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

'Dark Overlord' Hack Another Cautionary Tale For Law Firms

By **Ben Kochman**

Law360 (January 17, 2019, 9:23 PM EST) -- A hacking group calling itself "The Dark Overlord" has released a cache of confidential files it says it stole from a law firm involved in litigation stemming from the 9/11 attacks, and is now offering more sensitive documents to the highest bidder in the latest frightening example of how the legal industry is a prime target for cyberattacks.

In a series of since-removed social media posts, accounts identifying themselves as the cybercriminal syndicate have threatened to release documents related to post-9/11 lawsuits they claim will embarrass insurers Lloyd's of London and Bermuda-based specialist Hiscox Ltd. as well as New York-based real estate company Silverstein Properties Inc.

All three companies have denied their systems were breached, but Hiscox has pointed to the hack of an unidentified American "specialist law firm" it **reported** in April as the likely source of the stolen data.

The hacking group — best known for taking credit for leaking season 5 of the Netflix show "Orange is the New Black" in 2017 even after receiving a bitcoin ransom payment worth $50,000 — has so far released files mostly relating to post-9/11 insurance payouts, including legal memos sent between law firms and government agencies. It's far from clear whether any of the installments of what the media-hungry group is calling the "9/11 Files" will contain any truly newsworthy information about the attacks.

But the group's strategy appears to be to gain attention by releasing the pilfered material little by little — while ratcheting up the pressure on its extortion targets, cybersecurity experts say.

"This attack emphasizes a shift we're seeing from opportunistic broad attacks to more targeted ones featuring high-stakes extortion," said Mark Sangster, vice president for strategic marketing at the cybersecurity firm eSentire. "When it comes to targeting law firms, they understand the nature of the business and what buttons to push."

The hacking group says it will release the stolen files in five installments after receiving escalating payments in digital currency. It says it will release some of the documents publicly, while offering what it claims is the most sensitive information to those with the deepest pockets, be it a nation-state or one of the companies named in the files.

"If a full public release happens in the near future, we'll guarantee that we're going to withhold only the most highly confidential and sensitive documents for private sale. For the rest of you: don't worry, there's thousands of documents still to go around," posted a Twitter account identifying itself as the group in one since-deleted post.

"If you're one of the dozens of solicitor firms who was involved in the litigation, a politician who was involved in the case, a law enforcement agency who was involved in the investigations, a property management firm, an investment bank, a client of a client, a reference of a reference, a global insurer or whoever else, you're welcome to ... make a request to formally have your documents and materials withdrawn from any eventual public release of the materials. However, you'll be paying us," the post added.

you'll be paying us," the post added.

The Dark Overlord's data dumps, which the group has claimed will uncover 9/11-related "conspiracies," have yet to reveal any information coming near to inspiring the type of international headlines spawned when offshore tax haven information was exposed in 2016's Panama Papers, which led to the eventual shuttering of Panama firm Mossack Fonseca & Co.

"We have yet to see anything to suggest that the documents they've acquired are inherently new or ground-breaking, let alone justifying the extortion sums they are reportedly demanding," concluded a report compiled by the cybersecurity firm Digital Shadows and obtained by Law360.

But no matter what information is included in the files, the brazen extortion attempts are yet another reminder of why law firms are at the top of cybercriminals' hit lists, industry attorneys say.

"Law firms are going to continue to be targets because of the sensitive information we handle on a day-to-day basis, including bankruptcy records and trade secrets," said Steve Stransky, senior counsel in the privacy and cybersecurity group at Thompson Hine LLP. "This reinforces that law firms should take steps even beyond industry standards to protect clients' information."

One move law firms should be already making is educating attorneys, particularly those handling potentially controversial cases, on social engineering attacks, in which hackers can pose as a familiar client or vendor in bids to lure someone at the firm into handing them a way inside, said Sangster.

"If you are engaged with a politically charged client, involved in elections, for example, or a controversial merger that activists are making noise about, that is going to make you a lightning rod," he told Law360. Attorneys handling that type of case should be highly vigilant about phishing attempts and take their cyber hygiene to the next level by changing passwords and using multifactor authentication and secure virtual private networks, he added.

"If nothing else, that will slow them down," Sangster said.

Guillermo Christensen, a partner in Ice Miller LLP's data privacy and security and white collar defense groups, said he was not surprised to see hackers targeting law firms, which are by nature decentralized in the way they store and share information, with several attorneys often trading data on the same case.

"Many law firms operate as a conglomeration of CEOs doing their own thing, and that is very dangerous from a security perspective," said Christensen. "Hackers may think that law firms might be a better target than, for example, the defense contractors that they do business with."

Attempted hacks into law firms are more and more becoming the new normal, according to the results of an American Bar Association **poll** released in December 2017. More than one-fifth of respondents said their firms had experienced a data breach in 2017 — up from 14 percent in 2016, according to the ABA.

Among some of the key consequences reported from data hacks were downtime and loss of billable hours, destruction or loss of files, and having to pay consulting fees for repairing damage that resulted from the attacks.

In May 2017, BigLaw juggernaut DLA Piper was one of the victims of the ransomware worm known as WannaCry that struck more than 300,000 computer systems in 150 countries.

"I think the fact that such a large firm like DLA Piper was hit was a significant wake-up call for many firms," said Sangster. "But I still don't think law firms have gotten to a place where managing partners know what the risks are and know what questions to ask their IT teams in order to put the right policies and education in place to avoid those risks."

--Additional reporting by RJ Vogt. Editing by Philip Shea and Alanna Weissman.