The New York Times

Tech Firm in Steele Dossier May Have Been Used by Russian Spies

Aleksej Gubarev, a Russian technology entrepreneur. New evidence suggests that Russian spies used networks run by Mr. Gubarev to hack the Democratic Party in 2016. *Courtesy Aleksej Gubarev, via Associated Press*

By Matthew Rosenberg

March 14, 2019

WASHINGTON — Aleksej Gubarev is a Russian technology entrepreneur who runs companies in Europe and the United States that provide cut-rate internet service. But he

is best known for his appearance in 2016 in a dossier that purported to detail Russia's interference in the 2016 presidential election — and the Trump campaign's complicity.

Mr. Gubarev's companies, the dossier claimed, used "botnets and porn traffic to transmit viruses, plant bugs, steal data and conduct 'altering operations' against the Democratic Party leadership."

On Thursday, new evidence emerged that indicated that internet service providers owned by Mr. Gubarev appear to have been used to do just that: A report by a former F.B.I. cyberexpert unsealed in a federal court in Miami found evidence that suggests Russian agents used networks operated by Mr. Gubarev to start their hacking operation during the 2016 presidential campaign.

[Read the report here.]

His networks also appear to have been regularly used by cybercriminals and Russian agents to conduct other attacks, such as an assault on Ukraine's power grid in 2015, the report found.

Yet the report stops short of directly linking Mr. Gubarev or his executives to the hacking, as asserted in the dossier. As Anthony Ferrante, the report's lead author and a former F.B.I. agent, noted in a deposition: "I have no evidence of them actually sitting behind a keyboard."

Mr. Gubarev has insisted that neither he nor his businesses knowingly took part in the Russian hacking. He backed up his denials by filing a defamation lawsuit against BuzzFeed, the first news organization to publish the dossier, which became public in January 2017. The report unsealed Thursday was commissioned by BuzzFeed to fend off Mr. Gubarev's suit, which was dismissed in December when the court found BuzzFeed's decision to publish protected under the law.

Evan Fray-Witzer, a lawyer for Mr. Gubarev, said that hackers using a client's servers was hardly unique for a web-hosting company, or any tech company. Mr. Gubarev should not be held responsible for the misuse of his network by others that he neither approved nor knew about, Mr. Fray-Witzer said.

"You could say the same thing about Google's infrastructure and Amazon's infrastructure — and no one is accusing them of hacking anyone just because hackers used their infrastructure," he said.

The report was released after months of legal wrangling by Mr. Gubarev's lawyers, who strenuously fought to keep it under wraps, arguing that it was one-sided and would unfairly tar their client. The New York Times, acting independently of BuzzFeed and Mr. Gubarev, asked the court in October to unseal all of the evidence in the case.

For all of its details of Russia's hacking, the report is unlikely to settle the questions that linger around the dossier more than two years after it became public. But for those who believe the president's loyalties are with Moscow, the report's suggestions of a link between Mr. Gubarev and Russian hacking is likely to spur new demands for renewed investigations, even as Robert S. Mueller III, the special counsel, appears to be wrapping up his investigation.

The dossier is made up of a series of reports compiled in the summer and fall of 2016 by Christopher Steele, a former British spy who runs a firm that conducts investigations for businesses and other clients. The work was done at the behest of President Trump's political rivals, a fact that Mr. Trump and his allies have seized on in an effort to undermine the Russia inquiry by falsely claiming that it beganbecause of the dossier.

Parts of the dossier have proved prescient. Its main assertion — that the Russian government was working to get Mr. Trump elected — was hardly an established fact when it was first laid out by Mr. Steele in June 2016. But it has since been backed up by the United States' own intelligence agencies — and Mr. Mueller's investigation. The dossier's talk of Russian efforts to cultivate some people in Mr. Trump's orbit was similarly unknown when first detailed in one of Mr. Steele's reports, but it has proved broadly accurate as well.

Other parts of the dossier remain unsubstantiated, or nearly impossible to verify, such as its most salacious charge: that the Russians have a video of Mr. Trump cavorting with prostitutes in a Moscow hotel in 2013. At least one accusation — that Michael D. Cohen, Mr. Trump's former personal lawyer and fixer, met in 2016 with Russian officials in Prague — now looks false after Mr. Cohen, who has turned sharply against Mr. Trump, denied last month during congressional testimony ever visiting Prague.

The report commissioned by BuzzFeed to investigate the dossier did not set out to prove any of those accusations. It was done by FTI Consulting, a Washington-based firm, and focused solely on the accusations against Mr. Gubarev. It relied largely on analyzing internet traffic and other clues, and on digging through public records to glean insight into Mr. Gubarev's holding company, XBT, and its many affiliates, including Webzilla. Both XBT and Webzilla were named in the dossier as being used for the hacking.

While the report found no direct evidence of a direct link to the Russian hackers, it did conclude that Mr. Gubarev's web-hosting services are rife with lawlessness. His clients routinely pirate copyrighted material and spread malware, the report found, and his executives appear unconcerned with stopping them or helping authorities track them down.

Mr. Gubarev's "companies have provided gateways to the internet for cybercriminals and Russian state-sponsored actors to launch and control large scale malware campaigns over the past decade," the report concluded. "Gubarev and other XBT executives do not appear to actively prevent cybercriminals from using their infrastructure."

The evidence cited by the report included the use of I.P. addresses — the numbered codes that differentiate individual internet connections — run by an XBT subsidiary, Root S.A., by Russian hackers from two groups tied to the country's intelligence services, Fancy Bear and Cozy Bear. The investigators hired by BuzzFeed also found that at least one of the fake links used to trick John D. Podesta, the chairman of Hillary Clinton's 2016 presidential campaign, into giving up his email password to hackers was traced back to an I.P. address run by Root S.A.

The report also detailed evidence that it said suggested Mr. Gubarev's companies were used in other cybercrimes traced to Russian hackers. One was a sophisticated Russian cyberfraud operation known as the Methbot scheme. It used bots — computer programs that pretend to be people — to steal hundreds of millions of dollars.

During the three months the scheme was running in 2016, roughly three-quarters of the internet traffic flowing through two web-hosting companies owned by Mr. Gubarev — Servers.com and WZ Communications — was dedicated to the scheme, the report said.

Mr. Fray-Witzer, the lawyer, said Mr. Gubarev's companies did not make a habit of prying into the web traffic of its clients, and could not have known what its servers were being used for. But, he added, Servers.com and WZ Communications shut off internet access for those behind the Methbot scheme as soon as they found out about it, and saved all of the hard drives for any investigators who wanted to examine them — none have.

Asked about the numerous lawsuits that have claimed that Mr. Gubarev's companies were used to trade in copyrighted material, Mr. Fray-Witzer offered the same argument: Web-hosting companies are not typically held responsible for the traffic that flows through their servers, and Mr. Gubarev should not be held to a different standard.

In any case, Mr. Fray-Witzer said, the dossier accused Mr. Gubarev "directly of having been involved in the hacking of the D.N.C.," not of running networks used by thieves and criminals.

"Because they couldn't prove the allegations that they actually made about our client," he continued, "they pivoted to say, 'Well, your infrastructure was used from time to time to do bad things.'"

Gabriel J.X. Dance contributed reporting from New York.