SPYWARE

Dalla parte dell'attaccante...

SPYWARE

Firenze, 19 Maggio 2006

matteoflora.com
privacy & security consultancy - forensic examinations

DISCLAIMER

Il contenuto delle seguenti slide è da fruirsi obbligatoriamente con il commento personale dell'autore durante la presentazione.

L'eventuale fruizione del solo materiale potrebbe facilmente prestarsi ad erronea interpretazione ed è assolutamente sconsigliata.

L'autore si assume la completa responsabilità per la sua presentazione ma deglina ogni responsabilità nell'utilizzo, nella divulgazione e nella citazione del presente materiale.

SPYWARE

Matteo G.P. Flora

Lead Security Evangelist

LkProject Privacy, Security & Digital Intelligence

Consulente di Sicurezza

Agenzie di Investigazioni
Società Multinazionali
Associazioni Internazionali

Consulente Tecnico

Procura della Repubblica Tribunale di Milano
Nucleo Repressioni Frodi Informatiche Guardia di Finanza

Servizi Speciali Guardia di Finanza

Presidente

Presidente Provinciale AIP-ITCS MILANO
(Associazione Informatici Professionisti)

Membro

Osservatorio Permanente Privacy e Sicurezza AIP
IEEE CS

SPYWARE

matteoflora.com
privacy & security consultancy - forensic examinations

introduzione

SPYWARE

matteoflora.com
privacy & security consultancy - forensic examinations

SPYWARE

definizione

La definizione formale di Spyware recita:

"Uno spyware è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente … senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata.
…
In un senso più ampio, il termine *spyware* è spesso usato per definire un'ampia gamma di malware dalle funzioni più diverse..."

Wikipedia

SPYWARE

mascheramento

> Installazione

Spesso è impossibile rintracciare il processo di installazione o esso viene attivato senza il consenso dell'utente.

> Disclaimer fraudolenti

Le condizioni di utilizzo proposte non sono chiare e/o sono incomprensibili.

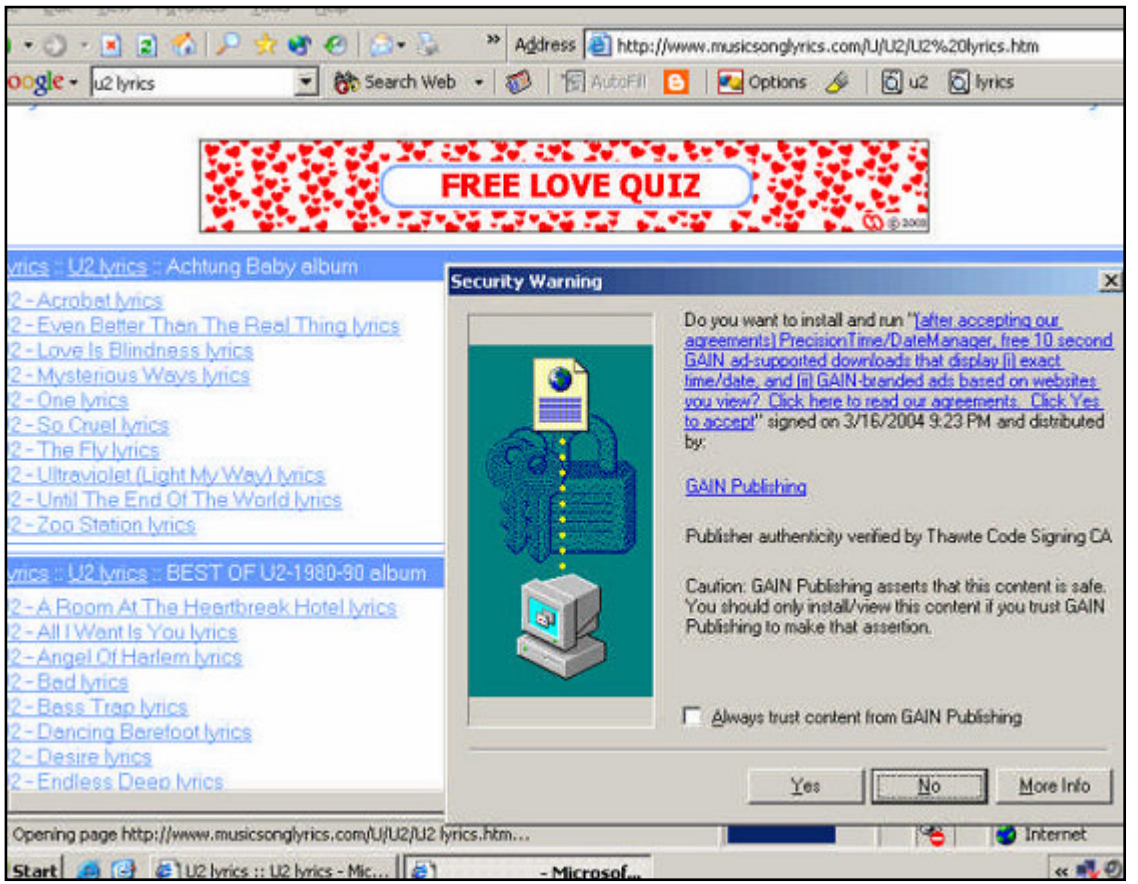
Claria propone un contratto di licenza testuale della dimensione 1023Kb (*esattamente la stessa della Divina Commedia*).

