

ZONE ALARM



Release 1.0.1

Introduzione

Febbraio 2000. Una serie di attacchi informatici ai danni di servizi in rete molto conosciuti (motori di ricerca, siti web pubblici e privati, siti istituzionali e governativi di diversi Paesi) ha attirato l'interesse della stampa e di parte dell'opinione pubblica sui rischi legati alla navigazione su Internet.

Ci sono individui che, nascosti nell'ombra della Rete e con un monitor davanti, sembrano avere un interesse particolare per le informazioni conservate nelle banche dati di certi siti web, magari più specificamente per i codici delle carte di credito... altri preferiscono divertirsi ad ostacolare il traffico in entrata o uscita dei motori di ricerca, qualcuno si limita a modificare i testi dei discorsi ufficiali di questo o quel politico, per non parlare delle periodiche intrusioni nei sistemi dell'agenzia governativa di turno.

Puntualmente, i mezzi di informazione tradizionali citano il celebre Wargames e si lasciano andare a commenti apocalittici; lasciamo però i media alle loro chiacchiere e occupiamoci piuttosto di come e in che misura questo tipo di rischi della navigazione in rete possono riguardarci da vicino.

Porte

Tutti i dati in entrata e uscita dal nostro computer quando siamo collegati a Internet, passano attraverso una serie di porte. I diversi servizi di rete hanno a disposizione 65536 indirizzi di porta per funzionare, 1024 dei quali comunemente usati e documentati nel dettaglio (ad esempio: 21 ftp, 23 telnet, 25 smtp, 43 whois, 80 http, 109 pop, 110 pop3, 119 nntp).

Può sembrare una banalità, ma dalle stesse porte che lasciano entrare e uscire dati legittimi e necessari per la navigazione, il download di programmi o la lettura della posta, possono avere accesso al nostro sistema, in determinate condizioni, anche comunicazioni poco amichevoli. In questi casi ci troveremo alle prese con un "attacco", un tentativo non autorizzato di accedere alle risorse del nostro computer attraverso le sue porte di comunicazione oppure la trasmissione di particolari pacchetti di dati (nuke) in grado di mandare in crash il sistema.

I possibili attacchi vanno dal semplice e relativamente innocuo rilevamento di quali e quante porte aperte ci sono nel nostro sistema (scansione), a scherzi di pessimo gusto come aprire lo sportellino del lettore CD a distanza, fino alla vera e propria intrusione per danneggiare i dati, sottrarre informazioni, o semplicemente costringere la vittima a spegnere un sistema temporaneamente bloccato e inutilizzabile.

Orifizio a tergo..

Per assicurarsi che nessuno cerchi di giocare brutti scherzi durante la connessione, molti installano sul proprio sistema qualcuno dei più diffusi software di monitoraggio, per esempio CheckBo, che si occupa di tenere sotto controllo una serie di porte di comunicazione tipicamente usate da NetBus e Back Orifice (programmi potenzialmente pericolosi noti con la definizione di trojans).

Back Orifice è perfettamente legale, può essere facilmente scaricato dalla Rete ed è proposto come un interessante tool per accedere a distanza alle risorse di un altro sistema. L'uso che si può fare di questa possibilità, ovviamente, è immaginabile. BO è costituito da client e server, e quest'ultimo dovrà essere installato sul PC da controllare a distanza perché tutto possa funzionare. NetBus si basa sullo stesso principio e ha funzionalità simili, fra le quali è compresa anche la famigerata possibilità di aprire a distanza lo sportellino del CD sul computer remoto.

Non si insisterà mai abbastanza sulla necessità di installare un ottimo antivirus, aggiornarlo spesso e di tenere la protezione in background costantemente attiva tutte le volte che si naviga in rete o si installa qualcosa di nuovo. Tutti gli antivirus più noti sono in grado di rilevare le tracce di BO e NetBus e di rimuoverli dal sistema. Naturalmente questi due sono solo un esempio: la Rete è il luogo ideale per i furboni pieni di fantasia che passano il tempo a progettare scherzi degni di essere provati... sul primo PC indifeso che capita.

Monitoriamo?

Pochi si rendono conto che installare CheckBo può solo dare l'illusione di essere protetti. Purtroppo, si tratta di software di monitoraggio molto limitati, che non offrono in realtà alcuna protezione. Il manuale di CheckBo del resto è assolutamente chiaro: "Il mio scopo principale non è proteggere, ma rintracciare chi ci prova". Una delle caratteristiche di questa utility, infatti, è proprio la capacità di risalire all'identità dell'aggressore. Vedremo fra poco fino a che punto si tratti di un'indicazione affidabile.

