

# Report 2006

## Italia: il miele che attira i malware



**v.2**  
*05/01/2007*

**Marco Giuliani**  
Prevx Malware Analyst  
[marco@prevxresearch.com](mailto:marco@prevxresearch.com)

## - INTRODUZIONE -

Per gli esperti del settore, ricercatori di sicurezza informatica o semplici interessati all'argomento, l'anno che si sta per chiudere segna un **cambio di rotta fondamentale** nella storia delle infezioni informatiche in Italia.

Fino a qualche anno fa, il mondo intero era paese quando si parlava di una possibile infezione di qualche nuovo malicious software. Lo scopo era quello di **infettare quanti più computer possibili**, a volte lanciandosi sfide personali tra i vari team che si occupavano di sviluppare determinati software malevoli.

Abbiamo visto, caso più recente, la guerra che era stata iniziata tra i creatori dei worm **Netsky, Bagle e Mydoom**, portata avanti per mesi interi e che ha visto come terreno di guerra l'intera utenza di internet. Recita, in modo più o meno esatto, un detto: *tra due elefanti che si scontrano, chi ne esce sconfitto è sempre l'erba*. Per mesi i tre worm si sono contesi la top ten dei malware più diffusi nel 2005.

Torniamo più indietro, vediamo nel 2003 e poi 2004 i casi clamorosi dei worm **Blaster e Sasser**, altro chiaro simbolo di un tentativo di infettare quanti più computer in tutto il mondo nel minor tempo possibile sfruttando due falle di sistema scoperte in Microsoft Windows.

Nel 2006 non ci sono stati casi particolarmente eclatanti. Infezioni dovute a worm, trojan, backdoor, ma niente di particolarmente grave a livello mondiale. Possiamo trovare una spiegazione se andiamo ad analizzare cosa è cambiato nel corso di questi anni: solo cambiando modo di osservare la situazione è possibile focalizzare la vera situazione di un anno, quello trascorso, che è risultato per l'Italia molto più dannoso di tanti anni passati precedentemente.

Bisogna innanzitutto focalizzarsi sullo **scopo perseguito** da chi scrive malware per computer. Se, negli anni passati, chi scriveva virus – si potevano ancora chiamare così – lo faceva al solo scopo di mostrare la propria bravura al mondo intero, negli ultimi cinque anni la rotta è sostanzialmente cambiata. La società

si è informatizzata sempre più, l'utilizzo dei pc è entrato di forza in ogni azione quotidiana, negli uffici statali, nelle società, in aziende piccole, medie e grandi. Il buon esito di un'infezione di uno di questi pc potrebbe significare l'**avere accesso a informazioni private**, da numeri di carte di credito a sottrazione di dati sensibili, con conseguenze che possono spaziare da furti di identità a vero e proprio **spionaggio industriale**. In altre parole, soldi.

Ecco che cambia sostanzialmente lo scopo di scrivere un malware informatico. Non più infettare tutti i file eseguibili che si trovano all'interno di un pc al puro scopo di mostrare un messaggio all'avvio, o un worm che sposta le icone o – peggio – cancella determinati file, bensì backdoor per controllare da remoto un pc, trojan per rubare informazioni, spyware per controllare le abitudini di uno user.

Cambiano anche i **target**, gli obiettivi di una possibile infezione. Ne sono un esempio tutti i worm che si sono diffusi a livello mondiale in maniera rapida, hanno attirato l'attenzione di tutti i ricercatori di sicurezza mondiali, portando ad una **rapida soluzione** del problema con aggiornamenti per i software antivirus. Chiaro che, mirando un solo obiettivo molto più piccolo, le possibilità di infezione sono maggiori e le capacità di isolamento, analisi e rimozione sono molto più limitate.

Ecco che vanno diffondendosi in questi ultimi anni i cosiddetti **attacchi mirati**, attacchi ben studiati verso un preciso obiettivo, evitando di dare così nell'occhio e potendo lavorare molto più tranquillamente con più possibilità di successo. Ne è un esempio l'attacco subito ad inizio 2006 dalla società che gestisce la borsa russa - *Russian Trading System (RTS)* – paralizzata per alcune ore dopo che un malware sconosciuto si era fatto un bel giro panoramico della rete interna rischiando di causare seri danni economici.