> Violazione delle Condizioni Contrattuali

Inoltre le condizioni citate sono speso e volentieri infrante apertamente dallo stesso produttore, parzialmente coperte da sofismi legali e/o burocratici

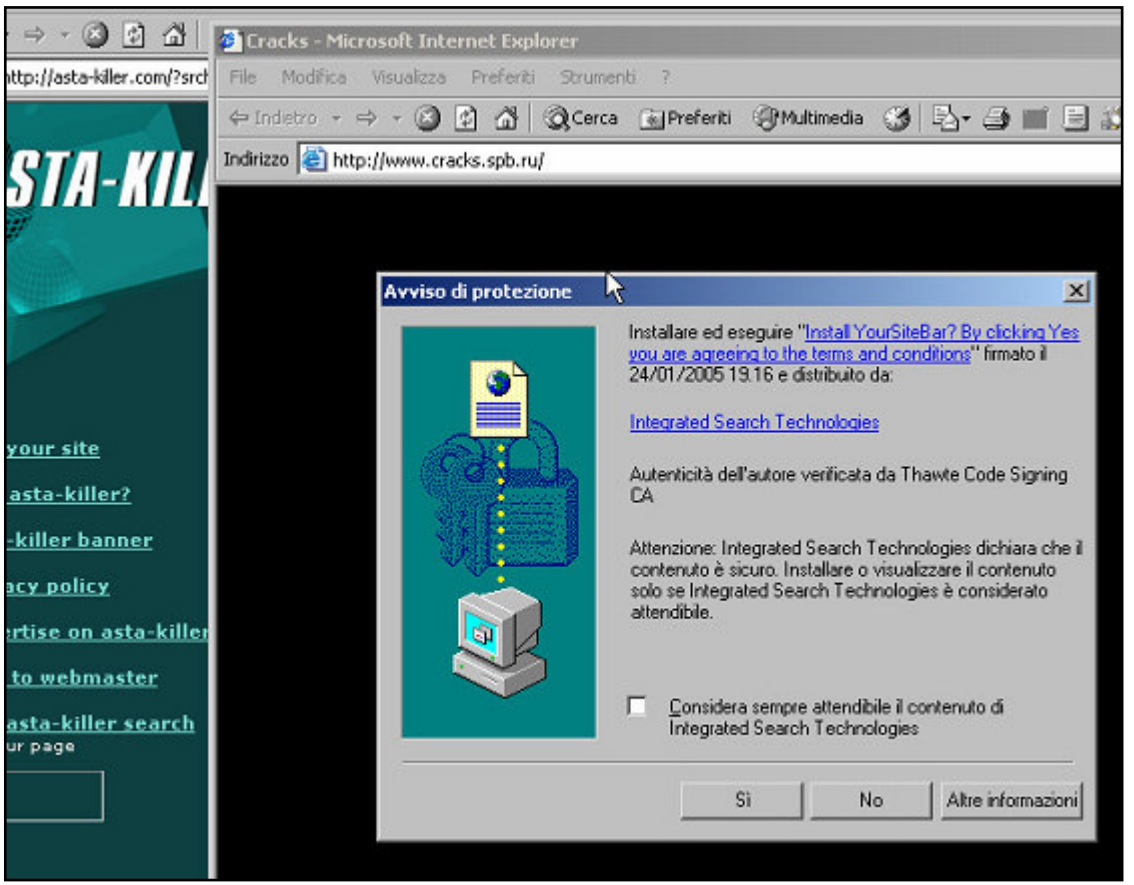
esempi

SPYWARE



esempi

SPYWARE



SPYWARE

statistiche

> Luglio 2004

Le macchine infette da almeno uno dei 5 maggiori spyware sono 64.000.000.

> Q1 2005

Una scansione su 4.3 milioni di PC ha rilevato che l'87% di questi è affetto da almeno una forma di codice malevolo tra Adware, Keylogger o Troyan.

Fonte: http://www.webroot.com/stateofspyware d

SPYWARE

statistiche

> Distribuzione

Un computer non protetto che effettua navigazione "Clean" con Internet Explorer è infetto da una media di ventiquattro (24) spyware alla fine del suo primo mese di vita.

> Soglia di pericolo

L'utilizzo di Internet Explorer per la navigazione "particolare" comporta una infezione media di centottanta (180) spyware nei primi sei mesi di vita.

SPYWARE

statistiche

Spyware Scan Results Spyware detected: 18 threats

Recommended Action	Threat Name	Threat Level
Remove	ShopAtHome (Spyware)	Severe
Remove	180search Assistant (Adware)	High
Remove	IST.PowerScan (Adware)	High
Remove	SideFind (Adware)	High
Remove	Xrenoder (Browser Plug-in)	Severe
Remove	IST.XXXToolbar (Toolbar)	High
Remove	YourSiteBar (Spyware)	High
Remove	AvenueMedia.DyFuCA (Browser Plug-in)	Severe
Remove	IST.ISTbar (Browser Hijacker)	Severe
Remove	MoneyTree (Dialer)	Severe
Remove	2020Search (Browser Plug-in)	Elevated
Remove	IST.XXXToolBar (Browser Plug-in)	Severe
Remove	webHancer (Spyware)	Severe
Remove	CoolWebSearch.StartPage (Browser Hijacker)	Severe
