EVERY State and Federal Server Has Been Broken Into!

Mon, 21 Dec 2015 15:12:11, admin45789, [post_tag: cisco-bacxk-door, post_tag: every-state-and-federal-server-has-been-broken-into, post_tag: hot-crime-topics, post_tag: juniper-networks-backdoor, category: news, post_tag: state-of-california-servers-hacked]

EVERY State and Federal 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

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.

Hillary Clinton Wants A 'Manhattan Project' For Encryption... But Not A Back Door. That Makes No Sense
from the politics-is-dumb dept
In the Democratic Presidential debate on Saturday night, Hillary Clinton followed up on her recent nonsensical arguments about why Silicon Valley has to "solve" the problem of encryption. As we've noted, it was pretty clear that she didn't fully understand the issue, and that was even more evident with her comments on Saturday night.

Here's what's clear: she's trying to do the old politician's trick of attempting to appease everyone with vague ideas that allow her to tap dance around the facts.

First, she proposed a "Manhattan-like project" to create more cooperation between tech companies and the government in fighting terrorism. The Manhattan Project was the project during World War II where a bunch of scientists were sent out to the desert to build an atomic bomb. But they had a specific goal of "build this." Here, the goal is much more vague and totally meaningless: have tech and government work together to stop bad people. How do you even do that? The only suggestion that has been made so far -- and the language around which Clinton has been echoing -- has been to undermine encryption with backdoors.

However, since that resulted in a (quite reasonable) backlash from basically anyone who knows anything about computer security, we get the second statement from Clinton that she doesn't want backdoors.
"Maybe the back door isn't the right door, and I understand what Apple and others are saying about that. I just think there's got to be a way, and I would hope that our tech companies would work with government to figure that out."
No, she clearly does not understand what Apple and others are saying about that. Just a week or so ago, she insisted that Apple's complaint about it was that it might lead to the government invading users' privacy, but that's only a part of the concern. The real concern is that backdooring encryption means that everyone is more exposed to everyone, including malicious hackers. You create a backdoor and you open up the ability for malicious hackers from everywhere else to get in.

So, she's trying to walk this ridiculously stupid line in trying to appease everyone. She wants the security/intelligence officials to hear "Oh, I'll get Silicon Valley to deal with the 'going dark' thing you're so scared of," and she wants the tech world to hear "Backdoors aren't the answer." But, that leaves a giant "HUH?!?" in the middle.

It seems to come down to this: None of the candidates for president appear to have the slightest clue how encryption or computer security work and that allows them to make statements like this that are totally nonsensical, while believing that they make sense.

The issue, again, is that what they're really asking for is "Can you make a technology where only 'good' people can use it safely, and everyone else cannot?" And the answer to that

question is to point out how absolutely astoundingly stupid the question is. Because there's no way to objectively determine who is "good" and who is "bad," and thus the only possible response is to create code that really thinks everyone is "bad." And to do that, you have to completely undermine basic security practices..

So this whole idea of "if we just throw smart people in a room, they'll figure it out" is wrong. It's starting from the wrong premise that there's some sort of magic formula for "good people" and "bad people." And without understanding that basic fact, the policy proposals being tossed out are nothing short of ridiculous.

Collapse
Privacy
by Tim Cushing
Filed Under:
catalog, cia, leak, nsa, phones, police, police militarization, surveillance

Permalink.
Leaked Documents Expose The US Government's Cell Phone Surveillance Options
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.

There is also a long list of newly-exposed product names that will be making their way into a host of future FOIA requests: Deerpark, Radiance, Carman, Garuda, Gilgamesh, Twister, Nebula…

Interesting (and disturbing) details are contained in data sheets on the products, including what the government feels are the potential drawbacks of the equipment. Harris' Blackfin, for instance, can intercept GSM voice communications as well as SMS messages from "preloaded target lists." In addition, the Blackfin can perform denial-of-service attacks on local phone networks and geolocate targeted phones. Perhaps the biggest surprise? The Blackfin is small enough to be worn surreptitiously by the operator.

Digital Receiver Technology, manufacturer of the US Marshals Service's flying "DRTboxes," also has some impressive technology on display. Its equipment supports "target lists of up to 10,000 entries" and can intercept (and record) voice communications over both digital and analog signals.

KeyW sells a product that tracks locations of cell phone users, targeting up to 500 cell phones at a time. Bonus: it can also negatively affect GSM networks to better track targets. (Referred to on the item's page as "Deny, Disrupt, Degrade and Deceive.")

Then there's this device, which is apparently an "in-house" offering produced by the NSA's Tailored Access Operations team.

This little spy box is built for use in "fixed-wing aircraft," like the FBI's Cessnas or unmanned drones. Bonus: it can be upgraded in the field, which presumably means firmware/software updates can be pushed to the system remotely.

Other notes of interest:

The government considers Deerpark's inability to wreak havoc on phone service a drawback ("does NOT cause denial of service").

The NSA-developed Nebula can "lock and hold traffic from 12 miles away."

AST's airborne ICARUS can geolocate Push-To-Talk handsets and RF tags.

Boeing's S-100 helicopter drone's fact sheet contains the warning that it cannot be armed with weapons.

This page shows just how low-profile some of this cell phone tracking hardware is.

Or, if it makes more sense logistically, you can just cram $180k worth of tracking equipment into a backpack.

