Furious Google throws down gauntlet to China over censorship

Google is done censoring search results in China and is prepared to abandon the country over the issue. The move comes amid revelations that Chinese hackers spied on human rights advocates around the globe by infiltrating Google's network.

By Nate Anderson | Last updated January 12, 2010 9:52 PM

Well, we've got to hand it to Google—the company's "don't be evil" schtick has long worn thin and governments around the globe are already probing its potential monopoly power, but who else would come out swinging against the entire Chinese government and announce an end to its own collaboration in censorship, all while recognizing that it could lose access to the entire Chinese market? And do it in a blog post?

This far but no further

The extraordinary announcement came this afternoon: Google has had it with China's pervasive web of censorship and spying, and the company is done censoring its search results in China. The decision wasn't made in a vacuum, but rather came after years of increasing cyberattacks from the Chinese mainland. A recent, massive infiltration attempt that targeted Google and 20 other tech companies was the final straw. Though Google stops short of naming the Chinese government as the party behind the attacks, the implication is clear.

In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident—albeit a significant one—was something quite different.

The attack hit major companies in the "Internet, finance, technology, media, and chemical sectors" as well. Its goal was "accessing the Gmail accounts of Chinese human rights activists," though it does not appear that anything more than subject lines were ever compromised. If that's not bad enough, Google also says it has acquired some intriguing evidence over the course of its investigation: "the accounts of dozens of U.S.-, China- and Europe-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. These accounts have not been accessed through any security breach at Google, but most likely via phishing scams or malware placed on the users' computers."

We have decided we are no longer willing to continue censoring our results on Google.cn...

The sheer scope of such attacks is staggering. They show a coordinated effort to target specific human rights advocates not just in China but around the world, and to do so by attempting to infiltrate some of the world's most advanced computer networks belonging to some of the
world's largest companies. (A Microsoft spokesperson tells Ars tonight, "We have no indication that any of our mail properties have been compromised." In response to some follow-up questions, we were told that the software giant would have no further comment.)

China has been well-known for going after the electronic communications of dissidents, and companies like Yahoo have in the past complied with Chinese government requests for e-mails. Those demands, however distasteful, at least followed a rough legal process in China. But Google's account indicates that, if the Chinese government is in fact linked to these recent attacks, it is willing to adopt extra-legal hacking in order to keep up its surveillance—and to do so anywhere in the world that communications of interest might be stored. Such a concerted program would be a marked escalation in the government's willingness to interfere in the operations of Internet companies in order to promote "stability."

Google has always claimed to be dissatisfied with the demands that it censor Chinese search results, but it has gone along with them since 2006. The argument has been that engagement with China, even in a censored fashion, was better than no access to tools like Google. But the recent attacks have caused a change of heart in Mountain View.

"We have decided we are no longer willing to continue censoring our results on Google.cn," announced Google's Chief Legal Officer David Drummond today, "and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all. We recognize that this may well mean having to shut down Google.cn, and potentially our offices in China."

That could be a big price to pay, given the size of China's burgeoning market. On the other hand, Google and other foreign search engines have had trouble gaining real traction in the local market and are regularly whipped by competitors like Baidu. And the price for operating in China is already high; the government has severe restrictions on ownership of businesses, which forces Internet companies into partnerships with local firms and subjects them to strict rules about censorship, pornography, and data retention.

A history of hacking?

China certainly isn't the only country to engage in hacking abroad, and it's certainly not the only country to employ powerful extra-legal surveillance of communications (the US' warrantless wiretapping comes to mind). China has become quite good at it, however, triggering reactions from countries as diverse as India, the US, New Zealand, and South Korea.

A recent report on Chinese cyber-warfare activities, produced by US military contractor Northrup Grumman, ends with a graphic showing the number of international incidents related to alleged Chinese hacking in the last decade. It's quite a list.
As to goals, one of the biggest is ripping off research breakthroughs in order to save time. The report notes that "Chinese industrial espionage is providing a source of new technology without
the necessity of investing time or money to perform research... Chinese espionage in the United States, which now comprises the single greatest threat to US technology, according to US counterintelligence officials, is straining the US capacity to respond. This illicit activity both from traditional techniques and computer-based activity are possibly contributing to China’s military modernization and its acquisition of new technical capabilities."

Did that approach extend to the attack on Google? It's not clear what "intellectual property" was stolen by the attackers, but it went beyond just trolling for the e-mails of human rights advocates.

VeriSign's iDefense unit has been looking at the attacks already. In an e-mail sent to Ars tonight, the group concluded that "the attack is the work of actors operating on behalf of or in the direct employ of official intelligence entities of the People’s Republic of China—and in many cases the attacks were successful." According to VeriSign's count, more than 30 companies were affected, up from the 20 counted by Google.