Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Organo strategia informatica della Confederazione OSIC
Servizio di analisi e prevenzione SAP

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/II (luglio – dicembre)

In collaborazione con:

KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

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

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

The Swiss Coordination Unit for Cybercrime Control

Indice

1 Cardini dell'edizione 2008/II

- **Cavalli di Troia contro l'e-banking – Ulteriore diffusione su differenti canali**
  Anche nel secondo semestre del 2008 sono proseguiti i tentativi di diffusione di software nocivo all'e-banking. All'inizio del semestre sono state nuovamente osservate diverse ondate di spam. Inoltre si è maggiormente puntato sulla diffusione tramite infezioni drive-by, ossia su infezioni provocate dalla semplice navigazione su una pagina Web, senza interazione dell'utente. Alla fine del semestre ha poi fatto la sua apparizione in Svizzera una nuova famiglia di cavalli di Troia contro l'e-banking.

► Situazione attuale in Svizzera: capitolo 3.1

- **Condanna di agenti finanziari**
  L'anno scorso sono state pronunciate alcune condanne contro agenti finanziari. Il Tribunale distrettuale di Zurigo ha condannato un agente finanziario a una pena di 30 aliquote giornaliere e a una multa di 500 franchi per riciclaggio di denaro. Il Tribunale ha inoltre accordato il pieno risarcimento alla persona danneggiata. In un altro caso il prevenuto è stato condannato a una pena pecuniaria di 150 aliquote giornaliere e a una multa di 1000 franchi. Anche in questo secondo caso vi si aggiungono le pretese in risarcimento dei danni e le spese giudiziarie.

► Situazione attuale in Svizzera: capitolo 3.5

- **Diversi attacchi phishing contro servizi Internet svizzeri**
  L'anno scorso sono stati osservati diversi tentativi classici di phishing contro prestatori svizzeri di servizi. Nel caso del phishing l'invio di e-mail con mittenti e link falsificati è destinato ad attirare la vittima su una pagina Web falsificata affinché vi immetta i suoi dati di login. La percentuale di tentativi di phishing ai danni di prestatori di servizi finanziari è estremamente piccola. Si è osservato un aumento per quanto riguarda i tentativi di phishing ai danni di fornitori di aste o delle piattaforme di inserzione.

► Situazione attuale in Svizzera: capitolo 3.6

- **Vettore di attacco stick USB**
  Nel novembre del 2008 l'US Strategic Command ha deciso il vietare fino a nuovo avviso l'utilizzazione di schede mobili di memoria ai membri dell'esercito statunitense. Questa decisione è stata provocata dalla rapida diffusione di un virus che si copiava sui sistemi collegati a partire da un supporto mobile di dati. Anche il verme informatico Conficker sfruttava gli stick USB come vettore di diffusione.

► Il capitolo 4.1 e l'allegato (capitolo 7.2) forniscono consigli sull'utilizzazione dei supporti mobili di memoria.

- **Come sbarazzarsi dei «rifiuti di dati» della società dell'informazione**
  Oggigiorno praticamente quasi ogni apparecchio elettronico dispone di una scheda di memoria. Ne consegue un forte aumento dei dati memorizzati che ogni persona accumula inconsciamente. La cancellazione corretta dei dati è pertanto molto importante, quando ad esempio l'apparecchio fotografico, il telefono cellulare o lo stick USB cambiano proprietario. Troverete consigli preziosi nell'allegato.

► Tendenze, cfr. prospettive: capitolo 5.3

► Allegato: capitolo 7.1

2 Introduzione

L'ottavo rapporto semestrale (luglio – dicembre 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** (**capitolo 6**) alla fine del presente rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate dal loro colore.

La struttura dei capitoli è stata semplificata rispetto alle precedenti edizioni. Essa comprende d'ora in poi i capitoli principali «Situazione attuale a livello nazionale» e «Situazione attuale a livello internazionale». I capitoli relativi alla nuova legislazione, alle attività private e statali, agli studi e alle statistiche sulle tematiche delle TIC sono stati integrati nei due capitoli principali.

I **capitoli 3 e 4** abbordano le avarie e i crash, gli attacchi, la criminalità e il terrorismo che presentano relazioni con le infrastrutture TIC. Per il tramite di esempi scelti sono illustrati i principali avvenimenti delle seconda metà del 2008.

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

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

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Cavalli di Troia contro l'e-banking – Ulteriore diffusione su differenti canali

Anche nel secondo semestre del 2008 sono proseguiti i tentativi di diffusione di *software nocivo (cavalli di Troia)* ai danni della clientela e-banking. Gli aggressori tentano di diffondere questi cavalli di Troia sia mediante l'invio di e-mail di spam, sia per il tramite di pagine Web infettate (drive-by). Verso la fine dell'anno MELANI ha chiaramente constatato uno spostamento dallo spam in direzione delle infezioni drive-by.

Il semestre è iniziato con diverse ondate di e-mail (contenenti il cavallo di Troia denominato WSNPoem) che inducevano le vittime a cliccare su un allegato. In questo contesto sono stati soprattutto messi in circolazione e-mail che pretendevano la mancata consegna di un pacchetto da parte della ditta UPS. Si doveva in merito stampare la fattura contenuta nel documento allegato per poter ritirare il pacchetto. Nel caso del documento in allegato non si trattava però dell'atteso file PDF, bensì di un file «exe» eseguibile. Gli e-mal erano redatti sia in tedesco che in francese, circostanza che sembra indicare che una gran parte della Svizzera si trovava nel frattempo nel mirino dei criminali informatici.

"UPS colis postal"

"Bon matin,
malheureusement, nous avons manque de livrer le pli (votre colis postal), que vous avez envoyé le 1er juillet, parce que ladresse du Destinataire nexiste pas.
S'il vous plait, imprimez la facture envoyee en fichier joint a ce message, et venez chercher le pli a notre office a ladresse indiquee a la facture.
Consultant Esther Jennings,
UPS"

Esempio di un e-mail di spam in francese con un cavallo di Troia in allegato

Il 28 agosto 2008 si assistette per il momento all'ultima ondata di questa famiglia di cavalli di Troia, questa volta camuffata come biglietto aereo:

"Your Online Flight Ticket N 12557"

"Good morning,
Thank you for using our new service "Buy flight ticket Online" on our website.
Your account has been created:
Your login: xxxxx@xxxxxx.ch
Your password: passNFEC
Your credit card has been charged for $641.68.
We would like to remind you that whenever you order tickets on our website you get a discount of 10%!
Attached to this message is the purchase Invoice and the airplane ticket.
To use your ticket, simply print it on a color printed, and you are set to take off for the journey!
Kind regards,
Spirit Airlines"

Esempio di un e-mail di spam in inglese con un cavallo di Troia in allegato

Dopo di allora le ondate di e-mail cessarono di colpo. Come comunicato due mesi dopo dal Ministero pubblico olandese proprio a quel momento era stata conclusa con successo un'operazione contro truffatori in ambito di e-banking, seguita dall'arresto di tre persone. Si presume che nel caso delle persone arrestate si possa essere trattato con molta probabilità

di una parte dei responsabili degli attacchi menzionati qui sopra. Il capitolo 4.2 fornisce ulteriori informazioni in merito a questo arresto.

Nel mese di dicembre altri criminali informatici hanno tentato di prendere piede in Svizzera con la nuova famiglia di cavalli di Troia Gozi alias Infostealer.Snifula. Per il tramite di e-mail ambigui di spam[1] si è tentato di attirare le vittime potenziali su diverse pagine pornografiche Internet appositamente predisposte. I nomi di dominio di queste pagine contenevano perlopiù la parola «Switzerland», ciò che evidenzia il fatto che questa ondata era specialmente diretta verso la Svizzera. Sulla pertinente pagina Internet l'utente era poi sollecitato a scaricare e installare un *cosiddetto plugin Flash* per poter visualizzare le immagini della pagina Internet. Dietro di esso si celava un cavallo di Troia specializzato nell'attacco ai sistemi e-banking.

Nel 2008 è ulteriormente aumentata la diffusione di cavalli di Troia per il tramite di infezioni drive-by. In questo caso basta che l'utente navighi su una pagina (drive-by) affinché il computer sia infettato.

Per caricare il codice nocivo sulla pagina Web i criminali informatici necessitano dei pertinenti conti FTP. Essi se li procurano per il tramite degli hacker, procedendo davvero in grande stile, come lo dimostrano le spiegazioni del capitolo 3.4.

Gli utenti dei computer devono osservare norme di comportamento sia nella manipolazione degli e-mai, sia nella navigazione in Internet: essi devono mantenere aggiornati il loro sistema operativo e le loro applicazioni e utilizzare software antivirus e di firewall aggiornato (cfr. in merito le raccomandazioni sulla homepage di MELANI).[2] La limitazione di *ActiveX*, rispettivamente di *Javascript* aiuta a proteggersi dalle infezioni drive-by. Limitate nella misura del possibile l'esecuzione degli ActiveX Controls tramite la configurazione del browser. Modificate i parametri di sicurezza di Internet Explorer portandoli sul livello «alto». Le modalità di attuazione sono descritte passo per passo sulle pagine 5 e 6 della «Guida per una configurazione sicura di Windows XP»[3]. Per il browser Firefox esiste il programma Noscript[4], per mezzo del quale è possibile limitare individualmente Javascript per ogni pagina Internet.

Le irregolarità di funzionamento delle sessioni e-banking devono essere comunicate immediatamente al pertinente istituto finanziario. Ne sono una manifestazione particolare il doppio processo di login, un'improvvisa modifica dell'iter di login non comunicata dalla banca o l'interruzione della sessione dopo l'immissione della totalità delle informazioni di login.

3.2 Problematica delle reti bot

Le reti bot sono un assembramento di computer infettati con software nocivo. Esse possono essere integralmente telecomandate dall'aggressore (il proprietario della rete bot). Il provider statunitense McColo (capitolo 7.4) ha ospitato una grande quantità di *server Command & Control,* ragione per la quale è stato temporaneamente staccato da Internet. Questa circo-

[1] http://www.melani.admin.ch/dienstleistungen/archiv/01074/index.html?lang=de (stato: 02.02.2009).
[2] Cfr.: http://www.melani.admin.ch/themen/00166/index.html?lang=de (stato: 02.02.2009).
[3] Guida disponibile su http://www.melani.admin.ch/dienstleistungen/00132/00149/index.html?lang=de (stato: 02.02.2009).
[4] Addon Noscript per Mozilla Firefox https://addons.mozilla.org/de/firefox/addon/722 (stato: 02.02.2009).

stanza ha avuto ripercussioni anche in Svizzera: una parte del software nocivo ai danni dell'e-banking non ha più potuto essere diffusa.

3.3 Invio di e-mail falsificati con minacce di suicidio

Nella notte del 5 agosto 2008 sono stati inviati a indirizzi svizzeri di posta elettronica oltre 100'000 e-mail di spam. Per questo tramite un giovane informatico minacciava di uccidere la sua compagna e il di lei amante e di poi togliersi la vita. Numerosi cittadini preoccupati dall'invio di questo e-mail si sono rivolti alla polizia cantonale di Zurigo che verso le due del mattino ha svegliato il presunto suicida. L'e-mail era stato falsificato e la minaccia non era vera. Dietro il link contenuto nell'e-mail non era celato alcun malware.

Secondo le valutazioni della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) si trattava nella fattispecie di una grande operazione di ritorsione da parte di criminali informatici nei confronti dell'informatico che da lungo tempo pubblica sul suo sito Web abuse.ch dettagli sui software che attaccano i sistemi e-banking. Sul sito in questione era stato pubblicato poco tempo prima un documento dettagliato che illustrava le connessioni dell'infrastruttura informatica dei criminali peraltro anche responsabili degli attacchi ai danni dell'e-banking degli istituti finanziari svizzeri. Questa pubblicazione ha probabilmente fatto traboccare il vaso, inducendo i criminali a prendere contromisure. L'azione di intimidazione è iniziata con un grande attacco *Denial of Service* contro la pagina Web di abuse.ch ed è stata proseguita con l'invio dell'e-mail citato qui sopra.

In numerosi casi la criminalità su Internet è ancora percepita come un fatto puramente virtuale e inafferrabile oppure come la monelleria di un paio di rari assi dell'informatica. Come già indicato nell'ultimo rapporto semestrale la realtà è ben diversa. La criminalità su Internet è il fatto di gruppi ben organizzati, in parte distribuiti sull'intero globo, che hanno chiaramente in vista un utile finanziario rapido. Anche in questo contesto criminale il mercato e la lotta concorrenziale svolgono un ruolo: gli aggressori approfondiscono un determinato modello commerciale finché spese e ricavi, rischio e utile combaciano. Nel caso della misura di ritorsione contro gli informatici svizzeri gli aggressori intendevano palesemente eliminare questo fattore, che poteva avere ripercussioni negative sui loro affari.

3.4 Utilizzo abusivo di conti FTP

La società di sicurezza israeliana Aladdin ha scoperto nel secondo semestre del 2008 un server sul quale si trovavano più di 200'000 dati d'accesso FTP a server pubblici, di cui almeno 3'000 collegati a server svizzeri5. Per caricare dati su un server web i titolari di pagine web utilizzano normalmente un conto FTP (File Transfer Protocol6) presso un provider di hosting. Tra i siti collegati a questi conti, 82'000 erano già stati infettati con codici nocivi. Tra i siti illustri infettati vi si trovano quelli di imprese d'armamento, dello US Postal Service, di diverse università e siti governativi.

