Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

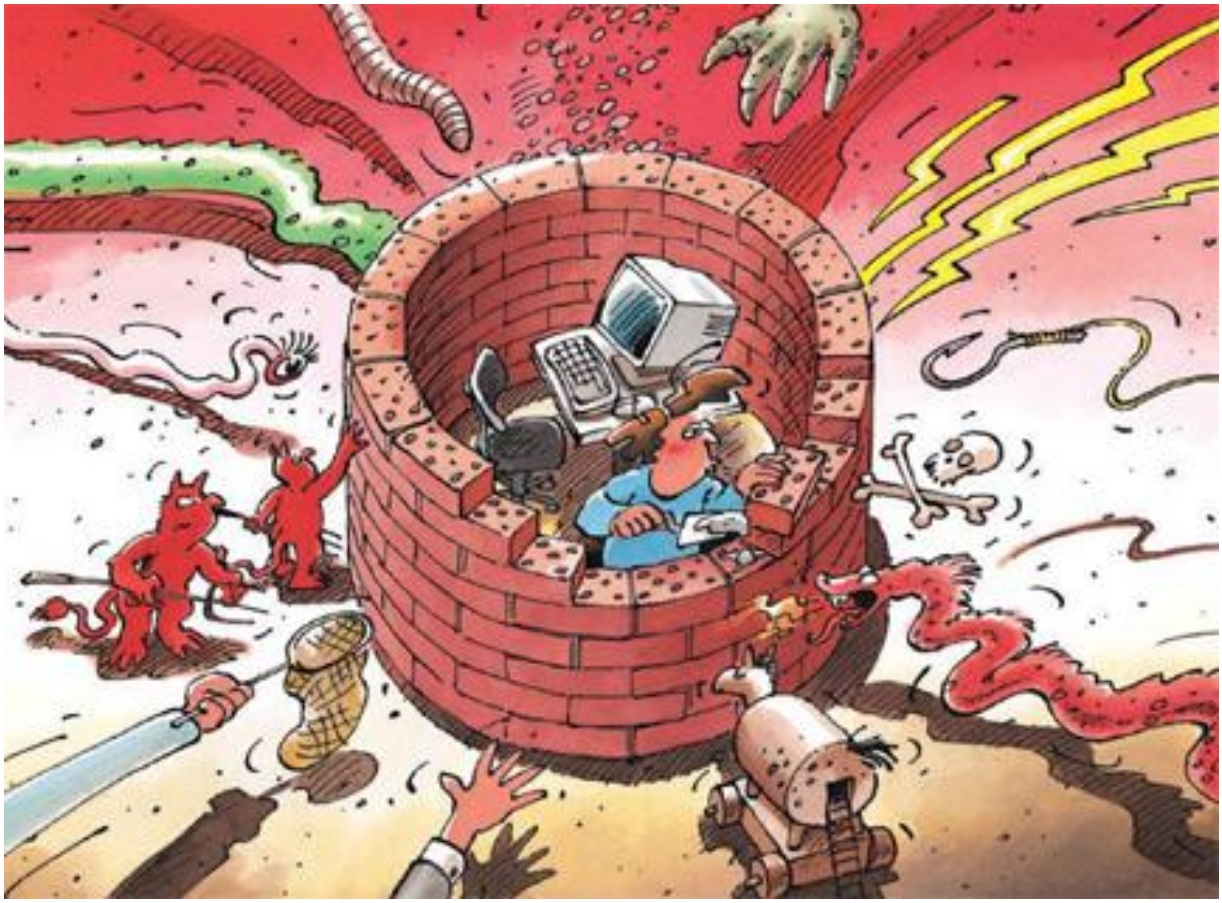
Organo strategia informatica della Confederazione OSIC
Ufficio federale di polizia fedpol

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI

Sicurezza dell'informazione

Situazione in Svizzera e a livello internazionale

Rapporto semestrale 2007/II (luglio – dicembre)



In collaborazione con:

KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

Le service national de coordination de la lutte contre la criminalité sur Internet

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet

The Swiss Coordination Unit for Cybercrime Control

Indice

1 Introduzione 5

2 Situazione attuale, pericoli e rischi 6

2.1 Punto vulnerabile: l'interfaccia uomo / computer 6

2.2 Malware: infezione in più fasi 6

2.3 Reti bot 8

3 Tendenze / Evoluzioni generali 8

3.1 Attacchi DDoS 8

3.2 Riciclaggio di denaro dopo il phishing 9

3.3 I telefoni mobili come bersaglio di attacchi? 10

4 Situazione attuale dell'infrastruttura TIC a livello nazionale 11

4.1 Attacchi 11
Attacco mirato di malware contro computer dell'Amministrazione federale 11
Attacco contro Parlament.ch 12
Attacchi DDoS in Svizzera 12

4.2 Criminalità 13
Infezioni drive-by tramite domini ch 13
Phishing tramite domini ch 13
Accesso non autorizzato a un PABX a Ginevra: utilizzazione fraudolenta di linee telefoniche 14

5 Situazione attuale dell'infrastruttura TIC a livello internazionale 15

5.1 Avarie 15
Avaria di Skype, il popolare software VoIP: fuori esercizio durante oltre 24 ore 15
Gran Bretagna: la perdita di CD-ROM provoca la divulgazione di quasi 25 milioni di serie di dati degne di particolare protezione 15

5.2 Attacchi 17
Gli attacchi mirati di spionaggio rimangono di attualità – Attacchi contro Rolls-Royce e Royal Dutch Shell 17
Malware: furto di dati e attacco mirato contro la clientela delle borse dei posti di lavoro 18
Reti bot: l'esempio di Storm 19
USA: un clic sul mouse potrebbe precipitare una città nel buio (test di penetrazione SCADA presso l'Idaho National Laboratory) 20

5.3 Criminalità 21
Una fonte frequente di criminalità informatica: il Russian Business Network (RBN) 21

5.4 Terrorismo 23
La «Cyber-Jihad» (attacco DDoS) preannunciata per l'11.11.2007 non si è verificata 23
Confermata la presunta relazione tra terrorismo e criminalità su Internet 24

6 Prevenzione: protezione dei PC e dei server di rete 25

6.1 Nell'ottica dell'utente 25

6.2 Nell'ottica dell'esercente di pagine Web 27

7 Attività / Informazioni 29

7.1 Stati 29
Germania: entrata in vigore della norma sulla conservazione dei dati 29
ITU: istituzione di un High Level Expert Group 29
Germania: entrata in vigore della disposizione penale sugli hacker 30
Gran Bretagna: entrata in vigore della Parte III del Regulation of Investigatory Power Act 30

7.2 Economia privata 31
Miglioramento dei meccanismi di sicurezza nell'e-banking 31

8 Basi legali 32
In pianificazione SEPA, uno spazio uniforme di pagamento euro 32

9 Glossario 33

10 Allegato 37

10.1 Reti bot con Fast Flux 37

10.2 Protezione tecnica dei PC 41

Fulcri dell'edizione 2007/II

- **Punto vulnerabile: interfaccia uomo / computer**
  Nel settore della sicurezza dell'informazione e della criminalità su Internet l'importanza dell'interfaccia uomo / computer occupa sempre più una posizione di primo piano. Se è vero che le misure tecniche costituiscono una protezione di base contro gli attacchi, esse bastano però sempre meno da sole.
  ► Situazione attuale: capitolo 2.1
  ► Incidenti in Svizzera: capitolo 4.1
  ► Incidenti a livello internazionale: capitolo 5.2

- **Spionaggio e furti di dati**
  Sussiste la minaccia costituita dallo spionaggio mirato sia contro i sistemi governativi sia contro le imprese private. Anche in questo ambito assume rilievo l'interfaccia uomo / computer, perché il *social engineering* e le ricerche preliminari a un attacco svolgono un ruolo sempre più importante. Questi modi di procedere consentono di perpetrare numerosi attacchi mirati che ne rendono difficile l'individuazione anche da parte di persone attente. L'istruzione e la sensibilizzazione dei collaboratori assumono sempre maggiore importanza, come pure chiare direttive sulla manipolazione, la conservazione e la disponibilità delle informazioni.
  ► Incidenti in Svizzera: capitolo 4.1
  ► Incidenti a livello internazionale: capitolo 5.2

- **Reti bote attacchi DDoS**
  Le *reti bot* rimangono la principale minaccia su Internet. I computer controllati a distanza possono tra l'altro essere sfruttati abusivamente per i seguenti obiettivi: invio di *spam*, hosting illegale, procacciamento di informazioni e *attacchi DDoS*. Il proprietario non è in genere al corrente che il suo PC fa parte di una rete bot. Nell'ultimo semestre si sono registrati anche in Svizzera attacchi DDoS e si deve presumere che il loro numero aumenterà ulteriormente in futuro.
  ► Situazione attuale: capitolo 2.3
  ► Tendenze per il prossimo semestre: capitolo 3.1
  ► Incidenti in Svizzera: capitolo 4.1
  ► Incidenti a livello internazionale: capitolo 5.2
  ► Appendice: capitolo 10.1

- **Malware / Vettori di attacco**
  Gli attacchi che si sono verificati nel corso dell'ultimo semestre hanno evidenziato ancora una volta la tendenza a *malware* più modulare e flessibile. Il malware viene assemblato individualmente e contiene esattamente le funzioni necessarie al singolo attacco. Sussiste la tendenza a diffondere malware tramite infezioni *drive-by*. I punti vulnerabili dei server Web e delle loro applicazioni sono sfruttati per infettare pagine Web insospettate e possibilmente visitate con grande frequenza. Gli attacchi sono sovente perpetrati per il tramite delle *lacune di sicurezza* non colmate delle applicazioni Web.
  ► Situazione attuale: capitolo 2.2
  ► Incidenti in Svizzera: capitolo 4.1
  ► Prevenzione: capitolo 6

1 Introduzione

Il sesto rapporto semestrale (luglio – dicembre 2007) 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 principali attività degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (*termini in corsivo*) sono riunite in un **glossario** alla fine del rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate dal loro colore.

Il **capitolo 2** descrive la situazione attuale, nonché i pericoli e rischi del semestre precedente. Il **capitolo 3** presenta in prospettiva le evoluzioni ipotizzate.

I **capitoli 4 e 5** 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 degli ultimi sei mesi del 2007. Il lettore dispone qui di esempi illustrativi e di informazioni complementari sui capitoli generali due e tre.

Il **capitolo 6** è consacrato di volta in volta a una tematica attuale in ambito di prevenzione, in stretta relazione con i pericoli menzionati nel capitolo 2.

Il **capitolo 7** è focalizzato sulle attività dello Stato e dell'economia privata in ambito di sicurezza dell'informazione in Svizzera e all'estero.

Il **capitolo 8** riassume le modifiche delle basi legali.

Il **capitolo 9** contiene il glossario dei principali concetti utilizzati nel rapporto.

Il **capitolo 10** è un allegato contenente spiegazioni e istruzioni tecniche estese su tematiche scelte del rapporto semestrale.

2 Situazione attuale, pericoli e rischi

2.1 Punto vulnerabile: l'interfaccia uomo / computer

In ambito di sicurezza dell'informazione e di criminalità su Internet l'importanza dell'interfaccia uomo / computer occupa sempre più una posizione di primo piano. Se è vero che le misure tecniche costituiscono una protezione di base essenziale contro gli attacchi (cfr. capitolo 6) è anche vero che esse bastano sempre meno. Per proteggersi con successo contro gli attacchi la prudenza dell'utente del computer assume un ruolo di sempre maggiore rilievo perché gli attacchi possono contenere *malware* che gli attuali comuni programmi antivirus non individuano al momento dell'attacco. Simultaneamente ricerche preliminari sempre più dettagliate e metodi sofisticati di *social engineering* consentono attacchi estremamente mirati, difficile da individuare anche da parte di una persona attenta.

Ogni computer è interessante per gli aggressori, forse anche se il suo proprietario non lo supporrebbe. Sono da un canto interessanti i dati e più precisamente quelli con i quali si può fare denaro. Rientrano in questo ambito le informazioni personali, come carte di credito, dati fiscali e di e-banking, chiavi di licenza di software e simili. D'altro canto possono anche essere derubate le prestazioni del computer e la larghezza di banda: i computer dai quali non possono essere defraudati dati preziosi possono comunque essere integrati in una *rete bot* e ad esempio sfruttati abusivamente per l'invio di *spam* o per perpetrare *attacchi DDoS* (cfr. capitolo 3.1).

Oltre che a raffinatezze tecniche, i malware, come ad esempio il verme informatico Storm, devono soprattutto la loro diffusione a un social engineering efficiente (cfr. capitolo 5.2). Questo genere di attacchi induce l'utente del computer a installare malware, riuscendo a fargli balenare che si tratta di qualcosa di diverso.

Anche nel caso dei continui attacchi di spionaggio (cfr. capitoli 4.1 und 5.2) l'interfaccia uomo / computer svolge un ruolo importante. A causa delle ricerche dettagliate preliminari gli attacchi sono perpetrati in maniera sempre più mirata perché l'aggressore sa cosa, dove e come carpire. A tale scopo gli aggressori si avvalgono sovente di contenuti e-mail adeguati alla vittima, di un link corrispondente o di un mittente degno di fiducia affinché l'attacco possa essere sferrato in maniera possibilmente insospettabile e non sia individuato come tale. Sovente il malware utilizzato non è riconosciuto dai programmi antivirus correnti. Sia le ricerche mirate, sia il social engineering svolgono un ruolo importante in questo genere di attacchi.

Le misure tecniche da sole offrono sempre meno protezione contro questi attacchi. Ne acquistano pertanto maggiore rilievo l'istruzione di ogni singolo utente di computer, specialmente dei collaboratori sul posto di lavoro, come pure chiare direttive sulla manipolazione di documenti e file. I computer sono oggetto di attacchi per derubare dati personali, praticare lo spionaggio, diffondere malware ed effettuare attacchi DDoS. I futuri attacchi si avvarranno sempre più del social engineering e, nel caso degli attacchi mirati, di una migliore ricerca delle loro vittime.

2.2 Malware: infezione in più fasi

Gli attacchi registrati nell'ultimo semestre hanno evidenziato ancora una volta la tendenza all'utilizzazione di *malware* maggiormente modulare e flessibile. Il malware viene assemblato

individualmente e contiene esattamente le funzioni necessarie al singolo attacco. I *cavalli di Troia*[1] in ambito di e-banking apparsi in Svizzera, ma anche gli attacchi di malware contro l'Amministrazione federale descritti nel capitolo 4.1, lo mostrano chiaramente.

Il malware moderno infetta in genere il computer in più fasi. Si utilizzano elementi di malware flessibili, che garantiscono una manipolazione semplice. Per diffondere il malware si fa capo a un piccolo programma ausiliario, un cosiddetto *downloader*. Per il tramite di *packer* e *crypter* i downloader possono essere adeguati in modo tale da non essere più individuati dai programmi antivirus. Il downloader prepara successivamente il computer per l'infezione vera e propria, disattivando ad esempio il firewall e il software antivirus. Il malware vero e proprio che viene successivamente scaricato da un server qualunque ha gioco facile.

Persiste la tendenza a diffondere il malware per il tramite di *infezioni drive-by*. Uno studio pubblicato di recente da Google conferma un aumento costante delle pagine Web sfruttate abusivamente per propagare infezioni drive-by.[2] A titolo di esempio il verme informatico Storm (capitolo 5.2), che si diffondeva inizialmente tramite gli allegati alle e-mail, è passato ben presto alla propagazione tramite e-mail contenenti link su pagine appositamente predisposte che sfruttano le *lacune di sicurezza*.

Si sfruttano soprattutto i punti vulnerabili dei server Web e delle loro applicazioni per sfalsare tramite infezioni drive-by pagine Web insospettabili e possibilmente visitate con grande frequenza. Per questo motivo il capitolo 6.2 è espressamente rivolto agli esercenti di pagine Web e illustra le possibilità di opporsi a questa tendenza.

A livello di *client* si sfruttano soprattutto i punti vulnerabili dei browser, degli add-on e delle applicazioni. Praticamente nessun programma è esente da lacune di sicurezza. Questi programmi sono esposti a pericolo non appena comunicano tramite Internet oppure aprono o riproducono file su Internet. Oltre ai browser, ne sono stati tra l'altro toccati nel corso dell'ultimo semestre i plugin di FlashPlayer, Acrobat Reader, Apple's Quicktime Real-Player; ma anche i programmi di Instant Messaging e i programmi antivirus hanno rivelato lacune di sicurezza. È pertanto assolutamente necessario mantenere aggiornati tutti i programmi installati. Il capitolo 6.1 esamina questa problematica e propone inoltre semplici misure tecniche.

