Operation Comando - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:57:11 UTC

APT group: Operation Comando

Names	Operation Comando *(Palo Alto)*
Country	[Unknown]
Motivation	Financial crime
First seen	2018
Description	(Palo Alto) In December 2018, Palo Alto Networks Unit 42 researchers identified an ongoing campaign with a strong focus on the hospitality sector, specifically on hotel reservations. Although our initial analysis didn't show any novel or advanced techniques, we did observe strong persistence during the campaign that triggered our curiosity. We followed network traces and pivoted on the information left behind by this actor, such as open directories, document metadata, and binary peculiarities, which enabled us to find a custom-made piece of malware, that we named "CapturaTela". Our discovery of this malware family shows the reason for the persistent focus on hotel reservations as a primary vector: stealing credit card information from customers. We profiled this threat actor and that has resulted in uncovering not only their delivery mechanisms, but also their arsenal of remote access tools and info-stealing trojans, both acquired from underground forums as well as open source tools found in GitHub repositories.
Observed	Sectors: Hospitality and specifically on hotel reservations. Countries: Brazil.
Tools used	AsyncRAT, CapturaTela, LimeRAT, NanoCore RAT, njRAT, RemcosRAT, RevengeRAT.
Information	<https://unit42.paloaltonetworks.com/operation-comando-or-how-to-run-a-cheap-and-effective-credit-card-business/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format