La tecnica degli attacchi mirati, differentemente dallo "sparare alla cieca", risulta essere sostanzialmente molto più proficua e pericolosa, proprio perché

non è visibile all'intero mondo e, come tale, impossibile in alcune circostanze da monitorare continuamente se non da chi vive personalmente l'attacco.

Per nascondere ancor di più eventuali attacchi mirati, si è andato diffondendo l'utilizzo di **rootkit**, particolari malware che – interagendo a basso livello con il sistema operativo Windows, riescono a nascondere agli occhi degli utenti i malware che poi si occupano di rubare informazioni, o che permettono il controllo da remoto del pc, o qualunque altro sia il payload.

Lo sviluppo dei rootkit per il sistema operativo Microsoft Windows è relativamente nuovo e molto più giovane rispetto a virus, trojan, worm o backdoor, sebbene il concetto su cui si basano è molto più antico e risale principalmente ai sistemi \*nix.

Al momento la combinazione di rootkit e attacchi mirati risulta essere l'arma migliore, tanto da rendere spesso molto difficile l'individuazione di una possibile infezione. Un pericolo, quello dei rootkit, che ha scosso particolarmente tutte le società di antivirus, le quali sono corse ai ripari sviluppando **nuove tecnologie per la rimozione** – sebbene, come ormai è storia vecchia nella guerra tra virus e antivirus, vengano spesso aggirate da nuovi rootkit studiati *ad hoc* per eluderne l'individuazione.

Quello che l'Italia ha potuto assaggiare nel 2006 è stata proprio questa combinazione, alcuni **attacchi mirati** che di fatto hanno infettato migliaia di pc senza che gli utenti se ne rendessero assolutamente conto.

Il caso più eclatante, quello di **Gromozon**, ha messo in evidenza quali siano state le forti difficoltà da parte delle società di sicurezza a monitorare attacchi mirati e a contenerne lo sviluppo e la diffusione. Ma Gromozon non è il solo, perché il 2006 ha riservato alcune sorprese particolarmente sgradite agli utenti italiani.

## - - TECNICHE DI ATTACCO CONTENUTO -

Come già specificato nell'introduzione, le tipologie di attacco a cui gli utenti sono stati abituati sono quelle **globali**, capaci di colpire – anche in maniera epidemica – gli utenti italiani come gli utenti statunitensi o giapponesi, in qualunque parte del mondo.

Risulta dunque interessante analizzare più da vicino come sia possibile contenere – o tentare di contenere il più possibile - un attacco ad **una sola nazione**, come è successo in più riprese e con differenti infezioni in Italia durante questo anno.

Innanzitutto, la tecnica più banale utilizzata è la **scrittura di un'eventuale e-mail in lingua madre**, per l'appunto l'italiano. In Italia risulta essere una tecnica relativamente più efficace che in altre nazioni, proprio perchè l'inglese non è una delle lingue madri.

Ciò implica che, se un utente italiano di conoscenze medio/basse ricevesse una e-mail in inglese, la eliminerà con molte più probabilità rispetto ad una e-mail scritta nella sua lingua madre. Giocoforza, per effetto contrario, una e-mail scritta in italiano difficilmente sarà presa in considerazione all'estero, dove la lingua italiana è raramente parlata.

Di fatto, con questa banale tecnica, un malware che si diffonde attraverso delle e-mail scritte in lingua italiana sarà con molta probabilità contenuto all'interno del territorio italiano. Questa modalità di diffusione **non esclude** ovviamente che e-mail vengano spedite all'estero, se qualche utente ha contatti in rubrica con persone straniere che non parlano italiano.

Questa tecnica, vista più volte nel corso degli anni precedenti, è utilizzata nei primi mesi del 2006 dal [Trojan.Spamlia](#) per diffondere il [Trojan.Bomka](#).

Sarà poi la tecnica anche utilizzata dai due trojan che hanno animato il fine 2006, cioè [Trojan.Spambot](#) e [Trojan.Hijacker](#).

Oltre alla semplice tecnica delle e-mail scritte in lingua madre, vengono utilizzati anche altri accorgimenti, visti in azione con il **Trojan.Spambot** ed ereditati dal [Gromozon](#), cioè il filtro degli indirizzi IP da server. Gli utenti, per rimanere infetti da Gromozon o dal Trojan.Spambot, devono collegarsi ad alcuni siti web che fanno da vettore di infezione, trasmettendo il malware. Interessante notare come, per arginare l'infezione allo stato italiano, **solo indirizzi IP provenienti dall'Italia hanno accesso all'infezione**. Tutti gli altri pc provenienti dalle restanti parti del mondo vengono reindirizzati ad altre pagine o viene mostrato un errore di server non raggiungibile.

