Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

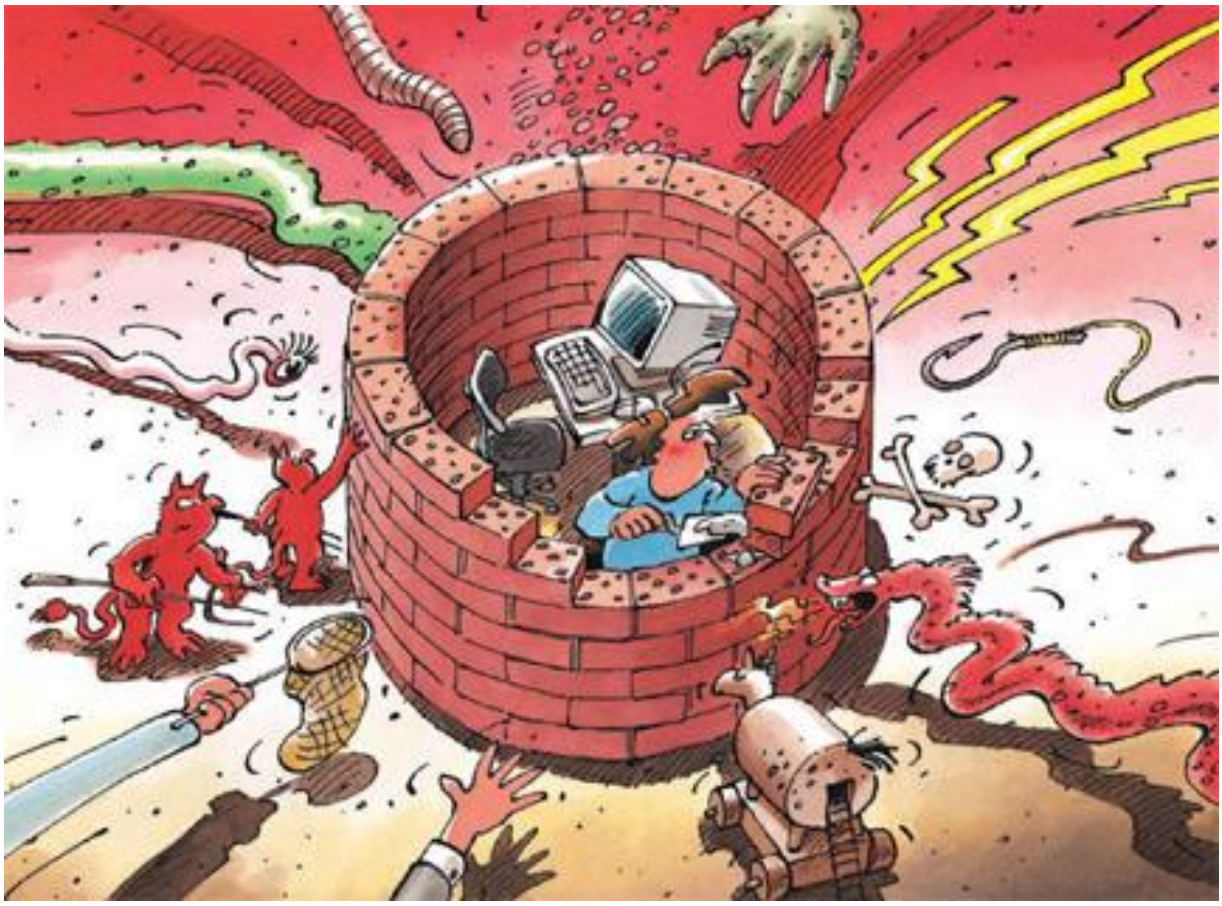
Centrale d'annuncio e d'analisi per la sicurezza dell'informazione
MELANI

www.melani.admin.ch

Sicurezza dell'informazione

Situazione in Svizzera e a livello internazionale

Rapporto semestrale 2009/I (gennaio – giugno)



Indice

1 Cardini dell'edizione 2009/I

- **Avanzata delle infezioni drive-by**
  Come già accennato nell'ultimo rapporto semestrale, si delinea uno spostamento dei vettori di attacco (dagli e-mail con allegati o link) verso infezioni di pagine Web – le cosiddette infezioni drive-by. Le vie di propagazione classiche dei malware non sono pertanto più così efficaci perché gli utenti reagiscono in maniera più sensibile e gli allegati di apparenza sospetta sono aperti con minore frequenza. Secondo le indicazioni della ditta di sicurezza Scansafe, nel terzo trimestre del 2009 il 74 per cento dei software nocivi è stato diffuso tramite pagine Web.
  ► Situazione attuale in Svizzera: capitolo 3.2
  ► Tendenze 5.4
  ► Misure di difesa Allegato 7.2

- **Il dibattito sulla sicurezza dei sistemi SCADA è sempre più ampio**
  La sorveglianza, il controllo e il comando di impianti industriali, di sistemi di distribuzione di beni di importanza vitale (corrente elettrica, acqua, combustibili, ecc.) o nel settore dei trasporti e del traffico (ferrovie, sistemi di direzione del traffico, posta, ecc.) sono da tempo impensabili senza l'impiego di tecnologie dell'informazione e della comunicazione (TIC). Lo sviluppo e l'esercizio di sistemi di sorveglianza, di controllo e di comando (in inglese: Supervisory Control and Data Acquisition, SCADA) vanta una lunga tradizione. Per questo motivo il dibattito sulla sicurezza dei sistemi SCADA guadagna terreno. È ovvio che siffatti sistemi sono di importanza centrale per il funzionamento della nostra società. I pericoli non provengono unicamente dagli attacchi di hacker (sabotaggi), bensì anche da avarie tecniche.
  ► Situazione attuale in Svizzera: capitolo 4.3
  ► Tendenze 5.2

- **Cloud Computing e Information Ownership**
  Il 17 maggio 2009 gli elettori svizzeri hanno approvato a una maggioranza risicata del 50,1 per cento l'introduzione del passaporto biometrico. Oltre che dai dubbi in ambito di protezione dei dati, sembra che l'esito di misura della votazione sia stato determinato soprattutto da un argomento legato alla sicurezza dell'informazione.
  ► Tendenze 5.1

- **Truffa in ambito di anticipi e trappola abbonamenti**
  Continuano a essere annunciati a MELANI e SCOCI i più svariati casi di truffa in ambito di anticipi, presunte vincite a lotterie e offerte gratuite. Questo genere di criminalità informatica è apparentemente ancora troppo efficace.
  ► Tendenzen 5.2

- **Conficker**
  Nel corso dell'ultimo semestre il verme informatico Conficker è stato uno dei principali argomenti IT nei media. L'interesse dei media si è enormemente amplificato soprattutto verso il 1° aprile 2009, quando il worm avrebbe dovuto aggiornarsi. A dire il vero nessuno si aspettava più una simile eruzione; ciononostante Conficker si è propagato in maniera estremamente efficace.
  ► Capitolo 4.2

2 Introduzione

L'ottavo rapporto semestrale (gennaio – giugno 2009) della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) espone 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, i principali sviluppi in ambito di prevenzione e una sintesi delle principali attività degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (*termini in corsivo*) sono riunite in un **glossario** (**capitolo 6**) alla fine del presente rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate con un colore.

I temi scelti del presente rapporto semestrale sono accennati al **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 prima metà del 2009. Il capitolo 3 tratta in merito tematiche nazionali, mentre il capitolo 4 si concentra sulla situazione internazionale.

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

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

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Gozi – nuovo cavallo di Troia propagato con e-mail di spam

Fin dal dicembre del 2008 la criminalità informatica ha tentato di prendere piede in Svizzera con la famiglia di cavalli di Troia Gozi alias Infostealer.Snifula. Si tratta nella fattispecie della terza famiglia di cavalli di Troia diretta contro l'e-banking, che ha nel mirino la clientela degli istituti finanziari svizzeri.

Mediante un e-mail di spam dal contenuto ambiguo[1] si tentava a quell'epoca di attirare le vittime potenziali su siti pornografici appositamente predisposti. Su queste pagine Internet l'utente veniva poi sollecitato a scaricare e a installare un cosiddetto *plug-in Flash* per poterne osservare i contenuti visuali. Questo plug-in Flash celava un cavallo di Troia contro l'e-banking.

Nel mese di gennaio di quest'anno sono state osservate diverse ondate di spam volte alla propagazione del medesimo tipo di cavallo di Troia. A tale scopo si veniva di volta in volta diretti a una pagina falsificata del quotidiano gratuito «20 Minuten». Questa pagina è stata copiata nella proporzione 1 a 1 e poteva pertanto essere smascherata solo in base all'indirizzo Web. Nell'e-mail di spam sono pure stati utilizzati estratti di articoli di «20 Minuten». Per questo motivo quella parte dell'e-mail era redatta in un tedesco corretto. Le parti modificate, rispettivamente aggiunte, erano invece scorrette.
I titoli si riferivano all'estensione del libero passaggio delle persone alla Bulgaria e alla Romania. Trattandosi di tematiche specificamente svizzere, questa circostanza consente di concludere una diffusione estremamente mirata degli e-mail.

```
Von: ZURICH Kontakt [mailto:alarm@20min.ch]
Betreff: ZURICH ALARM:2007 wurden erst 203 Einsteigerinnen aus den osteuropaischen
Staaten registriert.

ZÜRICH

50 Prozent mehr Ost-Prostituierte
Die Zahl der Prostituierten aus Osteuropa wächst rasant: Von dort stammt fast die Hälfte
der Frauen, die 2008 von der Stapo Zürich neu registriert worden sind.

Bis ins Einzelne>>
Mit den herzlichen Grüßen, Roseann Mansfield.
```

E-mail di spam sul tema del libero passaggio delle persone

[1] http://www.melani.admin.ch/dienstleistungen/archiv/01074/index.html?lang=it (stato: 21.08.2009).

Pagina falsificata del giornale «20 Minuten». Per visionare il video si è sollecitati a installare un plug-in Flash.

L'articolo di «20 Minuten» utilizzato da questo e-mail di spam è stato pubblicato la domenica sera alle ore 22:18. Gli e-mail di spam sono stati inviati già dall'indomani a mezzogiorno. Le ondate di spam si sono poi succedute il martedì e il mercoledì. Il contenuto era di volta in volta identico, ma i domini sui quali le pagine erano raggiungibili erano diversi ad ogni ondata. Le pagine erano ospitate su un cosiddetto «*fast flux network*», il che significa che ogni pagina è memorizzata in maniera ridondante su più server[2]. Se uno dei server è fuori uso la richiesta è automaticamente inoltrata a quello successivo. In tal modo se ne complica la disattivazione e si proroga il tempo durante il quale è possibile eseguire un attacco efficace. La totalità dei domini è stata registrata presso un registro in Cina, ma questo non dà indicazioni sulla provenienza degli autori.

Nella fattispecie si tratta per il momento dell'ultima grande ondata di e-mail che ha propagato cavalli di Troia contro l'e-banking. Apparentemente costi e utili non erano più in sintonia perché il profitto tratto dai computer compromessi con le ondate di spam è stato troppo esiguo. Dal mese di gennaio gli attacchi contro l'e-banking con cavalli di Troia sono in forte regresso. Gli aggressori sono viepiù passati ad altri modelli di affari, come il *rogue software*. Si tratta di un malware che dà a intendere di avere rintracciato parassiti su un computer e di poterli eliminare unicamente con la sua versione a pagamento. Ci si avvale inoltre sempre più del vettore di attacco dell'*infezione drive-by* (cfr. in merito il capitolo 3.2.) Troverete più ampie informazioni sulle reti fast flux nel rapporto MELANI 2007/2.[2]

[2] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it (stato 31.08.2009)

3.2 Avanzata delle infezioni drive-by

Come già accennato nell'ultimo rapporto semestrale, si delinea uno spostamento dei vettori di attacco (dagli e-mail con allegati o link) verso infezioni di pagine Web – le cosiddette infezioni drive-by. Le vie classiche di propagazione del malware non sono pertanto più così efficaci perché gli utenti reagiscono in maniera più sensibile: non si clicca più su ogni link ricevuto per e-mail e si aprono con minore frequenza gli allegati di apparenza sospetta. Secondo le indicazioni della ditta di sicurezza Scansafe[3], nel terzo trimestre del 2009 il 74 per cento dei software nocivi è stato diffuso tramite pagine Web. Un rapporto della ditta Websense indica che delle 100 pagine più popolari esaminate, 70 contenevano, o hanno contenuto per breve tempo, software nocivi o erano utilizzate dalla criminalità informatica[4] [5].

I motori di ricerca svolgono un ruolo non trascurabile nelle infezioni drive-by. Si tenta tra l'altro di compromettere le pagine Web che godono di un rating elevato nei concetti popolari di ricerca e che sono inoltre mal protette oppure presentano lacune di sicurezza. L'infezione drive-by comporta talvolta anche un'analisi del *referrer*: in questi casi l'infezione drive-by viene inserita soltanto quando si accede alla pertinente pagina via un motore di ricerca. L'amministratore della pagina Web, che nella maggior parte dei casi chiama direttamente la pagina, ha quindi grande difficoltà a individuarne la compromissione. Nel caso dell'attacco drive-by divenuto noto con il nome di Gumblar e osservato nel mese di maggio di quest'anno, il cavallo di Troia manipola i risultati delle ricerche Google visualizzate nel browser della vittima, che in tal modo è indotta a navigare su altre pagine pericolose, aggravando così il rischio di un'ulteriore infezione.

Le evoluzioni nel settore delle infezioni drive-by sono notevoli (cfr. capitolo 5.4 Tendenze). Ciò che è invece identico per tutti gli attacchi di questo genere è il fatto che deve anzitutto essere trovato un server Web adatto attraverso il quale propagare l'infezione. Gli aggressori penetrano pertanto in server Web esistenti per collocarvi il loro codice nocivo. A tale scopo si avvalgono di password *FTP* rubate oppure sfruttano le lacune di sicurezza del software del server. Sono particolarmente minacciati i *Content Management Systems (CMS)*, ma offrono aree di attacco anche i forum e i registri degli ospiti non senza le relative banche dati. In questo contesto vale la pena menzionare che nel caso dello sfruttamento di una lacuna di sicurezza non è solitamente colpita soltanto una singola pagina Web, ma anche altre pagine Web ospitate sul medesimo server.