Most of the pages note what authority is needed to deploy the equipment, with most citing Title 10/Title 50. The statutes pertain to military operations (Title 10) and military intelligence efforts (Title 50), with the latter sometimes encompassing the CIA's efforts. However, the documents contain fact sheets for equipment now being used by US law enforcement agencies, suggesting the transfer to domestic surveillance use occurred before law enforcement-specific rules were in place. The years of secrecy surrounding the devices further suggest domestic guidance trailed deployment by a sizable margin.

Finally, there are the forensic devices. The NSA SigDev team's CYBERHAWK basically cracks cell phones open and empties them of their contents.

"Exploitation includes phonebook, names, SMS, media files, text, deleted SMS, calendar items and notes."
The only drawback is that the operator must have possession of the handset to extract all of this information. It can't be collected "over the air." A competing product offered by TEEL (Cellbrite) does the same thing, but works on "95% of phones," encompassing more than the GSM handsets CYBERHAWK is limited to.

The obvious problem is we don't know how much of this military equipment has ended up in the hands of law enforcement. We do know most of Harris' products have, thanks to the waiver it acquired (by lying) from the FCC. We also know Digital Receiver Technology is, at minimum, selling its products to federal law enforcement.

Local law enforcement agencies are using equipment developed for military use in war zones as domestic surveillance devices. When seeking these products (or the financial aid to acquire them), law enforcement agencies routinely mention the threat of terrorism… before using them to track people suspected of petty crimes. As the EFF's Jennifer Lynch points out in The Intercept article, there is no public record of any law enforcement agency using these devices to apprehend a terrorist or disrupt a terrorist attack.

Federal agency policies pertaining to these devices now contain warrant requirements, but with large enough loopholes, warrants will rarely have to be sought. The rules governing the use at the local level are still mostly secret. What has been divulged suggests agencies are still obscuring the use of the devices through the use of parallel construction or stretching pen register statutes to cover the large scale interception of connection and location data and, potentially, the communications themselves.

Secret Code Found in Juniper's Firewalls Shows Risk of ... - Wired
cached
2 days ago ... Encryption backdoors have been a hot topic in the last few years—and the ... On Thursday, tech giant Juniper Networks revealed in a startling ...
google
http://www.wired.com/2015/12/juniper-n[...]show-the-risk-of-government-backdoors/
Juniper Networks backdoor confirmed, password revealed, NSA ...
cached
7 hours ago ... Juniper Networks makes a popular line of enterprise firewalls whose operating system is called Screen OS. The company raised alarm bells ...
google
https://boingboing.net/2015/12/21/juniper-networks-backdoor-conf.html
What's Juniper Networks to do? | Network World
cached
As soon as Ericsson and Cisco announced their strategic partnership on Monday, Juniper Networks' stock plummeted. Juniper was down over 8% on Monday …
bing
http://www.networkworld.com/article/30[...]bnet/whats-juniper-networks-to-do.html
Juniper Networks finds backdoor code in its firewalls - Engadget
cached
3 days ago ... Juniper Networks found a backdoor inserted in its firewall software.
google
http://www.engadget.com/2015/12/17/jun[...]-finds-backdoor-code-in-its-firewalls/

What is back door? - Definition from Whatls.com
cached
A back door (sometimes called a trap door) is a means of access to a computer system that bypasses security mechanisms.
bing
http://searchsecurity.techtarget.com/definition/back-door
“Unauthorized code” in Juniper firewalls decrypts encrypted VPN ...
cached
3 days ago ... Backdoor in NetScreen firewalls gives attackers admin access, VPN ... sold by Juniper Networks contains unauthorized code that surreptitiously ...
google
http://arstechnica.com/security/2015/1[...]ewalls-decrypts-encrypted-vpn-traffic/
FBI, DHS investigating Juniper hack; secret backdoor dates back 3 ...
cached
1 day ago ... The Department of Homeland Security and the FBI are reportedly investigating the 'rouge code' in Juniper Networks products which could ...
google
http://www.networkworld.com/article/30[...]ecret-backdoor-dates-back-3-years.html
Catalog Reveals NSA Has Back Doors for Numerous …
cached
Dec 29, 2013 · After years of speculation that electronics can be accessed by intelligence agencies through a back door, an internal NSA catalog reveals that such …
bing
http://www.spiegel.de/international/wo[...]ors-for-numerous-devices-a-940994.html
Juniper Networks "backdoor" computer hack may have put ...
cached
3 days ago ... The flaw was discovered Thursday in software called ScreenOS, from Juniper Networks, which enables VPN (virtual private network) ...
google
http://www.cbsnews.com/news/juniper-te[...]ack-could-put-government-data-at-risk/
US Gov't Agencies Freak Out Over Juniper Backdoor; Perhaps They ...
cached
5 hours ago ... Last week, we wrote about how Juniper Networks had uncovered some unauthorized code in its firewall operating system, allowing ...
google
https://www.techdirt.com/articles/2015[...]ealize-why-backdoors-are-mistake.shtml
Juniper Finds Backdoor that Decrypts VPN Traffic - Threatpost
cached
3 days ago ... Juniper Networks has removed "unauthorized code" capable of decrypting VPN traffic that it found in ScreenOS, which runs its enterprise ...
google
https://threatpost.com/juniper-finds-b[...]door-that-decrypts-vpn-traffic/115663/
Juniper Finds Backdoor In NetScreen Firewalls, Possibly Already ...
cached
3 days ago ... Juniper Networks announced that its ScreenOS operating system, which is used to manage NetScreen firewalls sold by the company, was ...
google
http://www.tomshardware.com/news/junip[...]rks-finds-screenos-backdoor,30786.htm