Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:34:03 UTC

Description(Microsoft) HAFNIUM primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.

HAFNIUM has previously compromised victims by exploiting vulnerabilities in internet-facing servers, and has used legitimate open-source frameworks, like Covenant, for command and control. Once they've gained access to a victim network, HAFNIUM typically exfiltrates data to file sharing sites like MEGA.

In campaigns unrelated to these vulnerabilities, Microsoft has observed HAFNIUM interacting with victim Office 365 tenants. While they are often unsuccessful in compromising customer accounts, this reconnaissance activity helps the adversary identify more details about their targets' environments.

HAFNIUM operates primarily from leased virtual private servers (VPS) in the United States.

(Recorded Future) Coalition officials pinned the attacks on groups tracked as APT 31, Judgment Panda, Zirconium and Leviathan, APT 40, TEMP.Periscope by cybersecurity experts, according to a press release from the UK National Cyber Security Centre. Supporting statements were also issued by NATO, the UK government, the European Union Council, Australia, Japan, Canada, Latvia, Lithuania, Estonia, Slovenia, Finland, and Denmark.
