Cina: il mercato illegale su Internet

Il mercato illegale cinese utilizza il canale della Rete per frodare gli utenti italiani.

Rossano Ferraris

Il mercato nero non è affatto un fenomeno nuovo in quanto sappiamo che esso esiste da molto tempo con la presenza di prodotti e servizi illegali subito disponibili come droga, sesso e merce rubata.

Caso di analisi

Vorrei portare all'attenzione degli utenti un caso che sto monitorando e che ho esaminato con attenzione molto recentemente.
Secondo le osservazioni svolte nell'arco di tre mesi si è notato che le caselle di posta elettronica italiane sono state bersagliate da innumerevoli email che offrono componenti elettroniche a prezzi più che interessanti.
Ciò che attira maggiormente l'attenzione dell'utente sono le offerte proposte a costi notevolmente inferiori al normale prezzo di mercato.
L'email inoltre suggerisce all'utente di visitare il loro sito per dare un'occhiata alle proposte.

Rossano Ferraris, Senior Research Engineer per Total Defense Inc.

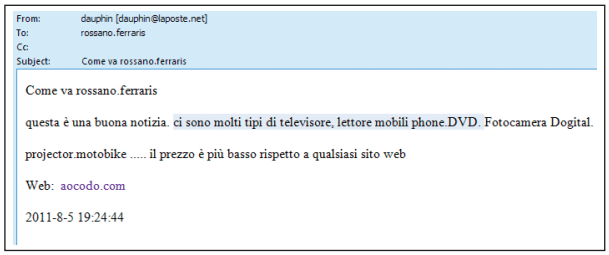

Figura 1 – Esempio di email ricevuta

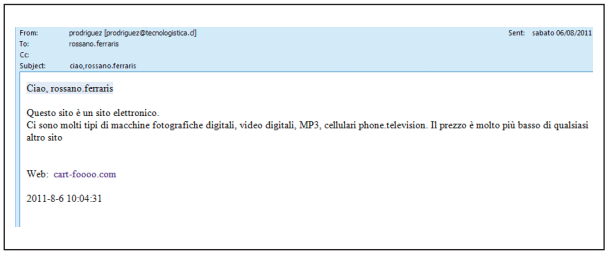

Figura 2 – Altro esempio di email ricevuta

Un altro aspetto interessante di questa forma di marketing promozionale è la richiesta di ricevuta di lettura.

Figura 3 – Richiesta di ricevuta di lettura

Dal punto di vista dell'analisi fin qui svolta si evince che l'intento dell'autore di questo sistema è quello di registrare le email che hanno avuto esito positivo (l'utente ha dato conferma di ricezione) per scopi personali:

- vendere le email registrate e attive agli spammer
- utilizzare le email attive per inviare ulteriori informazioni promozionali attraverso marketing illegale

Proseguendo con l'analisi si scopre che tutte le email ricevute – che apparentemente sembrano provenire

da utenti differenti – in realtà fanno riferimento ad una precisa località in Cina che pare essere la stazione di comando dell'autore del sistema di frode.

Figura 4 – Geolocazione della rete usata dall'autore del sistema di frode

Sicuramente tali coordinate non appartengono ad alcuna compagnia o azienda che offre servizi o vende componenti elettronici.
Ad ogni modo si procede con l'analisi del sito web:

Figura 5 – aocodo.com

da una prima osservazione si nota che il sito è molto ben organizzato, con un servizio di chat-live online disponibile per rispondere ad eventuali richieste degli utenti.
Inoltre il sito presenta molte offerte di prodotti di alta tecnologia e di ultima generazione a prezzi decisamente sotto costo.
Questo fatto genera ulteriori sospetti, non che prima non ne avessimo, che ci portano a svolgere ulteriori indagini e verifiche.
Dopo l'analisi della registrazione del sito risulta che un tale Mr. Chu WenBo è il proprietario del sito web aocodo.com registrato con scadenza di 1 anno: elemento sufficiente per giustificare i nostri sospetti iniziali. Un sito web aziendale ha una registrazione permanente e non temporanea, pertanto questo fa pensare immediatamente ai casi di siti scam che per non essere rintracciabili utilizzano scadenze molto brevi.