5 http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Windows&articleId=9116138&taxonomyId=125&pageNumber=1

6 http://www.faqs.org/rfcs/rfc959.html (stato il 17.02.2009)

MELANI è stata informata per quanto riguarda i siti ccTLD «.ch» In totale gli autori dell'attacco erano in possesso di più di 3'000 conti d'accesso FTP verso server svizzeri. Un accesso indebito è stato constatato in più di 130 siti web. Generalmente, i criminali hanno installato su di essi un'infezione di tipo «drive-by-download», che permette di infettare un computer attraverso la semplice visita del sito. I codici nocivi che sono stati diffusi attraverso questa tecnica sono soprattutto dei cavalli di Troia, che hanno come principale obietto la compromissione delle sessioni e-banking. I dati di connessione FTP possono essere raccolti in vari modi: attraverso dei codici nocivi – chiamati «keylogger» – installati sulle macchine degli amministratori dei siti, attraverso l'osservazione del traffico tra client e server o attraverso una lacuna di sicurezza presso l'hosting provider. Il protocollo FTP ha molti vantaggi, ma anche alcuni punti negativi: uno tra tutti il fatto che il traffico è trasferito in chiaro (non criptato) e quindi i codici d'accesso possono essere catturati.

Il servizio di gestione dei domini ccTLD «.ch», la fondazione SWITCH, è stato anch'esso informato. Questi dati sono in seguito stati trasferiti a diversi service provider. MELANI, dal canto suo, ha contattato direttamente i proprietari dei siti web più sensibili, per cercare di arginare il problema il più velocemente possibile.

Sulla stessa linea dell'operazione generata dalla ditta Aladdin, l'esercente dello Swiss Security Blog «abuse.ch» è riuscito ad individuare a fine 2008 un server sul quale erano stati salvati quasi 100 000 conti FTP. I dati sono stati poi trasferiti a MELANI, che dopo attenta analisi ha avvertito i titolari dei conti per il tramite del competente provider di hosting in Svizzera o per il tramite dei servizi competenti all'estero.

3.5 Condanna di agenti finanziari

In Svizzera si riaffacciano sempre e-mail che reclamizzano posti vacanti e promettono forti guadagni. Dietro di loro si celano in genere bande che intendono trasferire fondi provenienti da transazioni illegali con l'ausilio di cittadini inconsapevoli.

Dear Sir/Madam,

We're glad to offer you a position in our company Donation Europe. We are a charity organization in Central Europe. We help and support the community in Europe to help children of all ages. Donation Europe is an organization which supported by donations.

All information about us you can read at our website
You can earn money and help children with us. We are looking for freelance representatives in EUROPEAN COUNTRIES. Donation Europe receive donations in Europe, you have a possibility to become a Freelance representative? of our company. You do not need any funds to work and you do not need to find anybody. We hire people for freelance work. You can combine it with your full-time work, 2-3 hours a day are required from you. The salary is 450 – 2500 EUR per week. We have special offer for COMPANIES also. If you have an interest to our proposition and have a desire to help children send your reply to [e-mail at Yahoo]. Our manager will send you more information about the job and the terms of employment.

PLEASE REPLY TO [e-mail Yahoo] ONLY

Renee Johnson
Donation Europe.
Poland
Nowoursynowska st. 119,
02-776 Warsaw
Charity Registration No.: 101682
Company Registration No.: 2350841

E-mail pubblicitario dell'organizzazione caritativa fittizia «Donation Europe», inviato in grande quantità anche ai cittadini svizzeri

In genere chi reagisce a una siffatta offerta beneficia entro poco tempo di un trasferimento di denaro sul proprio conto. Dopo deduzione di una provvigione questo denaro deve essere trasferito all'estero, perlopiù per il tramite delle ditte di trasferimento di denaro «*Western-Union*» o «*Moneygram*». I fondi provengono sempre da operazioni illegali. Gli offerenti di simili occupazioni sfruttano partner inconsapevoli per trasferire all'estero il denaro lucrato fraudolentemente da canali online. Chi partecipa a siffatti «affari» o transazioni corre il rischio di un procedimento penale per riciclaggio di denaro (art. 305*bis* CP). Nel frattempo sono state pronunciate le prime condanne contro *agenti finanziari* svizzeri. La questione centrale è di accertare se si è agito intenzionalmente o se l'intenzione era eventuale e quindi se la fattispecie del riciclaggio di denaro è adempita anche dal profilo soggettivo. Un noto sito Web sul quale erano reclutati in grande stile agenti in tutta Europa era «Donation Europe». Qui si faceva credere i potenziali riciclatori di denaro che le donazioni dovevano essere trasferite in Russia e in Ucraina per il tramite di Moneygram. In realtà il denaro non proveniva da donazioni, bensì da truffe ai danni dell'e-banking.

«Donation Europe». Organizzazione caritativa che persegue l'obiettivo di trasferire in Russia e Ucraina fondi derubati con il phishing.

La pagina Web (cfr. illustrazione) suscita effettivamente un'impressione di professionalità. Un imputato che si era candidato a una simile occupazione ha confermato di avere preso visione della homepage dell'organizzazione «Donation Europe» e di averne tratto un'impressione di serietà. L'imputato ha nondimeno dovuto accettare il rimprovero di avere agito con ingenuità.[7] Nel corso dell'inchiesta esso ha infatti dichiarato di aver considerato un poco strano il modo in cui venivano effettuate le donazioni. Il fatto poi che i fondi dovessero essere trasferiti a mezzo MoneyGram avrebbe accresciuto i suoi dubbi. Ha quindi chiesto telefonicamente per quale motivo i fondi dovessero essere trasferiti unicamente a mezzo MoneyGram. Dalle ricerche che ha effettuato è emerso che diversamente da altre ditte di trasferimento di dena-

[7] https://www.a-i3.org/content/view/1535/130/ (stato: 02.02.2009).

ro MoneyGram verificava meno severamente la provenienza del denaro trasferito. Dal canto suo il tribunale ha constatato che è assolutamente inusitato che un'organizzazione caritativa inviti i suoi donatori a versare i doni sul conto di un terzo estraneo, non meglio noto all'organizzazione caritativa. Già per questo solo motivo l'imputato avrebbe dovuto dubitare che «Donation Europe» fosse un'organizzazione seria. Avrebbe peraltro dovuto suscitare la sua diffidenza il fatto di poter conservare per sé stesso una provvigione del 10 percento delle somme di denaro trasferite. Una provvigione di una simile entità non è affatto proporzionata all'esiguo dispendio di lavoro. Il tribunale è giunto alla conclusione che l'imputato avrebbe dovuto pensare alla possibilità che non si trattasse di un'organizzazione caritativa, bensì di un'organizzazione che trasferisce denaro lucrato illegalmente per il tramite di agenti finanziari. È quindi chiaro che l'imputato adempie la fattispecie del reato di riciclaggio di denaro anche dal profilo soggettivo.

Questo modo di vedere è condiviso anche da altri tribunali che hanno emanato sentenze che vanno nella medesima direzione. Il Tribunale distrettuale di Zurigo ha condannato un agente finanziario a una pena di 30 aliquote giornaliere per riciclaggio di denaro. Il tribunale ha inoltre statuito il pieno risarcimento della persona danneggiata. In un altro caso il Tribunale distrettuale di Arbon ha condannato un agente finanziario a una pena pecuniaria di 150 aliquote giornaliere e a una multa di 1'000 franchi. Anche in questo caso vi si aggiungono le pretese in risarcimento dei danni e le spese giudiziarie.

Le sentenze che sono state pronunciate finora evidenziano chiaramente che non si tratta affatto di reati bagatella, sebbene gli imputati abbiano di volta in volta preteso di non aver notato che si trattava di riciclaggio di denaro. In considerazione dei numerosi interrogativi e assurdità che comportano siffatte offerte di lavoro l'agente finanziario reclutato deve prima o poi avere necessariamente dei sospetti. Non mancano sufficienti indizi, come ad esempio il guadagno ingiustificato. Se l'agente trasferisce nonostante tutto la somma di denaro è dato il carattere intenzionale e la conclusione di tutto questo è la sua condanna. In questi casi l'ingenuità non protegge dalla pena. Se poi il denaro trasferito dall'agente finanziario non può essere recuperato – ciò che è raramente il caso – l'agente deve inoltre aspettarsi pretese in risarcimento dei danni dell'ordine di decine di migliaia di franchi. In ogni caso le offerte che prospettano ingenti guadagni vanno considerate con prudenza. I propri conti bancari non devono mai essere messi a disposizione di terzi. In caso di sospetto di truffa o di riciclaggio di denaro occorre informare le autorità (il posto locale di polizia oppure il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet SCOCI).

3.6 Diversi attacchi phishing contro servizi Internet svizzeri

L'anno scorso sono stati osservati diversi tentativi classici di *phishing* ai danni dei prestatori svizzeri di servizi Internet. Phishing significa l'invio di e-mail con mittenti e link falsificati, destinati ad attrarre la vittima su una pagina Web falsificata e a immettervi i propri dati di login. La percentuale di tentativi di phishing ai danni di prestatori di servizi finanziari è comunque estremamente piccola. Si sono inoltre registrati tentativi di phishing ai danni di fornitori di aste come ad esempio Ricardo[8] o piattaforme di inserzione come Autoscout24[9].

Nel caso di Autoscout24 i criminali informatici hanno sfruttato i dati di accesso per manipolare le inserzioni di commercianti di automobili degni di fiducia, al punto da porre improvvisamene in vendita per soli 44'000 franchi un'automobile originariamente offerta per 120'000

[8] http://www.online-betrug.ch/?p=105 (stato: 02.02.2009).

[9] http://www.tagesanzeiger.ch/digital/internet/story/19938467 (stato: 02.02.2009).

franchi. Gli hacker avevano corretto il prezzo verso il basso. Le vittime potenziali hanno approfittato di questo affarone. Gli utenti di Autoscout24 intenzionati a effettuare un acquisto sono stati informati a mezzo e-mail che l'automobile si trovava a Londra e che dovevano versarne preliminarmente il prezzo di vendita oppure un acconto su un conto all'estero. In realtà gli acquirenti truffati non hanno mai visto l'automobile.

Anche i provider sono nel mirino dei truffatori che praticano il phishing. In questo senso lo scorso mese di ottobre il provider di hosting Genotec ha messo in guardia i propri clienti da un'ondata di phishing[10]. In questo caso la motivazione dei criminali informatici dovrebbe essere evidente. Essi vogliono assumere il controllo del maggior numero possibile di pagine Web per ospitarvi i propri contenuti, come ad esempio cavalli di Troia o pagine di pornografia infantile. Anche i clienti di Bluewin sono nel mirino dei criminali informatici. In questo caso essi tentano di pervenire ai dati di accesso di Bluewin-Mail. Grazie a queste indicazioni essi possono ad esempio carpire i dati degli elenchi degli indirizzi oppure inviare e-mail di spam.

De : webmail.bluewin.ch <Suport@bluewin.ch> Date : 9 décembre 2008 10:53:21 GMT+01:00 À :
Objet : Confirm your

Dear bluewin.ch Subscriber,
To complete your bluewin.ch Account, you must reply to this email immediately and enter your password here (*********) Failure to do this will immediately render your email address deactivated from our database.

You can also confirm your email address by logging into your bluewin.ch Account at https://webmail.bluewin.ch
Thank you for using bluewin.ch!
THE bluewin.ch TEAM SUPPORT

Esempio di e-mail di phishing ai danni di Bluewin.ch

Anche le Università di Zurigo[11] e di Basilea[12] sono state oggetto di attacchi di phishing. Nella fattispecie si tentava di indurre gli studenti a fornire i dati di login dell'e-mail, rispettivamente i dati di login dell'università, tentativo che è riuscito in alcuni casi. Successivamente i conti di posta elettronica sono stati utilizzati abusivamente per attacchi spam o altre truffe. La conseguenza ne è stata l'iscrizione degli indirizzi di posta elettronica di entrambi gli istituti nella lista nera di alcune ditte anti-spam.

Se l'ultimo rapporto semestrale faceva ancora stato di una diminuzione dei tentativi di phishing ai danni dei prestatori di servizi finanziari, nel secondo semestre del 2008 si osserva un forte aumento dei tentativi di phishing ai danni di servizi Internet di ogni genere. Nel caso di questi tentativi l'interesse verte su tutto ciò che è «unicamente» protetto da un login e da una password e non da un'*autentificazione a due fattori*. I criminali informatici hanno notato che anche così è possibile fare soldi e che dati di questo genere consentono di accedere a ulteriori interessanti informazioni e diritti. Conserva quindi pienamente la sua validità e va estesa a tutte le prestazioni di servizi protette da password la raccomandazione di non indicare mai i propri dati di login.

[10] http://www.genotec.ch/desktopdefault.aspx/tabid-219/184_read-458/ (stato: 02.02.2009).
[11] http://www.20min.ch/news/schweiz/story/24375194 (stato: 02.02.2009).
[12] Cfr. per la comunicazione dell'Università di Basilea:
http://www.unibasel.ch/index.cfm?uuid=21A8F3823005C8DEA3B81CC699203FF9&type=search&show_long=1
(stato 02.02.2009).

3.7 Diversi attacchi contro server Web

Diversi attacchi di hacking hanno fatto sensazione nel secondo semestre. È stata infatti deturpata la pagina Web contenente i comunicati stampa della polizia cittadina di Zurigo. Si è trattato nella fattispecie di un cosiddetto *defacement* di pagine Web. L'aggressore ha lasciato il messaggio «Hacked by Burak». È inoltre apparso un disegno raffigurante due giovani che legano un terzo giovane[13].

Gli hacker sono parimenti penetrati in un server Web dell'Organizzazione europea per la ricerca nucleare (CERN), modificandovi le relative pagine Web[14]. Anche in questo caso gli hacker hanno lasciato un messaggio che ridicolizza i tecnici informatici del centro per la ricerca nucleare di Ginevra, trattandoli da «scolaretti» in considerazione delle lacune di sicurezza constatate.

Nel caso di simili deturpazioni non si verifica solitamente un accesso ai dati; si sfruttano le lacune di sicurezza del software dei server, rispettivamente delle applicazioni dei server. In entrambi i casi l'attacco è stato rapidamente individuato e non ne sono risultati danni.

Nel mese di ottobre gli hacker hanno tentato di penetrare nei server centrali della Scuola politecnica federale (SPF). La sorveglianza interna ha potuto individuare gli attacchi e adottare contromisure. Al seguito di questo incidente è stato esaminato un nuovo concetto di sicurezza[15].

[13] Ulteriori informazioni: http://www.bluewin.ch/de/index.php/25,77047/Unbekannte_hacken_Internetseite_der_Stadtpolizei_Zuerich/ (stato: 02.02.2009).

[14] Ulteriori informazioni: http://diepresse.com/home/techscience/wissenschaft/414065/index.do?from=rss (stato: 02.02.2009).

[15] http://www.infoweek.ch/security/hacking/articles/164957/ (stato: 02.02.2009).

3.8 Entrata in vigore della revisione della legge sul diritto d'autore

Il 1° luglio 2008 è entrata in vigore la revisione della legge svizzera sul diritto d'autore[16]. Le principali modifiche introdotte dalla novella sono:

Le misure tecniche (p. es. protezione contro la copia sui CD audio) sono d'ora in poi protette. È punibile chiunque offre o utilizza programmi per eludere questa protezione. Rimane ulteriormente autorizzato l'allestimento di una copia privata, sebbene tale allestimento corrisponda a un'elusione delle misure tecniche di protezione.

3.9 Il Parlamento adotta il divieto della pornografia sui telefoni cellulari

Dopo il Consiglio degli Stati anche il Consiglio nazionale si è pronunciato il 2 settembre 2008 a favore dell'elaborazione da parte, e contro la volontà, del Consiglio federale, di norme di legge in vista di un divieto della pornografia e della rappresentazione della violenza sui telefoni cellulari[17]. È possibile che questa decisione abbia ripercussioni anche sull'ordinanza dei servizi di telecomunicazione. Gli offerenti di prestazioni del servizio universale potrebbero essere se del caso tenuti a bloccare, nei confronti delle persone minori di 16 anni, tutte le comunicazioni con servizi commerciali a valore aggiunto con contenuti erotici o pornografici. I fornitori di prestazioni a valore aggiunto potrebbero essere tenuti a non vendere contenuti erotici o pornografici a persone minori di 16 anni.

I dibattiti parlamentari sono stati suscitati dalla mozione Schweiger[18]. Nella sua risposta alla mozione il Consiglio federale ha soprattutto rammentato che il Codice penale vieta fin d'ora l'offerta di scritti e immagini pornografiche ai minori di 16 anni, a prescindere dal fatto che essi siano offerti a scopo commerciale o a scopo non commerciale. Basterebbe quindi un'applicazione conseguente della legislazione in vigore, senza la necessità di una nuova norma supplementare. Va comunque osservato che la nuova ordinanza postulata deve essere strutturata in maniera possibilmente neutrale dal profilo delle tecnologie. La mozione era infatti chiaramente focalizzata sulle nuove offerte pornografiche commerciali per telefoni cellulari basate su Wap o MMS. Con l'incremento della convergenza tecnica i telefoni cellulari divengono sempre più degli apparecchi capaci di accedere a Internet. I contenuti che possono essere captati con questi smartphones non sono più contenuti appositamente predisposti per i telefoni cellulari, ma semplicemente quelli accessibili su Internet e destinati a tutti gli altri utenti di computer. Un divieto delle offerte pornografiche commerciali per i telefoni cellulari che non sia strutturato in maniera neutrale dal profilo tecnico potrebbe pertanto entrare in vigore quando questo fenomeno non esiterebbe ormai più nella realtà.

[16] Le principali modifiche della legge svizzera sul diritto d'autore: http://www.ige.ch/d/jurinfo/j10300.shtm (stato: 02.02.2009).

[17] http://www.heise.de/newsticker/Schweizer-Parlament-verabschiedet-Pornoverbot-auf-Handys--/meldung/116550 (stato: 02.02.2009).

[18] Cfr. mozione 06.3884 – Nessuna pornografia commerciale sui cellulari: http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20063884 (stato: 02.02.2009).

3.10 Scoperta una piattaforma Internet per pedofili

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI) ha individuato sulla base di ricerche su Internet e di indagini una pagina Web per pedofili, ospitato da un provider di San Gallo. Si trattava nella fattispecie di una piattaforma sulla quale venivano discussi interessi pedofili. Essa offriva agli utenti la possibilità di fare migliore conoscenza o di collegarsi in rete a livello privato. Lo SCOCI ha potuto constatare che sulla piattaforma venivano scambiati consigli ed esperienze sul modo di comportarsi con le fanciulle o istruzioni sulla prima presa di contatto con esse. Dalle ricerche è parimenti emerso lo scambio tramite il forum di file contenenti pornografia infantile.

L'Ufficio federale di polizia (fedpol) ha trasmesso direttamente ai Paesi interessati le indicazioni relative ai partecipanti stranieri e agli esercenti del forum. Si tratta di circa 600 persone in Germania, 40 in Austria e 4 nel Principato del Liechtenstein. Le informazioni relative agli utenti svizzeri sono state trasmesse alle autorità di perseguimento penale del Cantone di San Gallo, perché il provider vi ha la propria residenza. Finora sono stati avviati procedimenti penali nei confronti di 13 cittadini svizzeri. Quattro persone sono state arrestate per atti sessuali con fanciulli o per produzione di immagini e filmati contenenti abusi sessuali diretti con una fanciulla. Sono state effettuate perquisizioni al domicilio di tutte le persone sospettate ed è stato sequestrato ampio materiale, come rischi duri di computer e altri supporti di dati. La valutazione prenderà ancora un certo tempo. Sulla base dei primi risultati si può comunque constatare che grandi quantità di materiale fotografico e cinematografico concernente pornografia infantile hanno potuto essere sequestrate[19].

3.11 Diversi bloccaggi presso le grandi imprese

Nel corso dell'ultimo semestre numerose imprese, soprattutto del settore assicurativo e finanziario, hanno bloccato l'accesso ai siti sociali Web, come Facebook. I motivi di bloccaggio addotti sono l'utilizzazione eccessiva durante le ore di lavoro come anche il pericolo che le indicazioni fornite su queste pagine dai collaboratori possano essere utilizzate abusivamente per attacchi di *social engineering*. Le informazioni personali su Facebook possono senz'altro essere di ausilio per completare il profilo di una persona o di un gruppo di persone: chi fa parte di chi? dove lavora? cosa fa nel suo tempo libero? dov'è in questo momento? ecc. Queste informazioni possono poi essere correlate con altri dati esistenti su Internet e utilizzate per carpire con l'inganno la fiducia di questa persona e accedere più facilmente per questo tramite a dati confidenziali.

Il bloccaggio di pagine Internet all'interno delle imprese può essere dettato dai più svariati motivi. Da un canto si può impedire la diffusione di malware tramite un possibile canale, d'altro canto, proprio nel caso delle pagine Web 2.0 come Facebook, è possibile tutelare la morale del lavoro. Nel caso della preparazione di un *attacco di social engineering* il bloccaggio di una pagina Internet ha a seconda dei casi un impatto troppo ridotto. Solitamente poco importa che il collaboratore immetta i dati durante le ore di lavoro oppure al proprio domicilio. Importa invece che le imprese definiscano direttive integrali sul genere di informazioni riguardanti l'impresa che possono essere pubblicate su siffatte pagine Web.

Alcune imprese hanno bloccato anche Doodle, un pianificatore pubblico degli appuntamenti. Il bloccaggio è stato deciso in questo caso argomentando che i dati confidenziali come ap-

[19] Cfr. in merito al comunicato del Ministero pubblico sangallese: http://www.staatsanwaltschaft.sg.ch/news/staatsanwaltschaft/2008/09/internet_plattform.html (stato: 02.02.2009).

puntamenti d'affari e nomi di clienti non devono pervenire a piattaforme pubbliche «incontrollate».

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 USA: i militari vietano l'utilizzazione di supporti mobili di memoria

Nel mese di novembre 2008 l'US Strategic Command ha deciso che ai membri dell'esercito statunitense è vietata fino a nuovo avviso l'utilizzazione di supporti mobili di memoria (stick USB, CD, DVD ecc.). Questa decisione è stata suscitata dalla rapida diffusione di un virus che si copiava sui sistemi collegati a partire dagli stick USB [20]. I militari US hanno adottato in questo caso una misura radicale. Non si tratta però di una misura isolata quando si tratta di combattere i pericoli che comporta l'utilizzazione di supporti esterni di dati. In un suo rapporto anche Symantec ha messo ad esempio in guardia dalla diffusione di parassiti tramite gli stick USB[21].

Attualmente esistono in particolare due possibilità di diffusione dei parassiti con l'ausilio di uno stick USB o di un'altra scheda mobile di memoria: da un canto il software nocivo può copiarsi direttamente dal computer infettato a partire dallo stick USB collegato. Quando l'utente collega il suo stick USB al computer e chiama (inconsapevolmente) il file infettato il parassita si copia sul computer in questione. Per questo percorso infettivo è necessario che l'utente attivi manualmente il programma infettato. La seconda possibilità consiste nel fatto che il software nocivo crea o modifica una funzione di AutoRun del media di memorizzazione. Quanto l'utente collega la scheda mobile di memoria al suo computer il software nocivo può copiarsi automaticamente sul computer in questione.

Nell'estate del 2008 l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) ha pubblicato un rapporto che informa le imprese sui pericoli connessi all'utilizzazione di stick USB e fornisce consigli per una manipolazione sicura. Oltre che al pericolo di un percorso infettivo supplementare per i parassiti descritto qui sopra, il rapporto rinvia in particolare ai rischi di perdita o di furto degli stick USB. L'ENISA ribadisce l'importanza di una valutazione dei rischi e di direttive vincolanti sulla manipolazione delle schede mobili di memoria[22].

I principali consigli sulla manipolazione degli stick USB:

- Disattivate la funzione AutoRun. In conseguenza della disattivazione occorre sempre intervenire manualmente per chiamare lo stick. L'allegato fornisce una guida in merito.
- Verificate lo stick USB con un programma antivirus aggiornato.
- Codificate le informazioni confidenziali prima di memorizzarle. In caso di furto lo stick è certo perduto, ma l'informazione, rispettivamente i file sono protetti.

[20] http://blog.wired.com/defense/2008/11/army-bans-usb-d.html (stato: 02.02.2009).
[21] https://forums.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/220 (stato: 02.02.2009).
[22] http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf (stato: 02.02.2009).

- Ogni impresa, grande o piccola, dovrebbe stabilire imperativamente mediante direttive l'e modalità di utilizzazione degli stick USB. Tali direttive devono contenere istruzioni sulle condizioni alle quali è autorizzato l'uso degli stick USB. Alcuni stick tentano di installare software sull'apparecchiatura finale. La consegna di stick a livello centralizzato dovrebbe perlomeno limitare questo rischio. Ulteriori possibilità consistono nella limitazione dei diritti di amministratore o nella disattivazione della porta USB.

4.2 Successi contro la criminalità informatica

Nel secondo semestre del 2008 sono stati registrati numerosi successi nella lotta contro la criminalità informatica. In questo senso nel mese di ottobre il Ministero pubblico olandese ha reso noto che un gruppo responsabile – probabilmente anche in Svizzera – di numerose truffe in ambito di e-banking aveva potuto essere arrestato in Ucraina e in Russia[23].

Il danno provocato dai truffatori è stimato in oltre 100'000 euro. In diverse città dell'Ucraina e della Russia sono stati sequestrati computer e altri mezzi di prova. Le persone arrestate sono tre studenti in informatica. Si tratta del secondo grande colpo sferrato ai truffatori in ambito di e-banking dopo l'arresto, nel settembre del 2007[24], di otto sospetti in Germania da parte del Bundeskriminalamt (BKA). All'epoca si trattava di due donne di 22 e 23 anni e di sei uomini di età compresa tra i 20 e i 36 anni, provenienti dalla Russia, dall'Ucraina e dalla Germania.

4.3 Germania: grande furto di dati presso la Telekom

Nel 2008 sono state rese note numerose perdite di dati a livello mondiale. Ne sono stati vittima l'economia privata e anche i settori governativi.

In Germania in particolare la pubblicazione da parte della Telekom della notizia della perdita di oltre 17 milioni di dati della clientela ha riacceso il dibattito sulla sicurezza e sulla protezio-

[23] Comunicato stampa del Ministero pubblico olandese (in olandese) http://www.om.nl/actueel/nieuws-_en/@149040/internationale/ (stato: 02.02.2009).
[24] http://www.heise.de/newsticker/BKA-verhaftet-Phisher-Gruppe--/meldung/95928 (stato: 02.02.2009).

ne dei dati[25]. Le serie di dati derubate comprenderebbero i numeri telefonici segreti e gli indirizzi privati di noti esponenti politici e di dirigenti dell'economia. I dati sono però stati derubati fin dal 2006. All'epoca le autorità intervennero, ma il pubblico non fu però informato della perdita dei dati. I dati sarebbero stati successivamente offerti su Internet all'interno di cerchie criminali; nell'ottobre del 2008 venne poi reso moto al pubblico il caso del periodico di informazione «Der Spiegel»[26]. Il Governo decise quindi di effettuare analisi di pericolo per gli esponenti interessati.

