Notes on RWatcher, Scores, and nVIR

Experiments done on October 26 and November 3, 1988

John Norstad
Academic Computing and Network Services
Northwestern University
2129 Sheridan Road
Evanston, IL 60208

Bitnet: jln@nuacc
Internet: jln@nuacc.acns.nwu.edu

Introduction

These experiments tested RWatcher against Scores and two different strains of nVIR.

I used the standard System 6.0 and Finder 6.1 files as released by Apple for all the tests, on a pair of Mac SEs equipped with 1 meg and 2.5 megs of RAM and Apple internal 20 megabyte hard drives. The infected systems were on floppy disks. I did not infect my hard drives. I used SoloFinder for the tests, not MultiFinder. I did not use Vaccine in any of these tests. The infected floppy contained only the following files:

```
System Folder:
   System 6.0
   Finder 6.1
   RWatcher 1.0b1
MacWrite 4.6
```

nVIR Characteristics

I have two different strains of nVIR, which I call "nVIR A" and "nVIR B". nVIR A appears to be the one described by Mike Scanlin in the May 1988 MacTutor. nVIR B is the strain described by Alexis Rosen in a posting to comp.sys.mac on September 23, 1988.

Both strains use the same collection of INIT, CODE, and nVIR resources, but the resources have different sizes in the two strains.

An application infected by nVIR contains the following viral resources:

Type	ID	Size (strain A)	Size (strain B)
CODE	256	372	422
nVIR	1	378	428
nVIR	2	8	8
nVIR	3	366	416
nVIR	6	868	66
nVIR	7	1562	2106

The nVIR 2 resource contains the original main jump table entry.

When an infected application is run it infects the system file immediately on launch.

An infected system file contains the following viral resources:

Type	ID	Size (strain A)	Size (strain B)
INIT	32	366	416
nVIR	0	2	2
nVIR	1	378	428
nVIR	4	372	422
nVIR	5	8	8
nVIR	6	868	66
nVIR	7	1562	2106

When the system is infected and an uninfected application is run the application is infected immediately on launch. I used MacWrite 4.6 for my test application.

Behaviour of nVIR with RWatcher

I used RWatcher 1.0b1 in these tests. The RLIS 128 resource listed the 5 Scores viral resources, and specified nVIR resources of any ID or size. The list did **not** contain any entries for INIT 32. I test both strains of nVIR.

In my test I booted a floppy containing a clean system and Finder, RWatcher, and an infected copy of MacWrite. It booted fine. When I launched MacWrite it tried to infect the system, RWatcher caught it, beeped 10 times, and exited to shell. The System file was unchanged (see below).

After goofing around with ResEdit I managed to build a floppy containing a clean system, RWatcher, and infected copies of the Finder and MacWrite. This is an unusual situation that is unlikely to arise in practice - if your Finder is infected then usually your system is going to be infected also. I tried to boot from this strange disk. When the Finder was launched it tried to infect the system, RWatcher caught it, beeped 10 times, and exited to shell. The system tried to relaunch the Finder and the same sequence was repeated over and over, in an infinite loop.

In all my tests the System file remained uninfected - there were no nVIR resources created, and no INIT 32. Evidently nVIR tries to create an nVIR resource before INIT 32, since RWatcher was not configured to catch INIT 32.

To make sure, I used MPW to compare the original System file as released by Apple (in folder jln:old) to the System file after the foiled attempts at infection described above (in folder jln:new).

For some reason the MPW tool ResEqual aborted with an error message saying that it couldn't load a resource about 2/3 of the way through the comparison. Perhaps the files were just too big for ResEqual to handle.

I tried the following commands next:

```
rezdet -l jln:old:system >jln:old:out
rezdet -l jln:new:system >jln:new:out
compare jln:old:out jln:new:out
```

The Compare tool reported that the output files were identical except for the title lines at the top and the summary lines at the bottom. So the files were identical, and RWatcher did indeed prevent any changes.

The "files -l" command also reported that the two copies of the system had the same size and attributes.

Scores Behaviour with RWatcher

I also tested Scores with RWatcher. RWatcher worked fine - when an infected application was launched, RWatcher caught it, beeped 10 times, and exited to shell. The System file was unaltered. The Note Pad and Scrapbook files were unaltered. The Scores and Desktop files were not created.

Conclusions

RWatcher is effective protection against both Scores and nVIR (both strains A and B), provided you have a clean system to start with.

Just to be safe I have added two more entries to the RLIS 128 list to protect against nVIR:

```
  INIT  32  366    (nVIR A)
  INIT  32  416    (nVIR B)
```

Note: I still haven't disassembled nVIR and figured it out like I did with Scores. Maybe some day ... I also don't know exactly how many other variants of nVIR exist besides the two I have.