i servizi di polizia

[5] http://www.geschichtenausdeminternet.ch (stato: 10 gennaio 2011).

[6] http://www.bakom.admin.ch/themen/infosociety/01691/01710/index.html?lang=de (stato: 10 gennaio 2011).

e per l'informazione dei consumatori. L'opuscolo è stato esaurito in breve tempo e ha dovuto essere ristampato.

3.5 Phishing di conti e-mail

Dal mese di dicembre 2910 si osservano viepiù e-mail contro i provider di posta elettronica, fra i quali Swisscom. Diversamente dagli attacchi precedenti, nel cui ambito le vittima doveva indicare direttamente il login e la password in una e-mail da inviare a un indirizzo e-mail prestabilito, nel caso degli attacchi attuali si invia un link da cliccare, che poi dirotta su una pagina di phishing. Questa pagina Web falsificata assomiglia in maniera ingannevole all'originale e sollecita l'immissione del login e della password, come pure di altri dati personali. Questo modo di procedere è noto da precedenti attacchi ai fornitori di servizi finanziari e mostra due cose: le vittime potenziali non reagiscono più (rispettivamente meno) a e-mail grossolane e i dati di login dell'e-mail sono ulteriormente ricercati sul mercato clandestino perché possono essere venduti senza problema.

Il fatto che i dati di accesso ai servizi Internet e soprattutto i dati delle carte di credito siano viepiù nel mirino dei cibercriminali conferma le valutazioni di MELANI. I tentativi di phishing diretti contro i fornitori di servizi e-mail come Bluewin, Hotmail ecc. sono in aumento. Si assiste anche a un aumento dei dati di login degli amministratori di siti Web, dati che sono successivamente sfruttati per collocare *infezioni drive-by* sui siti Web. Esempi di truffe che possono essere perpetrate con siffatti dati di login sono descritti nei capitoli 3.3 del rapporto semestrale 2009/1[7] e 3.6 del rapporto semestrale 2008/2[8]. Il phishing classico nei confronti dei fornitori svizzeri di servizi finanziari è stato osservato solo sporadicamente. Ne è motivo l'introduzione dei più diversi elementi di sicurezza nell'e-banking.

Va osservato che dietro gli attacchi all'e-banking (phishing classico e software nocivo all'e-banking) con *due fattori di autentificazione* e il phishing ai danni di servizi Internet unicamente protetti dal login e dalla password si celano diversi modelli d'affari e quindi anche diversi gruppi criminali. I gruppi che praticano il phishing «semplice» sono interessati ai dati di login, ma non necessariamente alla truffa che può essere successivamente perpetrata con questi dati. Questa circostanza riduce l'energia criminale impiegata perché i dati sono invero «soltanto» venduti, mentre non si partecipa alla truffa vera e propria. Nel caso degli attacchi all'e-banking non è più possibile una separazione tra il conseguimento dei dati di login e la truffa vera e propria, perché l'autentificazione a due fattori comporta una piccola finestra temporale al cui interno si deve svolgere l'intero processo di truffa. Oltre alla maggiore complessità si pone soprattutto la questione della modalità di accesso al denaro carpito. A tale scopo il denaro deve essere riciclato, ciò che rende indispensabile un'ampia infrastruttura di agenti finanziari. Per questo sono necessarie una buona organizzazione e soprattutto una maggiore energia criminale.

Numerose prestazioni di servizi in Internet possono essere raggiunte con la semplice immissione del nome di utente e della password. Se scorda la propria password l'utente può richiederne una nuova tramite il link «Ripristinare la password». La nuova password gli è inviata a mezzo e-mail. Se un aggressore riesce a inserirsi illecitamente sul conto e-mail, esso può servirsi di questo conto per accedere ai più diversi servizi della vittima e sfruttarli in maniera abusiva per proprio conto.

[7] MELANI Rapporto semestrale 2009/1, capitolo 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de (stato: 10 gennaio 2011).

[8] MELANI Rapporto semestrale 2008/2, capitolo 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=de (stato: 10 gennaio 2011).

3.6 Avaria dell'Internet mobile

Il 9 novembre 2010 una perturbazione ha pregiudicato l'Internet mobile di Swisscom. Praticamente tutti i clienti di Swisscom Mobile sono stati tagliati da Internet per più ore. Secondo quanto riferito da Swisscom, verso le 7:30 si è verificata una perturbazione della *rete GPRS* nel corso di lavori di manutenzione. Per sopprimere la perturbazione il servizio ha dovuto essere riavviato nella mattinata. Il riavvio ha provocato problemi poi sfociati in questa avaria di vaste dimensioni[9]. Non ne sono stati toccati la telefonia sulla rete mobile, l'invio e il ricevimento di SMS, come pure i collegamenti alla rete fissa. A titolo di indennizzo Swisscom ha regalato dieci franchi ai suoi clienti Internet mobile. A prescindere dai telefoni mobili sono stati ad esempio toccati dall'avaria i terminali di pagamento delle carte di credito e i computer portatili dei capitreno delle FFS.

L'Internet mobile fa sempre più parte della vita quotidiana: consultazione rapida dell'ora di partenza dell'autobus, acquisto di un biglietto, scaricamento delle ultime notizie. Se l'Internet mobile subisce un'avaria occorre rinunciare a queste prestazioni di servizi. È una cosa senz'altro sopportabile.

Ma anche altre e «più importanti» prestazioni di servizi come ad esempio i terminali mobili per carte di credito funzionano con sempre maggiore frequenza su base Internet mobile. E diversa è anche la situazione per quanto riguarda le apparecchiature di controllo mobili dell'industria e dell'industria di approvvigionamento. Ne risulterebbero gravi conseguenze per parti della popolazione qualora esse non fossero più controllabili a distanza a causa di questa perdita di collegamento.

3.7 Avaria della radio nella zona di Berna

Il 16 dicembre 2010 alle 7:15 un automobilista è slittato sulla carreggiata, schiantandosi contro un traliccio del fornitore di energia (BKW). Questa circostanza è bastata a provocare un'interruzione di corrente nella regione. A prescindere dalle case che sono state private di corrente quella mattina, anche l'alimentazione elettrica della vicina torre emittente del Bantiger è stata interrotta. Questo fatto ha pregiudicato l'intera diffusione radiotelevisiva nella regione di Berna. Per evitare simili incidenti l'emittente può essere alimentata da due diverse fonti di corrente. Purtroppo l'interruttore che assicura in questi casi il passaggio dall'una all'altra fonte di alimentazione non ha funzionato.

La radio è utilizzata per allarmare in maniera capillare in caso di catastrofi o di avarie. Il concetto di emergenza delle centrali nucleari prevede che in caso di incidente a un reattore i Comuni ricevano via radio le direttive dei Cantoni e della Centrale nazionale d'allarme[10] dell'Ufficio federale della protezione della popolazione. La popolazione svizzera è cosciente se suonano le sirene d'allarme si deve accendere la radio. In merito occorre prestare una particolare attenzione alla sicurezza in caso di avaria e alla stabilità. Le emittenti OUC della SSR in Svizzera sono ripartite in classi di disponibilità. Pertanto le grandi emittenti sono assegnate a una classe di disponibilità più elevata. Ciò vale anche per la torre emittente del Bantiger. La caratteristica chiave è in questo caso il tempo massimo di avaria ammesso per caso di avaria. La disponibilità è comprensiva dell'intera catena di alimentazione e quindi non

9 http://www.swisscom.com/GHQ/content/Media/Medienmitteilungen/2010/20101109_MM_Stoerung_Mob_Internet_aufgehoben.htm (stato: 10 gennaio 2011).

10 http://www.ensi.ch/fileadmin/deutsch/files/nfs_2006d.pdf , pagina 8 (stato: 10 gennaio 2011).

soltanto l'emittente, ma anche del trasporto del programma, del controllo dell'emittente ecc. Non esistono invece direttive per quanto riguarda l'alimentazione d'emergenza del programma radio regolare, questo diversamente dall'informazione della popolazione da parte della Confederazione in situazioni di crisi. Ad essa si applicano esigenze di protezione più elevate. Per questo motivo è disponibile una propria emittente radio IBBK.

Ciononostante questo incidente dimostra in modo esemplare come sia importante una verifica regolare dei concetti di emergenza.

3.8 Campagna «Black hat SEO» anche con i domini «.ch»

L'ottimizzazione dei motori di ricerca o «Search Engine Optimization» (SEO) consiste in misure destinate a collocare i siti Web in un ranking più elevato nei motori di ricerca. Grazie a tecniche come il «*Cloaking*», il «*Keyword Stuffing*» o l'«*Hidden Text*» (rispettivamente *Hypertext*) è possibile collocare siti sconosciuti in testa alla classifica dei motori di ricerca e raggiungere così una migliore visibilità e un maggiore traffico. L'ottimizzazione etica dei motori di ricerca è denominata ottimizzazione «white hat». Essa rinuncia a pratiche indesiderate e segue le direttive dei singoli motori di ricerca. Al contrario l'ottimizzazione con l'ausilio di metodi indesiderati viene denominata ottimizzazione «black hat».

Se intende diffondere malware sul Web in maniera possibilmente efficace il truffatore infetta preferibilmente un sito Web visitato intensamente (cfr. il capitolo 5.5). Per il tramite di un solo sito Web è così possibile infettare decine di migliaia di computer. Si tratta in genere dei siti Web maggiormente visitati e anche meglio protetti (sul Web esistono numerose eccezioni che confermano la regola). Nel caso della tecnica SEO basta compromettere siti Web a debole traffico meno conosciuti (e meno protetti) e poi catapultarli in cima alla classifica dei motori di ricerca.

Nel mese di agosto 2010 si è svolta un'incessante campagna «black hat SEO» con l'obiettivo di diffondere uno «scareware». Essa si estendeva anche a diversi domini svizzeri[11]. Non appena veniva individuata una lacuna di sicurezza su un server Web svizzero veniva collocato sotto ogni nome di dominio di questo server Web un reindirizzamento (self.location.href) che rinviava l'utente a un sito Web con il *TLD* «co.cc», che visualizzava il messaggio «You're infected» e offriva all'utente un programma presuntamente in grado di disinfestare il computer (cfr. figura). I problemi incominciavano quando si scaricava e installava il programma. La tecnica grazie alla quale molti siti piratati rinviano a un unico sito mirato è denominata «*Linkfarm*». Anch'essa rientra nel concetto di «black hat SEO».

[11] Dancho Danchev, esperto della sicurezza informatica, ha analizzato in maniera esauriente la campagna nel suo blog: http://ddanchev.blogspot.com/2010/08/dissecting-scareware-serving-black-hat.html (stato: 10 gennaio 2011).

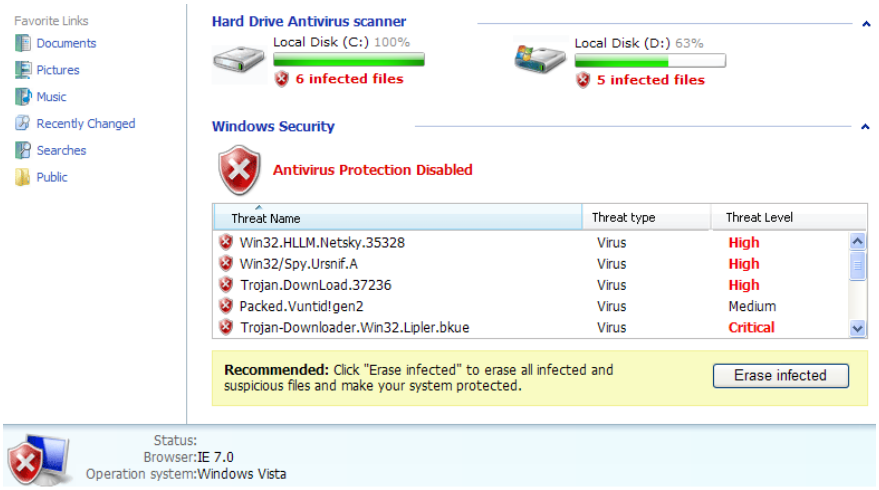


Figura 1: Navigando sul sito Web .ch si viene dirottati su un sito Web che indica che il computer è infettato.

Anche i siti che non sembrano particolarmente attraenti per gli aggressori devono essere protetti con la dovuta cura. Chi utilizza un *Content Management System* (CMS) come ad esempio «WordPress», «Joomla», «Drupal» ecc. deve aggiornare regolarmente queste applicazioni e impedire in tal modo che i malfattori abbiano via libera. Inoltre anche l'hosting provider dovrebbe provveder a una maggiore sicurezza dei server Web.

3.9 Lotta contro i siti Web nocivi

Situazione iniziale

I cibercriminali piratano sempre più siti Web legittimi, collocandovi codice nocivo. In tal modo è possibile affissare pagine Web di phishing (cfr. il capitolo 3.5) oppure insinuare infezioni di siti Web (cfr. il capitolo 3.13). In questo ultimo caso la sola chiamata di una pagina Web appositamente manipolata può già bastare per ritrovarsi con il computer infettato da *virus* e *cavalli di Troia*.

Tutti i calcolatori che possono accedere a Internet possono essere infettati dal malware. Gli utenti di Linux e di MacOS si cullano in una falsa sicurezza, se pensano che i virus e i cavalli di Troia siano unicamente un problema di Windows. Anche gli smartphone sono oggetto di attacchi con una tendenza all'aumento (cfr. il capitolo 5.3).

Misure da parte di MELANI e SWITCH

Da fine novembre 2010 SWITCH, il servizio svizzero di registrazione dei nomi di dominio, interviene con maggiore fermezza nei confronti dei siti Web svizzeri che diffondono software nocivo e infettano con malware i computer degli utenti che navigano in Internet[12]. SWITCH verifica ora segnalazioni di siti Web che diffondono malware e contatta i detentori e i gestori interessati (provider) invitandoli a sopprimere il problema. In caso di mancata reazione sull'arco del giorno di lavoro, SWITCH blocca per una durata fino a cinque giorni feriali l'indirizzo Internet, cancella durante questo periodo di tempo l'attribuzione a un server dei nomi e ne informa MELANI. Se il codice nocivo non viene rimosso, MELANI può richiedere la proroga di questa misura per 30 giorni[13].

[12] http://www.switch.ch/de/about/news/2010/malware-nov2010.html (stato: 10 gennaio 2011).

[13] http://www.admin.ch/ch/d/sr/784_104/a14bist.html (stato: 10 gennaio 2011).

Come già esposto nel capitolo 3.5 dell'ultimo rapporto semestrale di MELANI[14], queste misure si prefiggono anzitutto di proteggere gli utenti di Internet e di segnalare ai gestori di siti Web la compromissione delle loro pagine Web. Il bloccaggio dei nomi di dominio funge da ultima ratio quando il gestore non effettua la disinfestazione del sito Web e non è quindi possibile difendersi altrimenti dal pericolo. L'esperienza insegna che la maggior parte degli esercenti sono grati dell'informazione e ripristinano tempestivamente i loro siti Web. MELANI non ha mai dovuto esigere un bloccaggio e continuerà a far uso di questa possibilità come ultima ratio e in caso di effettiva grave messa in pericolo di un'ampia cerchia di utenti.

Misure di altre organizzazioni

In considerazione dell'aumento complessivo di siti Web compromessi e del fatto che non tutti i servizi di registrazione procedono in maniera altrettanto impegnata di SWITCH, un numero sempre maggiore di attori di Internet in questo settore se ne preoccupano, adottano misure e presentano prodotti per proteggere gli utenti. I produttori di browser in particolare hanno introdotto meccanismi che allertano prima della visita di siti possibilmente nocivi. In questo senso alla chiamata di un indirizzo Internet corrispondente viene inserita una pagina che avverte l'utente del pericolo incombente in caso di caricamento della pagina richiesta. Di recente Google contrassegna i siti Web potenzialmente nocivi fin dai risultati della ricerca. Inoltre diversi produttori di software anti-malware offrono prodotti che contrassegnano da un canto i risultati della ricerca come sicuri o problematici e, d'altro canto, allertano in caso di tentativo di chiamata di un sito Web nocivo.