Nel caso di questo incidente si tratta di un esempio particolarmente eminente di perdita di dati. Le perdite e le avarie di dati sono comunque numerose e ne sono colpiti tanto l'economia privata che i settori governativi. I motivi ne sono molteplici e comprendono il furto all'interno e all'esterno, la perdita e il furto di supporti digitali (laptop, stick USB ecc.), la pubblicazione e la diffusione involontaria, come pure la perdita di dati da parte di prestatori esterni di servizi (p. es. ditte di consulenza).

L'incremento delle raccolte di dati personali è un fenomeno concomitante naturale della nostra moderna società dell'informazione. I dati e le informazioni raccolti possono essere considerati ad un tempo un potenziale di valore aggiunto o un rischio. Ne consegue l'accresciuta importanza di un'utilizzazione dei dati sicura, basata sulla fiducia e disciplinata. Una chiara gestione dei rischi è di rilievo sia per l'economia privata, sia per il settore pubblico[27].

4.4 UE: adottato un piano di lotta totale e comune contro la criminalità su Internet

Alla fine del mese di novembre del 2008 i ministri della giustizia e dell'interno dell'Unione europea (UE) hanno adottato un piano di lotta totale e comune contro la criminalità su Internet. Le misure operative previste comprendono tra l'altro una piattaforma europea per la segnalazione dei reati su Internet, un più efficiente scambio di informazioni tra autorità di perseguimento penale ed economia privata, l'impiego di squadre transfrontaliere di inchiesta, un migliore coordinamento in ambito di bloccaggio e di chiusura di siti Web incriminati e l'allestimento di una lista nera comune, come pure l'agevolazione delle perquisizioni a distanza (ciò che dovrebbe corrispondere a delle perquisizioni online), sempreché la legislazione nazionale lo preveda[28].

[25] Cfr. in merito al comunicato stampa della Telekom: http://www.telekom.com/dtag/cms/content/dt/de/595698?archivArticleID=572376 (stato: 02.02.2009).
[26] http://www.spiegel.de/wirtschaft/0,1518,581938,00.html (stato: 02.02.2009).
[27] Cfr. sul tema delle imprese e della loro gestione delle informazioni il seguente studio effettuato su mandato dell'Economist Intelligence Unit: http://switzerland.emc.com/collateral/analyst-reports/economist-intell-unit-info-governence.pdf (stato: 02.02.2009).
[28] Cfr. in merito alle conclusioni finali del Consiglio della giustizia e dell'interno: http://register.consilium.europa.eu/pdf/de/08/st15/st15569.de08.pdf e per la comunicazione della Commissione dell'UE: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827&format=HTML&aged=0&language=DE&guiLanguage=en (stato: 02.02.2009).

4.5 Germania: conservazione dei dati anche per i provider di Internet

Dal 1° gennaio 2009 tutti i dati di collegamento Internet devono essere conservati per la durata di sei mesi in Germania, anche in assenza di un sospetto concreto. In Germania la direttiva dell'UE sulla conservazione dei dati concernenti le telecomunicazioni e i collegamenti a Internet è stata trasposta nella legislazione nazionale fin dall'inizio del 2008[29]. I dati di collegamento concernenti la telefonia fissa e la telefonia mobile sono già conservati fin dall'inizio del 2008. Per i provider di Internet era stato previsto un periodo transitorio che è scaduto a fine 2008[30].

4.6 Germania: entrata in vigore della revisione della legge sul BKA

Il 1° gennaio 2009 è entrata in vigore in Germania la revisione della legge sul Bundeskriminalamt (BKA). La legge introduce nuove competenze in materia di lotta contro il terrorismo e consente tra l'altro di effettuare perquisizioni online furtive[31].

4.7 Gran Bretagna: entrata in vigore della nuova legge sulla criminalità informatica

In Inghilterra e nel Galles è entrata in vigore il 1° ottobre 2008 la revisione del «Computer Misuse Act». Le principali novità riguardano l'inasprimento delle pene in caso di accesso non autorizzato a un sistema di computer come pure il divieto di *attacchi Denial-of-Service (DOS)* e la diffusione di «Hacker-Tools»[32].

5 Tendenze / Prospettive

5.1 Evoluzione generale della criminalità informatica

Dal profilo tecnico i mezzi della criminalità informatica non sono notevolmente cambiati rispetto all'ultimo semestre. Per la diffusione di software nocivo sono utilizzati e-mail di spam e

[29] Cfr. il rapporto semestrale MELANI 2007/2, capitolo 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=de (stato: 02.02.2009).

[30] Cfr. per informazioni dettagliate su questo tema la seguente pagina dell'Incaricato federale germanico della protezione dei dati: http://www.bfdi.bund.de/cln_007/nn_533578/DE/Schwerpunkte/Vorratsdaten/Artikel/Vorratsdatenspeicherung.html (stato: 02.02.2009).

[31] Cfr. per il testo d legge: http://www.bgblportal.de/BGBL/bgbl1f/bgbl108s3083.pdf; cfr. per il dibattito sulle perquisizioni online in Germania anche il rapporto semestrale MELANI 2008/1, capitolo 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=de (stato: 02.02.2009).

[32] Cfr. per l'atto legislativo: http://www.opsi.gov.uk/si/si2008/uksi_20082503_en_1; per il Computer Misuse Act: http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm e per il Police and Justice Act: http://www.opsi.gov.uk/Acts/acts2006/ukpga_20060048_en_1 (stato: 02.02.2009). Cfr. per ulteriori informazioni anche il seguente articolo: http://www.theregister.co.uk/2008/09/30/uk_cybercrime_overhaul/ (stato: 02.02.2009).

infezioni drive-by. Oltre che in inglese, gli e-mail contenenti malware ricevuti in Svizzera sono redatti anche in tedesco, francese e italiano. Per accedere ai dati personali si fa capo a cavalli di Troia e al phishing. I cavalli di Troia sono celati mediante funzioni *Root-Kit*. Le pagine di phishing sono ospitate su *reti fast-Flux*. Le reti bot costituiscono tuttora il mezzo più importante a tale scopo e sono sempre disponibili in grande numero. Le *lacune di sicurezza* svolgono sempre un ruolo (troppo) grande nella diffusione di software nocivo, come illustrato dal recente esempio della diffusione del *verme informatico* Conficker.

Ciò che comunque cambia sono le strutture d'affari della criminalità informatica: si afferma gradualmente una vera e propria organizzazione di prestazioni di servizi. Non si tratta più di singoli gruppi autonomi, bensì di strutture in rete che si concentrano sui singoli compiti. Lo scambio di informazioni tra questi gruppi funziona apparentemente in maniera eccellente. Ogni criminale informatico si mette alla ricerca di una nicchia e tenta successivamente di offrire il suo prodotto sul «mercato». In merito vengono offerti nel frattempo veri assortimenti di servizi (capitolo 5.2)

Poiché la problematica è frattanto nota si potrebbe supporre che le contromisure possano essere introdotte in maniera relativamente semplice. Singoli successi, come l'arresto di una banda di truffatori in ambito di e-banking (capitolo 4.2) oppure l'allontanamento del provider McColo (capitolo 7.4) forniscono una nota fiduciosa in questo contesto. Nonostante questi successi poco cambia alla dimensione del danno arrecato quotidianamente. I criminali sono in grado di adeguarsi di volta in volta al meglio alla nuova situazione. Se un membro sparisce quello successivo si introduce nella breccia e tenta di colmare la lacuna il più presto possibile. L'allontanamento di McColo, ad esempio, ha determinato un calo solo temporaneo degli e-mail di spam. Nella prima settimana del mese di febbraio 2009 la produzione media di spam ha raggiunto per la prima volta il livello anteriore all'allontanamento di McColo[33]. Anche l'arresto dei truffatori in ambito di e-banking ha provocato in Svizzera solo un breve periodo di recupero. Soltanto 4 mesi dopo un nuovo gruppo ha tentato di affermarsi con una nuova famiglia di cavalli di Troia.

Purtroppo la reazione da parte della lotta alla criminalità è parzialmente responsabile di questo stato di cose. Su diversi punti il dibattito in merito alle responsabilità in ambito di sicurezza su Internet non è ancora stato concluso esaurientemente. A seconda del caso o della situazione iniziale la responsabilità compete al perseguimento penale, ai provider, ai servizi di registrazione, agli esercenti delle pagine Web oppure agli stessi utenti di Internet. Non è affatto raro che gli attacchi possano essere totalmente impediti dalla reazione corretta o dalla messa in rete di molti di questi partner partecipanti. È quindi chiaro che tutti coloro che offrono o utilizzano servizi su Internet sono responsabili in una maniera o nell'altra. In molti casi purtroppo si preferisce giocare a Pietro Nero invece di trarre gli insegnamenti corretti e quindi di contribuire a una soluzione per il potenziamento della sicurezza su Internet.

5.2 Cybercrimine accessibile a tutti: uno stimolo per il 2009

Nell'ambito della criminalità del cyberspazio si è sviluppando nell'ultimo anno un modello commerciale chiamato Crimeware-as-a-Service (CaaS)[34]. I criminali, ben coscienti delle difficoltà tecniche legate alla gestione di server, all'installazione di toolkit o all'infezione di pagine web, preferiscono «affittare» un servizio. Attraverso queste piattaforme i criminali ottengono

[33] Cfr. anche: http://www.eleven.de/de/aktuell/pressemitteilungen/eleven-spam-aufkommen-hat-sich-von-mccolo-abschaltung-erholt-398.html (Stato: 02.02.2009).

[34] http://www.finjan.com/Pressrelease.aspx?id=1922&PressLan=1819&lan=3 (stato il 03.02.2009)

direttamente da altri criminali (Criminal-to-Criminal, C2C) i dati (carte di credito, dati d'accesso a conti bancari o a web server e altro) che poi potranno monetizzare (tra le tante operazioni vi sono le transazioni finanziarie, la rivendita degli stessi dati oppure l'acquisto di beni). Questa nuovo modello commerciale vedrà uno sviluppo importante nel corso del 2009[35] a seguito di vari fattori come la crisi economica o le difficoltà nell'individuare i criminali e soprattutto nel perseguirli penalmente.

Una domanda che molti si pongono è se l'accesso a questo tipo di attività criminale sia così semplice come viene descritto in diversi studi. Come tutte le attività illegali, anche la criminalità nel cyberspazio si sviluppa in ambienti ai più sconosciuti, cercando di evitare gli sguardi indiscreti di forze dell'ordine, ricercatori e curiosi. Sulla rete questo grado di offuscamento si può ottenere comunicando attraverso un protocollo chiamato Internet Relay Chat (IRC), prima forma di comunicazione istantanea su Internet[36]. Se vi sono server con solo alcuni canali, ne esistono altri che ospitano decine di migliaia di canali. Ed è su questi server che i criminali si contattano, ben coscienti del grado di offuscamento esistente. I criminali, sui canali IRC, offrono, vendono e comprano servizi[37]. Ma se da un lato i criminali vogliono offrire servizi tutto incluso a persone che non sono del ramo dall'altro vi è la difficoltà di avvicinare nuovi interessati. I canali IRC non sono per i neofiti di facile accesso, sia per una questione tecnica di utilizzo, sia per l'enorme quantità di canali che un server può offrire e la conseguente difficoltà nel trovare ciò che si cerca.

E allora cosa vi è di meglio di un servizio basato sul web? Primo embrione di questo nuovo modello il sito web 76service.com[38]. Gli abbonati, una volta identificatisi, potevano scaricare gli ultimi dati rubati da un codice malevolo chiamato Gozi[39]. E 76service.com ha fatto scuola, generando una moltitudine di servizi analoghi che mettevano in vendita praticamente in tempo reali, dati appena rubati per accedere a conti bancari o per duplicare carte di credito[40].

Ma l'audacia dei criminali va oltre. Non solo i servizi sono offerti oggigiorno alla luce del sole, ma anche i mezzi tecnici sono venduti ormai attraverso canali accessibili a tutti quanti, come ad esempio forum aperti. Spiegazioni su come utilizzare i codici acquistati, o aiuto sullo sviluppo ulteriore, chiunque si interessi di queste tematiche troverà il supporto ideale:

Forum	Last Post	Threads	Posts
Opensc related area News, announcement and suggestion/complaints forum.	**Don't Talk About tr0jans...** by LttCoder 08-01-2009 13:16	78	891
Trojan & malware releases (9 Viewing) Post your programs here	**[C++]HOC v1.0 In Progress...** by xSLaYaHx Today 06:40	571	7,481
Trojan discussion and general help Talk about trojan's and get help with them here	**Trojan vote the best in your...** by mjrod5 Today 04:10	196	1,266
Tutorials/articles (3 Viewing) Submit your own tutorials,articles or give suggestions/feedback to the already posted tutorials/articles.	**[REQ] Binder / Crypter...** by ishmoe12 21-01-2009 15:57	91	702
Opensource community projects (1 Viewing) Opensource projects that everyone can help build together	**Anyone want to code a botnet?** by UnkOwn Today 00:31	14	356

I codici nocivi sono spesso venduti in coppia con gli exploit per i navigatori più utilizzati, come El Fiesta o IcePack. Spesso si tratta di versioni piratate dei codici stessi. Gli sviluppatori di tali crimeware, per cercare di proteggere la proprietà intellettuale del loro lavoro, sono arri-

[35] http://www.finjan.com/GetObject.aspx?ObjId=641&Openform=50 (stato il 15.01.2009, iscrizione obbligatoria per scaricare lo studio)

[36] http://tools.ietf.org/html/rfc1459 (stato il 03.02.2009)

[37] http://www.symantec.com/content/de/de/about/downloads/PressCenter/20081124_UE_Report_Final.pdf (stato il 17.12.2008)