L'attacco stesso è perpetrato in più fasi. Sulla pagina violata dall'hacker si trova un *code* che agendo nell'ombra dirotta il visitatore su un server terzo. Nella maggior parte dei casi il dirottamento è operato per mezzo di *IFrame*, sovente generato tramite uno *JavaScript*. In futuro ci si deve parimenti attendere un maggior numero di reindirizzamenti automatici, i cosiddetti *META-Refreshes*, o aggiornamenti di metadati (cfr. capitolo 5.4, Tendenze). Il camuffamento con JavaScript ha lo scopo di ostacolare il rintracciamento di simili infezioni (ad esempio con programmi antivirus). Nel frattempo gli IFrames vengono però anche collocati direttamente sulla pagina, perché questo modo di procedere è più discreto se si considera l'ampia sensibilizzazione su JavaScript come vettore di attacco. Non appena la vittima è stata dirottata nelle fasi successive si verifica quali programmi sono installati sul computer e se si tratta di versioni non aggiornate che presentano lacune di sicurezza. In questo caso nel computer si introduce un malware predisposto su misura per questa lacuna

[3] http://www.scansafe.com/resources/global_threat_reports2/gtr_2008/Q3_2008_GTR.pdf (stato: 31.08.2009).

[4] http://securitywatch.eweek.com/exploits_and_attacks/most_popular_sites_were_hacked_in_08.html (in inglese, stato: 31.08.2009).

[5] http://securitylabs.websense.com/content/Assets/WSL_ReportQ3Q4FNL.PDF (in inglese, stato: 31.08.2009).

di sicurezza che infetta il sistema. Queste lacune non concernono affatto il solo browser, ma anche i relativi *plug-in di browser* come Flash e Acrobat Reader, oppure una lacuna critica di un elemento di controllo ActiveX (*ActiveX control*) ecc. Se non dovessero esserci lacune appropriate, si sollecita l'utente affinché installi manualmente il programma nocivo.

Migliorano celermente le tecniche di collocamento non identificabile il più a lungo possibile di infezioni drive-by su una pagina Web. Questa evoluzione è illustrata al capitolo 5.4.

Per proteggere il vostro computer dalle infezioni drive-by leggete il capitolo «Contromisure» dell'allegato 7.2.

3.3 Utilizzazione abusiva di conti svizzeri di e-mail

Nel suo ultimo rapporto semestrale MELANI ha rammentato che i dati di accesso ai servizi Internet sono viepiù nel mirino della criminalità informatica. Nella fattispecie si trattava soprattutto del collocamento di infezioni drive-by sulle pagine Web, rispettivamente dell'utilizzazione abusiva di conti di aste. Sono stati abbordati anche i tentativi di phishing ai danni dei fornitori di servizi di messaggeria elettronica come Bluewin, Hotmail ecc. Non è però stato illustrato tutto ciò che può essere combinato con un account e-mail derubato. Molte persone potranno pur considerare indifferente per se stesse che un terzo acceda ai loro account e che gli e-mail che ricevono non siano veramente confidenziali. Dietro tutto questo si cela però molto di più: anche in questo caso l'impulso che motiva i criminali è il denaro. Un caso reale accaduto in Svizzera illustra com'è possibile fare denaro con i dati di accesso derubati alla messaggeria elettronica:

Nel mese di giugno del 2009 con i dati di accesso rubati si è acceduto al conto di messaggeria elettronica di un cittadino svizzero e a tutti i suoi 350 contatti è stato inviato un e-mail secondo cui esso si trovava in difficoltà nel corso del suo presunto viaggio in Africa dopo il furto del passaporto, del denaro e di tutti i documenti. Per lasciare l'albergo aveva urgentemente bisogno di 1000 euro per il pagamento della relativa fattura e di altri 100 euro per il pagamento della fattura telefonica. Avrebbe poi ovviamente rimborsato integralmente l'importo non appena rientrato in Svizzera. Il denaro doveva essere trasferito ad Abidjan, a mezzo Western Union, a una persona ignota al destinatario dell'e-mail. A causa delle circostanze non era possibile raggiungerlo telefonicamente.

In questo caso non si è verificato alcun danno grazie allo scetticismo dei destinatari dell'e-mail, che prima di trasferire il denaro richiesto hanno voluto una conferma telefonica dal loro amico in difficoltà, e grazie alla notifica alla Western Union.

In conclusione, a essere interessato non è tanto il conto di messaggeria elettronica di un'unica persona, quanto tutti i suoi contatti. In futuro non si raccoglieranno unicamente gli indirizzi di e-mail, ma saranno anche rilevati con scrupolosa precisione i contatti. L'obiettivo è di adeguare possibilmente su misura l'e-mail alla potenziale vittima. Poiché il dispendio corrispondente è elevato, questo modo di procedere è stato finora osservato solo in singoli casi di attacchi estremamente mirati. Il dispendio però diminuisce se queste associazioni sono effettuate automaticamente e in grande stile, ragione per la quale ci si deve aspettare che questa tecnica venga utilizzata anche per attacchi «non mirati», il tutto nell'intento costante di indurre la vittima ad aprire un allegato o a eseguire una determinata azione. Non si tratta quindi più soltanto di adottare un atteggiamento critico nei confronti degli e-mail di persone sconosciute, ma di lasciarsi guidare dalla prudenza anche quando si conosce il mittente. Nel caso di eventi inusitati – soprattutto quando si tratta di denaro – MELANI raccomanda di verificare la raggiungibilità telefonica mediante domande alle quali solo questa persona può rispondere, di accertare la sua identità oppure di discutere con conoscenti comuni la credibilità della storia.

3.4 Interruzione di Internet e della telefonia presso Cablecom

Un attacco DDoS nei confronti di un cliente Cablecom ha causato il 19 gennaio 2009 un disturbo sulla rete del provider durante una buona ora. Il traffico Internet era aumentato di parecchi gigabyte/secondo. I servizi di Internet e di telefonia nella grande agglomerazione di Zurigo e dintorni ma anche in altre regioni sono risultati limitati o non disponibili. Cablecom ha deviato il traffico Internet su un collegamento alternativo della rete internazionale. Il traffico aggressore ha poi potuto essere impedito ai punti di entrata del *backbone* di Cablecom e del backbone internazionale di Internet. Secondo le informazioni fornite da Cablecom è stato colpito circa un terzo della clientela del circondario di Zurigo, ossia quasi 90 000 collegamenti, che non hanno potuto o solo parzialmente telefonare o utilizzare Internet tra le 12:50 e le 13:50.

In Svizzera sono già stati registrati diversi attacchi DDoS. Sono oggetto di attacchi particolarmente frequenti pagine Web con contenuti pornografici[6]. Nel dicembre del 2007 per il tramite di una *rete bot* è stato ad esempio attaccato (cfr. nota[7]) il sito Web www.sexy-tipp.ch. Anche altri siti Web in relazione con il milieu delle case chiuse di Zurigo hanno subito la medesima sorte. Nel caso di simili attacchi sono sovente compromessi anche altri siti Web ospitati sullo stesso server, ma viene perlopiù perturbata l'intera rete. Non si sa se l'attacco a Cablecom abbia uno sfondo analogo. Cablecom ha comunque sporto denuncia.

3.5 Attacchi mirati contro le maggiori imprese con e-mail contenenti un software nocivo

Nel corso del primo semestre del 2009 è stata osservata un'ondata di attacchi estremamente mirati[8] diretti contro i quadri di grandi imprese. Gli e-mail erano scritti in inglese e pretendevano che era stato effettuato un mandato di pagamento che necessitava l'apertura del documento allegato «details.rtf» per verificarne l'esattezza. Aprendo questo file si istallava un software nocivo (codice maligno).

Ecco un esempio di e-mail:

Subject: Re: Wire Transfer <Vorname Name des Empfängers>

The wire transfer has been released.

BENEFICIARY : <Vorname Name des Empfängers>
ABA ROUTING# : XXXX92729
ACCOUNT# : XXX-XXX-XXX25
AMMOUNT : $19,438.16

Please check the wire statement attached and let me know if everything is correct. I am waiting for your reply.
Laura

[6] http://www.pcwelt.de/start/sicherheit/firewall/news/192305/zwei_porno_sites_lassen_streit_eskalieren/ (in tedesco, stato: 31.08.2009)

[7] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it (stato: 31.08.2009)

[8] http://isc.sans.org/diary.html?storyid=6511 (in inglese, stato: 31.08.2009)

Dall'analisi del malware è emerso che tutte le cartelle aperte tramite Windows Explorer, tutte le pagine Web visitate con il browser e tutti i dati immessi nei formulari venivano registrati e inviati a diversi server. Questi, programmati in maniera stabile nel codice maligno, hanno potuto essere identificati e disattivati. Anche a livello internazionale sono state osservate ondate analoghe. Non si sa però quanti di questi e-mail sono stati inviati, ma solo che sono stati inviati quasi esclusivamente a quadri, ciò che lascia presumere un attacco estremamente mirato. Verso la fine del mese di dicembre 2008 si erano apparentemente già verificate altre ondate di spam dello stesso tipo [9] [10]. L'allegato era però diverso (bank_statement.scr o bank_statement.zip) e non è stato apparentemente inviato in maniera così mirata. Non si sa chi si nasconda dietro questi attacchi e quale obiettivo persegua.

4 La situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 Spionaggio IT ai danni di ONG tibetane e dell'ufficio del Dalai Lama

Il fine settimana del 29 marzo 2009 diversi media riportavano di uno studio canadese, intitolato «Tracking GhostNet – Investigating a Cyber Espionage Network»[11], sul tema dello spionaggio cinese in ambito di IT. Si tratta dei risultati di un'inchiesta su attacchi basati sulle IT e diretti sopratutto contro organizzazioni non governative tibetane e l'ufficio del Dalai Lama, che hanno infettato altri sistemi – fra i quali anche quelli di imprese e servizi governativi – in oltre 100 Paesi.

Fin dal 2007 sono stati resi pubblici rapporti confidenziali del capo del MI5 britannico[12], che mettevano in guardia contro attacchi mirati di spionaggio con *metodi raffinati di social engineering* basati su cavalli di Troia confezionati su misura. Secondo questi rapporti nel mirino cinese si trovavano anche *infrastrutture nazionali critiche* e servizi governativi. Da allora sono stati registrati attacchi simili contro servizi governativi anche in Svizzera. In questi casi gli aggressori inviano documenti appositamente predisposti e muniti di un falso mittente a persone chiave delle pertinenti imprese. Le informazioni erano confezionate su misura per i destinatari, il che può indicare che siano state procacciate informazioni preliminari per il canale dell'intelligence.

Sulla base delle informazioni disponibili, nel caso di questi attacchi – divenuti noti con il titolo di «Ghostnet» – occorre presumere che essi facciano parte del medesimo complesso di attacchi a istituzioni dello Stato, infrastrutture critiche e imprese resi pubblici già da alcuni anni. Si suppone che questi attacchi provengano dalla Cina[13]. Nel quadro delle indagini su Ghostnet sono stati individuati sistemi infettati anche in Svizzera. Si trattava però esclusivamente di rappresentanze di gruppi e di governi esteri in Svizzera. Le imprese e i servizi governativi svizzeri non facevano parte di Ghostnet.

---

[9] https://tools.cisco.com/security/center/viewAlert.x?alertId=17321 (in inglese, stato: 31.08.2009)

[10] http://fordhamsecureit.blogspot.com/2008/12/wire-transfer-phishing-email-sent-to.html (in inglese, stato: 31.08.2009)

[11] http://www.news.utoronto.ca/media-releases/international-affairs/information-warfare-monitor.html (stato: 31.08.2009)

[12] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it (stato: 31.08.2009)

[13] http://www.melani.admin.ch/dokumentation/00123/00124/00161/index.html?lang=it (stato: 31.08.2009)

4.2 Conficker

Nel corso dell'ultimo semestre il *verme* informatico Conficker (noto anche con il nome di Downadup) è stato uno dei temi TIC più trattati dai media. L'interesse dei media si è manifestato enormemente soprattutto verso il 1° aprile 2009, quando il verme (o «worm») avrebbe dovuto aggiornarsi.

La prima versione di questo verme di Windows è in circolazione dal 21 novembre 2008. All'inizio la sua propagazione è stata ridotta. Con il passaggio dell'anno il cambiamento è però stato drastico. Per propagarsi il worm sfrutta una lacuna di sicurezza del servizio Microsoft Windows Server (MS08-067), per il quale esiste un aggiornamento di sicurezza da fine ottobre 2008. Sono minacciate soprattutto le imprese e i privati che non hanno installato questo aggiornamento. Il verme dispone nondimeno di ulteriori possibilità di propagazione: sonda un elenco di password semplici[14] per copiarsi su svincoli di rete, oppure tenta di copiarsi sulle memorie mobili come gli stick USB e gli apparecchi fotografici digitali. Non appena si introduce uno stick infettato nel computer si apre una finestra sulla quale il verme genera un'icona standard di apertura delle cartelle. L'icona non figura però nel settore «opzioni», bensì nel settore «avvio del programma». Cliccando sull'icona il verme si installa sul computer. Si ritiene che Conficker abbia ha infettato milioni di computer.

Una volta installato, questo worm blocca tutti i processi di aggiornamento e crea un server Web locale. Successivamente esso tenta di propagarsi ulteriormente e di camuffarsi per rendere più difficile la sua rimozione. Esso può caricare ed eseguire qualsiasi file. Per finire Conficker blocca anche l'accesso a numerose pagine di sicurezza e servizi di aggiornamento antivirus.

L'interesse dei media è stato suscitato soprattutto dal meccanismo di aggiornamento e dalla data magica (1° aprile 2009), alla quale il verme avrebbe dovuto aggiornarsi. Il meccanismo di aggiornamento genera in funzione di un algoritmo nomi di domini con i quali tenta di prendere contatto per ricevere un aggiornamento corrispondente. Potenzialmente Conficker.C poteva generare 50 000 nomi di dominio al giorno con i quali prendere contatto. Se il contatto fallisce, il verme aspetta 24 ore prima di generare altri 50 000 nomi di dominio. Per quanto riguarda i vermi precedenti, nel corso dei primi mesi gli autori si sono soprattutto preoccupati di installare e di proteggere la rete (consolidamento della rete) e meno di sfruttare la rete per qualche azione strepitosa. Ne è prova il fatto che i programmatori del worm utilizzano gli algoritmi più moderni, in parte disponibili da poche settimane. La tecnica di codificazione integrata utilizzata per proteggersi dall'uso abusivo da parte di altri hacker è stata sviluppata soltanto nell'autunno del 2008. È la ragione per la quale si può supporre che il 1° aprile 2009 Internet non sarebbe stato molto pregiudicato. È soltanto il 7 aprile 2009 che la ditta di sicurezza Trend Micro ha osservato un incremento dell'*attività P2P* di Conficker.C, nell'ambito del quale il verme si è trasformato nella variante Conficker.E. Anche in questo caso il principale obiettivo del worm era fare sparire le proprie tracce. A tale scopo ha bloccato le pagine che offrono programmi di rimozione dei vermi. Inoltre ha fatto la sua apparizione con un nome di file casuale, cancellando tutte le tracce dal PC ospite. Per quanto riguarda le motivazioni degli autori di Conficker si possono unicamente avanzare congetture. Si potrebbe ad esempio trattare della costruzione di una *rete bot* da dare in locazione ad altri criminali. Come noto, Conficker.C installa uno *scareware,* il programma SpywareProtect2009[15].

