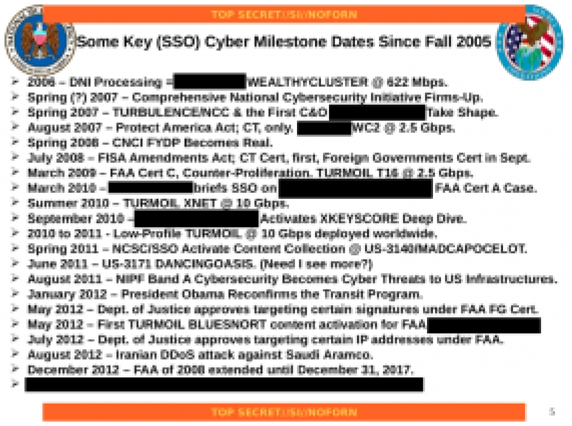
WHY IS THE ARAMCO HACK CONSIDERED A SIGNIFICANT NSA MILESTONE?



TOP SECRET//SI//NOFORN

Some Key (SSO) Cyber Milestone Dates Since Fall 2005

- 2006 – DNI Processing =[redacted]WEALTHYCLUSTER @ 622 Mbps.
- Spring (?) 2007 – Comprehensive National Cybersecurity Initiative Firms-Up.
- Spring 2007 – TURBULENCE/NCC & the First C&O [redacted]Take Shape.
- August 2007 – Protect America Act; CT, only. [redacted]WC2 @ 2.5 Gbps.
- Spring 2008 – CNCI FYDP Becomes Real.
- July 2008 – FISA Amendments Act; CT Cert, first, Foreign Governments Cert in Sept.
- March 2009 – FAA Cert C, Counter-Proliferation. TURMOIL T16 @ 2.5 Gbps.
- March 2010 –[redacted]briefs SSO on [redacted] FAA Cert A Case.
- Summer 2010 – TURMOIL XNET @ 10 Gbps.
- September 2010 –[redacted]Activates XKEYSCORE Deep Dive.
- 2010 to 2011 - Low-Profile TURMOIL @ 10 Gbps deployed worldwide.
- Spring 2011 – NCSC/SSO Activate Content Collection @ US-3140/MADCAPOCELOT.
- June 2011 – US-3171 DANCINGOASIS. (Need I see more?)
- August 2011 – NIPF Band A Cybersecurity Becomes Cyber Threats to US Infrastructures.
- January 2012 – President Obama Reconfirms the Transit Program.
- May 2012 – Dept. of Justice approves targeting certain signatures under FAA FG Cert.
- May 2012 – First TURMOIL BLUESNORT content activation for FAA[redacted]
- July 2012 – Dept. of Justice approves targeting certain IP addresses under FAA.
- August 2012 – Iranian DDoS attack against Saudi Aramco.
- December 2012 – FAA of 2008 extended until December 31, 2017.
- [redacted]

TOP SECRET//SI//NOFORN

5

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 Shamoon 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 SSO.

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