

# E-CRIME & MINACCE DEL WEB

---



SICURO DI ESSERE AL SICURO?

 **WEBSense**

# CONTENUTI

PANORAMICA GENERALE	PAGINA 2
SPYWARE & KEYLOGGING	PAGINA 3
PHISHING & PHARMING	PAGINA 5
BOT	PAGINA 7
INSTANT MESSAGING & P2P	PAGINA 9
CRIMEWARE & EXPLOIT 'ZERO-DAY'	PAGINA 11
COME PROTEGGERE L'ORGANIZZAZIONE	PAGINA 13
LE SOLUZIONI DI WEBSense PER LA SICUREZZA	PAGINA 14



# PANORAMICA GENERALE

Le minacce alla sicurezza delle informazioni che le organizzazioni si trovano oggi ad affrontare sono di un nuovo tipo: più ridotte nel numero, ma più insidiose e mirate, mosse da motivazioni di ordine economico e guidate dal crimine organizzato.

Scordatevi gli hacker adolescenti e pensate piuttosto che ora si tratta di affrontare criminali incalliti dediti all'e-crime perché hanno scoperto che rende di più ed è meno rischioso di altre forme di delinquenza. Il loro obiettivo sono le informazioni riservate – aziendali o personali che siano – che si possano rivendere o utilizzare per perpetrare frodi o estorsioni. Questo trend dell'hacking for profit è già stato ampiamente segnalato da fonti autorevoli, quali il SANS<sup>SM</sup> Institute (USA) o la Polizia Postale italiana, nonché dai Websense Security Labs<sup>SM</sup>.

I mezzi usati per questi attacchi (globalmente definibili come crimeware) sono i più diversi: spyware, phishing e pharming, bot network, keylogging e spesso un insieme di diversi tipi di attacchi. P2P, instant messaging (IM) e VoIP sono anch'essi a rischio, anche se non sono ancora al centro delle preoccupazioni dello staff addetto alla sicurezza IT. I file distribuiti da questi sistemi P2P, infatti, possono essere pericolosi veicoli di infezioni, con programmi quali eDonkey, Kazaa e BitTorrent tra i target,

mentre popolari proposte VoIP come Skype devono ancora dimostrare che la loro sicurezza è adeguata a un uso aziendale.

Un altro trend preoccupante è quello degli attacchi ai web server, che creano siti web corrotti che lanciano attacchi a chi li visita sfruttando le vulnerabilità dei browser. Particolarmente vulnerabili risultano i siti sviluppati usando PHP, il linguaggio di programmazione web più diffuso. Secondo il rapporto di SANS Institute sulle 20 principali vulnerabilità, nel 2005 non è trascorsa una settimana senza che venisse registrato un problema in qualche software creato con PHP.

## Le principali fonti di minacce:

- Spyware
- Phishing
- Pharming
- Bot networks
- Keylogging
- P2P
- IM
- VoIP
- Minacce miste

In futuro, non saranno solo i sistemi operativi ad aver bisogno di patch, ma anche le applicazioni, perché proprio queste sono sempre più oggetto di attacchi.

# SPYWARE & KEYLOGGING

---

Le infezioni da spyware dei PC sono spesso così subdole che gli utenti nemmeno ne hanno percezione; ma una volta che è penetrato nel sistema, lo spyware è in grado di causare rilevanti perdite di informazioni e di denaro.

Lo spyware incorpora programmi come keylogger e tool di spionaggio che registrano i comportamenti in Internet degli utenti. In pratica vedono quello che l'utente fa sul web, registrando le email inviate e ricevute e le comunicazioni IM, inviando poi le stesse informazioni a soggetti terzi.

I tipi di informazioni catturati variano, ma di solito includono username, password e informazioni personali quali account e dettagli di login, oltre a file e documenti riservati. I pericoli, specie per le aziende, sono rilevanti: per alcuni tipi di organizzazioni (per esempio nel settore della Sanità o finanziario) che hanno la responsabilità di custodire dati sugli utenti, sono previste sanzioni pesanti nel caso in cui tali informazioni vengano violate.

Secondo un'indagine di Forrester Research condotta presso 200 responsabili della sicurezza, nel 2005 circa il 65% delle aziende si stava dotando di software anti-spyware, che si è così configurato come vero prodotto dell'anno.