I tool professionali e di semplice utilizzazione consentono praticamente a chiunque di assemblare il proprio malware – a condizione di disporre di una certa energia criminale e di essere disposti a pagare il prezzo necessario. La chiave del successo consiste nell'introdurre in maniera efficiente il malware sul computer della vittima. In questo contesto svolgono un ruolo centrale lo sfruttamento della buona fede dell'utente del computer (*social engineering*) e l'aggiramento delle misure di sicurezza del computer. Considerate le innumerevoli varianti di malware e la relativa moltitudine di segnature presso i produttori di software antivirus, il metodo finora principalmente utilizzato, quello dell'individuazione della segnatura, raggiunge i propri limiti. Questa circostanza emerge anche dal calo del tasso di individuazione da parte dei software antivirus.

Si raccomanda agli esercenti di pagine Web di mantenere aggiornate le applicazioni Web e di garantire che anche i provider di hosting effettuino gli aggiornamenti e le misure di sicurezza necessari (capitolo 6.2).

[1] Cfr. per quanto concerne gli attacchi contro servizi finanziari svizzeri il rapporto semestrale MELANI 2007/1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it (stato: 19.02.2008).

[2] http://googleonlinesecurity.blogspot.com/2008/02/all-your-iframe-are-point-to-us.html (stato: 19.02.2008).

2.3 Reti bot

Le *reti bot* permangono la principale minaccia. I computer sono comandati a distanza e integrati furtivamente nella rete per poter essere sfruttati abusivamente per scopi illegali. Il proprietario non sa in genere che il suo computer fa parte di una rete bot. Gli indizi che un computer fa parte di una rete bot – rallentamento del computer o crash frequenti – sono in genere ignorati. Le persone che ne sono toccate non sono quindi consapevoli del fatto che il loro computer è un elemento piccolo ma pur sempre importante di una rete bot, rendendo così possibili numerose attività criminali su Internet. Rientrano tra di esse l'invio di *spam*, l'hosting di contenuti illeciti, il procacciamento di informazioni, la *frode clic*, l'installazione di programmi pubblicitari nonché gli *attacchi DDoS* (cfr. capitolo 3.1). Questi servizi sono offerti sul mercato clandestino e affittati ai criminali. Molti utenti si interessano troppo poco alla sicurezza del loro PC o la sottostimano, negligendo in tal modo le misure di sicurezza e le norme di comportamento.

La rete bot più famigerata del 2007 è stata la rete bot del verme informatico Storm (cfr. capitolo 5.2). Essa non è pilotata da un server centrale di Command and Control, bensì basata su un sistema *Peer to Peer*. Questo sistema e l'utilizzazione di Fast Flux (cfr. allegato 10.1) rendono difficili contromisure corrispondenti.

Gli attacchi DDoS perpetrati con l'ausilio di una rete bot dovrebbero aumentare in futuro (cfr. capitolo 3.1).

La lotta contro le reti bot permane una sfida a causa del *social engineering* efficiente utilizzato nella diffusione del *malware* e dei raffinati metodi tecnici che rendono difficile le contromisure. Sul numero effettivo di bot possono essere fatte soltanto speculazioni.

L'ignoranza di numerosi utenti di Internet per quanto concerne la sicurezza del loro PC e i pericoli su Internet fa sì che i criminali possano sviluppare questo genere di modello di affari. Ogni utente di Internet dovrebbe pertanto informarsi in merito alle misure preventive per un'adeguata protezione di base del proprio computer.[3] Questo in particolare anche perché i computer infettati e integrati in una rete bot alimentano le trame criminali.

3 Tendenze / Evoluzioni generali

3.1 Attacchi DDoS

Come già menzionato nel capitolo precedente, le *reti bot* sono tra l'altro utilizzate per perpetrare *attacchi DDoS*. I primi grandi attacchi conosciuti sono stati gli attacchi DDoS contro le strutture di informazione in Estonia o l'attacco al provider di prestazioni di sicurezza IT CastleCops.[4] Anche in Svizzera sono stati osservati nel corso dell'ultimo semestre numerosi attacchi DDoS, tra l'altro contro Swisscom e sexy-tipp.ch (cfr. capitolo 4.1).

[3] Le misure di protezione e le norme di comportamento sono reperibili in: http://www.melani.admin.ch/themen/00166/index.html?lang=it (stato: 22.02.2008).

[4] Cfr. in merito all'attacco DDoS contro l'Estonia il capitolo 5.1 del rapporto semestrale MELANI 2007/1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it e per quanto concerne

Nel caso degli attacchi DDoS viene però ancora posta in primo piano la sicurezza delle proprie reti bot. Gli attacchi sono pertanto diretti soprattutto contro la propria concorrenza a livello di reti bot. Nel reticolo possono nondimeno trovarsi persone, rispettivamente persone giuridiche, che possono divenire pericolose per la funzionalità della rete. Rientrano ad esempio in questo ambito gli attacchi contro i fornitori di prestazioni di servizi antispam.

Nei prossimi tempi è atteso un incremento degli attacchi DDoS a sfondo politico, religioso e soprattutto finanziario. Il potenziale tecnico necessario è assolutamente disponibile. La gamma di attacchi va dalla perturbazione delle operazioni su Internet di un concorrente fino alla classica estorsione DDoS. Un'ulteriore tendenza degli attacchi DDoS è l'utilizzazione di moltiplicatori. In questo senso non si invia più soltanto un numero eccessivo di richieste a un server Web ma si tenta ad esempio di sfruttare i punti vulnerabili di un server Web per sovraccaricarlo per il tramite di poche ma ben manipolate richieste di ricerca (cfr. capitolo 4.1). Anche gli attacchi ai server root DNS del febbraio 2007 hanno fatto sì che un attacco mirato a un punto vulnerabile ne incrementasse il risultato.[5]

3.2 Riciclaggio di denaro dopo il phishing

Anche nel secondo semestre del 2007 si sono verificati attacchi con *malware* diretto contro l'e-banking. La strettoia nel caso di questi attacchi permane il trasferimento di denaro all'estero. Il metodo classico è quello del trasferimento all'estero tramite Western Union, avvalendosi di cosiddetti agenti finanziari. Ogni agente finanziario può nondimeno essere utilizzato una sola volta perché successivamente la sua identità è nota alla banca, rispettivamente all'autorità del perseguimento penale, e possono pertanto essere adottate contromisure corrispondenti. Nel contesto di un'accresciuta sensibilità da parte della popolazione diventa sempre più difficile per l'aggressore reclutare agenti finanziari. È quanto emerge anche dalle pagine di reclutamento di agenti finanziari annunciate a MELANI. Se nell'estate del 2007 venivano ancora annunciati quasi quotidianamente e-mail e pagine di agenti finanziari, tali annunci sono sensibilmente diminuiti nell'inverno del medesimo anno.

Gli aggressori reagiscono in parte tramite una procedura più accurata nel reclutamento degli agenti finanziari (cfr. capitolo 5.2) e in parte spostandosi su altri Paesi. Comunque anche numerosi altri Paesi europei tengono il passo per quanto concerne la sensibilizzazione e il perseguimento penale. Un'ulteriore evoluzione potrebbe comunque risultare dallo spazio uniforme di pagamenti euro SEPA (Single Europe Payments Area; cfr. capitolo 8), grazie al quale i pagamenti transfrontalieri in euro dovrebbero essere strutturati in maniera più rapida e miglior mercato. A contare dal 2012 in particolare i pagamenti transfrontalieri dovranno essere disbrigati in maniera altrettanto rapida di quelli nazionali. Ciò potrebbe dare l'avvio a un nuovo mercato degli agenti finanziari perché nella zona euro si situano anche Paesi dove si presume la presenza di autori potenziali di reati in materia di e-banking.

Chi ricicla denaro è costretto a strutturare in maniera più efficiente la ricerca di cosiddetti «money mules» e a fare apparire più credibili le proprie offerte. È quanto emerge dall'attacco mirato alla clientela delle borse dei posti di lavoro illustrato al capitolo 5.2. MELANI si aspetta inoltre nuovi metodi, ancor più difficilmente riconoscibili del riciclaggio vero e proprio di dena-

---

l'attacco a CastleCops: http://www.networkworld.com/news/2007/091207-online-thugs-assault-security-help.html (stato: 15.02.2008).

[5] Cfr. in merito agli attacchi contro i server root DNS anche il capitolo 5.1 del rapporto semestrale MELANI 2007/1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it (stato: 15.02.2008).

ro. Una variante già nota è il pagamento diretto di automobili e di camere d'albergo con denaro proveniente dal *phishing*. Ad avvenuto storno il denaro deve essere nuovamente trasferito al destinatario fittizio tramite Western Union. MELANI ha già rinviato in passato a questa variante di riciclaggio di denaro.[6] Un ulteriore esempio è la costituzione di organizzazioni fittizie di donazione che ricercano persone di buona fede come «amministratori delle donazioni» per poi trasferire i fondi a presunti progetti di aiuto nell'Europa orientale.

3.3 I telefoni mobili come bersaglio di attacchi?

Il telefono mobile è un obiettivo di attacco per i criminali? La diffusione crescente di smartphone e di telefoni mobili con funzionalità affini a quelle dei PC, come pure la memorizzazione di dati sensibili su questi apparecchi rende assolutamente necessario porsi questo quesito. È opportuna una sana dose di scetticismo nei confronti degli interessi (non da ultimo anche commerciali) di singole imprese di sicurezza che sottolineano volentieri questo potenziale di pericolo. Corrisponde nondimeno a un dato di fatto che lo sviluppo e la diffusione incessanti di moderne apparecchiature mobili porta alla creazione di nuove zone d'attacco.

Nel 2004 il verme informatico Cabir, che si propaga attraverso l'interfaccia Bluetooth, ha attirato l'attenzione su di sé come primo virus smartphone. A prescindere dal fatto che era responsabile dello scaricamento delle batterie perché era costantemente alla ricerca di apparecchiature Bluetooth contattabili, Cabir non ha provocato grandi danni. Costituisce invece un problema il fatto che esistano anche parassiti in grado ad esempio di inviare autonomamente costosi MMS, di distruggere i dati o di rendere inutilizzabile un telefono.[7]

Alcuni produttori di programmi antivirus considerano elevato il potenziale di pericolo dei virus per telefoni mobili.[8] I casi di attacchi effettivi di *malware* contro i telefoni mobili rimangono tuttavia relativamente poco numerosi.[9] Un'inchiesta recente, effettuata dallo specialista IT antivirus G Data, argomenta che il pericolo di virus per gli smartphone è esiguo perché gli smartphone non costituiscono un obiettivo redditizio per l'industria del malware. Ne sarebbero motivo la molteplicità dei sistemi operativi, la difficoltà di diffusione del malware e l'assenza di «modelli d'affari di criminalità informatica». Finora il malware era sovente propagato attraverso Bluetooth o tramite MMS. Bluetooth è comunque poco adatto a una diffusione rapida e l'installazione di malware propagato tramite MMS esige un'azione da parte dell'utente. Un pericolo teorico, analogo a quello dei PC, sussiste navigando su pagine Web compromesse da *infezioni drive-by.*[10]

L'attrattiva dei telefoni mobili come obiettivo di attacchi malware o di furto di dati è determinata da almeno due fattori: anzitutto quanto più il telefono mobile adempie 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. Secon-

[6] Cfr. il seguente annuncio di MELANI: http://www.melani.admin.ch/dienstleistungen/archiv/01015/index.html?lang=it (stato: 15.02.2008).
[7] Cfr. per un'analisi dell'evoluzione dei parassiti per la telefonia mobile: http://www.cs.virginia.edu/~robins/Malware_Goes_Mobile.pdf (stato: 13.02.2008).
[8] Cfr. il presente studio pubblicato da McAfee: http://www.mcafee.com/de/about/press/corporate/2007/20070212_174646_p.html (stato: 13.02.2008).
[9] Cfr. http://www.computerworld.ch/aktuell/itsecurity/41264/index.html (stato: 13.02.2008).
[10] Cfr. in merito all'inchiesta di G Data: http://www.gdata.de/unternehmen/DE/articleview/3988/1/160/ (stato: 13.02.2008).

dariamente, in maniera analoga al malware diretto contro i PC, anche nel caso dei telefoni mobili si può presupporre che con l'aumento delle dimensioni del «pubblico mirato» accresca anche l'attrattiva di un attacco. Ci si deve quindi aspettare che con la loro crescente diffusione i moderni telefoni mobili divengano un obiettivo di attacco sempre più attraente. A mente di questa evoluzione i problemi di sicurezza su Internet dovrebbero trasferirsi in futuro sul mondo della telefonia mobile.

4 Situazione attuale dell'infrastruttura TIC a livello nazionale

4.1 Attacchi

Attacco mirato di malware contro computer dell'Amministrazione federale

MELANI ha già rinviato a più riprese al pericolo di spionaggio tramite l'impiego di malware. Nel periodo tra fine novembre e inizio dicembre 2007 è stata la volta dell'Amministrazione federale. Nel quadro di due ondate successive sono state inviate oltre 500 e-mail a collaboratori dell'Amministrazione federale. I messaggi e-mail erano personalizzati, ovvero provvisti dell'appellativo corretto del destinatario. Il mittente falsificato era un servizio federale che faceva riferimento a un presunto concorso fotografico. Per partecipare al concorso l'e-mail invitava a cliccare su un link contenuto nello stesso. Cliccando sul link si apriva una pagina Web del tutto somigliante a quella del predetto ufficio federale; la copia era stata precedentemente collocata su un server di un Internet Service Provider di uno Stato africano. Sotto la rubrica concorso fotografico erano presentate diverse fotografie. Si poteva dare il proprio voto cliccando sulla fotografia di propria scelta. Così facendo si scaricava sul computer un file salvaschermo che conteneva malware. A quell'epoca il malware in questione non era ancora individuato come tale dai programmi antivirus usuali.

Il GovCERT.ch, che assume dal 1 aprile 2008 il ruolo di Computer Emergency Response Teams CERT di MELANI ed è insediato presso l'Organo strategia informatica della Confederazione OSIC, ha esaminato dettagliatamente il malware. Dall'analisi del codice di programma e dalla valutazione del comportamento del malware è emerso che si tratta di un cavallo di Troia che, all'interno di una finestra temporale predefinita, scarica ed esegue programmi di spionaggio da diversi computer su Internet. Al momento dell'elaborazione del presente rapporto semestrale erano ancora in corso ulteriori chiarimenti.

Il genere e le modalità di preparazione dell'attacco, di programmazione del malware e dei tentativi di ostacolarne l'analisi fa concludere che gli autori sono professionisti, che dispongono di risorse finanziarie e tecniche proprie.

All'epoca il malware utilizzato non è stato individuato da nessuno dei software antivirus usuali. Esso si celava nei processi in corso, che in parte almeno sono sempre attivi. Per comunicare con i server su Internet ricorreva inoltre a porte che non venivano bloccate ai passaggi di rete (p. es. da firewall).

È estremamente difficile impedire gli attacchi mirati di spionaggio per il tramite delle sole misure tecniche. Ne deriva una maggiore importanza dell'istruzione e della sensibilizzazione dei collaboratori, nonché di direttive sulla manipolazione, la conservazione e la disponibilità delle informazioni. Nell'esempio del concorso fotografico il software nocivo ha potuto essere installato soltanto perché i collaboratori si sono lasciati indurre a partecipare al concorso (fittizio) e quindi a cliccare sul link. Simili tecniche di social engineering acquisteranno maggiore importanza in futuro proprio perché i sistemi operativi si difendono sempre meglio contro l'installazione automatica di malware.

Attacco contro Parlament.ch

La disponibilità della pagina Internet dei Servizi del Parlamento (parlament.ch) è stata ostacolata dal 14 al 18 dicembre 2007. Alla banca dati del Content Management System sono state presentate a brevi intervalli di tempo richieste di ricerca che forzavano lunghe liste di risultati, circostanza che ha pregiudicato i tempi di risposta del server. Le richieste provenivano da *indirizzi IP* resi anonimi.

Non è chiaro quali siano le motivazioni che si celano dietro queste richieste. La stabilità del sistema poté essere ripristinata dopo che le richieste di ricerca furono limitate.

Questo attacco mostra che non è assolutamente necessaria una grande quantità di richieste per ostacolare la disponibilità di una pagina. In questo caso è bastato manipolare le richieste di ricerca in maniera tale che anche un numero esiguo di esse avrebbe potuto pregiudicare i tempi di risposta del server. Nel caso dei contenuti Web interattivi si accorda pertanto generalmente una grande importanza a una validazione conseguente degli input, ossia alla verifica delle indicazioni immesse.

