Recent Phishing Attacks Against Attorneys Highlight Legal's Ongoing Susceptibility

Attorneys in several U.S. states received ransomware-carrying emails alleging legal action from "The Office of the State Attorney."

Ricci Dipshan, Law Technology News

January 9, 2017

In late December 2016, attorneys across the U.S. received emails with the subject line "The Office of The State Attorney Complaint," purporting to hold, in an attached PDF, information regarding a vague legal action against them that required their attention. Only, such emails were never sent by any government or legal official. Nor did the PDF files contain complaints, but instead hidden ransomware files.

The emails, which the New York Attorney General's office posted a copy of on its website, were but one of two phishing attacks—a method whereby cybercriminals try to trick unsuspecting users into voluntarily downloading malware on their systems—targeting attorneys in multiple states, including New York, Florida, Maryland, and Texas.

According to the Maryland State Bar Association, another version of the phishing emails were also sent to attorneys with the header subject line "see you in court," and a link to what was described as an encrypted document, but was in fact a malicious file.

Crag Bogner, systems engineer at Innovative Computing Systems and former IT manager at Denver-based law firm Montgomery, Amatuzio, Kolodny & Dusbabek, said the phishing attempts were novel in their design and targeting of an entire industry.

"This is the first time I've seen any kind of attack that is focused on an industry that flat out says the email comes from an official-sounding office and includes in the attachment what appears to be, at first blush, official [files]," he said.

Bogner added that such cyberattackers may be specifically targeting at the legal industry "because they have had success in the past."

"I've heard a lot of stories from other attorneys that they have simply paid the ransom. If they weren't getting that kind of reactions from law firms and domains that are law firms, they probably wouldn't be targeting them," he explained.

This type of phishing works by attempting to shock users into quickly opening a malicious file or link, in no small part because there are simple ways to discern these emails from official and safe correspondence.

For one, "you can tell [the emails] are not from legal professionals because at this point, there aren't any jurisdictions that require or allow legal service by email," Bogner explained.

Another tell-tale sign of a phishing attempt is the domain name from which the email was sent. Many of the phishing emails targeting attorneys were from "outlook.com," coming from the domain for Microsoft's free Outlook email client. "They aren't coming from a registered domain, but instead from a free service, so the name is a key differentiator," he added.

While training employees to effectively notice and resist phishing emails is the key factor in any cybersecurity program, law offices can also employ technology to make sure malware never arrives on their server in the first place.

"Email filters or 'mirror' email servers play a key role in protecting against this sort of attack," Bogner explained. "A firm can

use these services or equipment to filter out offending attachment automatically. The entire email may be withheld, but most importantly, the attachment will be stripped out of the email, thereby preventing it from even getting to the network."

Such technology may be pivotal given that lawyers generally handle a large tranche of emails and attachments, some of which are in file types usually employed by cybercriminals, during any given day.

Bonger noted, for example, that "ransomware is spread by compressed files. Unfortunately, lawyers still use compressed files to email data. So there is a thin line at play where the decision must be made to change how a firm communicates with other entities versus using outdated and potentially dangerous practices."