[14] http://blog.namics.com/2009/02/die_aktuelle_li.html (in tedesco, stato: 31.08.2009)

[15] http://www.heise.de/security/Deckt-der-Conficker-Wurm-jetzt-seine-Karten-auf--/news/meldung/136083 (in tedesco, stato: 31.08.2009)

All'estero questo verme ha colpito numerose reti aziendali e governative, come ad esempio l'ospedale e il governo regionale della Carinzia[16] e l'esercito tedesco[17]. Anche in Svizzera talune reti aziendali sono state paralizzate per alcune ore. In Svizzera sono noti circa 1000 *indirizzi IP* di computer infettati, la maggior parte dei quali si situa nondimeno in Russia, Brasile, Cina e India.

Problema dei sistemi certificati

Colpisce in particolare il fatto che il verme abbia colpito soprattutto reti del settore della sanità[18]. Ne potrebbe essere motivo il fatto che proprio su queste reti si trovano numerosi sistemi certificati di computer (ad esempio dispositivi di comando di apparecchiature di esame) ai quali non può senz'altro essere applicato un patch. Questi sistemi sono poi un obiettivo facile per il verme se sono per di più collegati a Internet. Un ulteriore problema è costituito dall'utilizzazione di laptop personali e di periferiche USB nelle reti aziendali. In questi casi l'infezione sui computer privati può essere trasferita alla rete aziendale. Il verme sfrutta alla perfezione questo sistema.

A dire il vero più nessuno si aspettava l'eruzione di un simile verme. Dall'epoca dell'introduzione di Windows XP nella versione con il service pack 2 – che contiene un firewall e installa regolarmente i più recenti aggiornamenti – chiunque dovrebbe di massima essere protetto dall'apparizione di un simile verme. La realtà è però ben diversa. Una tesi in merito è che nel caso della maggior parte dei computer compromessi siano in uso versioni non ufficiali di Windows, per le quali gli utenti hanno scientemente evitato di prendere contatto con il server di aggiornamento di Windows.

Una volta ancora risulta chiaro quanto sia importante la protezione di base del computer. Rientrano in tale ambito l'aggiornamento del sistema operativo e delle sue applicazioni, un firewall e un software antivirus aggiornato. Poiché numerose imprese non installano immediatamente gli aggiornamenti, ma ne collaudano preliminarmente la compatibilità con altri programmi, si verifica un ritardo nell'installazione che dovrebbe essere il più limitato possibile. Con la diffusione degli stick USB, degli apparecchi fotografici digitali, dei telefoni cellulari e dei *player MP3* il percorso infettivo via memorie mobili guadagnerà in importanza.

4.3 SCADA

La sorveglianza, il controllo e il comando di impianti industriali, di sistemi di distribuzione di beni di importanza vitale (corrente elettrica, acqua, combustibili, ecc.) o nel settore dei trasporti e del traffico (ferrovie, sistemi di direzione del traffico, posta, ecc.) sono da tempo impensabili senza l'impiego di tecnologie dell'informazione e della comunicazione (TIC). Lo sviluppo e l'esercizio di sistemi di sorveglianza, di controllo e di comando (in inglese: Supervisory Control and Data Acquisition, SCADA) vanta una lunga tradizione. In origine i sistemi SCADA avevano poche analogie con le TIC usuali: erano isolati dalle reti di computer, utilizzavano hardware e software proprietari e comunicavano attraverso protocolli propri con l'elaboratore centrale. Nel corso degli ultimi anni l'ampia disponibilità di apparecchiature comparativamente più convenienti e dotate di interfacce sul *protocollo*

[16] http://www.heise.de/security/Conficker-in-Kaernten-Nach-der-Landesregierung-nun-die-Spitaeler--/news/meldung/121570 (in tedesco, stato: 31.08.2009)
[17] http://www.netzwelt.de/news/79475-conficker-bundeswehr-kaempft-gegen-computerwurm.html (in tedesco, stato: 31.08.2009)
[18] http://diepresse.com/home/techscience/internet/sicherheit/473436/index.do (in tedesco, stato: 31.08.2009)

Internet (IP) ha introdotto forti cambiamenti in questo settore. Oggigiorno i sensori, le macchine e gli interruttori dispongono sempre più frequentemente di un proprio indirizzo IP e utilizzano il normale protocollo Internet per comunicare con l'elaboratore centrale. Il vantaggio proveniente dall'impiego di TIC usuali e più economiche è ottenuto al prezzo dell'esposizione in genere dei sistemi SCADA alle medesime minacce che ci sono note da Internet: si apre la strada a codici maligni e «hacker». I dibattiti sul tema della sicurezza dei sistemi SCADA sono sempre più ampi, come illustrato dagli esempi qui di seguito. Questi sistemi di importanza centrale per il funzionamento della nostra società non vengono però messi a repentaglio soltanto da hacker, ma anche da perturbazioni tecniche che possono provocare il crash di sistemi importanti, come illustra chiaramente l'esempio del crash del sistema ETCS delle FFS nell'estate del 2009.

Distrubo all'ETCS ha nuociuto al traffico ferroviario tra Mattstetten-Rothrist e al tunnel del Lötschberg

L'abbreviazione ECTS[19] sta per European Train Control System. Anche in questo caso si tratta di un sistema SCADA. L'obiettivo di ECTS è la creazione di un sistema di comando dei treni armonizzato a livello europeo. La standardizzazione riguarda in particolare la trasmissione delle informazioni tra binario e veicolo. Le informazioni che devono essere trasmesse tramite i componenti del sistema ETCS possono perlopiù essere ricavate o derivate dagli impianti di sicurezza preesistenti.

Sulla nuova tratta Mattstetten-Rothrist, nella galleria di base del Lötschberg e nella galleria di base del Gottardo – non ancora ultimata – si utilizza l'ECTS Level 2. Oltre i 160 km/h il macchinista non è più in grado di riconoscere visualmente i segnali. Per questo, gli vengono trasmessi il consenso per la corsa e le rispettive informazioni sulla tratta, indicati nella cabina di guida. Rimangono invece lungo il binario l'annuncio di binario libero e la supervisione della completezza del treno. Tutti i treni segnalano automaticamente e a intervalli regolari la propria posizione e direzione di marcia alla centrale di tratta, che li sorveglia costantemente. Il consenso per la corsa, insieme ai dati sulla velocità e ai dati di tratta, sono trasmessi ininterrottamente al veicolo tramite *GSM-R*. Il 29 luglio 2009 questo sistema ha subito un'avaria che ha avuto gravi ripercussioni su tutta la rete delle FFS. Se sulla tratta Mattstetten-Rothrist erano ancora disponibili i segnali convenzionali, ragione per la quale la tratta ha potuto continuare ad essere percorsa a una velocità di 160 km/h, nel tunnel di base del Lötschberg nessun segnale era più disponibile, ciò che ha avuto come conseguenza la deviazione dei treni sulla tratta di montagna.

Gli aggressori sono apparentemente entrati nel sistema di controllo della rete elettrica statunitense

Sfruttando una lacuna di sicurezza, gli aggressori sono apparentemente riusciti a installare nei sistemi di controllo un software che è in grado di perturbare sistemi importanti come gli impianti di distribuzione dell'energia elettrica e di depurazione delle acque degli USA. Secondo un rapporto pubblicato dal «Wall Street Journal[20]» che fa riferimento alle autorità di sicurezza statunitensi, gli aggressori sarebbero penetrati nella rete elettrica e avrebbero introdotto nel sistema programmi che potrebbero essere sfruttati per provocare una perturbazione dell'erogazione di corrente elettrica in tutto il Paese. Secondo il rapporto, le autorità statunitensi presumono che gli aggressori mirino a controllare la rete elettrica degli USA. Per il momento essi non avrebbero ancora tentato di danneggiare l'infrastruttura, situazione che potrebbe mutare rapidamente in caso di crisi o di guerra.

---

[19] http://mct.sbb.ch/mct/it/etcs-technologie-funktionsprinzip.htm?= (stato: 31.08.2009)

[20] http://online.wsj.com/article/SB123914805204099085.html (in inglese, stato: 31.08.2009)

Piano di *Smart Grid* esposto agli attacchi

In futuro le reti intelligenti (i cosiddetti *smart Grid*) sostituiranno quelle convenzionali. In quest'ottica la ditta californiana Pacific Gas and Electric intende distribuire entro il 2011 contatori intelligenti del gas e dell'elettricità ai suoi clienti. A tale scopo si installeranno ad esempio presso i consumatori finali contatori intelligenti che invieranno direttamente i dati di consumo del gas e dell'elettricità raccolti ai nodi di rete dell'erogatore. Grazie a una rete più fitta di dati, potranno essere meglio regolati anche la distribuzione e l'adeguamento, così come le avarie parziali di rete potranno essere individuate più rapidamente. Secondo uno studio tenuto segreto sembra che questi apparecchi siano vulnerabili dal profilo della sicurezza. Essi sarebbero ad esempio esposti ai *buffer overflow* e ai *rootkit*. I protocolli utilizzati non disporrebbero d'altra parte di meccanismi di sicurezza. Nell'ipotesi che le lacune possano essere sfruttate da un aggressore potenziale si potrebbe assistere a un'interruzione dell'erogazione di corrente. L'aggressore potrebbe ad esempio segnalare un forte carico. Qualora l'erogatore reagisse a questo presunto carico eccessivo si potrebbe verificare un'ipertensione sulla rete. Come via di comunicazione si utilizzano la procedura *Frequency Hopping Spread Spectrum (FHSS)* tra 902 e 928 Mhz, ma anche tecniche *WLAN* e *GPRS.* Attualmente i contatori intelligenti sono utilizzati soltanto in progetti pilota. La situazione potrebbe però cambiare in un prossimo futuro. Gli USA e l'Europa adotteranno viepiù gli Smart Grid dal 2011.

Gli esperti britannici mettono in guardia dall'uso di componenti di telecomunicazione cinesi

Secondo le affermazioni di esperti britannici[21] le componenti del gruppo cinese di telecomunicazione Huawei potrebbero essere utilizzate per provocare perturbazioni di importanti infrastrutture della Gran Bretagna, come le telecomunicazioni e l'erogazione di elettricità o acqua. Le componenti centrali della nuova rete di comunicazione di British Telecom provengono dalla ditta Huawei, che, con oltre 87 000 collaboratori, è uno dei maggiori fornitori del mondo di prodotti di telecomunicazione. Si tratta di una ditta privata non quotata in borsa. Il cardine della produzione è lo sviluppo e la fabbricazione di apparecchi per la tecnologia di comunicazione, segnatamente nel settore radio mobile, xDSL, reti ottiche e apparecchiature finali. I dubbi espressi dagli esperti inglesi non sono stati sinora né integralmente né parzialmente confermati.

Se in precedenza il comando delle infrastrutture veniva effettuato con soluzioni low-tech e in questo senso rimaneva chiaro e controllabile, con le attuali apparecchiature high-tech le funzioni non possono più essere verificate in maniera così semplice. Nella scelta delle apparecchiature e nell'aggiudicazione di commesse di progetti concernenti infrastrutture (critiche) si dovrà considerare non soltanto il prezzo d'acquisto, ma anche la sicurezza offerta (a lungo termine). Occorrerà parimenti ponderare accuratamente se l'esercizio dei sistemi SCADA dovrà essere effettuato introducendo una separazione logica e fisica da altre reti aziendali. Si raccomanda inoltre di utilizzare sistemi ridondanti per poter mantenere l'esercizio dell'infrastruttura nel limite del possibile anche in caso di avaria o di danni. Il crash delle telecomunicazioni (in particolare del collegamento Internet), dell'erogazione di corrente elettrica o dei mezzi di trasporto può provocare costi enormi alle imprese e alle persone private.

[21] http://www.telegraph.co.uk/news/worldnews/asia/china/5072204/Britain-could-be-shut-down-by-hackers-from-China-intelligence-experts-warn.html (in inglese, stato: 31.08.2009)

4.4 Maggiore focalizzazione su unità militari in diversi Paesi in vista della cosiddetta condotta della guerra dell'informazione

Il tema della cosiddetta guerra dell'informazione o Information Warfare figura in cima all'elenco dei servizi incaricati della difesa e della condotta della guerra dei singoli Stati di tutto il mondo – e questo non soltanto dall'epoca del massiccio attacco di Denial-of-Service alle reti del governo e delle imprese dell'Estonia. In Germania ad esempio è stata addestrata in questo contesto un'unità dell'esercito che si occupa delle cosiddette *Network Centric Operations (NCO)*.

In sintonia con la convergenza e la messa in rete tecnica generale (cfr. capitolo 5.1), anche i sistemi militari di condotta, comunicazione e controllo dipendono viepiù dalle reti integrate e possono quindi essere aggrediti con i mezzi TIC. Ciò significa che nel caso di conflitti armati si prospetterà non soltanto l'impiego di mezzi militari convenzionali, ma anche attacchi IT diretti. Con la costante messa in rete dei propri sistemi ogni esercito dovrà viceversa confrontarsi anche con la protezione assoluta di questi sistemi.
È noto che soprattutto le grandi potenze militari, come gli USA e la Cina, negli ultimi anni hanno intrapreso notevoli sforzi in questa direzione. Si presume che la costituzione di capacità corrispondenti non sia limitata ai soli mezzi difensivi di protezione delle reti.
Anche in Svizzera il concetto di «Information Operations» è stato sottoposto a un accurato esame dal 2001. Su questo tema è stato redatto uno studio di concetto i cui primi insegnamenti sono confluiti nell'istituzione di un *CERT* per le installazioni militari, il cosiddetto MilCERT.

Nel quadro di simili iniziative si affacciano nondimeno questioni politiche e di stato di diritto. Da un profilo generale è chiaro che le unità militari di uno Stato devono disporre della possibilità di proteggere i loro sistemi dagli attacchi avversi basati sulle TIC. A seconda delle circostanze ciò può anche significare che si faccia capo a mezzi offensivi per paralizzare o perturbare i sistemi dell'avversario, prima ancora che venga sferrato un attacco contro le proprie reti. Tali mezzi possono essere impiegati in maniera corrispondente come mezzo bellico ausiliario nelle operazioni di guerra. Ma proprio in un'epoca in cui i conflitti armati classici fra Stati dovrebbero costituire l'eccezione e gli scontri dovrebbero soprattutto essere risoluti al di sotto della soglia bellica, l'impiego offensivo di mezzi TIC è molto allettante, ma corrisponde a un passo scivoloso sul terreno del diritto internazionale.