Attacchi DDoS in Svizzera

Tra il 9 agosto 2007 e il 12 dicembre 2007 il sito Web www.sexy-tipp.ch è stato attaccato per il tramite di una rete bot. Il portale del sito è divenuto nuovamente accessibile a metà dicembre ma il suo forum, che conta oltre 50'000 visitatori ed era nel mirino degli aggressori, non è ancora online sebbene i proprietari abbiano cambiato a più riprese il provider.[11]

Sexy-tipp.ch non è comunque l'unico sito Web per adulti divenuto bersaglio di simili attacchi. Interi siti Web in contatto con le cerchie delle case chiuse zurighesi hanno conosciuto la medesima sorte. Anche il sito Web del Club 79 si è trovato nel mirino di attacchi DDoS. Le sue pagine Web sono state continuamente ostacolate, anche dopo essere state trasferite presso un provider statunitense.[12]

Swisscom è stata parimenti vittima di attacchi DDoS. Il 21 novembre 2007 è stato sferrato un attacco di notevoli dimensioni contro le infrastrutture di IP-Plus.[13] Secondo Christian Neuhaus, il portavoce di Swisscom, quasi 3'550 clienti hanno risentito le ripercussioni di questo

[11] Stato: 15.12.2007

[12] http://www.sonntagszeitung.ch/nachrichten/artikel-detailseiten/?newsid=4168 (stato: 04.02.2008).

[13] http://www.ip-plus.ch (stato: 26.11.2007).

attacco, tra l'altro Bluewin e Tamedia. Durante questo periodo di tempo la versione online del «Tages-Anzeiger» non è stata disponibile.[14]

4.2 Criminalità

Infezioni drive-by tramite domini ch

Nel secondo semestre del 2007 MELANI ha registrato domini Web che presentavano i sintomi di *infezioni drive-by*. Come nel caso dell'Italia, in merito al quale MELANI ha riferito nel suo ultimo rapporto semestrale[15], nel caso della Svizzera si è trattato di pagine Web di assoluta serietà.

A mente di questo tipo di attacchi Honeynet Project ha pubblicato nell'agosto del 2007 uno studio sulla tipologia dei siti Web inquinati.[16] Le 300'000 pagine registrate sono state suddivise in più categorie:

- per tipo di contenuto (per adulti, di musica, di news, con contenuti prodotti dagli utenti come ad esempio forum, blog, warez, ossia siti sui quali sono offerte copie piratate di software);
- server Web vulnerabili, link sponsorizzati sui quale si è diretti tramite ricerche in Google;
- URL sponsorizzati dal motore di ricerca Google (all'accesso di http://www.googspy.com);
- URL del tipo *squatter* (nei 500 siti Web più conosciuti secondo http://alexa.com);
- gli URL diffusi tramite spam (in caso di accesso all'archivio http://untroubled.org/spam)

Dall'analisi dell'Honeynet Project risulta che oltre 306 URL erano infettati, cifra che corrisponde all'1 per cento degli indirizzi esaminati. Nel quasi 60 percento dei casi si tratta di URL con contenuti per adulti. Al secondo posto della graduatoria si situa la categoria degli URL contenuti nelle e-mail di spam. Sebbene vengano tendenzialmente attaccati i siti Web più conosciuti per poter inquinare il maggior numero di PC, l'analisi ha evidenziato che sono soprattutto queste due categorie di URL che espongono gli utenti di Internet ai rischi maggiori.

Phishing tramite domini ch

Il *phishing* classico, ossia il furto di dati di login e di password con l'ausilio di pagine Web falsificate di banche, è sul punto di sparire in Svizzera. In altri Paesi invece, come ad esempio in Inghilterra, il phishing classico permane uno dei metodi preferiti per carpire dati sensi-

[14] http://www.tages-anzeiger.ch, «Erfolgreicher Hacker-Angriff auf Swisscom», (pubblicato il 22.11.2007).
[15] Cfr,. il capitolo 5.1 del rapporto semestrale MELANI 2007/1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it (stato: 04.02.2008).
[16] http://honeynet.org/papers/kye.html (stato 04.02.2008).

bili agli utenti di Internet. Nel secondo semestre del 2007 la Svizzera è incappata nel mirino di organizzazioni criminali che hanno registrato centinaia di nomi di dominio ch sui quali erano stati collocati siti Web di phishing. Si trattava nella fattispecie di attacchi phishing contro istituti finanziari inglesi.

I nomi di dominio che terminano con «ch» sono gestiti dalla fondazione Switch[17]. La procedura di registrazione di Switch consente ai criminali di acquistare URL di cui i compratori possono disporre immediatamente. Non appena il pagamento è stato effettuato (solitamente per il tramite di carte di credito derubate) il nome di dominio è attivato ed è pronto per essere utilizzato. Se il pagamento non è accettato da Switch perché la carta di credito è bloccata o per qualsiasi altro motivo, viene avviata una procedura amministrativa che può durare più mesi.

Per opporsi a questa prassi che provoca danni a Switch (fornitura di una prestazione di servizi non pagata), che mina l'immagine della Svizzera e nuoce in definitiva agli istituti finanziari inglesi, Switch e il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet SCOCI[18] hanno concluso una convenzione di collaborazione. Se si presuppone che un determinato dominio è utilizzato unicamente a scopi criminali, il Servizio di coordinazione ne dà comunicazione a Switch, che provvede al suo bloccaggio. Grazie a questa prassi MELANI e lo SCOCI hanno constatato un netto regresso dei casi di phishing per il tramite di domini svizzeri.

Accesso non autorizzato a un PABX a Ginevra: utilizzazione fraudolenta di linee telefoniche

L'utilizzazione fraudolenta di linee telefoniche non è fenomeno nuovo in Svizzera, ma continua a essere oggetto di perseguimenti penali. Alcuni casi sono già stati menzionati nel corso degli anni precedenti; in questa sede MELANI riferisce di un caso di accesso non autorizzato che si è verificato a Ginevra tra il luglio e il settembre del 2007.

Nella fattispecie i truffatori utilizzavano uno speciale software con il cui ausilio poteva essere riconosciuta la tonalità di una linea telefonica collegata a una segreteria telefonica. Non appena la linea telefonica veniva riconosciuta, il software sondava la centrale telefonica alla ricerca di eventuali lacune di sicurezza. Se una simile lacuna veniva individuata i criminali utilizzavano la rete per farvi passare le loro chiamate. Ciò significa che le telefonate erano convogliate dalla ditta attaccata e che i costi di comunicazione le erano addebitati.

Gli hacker che riescono a utilizzare linee telefoniche di terzi rivendono per il tramite di società telefoniche «low cost» minuti di conversazioni telefoniche. I prezzi di queste conversazioni sono concorrenzialmente bassi. Se il cliente intende ad esempio effettuare una chiamata in Pakistan, i costi del collegamento tra il domicilio del cliente e il PABX intercettato vengono addebitati a questa compagnia telefonica, mentre il saldo dei costi della chiamata è addebitato alla ditta danneggiata.

[17] http://www.switch.ch/it/ (stato: 04.02.2008).

[18] http://www.kobik.ch/index.php?language=it , Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (stato: 04.02.2008).

5 Situazione attuale dell'infrastruttura TIC a livello internazionale

5.1 Avarie

Avaria di Skype, il popolare software VoIP: fuori esercizio durante oltre 24 ore

Il servizio *VoIP* di Skype è stato massicciamente perturbato durante due giorni a partire dal 16 agosto 2007. Il collegamento alla rete Skype non è stato affatto possibile o soltanto sporadicamente. Secondo le indicazioni di Skype il crash dei servizi VoIP è stato determinato dall'aggiornamento Microsoft abituale del 14 agosto 2007[19] e dal successivo reboot. Quest'ultimo avrebbe provocato durante un periodo di tempo limitato una forte reazione di reboot che avrebbe pregiudicato le risorse di rete di Skype. Una lacuna di risorse di rete *P2P* avrebbe poi ampliato il problema. Le routine di autoriparazione, che funzionavano normalmente, si sarebbero bloccate a causa di un errore di software. Nondimeno questo non dovrebbe essere l'unico motivo, perché simili reboot si verificano regolarmente dopo un patchday Microsoft e non hanno finora provocato problemi paragonabili. Per questa ragione il giorno successivo Skype ha indicato a titolo complementare che nell'ambito di questo aggiornamento Microsoft la concomitanza di speciali fattori avrebbe provocato il crash. Non è la procedura di boot dei client, bensì quella dei *Supernodes* e il loro carico specialmente elevato che avrebbe sollecitato eccessivamente il processo di autoriparazione altrimenti funzionante.[20] Non si sa ancora per quale motivo il reboot abbia avuto queste gravi ripercussioni soltanto due giorni dopo l'aggiornamento Microsoft. Skype ha smentito ripetutamente con veemenza le voci secondo le quali il crash sarebbe dovuto a un *attacco DDoS*.

Sebbene nel caso di Skype si tratti di un sistema VoIP proprietario, questa avaria ha acceso il dibattito sull'affidabilità dei servizi VoIP. Se si pensa che il telefono «normale» è probabilmente il più affidabile di tutti i mezzi elettronici di comunicazione, che funziona anche quando manca la corrente, è certo che molte persone non sono abituate a subire un'avaria dei mezzi di comunicazione di più ore, se non addirittura di più giorni. Nel caso dei privati questa situazione è ancora sopportabile posto che non si debbano chiamare i pompieri o un'ambulanza. Nel caso invece delle imprese che contano sul VoIP un simile crash può costituire una minaccia esistenziale. È uno dei motivi per i quali le imprese ritardano il passaggio al VoIP. Un esempio noto è quello dell'UBS che ha deciso di recente di non passare al VoIP.[21] In ambito di passaggio al VoIP la ponderazione accordata alle considerazioni di sicurezza in caso di crash è in genere più elevata di quella applicata al timore di intercettazioni e di manipolazioni.

Gran Bretagna: la perdita di CD-ROM provoca la divulgazione di quasi 25 milioni di serie di dati degne di particolare protezione

Nel secondo semestre del 2007 si sono verificate nello spazio di poche settimane numerose perdite di dati in Gran Bretagna. Le perdite non furono però dovute all'introduzione clande-

[19] http://heartbeat.skype.com/2007/08/what_happened_on_august_16.html (stato: 18.2.2008).
[20] http://heartbeat.skype.com/2007/08/the_microsoft_connection_explained.html (stato: 18.2.2008).
[21] http://www.inside-it.ch/frontend/insideit?_d=_article&news.id=12590 (stato: 18.2.2008).

stina di cavalli di Troia o ad attacchi di hacker ai sistemi, bensì allo smarrimento di supporti di dati (CD, laptop).

2 CD contenenti dati confidenziali e personali di oltre 25 milioni di cittadini britannici sono stati smarriti il 18 ottobre 2007. Si trattava nella fattispecie dei dati di oltre 7.25 milioni di famiglie britanniche al beneficio di assegni per i figli. I dati sono compresivi del nome, dell'indirizzo, della data di nascita, del numero nazionale di assicurazione e in parte di informazioni concernenti le relazioni bancarie.[22] La perdita si è verificata perché i CD sono stati inviati per esame al National Audit Office senza osservare le apposite misure di sicurezza previste in merito. A tale scopo si è fatto capo al sistema postale interno. Entrambi i CD non hanno mai raggiunto il destinatario e non sono più reperibili. Non esistono però indizi che i dati siano finiti in mani sbagliate.

Un ulteriore caso è stato reso noto a metà dicembre 2007. I supporti di dati contenenti il nome, l'indirizzo e il numero di telefono di oltre tre milioni di allievi conducenti non erano più reperibili. L'impresa US che valuta gli esami di guida per conto delle autorità britanniche aveva smarrito i supporti di dati.[23]

Un terzo caso concerne il ministero britannico della sanità: un CD contenente informazioni relative a 160'000 bambini malati è sparito lungo il percorso a una grande clinica londinese. Mancano inoltre all'appello decine di migliaia di serie di dati concernenti i pazienti adulti di un totale di nove settori regionali del sistema sanitario statale. Il governo del primo ministro Gordon Brown è oggetto di pressioni in seguito a queste diverse perdite di dati.

Queste perdite di dati non sono affatto un fenomeno nuovo, ma sembrano ora divenire maggiormente di dominio pubblico. Gli esempi menzionati qui sopra mostrano che devono essere adottate adeguate misure di sicurezza non soltanto per l'invio di informazioni per il tramite di Internet, ma anche per l'invio di supporti fisici di dati come stick USB, CD-ROM, nastri di backup o altri media di memorizzazione. In questo contesto non vanno prese in considerazione unicamente le misure tecniche di sicurezza, ma anche le misure che dovrebbero già essere applicate in ambito di conservazione, di scambio e di disponibilità di informazioni.

I dati sensibili devono sempre essere sufficientemente cifrati in caso di invio. Anche i dati memorizzati sui notebook, smartphone e PDA devono essere cifrati. Sebbene la maggior parte dei ladri di laptop non sia primariamente interessata ai dati bensì alla rivendita del supporto, la memorizzazione non cifrata dei dati sui computer mobili costituisce un comportamento negligente. La vittima in particolare prova una sensazione spiacevole perché non è in grado di valutare quale sarà la sorte dei suoi dati. Nel caso dei dati degni di una particolare protezione la legge sulla protezione dei dati esige che essi siano protetti da adeguate misure tecniche e organizzative contro un'elaborazione non autorizzata.

[22] http://news.bbc.co.uk/2/hi/uk_news/politics/7103828.stm (stato: 21.02.2008).

[23] http://www.spiegel.de/politik/ausland/0,1518,523948,00.html (stato: 21.02.2008).

5.2 Attacchi

Gli attacchi mirati di spionaggio rimangono di attualità – Attacchi contro Rolls-Royce e Royal Dutch Shell

Lo spionaggio mirato, sia nei confronti dei sistemi governativi, sia nei confronti delle imprese private, permane di grande attualità anche nel corso del secondo semestre del 2007, con un'esplosività politica ancora maggiore.[24] Anche in Svizzera si sono registrati attacchi mirati di spionaggio contro l'Amministrazione federale (cfr. capitolo 4.1). Nei Paesi come gli USA, la Germania, la Gran Bretagna, la Francia, ma anche l'India, la Nuova Zelanda e l'Australia questa tematica è sempre più oggetto di dibattiti, non soltanto nei media, ma anche a livello politico e ufficiale. I media e le organizzazioni governative di alcuni di questi Paesi presumono un'implicazione del governo cinese dietro determinati attacchi di spionaggio. Il governo cinese dal canto suo respinge queste accuse e si considera a sua volta vittima dello spionaggio internazionale su Internet.[25]

In questo senso all'inizio del mese di dicembre 2007 il servizio segreto britannico M15 ha avvertito circa 300 imprese britanniche del pericolo di attacchi elettronici presumibilmente sostenuti da organizzazioni governative cinesi.[26] Poco tempo dopo è stato reso noto che le imprese Rolls-Royce e Royal Dutch Shell erano state vittime di spie su Internet, di cui si presumeva che operassero su mandato cinese.[27]

Gli attacchi di spionaggio si fondano su interessi politici, militari ed economici. Gli aggressori possono essere attori sostenuti da uno Stato, ma anche persone singole o organizzate. Nel mirino degli aggressori si trovano i sistemi governativi, in particolare informazioni concernenti la politica di difesa e la politica estera. Anche le imprese private che dispongono di interessanti conoscenze tecniche o strategiche possono trovarsi nel loro mirino, come lo dimostrano gli attacchi nei confronti di Rolls-Royce e di Royal Dutch Shell.

Il riconducimento degli attacchi a un determinato autore è comunque molto difficile perché gli autori utilizzano diversi server e *reti bot* per fare perdere le loro tracce. È quindi ancor più difficile distinguere gli aggressori sostenuti da uno Stato da quelli che operano a partire dalla medesima regione. È importate rammentare che lo spionaggio è un mezzo diffuso a livello mondiale per accedere alle informazioni e che presumibilmente molti Paesi sono attivi in questo settore. In questo senso il servizio segreto britannico M15 stima che almeno 20 servi-

---

[24] Cfr. in merito allo spionaggio con malware mirato nel primo semestre del 2007 il capitolo 2.3 del rapporto semestrale MELANI 2007/1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it (stato: 13.02.2008).

[25] Cfr. per alcune informazioni e prospettive sugli attacchi al governo, in Germania: http://www.spiegel.de/netzwelt/tech/0,1518,501954,00.html; http://www.spiegel.de/netzwelt/web/0,1518,512914,00.html, negli USA: http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html; http://www.uscc.gov/annual_report/2007/report_to_congress.pdf, in Gran Bretagna: http://www.guardian.co.uk/technology/2007/sep/04/news.internet, in Francia: http://www.theregister.co.uk/2007/09/12/french_cyberattacks/, in Cina: http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091200791.html; http://www.spiegel.de/netzwelt/web/0,1518,505462,00.html; per maggiori informazioni sul tema cfr. anche: http://www.securityfocus.com/news/11485 e http://www.mcafee.com/us/local_content/reports/mcafee_criminology_report2007_de.pdf (stato: 13.02.2008).

[26] http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece (stato: 15.02.2008).

