Progent

Case Study: A Successful Ransomware Recovery

A client engaged Progent after an attack on their organization by Ryuk ransomware. Ryuk is believed to have been launched by North Korean state hackers, possibly using technology leaked from the U.S. National Security Agency. Ryuk targets specific companies with little tolerance for disruption and is one of the most profitable versions of ransomware. Headline victims include Data Resolution, a California-based data warehousing and cloud computing firm, and the Chicago Tribune. Progent's client is a manufacturer based in Chicago and has about 500 employees. The Ryuk attack had shut down all business operations and manufacturing processes. The majority of the client's backups had been online at the time of the attack and were encrypted. The client considered paying the ransom (in excess of $200,000) and hoping for the best, but in the end called Progent.

"I cannot say enough about the support Progent gave us during the most critical time of (our) business life. We may have had to pay the Hacker if not for the confidence the Progent Team gave us. That you could get our e-mail and Servers back in less than 1 week was something incredible. Every single person I spoke to or e-mailed at Progent was hell bent on getting us operational and was working 24/7 on our behalf."

Progent worked with the client to identify and prioritize key areas that needed to be addressed in order to restart business operations:

- Active
- Email
- Accounting/ERP

To start, Progent followed AV/Malware Processes best practices by isolating and cleaning up infected systems. Progent then began the task of recovering Active Directory, the heart of enterprise networks built on Microsoft technology. Exchange email will not operate without Active Directory, and the client's accounting and ERP software used Microsoft SQL, which depends on Active Directory for access to the database.

Within two days, Progent was able to restore Active Directory to its pre-attack state. Progent then helped perform reinstallations and hard drive recovery on critical systems. All Exchange ties and attributes were intact, which facilitated the rebuild of Exchange. Progent was also able to locate intact OST files (Outlook Offline Folder Files) on various workstations to recover email data. A recent offline backup of the client's accounting/ERP software made it possible to return these vital applications back online. Although significant work remained to recover fully from the Ryuk attack, core services were restored quickly:

"For the most part, the manufacturing operation never missed a beat and we did not miss any customer shipments."

Over the next few weeks important milestones in the recovery process were achieved through close cooperation between Progent and the client:

- Internal web sites were brought back up with no loss of data.
- The MailStore Server with over 4 million archived emails was spun up and working.
- Orders/Invoices/AP/AR/BOM and inventory were 100% restored.
- A new Palo Alto 850 Firewall was installed.
- 90% of user workstations were operational.

"A lot of what happened that first week is mostly a blur for me, but we will not forget the countless hours each and everyone of you put in to give us our business back. I have been working with Progent for at least 10 years maybe more and every time, Progent has come through and delivered. This time was no exception but maybe more Herculean."

Conclusion

A potential business disaster was averted by hard work, a broad range of technical expertise, and close teamwork. Although in hindsight the ransomware attack described here could have been prevented with modern security technology, user training, and appropriate procedures for backup and applying software patches, the fact remains that government-sponsored cyber criminals from China, Russia, North Korea and elsewhere are relentless and are not going away. If you do fall victim to ransomware, remember that Progent's team has proven experience in ransomware virus removal and file recovery.

"So, to Darrin, Matt, Aaron, Dan, Claude, Jesse, Arnaud, Allen, Tony and Chris (and any others that were involved), thank you for allowing me to get some sleep after we got past the first week. All of you did an incredible job and if anyone is visiting the Chicago area, dinner is on me!"

For information about Progent’s ransomware recovery services, call 1-800-993-9400 or send email to information@Progent.com