Nel caso degli attacchi ai sistemi del governo georgiano si è sovente utilizzato il concetto di «guerra informatica». Si trattava però anzitutto di attacchi di natura criminale a sistemi di computer e reti di uno Stato. Nel contesto del conflitto militare le aggressioni erano di natura civile, ragione per la quale – dal profilo dello stato di diritto – vanno pertanto considerate come azioni illegali da perseguire penalmente nello Stato di chi ha subito il danno. Anche le azioni di un gruppo di attivisti in Israele durante la guerra di Gaza[22] devono essere analizzate da questo punto di vista. In entrambi i casi è nondimeno lecito considerare che questi attacchi rientrano, almeno in parte, nel diritto bellico perché si tratta di azioni eseguite nel quadro di operazioni militari tra due Stati o due parti analoghe a Stati.

Un improvviso allentamento di questi limiti e la qualificazione di queste azioni collaterali come operazioni belliche alle quali rispondere con corrispondenti operazioni TIC di natura

[22] http://www.heise.de/newsticker/Gaza-Konflikt-Der-Krieg-im-Internet--/meldung/121389 (in tedesco, stato: 31.08.2009)

militare comporterebbe nel contempo un'estensione della legittimazione di misure militari contro partecipanti civili che solo indirettamente partecipano al conflitto.

All'atto della creazione e dell'impiego di capacità TIC di offensiva di natura civile o militare, occorre stabilire esattamente in quali casi e soprattutto contro chi e in quali circostanze esse possono essere impiegate. Infatti non tutti gli attacchi a reti militari o statali costituiscono di per sé un atto bellico, neppure quando a seconda delle circostanze lo Stato si trova effettivamente in una situazione di conflitto analoga alla guerra. Anche la natura di tali attacchi è di difficile attribuzione. Un chiaro autore è difficilmente identificabile e misure di ritorsione possono comportare danni collaterali difficilmente prevedibili per il Paese preso di mira. Gli esempi dell'Estonia e della Georgia evidenziano che simili attacchi possono senz'altro essere di natura criminale e devono essere perseguiti e puniti con gli strumenti del perseguimento penale. Un occultamento di questa chiara linea di separazione comporta il pericolo di un inutile intervento con i mezzi disponibili nei settori chiave degli organi civili, organi ai quali è affidata primariamente la tutela della sicurezza interna. Ciò significa simultaneamente che le norme del perseguimento penale ordinario e in particolare la protezione dei diritti fondamentali dell'imputato sono scardinati senza necessità.

4.5 Incremento degli attacchi DDoS a sfondo politico

Secondo la Arbor Networks[23] gli attacchi a Internet a sfondo politico sono sempre più frequenti. La frequenza degli attacchi e il numero degli obiettivi aumentano costantemente. Un motivo possibile di tale incremento potrebbe consistere nel fatto che anche persone senza nozioni tecniche possono acquistare e utilizzare tools DDoS come «Black Energy» o «NetBotAttacker». È quanto illustra peraltro il test effettuato dalla BBC (cfr. capitolo 4.7). Se finora prevalevano gli attacchi DDoS attraverso pagine Web pornografiche, al più tardi dall'epoca dell'attacco all'Estonia è divenuto chiaro che questa tecnica può essere utilizzata anche come arma politica. Oltre agli attacchi in Georgia[24], lo scorso gennaio alcuni hacker russi sono ad esempio riusciti a interrompere il collegamento Internet del Kirghizistan[25]. L'attacco era diretto contro i due principali provider del Paese. Nella fattispecie si possono soltanto formulare speculazioni sui motivi che hanno spinto degli aggressori ad agire; è comunque possibile che fossero di natura politica.

Occorre rammentare in questa sede che si osserva un costante incremento di qualità nel settore degli attacchi DDoS. Il numero di computer necessari all'attacco è in continua diminuzione. Grazie ai cosiddetti attacchi DNS-Amplification è ad esempio possibile raggiungere una grande efficacia anche con una rete bot di piccole dimensioni. In un caso[26] è stato infatti possibile generare un trasferimento di dati di 5 gigabyte/secondo con soli 2000 computer.

[23] http://www.arbornetworks.com (stato: 31.08.2009)
[24] http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=it (stato: 31.08.2009)
[25] http://www.pcwelt.de/start/sicherheit/firewall/news/192009/russische_cyber_miliz_attackiert_kirgisistan/ (in tedesco, stato: 31.08.2009)
[26] http://www.pcwelt.de/start/sicherheit/firewall/news/192305/zwei_porno_sites_lassen_streit_eskalieren/ (in tedesco, stato: 31.08.2009)

4.6 Crash della rete T-Mobile

Lo scorso 21 aprile, dalle 16 alle 19 circa la rete mobile gestita dalla tedesca T-Mobile è stata paralizzata. Si tratta del più grande crash registrato finora da una rete di telefonia mobile in Germania[27]. Tutti i servizi vocali e SMS sono stati bloccati. Il crash è stato provocato da un errore di software nell'*Home Location Register (HLR)*, responsabile dello stabilimento del collegamento tra le stazioni di telefonia mobile e il corrispondente numero di telefonia. Il crash del HLR ha per conseguenza che non è più stato possibile stabilire collegamenti e che la rete non è più stata raggiungibile. La rete è stata in parte nuovamente disponibile dopo 3 ore, in seguito all'eliminazione della perturbazione.

Il 25 giugno 2009 anche la rete telefonica E-Plus è stata perturbata per circa due ore su tutto il territorio tedesco. In questo caso sembra che la causa sia stata un errore nel server centrale di commutazione[28].

In entrambi i casi sembra che una componente centrale sia responsabile dei crash. In genere questi sistemi sono concepiti in maniera ridondante, proprio per impedire simili crash. Questo modo di procedere protegge efficacemente dalle avarie dell'hardware, ossia dalla paralisi di un server. Perlomeno nel caso di T-Mobile sembra si sia trattato in un'avaria del software. Dato che sui sistemi ridondanti girano pressoché il medesimo software e la medesima configurazione non stupisce affatto che all'atto della commutazione sul sistema di backup siano apparsi gli stessi problemi di software del sistema principale e che anche il sistema di backup abbia subito un crash.

Va sottolineato inoltre il fatto che nel caso di T-Mobile sono state riscontrate difficoltà nella mobilitazione del servizio di picchetto. Raggiungere i tecnici competenti è stato particolarmente difficile perché vengono contattati con il sistema di telefonia mobile della stessa T-Mobile. Con la diffusione della telefonia mobile la raggiungibilità dei servizi di picchetto e di emergenza è stata scorporata sulla telefonia mobile. Occorre sempre prendere in considerazione le conseguenze che un crash della rete può avere sul dispositivo di emergenza.

4.7 Gran Bretagna: la BBC acquista una rete bot a scopi dimostrativi

Nel quadro della preparazione di un servizio sul tema della criminalità informatica, l'ente radiotelevisivo britannico BBC ha acquistato una *rete bot*. Secondo le indicazioni fornite, al momento dell'acquisto la rete «Click» – dal nome del programma della BBC – comprendeva circa 22 000 *computer zombie*. La BBC ha ottenuto il software di rete bot contattando corrispondenti chatroom. I criminali comunicano tra loro su chatroom di questo tipo e tentano altresì di offrire i loro servizi. Una rete bot è un insieme di computer infettati da software nocivi che può essere comandata a distanza dagli aggressori. Per i 22 000 bot sarebbero stati chiesti circa 700 dollari. È un prezzo piuttosto basso, perché si sarebbe trattato di una rete bot aspecifica e ramificata nel mondo intero. Migliore è la qualità della rete bot, più alto è il suo prezzo. La BBC parla di un prezzo compreso tra 300 e 400 dollari per 1000 bot. Per parecchie ore due indirizzi e-mail di test sono stati inondati da migliaia di messaggi spam a scopi dimostrativi. Sempre secondo le indicazioni fornite dalla BBC, è stato paralizzato un

[27] http://www.welt.de/webwelt/article3603796/T-Mobile-schenkt-Gratis-SMS-als-Entschuldigung.html (in tedesco, stato: 31.08.2009)

[28] http://www.zdnet.de/news/wirtschaft_telekommunikation_e_plus_netz_gestern_90_minuten_lang_ausgefallen_story-39001023-41005882-1.htm (in tedesco, stato: 31.08.2009)

sito Web con un attacco di Distributed-Denial-of-Service (DDoS) d'intesa con l'esercente. Ne è emerso che per paralizzare la pagina Web sarebbero bastate le sole richieste di rete di 60 computer. Secondo la BBC gli utenti dei pertinenti computer sono stati nel frattempo informati di queste operazioni. A tale scopo sullo sfondo del desktop dei computer infettati è apparso un messaggio di allarme.

Questo modo di procedere solleva la questione se una ditta di sicurezza possa ad esempio riprendere una rete bot e manipolarla in modo da poterla infine disattivare oppure da far comparire, come nella fattispecie, un messaggio di allarme sui computer infettati. In futuro si dibatterà certamente con maggiore frequenza se sia questa la via da seguire per combattere le reti bot. L'acquisto di reti bot dovrebbe nondimeno essere controproducente perché ne sprona il mercato, rendendolo ancor più lucrativo per i criminali informatici. Il rapporto della BBC evidenzia però anche molto chiaramente che una rete bot può essere comandata con programmi semplici che possono essere operati anche da non specialisti. La tendenza in questo settore va però ben oltre. Lo scorso anno i criminali informatici hanno sviluppato il modello Crimeware-as-a-Service[29]. In questo caso i criminali informatici, ben coscienti delle difficoltà tecniche, possono «affittare» un servizio corrispondente. Tramite queste piattaforme i criminali ricevono direttamente il servizio e non hanno bisogno di preoccuparsi di problemi tecnici. Si ritiene che nel corso del 2009 questo nuovo modello conoscerà una notevole propulsione di sviluppo.

4.8 USA: incremento massiccio delle avarie di dati nel 2008

Secondo l'Identity Theft Resource Center di San Diego[30] nel 2008 negli USA sono stati sottratte oltre 35 milioni di serie di dati, pari a un aumento del 47 per cento delle perdite di dati annunciate dalle imprese e dalle autorità rispetto all'anno precedente. La maggior parte di queste perdite concerne l'economia privata. Secondo uno studio del settore finanziario e delle imprese di carte di credito è in questo ambito che si registrano la maggior parte delle contromisure. L'Identity Theft Resource Center enumera cinque categorie responsabili della perdita di dati: perdita di memorie digitali (laptop, stick USB ecc.), furti interni ed esterni di dati, pubblicazione e diffusione involontaria di informazioni personali e perdita di dati da parte di fornitori di servizi esterni.

Si può presumere che verrà rubato un numero sempre maggiore di dati e che la pressione aumenti in vista dell'annuncio delle avarie di dati. In Svizzera non esistono informazioni ufficiali in merito al volume di avarie. La legislazione nazionale sulla protezione dei dati non reca peraltro alcuna norma esplicita che imponga al titolare di una raccolta di dati l'obbligo di annunciare le avarie. Ma anche in Svizzera sono noti incidenti, come ad esempio la pubblicazione di dati confidenziali relativi all'accordo di Schengen sulla pagina Web del Dipartimento federale di giustizia e polizia (DFGP) nel mese di maggio dell'anno scorso.

A mente delle varie possibilità di perdita di dati è chiaro che un concetto di sicurezza integrale deve essere focalizzato sulla protezione stessa dell'informazione. I canali di distribuzione, i diritti di accesso e i luoghi di conservazione devono essere adeguati al valore effettivo di un'informazione. Non tutti i canali e i luoghi di conservazione sono ugualmente sicuri e non tutti i documenti sono ugualmente sensibili. Ciò comporta una gestione rafforzata dei rischi nell'approccio dei dati e delle informazioni. La sensibilizzazione dei collaboratori è di grande rilievo in questo contesto. Le misure tecniche di protezione rientrano nella

[29] Rapporto semestrale 2008/II punto 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=it (stato: 31.08.2009)
[30] http://www.idtheftcenter.org (stato: 31.08.2009)

protezione di base in ambito di sicurezza dei dati, ma possono essere inefficaci nel caso di un approccio noncurante dell'informazione. Nella maggior parte dei casi l'anello più debole e maggiormente esposto nella catena della sicurezza è la componente umana.

4.9 Gli USA vogliono potenziare la lotta contro le minacce informatiche e aumentare la protezione

All'inizio dell'anno il governo degli USA, sotto la presidenza di Barack Obama, ha pubblicato l'agenda relativa alla sicurezza nazionale. In questo contesto le reti elettroniche del Paese sono state dichiarate «bene strategico», mentre alla protezione dell'infrastruttura IT è stato attribuito un valore elevato. Per coordinare i diversi servizi che si occupano di questi temi dovrà essere designato un «National Cyber Advisor» – noto anche come «Cyber Czar» –, direttamente subordinato al presidente. È stato parimenti annunciato un «Safe Computing Research and Development Effort», che dovrà portare allo sviluppo di una nuova generazione di hardware e software particolarmente sicuri per le reti delle autorità.

A fine maggio è poi stato pubblicata la «Cyberspace Policy Review»: una fotografia della situazione attuale del cyberspazio contenente raccomandazioni sulla procedura degli USA in questo settore. Gli autori sono giunti alla conclusione che in un'ottica a lungo termine Internet si fonde con le altre tecnologie tradizionali di telecomunicazione e che anche gli altri esercenti di infrastrutture utilizzeranno sempre più questa rete come canale primario di interconnessione dei sistemi (cfr. anche SCADA, capitoli 4.3 e 5.2).

L'esercizio di Internet, come quello di un grande numero di infrastrutture dell'approvvigionamento fisico di base, sarà garantito in maggioranza da attori privati. È quanto rileva la Cyberspace Policy Review, secondo cui la collaborazione con questi attori privati è imprescindibile. Lo Stato e gli esercenti privati di importanti infrastrutture sono in genere molto interessati a un funzionamento affidabile delle tecnologie utilizzate e a una trasmissione sicura dei dati all'interno delle infrastrutture di informazione. Per questo motivo anche agli USA si raccomanda pertanto un «public-private partnership for cybersecurity», in seno al quale i partecipanti devono promuovere in comune una migliore protezione, così come una maggiore sicurezza e solidità del mondo digitale, mediante lo scambio di informazioni e attività coordinate. È stato d'altra parte ammesso che i problemi in ambito di Internet non possono essere risolti dai soli USA, ma devono essere abbordati in un contesto internazionale. In tale ambito si tratta di migliorare i presupposti di una nazione digitale sicura e forte nel proprio Stato mediante l'elaborazione di basi legali e direttive rilevanti e l'istituzione di un quadro per le misure coordinate degli attori coinvolti a tutti i livelli – locale, nazionale e internazionale – in caso di incidenti nel cyberspazio.

