DP Solutions
Problem Solved.

CASE STUDY

A TALE OF TWO RANSOMWARE ATTACKS

HOW TWO ORGANIZATIONS WERE INFILTRATED BY FIERCE RANSOMWARE ATTACKS AND HOW THEY RECOVERED

Company A

A member-based association located in Bethesda, MD

THE ATTACK

This organization was infected by the .wallet variant of the Crysis Ransomware Virus on a Tuesday at 7:56 AM. An unused account was compromised and used to gain access to the organization's Remote Desktop Server and launched the virus. As a result, most of files on the Remote Desktop Server and the File server were encrypted. As Trend Micro[1] describes, "After encryption, a text file is dropped in the computer's desktop folder–often accompanied by an image set as the desktop's wallpaper. Unlike other ransomware, the information in the ransom note is limited to two email addresses, which victims can use to communicate with the cybercriminals. The users are then instructed to buy the decryption tool needed to unlock the files via the bitcoin crypto-currency–with prices varying between $455–$1,022 as of June 8, 2016."

THE RESOLUTION

The source virus was found and removed by 8:44 AM. A restore of the latest back up (Tuesday 7:00 AM) was kicked off by 9:00 AM. Due to the amount of data on the File Server, the restore took approximately four hours. By 3:00 PM, all files were recovered and confirmed, allowing the Association to be able to work as usual.

THE GOOD NEWS

The Association had a backup system in place, which took hourly snapshots and kept those backups on both a local appliance and in the cloud. This system allowed them to restore from a backup job that was taken very shortly before the incident, making any data loss negligible. The restore was run from the local appliance reducing the amount of time required for the restore.

WHAT COULD HAVE BEEN BETTER

A security assessment would have identified unused accounts and recommended that they be disabled. If the backup system had a provision for launching a virtual standby server, employees would have been able to work while the restore was running. Overall, the association lost nearly a full business day in productivity, which could have been reduced to an hour or so.

DP Solutions
Problem Solved.

CUSTOMER SUCCESS STORY

Company B

A law-firm located in Downtown Baltimore, MD

THE ATTACK

The firm was infected by the Cryptowall 3.0 Ransomware Virus on Monday at 2:27 PM. According to TechRepublic[2], "CryptoWall is classified as a Trojan horse, which is known for masking its viral payload through the guise of a seemingly non-threatening application or file. Its payload involves encrypting the files of infected computers in an effort to extract money for the decryption key."

In this case, a user clicked on an email attachment that was disguised as an overdue invoice. The user's laptop was infected as well as most of the files on the File Server.

THE RESOLUTION

The source virus was discovered and removed by 3:15 PM. A restore of the latest backup (Monday 12:00 AM) was kicked off at 3:30. The restore was very slow, since it was being pulled down from the cloud and the firm had a slow internet connection. It was finally completed at 8:56 PM on Friday.

THE GOOD NEWS

Most of the files were restored. However, since the backup was from midnight, all work saved on Monday prior to the infection was lost.

WHAT COULD HAVE BEEN BETTER

Security awareness training may have helped the user identify the email as suspicious and avoided the incident all together. A backup system with local storage, in addition to cloud, would have cut the time of the restore dramatically. Virtual standby capability would have cut the down time even more.

LESSONS LEARNED

Company A had managed backup and disaster recovery (MBDR) services in place that allowed for more recent data to be recovered and a significantly faster recovery. Company B's lack of protection caused them to lose data and much more productivity. In the end, because company A was more prepared, they were up in running the same day as the attack with all files restored. Company B did not have a local storage backup and therefore took much longer to restore with more data lost.

1. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crysis-to-take-over-teslacrypt
2. http://www.techrepublic.com/article/cryptowall-what-it-is-and-how-to-protect-your-systems/