



Never Mind the Corporate Spying

Google's Shareholder Theater

Scanning over the headlines of the *New York Times* this past Saturday, June 6th, the public relations team at Google scored a splashy front page spot which confidently boasts that the company is working hard to impede the NSA (e.g. to "erect barriers") by comprehensively encrypting data in transit through Google's networks [1]. Other hi-tech companies, like Yahoo, have implemented similar measures [2]. Of course, there are a number of particulars that this story fails to acknowledge...

Encryption Is Not a Panacea

One thing Google's PR team fails to acknowledge is that encryption represents little or no defense against hi-tech subversion. Specifically, hardware and software bugs (accidental or otherwise) as back doors trump encryption every time. As witnessed in both the cases of the Heartbleed bug [3] and the malware used in the recent breach of Target [4], if an attacker can leverage buggy code to compromise a computer and scrape its memory for cryptographic keys (i.e. passwords) it doesn't matter how strong the encryption is; attackers can walk right through digital bulwarks and sink your battleship.

Oh, and get this, thanks to Ed Snowden we know that one of the NSA's strategic goals is to industrialize the process of subversion: to launch mass attacks on millions of computers simultaneously using a system codenamed TURBINE and install software implants (also called rootkits, something your author is intimately familiar with [5]) that allow the government to maintain a concealed presence and covertly collect data [6]. The new director of the NSA, Vice Adm. Michael S. Rogers, has openly advocated this technology [7]. Does this sound like a tenable countermeasure for ubiquitous encryption?

It's part of the public record that hi-tech companies have placed back doors in their products as part of an industry-wide effort conducted by the NSA known as the *Signal Intelligence Enabling Project*. A document published by the *Guardian* states that [8]:

"The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable"

Please understand, this mindset emphasizes security for the 1%, where society's collective security is completely undermined on behalf of a small cabal of spies.

Though Microsoft stridently claims that it does not insert back doors for the NSA [9] there is evidence to the contrary. For instance, it's been revealed that Microsoft provides the NSA with early access to zero-day exploits (unpatched bugs) that arise in products like Windows [10]. After all, Microsoft recently

signed a \$617 million contract with the Department of Defense [11]. Don't think that this sort of gift comes without strings.

Never Mind The Corporate Spying...

Another subtle manipulation that's being employed is to frame the narrative so that focus is placed entirely on government surveillance. This is the same caveat that haunts surveillance reform efforts like "Reset the Net." *Pando Daily's* Yasha Levine spells it out [12]:

"Reset the Net is deeply flawed. The reason: the campaign is not against online surveillance, just government surveillance. It has nothing to say or critique about the massive for-profit dragnet operations run by telecoms and Silicon Valley megacorps that target every woman, man and child in the United States and beyond"

In contrast to the inflated fanfare about disrupting terrorist plots [13] the global surveillance apparatus is essentially being driven by powerful corporate interests [14]. This is the elephant standing in the corner that no one (especially hi-tech companies like Google) wants to talk about. Roughly 70 percent of the intelligence budget, which is in the neighborhood of 70 billion dollars, goes to the private sector [15]. So most of what we think of as government surveillance actually transpires in the private sector. How, exactly, do you think a Booz Allen Hamilton consultant named Ed Snowden got all of those classified documents? The NSA is a mere appendage of a much larger private sector data aggregation panopticon that rakes in \$200 billion every year [16].

Though Eric Schmidt has railed against government surveillance in public [17], Google has extensive long-standing connections with the defense industry [18]. Not to mention that WikiLeaks has released cables that describe some rather odd dealings between Google, the State Department, and the U.S. Military. Trips to the border of Iran [19] and signal intelligence in Afghanistan [20]. Google and the government are far more tightly linked than most people suspect. Is it any wonder that Google now spends more than Lockheed Martin and Boeing to lobby for influence in D.C. [21]? Something on the order of \$16 million in 2013.

Denouement

Google has exerted a lot of effort into creating the impression of revolt. But Google hasn't switched sides. Remember, the strategic goal of Google's public relations effort isn't necessarily to stymie government spies, but rather to give voice to the general sense of public betrayal and at least offer the *perception* that Google has switched sides; to courageously fend off the big bad government on behalf of irate users. More susceptible members of the audience who believe this storyline will continue to use Google services. This will reinforce the bottom line and subsequently reassure investors. Google will do what it's always done: follow its fiduciary responsibility to generate profits. The public be damned!

Bill Blunden is an independent investigator whose current areas of inquiry include information security, anti-forensics, and institutional analysis. He is the author of several books, including *The Rootkit Arsenal* and *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex*. Bill is the lead investigator at Below Gotham Labs.