Remove	CoolWebSearch (Browser Hijacker)	Severe
Remove	IST.SlotchBar (Toolbar)	High
Remove	DownloadWare (Adware)	High
Remove	Twain Tech (Adware)	High

SPYWARE

danni

> Fuga di informazioni

Uno spyware costituisce una seria minaccia per la privacy personale ed aziendale.

> Stress

Una machina affetta da spyware presenta all'utente una media di 90 schermate pubblicitarie al giorno, alcune delle quali contenenti testi od immagini oscene.

> Utilizzo illecito del PC

Spesso gli spyware utilizzano le risorse del computer ai fini di calcoli distribuiti, zombienet, spambots oltre che veicolo per ulteriori spyware.

in azione...

FIRENZE PE 2006

SPYWARE

AIP Associazione Informatici Professionisti

ITCS Italian Computer Society

LKPROJECT

matteoflora.com

privacy & security consultancy - forensic examinations

SPYWARE

gamma

> Pageview di banner

Presentazione banner pubblicitari.

> Banner & Site Hijacking

Alterazione di banner e/o siti web per la sostituzione di legittimi inserzionisti con clienti delle spyware factory.

> Marketing Mining

Acquisizione di dati comportamentali e di navigazione su una larghissimo userbase ad altissima possibilità di profiling.

> Commission Theft

Alterazione dei sistemi di commissioni di pagamento e referral online.

> Installazione software non autorizzato

Alterazione della macchina a fini illeciti o illegali.

SPYWARE

banner

> Funzione storica

La presentazione di banner all'incauto utente (e spesso l'homepage hijacking) è uno dei cardini storici dello spyware.

> Bassissimi costi

Il pageview si un banner sul circuito Claria/WhenU ha un costo medio di $.0,002 contro il normale prezzo di mercato di $.0,05.

