EXCLUSIVE

ALL GRU'D UP

'Lone DNC Hacker' Revealed as Russian Intelligence Officer

SPENCER ACKERMAN, KEVIN POULSEN

03.22.18 7:00 PM ET

PHOTO ILLUSTRATION BY THE DAILY BEAST

Guccifer 2.0, the "lone hacker" who took credit for providing WikiLeaks with stolen emails from the Democratic National Committee, was in fact an officer of Russia's military intelligence directorate (GRU), The Daily Beast has learned. It's an attribution that resulted from a fleeting but critical slip-up in GRU tradecraft.

That forensic determination has substantial implications for the criminal probe into potential collusion between President Donald Trump and Russia. The Daily Beast has learned that the special counsel in that investigation, Robert Mueller, has taken over the probe into Guccifer and brought the FBI agents who worked to track the persona onto his team.

While it's unclear what Mueller plans to do with Guccifer, his last round of indictments charged 13 Russians tied to the Internet Research Agency troll farm with a conspiracy "for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016." It was Mueller's first move establishing Russian interference in the election within a criminal context, but it stopped short of directly implicating the Putin regime.

Mueller's office declined to comment for this story. But the attribution of Guccifer 2.0 as an officer of Russia's largest foreign intelligence agency would cross the Kremlin threshold —and move the investigation closer to Trump himself.

Trump's longtime political adviser Roger Stone admitted being in touch with Guccifer over Twitter's direct messaging service. And in August 2016, Stone published an article on the pro-Trump-friendly Breitbart News calling on his political opponents to "Stop Blaming Russia" for the hack. "I have some news for Hillary and Democrats—I think I've got the real culprit," he wrote. "It doesn't seem to be the Russians that hacked the DNC, but instead a hacker who goes by the name of Guccifer 2.0."

Five months later, in January 2017, the CIA, NSA, and FBI assessed "with high confidence" that "Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data." But the assessment did not directly call Guccifer a Russian intelligence officer. Nor did it provide any evidence for its assertions.

It turns out there is a powerful reason to connect Guccifer to the GRU.

Guccifer 2.0 sprang into existence on June 15, 2016, hours after a report by a computer security firm forensically tied Russia to an intrusion at the Democratic National Committee. In a series of blog posts and tweets over the following seven months—conspicuously ending right as Trump took office and not resuming—the Guccifer persona published a smattering of the DNC documents while gamely projecting an image as an independent Romanian hacktivist who'd breached the DNC on a lark. As Stone's Breitbart piece demonstrated, Guccifer provided Moscow with a counter-narrative for the election interference.

Guccifer famously pretended to be a "lone hacker" who perpetrated the digital DNC break-in. From the outset, few believed it. Motherboard conducted a devastating interview with Guccifer that exploded the account's claims of being a native Romanian speaker. Based on

forensic clues in some of Guccifer's leaks, and other evidence, a consensus quickly formed among security experts that Guccifer was completely notional.

RELATED IN POLITICS

Guccifer 2.0 is a Russian Officer. Does That Mean Collusion?

Cambridge Analytica Looked to Pounce on Russian Hacks

The Opening Argument in the Trial of Donald J. Trump

"Almost immediately various cyber security companies and individuals were skeptical of Guccifer 2.0 and the backstory that he had generated for himself," said Kyle Ehmke, an intelligence researcher at the cyber security firm ThreatConnect. "We started seeing these inconsistencies that led back to the idea that he was created hastily… by the individual or individuals that affected the DNC compromise."

Proving that link definitively was harder. Ehmke worked on an investigation at ThreatConnect that tried to track down Guccifer from the metadata in his emails. But the trail always ended at the same data center in France. Ehmke eventually uncovered that Guccifer was connecting through an anonymizing service called Elite VPN, a virtual private networking service that had an exit point in France but was headquartered in Russia.

But on one occasion, The Daily Beast has learned, Guccifer failed to activate the VPN client before logging on. As a result, he left a real, Moscow-based Internet Protocol address in the server logs of an American social media company, according to a source familiar with the government's Guccifer investigation. Twitter and WordPress were Guccifer 2.0's favored outlets. Neither company would comment for this story, and Guccifer did not respond to a direct message on Twitter.

