

CRYPTOME

Cornering the Zero-Day Market

The Schizophrenia of the Deep State

By **Bill Blunden**, August 7, 2014

A few days ago Dan Geer, the chief information security officer at In-Q-Tel, gave a keynote address at Black Hat USA¹. According to the company's web site In-Q-Tel is a non-profit, but it's a special sort of non-profit. It offers venture capital funding on behalf of the "intelligence community" (read government spies). During his presentation Geer proposed, among other things, that the U.S. government bolster internet security by dominating the market for zero-day vulnerabilities.

Zero-days are basically flaws, unpatched bugs, in software and hardware which attackers can leverage to compromise a computer and covertly gain access. Think of a zero-day vulnerability like an unlocked door recessed back in an obscured alleyway of an otherwise secure home.

Geer's recommendation goes like this: using its buying power the United State government could act like a hi-tech billionaire who's snatching up real estate in Silicon Valley and wade out into the digital black market to outbid all of the other buyers. By driving up prices American security services would corner the market on zero-day vulnerabilities.

On an aside this strategy would also make zero-day middle-men like the Grugq extremely wealthy². Anyway, according to Geer's reasoning the government would then disclose the aforementioned unpatched bugs to hi-tech companies so that they could fix their products and shrink the attack surface available to intruders.

Conflicting Directives

There's a problem with this scheme. Behind closed doors, where officials feel comfortable enough to be honest, elements of the intelligence community confess that they aren't actually interested in bolstering Internet security. In fact, according to documents provided by Ed Snowden, spy agencies are intent on **doing the exact opposite**³:

"Classified briefings between the agencies celebrate their success at 'defeating network security and privacy ...'"

Please understand that hi-tech subversion is a pillar of the NSA's global surveillance apparatus. It's how they monitor people and defeat privacy measures like Tor⁴. Subversion empowers spies. Are we to assume that U.S. intelligence having engaged in an extensive industry-wide campaign to insert

backdoors in software and hardware⁵, and sitting on a mountain of zero-day vulnerabilities which it exclusively owns, will abruptly make an about face and completely disarm?

After all of the lies: about imaginary WMDs, about torture, about warrantless wiretaps, about spying on Senators. After all the death and destruction⁶, there's no reason to believe that the Deep State would act in the public's interest and voluntarily yield this sort of power. No sir.

Echoes of the Financial Collapse

In the aftermath of the 2008 financial meltdown the United States government intervened to bail out the banks. The average American ultimately paid for the short-term unenlightened self-interest of banking executives who handed out loans to anyone who could breathe⁷. Well, because doing so was wildly profitable⁸. The current bailout mindset offers bankers an implicit subsidy⁹ as the entire industry now recognizes that large banking houses can socialize their risk while keeping whatever profits they make to themselves¹⁰. In a nutshell mega-banks are fragile by design.

Technology is also fragile by design. The costs associated with the security lapses that arise from zero-day vulnerabilities are paid for by the victims. These same costs are viewed as a *negative externality* by the companies that sell hi-tech products. Vendors make money by adding features and selling new products. Well, because doing so is wildly profitable. Think about it. They aren't in business to do the right thing, they're in business to make money¹¹.

Assuming for the moment that the public were somehow able to marshal the raw political impetus needed to put an end to the NSA's sweeping campaign of mass subversion, we'd still have to worry about accidental bugs and the market forces that encourage them.

But why, pray tell, should the public be held responsible for sloppy engineering? **Why should we bear the cost of shoddy hi-tech design just as the American public paid for the banker's screw-ups?** Rather than have the victims of bad security pay for zero-day exploits, why not redirect the cost of security incidents back onto vendors so that they have incentives to get it right? Society as a whole is being exposed to risk and therefore regulation (i.e. via liability) is necessary. The never-ending stream of zero-days clearly shows that the market cannot deal with this problem on its own.

