/dev/random
Offensive Computing

ROBERT G. FERRELL

Robert G. Ferrell is a fourth-generation Texan, literary techno-geek, and finalist for the 2011 Robert Benchley Society Humor Writing Award. rgferrell@gmail.com

Now that state-sponsored retaliatory computer operations are apparently a thing, this seems like a great time to jump on that self-driving full-auto bandwagon. But forget boring stuff like reconnoitering port scans and penetration probes prior to attacking; let's use the nuke option on those nefarious puppers from the get-go and move on with our lives, what do you say? I stock an entire arsenal of potent ordnance for taking down the cyber bad guys, be they corporate, governmental, or just private mercenaries with a yen for easy money.

Most of the "best defense is a strong offense" proposals I've seen involve fighting fire with fire. Tedious and predictable, my young apprentice. The way to fight fire is to bury it under a deluge of sloppy wet stuff. As a longtime purveyor of same, here are some of my suggested tactical instruments of vengeance, both offensive and defensive, along with the philosophical statement you'll be making with each. All are dedicated to the proposition that protecting one's information assets can also count as entertainment.

Chaos in the Middle: intercept network traffic heading to and from your enemy and attach random headers and payloads derived from Pinterest or /r/SubredditSimulator. Then sit back and watch their logs fill up.

Message it sends: Hr r yr lulz.

Matrix Honeypot: divert hostile traffic into a honeypot universe where all of the attackers' initial strategic goals seem to be met perfectly. Once they're hooked, create increasingly more complex and comprehensive layers of alternate reality until they no longer have any objective means by which to differentiate that virtual world from the real one. They will now be trapped forever. Not recommended for teams on a budget, as the necessary pecuniary outlay can approach infinity over time.

Message it sends: Take two blue pills and WhatsApp me in the morning.

Grade School Playground: a bot that replies to every email, text message, or other enemy communication with, "I know you are, but what am I?" Attach optional raspberry.mp3, nyah-nyah.mp3 to complete the experience.

Message it sends: It's always recess somewhere.

Reverse Ransomware: threaten to break the enemy's encryption with your supercomputer and supply the key to their victims for free unless the crooks pay half the ransoms to you. Not so much an attack as a business model.

Message it sends: Thank you for your patronage.

Mirror, Mirror: automatically reflect every packet sent by an attacker in FILO order. Essentially a variation on the *Grade School Playground* method (cf.). Economical because it only requires a modified network appliance. Will not make you popular with your upstream neighbors, though, and renders the node pretty much useless for getting any real work done.

Message it sends: We're sorry, the number you have reached is not in service.

Blast Phishing: Perform both passive and active phishing-based reconnaissance on the target to establish patterns, methods, and locations. Once all the necessary intelligence has been gathered, launch absolutely everything in your malware database simultaneously along all mapped hostile vectors. Messy, but effective if you don't want any survivors. A healthy chunk of bandwidth is a must here.

Message it sends: Today is a good day to die().

Hydra Hail: Invest in sufficient infrastructure to spawn virtually endless numbers of cloned virtual machines on isolated VLANs. Every time the enemy attacks, take the affected virtual presence down instantly and plop another clone in its place. Rinse and repeat ad infinitum until the attacker gives up in frustration. Have a beer to celebrate your victory.

Message it sends: Sticks and stones may break my bones, but I have a heck of a lot of bones.

Catatonia: Trace the IP address of the attacker and forward every known cat video to it, effectively purr-alyzing the hostile network under a dense blanket of furry cuteness.

Message it sends: Get some of this meow up in your grill, evildoer.

And finally,

Utter Acquiescence: powers down the entire network and reverts everyone to slide rules and typewriters. See also RFC 1149.

Message it sends: We have a constitutionally mandated Postal Service for a reason.

If you don't know how to work a slide rule, I'll be happy to teach you, although admittedly I mostly used mine as a straightedge for drawing castles on my notebooks. I still have my Pickett N902-ES from high school, along with my grad school-era Brother Professional CX-90 daisy wheel electric typewriter. They've never been compromised, although I did misplace my italic daisy wheel once.

As for me, I do all of my mission-critical computing on my trusty Osborne 1 these days and thus I'm not too vulnerable to attack unless you're into crafting exploits for CP/M 2.2. And mailing them to me on a 5.25" disk.