THURSDAY MORNING: SNOWED IN (GET IT?)

[image: Jack Amick via Flickr]

Yes, it’s a weak information security joke, but it’s all I have after shoveling out.

Michigan’s winter storm expanded and shifted last night; Marcy more than caught up on her share of snow in her neck of the woods after all.

Fortunately nothing momentous in the news except for the weather…

Carmaker Nissan’s LEAF online service w-i-d-e open to hackers
Nissan shut down its Carwings app service, which controls LEAF model’s climate control systems. Carwings allows vehicle owners to check information about their cars on a remote basis. Some LEAF owners conducted a personal audit and hacked themselves, discovering their cars were vulnerable to hacking by nearly anyone else. Hackers need only the VIN as userid and no other authentication to access the vehicle’s Carwings account. You’d think by now all automakers would have instituted two-factor authentication at a minimum on any online service.

Researcher says hardware hack of iPhone may be possible
With “considerable financial resources and acumen,” a hardware-based attack may work against iPhone’s passcode security. The researcher noted such an attempt would be very risky and could destroy any information sought in the phone. Tracing power usage could also offer another opportunity at cracking an iPhone’s passcode, but the know-how is very limited in the industry. This bit from the article is rather interesting:

> IOActive’s Zonenberg, meanwhile, told Threatpost that an invasive hardware attack hack is likely also in the National Security Agency’s arsenal; the NSA has been absent from discussions since this story broke last week.
>
> “It’s been known they have a semiconductor [fabrication] since January 2001. They can make chips. They can make software. They can break software. Chances are they can probably break hardware,” he said. “How advanced they were, I cannot begin to guess.”

The NSA has been awfully quiet about the San Bernardino shooter’s phone, haven’t they?

‘Dust Storm’: Years-long cyber attacks focused on intel gathering from Japanese energy industry
“[U]sing dynamic DNS domains and customized backdoors,” a nebulous group has focused for five years on collecting information from energy-related entities in Japan. The attacks were not limited to Japan, but attacks outside Japan by this same group led back in some way to Japanese hydrocarbon and electricity generation and distribution. ‘Dust Storm’ approaches have evolved over time, from zero-day exploits to spearfishing, and Android trojans. There’s something about this collected, focused campaign which sounds familiar – rather like the attackers who hacked Sony Pictures? And backdoors…what is it about backdoors?

ISIS threatens Facebook’s Zuckerberg and Twitter’s Dorsey
Which geniuses in U.S. government both worked on Mark Zuckerberg and Jack Dorsey about cutting off ISIS-related accounts AND encouraged revelation about this effort? Somebody has a poor grasp on opsec, or puts a higher value on propaganda than opsec.

Wonder if the same geniuses were behind this widely-reported meeting last week between Secretary of State John Kerry and Hollywood executives. Brilliant.

Case 98476302, Don’t text while walking
So many people claimed to have bumped their heads on a large statue while texting that the statue was moved. The stupid, it burns…or bumps, in this case.

House Select Intelligence Committee hearing this morning on National Security World Wide Threats. Usual cast of characters will appear, including CIA Director John Brennan, FBI Director James Comey, National Counterterrorism Center Director Nicholas Rasmussen, NSA Director Admiral Michael Rogers, and Defense Intelligence Agency Director Lieutenant General Vincent Stewart. Catch it on C-SPAN.

Snow’s supposed to end in a couple hours, need to go nap before I break out the snow shovels again. *À plus tard!*