THE AMERICAN LAWYER
ALM.
THE AM LAW LITIGATION DAILY

Litigators of the Week: King & Spalding Wins a Botnet Case for Google, Sticks Defendants with Attorney Fees

By Ross Todd
March 10, 2023

You know things have gone haywire on the other side of a case when opposing counsel agrees to pay $250,000 of your fees before the case wraps up.

Our Litigators of the Week are **Laura Harris**, **Sumon Dantiki** and **Andrew Michaelson** of **King & Spalding**. U.S. District Judge Denise Cote in Manhattan previously granted case-terminating sanctions for their client Google against Dmitry Starovikov and Alexander Filippov. The two Russians were accused of creating a sophisticated botnet called Glupteba by infecting a network of computers with malware to mine cryptocurrency and steal user information.

The judge found the defendants, who showed up with counsel from attorney **Igor Litvak** after the entry of an *ex parte* restraining order and default judgment, had attempted to use the litigation as a means of extorting Google—or at least seeking discovery that could help them evade the company's efforts to shut down the botnet. Cote held the defendants and their lawyer jointly and severally liable for Google's attorney fees since the litigation fired back up after the default was vacated. This week, with Litvak already agreeing to settle for $250,000, Cote awarded more than $525,000 in attorney fees against the two defendants.

Lit Daily: Who was on your team and how did you divide the work?

Laura Harris: This matter required a cross-functional team around the globe with real breadth of experience. Here in the States, Sumon Dantiki spearheaded the cyber and technical aspects of the case, including working with a cryptocurrency investigative firm on the botnet's blockchain components, Andrew Michaelson interfaced with financial institutions, and they both worked with law enforcement. I led the litigation strategy, and Andrew and I both worked with an incredible team of associates (some of whom have since made partner!) to develop our factual record in the litigation, including **Matt Bush**, **David Mattern**, **Luke Roniger**, **Paul Weeks**, **Scott Hiers**, **Chris Meyer** and **Prachee Sawant**. The technical disruption and various aspects of the investigation also required input from our German and French offices, and work with co-counsel in various European countries. Finally, our wonderful partner **Katie McCarthy** helped with the IP-related claims.

Courtesy photos

(l-r) Laura Harris, Sumon Dantiki, and Andrew Michaelson of King & Spalding.

Andrew Michaelson: This matter required a cross-functional team with a breadth of experience. We needed the cyber and technical expertise to articulate the claims and to use the court order to disrupt the botnet's activities with third parties subject to the court order. We needed experience with complex civil litigation, including RICO. We needed to interface with financial institutions and law enforcement, including foreign law enforcement authorities.

What can you tell me about the Glupteba botnet? What stands out about it?

Sumon Dantiki: Glupteba was both technically advanced and criminally brazen. Sophisticated cybercriminals create botnets by infecting computers and other devices, hijacking them into secret zombie machines for fraud and other illicit purposes, and controlling them remotely through command and control (C2) servers, all without the user ever knowing. Botnets can even be leveraged to deploy ransomware or other destructive cyber attacks. The Glupteba botnet infected more

than a million devices and used them for a variety of frauds, including selling stolen Google user accounts, mining cryptocurrency, and credit card fraud. And unlike other botnets, Glupteba leveraged blockchain technology to protect itself from disruption: If the infected devices were cut off from the servers that controlled them, they would query the Bitcoin blockchain for certain transactions that had new C2 information encrypted in messages accompanying those transactions. The cybercriminals behind Glupteba also operated in a particularly bold way, operating shell companies in Delaware and posting job openings for developers on the internet.

How have the efforts to shut the Glupteba botnet down looked different than how Google and other companies have dealt with other botnets?

Michaelson: I would highlight two aspects of this litigation. The first is that we brought RICO claims. Civil RICO claims are frequently asserted but rarely successful. Here they made sense, and were successful, because the Glupteba botnet operators engaged in the very type of organized crime that the RICO statute was intended to deter. The RICO claims helped to result in appropriately broad injunctive relief that Google has used to disrupt the botnet. The second unique aspect of the case is that we named individual defendants. In these types of cases, it is more common to name only anonymous Doe defendants. The naming of individual defendants will hopefully make it harder for the named individuals to operate in the future and, of course, it ultimately resulted in them showing up in court to defend themselves… only to be ordered to pay our fees.

Harris: The other aspect of this case that was unique is that we used the disruption and the RICO claim as a jumping-off point to paint a much richer picture of the breadth of the Glupteba criminal enterprise and conspiracy. Most people think of malware or computer crimes as relatively narrow intrusions that can be solved by downloading antivirus software. This case demonstrates how expansive and complex these conspiracies actually are—they are not only using victims' computers to mine cryptocurrency (without the victim ever knowing it), they are setting up shell companies in Delaware. The complaint itself—and even the elements of the RICO claim—were a great tool to highlight the gravity of the threat and the sophistication of these actors.

How did you make the case that the defendants were abusing the court system and discovery in attempts to reap a profit from Google?

Harris: We were acutely aware of the fact that we were litigating against individuals who had no interest in appearing for trial in the United States given their criminal exposure, so their reasons for participating in civil litigation were immediately suspect. We became very focused on testing the veracity of every representation that was made both to us and to the court. Rather than wait for the lies to pile up, we brought issues to the court early and often. Frankly, the misrepresentations were so brazen and consequential that we did not have much choice. At the outset, for example, defense counsel told the court that defendants would appear and participate in discovery; minutes later, before we had even left the courthouse, he represented to us that they feared extradition. A day later, it was no longer the case that they wouldn't leave Russia, but instead that they couldn't leave because they didn't have the necessary passports, all of which underscored that defense counsel's initial representations that the defendants would appear in the U.S. for trial were false. Our associates—credit especially to Scott Hiers!—really became experts at uncovering the truth beneath the flurry of misrepresentations, and even found evidence that defense counsel had advised hackers how to avoid American law enforcement on Russian media.

What can companies in Google's position take from what unfolded here?

Michaelson: Affirmative litigation is an under-utilized tool to protect customers. Many companies shy away from using affirmative litigation as a tool because of the expense and concerns over the scope of discovery. These are valid concerns that must be evaluated, but this case is but one example of a situation where affirmative litigation made sense.

Harris: The litigation tools available in the United States and internationally are extraordinarily robust and flexible. Courts here and abroad can move quickly and even in novel ways, which gives us a lot to work with as litigators when we're looking for the best solution. Here, we had at least four jurisdictions working simultaneously to decapitate a threat after the Southern District issued an order. Then, when the criminal enterprise attempted to use the U.S. civil discovery system as a weapon to fight back, the court recognized the sham for what it was and punished them accordingly. This is really a demonstration of the system working as it should.

What will you remember most about this matter?

Michaelson: I will remember the creativity and hard work of our team, and the dedicated and exceptional contributions from the client. Google's Threat Analysis Group does extraordinary work to protect Google users and the internet at large.