Per quanto riguarda il **Gromozon**, un'altra modalità di contenimento dell'attacco al solo paese italiano utilizzata è il **creare siti web civetta contenenti collezioni casuali di parole italiane**. Collezionando molte parole sullo stesso sito, la pagina viene facilmente e rapidamente indicizzata dai motori di ricerca quali Google, permettendo così una facile individuazione da parte di utenti ignari che fanno semplici ricerche sul motore di ricerca.

Infine, sia il **Gromozon**, sia il **Trojan.Hijacker** che il [Rootkit.DialCall](#) installano un dialer che effettua chiamate verso numerazioni a tariffazione aggiunta presenti su linee italiane – numeri **899** e **892**.

Abbiamo dunque visto come la combinazione di:

- ✓ *e-mail inviate in lingua italiana;*
- ✓ *filtri sui server IP al fine di trasmettere infezioni ai soli pc italiani;*
- ✓ *creazione di pagine web ad hoc per catturare l'attenzione degli utenti italiani che fanno ricerche;*
- ✓ *l'utilizzo di dialer per numeri a tariffazione aggiunta presenti su linee telefoniche italiane*

possa rendere chiara l'idea di come i malware writer abbiano tentato di contenere su suolo italiano, con l'unione di tecniche vecchie e nuove, la diffusione di questi trojan.

Risulta altresì chiaro che, vista la diffusione della tipologia di attacchi mirati e di questi trojan che fanno utilizzo delle tecniche sopra descritte per contenere l'infezione, l'Italia sembra essere **finita sotto mira** dei virus writer come obiettivo "semplice" da attaccare e sul quale, magari, fare soldi facilmente.

Nel prossimo capitolo vedremo più in dettaglio i trojan citati.

## - MALWARE IN DETTAGLIO -

### Trojan.Bomka

Diffuso attraverso e-mail scritte in italiano quali, tra le più famose:

**OGGETTO:** Video caccia alle balene, drammatico

**TESTO:** a volte la tv non fa vedere certe cose... consiglio la visione del video allegato ad un pubblico "duro" buon lavoro a tutti

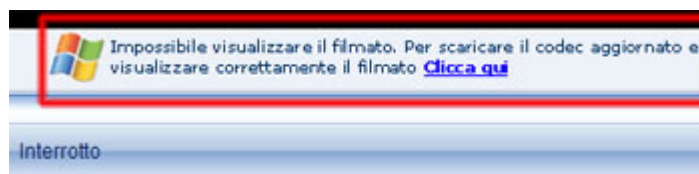
**ALLEGATO:** filevideo\_\_banned.asx

**OGGETTO:** che fine fanno gli eroi

**TESTO:** mi piacerebbe tanto sapere perchè certe cose non si vedono in TV ma solo in blog

**ALLEGATO:** archive\_banned\_in\_tv.asx

O numerose altre varianti. Il file allegato, con estensione **ASX**, un metafile utilizzato come indice al flusso di dati video. In realtà, il file è scritto a mano per mostrare questo banner nella finestra di Windows Media Player:



L'utente cliccando sul link **Clicca qui** scarica un finto codec, che in realtà installa il trojan **Bomka** sottoforma dei file **pio12.dll**, **msx.dll**. In una forma precedente, il trojan veniva diffuso attraverso un gioco di freccette realizzato in flash, **darts-freccette.exe**. Arrivava attraverso una e-mail quale:

**OGGETTO:** un attimo di relax

**TESTO:** Vi allego un giochetto divertente,  
è nello zip l'allegato!  
poi fatemi sapere il punteggio, il mio record è 67 :)

ciao

**ALLEGATO:** tiro\_a\_segno.zip

O varianti. Il gioco, una volta lanciato, registra la dll **kaboom.dll** come *Browser Helper Object (BHO)*, variante del trojan **Bomka** risalente a Gennaio/Febbraio 2006.

#### TECNICHE UTILIZZATE PER CONTENERE L'INFEZIONE

- ✓ *E-mail scritta in lingua italiana*

Come è possibile notare, la diffusione di questo trojan, queste precise varianti, tendono ad essere studiate per il territorio italiano, quindi a **colpire gli utenti italiani**. Tuttavia, come detto nel capitolo precedente, la tecnica non esclude che il trojan venga diffuso anche all'estero verso persone che conoscono la lingua italiana.

