Operation Black Atlas - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Black Atlas

Names	Operation Black Atlas *(Trend Micro)*
Country	[Unknown]
Motivation	Financial crime
First seen	2015
Description	(Trend Micro) With the coming holidays also come news of various credit card breaches that endanger the data of many industries and their customers. High-profile breaches, such as that of the Hilton Hotel and other similar establishments, were accomplished using point-of-sale (PoS) malware, leading many to fear digital threats on brick-and-mortar retailers this Thanksgiving, Black Friday, Cyber Monday, and the rest of the holiday season. Researchers also found a broad campaign that uses the modular ModPOS malware to steal payment card data from retailers in the US. However, from what we have seen, it is not only retailers in the US that are at risk of breaches. Our researchers recently found an early version of a potentially powerful, adaptable, and invisible botnet that seeks out PoS systems within networks. It has already extended its reach to small and medium sized business networks all over the world, including a healthcare organization in the US. We are calling this operation Black Atlas, in reference to BlackPOS, the malware primarily used in this operation. Operation Black Atlas has been around since September 2015, just in time to plant its seeds before the holiday season. Its targets include businesses in the healthcare, retail, and more industries which rely on card payment systems.
Observed	Sectors: Financial, Healthcare, Hospitality, Manufacturing, Retail. Countries: Australia, Chile, Germany, India, Taiwan, UK, USA.
Tools used	Alina POS, BlackPOS, Gorynych, ModPOS, NewPosThings.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/>

	<https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-part-2-tools-and-malware-used-and-how-to-detect-them/>

Last change to this card: 24 May 2020

Download this actor card in PDF or JSON format
