PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 452 di giovedì 29 novembre 2001

Virus BadTrans: gravi rischi per la privacy

Un virus "spione". Come accorgersi dell'infezione? Come rimuovere eventualmente il virus? PuntoSicuro l'ha chiesto ad un esperto di sicurezza informatica.

Non sembra arrestarsi la diffusione del virus "Badtrans" che da alcuni giorni imperversa nelle caselle di posta elettronica di molti utenti.
"Badtrans", del quale abbiamo parlato nei numeri 450 e 451 del nostro quotidiano, non e' distruttivo, ma potrebbe costituire un pericolo per la privacy degli utenti.

PuntoSicuro ha interpellato al riguardo Fabrizio Cassoni, esperto di sicurezza informatica della Symbolic, al quale abbiamo posto cinque quesiti.

Qual e' attualmente il grado di diffusione di BadTrans?

E' un po' presto per avere delle cifre certe: tutti i vendor lo classificano come "ad alta diffusione" ma ovviamente si tratta di stime basate su osservazioni empiriche.
Ad esempio, da ieri verso i nostri server in media arriva almeno una mail infetta ogni 20 minuti. Talora le mail arrivano a gruppi, quando una mailing list viene raggiunta dal worm e più partecipanti eseguono l'allegato.
Un fattore mitigante è costituito dal fatto che Badtrans.B non si spedisce più di una volta allo stesso indirizzo; ma come dicevo, un indirizzo potrebbe corrispondere a una mailing list, aumentando perciò la potenziale diffusione.
Considerato che Badtrans.B individua gli indirizzi secondo due modalità diverse, ha ampie possibilità di diffusione; ricavando gli indirizzi dalla casella della Posta in Entrata sfrutta un effetto "domino" (più posta arriva, più address vengono "acquisiti" dal worm). Il worm va inoltre a cercare gli indirizzi nei file .HT.* e .ASP sul disco della macchina infetta, e questo sicuramente aggiunge ulteriori potenzialità.

Quali sono i pericoli per l'utente in caso di infezione?

Badtrans.B non è intenzionalmente distruttivo e si limita a rispedirsi. Per le aziende, cosituisce un rischio di immagine e, in caso di diffusione massiccia su una rete, potrebbe portare a un degrado di prestazioni del server di posta.
Però, dal momento che il worm installa anche un trojan nella macchina infetta, è in grado di ricavare informazioni riservate sulla configurazione del PC e sulle password dell'utente e di spedirle a un indirizzo esterno.
Questo chiaramente compromette la sicurezza e la riservatezza delle informazioni dell'utente.

Come appurare se un PC e' stato infettato da BadTrans?

Se non si utilizza un antivirus e se non si controllano i log del proprio server di posta, non è facile accorgersi della presenza di Badtrans.B, visto che i nomi di alcuni dei file che utilizza sono variabili.
Due sono segni rivelatori della attivazione del worm sono la presenza del file 'kernel32.exe' nella directory di sistema di Windows e il suo riferimento nella chiave di registro:
[HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRunOnce] "Kernel32" =
il valore corrisponde al percorso e al nome del file kernel32.exe.
[n.d.r. Attenzione stiamo parlano del file Kernel32.exe e non del file Kernel32.dll che e' invece legittimo]

In caso di infezione quali accorgimenti deve adottare un utente inesperto?
Quali indicazioni devono seguire utenti esperti per rimuovere BadTrans?

La procedura è la stessa in entrambi i casi.
Prima di tutto è necessario installare la patch di Microsoft che elimina la vulnerabilità IFRAME sfruttata da Badtrans (e altri worm simili) per autoeseguirsi:
patch.
Poi bisogna eliminare, se è ancora presente, il valore Kernel32 dalla chiave di registro sopra citata.
Dopo il riavvio del sistema, si può usare un antivirus per rilevare i file infetti; questi andranno cancellati. In alcuni sistemi operativi, potrebbe essere necessario riavviare la macchina in DOS per cancellare completamente i file; oppure sarà necessario rinominare i file (o lasciare che lo faccia
il proprio antivirus) e dopo un ulteriore riavvio, eliminarli. Questo dipende da quale sistema operativo si utilizza e se i file sono in uso. Cancellare inoltre i messaggi di email che contengono l'allegato infetto (che è tipicamente un file con un nome casuale e una doppia estensione).

Purtroppo non si tratta di operazioni banali, specialmente per gli utenti inesperti; è fondamentale consultare le informazioni rilasciate dal vendor del proprio antivirus di fiducia per seguire esattamente la procedura consigliata in base al prodotto che si sta usando e al sistema operativo.
Consigliamo inoltre di utilizzare prodotti di provenienza certa, per effettuare la disinfezione: già in passato abbiamo assistito alla diffusione di tool "anonimi" che venivano propagandati come utility per rimuovere certi virus o worm, e che si rivelavano essere a loro volta veicoli di infezione messi in circolazione con intento malevolo per sfruttare il momento di panico degli utenti.

Altri consigli utili...

Questo incidente evidenzia ancora una volta la necessità di applicare le patch fornite dai produttori dei programmi che si utilizzano per leggere la posta o navigare in Internet; Badtrans sfrutta una vulnerabilità nota da mesi per autoeseguirsi nel momento stesso in cui si legge il messaggio infetto su alcuni client di posta: se le patch correttive fossero state installate su più sistemi, certamente non assisteremmo a una diffusione così massiccia. In ogni caso, qualunque sistema operativo o software si scelga di utilizzare, è fondamentale verificare periodicamente di essere allineati con le ultime versioni stabili e sicure.

---

www.puntosicuro.it