German authorities charge Russian hacker for 2015 Bundestag hack

By Catalin Cimpanu

Published: 2020-05-05 · Archived: 2026-04-05 22:58:43 UTC

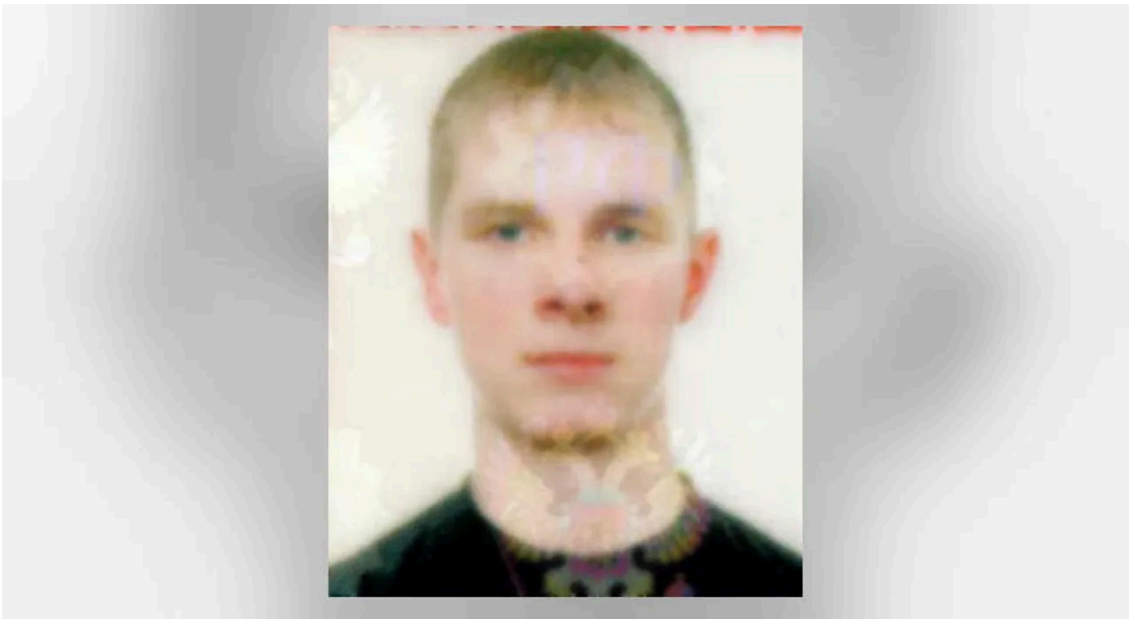

Image: FBI

German prosecutors have issued an arrest warrant today for a hacker working for the Russian military on charges of hacking the German Parliament in the spring of 2015.

German newspaper the Sueddeutsche Zeitung, who broke the story today, says German authorities are looking for Dmitriy Sergeyevich Badin, 29, from Kursk, Russia.

German authorities believe that Badin is a member of a Russian military Unit 26165, a unit part of the Russian Main Intelligence Directorate (GRU), the military intelligence agency of Russia's armed forces.

As part of this unit, German authorities believe that Badin was tasked with conducting cyber-espionage on behalf of the Russian state, being part of a hacking group identified by cyber-security firms as ATP28 (Fancy Bear, Sofacy, Strontium, Grizzly Steppe, and more).

The German newspaper says that between April and May 20, 2015, APT28 breached the internal network of the German Parliament (Bundestag).

Hackers used emails perpetrating to come from the United Nations to trick parliament staff into opening a malicious file about how Russia's involvement in the Ukrainian conflict has left the country's economy in shambles.

The boobytrapped document planted malware on staff computers, which allowed APT28 members to access the infected system and then spread to the Bundestag's entire network of more than 5,600 computers, including administrative systems.

Citing unnamed sources, Sueddeutsche Zeitung reports that German authorities have linked tools and malware used in this attack to Badin, personally, who at the time was one of the APT28 members.

The German Office of the Attorney General (Bundesanwaltschaft) was not immediately available for comment. German authorities have not yet made the arrest warrant and charges public.

Badin is also wanted in the US, where authorities have charged him and six other APT28 members in 2018 with attacks against the Democratic National Committee (DNC) and the World Anti-Doping Agency (WADA) between 2016 and 2018.

Badin is one of the FBI's most wanted cyber-criminals. He is still at large, believed to be living in Moscow.

Editorial standards