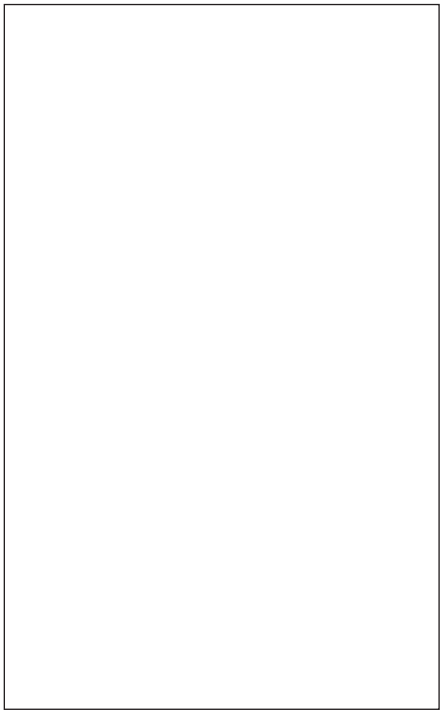

Figura 6 – Dettagli registrazione sito web

Inoltre in ulteriore analisi i dati telefonici forniti nella registrazione risultano appartenere al governo cinese.

Figura 7 – Mappa uffici governativi cinesi

Quale pericolo se si è fatto un acquisto?

Quali possono essere le conseguenze di un acquisto su un sito tipo aocodo.com?
Sono state ipotizzate e in alcuni casi realmente verificate 3 situazioni a seguito di un acquisto presso un sito come quello analizzato:

- Merce rubata: può fare parte di una operazione più grande che va sotto il nome di "money laundering" o riciclaggio; in questi casi l'utente è ingenuamente coinvolto in un gioco criminale punibile (in caso di rintracciamento e denuncia) dalle leggi locali italiane.
- Furto di carte di credito: l'operazione di acquisto prevede l'utilizzo di carta di credito; chi può dire che tale operazione non comporti il furto dei dati della carta?
- Soldi sprecati: è il caso migliore (tra i peggiori sopra menzionati) in quanto l'utente ha proceduto con l'acquisto di un bene che mai riceverà.

Conclusioni

Ovviamente di fronte ad un'economia come quella che stiamo assistendo, gli utenti sono fortemente attratti da offerte di acquisto interessanti soffocando ogni forma di allerta nei confronti di possibili frodi rendendo pertanto il mercato illegale fiorente e produttivo.
Internet si sta dimostrando un eccellente canale di comunicazione anche per questo mercato che nasconde forti e remunerative operazioni illegali a danno degli utenti di Internet e a vantaggio dei criminali.
Si raccomanda di:

- diffidare delle email il cui mittente è sconosciuto o sospetto;
- mantenere un'alta dose di scetticismo nei confronti di siti web commerciali che offrono servizi e prodotti a costi fortemente ridotti;
- dotarsi di software di sicurezza dotati do moduli anti-spam e filtro dei siti web;
- se si pensa di essere vittima di un sito web illegale com quello analizzato, avvertire immediatamente le autorità locali.

Rossano Ferraris

Rossano Ferraris è laureato in Informatica e possiede le certificazioni SANS (GCIH, GCFA, GREM).
Attualmente ricopre il titolo di Senior Research Engineer per Total Defense Inc. (www.totaldefense.com) ex divisione di CA Tecnologies ISBU.
È membro e co-fondatore del team ISI (Internet Security Intelligence) all'interno del Dipartimento di Ricerca della ISBU (Internet Security Business Unit) con la responsabilità di guidare l'area EMEA nello studio, analisi e tracciamento delle minaccie emergenti.
Consulente presso la Procura della Repubblica e le Forze dell'Ordine in materia di analisi forense e tematiche legate ai crimini informatici in Italia.
È inoltre socio AIPSI (capitolo italiano ISSA) e impegnato in attività di sensibilizzazione attraverso interventi pubblici e la scrittura di pubblicazioni sulle insidie provenienti dalla rete.
Rossano Ferraris è co-autore del libro "Qualcuno ci spia: spyware nel tuo pc", edito da Mondadori (2005) e ideatore del blog "SecuritySurfer" (www.securitysurfer.it).