4.10 La Commissione europea vuole una migliore protezione delle infrastrutture critiche

Anche l'UE ha riconosciuto che le TIC sono sempre più parte della vita quotidiana dei suoi cittadini e rappresentano una componente imprescindibile dell'economia e della società, dato che mettono a disposizione beni e servizi d'importanza fondamentale oppure costituiscono la base di altre infrastrutture critiche.

A motivo della sempre più forte dipendenza dalle infrastrutture critiche informatizzate, della loro ramificazione transfrontaliera e del loro collegamento con altre infrastrutture, come pure delle vulnerabilità e delle minacce alle quali sono esposte, è urgentemente necessario migliorarne sistematicamente la sicurezza e la resistenza. Per questo tramite esse devono

essere tutelate in prima linea da crash e attacchi, perché le perturbazioni delle infrastrutture critiche informatizzate possono pregiudicare severamente importanti funzioni sociali.

I recenti attacchi alle infrastrutture informatizzate in Estonia, Lettonia e Georgia hanno evidenziato che importanti reti e servizi elettronici di comunicazione sono costantemente minacciati.

Per questo motivo nella sua comunicazione del 30 marzo 2009 concernente la protezione delle infrastrutture critiche informatizzate [31] la Commissione dell'UE si esprime a favore di misure che incrementino la sicurezza, la resilienza e la stabilità di Internet e in genere delle infrastrutture critiche informatizzate. Per raggiungere questo obiettivo la Commissione intende promuovere i partenariati pubblico-privati. La Commissione progetta inoltre l'istituzione di capacità e di servizi comuni in vista di una cooperazione europea, di un forum per lo scambio di informazioni tra gli Stati membri e di un sistema europeo di informazione e di allarme. Essa invita gli Stati membri ad allestire piani nazionali di emergenza e a eseguire regolarmente esercitazioni di emergenza per sondare la capacità di reazione a violazioni di grande volume della sicurezza delle reti. Si dovrà ovviamente rafforzare ulteriormente anche la collaborazione tra i CERT e i CSIRT nazionali.

L'UE si consacra pertanto maggiormente alla protezione contro gli attacchi informatici e le perturbazioni di grande portata mediante un rafforzamento della prontezza di difesa, della sicurezza e della stabilità.

4.11 Facebook ha modificato le sue CCG – solo per poco tempo

All'inizio del mese di febbraio sono state rielaborate le condizioni contrattuali generali (CCG) di Facebook, che disponeva già in precedenza di un diritto irrevocabile di utilizzazione di tutti i dati pubblicati. La modifica delle CCG intendeva estendere tale diritto anche ai dati cancellati. A seguito di proteste massicce Facebook ha poi deciso di ripristinare le condizioni generali precedenti[32].

[31] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:IT:PDF (stato: 31.08.2009)

[32] http://www.heise.de/newsticker/Facebook-nach-dem-AGB-Debakel--/meldung/133094 (in tedesco, stato: 31.08.2009)

5 Tendenze / Prospettive

5.1 Cloud Computing, scorporo, centralizzazione e Information Ownership

Il 17 maggio 2009 il Popolo svizzero ha adottato con appena il 50,1 per cento di voti favorevoli l'introduzione del *passaporto biometrico*. Oltre che dai dubbi in ambito di protezione dei dati, sembra che l'esito risicato della votazione sia stato determinato soprattutto da timori legati alla sicurezza dell'informazione. Si trattava nella fattispecie delle modalità di memorizzazione dei dati biometrici, effettuata in maniera centralizzata dall'Ufficio federale di polizia, che rappresenta tutti i Cantoni a livello di Confederazione. Durante la campagna per la votazione questa soluzione è stata a più riprese qualificata come un inutile grande fattore di rischio. Se i dati venissero memorizzati dai singoli Cantoni di origine, un solo attacco efficace non pregiudicherebbe tutte le serie di dati, ma solo una parte di esse. Per accedere a tutte le registrazioni biometriche sarebbero necessari nel migliore dei casi 26 attacchi efficaci contro i centri cantonali di dati e non un solo attacco a livello di Confederazione.

Questo tipo di riflessioni sui rischi sono per l'appunto all'ordine del giorno nel settore della sicurezza dell'informazione. Se la sicurezza TIC continua a costituire uno dei principali pilastri di un concetto efficace di sicurezza dell'informazione, la protezione dell'informazione stessa assume viepiù una posizione di primo piano. Si tratta nella fattispecie di un processo classico di assessment e di management del rischio. A titolo di esempio, la decisione di bloccare l'accesso a Facebook nelle imprese non è dettata da considerazioni di etica professionale, ma soprattutto da motivi di tecnica di sicurezza. Il maggior rischio delle *pagine di social network* consiste nondimeno nel fatto che le persone possono essere associate al loro datore di lavoro, circostanza che a seconda dei casi è indesiderata nei settori spinosi. In questi casi solo chiare direttive consentono un approccio corretto all'informazione, sia personale che contestuale al posto di lavoro, a prescindere dalle tecnologie utilizzate. Occorre stabilire chiaramente se e quali dati possono essere diffusi o devono essere protetti.

A questa evoluzione in direzione di un severo Information Ownership e di una classificazione continua dei valori delle singole informazioni, dati e documenti si contrappongono le possibilità allettanti ed efficienti sul piano dei costi offerte da banche dati, applicazioni e piattaforme gestite e mantenute a livello centrale. Segnatamente sviluppi come il *cloud-computing*, monopoli di fatto nel settore del s*ocial networking* come Facebook, ma anche sistemi SCADA orientati sulla centralizzazione, sul rapporto in tempo reale alla direzione[33] e sull'efficienza. A titolo di esempio il *cloud-computing* promette applicazioni, produzione e gestione di documenti in un tutto completo, offerto da un terzo degno di fiducia che assume anche la responsabilità della sicurezza per l'intero sistema. Fanno così parte del passato diversi livelli di patch, di applicazioni all'interno della medesima impresa ecc. Nondimeno questo modo di procedere provoca anche una concentrazione del rischio e a seconda dei casi un Single-Point-Of-Failure. La fissazione di priorità nella gestione dell'informazione, l'efficienza e i costi, ma anche la gestione in proprio dei sistemi (sicurezza e manutenzione) vanno infine lasciati all'impresa stessa.

[33] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it (stato: 31.08.2009)

Si prevede che in futuro aumenteranno ulteriormente il campo di tensione tra pressione dei costi, efficienza e disponibilità dell'informazione da un canto e grandi rischi, business outsourcing di informazioni e dati e maggiore vulnerabilità consecutiva all'uniformità e alla messa in rete di piattaforme d'altro canto. La soluzione di questo conflitto di obiettivi e di interessi deve pertanto essere di volta in volta il risultato di una ponderazione dei rischi sorretta da un'informazione possibilmente completa e fare anzitutto riferimento al contenuto in termini di valore dell'informazione da proteggere e appartenente all'azienda.

In questo contesto la diffidenza opposta alla memorizzazione centralizzata dei dati biometrici a livello di Confederazione è già un segnale molto promettente. Nondimeno questa diffidenza va ora opposta anche a soluzioni private di qualsiasi genere. In merito ci limitiamo a rammentare i numerosi profili di clienti compilati e conservati da molte imprese.

5.2 SCADA

La conversione in ambito di sistemi SCADA proseguirà, mentre la pressione economica farà sì che non soltanto singole componenti ma sempre più anche intere sottostazioni saranno comandate a distanza, senza personale. Saranno ulteriormente semplificate le tecnologie di rete generalmente identiche, questo conformemente all'auspicio del management di collegare rete commerciale e rete di controllo. Ne sono un esempio i contatori d'elettricità intelligenti che si prevede di installare nel quadro del progetto per la nuova rete elettrica US. In futuro questa evoluzione porrà nuove sfide alla sicurezza delle TIC. Si tratterà così di impedire che incidenti come l'introduzione di codici maligni nelle reti aziendali si propaghino alla rete di controllo. È quindi indispensabile applicare anche ai sistemi di controllo i principi usuali della sicurezza oppure standard e direttive corrispondenti ed esigere dai produttori degli apparecchi utilizzati sufficienti meccanismi di sicurezza. Rientra parimenti in un pacchetto completo di misure lo scambio di esperienze tra esercenti di sistemi di controllo (p. es. in termini di vulnerabilità), come pure tra questi ultimi e le autorità, che possono tra l'altro fornire un contributo sotto forma di informazioni su situazioni attuali di minaccia. La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI è in stretto contatto con i distributori di elettricità svizzeri e partecipa allo scambio internazionale di informazioni.

5.3 Evoluzione generale della criminalità informatica

MELANI e SCOCI[34] ricevono quotidianamente notifiche di casi di truffa in ambito di anticipi, presunte vincite nelle lotterie e offerte gratuite. Questo genere di criminalità informatica è apparentemente ancora troppo efficace. È quanto emerge anche dai rapporti di Paesi dove vengono commesse queste truffe. Alcuni autori sono riusciti a intascare in poco tempo un cospicuo bottino. Suscitano parimenti interesse i guadagni apparentemente realizzati quotidianamente con le cosiddette offerte gratuite. Oltre alle evoluzioni tecniche in ambito di diffusione e di utilizzazione di software nocivi, esiste d'altra parte la possibilità di ottenere con l'imbroglio somme considerevoli senza disporre di un grande know-how tecnico, ma della necessaria ostinazione, perseveranza e creatività. A condizione di essere perseverante l'aggressore riesce quasi sempre a trovare la vittima adeguata tra la massa di utenti di Internet. Troverete qui ulteriori informazioni sui diversi tipi di truffa e i corrispondenti avvertimenti[35] [36].

[34] SCOCI: Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet http://www.kobik.ch)
[35] http://www.den-trick-kenne-ich.ch/4/it/ (stato: 31.08.2009)

Esempio di truffa in ambito di anticipi, truffa in ambito di lotteria

In questo genere di truffa si procede all'invio di massa di e-mail alle vittime potenziali. Le offerte proposte e le promesse nelle lettere sono inventate di tutto punto e servono unicamente a creare un retroscena credibile sul quale viene poi costruita la truffa. Anche gli e-mail che annunciano presunte vincite alle lotterie sono tuttora in circolazione. In questo caso si tratta parimenti di un tipo di truffa in ambito di anticipi.

Il trucco funziona, come illustrano rapporti provenienti dal Ghana, dove esiste il fenomeno «Sakawa»[37] [38]. Si tratta generalmente di giovani provenienti dagli strati più poveri della popolazione alla ricerca di denaro facile. L'atto criminale, perpetrato nella maggior parte dei casi in Internet caffè, comprende praticamente tutto ciò che è noto anche in altri Paesi della regione, soprattutto in Nigeria. La rapida propagazione di Sakawa si spiega con il fatto che numerosi autori sono riusciti a carpire in poco tempo somme considerevoli e fanno sfoggio della loro ricchezza, ciò che spinge molte altre persone a imitarli. Sorto nel contesto della criminalità informatica, Sakawa si è nel frattempo esteso anche ai crimini ordinari locali (anche omicidi[39]), fermo restando che l'obiettivo di questi atti è di procurarsi denaro.

Esempio di offerte gratuite

Si accumulano le segnalazioni a MELANI che fanno stato del ricevimento di una fattura d'abbonamento e successivamente di una diffida al pagamento dopo aver visitato una pagina Web. Queste offerte perseguono l'obiettivo di indurre l'utente di Internet a concludere rapidamente un contratto, rispettivamente un rapporto di prestazioni, fermo restando che il fattore costo, così come altre condizioni generali di contratto, sono presentate in maniera difficilmente percepibile. Una volta concluso un «contratto» di questo tipo si succedono diffide e minacce di precetto esecutivo per intimidire il cliente. Per disorientare la vittima e indurla al pagamento «volontario» del credito dubbio sulle lettere figurano talvolta come mittenti avvocati o società di incasso. Si tratta generalmente di pagine in lingua tedesca. Gli offerenti si mostrano sempre più creativi e impertinenti. Sovente sono state inviate fatture e diffide a persone che non hanno mai visitato tali pagine.

Finora si è soprattutto tentato di attirare gli utenti di Internet su queste pagine per il tramite di motori di ricerca. All'immissione di determinate parole chiave molte di queste offerte figurano in coma alla schermata di Google. Sembra che ora si tenti di raggiungere gli utenti anche via e-mail[40]. Anche le tecniche per presentare i costi nella maniera più anodina possibile sono costantemente migliorate. Dopo avere in precedenza fatto figurare i costi in caratteri molto piccoli o averli celati nelle CCG, ultimamente di è anche fatto ricorso a immagini animate. Il prezzo appare in dissolvenza dopo alcuni secondi, di modo che la vittima non ha affatto la possibilità di accertarlo. Anche in questo campo sembra che gli affari fioriscano. Si sa che gli offerenti incassano ogni giorno tra 15 000 e 20 000 euro[41].

La Segreteria di Stato dell'economia (SECO) raccomanda di non pagare questo genere di fatture e di segnalare mediante lettera raccomandata all'offerente, immediatamente dopo la scoperta dell'errore, che la pagina Web in questione induce in inganno, ragione per la quale

---

[36] http://www.fedpol.admin.ch/fedpol/it/home/aktuell/warnungen.html (stato: 31.08.2009)
[37] http://www.ghanaweb.com/GhanaHomePage/features/artikel.php?ID=162565 (in inglese, stato: 31.08.2009)
[38] http://www.modernghana.com/news/192603/1/female-sakawa-hits-accra.html (in inglese, stato: 31.08.2009)
[39] http://www.Ghanavoices.wordpress.com/2009/08/13/girls-killed-for-sakawa/ (in inglese, stato: 31.08.2009)
[40] http://www.melani.admin.ch/dienstleistungen/archiv/01089/index.html?lang=it (stato: 31.08.2009)
[41] http://www.pressebox.de/pressemeldungen/ct/boxid-261364.html (in tedesco, stato: 31.08.2009)

il contratto è impugnato. La SECO indica inoltre che basta una sola lettera; la successiva corrispondenza dell'offerente può essere ignorata.

Per ulteriori informazioni in merito raccomandiamo di leggere il seguente opuscolo: http://www.seco.admin.ch/dokumentation/publikation/00035/00038/02033/index.html?lang=it.

5.4 Infezioni drive-by

In futuro le infezioni drive-by saranno ulteriormente migliorate per renderne più difficile l'individuazione. Attualmente nella maggior parte dei casi le infezioni drive-by sono caricate staticamente sulle pagine Web. Per fare ciò ad esempio gli aggressori ottengono un elenco di dati di login FTP, con i quali accedono automaticamente ai conti, scaricano una pagina Web (in genere la *pagina di indice* oppure un file JavaScript «.js» disponibile), vi immettono il codice nocivo e poi la caricano nuovamente. Gli aggressori possono ovviamente procurarsi l'accesso sfruttando anche una *lacuna di sicurezza*. Lo script caricato è però visibile e può quindi essere individuato da ogni utente e pertanto anche dall'amministratore Web.