In termini pratici si tratta di 1/20 dell'investimento.

> Aggiramento sistemi antibanner

I banner erogati dagli spyware non sono bloccabili, agendo al di fuori dei meccanismi di protezione di Internet Explorer.

SPYWARE

investimento

- **Profiling di eccezione**

  Lo spyware mantiene la storia della navigazione dell'utente e propone banner in sintonia.

- **Controllo della navigazione**

  E' possibile erogare banner in occasione della visita di precisi siti web e/o precise parole contenute in pagina.

- **Intregazione con OS**

  L'alta integrazione consente di controllare anche applicazioni non inerenti la navigazione (messenger, posta…).

SPYWARE

adv hijacking

> Scalata del banner

La pubblicazione di banner in network ad alto traffico in posizioni prominenti ha raggiunto costi esorbitanti, in linea con gli equivalenti della carta stampata.

> La via economica…

E' molto più semplice ed economico acquistare i servizi della società di spyware per sostituire i banner legittimi con i propri.
L'investimento viene così ridotto sino ad 1/150.

> Siti danneggiati

Tra gli altri ricordiamo: MSN, Yahoo, Amazon, Google, Lycos, Utube, A9, CNN, The New York Times, CBS, NBC, Barnes&Nobles.

SPYWARE

adv hijacking

SPYWARE

web hijacking

> Sostituire un sito web

Ancora più efficace appare sostituire integralmente un sito web con quello di un competitor diretto.

> Una chance da non perdere

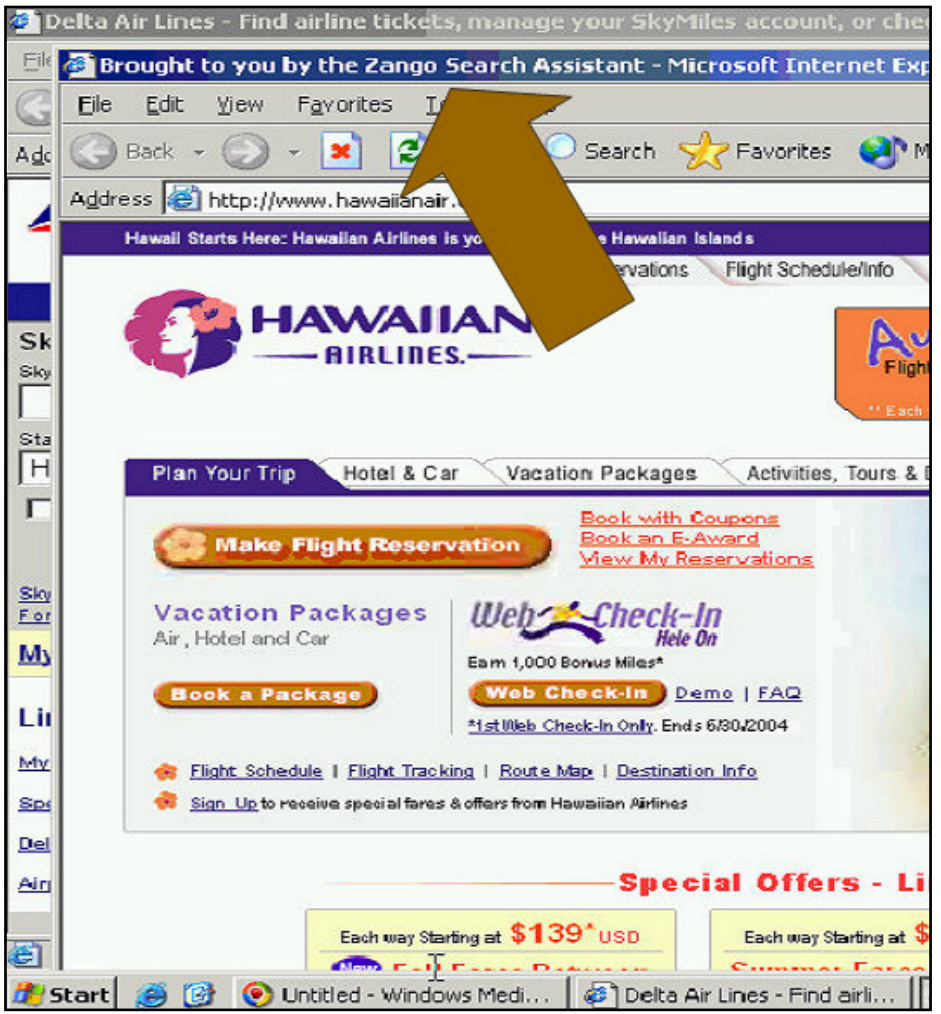
In questo caso, oltre alla pubblicità, otteniamo pageview per il nostro sito web e per qualunque altro banner che noi stessi proponiamo.

