



Websense® White Paper

## Tatort Internet: Bot-Netze

*Websense informiert zum Thema Bot-Netze und wie Sie Ihr Unternehmen vor der neuen Gefahr aus dem Internet schützen können*

### Synopsis:

Unternehmen sehen sich heute mit einer neuen Gefahr für die IT Sicherheit konfrontiert, die nicht mehr länger die Domäne von jugendlichen Hackern ist, sondern gezielt und heimtückisch vorgeht und überwiegend auf finanziellen Motiven beruht.

Es handelt sich hierbei um eine Form organisierten Verbrechens, kontrolliert von Kriminellen die online grössere Gewinne bei geringerem Risiko erzielen können. Sie haben es auf Informationen abgesehen – egal ob vertrauliche Unternehmensdaten oder persönliche Informationen - welche gewinnbringend weiterveräußert werden können oder aber als Druckmittel bei Betrugs- und Erpressungsversuchen eingesetzt werden.

## Inhaltsverzeichnis:

<b>Tatort Internet: Bot-Netze</b>	<b>3</b>
• Angriff der Computer-Zombies	3
• Catch me if you can	3
• Zu gut, um wahr zu sein – Too good to be true	4
• Ferngesteuerte Armeen	5
<b>Lösungswege für effektiven Schutz vor Bot-Netzen</b>	<b>6</b>
• Websense Security Labs	7
• Websense Web Security Suite – Lockdown Edition	7
• Websense Web Protection Services	8
• Websense Real-Time Security Updates	8
<b>Zusammenfassung</b>	<b>9</b>
<b>Websense Firmenprofil</b>	<b>9</b>

## Bot-Netze

### Angriff der Computer-Zombies

Bot-Netze sind eine der gefährlichsten Formen der Internetkriminalität. Tausende mit Trojanern infizierte Zombie-Rechner werden beispielsweise für Denial-of-Service-Attacken missbraucht, verbunden mit der Erpressung der angegriffenen Betreiber einer Webseite. Damit die eigenen PCs nicht in Hände solcher Schutzgelderpresser fallen, ist der Aufbau eines gestaffelten Schutzwalls auf Desktops und Notebooks, im LAN und am Internetzugang sinnvoll.

Der Amerikaner Jeanson James Ancheta muss für 4 Jahre und 9 Monate hinter Gitter. Über Computer-Würmer hatte der aus Los Angeles stammende Mann mehrere hunderttausend Rechner infiziert und sein Netzwerk aus Zombie-PCs für den Spam-Versand und Denial-of-Service-Attacken in 30 Fällen vermietet. Versucht mit der Zombie-Software von Ancheta waren nicht nur Privat-PCs, denn das FBI fand auch auf Computern der US-Marine und des Verteidigungsministeriums "Crimeware" aus Anchetas Giftküche.

*Das BKA verzeichnete in seinem Bericht "IuK Kriminalität 2004" mit 1,743 erfassten Fällen im Bereich "Ausspähen von Daten" einen Zuwachs von 223% zum Vorjahr.*

*Bundesrepublik Deutschland, BKA*

Und Ancheta ist kein Einzelfall. Im vergangenen Jahr wurden in den Niederlanden drei mutmaßliche Bot-Netz-Betreiber verhaftet. Die Strafverfolgungsbehörden werfen ihnen vor, mehr als 1,5 Millionen Rechner mit der Schadsoftware Backdoor.Win32.Codbot unter ihre Kontrolle gebracht zu haben. In unterschiedlichen Varianten ist der Trojaner auch unter der Bezeichnung Toxbot im Umlauf.

### Catch me if you can

Die niederländischen Behörden gehen davon aus, dass über Toxbot das Bot-Netz aufgebaut und weiter verbreitet wurde. Dabei haben die Verdächtigen den Trojaner permanent verändert, damit er nicht von vorhandenen Virenschannern entdeckt wird. Toxbot war den digitalen Spürhunden immer einen Schritt voraus. Das Gefährliche an Toxbot: Der Trojaner zeichnete Tastatureingaben auf. Nach Angaben der Ermittler haben die Bot-Netz-Betreiber den Keylogger auf Rechnern installiert, um an Zugangsdaten von Kreditkarten, Paypal-Konten und eBay-Accounts zu kommen. Diese Informationen hat das Trio dann weiterverkauft. Ein weiterer Anklagepunkt lautet: Erpressung eines Unternehmens. Die drei sollen Unternehmen in den USA mit einer Distributed-Denial-of-Service(DDoS)-Angriffe für den Fall bedroht haben, dass die Firmen keine „Schutzgelder“ zahlen.

