

<https://www.theguardian.com/us-news/2016/jul/26/russia-hackers-democratic-national-committee-email-leak>

US believes Russian hackers are behind Democratic National Committee leak

This article is more than **4 years old**

Growing consensus within Obama administration is that Russians infiltrated DNC but there is less certainty that Vladimir Putin's government is responsible

Sam Thielman and Spencer Ackerman in New York

Tue 26 Jul 2016 23.47 EDT Last modified on Wed 26 Feb 2020 13.00 EST



The cyberattack led to tens thousands of internal DNC emails spilling onto the internet ahead of the Democrat national convention, enraging Bernie Sanders supporters. Photograph: John Minchillo/AP

The emerging consensus within the Obama administration is that Russian hackers successfully infiltrated the data networks of the Democratic National Committee, the Guardian has learned, although there is less certainty that the Russian government is definitively responsible for the attack.

A senior administration official said indications in the code used to execute the data breach points to Russian culprits. That assessment matches the preliminary conclusions from a recent series of cybersecurity firms that have analyzed the hack.

The official, who was not cleared to discuss an attack that has roiled US politics and relations with Moscow, could not “unequivocally” attribute the attack to a “Russian state actor”.

Advertisement

But the operating theory and animating belief inside the administration is that the attack, which led to [tens thousands of internal DNC emails](#) spilling onto the internet ahead of the Democrats’ presidential nominating convention, enraging Bernie Sanders supporters by suggesting bias against him among party staff and leading to the [resignation of DNC chair Debbie Wasserman Schultz](#), was Russian in origin.

Neither the White House nor the office of the director of national intelligence would confirm a New York Times [article](#) late Tuesday reporting that US intelligence agencies consider Vladimir Putin’s government to be responsible for the attack on the DNC. Queries to the FBI, which Barack Obama has now placed [in charge of responding to cyber threats](#), were not immediately returned.

The Daily Beast reported on Monday that the FBI [believes](#) the Russian government to be behind the DNC hack. The FBI has confirmed that it is investigating the breach.

The self-proclaimed source for scores of DNC emails published by WikiLeaks, known as Guccifer 2.0, is not a single operator but [Russian cybercriminals designated Fancy Bear and Cozy Bear](#) by investigators who have invaded the White House and the Bundestag between them, according to leading cybersecurity firms.

Security firm ThreatConnect issued a comprehensive report on Tuesday using their own data and data from previous reports by rivals [CrowdStrike](#), Mandiant and Fidelis.

Advertisement

Crowdstrike associates Fancy Bear with other Russian intrusions, notably one into [the German Bundestag](#) in May and another into French television network [TV5 Monde](#). Cozy Bear has dug into the [state department](#) the [joint chiefs](#), and [the White House](#), said CrowdStrike, which analyzed those hacks.

“We’ve had lots of experience with both of these actors attempting to target our customers in the past and know them well,” [wrote](#) CrowdStrike’s Dmitri Alperovitch. “In fact, our team considers them some of the best adversaries out of all the numerous nation-state, criminal and hacktivist/terrorist groups we encounter on a daily basis.”

Alperovitch [told the Christian Science Monitor](#) earlier in July he had “high-level confidence” that Fancy Bear and Cozy Bear represented Russian spy agencies. Alperovitch said he believed with what he called “medium level confidence” that Fancy Bear represented Russia’s Main Intelligence Directorate (GRU), Russia’s largest intelligence agency. He had “low level confidence” that Cozy Bear was the work of the Federal Security Service (FSB).

The new ThreatConnect report suggests that the person who has been giving interviews under the name Guccifer 2.0 to the press isn't a hacker at all.

'I find it interesting'

In June, Guccifer contacted Vocativ writer [Kevin Collier](#) through Twitter to offer a story about the DNC leaks, insisting on encryption; Collier said the story he received by email was so offbeat he asked Guccifer what good it could possibly be. "I find it interesting" was the only reply.

Collier also said there was something else odd about the email: it had come from a French AOL service so insecure that it included the sender's IP address in the email.

"It's baffling," Collier said. "He's either an amateur, made a huge mistake, or this is part of an incredibly intricate disinformation campaign. Since the going theory of the DNC hack is that it was perpetrated by Russian government groups that then passed this information to propagandists or professional trolls to spread, my best guess is it was just a rookie mistake."

The sender had used a proxy, but the proxy masking Guccifer's location was Russian.

[Facebook](#)[Twitter](#)[Pinterest](#)

[Trump on claims that Russia hacked DNC emails for him: 'far-fetched'](#)

Advertisement

Guccifer 2.0 had always claimed to be Romanian like the original Guccifer, imprisoned hacker Marcel Lazăr Lehel, but the 2.0 version had regularly communicated with journalists in Russian. When Motherboard reporter Lorenzo Franceschi-Bicchieri asked Guccifer 2.0 to speak Romanian, the few sentences that came back were [filled with mistakes](#).

Then there was the way Guccifer claimed to have attacked the DNC with a "zero-day" hack into a software called Votebuilder used by the DNC. A zero-day hack finds a vulnerability in the software that was previously unknown to the target.

A backdoor into Votebuilder would only be valuable to someone attacking the DNC; most black-market activity focuses on exploitation of widely used software that can be used on multiple targets to make money until it is discovered and closed down.

Toni Gidwani, director of research operations for ThreatConnect, said: "There are much easier ways to get in."

Another security company, Secureworks, found what may be the culprit: [a fake Google login page](#) targeting the Clinton campaign.

Gidwani said the various mistakes and inconsistencies indicate to ThreatConnect that a lot of the decisions around the hack appear to have been arrived at by committee with varying degrees of knowledge about hacking.

“It would suggest to us that the operators of the Guccifer 2.0 persona were not the actors who breached the DNC,” she said. “You’re looking at the operations guys who don’t have the same technical credibility as these very sophisticated actors who exploited these networks. You’ve got a lot of cooks in this kitchen here, not just one actor.”