Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:28:09 UTC

Tool: CapturaTela

Names	CapturaTela
Category	Malware
Type	Info stealer
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.
Information	<https://unit42.paloaltonetworks.com/operation-comando-or-how-to-run-a-cheap-and-effective-credit-card-business/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:CapturaTela>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool CapturaTela

Changed	Name	Country	Observed	
APT groups				
	Operation Comando	[Unknown]	2018	

1 group listed (1 APT, 0 other, 0 unknown)
