The Great GOOGLE Hack! PART 2

Sat, 09 Jan 2016 16:00:00, newstips66, [post_tag: big-ticket-opposition-research-attacks-using-google, post_tag: consumer-complaints-about-google, post_tag: covert-google-operative-discusses-tactics-while-working-for-eric-schmidts-iqt, category: energy-dept-slush-fund, category: google-alphabet, post_tag: google-antitrust-case, post_tag: google-defamation-documents, post_tag: google-sex-scandals, post_tag: google-staff-character-studies, post_tag: google-stock-market-rigging, post_tag: googles-investores, post_tag: how-google-lied-to-the-public-and-manipulated-expectations, post_tag: mashable-google-falls-from-grace, post_tag: news-clippings-on-google, post_tag: ralph-nader-on-hostile-corporate-takeover-attempts-of-washington-dc, post_tag: the-google-case, post_tag: the-great-google-hack, post_tag: this-is-how-they-would-do-it, post_tag: what-does-google-do-with-consumers-deepest-secrets, post_tag: what-does-google-know-about-you, category: worldnews]

EVERY Server Has Been Broken Into!

- Any network with even a single Cisco, or Juniper Networks, device was "wide-open" to "any kid with a keyboard for last ten years"
- Hackers have "run amuck" through corruption records, political kick-back documents, Department of Energy files and background check files
- Agencies warned over eight years ago but refused to remove Cisco and Juniper hardware because of supplier kick-back deals
- Any Chinese hacker could get in "with ease, and very little skill"…
- HUGE implications for 2016 election revelations. Hacked campaign documents already rolling in…

(Mis)Uses of Technology

by Mike Masnick

Filed Under:
backdoors, **china**, **cybersecurity**, **privacy**, **russia**, **security**

Companies:
juniper networks

Permalink.

US Gov't Agencies Freak Out Over Juniper Backdoor; Perhaps They'll Now Realize Why Backdoors Are A Mistake

from the *wishful-thinking* dept

Last week, we wrote about how Juniper Networks had uncovered some unauthorized code in its firewall operating system, allowing knowledgeable attackers to get in and decrypt VPN traffic. While the leading suspect still remains the NSA, it's been interesting to watch various US government agencies totally freak out over their own networks now being exposed:

> *The FBI is investigating the breach, which involved hackers installing a back door on computer equipment, U.S. officials told CNN. Juniper disclosed the issue Thursday along with an emergency security patch that it urged customers to use to update their systems "with the highest priority."*
> The concern, U.S. officials said, ***is that sophisticated hackers who compromised the equipment could use their access to get into any company or government agency that used it.***
> One U.S. official described it as akin to ***"stealing a master key to get into any government building."***

And, yes, this equipment is used all throughout the US government:

> *Juniper sells computer network equipment and routers to big companies and to U.S. government clients such as the Defense Department, Justice Department, FBI and Treasury Department. On its website, the company boasts of providing networks that "US intelligence agencies require."*
> Its routers and network equipment are widely used by corporations, including for secure communications. Homeland Security officials are now trying to determine how many

> such systems are in use for U.S. government networks.

And, of course, US officials are insisting that it couldn't possibly be the NSA, but *absolutely must* be the Russians or the Chinese:

> *The breach is believed to be the work of a foreign government, U.S. officials said, because of the sophistication involved. The U.S. officials said they are certain U.S. spy agencies themselves aren't behind the back door. China and Russia are among the top suspected governments, though officials cautioned the investigation hasn't reached conclusions.*

Yeah, sure. Anything's possible, but the NSA still has to be the leading suspect here, and the insistence that it's the Chinese or the Russians without more proof seems like a pretty clear attempt at keeping attention off the NSA.

And, of course, all of this is happening at the very same time that the very same US government that is now freaking out about this is trying to force every tech company to install just this kind of backdoor. Because, as always, these technically illiterate bureaucrats still seem to think that you can create backdoors that only "good" people can use.
But that's not how technology works.
Indeed, now that it's been revealed that there was a backdoor in this Juniper equipment, it took one security firm all of six hours to figure out the details:

> *Ronald Prins, founder and CTO of Fox-IT, a Dutch security firm, said the patch released by Juniper provides hints about where the master password backdoor is located in the software. By reverse-engineering the firmware on a Juniper firewall, analysts at his company found the password in just six hours.*
> “Once you know there is a backdoor there, … the patch [Juniper released] gives away where to look for [the backdoor] … which you can use to log into every [Juniper] device using the Screen OS software,” he told WIRED. “We are now capable of logging into all vulnerable firewalls in the same way as the actors [who installed the backdoor].”

Putting backdoors into technology is a *bad idea*. Security experts and technologists keep saying this over and over and over and over again -- and politicians and law enforcement still don't seem to get it. And, you can pretty much bet that even though they now have a very real world example of it -- in a way that's impacting their own computer systems -- they'll continue to ignore it. Instead, watch as they blame the Chinese and the Russians and still pretend that somehow, when they mandate backdoors, those backdoors *won't* get exploited by those very same Chinese and Russian hackers they're now claiming were crafty enough to slip code directly into Juniper's source code without anyone noticing.

Permalink.

Blackberry CEO Gives Public One More Reason To Not Buy Its Phones By Arguing For Greater Law Enforcement Cooperation

from the *the-greater-good-is-apparently-whatever-the-government-says-it-is* dept

Blackberry's CEO John Chen feels the company hasn't hit rock-bottom yet. In a post for the company's blog, Chen announces that the phone favored by much of The Establishment will continue to support the hopes and dreams of The Establishment.

There will be no "going dark" at Blackberry.

Leaked Documents Expose The Cell Phone Surveillance System that listened in on crimes that Google executives, owners and VC's may have committed while rigging campaigns and policy decisions

from the *and-they-are-legion-(and-expensive)* dept

The Intercept has done it again. An anonymous source "concerned about the militarization of domestic law enforcement" has handed the site a catalog of cell phone surveillance equipment. Many of the products discussed in the pages are making their public debut, presumably to the deep chagrin of the manufacturers and the government agencies that use them.

While much of the equipment's capabilities has been sussed out with FOIA requests and the occasional courtroom disclosure, the leaked documents confirm that many law enforcement agencies not only have the technology to sweep up cell phone information in bulk, but also to intercept phone calls and text messages.