FOX NEWS .com

Print Close

Romanian hacker Guccifer: I breached Clinton server, 'it was easy'

By Catherine Herridge, Pamela K. Browne

Published May 04, 2016

FoxNews.com

EXCLUSIVE: The infamous Romanian hacker known as “Guccifer,” speaking exclusively with Fox News, claimed he easily – and repeatedly – breached former Secretary of State Hillary Clinton’s personal email server in early 2013.

"For me, it was easy ... easy for me, for everybody," Marcel Lehel Lazar, who goes by the moniker "Guccifer," told Fox News from a Virginia jail where he is being held.

Guccifer’s potential role in the Clinton email investigation was first reported by Fox News last month. The hacker subsequently claimed he was able to access the server – and provided extensive details about how he did it and what he found – over the course of a half-hour jailhouse interview and a series of recorded phone calls with Fox News.

Fox News could not independently confirm Lazar’s claims.

In response to Lazar’s claims, the Clinton campaign issued a statement Wednesday night saying, "There is absolutely no basis to believe the claims made by this criminal from his prison cell. In addition to the fact he offers no proof to support his claims, his descriptions of Secretary Clinton's server are inaccurate. It is unfathomable that he would have gained access to her emails and not leaked them the way he did to his other victims.”

The former secretary of state’s server held nearly 2,200 emails containing information now deemed classified, and another 22 at the “Top Secret” level.

2016 Election Headquarters

The latest headlines on the 2016 elections from the biggest name in politics. See Latest Coverage →

The 44-year-old Lazar said he first compromised Clinton confidant Sidney Blumenthal's AOL account, in March 2013, and used that as a stepping stone to the Clinton server. He said he accessed Clinton’s server “like twice,” though he described the contents as “not interest[ing]” to him at the time.

“I was not paying attention. For me, it was not like the Hillary Clinton server, it was like an email server she and others were using with political voting stuff," Guccifer said.

The hacker spoke freely with Fox News from the detention center in Alexandria, Va., where he’s been held since his extradition to the U.S. on federal charges relating to other alleged cyber-crimes. Wearing a green jumpsuit, Lazar was relaxed and polite in the monitored secure visitor center, separated by thick security glass.

In describing the process, Lazar said he did extensive research on the web and then guessed Blumenthal’s security question. Once inside Blumenthal's account, Lazar said he saw dozens of messages from the Clinton email address.

Asked if he was curious about the address, Lazar merely smiled. Asked if he used the same security question approach to access the Clinton emails, he said no – then described how he allegedly got inside.

“For example, when Sidney Blumenthal got an email, I checked the email pattern from Hillary Clinton, from Colin Powell from anyone else to find out the originating IP. … When they send a letter, the email header is the originating IP usually,” Lazar explained.

He said, “then I scanned with an IP scanner."

Lazar emphasized that he used readily available web programs to see if the server was “alive” and which ports were open. Lazar identified programs like netscan, Netmap, Wireshark and Angry IP, though it was not possible to confirm independently which, if any, he used.

In the process of mining data from the Blumenthal account, Lazar said he came across evidence that others were on the Clinton server.

"As far as I remember, yes, there were … up to 10, like, IPs from other parts of the world," he said.

With no formal computer training, he did most of his hacking from a small Romanian village.

Lazar said he chose to use "proxy servers in Russia," describing them as the best, providing anonymity.

Cyber experts who spoke with Fox News said the process Lazar described is plausible. The federal indictment Lazar faces in the U.S. for cyber-crimes specifically alleges he used "a proxy server located in Russia" for the Blumenthal compromise.

Each Internet Protocol (IP) address has a unique numeric code, like a phone number or home address. The Democratic presidential front-runner's home-brew private server was reportedly installed in her home in Chappaqua, N.Y., and used for all U.S. government business during her term as secretary of state.

Former State Department IT staffer Bryan Pagliano, who installed and maintained the server, has been granted immunity by the Department of Justice and is cooperating with the FBI in its ongoing criminal investigation into Clinton's use of the private server. An intelligence source told Fox News last month that Lazar also could help the FBI make the case that Clinton's email server may have been compromised by a third party.