---

### **Gromozon**

Considerato da più esperti del settore come uno dei **rootkit user mode** meglio scritti, attacca l'Italia dai primi mesi del 2006. Report affermano che da Aprile si hanno già avvistamenti di questa infezione, sebbene sia Maggio il mese in cui cominciano ad avvisarsi più infezioni.

Il rootkit **ha un team attivo** alle spalle, che costruisce un'architettura a livello server ben articolata grazie alla quale diffondere l'infezione.

Vengono create delle pagine web contenenti parole in italiano scelte casualmente, in modo tale da comparire spesso nelle ricerche degli utenti sui motori di ricerca quali Google. L'utente che utilizza il browser Internet Explorer rimane infettato automaticamente navigando nella pagina web costruita *ad hoc*, poiché i server utilizzati per diffondere l'infezione sfruttano alcune falle del sistema operativo di Microsoft, quali la falla nella gestione dei file **WMF**.

Internet Explorer esegue automaticamente il JavaScript inserito nella pagina web. Il sito web reindirizza ad un server che fa da ponte e reindirizza verso il

vero server che distribuisce l'infezione.



Nelle versioni successive dell'infezione, il server che fa da ponte **filtra gli indirizzi IP**, reindirizzando i pc che provengono da fuori Italia ad un server non infetto. Solo gli IP provenienti dall'Italia vengono indirizzati al server che distribuisce l'infezione.

Da Luglio/Agosto 2006 inizia una sorta di "guerra" tra ricercatori di sicurezza informatica e il team che sviluppa il rootkit Gromozon, con continue varianti dell'infezione che attacca e blocca i tool di rimozione provenienti dalle società di sicurezza e blocca l'accesso a determinati siti web che forniscono indicazioni su come rimuovere l'infezione.



Migliaia di pc in tutta Italia vengono infettati. Il **CERT** (*Computer Emergency Response Team*) italiano rilascia un **bollettino** e vengono pubblicate le prime **analisi tecniche** dell'infezione.

Alex Eckelberry, presidente di **Sunbelt Software**, parlando di Gromozon:

*"Now, we've only seen Gromozon in Italy. Why Italy, you ask? I would guess poor legislation and enforcement, and a plethora of vulnerable machines."*

L'infezione risulta complessa a causa delle numerosi parti che la compongono. Il file iniziale, denominato **www.google.com**, installa nella directory di sistema una dll, dal nome pseudo-random, che si occupa di installare il rootkit, un adware, denominato **LinkOptimizer** e un dialer contenente undici numeri telefonici, di cui nove adibiti a linee italiane e due per numeri satellitari.

L'analisi dell'infezione, come già detto complessa, è riassunta in queste poche righe. Per un'analisi più approfondita sono disponibili le descrizioni tecniche di [Prevx](#) e [Symantec](#).

I server che distribuiscono l'infezione Gromozon scompaiono a poco a poco nel mese di Novembre 2006. Dopo aver informato Polizia Postale italiana e FBI, il **CERT** americano chiude uno dei server, situato in America, che distribuiscono l'infezione. Per un effetto "domino", tutti gli altri server vengono momentaneamente chiusi dal team. Verranno subito dopo aggiornati per distribuire altre infezioni, di cui alcune sono il **Rootkit.DialCall** mentre altre sono tuttavia più blande.

#### **TECNICHE UTILIZZATE PER CONTENERE L'INFEZIONE**

- ✓ *Siti web creati per utenti italiani, contenenti parole italiane inserite a caso;*
- ✓ *Filtri IP sul server che distribuisce l'infezione. Il rootkit non viene installato in maniera diretta e automatica su pc che provengono da IP non italiani;*
- ✓ *Dialer installato dal rootkit studiato principalmente per linee italiane, con l'utilizzo di due numeri satellitari in caso gli altri numeri non abbiano successo*

Come è possibile vedere dallo schema riassuntivo, Gromozon è stata un'infezione studiata appositamente per colpire l'Italia, cercando di mantenere quanto più circoscritta l'epidemia.

