DNC hack: What you need to know

By Tal Kopan, CNN

Updated 1:30 PM ET, Tue June 21, 2016

Cyber experts: Russia hacked DNC, stole Trump research

Cyber experts: Russia hacked DNC, stole Trump research 02:27

STORY HIGHLIGHTS

The Democratic National Committee discovered it had been hacked and announced its findings last week

The perpetrators were believed to be linked to the Russian government

Washington (CNN)After the Democratic National Committee discovered it had been hacked, it made the unusual move of quickly revealing the breach to the public -- including that the perpetrators were believed to be linked to the Russian government.

Since initially making the cyberattack public last week, an online personality has surfaced, claiming to have documents from the DNC files and having no connection to the Russians.

But the claims made by the "Guccifer 2.0" individual are viewed with a dose of skepticism by experts who have analyzed the events.

Here's an explanation of what we know about the hack.

So what happened?

The DNC and the cybersecurity firm that investigated the hack announced last week that it had been breached by two separate cyberespionage groups. One set of these hackers had been in the system about a year and had been monitoring internal communications, including email.

The other group of hackers had only been in the system a few months and had one target: The DNC's opposition research on Donald Trump. That research file was the only data that researchers could definitively say had been taken by the hackers.

RELATED: Russian hackers stole Trump files, firm says

Both groups were linked to the Russian military-intelligence world by cybersecurity firm CrowdStrike, though they did not appear to even be aware of each others' presence in the DNC system. Given the divided nature of the Russian power structure, it's not uncommon to see hacking groups working for different branches of the Russian military and intelligence agencies without overall coordination, CrowdStrike co-founder and Chief Technology Officer Dmitri Alperovitch said.

Researchers could not definitively find how the groups got into the system, but the typical way in for the groups is through carefully crafted deceptive emails, called "spearphishing," that trick recipients into clicking malicious links.

The hackers were kicked out of the system the weekend before the DNC went public, and CrowdStrike continues to monitor for attempts to break in again.

Why do they believe it's the Russians?

High-level cyberespionage groups are skilled units of hackers, who work like digital thieves to break into chosen targets and take information.

Each of these groups has certain distinct signatures, from the way they get in, to the specially crafted malicious software they use, to the type of information that is taken and how it is transmitted out.

The cybersecurity firms that respond to breaches and monitor organizations' networks see these hackers regularly, and investigate them. They put together databases and files on the distinct groups, often giving them names for easy reference.

CrowdStrike names Russian-linked groups it researches "bears." It identified the hackers that took Trump's oppo file and got in this spring as "Fancy Bear," and the group that got in last year to monitor communications as "Cozy Bear."

RELATED: Trump: DNC hacked itself

Both "bears" have a long history of targeting organizations with strategic importance to Russia that CrowdStrike has monitored, and "Cozy Bear" has also been credited with hacking into the networks of the White House, State Department and Joint Chiefs of Staff.

"We've had lots of experience with both of these actors attempting to target our customers in the past and know them well," wrote Alperovitch in a blog post detailing their technical findings. "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."

And it isn't just CrowdStrike -- other cybersecurity firms have since backed up their findings. Fidelis wrote in a post that it had analyzed the samples of the software and technical findings from the breach and also found Cozy Bear (aka APT 29 and CozyDuke, depending on firm's naming systems) and Fancy Bear (aka APT 28, Sofacy and Strontium) to be responsible. Two other companies, Mandiant and ThreatConnect, also told The Washington Post they had verified the findings.

Why would the Russians even hack the DNC?

Many governments worldwide have high-level cyberespionage groups working for them, who may target secrets from other governments, intelligence agencies, government contractors, think tanks and academics.

Just like in traditional espionage, the goal of digital spying is to vacuum up information that could be useful to the motherland. That could be anything from secret engineering plans for fighter jets to classified state secrets to insight into political figures' motivations and behavior.

There is keen interest overseas in the U.S. presidential election, and understanding the candidates would be important to other nations that would have to deal with their potential administration.

And Trump's file may be of special interest, as he has one of the shortest political resumes of any modern presidential candidate. With his relative newness to the scene, insight and research into his history is valuable.

What about this other claim?

The person claiming to be Guccifer 2.0 posted several documents on the Internet and sent them to media outlets including Gawker, portraying the documents as coming from the hack of the DNC's files. The documents included a file about Trump and what looked like memos about DNC operations.

But there is no way to verify the identity of this Guccifer 2.0 individual. The name is a reference to a Romanian hacker who pleaded guilty to hacking several prominent politicians and figures, including Presidents George W. Bush and George H.W. Bush, who went online by Guccifer.

There is also no way to verify the authenticity of the documents. The DNC would not comment on their veracity and the alleged hacker offered no proof that they were what they purported to be.

The character could even be an invention of the Russians to try to lay seeds of doubt and plausible deniability about their involvement in the hack. And it could be an individual looking to capitalize on the media attention for his or her own ends.