An dem Fall aus den Niederlanden, bei dem noch kein abschließendes Urteil ergangen ist, lässt sich sehr gut die Entstehungs- und Verlaufsgeschichte von Bot-Netzen nachvollziehen. Bot-Netze arbeiten mit einer Kombination mehrerer Zutaten aus der Giftküche der Internetkriminalität: Keylogging, Phishing, Spyware, Trojaner, Würmer etc. Diese unterschiedlichen Programmcode-Varianten (Crimeware) werden auf verschiedenste Weise in Computersystemen eingeschleust.

Eines der gängigsten Verfahren besteht darin, dass die Crimeware über Mail-Attachments oder infizierte Applikationen auf die Rechner gelangt. Das kann einem Anwender mit seinem Home-PC passieren, aber auch Benutzer in Unternehmen sind davor nicht gefeit: nämlich dann, wenn die Anwender mit ihren Rechnern einen ungesicherten Zugang zu Web-Ressourcen haben und die IT-Abteilung nur „zahnlose“ oder leicht zu umgehende Security-Richtlinien implementiert hat.

### Zu gut, um wahr zu sein – Too good to be true

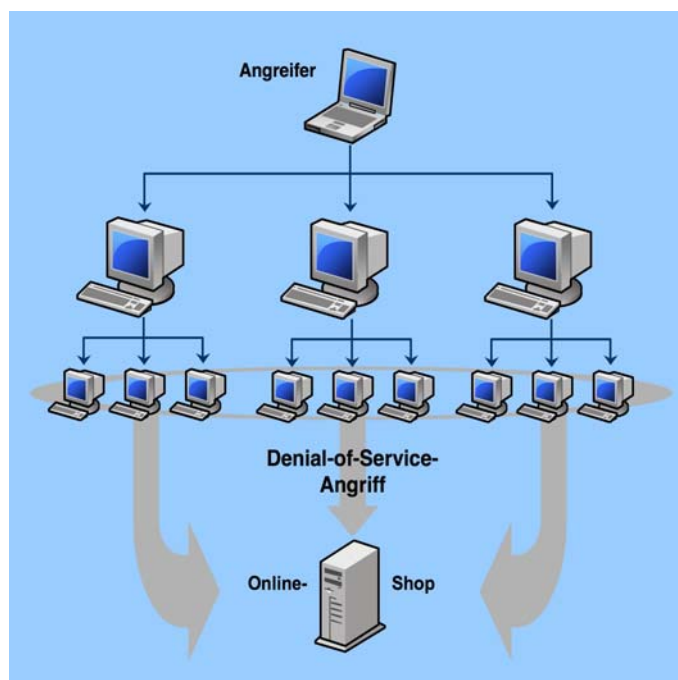
Um Bot-Netze in kurzer Zeit aufbauen zu können, bedienen sich die Betreiber ganz unterschiedlicher Methoden. Unter dem Begriff „Social Engineering“ werden aber häufig unglaublich klingende bzw. kostenlose Angebote lanciert, die den Anwender zu einer Aktivität im Netz bewegen sollen. Eine bekannte Gefahrenquelle sind hier kostenlose Programme, die sich Anwender während der Arbeitszeit, unterwegs mit dem Firmen-Notebook oder in ihrem Home-Office schnell zwischendurch aus dem Internet herunterladen. Auch Online-Games gelten als beliebtes Trägermedium, das im Huckepackverfahren „Trojanische Pferde“ (abgekürzt: Trojaner) einschleusen.

Nahe verwandt damit sind Methoden, bei denen über ein Backdoor direkt oder auch nachträglich Trojaner installiert werden. Potenzielle Betreiber von Bot-Netzen nutzen in dem Fall beispielsweise ungepatchte Sicherheitslücken in Betriebssystemen, Browsern oder Applikationen. Stark gefährdet sind auch Instant-Messaging-Anwendungen – unabhängig davon, ob sie privat oder auf den Firmen-PCs genutzt werden – und Peer-to-Peer-Netzwerke, über die Benutzer Musik und Filme austauschen.