Tutte queste iniziative e funzioni sono in linea di massima degne di plauso. In particolare le misure di protezione integrate e attivate in modo standard nei browser aiutano sicuramente a evitare le infezioni nel caso di utenti Internet meno versati. Il grado di individuazione dei siti Web nocivi è tuttavia molto diverso e la sola fiducia riposta in singoli prodotti può cullare l'utente in una falsa sicurezza. Come nel caso di tutte le misure di difesa contro contenuti nocivi di Internet nessuna soluzione offre una protezione al 100%, perché i metodi degli aggressori cambiano continuamente per difficoltare l'individuazione del codice nocivo insinuato. Oltre ai meccanismi di protezione «integrati» dai diversi offerenti nei browser, nelle pagine Internet o nelle *toolbar* è come in precedenza indispensabile installare un normale programma antivirus (scanner antivirus) a aggiornare regolarmente il sistema operativo e le applicazioni per ridurre a un minimo il rischio di infezioni.

L'iniziativa anti-phishing della Francia

La stessa cosa vale per i filtri anti-phishing: nel caso delle pagine Web di phishing che si affissano per breve tempo una reazione rapida è di importanza centrale. Il periodo critico è tipicamente costituito dalle prime ore successive all'invio delle e-mail contenenti il link al sito Web di phishing. La maggior parte dei browser dispongono di una funzione per il cui tramite possono essere annunciate le pagine di phishing. Esistono inoltre *toolbar* (dei produttori di software anti-malware e di offerenti specializzati) che allertano nel caso della presenza di siffatte pagine. Anche in questo caso gli utenti hanno la possibilità di annunciare la scoperta di una pagina di phishing. Gli annunci sono poi analizzati e poco tempo dopo il prodotto corrispondente mette tipicamente in guardia dalla pagina Web. All'inizio del 2011 Microsoft ha avviato in collaborazione con PayPal e con la CERT-LEXSI francese un'iniziativa di lotta

[14] MELANI Rapporto semestrale 2010/1, capitolo 3.5: http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html?lang=de (stato: 10 gennaio 2011).

focalizzata sul phishing in lingua francese. La popolazione può depositare i propri annunci su un sito Web specializzato[15].

Dato che i tempi di reazione dei gestori di siti Web e di provider di hosting sono molto diversi, si deve sfruttare appieno ogni possibilità di protezione degli utenti di Internet. Quanto maggiore è la velocità di diramazione degli avvertimenti, tanto minore è il numero di vittime potenziali. Anche in questo caso la molteplicità degli offerenti ha per conseguenza che non tutti i prodotti allertino in merito a tutti i siti Web pericolosi, perché non tutti gli offerenti hanno conoscenza di un sito Web specifico. Non si può pertanto partire dall'idea che non ci venga affissata alcuna pagina Web di phishing soltanto perché utilizziamo un prodotto anti-phishing. È molto più efficace ignorare tutte le e-mail che sollecitano l'immissione della password. In questo senso occorre come in precedenza un atteggiamento generalmente critico quando una e-mail ci sollecita a immettere o a «verificare» su un sito Web dati personali come le password o informazioni sulla carta di credito.

La registrazione del proprio sito Web nei filtri di malware o di phishing può risultare molto fastidiosa e tra l'altro tenere lontani i clienti potenziali. Ad avvenuto ripristino del sito Web si pone il problema della rimozione della registrazione in questi filtri ed elenchi di allerta. Si tratta di un'operazione difficile nella misura in cui non si sa da un canto in quanti e in quali elenchi è inserito l'indirizzo e, d'altro canto, il contatto con l'offerente funziona in maniera efficiente soltanto per il tramite del prodotto corrispondente. Ne consegue che dopo una compromissione del sito Web deve essere effettuata una rielaborazione dispendiosa dell'incidente. Gli offerenti controllano invero regolarmente l'attualità dei loro filtri – ma a seconda delle circostanze può passare un certo periodo di tempo finché la registrazione è nuovamente rimossa.

Per impedire che il proprio sito Web venga compromesso è indispensabile che le applicazioni Web siano costantemente mantenute aggiornate. Si raccomanda inoltre di sorvegliare la propria presenza sul Web per poter immediatamente annullare un'eventuale modifica abusiva, prima che l'indirizzo Internet corrispondente sia inserito negli elenchi di filtro e di allerta.

3.10 27C3: we come in peace – e ci inseriamo illecitamente sul tuo sito Web

Dal 27 al 30 dicembre 2910 si è svolto a Berlino il 27° «Chaos Communication Congress» all'insegna del motto «we come in peace»[16]. Nel corso di questa manifestazione organizzata dal Chaos Computer Club (CCC) i partecipanti hanno tra l'altro esaminato i più diversi siti Web alla ricerca di lacune di sicurezza. La loro ricerca è stata ad esempio coronata da successo nel caso del sito Web del Grasshopper Club Zürich. Il logo dell'associazione è stato brevemente sostituito con quello del FC Zürich, sono state estratte e messe online banche dati del Webshop, come pure informazioni sugli utenti registrati.

Ecco come si presentava il sito Web del CG la notte dal 28 al 29 dicembre 2010:

[15] http://www.phishing-initiative.com (stato: 10 gennaio 2011).

[16] http://events.ccc.de/congress/2010/wiki/Welcome (stato: 10 gennaio 2011).

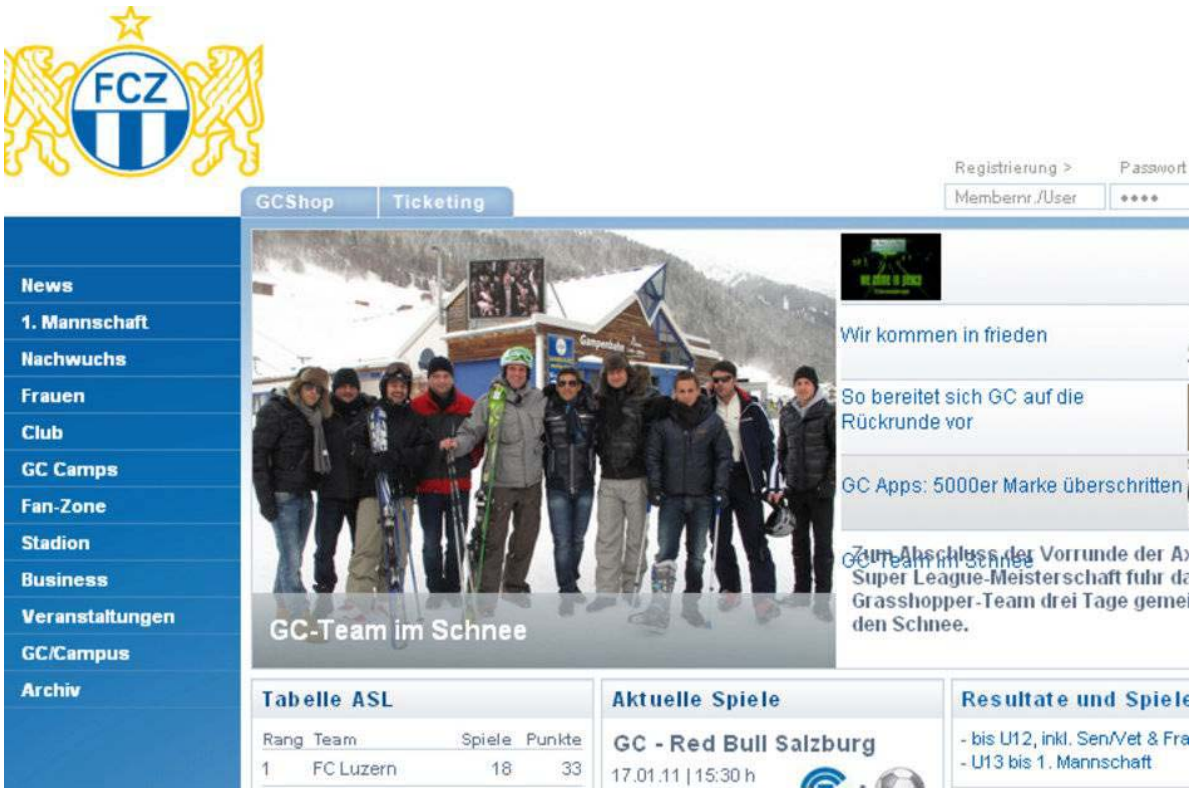


Figura 2: Sito Web modificato del GC.

Dopo il loro intervento gli hacker hanno inviato una e-mail a tutti gli abbonati alla newsletter del GC (i cui indirizzi erano memorizzati nella banca dati) con la quale segnalavano l'insufficiente protezione del sito Web.


We Come In Peace

Es ist Zeit dem Verein "uf de andere siite vo de Gleis" lebewohl zu sagen und das Spielfeld den echten Profis freizugeben.

Es ist tagisch, immer wenn ein Verein oder eine Seite aus dem Internet verschwindet, stirbt mit ihm ein Stueck Geschichte....
Um diesem auszuweichen, haben wir eine Sicherung der Datenbank der Shops und der Userdaten erstellt. - gern geschehn :)

Was vielleicht auch noch ganz informativ ist:

Dieses typo3 CMS ist so unfassbar scheisse. ich koennte pausenlos kotzen.
FCZ wird natuerlich wieder Meister und gcz wird abstreiten dass die Datenbank mit allen Benutzerdaten uA der Shops verloren gegangen sind.
Kann ja passieren, nicht jeder ist so fit mit Moderner technik. und so Datenbanken gehn nunmal einfach verloren, ist ja auch schon anderen grossen Firmen passiert. solange keine Kreditkarteninformationen in der Datenbank gesp... moment...

Figura 3: e-mail degli hacker agli abbonati alla newsletter del GC.

Dato che nella banca dati in questione le password erano registrate in testo pieno MELANI raccomanda agli utenti registrati di modificare immediatamente la password.

MELANI raccomanda di scegliere di volta in volta password diverse per i servizi Web per impedire che dopo una siffatta avaria dei dati l'intera identità online possa essere utilizzata abusivamente dagli hacker. In particolare non si dovrebbe MAI utilizzare per le registrazioni che constano di indirizzo e-mail e di password la medesima password del conto di posta elettronica. Quando gli aggressori non «intervengono in pace» come nella fattispecie, il conto e-mail è il primo obiettivo sul quale si tenta di effettuare il login con la password carpita; in un secondo tempo si prova ad accedere alle diverse reti sociali.

Sono state rilevate ulteriori lacune di sicurezza sui siti Web di partiti politici, gruppi della destra radicale, aeroporti, media, servizi governativi e molti altri ancora[17].Gli hacker si sono offerti una burla particolare ai danni della prima rete della televisione germanica, visualizzando il seguente falso annuncio sul suo sito Web:

Figura 4: Sito Web compromesso della prima rete della televisione germanica con falso annuncio.

3.11 Studio di valutazione «Iniziativa anti reti bot Svizzera»

Già ora le reti bot possono essere prese in affitto per pochi dollari al giorno, fermo restando che il prezzo finale dipende dalla capacità e dalla durata di impiego della rete bot desiderata. Non sorprende quindi che le reti bot siano oggigiorno alla base della maggior parte delle attività criminali su Internet.

Lottare con successo contro le reti bot implica un'intensa collaborazione tra i provider di Internet, lo Stato e se del caso le autorità inquirenti. Per questo motivo a fine 2010 MELANI ha incaricato la Hochschule für Technik di Zurigo di effettuare uno studio di valutazione. Tale studio è destinato a illustrare in quale forma sia possibile una siffatta collaborazione e in quale misura le iniziative in corso all'estero (p. es. botfrei.de[18]) possano essere adeguate alla Svizzera. Lo studio dovrebbe essere ultimato a fine giugno 2011.

3.12 Pro domo sua: capoprogetto «Cyberdefense»

Il Consiglio federale ha condotto il 10 dicembre 2010 un colloquio sulla minaccia nei confronti della Svizzera da parte di attacchi provenienti dal ciberspazio e sulle possibili contromisure. L'Esecutivo ha deciso di rafforzare le misure di protezione contri siffatti attacchi alla Svizzera.

---

17 http://events.ccc.de/congress/2010/wiki/Hacked (stato: 10 gennaio 2011).

18 Il centro di consulenza anti-bot germanico è un servizio di eco, l'associazione registrata germanica dell'economia interna, con il sostegno del Bundesamtes für Sicherheit in der Informationstechnik (BSI). https://www.botfrei.de/ (stato: 10 gennaio 2011).

A tale scopo ha nominato Kurt Nydegger, già capo della Base d'aiuto alla condotta dell'esercito (BAC), come capoprogetto a tempo determinato della «Cyber Defense». Nydegger dirigerà un gruppi di esperti che dovrà elaborare entro fine 2011 una strategia complessiva della Confederazione contro le ciberminacce[19].

3.13 Server OpenX

L'anno scorso sono state registrate numerose infezioni di siti Web, la cui origine può essere ricondotta a lacune di sicurezza dei *server AD*. In questo senso il software *OpenSource* per i server AD OpenX è stato affetto durante tutto l'anno da lacune di sicurezza che hanno consentito agli aggressori di accedere ai diritti di amministratore[20]. Dato che gli aggiornamenti che colmano tali lacune di sicurezza non sono effettuati automaticamente è qui in questione la diligenza degli amministratori Web. Fin dal mese di giugno del 2010 gli esperti della sicurezza hanno messo in guardia dalle versioni ormai divenute obsolete di OpenX a causa degli aggiornamenti in parte effettuati soltanto con lentezza[21].

Anche in Svizzera le *lacune di sicurezza* di OpenX hanno provocato nell'estate del 2010 numerose infezioni, fra le quali quella del sito Web di un grande giornale svizzero. In questo caso la pubblicità dell'edizione online è stata inquinata da un'infezione di sito Web. È ovvio che l'infezione di un simile sito Web ha conseguenze chiaramente più importanti di quelle di una homepage privata (cfr. anche il capitolo 5.5).

	200
hxxp://openx /www/delivery/ajs.php?zoneid=3&source=hxxp://www. .ch&cb= &loc=hxxp://www .ch&referer=hxxp://www .ch	200
about:blank	200
hxxp://www.dhfyjrud321.com/tds/in.cgi?default	**200**
hxxp://www.nbvhhdtn321.com/tds/in.cgi?8	**302**
hxxp://korkonvasiliy.com/hehehe/index.php?s=c4de1af395e576f5156ba255734c26c9	**302**
hxxp://korkonvasiliy.com/hehehe/404.php	**200**

Figura 5: Protocollo di collegamento di un'infezione Web con l'edizione online di un giornale svizzero.

Come si può evincere dal protocollo, dopo aver chiamato il sito Web del giornale l'utente è dirottato sul server «dhfyjrud321».com per sfruttare successivamente le diverse lacune di sicurezza del *browser* e delle *applicazioni*. È stato inoltre inserito un *cookie* affinché l'infezione sia visibile soltanto alla prima visita. Questa circostanza rende difficile l'analisi del sito da parte degli esperti di sicurezza, come pure l'individuazione e l'eliminazione degli errori sulla pagine dell'amministratore Web.

Le infezioni di siti Web sono al momento il vettore più utilizzato per la diffusione di *software nocivo*. In questo contesto svolgono un ruolo primario i server centrali che mettono contenuti a disposizione di diversi siti Web. Nel caso soprattutto della pubblicità online, ma anche in quello dei servizi di statistica, una sola compromissione può vere ampie conseguenze.
Per quanto riguarda gli offerenti di pubblicità in Internet, ma anche di altri contenuti, l'impiego del software applicato assume grande importanza. Anche in questo caso tutti i programmi

[19] http://www.news.admin.ch/message/?lang=de&msg-id=36731 (stato: 10 gennaio 2011).

[20] http://www.heise.de/security/meldung/Ein-Jahr-alte-Luecke-gefaehrdet-OpenX-Ad-Server-1077941.html (stato: 10 gennaio 2011).