---

## **Rootkit.DialCall**

A partire da Settembre 2006 un'altra infezione ha iniziato a colpire principalmente gli utenti italiani. Un file, denominato **service32.exe**, viene trovato su numerosi pc in alcuni casi già infetti dal rootkit Gromozon.

Il file **service32.exe** è accompagnato per i primi mesi da una dll, dal nome variabile tra quelli in elenco:

- *ctfmon32.dll*
- *iexplorer32.dll*
- *iexplorre32.dll*
- *lsas32.dll*
- *mdm32.dll*
- *scrss32.dll*
- *spoolvs32.dll*
- *sys32exploer.dll*
- *syshost.dll*
- *syst32.dll*
- *winsmgr32.dll*

e da un dialer, avente come sintassi del nome **it\_0[XXXX].exe**, dove XXXX sono dei numeri casuali. In alcune situazioni il dialer ha come nome **best\_0[XXXX].exe**. Il dialer, prodotto da **CallSolutions**, è studiato appositamente per il traffico italiano.

Il rootkit si è evoluto nel corso degli ultimi mesi del 2006, scaricando un file **winsyst32.exe**, che va ad installare due diverse infezioni:

- *lzx32.sys*, conosciuto come Rootkit **Rustock.B**;
- *12201[numeri\_casuali].dll*, contenente un **Trojan.Clicker**

Il rootkit **Rustock.B**, uno dei rootkit **kernel-mode** attualmente più complessi, trasforma il pc infetto in un server che invia spam.

Il rootkit viene installato negli **ADS** (*Alternate Data Streams*):  
C:\WINDOWS\System32\lzx32.sys

Dopo circa tre mesi, da Settembre a inizio Dicembre, il rootkit cambia nome, da **service32.exe** a **winsys.exe**.

#### **TECNICHE UTILIZZATE PER CONTENERE L'INFEZIONE**

- ✓ *Dialer installato dal rootkit studiato per linee italiane, come recita chiaramente il sito della società che lo produce;*
- ✓ *Spesso i link all'installazione del rootkit sono contenuti in pagine web scritte in lingua italiana, in alcuni casi sono le vecchie pagine web che ospitavano Gromozon*

Come è possibile vedere, anche qui si tende a colpire principalmente l'Italia, sebbene altri pc possano essere infettati dal rootkit e da ciò che installa subito dopo.

---

### **Trojan.Spambot**

Infezione tutt'ora attiva, il **Trojan.Spambot** si diffonde attraverso e-mail con un testo scritto particolarmente bene, tanto da far cadere nel tranello molti utenti italiani.

Tra le varie e-mail utilizzate per diffondersi, la più comune è:

**TESTO:** *Gentile utente ,*

*sono l'avvocato Gianluca Gentili proprietario dell'omonimo studio Legale, mi trovo costretto a riscriverle perchè continuano ad arrivarci dal suo indirizzo di posta elettronica messaggi dal contenuto esplicito.*

*La rimando a tal proposito a verificare l'ultimo arrivato, che riporto sotto a questo messaggio.*

*Non sono un esperto in materia, tuttavia il sistemista del nostro studio sostiene che questi invii da parte sua sono probabilmente involontari e causati da un virus informatico.  
Dice inoltre che è possibile rimuovere questo worm con il programma antivirus scaricabile dall'indirizzo .*

*Io non ho nè le competenze nè il tempo per verificare l'esattezza di questa teoria, purtroppo mi trovo costretto a DIFFIDARLA dal continuare questi invii non sollecitati alla mia posta di lavoro.  
Se riceverò UN SOLO ALTRO MESSAGGIO di questo genere procederò a denunciarla senza ulteriore avviso.*

*Sospenda questi invii o, se si tratta di un virus worm, ripulisca il suo computer al più presto perchè forse non sono l'unico che sta ricevendo questa immondizia da lei.*

*Le ricordo che i reparti di polizia informatica hanno i mezzi per risalire alla vera identità del proprietario di un indirizzo email, per quanto registrato con dati inventati o internazionale. Per cui non creda di poter continuare a inquinare la mia casella email con queste promozioni.*

*in attesa di un suo cortese riscontro,  
saluti cordiali*

L'e-mail invita l'utente a scaricare un **finto programma** per rimuovere questa presunta infezione. Il sito a cui fa riferimento l'e-mail, una copia graficamente ben sviluppata di un software antivirus, è raggiungibile solo da indirizzi IP provenienti dall'Italia.

