INTERNET CATS, WEAPONIZED: US DEFENSE CONTRACTOR CONSULTED ON TARGETED NETWORK INJECTION SURVEILLANCE FOR COMMERCIAL SALES ABROAD

[photo: liebeslakritze via Flickr]

First, a caveat: I would not click on the links embedded in the story I'm recommending (I'm this || close to swearing off embedded links forever). I don't trust traffic to them not to be monitored or exploited.

But as Jeremy Scahill tweeted last evening, read this piece by WaPo's Barton Gellman on malicious code insertion. This news explains recent changes by Google to YouTube once it had been

disclosed to the company that exploits could be embedded in video content as CitizenLab.org explains:

> "… the appliance exploits YouTube users by injecting malicious HTML-FLASH into the video stream. …"
> "… the user (watching a cute cat video) is represented by the laptop, and YouTube is represented by the server farm full of digital cats. You can observe our attacker using a network injection appliance and subverting the beloved pastime of watching cute animal videos on YouTube. …"

The questions this piece shake loose are Legion, but as just as numerous are the holes. Why holes? Because the answers are ugly and complex enough that one might struggle with them. Gellman's done the best he can with nebulous material.

An interesting datapoint in the first graf of the story is timing – fall 2009.

You'll recall that Google revealed the existence of a cyber attack code named Operation Aurora in January 2010, which Google said began in mid-December 2009.

You may also recall news of a large batch of cyber attacks in July of 2009 on South Korean targets.

The U.S. military had already experienced a massive uptick in cyber attacks in 1H2009, more than double the rate of the entire previous year.

And neatly sandwiched between these waves and events is a visit by a defense contractor CloudShield Technologies engineer from California, to Munich, Germany with British-owned Gamma Group.

Note the WaPo article contains no references whatsoever to zero day exploits, though Microsoft and Adobe are mentioned. Chinese-

launched Operation Aurora made use of these in what appears to be an intelligence gathering effort. Yet reading the underlying report by CitizenLab.org upon which the WaPo article was based you'll see "0-day" exploits have been involved. Probably just coincidence since zero day exploits have been problematic whether the originator is private hacker or state actor. But the likelihood Gamma Group was working on a non-state exploit for intelligence gathering intended for commercialization seems slim given the timeframe.

Plus the whole off-the-books bit — yeah, legal commercialized products for global marketplace need only an NDA, not the covert slinking around. CloudShield engineer Eddy Deegan said,

> "Nothing came of the work I was involved in at the time," he said. "I asked, and was assured that nothing illegal was undertaken. I have no further comment."

Because Deegan could see the line item entry in Gamma Group's books where it said PROJECT TERMINATED. At this point an emoji depicting the act of laughing one's self to death would be appropriate.

This bit in WaPo really jogs a lot of questions:

> The computer exploitation industry markets itself to foreign government customers in muscular terms. One Gamma brochure made public by WikiLeaks described its malware injection system, called FinFly ISP, as a "strategic, countrywide" solution with nearly unlimited "scalability," or capacity for expansion. Hacking Team, similarly, says it provides "effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities."
>
> In rare comments to the general public, the companies use the term "lawful intercept" to describe their products

> and say they do not sell to customers on U.S., European or U.N. black lists.
>
> “Our software is designed to be used and is used to target specific subjects of investigation,” said Eric Rabe, a U.S.-based spokesman for Hacking Team, in an extended e-mail interview. “It is not designed or used to collect data from a general population of a city or nation.”
>
> He declined to discuss details of the Citizen Lab report, which is based in part on internal company documents leaked to Marquis-Boire, but he appeared to acknowledge indirectly that the material was authentic.

You can drive a 40-foot dry van through the term “lawful intercept.” This technology could be easily transferred to any another entity, especially since key parties are located overseas, ostensibly out of U.S. purview. How can we be expected to believe this is only being sold to the “good guys” when even the “good guys” are sketchy and worse these days? What’s to say this technology isn’t being used on U.S. citizens right now by multiple entities at any one time, and Deegan’s allegedly terminated efforts were only a parallel alternative proof-of-concept for the injection tool deployed?