[21] http://news.softpedia.com/news/OpenX-Based-Malvertising-Attack-Discovered-145903.shtml (stato: 10 gennaio 2011).

devono essere aggiornati. Nel casi per l'appunto di siffatti servizi un sito Web può in definitiva essere solo altrettanto quanto il suo elemento più debole. Si tratta sovente di offerte di terzi che sono introdotte sul sito Web e che sono quindi incontrollabili da parte dei gestori dei siti Web.

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 «Stuxnet» – Attacco ai sistemi industriali di controllo

A metà giugno 2010 è stato scoperto un nuovo *verme informatico* che per il tramite di una *chiavetta USB* è stato in grado di infettare un intero sistema Windows 7 riparato. Questo è successo perché nel verme sono tra l'altro integrati due driver con funzione *rootkit*, provvisti delle *firme digitali* regolari, ma derubate, di due diverse ditte, che si sono quindi installati senza avvertimento nel sistema. A quel momento nessuno sapeva ancora che questo sarebbe divenuto il programma nocivo più discusso dell'anno[22]. Dalle analisi è emerso che per la sua diffusione sono state sfruttate le lacune di sicurezza già utilizzate nel verme «Conficker», nonché numerose altre lacune di sicurezza di Windows che fino a quel momento non erano ancora state oggetto di un patch. Il verme, denominato «Stuxnet», può propagarsi ulteriormente tramite lo spooler della stampante e reti svincolate e dispone anche di una componente *peer-to-peer* che rende possibile aggiornamenti reciproci di sistemi infettati all'interno della medesima rete. In questo modo Stuxnet può aggiornarsi anche su reti non collegate a Internet non appena vi viene importata una versione più recente.

Oltre a questa straordinaria varietà di vettori di infezione di Windows, Stuxnet contiene un codice per manipolare applicazioni destinate alla programmazione di sistemi industriali di controllo (i *cosiddetti controllori logici programmabili CLP* – in inglese *Programmable Logic Controllers, PLC*). Anche queste applicazioni sono state infettate da «Stuxnet» e sfruttate per la sua diffusione e per infettare i CLP. In questo caso «Stuxnet» è ormai prossimo al suo obiettivo, che consiste nel pregiudicare le funzionalità di determinati CLP. Stuxnet sviluppa tutta l'efficacia pianificata e manipola i processi in corso soltanto se il sistema adempie criteri specifici.

«Stuxnet» camuffa la propria presenza non soltanto sui sistemi Windows, ma anche su tutte le altre componenti colpite. In questo senso ad esempio viene memorizzata la configurazione originale affinché all'atto del configurazione non venga visualizzato il codice modificato, bensì la configurazione apparentemente intatta del programma di elaborazione. Anche i dati che il CLP fornisce al sistema di sorveglianza in corso di esercizio sono modificati in maniera tale che non vengano visualizzate le manipolazioni del pertinente impianto industriale.

Le modalità di funzionamento estremamente complicate di questo malware sono finora considerate uniche. Un'ulteriore caratteristica inusitata di «Stuxnet» è il fatto che non infetta possibilmente molti sistemi, ma soltanto quelli che hanno particolarità specifiche - «Stuxnet» è molto esigente. La sua programmazione non è diretta a sfruttare in maniera abusiva i

[22] http://www.heise.de/thema/Stuxnet; http://www.spiegel.de/thema/stuxnet/; (stato: 10 gennaio 2011); http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html; (stato: 10 gennaio 2011) http://www.symantec.com/business/theme.jsp?themeid=stuxnet; (stato: 10 gennaio 2011); http://www.langner.com/en/blog (stato: 10 gennaio 2011).

computer catturati in vista di qualunque attività criminale o per danneggiare sistemi IT; «Stuxnet» ricerca piuttosto determinati sistemi per poter colpire e manipolare CLP esattamente definiti. Per il tramite di «Stuxnet» è stato eseguito un attacco estremamente mirato.

4.2 Wikileaks

La piattaforma di denuncia «Wikileaks» non eccita i sentimenti soltanto dal secondo semestre del 2010. Dal 2007 «Wikileaks» offre alle persone del mondo intero la possibilità di trasmettere in maniera anonima documenti confidenziali, censurati o non pubblici. Secondo le proprie affermazioni, ad avvenuto invio «Wikileaks» sottopone questi documenti a un esame approfondito all'insegna dei principi giornalistici ed etici e mette a disposizione del pubblico anche i dati greggi, oltre a un'elaborazione giornalistica o a un semplice commento. L'idea alla base di questo modo di procedere è relativamente semplice: la pubblicazione simultanea di articoli e di materiale di base è destinata a garantire un massimo di trasparenza. Di conseguenza «Wikileaks» non procede a nessuna selezione interna del complesso informativo fornito, ma pubblica tutto dopo una prima visione. In questo senso spetta al lettore stesso decidere se intende o no prestare fede alle informazioni messe a disposizione. In maniera corrispondente i lettori non devono essere esposti all'arbitrio di un media funzionante secondo i principi classici, che opera una preselezione delle storie e decide autonomamente – sia in base a riflessioni giornalistiche, sia in base a considerazioni etiche o commerciali – quali di queste storie debbano in definitiva essere pubblicate.

Gli accadimenti degli ultimi sei mesi intorno alla pubblicazione progressiva di circa 250'000 dispacci del Dipartimento di Stato statunitense da parte di«Wikileaks» hanno suscitato numerose problematiche indipendenti. Da un canto si è nuovamente accesa una discussione sui media e sull'etica, prevalentemente incentrata sulla questione della sostenibilità del semplice accesso del pubblico a documenti classificati in base a un principio di full-disclosure de facto. In questo contesto ha svolto un ruolo anche la questione delle intenzioni e delle motivazioni di Julian Assange, (co)fondatore di «Wikileaks». D'altro canto la misura nella quale misura si devono valutare la personalizzazione delle attività di «Wikileaks» nella figura di Assange, la priorizzazione delle informazioni da parte di «Wikileaks» nonostante il suo proprio credo, come pure la scelta selettiva da parte di Assange di operatori mediatici dotati di diritti di esclusività e quindi la contraddizione che si manifesta con lo spirito vero e proprio di «Wikileaks», costituiscono una mera discussione filosofica e sull'etica dei media che non va avviata in questa sede.

Due ulteriori accadimenti in questo contesto hanno nondimeno un chiaro riferimento al tema della sicurezza dell'informazione. Anzitutto la questione di come 250'000 dispacci classificati d'ambasciata abbiano potuto pervenire nelle mani di «Wikileaks». Non è tuttora chiaro se una sola persona o più fonti abbiano fornito a «Wikileaks» questi e altri documenti. Sembra comunque assodato che i grandi rischi sarebbero stati presi in considerazione di una migliore e più efficiente messa in rete all'interno dei servizi governativi degli Stati Uniti. In merito sembra che documenti di diversa classificazione siano stati archiviati sulla medesima rete sicura con diritti di accesso relativamente ampi per un grande numero di utenti. Qualora questa circostanza dovesse trovare conferma il furto di questi documenti costituirebbe un classico esempio di assenza di una strategia di sicurezza dell'informazione, circostanza più volte tematizzata nei rapporti semestrali di MELANI[23]. Si tratta anzitutto di garantire non

[23] MELANI Rapporto semestrale 2009/1, capitolo 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de (stato: 10 gennaio 2011) oppure

soltanto la sicurezza dei canali di informazione, dei supporti di memorizzazione e delle reti, ma anche di avviare ampie misure di tutela nel quadro di un processo consapevole di gestione dei rischi, anche in considerazione di un determinato valore dell'informazione. Una mera strategia tecnica «One Size Fits All» senza restrizioni e diritti di accesso specifici, anche a livello fisico e personale, e non adeguata al valore effettivo di una determinata informazione, non può che condurre imperativamente alla perdita totale di queste informazioni.

Un secondo incidente nel contesto di «Wikileaks» è stata la mobilitazione messa in atto da «Anonymous» per punire virtualmente – secondo i suoi propri termini – i presunti avversari di «Wikileaks». Questo incidente è descritto nel capitolo 3.2.

Gli incidenti nel campo della pubblicazione di documenti da parte di «Wikileaks» illustrano l'intera gamma di problematiche nel settore della sicurezza dell'informazione. La consegna a terzi di documenti classificati costituisce un problema crescente nel mondo delle tecnologie dell'informazione e della comunicazione. Spesse volte si intraprende troppo poco per tutelare l'informazione in profondità («in depth») perché ci si accontenta di parametri tecnici per quanto possibile perfezionati. Purtroppo questo approccio è innanzitutto fonte di grandi rischi e non tiene conto né della problematica insider, né del fatto che non tutte le informazioni hanno il medesimo valore e che quindi una protezione completa deve primariamente prendere in considerazione l'informazione da tutelare e non la rete sulla quale essa è archiviata.

Anche gli «attacchi di rivalsa» eseguiti dopo il dibattito «Wikileaks» mostrano ancora una volta a qual punto le istituzioni e le persone private possano essere vulnerabili agli attacchi e come i ciberattacchi comportino in maniera pressoché inerente il pericolo di danni collaterali come già nel caso di azioni precedenti, ad esempio contro i gestori di siti sessuali in Svizzera[24]. Sono proprio gli attacchi penalmente rilevanti a PostFinance che hanno evidenziato una grande assenza di sensibilizzazione e di senso della giustizia da parte dei partecipanti. In questo senso va caldeggiato il perseguimento penale dei complici in alcuni Paesi.

4.3 SSL e autenticazione a due fattori – Sicurezza per i propri clienti

Nel mese di ottobre 2010 il programmatore Eric Butler ha pubblicato sul proprio sito un'estensione per il navigatore Firefox assai interessante: Firesheep[25].
Durante la conferenza Toorcon di San Diego, Butler ha presentato un'analisi[26] del pericolo causato dai provider del cosiddetto Web 2.0, primo fra tutti Facebook. Al momento dell'accesso a un sito come Facebook il navigatore salva un cookie contenente il nome utente e la password dell'utente.

Se la connessione tra navigatore e destinatario non è criptata, e se l'utente sta utilizzando una connessione WiFi pubblica o semi-privata (per esempio si trova con il proprio computer

---

MELANI Rapporto semestrale 2009/2, capitolo 5.1
http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=de (stato: 10 gennaio 2011).

[24] MELANI Rapporto semestrale 2009/2, capitolo 3.3
http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=de (stato: 10 gennaio 2011) .

[25] http://codebutler.com/firesheep (ultima visita 07.01.2011).

[26] http://codebutler.github.com/firesheep/tc12/#1 (stato: 10 gennaio 2011) .

portatile in uno Starbucks o in un McDonalds o in una conferenza dove viene messa a disposizione una connessione), il cookie creato può essere "catturato" e usato per identificarsi al posto dell'utente legimittimo: ciò si chiama in gergo un *sidejacking*. Per proteggersi contro questo tipo attacco è necessario instaurare una connessione crifrata tra l'utente e il destinatario: Google ha corretto questo problema per Gmail nel gennaio 2010, ma il maggiore sito web del 2010, Facebook, ne soffre ancora.
Per mostrare in modo pratico la facilità con cui un sidejacking funziona, Butler ha pubblicato Firesheep. Installata l'estensione, basta connettersi ad un WiFi insicuro (come quelle di Starbucks appunto), avviare l'applicazione e aspettare che un utente si connetta a Facebook. Si potrà quindi rubare il cookie generato e identificarsi su Facebook con il conto dell'altra persona. Non provare per credere.

Questo è un problema conosciuto. Finora comunque si richiedeva una certa conoscenza per poter rubare un cookie. Con Firesheep diventa un gioco da ragazzi . Gli utenti devono essere attenti ad utilizzare unicamente pagine con SSL, mentre le imprese devono fornire questo servizio. Allo stesso modo MELANI ricorda che sempre più attacchi avvengono nei confronti di quegli operatori che mettono a disposizione un solo fattore di autenticazione, come ad esempio le aste online e diversi sistemi di pagamento. Anche in questo caso è importante ricordare alle imprese che un secondo fattore di autenticazione riduce il rischio di furto di sessioni evitando perdite importanti sia per le impresi che per i loro clienti.

4.4 Incidenti nel contesto del commercio di diritti di emissione

Fin dall'inizio del 2010 si sono verificati attacchi di phishing al registro di commercio delle emissioni, nel senso che i diritti di emissione sono stati trasferiti illegalmente[27]. Una delle ditte danneggiate in questo contesto ha successivamente citato in giudizio la Repubblica federale di Germania in vista del risarcimento dei danni, motivando la propria azione con l'insufficienza degli standard di sicurezza delle autorità competenti.[28]

In un suo comunicato del 16 novembre la Deutsche Emissionshandelsstelle (DEHSt) ha annunciato l'introduzione di un'*autenticazione a due fattori* mediante smsTAN per accedere al registro delle emissioni[29].

Lo stesso giorno sono stati derubati alla filiale rumena di un produttore svizzero di cemento 1,6 milioni di certificati di emissione presso il registro nazionale rumeno, dopo che i criminali ebbero spiato i dati di accesso della ditta per il tramite di un cavallo di Troia. Il cavallo di Troia utilizzato è finora stato impiegato soprattutto ai danni di clienti delle banche americane. Le sue caratteristiche (tra l'altro il furto di certificati chiave privati, la registrazione dei dati digitati sulla tastiera, la copia di dati dall'area temporanea di memoria) si prestano anche per carpire informazioni di annuncio su altri servizi – in particolare quando si tratta unicamente del login e della password. L'apparizione di «Nimkey» in questo contesto ha fatto sì che a fine novembre diversi registri europei di commercio delle emissioni sospendessero il commercio, perlomeno a breve termine.

---

[27] Cfr. MELANI Rapporto semestrale 2010/1, capitolo 4.9 http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html (stato: 10 gennaio 2011).

[28] http://www.heise.de/security/meldung/Datenklau-bei-Emissionsrechten-kommt-vor-Gericht-1098072.html (stato: 10 gennaio 2011).

[29] http://www.dehst.de/cln_153/nn_1662430/SharedDocs/Mailings/DE/2010/10-11-16__smsTAN.html (stato: 10 gennaio 2011).

All'inizio del mese di dicembre numerose imprese hanno ricevuto una e-mail dall'«European Climate Registry», che sollecitava i destinatari ad aprire un conto sul suo sito Web, rispettivamente a validare i dati di login. La Commissione europea e i registri nazionali si sono distanziati da questa impresa: non si tratterebbe di un registro ufficiale, ma di una mera offerta Internet di diritto privato, la cui serietà e utilità non potrebbe essere valutata – ma il suo sito Web permane online[30].

La Commissione europea intende potenziare gli standard di sicurezza dei servizi del commercio di emissione. In una fase successiva il commercio sarà disbrigato per il tramite di un registro europeo unico[31]. Fino alla riunione dei registri, i registri nazionali dovranno provvedere a una protezione sufficiente e introdurre procedure più sicure. Diverse di queste misure sono già state eseguite.

Come già menzionato in precedenti rapporti semestrali[32], si constata uno spostamento degli attacchi dei cibercriminali dall'online-banking in direzione di servizi e di piattaforme (di commercio) meno bene protetti. Sono particolarmente minacciati i servizi che sono unicamente protetti dal login e dalla password e tramite il cui accesso è possibile guadagnare direttamente o indirettamente denaro. Oltre al commercio di emissione ne sono tra l'altro colpiti le carte di credito, i sistemi di pagamento online, le piattaforme di asta, i provider di e-mail e le reti sociali.

4.5 La NATO esercita la ciberdifesa e inserisce la ciberminaccia nel suo concetto strategico

Dal 16 al 18 novembre 2010 la NATO ha effettuato un esercizio denominato «Cyber Coalition 2010»[33]. Sono stati testati gli iter e il coordinamento tra i diversi attori che devono collaborare in caso di ciberattacco alla NATO e ai suoi Stati membri. Si trattava del terzo esercizio di questo genere.