Inoltre, una volta eseguito, il trojan controlla che il pc non sia utilizzato da qualche ente governativo o testata giornalistica italiana.

```
0040A0D0 72 00 00 00 7C 2A 70 6F r...!#po
0040A0D8 6C 69 63 65 2E 69 74 7C lice.it!
0040A0E0 2A 70 6F 6C 69 7A 69 61 #polizia
0040A0E8 64 69 73 74 61 74 6F 2E distato.
0040A0F0 69 74 7C 2A 70 6F 6C 69 iti#poli
0040A0F8 7A 69 61 2D 70 65 6E 69 zia-peni
0040A100 74 65 6E 7A 69 61 72 69 tenziari
0040A108 61 2E 69 74 7C 2A 70 6F a.it!#po
0040A110 6C 73 74 72 61 64 61 2E lstrada.
0040A118 69 74 7C 2A 70 6F 6C 69 it!#poli
0040A120 7A 69 61 6D 75 6E 69 63 ziamunic
0040A128 69 70 61 6C 65 2E 69 74 ipale.it
0040A130 7C 2A 70 6F 6C 6D 75 6E !#polmun
0040A138 69 63 69 70 61 6C 65 6D icipalem
0040A140 61 72 74 69 6E 61 2E 69 artina.i
0040A148 74 70 69 69 6F 6F 69 69
```

In caso negativo, installa un dll, **webdesk.dll**, che si connette a dei server remoti. Curiosamente, la dll tenta di connettersi a dei server già contattati da una variante precedente del **Trojan.Spamlia**.

Durante la fine di Dicembre 2006 un'altra variante del Trojan.Spambot viene diffusa, utilizzando altri testi dell'e-mail.

Una delle e-mail risulta essere:

**OGGETTO:** Buone feste e buon anno con video

**TESTO:** Salve a tutti,  
vi mando questo pensiero davvero divertente,  
con tanti auguri per un sereno natale, buone feste e felice anno nuovo!

**ALLEGATO:** nata\_leperduto.asx

O, un'altra variante:

**OGGETTO:** Video di babbo natale

**TESTO:** Gustatevi questo video-gag per natale!  
tantissimi auguri!

**ALLEGATO:** nata\_le.asx

Esistono tuttavia altre varianti del testo.

L'allegato utilizza la stessa tecnica del **Trojan.Bomka**, file con estensione **ASX** che chiede di scaricare i codec corretti.

Per un'analisi più dettagliata del trojan è possibile leggere [qui](#).

**TECNICHE UTILIZZATE PER CONTENERE L'INFEZIONE**

- ✓ E-mail scritta in un italiano fluido e corretto;
- ✓ Server che distribuisce l'infezione con filtro degli indirizzi IP;
- ✓ Controllo del trojan se il pc è utilizzato da qualche ente governativo italiano, polizia, o testate giornalistiche

Come è possibile vedere dallo schermo riassuntivo, anche il **Trojan.Spambot** è stato studiato per essere contenuto nel territorio italiano. Inoltre, il team che è alle spalle di questo trojan è costantemente attivo, rilasciando continue versioni del trojan per evitare che i software antivirus riconoscano la minaccia.

---

## **Trojan.Hijacker**

Altra infezione studiata appositamente per l'Italia, si diffonde alla fine del 2006 attraverso e-mail.

Testo scritto in italiano, l'e-mail si diffonde principalmente attraverso una di queste due e-mail:

**OGGETTO:** *Avviso di sanzione per interessi su insoluto Verbale P.M. N. 326123-1 del 4.12.2006*

**TESTO:** *La presente per informarLa che la somma di € 2.623,44 dovuta alla nostra società e scaduti in data 10.11.2006 i termini come da nostra informativa precedente e visti maturazione interessi pari al 18,6% per la sua pratica N. 326123-1 sono soggetti a sanzione e decreto ingiuntivo se non corrisposti entro la data 20.12.2006*

*Certi di una sua celere risposta la invitiamo a visualizzare i dettagli della sanzione attraverso il nostro servizio automatico,*

*Come agire*

*Al fine di chiarire la sua posizione qualora non corrispondano le suddette somme a contattare il nostro servizio riscossione crediti*

*Cordiali saluti*

*Avv. Cons. Dpe Giordano Lanza*

Esistono varianti di questa e-mail, tra le quali nelle settimane passate:

