How the NSA Thinks About Secrecy and Risk

By Bruce Schneier

The former monitoring base of the NSA in Bad Aibling, Germany (Reuters)

As I report in *The Guardian* today, the NSA has secret servers on the Internet that hack into other computers, codename FOXACID. These servers provide an excellent demonstration of how the NSA approaches risk management, and exposes flaws in how the agency thinks about the secrecy of its own programs.

Here are the FOXACID basics: By the time the NSA tricks a target into visiting one of those servers, it already knows exactly who that target is, who wants him eavesdropped on, and the expected value of the data it hopes to receive. Based on that information, the server can automatically decide what exploit to serve the target, taking into account the risks associated with attacking the target, as well as the benefits of a successful attack. According to a top-secret operational procedures manual provided by Edward Snowden, an exploit named Validator might be the default, but the NSA has a variety of options. The documentation mentions United Rake, Peddle Cheap, Packet Wrench, and Beach Head—all delivered from a FOXACID subsystem called Ferret Cannon. Oh how I love some of these code names. (On the other hand, EGOTISTICALGIRAFFE has to be the dumbest code name ever.)

Snowden explained this to *Guardian* reporter Glenn Greenwald in Hong Kong. If the target is a high-value one, FOXACID might run a rare zero-day exploit that it developed or purchased. If the target is technically sophisticated, FOXACID might decide that there's too much chance for discovery, and keeping the zero-day exploit a secret is more important. If the target is a low-value one, FOXACID might run an exploit that's less valuable. If the target is low-value and technically sophisticated,

FOXACID might even run an already-known vulnerability.

We know that the NSA receives advance warning from Microsoft of vulnerabilities that will soon be patched; there's not much of a loss if an exploit based on that vulnerability is discovered. FOXACID has tiers of exploits it can run, and uses a complicated trade-off system to determine which one to run against any particular target.

This cost-benefit analysis doesn't end at successful exploitation. According to Snowden, the TAO—that's Tailored Access Operations—operators running the FOXACID system have a detailed flowchart, with tons of rules about when to stop. If something doesn't work, stop. If they detect a PSP, a personal security product, stop. If anything goes weird, stop. This is how the NSA avoids detection, and also how it takes mid-level computer operators and turn them into what they call "cyberwarriors." It's not that they're skilled hackers, it's that the procedures do the work for them.

And they're super cautious about what they do.

While the NSA excels at performing this cost-benefit analysis at the tactical level, it's far less competent at doing the same thing at the policy level. The organization seems to be good enough at assessing the risk of discovery—for example, if the target of an intelligence-gathering effort discovers that effort—but to have completely ignored the risks of those efforts becoming front-page news.

It's not just in the U.S., where newspapers are heavy with reports of the NSA spying on every Verizon customer, spying on domestic e-mail users, and secretly working to cripple commercial cryptography systems, but also around the world, most notably in Brazil, Belgium, and the European Union. All of these operations have caused significant blowback—for the NSA, for the U.S., and for the Internet as a whole.

The NSA spent decades operating in almost complete secrecy, but those days are over. As the corporate world learned years ago, secrets are hard to keep in the information age, and openness is a safer strategy. The tendency to classify everything means that the NSA won't be able to sort what really needs to remain secret from everything else. The younger generation is more used to radical transparency than secrecy, and is less invested in the national security state. And whistleblowing is the civil disobedience of our time.

At this point, the NSA has to assume that all of its operations will become public, probably sooner than it would like. It has to start taking that into account when weighing the costs and benefits of those operations. And it now has to be just as cautious about new eavesdropping operations as it is about using FOXACID exploits attacks against users.

This article available online at:

http://www.theatlantic.com/technology/archive/2013/10/how-the-nsa-thinks-about-secrecy-and-risk/280258/