Victims of Ransomware Attacks May Incur Federal Penalties if They Choose to Pay

October 7, 2020 - Victims of ransomware are confronted with a choice. Make payment to the criminals behind the attack in order to regain access to their computer files, or choose not to pay and face the risk of having their businesses be damaged or shut down entirely. Not a pleasant prospect under any circumstances, and it is really no wonder that many businesses choose to make the payment. But now, there is a new threat. Two offices in the Treasure Department - The Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCIN) - have issued a joint advisory. It warns victims and anyone aiding them in making payment (including banks and other financial institutions) that paying a ransom may get them into hot water with the federal government.

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);
})();

OFAC and FinCIN deal with different areas of the law, but they are both concerned with making illegal payments; especially to overseas entities. These payments are often going to accounts that are difficult or impossible to trace. And they may be going to terrorists or other sanctioned entities. Additionally, ransomware has become a major financial issue for the country and American businesses. Part of the impetus behind the advisory is likely the fact that allowing ransomware payments to continue unhindered only inspires other bad-actors to engage in this crime.

The intermediaries that assist companies and individuals in making ransomware payments have certain obligations under federal law. Anyone choosing to make a ransomware payment on their own also has those obligations. Among these are requirements that they check with the federal government first to ensure that payments are not being made to entities or individuals that are sanctioned by the United States. That's something that can be difficult for organizations that are setup to make payments, and which can be nearly impossible for individuals making payments on their own.

In the case of financial institutions that help to facilitate these types of transactions, there are also obligations to report suspicious financial activities to the government.

The bottom line here is that the US Government appears to be determined to significantly reduce ransomware payments. Unfortunately for victims, the advisory clearly spells out that they may get squeezed in the process. If you don't make payments, you lose access to your computer information. If you do, you could face fines or worse from the federal government.

It is impossible to say how all of this will play out in the long run, but anyone who finds themselves with a ransomware predicament would be well advised to check with an attorney before making any payments. Making the wrong decision could be akin to going from the frying pan into the fire.

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