Red Key Solutions wins a new client by handling ransomware settlement & recovery. A repeatable playbook for future client wins.

Highly Urgent Call:

In the fall of 2017 Paul Grenci, CEO of Red Key Solutions received a cold inbound request from a local construction company. The Westchester, New York based company was crippled by a ransomware attack. All of their operational and communication systems were encrypted, grinding productivity to a halt. Desperate, the company reached out to Red Key, who has developed a strong reputation in the region for its managed IT services.

"In our experience, if you can recover a new prospect from ransomware quickly, it's a great way to start the relationship." *--Paul Grenci, CEO of Red Key Solutions*

"We regularly get approached by companies with ransomware. This case was unique though because the entire company was down, not just a single machine or partitioned cluster." remembered Paul. "In our experience, if you can recover a new prospect from ransomware quickly, it's a great way to start the relationship." Getting the new prospect through the incident quickly is key though, as it sets the tone for the long term relationship. In this particular case, Paul and his team decided to step out of their comfort zone to help.

Field Evaluation:

After performing a field evaluation of the company's encrypted machines, and doing hours of security research, Paul's team was able to identify the strain of ransomware. The strain was identified, and had no known decryptor tool available. The company did not have backups available, so settling the ransom was the only option recover the lost data. "When we realized that paying the ransom was the only choice, we really had to take a step back and think through how we were going to handle all the logistics, not just figuring how to buy the cryptocurrency, but how to safely set up contracts with the construction company. It was tricky all around, and consumed a lot of time."

"When we realized that paying the ransom was the only choice, we really had to take a step back and think through how we were going to handle all the logistics."

Finding a balance between speed and safety:

Despite the urgency and pressure from the construction company, Paul's team scripted out how they would contract with the construction company, collect the ransom amount from them securely, purchase the requisite amount of cryptocurrency, and then communicate with the cyber criminals to coordinate the settlement. "All in, the logistics probably added 24-36 hours of downtime, but there was no other way. This was a new relationship to us, so we cut no corners." Procuring and sending the cryptocurrency took a fair amount (of time) as well." remarked Paul. Despite the hurdles and additional downtime, Paul's team ultimately prevailed.

"We built a great deal of trust with the company by helping them through that initial incident. They are loyal to this day because of it" *-Paul Grenci, CEO of Red Key Solutions*

Settlement & Recovery:

Red Key was able to procure about $1,000 of bitcoin after a day or so, and the decryption keys were released after the cryptocurrency was received. The team then began to restore the company network so work could commence. After four days of restoration the company was back to full productivity. It was a lesson learned the hard way, and the construction company took the opportunity to significantly upgrade their security and backup services, all through their new IT partner, Red Key.

Despite the positive outcome of this case, Paul saw significant room for improvement in the future. The prospect suffered several days of downtime and the ability to end the downtime in a hours instead of day would bolster an MSP's ability to onboard a prospective client in a similar situation, and save a lot of time, stress and money.

Communicating with cyber criminals and settling ransomware using cryptocurrencies is not a common practice of most managed service providers. Each case can take days to research and put in motion. Coveware's platform has productized this process as a disaster recovery service. As Red Key discovered, successfully recovering a prospect from ransomware can make a material difference in the ability to win a new client.

"A lot of companies really want an immediate painkiller.

Stories like our construction client are great, but there are others that we could not onboard because of the amount of downtime they face.

That changes now that we joined the Coveware partner community."
-Paul Grenci, CEO of Red Key Solutions