Operation Ghoul - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Ghoul

Names	Operation Ghoul *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2016
Description	(Kaspersky) Kaspersky Lab has observed new waves of attacks that started on the 8th and the 27th of June 2016. These have been highly active in the Middle East region and unveiled ongoing targeted attacks in multiple regions. The attackers try to lure targets through spear phishing emails that include compressed executables. The malware collects all data such as passwords, keystrokes and screenshots, then sends it to the attackers. We found that the group behind this campaign targeted mainly industrial, engineering and manufacturing organizations in more than 30 countries. In total, over 130 organizations have been identified as victims of this campaign. Using the Kaspersky Security Network (KSN) and artifacts from malware files and attack sites, we were able to trace the attacks back to March 2015. Noteworthy is that since the beginning of their activities, the attackers' motivations are apparently financial, whether through the victims' banking accounts or through selling their intellectual property to interested parties, most infiltrated victim organizations are considered SMBs (Small to Medium size businesses, 30-300 employees), the utilization of commercial off-the-shelf malware makes the attribution of the attacks more difficult.
Observed	Sectors: Education, Engineering, Industrial, Manufacturing, IT, Pharmaceutical, Shipping and Logistics and Tourism and Trading. Countries: Azerbaijan, China, Egypt, France, Germany, Gibraltar, India, Iran, Iraq, Italy, Pakistan, Portugal, Romania, Qatar, Saudi Arabia, Spain, Sweden, Switzerland, Taiwan, Turkey, UAE, UK, USA.
Tools used	OpGhoul.
Information	<https://securelist.com/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/75718/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
