Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:49:50 UTC

APT group: TA2552

Names	TA2552 *(Proofpoint)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2019
Description	(Proofpoint) Since January 2020, Proofpoint researchers have tracked an actor abusing Microsoft Office 365 (O365) third-party application (3PA) access, with suspected activity dating back to August 2019. The actor, known as TA2552, uses well-crafted Spanish language lures that leverage a narrow range of themes and brands. The lures entice users to click a link in the message, taking them to the legitimate Microsoft third-party apps consent page. There they are prompted to grant a third-party application read-only user permissions to their O365 account via OAuth2 or other token-based authorization methods. TA2552 seeks access to specific account resources like the user's contacts and mail. Requesting read-only permissions for such account resources could be used to conduct account reconnaissance, silently steal data, or to intercept password reset messages from other accounts such as those at financial institutions. While organizations with global presence have received messages from this group, they appear to choose recipients who are likely Spanish speakers.
Observed	
Tools used	
Information	<https://www.proofpoint.com/us/blog/threat-insight/ta2552-uses-oauth-access-token-phishing-exploit-read-only-risks>

Last change to this card: 19 October 2020

Download this actor card in PDF or JSON format