[27] http://business.timesonline.co.uk/tol/business/markets/china/article2988228.ece (stato: 15.02.2008).

zi segreti stranieri effettuano attività di spionaggio in Gran Bretagna o contro gli interessi britannici.[28]

Per quanto concerne le modalità degli attacchi di spionaggio il *social engineering* e le ricerche preliminari alla scelta dell'obiettivo svolgono un ruolo sempre maggiore. Ciò consente di definire attacchi particolarmente mirati al punto da renderne difficile l'individuazione anche da parte di persone attente. Si osserva un aumento di questi attacchi particolarmente mirati, precipuamente contro gli impiegati con funzione di quadro delle imprese.[29] Le informazioni necessarie in merito alle persone interessate (indirizzo e-mail, posizione ecc.), di cui i phisher abbisognano per perpetrare questi attacchi mirati, sono sovente liberamente accessibili su Internet.[30]

Malware: furto di dati e attacco mirato contro la clientela delle borse dei posti di lavoro

A metà agosto 2007 è stato reso noto che un *cavallo di Troia* sfruttava i dati di login a Monster.com, presumibilmente derubati ai datori di lavoro, per accedere alle informazioni personali delle persone alla ricerca di lavoro. Grazie all'accesso ai settori riservati agli offerenti di posti di lavoro, il cavallo di Troia poteva accedere ai dati di numerose persone alla ricerca di un lavoro. I dati derubati erano trasmessi a un server che conteneva presumibilmente oltre 1.6 milioni di registrazioni personali. Per il tramite dei dati derubati i ladri intendevano reclutare ausiliari per il riciclaggio di denaro nonché inviare *spam* personalizzati.[31]

Per quanto concerne il riciclaggio di denaro gli autori operavano come segue: per il tramite di e-mail nominative essi ricercavano cosiddetti «Transfer Manager» che mettessero a disposizione il loro conto per dirottare il denaro. Il denaro derubato che si tratta in realtà di «riciclare» è carpito mediante attività di phishing o altri metodi. Il cavallo di Troia è stato utilizzato per l'invio di queste e-mail mirate. Da un canto l'e-mail si rivolgeva direttamente al destinatario, d'altro canto era chiaro che doveva trattarsi di una persona alla ricerca di un lavoro. A ciò si aggiunge il fatto che le e-mail erano redatte in maniera molto professionale e inviate in nome di Monster.com o di Careerbuilder.com.[32]

È stato inoltre individuato un collegamento di questo cavallo di Troia con un parassita utilizzato a scopi di estorsione. A tale scopo venivano inviate e-mail in nome di Monster.com e contenenti i dati personali del destinatario. L'e-mail sollecitava il lettore a scaricare un programma di ricerca. In realtà si trattava di un malware a fini di estorsione, il cosiddetto *Ransomware*, che cifrava i dati sul disco rigido per poi estorcere denaro dall'interessato in vista della loro decodificazione.[33]

---

[28] http://www.mi5.gov.uk/output/Page20.html (stato: 13.02.2008).

[29] Cfr in merito la seguente comunicazione di MessageLabs: http://www.messagelabs.co.uk/resources/news/6592 (stato: 13.02.2008).

[30] Per ulteriori informazioni sugli attacchi mirati diretti contro gli impiegati con funzione di quadro: http://www.networkworld.com/news/2007/111407-whaling.html e http://www.darkreading.com/document.asp?doc_id=134229 (stato: 13.02.2008).

[31] Cfr in merito: http://www.symantec.com/enterprise/security_response/weblog/2007/08/a_monster_trojan.html (stato: 13.02.2008).

[32] Cfr. in merito: http://www.symantec.com/enterprise/security_response/weblog/2007/08/post_3.html (stato: 13.02.2008).

[33] Cfr. in merito: http://www.symantec.com/enterprise/security_response/weblog/2007/08/a_monster_trojan.html; http://www.heise.de/security/news/meldung/94570 e http://www.pcwelt.de/computerundtechnik/sicherheit/virenticker/news/91162/ (stato: 13.02.2008).

Per quanto concerne la complicità in materia di riciclaggio di denaro, il proprio conto non dovrebbe mai essere messo a disposizione per dirottare denaro di terzi. In futuro queste offerte fraudolente – unitamente ad altre varianti sofisticate (cfr. capitolo 3.2) – dovrebbero verificarsi con maggiore frequenza in relazione con dati personali derubati. Ciò consente ai criminali di strutturare in maniera più efficiente la ricerca di cosiddetti «money mules» per il riciclaggio e di fare apparire più credibili le loro offerte.

Per proteggere la propria identità devono essere divulgate su Internet soltanto informazioni personali limitate. I dati sensibili (conti bancari, numero del passaporto ecc.) non dovrebbero mai essere comunicati a datori di lavoro potenziali finché la serietà dell'offerta non possa essere accertata.

Reti bot: l'esempio di Storm

L'anno scorso nessun altro verme informatico ha suscitato altrettanto scalpore nei media come il verme Storm. Esso si illustra non soltanto per la sua tecnica sofisticata, ma anche per il suo social engineering efficiente e molteplice in ambito di propagazione. Nelle e-mail che inviano gli aggressori sfruttano soprattutto la curiosità dei lettori e reagiscono all'attualità, nonché a giorni di festa come Natale, Capodanno, halloween e San Valentino. L'attualità induce numerose persone a cliccare il link dell'e-mail, pur sapendo che si dovrebbe sempre usare prudenza quando si riceve un'e-mail da uno sconosciuto. Non appena ha cliccato sul link, la vittima è dirottata su una pagina Web contenente un link sul *malware*, camuffato ad esempio come gioco o filmato. Simili pagine contengono anche *infezioni drive-by* che sono eseguite in maniera mirata, a prescindere dal browser e dal sistema operativo. In genere tali pagine hanno un aspetto insospettabile e propongono i contenuti che se ne attendono. Ad avvenuta infezione una seconda visita di queste pagine non esegue nuovamente l'infezione drive-by. Questo modo di procedere è destinato a mantenere basso il grado di sfiducia degli utenti, ad esempio dopo un crash del browser, e a propagare all'insaputa il malware. Lievi e continue modifiche del malware ne rendono inoltre difficile l'individuazione da parte dei programmi antivirus. Successivamente il computer viene integrato in una *rete bot*. Tale rete non è però pilotata da un Command and Control Server centrale, bensì basata su un sistema *Peer to Peer*. Il verme informatico contiene anche una funzione *Rootkit*. Il proprietario della rete può successivamente pilotare e utilizzare liberamente il computer per i suoi propri scopi.

Le stime in merito alle dimensioni della rete bot Storm divergono fortemente e variano tra 40'000[34] e parecchi milioni[35]. L'inserimento del verme informatico Storm nel Malicious Software Removal Tool di Microsoft nel settembre del 2007 ha certamente ridotto in misura notevole le dimensioni della rete bot.[36] Al momento il verme informatico Storm appare soprattutto dietro talune ondate di spam e non dietro ad *attacchi DDoS*. Gli attacchi DDoS tramite Storm che sono stati registrati sono soprattutto diretti contro le ditte produttrici di software di sicurezza che tentano di penetrare la struttura di comando e la struttura operativa del verme informatico Storm.[37] Si ritiene che gli esercenti, rispettivamente i proprietari della rete bot, la

[34] http://honeyblog.org/archives/156-Measuring-the-Success-Rate-of-Storm-Worm.html (stato: 11.2.2008).
[35] http://www.informationweek.com/news/showArticle.jhtml?articleID=201500196 (stato: 11.2.2008).
[36] http://arstechnica.com/news.ars/post/20071025-storm-worm-going-out-with-a-bang-mounts-ddos-attacks-against-researchers.html (stato: 11.2.2008).
[37] http://www.tecchannel.de/sicherheit/news/1737125/ (stato: 11.2.2008).

affittino a persone interessate e che non siano opposti a tutti i mandati (quindi anche al DDoS). Esistono ad esempio indizi che la rete è affittata ai phisher.[38] Una descrizione della struttura *P2P* sulla quale poggia il verme informatico Storm figura nell'allegato 10.1. Per quanto concerne la valutazione dell'evoluzione e del pericolo delle reti bot si rinvia al capitolo 2.3.

USA: un clic sul mouse potrebbe precipitare una città nel buio (test di penetrazione SCADA presso l'Idaho National Laboratory)

La sorveglianza, il controllo e il comando degli impianti industriali (chimica, centrali elettriche, industria automobilistica ecc.), dei sistemi di distribuzione di beni di prima necessità (elettricità, acqua, carburanti ecc.) o del settore dei trasporti e del traffico (ferrovie, sistemi di direzione del traffico posta ecc.) sono ormai da tempo impensabili senza l'impiego delle tecnologie dell'informazione e della comunicazione (TIC). Lo sviluppo e l'esercizio di sistemi corrispondenti di sorveglianza, di controllo e di comando (in inglese Supervisory Control and Data Acquisition SCADA) ha una lunga tradizione.

Originariamente i sistemi SCADA avevano poche somiglianze con le TIC usuali; essi erano isolati dalle reti di computer, utilizzavano hardware e software proprietari e stabilivano propri protocolli di comunicazione con l'elaboratore centrale.[39] Nel corso degli ultimi anni l'ampia disponibilità di apparecchiature relativamente a miglior mercato, provviste di interfaccia con il protocollo Internet, ha introdotto grandi cambiamenti in questo settore. I termometri, i manometri, le pompe, gli interruttori e altri cosiddetti elementi sul campo dispongono ora sovente di un indirizzo proprio e utilizzano il protocollo TCP/IP per comunicare con l'elaboratore centrale. Il vantaggio dell'impiego di TIC usuali e a buon mercato è pagato a prezzo dell'esposizione in genere dei sistemi SCADA alle medesime minacce che ci sono note da Internet: il malware (virus, vermi informatici ecc.) e gli aggressori («hacker») fanno il proprio ingresso.

Nel mese di settembre CNN ha riferito di un esperimento condotto dall'Idaho National Laboratory del Dipartimento US dell'energia.[40] L'esperimento ha mostrato come un attacco, pilotato da un computer, a un sistema di controllo potesse provocare la distruzione di un generatore di corrente. In un video era possibile vedere come il generatore iniziava a vibrare e a fumare prima di arrestarsi definitivamente. Hanno poi fatto il giro titoli a caratteri cubitali come «un clic sul mouse può precipitare una città nel buio».

L'esperimento dell'Idaho National Laboratory va inteso come studio di fattibilità. Diverse circostanze, come il genere e il tipo dei relais utilizzati, la disposizione degli interruttori, le misure di sicurezza IT ecc. rendono attualmente molto probabili simili attacchi a fornitori di energia in Europa. Si deve comunque essere consapevoli del fatto che il passaggio ai relais numerici progredisce ulteriormente e che la pressione economica farà sì che non soltanto singoli relais ma viepiù intere sottostazioni saranno telecomandate e esercitate senza personale. La medesima tecnologia usuale di rete semplifica inoltre la realizzazione del desiderio del management di collegare rete commerciale e rete di controllo. I dati e le informazioni sulla produzione possono quindi essere direttamente visualizzati dal management; anzi la produzione può addirittura essere pilotata dal management. In futuro questa mentalità («from

[38] http://blog.trendmicro.com/2008/01/08/ (stato: 11.2.2008).

[39] Per una letteratura più approfondita cfr.:http://www.industrialdefender.com/general_downloads/nist/nist-sp-800-82_draft.pdf (stato: 30.1.2008).

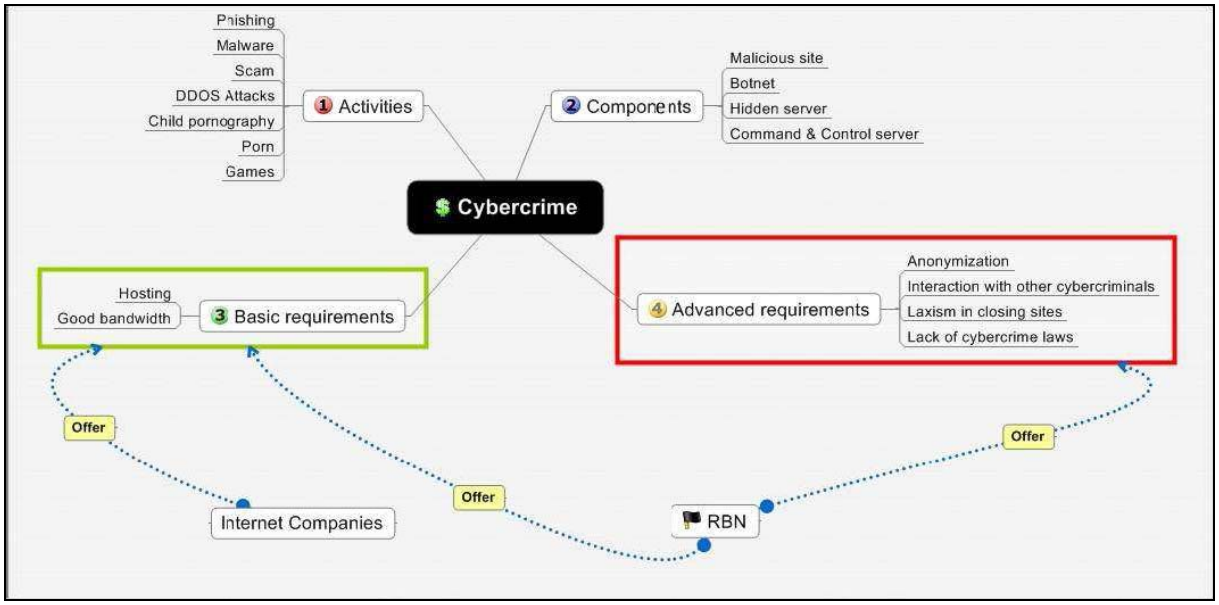
[40] http://edition.cnn.com/2007/US/09/27/power.at.risk/index.html (stato: 30.1.2008).

shop-floor to top-floor») porrà nuove sfide alla sicurezza IT. Si tratterà ad esempio di impedire che la penetrazione di virus nella rete aziendale si estenda alla rete di controllo. Diviene pertanto indispensabile applicare anche ai sistemi di controllo i principi della sicurezza TIC (p. es. «difesa in profondità») oppure standard e direttive corrispondenti. Rientra parimenti in un pacchetto completo di misure lo scambio di esperienze tra esercenti di sistemi di controllo (p. es. in merito ai punti vulnerabili), come pure tra gli esercenti e le autorità, che devono tra l'altro contribuire all'informazione sulla situazione attuale di pericolo. MELANI è in stretto contatto con i distributori svizzeri di energia e partecipa allo scambio internazionale di informazioni, come ad esempio nel quadro dell'European SCADA and Control Systems Information Exchange EuroSCSIE.

5.3 Criminalità

Una fonte frequente di criminalità informatica: il Russian Business Network (RBN)

Il Russian Business Network (RBN) è un Internet Service Provider (ISP) russo. Esso è divenuto tristemente famoso perché è il provider preferito dalla criminalità informatica. Per una migliore comprensione delle funzioni del RBN nel mondo della criminalità informatica rinviamo allo schema qui appresso[41]:



RBN offre un'infrastruttura completa per l'accoglienza di attività illegali. Eccone alcuni esempi ai fini di una migliore comprensione:

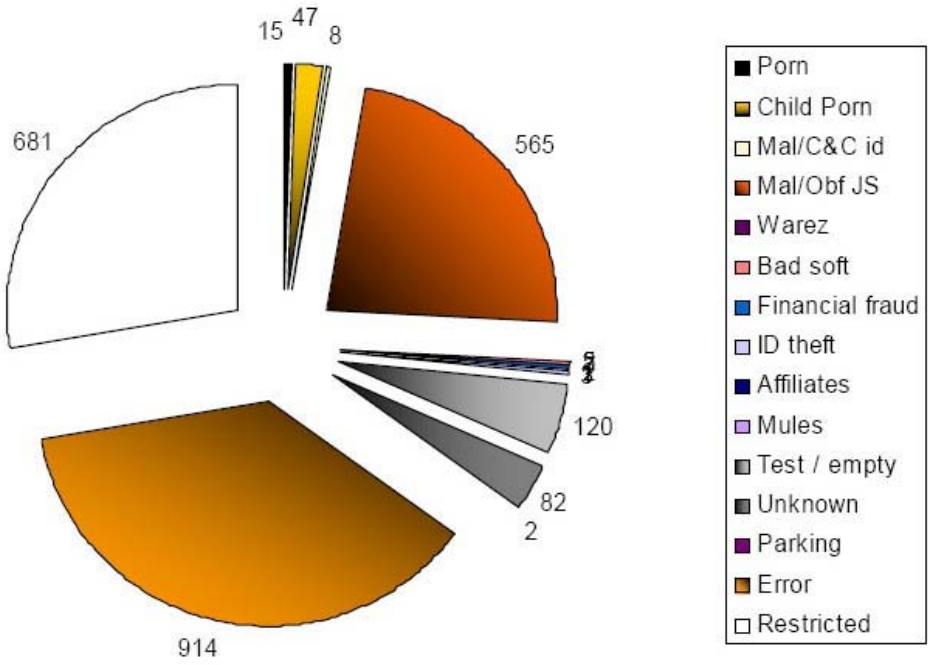
- diffusione di *malware*: tramite gli indirizzi IP di RBN è stata propagata una grande quantità di codici nocivi (CoolWebSearch, VML exploit, Mpack, Torpig/Sinowal, Haxdoor, Pinch, Storm e molti altri);

[41] Russian Business Network study, David Bizeul: http://bizeul.org/files/RBN_study.pdf (stato: 21.02.2008).

