Colonial Pipeline Co Back In Business after Paying Ransom

May 14, 2021 - After the much ballyhooed cyberattack on Collonial Pipeline shut down the movement of petroleum products on much of the US East Coast, gas stations began to run out of fuel. One station in Virginia reportedly raised the price of a gallon of fuel to $6.99 in a matter of hours and gas lines have become common. So there was a lot of pressure on the company to get their operations back to normal. Since the attack on the company was all about extortion - their files became encrypted due to ransomware - the easiest thing to do was for them to make payment. And that is just exactly what they did. $5 million to be exact. But that raises a couple of significant questions. First, was the payment legal? And second, will the federal government do anything about it?

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);
})();

According to a declaration made late last year by the Treasury Department, Colonial's payment may very well have been illegal. In October of last year, Treasury's Office of Foreign Asset Control (OFAC) made an official announcement that making ransomware payments is illegal. (If you click on the link, you'll see the announcement on Treasury's website.) Based on the wording of the Treasury's declaration, both Colonial and any financial institutions involved in the payment probably broke the law.

The reason that the federal government is attempting to shut down ransomware payments is that the money typically goes to governments and organizations that pose national security threats. Monies paid to them allow them to continue to operate; something that the United States would very much like to prevent.

But in the case of the Colonial attack, it is highly unlikely that the government will do anything about the payment. To say the least, the shutdown of Colonial's pipeline system has been politically inconvenient and created substantial problems for both the voting public and the government. Anyone who was alive during the gas shortages of the late 1970's can tell you that those shortages, fuel price increases and lines at gas stations had a huge impact on the 1980 elections; one that the current administration is unlikely to want repeated.

The fact is that Treasury's proclamation on the legality of ransomware payments is probably more wishful thinking that anything else. When it comes to attacks against critical infrastructure such as the Colonial pipeline, it isn't in the governments interest to stop companies from making payments when preventing them would infuriate voters. And that will remain the case until the federal government takes strong action against any government that participates in this type of action or harbors those to do.

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