SOPHOS MDR THREAT CASE

DPRK Fake IT Worker discovered by Sophos MDR proactive threat hunt

ORGANIZATION

Industry Marketing
Size 1,000 Employees
Region USA

SOLUTION

Sophos MDR
+ Microsoft 365 Mgmt. Activity integration

Adversary activity

IT workers are sent by the Democratic People's Republic of Korea (DPRK) government to live primarily in China and Russia with a mission to secure lucrative roles within Western organizations – particularly in the U.S. tech sector – for financial exploitation.

21:00 UTC Sophos MDR analysts begin a **proactive threat hunt** relating to a known DPRK threat group and discover a **fake IT worker** within a customer's environment.

Threat detection

21:00–22:50 UTC The Sophos MDR team discovers a user persistently logging in using a **suspicious VPN** not used by other employees in the company.

An attempted **login blocked** by a Microsoft 365 Conditional Access Policy identifies that the user is located in Russia. The user has been **posing** as a remote software developer for the company for approximately six months.

Investigation

21:00–22:50 UTC Following analysis of the user's Microsoft 365 login activity, the Sophos MDR team investigates the threat actor's emails and identifies that, as a company employee, the user has gained **highly privileged** access within the organization's AWS cloud environment.

Response

22:51 UTC The Sophos MDR team **immediately alerts** the customer of the activity.

23:55 UTC Customer responds; the Sophos MDR team initiates a **live conference call** and provides guidance on next steps.

01:25 UTC Customer confirms that the user account has been **disabled**.

Learn more at sophos.com/MDR