- *phishing*: RBN ha ospitato sui suoi server un grande numero di cavalli di Troia, programmati per attaccare i sistemi di e-banking. Numerose tracce di attacchi contro le banche svizzere riconducono alle infrastrutture di RBN;

- altre attività criminali, come ad esempio l'alloggiamento di Rustock, un malware utilizzato per l'invio di «stock pump and dump spam»[42] o sferrare attacchi DDoS contro gli istituti finanziari. RBN è stato indicato anche da Spamhaus.org come provider di una grande quantità di attività illegali.

Nella sua analisi David Bizuel è giunto alla conclusione che il blocco di indirizzi IP in possesso di RBN comprende 406 indirizzi attivati. Su questi 406 server sono alloggiati 2090 nomi di dominio. Le attività di questi siti Web sono illustrate nel grafico qui appresso:



RBN è un sistema molto complesso. Vi sono collegate numerose altre ditte unicamente destinate a meglio camuffare la centrale di comando e soprattutto a rendere possibile a RBN il collegamento con altri provider legali e quindi a sfuggire all'isolamento. Ditte come Nevacom, RusTelekom, AkiMon, Silvernet, Datapoint, Infobox oppure SBT-Telecom sono strettamente collegate a RBN. Se si esaminano i dati nelle cartelle dei provider o in cartelle memorizzate altrove si scopre che le medesime persone sono responsabili di più URL/DNS. È sovente menzionato segnatamente Vladimir Kuznetsov[43], ritenuto uno dei leader del RockPhish Group. Si tratta di un'organizzazione di cui si presume che sia all'origine di numerosi casi di phishing.[44]

---

[42] Per ulteriori informazioni in merito cfr. il rapporto semestrale MELANI 2007/1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it (stato: 21.02.2008).

[43] http://labs.idefense.com/presentations/online/replays/rbn_2007_08_08.php (stato: 15.02.2008).

[44] Per ulteriori informazioni in merito al RockPhish Group, cfr. il rapporto semestrale MELANI 2006/2: http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=it (stato: 15.02.2008).

Nondimeno RBN, divenuto sempre più noto anche all'infuori della stampa specializzata[45] e menzionato con sempre maggiore frequenza nei forum e nei blog[46], ha deciso di ritirarsi dalla ribalta. Uno dei primi cambiamenti che sono stati avvertiti è il fatto che tutti i nomi di dominio sui quali era alloggiato malware sono passati a un provider nella Repubblica Ceca (UPL Telecom): successivamente RBN ha acquistato otto blocchi di indirizzi IP cinesi, che sono stati tuttavia bloccati pochi giorni dopo.[47]

Numerose fonti presumono che RBN sia alla ricerca di una nuova strategia per una migliore sopravvivenza. Lo statuto di provider di grandi dimensioni comporta una visibilità non auspicata. La suddivisione in numerose piccole unità più facilmente occultabili è forse il metodo migliore, anche se vi si devono investire maggiori risorse. Un'ulteriore variante potrebbe consistere nel puntare sulle *reti bot*.[48]

5.4 Terrorismo

La «Cyber-Jihad» (attacco DDoS) preannunciata per l'11.11.2007 non si è verificata

All'inizio di novembre il sito Web israeliano DEBKAfile ha avvertito il pericolo di una presunta «Cyber-Jihad», pianificata per l'11 novembre 2007 da Al-Qaïda.[49] L'attacco non si è comunque verificato. Già nel corso degli anni precedenti erano stati dati avvertimenti del presunto pericolo imminente di attacchi terroristici al Web, che non si sono poi avverati.[50] Anche in questo caso la possibilità di un attacco di grandi dimensioni al Web da parte di terroristi, come pure la serietà dell'informazione sono state fin da principio valutate scetticamente dagli esperti.[51]

Conformemente a questo avvertimento le pagine Web occidentali, ebraiche, israeliane, antimusulmane e sciite avrebbero dovuto essere messe fuori servizio quel giorno da un *attacco DDoS*. L'attacco avrebbe dovuto inizialmente essere diretto contro 15 siti Web, per poi essere esteso gradualmente.[52]

Secondo gli esperti un simile attacco potrebbe essere perpetrato per il tramite del software «Electronic Program of Jihad». In questo senso l'attacco non verrebbe perpetrato a partire da una rete bot di computer compromessi, bensì da numerosi singoli utenti che scaricano il software quivi menzionato.[53] Ne risulterebbe quindi una rete bot manuale, il cui successo dipenderebbe dalla coordinazione di un numero elevato di partecipanti.

---

[45] http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html (stato: 15.02.2008).
[46] A titolo di esempio: http://rbnexploit.blogspot.com (stato: 21.02.2008).
[47] http://theregister.co.uk/2007/11/13/rbn_quits_china/ (stato: 15.02.2008).
[48] http://rbnexploit.blogspot.com/2008/01/rbn-out-with-new-and-in-with-old.html (stato: 15.02.2008).
[49] http://www.debka.com/headline.php?hid=4723 (stato: 13.02.2008).
[50] A titolo di esempio a fine 2006 lo statunitense Department of Homeland Security (DHS) ha avvertito il mondo finanziario della possibilità di un attacco di Al-Qaïda al sistemi di banking. L'attacco non si è verificato.
[51] Cfr. in merito ad esempio http://dshield.org/diary.html?storyid=3615 (stato: 13.02.2008).
[52] http://www.debka.com/headline.php?hid=4723 (stato: 13.02.2008).
[53] Per informazioni sul software: http://www.darkreading.com/document.asp?doc_id=128281; http://www.theregister.co.uk/2007/11/08/electronic_program_of_jihad_discovered/ e http://www.networkworld.com/news/2007/103107-report-cyber-jihad-set-for.html?nlhtsec=1029securityalert4&&nladname=110107securityal (stato: 13.02.2008).

Questo esempio illustra ancora una volta che il terrorismo informatico – ossia l'attacco contro Internet o contro le infrastrutture critiche nazionali con risorse della tecnologia dell'informazione – rappresenta tuttora un pericolo ridotto. Sembra in genere che con le loro azioni le organizzazioni terroristiche intendano propagare possibilmente molta paura e terrore, operazioni alle quali meglio si adeguano gli attacchi fisici. D'altra parte i terroristi dipendono soprattutto da Internet, che sfruttano per la propaganda, l'ideologizzazione, la comunicazione, l'informazione e il procacciamento di risorse finanziarie. È d'altronde molto improbabile che i gruppi terroristici dispongono già del know-how necessario a un attacco alle infrastrutture critiche con le risorse della tecnologia dell'informazione. Per quanto concerne gli attacchi a singoli siti Web per motivi ideologici, non si tratta di una novità ed essi hanno inoltre ripercussioni limitate. Gli attacchi DDoS contro l'Estonia dell'inizio del 2007 erano comunque nuovi quanto alle loro dimensioni.[54] Secondo quanto ritiene MELANI è nondimeno improbabile un massiccio attacco DDoS da parte di terroristi, come quello che avrebbe dovuto presuntamente verificarsi. In ambito di sicurezza di Internet e delle infrastrutture che ne dipendono, il pericolo di gran lunga maggiore è quello costituito dalla criminalità generale su Internet. Come illustrato dal capitolo successivo anche le organizzazioni terroristiche sfruttano i metodi della criminalità informatica per procacciarsi risorse finanziarie.

Confermata la presunta relazione tra terrorismo e criminalità su Internet

Nel luglio del 2007 Younis Tsouli, conosciuto come «Irhabi007», è stato condannato in Inghilterra a 10 anni di reclusione per incitamento all'omicidio. Questo caso illustra in quale misura i terroristi sfruttano Internet a scopi di propaganda, di radicalizzazione, di comunicazione e di procacciamento di risorse finanziarie e come anche Internet sia in relazione con il terrorismo del mondo reale. Il caso in questione conferma in particolare la relazione tra terrorismo e criminalità su Internet, ossia il fatto che i terroristi sfruttano Internet per procacciarsi risorse finanziarie.[55]

Grazie ai dati di accesso di carte di credito che si era procurato tramite attacchi *phishing* e la propagazione di cavalli di Troia, Tsouli e i suoi due congiurati si sono procacciati le risorse finanziarie necessarie per reclutare e sostenere jihadisti potenziali. Sul suo computer sono stati rintracciati 37'000 numeri di carte di credito derubate e i relativi dati personali. Questi dati derubati sono tra l'altro stati utilizzati per l'acquisto di beni di equipaggiamento e di materiale (biglietti aerei, handy a prepagamento ecc.), come pure per la registrazione del sito Web. Sul sito Web è stato reperito materiale come ad esempio guide per la fabbricazione di bombe e per lo hacking di computer, nonché video di atti terroristici.[56]

Internet consente alle persone di svolgere un ruolo importante nell'ambito dell'ideologizzazione, del reclutamento, della comunicazione e del finanziamento del terrorismo internazionale, il tutto ben lungi dal terrorismo del mondo reale. Questo caso conferma in particolare

[54] Cfr. in merito all'attacco DDoS contro l'Estonia il capitolo 5.1 del rapporto semestrale MELANI 2007/1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it (stato: 21.02.2008).
[55] Cfr. per ulteriori informazioni in merito a questo caso: http://news.bbc.co.uk/1/hi/uk/6273732.stm; http://www.economist.com/world/displaystory.cfm?story_id=9472498; http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html; http://counterterrorismblog.org/2008/01/credit_cards_and_terrorists.php e http://www.spiegel.de/politik/ausland/0,1518,495468,00.html (stato: 13.02.2008).
[56] Cfr. in merito: http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945_pf.html (stato: 13.02.2008).

che i terroristi sfruttano la criminalità su Internet per procacciarsi risorse finanziarie. Anche i terroristi e non soltanto i singoli criminali e la criminalità organizzata hanno scoperto che la criminalità su Internet è una fonte di denaro.

6 Prevenzione: protezione dei PC e dei server di rete

Sia in ambito privato che nel settore aziendale l'attenzione degli aggressori si focalizza sempre più sull'interfaccia uomo / computer. Sono interessanti tutti i dati con i quali si può fare denaro. È però anche possibile derubare le prestazioni del computer o la larghezza di banda e rivenderle con profitto a *spammer*, *phisher* o autori di attacchi *DDoS*. Ogni singolo PC è quindi interessante per gli aggressori.

Gli ultimi due rapporti semestrali di MELANI hanno incentrato la tematica sul *social engineering* e le *infezioni drive-by*. Il presente capitolo è incentrato sulle misure destinate a sostenere gli utenti in materia di prevenzione. In questo contesto ci rivolgiamo sia ai visitatori di pagine Web (6.1), sia agli amministratori Web (6.2). L'obiettivo è di ridurre con mezzi semplici la probabilità di essere infettati dal malware.

Nel mese di maggio del 2007 4.5 milioni di pagine Web sono state analizzate nel quadro di un progetto dal profilo della presenza di malware; in questa occasione si è constatato che il 10% delle pagine era chiaramente infettato e che altre 700'000 pagine provocano il download di programmi sospetti. È stato altresì constatato che la presenza del malware era accertata anche in settori nei quali gli esercenti di pagine Web non si sentono responsabili, come ad esempio quello degli *inserti pubblicitari.*[57] Il rischio di vedersi scaricare involontariamente malware sulla propria pagina Web non concerne soltanto chi fa l'amministratore privato per hobby. Nel febbraio del 2007 il sito Web della squadra di football americano Miami Dolphins è stato oggetto di hacking poco tempo prima della finale del «Superbowl» e inquinato con un malware che tentava di infettare i computer dei visitatori.[58]

Soprattutto nell'ambito di Euro08 vengono inserite sul Web pagine ufficiali e private che potrebbero facilmente ritrovarsi nel mirino di simili infezioni drive-by.

6.1 Nell'ottica dell'utente

Rischi

Al giorno d'oggi la manipolazione prudente degli e-mail e del software scaricato dovrebbe costituire un'ovvietà. Anche l'aggiornamento automatico del sistema operativo e del browser,

[57] Cfr.: http://www.pcwelt.de/start/software_os/sicherheit/news/80130/ e http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf (stato: 13.02.2008).
[58] Cfr per informazioni in merito: http://blogs.zdnet.com/security/?p=15 e http://www.sophos.com/pressoffice/news/articles/2007/02/superbowl.html (stato: 13.02.2008).

del software antivirus e del firewall fanno parte della protezione di base di ogni computer.[59] Nella scelta del firewall si dovrebbe provvedere affinché esso possa sorvegliare sia il traffico entrante che quello uscente e comunichi se un nuovo programma intende accedere a Internet. Una scelta di simili programmi figura in un elenco di link sulla homepage di MELANI.[60] Nondimeno, pur osservando le norme usuali di comportamento, non si è attualmente al cento percento al riparo dai danni. Ne sono motivo di crescente importanza le *infezioni drive-b*y. Con tale termine si intende un'infezione da *malware* consecutiva alla mera visita di una pagina Web.

Le misure tecniche non consentono di eliminare completamente la probabilità di un'infezione, ma la possono diminuire. Va osservato in generale che questi provvedimenti causano un dispendio e che nella maggior parte dei casi provocano limitazioni alla facilità d'uso. In considerazione dei pericoli esistenti un simile dispendio è comunque sopportabile e richiede sicuramente una minore intensità di lavoro che non l'eliminazione del danno subentrato.

Prevenzione

- **Navigazione tramite un conto limitato o una sandbox**

  Una cattiva abitudine diffusa è l'utilizzazione negligente di conti con diritti di amministratore. Tali diritti sono ad esempio concessi in standard da alcuni sistemi operativi Windows nello stato di fornitura standard. Quando si naviga in Internet l'utilizzazione di conti con diritti limitati può contribuire a una maggiore sicurezza. Questa misura di sicurezza è particolarmente utile nel caso delle *infezioni drive-by* perché l'utente è invitato a immettere la password di amministratore per l'installazione di programmi (indesiderati). La misura in questione è di utilità anche quando si clicca su programmi camuffati come documenti poco appariscenti. La misura è ovviamente inutile se a ogni sollecitazione viene immessa la password di amministratore.

  Il metodo più semplice per proteggersi dalle infezioni drive-by è la creazione di uno speciale conto di lavoro con diritti limitati. Soltanto quando si lavora intenzionalmente al sistema si dovrebbe operare con pieni diritti di amministratore. Un conto con diritti limitati offre anche la possibilità di limitare i diritti nel browser, come illustrato nella sezione seguente. Oltre a ciò esistono programmi e funzionalità che fanno girare il browser in un settore «protetto». Dato che la maggior parte degli utenti utilizza Internet Explorer, questo browser costituisce il principale bersaglio degli autori di malware. Per gli altri browser come Mozilla Firefox o Opera esistono *exploit* meno noti.

- **Navigazione senza ActiveX e Javascript**

  Alcune pagine Web consistono unicamente di documenti di testo e non offrono ulteriori funzioni supplementari, mentre altre pagine Web recano anche contenuti dinamici. Ne sono esempio i testi scorrevoli, i formulari Web per le commesse online, le immagini animate o gli inserti pubblicitari in sovrapposizione. Queste funzioni dinamiche possono essere realizzate con i controlli ActiveX o con JavaScript. La navigazione senza queste funzioni è faticosa, ma procura un notevole vantaggio in termini di sicurezza perché ActiveX assume pur sempre un ruolo di apripista nelle infezioni drive-by. Per questo motivo i parametri di sicurezza in Internet Explorer devono essere regolati sul livello di protezione «alta». Dato

[59] Le norme di comportamento sono disponibili in:
http://www.melani.admin.ch/themen/00166/00172/index.html?lang=it (stato: 14.02.2008).
[60] http://www.melani.admin.ch/dokumentation/00126/index.html?lang=it#sprungmarke2_5 (stato:14.02.2008)

che l'Active Scripting è applicato a molte pagine Web su Internet, alcune di esse non possono essere pienamente regolate sul livello di protezione «alta». Si raccomanda pertanto di inserire taluni siti Web (dei quali vi fidate) nell'elenco dei «siti attendibili». La procedura è descritta nel documento «Parametri di sicurezza per Window XP»[61]. Per quanto concerne Firefox si rinvia al plugin NoScript[62], che vieta in genere JavaScript, ma ne consente l'attivazione nel caso di singole pagine (attendibili). Una descrizione figura nell'allegato 10.2.