**OGGETTO:** *Proposta di lavoro*

**TESTO:** *Buongiorno,  
La nostra azienda opera da 15 anni nel campo della comunicazione su internet vantando partnership con le più grandi realtà italiane oggi presenti su internet. Ricerchiamo persone ben organizzate, responsabili, desiderose di guadagnare lavorando comodamente da casa attraverso il proprio personal computer.*

*La preghiamo di leggere attentamente questa email:*

*La nostra offerta di lavoro è compatibile con il vostro lavoro principale La nostra offerta di lavoro non occuperà più di un'ora al giorno La nostra offerta di lavoro verrà retribuita mensilmente mediante assegno o bonifico bancario*

*Questa potrebbe essere un'importante possibilità e potrai guadagnare fino a 2.500 Euro al mese !*

*I posti disponibili sono limitati a 32,  
Per aggiudicarsi un posto nella nostra lista di candidati potrà riempire il form sul nostro sito [www.guadagnosicuro.com/form.html](http://www.guadagnosicuro.com/form.html)  
<link al sito web [xread.biz](http://xread.biz)>*

*Entro 15 giorni dalla compilazione del form riceverà risposta.*

*Cordiali saluti*

*Uff. Reclutamento*

Entrambe le e-mail, o varianti, rimandano a scaricare uno di questi file:

- *stampa\_tutte\_le\_pagine.exe*
- *apri\_tutte\_le\_pagine.exe*
- *certificazione.exe*

Il **Trojan.HiJacker** contiene al proprio interno un **dialer**, che effettua chiamate a numeri a tariffazione aggiunta su linee italiane. Inoltre, reindirige l'home page di Internet Explorer ad una **falsa versione** del motore di ricerca *Google.it* che tenta di installare altri malware.

Un'analisi del **Trojan.Hijacker** approfondita è possibile trovarla [qui](#).

#### **TECNICHE UTILIZZATE PER CONTENERE L'INFEZIONE**

- ✓ *E-mail scritta in un italiano fluido e corretto;*
- ✓ *Dialer studiato per linee italiane;*

Anche il **Trojan.Hijacker** evidenzia che l'attacco è stato studiato per colpire l'utenza italiana, sia per i motivi sopracitati nello schema riassuntivo, sia perchè viene falsificata la versione italiana del motore di ricerca Google.

```
<frameset rows="1,*" frameborder="NO" border="0" framespacing="0">  
<frame src="up.asp" name="topFrame" scrolling="NO" noresize>  
<frame src="http://www.google.it" name="mainFrame">  
</frameset>
```

## - OBIETTIVO ITALIA: MOTIVAZIONI -

Risulta difficile dare delle motivazioni precise sul perchè molte infezioni nell'anno che si sta chiudendo, il 2006, abbiano preso di mira esclusivamente l'Italia.

Nei capitoli precedenti è stata data una spiegazione tecnica del come gli attacchi siano stati sferrati tentando di contenerne l'effetto, circoscrivendolo in modo da effettuare degli attacchi mirati.

Si è registrato, soprattutto durante la fine dell'anno, un incremento di utilizzo di **dialer**, spesso inclusi in altre infezioni – come mostrato nelle pagine precedenti.

La situazione in Italia non è delle più rosee a livello di connettività. Sono molte le zone in cui **la linea digitale ADSL non arriva** e si fa ancora largo utilizzo di linee analogiche, di modem 56k.

Se si aggiunge a questo elemento il fatto che in Italia i numeri a tariffazione aggiunta, quali 899 e 892 – utilizzati dai dialer, sono **abilitati automaticamente** nel momento in cui si attiva una linea telefonica e la loro disattivazione deve essere richiesta specificatamente dall'utente, si ha il quadro più preciso del perché i dialer siano particolarmente utilizzati sulle linee italiane.

L'utilizzo di un dialer è **la via più efficace e veloce per fare dei soldi**, aspetto che i virus writer e i malfattori in generale hanno oramai capito.

Inoltre, l'Italia non è indietro solo a livello di infrastruttura, ma anche a **livello organizzativo** per quanto riguarda la sicurezza informatica.

Non esiste un centro vero e proprio che coordini eventuali situazioni di emergenza informatica a livello nazionale, **non esiste un punto di riferimento** attivo attraverso il quale aziende, enti statali o cittadini comuni possano verificare eventuali novità o minacce a livello di sicurezza informatica.

