The Great GOOGLE Hack! A Tsunami Of Sadness For Eric Schmidt

Fri, 08 Jan 2016 16:00:00, newstips66, [category: brotopia, post_tag: consumer-complaint-song, post_tag: covert-google-operative-discusses-tactics-while-working-for-eric-schmidts-iqt, category: elon-musk, category: energy-dept-slush-fund, category: google-alphabet, post_tag: google-defamation-documents, post_tag: google-sex-scandal, category: idea-theft, category: lithium-batteries, post_tag: news-clippings-on-google, category: sony_pictures, category: stanford_univ_bribes, post_tag: the-google-case, post_tag: the-great-google-hack-a-tsunami-of-sadness-for-eric-schmidt, post_tag: valleybeat-why-google-is-the-new-evil-empire, post_tag: what-becomes-of-a-consumers-private-data-when-they-use-google, post_tag: what-does-google-do-with-consumers-deepest-secrets, post_tag: what-does-google-know-about-you, category: worldnews]

The Great GOOGLE Hack! A Tsunami Of Sadness For Eric Schmidt

By Ellen K and Tom L.

It is now commonly reported in the news that The White House ordered the NSA to order Cisco, Juniper Networks and other network providers to put spy back-doors into their equipment so that officials could cull any communications that indicated potential criminal terrorist activity.

Catching epically huge criminals is, generally, considered to be a good thing, by the majority of the public. Spying on the public in order to control votes and ideology is, almost entirely, frowned upon by the public.

There is a strange twilight zone in-between those concerns. What if an epically huge organization was doing bad criminal things in order to control the votes and ideology of the public. That would be: **GOOGLE.**

It is also commonly reported in the news that Chinese, Russian and entrepreneurial hackers got the “keys” to Cisco's, Juniper Networks, and most of the other back-door'd server companies gear. They came in to the top Fortune 2000 companies and spent over a decade taking everything. They swept through the U.S. Department of Energy over 300 times. They took EVERY background check file the U.S. government has produced. They got into the White House, The CIA and … everything.

At the same time the Chinese, and entrepreneurial dark web independent hackers, went on a shopping spree through every R&D department of every defense company and Silicon Valley company that had interesting technology. They Hoover-ed up the keys to the kingdoms.

Cisco and Juniper Networks executives are now known to have fully cooperated in the placing of these back-doors in their customers products. History has proven that the back-doors had high-school level security which any good hacker could crack in less than an hour. John Chamber's has left Cisco at the same time this was discovered. In a few years, you can expect hundreds of billions of dollars of lawsuits over this, from companies who lost everything because their security supplier sold them swiss cheese security hardware. Typical daily news revelations now include stories such as this:

reuters2

Related: Tech

Juniper Networks will drop code tied to National Security Agency

SAN FRANCISCO | By Joseph Menn

[caption id="attachment_272" align="alignnone" width="461"] A National Security Agency (NSA) data gathering facility is seen in Bluffdale, about 25 miles (40 km) south of Salt Lake City, Utah, December 16, 2013. Jim Urquhart/REUTERS[/caption]

Juniper Networks Inc said late on Friday it would stop using a piece of security code that analysts believe was developed by the National Security Agency in order to eavesdrop through technology products.

The Silicon Valley maker of networking gear said it would ship new versions of security software in the first half of this year to replace those that rely on numbers generated by Dual Elliptic Curve technology.

The statement on a blog post came a day after the presentation at a Stanford University conference of research by a team of cryptographers who found that Juniper's code had been changed in multiple ways during 2008 to enable eavesdropping on virtual private network sessions by customers.

Last month, Sunnyvale-based Juniper said it had found and replaced two unauthorized pieces of code that allowed "back door" access, which the researchers said had appeared in 2012 and 2014.

The 2014 back door was straightforward, said researcher Hovav Shacham of the University of California, San Diego, allowing anyone with the right password to see everything.

The 2012 code changed a mathematical constant in Juniper's Netscreen products that should have allowed its author to eavesdrop, according to Shacham and his fellow investigators.

Juniper's initial patch had gotten rid of that constant in Dual Elliptic Curve and replaced it with the version it had been using since 2008.

But the academics who studied the code said that while Juniper had not disavowed the 2008 code, it had not explained how that constant was picked or why it was using the widely faulted Dual Elliptic Curve at all.

Still another curve constant, quietly provided by the NSA and required for some federal certification, was exposed in documents leaked by former NSA contractor Edward Snowden as a key to the back door.

Until now, the most influential adopter of Dual Elliptic Curve was believed to be RSA, part of storage company EMC, which Reuters reported received a $10-million federal contract to distribute it in a software kit for others.

Though the academic team looking at Juniper has not named a suspect in the 2008, 2012 or 2014 changes, 2008 was one year after veteran cryptographers raised questions about Dual Elliptic Curve.

A very advanced adversary could have seen how to manipulate Dual EC and in theory managed to insert code through a cooperative or unsuspecting Juniper employee, but the company had not advertised the fact that it was using the formula at all.

A more logical suspect, said expert Nicholas Weaver of the International Computer Science Institute, was the NSA, which might have been displaced later by other countries' agencies or top-level hackers in 2012 and 2014.

The NSA did not immediately respond to an emailed request for comment.

Juniper said it was continuing to investigate. here

It declined to answer questions from Reuters about the revisions.

(Reporting by Joseph Menn; Editing by Clarence Fernandez)

So the spy stuff is out. The back-doors were/are there. They were poorly secured. They cost U.S. companies trillions of dollars in information and competitive market losses. But; this is not the end of the story.

Google has been facing, and losing, an escalating number of abuse lawsuits. Wouldn't it be great if those who are suing Google, for using their global architecture to abuse and attack, people, had copies of Eric Schmidt's emails and text messages saying “Go wipe him out, use the entire Google network to turn him, and his company, into dirt..”?