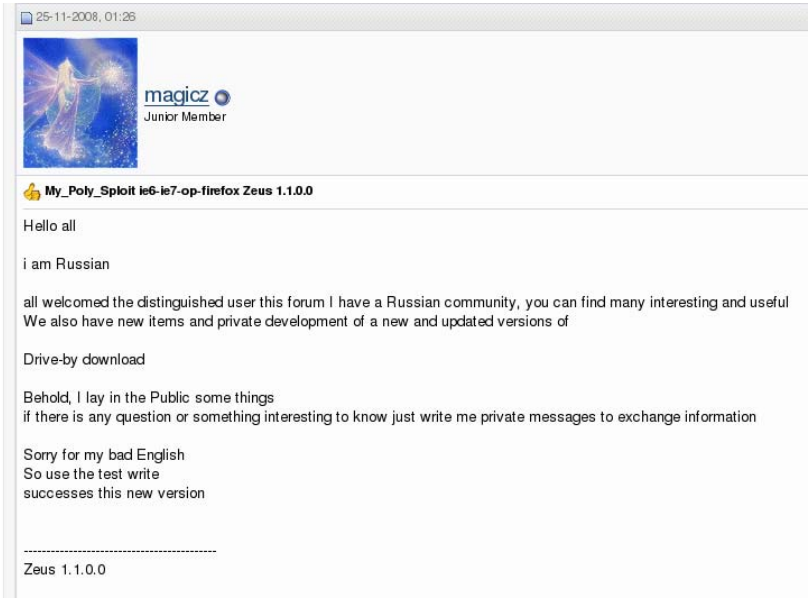
[38] http://rbnexploit.blogspot.com/2007/10/rbn-76service-gozi-hangup-team-and-us.html (visitato l'11.02.2009)

[39] http://www.secureworks.com/research/threats/gozi/?threat=gozi (stato il 11.02.2009)

[40] http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

vati addirittura ad aggiungere delle licenze esclusive per l'utilizzo, come mostrato nel primo rapporto semestrale 2008 di MELANI[41]

Ma non vi è solo la semplice vendita di codici nocivi, il supporto è pure garantito, è solo una questione di prezzo:



[41] http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=it («Professionalizzazione della criminalità su Internet sull'esempio di ZeuS», stato il 12.02.2009)

Che il cybercrime vada verso l'outsourcing o che rimanga un affare per persone che possiedono almeno conoscenze di base nel settore, una cosa è sicura: in un periodo di crisi economica e in una situazione dove il perseguimento penale soffre di diversi problemi, proporre i mezzi per compiere atti criminali attraverso canali di facile accesso per qualsiasi utente della rete, darà un impulso importante al settore durante il 2009.

5.3 Come sbarazzarsi dei rifiuti di dati della società dell'informazione

Lo spazio di memorizzazione sulle apparecchiature elettroniche aumenta a vista d'occhio. Inoltre quasi ogni apparecchiatura elettronica dispone attualmente di una scheda di memoria. La quantità di dati memorizzati accumulata da ogni persona aumenta di continuo. Per ottenere maggiore spazio occorre cancellare i dati non più utilizzati.

La cancellazione corretta dei dati non è però chiara per tutti. La cancellazione dei dati è imprescindibile proprio quando ad esempio si cede ad altre persone l'apparecchio fotografico, il telefono cellulare o lo stick USB. In merito vanno osservate alcune indicazioni e va scelta una procedura adeguata al fabbisogno di protezione dell'informazione e al caso di applicazione concreto.

Il capitolo 7.1 in allegato fornisce alcuni consigli pratici in merito, che possono essere applicati sia in ambito privato, sia dalle imprese. Ne diamo qui una sintesi:

- La mera cancellazione non basta perché così i dati possono essere ripristinati.
- Il metodo di cancellazione dipende dalla confidenzialità dei dati.
- Occorre utilizzare speciali tool di cancellazione (Wipe-Tools).
- Nel caso dei supporti ottici il miglior metodo è la distruzione del supporto.

5.4 I dati di accesso ai servizi Internet viepiù nel mirino della criminalità informatica

Si potrebbe supporre che il problema appartenga ormai al passato da quando in Svizzera il phishing classico è utilizzato in misura minore ai danni della clientela e-banking. Il phishing classico rimane però un problema, come risulta dagli annunci che MELAN e SCIOCI ricevono regolarmente. Tutti i servizi su Internet necessitano di un nome di utente e di una password: così ad esempio nel caso del conto e-mail, dell'accesso ai server dei siti Web, alle piattaforme di asta o di trading come pure all'e-shop. In futuro questi dati saranno viepiù nel mirino della criminalità informatica. Diversamente dai conti di e-banking in questi casi non si effettua un'autentificazione a due fattori: la protezione si limita al login e alla password. I titolari dei conti non costituiscono in genere l'obiettivo. I conti sono soltanto un mezzo per raggiungere l'obiettivo e sono utilizzati abusivamente per la commissione di un reato: sia ad esempio per presentarsi con una personalità diversa, sia per sfruttare il rating elevato di un conto aste o per introdurre infezioni drive-by su pagine Web o ancora per diffondere cavalli di Troia in ambito di e-banking. In questo ultimo caso si ricorre al phishing per diffondere malware che è poi nuovamente diretto contro le applicazioni di e-banking.

In futuro alcuni aspetti di sicurezza non potranno più essere presi in considerazione isolatamente, ma dovranno essere visti e combattuti come un tutto. Ogni singola persona che utilizza od offre un servizio su Internet è parte integrante di questa sicurezza su Internet. Questa consapevolezza ma anche la responsabilità dovranno essere rafforzate nel corso dei prossimi anni. In futuro i provider soprattutto finiranno nel mirino della criminalità informatica.

6 Glossario

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

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	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.
Autentificazione a due fattori	A tal fine sono necessari almeno due dei tre fattori di autenticazione: 1. una cosa che si conosce (ad es. passwort, PIN ecc.); 2. una cosa che si ha (ad es. certificato, token, elenco da cancellare ecc.); 3. una cosa che si è (ad es. impronte digitali, scanner della retina, riconoscimento vocale ecc.)
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.
Agente finanziario	È un agente finanziario chiunque svolge legalmente l'attività di intermediario monetario e quindi anche operazioni di trasferimento finanziario. In tempi recenti questo concetto è utilizzato nel contesto delle transazioni finanziarie illegali.
CA	Certificate Authority (italiano: servizio di certificazione) Un servizio di certificazione è un'organizzazione che rilascia certificati digitali. Un certificato digitale è in un certo qual senso l'equivalente di una carta d'identità a livello di cyberspazio ed è destinato

	all'assegnazione di una determinata chiave pubblica a una persona o a un'organizzazione. Tale assegnazione è autenticata dal servizio di certificazione che provvede a tale scopo apponendovi la propria firma digitale.
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.
ccTLD	Country Code – Top Level Domain Ogni nome di dominio in Internet consta di una sequenza di caratteri separati da punti. La designazione Top Level Domain si riferisce all'ultimo nome della sequenza e costituisce il massimo livello di risoluzione del nome. Esempio: nel caso di http://www.melani.admin.ch il TLD corrisponde a «ch». Se tale TLD è assegnato a un Paese si parla di un ccTLD.
Certificati di server SSL/TLS	Un certificato digitale è in un certo qual senso l'equivalente di una carta d'identità a livello di cyberspazio ed è destinato all'assegnazione di una determinata chiave pubblica a una persona o a un'organizzazione. Tale assegnazione è autenticata dal servizio di certificazione che provvede a tale scopo apponendovi la propria firma digitale.
Command & Control Server	La maggior parte dei bot possono essere sorvegliati da un botmaster e ricevere comandi attraverso un canale di comunicazione. Tale canale di comunicazione è denominato Command and Control Server.
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 l'utente possono utilizzare nomi (ad es. www.melani.admin.ch).
Exploit-Code	(abbr.: Exploit) Un programma, uno script o una riga di codice per il cui tramite possono essere sfruttate le lacune di sicurezza dei sistemi di computer.
Fast Flux	Fast Flux è una tecnica DNS utilizzata dalle reti bot per ripartire e quindi dissimulare su diversi host le pagine phishing o le pagine che diffondono malware. Se un computer subisce un'avaria il computer successivo colma la breccia.
Flash	Adobe Flash (abbr. Flash, già Macromedia Flash) è un ambiente proprietario e integrato di sviluppo per la produzione di contenuti multimediali. Attualmente Flash è utilizzato in numerose applicazioni Web, sia come insegna pubblicitaria, sia come parte di una pagina Web, ad esempio come menu di comando o sotto forma di pagina

	Flash completa.
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.
Funzione hash MD5	Algoritmo che genera costantemente una serie di cifre di uguale lunghezza a partire da qualsiasi testo. Le funzioni hash sono utilizzate in tre settori: • nella crittografia; • nei sistemi di banche dati. Essi le utilizzano per effettuare ricerche più efficienti nelle grandi raccolte di dati delle banche dati; • nelle somme di controllo. Un valore hash può essere attribuito a qualsiasi file. Un valore hash modificato fa presagire una manipolazione.
ICANN	Internet Corporation for Assigned Names and Numbers (ICANN) L'ICANN e un'organizzazione senza scopo di lucro con sede nella cittadina costiera californiana di Marina del Rey. ICANN decide in merito ai principi di gestione dei Top Level Domain. Così facendo ICANN coordina gli aspetti tecnici di Internet, senza peraltro stabilire norme di diritto vincolanti. ICANN sottostà al Dipartimento statunitense del commercio (Department of Commerce) e pertanto al Governo americano.
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.
IRC	Internet Relay Chat Uno dei primi protocolli di chat (senza Instant Messaging).
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 corrispondo-

	no 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 JavaScripts sono supportati da tutti i browser.
Lacune di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
Malware	Termine composto dalle parole inglesi «Malicious» e "Software". Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di Troia.
MoneyGram	MoneyGram International Inc. è un'impresa finanziaria statunitense con sede a Minneapolis, rappresentata sul mercato finanziario. Facendo capo a MoneyGram è possibile trasferire una somma di denaro tra 2 persone effettuando un versamento in una sua filiale.
Peering	Per peering (dall'inglese peer = di pari rango) si intende un collegamento diretto tra reti IP per effettuare lo scambio di dati tra due partner (p. es. tra provider).
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.
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.
Rete bot	Un insieme di computer infettati da Malicious Bot. Essi possono essere interamente comandati a distanza da un aggressore (il proprietario della rete bot). A seconda delle dimensioni, una rete può constare di poche centinaia fino a milioni di elaboratori infettati.
Rootkit	Un insieme di programmi e di tecniche che consentono di accedere inosservatamente a un elaboratore e di assumerne il controllo.
Scheda di memoria Flash	Le memorie Flash sono chip digitali di memoria. Le memorie Flash sono utilizzate ovunque devono essere memorizzate informazioni su uno spazio piccolissimo. Esempi: stick USB, scheda di memoria per apparecchi fotografici digitali, telefoni cellulari, palmari, player MP3.
SHA	Secure Hash Algorithm (inglese per algoritmo hash sicuro) Il concetto di SHA designa un gruppo standardizzato di funzioni crittografiche hash. Esse servono a calcolare un valore univoco di verifica per qualsiasi dato elettronico.

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.
UDP	User Datagram Protocol USP è un protocollo di rete minimo e senza connessioni che fa parte della suite di protocolli di trasporto della famiglia di protocolli Internet. Il compito di UDP è di far pervenire all'applicazione corretta i dati trasmessi via Internet.
Verme informatico	Diversamente dai virus, i vermi informatici non necessitano di un programma ospite per diffondersi. Essi sfruttano piuttosto le lacune di sicurezza o gli errori di configurazione del sistema operativo o delle applicazioni per diffondersi autonomamente da un computer all'altro.
Western Union	Western Union è l'offerente di primo piano a livello mondiale per il trasferimento di denaro e offre la possibilità di trasferire rapidamente denaro, pagare fatture e ricevere ordini di pagamento nel mondo intero.

7 Allegato

7.1 Cancellazione definitiva dei dati dai supporti di dati[42]

Affinché i dati memorizzati non finiscano in mani sbagliate è necessario un modo di procedere regolamentato per cancellare o distruggere i dati e i supporti di dati. Prima di poter riutilizzare i supporti di dati i dati che vi sono memorizzati devono essere completamente cancellati. Questa esigenza è particolarmente importante se i supporti di dati devono essere ceduti a terzi.

Esistono diversi metodi di cancellazione delle informazioni memorizzate sui supporti di dati. La scelta del metodo dipende per l'essenziale dal fabbisogno di protezione dei dati da cancellare, ma ovviamente anche dal genere di supporto di dati. Attualmente si utilizzano i seguenti supporti di dati:

- media magnetici di memorizzazione, come dischi rigidi, dischetti, dischi rigidi rimovibili, dischetti ZIP, nastri magnetici;
- media ottici di memorizzazione (p. es. CD, DVD);
- media elettronici di memorizzazione (p. es. memorie o schede Flash, come stick USB, rispettivamente stick di memoria o altre schede elettroniche di memorizzazione).

[42] I modelli di questa guida sono «Sicheres Löschen von Datenträgern» https://ssl.bsi.bund.de/gshb/deutsch/m/m02167.htm e «Brennpunkt: Minianwendungen sicher nutzen» http://www.bsi-fuer-buerger.de/brennpunkt/index.htm del Bundesamtes für Sicherheit in der Informationstechnik BSI della Germania.

Qui di seguito sono presentate indicazioni e raccomandazioni relative ai principali metodi di cancellazione e di distruzione dei supporti di dati:

Comandi di cancellazione

I comandi di cancellazione sono comandi e funzioni che il sistema operativo mette a disposizione per cancellare i file e le cartelle. Quando si utilizza il comando di cancellazione va osservato che in linea di massima non vengono cancellate effettivamente le informazioni del file, bensì unicamente il rinvio a queste informazioni nell'«indice» del supporto di dati. Il file è ulteriormente disponibile.