Fin dall'anno scorso esistono tecniche che rendono difficile tale identificazione, sopratutto da parte degli esercenti di pagine Web. Nel mese di giugno del 2008 numerose pagine Web svizzere sono state oggetto di hacking e vi è stato collocato un JavaScript nocivo. Il carattere maligno di questo attacco consiste nel fatto che in caso di normale chiamata di questa pagina il codice nocivo non viene eseguito. Se però la pagina è chiamata via un motore di ricerca, come Google o Yahoo, il codice nocivo viene attivato. Il motivo di questa tattica di camuffamento risiede nel fatto che il proprietario della pagina Web chiama frequentemente la propria pagina, in genere direttamente o tramite un elenco di siti favoriti. In questo modo si contribuisce a mantenere ignota l'infezione il più a lungo possibile.

Se nel caso dell'esempio illustrato qui sopra si è operato con un JavaScript che ha potuto essere individuato mediante un'analisi del codice fonte, le tendenze attuali mostrano già un'ulteriore evoluzione. Il codice non figura più direttamente sulla pagina Web, ma viene immesso dal server Web. A ogni visita si decide se e su quale pagina deve essere inserito il codice nocivo. Per il Webmaster è quindi praticamente impossibile riprodurre l'infezione. In un caso di attualità, nel cui ambito è stato colpito anche un provider svizzero di hosting, l'attacco sembra essere stato effettuato per il tramite di un conto FTP compromesso. Successivamente è stato caricato sul server uno script PHP. In questo caso non è stata modificata la pagina Web, ma è stato modificato il server Web in maniera da dirottare di tanto in tanto il visitatore su una determinata pagina di software nocivo. Un *cookie* installato dal malware aiuta l'aggressore a identificare il computer. I reindirizzamenti non sono unicamente celati dietro le pagine di indice, ma anche dietro le immagini e le *icone dei siti favoriti*.

I dirottamenti sono stati collocati nel comando di aggiornamento dei metadati (META-Refresh) anziché nelle IFrames. Nei browser questi reindirizzamenti sono disattivati in misura minore che nel comando IFrame. Combinato con un inserimento unico, questo modo di procedere è praticamente altrettanto difficilmente rintracciabile quanto un exploit IFrame.

Per sapere come proteggere il vostro computer dalle infezioni drive-by si veda il capitolo «Contromisure» nell'allegato 7.2.

6 Glossario

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

ActiveX	Una tecnologia sviluppata da Microsoft, che consente di caricare piccoli programmi – i cosiddetti ActiveX Controls – sul computer del visitatore al momento della visualizzazione di pagine Web, dove vengono poi eseguiti. Essi permettono di convertire diversi effetti e funzioni. Purtroppo questa tecnologia viene sovente sfruttata in modo abusivo e rappresenta pertanto un rischio per la sicurezza. A titolo d'esempio, sul computer vengono scaricati ed eseguiti Dialer. I problemi di Active-X concernono unicamente Internet Explorer dato che gli altri browser non supportano questa tecnologia.
Attacco DoS	Attacco Denial-of-Service. Ha lo scopo di rendere irraggiungibile un determinato servizio all'utente o perlomeno di ostacolare notevolmente la raggiungibilità di detto servizio.
Bot / Malicious Bot	Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione.
Buffer overflow	I traboccamenti della memoria tampone (in inglese «buffer overflow») fanno parte delle più frequenti lacune di sicurezza dei software attuali, che possono tra l'altro essere sfruttate anche via Internet. Nel caso di un traboccamento della memoria tampone dovuto a un errore di programma vengono per l'essenziale scritte quantità di dati troppo grandi per un settore riservato di memoria troppo piccolo, il tampone, ragione per la quale il settore mirato di memoria è sovrascritto con le informazioni di memoria successive.
Cloud-computing	o «cloud computing» (sinonimo: «cloud IT», in italiano: «calcolare tra le nuvole»); concetto della tecnica dell'informazione (IT). Il paesaggio IT non è più esercitato/messo a disposizione dall'utente stesso, bensì proposto da uno o più offerenti. Le applicazioni e i dati non si trovano più sul computer locale nel centro di calcolo della ditta, ma in una nuvola («cloud»). L'accesso a questi sistemi a distanza è effettuato per il tramite di una rete.
Code	Istruzioni di programma che definiscono i comandi che deve eseguire il computer.
Computer Emergency Response Team (CERT)	Computer Emergency Response Team Si designa come CERT (ma anche come CSIRT per Computer Security Incident Response Team) un gruppo che si occupa del coordinamento e dell'adozione di misure nel contesto di incidenti rilevanti ai fini della sicurezza delle IT.
Computer zombie	Sinonimo di «bot» / «malicious bot»
Content Management	Un «Content Management System» (acronimo CMS, in italiano «sistema di gestione dei contenuti») è un sistema che rende

Systems (CMS)	possibile e organizza la produzione e l'elaborazione comune di contenuti, consistenti in documenti di testo e multimediali, in genere destinati al World Wide Web. Un autore può servirsi di un simile sistema anche senza conoscenze di programmazione o di HTML. In questo caso il contenuto informativo da presentare è detto «content» (contenuto).
Cookie	Piccolo file di testo depositato sul computer dell'utente alla visita di una pagina Web. Con l'ausilio dei cookies è per esempio possibile salvaguardare le impostazioni personali di una pagina Internet. Essi possono però anche essere sfruttati in modo abusivo per registrare le abitudini di navigazione dell'utente e allestire in tale modo un profilo di utente.
Domain Name System	Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo l'utente possono utilizzare nomi (ad es. www.melani.admin.ch).
European Train Control System (ETCS)	Si tratta di una componente di un sistema uniforme europeo di direzione del traffico ferroviario. L'ETCS è destinato a sostituire i molteplici sistemi di sicurezza utilizzati nei Paesi europei. Esso sarà applicato a medio termine al traffico a grande velocità e a lungo termine a tutto il traffico ferroviario europeo.
Fast Flux	Fast Flux è una tecnica DNS utilizzata dalle reti bot per ripartire e quindi dissimulare su diversi host le pagine phishing o le pagine che diffondono malware. Se un computer subisce un?avaria il computer successivo colma la breccia.
Flash	Adobe Flash (abbr. Flash, già Macromedia Flash) è un ambiente proprietario e integrato di sviluppo per la produzione di contenuti multimediali. Attualmente Flash è utilizzato in numerose applicazioni Web, sia come insegna pubblicitaria, sia come parte di una pagina Web, ad esempio come menu di comando o sotto forma di pagina Flash completa.
FTP	File Transfer Protocol FTP è un protocollo di rete per la trasmissione di dati tramite reti TCP/IP. FTP può ad esempio essere utilizzato per caricare pagine Web su un server Web.
General Packet Radio Service (GPRS)	In italiano «servizio generale radio a pacchetti»; servizio utilizzato nelle reti GSM (telefonia mobile) basato su pacchetti per la trasmissione dei dati.
Global System for Mobile Communications – Rail(way) (GSM-R)	Il «Global System for Mobile Communications – Rail(way)» (GSM-R o GSM-Rail) è un sistema di telefonia mobile basato sullo standard mondiale GSM e adeguato all'utilizzazione in ambito ferroviario.
Home Location Register (HLR)	In italiano «elenco del luogo di origine»; si tratta di una banca dati (distribuita) e costituisce un elemento centrale della telefonia mobile. È considerato il registro di origine di un numero di telefonia mobile, nel senso che ogni stazione mobile registrata e il suo corrispondente numero di telefonia mobile sono memorizzati nella banca dati.

IFrame	Un IFrame (anche Inlineframe) è un elemento HTML che serve alla strutturazione delle pagine Web. Esso viene utilizzato per integrare contenuti Web esterni nella propria homepage.
Infezione da «drive-by-download»	Infezione del computer mediante malware unicamente attraverso la consultazione di una pagina web. Le pagine web interessate contengono nella maggior parte dei casi offerte serie, ma sono state dapprima compresse allo scopo di diffondere il malware. L?infezione avviene perlopiù per il tramite dell?utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
IP-Adresse	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
JavaScript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. Ne può essere un esempio il controllo dei dati immessi dall'utente in un modulo Web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX Controls, gli JavaScripts sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Controls, gli JavaScripts sono supportati da tutti i browser.
Lacune di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
META-Refresh	In italiano «Aggiornamento dei metadati»; per reindirizzare (inglese «forwarding») su un altro URL alla chiamata di una pagina si può utilizzare il Refresh-Tag. Tramite il parametro di Content si può stabilire un periodo di tempo entro il quale avviene il reindirizzamento. Esempio: <meta http-equiv="refresh" content="5; URL=http://www.melani.admin.ch" /> In questo caso si è reindirizzati sulla pagina Web http://www.melani.admin.ch dopo 5 secondi.
Network Centric Warfare (NCW)/ Network Centric Operations (NCO)	In italiano «condotta net-centrica della guerra»; concetto militare di guerra nell'era dell'informazione. In merito si fa capo a moderni mezzi IT per la condotta della guerra. Network Centric Operations (NCO) designa la condotta di operazioni sulla base del Network Centric Warware.
P2P	Peer to Peer Un'architettura di rete nel cui ambito i sistemi partecipanti possono assumere le medesime funzioni (diversamente dalle architetture cliente-server). Il P2P è sovente utilizzato per lo scambio di dati.
Pagina di indice	File su un server Web / sito Web, utilizzato perlopiù come pagina iniziale.

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.
Passaporto biometrico	Passaporto munito di dati biometrici consultabili elettronicamente. Su un chip RFID sono memorizzati dati personali come nome, sesso, data di nascita ecc.
PHP	PHP è un linguaggio script che viene principalmente utilizzato per l?allestimento di pagine Web dinamiche e di applicazioni Web.
Player MP3	Software o hardware che può riprodurre file compressi di dati musicali (MP3).
Procedura «Frequency Hopping Spread Spectrum» (FHSS)	Tecnica di ampliamento delle frequenze nella trasmissione radio dei dati, suddivisa in Fast e Slow Hopping. La frequenza portante cambia e la sequenza del salto di frequenza è determinata da numeri pseudocasuali.
Protocollo Internet (IP)	Protocollo di rete molto diffuso nelle reti di computer che costituisce la base di Internet. Si tratta dell'implementazione dello strato di trasmissione (inglese «Network Layer») del modello TCP/IP, rispettivamente dello strato di trasmissione del modello OSI.
Referrer	Corrisponde all'indirizzo Internet della pagina Web a partire dalla quale l'utente è giunto sulla pagina attuale cliccando su un link (inglese «to refer», «indirizzare»). Il Referrer costituisce un elemento della richiesta HTTP inviata al server Web.
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 / rogueware	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.
Rootkit	Un insieme di programmi e di tecniche che consentono di accedere inosservatamente a un elaboratore e di assumerne il controllo.
Scareware	Software destinato a disorientare e intimorire l'utente. Si tratta di una forma automatizzata di «social engineering». Se la vittima cade nel tranello e si sente minacciata le viene offerta frequentemente l'eliminazione a pagamento di un pericolo inesistente. In altri casi la vittima è indotta dalla convinzione di un avere subito un attacco efficace a effettuare azioni che rendono possibile l'attacco vero e proprio.
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.
Time to live (TTL)	Nel protocollo utilizzato dai server DNS, un dato Time-to-live è presente e indica il tempo durante il quale l'informazione data dal server (sovente un nome a dominio o un altro server DNS) deve essere conservato in cache. Una volta questo termine sorpassato, l'informazione deve essere considerata come obsoleta e quindi aggiornata con una nuova richiesta.
USB Memory Stick	Piccoli dispositivi di memoria che possono esser raccordati al computer per il tramite di un'interfaccia USB.
Verme informatico	Diversamente dai virus, i vermi informatici non necessitano di un programma ospite per diffondersi. Essi sfruttano piuttosto le lacune di sicurezza o gli errori di configurazione del sistema operativo o delle applicazioni per diffondersi autonomamente da un computer all'altro.
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.

7 Allegato

7.1 Lotta ai fast flux: ICANN e UFCOM scendono in campo

Nel rapporto semestrale 2007/II[42], MELANI si era occupata degli aspetti tecnici legati alle reti fast flux. Nel corso degli ultimi due anni questo fenomeno si è aggravato, obbligando l'ICANN[43], l'organizzazione che si occupa della gestione dei nomi a dominio, ad analizzare il problema. Un primo rapporto è stato pubblicato nel marzo del 2008 da parte dell'ICANN Securtiy and Stability Advisory Committee (SSAC)[44]. L'ICANN è particolarmente sollecitato da questo problema in quanto alla base dei servizi fast flux vi è lo sfruttamento del DNS attraverso IP "fast flux" (A record con TTL breve) e cambiamento dei name server (double fast flux).

In questo primo rapporto, SSAC porponeva già una serie di possibili soluzioni volte a mitigare l'espansione del fenomeno. Tra di esse ricordiamo la sospensione dei bots che ospitano l'infrastruttura fast flux, la sospensione dei nomi a dominio coinvolti e la limitazione nel cambiamento dei name server.

---

42 http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ah2oZn4Z2qZpnO2Yuq2Z6gpJCDdIB7gGym162epYbg2c_JjKbNoKSn6A— (stato 01.09.2009)

43 http://www.icann.org (stato 01.02.2009)

44 http://www.icann.org/en/committees/security/sac025.pdf (stato 01.09.2009)

In seguito a questo rapporto, la Generic Names Supporting Organization (GNSO) dell'ICANN[45] ha pubblicato nel gennaio del 2009 un primo rapporto redatto dal Working Group on fast flux hosting (FFWG[46]). La versione finale del rapporto è apparsa il 6 agosto 2009[47].

Nella prima parte analizzeremo il rapporto appena pubblicato, nella seconda le iniziative di altre associazioni volte a limitare le reti fast flux illegali (soprattutto nell'ambito del phishing) e nella terza parte vedremo ciò che si sta facendo in Svizzera per adattare la legislazione in questo ambito.

Parte prima

Il primo problema incontrato dalla GNSO è stato quello di definire e differenziare le reti fast flux utilizzate a scopi illegali (fast flux attack networks) dalle reti volatili (volatile networking) utilizzate in ambiti legali. In seguito al rapporto intermedio del gennaio 2009, l'ICANN ha dato la possibilità alla comunità di criticare la ricerca finora compiuta. Ne è scaturito materiale interessante, di provenienza soprattutto dai maggiori attori del settore ma anche da privati cittadini. Vi è stata una presa di coscienza che diversi operatori utilizzano tecniche simili alle reti fast flux per la gestione delle loro attività. Chi ha dunque bisogno di questo tipo di reti?