Lo spyware riesce a intrufolarsi in un computer in diversi modi: può essere installato inconsapevolmente in quanto parte di un programma gratuito, come ad esempio uno screen saver. Oppure scaricando programmi dichiarati necessari per la visualizzazione di alcuni siti, o ancora attraverso email usando tecniche del social engineering per allettare gli ingenui utenti con offerte fasulle.

Uno dei problemi con lo spyware è che le infezioni sono difficili da individuare. Uno dei sintomi più comuni, tuttavia, è che i computer cominciano a comportarsi in modo strano. Sono più lenti o più instabili, perché spyware, Trojan e altri fastidiosi programmi consumano risorse quali CPU, memoria e banda. Attenzione quindi ai bruschi cambiamenti di comportamento del vostro computer: potrebbero essere un segno che lo spyware si sta dando da fare sulla vostra macchina

C'è una certa confusione tra adware e spyware. L'adware è un software che instrada verso di voi pubblicità non richiesta o punta il vostro browser su siti che forniscono advertising. L'adware è un fastidio, mentre lo spyware è un rischio per la sicurezza delle informazioni. Ora c'è un nuovo termine che sta emergendo a indicare insieme entrambi i fenomeni: 'greyware'.

Stanno emergendo parecchi " esempi orrendi" che dimostrano i tipi di danni che possono fare a un'organizzazione gli attacchi spyware.

Nel 2005, alcuni criminali sono stati scoperti prima che potessero portare a termine un colpo con l'ausilio di spyware che avrebbe dovuto fruttare 220 milioni di sterline sottratti agli uffici londinesi della banca giapponese Sumitomo Mitsui. Era previsto l'uso di software di keylogging per mandare password e informazioni per l'accesso ai criminali per poi effettuare trasferimenti elettronici dei fondi.

Negli Stati Uniti, un broker ha perso 40.000 dollari dopo aver installato quello che pensava fosse un programma di analisi finanziaria, ma che invece era uno spyware che ha trasmesso i dettagli per il login al suo conto.



# PHISHING & PHARMING

---

Il phishing usa siti web fasulli, email spam e altre tecniche basate su codice maligno per spingere le persone a divulgare le proprie informazioni personali confidenziali.

Il phishing usa la tecnica definita del 'social engineering', ovvero fa leva sulla psicologia degli individui per ottenere informazioni su un'organizzazione o i suoi sistemi informatici.

In un attacco di phishing condotto con le tecniche del social engineering, i phisher di solito inviano ondate di email spam contenenti un messaggio che finge di provenire da un'organizzazione autorevole: ad esempio una banca o una multinazionale con un marchio molto noto. Il messaggio sembra credibile perché sia la mail che il sito cui punta il link in essa contenuto appaiono estremamente simili al look del marchio contraffatto. Il phishing spesso fa leva anche sulla generosità delle persone, sfruttando ad esempio un disastro naturale, come è successo in occasione dell'uragano Katrina a New Orleans.

Se la vittima, in buona fede, comunica le informazioni richieste, il criminale le usa o per prosciugare il suo conto corrente o per attivare una nuova carta di credito a nome del truffato o, in alcuni casi, le vende al miglior offerente.

Tra le organizzazioni che sono state fatte oggetto di attacchi di phishing in Italia, vi sono in prevalenza le banche (molte delle principali), mentre negli USA sono stati colpiti molti dipartimenti governativi, negozi online, grandi istituzioni finanziarie e alcune grosse federazioni sportive.



Nel corso del 2005, gli attacchi di phishing si sono fatti più sofisticati per aggirare il fatto che le persone sono sempre più informate sul fenomeno e quindi meno ingenui.

Il cosiddetto 'spear (fiocina) phishing', ad esempio, è molto più mirato del phishing tradizionale ed è indirizzato a persone o gruppi specifici, che vengono tratte in inganno, ad esempio, da una email che sembra in tutto e per tutto proveniente dalla direzione del personale che chiede al dipendente informazioni personali riservate.

Un altro nuovo trend vede diminuire progressivamente l'interesse verso il phishing mirato a furti di identità perpetrati ai danni di singoli e crescere di contro quello finalizzato allo spionaggio industriale, ovvero alla sottrazione di piani per i lanci di nuovi prodotti o di informazioni di progettazione, che possono essere vendute sottobanco ai concorrenti.

