January 7, 2019

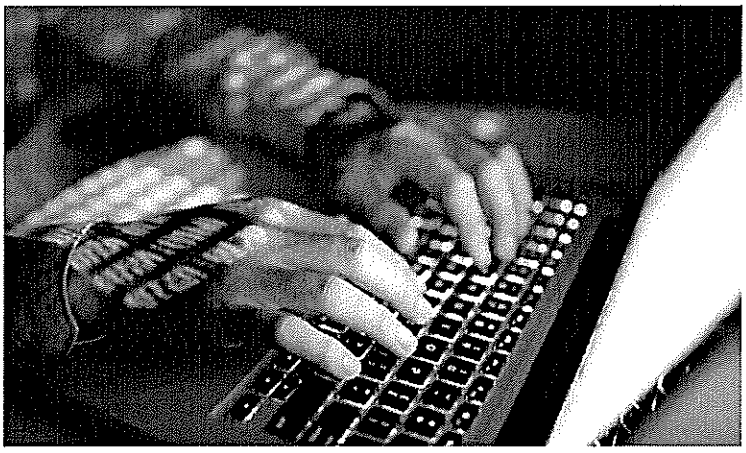
American Lawyer Art re Dark Overlord Hacking (00795992x9C8CB).pdf

Dan Packel, *The American Lawyer*

'Dark Overlord' Hack Shows Mounting Cyber Risks for Law Firms

The hacker group wants ransom payments from dozens of firms involved in the Sept. 11 litigation, and experts warn that more attacks are coming.

By Dan Packel | January 07, 2019



(Image: Shutterstock.com)

Dozens of law firms had their hands in the sprawling litigation that stemmed from the Sept. 11, 2001, attacks on the World Trade Center in New York City.

They represented a sweeping array of entities: first responders seeking compensation for exposure to contaminants at the site, the owner of the towers looking to collect from the airlines (https://www.law.com/newyorklawjournal/almID/1202611552817/silverstein-loses-bid-to-collect-35-billion-from-airlines-for-911/) that let the hijackers on board,

victims looking to haul the government of Saudi Arabia into U.S. court (https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2018/01/18/judge-mulls-if-new-law-allows-911-victims-claims-against-saudi-arabia/), and others.

Leaders of those law firms are all likely scratching their heads about how to handle a recent announcement from a nebulous hacker entity calling itself the Dark Overlord, which claims to be in possession of 18,000 legal and insurance documents pertaining to the court fight.

How the Dark Overlord obtained the material is still unclear. It says it hacked insurers Hiscox and Lloyd's of London, as well as World Trade Center owner Silverstein Properties. Hiscox, meanwhile, has pinned the breach on an unidentified "specialist" law firm that advised it and other insurers, as well as some of its commercial policyholders.

There might have been other points of access, which the Dark Overlord is keeping under wraps. Obviously, no one—including law firms, insurers or others in the mix—is owning up to the breach. "That's a reputational issue and a stance that they have to take," said Tom Ricketts, executive director at Aon Professional Services. "There is no certainty as to where the Dark Overlord has obtained the materials."

What's clear is that the Dark Overlord does have some material. It has released over 45 documents, ranging from pleadings and opinions readily accessible from the federal court docket, invoices to clients, emails between parties in the litigation, to discovery material that's marked confidential.

And the hacker is also open about its aims: it wants the law firms—along with insurers, investment banks, law enforcement agencies involved in the investigation into the attacks, and other parties with documents in the mix—to pay up in order to make sure the material doesn't see the light of the day. At the same time, it says it's offering the

world—or more specifically terrorist groups like Al-Qaeda, ISIS, rival nation states like Russia and China and anyone else willing to pay—the "truth" about "one of the most recognisable incidents in recent history."

Law Firms in the Crosshairs

In a sense, the Dark Overlord has fused the information-seizing-and-publicizing strategy pioneered by Wikileaks with the desire to cash in that's at the core of traditional ransomware attacks, where hackers encrypt a target's files and shut them out until they make a payment, usually via Bitcoin. In previous hacks (https://jezebel.com/the-hacking-collective-the-dark-overlord-keeps-holding-1795866147), the hacker has targeted Netflix and other studios including ABC, HBO, and CBS, threatening to release episodes if the ransom isn't paid.

Now, law firms are in the line of fire.

"Hackers often want to expose things of value to them or others, and this fits in the sad but predictable pattern of hackers doing just that," said Crowell & Moring cybersecurity partner Paul Rosen, formerly chief of staff at the Department of Homeland Security and a federal prosecutor.

One obvious takeaway from the breach: Firms connected to the Sept. 11 litigation would be wise to undertake an immediate audit of their data systems, both to probe the possibility that they were a weak link exploited by the Dark Overlord and to forestall the prospect of future incursions.

