US investigating hacker ring paid to target corporate critics

June 10 2020, by William Turton, Bloomberg News

Credit: CC0 Public Domain

U.S. authorities are investigating a vast hacking-for-hire operation that involves attempts to pilfer confidential communications from investigative journalists, short sellers and advocacy groups fighting climate change, according to law enforcement officials, court documents

and cybersecurity officials who have tracked the scheme for years.

The overall operation was stunning in scale and in some instances successful, according to several cybersecurity researchers who have been tracking the hackers. Among the thousands of entities allegedly targeted were hedge funds Coatue Management LLC and Blue Ridge Capital LLC, nonprofit groups fighting telecommunications companies over control of the internet, and journalists from multiple news organizations, according to several cybersecurity researchers including the Toronto-based research group Citizen Lab, which tracks illegal hacking and surveillance.

The hackers are based in northern India and are typically hired by private investigators and other middlemen in Israel, the U.S. and Europe, the researchers say. But their ultimate clients are often law firms or corporations, which may receive pilfered material under the guise of corporate intelligence or litigation preparation, according to court documents and several people familiar with the scheme.

Although it's unclear who wrote the checks that ultimately funded the hacking operations, the apparent beneficiaries include specific industries and major companies, including embattled German technology firm Wirecard AG, according to Citizen Lab and other cybersecurity researchers.

U.S. prosecutors in New York and FBI agents are investigating the hacker-for-hire scheme, according to three people familiar with the probe. At least one person implicated in the scheme has already been arrested. In an indictment last year, Aviram Azari, an Israeli private investigator, is accused of working with a group of Indian hackers to target hundreds of potential victims with phishing emails. He has pleaded not guilty, according to his attorney Barry S. Zone, who called the charges exaggerated.

The indictment doesn't identify what hackers, victims or companies may benefited from any such activities.

A Wirecard spokeswoman, Iris Stoeckl, said her company hasn't been in contact, either directly or indirectly, with a hacker group in India. Wirecard said it acted legally in its investigation into short sellers and critics of the firm.

A spokesman for the U.S. attorney's office in Manhattan declined to comment, as did a spokeswoman for the FBI.

Many cyberattacks involve criminal gangs who try to steal log-in credentials or credit-card data; in these cases, the groups both plan the operation and benefit from the stolen data. But in this instance, the hackers were paid to carry out targeted attacks by third parties.

Digital sleuths working at Citizen Lab and two other cybersecurity companies have tied at least some of the hacking back to an Indian company called Belltrox Infotech Services, which operates from a crowded neighborhood of New Delhi. Working independently, the researchers said they tracked the intrusions back to Belltrox through a series of apparent mistakes made over the years by its hackers.

Belltrox didn't respond to requests for comment sent to multiple email accounts associated with the company and its officers. Sumit Gupta, who is listed in corporate registration documents as Belltrox director, couldn't be reached for comment. Veenu Arora, who is Gupta's wife and is also listed as a Belltrox director, denied any wrongdoing in an interview with Bloomberg News. She said that she runs a medical transcription company and that Gupta runs a cake shop.

Surender Mehra, who said he co-founded an earlier incarnation of the company with Gupta called Belltrox Digital Security, said in an

interview with Bloomberg News that he left the company after becoming concerned about some of Gupta's activities. "He was into hacking," Mehra said. After the split, Mehra said that Gupta started a different company, Belltrox Infotech Services. On Tuesday, Belltrox Infotech Services' website, which was functioning as recently as two weeks ago, was down. "This account has been suspended," read a message on the home page.

A major investigation into hacking-for-hire would probably trigger probes in other countries, said Polly Sprenger, a United Kingdom-based corporate investigations attorney and member of a 2012 Home Office inquiry into private spying. "The more important effect of the case is not the actions of this one set of hackers. It's bringing attention to the people who cause this industry to occur—the lawyers, the consultants and the corporate clients," she said. "Where the DOJ goes, other countries and other prosecutors will follow."