Working off the IP address, U.S. investigators identified Guccifer 2.0 as a particular GRU officer working out of the agency's headquarters on Grizodubovoy Street in Moscow. (The Daily Beast's sources did not disclose which particular officer worked as Guccifer.)

Security firms and declassified U.S. intelligence findings previously identified the GRU as the agency running "Fancy Bear," the ten-year-old hacking organization behind the DNC

email theft, as well as breaches at NATO, Obama's White House, a French television station, the World Anti-Doping Agency, and countless NGOs, and militaries and civilian agencies in Europe, Central Asia, and the Caucasus.

Timestamps in Guccifer 2.0's first leaks show they were packaged for release over the course of a single day in June 2016, beginning just hours after the DNC intrusion and its attribution to Russia were made public. The moniker was an homage to Romanian hacker Marcel Lazăr Lehel, who as "Guccifer" achieved notoriety in 2013 for a string of hacks against celebrities and politicians.

In his inaugural blog post, Guccifer 2.0 disputed Russia's involvement and claimed credit personally for the DNC breach, positioning himself as a one-time hacking operation working to expose "the Illuminati." The post included the world's first glimpse of the enormous cache of documents siphoned from the DNC's network, including the Democrats' opposition research report on Trump. Presaging the leaks that would roil the election, Guccifer 2.0 declared that he'd already sent the bulk of the stolen material to WikiLeaks—which has spent the time since obfuscating whether Guccifer was its source.

On July 22, 2016, WikiLeaks began releasing its cache of approximately 19,000 emails and 8,000 attachments stolen in the hack. While Trump promoted the leak on Twitter and in rallies, his surrogate Roger Stone pushed back against the Kremlin attribution. In his August 2016 article for Breitbart, he argued that Guccifer 2.0 was the Romanian hacktivist he claimed to be. "Guccifer 2.0 is the real deal," he wrote.

Last May, Stone admitted that he'd also exchanged direct messages with the Guccifer 2.0 persona, and he released what he claimed was a complete transcript of his communications with the account. The transcript is brief and banal, showing Stone congratulating Guccifer 2.0 on returning to Twitter after a brief suspension, and then mostly ignoring him. Then and since, Stone has consistently denied that Guccifer was connected to the Kremlin.

"I myself had no contacts or communications with the Russian State, Russian Intelligence or anyone fronting for them or acting as intermediaries for them," he wrote.

Guccifer 2.0 maintained a sporadic online presence throughout the election, posting to his dedicated WordPress blog and on Twitter, and spilling more DNC documents, sometimes in private emails to journalists.

While the national election clearly interested him ("Democrats prepare new provocation against Trump," he thundered in October 2016), Guccifer 2.0 reached down the ballot as

well, posting documents from the Democrats' national campaign committee on his WordPress blog. There, readers could find internal Democratic candidate assessments relevant to battleground states like Pennsylvania and Florida; internal assessments of key congressional districts, with granular analyses of their demographics; and campaign recruitment material.

The GRU officer was eager to share this trove, as well. A GOP political operative in Florida, Aaron Nevins, DM'd Guccifer 2.0 a request for "any Florida based information" and received 2.5 gigabytes' worth, according to *The Wall Street Journal*. The data, he enthused to Guccifer 2.0, was "probably worth millions of dollars." A consultant for a successful Florida Republican congressional candidate told the paper, "I did adjust some voting targets based on some data I saw from the leaks."

Sometime after its hasty launch, the Guccifer persona was handed off to a more experienced GRU officer, according to a source familiar with the matter. The timing of that handoff is unclear, but Guccifer 2.0's last blog post, from Jan. 12, 2017, evinced a far greater command of English than the persona's earlier efforts.

"It's obvious that the intelligence agencies are deliberately falsifying evidence," the post read. "In my opinion, they're playing into the hands of the Democrats who are trying to blame foreign actors for their failure."

(Contrast that with the language from a June 2016 post: "I made some conclusions from the Marcel's story and decided not to put all eggs in one basket. Moreover, other cases weren't so successful and didn't bring me the glory.")

Today the most popular counter-narrative surrounding Guccifer 2.0 concedes that the account was a fake persona but posits that it was created by the DNC to support a false-flag operation implicating Russia. In this theory, advanced in two widely cited anonymous blogs, Guccifer 2.0 was the DNC posing as Russia posing as a Romanian hacker.

© 2017 THE DAILY BEAST COMPANY LLC