End Notes

- [1] David E. Sanger And Nicole Perlroth, "Internet Giants Erect Barriers to Spy Agencies," *New York Times*, June 6, 2014, <http://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html>
- [2] Seth Schoen, "Yahoo Protects Users with Lots More Encryption," *Electronic Frontier Foundation*, April 2 2014, <https://www.eff.org/deeplinks/2014/04/yahoo-protects-users-lots-more-encryption>
- [3] Jordan Robertson, "Heartbleed Hackers Steal Encryption Keys in Threat Test," *Bloomberg*, April 15, 2014, <http://www.bloomberg.com/news/print/2014-04-14/heartbleed-hackers-steal-encryption-keys-in-threat-test.html>
- [4] Jim Finkle and Mark Hosenball, "Exclusive: More well-known U.S. retailers victims of cyber attacks - sources," *Reuters*, January 12, 2014, <http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112>
- [5] Bill Blunden, *The Rootkit Arsenal: Escape and Evasion In the Dark Corners of The System*, Jones & Bartlett Learning; 2 edition, March 16, 2012, ISBN-13: 978-1449626365
- [6] Ryan Gallagher and Glenn Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware," *Intercept*, March 12, 2014, <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/>
- [7] David Sanger, "N.S.A. Nominee Promotes Cyberwar Units," *New York Times*, March 11, 2014, <http://www.nytimes.com/2014/03/12/world/europe/nsa-nominee-reports-cyberattacks-on-ukraine-government.html>
- [8] "Sigint – how the NSA collaborates with technology companies," *Guardian*, September 5, 2013, <http://www.theguardian.com/world/interactive/2013/sep/05/sigint-nsa-collaborates-technology-companies>
- [9] Brad Sams, "Microsoft fights back, calls out China on its Windows 8 claims," *Neowin*, June 6, 2014, <http://www.neowin.net/news/microsoft-fights-back-calls-out-china-on-its-windows-8-claims>
- [10] Michael Riley, "U.S. Agencies Said to Swap Data With Thousands of Firms," *Bloomberg*, June 15, 2013, <http://www.bloomberg.com/news/print/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html>
- [11] Nick Taborek, "Microsoft's Windows 8 Lifted by \$617 Million Defense Deal," *Bloomberg*, January 5, 2013, <http://www.bloomberg.com/news/print/2013-01-04/microsoft-s-windows-8-lifted-by-617-million-defense-deal.html>

[12] Yasha Levine, "Reset the Net wants to end NSA snooping, is fine with Google snooping," *Pando Daily*, June 6, 2014, <http://pando.com/2014/06/06/reset-the-net-wants-to-end-nsa-snooping-is-fine-with-google-snooping/>

[13] Justin Elliott and Theodoric Meyer, "Claim on "Attacks Thwarted" by NSA Spreads Despite Lack of Evidence," *ProPublica*, October 23, 2013, <http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence>

[14] "Segment: Heidi Boghosian on Spying and Civil Liberties," *Bill Moyers and Company*, November 8, 2013, <http://billmoyers.com/wp-content/themes/billmoyers/transcript-print.php?post=48454>

[15] Tim Shorrock, "Put the Spies Back Under One Roof," *New York Times*, June 18, 2013, <http://www.nytimes.com/2013/06/18/opinion/put-the-spies-back-under-one-roof.html>

[16] Yasha Levine, "What Surveillance Valley knows about you," *Pando Daily*, December 22, 2013, <http://pando.com/2013/12/22/a-peek-into-surveillance-valley/>

[17] Deborah Kan, "Google's Eric Schmidt Lambasts NSA Over Spying," *Wall Street Journal*, November 4, 2013, <http://online.wsj.com/news/articles/SB10001424052702304391204579177104151435042>

[18] Yasha Levine, "The revolving door between Google and the Department of Defense," *Pando Daily*, April 23, 2014, <http://pando.com/2014/04/23/the-revolving-door-between-google-and-the-department-of-defense/>

[19] Julian Assange, "Op-ed: Google and the NSA: Who's holding the 'shit-bag' now?," *WikiLeaks*, August 27, 2013, <https://wikileaks.org/Op-ed-Google-and-the-NSA-Who-s.html>

[20] "WikiLeaks claims Google director helped the NSA spy on Afghanistan," *RT*, May 28, 2014, <http://rt.com/usa/162036-wikileaks-google-nsa-afghanistan/>

[21] Center for Responsive Politics, Influence & Lobbying/ Lobbying / Top Spenders, <https://www.opensecrets.org/lobby/top.php?showYear=2013&indexType=s>