counterpunch

WEEKEND EDITION JUNE 8-10, 2012

Security for the One Percent

Stuxnet Unbound

by BILL BLUNDEN

After its initial discovery in 2010 by an antivirus vendor from Belarus, the culprit behind the Stuxnet computer worm has been revealed. Last week, based on information leaked by inside sources[1], an article in the New York Times reported that the United States and Israel had secretly embarked on a joint project (code-named Olympic Games) which developed the malware we know as Stuxnet[2]. Despite the ruckus that members of the establishment make in public about foreign hackers (e.g. warning that China is a "threat to world order"[3]), the U.S. is admittedly one of the most active players in this field. While coverage in the press may adopt a seemingly congratulatory tone, there are reasons why this is an unsettling state of affairs.

Containment and control are not trivial issues. As the White House discovered first-hand, once you deploy offensive software there's no guarantee that it won't find its way out into the wild and infect otherwise uninvolved third parties. Will the CIA be covering the costs incurred from Stuxnet breaches outside of Iran? What about the tax-payer money spent by the likes of the DHS to analyze and dissect the CIA's creation[4]? And do you suppose there's a risk that some enterprising Black Hat out there on the Internet will scavenge captured components from U.S-sponsored malware for their own purposes? These types of concerns are exactly what discouraged the Pentagon from launching a cyber-attack against Saddam Hussein's financial system before the invasion of Iraq[5].

Then there's also the matter of efficacy. Was the Stuxnet attack actually as debilitating as a conventional military strike? Or have decision makers merely shown their hand and tipped off the Iranians. When Iranian military leaders originally assigned blame to the U.S. and Israel many people probably dismissed the accusation as a wild conspiracy theory[6]. The Iranians don't seem so paranoid after all, do they?

One aspect of Stuxnet, which has been corroborated at length by forensic investigators, is that the worm leveraged unpatched software flaws (also known as zero-day attacks) to do its job. It's generally known among Black Hats that the United States is a principal customer in the underground market for zero-day exploits[7]. As Bruce Schneier notes, the very existence of a market like this undermines our collective security[8]:

"The new market for security vulnerabilities results in a variety of government agencies around the world that have a strong interest in those vulnerabilities remaining unpatched. These range from law-enforcement agencies (like the FBI and the German police who are trying to build targeted Internet surveillance tools, to intelligence agencies like the NSA who are trying to build mass Internet surveillance tools, to military organizations who are trying to build cyber-weapons."

The end result is security for the 1%, who reside behind the shroud of secrecy, and relative insecurity for everyone else.

Finally, and most importantly, Stuxnet has once again exposed American exceptionalism. Espionage and sabotage are presented as intolerable criminal transgressions, normally causing our elected officials and military leaders to erupt in fits of righteous indignation. That is, unless the United States is doing the spying and the sabotaging (in which case we're seemingly rather proud of our status as leading rogue state). By crossing the Rubicon, our leaders have irrevocably lost the moral high ground. Not a wise decision for a country that, itself, depends heavily on the same buggy software that it regularly subverts.

Bill Blunden *is the author of The Rootkit Arsenal and the primary investigator at Below Gotham Labs.*

Notes.

[1] Evan Perez and Adam Entous, "FBI Probes Leaks on Iran Cyberattack," Wall Street Journal, June 5, 2012

[2] David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," New York Times, June 1, 2012

[3] Jamie Metzl, "China's Threat to World Order," Wall Street Journal, August 17, 2011,

[4] Tabassum Zakaria, “Idaho laboratory analyzed Stuxnet computer virus,” Reuters, September 29, 2011

[5] John Markoff and Thom Shanker, “Halted ’03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk,” New York Times, August 1, 2009.

[6] “Iran blames U.S., Israel for Stuxnet malware,” Associated Press, April 16, 2011

[7] Andy Greenberg, “Shopping For Zero-Days: A Price List For Hackers’ Secret Software Exploits,” Forbes, March 23, 2012.

[8] Bruce Schneier, “The Vulnerabilities Market and the Future of Security,” June 1, 2012.