Laut Definition verrichtet ein Trojaner seine Arbeit im Hintergrund, ohne Wissen des Anwenders. Das heimtückische daran: Eingebunden in ein Bot-Netz lassen sich Trojaner beliebig fernsteuern, wie es im Fall der niederländischen Bot-Netzbetreiber auch praktiziert wurde. Die Aktivität des Trojaners kann beispielsweise auch darin bestehen, dass sich die Software einem Anwender gegenüber als Loginprozess ausgibt und im Hintergrund heimlich das Passwort aufzeichnet. Der Betreiber eines Bot-Netzes hat dann ungehindert Zugang zum Rechner und kann den Zombie-PC für seine eigenen kriminellen Zwecke einsetzen.

Eine weitere Variante, wie Programmcode auf fremde Rechner geladen wird, sind so genannte „Drive-by-Downloads“: Besuchen Surfer nichts ahnend eine scheinbar harmlose Webseite müssen sie später feststellen, dass im Hintergrund irgendeine Form von Malware auf ihren Rechnern installiert wurde. Passieren kann das zum Beispiel durch das Akzeptieren unklarer Nutzungsbestimmungen oder durch unsichere Browsereinstellungen. Schätzungen der Websense Security Labs zufolge bewegt sich die Zahl der Websites, die Schadsoftware über Drive-by-Downloads installieren wollen zwischen hunderten und tausenden – die Statistiken schwanken hier von Monat zu Monat, denn viele solcher Seiten sind nur für kurze Zeit aktiv, weil sie zu Recht befürchten, dass sie von digitalen Ermittlern aufgespürt werden.

Die Varianten und Kombinationen, mit denen Trojanische Pferde Zugang zu Rechnern erhalten, sind nahezu unbegrenzt. Das hinterhältige daran: In dieser Form verhalten sich die Trojanischen Pferde dem „Gastgeber“ gegenüber weitgehend freundlich: Sie beeinträchtigen nicht die tägliche Nutzung des Rechners und richten ansonsten, im Gegensatz zu Viren, keinen Schaden auf dem PC an. Allerdings ist ihre indirekte Wirkung dafür umso gravierender.



### Ferngesteuerte Armeen

In der Anfangsphase wird es ein Bot-Netzbetreiber aus nachvollziehbaren Gründen darauf anlegen, eine möglichst große Zahl von Rechner mit seiner Crimeware auszustatten. Je größer das Reservoir aus dem er schöpfen kann, desto besser. Internet-Security-Experten wie Websense konnten in verschiedenen Fällen nachweisen, dass Bot-Netz-Betreiber unter Einbeziehung von Suchmaschinen gezielt nach Sicherheitslücken und Verwundbarkeiten suchen, um neue Computer unter ihre Kontrolle zu bekommen.

Ist das Bot-Netz, in Form eines virtuellen Verbunds tausender infizierter Clients startklar, wird bei den heute bekannten Varianten meist das Internet-Relay-Chat-Netzwerk (IRC) zur Kommunikation zwischen dem Master (Bot Herder) und der Zombie-Armee (den Bots) eingesetzt. Über einen gemeinsamen Kanal (den Channel) können sich Teilnehmer abstimmen. Häufig ist der Channel mit einem Passwort geschützt und zudem wird der Datenverkehr verschlüsselt.

Das alles macht es den Sicherheitsbehörden schwer, in einer Art Reverse Engineering die Arbeitsweise und die Struktur eines Bot-Netzes nachzuzeichnen. Der Bot Herder bedient als Administrator beziehungsweise Operator den IRC-Server als Relaisstation. Die Bots werden so aus der Ferne gesteuert. Mögliche Aufträge lauten: Beteilige dich an einem Denial-of-Service-Angriff. Suche nach PCs, die mit anderer oder konkurrierender Bot-Software infiziert sind. Deinstalliere bekannte AV-Programme usw.

Neben Denial-of-Service-Attacken und der Verbreitung neuer Malware ist der Einsatz von Bot-Netzen als Spam-Relay ein weit verbreitetes Szenario. Hier wiederum treten zwei Varianten auf: Entweder der „Bot-Netz-Eigentümer“ verschickt selbst Spam-Nachrichten, um die Adressaten zu irgendwelchen Aktionen zu veranlassen – möglicherweise einen Dateianhang mit einem bösartigen Programm zu installieren – oder er vermietet seine Infrastruktur an Dritte, die dann beispielsweise Phishing-E-Mails versenden.