But the Dark Overlord's hack presents not just an immediate dilemma for firms connected to the Sept. 11 litigation, but a broader challenge for all law firms, which are in a unique position: Not only are they under an obligation to their clients to protect their confidential and sensitive materials, but they also rely on their own service providers, who might have their own vulnerabilities. Furthermore, the everyday business of lawyers involves sensitive communications with co-counsel, opposing counsel, third-party witnesses and law enforcement agencies.

"There's all sorts of external entities that law firms may have to engage in communications with, and if those are obtained by a hacker, at the very least it's embarrassing, but also quite damaging, not just to the firm but also to its clients," said Steptoe & Johnson cybersecurity partner Michael Vatis. "The duties for a law firm go far beyond making sure its own networks and data responsibilities are kept securely."

U.K.-based insurer Beazley issued a report (https://www.beazley.com/documents/TMB/Insights/20181031_beazley-breach-insight-ransomware_attacks-surge.pdf)in October finding that professional services were the second most targeted industry for ransomware attacks, trailing health care.

"We have really now started to scratch the surface of the exposures that law firms have. There is no question that the bad actors are really beginning to understand just how valuable the information that law firms hold is," Ricketts said. "It is making law firms more of a target and is making hackers a lot more sophisticated in how they leverage this information."

Just as audits should be on the mind of decision-makers in all firms, not just those immediately affected, so should the question of cybersecurity insurance. According to Ricketts, extortion—where confidential data has been breached and is being held to ransom—is one of the five principal areas covered by cybersecurity policies. But how different policies treat the matter varies.

Most, said Ricketts, will pay for a third party digital forensics firm to investigate and determine whether or not the firm's systems were hacked. A smaller set of policies, however, won't kick in except in the event of a proven breach.

Even if there's no breach, firms then have to wrestle with the question of the ransom. The Dark Overlord has provided no details on what it's seeking, save for the indication it wants to be paid in Bitcoin. But ransom demands are swelling, with Beazley reporting a highwater mark of $2.8 million.

If a firm is lucky, even if its not responsible for the breach, its cyberinsurance policy may help out here, too. While some policies depend on an actual breach, others are predicated on a firm's liability or responsibility for confidential information. In that circumstance, the insurer would take on the task of investigating the ransom demand and negotiating a payment.

There's another scenario as well. A firm might also have a kidnap, ransom and extortion policy that would cover the hacker's demand.

"The firm is going to have to do a lot of work with their broker to analyze the two polices, determine how they're interrelated and analyze what sort of response is going to have to be employed," Ricketts said.

Whether it's the insurer or the firm itself that elects to negotiate with hackers, they need to keep several things in mind: "The party that's seeking your ransom is a thief," said Barry Temkin, a partner at Mound Cotton Wollan & Greengrass and an expert on professional responsibility. Consequently, the success of the effort depends on an unethical actor behaving honestly.

"What I've heard anecdotally: There is a certain amount of honor among thieves," Temkin added.

To hear the Dark Overlord tell the story, its hack is currently in the public eye because someone else failed to act honorably. The hacker claims that it was first introduced to the cache of 9/11 documents via a hack into a "seemingly ordinary company located in the United States." That company allegedly complied with an initial ransom request, before taking the matter to law enforcement, violating what the hacker said were the terms of the deal.

"We were absolutely appalled by this transgression against our agreement. We decided to offer this company a second chance to repent, accept responsibility, and satisfy our penalty request. They declined to accept our offer, so we're here today," the group said.

Another wrinkle in ransom payments comes from the ambiguous identity of a given hacker. While one associate in cybercrime has pegged the Dark Overlord as a group of three individuals between ages 20 and 40 (https://motherboard.vice.com/en_us/article/ae5w7a/meet-the-hackers-holding-netflix-to-ransom), there's always the prospect that an anonymous hacker could be a sanctioned entity or regime. Making payments to a member of the designated terrorist could invite legal trouble.

Luckily, those in positions of power in this industry have gotten where they are in part because of their skill in weighing competing theories and forms of evidence.

"The decision about whether to pay a ransom for the return or release of data is often a business one, after appropriately evaluating the legal, practical and associated risks," Rosen warned.

Read More:

Hacked 9/11 Docs Weren't Stolen From Husch Blackwell, Firm Says (https://www.law.com/americanlawyer/2019/01/02/hacked-911-docs-werent-stolen-from-husch-blackwell-firm-says)

Cybersecurity for Law Firms: Recent Developments (https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2018/02/02/cfor-law-firms-recent-developments/?slreturn=20180417134553)

Are Lawyers Easy Marks for Hackers? (https://www.law.com/americanlawyer/almID/1202757856163/)