PUBLIC TRANSPORTATION CASE STUDY

Pierce Transit Network Receives Clean Bill of Health from Infocyte

ORGANIZATION

Pierce County Public Transportation Benefit Area Corporation (Pierce Transit) is a nationally recognized leader in the public transportation industry.

INDUSTRY

Public Transportation

CHALLENGE

Understand if any malware or advanced persistent threats (APT) were residing on the network, lying dormant or active.

SOLUTION

Infocyte HUNT™
Compromise Assessment

RESULTS

- Over 600 endpoints enumerated and scanned by Infocyte HUNT
- Clean bill of health with no malware or APTs present on the network
- Easy to understand compromise assessment report for executives and IT staff
- Non-invasive technology easily implemented and quick to scan and assess

The Organization

Pierce Transit covers 292 square miles of Pierce County with roughly 70 percent of the county population. Serving Washington state's second largest county, Pierce Transit is dependent on technology not just for its core business activities (HR, payroll, etc.), but to service the complex and complicated transit systems.

Keith Messner, Chief Technology Officer at Pierce Transit explains, "We have passengers planning trips five days in advance to service people with disabilities or elderly. We also have route dependencies timed to get passengers to jobs, schools and appointments. These systems constantly update in real-time; any disruption or downtime can be catastrophic to our agency operations."

Targets of Cyber Security Threats

Cyber threats are on the rise for public transit companies. According to Messner malware is the primary attack point for transit agencies, and in many cases an infection is the result of a successful phishing attack. Messner continued, "We've seen cyber attacks take down transit agencies. In many cases, it's from employees opening links they shouldn't, introducing malware that can lay dormant for months. Huge repercussions follow – transit systems are attacked and systems operations go down for days to weeks, email across the entire network doesn't work and expensive professionals must be brought in to remediate the breach."

Messner was introduced to Infocyte by a peer sharing his agency's experiences at a consortium of transit CIOs and CTOs discussing cyber security threats on public transportation. "I walked away from the session with a keen desire to understand what may be residing in the background of our network. I needed to know if any malware was lying dormant and waiting to attack, because even with best practices in place, we've seen others brought to their knees by malware."

Messner and his team embarked on a project to find a solution that could look for any hidden compromises that had managed to evade their existing security tools.

“We evaluated other major players in the market, and while these systems were good, we had evidence from other transit systems that Infocyte found malware when others gave them a clean bill of health,” said Messner. “Our comparisons appeared to be apples to oranges so we stopped comparing and went with Infocyte HUNT paired with compromise assessment services.”

Infocyte HUNT Assesses Pierce Transit’s Systems

Pierce Transit has a relatively small internal IT team that manages all of their systems. In order to best manage limited internal resources Messner chose to have Infocyte run a compromise assessment using Infocyte HUNT. This service verifies whether a network is breached using Infocyte HUNT scans to proactively discover the presence of malware and persistent threats, active or dormant, that may have successfully evaded the organization’s existing security defenses. Infocyte operators then provide an in-depth analysis of the scan results and remediation if needed, provide recommendations, as well as deliver an easy to understand executive report documenting the results.

The Methodology and Process

Pierce Transit was impressed by how Infocyte’s agentless platform was able to evaluate the entire network without the burden of complicated equipment or endpoint software installations.

“We were particularly impressed with Infocyte’s methodology used to search for adversaries and malicious programs already on the networks. The scans were essentially seamless and non-invasive, and were pleased with the speed and efficiency of the entire scanning process,” continued Messner.

After the initial set up, Infocyte HUNT was used to enumerate and scan all of the endpoints on Pierce Transit’s complex transit systems using agentless technology that does not require endpoint software installations. The solution quickly scanned over 600 endpoints looking for malware and suspicious code, documenting findings in a scan summary report. As part of the compromise assessment, the Infocyte team then analyzed the scans using the product’s Advanced Analysis capabilities. Infocyte HUNT uses dynamic threat scoring to flag the severity of any identified issues and allows users to examine them in closer forensic detail. The findings were then packaged into an executive level report and presented to Messner in less than 3 days.

Messner said, “The compromise assessment explained our current posture in an easy to understand report for the IT team and our executives.”

A Clean Bill of Health for Pierce Transit

The Infocyte assessment confirmed that Pierce Transit’s systems had a clean bill of health. Further, the report provided some recommendations to ensure Pierce Transit stays malware free.

“To complete a full evaluation internally without Infocyte HUNT, we would require two additional staff and over a month to evaluate our network and servers. With Infocyte’s methodology and hunt technology, we had a cost-effective solution in place that in a matter of days gave us the reassurance that our systems weren’t compromised.”

Pierce Transit continues to use Infocyte to scan its systems to maintain its clean bill of health.

Infocyte®

CORPORATE HEADQUARTERS

110 E. Houston St. Floor 6

San Antonio, TX 78205

+ 1.844.INFOCYTE (844.463.6298)

sales@infocyte.com

www.infocyte.com

@InfocyteInc