Im Internet kursieren in den einschlägigen Foren immer wieder Preislisten zum Botnet Leasing, die zeigen, dass die Vermietung der Infrastruktur ein durchaus lohnendes Nebengeschäft ist. Statt von einem, werden die Mails dann von tausenden von Servern verschickt. Die folgende Berechnung verdeutlicht den Wirkungsgrad: Man mietet 1.000 infizierte PCs und verschickt von jedem 100 Spam-Nachrichten. Mit einem Schlag lassen sich so 100.000 Werbebotschaften versenden. Gleichzeitig bedeutet dies, dass die Spam-Versender technisch nur sehr schwer zu lokalisieren und zu neutralisieren sind.

Die nebenstehende Tabelle verdeutlicht die Schlagkraft von Bot-Netzen unterschiedlicher Größe:

**3.000-Zombies Botnet**

Angriff	Requests/Bot	Botnet Total	Ressourcenverbrauch
Bandwidth Flood (Uplink)	186 kbps	558 Mbps	T1, T3, OC-3 (155Mbps) Feb 2002 South Korea (355Mbps)
Bandwidth Flood (Downlink)	450 kbps	1,35 Gbps	T1, T3, OC-3, OC-12 (622Mbps)
Syn Flood	450 SYNs/sec	1,35M SYN/sec	Dedizierter Cisco Guard (@\$90k) oder 6 High-End Server
Static http get (cached)	93/sec	279.000/sec	5 Server
Dynamic http get	93/sec	279.000/sec	93 Server
SSL Handshake	10/sec	30.000/sec	50 Server

**10.000-Zombies Botnet**

Angriff	Requests/Bot	Botnet Total	Ressourcenverbrauch
Bandwidth Flood (Uplink)	186 kbps	1,86 Gbps	T1, T3, OC-3, OC-12
Bandwidth Flood (Downlink)	450 kbps	4,5 Gbps	T1, T3, OC-3, OC-12, OC-48 (2.488Gbps) 50% des Taiwan/US backbone
Syn Flood	450 SYNs/sec	4,5M SYN/sec	4 dedizierte Cisco Guard (@\$90k) oder 20 High-End Server
Static http get (cached)	93/sec	929.000/sec	15 Server
Dynamic http get	93/sec	929.000/sec	310 Server
SSL Handshake	10/sec	100.000/sec	167 Server

## Lösungswege für effektiven Schutz vor Bot-Netzen

In Anbetracht der massiven Bedrohungen bleibt abschließend die Frage: Wie kann sich ein Unternehmen schützen? Firewalls und Virens Scanner reichen hier bei weitem nicht mehr aus. Notwendig ist vielmehr eine mehrstufige integrierte Web Security-Lösung wie sie etwa Websense bietet. Sie besteht aus Tools, die für eine Einhaltung der einmal definierten Sicherheitsrichtlinien am PC, im LAN und am Internet-Gateway sorgen.

Im Mittelpunkt der Sicherheitsmassnahmen stehen die von den Mitarbeitern genutzten Desktopsysteme und Notebooks. Das Ziel ist hier, den Start bestimmter Applikationen und Dateitypen, die Viren, Würmer, Trojaner oder Spyware verbreiten, auf den Rechnern zu verhindern. Sicherheitskräfte in den Unternehmen definieren dazu Policies, die darüber wachen, ob jemand versucht, Hacking-Tools oder zum Beispiel Online-Spiele zu starten.

Diese Policies müssen natürlich auch Mitarbeiter schützen, die mit ihren Notebooks außerhalb des Firmennetzes an einem Hotspot, im Hotel oder einem Internetcafé im Web surfen. Unabhängig davon, mit welchen Endgeräten und an welchem Ort Mitarbeiter auf das Internet zugreifen: Für alle müssen die identischen zentral vorgegebenen Sicherheitsrichtlinien aktiviert sein.

Die zweite Verteidigungslinie bildet das Firmen-LAN. Auf der Agenda steht hier beispielsweise, die Bandbreitennutzung der Internetanbindung zu analysieren: Gibt es während der Arbeitszeit auffällig hohe Spitzenwerte von Anwendungen die mit dem Internet kommunizieren? Sind einzelne Systeme dauerhaft aktiv, obwohl diese nur in Ausnahmefällen von Mitarbeitern genutzt werden? Solch ungewöhnliches Verhalten liefert oft Anzeichen für Missbrauch durch Hacker.

