

Paying ransomware demands could land you in hot water with the feds

reader comments

104 with 68 posters participating

Share this story

Businesses, governments, and organizations that are hit by crippling ransomware attacks now have a new worry to contend with—big fines from the US Department of Treasury in the event that they pay to recover their data.

Treasury Department officials made that guidance official in an advisory published on Thursday. It warns that payments made to specific entities or to any entity in certain countries—specifically, those with a designated “sanctions nexus”—could subject the payer to financial penalties levied by the Office of Foreign Assets Control, or OFAC.

The prohibition applies not only to the group that is infected but also to any companies or contractors the hacked group’s security or insurance engages with, including those who provide insurance, digital forensics, and incident response, as well as all financial services that help facilitate or process ransom payments.

Enabling criminals

“Facilitating a ransomware payment that is demanded as a

result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims,” the advisory stated. “For example, ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom to cyber actors does not guarantee that the victim will regain access to its stolen data.”

Under law, US persons are generally prohibited from engaging directly or indirectly in transactions with people or organizations on the OFAC’s Designated Nationals and Blocked Persons List, other prohibited lists, or in Cuba, Iran, North Korea, and other countries or regions. In recent years, the Treasury Department has added several known cyber-threat groups to its designation list. They include:

To pay or not to pay?

Law enforcement officials and security consultants have generally advised against paying ransomware demands because the payments only fund and encourage new attacks. Unfortunately, paying the ransom is often the fastest and least-expensive way to recover. The City of Baltimore incurred a loss of more than \$18 million after it was locked out of its IT systems. Attackers behind the ransomware had demanded \$70,000. In response, some companies claiming to offer incident-response services for ransomware attacks simply pay the attackers.

Thursday’s advisory didn’t say that people are prohibited in all cases from paying ransoms.

“Under OFAC’s Enforcement Guidelines, OFAC will also consider a company’s self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant

mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

Thursday's advisory warned that there are other reasons not to pay. It further explained that the prohibitions against ransom payments are broader than many people may assume. Fines may be levied against any US person who, regardless of location, engages in a transaction that causes a non-US person to perform a prohibited action. The OFAC may also impose civil penalties based on "strict liability," a legal principle that holds the person or group liable even if they didn't know or have reason to know they were engaging with someone who's prohibited under the sanctions laws.

"As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations," the advisory stated. "This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services."

The advisory went on to say that people won't be penalized in all cases for paying ransoms. In some cases, victims can receive a dispensation in advance for paying a ransom. In other cases, infractions may be excused or mitigated.

"Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a

sanctions nexus,” officials wrote. “OFAC will also consider a company’s full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.”

Post updated to add the last two paragraphs.

<https://arstechnica.com/?p=1711128>