Operation Epic Manchego - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Epic Manchego

Names	Operation Epic Manchego *(NVISO)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2020
Description	(NVISIO) In July 2020, NVISO detected a set of malicious Excel documents, also known as “maldocs”, that deliver malware through VBA-activated spreadsheets. While the malicious VBA code and the dropped payloads were something we had seen before, it was the specific way in which the Excel documents themselves were created that caught our attention. The creators of the malicious Excel documents used a technique that allows them to create macro-laden Excel workbooks, without actually using Microsoft Office. As a side effect of this particular way of working, the detection rate for these documents is typically lower than for standard maldocs.
Observed	Countries: Bulgaria, Canada, China, Czech, France, Germany, Hungary, Italy, Japan, Malaysia, Netherlands, Poland, Romania, South Korea, Sweden, UK, Ukraine, Uruguay, USA, Vietnam.
Tools used	Agent Tesla, AZORult, Formbook, Matiex, njRAT.
Information	<https://blog.nviso.eu/2020/09/01/epic-manchego-atypical-maldoc-delivery-brings-flurry-of-infostealers/>

Last change to this card: 17 September 2020

Download this actor card in PDF or JSON format