Cyber Spies Sway Litigation Battles and Break into Attorney Emails

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

Straight From the Headlines

Reuters reported in late June that thousands of email records it had uncovered showed Indian cyber spies hacking into parties and law firms involved in lawsuits around the world. Apparently, hired spies have become a weapon of litigants looking for an advantage.

As you might imagine larger firms are particularly at risk given how many high dollar litigation matters they handle.

Who in the Heck is Sumit Gupta?

We had never heard of him until we read the Reuters story. The answer to the question is that Sumit Gupta is a cybersecurity expert who worked with a group of Indian associates to build an underground hacking operation that became a center for private investigators who were looking to bring an advantage to clients in lawsuits.

As the article noted, Gupta was never apprehended by U.S. authorities. Reuters has not been able to reach him since 2020, when he told the news agency that while he did work for private investigators, "I have not done all these attacks." Recent attempts to speak with or locate him were unsuccessful.

Reuters identified 35 legal cases since 2013 in which Indian hackers attempted to obtain documents from one side or another of a courtroom contest by sending them password-stealing emails.

The messages often looked like innocuous communications from clients, colleagues, friends or family. Their purpose was to get the hackers access to targets' inboxes and then private or attorney-client privileged information. Examples are provided in the article of the initial emails from the hackers. Probably a good idea to take a look at those so you know how to instruct your employees on what those emails looked like – law firm cybersecurity training should always be top of mind for law firms.

At least 75 U.S. and European companies, three dozen advocacy and media groups and numerous Western business executives were the subjects of these hacking attempts that Reuters documented.

What Makes the Report Reliable?

The Reuters report was based on interviews with victims, researchers, investigators, former U.S. government officials, lawyers and hackers, plus a review of court records from seven countries. It drew on a unique database of more than 80,000 emails sent by Indian hackers to 13,000 targets over a seven-year period. The database is effectively the hackers' hit list, and it lets us see who the cyber spies sent phishing emails to between 2013 and 2020.

As much as we were surprised by the existence of these cyber mercenaries, we were even more surprised that this activity has been going on since 2013. We're not quite sure how this flew under the radar for so long.

The data supporting the report came from two providers of email services the spies used to carry out their espionage campaigns. Why would they cooperate? It seems the providers gave Reuters access to the material after it asked about the hackers' use of their services; they offered the sensitive data on condition of anonymity. We can see where that might have seemed a tempting deal.

Reuters vetted the authenticity of the email data with six sets of experts. Scylla Intel, a boutique cyber investigations firm, analyzed the emails, as did researchers from British defense contractor BAE, U.S. cybersecurity firm Mandiant, and technology companies LinkedIn, Microsoft and Google.

You've got to admit, that's an impressive roster.

Each firm independently confirmed the database showed Indian hacking-for-hire activity by comparing it against data they had previously gathered about the hackers' techniques. Three of the teams, at Mandiant, Google and LinkedIn, provided a closer analysis, finding the spying was linked to three Indian companies – one that Gupta founded, one that used to employ him and one he collaborated with.

Apparently, this was a "Gupta" kind of world.

"We assess with high confidence that this data set represents a good picture of the ongoing operations of Indian hack-for-hire firms," said Shane Huntley, head of Google's cyber threat analysis team.

Did Reuters Communicate with Every Person in the Database?

It sure did – sending requests for comment to each email address – and it spoke to more than 250 individuals. Most of the respondents said the attempted hacks revealed in the email database took place either before anticipated lawsuits or when litigation was ongoing.

The targets' lawyers were often targeted too. The Indian hackers tried to break into the inboxes of some 1,000 attorneys at 108 different law firms. Now that should catch the interest of litigators!

Among the law firms targeted were global practices, including U.S.-based Baker McKenzie, Cooley and Cleary Gottlieb. Major European firms, including London's Clyde & Co. and Geneva-based arbitration specialist LALIVE, were also hit.

Cleary declined comment. The five other law firms did not return messages. That, we are sure, surprises no one. Which is not to say that no action was taken – we suspect that defenses against such attacks were expeditiously fortified.

Who Were the Spies After?

The legal cases targeted varied in profile and importance. Some involved personal disputes. Others involved multinational companies with a lot of money at stake.

From London to Lagos, at least 11 separate groups of victims had their emails leaked publicly or entered into evidence mid-trial. In several cases, court records showed that stolen documents affected the verdict. Not surprising, but quite alarming.

"It is an open secret that there are some private investigators who use Indian hacker groups to target opposition in litigation battles," said Anthony Upward, managing director of Cognition Intelligence, a UK-based countersurveillance firm.

You'll want to check out Reuters' Hacker Hit List, which shows you how Indian mercenary hackers hunted lawyers' inboxes. The far left hand column shows when malicious emails were sent; the left hand column shows who the emails were sent to; the middle column shows the services – such as LinkedIn or YouPorn – that the hackers were imitating; the right hand column shows the subject lines the hackers used to entice their targets. All of this fascinating information may be found in the excellent (if long) Reuters article at https://www.reuters.com/investigates/special-report/usa-hackers-litigation/.

Techniques for breaking into attorneys' emails varied. Sometimes the hackers tried to rouse attorneys' interest in news about colleagues. Sometimes the hackers impersonated social media services. In other cases, the hackers posed as porn sites. Now there's a sure winner. Finally, there were weird or scandalous news subject lines to get the targeted lawyers to click.

Is There Good Money in Being a Cyber Spy?

Apparently so. Gupta could charge from a few thousand dollars per account to up to $20,000 for "priority" targets, said Chirag Goyal, a former BellTroX executive who split from Gupta in 2013 and has since started several tech startups in India.

Goyal said repeat customers comprised much of BellTroX's income. "In this industry, genuine work comes only from recommendations," Goyal said. Reuters was unable to determine the total annual revenue of Gupta's firm, but we're betting it was a tidy sum.

Parting Shot

Among the many stories contained in the article, there is one in which **a lawyer was alleged to have commissioned a hack**. Think THAT might interest a disciplinary board? We sure do.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* snelson@senseient.com

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* jsimek@senseient.com.

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* mmaschke@senseient.com.