Formattazione

Nel caso dei dischi rigidi si opera una distinzione tra formattazione Low-Level, nel cui ambito le piste e i settori sono nuovamente generati, e la formattazione logica o formattazione High-Level, effettuata dal sistema operativo. La formattazione High-Level è inadeguata come procedura di cancellazione perché essa non fa che ricostituire la struttura del sistema dei file.

In passato l'utente poteva effettuare una cosiddetta formattazione Low-Level con riscrittura della struttura magnetica di base. Nel caso dei dischi rigidi moderni questa operazione può essere effettuata in genere dai soli fabbricanti.

Per quanto riguarda i CD-ROM riscrivibili (CD-RW), i dischetti o i supporti analoghi di dati va osservato che la formattazione rapida non cancella i dati. È pertanto necessaria una cancellazione integrale.

Sovrascrittura di singoli file

I dati sui dischi rigidi intatti possono essere cancellati completamente e resi irrecuperabili tramite sovrascrittura con speciali software. In questo caso i dati sono sovrascritti una o più volte da caratteri predefiniti o aleatori. I supporti di dati sono riutilizzabili dopo l'operazione di sovrascrittura. La maggior parte di questi tool offre diverse procedure di sovrascrittura. I metodi noti sono la procedura estremamente sicura, ma anche molta lenta, Peer-Gutmann[43], che sovrascrive 35 volte i dati con serie variabili di cifre. Poi il Russian GOST P50739-95 oppure la procedura DoD 5220.22-M (E), che sovrascrive 3 volte i dati, ciò che nella maggior parte dei casi è sufficiente a livello di uso privato. La procedura adottata in definitiva dipende comunque dalle esigenze personali in fatto di sicurezza.

Esempi di programmi gratuiti che cancellano con sicurezza i dati son «Eraser»[44], «Secure Eraser»[45] e «KillDisk»[46].

Gli utenti esperti possono utilizzare il programma di cancellazione cipher.exe[47], integrato in Windows. Il programma è disponibile in Windows XP e in Windows Vista e cancella i settori senza dati mediante una tripla sovrascrittura.

Ecco le modalità di utilizzazione di cipher.exe:

1. Cancellate tutti i file nel cestino.

[43] http://de.wikipedia.org/wiki/Gutmann-Methode (stato: 02.02.2009).
[44] http://www.chip.de/downloads/Eraser-5.8.6a_12994923.html (stato: 02.02.2009).
[45] http://www.chip.de/downloads/Secure-Eraser_13008545.html (stato: 02.02.2009).
[46] http://www.killdisk.com/ (stato: 02.02.2009).
[47] http://support.microsoft.com/kb/315672/en-us/ (stato: 02.02.2009).

2. Andate su Start/Run e digitate la riga di comando cmd. Si apre una console.
3. Digitate il comando cipher.exe /w:C:\\. C:\\ designa il drive che deve essere ripulito. Il programma sovrascrive unicamente i settori senza dati; in altre parole i vostri file non vengono modificati! Premete il tasto <Enter>
4. Viene ora avviato il processo, che può durare un certo tempo a seconda delle dimensioni del disco rigido.

Attenzione: utilizzando questo tool occorre prendere in considerazione che i contenuti di piccoli file (inferiori a 4 KB) che sono stati cancellati possono rimanere non sovrascrivibili se figurano direttamente nella Master File Table (MFT), per così dire l'indice del disco rigido. cipher.exe non è disponibile in Windows XP Home Edition.

Eliminazione fisica dei supporti di dati

I supporti di dati riscrivibili, ad esempio i CD-RW, possono in linea di massima essere cancellati mediante sovrascrittura integrale. È però teoricamente possibile che rimangano tracce delle vecchie informazioni e che queste possano essere ricostruite. In caso di elevato fabbisogno di protezione anche questi supporti riscrivibili di dati devono pertanto essere distrutti con apposite apparecchiature (Shredder) per rendere illeggibili le informazioni che vi sono memorizzate.

I supporti ottici di dati, ad esempio i CD-R, che non sono riscrivibili , non possono essere cancellati e devono pertanto essere distrutti con apposite apparecchiature (Shredder) per rendere illeggibili le informazioni che vi sono memorizzate.

Nel caso dei dischi rigidi difettosi che non possono più essere sovrascritti la sola procedura di cancellazione è la loro distruzione. La distruzione può essere effettuata con uno Shredder, ma sono adeguate anche le procedure termiche come la combustione o la fusione. Le cassette di nastri magnetici possono essere distrutte meccanicamente o termicamente come i dischi rigidi.

Apparecchiature di cancellazione dei supporti magnetici di dati

Le apparecchiature di cancellazione sono destinate a cancellare i dati bisognosi di protezione memorizzati sui supporti magnetici di dati in maniera tale che tali supporti possano essere successivamente riutilizzati. Le apparecchiature di cancellazione (Degausser) per i supporti magnetici di dati dispongono di un potente magnete a corrente continua o a corrente alternata. All'atto della cancellazione con un'apparecchiatura di cancellazione i supporti di dati sono attraversati dal flusso del campo magnetico dell'apparecchiatura («cancellazione mediante flusso magnetico»).

Va comunque osservato che i dischi fissi e diversi nastri magnetici non possono più essere utilizzati dopo la cancellazione perché unitamente ai dati memorizzati è stata cancellata anche la pista di guida della testina di scrittura/lettura.

Memorie mobili, apparecchi fotografici, telefoni cellulari, ecc.

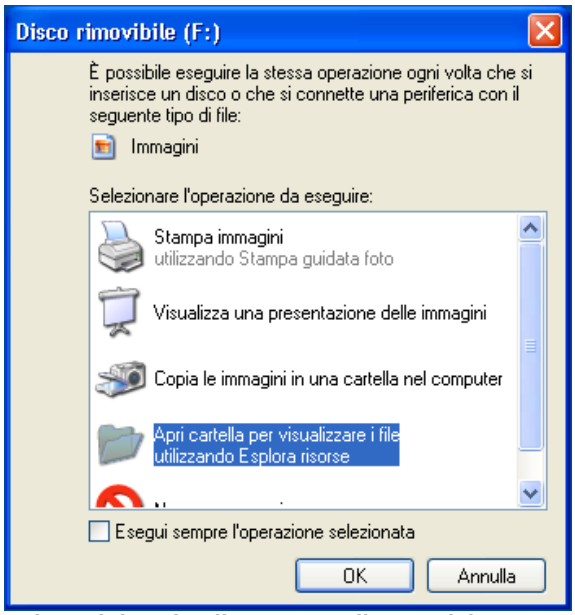
Una particolare attenzione va rivolta ai telefoni cellulari e agli apparecchi fotografici. Questi hanno in genere una breve durata di vita e sono successivamente perlopiù riutilizzati o ceduti a terzi. Ma proprio su questi media di memorizzazione possono inoltre trovarsi informazioni particolarmente confidenziali, come immagini o numeri telefonici personali che non si comunicano volentieri a terzi. Questi media di memorizzazione sono in genere collegati al computer per il tramite della porta USB e vi appaiono come drive. Il drive può allora essere sovra-

scritto con il tool di cancellazione menzionato qui sopra. Se l'apparecchio non può essere collegato al computer non rimane che la distruzione fisica.

- Il metodo di cancellazione dipende dalla confidenzialità dei dati.
- La semplice cancellazione non è sufficiente.
- Così facendo è possibile ripristinare i dati.
- Si devono utilizzare speciali programmi di cancellazione (Wipe-Tools).
- Nel caso dei supporti ottici di dati la miglior soluzione è la distruzione.

7.2 Disattivazione della funzione AutoRun in Windows

La funzione AutoRun dei media di memorizzazione è responsabile dell'avvio di determinate azioni al momento del collegamento del media rimovibile. Queste funzioni possono consistere nella riproduzione automatica o nell'avvio di un menù contestuale. Nel caso della riproduzione automatica viene analizzato il file «Autorun.inf» del media. Questo file stabilisce quali comandi devono essere eseguiti dal sistema. Numerose ditte sfruttano queste funzionalità per avviare programmi di installazione.



Azione tipica al collegamento di uno stick USB

La funzione AutoRun di Windows comporta però anche pericoli. Un numero sempre crescente di parassiti sfruttano le memorie Flash come vettore di diffusione. La funzione AutoRun svolge in questo caso un ruolo centrale. Se questa funzione viene disattivata si raggiunge già un notevole incremento di sicurezza. Purtroppo la disattivazione non è affatto semplice e si deve intervenire sulla banca dati del registro di Windows. La guida qui appresso è destinata a illustrare i passi necessari.

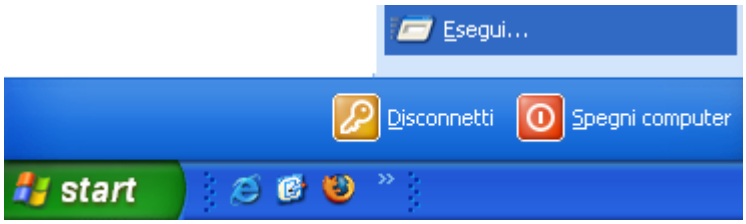
ATTENZIONE: la disattivazione della funzione AutoRun è possibile soltanto dopo l'installazione di un aggiornamento di Windows. Questo aggiornamento non è effettuato automaticamente[48].

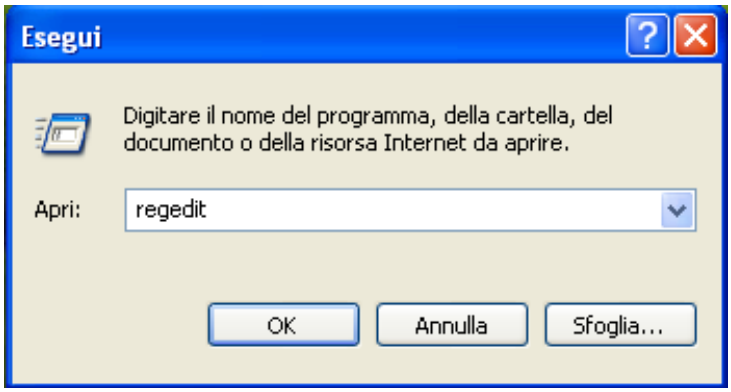
Aggiornamento di Windows XP (KB950582)
http://www.microsoft.com/downloads/details.aspx?FamilyId=CC4FB38C-579B-40F7-89C4-1721D7B8DAA5&displaylang=de
Aggiornamento di Windows Server 2003 per sistemi Itanium (KB950582)
http://www.microsoft.com/downloads/details.aspx?FamilyId=5795F63E-1FD9-4A13-9650-1015E14B6D11&displaylang=de
Aggiornamento di Windows Server 2003 x64-Edition (KB950582)
http://www.microsoft.com/downloads/details.aspx?FamilyId=E8507286-CDF8-4BCB-AFC5-9734FE772C53&displaylang=de
Aggiornamento di Windows Server 2003 (KB950582)
http://www.microsoft.com/downloads/details.aspx?FamilyId=705305E5-7060-4236-B5D2-40CA63A967FB&displaylang=de
Aggiornamento di Windows XP x64-Edition (KB950582)
http://www.microsoft.com/downloads/details.aspx?FamilyId=21A0124C-6F50-4281-923E-E2B28068147A&displaylang=de
Aggiornamento di Windows 2000 (KB950582)
http://www.microsoft.com/downloads/details.aspx?FamilyId=C192EDCF-CA3D-44E3-8ECC-49C5F4DA5405&displaylang=de

Sui sistemi Windows Vista e Windows Server 2008 deve essere installato l'aggiornamento 950582 (bollettino di sicurezza MS08-038 (http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms08-038.mspx) per poter utilizzare la chiave di configurazione del registro destinata alla disattivazione di AutoRun.

Non appena queste condizioni sono adempiute, eseguite i passi qui appresso per disattivare AutoRun.

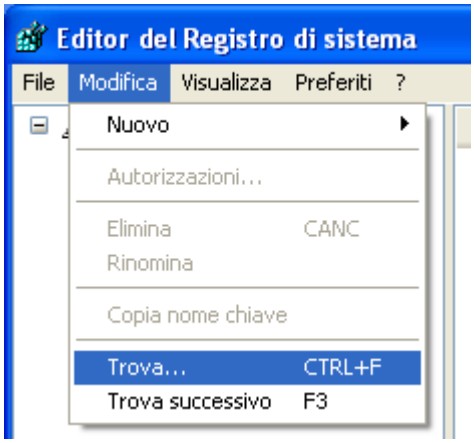
Anzitutto deve esser avviato l'editore del registro. A tale scopo selezionate il menu «Run» e premete il pulsate «Ok» dopo aver digitato «regedit».

