**Ziggy Ransomware Gang Offers Refund to Victims**

**Reporter** Priyansha Sharma

**Description**

**The Ziggy ransomware gang announced in early February they were getting out of the cybercrime business. Now they say they’re ready to refund victim’s money.**

**Anyone who paid the ransom to Ziggy just needs to shoot them an email with proof of payment calculated in Bitcoin and the Computer ID. After that , the money will be returned to the bitcoin wallet in about two weeks, according to Bleeping Computers,who spoke to Ziggy’s Administrator.**

**Threatpost reached out to the Ziggy admin and received a response: “Hello dear. Yes, I’m Ziggy ransomware developer. We decided to return victims money because we fear law-enforcement action.”**

**Consciousness Arose among the Ransomware Operators**

Ziggy operators apparantely decided to stop their cybercrime business in February soon after the law enforcement came into action against similar ransomware group i.e., Emotet, Trickbot and Netwalker.

Ziggy ransomware admin leaked a SQL file containing 922 decryption keys along with a decryptor and source code on 7th of February. They even shared their file with ransomware expert Michael Gillespie, who in turn created a free decryption tool for the ziggy victims to unlock their files.

However, Experts have noted that Ziggy will still be able to make a profit from its action by manipulating fluctuation in the value of Bitcoin. The deal made by Ziggy was, they will refund money based on the value of Bitcoin on the date the payment was made. For example –the day ziggy released the decryption keys, the exchange rate for bitcoin was about 1BTC to $39000, the next day Bitcoins value spiked to just $59000 per BTC. This ultimately helped the Ziggy operators with tidy profit even while returning the money.

In their statement to threatpost, they claimed they were selling their homes to afford the refunds. “I’m going to be ransomware hunter. We have some ideas to create other ransomware(s) decryption tools. There is some ways to recover PHOBOS ransomware victims files without paying money and now I’m working on PHOBOS ransomware free decryption tool. Just looking for a job.”

**RIP: Ziggy, Fonix,Emotet**

Ziggy is not alone in calling off their ransomware activities, Fonix said they too were switching sides and had come to a conclusion to use their abilities in a positive way to help others.

A subsequent tweet included an apology and a pledge to launch a site to analyze malware and to make up for their mistakes.

Atleast we have special apology for all infected system users.To make up for our mistakes we will soon launch a malware analyze website soon to use our abilities in positive way.

“We cannot despair of humanity, since we ourselves are human beings.”

Large scale police operation have not only disrupted Emotet in late January but they even took the Netwalker’s Dark Web leaks site down. After the demolition of Emotet ,Trickbot took its place along with Qakbot and Ryuk ransomware.

Whatsoever the reason it is, Ransomware affiliates are getting out of the business now.

While large ransomware operations such as Clop, Sodinokibi and Darkside are unlikely to be discouraged from continuing the launch attacks, the recent arrests will make the cybercriminals think twice before becoming a ransomware affiliates.

Ivan Righi(an analyst with digital shadow) added unlocking victims files won’t mitigate the harm done to their businesses. “However Ziggi may return the ransom payment they received, this won’t fulfill the damage done to the victims who suffered lengthly downtimes due to their operations and are unlikely to recover completely from their losses.”