Cybersecurity experts see merit in claims of Russian hacking

July 26 2016, by Raphael Satter

In this July 1, 2016 file photo, a ruby star on the Kremlin's Nikolskaya Tower is reflected in a window glass of GUM department store in Red Square in Moscow, Russia. Experts who've followed the leak of Democratic National Committee documents say they believe the party's claim that Moscow had a hand in the hack, lending weight to the extraordinary allegation that the Kremlin is trying to tamper with the U.S. presidential contest. (AP Photo/Ivan Sekretarev, File)

Experts who've followed the leak of Democratic National Committee documents say they believe the party's claim that Moscow had a hand in the hack, lending weight to the extraordinary allegation that the Kremlin is trying to tamper with the U.S. presidential contest.

"You're left with all the signs pointing to Moscow," said Matt Tait, a U.K.-based cybersecurity consultant who has put in roughly 20 hours combing through the leaked DNC documents.

Tait and others invoke several categories of evidence. The first was provided by threat intelligence firm CrowdStrike, an Irvine, California company that was hired by the Democrats to clean out the party's network. It delivered a report last month identifying Russia's intelligence services as being behind two separate electronic break-ins at the DNC. The second category of evidence was provided by electronic fingerprints on some of the documents suggesting the files had been run through Russian language-configured machines.

Most convincing for Tait was evidence that the internet infrastructure tied the DNC hackers to a separate campaign that targeted Germany's parliament last year. In May, Germany's domestic intelligence chief took the unusual step of publicly blaming that attack on Moscow, saying the Kremlin wasn't just spying—it was gearing up for sabotage.

"More than anything else I think (that) really puts to rest the 'Who is this?'" Tait said Tuesday. "It's one thing to say that they were typing stuff in Russian or they were coming from a Russian IP (internet protocol) address or their systems were configured in Russian. It's another thing to say this was being run by the same servers being publicly attributed by German intelligence as being Russian."

Hillary Clinton's campaign, citing CrowdStrike, blamed Russia for hacking the party's computers and suggested the goal was to benefit

Donald Trump's campaign. On Twitter, Trump dismissed that idea as a joke. A spokesman for Russian President Vladimir Putin on Tuesday called the allegation "paranoid."

WikiLeaks founder Julian Assange, who began publishing thousands of the emails last week, said Monday that there was "no proof" Russia was behind the hack.

On Tuesday, leaders of the Senate Judiciary Committee pressed the FBI and Justice Department for details on the investigation, including how and when federal investigators learned of the breach and what action is being taken in response.

Assigning blame in the world of cyberespionage is extraordinarily difficult. Some of the clues uncovered by Tait are easy to forge and attackers routinely use misdirection to lead investigators astray. Others in the field are wary of companies such as CrowdStrike, which may face pressure from clients or investors to spin gripping stories about government hackers with codenames like "Fancy Bear" or "APT28."

"I don't like circumstantial evidence when it comes to blaming a foreign government," said Jeffrey Carr, the chief executive of Taia Global, a threat intelligence company. Carr rejected the idea of tying the DNC attackers to previous breaches based on their tools or their methods, saying it was "like finding a gun that was used in the commission of a crime. Anybody could be pulling the trigger."

So far the only public claim of responsibility for the breach has come from a previously unknown actor calling himself Guccifer 2.0. The self-described lone Romanian hacker has uploaded several tranches of DNC material to a website in the past month and boasted of handing a larger trove to WikiLeaks.

Guccifer 2.0 has not responded to repeated messages from The Associated Press, but doubts about his story are growing. On Tuesday, ThreatConnect, an intelligence firm based in Arlington, Virginia, said it found evidence that the hacker was communicating with journalists via a dedicated virtual private network based out of Russia. Motherboard journalist Lorenzo Franceschi-Bicchierai said the hacker stumbled through an interview over Twitter when quizzed in Romanian last month.

"We showed it to half a dozen Romanians and no one had one iota of a doubt that the person behind the keyboard was not Romanian," Franceschi-Bicchierai said in an email.

Thomas Rid, a cybersecurity expert with King's College London, first identified the common infrastructure linking the DNC and German parliamentary hacks. He said there was a "very high level of confidence" both attacks were the work of the same group and that it was noteworthy that German officials had tied the group to Moscow.

"Traditionally Germany's intelligence has a very good coverage of Russia," Rid said. "When they come out and explicitly name a Russian military intelligence service—and they do that at significant political cost—then we just have to take that very seriously."

Citation: Cybersecurity experts see merit in claims of Russian hacking (2016, July 26) retrieved 19 April 2024 from
https://phys.org/news/2016-07-cybersecurity-experts-merit-russian-hacking.html