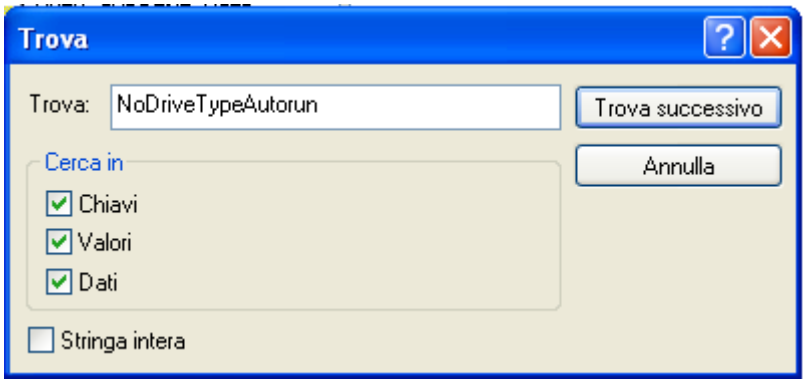


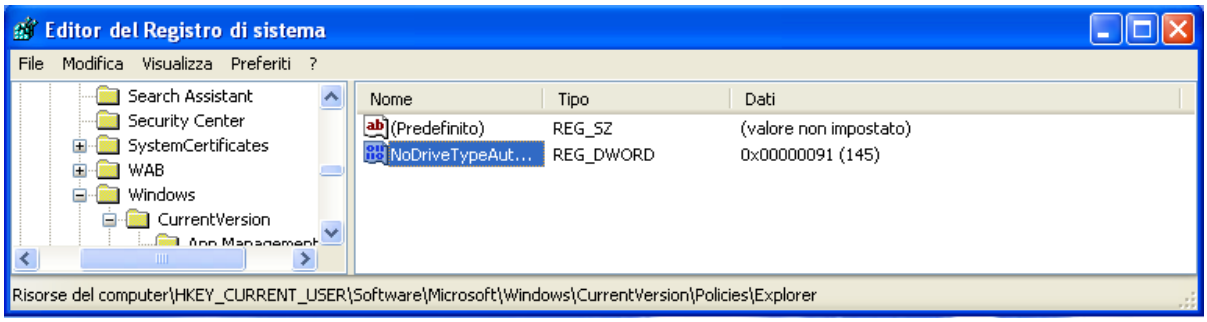


[48] Tutte le informazioni su http://support.microsoft.com/kb/953252/de (stato: 02.02.2009).

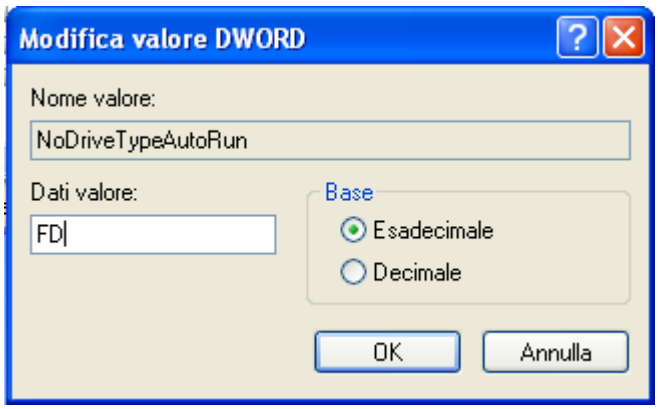
Ora deve essere reperita la corrispondente chiave «NoDriveTypeAutoRun», che controlla la funzione AutoRun. A tale scopo avviate la ricerca nell'editore del registro.







Non appena trovate la chiave, aprite il seguente campo di dialogo effettuando un doppio clic sulla chiave:



Introducendo il valore esadecimale «FD» si disattivano le funzioni AutoRun di tutti i drive.

ATTEZIONE: Questa configurazione vale per il solo utente attuale.

È possibile definire una configurazione d'utente con l'ausilio della tabella qui appresso. Potete stabilire esattamente quali tipi di drive devono utilizzare o no la funzione AutoRun.

Nella tabella qui sotto sono indicati i singoli drive. Osservate che a causa della loro formattazione gli stick USB sono in genere classificati come supporti rimovibili di dati, mentre i dischi rigidi USB sono classificati come dischi rigidi.

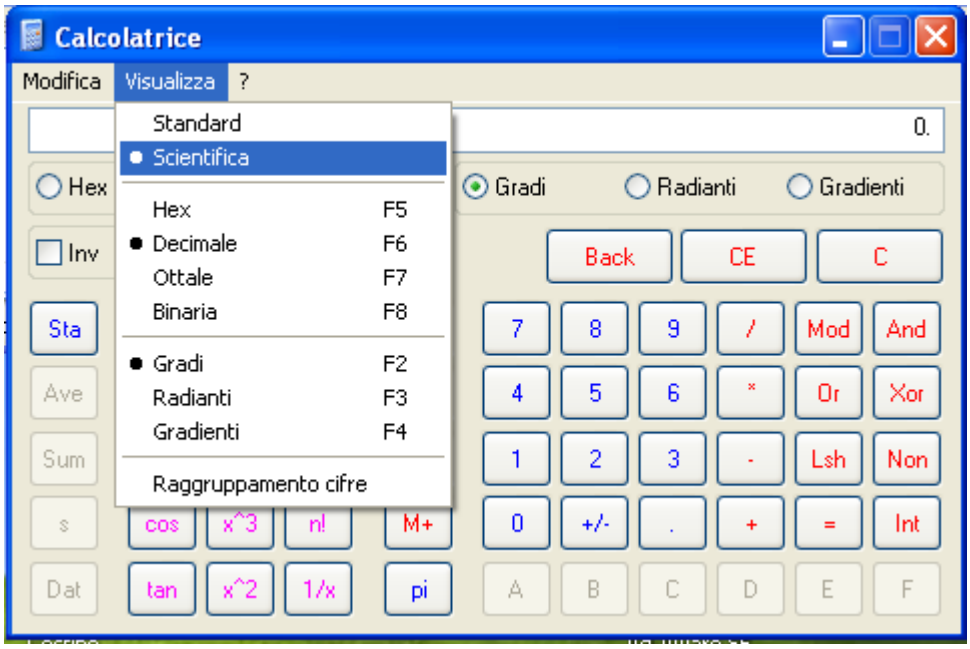
Se intendete attivare AutoRun digitate «0» nella colonna corrispondente. Digitate invece «1» se AutoRun deve essere disattivato. Nelle rubriche «Riservato» e «Disco estraneo» dovrebbe sempre figurare un «1», mentre nella rubrica «Drive senza root» dovrebbe sempre figurare uno «0».

Questi numeri iscritti in successione formano il cosiddetto valore binario della configurazione desiderata.

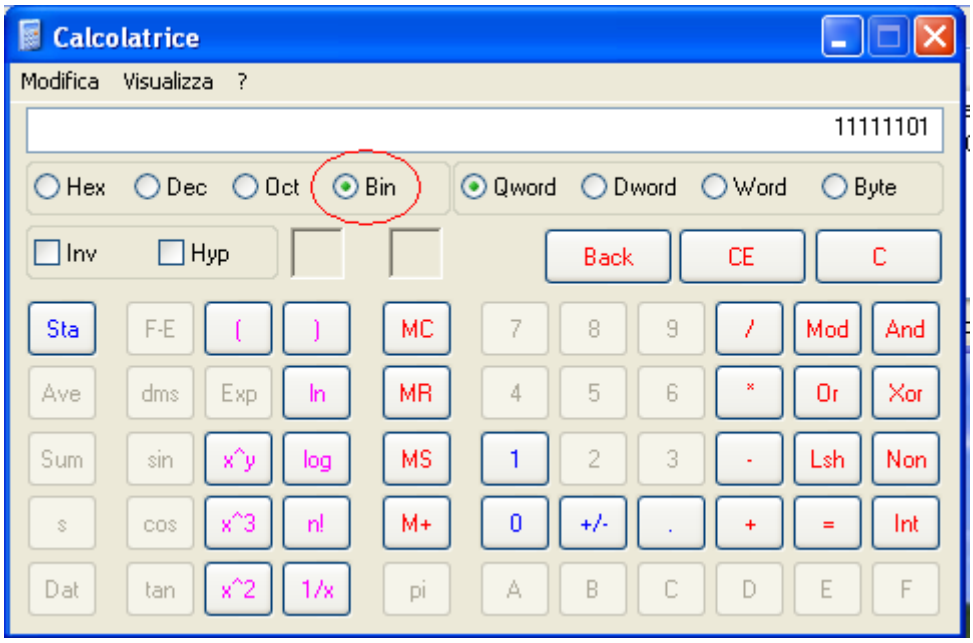
Riservato	Disco Ram	Drive CD-Rom	Drive di rete	Disco fisso	Disco rimovibile	Drive senza root	Drive estraneo	Valore binario
1	1	1	0	1	1	0	1	11101101
1	0	0	0	0	0	0	1	10000001
1						0	1	

Tabella di generazione del valore binario della funzione AutoRun. La configurazione 1 disattiva i dischi fissi e gli stick USB, mentre la configurazione 2 autorizza la funzione AutoRun su tutti i tipi di drive. Nell'ultima riga potete raggruppare i vostri propri valori binari

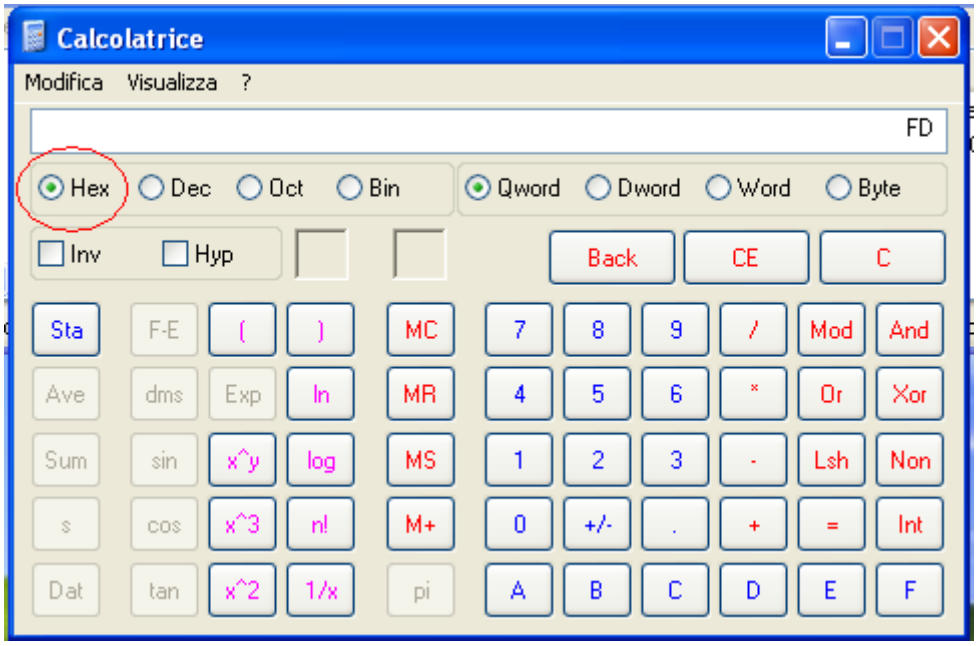
Successivamente questo valore binario deve essere convertito in un valore esadecimale. A tale scopo potete avviare la calcolatrice nel modo scientifico.



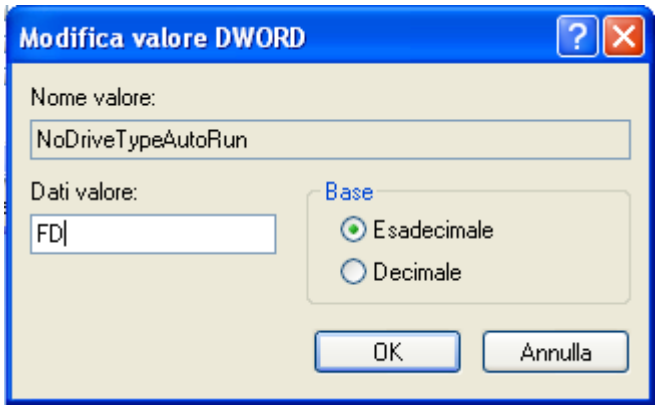
Selezionate in seguito il modo binario e digitate il valore binario che avete generato nella tabella qui sopra.



Selezionate ora il modo HEX: il valore binario sarà convertito automaticamente.



Ora potete immettere questo valore nell'editore del registro.



7.3 Le lacune del DNS e della MD5

Nel quadro del 25° Chaos Communication Congress (25C3) un gruppo internazionale di ricercatori che ha collaborato con il PFL ha dimostrato come le note vulnerabilità della funzione crittografica hash MD5 a livello di resistenza alle collisioni possano essere sfruttate per conseguire il possesso di un certificato CA affidabile (http://www.win.tue.nl/hashclash/rogue-ca/). Un siffatto certificato potrebbe ad esempio essere utilizzato per emettere un numero qualsiasi di certificati di server SSL/TLS in vista di un attacco di phishing su vasta scala. Per l'essenziale si dovrebbero allestire due richieste di certificato: una richiesta di certificato di utente e una richiesta di certificato CA. I dati di entrambe le richieste, ossia i dati che sono iscritti in definitiva nei certificati, sono creati in maniera tale da collidere in MD5, nel senso che entrambi i certificati hanno il medesimo valore hash MD5 e quindi anche la stessa firma. Se il certificato di utente viene firmato da un CA affidabile, il certificato CA può essere emesso con l'ausilio di questa firma e senza che debba nuovamente intervenire il CA affidabile.

Questo certificato sarà successivamente accettato dai browser di uso commerciale senza feedback all'utente.

Dal profilo teorico il risultato di questa ricerca è interessante nella misura in cui viene fornita per la prima volta la prova che le vulnerabilità di MD5 a livello di resistenza alle collisioni note fin dal 2004 possono essere sfruttate abusivamente in vista di attacchi reali. Dal profilo pratico il risultato è meno spettacolare, perché ormai sono pochi i CA che utilizzano ancora MD5. Questa tendenza ad allontanarsi da MD5 in direzione di SHA-1 o di funzioni hash ancor più resistenti alle collisioni (in particolare SHA-2 e in futuro SHA-3) si rafforzerà ulteriormente fin d'ora. Nondimeno la resistenza alle collisioni delle funzioni hash utilizzate non è il solo tallone d'Achille nell'uso dei certificati. Attualmente molti attacchi poggiano sul fatto che non viene utilizzato alcun certificato oppure un certificato analogo, ma falsificato: gli utenti lo accettano e ignorano l'avvertimento a causa dei frequenti messaggi simili generati dai browser. Questi attacchi non sono meno efficaci e comportano costi sensibilmente minori per gli aggressori.

