To Pay or Not to Pay: A Ransom Discussion

P2P2-W03: To Pay or Not to Pay: A Ransom Discussion

Lee Parrish, Vice President Chief Information Security Officer, Blucora

To Pay or Not to Pay: A Ransom Discussion

As an industry, we understand the need for protecting our endpoints from malware to prevent negative impacts to our corporate infrastructures. But, for whatever reason, let's imagine that your company fell victim to a ransomware attack; does the organization pay the ransom? What are the criteria for determining when to pay? Do we never pay? These were the topics of discussion for two dozen security professionals (that included international attendees representing Sweden, South America, UK) in a RSA Conference 2019 Peer-to-Peer session in San Francisco.

Pre-Conference Survey

1. *Do you believe a company should pay a ransom in order to retrieve encrypted data?*
    - Yes, as a general practice until protections can be put in place: 14.29%
    - Yes, but determined by the type and significance of data: 28.57%
    - No, Never: 28.57%
    - Other: 28.57%
2. *Do you believe there is a risk in paying a ransom?*
    - Yes, there is no assurance the data will be returned: 100%
3. *Pros and Cons of paying a ransom?*
    - Potential issues from regulators/law enforcement/consumers.
    - Sets precedent for bad actors to do it again; loss of control.
    - Opposed to paying ransom but in reality, I am responsible for getting people back to work.
    - You might get the data back but no guarantees that data will be returned, or if the data returned has integrity, and if the data was copied.

P2P Session: Main Themes

As we outlined the discussion and the areas of focus we wanted to dive into, a few main themes became apparent:

⇒ What is the risk?

- exposure risk if not paid (or even if it is paid)
- reputational risk

⇒ What are the impacts?

- cost of recovery due to the loss
- loss of productivity

Top 10 Highlights

1. In order to provide leadership with the adequate information to make a decision, we should evaluate: value of the data, time constraints in rebuilding the data, cost of idle time while data is encrypted, type of attack (infiltration or ransomware). An interesting reminder from our healthcare representatives was the risk to our patients due to the ransomware attack.
2. Certainly there may be reputational risks associated with paying. Additionally, the group discussed potential issues with regulators and laws associated with paying ransom. Some mentioned that paying a ransom may be considered funding illegal activities. All agreed that looping in your legal team (and potentially outside counsel) into the conversation is a good approach.
3. Many agreed that even paying a ransom does not guarantee that your data will be returned (unlocked) or that the data has good integrity – it is the same data that was encrypted. The group also was concerned with repeat attacks since the adversary now knows you will pay (and may have shared that fact with other attackers).
4. We had a wonderful discussion on the fact that the cultural values of your organization will impact the decision that is made with regards to paying the ransom.
5. The group discussed the logistics of paying a ransom; does your organization have an agreed upon process for actually paying the attacker (if the decision is made to pay).
6. It is unanimous that we need more laws around this topic, and at the international level.
7. A quick, but valuable discussion occurred on the topic of organizations attacking back. The majority agreed that attacking back is not a good option.
8. The biggest point made during the discussion was to practice these types of scenarios in a table top exercise. Gather all of the leaders and stakeholders and run through a ransomware scenario – before it occurs. Who is going to do what? What factors will go into our decision to pay or not pay? We also talked about the idea of keeping the process documented (or a copy of it) in an out of band storage area.
9. We need to learn from our incidents. How did the attacker get in? What can we do to prevent similar things in the future? Why did it happen, was it a lack of anticipating an attack?
10. And finally, all agreed that preventative measures are the best practice so that the risk of your company falling victim to ransomware attacks is reduced. Endpoint protection, end user training, and all of the other measures we understand are effective.