Il pharming è un tipo di attacco che reindirizza verso siti fraudolenti gli utenti che tentano di connettersi a un sito autentico. L'utente ignaro digita l'indirizzo del sito – spesso archiviato tra i preferiti - a quello che sembra un sito di banking online familiare e viene indirizzato su un sito fraudolento

La maggior parte degli exploit usati per il pharming usa wildcard DNS e URL encoding per creare link email che sembrano portare a siti autentici. Invece indirizzano su siti fasulli, dove i phisher provano a sottrarre informazioni confidenziali su account online o numeri di carta di credito..

Ciò che aggrava i problemi per gli staff IT impegnati nella protezione delle organizzazioni da minacce sempre meno prevedibili è che molti utenti interni pensano di essere al sicuro perché alla protezione pensano i servizi IT.

Secondo un recente sondaggio, circa il 40% degli utenti aziendali è convinto che l'IT si occupi di impedire che loro cadano vittime del phishing e quindi assumono comportamenti fortemente a rischio.

Nel 2005, 200 aziende di tutto il mondo, tra le quali DaimlerChrysler, American Express e Visa, sono cadute vittime di un worm chiamato Zotob, che causava un continuo riavvio dei computer infettati.

Zotob è stato in fondo meno dannoso di molti predecessori, interessando soprattutto grandi aziende con migliaia di desktop con ancora installato Windows 2000. Zotob è uno dei più recenti esempi noti di attacco sferrato con l'ausilio di una 'bot network' o 'botnet'.

I 'bot' – insieme di computer trasformati in 'robot' da virus Trojan – stanno diventando un problema sempre più serio, considerando che nel 2005 il numero stimato di bot sembra essere raddoppiato, se non triplicato, rispetto al 2004.

Un PC con software 'bot' installato – magari mediante un sito maligno o un Trojan horse – viene chiamato 'zombie'. Questi zombie vengono controllati da remoto dai cybercriminali. Una volta installato su un PC, il software bot tipicamente si collega a Internet Relay Chat (IRC) per ricevere i comandi.

Il fenomeno è preoccupante perché le bot offrono la protezione dell'anonimità. Una botnet può essere predisposta per operare da qualsiasi luogo del mondo per infettare i vostri computer o mandare in down il vostro sito mediante un attacco Distributed Denial of Service (DDoS) e individuare chi ha sferrato l'attacco sarà molto difficile.

Gli attacchi DDoS sono lo scopo più comune per il quale sono create le botnet, che vengono schierate per un attacco coordinato di massa sferrato attraverso migliaia di bot controllati ai danni di siti web mediante saturazione della capacità di banda e l'impossibilità quindi di rispondere alle connessioni legittime.



Un grosso sito di gioco online ha subito un attacco DDoS quando una botnet ha ordinato a un enorme numero di PC di visitare il sito, causandone così il collasso. Come conseguenza, gli utenti che davvero desideravano giocare non riuscivano a collegarsi, facendo perdere guadagni ai gestori del sito. In questo caso, i criminali hanno anche ricattato l'azienda, offrendosi di interrompere l'attacco dietro pagamento di una ingente somma di denaro.

Le botnet vengono anche affittate dai loro 'proprietari' a chi desidera usarle per rilanciare attacchi phishing o distribuire spam.

La preoccupazione è che le botnet sono diventate uno dei più efficaci "modelli di business" per il cybercrime. I PC di una grande azienda potrebbero essere ai comandi di un gruppo di creatori di malware senza che nessuno se ne accorga. Una botnet potrebbe perfino essere affittata a un'azienda per sferrare un attacco DDoS a un concorrente. La cosa è meno incredibile di quanto potrebbe sembrare.

La cattiva notizia è che le cose potrebbero peggiorare, poiché per mantenere il controllo sui PC zombie, i cybercriminali potrebbero aggiungere al loro software crittografia in grado di impedire l'individuazione e la rimozione da parte dei tool di sniffing. Ciò renderà l'individuazione delle botnet sempre più complicata.

Ma allora come possono difendersi le organizzazioni contro un attacco botnet? Nel caso di Zotob, si crede che molte delle aziende potrebbero essere state colpite quando un notebook infetto è stato ricollegato alla rete aziendale, senza patch installate e quindi non sicuro. E' infatti più una scarsa propensione al patching che una mancanza di sistemi di difesa a mettere spesso a rischio i sistemi. Sistemi con tutti i patch a posto e aggiornati sono meno vulnerabili agli attacchi bot.

