**The Internet Kill Switch; With Global Wiretapping Capability?**

One company to rule them all One company to find them; One company to bring them all And in the darkness bind them

Recently run any whois queries on Google? No? How about Facebook? MSN, or Hotmail? Yahoo? You might be surprised, comparing the results.

Nice, innit? See the "Last Updated" part also.

The brand-protecting, anti-piracy company MarkMonitor Inc. has had all these DNS names under its control for several months now.

They also control the Wikimedia name services, even though that doesn't show up on the Wikimedia.org whois record. There are many others. Apple.com falls under their jurisdiction, as does ubuntu.com. Nokia.com? Yep, under MarkMonitor. See a pattern here?

MarkMonitor also is a trusted Certificate Authority; they have, in essence, the means to fabricate safe-looking SSL connections for you, to whichever host they want. Your browser will not sound any warnings of possible man-in-the-middle attacks.

MarkMonitor is a company that can own most people's "Internet" in minutes. It now controls all three top free e-mail providers directly, and I suppose it's safe to say, most currently active social media sites too.

See for yourself. Whois yahoo.com, whois google.com, whois gmail.com, whois facebook.com, whois fbcdn.com, whois hotmail.com, whois msn.com... the list seems endless.

How'd all this happen?

This company has acquired complete access to monitor, eavesdrop, censor and fake any user of these popular Internet services in about one year (2011). In almost complete silence. For several of the sites, it also provides "firewall proxy" services, which means it is actually paid to intercept all communications. In and out.

The situation reminds me of Joseph Lieberman's 2010 initiative to create an "Internet kill switch" for the U.S.

The government only needs to control this one company, and most social media, most free e-mail, most search engines will be under its control. Not to mention most operating systems, for both computers and mobile devices.

Not only inside U.S., but globally. One company to rule them all.

I, for one, would like to ask; WTF is going on? How did these guys, this relatively small domain-hogging and pirate-chasing company, get the resources to simply acquire the DNS records of all the most popular Internet services? How can this be so totally ignored by the media, and even privacy advocates? Even conspiracy theorists seem to be completely ignoring the situation.

Secure communication is an illusion

Only one company to rule them all? As if all this doesn't sound bad enough, the problem is far more widespread. MarkMonitor could easily act as a global "kill switch" for the sites under its rule. But as it turns out, most anyone with some resources could just as easily impersonate MarkMonitor itself.

Because, as one might have noticed in the past few months, the whole SSL certificate scheme is broken. Not in a technical sense - there's no known inherent weakness in the algorithms. But the whole SSL protection is based on trust, and that trust has failed us.

According to several sources, SSL CA certs are routinely given out to anyone willing to pay for them. As The Register points out in its analysis on TrustWave spying scandal:

"Those defending Trustwave suggested that other vendors probably used the same approach for so-called "data loss prevention" environments - systems that inspect information flowing through a network to prevent leaks of commercially sensitive data." ... "In fact Geotrust was openly advertising a 'Georoot' product on their website until fairly recently."

http://www.theregister.co.uk/2012/02/14/trustwave\_analysis/

Oh, so the ability to impersonate anyone is normal day-to-day practise for big business? Just imagine what government agencies must be doing - for example in Sweden, where the military intelligence organisation FRA has the mandate to monitor all traffic across borders.

Who can seriously claim they trust all the hundreds of different CA companies, several of which have been caught red-handed with selling out their customers' security, or covering up very serious breeches (up to and including their root certificates being stolen).

http://nakedsecurity.sophos.com/2011/04/06/eff-uncovers-further-evidence-of-ssl-ca-bad-behavior/

MarkMonitor is a "brand-protecting" company. Traditionally its business has been reserving domains to protect brands. You buy its service, it makes sure that nobody else can have "mybrandsucks.com".

Also, they're an anti-piracy outfit. Their entire business is based on protecting IP.

http://www.marketwatch.com/story/markmonitor-to-exhibit-at-internet-tech-policy-exhibition-and-reception-to-be-held-on-capitol-hill-2012-01-24

Just saying, someone should probably question them and their customers. Why does Google, who always "do things themselves", externalise these vital parts of its network? How come all the competing phone and OS vendors, who sue each other all the time, suddenly trust this one company?

And then there's all those competing social media companies, who practically thrive on what others call "IP theft", including their users sharing text, images, music, videos and links?

Big questions. Defy common sense. Need answers.