In occasione del vertice della NATO che si è svolto a Lisbona dal 19 a 20 novembre 2010 i capi di Stato e di Governo hanno adottato un nuovo concetto strategico del Patto atlantico secondo il quale i ciberattacchi vanno considerati una seria minaccia. Di conseguenza la NATO intende sviluppare ulteriormente le proprie capacità e quelle dei suoi Stati membri per impedire, individuare, difendersi e riprendersi dagli attacchi alle reti di computer. Si dovranno inoltre potenziare e meglio coordinare le capacità nazionali di lotta alla cibercriminalità. D'altra parte si dovranno sviluppare capacità per contribuire alla sicurezza energetica e in questo senso anche alla protezione delle infrastrutture energetiche critiche.

La questione se e rispettivamente quando gli attacchi alle reti di computer debbano essere considerati attacchi armati e quindi un «casus foederis» ai sensi dell'articolo 5 del Patto atlantico non è stata chiarita nell'ambito del vertice di Lisbona. Entro il mese di giugno del 2011 dovrà essere sviluppata una politica NATO dettagliata sulla protezione contro la

[30] L'European Climate Registry ha già inviato nell'estate del 2009 una e-mail corrispondente. Dal dicembre del 2008 il dominio «europeanclimateregistry.eu» è registrato sotto il nome di una persona di Bruxelles.

[31] Direttiva 2009/29/CE del 23.04.2009, punto (38).

[32] Cfr. ad esempio: MELANI Rapporto semestrale 2008/2, capitolo 3.6 http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=de (stato: 10 gennaio 2011).

[33] http://www.nato.int/cps/en/SID-70CABE49-11886860/natolive/news_69805.htm

cibercriminalità («cyber defence policy» / «politique de cyberdéfence») e dovrà essere elaborato un piano d'azione in vista della sua attuazione.

È interessante il fatto che il concetto di «cyber-defence» (inglese) / «cyberdéfence» (francese) utilizzato in entrambe le lingue ufficiali inglese e francese della NATO sia stato tradotto con «Schutz vor Computerkriminalität» dalla rappresentanza permanente della Germania presso la NATO in occasione della dichiarazione del vertice e nel concetto strategico[34]. Ciò potrebbe segnalare che i membri del Patto atlantico non hanno (ancora) convenuto se si debba reagire militarmente a un ciberattacco o se magari sia piuttosto adeguata una reazione di carattere civile. È invece incontestato il fatto che anche i militari debbano essere in grado di proteggere le proprie infrastrutture.

4.6 Trend in direzione dei vermi USB

I *supporti di dati USB* sono utilizzati con sempre maggiore frequenza come mezzo di diffusione di software nocivo. «Stuxnet»[35] e «Conficker»[36] sono soltanto i rappresentanti più eminenti di questa categoria. I supporti di memorizzazione USB sono sempre più economici e sono utilizzati sempre più sovente. Inoltre numerosi sistemi di computer sono meno protetti contro i parassiti USB che non ad esempio contro i parassiti diffusi attraverso le reti o le e-mail. Secondo quanto riferisce la ditta spagnola «Panda Security» il 25% dei vermi immessi per la prima volta in circolazione nel 2010 possono diffondersi tramite USB[37]. Questo dato risulta da uno studio condotto presso 10'470 imprese in Europa, in America del Nord e in America latina. Su numerosi computer aziendali non è ancora stato disattivato il file autorun.inf, che consente l'avvio automatico di programmi. Per il tramite di questa funzione è possibile installare senza problemi programmi nocivi, questo già all'atto del collegamento dell'apparecchiatura USB al computer.

Il vettore di infezione USB viene soprattutto sfruttato in combinazione con altri vettori di infezione. In questo caso il supporto USB serve anzitutto per superare la barriera del firewall. Una volta che il software nocivo si trova sulla rete aziendale gli ostacoli alla sua diffusione sono nettamente minori.

Le ripercussioni che può avere una chiavetta USB privata sono illustrate dal software nocivo arrivato nel 2008 sulla rete del Pentagono. Un soldato ha inserito una chiavetta USB privata infettata da malware in un computer situato in Medio Orimte e collegato alla rete militare. Da lì il software nocivo si è propagato su numerose reti interne, per raggiungere infine il settore classificato segreto della rete[38]. Anche il software nocivo «Conficker» si è insinuato in numerose reti aziendali, fra le quali reti di ospedali e reti militari.

I supporti di dati USB sono particolarmente adatti agli attacchi contro le imprese come vettori di software nocivo e sono quindi pericolosi. Nel frattempo ogni impresa ha installato buoni metodi di difesa della rete e anche il traffico e-mail è nella maggior parte dei casi sorvegliato contro i parassiti. Il parassita via USB ha però via libera se attraverso il computer di un

[34] http://www.nato.diplo.de/Vertretung/nato/de/04/NATO__Gipfel__Lisboa__1911_Seite.html (stato: 10 gennaio 2011).

[35] Cfr. i capitoli 4.1 e 5.1 del presente rapporto.

[36] Cfr. http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de, capitolo 4.2 (stato: 10 gennaio 2011).

[37] http://press.pandasecurity.com/news/25-of-new-worms-in-2010-are-designed-specifically-to-spread-through-usb-devices/ (stato: 10 gennaio 2011).

[38] http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (stato: 10 gennaio 2011).

collaboratore riesce a insinuarsi sulla rete al di là del firewall. Si tratta di un vettore di attacco adeguato per gli attacchi mirati e per i sistemi particolarmente isolati. La probabilità è grande che un collaboratore colleghi una volta o l'altra una chiavetta USB o un'altra apparecchiatura USB, come una fotocamera o uno smartphone, sia al computer privato che a quello aziendale. Anche la verifica preliminare delle chiavette USB con più programmi antivirus non garantisce una protezione integrale, proprio perché i programmi antivirus falliscono generalmente nel caso di software nocivi mirati e diffusi in piccole quantità.

4.7 Verme informatico «Here you have» – «Iraq Resistance»

Il 9 settembre 2010 ha incominciato a diffondersi su Internet un verme informatico sconosciuto che ha perturbato il traffico e-mail di numerose imprese americane. Il verme inviava e-mail recanti il soggetto «Here you have» e contenenti il testo «This is The Document I told you about, you can find it Here» o «Just For you» oppure ancora il testo «This is The Free Download Sex Movies, you can find it Here». Dietro la parola «Here» ci celava di volta in volta un link a un codice nocivo. Il link rinviava presuntamente a un documento o a un file video, mentre cliccandolo si scaricava in realtà il software nocivo sul proprio computer e si veniva invitati a eseguire un file. Il verme si propagava successivamente grazie ai diritti d'accesso e inviava l'e-mail contenente il link ai contatti dell'elenco degli indirizzi. A prescindere dalla sua propagazione e dall'attività di invio di e-mail che ha sovraccaricato determinati server, il verme non ha provocato danni particolari. Ne ha assunto la paternità una persona con il *Nickname* «Iraq Resistance», che ha preteso di fare parte del gruppo «Tariq bin Ziyad Brigades for Electronic Attack (TbZBEA)», gruppo finora sconosciuto. L'obiettivo del creatore del verme non era però di arrecare i maggiori danni possibili. In un messaggio di rivendicazione inviato a YouTube esso afferma di non essere un terrorista[39]. Anzi la sua azione andrebbe intesa come protesta contro l'invasione dell'Iraq da parte degli Stati Uniti e contro l'annuncio del rogo del Corano l'11 settembre 2010 negli Stati Uniti (che non fu in definitiva eseguito, ma questo per altri motivi).

Il metodo consistente nell'accesso all'elenco degli indirizzi dei sistemi e nell'invio di un testo allettante di e-mail da cliccare è un «*social engineering*» semplice, ma molto efficace. Si accorda maggiore importanza alla e-mail quando se ne conosce il mittente e se il testo della notizia è redatto in maniera tanto generale da apparire plausibile a molti destinatari. Negli anni 2000 (virus «I LOVE YOU») e 2001 (virus «Anna Kurnikova») sono stati propagati virus analoghi usando metodi paragonabili. Un'importante regola nell'impiego della posta elettronica consiste perciò nell'usare in linea di massima prudenza con le notizie contenenti link o allegati (anche quelle provenienti da mittenti conosciuti) e, in caso di dubbio, nel chiedere al mittente di che cosa si tratta esattamente. Negli ultimi tempi si utilizzano con maggiore frequenza allegati sotto forma di file PDF come vettori di infezioni. Per infettare il computer basta semplicemente cliccare il link a un sito Web appositamente predisposto oppure aprire un file.

Il virus qui descritto e battezzato «Here you have» è stato messo in circolazione in vista di una ciber-protesta dettata da motivi politici e religiosi. Se a prescindere dai suoi meccanismi di propagazione il virus avesse anche contenuto istruzioni per danneggiare su vasta scala i dati la faccenda si sarebbe rivelata nettamente meno blanda per alcune imprese.

[39] http://www.youtube.com/watch?v=IkMifFGqt78 (stato: 10 gennaio 2011).

4.8 Vasta rete bot staccata da Internet dalla polizia dei Paesi Bassi

Lunedì 25 ottobre 2010 la polizia dei Paesi Bassi ha staccato dalla rete il server di comando della rete bot «Bredolab». Si ritiene che «Bredolab» abbia infettato oltre 30 milioni di computer in tutto il mondo. La polizia dei Paesi Bassi ha staccato da Internet un complesso di 143 server che pilotavano la rete bot. Parallelamente è stato arrestato all'aeroporto di Erewan un uomo ventisettenne. La persona arrestata è sospettata di essere la mente dirigente della gestione della rete bot. Nel corso delle settimane precedenti gli inquirenti avevano analizzato in maniera approfondita l'infrastruttura.

Il gestore della rete bot perseguiva principalmente la diffusione di un software nocivo, utilizzando a tale scopo infezioni di siti Web. Non appena il computer era stato infettato dal software nocivo, questo si metteva alla ricerca del login e della password degli amministratori dei siti Web. I dati rinvenuti venivano a loro volta utilizzati per infettare altri siti Web in maniera completamente automatica. I server ora disinseriti erano gestiti dal gestore olandese «Leaseweb». Solitamente i server sono staccati immediatamente dalla rete dopo una simile scoperta, ma in questo caso «Leaseweb» ha continuato a utilizzarli su indicazione della polizia affinché la rete potesse essere analizzata.

L'autore o gli autori del reato si erano specializzati nella realizzazione di una rete bot possibilmente grande per affittare o vendere parti di essa. Dato che nel caso di «Bredolab» si tratta di un cosiddetto downloader, sul computer infettato è successivamente possibile scaricare qualsiasi genere di software nocivo.

Fin dal 9 aprile 2010 MELANI aveva segnalato nella sua newsletter questo software nocivo e il pericolo accresciuto di infezioni di siti Web[40]. Questo avvertimento è stato motivato dal fatto che il nuovo tool di controllo sviluppato dalla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI – che verifica sui siti Web svizzeri la presenza di eventuali infezioni di siti Web – aveva scoperto numerosi siti Web infettati da «Bredolab». I gestori e i provider sono stati successivamente contattati per rimuovere le infezioni.

La polizia dei Pesi Bassi ha scelto un nuovo modo di procedere per avvertire gli utenti dei computer infettati. A tale scopo si utilizzano i domini dei server di controllo e di comando corrispondenti per visualizzare sugli schermi dei singoli computer infettati un avvertimento «*pop-up*» indicante che il computer è inquinato da un software nocivo.

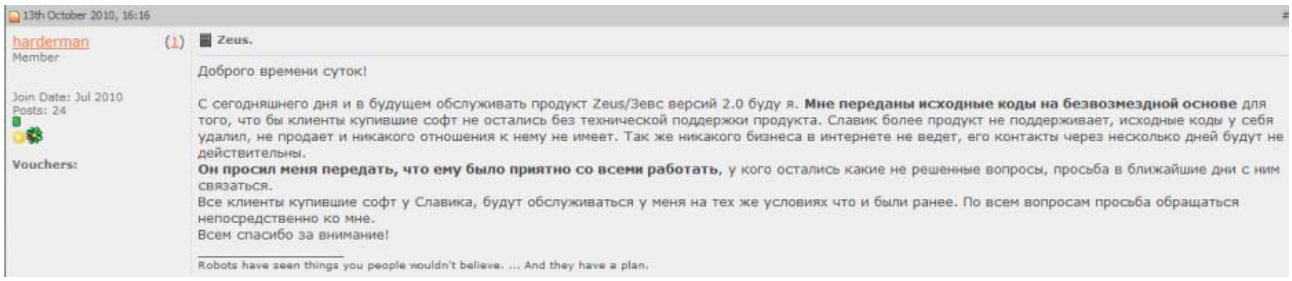
4.9 ZeuS e SpyEye – Fusione tra due dei maggiori cavalli di Troia dell'e-banking?

Il cavallo di Troia ZeuS è forse il banker più utilizzato al momento. Innumerevoli i rapporti, gli articoli e le attività organizzate intorno ad esso[41].

[40] http://www.melani.admin.ch/dienstleistungen/archiv/01107/index.html?lang=de (stato: 10 gennaio 2011).

[41] Ad esempio il sito di Brian Krebs, giornalista specializzato in criminalità del cyberspazio, contava 15 articoli in cui ZeuS era protagonista nel semestre preso in considerazione - http://krebsonsecurity.com (stato: 10 gennaio 2011). Il sito web https://zeustracker.abuse.ch/ (stato: 10 gennaio 2011) riporta più di 500 ZeuS C&C e una media di identificazione del codice nocivo da parte dei maggiori antivirus del 36.85%.

Sulla scena è emerso da inizio 2010 un altro banker simile il cui nome è SpyEye. Quest'ultimo integrava una funzione chiamata "ZeuS Killer Code", il cui scopo era identificare se il computer che stava infettando ospitava già ZeuS e in caso positivo eliminava il rivale. Si poteva quindi parlare di guerra tra i due codici. Invece l'autore di SpyEye, conosciuto con gli pseudonomi Gribodemon o Harderman[42], è diventato recentemente famoso nella scena underground quando a luglio ha annunciato che l'autore di ZeuS gli aveva ceduto il codice sorgente del malware e la gestione della clientela:


13th October 2010, 16:16

harderman (1)
Member

Join Date: Jul 2010
Posts: 24

Vouchers:

Zeus.

Доброго времени суток!

С сегодняшнего дня я в будущем обслуживать продукт Zeus/Зевс версий 2.0 буду я. **Мне переданы исходные коды на безвозмездной основе** для того, что бы клиенты купившие софт не остались без технической поддержки продукта. Славик более продукт не поддерживает, исходные коды у себя удалил, не продает и никакого отношения к нему не имеет. Так же никакого бизнеса в интернете не ведет, его контакты через несколько дней будут не действительны.
Он просил меня передать, что ему было приятно со всеми работать, у кого остались какие не решенные вопросы, просьба в ближайшие дни с ним связаться.
Все клиенты купившие софт у Славика, будут обслуживаться у меня на тех же условиях что и были ранее. По всем вопросам просьба обращаться непосредственно ко мне.
Всем спасибо за внимание!

Robots have seen things you people wouldn't believe. ... And they have a plan.

Figure 6: Il post di Hardermann su un forum underground

In alcuni post seguiti a quello sopra pubblicato, Harderman ha reso pubblico il fatto che non vi sarà più uno sviluppo della versione 2 di ZeuS, ma che la comunità dovrà aspettarsi un nuovo malware, che nascerà dalla fusione tra SpyEye e ZeuS.

4.10 Distrutta l'organizzazione di riciclaggio di denaro «J1 Network»

Il J1 Network, l'organizzazione di riciclaggio di denaro sporco proveniente da crimini online, così chiamata in quanto i suoi membri erano studenti stranieri in possesso del visa J1 per risiedere negli Stati Uniti, è stata smantellata dall'FBI. L'organizzazione era utilizzata da diversi gruppi criminali del cyberspazio, soprattutto da coloro che utilizzavano dei banker per rubare denaro dai conti bancari online. L'FBI ha annunciato aver arrestato 37 persone facenti parte dell'organizzazione[43].

