Sephno Systems partners with Coveware to overcome TNT Ransomware

The Incident:
In early July of 2018, San Diego based managed service provider Sephno Systems was alerted to a potential ransomware infection at one of their end clients. Upon initial inspection, the team discovered that several individually partitioned servers had become encrypted with ransomware.

Sensing that the ransomware was encrypting via remote access, the team immediately locked down all remote access points. They then began a two pronged remediation effort. First, to assess the state of the back-ups for each server, and second, to determine the origin of ransomware.

Sticker Shock:
Each unique infection carried its own ID, and demanded 10 Bitcoins, or roughly $65,000 in total for the entire network. "Our client was international, and given the time the encryption began, we are able to narrow our search down to a handful of employees. Review of those employee laptops uncovered foreign remote access executables, remarked Dale Leuty, the field manager in charge of the recovery. It was clear from the pervasiveness of the ransomware and the tailored way in which the attackers gained access, that Sephno was dealing with relatively sophisticated attackers. The size of the ransom demanded bolstered this assumption.

Sephno was able to engage with Coveware in a matter of minutes. After submitting just a small amount of information about the ransom notice text, Coveware was able to diagnose the strain and provide some immediate context to Sephno about their options

"Our client is pretty small, and we knew forensic consultants were not in the budget. We were lucky to find a willing partner in Coveware." *- Dale Leuty, Field Support Manager*

"Negotiating and cryptocurrency adds stress and anxiety to situations that are already really tough. We remove a lot of that exposure and eliminate client downtime one way or another." *- Alex Holdtman, CTO & Co-Founder of Coveware*

"Less than half of ransomware victims are able to recover from backups due to unmonitored or failed backups, along with backups also becoming encrypted." *-Barkley Protects Inc, 2018 infographic*

Negotiations and Alternatives:
The Coveware support team was quickly able to identify the strain and the specific cyber criminal group behind it. There is no known decryptor tool available, so settlement was the only option for decryption. The Sephno and Coveware support teams agreed to a ransom budget, time frame and communication cadence. From there Coveware began to execute Plan B.

Communicating with cyber criminals and settling ransomware using cryptocurrencies is not a common competency of most managed service providers. Each aspect could take several days to research and put in motion if handled by an inexperienced team. Coveware's platform has turned this into software as a service.

Over the course of 3 days, Coveware was able to negotiate the ransom to an amount that fit the victims budget. Now the Sephno team knew they had a viable option if the restore process fell short. "Thankfully no payment was necessary, and the Sephno team was able to remain heads down on the restoration while we dealt with the attackers and maintained our readiness." remarked the Coveware support team.

"Knowing that Coveware was running Plan B, while my team worked to restore back-ups gave us a lot of confidence that one way or another, we would reach a resolution quickly." *-Dale Leuty*

It's just not prudent, and I'd worry about losing a client if the downtime really got extended. Going forward we will have multiple options with Coveware as our partner." *-Dale Leuty*

Looking Forward:
Now that the incident has passed, the Sephno team is taking the time to update their DR plans for all their clients to include Coveware's solution for ransomware incident response. They also plan to use Coveware's analytics & content to showcase their domain expertise through regular security awareness trainings with end clients. When the dust settled, Sephno realized that backups alone won't cut it against today's ransomware threats. "We don't want to imagine getting into this situation again with only a single path to recovery," concluded Sephno.

As organizations assess their incident response capabilities, cases like this demonstrate the importance of having a comprehensive IR / DR plan that includes ransomware response, cyber extortion and cryptocurrency settlement.