Am Internet-Gateway – der letzten Verteidigungslinie für Crimeware-Risiken – geht es darum, Sicherheitsrisiken aus dem Internet zeitnah zu entdecken, zu analysieren und sich so binnen kürzester Zeit vor Bedrohungen aus dem Internet zu schützen: Viren, Spyware, Phishing-Angriffe und Trojaner. Durch die Festlegung zentraler Policies lassen sich die Sicherheitseinstellungen wirksam steuern und kontrollieren. Der Zeitfaktor ist hierbei nicht zu unterschätzen, da immer häufiger legitime Webseiten gehackt und als Infektionsweg missbraucht werden.

Denn ist möglicherweise doch ein Trojaner, der sich später als Bot verhält, unbemerkt ins LAN eingeschleust worden, muss eine wirksame Web Security-Lösung sofort verhindern können, dass der Trojaner Kontakt mit der Botzentrale aufnehmen kann – noch bevor der Administrator Zeit hat, das System vom Netz zu nehmen und neu zu installieren. Es geht also nicht nur darum, den eingehenden Verkehr zu analysieren, wichtig ist auch, ausgehende Daten unter Kontrolle zu haben. Erst diese Zwei-Wege-Funktion macht eine Security-Lösung wirklich effektiv.

### In die Falle gelockt ...

Eine der Methoden, um Bot-Netzen auf die Spur zu kommen sind „Honigtöpfe“ (Honeypots). Sie sollen Bots, Spyware, Trojaner und andere Malware anlocken. Sind die digitalen Schädlinge dann in die Falle gegangen, haben Internet-Security-Spezialisten die Möglichkeit, die Angriffsmethoden und Vorgehensweisen unterschiedlicher Formen der Cyberkriminalität detailliert zu untersuchen. Mit Verfahren des Reverse Engineering (ausgehend von einer tatsächlichen Attacke wird die Vorgehensweise rekonstruiert) lässt sich die Arbeitsweise ein Bot-Netzes entschlüsseln. Dazu kommen Methoden der digitalen Forensik. Hier werden etwa die Protokolle des Netzwerkverkehrs genauer untersucht, um Spuren der Bots nachzuzeichnen, zu verstehen und schließlich Maßnahmen zur Abwehr entwickeln zu können.

## WebSense Security Labs

Alle Security-Produkte von Websense verwenden Technologien und Erkenntnisse der Websense Security Labs. Durch die Recherche und Analyse von wöchentlich über 650 Millionen Websites, dem Entdecken von betrügerischen Aktivitäten im Internet durch Protokolle bzw. Anwendungen ermöglichen die Websense Security Labs zeitnahe Produktaktualisierungen und frühzeitige Warnhinweise für Kunden und Sicherheitsfachleute, die auf diese Weise bei der Optimierung von Sicherheitsvorkehrungen unterstützt werden. Die Vorgehensweise der Websense Security Labs unterteilt sich wie folgt:

- Internetanalyse - weltweit und rund um die Uhr.
- Automatisierte Data Mining- und manuelle Analyseprozesse zur systematischen Begutachtung von Websites, P2P-Netzwerken und anderen Systemen auf der Suche nach gefährlichen Inhalten und schädlichen Anwendungsprogrammen.
- Die zum Patent angemeldeten Technologien WebCatcher™ und AppCatcher™, durch die Kunden Vorkommnisse melden können.
- Fortlaufende Überwachung von Newsgroups, Chat-Räumen, sicherheitsbezogener Websites und Onlineforen auf der Suche nach Sicherheitslücken und Exploits.

Die Websense Security Labs spüren eigenständig Gefahrenquellen im Internet auf und bieten sofortigen Schutz. So wurden u. a. folgende Sicherheitsrisiken zuerst durch Websense ermittelt:

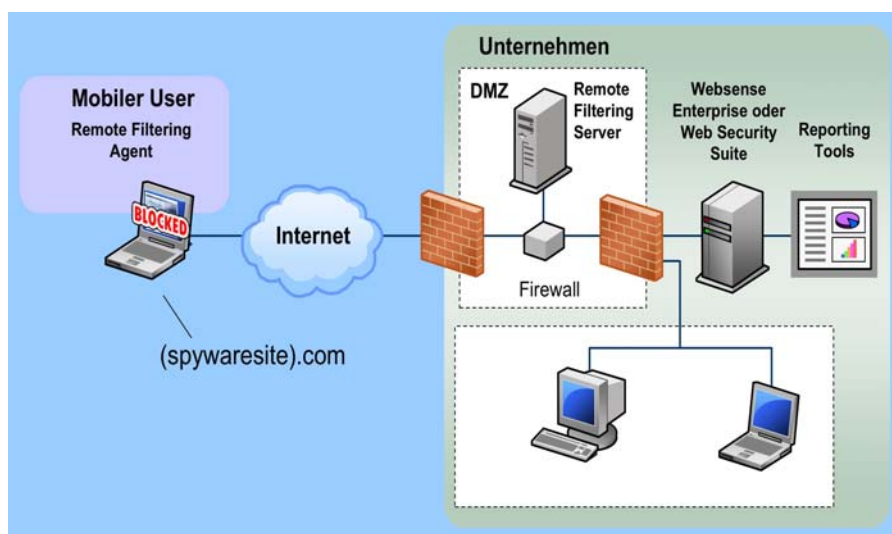
- Websites, die über eine Sicherheitslücke in Microsoft Windows in Zusammenhang mit .WMF-Bilddateien nutzten, um Spyware zu verbreiten.
- Verbreitung von schädlichem Programmcode über eine gehackte Microsoft-Website.
- Erpressungsversuche per Internet (auch bekannt als Ransomware).
- Sicherheitslücke im Sony Digital Restrictions Management (DRM) Rootkit.

## WebSense Web Security Suite – Lockdown Edition

Die Web Security Suite – Lockdown Edition™ von Websense® ist die international führende Software-Lösung, die Unternehmen Schutz vor bekannten und neuen Gefahren im Internet bietet. Websense wehrt Bot-Netze, Spyware, Trojaner und Keylogger ebenso wie Phishing-Angriffe ab.

Im Gegensatz zu anderen Lösungen stoppt Websense auch den Datentransfer von Bot-Controllern, Spyware bzw. Keylogger an den Host Server im Internet.

Unternehmen haben so die Option, Ihr Sicherheits-konzept nahtlos auf alle Endpoints auszudehnen, und können so mobile Anwender unterwegs bzw. an Remote-Standorten genauso gut zu schützen, als ob Sie im eigenen Netzwerk sind.



### WebSense Web Protection Services

Neben den oben genannten Schutzfunktionen bieten die Web Security Suites von Websense die am Markt einzigartigen Web Protection Services, um unternehmenseigene Webseiten, Marken und Webserver besser vor Missbrauch zu schützen.

Mit den nur bei Websense erhältlichen Web Protection Services steht allen Kunden die einzigartige Fachkompetenz der Websense Security Labs™ zur Verfügung, wenn es um Sicherheitsfragen und Verwundbarkeiten bezüglich Websites, Markenmissbrauch und Webservern geht.

#### SiteWatcher™

SiteWatcher benachrichtigt Kunden bei einer Infektion der unternehmenseigenen Webseiten mit Web-Viren oder Würmern. SiteWatcher stellt sicher, dass die IT Abteilung umgehend Maßnahmen ergreifen kann, um die Verbreitung dieser Risiken beim Besuch der Website durch Kunden, Interessenten und Partner zu verhindern.

#### BrandWatcher™

BrandWatcher benachrichtigt Websense-Kunden, deren Websites oder Markennamen Ziel eines Angriffs per Phishing oder Keylogging sind. Nutzer des BrandWatcher-Services erhalten Informationen, über Ablauf und Inhalt des Angriffs und können so die eigenen Kunden rechtzeitig warnen.

#### ThreatWatcher™

ThreatWatcher analysiert den Webserver der Websense-Kunden auf Sicherheitslücken, die üblicherweise von Hackern ausgenutzt werden. Eine regelmäßige Untersuchung auf Sicherheitslücken und Gefahrenpotentiale sowie Berichte zur Risikoeinschätzung mit empfohlenen Abhilfemaßnahmen stehen über mywebsense.com bereit. Mit ThreatWatcher können mögliche Angriffsziele unternehmenseigener Webserver erstmals aktiv ausgeschlossen werden.