Denouement

Sadly, regulating the banks has been wishful thinking ever since executives and their operatives in D.C. rolled back Glass-Steagall during Bill Clinton's tenure in the White House. Witness also the Commodity Futures Modernization Act of 2000 which left the financial market for derivatives largely unregulated. Put bluntly, the banks have the resources and power to reward those who serve them¹². A similar dynamic holds in the domain of hi-tech. For example, in 2013 Google spent more lobbying on the beltway than Lockheed Martin or Boeing¹³.

So is it surprising that major players in both industries have considerable links to intelligence services? Former LAPD detective Michael Ruppert declared "*The CIA is Wall Street. Wall Street is the CIA.*" A look

into the origins of the CIA reinforces this notion¹⁴. Likewise, thanks to Ed Snowden¹⁵ and WikiLeaks¹⁶, we know that companies like Google have gladly clambered into bed with government spies. CIA officer John Stockwell observed that:

“The CIA and the big corporations were, in my experience, in step with each other. Later I realized that they may argue about details of strategy - a small war here or there. However, both are vigorously committed to supporting the system.”

Poor cyber security is rooted in zero-day vulnerabilities, accidental and intentional. Yet disarming the intelligence services and implementing meaningful regulation within the hi-tech sector will oblige massive political shifts. In both cases such efforts will run up against profound sources of influence outside the government, **oligarchic factions** that convey their mandates through the Deep State.

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.

Notes

¹ Kim Zetter, “CIA Insider: U.S. Should Buy All Security Exploits, Then Disclose Them,” *Wired*, August 6, 2014, <http://www.wired.com/2014/08/cia-0day-bounty/>

² Nicole Perlroth and David Sanger, “Nations Buying as Hackers Sell Flaws in Computer Code,” *New York Times*, July 13, 2013, <http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted%253Dall>

³ James Ball, Julian Borger, and Glenn Greenwald, “Revealed: how US and UK spy agencies defeat internet privacy and security,” *Guardian*, September 5, 2013, <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security/print>

⁴ Bill Blunden, “Mass Subversion is a Reality,” *Counterpunch*, July 24, 2014, <http://www.counterpunch.org/2014/07/24/mass-subversion-is-a-reality/>

⁵ 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>

⁶ <http://costsofwar.org/article/civilians-killed-and-wounded>

⁷ Martin Smith, “The Untouchables,” *Frontline*, January 22, 2013, <http://www.pbs.org/wgbh/pages/frontline/business-economy-financial-crisis/untouchables/transcript-37/>

⁸ Yves Smith, “How the Banks Put the Economy Underwater,” *New York Times*, October 30, 2010, <http://www.nytimes.com/2010/10/31/opinion/31smith.html>

⁹ Matt Taibbi, “Secrets and Lies of the Bailout,” *Rolling Stone*, January 4, 2013, <http://www.rollingstone.com/politics/news/secret-and-lies-of-the-bailout-20130104>

¹⁰ Gretchen Morgenson, "Big banks Still a Risk," *New York Times*, August 2, 2014, <http://www.nytimes.com/2014/08/03/business/big-banks-still-a-risk.html>

¹¹ George Smith, "Keith Alexander Really IS a Pariah," *Escape from WhiteManistan*, August 2, 2014, <http://dickdestiny.com/blog1/?p=18406>

¹² David Corn, "Hillary Clinton's Goldman Sachs Problem," *Mother Jones*, June 4, 2014, <http://www.motherjones.com/politics/2014/06/hillary-clintons-goldman-sachs-problem>

¹³ <http://www.opensecrets.org/lobby/top.php?showYear=2013&indexType=s>

¹⁴ Peter Dale Scott, "The Deep State and the Wall Street Overworld," *Asia-Pacific Journal: Japan Focus*, March 10, 2014, http://japanfocus.org/-Peter_Dale-Scott/4090

¹⁵ Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *Guardian*, June 6, 2013, <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data/print>

¹⁶ <http://search.wikileaks.org/gifiles/?viewemailid=1121800>