> Siti danneggiati

Tra gli altri ricordiamo: MSN, Yahoo, Amazon, KMart, Lufthansa, Mastercard, Visa, AmericanExpress, Berkley, CityBank, Bank of America…

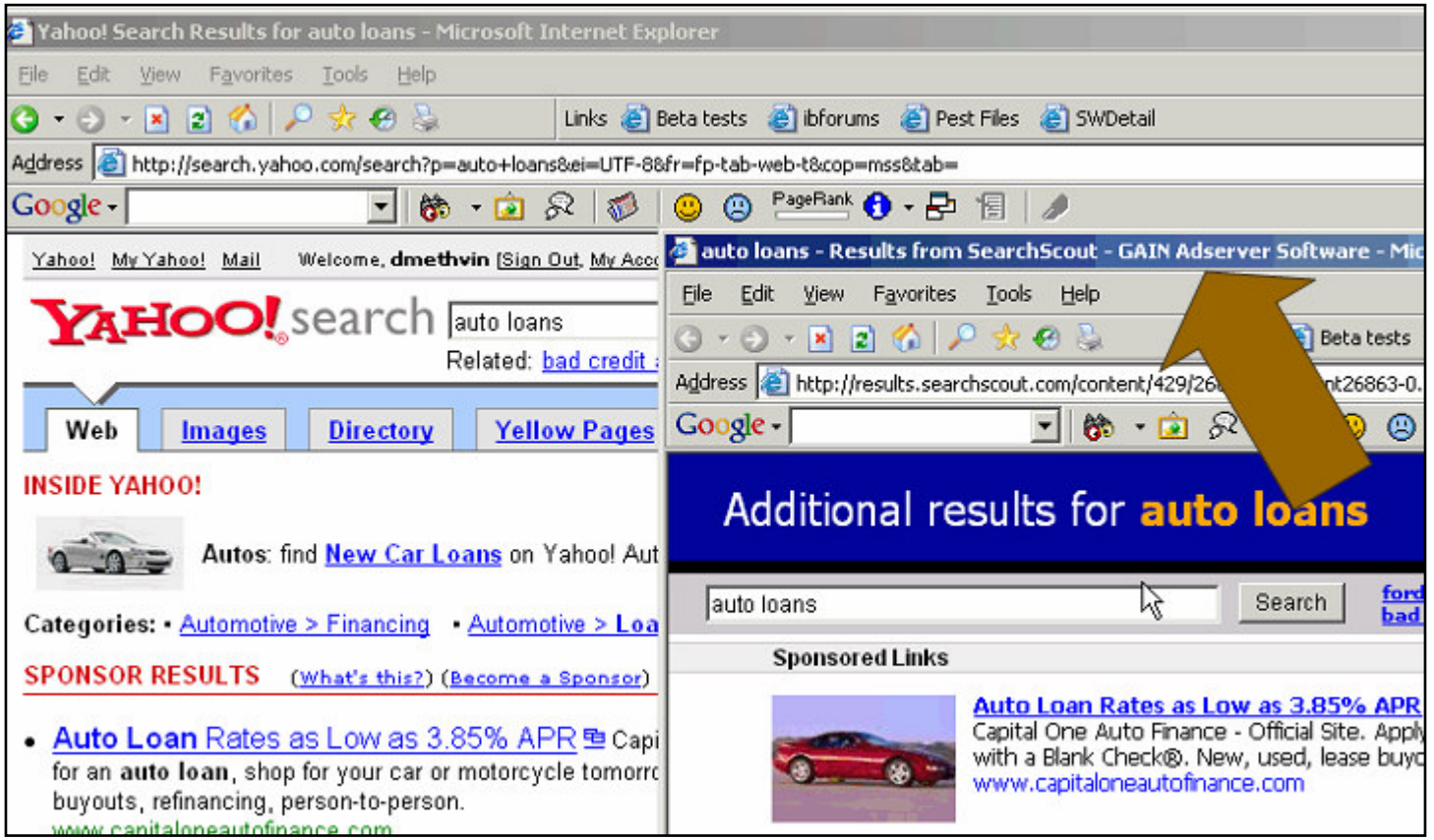
SPYWARE

web hijacking



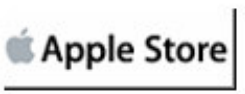
web hijacking

SPYWARE



truffati

SPYWARE



SPYWARE

mkt profiling

