Operation Potao Express - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Potao Express

Names	Operation Potao Express *(ESET)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2015
Description	(ESET) We presented our initial findings based on research into the Win32/Potao malware family in June, in our CCCC 2015 presentation in Copenhagen. Today, we are releasing the full whitepaper on the Potao malware with additional findings, the cyberespionage campaigns where it was employed, and its connection to a backdoor in the form of a modified version of the TrueCrypt encryption software. Like BlackEnergy, the malware used by the so-called Sandworm Team, Iron Viking, Voodoo Bear APT group (also known as Quedagh), Potao is an example of targeted espionage malware directed mostly at targets in Ukraine and a number of other post-Soviet countries, including Russia, Georgia and Belarus.
Observed	Countries: Belarus, Georgia, Russia, Ukraine.
Tools used	FakeTC, Patao.
Information	<https://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf>

Last change to this card: 15 February 2023

Download this actor card in PDF or JSON format