BLUVECTOR®

International Bank of Commerce Detects Jaff Malware

Financial Case Study

Serving 88 communities throughout Texas and Oklahoma, Laredo, Texas-based International Bank of Commerce (IBC) is the 83rd largest bank in the U.S. based on asset size. Today, it runs 204 facilities and 309 ATMs within its territory of operations.

As one of the largest independent bank holding companies in Texas, it takes cyber threats very seriously.

The Challenge

In 2017, IBC faced a new zero-day ransomware threat known as Jaff. The high-volume phishing malware, which affects Windows machines, enters an end-user's machine through the opening of a PDF document embedded in an email message that tricks the user into thinking that the enclosed document contains business-related documents or invoices.

Enclosed within that PDF file is a Word file that then uses JavaScript to set a series of events that ultimately work together to encrypt the machine's critical business files with a new ".jaff" extension. Once infected, machines would need to be reformatted and reimaged to stop the spread of Jaff. Any documents that were not backed up prior to the infection may be lost. Or the victim could pay the ransom to restore the documents.

The Solution

Thankfully, IBC already had a better option. Before news about the new zero-day malware broke publicly, IBC's threat team observed over 2,000 instances of Jaff in just a week. Thanks to the BluVector® Cortex™ platform, powered by the file-based Machine Learning Engine to sort through the millions of files on its network, the threat team detected Jaff before it even had a name. With that knowledge, the team then used its containment software to halt the further spread of the malware.

Industry: Finance

Challenge

- ▶ Detecting zero-day malware
- ▶ Alerting threat response team about malware activity
- ▶ Reducing impacts of breach

Results

- ▶ Minimized the effects of Jaff across its enterprise
- ▶ Increased detection capabilities to track new zero-day threats
- ▶ Improved its ability to respond to and remediate attacks

Conclusion

While IBC could have spent tens of millions of dollars through lost hours of worker productivity and impaired access for its customers, the bank ensured its continuity of operations with no significant effect across its enterprise network. BluVector delivered the IBC threat team the knowledge it needed to detect and respond to what would later be known as the Jaff malware before it became a problem.