Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New Ransomware Ring Aims To Publicly Shame Its Victims

By **Ben Kochman**

Law360 (February 14, 2020, 8:46 PM EST) -- A ransomware ring that claims to have hacked into five law firms has turned up the heat on targets by stealing and threatening to post their sensitive data, adding a new wrinkle to the already nightmarish scenario victims face.

The hacker group, which calls itself Maze, uses complex tactics rarely seen in prior ransomware attacks — including taking the extra step of exfiltrating victims' data before locking victims out of their networks, cybersecurity experts say.

The hacker group Maze has claimed nearly 30 victims, including health care clinics, construction companies and at least five law firms. (AP)

If a target does not pay the group's ransoms, some of which have amounted to several million dollars in digital currency, the group posts the victim's name on its website in an effort to shame them into complying, industry experts say. In a further escalation, the group has posted what appears to be sensitive stolen data from victims on its website.

The group's nearly 30 claimed victims have spanned several industries, including health care clinics, construction companies and shipping firms. Among its claimed victims are at least five law firms. Cybersecurity experts have long considered the legal industry attractive to hackers because of the bevy of sensitive data attorneys hold, from medical data to trade secrets.

A potential ransomware attack should already be at the top of any business' list of concerns, but this new threat brings with it a new set of problems. As victims race to restore their networks, they also may be legally obligated to report intrusions as data breaches under one of the 50 different U.S. state breach notification laws or under European rules, depending on what data was taken.

"The Maze ransomware raises the stakes for victims," said Alex Iftimie, of counsel at Morrison & Foerster LLP. "In addition to worrying about how to get their business operations back up and running,

victims face difficult choices about how to stop the proliferation of confidential information about their company, customers and employees."

"This strand of ransomware also may create additional regulatory, contractual and ethical notification obligations," Iftimie added.

Among the hacking group's purported victims is prominent cable and wire manufacturer Southwire Co., which in December filed suit against the group in Georgia federal court. In court papers filed against a "John Doe," Southwire's attorneys wrote that the hackers "wrongfully posted" the company's confidential data on a publicly accessible website, after Southwire refused the hackers' demands of "several million dollars to keep the information private."

The Maze group has also posted what appear to be private documents from at least two law firms: Texas-based Baker & Wotring LLP and Indiana-based Woods & Woods LLC, according to Brett Callow, a threat analyst with the New Zealand-based cybersecurity company Emsisoft.

The hacking group has also published a note on its website naming three small South Dakota law firms as victims and threatening to publish their data if they refuse to pay a ransom.

Woods & Woods attorney Neil Woods confirmed in a statement that the firm, which largely handles disability and injury claims for veterans, has "been the victim of a criminal cyber ransomware attack," has notified the FBI, and "continues to take prompt action to contain the incident, mitigate its effects, and fully investigate."

"The firm will provide additional information to its clients as the investigation continues," Woods added.

Baker & Wotring, a boutique firm that according to its website has 11 attorneys, did not respond to requests for comment.

Callow called it "critical" that companies alert their clients and others with whom they share data in the case of such an attack, so that their partners can protect themselves.

"Depending on the nature of the data that was compromised, clients or business partners face the risk of identity theft, [business email compromise] scams or being extorted themselves by the cybercriminals," he said. "They need to know what has happened so that they can set up credit monitoring and be on the lookout."

Law firms have been particularly on edge about the risk of cyberattacks after multinational firm DLA Piper said in June 2017 that it had taken down much of its phone and email service after being hit with a malicious software virus now dubbed by security experts as "NotPetya." In October 2018, the American Bar Association unveiled ethics requirements saying that attorneys should tell current clients about data breaches, and keep them updated on subsequent investigations.

"Law firms have everything an attacker might want, from personally identifiable information on employees, to medical information, bank information, trade secrets, and other privileged information," said Keith Wojcieszek, an associate managing director in the cyber risk practice at Kroll who formerly investigated ransomware attacks at the U.S. Secret Service.

"It's almost like a treasure trove of information that these law firms possess," Wojcieszek added. "Even a basic partner could have thousands of emails that could be very damaging in the wrong hands."

On top of ethical considerations, ransomware attacks like the Maze wave may trigger what can be sometimes confusing data breach notifications to U.S. state regulators or international authorities, if the attackers have truly exfiltrated data, MoFo's Iftimie said. Victims first need to figure out whether the data that was taken is "personal" or "sensitive" under a particular law before knowing what sort of disclosure to make, he said.

At the same time, victims must decide whether to pay the ransoms — which has itself proven to be a thorny issue.

Some cybersecurity attorneys say that it can make rational sense for a private company responsible to its shareholders, for example, to pay a ransom if doing so is far cheaper than the alternative of rebuilding its network. But federal officials have long warned that doing so doesn't guarantee that criminals will give an organization back access to its data, or that they won't mount more attacks in the future.

"You're making a deal with a known criminal," Wojcieszek said. "It's hard to trust that they are going to decrypt that data, and how do you know that they didn't put in some sort of backdoor so that they could go back in?"

--Additional reporting by Emma Cueto. Editing by Breda Lund and Aaron Pelc.