Fishing Elephant - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Fishing Elephant

Names	Fishing Elephant *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2019
Description	(Kaspersky) During the last months of 2019, we observed an ongoing campaign conducted by Fishing Elephant. The group continues to use both Heroku and Dropbox in order to deliver its tool of choice, AresRAT. We discovered that the actor incorporated a new technique into its operations that is meant to hinder manual and automatic analysis – geo-fencing and hiding executables within certificate files. During our research, we also detected a change in victimology that may reflect the current interests of the threat actor: the group is targeting government and diplomatic entities in Turkey, Pakistan, Bangladesh, Ukraine and China.
Observed	Sectors: Government. Countries: Bangladesh, China, Pakistan, Turkey, Ukraine.
Tools used	AresRAT.
Information	<https://securelist.com/apt-trends-report-q1-2020/96826/>

Last change to this card: 01 May 2020

Download this actor card in PDF or JSON format