[42] Il blog MalwareIntelligence riporta un'intervista con questa persona: http://www.malwareint.com/docs/spyeye-analysis-ii-en.pdf (stato: 10 gennaio 2011).

[43] Il comunicato dell'FBI di New York può essere letto a questo indirizzo: http://newyork.fbi.gov/dojpressrel/pressrel10/nyfo093010.htm (stato: 14 febbraio 2011).

Figure 7: J1 Network smantellato dal FBI.

Le persone incriminate, la maggior parte delle quali risiedeva su suolo americano grazie a un visa da studente, aprivano conti in vari istituti finanziari utilizzando documenti d'identità fasulli. Una volta ricevuti i soldi rubati da conti online, trattenevano una percentuale per se stessi e inviavano la somma restante verso la Russia. L'FBI stima a circa 3 milioni di dollari la somma totale riciclata.

4.11 «Money mules» di carte di credito

A fine dicembre 2010 ha fatto notizia l'e-mail qui appresso. Ai destinatari è stato illustrato in cattivo tedesco quanto fosse allettante fungere da cosiddetto «*money mule* di carte di credito». Sarebbero loro state inviate per posta carte di credito falsificate o derubate con le quali avrebbero dovuto prelevare denaro da inviare, dopo deduzione di una provvigione, all'autore del reato, rispettivamente a un altro agente finanziario. L'e-mail conteneva altresì risposte dirette a domande frequenti e la prima frase rendeva già attenti alle possibili conseguenze penali:

Esempio unicamente in tedesco!

Subject: Subject: Unternehmensfuhhrung sucht Teammitglieder

Eine Arbeit fur jemanden der sich im Klaren ist, dass falls was schief gehen sollte er im bestenfalls mit einer Bewahrungsstrafe auskommt , im schlimmsten ....

Ich bin in diesen Business seit 2002, mit mir hat eine Menge Leute gearbeitet , aber nur 2 wurden verhaftet und auch die nur wegen Ihrer Gierigkeit und Dummheit. Jeder einzelne der geschnappt wird, ist nicht nur ein finanzieller Verlust, sondern auch eine grosse Gefahr fur die gesamte Mannschaft. Deswegen sind folgende Regel zu befolgen:

1. Die Vorschriften werden strengstens eingehalten. Das Geld wird nur in den von mir bestimmten Bankautomaten zu der von mir angesagten Zeit abgehoben. Es wird nur die abgesprochene Summe abgehoben. Die Vorschriften fur das Erhalten der Kreditkarten und fur die Gelduebergabe werden strengstens befolgt. 2. Das Geld ist ehrlich abzugeben (keine Tauschungsversuche) 3. Nur anonyme Simkarten benutzen, dieses Telefon fur Anrufe der Freunde und Verwandte nicht verwenden 4. Sich nie mit *Arbeitskollegen* dieses Businesses treffen, wenn sich einer mit dir treffen moechte, arbeitet er zu

99% fur die Bullen 5. Wenn du keine Disziplin hast, die Regeln nicht einhalten kannst, bzw. mich fur paranoid haltst - dann sollen wir keine Zusammenarbeit auch versuchen.

Arbeitsbeginn
Du hollst die Kreditkarte ab. Wo das sein wird gebe ich am Telefon durch (meist bei dir in der Stadt oder in einer Grossstadt in deiner Umgebung. Zusammen mit der Karte erhalst du eine genaue Anweisung wo, wann und wie viel Geld abzuheben ist. Die Anweisung ist 100% genau auszufuhren, davon hangt unser Verdienst und auch deine Sicherheit ab. Fur die erste Karte musst du eine Pfandsumme von 300 Euro hinterlassen. Dies ist fur die Sicherheit, dass falls du alles abhebst und verschwindest, ich meine Kosten fur die Kreditkartenbeschaffung und die Transportkosten zu dir, decke. Du erhalst diese Pfandsumme bei der ersten Abhebung zurück, also bei den ersten Bankautomaten. Fur das erste mal erhallst du eine Kreditkarte und die dazugehorige Pin mit einen Abhebelimit von 1500 Euro. Hebst so viel ab, wie es in der Anweisung angegeben wird. Aus den abgehobenen Geld erhallst du 600 Euro , - 300 als Pfandruckgabe und 300 als dein Verdienst. Das restliche Geld ubergibst du an mich, wie das geschehen soll schreibe ich dir per sms. Weiter erhallst du 2-4 Karten pro Woche (Pfand brauche ich nicht mehr). Zum Anfang werden die Karten mit einen kleineren Guthaben sein 1000 bis 2000 Euro, davon erhallst du 300 bis 600 Euro als deine Provision. Spater, wenn unsere Zusammenarbeit gut verlauft und du alle Regel befolgst, arbeitest du mit Karten mit maximalen Guthaben, wo du pro Karte bis zu 1500 Euro verdienen kannst.

Um die Arbeit starten zu konnen, brauchst du eine anonyme Simkarte die du in jeden zweiten Internetkafe oder Callcenter erhalten kannst. So bald du diese hasst, teilst du mir die Nummer an meine Email: mit. Weiter schreibe ich dir eine Sms was du weiter zu tun hasst.

Gleich die Antworten auf meisstgestellte Fragen:
1. Was fur Garantien habe ich, dass Sie mit meinen 300 Euro nicht verschwinden?

An.: Gar keine, aber anders wird es nicht gehen. Wenn du Angst um 300 Euro hasst (vielleicht ist es eine grosse Summe fur dich) dann hoere ich von dir zu 100% nichts mehr, so bald du um die 5000 Euro abgehoben hasst.

2. Ich habe keine 300 Euro, kann ich als Garantie meinen Pas, meinen Studentenausweis, mein Wort, meine Freundin , meinen Arsch, etc. hinterlassen?

An: NEIN, ich stelle jeden Tag einen neuen Mitarbeiter an, meine Ausgaben pro Kartenzubereitung und den Transport zu dir sind ca. 300 Euro und falls du mit der Karte verschwindest habe ich 300 Euro Verlust- das muss nicht sein.

P.S So lange du nicht probierst an Geld zu kommen, weisst du nicht wo fur du geboren bist. Dein Leben lang auf Hartz 4 zu sitzen bzw. fur 1000 Euro im Monat deinen Arsch aufzureissen oder einige Male deinen Mut zusammen zu nehmen und vom Leben alles zu bekommen versuchen. Die, welche Mut und Nerven genug haben, diese Arbeit an zu nehmen, werden in ca. einen halben Jahr zu wohlhabenden Menschen und kriegen mit, dass das Geld nicht alles ist. Bevor du also meinen Angebot annimst uberlege ernsthaft ob du es wirklich brauchst und durchziehen kannst!!!

I money mules o cosiddetti agenti finanziari sono rari presso i criminali e sono quindi molto richiesti. Normalmente si ricorre ai loro servizi per riciclare il denaro proveniente da pagamenti bancari fraudolenti. A tale scopo si inventano storie più o meno plausibili affinché la vittima non abbia alcun sospetto che queste transazioni costituiscano una truffa oppure un'operazione di riciclaggio di denaro. Nella fattispecie la situazione è diversa perché l'autore invita apertamente a compiere un reato e fornisce anche consigli su come evitare di essere acciuffati. Nel caso dei money mules di carte di credito il pericolo di essere acchiappati è effettivamente minore. Mentre in caso di truffa all'e-banking l'agente finanziario funge da destinatario ma balza agli occhi fin dal primo pagamento fraudolento, ragione per la quale viene tolto dal circuito, nella presente fattispecie la tracciabilità è più difficile. Per questo motivo anche l'e-mail è volutamente predisposta non per reclutare persone inconsapevoli, ma è diretta a persone con un potenziale criminale. Non si può tuttavia escludere che si tratti nella fattispecie di una variante della «truffa alla nigeriana» e che dopo l'invio dei 300 euro di tassa iniziale il candidato non abbia più notizie del suo «datore di lavoro». In questo caso l'autore non teme alcuna querela perché la vittima stessa ha tentato di divenire un criminale.

5 Tendenze / Prospettive

5.1 «Stuxnet» – l'inizio dei cavalli di Troia SCADA

In origine i sistemi *SCADA* avevano poche analogie con le TIC usuali; essi erano isolati dalle reti di computer, utilizzavano hardware e software proprietari e facevano capo a protocolli propri per comunicare con l'elaboratore centrale. Nel corso degli ultimi anni l'ampia disponibilità di apparecchiature comparativamente a miglior mercato, provviste di interfacce per il protocollo Internet, è stata apportatrice di grandi cambiamenti in questo settore. Oggigiorno termometri, manometri, pompe, interruttori e altri cosiddetti elementi di campo dispongono sovente di un proprio indirizzo IP o utilizzano *TCP/IP* per comunicare con l'elaboratore centrale. Ci si procura a basso costo i vantaggi dell'uso di TIC esponendo in linea di massima i sistemi SCADA alle medesime minacce che conosciamo da Internet: si apre la porta al malware e agli aggressori («hacker»). Per via di corrispondenza si intensificano specialmente in questo senso i contatti internazionali e una più profonda collaborazione tra Stato e gestori di infrastrutture critiche di informazione in questo settore per scambiare informazioni attuali sui nuovi pericoli imminenti e sulle misure di difesa. MELANI è in stretto contatto con i distributori svizzeri di energia e partecipa allo scambio internazionale di informazioni nel quadro dell'«European SCADA and Control Systems Information Exchange» EuroSCSIE.

Nonostante le numerose speculazioni su chi si cela dietro il software nocivo «Stuxnet», l'autore è tuttora sconosciuto ed è probabile che lo rimanga. Gli attacchi di questo genere vivono proprio del vantaggio proveniente da una tracciabilità estremamente difficile se non addirittura impossibile. Dato che nel caso di questo attacco l'intento finanziario era di interesse subordinato e che la motivazione era piuttosto di natura politica è ovvio presumere l'intervento da parte di uno Stato. Le possibilità di spionaggio e di sabotaggio elettronico sono note da lungo tempo nelle cerchie dei servizi segreti e sono anche utilizzate attivamente. «Stuxnet» è stato soltanto il primo caso a destare l'attenzione del mondo intero. Diversamente dai terroristi che scelgono accuratamente i loro obiettivi e attaccano solo gli impianti la cui perturbazione è graduata come indispensabile ai fini della tutela degli interessi nazionali. In presenza di una motivazione altrettanto forte e di risorse sufficienti praticamente ogni sistema può prima o poi essere infiltrato o sabotato. Ci si deve aspettare che simili attacchi si ripetano in futuro.

5.2 DDoS – Retroscena e motivazioni

Gli attacchi alla disponibilità dei siti Web, i cosiddetti attacchi di Distributed Denial of Service (DDoS) sono utilizzati per i più diversi scopi nel ciberspazio. Inizialmente gli attacchi avevano il carattere di semplici atti di vandalismo. Nel frattempo ne sono mutate le motivazioni. Si osservano ad esempio attacchi DDoS come strumento di vendetta, per danneggiare la concorrenza, per estorcere protezione o per motivi politici. Se la maggior parte degli attacchi DDoS di minori dimensioni rimangono nascosti e non pervengono alla conoscenza del pubblico, si verificano sempre attacchi DDoS di maggiori dimensioni volti a destare una maggiore attenzione (mediatica). I siti Web e i server Web rientrano nella categoria degli obiettivi preferiti. Ma si può però anche trattare di server di posta elettronica, di serverDNS, di router e di firewall o di altri tipi di servizi Internet. Qui appresso sono descritte diverse motivazioni degli autori.

Attacchi politici

Gli attacchi a sfondo politico non costituiscono un fenomeno nuovo. Gli hacker si servono di una varietà di risorse illegali o perlomeno dubbie per attirare l'attenzione sulle loro richieste. Si sferrano attacchi DDoS contro le applicazioni più frequenti oppure si deturpano siti Web.

L'esempio più rilevante di attacco DDoS a sfondo politico è stato quello del 2007 ai danni dell'Estonia. Dopo una controversia concernente lo spostamento di un monumento sovietico ai morti nella città di Tallinn i siti Web estoni sono rimasti irraggiungibili per più settimane. Gli attacchi DDoS sono però anche stati utilizzati come misure di sostegno bellico. Nel 2008, nel contesto delle azioni militari del conflitto che coinvolgeva le repubbliche ribelli dell'Ossezia del Sud e dell'Abcasia numerosi siti Internet ufficiali della Georgia non sono più stati raggiungibili o sono stati deturpati. Ne sono in particolare stati colpiti i siti del Governo georgiano. Un anno dopo, il giorno dell'anniversario dell'offensiva russa, sono stati osservati attacchi DDoS ai danni di «Twitter», «Facebook» e «LiveJournal», attribuiti a un *blogger*[44] georgiano denominato «Cyxymu»[45] che nei suoi post si è di volta in volta espresso criticamente nei confronti della politica caucasica della Russia[46]. Un attacco DDoS che si ritiene altresì a sfondo politico è quello che è stato sferrato nell'aprile del 2008 contro l'emittente bielorussa «Radio Free Europe», sostenuta dagli Stati Uniti. L'attacco è iniziato il giorno dell'anniversario della catastrofe nucleare di Chernobyl. Quel giorno la radio trasmetteva la diretta di un'azione di protesta a Minsk che ricordava lo stato di difficoltà delle vittime e si esprimeva contro un decreto del Governo relativo alla costruzione di una nuova centrale nucleare. Si presume che al culmine dell'attacco il sito Web dell'emittente sia stato sommerso da quasi 50'000 richieste al secondo.

Anche in Svizzera si sono già verificati attacchi DDoS a sfondo politico. Nel nostro Paese il primo attacco DDoS a sfondo probabilmente politico si è verificato nel 2007. A quell'epoca la disponibilità del sito Internet dei Servizi del Parlamento (parlament.ch) è stata pregiudicata per diversi giorni. Vi sono state inviate a brevi intervalli richieste di ricerca che costringevano a lunghi elenchi di risultati, compromettendo i tempi di risposta del server. Il motivo esatto di questo attacco non è mai stato chiarito, ma il suo obiettivo consente di presumere ragioni politiche o perlomeno non un motivo finanziario.[47] Tre anni più tardi, nel novembre del 2010, sono stati attaccati i siti Web di quattro partiti politici di Governo. Anche in questo caso si presume una motivazione politica, in particolare perché l'attacco è stato sferrato al momento della votazione sull'iniziativa espulsione (cfr. il capitolo 3.1). È invece chiara la motivazione dell'attacco DDoS del dicembre 2010 a PostFinance, dopo la chiusura del conto di Julian Assange, fondatore di «Wikileaks». La peculiarità di questo attacco consiste nel fatto che i simpatizzanti di «Wikileaks» abbiano potuto scaricare e utilizzare un programma denominato «Low Orbit Ion Canon» che ha poi scatenato una gran quantità di richieste a PostFinance (cfr. il capitolo 3.2). Un siffatto modo di procedere era già stato osservato nel caso dell'attacco DDoS all'Estonia. In quell'occasione si era fatto circolare nei forum in lingua russa uno script che ha sommerso di richieste ping gli indirizzi IP e i server DNS di circa 19 siti Web estoni.

---

44 http://news.cnet.com/8301-27080_3-10305200-245.html (stato: 14 febbraio 2011).

45 http://cyberinsecure.com/distributed-denial-of-service-attack-takes-down-twitter/ (stato: 14 febbraio 2011).

46 http://wwwguardian.co.uk/world/2009/aug/07/georgian-blogger-accuses-russia (stato: 14 febbraio 2011).

47 MELANI Rapporto semestrale 2007/2, capitolo 4.1
http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it (stato: 14 febbraio 2011).

Estorsione e danneggiamento della concorrenza

Il crash dell'infrastruttura Web significa un grave danno finanziario per le imprese che svolgono una grande parte dei loro affari su Internet. Se il crash perdura per più giorni il danno può financo minacciarne l'esistenza. In questo caso i criminali ricorrono e utilizzano reti bot per estorcere denaro dalle imprese attive su Internet. La procedura utilizzata ricorda fortemente il racket protettivo. L'esempio qui appresso illustra come può presentarsi una simile lettera di estorsione.