> Una base dati enorme

Contenente abitudini di navigazione, banner visionati o cliccati, siti visitati, acquisti effettuati….

> Informazioni in vendita

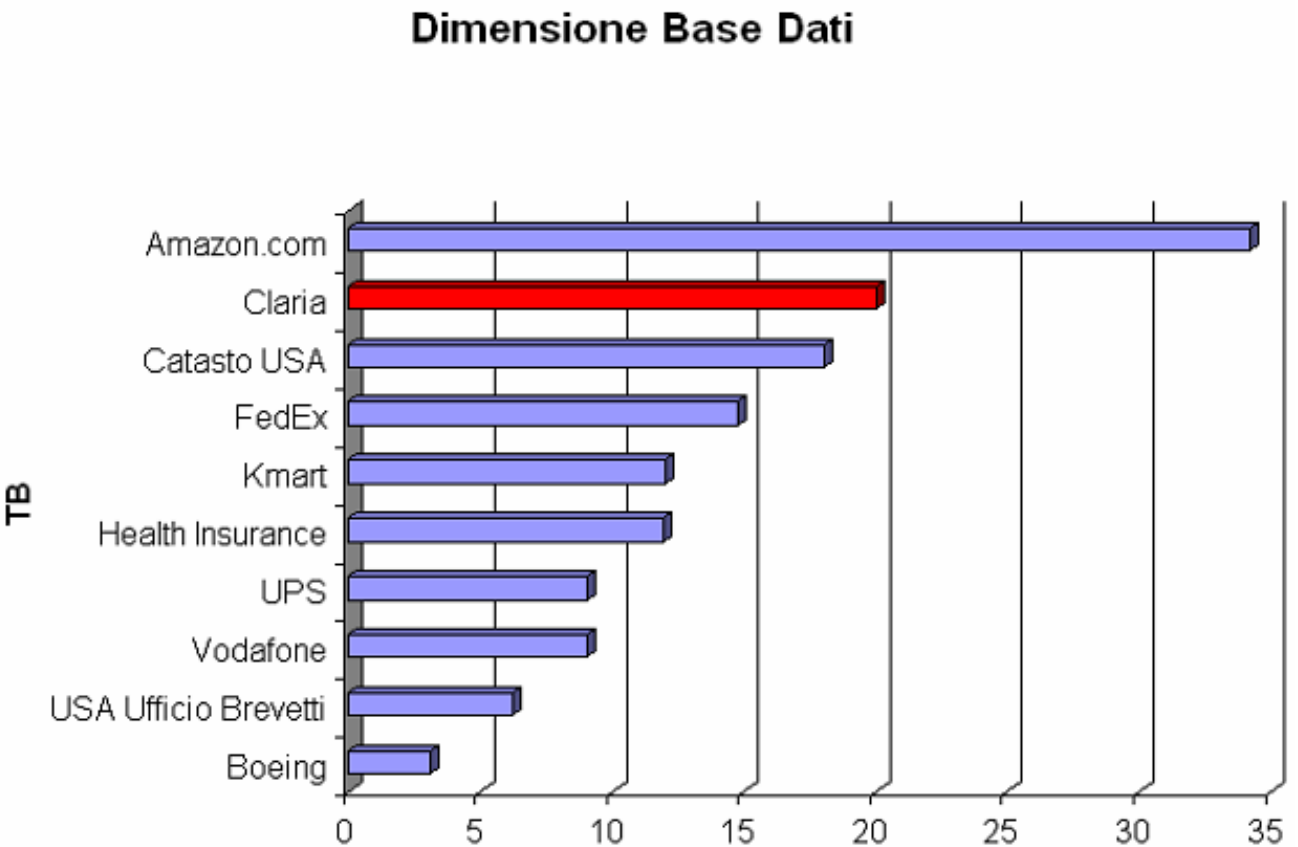
Sono disponibili statistiche generali o statistiche dettagliate sul proprio settore di attività o su un profilo particolare.

