Shadow Academy - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Shadow Academy

Names	Shadow Academy *(RiskIQ)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2020
Description	(RiskIQ) In early July 2020, RiskIQ began tracking a phishing campaign identified through our internet intelligence graph targeting colleges and universities worldwide. From July 2020 into October 2020, RiskIQ systems uncovered 20 unique targets in Australia, Afghanistan, the UK, and the USA. All these attacks used similar tactics, techniques, and procedures (TTPs) as Mabna Institute, Cobalt Dickens, Silent Librarian, an Iranian company that, according to the FBI, was created for illegally gaining access 'to non-Iranian scientific resources through computer intrusions.' Mabna Institute earned the moniker 'Silent Librarian' due to its focused efforts to compromise university students and faculty by impersonating university library resources using domain shadowing to harvest credentials. However, while RiskIQ's findings are consistent with TTPs in use by Silent Librarian, they alone are not sufficient to attribute the threat activity we've detected against these 20 universities directly to Mabna Institute. Therefore, RiskIQ has named actors identified during this research as 'Shadow Academy.'
Observed	Sectors: Education. Countries: Afghanistan, Australia, UK, USA.
Tools used	
Information	<https://www.riskiq.com/blog/external-threat-management/shadow-academy/>

Last change to this card: 06 January 2021

Download this actor card in PDF or JSON format