NAME

infect − Give a virus to another UNIX system

SYNOPSIS

infect [−v] [−clev] [−slev] [−a] [−wdev] [−idays] tn

DESCRIPTION

Infect uses the cu(1C) command to dial the UNIX system with telephone number *tn*, and infects that system with a virus program. The arguments allow you to specify the type of virus. You can give anything from a mild cold, which will only cause occasional sneezes and sniffles, to a virulent plague that will kill the system immediately. If *tn* is −, *infect* gives the virus to its own UNIX system.

Once a UNIX system has been infected with a virus, the only proven way of curing that system is to vaccinate it (see −v). There have been cases of spontaneous remission, but such things are very rare. Attempts to *flog*(1) an infected system will be counter-productive.

Unfortunately, VAX 11/780 based UNIX systems seem to be naturally immune to all viruses that *infect* can produce. It seems that such systems are self-VAXcinated.

−v Causes *infect* to create a vaccine to combat a virus with the indicated characteristics, and to vaccinate the UNIX system. Only certain users may do vaccinations, and those users must pay the author (and how!). Warning: The distinction between virus and vaccine is marginal at best. Vaccinating a UNIX system that doesn't have the virus may do more harm than good (the dreaded Swine Flu Syndrome). Even if the UNIX system does have the virus, the vaccine might still make things worse −− and heaven help you if the vaccine mutates.

−c Level of contageousness: this specifies how likely it will be for the infected system to pass the virus onto another UNIX system. (Vaccines are never contagious.) Recognized levels include:

- **n** Not contagious (default); the virus cannot spread to other systems.
- **l** Low: the virus can only spread to other systems that share memory or disks with the infected system.
- **m** Mild: the virus can spread through DA links, PCL links, or CE's (CE's act as common carriers).
- **h** High: the virus can spread through tapes.
- **v** Virulent: the infected UNIX calls other UNIX systems, via *cu*(1C) or *uucp*(1C), and infects them.
- **x** Carrier: highly contagious, execpt that the infected UNIX system doesn't suffer from the virus itself, but just passes it on to other systems.

−i The incubation period, in days. The system will not suffer from the affects of the virus until the incubation period is over. If 0, the virus takes affect immediately. A high incubation period allows the virus to infect the system's backup tapes. The system is contagious during the incubation period.

−s Severity level: mild, severe (the default), or deadly. A mild virus is like a slight cold: the infected system crashes (or loses files, or exhibits other noxious behavior) once or twice a day. If the system was not in perfect health before, the users of the infected system might not realize that it has been given a virus, execpt through statistical analysis. A severe virus causes crashes (or whatever) at least every hour. While a system is obviously very sick, it is usuable (but just barely). A UNIX system with a deadly virus is totally unusable.

−a If specified, the virus will be acute; otherwise, it will be chronic. A chronic virus stays at

the severity level specified by **−s**, and the symptoms come and go irregularly. An acute virus starts at the severity level selected by **−s**, but slowly gets worse until it becomes deadly. For example, a system can suffer from a mild, chronic virus for years before anyone realizes that it has a virus.

−w This specifies what "device" (hardware or software) the virus will attack. Recognized codes are:

kern	the UNIX systems's kernal (can cause it to pop)
file	the file system (can cause lost an/or scrambled files)
cc	C compiler (causes it to crash and/or generate bad code)
doc	documentation tools (can cause athlete's footnote)
cmds	any and all commands on the UNIX system
su	super-user (root-rot −− the kryptonite disease)
unauth	unauthorized users (usually a benevolent virus!!)
cpu	the obvious
mem	memory (perhaps causing parity errors)
disk	disk drives (can cause disk-head dandruff)
back	backplane and/or unibus (e.g. nagging back-ache)
air	air conditioning system (a rare pneumonic virus)
any	any or all of the above (a wide spectrum virus)

CAVEATS

The viruses are stored in a special, sealed RV01 disk pack, mounted on **/dev/andromeda**. If this pack is broken, the viruses will spread like wildfire (the Pandora Syndrome).

DIAGNOSTICS

Many, but they're always wrong.

BUGS (pardon the pun)

For some unknown reason, attempting to infect a system via a dataswitch connection does not work. Dataswitches have a tendency to intercept viruses first and hog them for themselves.

NOTE:

This page was copied from PWB/UNIX release 2.0 (IH) and brought to you for your amusement.