Sehr geehrter Shop-Admin,

am , um 12:00 Uhr werden wir Ihren Shop für 30 Minuten unerreichbar für Sie und Ihre Kunden machen.

Dies hat folgenden Grund:

Wir werden Ihren Online Shop mit einfachen DDoS attackieren, so dass weder Sie, noch Ihre Kunden Zugriff auf Ihre Webseite, geschweige denn auf den Server haben.

Dies wird nur ein kleiner Testlauf sein damit Sie sehen wie ernst es uns ist!

Wir bieten Ihnen hiermit die Option an, weder die Testattacke noch den folgenden DDoS zu bekommen, indem Sie bis morgen 300 Euro in Form eines Ukash Vouchers (an jeder Tankstelle zu erhalten) uns via eMail, an die angegebene E-Mail Adresse (@) senden.

Informationen über Ukash finden Sie auch auf http://www.ukash.com oder an Ihrer Tankstelle.

Sollte bis morgen 11:45 Uhr kein Ukash Code eingegangen sein, so werden wir um Punkt 12:00 Uhr den DDoS starten, anfangs nur für 30 Minuten. Falls Sie nicht zahlen wird Ihr Service für längere Zeit offline bleiben,was ihren Umsatz wohl stark sinken lassen wird.

Figura 8: Lettera di estorsione al proprietario di un Web shop.

Il gestore del Web shop ha quindi la possibilità di pagare oppure di accettare l'attacco e di difendersene con l'aiuto del provider. A seconda delle dimensioni della rete bot che si cela dietro l'attacco è molto difficile difendersi e non da ultimo può anche subentrare una disdetta da parte del provider. In Svizzera sono stati finora osservati prevalentemente attacchi DDoS ai danni di siti del commercio sessuale. Già nel 2007 diversi siti sono stati tra l'altro attaccati per il tramite di una rete bot. Sebbene i proprietari abbiano frequentemente cambiato provider, il loro portale è rimasto irraggiungibile per parecchi mesi. Anche i grandi provider come Swisscom e Cablecom sono già stati oggetto di attacchi DDoS. In questo caso gli attacchi non erano diretti contro i provider, bensì contro il loro clienti[48].

La pericolosità di questi attacchi consiste nel fatto che essi possono avere ripercussioni sulla rimanente infrastruttura di rete e, nella peggiore delle ipotesi, sull'intera rete. Nel mondo reale ciò sarebbe paragonabile all'attentato a una determinata persona in un edificio. Per raggiungere questa persona l'intero edificio è raso al suolo. Le altre persone che si trovano nel momento sbagliato nell'edificio e che riportano danni, sono consapevolmente tollerate come danni collaterali dagli aggressori.

[48] MELANI Rapporto semestrale 2009/1, capitolo 3.4 http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de (stato: 14 febbraio 2011) e MELANI Rapporto semestrale 2009/2, capitolo 3.3 http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=de (stato: 14 febbraio 2011).

Strumento di vendetta

Nelle cerchie della cibercriminalità il Denial of Service costituisce da lungo tempo uno strumento per tenere lontani i concorrenti sgraditi, rispettivamente per convincere i «clienti» potenziali a passare sulle proprie reti o ai propri servizi. I concorrenti o i commenti spiacevoli sono puniti in maniera conseguente. Oltre ai concorrenti, nel mirino dei criminali figurano soprattutto le ditte di sicurezza IT. In questo senso ad esempio «Storm Worm» integrava un meccanismo per colpire e paralizzare con attacchi DDoS i siti di scanner antivirus online e quindi proteggere la propria rete bot dall'essere scoperta. Un ulteriore esempio riguarda la ditta di sicurezza IBM/ISS, i cui esperti avevano analizzato la struttura di una rete bot. Poco tempo dopo il collegamento Internet dell'impresa è stato perturbato per parecchi giorni da un attacco DDoS.[49]

Dato che gli attacchi non sono sempre diretti verso un obiettivo specifico (nella maggior parte dei casi un sito Web), ma contro l'infrastruttura sottostante del provider (di hosting), ne sono compromessi anche altri siti Internet e reti. Nella migliore delle ipotesi ai non partecipanti ne risultano soltanto perdite finanziarie; ma nella peggiore delle ipotesi possono essere perturbati o interrotti processi estremamente più critici che dipendono dalla rete sotto attacco.

5.3 Mobile (in)security

Il primo virus per smarphone ad attirare l'attenzione nel 2004 è stato il verme «Cabir», che si propagava attraverso l'interfaccia Bluetooth. A prescindere dal fatto che era responsabile dello scaricamento delle batterie, perché era costantemente alla ricerca di apparecchiature *Bluetooth* raggiungibili, questo verme non ha arrecato grandi danni.

Per lungo tempo si è ritenuto che il pericolo di virus per gli *smartphone* fosse esiguo perché gli smartphone non costituirebbero un obiettivo redditizio per l'industria del malware. Ne sarebbero motivo la molteplicità dei sistemi operativi, la difficile diffusione del malware e l'assenza di «modelli d'affari della criminalità informatica». La diffusione crescente degli smartphone e di telefoni mobili con funzionalità di tipo PC come pure la memorizzazione di dati sensibili su questi apparecchi li rende però maggiormente attraenti anche per i criminali.

Con un'affermazione e una concentrazione dei sistemi operativi per la telefonia mobile come quelle che alle quali si assiste in questo momento[50], aumenta inoltre il pericolo di incidenti con software nocivo simili a quelli noti dai computer. Il segnale del risveglio è sicuramente venuto da una lacuna critica PDF sull'iPhone nell'agosto del 2010, che ha suscitato grande interesse nei media. Quando un file PDF appositamente predisposto veniva aperto con il browser «Safari Mobile» sugli apparecchi «iPhone», «iPad» e «iPod Touch» di Apple era possibile effettuare un *Jailbreak.* È ovvio che una simile lacuna sia interessante per i criminali. Ma anche sul sistema operativo «Android» è stato individuato nel mese di agosto il primo cavallo di Troia per SMS. Camuffato come mediaplayer, ad avvenuta installazione esso invia SMS soggetti a pagamento. L'installazione è invero disagevole ed esige una grande interazione da parte dell'utente. Ciononostante anche in questo caso gli utenti si sono fatti indurre a eseguire l'installazione. Anche un software nocivo che si spaccia per

[49] http://www.tecchannel.de/sicherheit/news/1737083/storm_worm_schlaegt_zurueck_it_security_forscher_angegriffen/ (stato: 17 febbraio 2011).

[50] http://www.zeit.de/digital/mobil/2011-02/nokia-microsoft-wp7 (stato: 17 febbraio 2011).

«Angry Bird»[51], il gioco «Tap Snake» – che non è soltanto un gioco[52] – e di recente «Geinimi»[53] hanno preso di mira gli smartphone «Android».

ZeuS Mitmo: Man-in-the-mobile

Nel mondo clandestino sono in atto sforzi in vista di ulteriori innovazioni. Nel caso di «ZeuS», sicuramente il cavallo di Troia maggiormente diffuso in ambito di e-banking, si manifestano in questo senso segnali di una sua utilità anche nel mondo della telefonia mobile. L'impresa spagnola di sicurezza «S21» ha pubblicato recentemente un articolo relativo a una variante della quale si presume che venga impiegata per i sistemi di autenticazione a due canali che utilizzano il telefono mobile come secondo canale[54]. All'utente del computer infettato da una versione speciale di «ZeuS» vengono poste in questo caso, durante la sessione di e-banking, diverse domande sul suo telefono mobile, compreso il numero telefonico. Si spiega poi alla vittima che per motivi di sicurezza l'istituto finanziario invierà al telefono mobile un nuovo certificato (il numero infatti è ora noto al truffatore) che dovrà essere installato. Grazie a questo presunto certificato anche il telefono mobile è infettato. All'atto della transazione di e-banking, quando la banca invia tramite SMS il codice di autenticazione, questa comunicazione non è visibile al cliente. Essa perviene invece al truffatore che può allora effettuare il login.

È prevedibile che n futuro gli utenti dell'e-banking disbrighino viepiù le loro transazioni per mezzo del loro telefono mobile. Questa circostanza pone gli istituti finanziari davanti a nuove sfide e questo non soltanto perché il telefono mobile non dispone ancora della medesima protezione dei computer «normali». Nel caso per l'appunto dell'autenticazione a due canali a mezzo SMS-TAN si schiudono nuove possibilità di inganno degli utenti dell'e-banking, a prescindere dal fatto che in tal modo lo smartphone non possa più essere utilizzato come canale indipendente di autenticazione. I pericoli non sono certamente immediati, ma queste riflessioni vanno integrate fin d'ora nella pianificazione della prossima generazione di autenticazione in ambito di e-banking.

Applicazioni di spionaggio per la telefonia mobile

Nel secondo semestre del 2010 sono state pubblicate numerose applicazioni per il tramite delle quali è possibile spiare colloqui, comunicazioni e altri dati personali (agenda, GPS ecc.) sui telefoni mobili. Oltre ai programmi già noti, come «FlexiSpy» e «SpyPhone», si ritrovano nuovi nomi come «Phone Creeper» oppure «Remote iPhone Spy». L'apparizione di numerose applicazioni a scopo di spionaggio solleva diverse questioni: queste funzioni o funzioni analoghe sono integrate anche in altre applicazioni palesemente inoffensive? In quale ambito le applicazioni di spionaggio possono in genere essere utilizzate? Una risposta possibile a questa ultima domanda è fornita dall'arresto in Romania di 50 persone che avevano utilizzato applicazioni di spionaggio per la telefonia mobile[55]. Fra i motivi addotti più frequenti figuravano lo spionaggio del coniuge o di un concorrente.

[51] http://www.heise.de/security/meldung/Android-Luecken-ermoeglichen-heimliche-Installation-von-Apps-1134661.html (stato: 10 gennaio 2011).

[52] http://www.f-secure.com/weblog/archives/00002011.html (stato: 14 febbraio 2011).

[53] http://blog.mylookout.com/2010/12/geinimi_trojan/ (stato: 14 febbraio 2011).

[54] http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html (stato: 14 febbraio 2011).

[55] http://www.theregister.co.uk/2010/07/01/romanian_spyware_arrests/ (stato: 14 febbraio 2011).

Non soltanto smartphone: attacco alla rete GSM e SMS of Death

Anche se viene fatta molto pubblicità per gli smartphone, la loro quota rispetto al mercato mondiale della telefonia mobile è per il momento del solo 19%[56]. I ricercatori Collin Mulliner e Nico Golde hanno pertanto presentato al «Chaos Communication Congress»[57] uno scenario possibile per attaccare i telefoni mobili «normali», che costituiscono la quota principale del mercato mondiale. L'attacco è stato perpetrato per il tramite di un semplice SMS che era stato appositamente predisposto per il trasporto del codice *binario* di attacco. Questo principio è peraltro utilizzato dai provider di telefonia mobile per effettuare configurazioni sui telefoni mobili o installarvi servizi supplementari. L'attacco presentato in quella sede ha provocato il crash del telefono mobile.

L'attrattiva dei telefoni mobili come obbiettivo di attacchi di malware o di furto di dati è determinata da due fattori: anzitutto quanto più un telefono mobile svolge le medesime funzioni di un PC (accesso a Internet, memorizzazione di dati sensibili, disbrigo di transazioni finanziarie ecc.) tanto più esso diviene un obiettivo lucrativo di attacco per i criminali. Secondariamente, in maniera analoga al malware destinato ai PC, anche nel caso del malware per i telefoni mobili si può partire dall'idea che con le dimensioni del «pubblico mirato» aumenti anche l'attrattiva di un attacco. Ci si deve quindi aspettare che la crescente diffusione dei telefoni mobili moderni costituisca un obiettivo di attacco sempre più attraente. Per il fatto di questa evoluzione i problemi di sicurezza in Internet dovrebbero trasferirsi in futuro sul mondo mobile. Nel corso degli anni a venire gli smartphone si svilupperanno ulteriormente come personal computer di piccole dimensioni. Già ora appare fluttuante la differenziazione tra smartphone, PC tablet e notebook. Esiste però una differenza a livello di protezione dei sistemi. Mentre sui computer i programmi di sicurezza fanno parte della dotazione standard, tali programmi sono invece praticamente inesistenti nel settore degli smartphone. Inoltre più dell'85% dei telefoni mobili utilizzati nel mondo intero sono cosiddetti «Feature Phones», semplici apparecchi con un numero esiguo di funzioni, come ad esempio l'ascolto di file mp3 e soprattutto nessuna possibilità di aggiornamento[58]. Ma anche nel caso degli altri smartphone l'esperienza insegna che l'aggiornamento non è installato immediatamente, perché lo smartphone deve essere collegato al computer e non funziona in sottofondo attraverso la rete, come siamo abituati con il PC.

5.4 «Cloud Computing» – Misure cautelari

Non risale certamente a ieri il concetto di «*cloud*» nel contesto delle modalità che i privati, le imprese e le amministrazioni dovrebbero usare nel maneggiare i loro documenti, applicazioni e simili. Il principio alla base è relativamente semplice e ci riporta agli albori dei computer e delle reti. Diversamente dai sistemi cliente ormai adulti – dove il sistema operativo gestisce tutto, dalle applicazioni ai documenti – nel cloud il computer deve anzitutto funzionare come terminale, sia a casa che sul posto di lavoro. I programmi di elaborazione dei testi necessari, i dati e altre applicazioni sono collocati in maniera centralizzata su un elaboratore e sono messi a disposizione attraverso un collegamento via rete. Il vantaggio di una simile soluzione è evidente. Invece che sul dispendio amministrativo di ogni singolo computer e dei programmi e dati che contiene, ci si può concentrare sui sistemi centrali. I cicli di patch riguardano ormai un solo sistema e ogni utente che vi è collegato dispone sempre della

[56] http://www.gartner.com/it/page.jsp?id=1466313 (stato: 14 febbraio 2011).

[57] Chaos Communication Congress (Berlino, 27-30 dicembre 2010).

[58] http://www.wired.com/threatlevel/2010/12/simplest-phones-open-to-%25E2%2580%259Csms-of-death%25E2%2580%259D/ (stato: 10 gennaio 2011).

versione più recente dell'applicazione, corrispondente al suo ultimo stato. Anche i documenti divengono accessibili in maniera più semplice e ovunque, perché non esistono più soltanto a livello locale su un *network-share* o su un computer.

Questo approccio ripropone tuttavia questioni sollevate da lungo tempo e dubbi in fatto di sicurezza. L'ownership dell'informazione sfugge de facto di mano e l'intera fiducia nella sicurezza dei dati è in mano a terzi. In questo senso la tendenza in direzione del cloud computing è anche una tendenza a ritroso in direzione di una fiducia cieca nei tecnici e negli esperti di sicurezza IT. Proprio questa evoluzione era in fase di inversione nel corso di questi ultimi anni, perché le imprese e le amministrazioni hanno viepiù considerato la sicurezza delle reti e delle IT in generale come valori strategici e non come mere funzioni di sostegno. In questo senso si profila in tempi prevedibili un conflitto classico di obiettivi tra minori costi di transazione, sicurezza tecnica più efficiente e tendenza a preoccuparsi delle informazioni all'interno dell'impresa mediante adeguate misure di sicurezza a livello tecnico, personale e fisico.

Anche a livello di offerenti di cloud computing si pongono al momento ancora alcuni problemi. In questo senso nel caso della maggior parte degli offerenti i dati della clientela e i servizi offerti non sono sempre lasciati localmente e staticamente allo stesso posto, ma spostati in maniera distribuita su più centri di calcolo e riuniti a seconda delle necessità. In questa misura non è possibile dire con esattezza quando e dove si trova quale documento. Questa circostanza solleva anche questioni giuridiche, perché vigono leggi diverse a seconda del Paese nel quale un determinato documento si trova a un determinato momento.

