Exclusive: Third Parties Leaking Email Addresses, Passwords From Leading Firms on Dark Web

Security experts provide LTN with the most email addresses by law firm domain name compromised in third-party hacks. Do your firm's policies cover this threat?

Zach Warren, Law Technology News

November 29, 2016

In August, security experts revealed that 68 million Dropbox user emails and passwords were leaked onto the dark web. For LinkedIn, the number was 167 million leaked credentials. For Yahoo: more than 500 million.

Now, you may have heard about these breaches, but perhaps you haven't considered how it involves you: What email did you use to sign up for these platforms? If you're a law firm employee, and you used your company email address, you may have opened the law firm up to risk. If you use the same two or three passwords on multiple different accounts, particularly connected with your work log-in, this risk potential skyrockets.

"People don't quite understand that when you use your corporate email domain for your fantasy football league or your dating site, you're bringing exposure to the organization," says Kevin Lancaster, CEO at Protorion Systems.

This exposure comes in the form of employee passwords, credit cards and other information in the hands of hackers. For law firms, the risk comes when these hackers then turn around and use the stolen data to try and enter firm systems, a similar goal to email phishing attacks and one that can affect any enterprise.

Lancaster says he has seen these threats to law firms firsthand. Protorion Systems' cyber intelligence platform Dark Web ID uses a combination of people (formerly malicious hackers that now "help the good guys out") and technology (artificial intelligence) to rummage through the dark web, finding these compromised credentials for clients.

Most credentials appear "not within the popular dark web or deep-web sites," Lancaster says, but instead in "private chat rooms and member communities" in which hackers operate. These hackers can then take the compromised credentials and use them to attempt entering organizations' systems.

These credentials are not evidence of a hack on an organization. Instead, they are credentials usually stolen in a third-party hack, such as those against social media sites like LinkedIn, work operations sites like Dropbox, or even leisure sites like Sony PlayStation or Ashley Madison. And it's not just email addresses and passwords that are stolen: "It's a credit card number, it's a Social Security number, it's a home address, it's a PayPal account," Lancaster says.

Many law firms are aware of these risks, but believe their current policies have the risk properly assessed. Peter Devlin, president of law firm Fish & Richardson, told Legaltech News that while leaks can occur, "Fish has not experienced any issues from leaks of firm email addresses on third-party websites, and we don't anticipate any problems arising from those leaks. We are confident that due to security training and policies regarding network IDs and password security, hacked email addresses are not linked to the passwords used on our network."

Many other law firms contacted by Legaltech News echoed similar sentiments, though did not agree to speak on the record given cybersecurity's perilous nature.

Still, as Legaltech News has previously reported, the ultimate risk is shadow IT—the actions employees are taking outside of policy. Ryan McClead, business transformation and innovation architect at HighQ, told Legaltech News, "We talk to law firms all the time. [They say], 'Oh, we don't use those types of things. We don't use Box or Dropbox.' But if you actually go through and see what people are doing with their domain email address, there are lots of people using these things, and IT isn't aware of it, and the firm management isn't aware of it."

And these threats are only increasing, as evidenced by a September Dropbox leak. To provide an example of the potential threat, Protorion Systems exclusively provided Legaltech News with the most frequently-found law firm email address domains on its dark web searches, accurate as of Oct. 27, 2016.

Note: DWID Hits indicates that an email and password were discovered from a specific law firm domain. In the case of DLA Piper, for instance, the compromised email would be "XXX@dlapiper.com." Percentages measured here are by ALM figures of firm attorneys as of the end of 2015, not total firm employees, for all firms over 100 attorneys. Percentages can go over 100 percent for this reason, as well as Dark Web ID finding the same email address in multiple locations. Explanations for potential false positives, mergers of differing domains, and other factors below.

Most Compromises by Total DWID Hits Found

Firm Name	Domain	Number of attorneys	DWID Hits
DLA Piper	@dlapiper.com	3702	5078
Jones Day	@jonesday.com	2510	2860

Greenberg Traurig	@gtlaw.com	1730	2841
Latham & Watkins	@lw.com	2101	2675
Skadden, Arps, Slate, Meagher & Flom	@skadden.com	1654	2409
Fish & Richardson	@fr.com	345	2229
Norton Rose Fulbright	@nortonrose.com	3461	2103
Reed Smith	@reedsmith.com	1638	2019
K&L Gates	@klgates.com	1952	1966
Holland & Knight	@hklaw.com	1009	1933

Most Compromises by Percentage of Firm Attorneys

Firm Name	Domain	Number of attorneys	DWID Hits	%
Fish & Richardson	@fr.com	345	2229	646.1%
Foster Pepper	@foster.com	117	335	286.3%
Jackson Walker	@jw.com	328	932	284.1%
Epstein Becker & Green	@ebglaw.com	200	553	276.5%

