Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:46:57 UTC

APT group: TA558

Names	TA558 *(Proofpoint)*	
Country	[Unknown]	
Motivation	Financial crime	
First seen	2018	
Description	(Proofpoint) Since 2018, Proofpoint has tracked a financially-motivated cybercrime actor, TA558, targeting hospitality, travel, and related industries located in Latin America and sometimes North America, and western Europe. The actor sends malicious emails written in Portuguese, Spanish, and sometimes English. The emails use reservation-themed lures with business-relevant themes such as hotel room bookings. The emails may contain malicious attachments or URLs aiming to distribute one of at least 15 different malware payloads, typically remote access trojans (RATs), that can enable reconnaissance, data theft, and distribution of follow-on payloads.	
Observed	Sectors: Construction, Education, Energy, Financial, Government, Hospitality, Industrial, IT, Pharmaceutical, Transportation. Countries: Algeria, Argentina, Brazil, Bulgaria, Chile, Colombia, Costa Rica, Czech, Dominican Republic, Ecuador, Germany, Guatemala, India, Indonesia, Lebanon, Macedonia, Mexico, Morocco, Pakistan, Peru, Poland, Romania, Russia, Serbia, Slovenia, South Korea, Spain, Thailand, Turkey, Uruguay, USA.	
Tools used	AsyncRAT, AZORult, Loda, njRAT, RemcosRAT, Vjw0rm, RevengeRAT, XtremeRAT.	
Operations performed	Jun 2023	SteganoAmor campaign: TA558 mass-attacking companies and public institutions all around the world <https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/>
Information	<https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel>	

Last change to this card: 22 April 2024

Download this actor card in PDF or JSON format
