- Crypto Ransomware has become a notable concern
- Over the last year, the count of such Ransomware attacks have surged by more than 300%
- US OFAC has issued a notice noting three major points to to stop such activities
- Bitcoin ATM's hardware and software are found vulnerable and requires to be resolved soon

Crypto Ransomware attacks count has continued to rise, as prices in the cryptocurrency market. Over the past couple of years, we have noted that these categories of attacks have increased, and the illicit actors are asking for cryptocurrencies as ransom amounts. According to the recent report published by Chainalysis, it has been revealed that such attacks have surged by more than 300% over the past year and a half. Notably, such e attacks have shown no signs of slackening since the beginning of this year. The complete scenario has forced the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) to take additional estimates

OFAC shows crypto Ransomware concerns

Crypto Ransomware Payments have evolved into sophisticated and aggressive forms of malware. These attacks are shutting the network and systems down until the victim pays off a good amount in crypto assets. Recently the OFAC has issued an updated advisory. Notably, OFAC highlighted the sanction risks associated with making ransomware payments. Moreover, the agency suggested some remedies to determine the future of cyber-extortion attacks.

Recent ransomware attacks have shut down public transportation, which is one of the largest fuel pipelines in the United States. Moreover, the attackers have stolen the private data of more than 40 million individuals. A ransomware tracker data reveals that more than 20 major cyber-attacks take place each month on an average.

How will OFAC address such a rising issue?

To address the rising issue, the OFAC has updated its ransomware advisory. Indeed, the authority has focused on three major points. First, the authority reiterated that it is strongly prohibited for companies to pay ransoms. Moreover, OFAC observed that no victims of such attacks should facilitate such payments, as it would encourage the malicious actors to violate the United States sanctions.

Secondly, the authority insisted that the firms should revisit their security measures. Undoubtedly, it is necessary to make sure that the practices are up-to-date.

And the last point is that the organizations and corporations are obliged to report and cooperate with the agency and other similar authorities. Indeed, the updated advisory notes meaningful steps to reduce the risk of extortion. Moreover, such norms will be considered as an essential mitigating factor in any

enforcement response.

BTC ATMs are loaded with vulnerabilities

Besides this crypto Ransomware concerns, it has been noted that Bitcoin ATMs are also vulnerable. The officials have highlighted the requirement for additional securities measures. Hence, they have found that such ATMs are stacked with numerous vulnerabilities. Notably, a recent study by the Kraken Security Labs unbeils that a specific model of such ATMs that are dubbed as GBBATM2, possess multiple hardware and software loopholes. However, if we consider that the industry will soon witness massive growth, such issues should be addressed.

Source: **Crypto Ransomware payments soaring crossed $400M**