Related news

cyberscoop.com/belgium-cyber-espionage-china-microsoft-exchange/

May 26, 2021

government

Belgium uproots cyber-espionage campaign with suspected ties to China

Townhouses face and old canal and bridge in Brugge, or Bruges, Belgium. (Getty Images)
Written by Tim Starks
May 26, 2021 | CYBERSCOOP
A Belgian government ministry said this week that it was the victim of a cyber-espionage campaign that began two years ago, one that has apparent links to Beijing.

The Federal Public Service Interior said it began an investigation in March after Microsoft revealed that Chineses state-sponsored hackers had used zero-days to attack its Exchange Server technology. The ministry called in the Centre for Cyber Security Belgium for aid.

“The complexity of this attack indicates an actor who has cyber capacities and extensive resources,” the ministry aid in a statement on it website Tuesday. “The perpetrators acted in a targeted manner, which suggests espionage.”

A ministry spokesperson didn’t immediately answer a message about whether the attack it endured dating back to 2019 were explicitly linked to the espionage Microsoft first alleged two months ago, instead of merely triggering a probe that uncovered a separate campaign.

The earliest reported attacks exploiting the Exchange Server vulnerabilities surfaced in January of this year. But those vulnerabilities had been in its code base for more than 10 years. Microsoft blamed a Chineses government-connected group it calls Hafnium for exploiting the Exchange Server vulnerabilities.

Either way, Belgium cyber experts told local press that the campaign the FPS Interior described suggests Chinese involvement. Regardless of any direct links, the Microsoft Exchange Server zero-day announcement prompted reviews that turned up attacks across Europe.

The FPS Interior suggested that despite the attackers spending two years in its systems, the damage was both limited and now contained.

“Urgent action has been taken: attacker access has been stopped, malware has been removed and important information has been secured,” the website statement reads.

That said, the ministry also said its investigation is ongoing.

The announcement is the second time this month that news has broken about a cyberattack affecting the Belgium government. Earlier this month Belnet — which provides internet services to the nation’s parliament, government agencies, universities and scientific institutions — said a distributed denial of service attack disrupted internet availability.