Virus nVIR

Autor:
Data de publicació: 26-06-2021

Família de virus nVIR

Nom comú
nVIR

Nom tècnic
Virus Mac OS/nVIR

Àlies
Sida, Merda, Hpat, Jude, nVIR, MEV#, MODM, nCAM, nFLU, kOOL, MERDA, prod, PISS

Família
nVIR, tres soques predominants: nVIR-A, nVIR-B, nVIR-C

classificació
virus

tipus
Macintosh

Subtipus
Sol·licitud d'infecció. Molèsties; perxa del sistema.

Aïllament
1987 (nVIR-A i nVIR-B), 1991 (nVIR-C)

Punt d'aïllament
desconegut

Punt d'origen
desconegut

Autor(s)
desconegut

nVIR és un virus informàtic obsolet que es pot replicar en ordinadors Macintosh que executen qualsevol versió del sistema de 4.1 a OS 8. El codi font de la nVIR original s'ha posat àmpliament a disposició, per la qual cosa han sorgit nombroses variants. Cada variant causa símptomes una mica diferents, com ara: bloquejos d'aplicació, errors d'impressió en impressores làser, temps de resposta lent del sistema o bloquejos imprevisibles del sistema. nVIR s'estén a través de qualsevol programa infectat per nVIR, però a causa del llarg període de temps nVIR es troba bàsicament inactiu en un sistema hoste, nVIR generalment troba el seu camí en les còpies de seguretat del sistema i no es detecta fins que apareixen els primers símptomes overt. Per exemple, si s'elimina i s'insereix un disc utilitzat en un Macintosh infectat en un segon Macintosh, l'altra màquina s'infectarà si s'executa qualsevol aplicació d'aquest disc a la segona màquina. A més, qualsevol mètode utilitzat per transferir programes entre Macintoshes difondrà nVIR, inclosa la transferència de fitxers a una xarxa. No obstant això, nVIR no es pot difondre a través del maquinari d'una xarxa d'impressió.

nVIR porta un recurs de codi addicional, CODE 256 (encara que algunes variants porten codi 255), i apedaça la taula de salts per apuntar-hi. El punt d'entrada de l'aplicació original es desa en el recurs nVIR 2. nVIR introdueix al fitxer Sistema el recurs INIT 32 que s'executa en iniciar, moment en què nVIR apedaça la trampa teInit. Qualsevol aplicació que truqui posteriorment a aquesta trampa s'infectarà. El recurs nVIR 3 (o nVIR 5) és una còpia de l'INIT 32. Un recurs nVIR 10 al fitxer del sistema evitarà la infecció de nVIR. Si una aplicació crida OpenResFile abans de TEInit, aquesta aplicació es veurà danyada.

El recurs nVIR 0 conté un comptador que està establert a 1000 en la primera infecció del sistema. Cada reinici decreix el comptador per 1. Cada llançament d'aplicacions el decreixo per 2. Quan el comptador arriba a 0, nVIR emetrà un so d'1 de cada 8 reinicis i 1 de cada 4 llançaments d'aplicacions infectats. Si MacinTalk està instal·lat a la carpeta Sistema de la màquina, la màquina pot dir ocasionalment "No t'espantis". En cas contrari, pot piular inesperadament.

NVIR ha sabut 'hibridar' amb diferents variants de nVIR en una mateixa màquina.

Enllaços externs

Una vacuna per al virus 'nVIR',per Mike Scanlin, MacTech
Virus Mac OS/nVIR, per McAfee
nVIR A, per Virus-Test-Center, Universitat d'Hamburg
nVIR B, per Virus-Test-Center, Universitat d'Hamburg
nVIR C, per Virus-Test-Center, Universitat d'Hamburg
nVIR B contramesures, UC Berkeley