# SIDE BY SIDE: TIMELINE OF NSA'S COMMUNICATIONS COLLECTION AND CYBER ATTACKS

In all the reporting and subsequent hubbub about the National Security Administration's ongoing collection of communications, two things stood out as worthy of additional attention:

– Collection may have been focused on corporate metadata;

– Timing of NSA's access to communications/software/social media firms occurred alongside major cyber assault events, particularly the release of Stuxnet, Flame, and Duqu.

Let's compare timelines; keep in mind these are not complete.

| Date | NSA/Business | Cyber Attacks |
|---|---|---|
| 11-SEP-2007 | Access to MSFT servers acquired | |
| 15-NOV-2007 | | Stuxnet 0.5 discovered in wild |
| XX-DEC-2007 | | File name of Flame's main component observed |
| | | |
| 12-MAR-2008 | Access to Yahoo servers acquired | |

| | | |
|---|---|---|
| All 2008 (into 2009) | | Adobe applications suffer from 6+ challenges throughout the year, including attacks on Tibetan Government in Exile via Adobe products. |
| | | |
| 11-JAN-2009 | | Stuxnet 0.5 “ends” calls home |
| 14-JAN-2009 | Access to Google servers acquired | |
| Mid-2009 | | Operation Aurora attacks begin; dozens of large corporations confirming they were targets. |
| 03-JUN-2009 | Access to Facebook servers acquired | |
| 22-JUN-2009 | | Date Stuxnet version 1.001 compiled |
| 04-JUL-2009 | | Stuxnet 0.5 terminates infection process |
| 07-DEC-2009 | Access to PalTalk servers acquired | |

| | | |
|---|---|---|
| XX-DEC-2009 | | Operation Aurora attacks continue through Dec 2009 |
| | | |
| 12-JAN-2010 | | Google discloses existence of Operation Aurora, said attacks began in mid-December 2009 |
| 13-JAN-2010 | | Iranian physicist killed by motorcycle bomb |
| XX-FEB-2010 | | Flame operating in wild |
| 10-MAR-2010 | | Date Stuxnet version 1.100 compiled |
| 14-APR-2010 | | Date Stuxnet version 1.101 compiled |
| 15-JUL-2010 | | Langner first heard about Stuxnet |
| 19-SEP-2010 | | DHS, INL, US congressperson informed about threat posed by “Stuxnet-inspired malware” |
| 24-SEP-2010 | Access to YouTube servers acquired | |
| 29-NOV-2010 | | Iranian scientist killed by car bomb |

| | | |
|---|---|---|
| 06-FEB-2011 | Access to Skype servers acquired | |
| 07-FEB-2011 | | AOL announces agreement to buy HuffingtonPost |
| 31-MAR-2011 | Access to AOL servers acquired | |
| 01-SEP-2011 | | Duqu worm discovered |
| | | |
| XX-MAY-2012 | | Flame identified |
| 08-JUN-2012 | | Date on/about “suicide” command issued to Flame-infected machines |
| 24-JUN-2012 | | Stuxnet versions 1.X terminate infection processes |
| XX-OCT-2012 | Access to Apple servers acquired (date NA) | |

Again, this is not everything that could be added about Stuxnet, Flame, and Duqu, nor is it everything related to the NSA’s communications collection processes. Feel free to share in comments any observations or additional data points that might be of interest.

Please also note the two deaths in 2010; Stuxnet and its sibling applications were not the only efforts made to halt nuclear proliferation in Iran. These two events cast a different light on the surrounding cyber attacks.

Lastly, file this under “dog not barking”:

Why aren’t any large corporations making a substantive case to their customers that they are offended by the NSA’s breach of their private communications through their communications providers?