# [Ferdez]

“Details, details. You always get caught from the small stuff. If you don’t cycle that generator like we were never here it’ll start throwing alerts. Bring in all sorts of nosy types askin questions we don’t want asked.”

Ferdez was a gruff old thief who rarely worked with new people. If you were lucky enough to work with him you stood a chance of learning how to not get caught. Ferdez was the best. Is the best. Somehow he’s never turned up once in anyone’s records of investigations, persons of interest, suspects or otherwise. On paper Hardison P. Ferdez was just your average taxpaying citizen, and he meant to keep it that way.

“How you even cycle that old thing? Nobody uses them any more”, Romero asked. He was a young man in his early twenties who’d grown up in the prefab complexes where all the machinery was more or less the same.

They had tapped into the grid down in the maintenance room. Water systems were automated like everything else, but few knew that the sensors were lightly guarded. The defenses the did have were designed to thwart software takeovers that attacked via wireless signals. Physical attacks that impersonated water were unheard of. Ferdez was particularly fond of that innovation. The telemetry from this sort of attack looked like a small patch of water flowing by that happened to contain some compounds that failed to register on the sensors. The sensor array would notice this anomaly and call home to update its catalog, thinking it was out of date. If you sniffed the outbound call you could pick up the authentication credentials (aka ‘auth’ or ‘creds’) and replay them. Ferdez had been impersonating water sensors for years in this district, and given its industrial tenants and their questionable ethics towards dumping there were always sensors getting confused and calling for updates. Ferdez’s tactics were not even a blip on the radar in this environment.

The trick however was that you had to be proximal to the sensors. Auth protocols were sophisicated enough to encode geospatial coordinates in the equation along with other private keys burned into the boards, ensuring that remote attacks were not worth the trouble. Physical proximity allowed you to capture a well-formed auth request with all the magic already baked into it. Ferdez had discovered this years before, and had gotten to know the waterfront well.

“You read up on ‘em. Take a job as a maintenance jockey. Truth is, it’s an art form. You get a feel for them. They breathe. Have a pulse. Put your hand on it. Feel the vibrations. That’s the diff versus the sims, hard matter sometimes acts in ways the sims can predict or understand. You can hear a change in pitch or a creak or a groan in the metal. But you gotta actually be here. Not ‘here’ via goggles, but *here* here. You smell that? That’s healthy machine oil, not burnt. This baby’s well taken care of, which is what we’re gonna do. Leave it as good as we found it, sometimes better.”

“Dude you a zen master or something? Don’t sound like any hackers I know.”

“Exactly. That you know. You tap in down here in the physical, you stay secret. If you’re lookin to make a name for yourself or do a big exploit I’m not your guy. If you want to be in a position to gather valuable data on the sly, then here you go. Synth told me you had a level head, not flashy. Was he wrong?”

“No, not wrong. This just… isn’t what I expected.”

“Thank you very much. I take pride in never doing what they expect.”

“Yeah, I’m starting to get that.”

Fifteen minutes later the substation cycled, being convinced the updates downloaded were enough to require one. By the time the cycle was complete and central received the station telemetry Ferdez and Romero were long gone.

“So tell me again how a water sensor array is allowed to ask for the Consulate General’s flight plans?”

“Stepping stones. Once we get the sensor creds we can run code on the substation processor boards. I load one of my own code blocks up there that tells the station it needs to check power routing, so it makes that call and we sniff those creds. Power creds have a lot more priveleges, including requesting data packet routing (DPR) hints for signal latency optimization. DPR’s come from the network supernodes. Once you’re talking to a supernode you can ask lots of interesting questions.”

“Damn. All from some dirty water and patch cords.”

“And some serious blocks once we’re in. Blocks like those know how to look innocuous and then clean up after themselves.”

Ferdez downplayed the true difficulty of running code on a supernode for now, not wanting to overwhelm Romero nor give away all his secrets just yet. The real truth was much larger. For the past decade Ferdez had been observing and recording patterns from every incursion. Patters of what legitimate applications look like, their runtime lifecycles, the manner in which they release memory resources when complete, and where they store their creds while running. He learned subtle tricks like copying an entire app and rerunning it moments after its removal, to make it look like a minor blip had caused it to restart. The app already had clearance so he didn’t even have to capture nor decrypt its creds. Decryption took rooms full of servers, time and lots of energy. Restarting an app that ‘accidentally terminated too soon’ required none of those, and its eventual cleanup left no traces.

Leave nothing running – this was the most important rule of them all. Resident code will eventually be found. Always. And it will piss people off. Really serious people. People that will make it their personal mission to find the breach and fix it.

Ferdez’s code always politely notified the system when its job was complete and requested teardown. No footprints. Server logs would contain records of all the calls, but the app Id’s are all real and always changing. The pattern he left behind was a tiny echo of the pattern of worldwide traffic itself, rendering it invisible in plain sight.

The real truth was immense. Ferdez was the best listener on the entire planet.