Asked what he would say to those skeptical of his claims, Lazar cited "the evidence you can find in the Guccifer archives as far as I can remember."

Writing under his alias Guccifer, Lazar released to media outlets in March 2013 multiple exchanges between Blumenthal and Clinton. They were first reported by the Smoking Gun.

It was through the Blumenthal compromise that the Clintonemail.com accounts were first publicly revealed.

As recently as this week, Clinton said neither she nor her aides had been contacted by the FBI about the criminal investigation. Asked whether the server had been compromised by foreign hackers, she told MSNBC on Tuesday, "No, not at all."

Recently extradited, Lazar faces trial Sept. 12 in the Eastern District of Virginia. He has pleaded not guilty to a nine-count federal indictment for his alleged hacking crimes in the U.S. Victims are not named in the indictment but reportedly include Colin Powell, a member of the Bush family and others including Blumenthal.

Lazar spoke extensively about Blumenthal's account, noting his emails were "interesting" and had information about "the Middle East and what they were doing there."

After first writing to the accused hacker on April 19, Fox News accepted two collect calls from him, over a seven-day period, before meeting with him in person at the jail. During these early phone calls, Lazar was more guarded.

After the detention center meeting, Fox News conducted additional interviews by phone and, with Lazar's permission, recorded them for broadcast.

While Lazar's claims cannot be independently verified, three computer security specialists, including two former senior intelligence officials, said the process described is plausible and the Clinton server, now in FBI custody, may have an electronic record that would confirm or disprove Guccifer's claims.

"This sounds like the classic attack of the late 1990s. A smart individual who knows the tools and the technology and is looking for glaring weaknesses in Internet-connected devices," Bob Gourley, a former chief technology officer (CTO) for the Defense Intelligence Agency, said.

Gourley, who has worked in cybersecurity for more than two decades, said the programs cited to access the server can be dual purpose. "These programs are used by security professionals to make sure systems are configured appropriately. Hackers will look and see what the gaps are, and focus their energies on penetrating a system," he said.

Cybersecurity expert Morgan Wright observed, "The Blumenthal account gave [Lazar] a road map to get to the Clinton server. ... You get a foothold in one system. You get intelligence from that system, and then you start to move."

In March, the New York Times reported the Clinton server security logs showed no evidence of a breach. On whether the Clinton security logs would show a compromise, Wright made the comparison to a bank heist: "Let's say only one camera was on in the bank. If you don't have them all on, or the right one in the right locations, you won't see what you are looking for."

Gourley said the logs may not tell the whole story and the hard drives, three years after the fact, may not have a lot of related data left. He also warned: "Unfortunately, in this community, a lot people make up stories and it's hard to tell what's really true until you get into the forensics information and get hard facts."

For Lazar, a plea agreement where he cooperates in exchange for a reduced sentence would be advantageous. He told Fox News he has nothing to hide and wants to cooperate with the U.S. government, adding that he has hidden two gigabytes of data that is "too hot" and "it is a matter of national security."

In early April, at the time of Lazar's extradition from a Romanian prison where he already was serving a seven-year sentence for cyber-crimes, a former senior FBI official said the timing was striking.

"Because of the proximity to Sidney Blumenthal and the activity involving Hillary's emails, [the timing] seems to be something beyond curious," said Ron Hosko, former assistant director of the FBI's Criminal Investigative Division from 2012-2014.

The FBI offered no statement to Fox News.

Catherine Herridge is an award-winning Chief Intelligence correspondent for FOX News Channel (FNC) based in Washington, D.C. She covers intelligence, the Justice Department and the Department of Homeland Security. Herridge joined FNC in 1996 as a London-based correspondent.

Pamela K. Browne is Senior Executive Producer at the FOX News Channel (FNC) and is Director of Long-Form Series and Specials. Her journalism has been recognized with several awards. Browne first joined FOX in 1997 to launch the news magazine "Fox Files" and later, "War Stories."

Print Close

URL

http://www.foxnews.com/politics/2016/05/04/romanian-hacker-guccifer-breached-clinton-server-it-was-easy.html

Home | Video | Politics | U.S. | Opinion | Entertainment | Tech | Science | Health | Travel | Lifestyle | World | Sports | Weather

Privacy | Terms