SOPHOS MDR THREAT CASE

Rockstar 2FA phishing attack neutralized by Microsoft 365 response actions

SOPHOS

ORGANIZATION

Industry Automotive
Size 2,800 employees
Region Alabama, USA

SOLUTION

Sophos MDR
+ M365 Mgmt. Activity integration
+ M365 Response Actions integration

Adversary activity

12:56 UTC The adversary successfully **executes a phishing attack** and logs in to the user's Microsoft 365 account with the **stolen credentials**.

The attacker uses the "**Rockstar 2FA**" phishing kit designed to target Microsoft and Google accounts using adversary-in-the-middle (AiTM) techniques to steal credentials and bypass MFA. The phishing-as-a-service (PaaS) kit often uses compromised accounts and legitimate email platforms to deliver phishing links, directing victims to realistic fake login portals.

Threat detection

13:12 UTC A **proprietary Sophos detection rule** for Microsoft 365 identifies the use of the Rockstar 2FA phishing kit for authentication.

Investigation

13:13 UTC A case is generated automatically and assigned to a Sophos MDR security analyst. The analyst investigates and **uses Microsoft 365 response actions** to neutralize the threat.

Response

13:46 UTC The Sophos MDR analyst uses Microsoft 365 response actions to **disable sign-in** and **terminate active sessions** for the compromised user account.

13:48 UTC The Sophos MDR analyst escalates the activity to the customer and requests a **password reset** for the user's Microsoft 365 account.

14:05 UTC The customer confirms that the user's password has been reset. The analyst then **re-enables user sign-in** to restore access to the M365 account.

Learn more at sophos.com/MDR

SOPHOS