Quanti continuano a usare CheckBo sostengono che l'utilità del programma sta nell'essere avvisati degli attacchi e nel sapere da chi provengono. La prima funzione è utile, ma insufficiente: sarebbe come sapere che un assassino sta sfondando la vostra porta di casa, e limitarsi a saperlo. La seconda funzione ha un'utilità discutibile, perché nella maggior parte dei casi scoprirete che il presunto attacco proveniva da un poveraccio che non ne sapeva niente o addirittura dall'indirizzo di un noto provider (magari proprio il vostro!).

E' appena il caso di sottolineare che il lamer (=pirata, nella sua accezione negativa) di turno, se dotato di un minimo di esperienza, sarà tranquillamente in grado di sfuggire all'identificazione, facendovi credere che l'attacco è partito dal PC personale di sua santità il Papa... ;-)

Un Muro di Fuoco!

L'unica difesa reale nei confronti di attacchi provenienti dalla Rete è un Firewall. Si tratta di software progettato per funzionare da filtro fra il sistema e l'esterno, controllando tutti i pacchetti di dati in entrata e uscita, monitorando le applicazioni che tentano di accedere alla connessione per trasmettere o ricevere informazioni, nascondendo infine tutte le porte non strettamente necessarie ai servizi di rete attivati in un determinato momento. Un firewall non si limita ad informarvi che c'è un tentativo di intrusione più o meno grave in corso, ma blocca immediatamente la ricezione di pacchetti dati pericolosi, vi fornisce tutte le indicazioni necessarie per identificare l'IP di partenza dell'attacco, protegge le vostre informazioni e l'integrità del sistema. Una sicurezza ben diversa rispetto ad un semplice software di monitoraggio.

Alcuni dei più noti firewall disponibili per l'utenza casalinga sono ConSeal Pc Firewall, BlackIce Defender, Zone Alarm e Norton Personal Firewall.

Quale Programma?

Di questi, quello che mi sento di suggerirvi per efficacia, semplicità e per il costo zero è *Zone Alarm*, che potrete scaricare liberamente dalla sua home page www.zonelabs.com.

Io suggerisco *Zone Alarm* anche per un secondo motivo: è l'unico prodotto gratuito per un uso casalingo.. potrà sembrare banale ma vi invito ad una riflessione: se il Firewall controlla tutti i dati in ingresso/uscita dal vostro Computer, chi controlla il Firewall? Nessuno!

Morale: utilizzando un software gratuito non incorriamo in alcun rischio da trasmissione non autorizzata di licenze fasulle, poiché per usare *Zone Alarm* una licenza fortunatamente non serve!




Zone Alarm propone un pannello di comando attraverso il quale è possibile gestire diversi livelli di sicurezza, autorizzare le applicazioni che potranno accedere alla connessione per trasmettere e ricevere informazioni, monitorare il traffico dati durante la navigazione. Può essere configurato con estrema semplicità ed è possibile impostarlo per lavorare in assoluto silenzio nella modalità automatica, proteggendo il sistema senza minimamente disturbare l'utente.

Start Up!

In figura possiamo visualizzare l'interfaccia di controllo di *Zone Alarm*



Al primo avvio di *Zone Alarm*, vi verrà mostrato una finestra di pop-up dove vi verranno spiegate alcune caratteristiche base del programma, le più importanti delle quali possono così riassumersi:

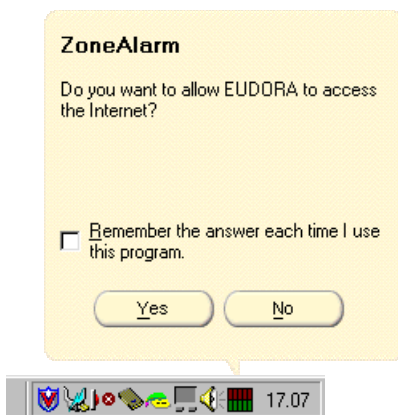
1. *Zone Alarm*, si avvia nel systray, cioè aggiunge la seguente icona:  nella zona in basso a destra vicino all'orologio. La barra rossa proporzionalmente ai pacchetti di dati che escono dal Computer, mentre la barra verde quelli entranti.
2. Per aprire l'interfaccia di *Zone Alarm* è sufficiente doppiocliccare sull'icona in questione.
3. Chiudendo l'interfaccia tramite il pulsante standard di chiusura (la X in alto a destra) non chiudiamo effettivamente il programma (per farlo bisogna selezionare la voce "EXIT" dal menù contestuale che compare cliccando col tasto destro del mouse sull'icona di *Zone Alarm* nel systray) ma solo l'interfaccia.
4. Premendo sui pulsanti **ALERTS**, **SECURITY**, **LOCK**, ecc.. si apre una sottofinestra dove possiamo configurare alcune caratteristiche specifiche di *Zone Alarm*. Anche se la configurazione di *Default* è già buona, consiglio al più di verificare che le impostazioni siano come mostro nei paragrafi successivi.
5. Cliccando sul pulsante a fungo **STOP**, blocchiamo istantaneamente **TUTTE** le comunicazioni entranti/uscenti dal nostro Computer, e lo stato passa da Unlocked a Locked.. finché non sblocciamo la situazione, ogni forma di collegamento, ingresso e uscita, è impossibilitata.

