isogent

ANNA, TEXAS CASE STUDY

Isogent takes a city held hostage, and turns it into a city ready for anything

PROBLEM

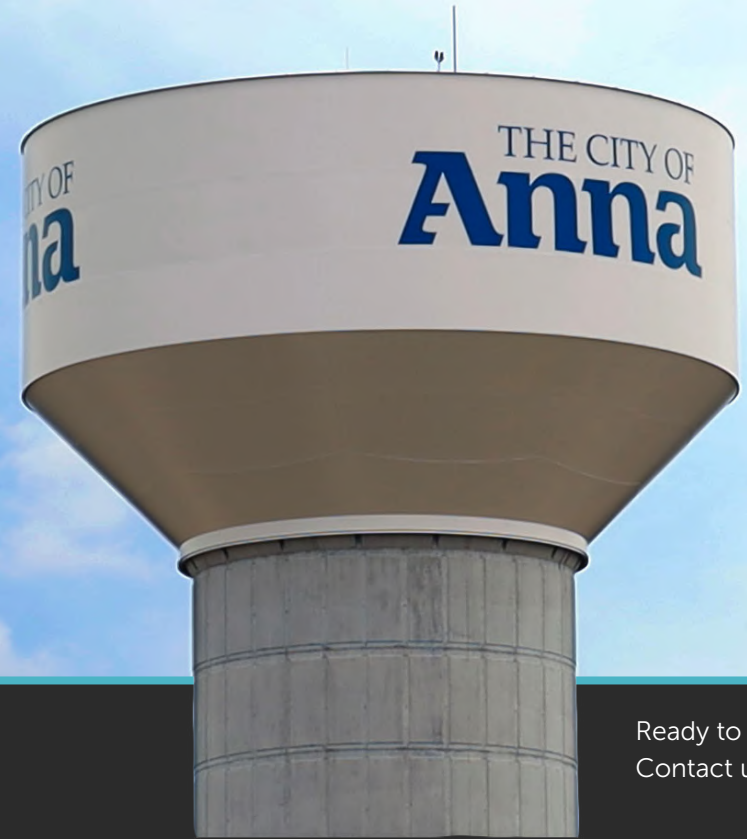
Rapid Ransomware v1.0 targeted the the City of Anna's internal network. The virus was introduced into the network, most likely through email, and then it proceeded to clear the Windows shadow volume copies while terminating critical services and disabling the network anti-virus. Once that was complete, the virus scanned each system for data files and encrypted them using an unknown form of cryptography.

The virus directly attacked 34 unique systems and indirectly hit six additional systems. Those systems had files encrypted with the '.rapid' extension appended to the file name. The virus performed this function on all local, attached, and mapped drives.

SOLUTION

Isogent immediately found multiple emails masquerading as legitimate notices, including one from the 'IRS' containing the subject line 'urgent' contained a zipped file attachment or spoofed hyperlink linked to the Rapid Ransomware malware. Rapid Ransomware, like many crypto viruses, propagates through the 'lateral movement' process. 'Lateral movement' can run millions of scripting iterations in a matter of seconds and replicate infected code across any network shares or pinholes it finds.

As part of a comprehensive strategy, Isogent used its access to next-generation, artificial intelligence based anti-virus software to help neutralize the attack.



SECURE OUTCOME

Isogent removed the Rapid Ransomware, activated Microsoft Advanced Threat Protection licensing for front-end email analysis, and implemented its security policies across the municipality's network. Clean data was restored to the city with the application of a cold spare for the city's SCADA infrastructure.

Over the next week, Isogent Network Engineers rolled out new security measures that both protected Anna's data and increased the effectiveness of its internal communication. This included an implementation plan of multi-factor authentication on all critical systems, network segmentation to limit broadcasts, email encryption for sensitive data, and an expanded back-up system with updated security methods.

Ready to take your business to the next level with our IT solutions?
Contact us at www.isogent.com or by phone: (214)-790-7220