TIP Jar

Agency Case Study: Lessons from a Real-Life Cyberattack

Spring 2017

The Lindsay Unified School District, a K-12 school district that serves over 4,000 students in California's San Joaquin Valley, knows firsthand what a ransomware attack looks like: The district recently experienced one, when attackers infected servers through phishing emails that looked like legitimate communications. Fortunately, the district had policies and procedures in place that minimized the attack's effects on its servers.

The district agreed to share its experience with the TIP Jar to show readers what an attack looks like and to help other public agencies be better prepared for a ransomware attack.

While the district's network administrator, Peter Sonksen, said it's difficult to pinpoint the exact root of the ransomware attack, Sonksen believes it stemmed from a phishing email sent to several employees, some of whom either clicked a link or opened an attachment in the email, which allowed the ransomware to embed in their computers.

The district realized an attack may be taking place when several of its programs stopped working and employees began receiving error messages when they tried to access files or run programs. Sonksen said that both are common signs of a malware or ransomware infection. Unfortunately, ransomware victims are often unaware they are under attack until it's already completed encryption.

Once that occurred, the district received a pop-up web page that confirmed its files had been encrypted and demanded payment in Bitcoin to decrypt the files and restore access. The web page also provided an email address to contact the attacker and to obtain additional instructions for making a ransom payment.

In anticipation of just such a scenario, the district had already put a number of policies and procedures in place that were designed to prevent or at least mitigate the impact of cyberattacks. One of the district's procedures entailed making full backup copies of its servers on a periodic basis, and incremental backups on a more frequent basis. The backups helped the district immediately erase most of its infected servers and reinstall nearly all of its infected files and folders with clean copies.

The district's IT staff then worked to clear ransomware from employees' computers, identifying all employees whose computers were infected, wiping them clean and resetting the employees' credentials. While taking this step, the district's IT staff learned something that Sonksen said may be useful to other agencies dealing with an attack: The ransomware that attacked their servers can attach itself to user profiles, allowing it to embed itself in every computer a user logs into. That meant that IT staff had to wipe clean every computer an infected user logged into in order to completely erase the ransomware program.

Devon B. Lincoln
Partner and Co-Chair
Facilities & Business Practice Group
Monterey Office
dlincoln@lozanosmith.com

Travis E. Cochran
Associate
Monterey Office
tcochran@lozanosmith.com

Lozano Smith
ATTORNEYS AT LAW

Unfortunately, the district had one server it hadn't yet backed up, leaving district leaders with two options: Wipe the system clean and lose all of its information or pay the ransom. After evaluating factors that included the amount and type of information that would be lost, the impact of the loss and the difficulty to recreate the information, the cost of paying the ransom and the risk that files wouldn't be restored after payment was made, the district determined that paying the ransom was its best option. After making the payment, the district received the code needed to decrypt its files.

In addition to ridding itself of the ransomware infection and restoring access to its files, the district quickly sought to determine whether any of its information had been accessed or taken by the attackers. In order to protect its data once it learned about the infection, the district immediately shut down remote access to its servers. IT staff repeatedly checked the district's filters and web traffic logs to ensure that no information was transmitted offsite during the ransomware attack. The district also filed reports with the local police and the FBI.

When asked for advice on preventing, mitigating or addressing ransomware attacks, Sonksen and Chief Business Official Grant Schimelpfening said school districts should prepare by creating backup copies of the contents of their servers so they can wipe systems clean and reload information. They said this is a much less expensive and risky approach to resolving a ransomware attack then being forced to pay a ransom to regain access to files. In the district's case, server backups were instrumental in mitigating and resolving the attack.

Sonksen and Schimelpfening said that educating employees is also key: Attackers have designed phishing emails that cater to consumers, and no level of anti-ransomware software, network firewall or web filter can protect an agency's servers if employees inadvertently download malware. The district frequently sends out instructional material to employees and reminders about identifying and avoiding malicious content. It also incorporated a cybersecurity training program into its required annual trainings.

The district's motto, they said, is "Be careful what you click."