> Marketing mirato

La disponibilità di un archivio storico consente di individuare ed estrapolare profili estremamente precisi (es. “tutti gli utenti che hanno comperato da Amazon e visitato almeno una voltsa RyanAir”).

mkt profiling

SPYWARE



SPYWARE

commission

> Il referral come mercato

Il mercato delle commissioni è oggi affermato in ambito web e conta movimentazioni di denaro nell'ordine di $.850.000.000,00 annui.

> Commissioni dignitose

Le commissioni di vendita variano dal 3% al 15% a seconda del network e sono erogate in modo assolutamente automatico..

> La vita dei piccoli

Per molti siti di informazione o riviste online il pagamento delle commissioni rappresenta la prima ed unica forma di finanziamento.

SPYWARE

commission

SPYWARE

com theft

> Interposizione

Mediante apertura di nuove finestre, codice iniettato o semplice rewrite lo spyware (180search/Gator/WhenU) si interpone nel processo.

> Furto di commissioni

Le commissioni “legitime” vengono traghettate alla società di spyware e sottratte al vero proprietario.

SPYWARE

com theft

SPYWARE

com theft

> Lauti guadagni

Nel mese di Marzo 2004, Gator ha incassato per sottrazione a MSNBC sul solo cliente Dell oltre $.100.000,00.

> AdWords

Lo stesso meccanismo viene da qualche mese utilizzato per sostituire i codici di AdWords di Google e sottrarre commissioni PPC.

SPYWARE

inst worms

> Incentivo a delinquere

Gator Corp., Claria e 180Search promuovono l'installazione di software da parte di "terze parti".

> Commission per install

Per ogni installazione su di una macchina viene riconosciuta una commissione di circa $.0,70.

Un worm che infetti in modo autonomo 20.000 macchine avrà quindi un ritorno immediato effettivo di circa $.14.000,00.

SPYWARE

inst worms

> Vantaggi per entrambi

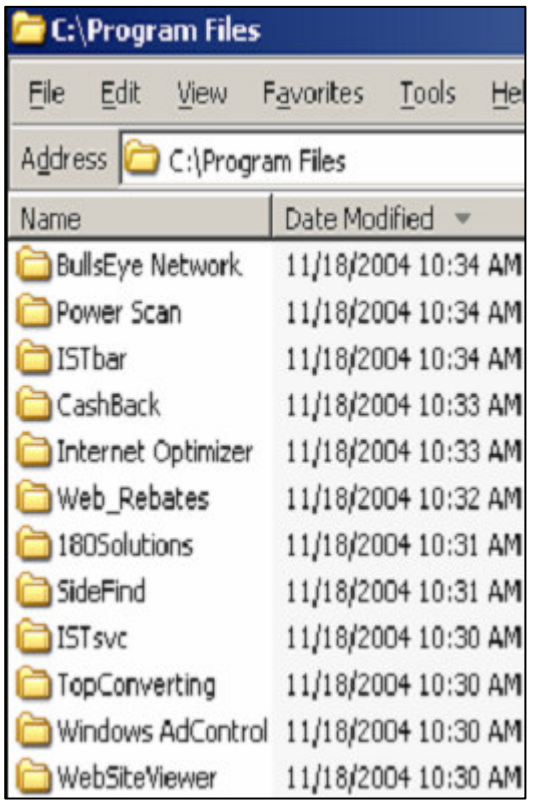
Con questo meccanismo molti malicious coders ottengono lauti guadagni mentre la società di spyware è tutelata da eventuali lamentele poiché "non colpevole" di azioni compiute da terzi in differenti giurisdizioni.

