# Netherlands can use intelligence or armed forces to respond to ransomware attacks

therecord.media/netherlands-can-use-intelligence-or-armed-forces-to-respond-to-ransomware-attacks/

October 7, 2021

Image: Jason Leung

The Dutch government said it would use its intelligence or military services to counter cyber-attacks, including ransomware attacks, that threaten its national security.

Answering a parliamentary inquiry into the country's possible avenues of response to ransomware attacks, Ben Knapen, Dutch Minister of Foreign Affairs, said under normal circumstances, diplomatic avenues take precedence, but the country's response could be escalated in the case of more severe incidents.

"If a ransomware attack, whether or not with a financial objective, crosses the threshold of a (manifesting) threat to national security, for example due to the failure of critical sectors, then the government also has other resources at its disposal," Knapen said in a letter to the Dutch Parliament.

This process would involve investigating the attack, attributing it to a specific threat actor, and taking action against the aggressor.

"An example of the latter is taking IT infrastructure offline (or having it taken offline) that is part of the attack infrastructure or that is misused for digital espionage or sabotage," Knapen told the Dutch Parliament.

“In addition to action by [intelligence] services, the Netherlands can also respond with the Armed Forces. For example, the Defense Cyber Command can carry out a counter-attack *at the end of* the day to avert an enemy action or to protect an essential interest of the state,” Knapen added (emphasis taken from the minister’s letter).

## A warning shot for ransomware operators

Knapen said the Netherlands does not respond to all cyber-attacks in this manner but ordinarily relies on “diplomatic or legal channels” first.

But such responses are not unheard of. For example, following a series of attacks carried out by a state-sponsored hacking group known as APT29, the Dutch intelligence service AIVD hacked them back in 2014, with their intrusion allowing AIVD to warn the US State Department of an impending cyber operation.

However, Knapen told the Parliament that the Netherlands has not yet faced a ransomware attack large or severe enough to require involvement from its intelligence or military forces.

Ransomware attacks have hit Dutch companies in the past but only in isolated attacks, usually targeting private sector operators.

However, reading between the lines, the Dutch official’s letter is also a shot across the bow to ransomware gangs—a clear threat that if they cross the line, the Dutch state will reply, without warning and regardless of the country they operate from.

The move also comes after UK officials announced this week a similar plan to use the offensive cyber capabilities of their intelligence services to go after foreign threats, including ransomware gangs.

Tags

- AIVD
- Government
- intelligence agency
- military
- Netherlands
- Ransomware

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.