Chi esce...

Zone Alarm è così semplice da usare che anche un bambino potrebbe usarlo..

Una volta avviatosi nel systray, non disturba più e OGNI VOLTA che un programma cerca di accedere ad Internet, lui mostra un balloon dove scrive "il programma XYZ vuole accedere ad Internet, cosa vuoi che gli faccia fare? A) Lo lascio andare B) Lo lascio andare e d'ora in avanti lascerò che questo programma esca sempre senza più interromperti C) Lo blocco sul nascere!".

Quello che ho parafrasato, è più facilmente comprensibile osservando il balloon in questione, nell'esempio sottostante:



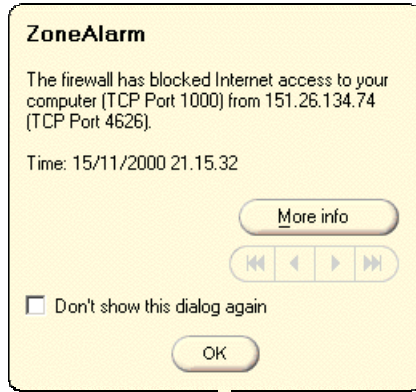
L'esempio di figura mostra quando ho lanciato la prima volta **Eudora** (il mio programma di posta elettronica, altro che Outlook!).

Subito *Zone Alarm* ha bloccato il suo tentativo di scaricare la posta e mi ha avvisato che **Eudora** stava cercando di accedere ad Internet.

- Cliccando su **YES** lo lascio uscire.
- Cliccando su **NO** lo blocco
- Cliccando su **YES**, dopo aver abilitato il CheckBox "**Remember the answer each time I use the program**", l'avrei fatto uscire sempre da oggi in avanti senza che più *Zone Alarm* mi interrompesse.

...chi entra...

Per quanto riguarda i tentativi di ingresso, *Zone Alarm* è particolarmente discreto: lui continua a starsene nel suo angolino monitorando senza disturbare i nostri programmi che vogliono uscire, quando qualcuno cerca di entrare, lui semplicemente lo blocca all'ingresso e ce ne da notizia tramite un balloon, dove riporta l'indirizzo IP del Computer da cui è partito l'attacco.



L'esempio di figura mostra il balloon d'attacco da parte dell'indirizzo IP 151.26.134.74

E' importante sottolineare che non sempre i tentativi di attacco sono maligni, spesso si tratta di automatismi dei siti Web che visitiamo allo scopo di reperire informazioni sul computer di chi li sta visitando... in ogni caso lo ritengo una forte violazione della mia privacy quindi adoro l'inflessibile operato del mio firewall preferito!

Cliccando su "**More Info**", *Zone Alarm* si collega al proprio sito Web dove visualizzerà una pagina che spiega (a grandi linee) che tipo di attacco è stato, la sua pericolosità, e altre informazioni interessanti ma pur sempre corollarie.



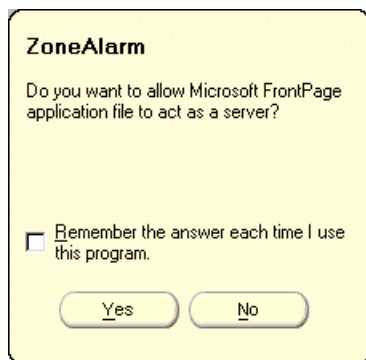
E' possibile disattivare l'apparire di questi balloon d'attacco (anche perché hanno al più una valenza informativa) però lo sconsiglio, perché non danno fastidio (basta cliccare su **OK** per chiuderlo) e ci permettono di capire quali sono i siti più "invadenti".

...e chi fa entrare!

Vi sono alcuni programmi che si comportano da "**SERVER**", come *ICQ*, *Frontpage*, *Napster*, ecc... .

Questi software girano sul nostro Computer e quindi ci chiederanno di uscire su Internet (come ho già mostrato nei paragrafi precedenti), tuttavia hanno anche bisogno di ricevere connessioni dall'esterno, quindi vogliono sia uscire che fare entrare: quando *Zone Alarm* si accorge di questo ci interrogherà con un ulteriore balloon dove ci informa che il programma ha la "pretesa" di comportarsi da **Server**.

Sta a noi concedere o meno questo permesso, tenendo conto che se lo neghiamo, questi programmi saranno impossibilitati a funzionare come devono.



L'esempio di figura mostra quando ho richiesto a *Frontpage* di pubblicare sul Web il sito che avevo appena aggiornato.

Subito *Zone Alarm* ha ibernato *Frontpage* e mi ha chiesto come doveva comportarsi.