Ad inizio anno, il ricercatore ed esperto di sicurezza Dan Kaminsky[49] ha scoperto una grave falla nel sistema DNS. Il senso di responsabilità del ricercatore l'ha portato a contattare i maggiori attori del settore (come Microsoft, Cisco e altri) e cercare insieme a loro una soluzione per ovviare al problema. Dopo sei mesi di lavoro, l'8 luglio del 2008 è stata distribuita una patch: si è trattato in sostanza del maggiore aggiornamento di sicurezza contemporaneo della storia di Internet.

Sebbene il DNS cache poisoning avesse già posto dei problemi in passato (ovviati attraverso un algoritmo che genera i QID delle richieste in modo aleatorio), Kaminsky ha trovato una forma di cache poisoning molto più inquietante. «Alzandosi» di livello, quest'attacco poteva essere portato contro gli Authority records, permettendo a un criminale potenzialmente di «deviare» il flusso di informazioni (http, email e altro) per una data zona (un nome di dominio ad esempio) verso un server appositamente preparato. Per ovviare questo problema si è reso necessario fornire la source port (la porta di uscita UDP del nameserver) in modo aleatorio[50].

7.4 Service provider: dopo McColo il vento soffia a est

Erano le 19:30 (EST) dell'11 novembre 2008 quando, secondo il rapporto CIDR[51], il provider Hurricane Electric (HE) smise di eseguire il routing per McColo (de-peered).

McColo[52] fu un hosting provider americano tristemente famoso per aver ospitato una gran quantità di attività illegali, come siti web di prodotti farmaceutici o server di gestione (Command&Control, C&C) di alcune delle maggiori reti bot[53]. A seguito degli elementi raccolti dal-

[49] http://www.doxpara.com

[50] Una spiegazione di facile comprensione la si può trovare all'indirizzo seguente (in inglese): http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html (stato il 13.02.2009)

[51] http://www.cidr-report.org/cgi-bin/as-report?as=AS26780 (stato il 17.12.2008)

[52] http://web.archive.org/web/*/http://www.mccolo.com/

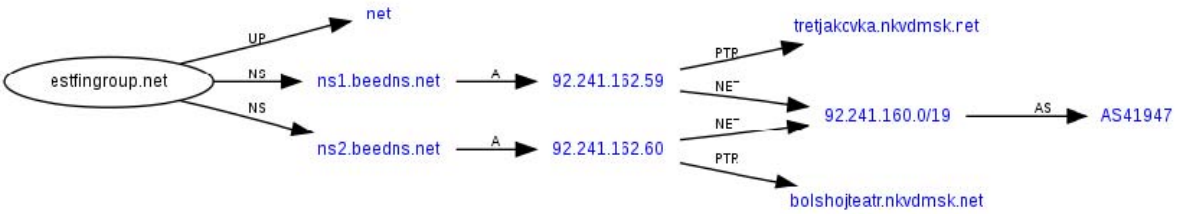
[53] http://voices.washingtonpost.com/securityfix/2008/11/the_badness_that_was_mccolo.html (stato il 17.12.2008), l'ottimo rapporto su McColo di Hostexploit.com: http://hostexploit.com/downloads/Hostexploit%20Cyber%20Crime%20USA%20v%202.0%201108.pdf (stato il 17.12.2008)

la comunità di sicurezza informatica[54] e soprattutto dal Washington Post[55], elementi inviati dal giornalista Brian Krebs ai provider di McColo, HE decise di staccare la spina al suo cliente. Lo stesso Krebs il giorno seguente pubblicò un articolo in cui fu mostrata la drastica diminuzione del volume di spam a livello mondiale[56].

Ebbene, una volta tolto McColo dalla scena degli Internet Service Provider che si mettono a disposizione del crimine, quali sono le conseguenze a medio termine? Se a corto termine, quindi nei giorni seguenti il depeering diverse fonti hanno registrato una sensibile diminuzione di spam a livello mondiale, a medio termine, quindi dopo un paio di settimane, si sono incominciate a registrare rinnovate attività[57]. Non più a ovest negli Stati Uniti, ma a est, in paesi come la Russia o l'Estonia[58].

Ma le reti bot non sono le uniche ad aver trovato una nuova casa in Russia e nei paesi limitrofi. Alla fine di novembre del 2008, un'ondata di spam ha invaso la Confederazione con lo scopo di reclutare persone disposte a riciclare denaro per conto dei gruppi criminali che durante il 2008 hanno attaccato i sistemi e-banking delle banche svizzere[59]. L'email era firmato dalla fantomatica società estfingroup.net.

L'URL estfingroup.net ha come NS beedns.net agli indirizzi 92.241.162.59 e 92.241.162.60. Il routing di questi indirizzi ci porta all'AS41947, appartenente alla società Webalta Wahome Networks.



[54] http://www.secureworks.com/research/threats/warezov/ (stato il 17.12.2008), http://blog.fireeye.com/research/2008/10/mccolo-hoting-srizbi-cc.html (stato il 17.12.2008), http://www.threatexpert.com/report.aspx?uid=745bcad4-9f9d-4a32-ba95-7cb7d5fc14f8

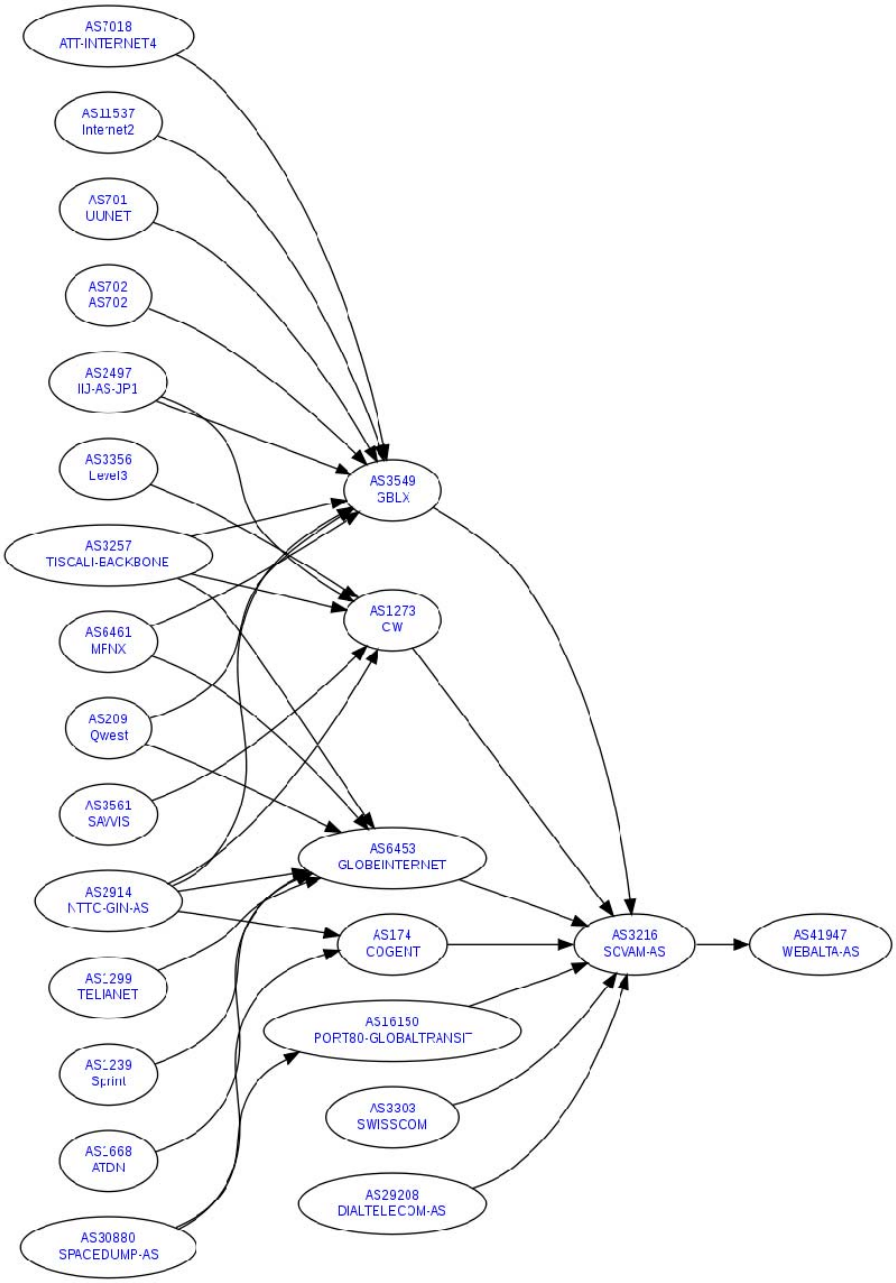
[55] http://voices.washingtonpost.com/securtiy/2008/11/major_source_of_online_scams_a.html (stato il 17.12.2008)

[56] http://voices.washingtonpost.com/security/2008/11/spam_volumes_drop_by_23_after.html (stato il 17.12.2008), http://www.securityfocus.com/brief/855 (stato il 17.12.2008)

[57] http://www.theregister.co.uk/2008/11/18/short_mccolo_resurrection/ (stato il 17.12.2008)

[58] http://blog.fireeye.com/research/2008/11/rustocks-new-home.html (stato il 17.12.2008) e http://blog.fireeye.com/research/2008/11/its-srizbi-trun-now.html (stato il 17.12.2008)

[59] http://www.melani.admin.ch/dienstleistungen/archiv/01073/index.html?lang=de (stato il 16.02.2009)



Webalta.ru è un service provider russo che ospita numerose attività criminali. Presso Spamhaus questa società ha attualmente più di una decina di SBL Advisories (SBL59981, SBL64756, SBL66771, SBL69825, SBL70442, SBL70445, SBL71946, SBL71948, SBL71955, SBL71957, 72319, SBL72604, SBL72607), soprattutto per quanto riguarda l'hosting di Botnet C&C, di drop server di diversi codici nocivi, di invio di spam e di siti web che veicolano infezioni. Una breve ricerca ci porta a diversi risultati utili per quanto riguarda i domini criminali ospitati da Webalta[60]. Alcuni esempi sono forniti nella lista sottostante:

[60] http://www.spamhaus.org/sbl/sbl.lasso?query=SBL69825 (stato il 16.02.2009), http://msmvps.com/blogs/hostsnews/archive/2008/11/10/1653730.aspx (stato il 16.02.2009), http://www.forumpostersunion.com/showthread.php?t=3356 (stato il 16.02.2009),

77.91.229.38 try-count .net
77.91.229.55 v2statscount .net
77.91.229.55 v2count .net
77.91.229.55 pluscount .net
77.91.229.55 newv2count .net
92.241.163.27 adv-a-v .com
92.241.163.27 a-a-v-2008 .com
92.241.163.27 aav2008 .com
92.241.163.30 wi-a-v .com
92.241.163.30 wav2008 .com
92.241.163.30 windows-av .com
92.241.163.31 uav2008 .com
92.241.163.32 spypreventers .com
92.241.163.32 sp-preventer .com
92.241.163.33 download.wi-a-v .com
92.241.163.33 download.wav2008 .com
92.241.163.33 download.uav2008 .com
92.241.163.33 download.adv-a-v .com
92.241.163.33 download.a-a-v-2008 .com
92.241.163.33 download.aav2008.com
92.241.163.33 download.windows-av .com
92.241.163.33 download.spypreventers .com
92.241.163.33 download.sp-preventer .com
92.241.163.34 secure2.softpaydirect .com
92.241.163.34 secure.softpaydirect .com
92.241.163.90 piterserv .com
91.208.0.220 rapidantivirus .com
91.208.0.223 microantivirus-2009 .com
91.208.0.223 microantivirus2009 .com
91.208.0.223 microantivir2009 .com
91.208.0.223 microantivir-2009 .com
91.208.0.223 micro-antivir-2009 .com
91.208.0.224 soft-traff6 .com
91.208.0.224 soft-traff5 .com
91.208.0.224 soft-traff4 .com
91.208.0.224 soft-traff3 .com
91.208.0.224 soft-traff2 .com
91.208.0.224 soft-traff .com
91.208.0.228 scanner.ms-scanner .com
91.208.0.228 scanner.msscanner .com
91.208.0.228 scanner.ms-scan .com
91.208.0.229 msantivirus-xp.com
91.208.0.239 winxsecuritycenter .com
91.208.0.240 download.vav2008 .com
91.208.0.240 vav2008 .com
91.208.0.241 winsafer .com
91.208.0.244 software-traffic .com
91.208.0.244 software-traff .com
91.208.0.246 scanner.vav-x-scanner .com
91.208.0.246 scanner.vav-scanner .com
91.208.0.246 scanner.vav-scan .com
91.208.0.246 scanner.vavscan .com
91.208.0.246 scanner-pwrantivirus .com
91.208.0.249 watcher-scan .com
91.208.0.249 scanner2.defender-scan .com
91.208.0.251 scanner.win-x-defenders .com
91.208.0.251 win-x-defenders .com
91.208.0.251 win-x-defender .com

Sebbene il depeering di McColo sia stato salutato da molti come un successo, resta ancora molto da fare. Abbiamo dimostrato come le attività criminali e i loro attori riescano a ristrutturarsi in pochi giorni da un'importante battuta d'arresto. Sebbene sia ovvio, bisogna sottolineare che la cooperazione internazionale è l'unico modo per combattere questo tipo di crimine. Iniziative come quelle di ICANN per valutare il miglior modo di procedere per combattere i fast flux illegali[61] sono da sostenere: la via della collaborazione è l'unica praticabile.

[61] http://www.icann.org/en/public-comment/#ff-initial (stato il 16.02.2009)