> Cascade Install

Molti di questi software agiscono da troyan e installano a cascata decine di differenti spyware per "ottimizzare le revenues".

SPYWARE

inst worms



identity

FIRENZE PE 2006

SPYWARE

AIP Associazione Informatici Professionisti

ITCS Italian Computer Society

LKPROJECT

matteoflora.com

privacy & security consultancy - forensic examinations

SPYWARE

capitali

> Enormi Venture Captialist

I top players del mercato dello spyware non fanno capo ad organizzazioni mafiose e/o residenti in paradisi fiscali, ma ad enormi VC quotate regolarmente in borsa..

> Capitali di rischio

Se è pur vero che si tratta di "capitali a rischio" è anche vero che NESSUNA di queste aziende ha chiuso con meno di un incremento netto di fatturato del 7% MENSILE nel corso del biennio 2003-2004.

SPYWARE

VC

> 180 Solutions (Zango, ncase)

Spectrum Equity Investors: $.40.000.000

investe anche in Cellular One, Loews Coneplex, Eutelsat, Metrics Direct

> Claria (Gator, GAIN)

Investimenti totali: $.58.000.000

US Venture Partners

investe anche in Cisco, Iomega, Sun, AskJeeves, Cogency, Epic, Sandisk, Alcatel

GrayClock

investe anche in RedHat, DoubleClick, LinkedIn, Lumigent, Raptor, SightPath

Crosslink Capitals

investe anche in Cisco, Iomega, Sun, AskJeeves, Cogency, Epic, Sandisk, Alcatel

Le informazioni presentate sono aggiorante al Gennaio 2005

SPYWARE

VC

> continua… Claria (Gator, GAIN)

Garage Technology Ventures

investe anche in Psionic, Tripwire, The Motley Fool

Rosewood Stone Group

investe anche in Allaire, Concentric, Excite!, Prospero, Salon.com,

Investor AB

investe anche in Ericsson, Saab, ABB, Atlas Copco, Electrolux, Scania

Technology Crossover Venture

investe anche in BrightMail, C|Net, eBags, Expedia, eHarmony, NetFix, Real

Le informazioni presentate sono aggiorante al Gennaio 2005

SPYWARE

VC

> DirectRevenues (Optimixer)

Insignt Revenues:	$.20.000.000
Technology Investments Capital Group:	$.6.700.000

> eXact Advertising (BergainBuddy)

Tecnology Investments Capital Group:	$.20.000.000

Le informazioni presentate sono aggiorante al Gennaio 2005

SPYWARE

clienti

- **Utenti Gator identificati dai banner presentati**

  ING Direct, Apple Store, Avon, Crysler, Disneyland Resort, Expedia, Palm, Priceline, uBid, Verizon, Western Union, Rail Europe, Sun Microsystems.

- **Utenti whenU identificati dai banner presentati**

  Travelocity, EBay, Proceline, Thrifty, Best Western, Time Life, Walt Disney Classics, KaBloom, Virgin Mobile, Sprint PCS, T-Mobile, Verizon, Chase, ING Direct, AmericanExpress, Ameriquest, University of Phoenix Online, Lloyds TBS.

Le informazioni presentate sono aggiorante al Gennaio 2005

licenza

SPYWARE

creative commons

COMMONS DEED

Attribuzione - Non commerciale - Non opere derivate 2.5 Italia

Tu sei libero:

- di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera

Alle seguenti condizioni:

Attribuzione. Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza.

Non commerciale. Non puoi usare quest'opera per fini commerciali.

Non opere derivate. Non puoi alterare o trasformare quest'opera, ne' usarla per crearne un'altra.

- Ogni volta che usi o distribuisci quest'opera, devi farlo secondo i termini di questa licenza, che va comunicata con chiarezza.
- In ogni caso, puoi concordare col titolare dei diritti d'autore utilizzi di quest'opera non consentiti da questa licenza.

Le utilizzazioni consentite dalla legge sul diritto d'autore e gli altri diritti non sono in alcun modo limitati da quanto sopra.

http://creativecommons.org/licenses/by-nc-nd/2.5/it/

www.matteoflora.com
mf@matteoflora.com

SPYWARE