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

Wed, 23 Dec 2015 16:00:00, admin45789, [post_tag: and-servers-just-became-as-easy-as-sliced-pie, post_tag: hacking-corporate-and-political-emails, post_tag: hot-crime-topics, post_tag: juniper-networks-back-door, post_tag: juniper-networks-hack, category: news]

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

- US Patent Office taken off-line by hack?

- 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

REDDIT AND VOAT reveal extent of the incursions:

-

(Image: file photo via CBSNews.com)
Aaron Sorkin may not be a household name, but you've probably heard of his work. From "The West Wing" to "The Social Network," and "Studio 60 on the Sunset Strip," and "The Newsroom," Sorkin has dedicated the name of one episode in each of his productions to asking the same question:
"What kind of day has it been?"

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.