Poseidon Group - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Poseidon Group

Names	Poseidon Group *(Kaspersky)* G0033 *(MITRE)*
Country	Brazil
Motivation	Information theft and espionage
First seen	2005
Description	(Kaspersky) During the latter part of 2015, Kaspersky researchers from GreAT (Global Research and Analysis Team) got hold of the missing pieces of an intricate puzzle that points to the dawn of the first Portuguese-speaking targeted attack group, named “Poseidon.” The group’s campaigns appear to have been active since at least 2005, while the very first sample found points to 2001. This signals just how long ago the Poseidon threat actor was already working on its offensive framework. The Poseidon Group is a long-running team operating on all domains: land, air, and sea. They are dedicated to running targeted attacks campaigns to aggressively collect information from company networks through the use of spear-phishing packaged with embedded, executable elements inside office documents and extensive lateral movement tools. The information exfiltrated is then leveraged by a company front to blackmail victim companies into contracting the Poseidon Group as a security firm. Even when contracted, the Poseidon Group may continue its infection or initiate another infection at a later time, persisting on the network to continue data collection beyond its contractual obligation. The Poseidon Group has been active, using custom code and evolving their toolkit since at least 2005. Their tools are consistently designed to function on English and Portuguese systems spanning the gamut of Windows OS, and their exfiltration methods include the use of hijacked satellite connections. Poseidon continues to be active at this time.

Observed	Sectors: Energy, Financial, Government, Media, Manufacturing, Telecommunications, Utilities. Countries: Brazil, France, India, Kazakhstan, Russia, UAE, USA.	
Tools used	IGT supertool.	
Counter operations	Feb 2016	The C2 servers have been sinkholed by Kaspersky. <https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/>
Information	<https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0033/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