- **Aggiornamento di add-on (plugin) e applicazioni**

  Non è unicamente importante mantenere aggiornato il browser e il sistema operativo, lo stesso vale anche per gli add-on e le applicazioni. Infatti le *lacune di sicurezza* delle applicazioni usuali, come Flash-Player, Real Player, WinZip e numerosi altri programmi sono viepiù nel mirino degli aggressori. Occorre pertanto disporre di una visione d'insieme degli add-on e delle applicazioni installati sul computer. I plugin possono ad esempio essere visualizzati nel browser corrispondente tramite la rubrica di menu Strumenti ➔ «Add-On», rispettivamente «gestione degli Add-on». Sia Firefox che Internet Explorer dispongono di una funzione di aggiornamento dei plugin. Purché sia disponibile, si dovrebbe utilizzare una funzione di aggiornamento automatico. Una guida precisa per Internet Explorer figura nell'allegato 10.2. In Windows l'elenco dei software installati è accessibile a partire dalla rubrica di menu Start ➔ Configurazione ➔ Sistema ➔ Software.

  I programmi che sorvegliano lo stato di aggiornamento dei programmi (ad esempio Secunia Software Inspector[63]) possono essere di ausilio per conservare una visione d'insieme dell'attualità dei programmi installati.

6.2 Nell'ottica dell'esercente di pagine Web

Rischi

L'utilizzazione crescente di Internet per lo scambio di informazioni e l'accresciuta disponibilità di programmi di gestione dei siti Web vanno di pari passo con un aumento del numero di persone private che inseriscono su Internet siti Web complessi. Per il tramite di «Web 2.0» o di sistemi di Content Management CMS si dispone di numerose possibilità di creazione gratuita semplice di pagine Web multimediali con contenuti interattivi (blog, forum, Wiki ecc.). I pacchetti di software come Joomla, che rendono possibili queste realizzazioni, sono comunque complessi e poggiano su diverse componenti. Ogni elemento e il sistema operativo sottostante possono presentare lacune di sicurezza che devono essere colmate nella misura del possibile. A queste si aggiungono lacune di sicurezza ignote, i cosiddetti *Zero-Day-Exploits*.

Numerosi utenti non si rendono conto di questa combinazione complessa, ma si rallegrano della possibilità agevolata di integrare funzioni estese nelle pagine Web. Se però la manutenzione dei programmi è cattiva essi possono divenire un bersaglio attraente per chi propaga malware. Molti esercenti di pagine Web non sono informatici professionisti. I siti Web ge-

[61] http://www.melani.admin.ch/dienstleistungen/00133/00157/index.html?lang=it e http://www.melani.admin.ch/dienstleistungen/00132/00149/index.html?lang=it (stato: 14.02.2008)
[62] https://addons.mozilla.org/de/firefox/addon/722 (stato: 14.02.2008).
[63] http://secunia.com/software_inspector/ (stato: 14.02.2008).

stiti da professionisti non sono immuni da simili carenze di manutenzione: in ambito di sicurezza anche i professionisti non sono in parte sufficientemente sensibilizzati.

Un'altra area di attacco è costituita dagli elementi interattivi di utente, come quelli che si riscontrano nei blog o nei Wiki. Nella peggiore delle ipotesi un cattivo controllo dell'immissione dei dati (circostanza che si può senz'altro verificare quando si riprendono i parametri standard) nei software per forum o nei formulari può consentire a un aggressore di accedere al server e/o ai dati. L'accesso integrale consente poi di inserire pagine o elementi inapparischenti di pagine (come la sovrapposizione di inserti pubblicitari menzionata qui sopra) contenenti *infezioni drive-by*.

Tramite la scelta di password di facile risoluzione, l'installazione di *keylogger* o di computer (domestici) infiltrati dagli hacker è parimenti possibile l'accesso alle console di amministratore o alle interfaccia Web.

Prevenzione

Gli esercenti di pagine Web possono proteggere il sito e i visitatori dal malware osservando i seguenti tre principi:

- Gli amministratori di pagine Web dovrebbero prendere nota del software Web utilizzato come pure delle versioni del sistema operativo e delle applicazioni ed esaminarne la configurazione.

- Aggiornamento automatico del sistema operativo del server Web e ricerca regolare di aggiornamenti delle applicazioni. Questi aggiornamenti possono essere in parte automatizzati nei sistemi Windows e Linux. Occorre informarsi regolarmente sulle possibili lacune di sicurezza e sugli aggiornamenti dei programmi utilizzati.

- Scansione occasionale (verifica attiva) del proprio sito Web quanto alla presenza di malware per il tramite di strumenti generali di sicurezza IT, come Nmap, Nessus ecc., in particolare dopo l'integrazione di nuove funzioni.[64] L'esperto di sicurezza IT Niels Provos ha sviluppato un programma SpyBye[65] che consente ai webmaster di effettuare la scansione delle loro pagine quanto alla presenza di malware.

[64] Cfr.: http://nmap.org e http://www.nessus.org/nessus/ (stato: 13.02.2008).

[65] Il programma è descritto nel libro «Virtual Honeypots: From Botnet Tracking to Intrusion Detection» (Provos & Holz, Addison-Wesley 2007) pag. 268 segg. Cfr. anche: http://monkey.org/~provos/spybye/ e http://www.spybye.org (stato: 13.02.2008).

7 Attività / Informazioni

7.1 Stati

Germania: entrata in vigore della norma sulla conservazione dei dati

Dal 1 gennaio 2008 è in vigore in Germania la legge sul nuovo ordinamento della sorveglianza della telecomunicazione.[66] La Germania traspone pertanto nel diritto nazionale la direttiva dell'UE sulla conservazione dei dati.[67] I dati dei collegamenti telefonici e Internet devono essere memorizzati per una durata di sei mesi a prescindere da un sospetto concreto. Ai provider di Internet si applica un periodo transitorio fino al gennaio 2009. La nuova legge è fortemente controversa e un ricorso di diritto costituzionale è stato interposto alla Corte costituzionale federale.[68]

In Svizzera la conservazione dei dati è già stata disciplinata. Conformemente alla legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni gli offerenti di servizi di telecomunicazione devono conservare per una durata di sei mesi determinati dati di collegamento.[69]

ITU: istituzione di un High Level Expert Group

Il 17 maggio 2007 l'Unione internazionale delle telecomunicazioni (ITU) ha pubblicato la sua agenda biennale di Global Cybersecurity. Nell'ambito di questa agenda sono definite imprescindibili una coordinazione transtatale e transettoriale e l'istituzione di standard e leggi internazionali. Questa esigenza è motivata dalla crescente messa in rete e dalla dipendenza della società, dell'industria e degli Stati dalle tecnologie dell'informazione e della comunicazione. Soltanto così sarebbe possibile arginare e combattere con successo le minacce e i punti deboli. L'ITU, con i suoi 191 Stati membri e 700 partner provenienti dai più diversi settori dell'economia privata e dalle organizzazioni non governative, si considera equipaggiato al meglio per portare avanti l'elaborazione di simili concetti integrati e multilaterali. A tale scopo l'attività deve essere incentrata sui seguenti temi: lo sviluppo di condizioni quadro giuridiche e la messa in atto di istituzioni e di standard vincolanti nel settore delle risorse TIC in vista della lotta a una criminalità informatica in crescita.

Su questa base l'ITU ha ora dato vita allo High Level Expert Group (HLEG) che si è riunito per la prima volta il 5 ottobre 2007. Questo gruppo è composto da circa 60 esperti provenienti dall'amministrazione, dall'industria, dalle organizzazioni internazionali e dal settore della ricerca. L'obiettivo del gruppo è di presentare al direttore dell'ITU documenti strategici corri-

---

[66] Cfr. in merito alla legge: http://www.bundesrat.de/cln_051/SharedDocs/Drucksachen/2007/0701-800/798-07,templateId=raw,property=publicationFile.pdf/798-07.pdf (stato: 13.02.2008).
[67] Cfr. in merito alla direttiva dell'UE sulla conservazione dei dati: http://www.bmj.de/files/8bb57015feb3792008793d7535469da9/2552/EU-Richtlinie%20Vorratsdatenspeicherung.pdf (stato: 13.02.2008).
[68] Cfr. in merito al ricorso di diritto costituzionale: http://www.heise.de/newsticker/meldung/100737; http://www.vorratsdatenspeicherung.de/content/view/184/79/; http://www.heise.de/newsticker/meldung/101073 e http://www.heise.de/newsticker/meldung/101159 (stato: 13.02.2008).
[69] LSCPT, RS 780.1: http://www.admin.ch/ch/d/sr/7/780.1.de.pdf (stato: 13.02.2008).

spondenti nei settori misure legali, tecniche e di processo, cooperazione internazionale, creazione di competenze e istituzione di strutture organizzative. I primi disegni di documento sono disponibili dal febbraio del 2008.

Con la pubblicazione della sua Global Cybersecurity Agenda (GCA) nel maggio del 2007, l'ITU ha posto l'asticella molto in alto: entro il 2009 occorre realizzare un approccio giuridico, organizzativo e tecnico mondiale, sorretto dalla maggior parte dei Paesi, affinché le minacce nel campo dei mezzi di comunicazione e di informazione possano segnatamente essere combattute in comune. In tale ambito è compito del HLEG trovare non soltanto nuovi concetti nei settori parziali incentivati, ma anche porli in sintonia con le convenzioni, gli standard e le prescrizioni esistenti. In questo senso ad esempio con gli standard esistenti in ambito di sicurezza TIC o di Cybercrime Convention del Consiglio d'Europa, che prevedono un'armonizzazione a livello internazionale di alcune basi di diritto penale e un'assistenza giudiziaria rapida e abbreviata tra gli Stati firmatari. Per corrispondenza non è nell'intenzione dei singoli Stati inventare nuovamente la ruota, bensì assumere soprattutto un ruolo di coordinamento e sussidiario. La Svizzera è rappresentata in seno al HLEG da membri dell'Ufficio federale delle comunicazioni (UFCOM) e della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI).

La CGA offre inoltre all'ITU la possibilità di assumere uno statuto di condotta nel settore di Internet, segnatamente nell'ambito della tutela dei mezzi di informazione e di comunicazione e di una più efficace collaborazione nella lotta contro le minacce alla società dell'informazione.

Germania: entrata in vigore della disposizione penale sugli hacker

Nel mese di agosto è entrata in vigore in Germania, tramite una novella del codice penale, la cosiddetta disposizione penale sugli hacker. È così punita la preparazione di reati volti a spiare o carpire dati in vista della produzione, del procacciamento, della vendita, della cessione, della diffusione o dell'accessibilità di password, di altri codici di sicurezza per l'accesso ai dati nonché di appositi programmi informatici.[70]

Gli oppositori temono che queste disposizioni criminalizzino anche il software utilizzato dagli specialisti IT per analizzare le lacune di sicurezza. MELANI giudica di massima positivamente la punibilità della diffusione e della produzione di software in un chiaro intento criminale. Il fatto di rendere forfetariamente illegale il software, parimenti utilizzato per valutare primariamente la vulnerabilità e la sicurezza dei sistemi, sarebbe invece problematico. La giurisprudenza a venire illustrerà le modalità di applicazione della legge nella prassi.

Gran Bretagna: entrata in vigore della Parte III del Regulation of Investigatory Power Act

Nel mese di ottobre del 2007 è entrata in vigore in Gran Bretagna la Parte III del Regulation of Investigatory Power Act. Il Regulation of Investigatory Power Act è stato emanato nel 2000 per offrire alle autorità di perseguimento penale ulteriori possibilità di accertamento e di con-

[70] Cfr. paragrafo 202c CP: http://www.gesetze-im-internet.de/stgb/__202c.html e in merito alle disposizioni penali per la lotta contro la criminalità informatica: http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s1786.pdf; per ulteriori informazioni sul tema cfr.: http://www.heise.de/newsticker/meldung/94190 (stato: 13.02.2008).

trollo in un'epoca di progressi della tecnica dell'informazione. La Parte III consente alle autorità di perseguimento penale di estorcere password e chiavi di cifratura con la comminatoria di pene detentive. La legge intende rendere difficile ai criminali e ai terroristi la dissimulazione dei loro dati tramite cifratura.[71]

La censura a questa legge si attacca a più punti. Gli oppositori temono che l'obbligo di pubblicazione delle chiavi possa in particolare cacciare dal Paese imprese del settore finanziario. Infatti l'obbligo di rendere pubbliche le chiavi può pregiudicare la confidenzialità di tutti i dati tutelati con chiavi. Sono inoltre poste in forse l'efficacia e l'attuazione della legge perché le persone sospette potrebbero semplicemente indicare di avere smarrito o dimenticato le chiavi. A ciò si aggiunge il fatto che numerosi prodotti di cifratura operano con cosiddetti *container*. Pertanto anche quando il container più esterno è decodificato è possibile contestare l'esistenza di un container dissimulato interno.[72]

In Svizzera non esistono disposizioni che consentono di estorcere la pubblicazione delle password con la comminatoria di pene detentive pluriennali. Uno dei principi della procedura penale svizzera è che nessuno deve incriminare sé stesso. Questo principio è ancorato anche nel diritto internazionale, tra l'altro nel patto dell'ONU relativo ai diritti civili politici.

7.2 Economia privata

Miglioramento dei meccanismi di sicurezza nell'e-banking

Diversi istituti finanziari stanno attualmente collaudando o introducendo nuovi metodi di autentificazione. Tutti questi metodi si propongono di accrescere la sicurezza, conservando possibilmente la medesima facilità di uso. I metodi più correnti sono la trasmissione dei dati relativi alle transazioni su un secondo canale (telefono mobile) o un browser potenziato, messo ad esempio a disposizione del cliente su uno stick USB. Un ulteriore metodo è costituito dall'autorizzazione della transazione per il tramite del calcolo crittografico del numero di transazione (TAN).[73] Diversamente dall'autorizzazione della transazione con un TAN semplice, in questo caso il TAN è in relazione diretta con la transazione da autorizzare. A titolo di parametro di calcolo sono utilizzati i dati di transazione, come ad esempio il numero di conto del destinatario o l'importo della transazione. Il calcolo è effettuato da un lettore esterno munito di un processore crittografico.

La SmartCard «Internetpassport» sviluppata da una ditta svizzera consente anch'essa il calcolo crittografico dei TAN. Nella fattispecie i dati di transazione utilizzati non devono essere immessi manualmente, ma sono trasferiti sulla carta tramite segnale ottico (via schermo). Il cliente deve successivamente verificare i dati di transazione sul display della carta e riceve un codice da immettere a titolo di conferma.[74]

La transazione da controllare e confermare per il tramite di un secondo canale di autentificazione e l'autorizzazione mediante calcolo crittografico del TAN sono attualmente considerate

[71] RIPA 2000: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; per maggiori informazioni sulla Parte III della legge cfr.: http://security.homeoffice.gov.uk/ripa/encryption/ (stato: 13.02.2008).
[72] Cfr. in merito: http://news.zdnet.co.uk/security/0,1000000189,39269746,00.htm e http://www.heise.de/newsticker/meldung/97050 (stato: 13.02.2008).
[73] http://www.bw-bank.de/privatkunden/1000006911-de.html (stato: 13.02.2008).
[74] http://www.axsionics.ch/tce/frame/main/471.htm (stato: 13.02.2008).

sicure. L'utente ha però tendenza a scordare una manipolazione perché non presta la dovuta attenzione al messaggio affisso sul display. I numeri di destinatario immessi manualmente richiedono un maggiore dispendio, ma mettono anche l'utente al riparo da una sua propria eventuale negligenza.[75]

In Svizzera non sembra delinearsi un metodo uniforme di autentificazione nell'e-banking. Nel nostro Paese dovrebbe però verificarsi una tendenza al passaggio dall'autentificazione della sessione alla firma della transazione.

8 Basi legali

In pianificazione SEPA, uno spazio uniforme di pagamento euro

A livello europeo si pianifica uno spazio uniforme di pagamento euro SEPA (Single Europe Payments Area) grazie al quale il traffico transfrontaliero dei pagamenti in euro dovrebbe essere accelerato e reso miglior mercato. La relativa base legale è costituita dalla Direttiva dell'UE relativa ai servizi di pagamento nel mercato interno PSD (Payment Services Directive), che deve essere trasposta entro il 1 novembre 2009 nelle legislazioni nazionali degli Stati membri. La data di avvio del SEPA è stata il 28 gennaio 2008. Successivamente le procedure SEPA dovrebbero sostituire gradualmente le procedure nazionali per i pagamenti in euro. A partire dal 2012 in particolare le rimesse transfrontaliere dovranno essere disbrigate in maniera altrettanto rapida e buon mercato delle rimesse nazionali. Invece degli attuali tre a cinque giorni feriali, i pagamenti all'estero dovrebbero essere effettuati entro la fine del giorno feriale successivo. Anche la Svizzera partecipa al SEPA, ma non è vincolata dalla Direttiva dell'UE.[76]

Si veda il capitolo 3.2 per una valutazione delle ripercussioni di questo spazio uniforme di pagamento sul reclutamento di «money mules» e quindi sul riciclaggio di denaro.