In addition to the research conducted by Citizen Lab, at least two confidential reports on Belltrox have been produced by BAE Systems Applied Intelligence, part of the European defense contractor BAE Systems Plc. It refers to Belltrox by the code name Amanda Lovers, because many of its phishing emails were sent from a fictional persona using that name. The reports were described by people familiar with BAE's investigation.

Additional details were provided to Bloomberg News by a researcher for another global cybersecurity company that tracked the Belltrox hackers over several years and asked not to be identified.

Wirecard, which was founded in 1999 and processes financial transactions over the internet, became one of Germany's hottest technology companies. But its success has been marred by allegations of accounting improprieties by short sellers and financial analysts. Activist

investors have called for the ouster of Markus Braun, the chief executive officer. Last week, German authorities searched its headquarters as part of a probe into suspected market manipulation. Wirecard said the investigation wasn't targeting the company but members of the management board and that it was confident the allegations would prove unfounded.

Along the way, financial firms and reporters looked into market manipulation by Wirecard. Hedge funds, short sellers, journalists and investigators who explored the topic were among those targeted by the hacking-for-hire operation, Citizen Lab concluded. "Some individuals were targeted almost daily for months, and continued to receive messages for years," according to the Citizen Lab report, which didn't identify who hired the hackers.

The hackers may have been betrayed by their own mistakes. In trying to attribute a cyberattack to a specific hacker or group, cybersecurity researchers often search for signature patterns in code or tools used by hackers.

In this instance, when the hackers attempted to steal a target's passwords, they often sent emails with custom link shorteners, which linked to fake pages designed to steal login credentials, according to cybersecurity researchers. The shorteners, used to disguise the phishing links, including "strongbolthostinghk(.)com" and others associated with India, such as Holi, a well-known Indian celebration, according to Citizen Lab.

At the end of those links would be a combination of two letters, like "bG." By sticking variations of two letters at the end of the domains, researchers found large caches of fake sign-in pages with the target's email address already filled in, the researchers said.

Security researchers matched link shorteners used by Belltrox to those

used against short sellers for Wirecard and journalists who had published critical articles, among others. At least 130 of these fake sign-in pages were uploaded on Nov. 29, 2017, to the Internet Archive, otherwise known as the Wayback Machine, a nonprofit digital library that stores copies of internet pages. It's not clear who uploaded the pages there.

Those pages show that dozens of people from at least 10 hedge funds and research firms were targeted with a variety of phishing attempts. They all had a history of short-selling Wirecard stock or publishing critical reports about the firm.

Custom link shorteners used in hacking operations have also been used publicly by Belltrox employees, including in one case to link to an online version of the employee's resume, according to Citizen Lab and another cybersecurity researcher.

The archived pages show these hackers set up bogus log-in pages for several top executives at Coatue Management, including the chief investment officer, chief financial officer, chief legal officer, general counsel and two senior managing directors. At a second firm, the hedge fund Theleme Partners, four people were targeted, including the firm's founder and chief executive officer, Patrick Degorce. Five employees at Blue Ridge Capital were targeted.

Coatue declined to comment. Theleme and Blue Ridge didn't respond to requests for comment.

In another alleged Belltrox operation, the Electronic Frontier Foundation in a 2017 blog post detailed cyberattacks on activists fighting for "net neutrality," a policy that seeks to treat all internet traffic equally and which telecommunications companies have aggressively lobbied against. One of the targets of the alleged attacks, Evan Greer, told Bloomberg News that she was already on high alert when she realized someone was

trying to hack her email.

For several weeks in 2017, her colleagues at Fight for the Future, an advocacy group engaged in a battle over the internet rules, had been receiving "phishing" emails—phony messages that appeared to be from friends, family and colleagues but in fact were trying to trick them to give up passwords. Among them was an email Greer received from an account in the name of Sophia Johnson, saying she wanted to buy some of Greer's music.

Greer replied with a link to her Bandcamp page. But the Johnson account sent back a message saying she was having problems purchasing the music and included a link asking if it was the right one. "Thanks for your reply, but link is not working. Kindly check this link," said the email, which was published in the blog post. It led to a bogus Google sign-in page, an apparent attempt to steal her password.

