Operation Groundbait - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Groundbait

Names	Operation Groundbait *(ESET)*
Country	Ukraine
Motivation	Information theft and espionage
First seen	2008
Description	(ESET) After BlackEnergy, which has, most infamously, facilitated attacks that resulted in power outages for hundreds of thousands of Ukrainian civilians, and Operation Potao Express, where attackers went after sensitive TrueCrypt-protected data from high value targets, ESET researchers have uncovered another cyberespionage operation in Ukraine: Operation Groundbait. The main point that sets Operation Groundbait apart from the other attacks is that it has mostly been targeting anti-government separatists in the self-declared Donetsk and Luhansk People's Republics. While the attackers seem to be more interested in separatists and the self-declared governments in eastern Ukrainian war zones, there have also been a large number of other targets, including, among others, Ukrainian government officials, politicians and journalists.
Observed	Sectors: Government and politicians and journalists. Countries: Ukraine.
Tools used	Prikormka.
Information	<https://www.welivesecurity.com/2016/05/18/groundbait/>

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format