Amazon identified internet domains abused by APT29 | Amazon Web Services

Published: 2024-10-24 · Archived: 2026-04-05 13:31:25 UTC

AWS Security Blog

APT29 aka Midnight Blizzard recently attempted to phish thousands of people.

Building on work by CERT-UA, Amazon recently identified internet domains abused by APT29, a group widely attributed to Russia's Foreign Intelligence Service (SVR). In this instance, their targets were associated with government agencies, enterprises, and militaries, and the phishing campaign was apparently aimed at stealing credentials from Russian adversaries. APT29 sent the Ukrainian language phishing emails to significantly more targets than their typical, narrowly targeted approach. Some of the domain names they used tried to trick the targets into believing the domains were AWS domains (they were not), but Amazon wasn't the target, nor was the group after AWS customer credentials. Rather, APT29 sought its targets' Windows credentials through Microsoft Remote Desktop. Upon learning of this activity, we immediately initiated the process of seizing the domains APT29 was abusing which impersonated AWS in order to interrupt the operation. CERT-UA has issued an advisory with additional details on their work.

I'd like to thank the cyber threat intelligence teams at Amazon and CERT-UA for all their efforts to make the internet more secure.

This was originally shared on LinkedIn by Chief Information Security Officer and Amazon VP of Security Engineering CJ Moses.

If you have feedback about this post, submit comments in the **Comments** section below. If you have questions about this post, contact AWS Support.
