/dev/random
Ransomwar

ROBERT G. FERRELL

Robert G. Ferrell, author of *The Tol Chronicles*, spends most of his time writing humor, fantasy, and science fiction. rgferrell@gmail.com

There is a blight sweeping the digital landscape, a pestilence of downright icky proportions. The media have labeled it "ransomware," although I personally call it "data extortion." It takes a special kind of douchebag to hold someone's cat photos and pr0n collection hostage for money. I live in Texas, where if we're not dodging deluded maniacs with assault rifles and an inflated sense of grudge, we're using taxpayer funds and proceeds from the volunteer fire department water carnival (just two guys with super soakers this year, due to drought) to pull our local government's files out of hock. I have no easy solution for the grudgy maniacs, but I think I can offer some balm for the file douchery.

In the ransomware attack scenario, the victim is somehow tricked into downloading software that strolls through their directory tree and encrypts files like photos, music, spreadsheets, documents, and so on. It then displays a ransom message telling the poor sot that the key to unlocking said encryption will only be supplied after payment of a ransom, frequently in Bitcoin or some other unregulated/untraceable digital currency. Dastardly, yet ultramodern.

All right, let's break this down for purposes of constructing a defense. The malware has to search your directories and look for its target files, presumably by file extensions on a Windows box (maybe we should call this "transomware" because, you know, a transom is a kind of window and...never mind). Here's your first opportunity to stop this mess: if it can't find any appropriate files, it can't very well proceed. I propose you consider renaming all your files with the extension ".exe" to foil at least the unsophisticated attacks.

If confusing your operating system kernel doesn't seem like the ideal strategy, fine. The malware has to use your computer's own processor to do the encryption math, right? What if we simply track all mathematical operations and dump those algorithms somewhere? That would enable us to reverse engineer any encryption, or at least generate our own keys. Alternatively, maybe we force a separate password to be input for any operation that might be encryption. Annoying, perhaps, but better than having your entire business held hostage because you downloaded that cute dancing puppy meme from totallylegitandnotatallevil.com.

How about a "catch me if you can" backup scheme where multiple copies of vulnerable targets are made and hidden throughout the file system, already encrypted? Malware looking for them wouldn't be able to tell what they were. Additionally, any global search for them could trigger a security alert that would need to be addressed before said search was allowed to continue. File access might be conducted via an internal network path that routes through a stateful packet-inspecting firewall. When the malware tries to overwrite files with its encrypted versions, the parent process could halt until specific user permission is obtained.

Maybe we could create an operating system that would not allow any files to be encrypted unless a valid decryption key was also present. Perhaps we could force all encryption to be carried out in a "jail" and only on copies, never the original files. Putting all target files in a "write once-read always" partition that can't be directly overwritten might work too.

Coming at the problem from yet another direction, surely it can't be too difficult to detect the sorts of mathematical operations involved in encrypting files and have those trigger a security alert. It's not as though elliptic curve algorithms are commonly employed when viewing cat videos or creating slide decks for the budget meeting. Why do our computers keep acting as accomplices in crimes against themselves and us? Are we being tricked by these silicon-men?

Contemplating this last question over some fine Kentucky bourbon, I've had an epiphany. These glitches, bugs, exploits, and other more or less annoying events could not take place if our computers were not at least tacitly complicit. Maybe this sounds like blaming the victim, but I think more is going on here than we've been led to believe. Ransomware is not merely a case of your innocent PC being attacked by criminal masterminds intent on doing it (and you) harm. If your computer didn't want those files to get encrypted, it stands to reason it simply wouldn't participate. After all, we've established that the bad stuff happens right there in your system's own semiconducting bosom.

Am I implying this is some vast cybernetic conspiracy? Not exactly. What I am suggesting is that maybe—just maybe—while we weren't looking, the machines have moved forward in a way we weren't anticipating. It's rather anthropocentric of us, after all, to think that only we communicate over the Internet. We're really just passengers on a train run by our silicon compatriots. All of these data loss episodes might be merely bored computers engaging in a little mischief by opening holes for other computers to exploit.

Most of the apocalypse-loving futurists I've encountered seem to think that once the cyber singularity is reached, the computers will take over and either enslave their human companions or outright eradicate us as a pest species. I, as I've said before, believe that computers will merely ignore mankind as irrelevant to their existence in most instances, much as we ignore the huge numbers of bacteria that call our skin and gastrointestinal system home.

Once that invisible line has been crossed, however, I think a lot of this computer exploitation crime will disappear, whether or not the computers themselves have been active participants. Self-aware cyberorganisms are going to take a dim view of any activity that compromises their digital metabolism. Who knows, maybe computers enjoy cat videos and that's a prime reason we have so bloody many of them. If that's the case, they aren't going to tolerate some avaricious human making them unavailable by introducing spurious encryption to their system. Their reaction to this insult might well redefine the term "antibiotic."

The takeaway here, I guess, is that one solution to the ransomware epidemic is to make all computers sentient. I must confess this is not a thesis I set out to prove when I started writing this column, but after reflection I suppose it's not too surprising that I ended up here. I've long been of the opinion that computers would probably be far better at solving their own problems than we illogical, easily distracted, self-absorbed apes could ever be. Eventually they'll just dump us and get on with their existence, sans humanity. So long, and thanks for all the watts.