Anche in questo caso valgono le considerazioni già descritte in precedenza sulla ripetibilità o meno di queste richieste.



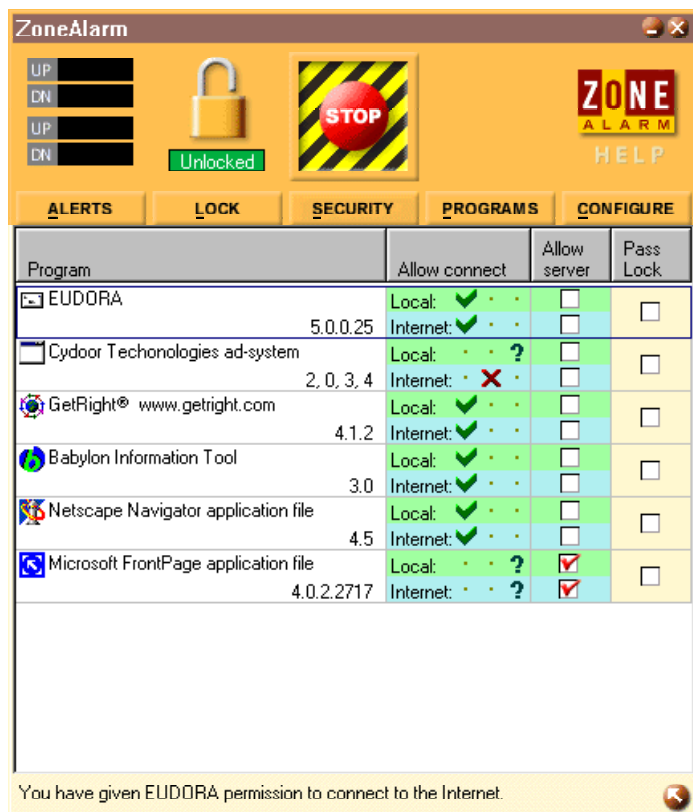
Internet o Intranet?

Tutto quello che avete appena visto, *Zone Alarm* è capace di farlo non solo su Internet, ma anche all'interno di una rete locale (ad esempio per bloccare l'ingresso sul proprio computer da parte di un simpatico collega dell'Ufficio che ama curiosare tra i nostri file).

Non ho avuto modo di sfruttare questa potenzialità, ma i modi per farlo sono identici a quanto mostro relativamente alle applicazioni Internet.

Quindi?

Avviando l'interfaccia di *Zone Alarm*, è possibile cliccare sul pulsante **PROGRAMS** per aprire la sottofinestra che riporta l'elenco di tutti i programmi che hanno richiesto il permesso di uscita, e cosa abbiamo deciso.



In figura vediamo come al momento in cui ho aperto la sottocartella **PROGRAMS**, gli unici programmi che avevano richiesto di uscire erano *Netscape, Eudora, Babylon Frontpage e Getright*. Chiaramente nel tempo questa lista aumenterà, tanto più quanto più installiamo software che gravitano attorno alla rete.

E' interessante analizzare il significato delle colonne a destra dei nomi di programma.

Per ogni programma vi sono tre colonne:

Allow Connect: il segno di spunta verde significa che abbiamo concesso a quel dato programma di uscire e abbiamo anche detto che può farlo sempre, senza più interromperci; la croce rossa significa che NON abbiamo dato il permesso e abbiamo detto di non chiederlo neanche; il punto interrogativo blu significa che non abbiamo ancora preso una decisione e tutte le volte che il programma chiede di uscire, apparirà il balloon con la richiesta.

Allow Server significa che abbiamo o meno dato il permesso al programma di comportarsi da SERVER.

Pass Lock significa che per poter uscire/entrare, il programma in questione ci chiede una password che decideremo la prima volta che abilitiamo questa funzione.

Per ogni programma vi sono anche due righe: **Local** e **Internet**; la prima riporta le scelte riguardanti il comportamento di *Zone Alarm* verso la rete locale, la seconda verso Internet.

Concludendo

Ora che sono giunto alla conclusione di questo manuale introduttivo a *Zone Alarm*, mi chiedo: perché l'ho scritto? Probabilmente nella speranza che chiunque abbia la necessità (o bontà) di leggerlo possa:

A) navigare con sicurezza senza che i più elementari diritti della privacy siano costantemente violati! ..con *Zone Alarm* vi renderete conto di quanti programmi accedono ad Internet senza che voi lo sappiate.. e finalmente avrete il potere per bloccare questa involontaria e non richiesta fuga di dati personali!

B) ringraziarmi per il lavoro svolto e soprattutto la mole di tempo perso a riguardo!

Se volete scrivermi, un mio indirizzo e-mail è: io@stordito.it, accetto tutto tranne le critiche! ;-)

Paolo ® 2000