[75] Attacchi attuali di malware contro i portali di e-banking: Lösungsansätze für sichere Authentifizierung und Zahlungsabwicklung, lavoro di diploma FH Zentralschweiz, T. Holderegger, 2008.

[76] Cfr. in merito alla Direttiva sui servizi di pagamento PSD: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:DE:PDF; per ulteriori informazioni cfr. anche http://www.sic.ch/de/tkicch_home/tkicch_standardization/tkicch_standardization_sepa.htm (stato: 13.02.2008).

9 Glossario

Il presente glossario contiene tutti i termini indicati in *italico*. Un glossario più completo lo si può trovare all'indirizzo:
http://www.melani.admin.ch/glossar/index.html?lang=it.

Attacco DoS/ Attacco DDoS	Attacco Denial-of-Service Halo scopo di rendere irraggiungibile un determinato servizio all'utente o prelomeno di ostacolare notevolmente la raggiungibilità di detto servizio. Attacco Distributed-Denial-of-Service Un *attacco DoS* in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Bulletproof hosting	Approntamento «a prova di bomba» di servizi o di spazio di memoria senza le usuali limitazioni di contenuto. Su questi sistemi sono sovente offerti pornografia (infantile) dura, pagine di phishing e altri contenuti illegali. Gli esercenti proteggono la loro clientela dalla concorrenza e non collaborano con la giustizia. Il «Russian Business Network» (RBN) è conosciuto per simili prestazioni di servizi a prova di bomba.
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.
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.
Client	Programmi o computer che richiamano informazioni in collegamento diretto con un server.
Container	Contenitore (cifratura). Concetto di file che contiene un sistema cifrato di file. Ad avvenuta immissione della password il container appare all'utente con la trasparenza di un drive normale. Il container si richiude non appena l'utente effettua il logout, mentre i dati sono presenti soltanto in forma codificata.
Crypter	Strumento di cifratura, algoritmo di cifratura. (Elemento di un programma che esegue la cifratura).
Downloader	Può provocare un'infezione da programma maligno. In questo caso il downloader scarica i veri e propri virus, cavalli di Troia ecc. e li avvia sul sistema infettato.
DNS	Domain Name System Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo l'utente possono utilizzare nomi (ad es. www.melani.admin.ch).
Codice Exploit	(abbrev.: Exploit) Un programma, uno script o una riga di codice per il tramite dei quali è possibile sfruttare le lacune dei sistemi di

	computer.
Frode clic	Per frode clic si intende un genere di frode su Internet che persegue primariamente la retribuzione degli inserti pubblicitari per numero di clic. I truffatori possono procedere manualmente o con l'ausilio di programmi. In questo caso sono simulati clic pubblicitari per manipolare in maniera mirata i sistemi di conteggio sottostanti.
Indirizzo IP	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
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 e*xploit* che sfruttano le *lacune nel sistema di sicurezza* lasciate scoperte dal visitatore.
Infrastrutture critiche (nazionale)	Infrastruttura o parte dell'economia la cui avaria o il cui danneggiamento ha ripercussioni massicce sulla sicurezza nazionale o sul benessere sociale e/o economico di una nazione. In Svizzera sono definite critiche le seguenti infrastrutture: approvvigionamento energetico e idrico, servizi d'emergenza e di salvataggio, telecomunicazione, trasporti e traffico, banche e assicurazioni, governo e pubbliche amministrazioni. Nell'era dell'informazione il loro funzionamento dipende sempre più dai sistemi di informazione e di comunicazione. Tale sistemi sono detti infrastrutture critiche di informazione.
Inserti pubblicitari (Banner)	Elementi di una pagina che inseriscono una pubblicità. I banner possono fungere da vettori non appariscenti di attacco perché il loro contenuto è raramente controllato dagli amministratori Web.
Keylogger	Apparecchi o programmi intercalati tra il computer e la tastiera per registrare i dati immessi sulla tastiera.
Lacune di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
Malware	Termine composto dalle parole inglesi «Malicious» e "Software". 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*.
Packer	Programma di compressione o algoritmo di compressione di un programma. Ideato in origine per ottimizzare le dimensioni di un programma sul disco rigido. Il malware si avvale sovente di packer a monte per impedire la propria individuazione da parte dei software antivirus e per ostacolare l'analisi del malware (reverse engineering).
Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza.

	Vedi anche Hotfix.
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.
Plugin	Un software di complemento che amplia le funzioni di base di un'applicazione. Esempio: i Plug-In di Acrobat per i browser di Internet consentono la visualizzazione diretta di file PDF.
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.
Ransomware	Malware tramite il quale i proprietari dei computer infettati sono ricattati (ransom: termine inglese per riscatto). Nel caso tipico i dati sono cifrati e nuovamente messi a disposizione dall'aggressore dopo il pagamento del riscatto per la chiave di decodificazione necessaria al loro ripristino.
Relay	Il relay costituisce un sistema che funge da stazione intermedia per la fornitura di un servizio. Nel contesto del malware e dello spam è destinato a occultare il vero mittente e a impedire il bloccaggio. Vanno in particolare menzionati i relay aperti SMPT. Si tratta nella fattispecie di un elaboratore che riceve e-mail da un qualsiasi elaboratore e le trasmette a qualsiasi terzo, sebbene non abbia la competenza di gestire le e-mail dell'uno o dell'altro. Le reti bot sono d'altronde sovente sfruttate abusivamente a scopi di relay. In questo contesto va pure menzionato l'Internet Relay Chat (IRC), sovente sfruttato abusivamente dalle reti bot come interfaccia di comunicazione.
Rete Bot	Un insieme di computer infettati da Malicious *Bot*. Essi possono essere interamente comandati a distanza da un aggressore (il proprietario della rete bot). A seconda delle dimensioni, una rete può constare di poche centinaia fino a milioni di elaboratori infettati.
Rootkit	Un rootkit (inglese: «elemento di amministratore») è una collezione di strumenti che viene installata sul sistema compromesso ad avvera effrazione di un sistema di computer per nascondere la presenza dell'intruso (hacker o *malware*) e occultare processi e file. I rootkit costituiscono importanti componenti del malware, ad esempio per impedire che essi vengano individuati dai programmi antivirus.
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.
Spam	Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di massa, definizione nella quale rientrano anche gli e-

	mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming.
Squatter	Gli squatter sono persone o organizzazioni che registrano domini Internet con leggere modifiche tipografiche nella speranza che gli utenti pervengano a queste pagine Web in seguito a errori di battitura (es. www.melani.admim.ch invece di www.melani.admin.ch). Questo modo di procedere può essere sfruttato per collocare pubblicità su queste pagine Web, ma anche per diffondere malware. La definizione viene altresì applicata a persone che registrano domini attraenti e non utilizzati nella speranza di poterli rivendere successivamente.
Supernodes	Nelle *reti Peer-to-Peer* i supernodes sono responsabili del flusso di dati e dei collegamenti con gli altri utenti e fungono da *relay* e proxy.

10 Allegato

10.1 Reti bot con Fast Flux

Reti bot: sopravvivenza grazie a nuovi sviluppi

Come ogni attività economica, anche le attività illegali su Internet perseguono l'obiettivo fondamentale di garantire la loro propria sopravvivenza. Nel mondo della criminalità informatica occorre nascondersi per sopravvivere; si devono attirare gli investigatori su false piste e fare sparire le proprie tracce. Le reti bot IRC[77] – reti di PC infettate da malware, che ricevono comandi di esecuzione di compiti diversi (invio di spam, attacchi Denial of Service, Bulletproof Hosting ecc.) da server IRC centrali – possiedono un'architettura sensibile. Ciò significa che la rete può essere disattivata se viene scoperto il server IRC centrale.

Per accrescere la resistenza di queste reti sono state sviluppate nuove tecniche: da un canto fanno la loro apparizione sistemi decentrali (serverless) che si fondano sui protocolli Peer-to Peer (medesima evoluzione di altri settori, come ad esempio le borse online di scambio di musica, da Napster a Kademlia). D'altro canto si constata che le reti bot puntano sulle cosiddette reti Fast Flux (Fast Flux service networks). Nel presente allegato esaminiamo in maniera più approfondita queste nuove tendenze, che segnano un'importante evoluzione nel settore della criminalità informatica.

L'ulteriore evoluzione di Command and Control: P2P

Con la denominazione di Command and Control (C2) si intende la centrale di comando di una rete bot. Finora il metodo preferito consisteva nell'utilizzazione dell'Internet Relay Chat come punto nevralgico dell'architettura di sistema (cfr. figura 1). Per garantire una maggiore durata di vita al server IRC e quindi alla rete bot, si applicano diverse tecniche: tra di esse la cifratura delle comunicazioni tra il cliente IRC e il server o il cambiamento frequente del server. Ciò non basta però per garantire la sopravvivenza del server. La criminalità informatica si è sforzata di eliminare i punti vulnerabili; oggigiorno si tratta pertanto di non dipendere più da un server centrale.

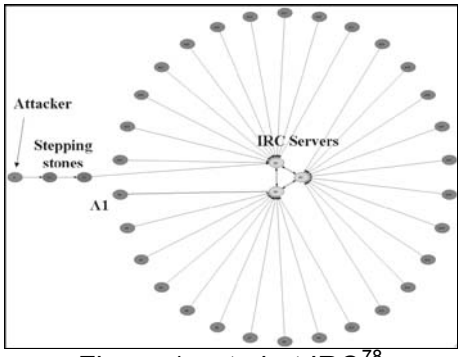


Figura 1: rete bot IRC[78]

[77] Per maggiori informazioni in merito cfr. il rapporto semestrale MELANI 2005/2: http://www.melani.admin.ch/dokumentation/00123/00124/00161/index.html?lang=it (stato: 21.02.2008).

[78] Fonte: «Command and control structures in malware: from handler/agent to P2P», ;LOGIN: Vol. 32, No. 6, http://www.usenix.org (stato: 14.02.2008).

L'impiego di reti P2P decentrali nel settore della borse online di scambio di musica poggia su questa considerazione. Napster (1998) è la prima versione di un distributore di musica tramite un sistema P2P. Spiegato succintamente, il cliente effettuava il login su un server Napster per ottenere l'indirizzo IP degli altri clienti che mettevano a disposizione il brano musicale desiderato. Non appena disponevano di questa informazione i clienti si collegavano direttamente per utilizzare in comune il file sonoro. L'ulteriore sviluppo di questi sistemi è ad esempio sfociato nella creazione di Kademlia[79], una rete utilizzata da noti sistemi P2P come Overnet (Overnet, MIDoneky), Kad (eMule, aMule, MIDonkey), BitTorrent (il BitTorrent originale, ma anche Azureus, BitComet, µTorrent). Espresso in termini semplici Kademlia è una tabella hash distribuita (DHT, Distributed Hash Table) che crea una rete nella quale ogni nodo (Client) è caratterizzato da un numero ID. Ogni nodo dispone delle informazioni necessarie per ottenere un file o un servizio – il server diviene quindi superfluo. I criminali hanno ripreso le tecniche P2P e dato vita a una nuova generazione di reti bot (cfr. figura 2).

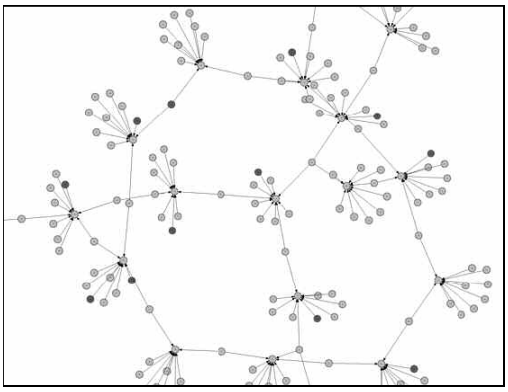


Figura 2: Struttura possibile di una rete bot basata su P2P[80]

Storm, una delle reti bot più conosciute (cfr. anche il capitolo 5.2), utilizza il protocollo Overnet per la distribuzione di informazioni e la fornitura di funzioni eventualmente desiderate ai peer infettati. Secondo un'analisi su Storm[81] ogni nuovo PC infettato contiene una lista di 300 peer sui quali sono indicati la funzione hash, l'indirizzo IP, la porta e il tipo di peer. Sulla scorta di questa lista ogni nuovo membro della rete può effettuare il login e ottenere le informazioni più recenti sullo stato della rete. Peer particolarmente efficienti (dal profilo dell'uptime e della velocità di collegamento) assumono le funzioni di server che alloggiano modelli di e-mail, elenchi di e-mail e server di e-mail (Storm è anzitutto un bot per l'invio di spam). L'informazione non è di per sé inviata dal server; è il membro della rete bot che va a prenderla. Paragonati ad altri sviluppi come ad esempio Fast Flux (cfr. qui appresso), le reti bot P2P non utilizzano praticamente mai servizi DNS. Dato che i DNS non sono utilizzati né per la distribuzione di liste peer, né per l'identificazione di un canale C2, né tantomeno per il login sulla rete, le tecniche di identificazione basate su DNS si rivelano inefficaci contro questo tipo di strutture. Storm utilizza i DNS unicamente per le richieste MX (mail exchange record). Nell'utilizzazione di Storm per attacchi Denial-of-Service si effettuerebbero sicuramente anche richieste DNS.

Non è facile individuare simili bot sulla rete. È un'impresa molto complessa differenziare il traffico P2P legale da quello basato su Storm. Sarebbe molto più semplice sorvegliare le porte TCP/25 dal profilo di un aumento dell'attività. Nella fattispecie si tratta però di una mi-

[79] http://pdos-csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf (stato: 13.02.2008).

[80] Fonte: «Command and control structures in malware: from handler/agent to P2P», Dave Dittrich, Sven Dietrich, LOGIN: Vol. 32, No. 6, http://www.usenix.org (stato: 14.02.2008).

[81] «Analysis of the Storm and Nugache trojans: P2P is here», Sam Stover, Dave Dittrich, John Hernandez, Sven Dietrich, LOGIN: Vol. 32, No. 6, http://usenix.org (stato: 14.02.2008).

sura di reazione pertinente a un determinato PC. D'altra parte malware come Nugache e Storm aggiungono un rootkit che ne ostacola ulteriormente il rintracciamento.

Storm e Nugache sono i primi esempi di applicazione della tecnologia P2P alle reti bot. Attualmente i gruppi criminali tentano di sbarazzarsi dei server centrali – gli elementi più vulnerabili – e di puntare su reti decentrali: non appena avranno raggiunto il loro grado di maturità questi sistemi fungeranno da base alla maggior parte delle attività criminali su Internet.

Fast Flux

Per accrescere la sicurezza di crash delle *reti bot* e per rendere più difficile l'identificazione delle reti e aumentare quindi l'attrattiva delle loro reti per i phisher, gli esercenti di reti bot utilizzano sempre più le tecniche Fast Flux.

Le funzioni Fast Flux[82] delle reti bot consentono di meglio camuffare le tracce e di meglio garantire la stabilità dei sistemi. Come in altri settori dell'economia anche in questo caso i criminali si preoccupano dei costi e della sicurezza. Sicurezza significa protezione nei confronti della concorrenza e delle autorità di perseguimento penale e garanzia di disponibilità.

Alla chiamata di un nome di dominio (www.example.com), ad esempio in un browser, il *sistema DNS* converte questo nome in un *indirizzo IP* (192.168.0.1). Questo indirizzo IP è a sua volta assegnato a un server/computer. Tali tabelle di assegnazione sono memorizzate su un server dei nomi. A causa del grande numero di richieste, nel caso di pagine visitate frequentemente come google.com oppure admin.ch, si assegna un nome di dominio a diversi indirizzi IP per poter ripartire il carico su più elaboratori.

Figura 3: Diversi indirizzi IP sono assegnati a google.com

Le tabelle di assegnazione del server dei nomi indicano parimenti l'intervallo di tempo durante il quale la registrazione è valida. Se l'intervallo di tempo è trascorso, occorre ripetere la risoluzione del nome e si possono caricare nuove tabelle di assegnazione che contengono a loro volta un nuovo indirizzo IP e dirigono pertanto su altri elaboratori. Si parla di Fast Flux se si combina la procedura descritta qui sopra con una durata di vita ridotta.

[82] In questo contesto Flux significa in inglese «essere sul punto di cambiare». La rapidità (Fast Flux) è riferita allo scambio rapido tra i diversi elaboratori

Vantaggi per i criminali

Questa tecnica può essere utilizzata abusivamente dai criminali per i loro scopi. In questo caso i diversi elaboratori sono computer compromessi (*bot*) che recano le pagine Web con contenuti criminali. Poiché queste pagine cambiano continuamente di elaboratore, poco importa ai criminali che l'elaboratore subisca un crash. A che se alcuni computer sono tolti dalla rete o non funzionano, il resto delle rete sussiste. Questa circostanza accresce la stabilità della pagina e ostacola le contromisure.