# INSTANT MESSAGING & P2P

---

La società di ricerche Gartner descrive l'instant messaging (IM) come 'il gigante dormiente di internet' predicendo che alla fine quasi tutti lo useranno per le comunicazioni aziendali o personali. Da semplice strumento per lo scambio istantaneo di messaggi, l'IM sta evolvendo verso una piattaforma di front-end per le applicazioni aziendali. Questo in un momento in cui i livelli di spam, spyware e phishing in circolazione hanno minato la fiducia nei confronti della posta elettronica.

L'ironia è che le aziende hanno speso un mucchio di soldi e molti anni-uomo per rendere sicuri i sistemi email e adesso si trovano a dover affrontare il rischio che virus, worm e codice maligno attacchino l'azienda attraverso l'IM.

Un recente sondaggio ha verificato che il 62% delle organizzazioni ha adottato misure per difendere dalle minacce i sistemi di posta elettronica, ma non ritiene che adottare le stesse misure per proteggersi da IM e P2P sia una priorità. In un sondaggio condotto presso oltre 100 aziende, solo l'11% è risultato avere soluzioni IM attive, a confronto di un 73% dotato di email. Il 50% dei partecipanti ha dichiarato di non aver mai considerato una soluzione IM.

Pensate ad esempio a un dipendente scontento che decida di passare segreti aziendali via IM a un amico che lavora per un concorrente. Per evitare di essere scoperto, potrebbe usare utility che "travestono" i file riservati da MP3 e spedirli inviando i servizi di file sharing P2P dell'azienda. Particolarmente preoccupante è l'uso degli allegati IM poiché essi non sono intercettati dai sistemi per la sicurezza della rete. I messaggi IM che li veicolano magari sono innocui, ma determinati allegati possono invece essere rischiosi.



Questa esplosione di applicazioni IM e P2P sul luogo di lavoro pone una nuova sfida alla sicurezza, giacchè i dipendenti sono liberi di scaricare queste applicazioni gratuite, senza essere individuati dagli strumenti di monitoraggio dei dipartimenti IT. E' quindi importante che i responsabili IT siano sensibilizzati sui rischi associati alla rapida diffusione di IM e P2P.

Oltre al rischio di spionaggio industriale, le applicazioni IM e P2P offrono anche ulteriori punti di ingresso alla rete aziendale per intrusioni, furti di dati, attacchi denial-of-service, virus e worm. I sistemi P2P spesso favoriscono lo spyware tramite reti per il music-sharing come Kazaa.

Le applicazioni IM e P2P sono abili a bypassare i firewall, usando tecniche di port-scanning e tunnelling. Nessuno dei sistemi IM più noti offre autenticazione forte o crittografia. Essi sono quindi vulnerabili nei confronti di occhi e orecchi indiscreti o della divulgazione di informazioni riservate.

La possibilità di ridurre i costi delle comunicazioni adottando reti P2P che usano servizi VoIP come Skype deve essere bilanciata con le minacce per la sicurezza poste da una tecnologia ancora poco nota e potenzialmente non sicura.

A novembre 2005, ammontavano a oltre 215 milioni i download del client VoIP gratuito Skype. Tuttavia, contemporaneamente è partita una campagna di sensibilizzazione contro i rischi di Skype, con alcuni analisti che mettono in guardia le aziende in merito alla sua adozione, bollandolo come "non controllabile, non tracciabile, non verificabile" e perfino in grado di mettere a rischio la capacità delle aziende di ottemperare alle norme per la sicurezza.

Il consiglio per le organizzazioni che stanno pensando di usare Skype è di gestirlo con attenzione e policy di sicurezza idonee.

# CRIMEWARE & EXPLOIT 'ZERO-DAY'

---

Con il termine crimeware si intende ogni programma o tool software espressamente progettato per favorire attività illegali online.

Il crimeware abbraccia una varietà di tecniche efferate o criminali – come spyware e keylogging – dove la motivazione degli attacchi è il profitto. Rientrano in questa categoria le cyber estorsioni dove i criminali chiedono soldi per non mandare in down i siti web; oppure la creazione di un problema con lo scopo di ottenere del denaro per risolverlo, come nel caso degli attacchi DDoS.

Molti programmi spyware, keylogger, backdoor e Trojan possono essere considerati crimeware, così come i cosiddetti 'phishing kit', che contengono tool per permettere anche ai meno esperti di lanciare un attacco phishing.