- Organizzazioni che gestiscono reti con alto potenziale di aggressione (reti governative, militari, ma anche di multinazionali o attori importanti di Internet): esse devono essere praticamente sempre disponibili e poter usare *TTL* brevi per poter riallocare le risorse necessarie;

- Reti di distribuzione di contenuto (come ad esempio Akamai): in questo caso le reti volatili permettono di bilanciare il carico generato dalle comunicazioni su più server o diminuire i tempi d'attesa avendo diversi server sparsi in altrettante zone geografiche;

- Supporto alla mobilità: anche in questo caso TTL brevi permettono di costruire reti ad hoc per supportare un certo tipo di mobilità;

- Libertà di parola / gruppi d'interesse: evitare la censura e permettere la pubblicazione di materiale altrimenti impossibile da rendere pubblico (vi sono altre tecniche oltre alle reti fast flux, come ad esempio Tor, che permette di ospitare materiale su macchine difficilmente rintracciabili).

Queste considerazioni devono essere fatte a monte per poter identificare gli strumenti corretti volti a limitare le reti fast flux utilizzate a fini criminali. Ad esempio impedire TTL brevi sarebbe dannoso sia ai fast flux criminali ma anche a quelli legali. In seguito la GNSO ha cercato di definire le reti fast flux criminali, individuandone le caratteristiche principali:

- I nodi della rete possono (ma non devono) essere operati su macchine infettate;

- Sono volatili in quanto utilizzano un gruppo di bots per ottenere questo effetto;

- I bots si trovano dispersi su diversi sistemi autonomi (autonomous systems);

- Vi sono frequenti cambiamenti nel NS (name server);

---

[45] http://gnso.icann.org (stato 01.09.2009)
[46] http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.pdf (stato 01.09.2009)
[47] http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf (stato 01.09.2009)

- Gli IP delle macchine si trovano soprattutto nella fascia dei clienti finali a banda larga (ADSL, cavo TV);

- La qualità degli Whois è scarsa, vi sono poche informazioni (fasulle) sul registrante (registrant) dei nomi a dominio;

- Il proxy server nginx[48] si trova spesso installato sui bots, esso infatti permette la costituzione di reverse proxy creando un tunnel tra vittima, bot e la mothership che invia i contenuti (ad esempio una pagina web);

- Il nome di dominio è registrato attraverso un conto compromesso e quindi insospettabile;

- Spesso vi sono nomi a dominio che si susseguono con combinazioni numeriche (ad esempio as1.com, as2.com, as3.com e di seguito);

- L'unico scopo della reste fast flux è quella di prolungare l'attacco (ad esempio un attacco di phishing contro un istituto finanziario).

In seguito a queste considerazioni sono maturate due differenti correnti di pensiero volte a contrastare le reti fast flux con fini illegali. La prima che predica lo scambio di informazioni come strumento di lotta, la seconda che vorrebbe azioni più concrete da parte dell'ICANN e dei suoi affiliati (registries e registri[49]). Per quanto riguarda lo scambio di informazioni sono state proposte le seguenti idee:

- Rendere pubbliche informazioni non sensibili per quanto riguarda i nomi a dominio registrati attraverso le richieste DNS (e non Whois). Le informazioni potrebbero includere l'età del dominio, la quantità di cambiamenti del name server durante un periodo determinato e simili;

- Pubblicare un riassunto dei reclami contro un dominio ordinato per registro, TLD, o name server;

- Incoraggiare gli ISP ad utilizzare netflow/sflow per identificare l'esistenza di bot all'interno della loro clientela;

- Stimolare le iniziative private volte a rafforzare lo scambio di informazioni (come ad esempio l'Anti-Phishing Working Group per quanto riguarda la lotta al phishing)

Dall'altro lato vi sono i fautori di una più incisiva azione da parte dell'ICANN e dei suoi affiliati i quali propongono le seguenti soluzioni:

- Adottare procedure velocizzate per sospendere un nome a dominio in collaborazione con organi ufficiali accreditati;

- Stabilire delle regole nell'utilizzo di TTL brevi e limitare il numero di modifiche che si possono apportare in un dato intervallo di tempo agli A o NS record;

- Identificare i name server come statici o dinamici. Se statici, l'indirizzo IP del name server deve essere fornito. Se dinamici, si potrebbe considerare di imporre una sovrattassa;

---

[48] http://nginx.net (stato 01.09.2009)

[49] Registries: sono gli organi che si occupano di distribuire le risorse di allocazione dei numeri Internet (numeri IP, sistemi autonomi). Registri sono invece gli organi che ci occupano di gestire la riservazione di nomi a dominio.

- Imporre una sovrattasse per i cambiamenti dei name server statici, la quale sarà attribuita in egual misura a ICANN e registro. I fondi raccolti saranno utilizzati per migliorare la lotta contro gli abusi;

- Migliorare le procedure di registrazione dei nomi a dominio;

Come vedremo più avanti alcune di queste procedure sono già state adottate o sono in consultazione in Svizzera. Altre invece non hanno riscontrato il favore delle associazioni interessate, soprattutto quella che vuole imporre una sovrattassa per il cambiamento dei name server. Sarebbe, a livello commerciale, controproducente.

A fine rapporto, il gruppo di lavoro raccomanda di analizzare le seguenti idee per un futuro sviluppo:

- Identificare quali soluzioni di quelle proposte potrebbero venir adottate in ambito legislativo, o integrate in ambito commerciale o semplicemente generare delle best practices;

- Valutare in quale modo registries e registri possono venir coinvolti nella politica di sospensione di nomi a dominio;

- Implementare un Fast Flux Data Reporting System (FFDRS), ovvero una banca dati che raccolga informazioni sulle reti fast flux;

- Identificare ICANN come promotore di best practices volte a regolamentare maggiormente il settore con lo scopo di limitare gli atti illeciti;

- Esplorare la possibilità di coinvolgere altri partners nel processo di sviluppo di politiche di lotta contro i fast flux illegali.

Parte seconda

Nel rapporto finale del gruppo di lavoro del GNSO, si sono spesso citate le iniziative di altre associazioni volte a limitare le reti fast flux illegali (soprattutto nell'ambito del phishing). Ora vedremo più da vicino di cosa si tratta.

Sicuramente uno dei gruppi più attivi in questo ambito è l'Anti-Phishing Working Group (APWG[50]). Si tratta di un'associazione di attori economici votata alla lotta contro il furto di identità e la frode a seguito di phishing e degli e-mail che lo propagano. In un rapporto dell'ottobre 2008[51], l'APWG si indirizza ai registri proponendo loro delle raccomandazioni per prevenire o mitigare il fenomeno del phishing.

Secondo l'APWG le soluzioni a disposizione sono diverse e spaziano dall'educazione dell'utenza fino alle tecniche d'individuazione delle frodi, passando per sistemi di autentificazione complessi e risposte rapide per la sospensione di un sito di phishing. Le 5 principali raccomandazioni sono le seguenti:

- Un processo velocizzato per la sospensione di nomi a dominio che comprende la stretta collaborazione tra registro e gli organi ufficiali accreditati;

---

[50] http://www.antiphishing.org (stato 01.09.2009)

[51] Anti-Phishing Best Practices Recommendations for Registrars, http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf (stato 01.09.2009)

- Utilizzare attivamente i dati raccolti per identificare e sospendere i nomi a dominio utilizzati per gli attacchi;

- Scambiare le informazioni di registrazione dei nomi a dominio utilizzati per gli attacchi con le forze dell'ordine;

- Proteggere i clienti dai tentativi di phishing. Una volta ottenuti i dati dei registranti, cioè i clienti dei registri, i criminali possono cambiare i DNS dei domini già esistenti o registrarne di nuovi utilizzando l'identità insospettabile di un cliente normale52;

- Proibire o limitare l'utilizzo di siti fast flux. Con questo si intendono le limitazioni per quanto riguarda i cambiamenti dei name server o un minimo di minuti per il TTL.

Il rapporto dell'APWG inoltre inserisce una serie di ulteriori raccomandazioni:

- Una volta identificato un nome a dominio legato ad una attività illegale, oltre alla sua sospensione bisognerebbe cercare oltre e vedere se con gli stessi dati (nome, IP, email, indirizzo, carta di credito) sono stati registrati altri nomi a dominio;

- Avere un sistema di bloccaggio per le registrazioni ritenute sospette (registrar lock), in seguito raccogliere la maggior quantità possibile d'informazioni, dall'http request headers fino ai dati personali del registrante. In seguito cercare di validare i dati ottenuti: analizzare se vi sono nomi a dominio con caratteristiche simili (ad esempio se si susseguono con combinazioni numeriche come mostrato più in alto), identificare se all'interno dei nomi vi sono parti di nomi a dominio o marche già conosciuti (eBay, PayPal, vari istituti finanziari), esaminare gli indirizzi IP utilizzati per registrare i nomi, e cercare di validarli confrontandoli con le liste nere disponibili (come la Spamhaus XBL), esaminare gli indirizzi email e verificarne l'autenticità, obbligare l'inserimento sia del "fully qualified domain name" (FQDN) sia degli indirizzi IP, verificare le carte di credito utilizzate;

- In seguito si potrebbe sviluppare un sistema di attribuzione di un punteggio per i dati raccolti, ottenendo così un metodo di screening il più preciso possibile;

Le proposte dell'APWG sono molteplici e domandano uno sforzo e una volontà di cooperazione importanti. Ma l'APWG non è l'unico ad essersi mosso in questa direzione. Vi sono altre iniziativi degne di nota. Ad esempio il Whois Data Problem Reporting Service (WDPRS)[53] Si tratta di un'interfaccia web che permette a qualsiasi utente di inviare un'informazione ai registri affiliati all'ICANN per quanto concerne i dati Whois incompleti o chiaramente fasulli di nomi a dominio. Questo può essere un primo indizio di un utilizzo fraudolento di questi nomi. Un'altra iniziativa è il portale Phishtank[54]. Attraverso questo portale chiunque ha la possibilità di segnalare un e-mail di phishing (e il relativi nome di dominio in esso inserito). La banca dati così costituita è messa a disposizione, nel senso che chiunque può testare un indirizzo per sapere se si tratta di un sito di phishing già conosciuto. Altre attività sono promosse da Messaging Anti-Abuse Working Group (MAAWG[55]), un gruppo di lavoro che riunisce i maggiori attori mondiali nell'ambito della messaggeria elettronica, la fondazione ShadowServer[56], che si occupa principalmente di monitorare le

[52] http://www.icann.org/committees/security/sac028.pdf (stato 01.09.2009)
[53] http://wdprs.internic.net (stato 01.09.2009)
[54] http://www.phishtank.com (stato 01.09.2009)
[55] http://www.maawg.or g (stato 01.09.2009)
[56] http://www.shadowserver.org (stato 01.09.2009)

attività delle reti bot e StopBadware[57], che si concentra sulla creazione di una banca dati dei codici nocivi diffusi in rete.

Parte terza

La Svizzera, dal canto suo, non è proprio stata a guardare. Anzi, alcune innovazioni legislative hanno permesso di dare il via alla lotta contro questo tipo di criminalità. Un primo passo è stato compiuto con la modifica delle condizioni generali del registro dei nomi a dominio ".ch", la fondazione SWITCH. In effetti fino all'inizio del 2009, era possibile acquistare un nome a dominio e utilizzarlo immediatamente. Una fattura veniva emessa e quindi si avevano a disposizione almeno 30 giorni per utilizzare il prodotto acquistato. Questo poteva facilitare il compito dei malintenzionati, che vedevano la possibilità di registrare nomi a dominio per la durata di un mese senza dover pagare. A scadenza del mese, dopo le pratiche di richiamo, il nome a dominio poteva venir sospeso. Per evitare questo tipo di sfruttamento, SWITCH ha modificato le clausole del contratto di registrazione[58]. Ora nelle condizioni contrattuali si può leggere che "l'iscrizione nel zone file avviene di norma entro le 24 ore dall'elaborazione da parte di SWITCH del pagamento pervenuto". In sostanza per utilizzare un nome a dominio bisogna pagare anticipatamente. Questa prima misura è stata un valido deterrente contro le massicce registrazioni dei ".ch" utilizzati a scopi di phishing durante il 2008.

Ma non finisce qui. L'Ufficio federale della Comunicazione (UFCOM) ha elaborato un progetto di legge che deve ancora essere sottoposto agli organi politici. Esso prevede l'aggiunta di un articolo nell'Ordinanza concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT). Questo articolo prevede la possibilità da parte di SWITCH di bloccare e sopprimere un nome a dominio ".ch" nel caso in cui si sospetti che esso:

- Viene utilizzato per veicolare codici nocivi;
- Viene utilizzato per accedere attraverso metodi illeciti a dati sensibili

L'informazione di sospetto deve pervenire da un organo accreditato dall'UFCOM.

Il punto più importante e maggiormente discusso nei vari rapporti (ad esempio nel documento dell'APWG o della GNSO di cui abbiamo visto i particolari più sopra) è stato appunto quello di adottare delle procedure snelle per poter sospendere o sopprimere un nome a dominio grazie alla collaborazione tra registri e organi accreditati. Con questo progetto di modifica di legge, la Svizzera potrebbe fare un gran passo avanti nella lotta alla criminalità nel cyberspazio.

[57] http://www.stopbadware.org (stato 01.09.2009)

[58] https://www.nic.ch/reg/ocView.action?res=EF6GW2JBPVTG67DLNIQXU234MN6SC2T4PAQGM6TDMI#a8 (stato 01.09.2009)

7.2 Parametraggio dei navigatori contro le più comuni infezioni drive-by

Introduzione

Ogni pagina Web consta di diverse istruzioni, il cosiddetto codice HTML, che prescrivono al browser (p. es. Internet Explorer) le modalità di riproduzione dei contenuti delle pagine Web. Alcune pagine Web constano unicamente di documenti di testo e non offrono funzioni supplementari (pagine statiche), mentre altre offrono contenuti dinamici. Ne sono esempio le scritte scorrevoli, i formulari Web per gli ordini online, le immagini animate o i banner pubblicitari inseriti dinamicamente. Queste funzioni dinamiche possono essere realizzate con i controlli ActiveX e con JavaScript. Purtroppo se ne abusa per provocare azioni indesiderate e nocive sul computer del visitatore.

In linea di massima vale quanto segue:

Aggiornare regolarmente il sistema operativo e le applicazioni
Alcuni prodotti mettono a disposizione una funzione di aggiornamento automatico che si dovrebbe assolutamente utilizzare. Verificate regolarmente se tale funzione è attivata. Le informazioni sugli aggiornamenti attuali del software sono solitamente disponibili sulle pagine Web dei pertinenti produttori.