5.5 Monopoli di rete – un problema di sicurezza?

Pochi grandi attori della rete sono in grado influenzare lo sviluppo di Internet e delle infrastrutture della rete[59]. Alla fine del 2010 diversi record sono stati battuti. Quali sono gli effetti da un punto di vista della sicurezza a causa di tali concentrazioni?

Google ha battuto un nuovo record di traffico[60], arrivando a rappresentare il 6.4% del traffico totale di Internet. Secondo Arbor Networks, se Google fosse un ISP sarebbe il secondo maggiore al mondo, il primo essendo quello che fornisce gran parte del transito per Google. Facebook è diventato il sito più visitato negli Stati Uniti[61], superando il peso massimo della categoria, Google.

«BitTorrent», la compagnia responsabile per i client di file-sharing «BitTorrent» e «µTorrent» ha annunciato[62] che 100 milioni di utenti utilizzano uno dei due software da essa prodotti.

---

[59] A titolo di esempio basti pensare all'iniziativa di Google per la costruzione di una a fibra ottica che dia la possibilità all'americano medio di viaggiare in rete ad una velocità 100 volte superiore a ciò di cui dispone ora - http://googleblog.blogspot.com/2010/02/think-big-with-gig-our-experimental.html (stato: 10 gennaio 2011). Oppure agli obiettivi del padre di Facebook, Mark Zuckerberg, che con la sua piattaforma vorrebbe diventare il punto di entrata nel web (http://www.wired.co.uk/news/archive/2010-11/04/facebook-mobile-platform (stato: 10 gennaio 2011); http://www.spiegel.de/wirtschaft/unternehmen/0,1518,719920,00.html (stato: 10 gennaio 2011); http://www.ustream.tv/recorded/3848950 (stato: 10 gennaio 2011); http://www.newyorker.com/reporting/2010/09/20/100920fa_fact_vargas (stato: 10 gennaio 2011).

[60] http://asert.arbornetworks.com/2010/10/google-breaks-traffic-record/ (stato: 10 gennaio 2011).

[61] http://www.hitwise.com/us/press-center/press-releases/facebook-was-the-top-search-term-in-2010-for-sec/ (stato: 10 gennaio 2011).

«Drupal», il noto gestore di contenuti (CMS) ha dal canto suo rilasciato una nuova versione: in occasione del lancio Drupal ha affermato[63] che l'1% di tutti i siti web del mondo sono gestiti grazie a questo software.
Secondo «Twitter», in Giappone, negli attimi seguiti all'inizio del nuovo anno, sono stati pubblicati oltre 7'000 tweets al secondo: impressionante la rappresentazione su una mappa della pubblicazione di tweets durante il capodanno nelle varie fasce orarie mondiali[64].

Infezioni da malware

La presenza di una pagina infetta su una piattaforma molto frequentata rappresenta un incubo per qualsiasi esperto in sicurezza informatica. I casi legati alla compromissione di server di pubblicità (ad servers) seguono questo schema (vedi capitolo 3.13). Se si riesce ad accedere a un Ad-Server, è molto probabile che si riesca ad infettare una grande quantità di utenti. Sul social network Facebook sono transitate una miriade di infezioni, la più famosa quella di «Koobface». Ma oltre ai messaggi, i codici nocivi si possono veicolare attraverso tecniche quali il drive-by. Le piattaforme P2P costituiscono un vettore di infezione spesso sottostimato. Spesso un film, una canzone o un software scaricati da reti P2P contengono, oltre al documento stesso, anche un cavallo di Troia o un dropper. Un altro pericolo viene dai CMS maggiormente utilizzati, come «Drupal» o «WordPress». Una lacuna di sicurezza in un tale software (e WordPress ne ha avute), lascerebbe centinaia di migliaia di siti vulnerabili ad attacchi. Si potrebbe anche pensare ad un attacco contro il Domain Name Service (DNS) di siti importanti, in modo da fornire agli utenti delle copie appositamente modificate delle pagine richieste con lo scopo di infettare i computer dei visitatori.[65].

Utilizzo di dati personali

Grandi imprese come Facebook raccolgono un'enorme quantità di dati. Google StreetView , oltre a fotografare le strade per la propria mappa, raccoglieva dati riguardanti le connessioni wireless che incontrava sul suo cammino[66]. Siti web come Groupon.com raccolgono dati importanti sui propri utenti, come geolocalizzazione e preferenze[67]. Foursquares.com sa esattamente chi si trova dove e quando . Da una parte utilizzando pochi siti web è possibile costruire l'identikit di una persona, le sue abitudini. Dall'altra poco si sa dei dati raccolti da queste imprese e l'impiego che di essi viene fatto. Gli utenti della rete sono sempre più disposti a disseminare i propri dati personali sui maggiori siti web.
Sorgono quindi diverse domande in seguito alla nascita dei grandi giganti della rete: domande legate alla sicurezza dei dati e degli utenti ma anche domande legate alla trasformazione della morfologia di Internet, in mano sempre più a gruppi che producono miliardi di dollari e di cui sa poco o niente.

---

62 http://www.bittorrent.com/pressreleases/2011/01/03/bittorrent-inc-grows-to-over-100-million-active-monthly-users-massive-user- (stato: 10 gennaio 2011).

63 http://buytaert.net/drupal-7.0-released (stato: 10 gennaio 2011).

64 http://www.flickr.com/photos/twitteroffice/5330386295/ (stato: 10 gennaio 2011).

65 Un caso celebre è quello di Twitter sul finire del 2009 (http://www.wired.com/threatlevel/2009/12/twitter-hacked-redirected/ (stato: 10 gennario 2011). Se al posto di un messaggio di defacement gli utenti avessero trovato una copia modificata del sito di Twitter, l'attacco avrebbe potuto avere conseguenze drammatiche.

66 MELANI Rapporto semestrale 2010/1, capitolo 4.5: http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html?lang=it (stato: 10 gennaio 2011)

67 http://www.zdnet.com/blog/feeds/foursquares-privacy-loopholes/2607 (stato: 10 gennaio 2011).

6 Glossario

Il presente glossario contiene tutti i concetti che figurano in *caratteri corsivi* nel testo. Un glossario completo è disponibile in: http://www.melani.admin.ch/glossar/index.html?lang=it.

AdServer	Gli AdServer sono utilizzati per distribuire e misurare il successo della pubblicità su Internet. Sia lo stesso server fisico, sia il software Ad che gira su di esso possono essere designati come AdServer.
Adresse IP	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
Agente finanziario	È un agente finanziario chiunque svolge legalmente l'attività di intermediario monetario e quindi anche operazioni di trasferimento finanziario. In tempi recenti questo concetto è utilizzato nel contesto delle transazioni finanziarie illegali.
Applicazione	Un programma per computer che esegue un determinato compito. I programmi di elaborazione dei testi e i browser per Internet sono esempi di applicazioni.
Attacco (Distributed-) Denial-of-Service (DDoS)	Ha lo scopo di rendere irraggiungibile un determinato servizio all'utente o perlomeno di ostacolare notevolmente la raggiungibilità di detto servizio.
Autenticazione a due fattori	A tal fine sono necessari almeno due dei tre fattori di autenticazione: 1. una cosa che si conosce (ad es. passwort, PIN ecc.); 2. una cosa che si ha (ad es. certificato, token, elenco da cancellare ecc.); 3. una cosa che si è (ad es. impronte digitali, scanner della retina, riconoscimento vocale ecc.)
Blog	Un blog è un diario tenuto su un sito Web e quindi nella maggior parte dei casi visibile al pubblico, sul quale almeno una persona, il Web-logger o blogger (in forma abbreviata), registra annotazioni, elenca circostanze o mette per scritto riflessioni.
Bluetooth	Una tecnologia che consente la comunicazione senza fili tra due apparecchi finali e utilizzata soprattutto in ambito di telefonia mobile, di laptop, di PDA e di dispositivi di immissione (ad es. il mouse del computer).
Bot / Malicious Bot	Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione.
Browser/Navigatore	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Opera, Firefox e Safari.

Cavalli di Troia	I cavalli di Troia (sovente chiamati troiani) sono programmi che eseguono di nascosto operazioni nocive, camuffandosi in applicazioni e documenti utili per l'utente.
Computer Emergency Response Team (CERT)	Si designa come CERT (ma anche come CSIRT per Computer Security Incident Response Team) un gruppo che si occupa del coordinamento e dell'adozione di misure nel contesto di incidenti rilevanti ai fini della sicurezza delle IT.
Certificato digitale	Certifica l'appartenenza di una chiave pubblica (PKI) a un soggetto (persona, elaboratore).
Cloaking	Il cloaking (dall'inglese dissimulare) è una tecnica di ottimizzazione dei motori di ricerca nel cui ambito al Webcrawler dei motori di ricerca viene presentata con il medesimo URL una pagina diversa da quella dell'utente. Esso è destinato a migliorare la graduatoria e l'indicizzazione dei risultati dei motori di ricerca.
Cloud Computing	o «cloud computing» (sinonimo: «cloud IT», in italiano: «calcolare tra le nuvole»); concetto della tecnica dell'informazione (IT). Il paesaggio IT non è più esercitato/messo a disposizione dall'utente stesso, bensì proposto da uno o più offerenti. Le applicazioni e i dati non si trovano più sul computer locale nel centro di calcolo della dit-ta, ma in una nuvola («cloud»). L'accesso a questi sistemi a distanza è effettuato per il tramite di una rete.
Content Management Systems (CMS)	Un «Content Management System» (acronimo CMS, in italiano «sistema di gestione dei contenuti») è un sistema che rende possibile e organizza la produzione e l'elaborazione comune di contenuti, consistenti in documenti di testo e multimediali, in genere destinati al World Wide Web. Un autore può servirsi di un simile sistema anche senza conoscenze di programmazione o di HTML. In questo caso il contenuto informativo da presentare è detto «content» (contenuto).
Controllore logico programmabile (CLP)	Un controllo logico programmabile (CLP), in inglese Programmable Logic Controller (PLC), è un'apparecchiatura utilizzata per il controllo o la regolazione di una macchina o di un impianto che viene programmata su base digitale. Da alcuni anni esso sostituisce nella maggior parte dei settori il controllore programmabile cablato a livello di hardware.
Cookie	Piccolo file di testo depositato sul computer dell'utente alla visita di una pagina Web. Con l'ausilio dei cookies è per esempio possibile salvaguardare le impostazioni personali di una pagina Internet. Essi possono però anche essere sfruttati in modo abusivo per registrare le abitudini di navigazione dell'utente e allestire in tale modo un profilo di utente.
Critical Infrastructure Protection / Critical Information Infrastructure	Importante elemento della politica nazionale di sicurezza e della pianificazione della difesa. Espressione generale per concetti e strategie per la protezione di infrastrutture critiche /

Protection (CIIP)	infrastrutture critiche di informazione.
Domain Name System (DNS)	Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo l'utente può utilizzare nomi (ad es. www.melani.admin.ch).
DNS Amplification Attack	Attacco di Denial of Service (DoS), che sfrutta abusivamente server DNS accessibili al pubblico e li utilizza come amplifier (amplificatore).
File binario	Un file binario è un file che diversamente dai file di testo contiene anche caratteri non alfabetici. Ci può quindi essere qualsiasi valore di byte.
General Packet Radio Service (GPRS)	In italiano «servizio generale radio a pacchetti»; servizio utilizzato nelle reti GSM (telefonia mobile) basato su pacchetti per la trasmissione dei dati.
Hidden Text	Testo nascosto sui siti Web che esiste di fatto ma non è leggibile per l'uomo. Ad esempio quando il colore del testo è trasparente.
Hypertext	Un hypertext è un testo che per il tramite di una struttura di tipo rete degli oggetti collega informazioni a mezzo hyperlink tra nodi hypertext. L'hypertext è scritto in linguaggio markup che oltre alle indicazioni di formato contiene anche comandi per gli hyperlink. Il più conosciuto è l'Hypertext Markup Language (HTML) per i documenti Internet.
Infezione da «drive-by-download»	Infezione del computer mediante malware unicamente attraverso la consultazione di una pagina web. Le pagine web interessate contengono nella maggior parte dei casi offerte serie, ma sono state dapprima compresse allo scopo di diffondere il malware. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
Jailbreak	Con il termine jailbreaking (dall'inglese evasione dalla prigione) si intende il superamento delle limitazioni di uso dei prodotti Apple per il tramite di un apposito software.
Keyword Stuffing	Il keyword stuffing è considerato un metodo non etico di ottimizzazione dei motori di ricerca. Si tenta di ingannare il motore di ricerca per il tramite di parole chiave (keywords) superflue e frequentemente ripetute nei meta-tag o nel contenuto del sito Web.
Lacune di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
Linkfarm	È designata linkfarm una collezione di siti Web o di interi domini Web che persegue primariamente lo scopo di collocare il maggior numero possibile di hyperlink a un altro sito Web.
Malware	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus,

	vermi informatici, cavalli di Toia, nonché le Logic Bombs. Vedi anche Malware.
Network-Share	Un network-share o uno svincolo di rete è costituito da un'apparecchiatura o da informazioni su un computer alla quale o alle quali si può accedere a distanza da un altro computer attraverso la rete.
Nickname	Per nickname si intende nell'uso attuale della lingua il nome (generalmente abbreviato) che l'utente di un computer utilizza come pseudonimo nei forum e nelle chat.
OpenSource	L'Open Source è una gamma di licenze di software il cui testo fonte è liberamente accessibile e che per il tramite della licenza ne promuove lo sviluppo ulteriore.
Peer to Peer (P2P)	Peer to Peer Un'architettura di rete nel cui ambito i sistemi partecipanti possono assumere le medesime funzioni (diversamente dalle architetture cliente-server). Il P2P è sovente utilizzato per lo scambio di dati.
Phishing	Nel caso del phishing i truffatori tentano di accedere ai dati confidenziali di ignari utenti di Internet. Si può trattare per esempio di informazioni sui conti di offerenti di aste online (ad es. eBay) o di dati di accesso a servizi bancari via Internet. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro e-mail nei quali l'indirizzo del mittente è falsificato.
Pop-up	Un pop-up è un elemento visuale di un programma per computer. Il suo nome proviene dal fatto che questo elemento «prorompe» (dall'inglese «pop up») ricoprendo altre parti.
Programmable Logic Controller (PLC)	Designazione inglese dei controllori logici programmabili (CLP).
Proof of Concept (PoC)	Proof of Concept Una prova succinta, ma non necessariamente completa, del funzionamento di un'idea o di un metodo. Sovente i codici Exploit sono pubblicati sotto forma di PoC per sottolineare le ripercussioni di una lacuna.
Resolver	I resolver sono moduli software di struttura semplice installati sull'elaboratore di un partecipante al DNS che possono richiamare informazioni dei server dei nomi. Essi costituiscono un'interfaccia tra l'applicazione e il server dei nomi.
Rootkit	Un insieme di programmi e di tecniche che consentono di accedere inosservatamente a un elaboratore e di assumerne il controllo.
Scareware	Software destinato a disorientare e intimorire l'utente. Si tratta di una forma automatizzata di «social engineering». Se la vittima cade nel tranello e si sente minacciata le viene offerta frequentemente l'eliminazione a pagamento di un pericolo inesistente. In altri casi la vittima è indotta dalla convinzione di un avere subito un attacco efficace a effettuare azioni che

	rendono possibile l'attacco vero e proprio.
Secure Sockets Layer (SSL)	Un protocollo di comunicazione sicura in Internet. Attualmente lo SSL viene ad esempio utilizzato in ambito di transazioni finanziarie online.
Smartphones	Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale.
Social Engineering	Gli attacchi di social engineering sfruttano la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni.
Systemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
Three-Way-Handshake	La stretta di mano a tre vie (three-way-handshake) è una procedura per instaurare tra due istanze una trasmissione di dati senza perdite. Sebbene essa sia prevalentemente applicata nella tecnica di rete, la stretta di mano a tre vie non è limitata ad essa.
Toolbar	Barra dei simboli di un programma per computer sulla quale vengono collocati pulsanti di comando, simboli, menu o altri elementi.
Top-Level-Domains	Ogni nome di dominio in Internet consta di una successione di serie di caratteri separate da un punto. La designazione Level-Domain si riferisce all'ultimo nome di questa successione e costituisce il livello più elevato della risoluzione del nome. Se ad esempio il nome completo di dominio di un computer, rispettivamente di un sito Web, è de.example.com, l'elemento a destra (com) rappresenta il Top-Level-Domain di questo nome.
Transmission Control Protocol / Internet Protocol (TCP/IP)	TCP/IP è una famiglia di protocolli di rete che a causa della sua grande importanza per Internet è anche denominata famiglia di protocolli Internet.
Universal Serial Bus (USB)	Bus seriale che (per il tramite di corrispondenti interfacce) consente il raccordo di periferiche come tastiera, mouse, supporti esterni di dati, stampante ecc. Al momento del raccordo o della disgiunzione di un dispositivo USB il computer non deve essere riavviato. I nuovi dispositivi sono per lo più riconosciuti e configurati automaticamente (a dipendenza però del sistema operativo).
USB Memory Stick	Piccoli dispositivi di memoria che possono esser raccordati al computer per il tramite di un'interfaccia USB.
Verme informatico	Diversamente dai virus, i vermi informatici non necessitano di un programma ospite per diffondersi. Essi sfruttano piuttosto le

	lacune di sicurezza o gli errori di configurazione del sistema operativo o delle applicazioni per diffondersi autonomamente da un computer all'altro.
Virus	Un programma informatico capace di autoreplicarsi e provvisto di funzioni nocive, che si aggancia a un programma ospite o a un file ospite per diffondersi.
Web 2.0	Web 2.0 è un nome utilizzato per una serie di elementi interattivi e collaborativi di Internet, specialmente del World Wide Web. Il concetto postula in abbinamento con il numero di versione una nuova generazione di Web e la delimita rispetto a tipi di utilizzazione precedenti.
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.