Tali kit tipicamente includono software per lo sviluppo di siti web che imitano in modo convincente siti reali e software di spamming per automatizzare il processo di mass mailing. Questi phishing kit e altri tipi di crimeware sono facilmente reperibili su internet.

Secondo un rapporto dell'Anti-Phishing Working Group (APWG) – una delle organizzazioni più impegnate nella prevenzione del cybercrime – i siti che distribuiscono crimeware risultavano quasi raddoppiati da novembre a dicembre 2005: da 4630 a 7197.

Alcuni ritengono che l'industria dell'e-crime abbia raggiunto un livello di efficienza e sofisticazione tale da avere il potenziale per minacciare l'intera economia online.



La crescente sofisticazione degli attacchi da parte del crimine organizzato è coincisa con il successo riscontrato dai cybercriminali nello sfruttamento delle vulnerabilità di programmi popolari come Microsoft Windows. Tra questi vi sono i cosiddetti attacchi 'zero-day', ovvero quelli che sfruttano una vulnerabilità il giorno stesso in cui viene resa nota. Un po' come il "Santo Graal" per gli autori di virus e programmi maligni.

Creando un exploit in grado di sfruttare una vulnerabilità della quale il produttore del programma non è ancora a conoscenza e dunque per la quale non è disponibile alcuna patch, il cybercriminale può provocare il massimo dei danni.

Tra il Natale e il Capodanno del 2005, si è verificato un tipico attacco 'zero-day', che ha sfruttato una vulnerabilità sconosciuta di Microsoft Windows relativa all'elaborazione dei file grafici Windows Meta File (WMF). La vulnerabilità è stata scoperta dai Websense Security Labs.

La minaccia portata dalla vulnerabilità WMF è stata potente perché tutto ciò che gli hacker dovevano fare era di incorporare codice maligno all'interno di un'immagine, collocarla su un sito e quindi attirarvi gli utenti. Semplicemente navigando sul sito, il sistema operativo dell'utente eseguiva il codice maligno contenuto nell'immagine.

La vulnerabilità WMF è stata alla fine risolta con un patch rilasciato da Microsoft prima della scadenza mensile normalmente prevista, cosa che dimostra la pericolosità reale della minaccia.

Questo episodio insegna che le aziende dovrebbero sempre avere procedure di patching efficienti e tempestive. Purtroppo talvolta solo incidenti potenzialmente molto seri come quello WMF possono scuotere l'azienda dall'inerzia e convincerla a attuare le procedure di protezione necessarie.

# COME PROTEGGERE L'ORGANIZZAZIONE

Con l'aumento di questi nuovi tipi di crimeware, antivirus e firewall non bastano per proteggere le organizzazioni dagli attacchi. La checklist che segue vi mostra ciò che dovete fare per proteggere la vostra organizzazione dal crimine online.

- ❑ Policy per la sicurezza scritte con procedure chiare per controllo dei rischi e adeguamento delle policy continui.
- ❑ Policy scritte ben definite e accettate per l'uso degli asset IT e della rete.
- ❑ Guida alla sicurezza IT e procedure definite per la formazione dei nuovi assunti e dello staff esistente.
- ❑ Firewall di rete installato.
- ❑ Soluzione antivirus.
- ❑ Procedure di autenticazione forte, che comprendano la biometria o altri metodi di autenticazione a due fattori.
- ❑ Efficaci procedure interne di gestione delle patch per garantire che siano installate sui computer il più rapidamente possibile.
- ❑ Penetration test eseguiti regolarmente per una continua verifica dei rischi.
- ❑ Soluzione di intrusion detection e prevention (IDS/IPS).
- ❑ Soluzioni che forniscono livelli di difesa multipli contro le minacce miste.
- ❑ Soluzione per prevenire l'esposizione alle minacce del web.
- ❑ Soluzione che consenta di attuare una policy d'uso accettabile per l'accesso a internet da parte dei lavoratori interni e remoti.
- ❑ Soluzione che consenta di attuare una policy d'uso accettabile per applicazioni quali P2P e IM (specialmente relativamente agli allegati).
- ❑ Soluzione anti-spyware in grado non solo di identificare e bloccare lo spyware ma anche la comunicazione backchannel per prevenire danni derivanti da spyware installato.
- ❑ Soluzione per il blocco delle applicazioni per prevenire l'installazione ed esecuzione di quelle non autorizzate.
- ❑ Procedure robuste per la verifica e il controllo della conformità alle policy dei computer remoti al momento della riconnessione alla rete aziendale per evitare che la infettino.
- ❑ Tool per gestire l'accesso a strumenti che presentano rischi potenziali di furto di dati, come ad esempio drive USB e lettori CD/DVD.
- ❑ Soluzione di sicurezza completa e robusta per proteggere lavoratori remoti e mobili dagli attacchi quando sono lontani dall'ufficio.
- ❑ Tool che forniscono capacità di forensic analysis per il risk assessment e il tracciamento dell'esposizione ai rischi di sicurezza.
- ❑ Soluzioni che forniscono intelligence aggiornata in tempo reale contro le minacce per ridurre o prevenire l'esposizione ai rischi.
- ❑ Software e processi interni per la gestione delle password, in particolare per i lavoratori temporanei (talvolta utilizzati per lo spionaggio industriale).
- ❑ Formazione per creare nel personale consapevolezza dell'esistenza delle tecniche di social engineering utilizzate per il phishing e altri attacchi.