Godfrey & Kahn	@gklaw.com	159	436	274.2%
McNees Wallace & Nurick	@mwn.com	126	325	257.9%
Jeffer, Mangels, Butler & Mitchell	@jmbm.com	128	320	250.0%
Gardere Wynne Sewell	@gardere.com	219	542	247.5%
Lane Powell	@lanepowell.com	151	371	245.7%
Mitchell Silberberg & Knupp	@msk.com	122	296	242.6%

Fewest Compromises by Percentage of Attorneys

Firm Name	Domain	Number of attorneys	DWID Hits	%
Lewis Brisbois Bisgaard & Smith	@lewisbrisbois.com	891	6	0.7%
Maynard, Cooper & Gale	@mcglaw.com	203	22	10.8%
Squire Patton Boggs	@squiresanders.com	1356	216	15.9%

Faegre Baker Daniels	@faegrebd.com	672	168	25.0%
Dentons	@snrdenton.com	2285	593	26.0%
Davis Polk & Wardwell	@davispolk.com	871	236	27.1%
Babst Calland Clements and Zomnir	@babstcalland.com	130	37	28.5%
Quintairos, Prieto, Wood & Boyer	@qpwblaw.com	288	101	35.1%
BuckleySandler	@buckleysandler.com	142	55	38.7%
Baker & McKenzie	@bakermckenzie.com	4245	1704	40.1%

Are All These My Employees?

Lancaster says his team “won’t get many false positives” for these figures. However, there are a few caveats that mean not all of the compromised emails they encounter are from current law firm employees.

The first is simple movement: People often don’t stay in the same firm for too long, and Protorion Systems does not verify that any particular compromised email address is actually one of a current employee unless explicitly asked by a client. To explain this point, consider a breach of LinkedIn, Lancaster says, noting that many of the site’s users have had the same LinkedIn account for five years or even longer.

“For DLA Piper, let’s say they had 350 exposures with LinkedIn. It’s possible half of those aren’t even employees anymore,” Lancaster explains. “We don’t make that designation because we don’t have the resources and time to do that, and we don’t have access to their active directory.”

The second issue that can occur is fake website registrations under a specific domain. This is more common, Lancaster says, for shorter domains that users simply plug in during registration. This can provide a potential explanation for law firms with these short domains—notably Fish & Richardson (fr.com) and Jackson Walker (jw.com), two of the top three by highest percentage of attorneys.

But when contacted by Legaltech News, Fish & Richardson notes that for the firm, not all emails are used as log-ins, and the public nature of email addresses can lead to further false positives.

“As is the case with virtually every law firm, all Fish legal staff email addresses are public, and posted on our website, because we want to make it easy for clients to contact us,” Devlin says. “We know that this creates an unavoidable opportunity for criminals to spoof our email addresses. On the other hand, firm network usernames are unique and are not publicly available. The firm network requires complex passwords that are frequently changed. These protocols ensure that our network is protected even when third-party sites are hacked.”

So What Does It Mean?

Lancaster stresses that these compromises are not breaches, but rather vulnerabilities. The key, he says, is to make sure that proper procedures are in place to both be aware of and protect against hacking attempts coming from these emails, especially when it comes to making sure employees follow these procedures.

“What we’re trying to suggest is, it’s not about your exposure yesterday and what we find, it’s actually about your exposure tomorrow,” Lancaster says. “It’s not about if you’re going to get hacked, it’s about detection of when it happens and the actions taken from that.”

He suggests three courses of action. First, firms should establish and enforce policy about using corporate emails owned by the law firm. Many firms already have these policies, and many that he works with will “use our platform to reinforce policy,” he says.

Second, he stressed the importance of two-factor authentication (“the password plus something”), which utilizes a text message or biometrics as an additional entry barrier to the system, as well as other technologies. Fish, for example, uses “software that screens emails to filter and quarantine incoming email from viruses, malware, and phishing attempts,” Devlin explains.

Third, he notes the importance of training employees to not click on unknown links and to be knowledgeable about the dangers of unsecured Wi-Fi connections.

These points are especially true, he says, for midsized law firms. While larger law firms may have the most total number of hits, as the table by percentage indicates, midsized firms may be the most at risk.

Finally, he adds that an important step is to have conversations about these security concerns. This means not only conversing with corporate clients—many of whom may already have the data, Lancaster stressed—but also with all of the stakeholders within the organization.

Devlin says his firm has taken this to heart. “Fish has a cybersecurity committee that includes our general counsel, attorneys who are cybersecurity experts, and IT leadership. The committee creates policies, promotes security awareness training for all employees, and is quickly made aware of any potential security issues identified by proprietary screening technologies.”

Legaltech News will be following up with this story and provide more insights from the numbers in the coming weeks.