### WebSense Real-Time Security Updates™

Die Real-Time Security Updates von Websense bieten Unternehmen unmittelbaren Schutz vor neuen Sicherheitsrisiken bei der Internetnutzung. Bei der Entdeckung neuer Sicherheitsrisiken im Internet sind Kunden durch Real-Time Security Updates unverzüglich vor internet- und anwendungsbezogenen Gefahren geschützt.

Die Vorteile der Real-Time Security Updates:

- Unmittelbare Sicherheit auf Website-Ebene: Sobald Websense die Infektion einer als vertrauenswürdig eingestufte Website mit Malicious Mobile Code oder anderen Gefahren entdeckt, wird die Datenbank beim Kunden automatisch innerhalb weniger Minuten durch Real-Time Security Updates aktualisiert und der Zugriff auf die betroffene Seite gesperrt.
- Unmittelbarer Schutz auf Anwendungsebene: Bei der Entdeckung neuer Trojaner, Würmer oder anderer gefährlicher Programme wird die lokale Datenbank per Real-Time Security Update aktualisiert, so dass alle angeschlossenen Kundenunternehmen umgehend die Ausführung des schädlichen Programms auf Desktop-PCs und Notebooks sperren kann.
- Automatische Sicherheitsupdates: Die Websense Datenbank wird automatisch aktualisiert. Der Systemadministrator muss nicht manuell eingreifen bzw. muss keinen Patch installieren.
- Einfache Implementierung: Nach dem Kauf genügt die einmalige Auswahl des Dienstes durch den Systemadministrator, alle Echtzeit-Updates erfolgen automatisch.

## Zusammenfassung

Noch zu wenige IT-Abteilungen in Unternehmen haben geeignete Mittel und Wege, um PCs nach Infizierungen mit Bot-Software zu untersuchen. Da sich Bot-Netze aber als wirkungsvolles "Geschäftsmodell" innerhalb der Internetkriminalität bewährt haben, ist von einer weiteren Zunahme auszugehen. So könnte eine Gruppe von Hackern die Kontrolle über die Computer eines Unternehmens erlangen, ohne dass die Betroffenen überhaupt davon wissen.

Mit den Web Security Suites von Websense stehen Unternehmen effektive Software-Lösungen zur Verfügung, die zuverlässigen Schutz vor bekannten und neuen Gefahren im Internet bieten. Eine umfassende Security-Analyse von Netzwerken und PCs auf Bot-Netze und andere Crimeware-Risiken kann jederzeit durch einen unverbindlichen Test der Websense Vollversion (auf 30 Tage begrenzt) durchgeführt werden: [www.websense.com/downloads](http://www.websense.com/downloads)

## Websense Firmenprofil

Websense ist der weltweit führende Anbieter von Web Security-Software mit über zehn Jahren Erfahrung. Weltweit mehr als 24.000 Kunden mit rund 24 Mio. Lizenzen in allen Unternehmensbereichen vertrauen auf die Security-Produkte von Websense. Die technologische Weiterentwicklung des Internets begleitet Websense mit intelligenter Analyse, ausgereiften Tools zu Kategorisierung von Risiken und den Security-Updates in Echtzeit. Kunden bevorzugen Websense aufgrund der Produkt-Qualität, messbarer ROIs und der nahtlosen Integration in bestehende IT-Systeme – heute und in Zukunft.

### Quellenangaben:

Dieses White Paper basiert auf Recherchen und Informationen aus den Websense Security Labs und anderen Quellen. Wir bedanken uns für die Bereitstellung der Informationen bei allen Beteiligten.

Websense, Inc  
Hauptsitz  
10240 Sorrento Valley Road  
San Diego, California 92121  
USA

Tel: +1 800 723 1166  
Fax: +1 858 458 2950

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

Websense Deutschland GmbH  
(Deutschland, Österreich, Schweiz)  
Kaiser-Wilhelm-Ring 27-29  
50672 Köln  
Germany

Tel: +49 221 5694 460  
Fax: +49 221 5694 354

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



Download der kostenlosen 30 Tage Testversion unter [www.websense.de](http://www.websense.de)

© 2006, Websense. Alle Rechte vorbehalten. Websense und Websense Enterprise sind in Warenzeichen oder eingetragene Warenzeichen von Websense, Inc. Websense ist geschützt durch US-Patent Nr. 6,606,659 und weltweit durch weitere Patente. Alle sonstigen Warenzeichen sind Eigentum ihrer entsprechenden Firmen. 12.10.2006