# LE SOLUZIONI WEBSENSE PER LA SICUREZZA

Per avere la certezza di implementare la soluzione più efficiente e conveniente per il livello di protezione che la vostra organizzazione richiede, dovete:

- attivare misure di sicurezza preventiva contro le minacce e migliorare la reazione agli attacchi via web
- migliorare la produttività dell'utente finale aumentando il livello di servizio e minimizzando i downtime
- rendere disponibile una soluzione per la sicurezza flessibile e scalabile che riduca i costi di gestione IT
- aderire alle normative di conformità proteggendo utenti e informazioni riservate

Per soddisfare queste esigenze, in aggiunta alle soluzioni di sicurezza tradizionali è necessario un livello di protezione extra: Websense Web Security Suite™. Le organizzazioni che implementano la Websense Web Security Suite sono protette da una soluzione per la sicurezza avanzata che consente di:

- risparmiare tempo e denaro bloccando le minacce prima che raggiungano il desktop
- ridurre il tempo di esposizione alle minacce
- evitare che lo spyware installato sui sistemi faccia danni
- colmare il gap in termini di sicurezza e compliance dell'IM
- evitare che applicazioni dannose causino problemi di sicurezza
- avere il massimo controllo sui desktop

---

## Referenze

**Panoramica generale:** <http://www.sans.org/top20/#w2>

**Spyware:** <http://www.computerworld.com/printthis/2005/0,4814,99727,00.html>; <http://www.net-security.org/article.php?id=588>;  
<http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,100455,00.html>

**Phishing:** <http://www.vnunet.com/vnunet/news/2142275/work-pc-users-ignore-security>

**IM & P2P:** [http://www.akonix.com/news/press\\_releases\\_2006/01172006.asp](http://www.akonix.com/news/press_releases_2006/01172006.asp);  
<http://www.computerweekly.com/Articles/2006/01/09/213582/VoicingconcernsonSkype.htm>

**Bot:** <http://www.baselinemag.com/article2/0,1397,1901716,00.asp>; [http://www.toptechnews.com/story.xhtml?story\\_id=41146](http://www.toptechnews.com/story.xhtml?story_id=41146)

**Crimeware & Exploit Zero-Day:** <http://www.financetech.com/news/showArticle.jhtml?articleID=180202327>

© 2006, Websense, Inc. Tutti i diritti riservati. Websense e Websense Enterprise sono marchi registrati di Websense, Inc. negli Stati Uniti e in alcuni mercati internazionali. Websense ha numerosi altri marchi commerciali non registrati negli Stati Uniti e in altri paesi. Tutti gli altri marchi sono di proprietà dei rispettivi proprietari.

## Informazioni su Websense

Websense, Inc. (NASDAQ:WBSN), leader globale nel web filtering e nella web security, fornisce le proprie soluzioni a oltre 24.000 organizzazioni nel mondo. Websense scopre preventivamente e protegge immediatamente contro le minacce web-based come spyware, phishing, virus e crimeware. Grazie anche a numerose partnership e integrazioni, Websense completa gli ambienti di rete e di sicurezza dei clienti.

[www.websense.it](http://www.websense.it)

### **Websense Italy**

Piazzale Biancamano 8, Milan 20121, Italy  
TEL: + 39 02 6203 3040

### **Websense, Inc.**

10240 Sorrento Valley Road, San Diego, CA 92121, USA  
TEL: +1 858.320.8000