PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 456 di mercoledì 05 dicembre 2001

Attenti al falso screen saver!

Si diffonde via e-mail un nuovo worm capace di bloccare il sistema colpito.

E' stata rilevata nella giornata di ieri la diffusione di un nuovo e temibile worm: Goner (ALIAS W32/Gone.A@mm, I-Worm.Goner).

La notizia giunge dalla Symbolic, azienda attiva nel campo della sicurezza informatica.
Il worm Goner si propaga usando Outlook e ICQ, se installati sulla macchina infetta; inoltre rilascia alcuni script nella directory del client MIRC (programma per chat). Questi codici hanno lo scopo di saturare alcuni canali IRC (usati per le chat).

Quando viene eseguito, il worm mostra una finestra di dialogo con alcune animazioni, per dissimulare la propria presenza. Viene poi visualizzato un finto messaggio di errore: "Error While Analyze DirectX!".

Nel frattempo il worm si copia con il nome GONE.SCR nella cartella di sistema di Windows e cerca di creare una chiave di avvio nel Registro.
Goner gira in memoria e non e' facilmente individuabile con i normali controlli.

La diffusione del virus puo' avvenire con e-mail e tramite chat.
Infatti se Outlook è installato sul sistema, Goner ricava gli indirizzi di posta contenuti nella rubrica e invia loro un messaggio formato nel modo seguente.
Soggetto: Hi
Messaggio: How are you ?
When I saw this screen saver, I immediately thought about you
I am in a harry, I promise you will love it!
Allegato: Gone.scr

Goner cerca anche di spedirsi tramite ICQ, usando un componente standard per inviare il proprio file. Il worm invia una richiesta di trasferimento di file a un contatto o a un altro utente infetto che si trovi on-line: se il destinatario approva il trasferimento, il worm gli invia il proprio file.

Il worm ricerca e blocca i seguenti processi:
APLICA32.EXE, ZONEALARM.EXE, ESAFE.EXE, CFIADMIN.EXE, CFIAUDIT.EXE, CFINET32.EXE, PCFWallIcon.EXE, FRW.EXE, VSHWIN32.EXE, VSECOMR.EXE, WEBSCANX.EXE, AVCONSOL.EXE, VSSTAT.EXE, PW32.EXE, VW32.EXE, VP32.EXE, VPCC.EXE, VPM.EXE, AVP32.EXE, AVPCC.EXE, AVPM.EXE, AVP.EXE, LOCKDOWN2000.EXE, ICLOAD95.EXE, ICMON.EXE, ICSUPP95.EXE, ICLOADNT.EXE, ICSUPPNT.EXE, TDS2-98.EXE, TDS2-NT.EXE, FEWEB.EXE.

Goner cerca inoltre di cancellare questi file; se la cancellazione fallisce, crea WININIT.INI che rimuovera' quei file al successivo riavvio del sistema.
Il worm rimuove poi il proprio file dalla cartella in cui era stato originariamente attivato. In questo modo, l'unica copia esistente sara' nella cartella di sistema di Windows.

Una raccomandazione sempre attuale: tenete aggiornato l'antivirus, nel caso riceviate il file Gone.scr, o altri file "sospetti" non apriteli in nessun caso.