Threat Group Cards: A Threat Actor Encyclopedia

APT group: Sphinx

Names	Sphinx *(Qihoo 360)* APT-C-15 *(Qihoo 360)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2014
Description	(Qihoo 360) Operation Sphinx is a cyber-espionage activity in the Middle East. The main victims are political and military organizations in Egypt, Israel and possibly other countries. Sensitive data theft is what the attackers plotted for during the period from June, 2014 to November, 2015 when the activity was in its prime. We encountered some timestamps of the samples to be as early as December, 2011 which suggests the attack might be started much earlier, though further sound proof is needed. The main approach of Sphinx is watering hole attack on social web sites. Until now, we have obtained 314 pieces of sample malicious codes and 7 C2 domains.
Observed	Countries: Egypt, Israel.
Tools used	AnubisSpy, Havex RAT, njRAT, ROCK.
Information	<https://docplayer.net/83717233-Sphinx-apt-c-15-targeted-cyber-attack-in-the-middle-east-table-of-contents.html> <https://blog.trendmicro.com/trendlabs-security-intelligence/cyberespionage-campaign-sphinx-goes-mobile-anubisspy/>

Last change to this card: 21 May 2020

Download this actor card in PDF or JSON format