Un ulteriore vantaggio è l'occultamento dell'indirizzo IP. Gli elaboratori finali cambiano continuamente l'indirizzo IP e sono protetti contro gli inseguimenti. È quanto illustra la figura 4, nel cui contesto lo «zombie home PC» è membro di un'intera rete bot ed è sostituto regolarmente (al ritmo di ogni minuto o di ogni secondo) da un altro membro. Il navigatore in Internet, ad esempio la vittima di una *truffa phishing*, che clicca sul link di un'e-mail non si collega più direttamente a un elaboratore, bensì al membro in costante cambiamento di una rete bot. Non occorre che la pagina di phishing sia direttamente situata su questo elaboratore; basta la trasmissione a un server centrale sul quale sono memorizzati i dati veri e propri e sul quale può anche trovarsi il server di controllo. In questo senso l'elaboratore di controllo o quello di attacco (anche denominati elaboratori «mothership» o elaboratori «Command and Control [C&C)]») sono difficilmente localizzabili. Senza questa tecnica l'indirizzo IP dell'elaboratore aggressore è facilmente visibile.

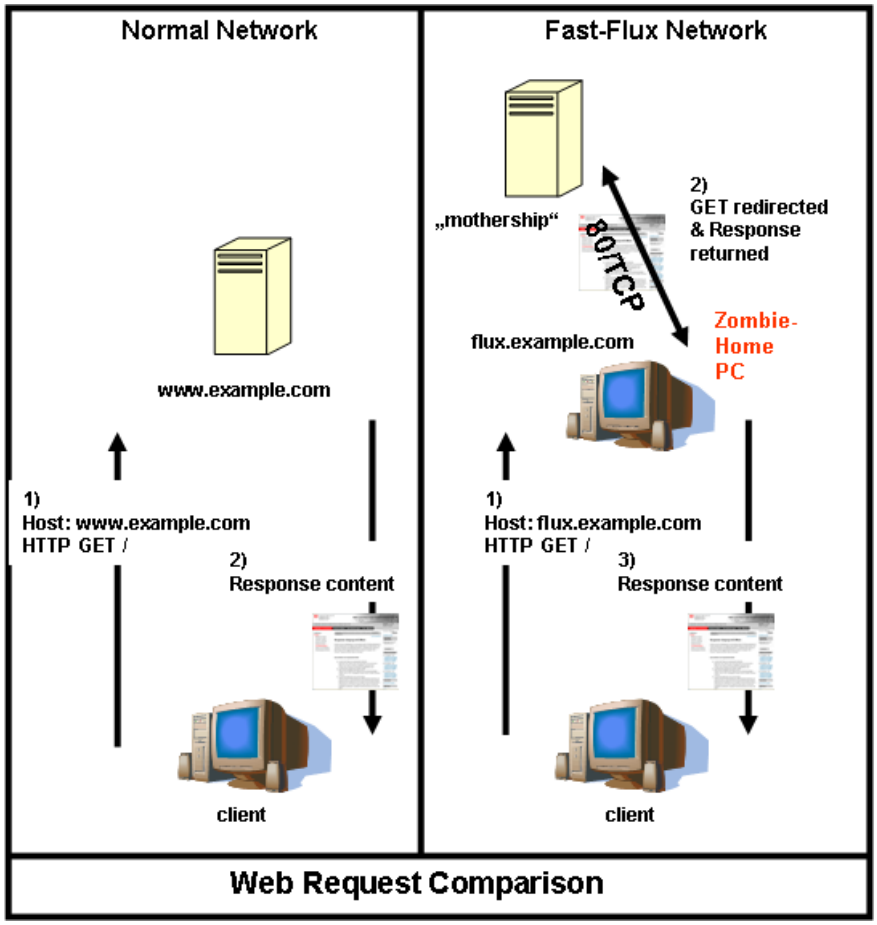


Figura 4: Modalità di funzionamento di una rete normale e di una rete Flux[83]

[83] Presentato in http://www.honeynet.org/papers/ff/index.html (stato 14.02.2008).

Questo occultamento protegge pertanto gli elaboratori di controllo che – diversamente dai membri infettati della rete bot – contengono i codici produttivi di attacco (il malware), i file di configurazione o le pagine Web falsificate.

Dimensioni del problema

In uno studio dell'Honeynet Project[84] i ricercatori hanno osservato durante un periodo di due settimane, nel febbraio del 2007, le attività criminali Fast Flux su un dominio. Questa rete Fast Flux constava di 3'241 indirizzi IP: su questo numero 1'516 elaboratori indicavano di avere competenze a livello di dominio, mentre 2'844 fungevano da elaboratori intermedi interscambiabili. Fino al mese di luglio 2007 i ricercatori hanno osservato un totale di 80'000 indirizzi IP Flux su oltre 1.2 milioni di assegnazioni univoche di IP ai nomi («unique mappings»). Nel contesto dell'aggiornamento successivo i ricercatori hanno rintracciato fino al settembre del 2007 40'000 domini, 150'000 indirizzi IP Flux e 2.5 milioni di simili assegnazioni univoche.[85]

Prevenzione

Gli affari degli esercenti di reti bot possono essere perturbati se gli utenti di Internet hanno «adeguatamente» cura del loro computer domestico e ne mantengono aggiornato lo stato di sicurezza. Infatti, così facendo viene a mancare ai truffatori la «massa» dietro alla quale possono occultarsi.
Per combattere le reti bot Fast Flux sono anche necessari ISP o tenitori di registri per poter utilizzare risorse tecniche contro questi parassiti nocivi. Proposte dettagliate in merito sono contenute nella documentazione Honeynet. Esse comprendono:

- Bloccaggi di accesso contro le infrastrutture dei criminali
- Migliori reazioni da parte dei tenitori di registri alle comunicazioni concernenti domini fraudolenti e nuove registrazioni
- Osservazione e collezione («harvesting», raccolta) di serie di dati DNS
- Liste nere basate sui *DNS* ed eventuali modifiche dei router per impedire il percorso agli elaboratori di management dei criminali

10.2 Protezione tecnica dei PC

Gestione degli add-on

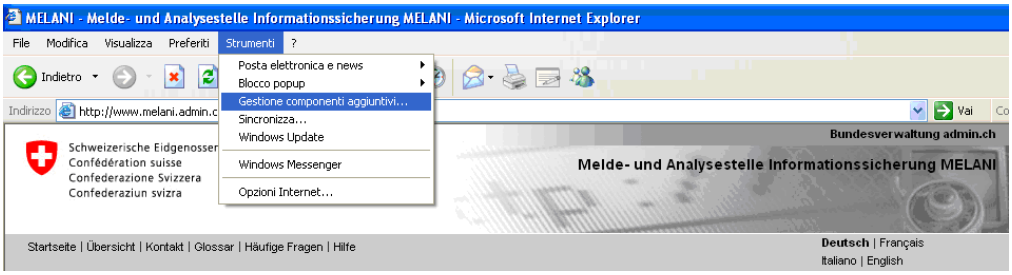
Non è unicamente importante mantenere aggiornati il browser e il sistema operativo: lo stesso vale anche per i plugin e le applicazioni. È importante avere una visione d'insieme degli add-on e delle applicazioni installati sul computer. In questa sede si intende spiegare come

[84] Presentato in http://www.honeynet.org/papers/ff/index.html (stato 14.02.2008).
[85] Per quanto concerne l'aggiornamento cfr. la pagina qui sopra dell'Honeynet Project, «Fast Flux PowerPoint Presentation» (stato 14.02.2008).

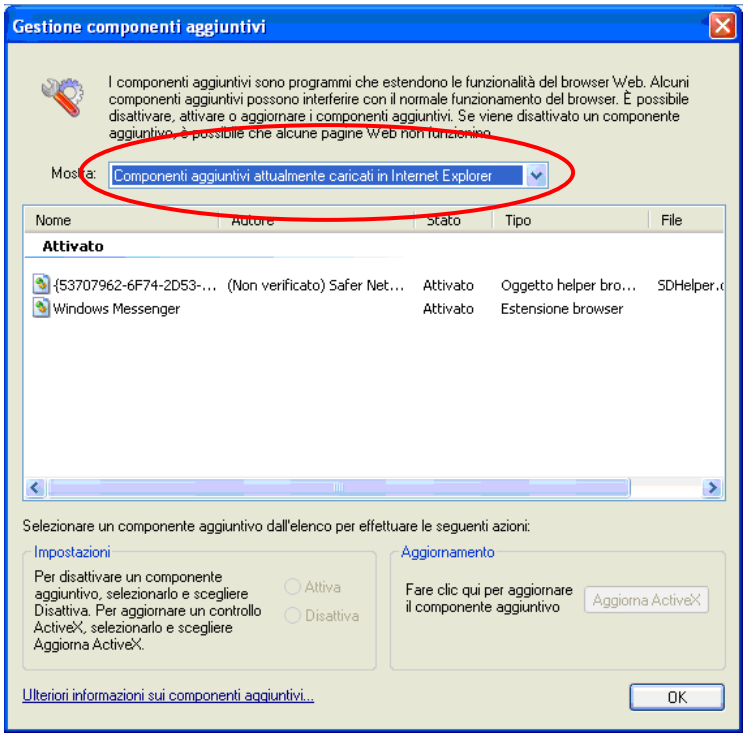
l'utente del computer possa individuare quali plugin siano istallati nel suo browser. Saranno esaminati i due browser maggiormente utilizzati (Internet Explorer und Firefox).

Internet Explorer 6

Selezionate in Internet Explorer la funzione Gestione componenti aggiuntivi sotto la rubrica strumenti …



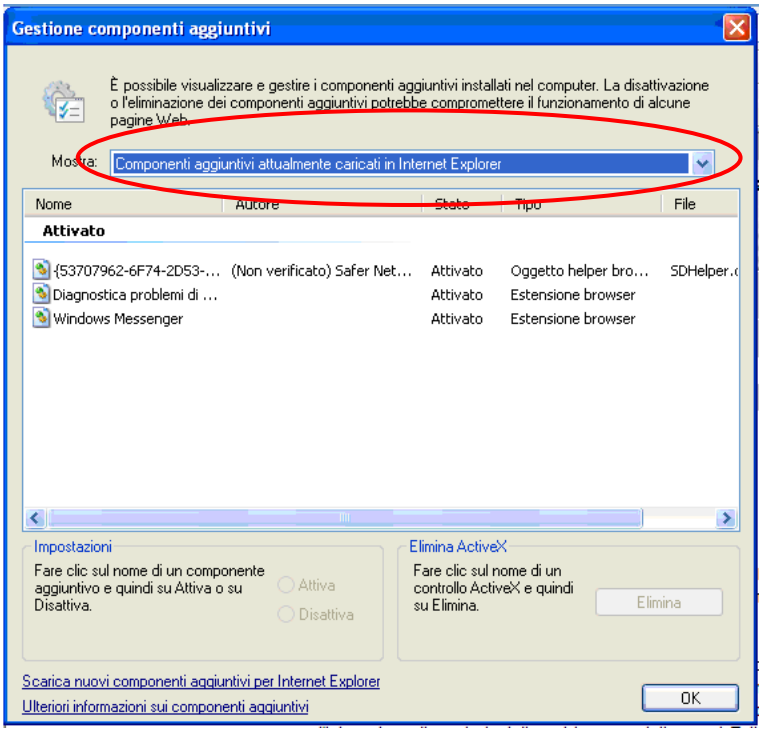
Saranno allora mostrati tutti gli add-on caricati in Internet Explorer. Potete anche visualizzare gli add-on utilizzati selezionando l'opzione corrispondente (cerchio rosso). Gli add-on possono essere attivati o disattivati. Tramite il pulsante «Aggiorna ActiveX» potete aggiornare gli add-on allo stato più recente. Questa funzione non è possibile per tutti i programmi.



Internet Explorer 7

Selezionate in Internet Explorer la funzione gestione componenti aggiuntivi sotto la rubrica strumenti e cliccate successivamente sull'opzione attivare, rispettivamente disattivare i componenti aggiuntivi.

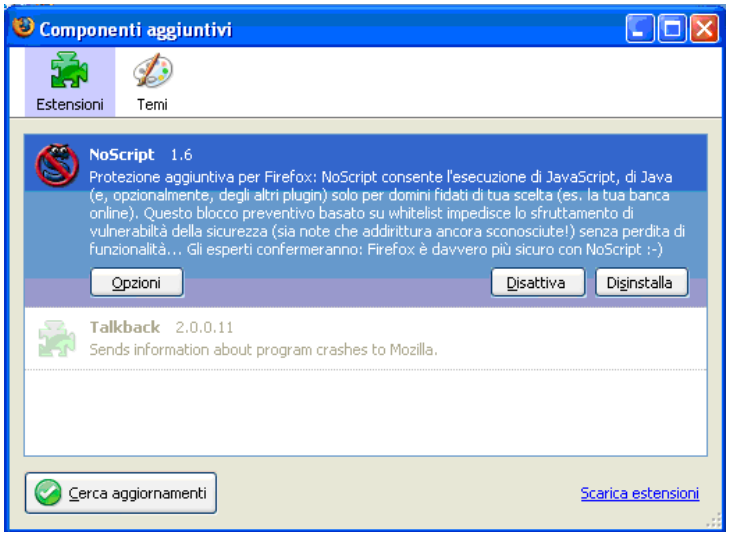
Saranno allora mostrati tutti gli add-on utilizzati in Internet Explorer. Potete anche visualizzare gli add-on caricati selezionando l'opzione corrispondente (cerchio rosso). Gli add-on possono essere attivati o disattivati.

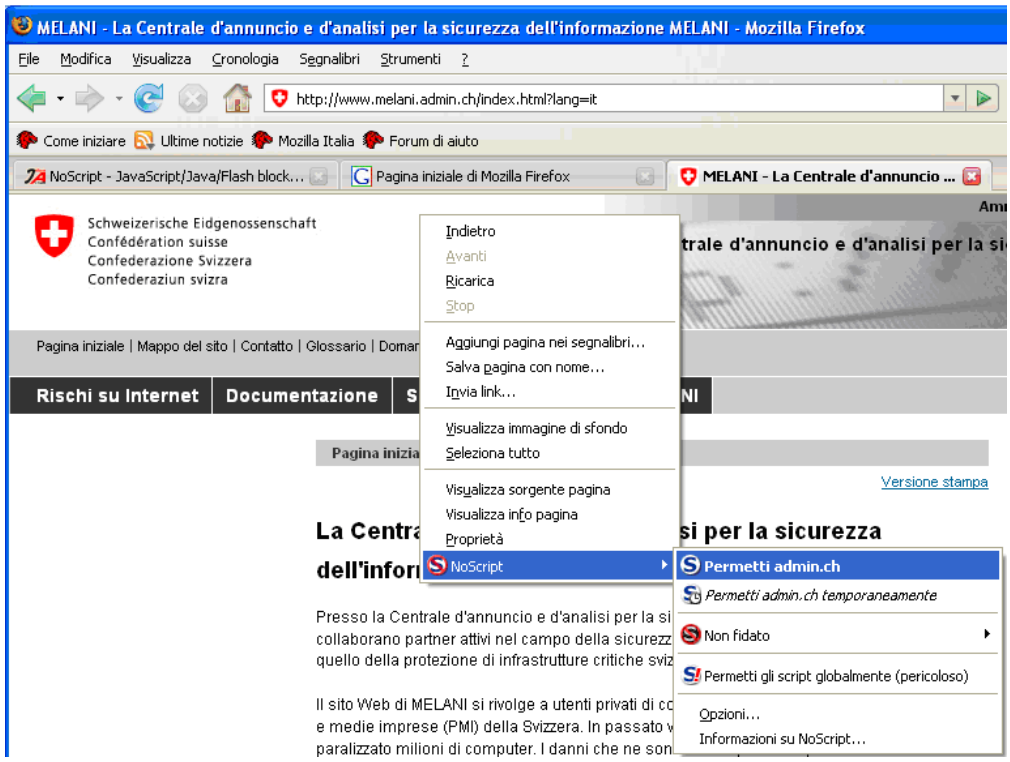


Firefox

Selezionate in Firefox la funzione Componenti aggiuntivi sotto la rubrica strumenti …

Saranno allora mostrati tutti gli add-on utilizzati in Firefox. Tramite il pulsante «Cerca aggiornamenti» potete aggiornare gli add-on allo stato più recente. Questa funzione non è possibile per tutti i programmi.



Utilizzazione di NoScript in Firefox

Dopo l'installazione di NoScript i contenuti Javascript di praticamente tutte le pagine sono bloccati. Sono autorizzate soltanto le pagine selezionate da NoScript. Esse possono ovviamente essere inserite manualmente. Si dovrebbe provvedere a inserire nella lista unicamente pagine che necessitano di Javascript e che sono affidabili. Se ci si trova su una pagina simile basta cliccare sul tasto destro del mouse e poi selezionare in NoScript l'opzione Javascript autorizzato o autorizzato temporaneamente.