Esistono alcune fonti private o organizzazioni governative che tuttavia in determinati casi non riescono a fornire adeguate informazioni o tempestivi aggiornamenti in caso di situazioni critiche.

Utenti, enti ed aziende devono in qualche modo adattarsi alla situazione e, spesso, **la sicurezza informatica viene presa sottogamba** rischiando di causare poi danni ingenti.

Se a ciò si aggiunge una disinformazione particolarmente avanzata per quanto riguarda le **norme basilari della sicurezza** su internet, aggravata dalla mancanza di informazioni chiare e precise fornite da media o testate giornalistiche, si può avere il quadro abbastanza completo sul perché l'Italia è entrata nel 2006 nell'occhio del ciclone. Un 2006 movimentato dunque per gli utenti italiani, che non lascia prevedere niente di buono per il prossimo anno.

## - FONTI -

### **Trojan.Spamlia/Trojan.Bomka**

<http://www.symantec.com/avcenter/venc/data/trojan.spamlia.html>

<http://securityresponse.symantec.com/avcenter/venc/data/trojan.bomka.html>

<http://www.pcalsicuro.com/main/?p=6>

<http://www.pcalsicuro.com/main/2006/05/pio12dll-come-lo-rimuoviamo/>

[http://www.hwupgrade.it/news/software/trojan-attenzione-al-gioco-delle-freccette\\_16286.html](http://www.hwupgrade.it/news/software/trojan-attenzione-al-gioco-delle-freccette_16286.html)

### **Rootkit.Gromozon**

<http://www.pcalsicuro.com/gromozon.pdf>

<http://www.pcalsicuro.com/main/2006/08/gromozon-linkoptimizer-e-la-saga-senza-fine/>

<http://www.pcalsicuro.com/main/2006/11/gromozon-ora-va-sul-personale/>

<http://www.pcalsicuro.com/main/2006/11/dopo-la-parte-tecnica-ora-la-legge/>

[http://www.symantec.com/security\\_response/writeup.jsp?docid=2006-082416-2803-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2006-082416-2803-99&tabid=2)

[http://www.difesa.it/NR/rdonlyres/D4932D9D-3002-4F96-A87E-](http://www.difesa.it/NR/rdonlyres/D4932D9D-3002-4F96-A87E-E394872B7AE6/11996/gromozonlinkoptimizer.pdf)

[E394872B7AE6/11996/gromozonlinkoptimizer.pdf](http://www.difesa.it/NR/rdonlyres/D4932D9D-3002-4F96-A87E-E394872B7AE6/11996/gromozonlinkoptimizer.pdf)

<http://sunbeltblog.blogspot.com>

### **Rootkit.DialCall**

<http://fileinfo.prevx.com/fileinfo.asp?PXC=372941044121>

<http://fileinfo.prevx.com/fileinfo.asp?PXC=d0ba41121848>

<http://fileinfo.prevx.com/fileinfo.asp?PXC=498f57503068>

<http://www.pcalsicuro.com/main/?p=41>

<http://www.pcalsicuro.com/main/2006/10/service32exe-torna-di-moda/>

<http://www.pcalsicuro.com/main/2006/11/new-gromozon-e-rootkitdialcall/>

<http://www.pcalsicuro.com/main/2006/12/altra-variante-di-service32exe/>

<http://www.pcalsicuro.com/main/2006/12/aggiornamenti-post-natale/>

### **Trojan.Spambot**

<http://www.pcalsicuro.com/main/2006/11/uno-studio-legale-ci-denuncia/>

<http://www.pcalsicuro.com/main/2006/12/alcuni-pensieri-su-trojanspambot/>

<http://www.pcalsicuro.com/main/2006/12/spambot-torna-per-gli-auguri-di-natale/>

[http://fileinfo.prevx.com/spyware/qqfe5659014390-remo29598908/removal\\_tool.exe.html](http://fileinfo.prevx.com/spyware/qqfe5659014390-remo29598908/removal_tool.exe.html)

### **Trojan.Hijacker**

<http://fileinfo.prevx.com/fileinfo.asp?PXC=cdf960075916>

<http://www.pcalsicuro.com/main/2006/12/gli-avvocati-di-moda/>

<http://www.pcalsicuro.com/main/2006/12/gli-avvocati-di-moda-parte-seconda/>

<http://www.pcalsicuro.com/main/2006/12/il-reclutamento-pericoloso/>