7 Allegato

7.1 DDoS – Analisi di un fenomeno sempre più frequente

L'attacco Denial-of-Service (DoS) persegue l'obiettivo di rendere inaccessibile ai suoi utenti un determinato servizio o perlomeno di limitarne fortemente la raggiungibilità. Si parla invece di un attacco di Distributed Denial of Service (DDoS), ossia di un DoS «distribuito» quando la vittima è attaccata in maniera coordinata e simultanea da diversi e numerosi sistemi. Per quanto riguarda i sistemi che sferrano l'attacco si tratta nella maggior parte dei casi di computer infettati, organizzati all'interno di una rete bot. Il capitolo 5.2 abborda anche le motivazioni dei DDoS. Il presente capitolo invece intende fornire uno sguardo approfondito sulle tecniche che si celano dietro simili attacchi e sulle risorse che vi sono prevalentemente profuse per mantenere entro determinati limiti i danni provenienti da simili attacchi.

Attacchi DoS – Metodi e modalità di funzionamento

In generale è possibile distinguere due diversi tipi di attacchi DoS. Gli uni perseguono la messa fuori esercizio di un sistema sovraccaricando le risorse di calcolo e di memoria (protocol-based e application-based). Gli altri tentano di saturare la rete con richieste (spazzatura) in modo tale da ostacolare il traffico legittimo di dati (flood-based). Secondo quanto riferisce Arbor Networks nel caso del 45% degli attacchi constatati nel 2009 si tratta di attacchi flood-based e nel caso del 49% di attacchi application-based[68].

Nel caso degli attacchi application-based o protocol-based sono tra l'altro state applicate le seguenti tecniche:

Attacco SYN-Flood
Un attacco SYN-Flood sfrutta l'instaurazione di un collegamento TCP/IP, ossia della cosiddetta *stretta di mano*. Per instaurare un siffatto collegamento – ad esempio per chiamare un sito Web da un server – l'utente invia una richiesta «SYN» al server. Quest'ultimo risponde con una comunicazione «SYN-ACK», alla quale fa normalmente seguito una risposta «ACK» dell'utente. A questo momento il collegamento è instaurato[69]. Entrambe le parti utilizzano pertanto il cosiddetto «three-way handshake» (o «3-step handshake»). Se però il computer di un utente non conclude il «three-way handshake» con un «ACK» il server continua ad aspettare questa risposta, utilizzando in tal modo risorse di memoria. L'attacco DoS avviene quando l'aggressore invia migliaia di «SYN» senza concludere l'instaurazione del collegamento con un «ACK». Il server deve successivamente utilizzare la propria memoria per mantenere tutti i collegamenti. Ciò dura finché la memoria è piena e non è più in grado di accettare nuove richieste – anche legittime.

Inondazione dei processi
Il fatto che un server Web possa essere paralizzato anche con esigue risorse di rete è illustrato dal seguente modo di procedere, che funziona ad esempio sui server Web Apache 1.x e Apache 2.x. A ogni richiesta inviata a un sito Web il server Web avvia un processo che viene nuovamente chiuso quando la richiesta è conclusa, ossia quando è terminato il

[68] «Worldwide Infrastructure Security Report», Arbor Networks 2009, http://www.arbornetworks.com/dmdocuments/ISR2009_EN.pdf (stato: 10 gennaio 2011).

[69] Abbiamo semplificato il sistema di stabilimento di un collegamento. «Computer Network» di Andrw S. Tanenbaum costituisce una lettura raccomandabile e interessante.

caricamento del sito Web. Se si tenta di aprire il maggior numero di collegamenti e di lasciarli aperti il più a lungo possibile, raggiungendo a un certo momento il numero massimo autorizzato di collegamenti paralleli, le nuove richieste non sono più ammesse e il sito non è più raggiungibile[70]. L'attacco è particolarmente interessante perché non esige una grande larghezza di banda. Sulla rete sono poi disponibili programmi, come ad esempio Slowloris, che eseguono questo attacco e sono di uso semplice (anche via Proxy o Tor)[71].

«Ping of Death» e attacchi smurf
Una tecnica conosciuta da lungo tempo è il «Ping of Death» nel cui ambito si invia un pacchetto ping deformato[72]. Nel caso del cosiddetto attacco smurf l'aggressore invia ping (ICMP-Echo-Requests) all'indirizzo broadcast di una rete. Il mittente viene falsificato, mentre l'indirizzo della vittima viene registrato. A seconda della configurazione del router la richiesta è convogliata sulla rete e si costringono tutti i computer collegati a rispondere alla vittima. I router che autorizzano questo comportamento sono anche denominati smurf amplifier. L'ordine di grandezza di una sola richiesta può essere amplificato a seconda del numero di computer collegati alla pertinente rete.

Application Attack
Un ulteriore tipo di attacco prende di mira le funzioni dei server Web che esigono ampie risorse. Ne è ad esempio il caso delle funzioni di ricerca all'interno di un sito Web o dell'esercizio di un Content Management System (CMS) (come WordPress or Drupal), che creano la pagina all'atto della ricerca (diversamente dalle pagine statiche che sono a disposizione sul server). Un attacco a siffatte pagine è ovviamente molto più efficiente.

Nel caso degli attacchi flood-based gli accessi provengono da diversi computer (nella fattispecie si tratta nella maggior parte dei casi di computer infettati, appartenenti a una rete bot. Ulteriori computer vengono utilizzati in maniera completamente consapevole per eseguire l'attacco). In tale ambito si sfrutta con le richieste tutta la larghezza di banda upstream del server affinché esso non possa più inviare la pagina o non possa più fornire il servizio richiesto. L'efficacia di questo genere di attacco dipende dalla larghezza di banda corrispondente del server. In generale si presume che una grande rete bot sia in grado di perpetrare attacchi di maggiori dimensioni. Esistono tuttavia diverse tecniche per potenziare questi attacchi, per poter fare capo a reti bot di piccole e medie dimensioni anche per i grandi attacchi.

Attacchi basati sui DNS
Si può rispondere seguendo tre diverse procedure a una richiesta DNS:

- autoritativa: il server prende il file dal file locale di zona;
- ricorsiva: il server prende il file da un altro server di nomi;
- iterativa: il server risponde rinviando a un altro server di nomi.

Nel caso delle richieste ricorsive il *resolver* invia anche una richiesta al server di nomi che gli è assegnato. Se neanche il server di nomi dispone dell'informazione desiderata nel proprio corpo di dati esso contatta ulteriori server finché riceve una risposta positiva oppure una risposta negativa da un sistema autoritativo. Il server di nomi dovrebbe di per sé accettare unicamente richieste provenienti da clienti locali o autorizzati. In realtà numerosi server DNS

[70] http://www.securityfocus.com/archive/1/456339/30/0/threaded (stato: 10 gennaio 2011).

[71] http://vimeo.com/7618090 (stato: 10 gennaio 2011).

[72] http://insecure.org/sploits/ping-o-death.html (stato: 10 gennaio 2011).

accettano richieste da qualsiasi fonte. In simili casi essi sono designati come open resolver[73]. In caso di attacco si possono inviare richieste unicamente a siffatti open resolver, presso i quali l'indirizzo della vittima è indicato come indirizzo di risposta. La vittima viene in seguito sommersa da risposte DNS che non ha richiesto. Un'altra conseguenza ne è il fatto che è unicamente visibile l'indirizzo IP del server di nomi, non però quello dell'aggressore. Questa anonimizzazione dell'attacco rende difficile una difesa efficace. Una tecnica destinata a potenziare questo attacco è l'*amplificazione DNS*. In determinati casi i server di nomi reagiscono con pacchetti estremamente lunghi a brevi pacchetti di richieste. Una richiesta della lunghezza di 60 byte può provocare una risposta di oltre 4000 byte. Il fattore di potenziamento è in questo caso superiore a 65. A ciò si aggiunge un maggiore dispendio di calcolo dovuto alla frammentazione degli IP. L'estensione EDNS dei DNS è responsabile del fatto che questo genere di attacchi sia divenuto praticabile, perché in precedenza la lunghezza massima di un pacchetto DNS era limitata a 512 byte (il che corrisponde a un fattore di potenziamento inferiore a 10). Da un'inchiesta divenuta nel frattempo obsoleta (2005)[74] risulta che il 75% dei DNS esterni hanno reso possibili richieste non autorizzate e quindi attacchi di poisoning[75] o attacchi DoS.

L'utilizzazione delle reti P2P consente di raggiungere un effetto di ampliamento. In simili casi il server della vittima è indicato come unica fonte di un file conosciuto (film, album o altro), in maniera tale che gli utenti della rete P2P richiedano il file desiderato a quell'indirizzo IP. Numerosi ricercatori si occupano di questa tematica[76].

Si è pure osservato un crescente incremento di efficienza degli attacchi eseguiti per il tramite di reti bot. A titolo di esempio gli aggressori non utilizzano simultaneamente tutti i computer di una rete bot. Le ripercussioni sono maggiori e perdurano più a lungo se si fa capo a macchine a traffico moderato, scelte casualmente, e appartenenti a diversi sottogruppi della rete bot (ripartite su diversi provider e differenti regioni geografiche). Questa circostanza ritarda il processo di filtraggio degli indirizzi IP da parte della vittima.

Attacchi DoS – Contromisure

Il CERT del Governo dei Paesi Bassi ha recentemente pubblicato un documento che elenca una serie di misure utili per proteggersi dagli attacchi DoS[77]. Il primo punto non concerne gli aspetti tecnici, bensì gli aspetti organizzativi della *comunicazione d'impresa*:
È incontestabile che ciò che l'impresa comunica e le modalità di tale comunicazione costituiscono un fattore decisivo. Una strategia di comunicazione può fungere da prima misura contro gli attacchi DoS, ma anche costituire il fattore scatenante di un simile attacco. È quanto illustra l'esempio di PostFinance nel dicembre del 2010: il fatto di aver comunicato la volontà di bloccare il conto di Julian Assange ha provocato una reazione da parte del movimento Anonymous e determinato successivamente un attacco DDoS. I rischi e le ripercussioni di una comunicazione a un vasto pubblico devono pertanto essere valutati in precedenza.

---

[73] Una lettura sicuramente interessante è costituita dal testo di Randal Vaughn e Gadi Evron «DNS Amplification Attacks», http://www.isotf.org/news/DNS-Amplification-Attacks.pdf (stato: 10 gennaio 2011).

[74] http://dns.measurement-factory.com/surveys/sum1.html (stato: 10 gennaio 2011).

[75] Cfr. il capitolo 7.3 del rapporto MELANI 2008/2: http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=it (stato: 10 gennaio 2011).

[76] http://www.pank4j.com/research/p2pddos.pdf (stato: 10 gennaio 2011) e http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5254891%2F5273826%2F05273837.pdf%3Farnumber%3D5273837&authDecision=-203 (stato: 10 gennaio 2011).

[77] http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html (stato: 10 gennaio 2011).

Le misure tecniche possono essere applicate all'entrata della rete oppure presso il provider:
Analisi esatta del traffico.
Si tratta di una prima misura per capire quale traffico approda sui server. È quindi anche possibile accertare cosa deve essere filtrato. Fanno tra l'altro parte delle applicazioni di analisi dei dati di netflow più sovente utilizzate i tool Open Source come NFSen[78] e NFDump[79].

Filtraggio dei pacchetti e limite delle richieste:
Individuazione[80] dei pacchetti nocivi e filtraggio affinché il server reagisca unicamente alle richieste autorizzate. Limitazione temporale del numero di richieste per IP per impedire che ogni bot possa generare centinaia di richieste al secondo.

Scrubbing:
Implementazione di un sistema complesso e distribuito di server che sia anche in grado di gestire le punte di traffico. A titolo alternativo si possono parimenti utilizzare servizi CNS (Content Delivery Network) come Akamai[81].

Utilizzazione del Load Balancing e della Cahe:
Utilizzazione di diversi server collegati a più reti (più provider) che si ripartiscono il traffico in entrata. A titolo complementare si può fare capo alla funzione di cache di server reverse-proxy, come ad esempio nginx[82] oooure squid[83].

Utilizzazione del Dynamic Rerouting:
Per il tramite di questo metodo si comunica ai computer aggressori che non esiste alcuna route valida per contattare la macchina della vittima (Null-Route oppure Blackhole-Route).

Approvazione del solo traffico autorizzato dal protocollo:.
Se nel caso delle richieste autorizzate al server Web si tratta di TCP:80 e TCP:443 si può bloccare UDP:80 perché questo protocollo non è utilizzato dal protocollo HTTP.

Chiedere al provider
se mette a disposizione soluzioni come ad esempio IDMS[84] oppure RTBH (Remotely Triggered Black Hole[85]) per difendersi dagli attacchi DoS.

---

78 http://nfsen.sourceforge.net/ (stato: 10 gennaio 2011).

79 http://nfdump.sourceforge.net (stato: 10 gennaio 2011).

80 Nel caso dell'attacco di Anonymous contro diversi obiettivi è stato utilizzato il tool LOIC (Low Orbit Ion Cannon). Questo tool ha inviato la comunicazione «wikileaks.org» come payload dei pacchetti TCP e UDP. È stato così possibile predisporre regole di filtraggio.

81 http://www.akamai.com (stato: 10 gennaio 2011).

82 http://nginx.net/ (stato: 10 gennaio 2011).

83 http://www.squid-cache.org/ (stato: 10 gennaio 2011).

84 http://www.arbornetworks.com/en/docman/the-growing-need-for-intelligent-ddos-mitigation-systems/download.html (stato: 10 gennaio 2011).

85 http://www.google.ch/url?sa=t&source=web&cd=1&sqi=2&ved=0CBcQFjAA&url=http%3A%2F%2Fwww.cisco.com%2Fen%2FUS%2Fprod%2Fcollateral%2Fiosswrel%2Fps6537%2Fps6586%2Fps6642%2Fprod_white_paper0900aecd80313fac.pdf&rct=j&q=remotely%20triggered%20black%20hole&ei=1iMwTZPZO4ztsgbq8P2lCg&usg=AFQjCNEZ-kPQ3RiLBBecuEFuKAQ2fQO4OQ&cad=rja (stato: 10 gennaio 2011).