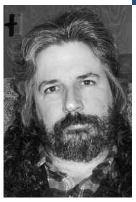
ROBERT G. FERRELL

/dev/random



Robert G. Ferrell is an information security geek who enjoys surfing (the Internet), sashimi (it makes great bait), and long walks (to the coffee machine and back).

rgferrell@gmail.com

THE TIME HAS COME, THE WALRUS said, to address the widespread and wholly erroneous notion that UNIX is immune from malware and therefore needs no vetting for the detection and removal thereof. Although it's true that certain other operating systems (which shall remain nameless but which rhyme with "ten toes") are far more attractive targets for exploitation and therefore receive the lion's share of attention from malware authors, "security through lesser market penetration" is hardly what one might term a robust information protection strategy.

If at this point, dear reader, you're expecting me to take you on a myopic retrospective through the history of UNIX viruses, trojans, and worms (oh my), you've once again failed to reckon with my formidable aversion to doing actual research. Looking at the big picture, I've come to the conclusion that at least part of the reason UNIX hasn't suffered more at the pale fingers of the bad guys is the habit of antivirus companies and the media of labeling newly discovered malware with downright silly names. Lupper, Scalper, and Slapper spring to mind, as do Pooper, Gasser, Ripper, and Stupor. Well, I probably owe those last few examples to a late-evening peanut butter and roasted habanero sandwich rather than any actual virus alert, but you get my drift.

Think about it: Who really wants to spend long hours slaving over a hot keyboard only to have the resultant glittering black pearl of slithery digital evil referred to by some pansy malware-tracking site as the "Foofer" worm? Indignity of indignities. Sure, "Win32/DEL.100907.ZZA" isn't exactly a coolly ominous moniker, either, but at least it gives the impression that someone's taking your work semi-seriously, providing a light at the end of the carpal tunnel, as it were.

Most modern malware contains two broad functional elements: the operational component, which takes care of infection, propagation, sanitization, amortization, and defenestration, and the payload (where the peanuts and nougat are found), also known as the business end. Even though it is the operational code that exhibits the real innovations in areas such as antiviral avoidance, stealth, firewall-dodging, polymorphism, consumer confidence index, and so on, the payload is where the rubber meets the road so far as your hapless data is concerned. Payloads range from whimsical taunting ("You've been pwned!!!!") to the downright vicious (rm -rf *).

Pretty much everyone and their sentient canine has heard of the major classes of malware (i.e., viruses, trojans, spyware, worms, eels, and hagfish); the attack mechanisms of the most famous and widespread are well documented. There are many thousands of lesser pathogens out there, however, the chewy cream centers of which remain shrouded in palate-adhering gooey mystery. As a public service I've prepared a handy pocket reference to a few of these chigger bites in the picnic of computing, crafted with the same careful attention to detail and accuracy as is your local commuter train schedule. Antihistamines and anesthetic available on request from the front desk.

#*$!: Reverses "copy" and "delete" hotkeys; disables "undo."

Bunion: Hobbles snmpwalk.

Compost: Forces every running process to dump core; disables garbage collection; resides entirely in the heap.

Creosote: Downloads and installs bloatware until all disks are full, then crash dumps at the first user command input.

LiteSabr: Publishes any video files it finds on the system to YouTube—all of them.

Lumbago: Causes disks to spin out of control until they slip and rupture.

Nronn: Multiplies all arithmetic operations by 10.

Odie: Reboots whenever a user types "cat."

QRN: Replaces all semaphores with Morse code.

Qu'vatlh: Translates every text file on the system into Klingon.

Reverse Engineer: Plays all your .mp3, .ogg, and .wav files backward, then replaces them with a scratchy recording of "The Wabash Cannonball" (in one particularly virulent variant, on zither).

Roid: Drops the network connection and fills system logs until they push painfully against their partitions.

SafeSeks: Loads itself into the kernel, puts network interface into promiscuous mode, then hits random adult sites; will not unload until it encounters a trojan.

Scooter: Mails /etc/hosts to everyone in $HOME/.addressbook.

Upgr8: Renames /usr/bin/cd to /usr/bin/dvd.

Windozer: Disguises itself as a useful application but halts the system when invoked; at next reboot it blames the user, modifies the interface and application icon slightly, and repeats the process.

Xtinkt: Deletes awk.

ZZZZ: Deletes all rc files and replaces them with `perl -e 'sleep'`.

Don't scratch; it just makes it worse.