Limitare i JavaScript
Limitate nella misura del possibile (o disattivate) l'esecuzione di JavaScript (Active Scripting, o script attivo) tramite la configurazione del browser. In questo caso va comunque osservato che numerose pagine Web non funzionano più correttamente. Se ne doveste essere fortemente perturbati nella navigazione diminuite (gradualmente) le limitazioni fino alla misura sopportabile.

Limitare i controlli ActiveX (solo per Internet Explorer)
Limitate nella misura del possibile l'esecuzione dei controlli ActiveX tramite la configurazione del browser.

Modificate i parametri di sicurezza di Internet Explorer sul livello «alto». Le pagine 5 e 6 della guida «Parametri di sicurezza per Windows XP»[59] spiegano passo per passo il modo di procedere (questa guida di definizione dei livelli di sicurezza di Internet Explorer vale anche per altri sistemi operativi Windows).
Importante: dato che l'Active Scripting è utilizzato da numerose pagine Web su Internet, alcune di queste non sono più riprodotte integralmente dopo la modifica di questi parametri. Per questo motivo raccomandiamo di inserire le pagine frequentemente consultate (e che considerate affidabili) nell'elenco dei «siti attendibili». Le relative modalità di inserimento figurano anch'esse alla pagina 6 del documento «Parametri di sicurezza per Windows XP».

Attenzione: in Internet Explorer l'uso del livello di sicurezza alto comporta la disattivazione automatica delle seguenti funzioni: JavaScript, IFrame e Aggiornamento metadati.

[59] http://www.melani.admin.ch/dienstleistungen/00132/00149/index.html?lang=it (stato: 01.09.2009)

Qui appresso esaminiamo le singole minacce nel settore delle infezioni drive-by e proponiamo misure corrispondenti.

Caso 1: JavaScript offuscato (camuffato) (Per il tramite di JavaScript si tenta di dirottare il computer su una pagina nociva)

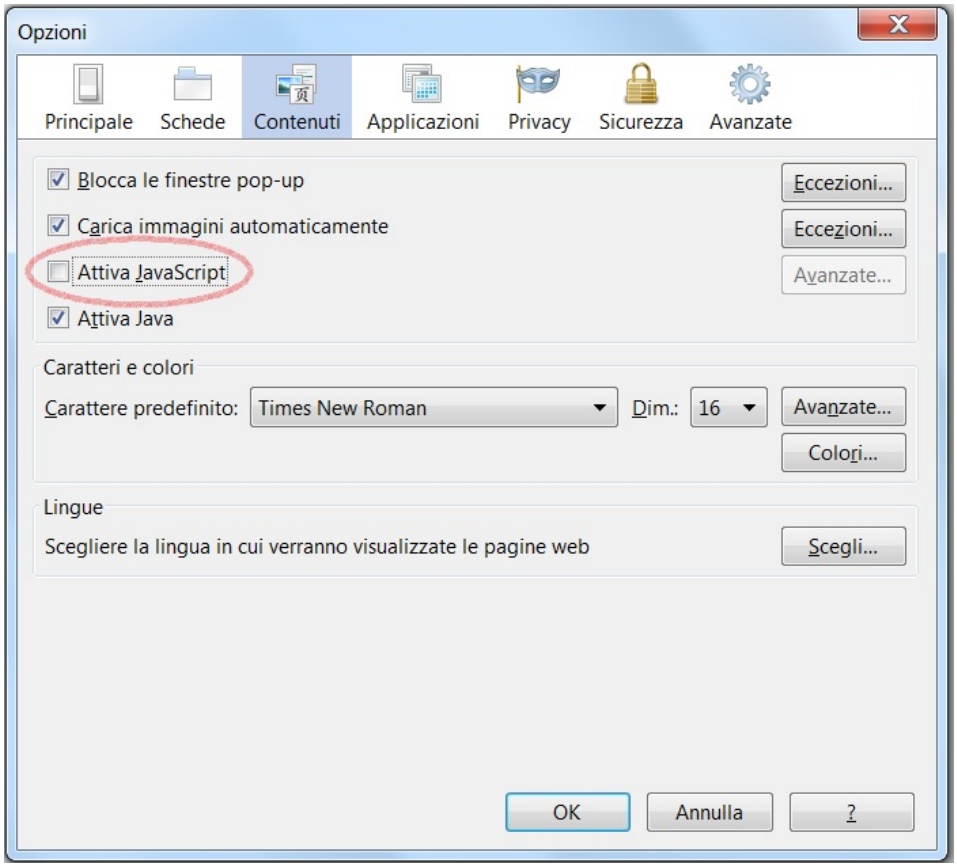
➔ Soluzione: disattivare JavaScript

➔ Inconveniente: le pagine che utilizzano JavaScript non funzionano più

Firefox

Possibilità 1: utilizzare il programma NoScript[60]. Con il suo ausilio è possibile ripristinare durevolmente o per breve tempo JavaScript su singole pagine.

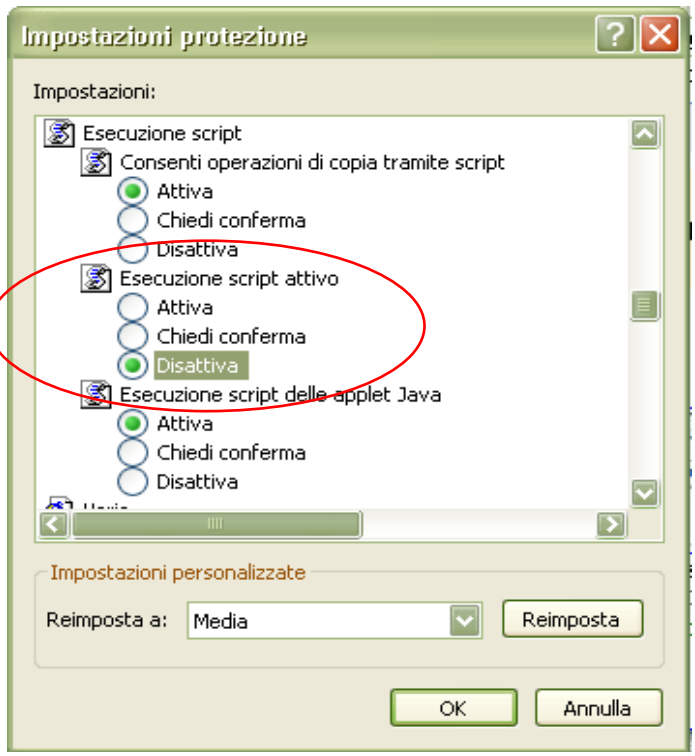
Possibilità 2: sotto Opzioni ➔ Configurazione ➔ Contenuto: disattivare JavaScript.



Internet Explorer

Sotto Strumenti ➔ Opzioni Internet ➔ Protezione, adeguare il livello di protezione per l'area. Lo scripting può essere disattivato automaticamente o attivato (prompt) per ogni pagina contenente JavaScript .

[60] https://addons.mozilla.org/it/firefox/addon/722 (stato: 01.09.2009)



Caso 2: Exploit IFrame-Exploit (il browser apre una pagina nociva in sottofondo per il tramite di un IFrame – pagina nella pagina).

➔ Soluzione: disattivare gli IFrame

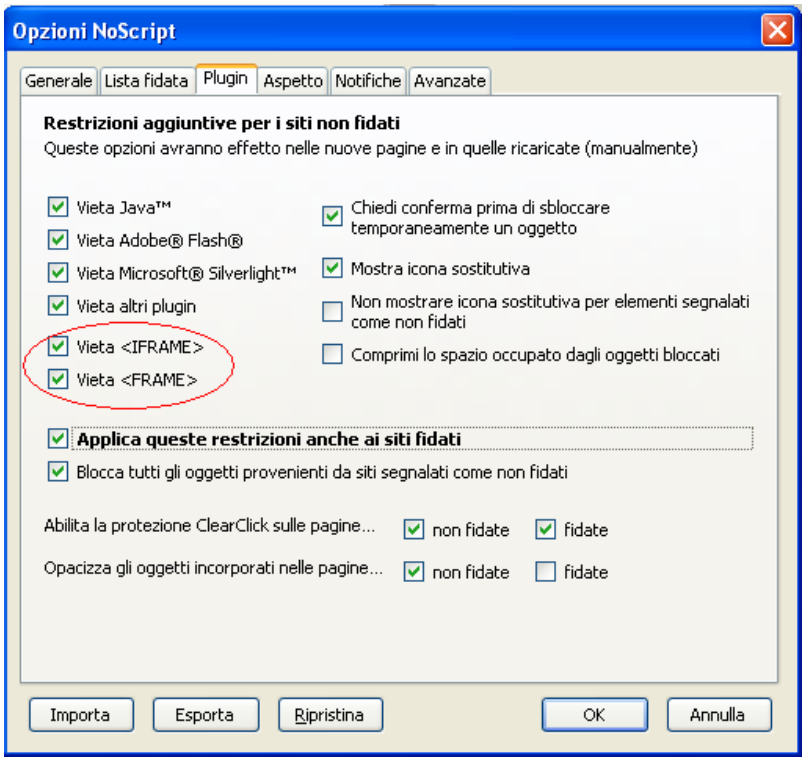
➔ Inconveniente: la pagine che necessitano di IFrame funzionano solo parzialmente

Firefox

Possibilità 1: utilizzare il programma NoScript

Dopo aver installato del programma NoScript, cliccare sul tasto destro del mouse nel browser, selezionare NoScript e passare alla rubrica «Configurazione»

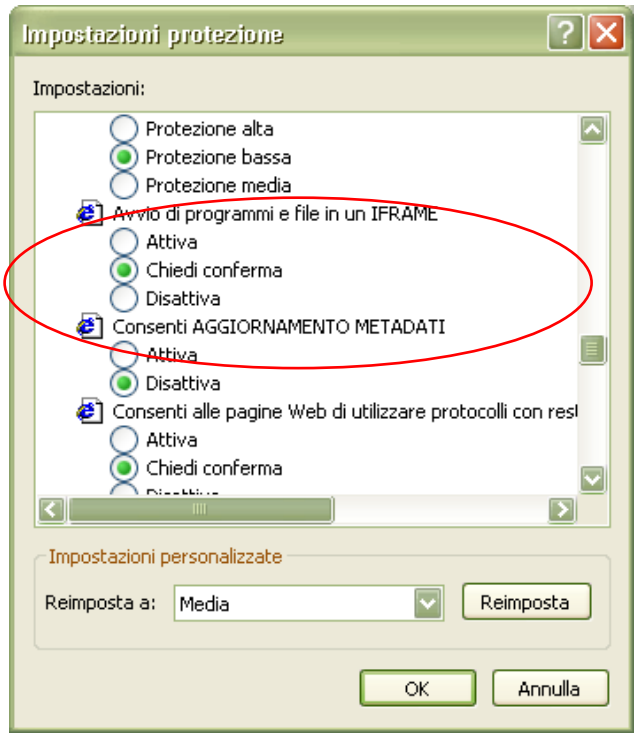
Selezionare «Vieta <IFRAMES>» e «Vieta <IFRAME>»



Possibilità 2: Immettere nella barra degli indirizzi del browser il comando: **About:config** e impostare la funzione **Browser.frames.enabled** su **false**.

Internet Explorer

Sotto Strumenti ➔ Opzioni Internet ➔ Protezione, adeguare il livello di protezione per l'area. Gli IFrame possono essere disattivati automaticamente o attivati (prompt) mediante conferma manuale per ogni pagina contenente un IFrame.



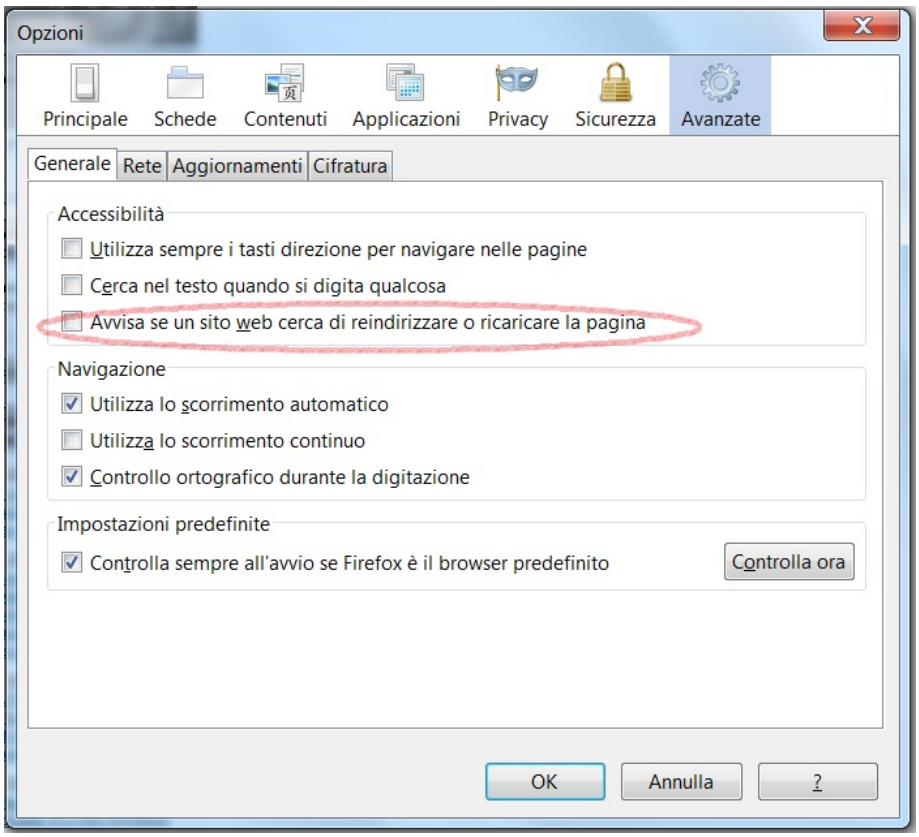
Caso 3: Aggiornamento di metadati (Per il tramite del comando di aggiornamento dei metadati il browser è reindirizzato automaticamente su una pagina nociva).

➔ Soluzione: limitare gli aggiornamenti di metadati

➔ Inconveniente: le pagine che prevedono un reindirizzamento funzionano solo parzialmente

Firefox

Sotto Opzioni ➔ Configurazione «Avverti quando i siti Web tentano un reindirizzamento o un aggiornamento». Ogni volta che si tenta di reindirizzare il browser occorre darne conferma manuale.



Internet Explorer

Sotto Strumenti ➔ Opzioni Internet ➔ Protezione ➔ Livello personalizzato: nell'area Internet l'aggiornamento dei metadati può essere disattivato completamente.