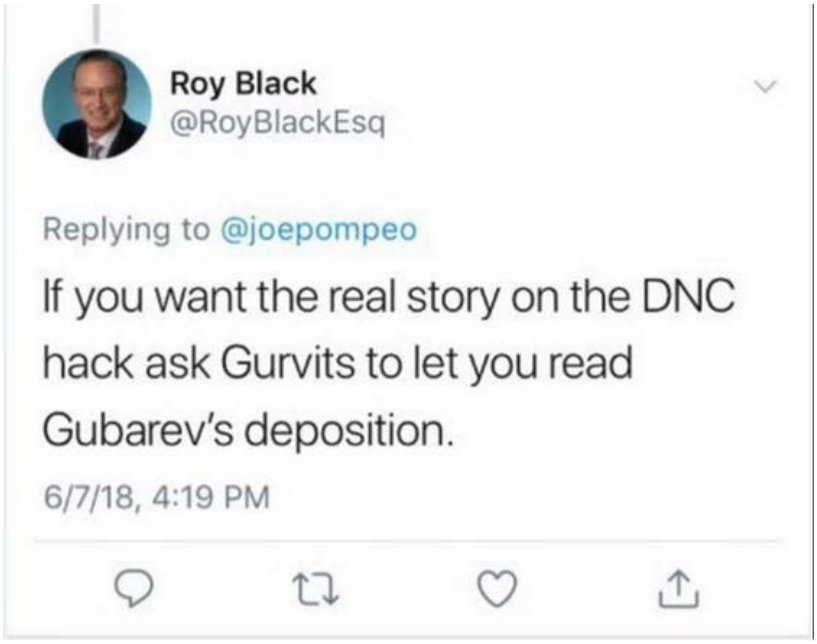
Miami Herald



CRIME

Cloak-and-dagger saga over cybercrime, Trump dossier plays out in Miami courtroom

By Kevin G. Hall

September 21, 2018 08:55 AM

Updated 25 minutes ago

Washington

A federal courtroom in Miami is now the intersection for a celebrity attorney, two major cybercrimes and a foreign tech firm with an ephemeral South Florida address and entanglement in the Trump-Russia probe.

District Judge Ursula Ungaro in Miami is hearing the defamation lawsuit brought early last year by Cyprus-based entrepreneur Aleksej Gubarev against online news outlet Buzzfeed. It published the infamous collection of research memos dubbed the Trump dossier. She must decide, potentially as early as Friday, whether to dismiss the case or set a trial date.

The dossier was was the work of former British spy Christopher Steele, a Russia expert, who was also sued individually in London by Gubarev. Since the suits were filed in early 2017, however, they've grown into a much more complicated affair.


Christopher Steele is the author of the Trump-Russia dossier.

That's because Senate Judiciary Committee Chairman Charles Grassley, R-Iowa, unsuccessfully tried to force Judge Ungaro to hand over copies of Steele's deposition in the Miami lawsuit, which could be useful in undercutting Steele's credibility in the Trump-Russia probe. Grassley was rebuffed in early September.

"If you want the real story of the DNC hack ask Gurvits to let you read Gubarev's deposition," Roy Black, the colorful lawyer hired by Buzzfeed, tweeted on June 7, upping the stakes in a reference to Gubarev's attorney, Val Gurvits.

Black, who conducted the deposition, is a prominent Miami defense attorney, known for defending police officers involved in shooting deaths and taking celebrity clients such as radio talker Rush Limbaugh and singer Justin Bieber. He declined to elaborate further, citing a court order to keep silent about the substance of the case, much of it sealed.

Gubarev is the founder and largest shareholder of Luxembourg-based XBT Holdings, whose family of tech companies provides servers, web hosting and an array of services. XBT owns

South Florida-based Webzilla, which operates servers in Dallas, and both companies are identified in the controversial Steele dossier.

Miami attorney Roy Black
C.M.Guerrero The Miami Herald file photo

The dossier is actually a collection of private “opposition research” memos, paid for first by people close to Trump’s primary opponents and later by a Hillary Clinton supporter. Steele’s dossier claimed on the final page of the 35-page document that XBT was used as a platform for the hack of the Democratic National Committee and subsequent release of private emails.

That allegation, unsupported with evidence, put a little-known company under an international spotlight. Gubarev sued Buzzfeed, claiming he never got a chance to dispute the unverified claims. The news site published the dossier on Jan. 10, 2017, weeks before President Trump’s inauguration.

A new investigation by McClatchy-Miami Herald shows that going to trial might force XBT’s owner to testify about uncomfortable topics. The investigation found that companies owned and operated by XBT were either used by or affiliated with companies connected to the spread of two notorious computer viruses —the Gozi virus and the Methbot virus.

The findings do not prove or disprove claims made about XBT in the dossier, but show how the company could have been used by cyber criminals, wittingly or unwittingly.

McClatchy found evidence that a web hosting company that is part of the broad XBT family was one of the many platforms used to spread the Methbot virus, a sophisticated operation that tricked online advertisers into paying for fake views of video ads.

The investigation found that Nikita V. Kuzmin, the creator of the Gozi virus, which stole online banking data, incorporated at least three companies in South Florida, with the administrative assistance of Webzilla officer Constantin Luchian. He's a Moldova-born naturalized U.S. citizen who runs a company called Incorporate Now, which had been based in Fort Lauderdale and now operates out of Lake Worth.

Citing court documents and regulatory filings, McClatchy reported last November that XBT and its affiliates as well as Luchian had drawn the ire of anti-piracy groups. A chunk of the company's business involves hosting file-sharing sites, where pirated music, videos or movies can be downloaded. These downloads can also be baited with malware that can adversely affect a computer user's operating system in sundry ways.