That may be about to happen.

Since before 2008, Google investors, executives, contractors and owners have had all of their email and business information on network systems which were run by Juniper and Cisco network hardware. It only takes a SINGLE Cisco or Juniper device to let you inside of an entire corporate network. Ask Sony! Even though IT experts warned Google that “we might have a problem”, the thought of finding, and pulling out, every single Juniper and Cisco hardware device, in every building and email system, was more than the Google finance people could wrap their heads around. Short term profit greed overcame long term vision.

So the great Google Hack happened.

A huge number of people and organizations hate Google. Many would have just plundered Google for pure revenge and spite.

The Chinese, Russian, Anonymous, Lizard Squad, North Korean, Guccifer-like and weird Ukrainian bored 14 year old contingent went on a rampage throughout Google, Google's partners, Google's investor's and anybody that an interesting Google executive had emailed or Google-voiced to.

Want to read an email between the notorious Kleiner Perkin's Cartel boss John Doerr and Eric Schmidt plotting a campaign financing scam? Just post the dates of the email sets that you want on 4Chan, or some other dark web site, and you will get a price quote from a Chinese or Estonian IP address. The files will show up on GitHub 48 hours after you send your Bitcoin payment. These state-class hackers have set up a mall-type commerce system to sell all of the info they scooped up.

Google has often felt like they were untouchable because they controlled Eric Holder, Half the White House, The U.S. Patent Office, The FCC and had paid off half of Congress and the California Senate. Holder is gone. Snowden happened. More leaks are coming. Russia, China, the entire EU, the Cable and Wireless industry, the GOP, and many others have gone to war against Google, advertisers are running to the hills and Google is hated by more and more of the world.

Anything, that any law enforcement or litigation investigator finds on-line is fair game. Hackers even have “Chinese take out” menus of information sets:

Hillary emails $220,000.00 US

Eric Schmidt divorce emails $80,000.00 US

Brin Sex Scandal sexy texts and emails with Google Glass girl $71,000.00 US

The truth is out there. It is in a little apartment in Beijing. It is in a trailer in Minsk. It is in a warehouse in Sao Paolo. In most cases, it only took a 22 year old with a laptop to gut the biggest darkest, spookiest secrets of the biggest Internet company in history. How could one or two of these kids scour through millions of pages of Google documents? *Microsoft File Search* tools, left running all night, help the hacker kiddies plow through reams of material by simply putting the keyword “campaign funds”, “antitrust”, “Musk”, or other interesting phrases, in the search fields.

Google's “don't do evil” motto turned out to be the exact opposite of what Google actually did do. Their billions, their hubris, and their immorality without consequence, left Google feeling like it was above the law. Now, the reality will dawn on Google. The law has a long arm!

How Do Back Doors Work?

Hacking Corporate and Political emails, and servers just became as easy as sliced pie

- Every Political candidate paying “Opposition Researchers” for hacked secrets on the other candidates

- NO MORE SECRETS may even be possible due to wide-open back-doors with the poorest security in the world

Let me tell you that almost every day of the year, it's been a complete and unmitigated disaster for security. Encryption is used by banks to keep your money safe, it's used by government to keep its secrets safe, and it's used by companies to protect your data. But despite being the very fabric of keeping society and the internet safe and secure, encryption has been threatened by far too many narrow-minded bureaucrats with little knowledge or foresight to the consequences of its unraveling, who are paid by businesses to act as proxy spokespeople on their behalf for the trade-off of staying in power.

Encryption. It's become the hot topic of the year, with sides both for and against fighting for their heartfelt belief. The security community has consistently had to fight to be heard, knowing their views will be unlikely to influence policy, because they are -- sadly -- people without a badge or an embossed business card, or an office on the Washington DC political mile.

FBI director James Comey has called on companies to use encryption backdoors, so much so he's promised he's not a "maniac" about it. Senate intelligence committee chair Richard Burr called encryption a "big problem out there that we are going to have to deal with," despite also saying that it likely wasn't used in the Paris terrorist attacks, or more recently, the shooting in San Bernardino. And Britain, on the other side of the pond, is pushing for counter-encryption legislation, which may force companies to weaken or ditch encryption at the behest of the government.

All too often, the encryption debate has been driven by the ill-informed media citing unnamed and anonymous US intelligence officials, who by virtue of their jobs have a biased stances. And yet some of those media outlets also called the Juniper firewall backdoor code discovery akin to "stealing a master key to get into any government building."

In the case of Juniper, it really is that bad. The networking equipment maker, with thousands of enterprise customers, said last week it had found "unauthorized" code that effectively allowed two backdoors to exist for as long as three years. Nobody disputes that this was a backdoor. Juniper said it had no evidence to suggest the backdoor had been used, but also warned there was "no way to detect" if it had been.

The NSA was blamed for creating weakened cryptography that Juniper went on to modify -- and badly. Exactly how the other backdoor got there remains a big question. In any case, companies who were running affected versions of Juniper's firewalls were likely also targets of the suspected nation state attacker.

Juniper's clients also include the US government, including the Defense Dept., Justice Dept. and the FBI, and the Treasury Dept., reports The Guardian, which may put federal government data at risk.

If ever there's been a shining example of why government backdoors are a bad idea, the motherlode just got served up hot on a platter.

The Juniper breach is by far the best example of why backdoors in any products, services, or technology is a bad thing. Once the backdoors were found, it took just three days for the master password used in the backdoor to be posted online, sparking open season for any hacker to target a Juniper firewall.

If whoever planted the backdoor was non-American, it highlights the point the security community has been making for months: these backdoors can and will be used and abused by the enemy.
