

WHY IS THE ARAMCO HACK CONSIDERED A SIGNIFICANT NSA MILESTONE?

I've been puzzling over the list of "key SSO cyber

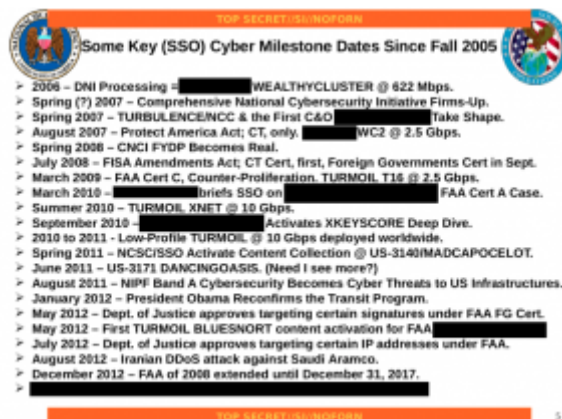
milestone dates" released with the upstream 702 story the other day.

For the most part, it lists technical and legal milestones leading to expanded collection targeting cyber targets (which makes sense, given that's what Special Source Operations does – collect data off switches). There's the one redacted bullet (which, if it referred to an attack thwarted, might refer to this thwarted attack on a US defense contractor in December 2012).

But what is the August 2012 DDOS attack on Saudi Aramco doing on the list? And, for that matter, why is it referred to as a DDOS attack?

The attack was publicly described as a two-step hack targeted against both Aramco and Qatar's gas industry which copy-catted an attack associated with the Flame attack on Iran. It is generally now described as Iranian retaliation for StuxNet. Though at the time, potential attribution ranged from hacktivists, a single hacker, or Aramco insiders. The Sony hack used tools related to the Shamoan attack.

Not long after the Aramco hack, the NSA expanded their Third Party SIGINT relationship to include



the Saudi Interior Ministry (then led by close US ally Mohammed bin Nayef). The next month the Saudis (again, with MbN in the leader) prematurely renewed their Technical Cooperation Agreement with the US, adding a new cybersecurity component.

So regardless of how serious an attack it was (on that, too, accounts varied) it did have a significant effect on our role in cybersecurity in the Middle East, potentially with implications for SS0.

But unless SS0 thwarted the attack – or at least alerted the Saudis in time to pull their computers offline – why would that be a significant milestone for SS0?