Should Use of Cross Border Ransomware be Considered an Act of Economic Warfare by the US Government?

May 11, 2021 - In case you haven't been paying attention, within the past few days the Colonial Pipeline Co. was hit with a ransomware attack that shut down its pipeline system on East Coast of the United States. The attack is causing fuel shortages up and down the East Coast, and forcing fuel prices to rise. It is widely believed that the group behind the attack - known as the DarkSide - operates out of Russia. That's because the software they use is setup to avoid targeting companies with Russian language websites. While the Russian government isn't believed to be directly involved with the DarkSide, they aren't exactly rushing to arrest its members either. This begs the very real question: Should the United States hold the Russian government responsible for the attack and take appropriate measures against them? And should we do the same with other governments, such as China?

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];

s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Malware and ransomware aren't anything new. Computer experts have been issuing warnings for years about the potential to disrupt or disable critical American infrastructure via the internet. Until this week, those discussions were largely academic. Hypothetical situations that were only discussed in geek-circles. The attack on Colonial changes that. We aren't talking about a hypothetical situation any longer.

While it is believed that the group behind this attack resides in Russia, that is far from the only problem country involved in cybercrime. Both North Korea and China have dedicated considerable resources to committing cyber warfare against the US and its allies. And they've often been successful in their efforts. China has been behind some major hacks of US Government systems including an attack on the Office of Personnel Management and North Korea actually launched a cyber-attack against Sony Studios when the company released a movie that the North Korean Government didn't approve of.

While these sorts of attacks may not result in loss of life, they certainly cause economic damage that can be as great or greater than that which would be inflicted by an actual military campaign. Yet, to date, the US Government's response to this kind of behavior has been tepid at best.

With regard to the attack on Colonial, President Biden has talked about American efforts to guard critical infrastructure. His statement pretty well made that the responsibility of American businesses. He also talked about trying to bring the criminals behind the attack to justice; something that isn't too likely to happen when you consider that the United States doesn't have an extradition treaty with Russia. But he said almost nothing about holding the Russian government

accountable. In fact he went out of his way to say that the US had "...no evidence from our intelligence people that Russia is involved...". While he did say that he thought the Russian government had a responsibility to deal with the issue, he didn't mention any consequences if they don't.

The United States is arguably the largest consumer economy in the world. On a per capita basis, there is no doubt that the US is the largest economy. It's time for the US to use that market power. Whether countries actively participate in cyber attacks on the United States, or passively allow their residents to do so without any consequences, the results here are still the same. It is time that those countries feel some pain. And the easiest way to inflict that pain is to deny them access to American consumers. Kick them out. If we don't, the next attack could be far worse; impacting things like the electric grid, water systems and even nuclear power plants. And if that happens, cyber attack or not, Americans will wind up dead.

This approach would do a couple of things. First, it would force American companies to manufacture their goods in countries that weren't anti-American. It might even get some of them to bring their manufacturing back home. Secondly, it would cut off a major source of funding to governments that are anti-American.

There is no doubt that such an approach would cause some disruption in daily life here. After all, there probably isn't a household in the United States that can say that it doesn't have some products that were manufactured in China. And there are some products that are probably not manufactured anywhere else. But if those products are actually in demand, the disruption would only be short term as manufacturers and suppliers shift their supply chain.

It remains to be seen if the Biden administration has any appetite for this type of confrontation. So far though, the indication is that it doesn't.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS