brysleysystems® MANAGED IT SERVICES

Manage • Optimize • Secure – Since 1987™

Email That Spoofs Company CEO Helps Launch Malware Attack; Forces Manufacturing Firm Into Manual Order-Fulfillment Mode

The following event depicts a real-life malware attack that infected a New England manufacturing firm. The company has chosen to share its story anonymously to help other businesses avoid a similar fate.

The unsuspecting sales rep certainly reacted in a way anyone would expect. He received an email with a voicemail attachment that looked like it came from the company CEO. When the CEO calls, reps jump to attention, and at this particular manufacturing firm based in New England, the business relies on a communication system that sends voicemails as email attachments. So the sales rep had no reason to suspect anything was wrong.

As it turns out, something was very wrong.

CryptoLocker Malware Corrupts Shared Files

Leveraging a nasty, new malware called CryptoLocker, the email used a spoofing technique to make the sales rep think it came from the company CEO. When the rep clicked on the attachment to launch the voicemail, nothing happened. He decided it probably was not urgent and that he would eventually check with his sales manager to see what the voicemail might have been. He then went about his daily routine.

A short time later, the rep tried accessing a shared spreadsheet file on the company’s main file share. When the file opened, all the text appeared as hieroglyphics. The sales rep called the IT help desk, which had him try a few more files. Some opened with hieroglyphics while others opened normally.

As the help-desk engineer investigated the incident, two more sales reps called in reporting a similar problem. The help-desk engineer then realized that malware was likely infecting the company’s network: With 100+ users spread across the company’s headquarters and two remote facilities as well as several home-office employees, the internal IT team needed to act fast to limit the damage.

Isolated Malware Requires Advanced Expertise to Eradicate

After shutting down most servers (including the terminal servers, file server, and ERP server) to isolate the problem and prevent it from spreading to remote users, the internal IT team tried to identify the malware and determine where it originated. They could see which files had been infected on the company’s main file server, but were not sure how to find the source and implement a remedy.

That’s when IT called in Bryley Systems, the manufacturing firm’s long-time, IT service provider. Bryley experts diagnosed the issue remotely; they determined that it was a CryptoLocker-based issue and had likely come in over a terminal-server connection. Bryley then sent two senior network engineers to the main headquarters, and, within 30 minutes, they identified the source of the infestation.

“Because the infected server was a virtual server, booting it up without connecting to the corporate network required a little finesse,” says Michael Carlson, a member of the responding team and CIO for Bryley Systems. “Booting any potential affected server attached to the network is a risk. Plus, determining who altered a file and how they accessed the network requires some network-level investigation.”

Thwarted Attack Avoids Possible Ransom

The CryptoLocker malware that attacked the server is a form of a ransomware that surfaced in the fall of 2013; the malware-protection software vendors had not yet developed a defense mechanism against CryptoLocker when it hit this particular manufacturer.

“The leading anti-malware software solutions do a great job at protecting devices and networks from known malware attacks, but hackers with malicious intent are always developing something new that can slip through perimeter defenses,” Carlson says. “It can take the anti-malware vendors as long as a week to develop a counter-measure and update their solutions.”

As a form of ransomware, CryptoLocker targets computers running Windows and often attacks while disguised as a legitimate email attachment. When activated, the malware encrypts certain types of files stored on local PCs and server drives using public-key cryptography, with the private key stored only on the malware's control servers. The malware sometimes displays a message that offers to decrypt the data if a ransom payment (through either Bitcoin or a pre-paid voucher) is paid by a stated deadline. (See *Wikipedia’s* http://en.wikipedia.org/wiki/Cryptolocker.)

For this particular manufacturing firm, the end-users never received a ransom note, largely because the company reacted quickly and shut things down. They did, however, have over 35,000 files encrypted by the malware.

Bryley Quickly Identifies Malware and Brings Users Back Online

After identifying and eradicating the malware, the Bryley team brought the firm’s main ERP server back online so the company could start functioning on a limited basis. Within two more hours, Bryley brought all the other company servers and end-user PCs back online. Under Bryley's direction, the internal IT team then restored the encrypted files to their normal state using the company's back-up-and-restore capability.

"Having reliable back-ups proved to be a key factor," Carlson said. "It's one thing to identify, isolate and eliminate the problem, but any files the malware encrypted can only be restored properly from a reliable back-up."

During the attack, the manufacturing firm continued servicing customers and shipping products, but had to resort to manual operations and sending faxes back-and-forth to the remote facilities. All the work completed during the down time, which lasted approximately eight business hours, had to be keyed into the system the following day.

Lessons Learned

The manufacturing firm now plans to better educate its staff on avoiding email attachments from unexpected sources. IT also plans to tighten the global settings of its anti-malware and anti-spam software while also conducting a thorough security review.

"With new, malicious software emerging all the time, software defenses can only do so much, and businesses can't completely lock down their environment without hampering user productivity," Carlson warns. "Businesses must educate their employees to avoid opening suspicious emails and to not launch any attachments. If there's any doubt at all, check with IT first."