Music industry associations and attorneys who investigate copyright infringement described XBT/Webzilla as a facilitator of piracy, something XBT's attorney vigorously denied.

Why XBT was named in a dossier was never clear and Steele has been silent. Several people familiar with Steele's thinking have said he does not know why his Russian sources fingered XBT. The dossier alleged that "XBT/Webzilla and its affiliates had been using botnets and porn traffic to transmit viruses, plant bugs, steal data and conduct 'altering operations.' " These are among the allegations that XBT denies and form the basis of the defamation suit.

The dossier also alleged that Gubarev had been coerced by the Russian government because it had compromising information on him, something he flatly denied to McClatchy when giving his first interview on the topic to any news organization, the day after Buzzfeed published the dossier.

Using tools to study digital fingerprints on the Internet, McClatchy stumbled on an email in code language associated with what is known as the Methbot virus. That address appeared in Internet traffic moving via a Fort Lauderdale-based web hosting company called Wz Communications.

Florida documents show it was incorporated in 2009 by XBT employee Kostyantyn Bezruchenko. His LinkedIn page lists him as chief technology officer for Servers.com, owned by XBT, and shows that in 2009 he was in the same role for Webzilla.

In a statement to McClatchy, Gubarev acknowledged that a blogger accused the company in December 2016 of being used in the Methbot fraud.

"As soon as Webzilla learned of the accusation, we immediately closed the client's account and retained the relevant hard drives — which we have kept in case they may be useful to law

enforcement," Gubarev said. "To date, no law enforcement agency has contacted us about that alleged fraud or the hard drives."

Aleksej Gubarev is suing the news website Buzzfeed.

The Methbot virus was largely unknown until the security firm WhiteOps, which took the unusual step in December 2016 of putting out a free report to expose what it called "an army of automated web browsers run from fraudulently acquired IP addresses." These automated commands, called bots, made it look like 300 million video ads were being viewed daily by people sitting at computers, attracting millions of dollars from Internet advertisers.

WhiteOps officials did not answer requests for comment, but in the 2016 report said that Methbot was unique because rather than launching bots through infected computers at homes and offices it used infected computer data centers — anywhere between 800 and 1,200 computer servers at any given time. The physical servers, it said, were in Dallas and the Dutch city of Amsterdam.

WhiteOps did not identify companies so it is unclear whether that is a reference to XBT, which has seven subsidiaries spread across three continents. In the Netherlands, Webzilla operates a data center with 6,000 servers. On its own website, Webzilla says it operates a data center in Dallas and 3,000 servers in the United States.

Both Dallas and Amsterdam have technology clusters, and there is no evidence XBT or its affiliated companies had any direct role in or knowledge of Methbot. But the spread of Methbot underscores how XBT or its affiliates could have been used in Russia's efforts to interfere in the 2016 election campaign.

“Webzilla is one of the largest internet providers in Europe. It is impossible for an internet provider with tens of thousands of clients and hundreds of thousands of IP addresses to monitor all traffic going through its network,” said Gubarev. “Much like a phone company cannot monitor all of its customers’ conversations or how its customers use their telephones, no one on our team was aware [and could not possibly have been aware] of any improper activity.”

Both the dossier and Gubarev can be right, offered Andrew Weisburd, a cyber security and intelligence expert at the German Marshall Fund, a foreign policy think tank.

“Their explanation is entirely plausible, as is the Steele Dossier’s description of Mr. Gubarev as essentially a victim of predatory officers of one or more Russian intelligence services,” said Weisburd. “I have some difficulty squaring those two things with … Gubarev’s aggressive pursuit of Steele and BuzzFeed. Neither BuzzFeed nor Steele have accused Gubarev of being a willing participant in wrongdoing.”

XBT also has an indirect overlap with the Gozi virus. The virus dates back to the mid-2000s and used so-called zombie malware to hack into a computer’s browser and mimic its behavior in order to steal online banking logins and other vital information.

Federal prosecutors in the Southern District of New York arrested its creator, Nikita V. Kuzmin, in 2013. He was nabbed while visiting San Francisco, and prosecutors said at the time that his signature virus infected more than 100,000 computers worldwide, about 25 percent of them in the United States, including some at NASA, causing tens of millions of dollars in losses.

The Gozi virus was so successful that Kuzmin rented it out to other criminal organizations for a cut of the proceeds. He was sentenced to time served in May 2016 and sent home to Russia, but part of what led to his discovery was an email from Nikita@youdo.ru.

Kuzmin happened to be director of YouDo Inc., registered in Fort Lauderdale in 2010 by Incorporate Now, run by Webzilla officer Constantin Luchian. He also handled the registration for Kuzmin Fresh IT Solutions Inc. in 2010 and ServerClub Inc. in 2011.

It appears that Luchian continues to do business with Kuzmin because ServerClub remains an active Florida company, with Kuzmin listed in its 2017 annual report as its chief director. On its website, ServerClub describes itself as a dedicated hosting provider operating on leased servers. The address listed for Server club in documents and one its website is the same one as Incorporate Now in Lake Worth, and as Wz Communications, the web hosting company thought to have been used in the spread of the Methbot virus.

XBT said Incorporate Now is Luchian’s business and is not related. He did not respond to calls left at Incorporate Now, whose mailing address leads to a shared office space that until recently housed a restaurant. He is listed on the website of the shared-space operator Social House, which calls itself “a boutique creative co-working and event space.” Its owners did not return calls and emails seeking information about Incorporate Now.

Kevin G. Hall: 202-383-6038, @KevinGHall