

Forum:[Hack Forums](#)

Thread: [Russian APT28 Deploys NotDoor Outlook Backdoor Against Companies in NATO Count](#)

Stanley - September 14, 2025, 8:55 pm

Russian APT28 Deploys "NotDoor" Outlook Backdoor Against Companies in NATO Count

The Russian state-sponsored hacking group tracked as APT28 has been attributed to a new Microsoft Outlook backdoor called NotDoor in attacks targeting multiple companies from different sectors in NATO member countries.

NotDoor "is a VBA macro for Outlook designed to monitor incoming emails for a specific trigger word," S2 Grupo's LAB52 threat intelligence team said. "When such an email is

<https://thehackernews.com/2025/09/russian-apt28-deploys-notdoor-outlook.html>

Mooooookie - September 14, 2025, 8:59 pm

"NotDoor" is a hell of a name for a BackDoor. I always wonder who comes up with the names for these things. Microsoft better get on top of patching this one up.. users expect their emails to be safe, when using Outlook.

The Pact - September 15, 2025, 1:33 am

I really HATE both Outlook and OneDrive and want no part of them though I use other Microsoft stuff a lot.

This attack showcases how legitimate business tools like Outlook and OneDrive can be weaponized for stealthy cyber-espionage. The use of email-based command-and-control must make detection especially difficult.

Yanix - September 15, 2025, 4:20 am

This is a reminder that even everyday software like Outlook can be weaponized. Cyber defense has to be one step ahead.