Russian hackers breached Dutch police systems in 2017

therecord.media/russian-hackers-breached-dutch-police-systems-in-2017/

June 10, 2021

Hackers working on behalf of Russian intelligence services breached the internal network of Dutch police in 2017 during the country's investigation of the MH-17 crash.

The intrusion was kept under wraps by Dutch investigators until this week when multiple sources revealed the incident to Dutch newspaper the Volkskrant.

Breach occurred via Police academy server

According to the newspaper's reporting, the attack was traced back to September 2017, when Russian hackers used a vulnerability in an "exotic software" to breach a server belonging to the Dutch Police Academy, from where they pivoted to the main Dutch police network.

The intrusion was uncovered by AIVD, the Dutch intelligence service, after it saw a Dutch police IP address communicating with known malicious servers operated by Russian state-sponsored threat actors.

The AIVD, which previously breached a Russian intelligence service itself in 2014, alerted Dutch police.

Volkskrant said that due to a lack of monitoring/logging, the AIVD and Dutch Police have very little knowledge of what the hackers did inside the police network.

Sources also described several moments of friction between the two Dutch agencies when it came to deciding on how to handle the intrusion and subsequent clean-up, with the AIVD wanting to keep the hackers under surveillance while police officials wanted them removed from their systems due to the possibility of compromising sensitive cases.

Intrusion linked to Russian intelligence

Volkskrant said that sources linked the 2017 Dutch police hack to APT29 (Cozy Bear), a well-known hacking group that the White House linked earlier this year to the Russian Foreign Intelligence Service, also known as the SVR.

However, in a subsequent article update, Volkskrant said that attribution of the hack is far from accurate, as some sources also linked the attack to APT28 (Fancy Bear), a hacking group that was previously linked to the GRU, the Russian military intelligence service.

Neither Dutch police nor the AIVD confirmed or commented on the newspaper's reporting.

Either way, investigators were positive the attack was carried out by Russian intelligence as Dutch authorities were investigating the case of Malaysia Airlines Flight 17 (MH17), which they concluded was downed by a missile shot by rogue Russian-backed rebel forces active in eastern Ukraine.

During the investigation into the flight's crash, which was led by Dutch authorities, several Dutch organizations were targeted by both APT28 and APT29 on multiple occasions.

As part of the Russian government's desperate attempts at gaining insights into the investigation, Russian intelligence agents also traveled to the Netherlands to hack a police station and the Organisation for the Prohibition of Chemical Weapons (OPCW), a notorious incident for which the EU imposed sanctions against the Russian intelligence agents in 2020.

Tensions between Russia and the Netherlands remain high due to the MH-17 investigation.

A recent AIVD report claimed that Russia still ran influence operations in 2020, trying to discredit the findings of its MH-17 investigation.

Earlier this year, the Netherlands also said it discovered and kicked out two SVR agents working at the Russian embassy in The Hague under diplomatic accreditation.

Dutch officials, led by the AIVD, are also currently looking into making espionage a crime.

> Fun fact: espionage, while a crime in many places, is not in any extradition treaties.
>
> This causes some weird pretenses when country A might very much want to extradite a person from country B □👀 https://t.co/rOr4HUi5Ux
>
> — John Wetzel (@johnwetzel) June 9, 2021

Tags

- APT
- APT29
- Dutch police
- hack
- nation-state
- Russia
- SVR
- The Netherlands

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.