"That's when we were like 'This is serious. This is sophisticated,'" Greer said. "Clearly whoever was doing this had done some amount of research on us. They were clearly targeting us, and it seems very likely that someone was paying them to do so."

Eva Galperin, a cybersecurity researcher at the Electronic Frontier Foundation, said the hackers who targeted Greer also attempted to hack activists in similar groups for months. (EFF provided assistance to Greer and other activists who were attacked.) Although she's seen more sophisticated attacks in her career, these stood out for their ingenuity and persistence. "All they needed to do to get access was to have one of their targets have one bad day and rush through and click something. They took advantage of that very, very quickly." EFF's blog post didn't identify the hackers. Citizen Lab linked the EFF hack to the Belltrox hacking operation, and it said another net neutrality advocacy group, Free Press, was also targeted.

The hacker-for-hire scheme also targeted climate-change activists involved in a campaign called #ExxonKnew, according to Citizen Lab. Hacking attempts were made against the personal and business email accounts of those involved in the campaign, which accused Exxon of conspiring to cover up its early knowledge of climate change. Family members, including a minor child, were also targeted, according to Citizen Lab.

A document stolen by hackers that outlined a potential legal strategy against Exxon was published in a news article, according to court documents. The filings don't identify who stole the document. Exxon Mobil has no knowledge of, or involvement in, the hacking activities outlined in Citizen Lab's report, the company said.

Although the full scope of the federal investigation into the hacking-for-hire operation isn't known, Azari's arrest by federal agents last September after he arrived at New York's John F. Kennedy Airport provides a glimpse into the inquiry.

U.S. prosecutors accuse Azari, who ran an investigations firm in Haifa, Israel, of working with a group of Indian hackers that targeted hundreds of victims and infiltrated the accounts of at least six, including several in New York City, according to the indictment, which was unsealed the day after his arrest. Azari was an alleged facilitator for hackers who used "spear-phishing" attacks against targets he identified to steal login credentials for all manner of digital troves—work and personal email accounts, social media sites, online storage services.

The indictment doesn't name the Indian hacking group working with Azari. However, because of an apparent error, the indictment reveals the last name of one of the hackers, which also matches the name of a Belltrox employee whose LinkedIn account lists a variety of hacking skills. That person didn't respond to a request for comment.

According to the indictment, the hackers described themselves as "Email Penetration Experts, sophisticated developers for extracting files," capable of getting "the backup of the email from any account and files from any windows computer." The hackers told Azari: "We can make some money working together."

Belltrox Digital Security was incorporated in Rajasthan, India, in 2012 and marketed itself as "a leading cyber investigation litigation support firm." The company's partners split in 2013, according to Mehra, and Gupta renamed the firm Belltrox Infosec Services. The latest incarnation of the website advertised, "You desire, we do."

In an online biography, Gupta describes Belltrox as a "cyber intelligence services company" that caters to "private investigators, corporate lawyers, corporate investigators, corporate firms, celebrities and politicians." Although Belltrox Infotech Services markets itself as a medical transcription company, several of its employees tout their hacking skills or cybersecurity expertise on LinkedIn.

In 2015, Gupta, who also goes by Sumit Vishnoi, was indicted by federal prosecutors in 2015 in California on 10 counts of email and computer hacking. Two San Francisco-area private investigators were charged with hiring Gupta to access the emails of defendants in a legal dispute between two multilevel marketing companies.

Prosecutors unsuccessfully sought his arrest in India; a person familiar with the case said U.S. authorities had difficulty getting cooperation from the Indian government. The case against Gupta stalled, and it was ultimately rolled into a larger federal investigation, said the person, who declined to elaborate. It's not clear whether there's a link between the Gupta case and the current hacker-for-hire investigation.

Nonetheless, it illustrates the difficulty of prosecuting such an operation.

The middlemen in that case, the two private investigators, pleaded guilty; Gupta remains at large.