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

Click Fraud Trial Shows Prosecutors Must Be Storytellers

By **Christopher Crosby**

Law360, New York (August 9, 2017, 8:55 PM EDT) -- With the acquittal of an Italian man of all but one misdemeanor charge in what prosecutors described as a worldwide "click fraud" scheme to defraud advertisers, former federal prosecutors and cybercrime experts say the landmark trial may be a turning point in how complex cybercrimes are delivered to juries.

A Brooklyn federal judge sentenced Fabio Gasperini to a year in prison and a fine of $100,000 Wednesday after he was convicted of a single count of obtaining information on Aug. 4, the least severe of the five federal counts he faced and far short of the global wire fraud conspiracy prosecutors alleged that he ran.

For more than a week prosecutors submitted thousands of pages of documents as cybersecurity experts told jurors that Gasperini obtained unauthorized access to roughly 150,000 computers in the U.S. and abroad in order to create an army of infected computers known as a botnet, which was then used to fraudulently inflate the number of times online ads were viewed on websites he owned in an effort to trick advertisers into paying for fake clicks.

Although federal prosecutors have secured guilty pleas in click fraud schemes before, security experts said this trial was the first of its kind, and they were closely watching to see how the government would craft a narrative and humanize technical, complicated evidence.

"Ultimately, though jurors are instructed to ignore it, each is asking himself or herself whether they feel like the crimes as alleged are worth throwing someone behind bars," said Squire Patton Boggs LLP partner Tara Swaminatha.

Swaminatha, a former federal prosecutor who conducted forensic cyber investigations for the U.S. Department of Justice, said the verdict highlighted the tension prosecutors face between adhering to the technical evidence and telling a compelling story.

"I looked at the jury instructions, and they clearly defined what the crime is. But CSI has ruined all of us; jurors expect to see someone at a keyboard launching the attack," Swaminatha said.

Prosecutors had presented evidence of just that: a supposed screenshot found in a Gmail account said to have belonged to Gasperini purporting to show instructions to the botnet being sent from his computer. On top of that, prosecutors had what they said was a smoking gun: notes found on the same

email account written in Italian explaining how the malicious code used to launch the attack broke into and took control of computers.

But even with that, it's difficult for juries to empathize with a company, let alone an advertiser, if prosecutors can't show that the purported theft of money led to layoffs or had a real effect on people's lives, Mayer Brown LLP partner Marcus Christian said.

"People have certain concerns about advertising firms, and a defense attorney will want to play on these associations," Christian said. "One of the greatest difficulties is coming up with a compelling narrative where people are confident a crime was committed and feel it in their gut without prosecutors making inflammatory remarks."

In fact, prosecutors had tried to do just that, bringing forth witnesses from New York City, including a small business owner and an attorney, who said they were robbed of their privacy when their computers were unwittingly roped into the scheme.

Although prosecutors also produced a spreadsheet they said showed Gasperini and several co-conspirators stole roughly $120,000 from advertisers, it's possible the jury was underwhelmed by that figure, and downplayed the severity of the crime in their minds, Christian and Swaminatha said.

"People understand that these are big cyber cases, and may think the figure can be higher than that," Christian said.

The technical underpinnings of the evidence can make it hard to keep the bigger picture in mind, Swaminatha said. During their closing statements, prosecutors retold the case in chronological order, beginning with a vulnerability discovered in late 2014 that, if probed with malicious code, allowed hackers to create a doorway into computer systems made by a major manufacturer.

From there a hacker could take complete control of the computer, ordering it to scour the internet and infect other vulnerable systems and wipe its tracks clean afterwards.

In hours of testimony, cyber experts pored over the code said to have launched the attack, explaining how each piece corresponded to instructions that made computers mimic human behavior by randomly selecting web browsers that "clicked" banner ads.

The code used to launch the attack and an email address that sent invoices to advertisers could both be traced to Gasperini's IP address, as well as to his physical address at an apartment in Rome, witnesses testified.

That trail of evidence is known to some prosecutors as "collections of little pieces of paper," said Kroll cybersecurity managing director Jonathan Fairtlough. A former prosecutor who investigated nascent click fraud cases at the Los Angeles County District Attorney's Office, Fairtlough said prosecutors try to lay a careful trail of computer logs and emails needed to establish a crime without losing jurors in the weeds.

"For instance, you have to show access to establish intrusion," Fairtlough said. "Its definition means to basically control a computer system or network. But that access is diffuse, and the means to show it are logs, which are completely unintelligible and require tremendous cleanup to explain what they mean."

“It’s not like a robbery where the crime and potential criminal are clear,” he said. “It’s missing the easy stuff, like an eyewitness.”

But even assuming jurors believed each piece of evidence corresponded to the narrative framed by the government, a defense attorney needs just one expert to knock small holes in the story, Swaminatha said.

During the trial Gasperini’s attorney, Simone Bertollini, tried to do just that, repeatedly ripping the government’s case as a click fraud trial without evidence of a click.

He called on just one witness in the case, a cybersecurity professional who testified the botnet attack could not have occurred as described. During his closing statement, Bertollini then likened the case to an episode of the TV show "Law & Order" where there was no victim and no evidence.

“Would you remember that episode for a long time?” Bertollini asked.

Shy of emails between co-conspirators bragging about crimes, or a confession, Swaminatha said doubts about the connection between identity and attribution can grow in jurors minds.

“Cases from what we see aren’t about whether the person did it, but how complicated it is to understand,” she said.

The case could have substantial ripple effects on future enforcement by forcing prosecutors to spend more resources on longer investigations, Christian said. Over time, though, prosecutors will become more adept at forecasting pitfalls, and figuring out how juries will react to evidence.

At trial, two expert cybersecurity witnesses, one for the government and one for defense, testified that it was their first time on the stand. That inexperience, Christian said, will become less common as more and more cases are brought.

Also, as tech-familiar young people grow up, the background of juries will begin to reflect an innate savvy with the evidence that seems overly technical right now, Swaminatha said.

“I thought [the indictment] was perfectly well-written, but it don’t know if a layperson would agree,” she said.

Sophisticated cybercrimes are the new norm as readily available software puts easy-to-use tools in the hands of criminals who may be hacking novices, Christian said. Prosecutors will be eager to bring these cases to assure the public they’re on top of what boils down to theft.

“People trying to draw significance in the case should be aware that there will be aspects important to the future, and other aspects that are particular,” Christian said. “Only time will tell if this is a sign of things to come or a one-off.”

Although he’s in the camp of observers who see the case as a one-off, Fairtlough said the case would become a classic, dissected and worked on until prosecutors perfect their methods.

The case underscores the fact that cybercrimes are international in scope, requiring complicated triangulation over evidence and statutes between U.S. and foreign authorities, Fairtlough said. It also

highlights the fact that, to a layman, the federal statutes need to be clarified.

“I commend the office for bringing this kind of case,” he said. “Click fraud is a large loss for many, many companies. It becomes difficult to understand because of the algorithms used, but it’s a huge concern.”

The government is represented by Saritha Komatireddy and Melody Wells of the U.S. Department of Justice.

Gasperini is represented by Simone Bertollini of the Law Office of Simone Bertollini.

The case is U.S. v. Gasperini, case number 1:16-cr-00441, in the U.S. District Court for the Eastern District of New York.

--Additional reporting by Allison Grande. Editing by Brian Baresch and Breda Lund.
