McClatchy DC BUREAU

Expert in Trump dossier trial says tech firm's services were used in hack of Democrats

BY KEVIN G. HALL
MARCH 14, 2019 08:47 PM

Documents unsealed Thursday in a South Florida court case provide the most convincing evidence yet that Russian spies piggybacked on a Russian-tied foreign tech company with offices in Florida and Texas to hack the Democratic National Committee and party leaders.

The documents were unsealed in the aftermath of a failed defamation lawsuit brought against online news company BuzzFeed by XBT Holding and its founder, Aleksej Gubarev. BuzzFeed had identified him and his company when it

published in January 2017 the so-called Trump dossier, compiled by former British spy Christopher Steele.

The research that made up the dossier was mostly paid for by political opponents of Donald Trump from both major parties during his 2016 campaign, and among its explosive allegations were that XBT's Internet platform was used to launch cyber warfare that interfered in the U.S. elections.

XBT and Gubarev are based in Cyprus but boast web-hosting operations globally and XBT operates servers in Russia. In a series of stories, McClatchy had reported how Russian-linked hackers used the little-known XBT and Webzilla infrastructure to help spread the Methbot and Gozi viruses, giving more credibility to the dossier's assertions. McClatchy also discovered that another alleged bad actor named in the dossier was a twice-convicted pedophile with cyber expertise.

Those stories helped fill in blanks about the company named in a document that became part of the basis for Special Counsel Robert Mueller III's investigation into Russian election meddling. But the technical details of how the hack happened and efforts to trick people into opening fake documents — called spear phishing — remained relatively murky.

That was until Thursday, when an expert's report entered into the court record by a former top National Security Council cyber leader was unsealed, giving more clarity to the technical mechanisms deployed to hack the DNC and party leaders back in 2016.

"Technical evidence suggests that Russian cyber espionage groups used XBT infrastructure to support malicious spear phishing campaigns against the Democratic Party leadership, which resulted in the theft of emails from a senior member of the Hillary Clinton presidential campaign," said the report prepared by Anthony J. Ferrante, who beyond his NSC role had also served as chief of staff of the FBI's cyber division.

Among Ferrante's conclusions:

▪ A Russian cyber espionage group linked to the DNC hack has used an XBT-owned IP address in the past. IP addresses are a computer's unique identifier when connected to the Internet.

▪ Technical evidence points to XBT-owned infrastructure used to support malicious cyber campaigns.

▪ XBT-owned IP addresses have been tied to cyberattacks on critical infrastructure networks across the globe.

▪ A “significant” number of XBT-owned IP addresses were used to support a digital ad fraud scheme that siphoned away millions from U.S. media companies in ad dollars.

Ferrante’s report also gives more detail on how former Clinton campaign chair John Podesta was hacked. He was tricked into clicking on a link-shortening site that opened to a faux Google security page. That shortened link was created by web user john356gh, and working off the link Podesta clicked Ferrante was able to find three nearly identical fake Google security pages that had virtually the same underlying phishing codes in the shortened links. One had an IP address at an XBT subsidiary called Root S.A.

Ferrante, now a cyber sleuth for FTI Consulting, stopped short of directly connecting XBT to the links used in the phishing. But he said the link found with the XBT subsidiary’s IP address “was created with the intent to steal John Podesta’s email credentials as part of the cyber operations launched against the DNC and Democratic Party leadership.”

XBT has maintained throughout that it isn’t responsible for what users of its services do.

In a statement to McClatchy, BuzzFeed said the unsealed documents show why it was important to have published the dossier back in January 2017.

“Now, because BuzzFeed News published the dossier, we’re learning more about the facts of foreign influence in the 2016 presidential election,” said Matt Mittenthal, BuzzFeed’s spokesman.

A spokesman for the Office of the Special Counsel declined to discuss Ferrante’s findings or whether Mueller is examining XBT.

Among the trickle of unsealed documents becoming publicly available late Thursday, in a case that was tossed out by a Miami federal judge, Ursula Ungaro, was the transcript of a short deposition of Steele. The former British spy worked for years in Russia and has said little publicly since BuzzFeed's publication of the dossier.

Lawyers for Gubarev pressed Steele about why he didn't try to verify the information the ex-spy shared with clients, and Steele responded that his work differs from journalism, which generally requires reporters to put allegations to a subject.

"It is not standard practice in our sector because of the exposure of sources, potentially. And, indeed, the confidentially of enquiries made by clients," Steele explained in the brief seven-page transcript.

Weeks before the dossier was published by BuzzFeed, but at a time when it was in the hands of the FBI and numerous news organizations including McClatchy, a top official of the State Security Service, the successor to the Soviet-era KGB, was found dead in his car the day after Christmas.

First news reports in Russia said Gen. Oleg Erovinkin, 61, was murdered in Moscow and found dead in the back of his car. Hours later, the story in Kremlin-linked news sites was that he'd had a heart attack.

It has been widely rumored that Erovinkin was Steele's source.

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