Retefe Gang, Operation Emmental - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:52:06 UTC

Other threat group: Retefe Gang, Operation Emmental

Names	Retefe Gang *(GovCERT.ch)* Operation Emmental *(Trend Micro)*
Country	Russia
Motivation	Financial crime
First seen	2013
Description	(GovCERT.ch) Surprisingly, there is a lot of media attention going on at the moment on a macOS malware called OSX/Dok. In the recent weeks, various anti-virus vendors and security researchers published blog posts on this threat, presenting their analysis and findings. While some findings where very interesting, others were misleading or simply wrong. We don't know where the sudden media interest and the attention from anti-virus vendors on this threat actor are coming from. As a matter of fact, the threat actor behind OSX/Dok, which we call the the Retefe gang or Operation Emmental, has already been around for many years and GovCERT.ch is tracking their activities since the very beginning (2013). The purpose of this blog post is to put the puzzle pieces together and trying to bust some of the myths that have made the round in the media recently.
Observed	Sectors: Financial. Countries: Austria, Germany, Japan, Romania, Sweden, Switzerland, Turkey, UK.
Tools used	Citadel, Retefe, Retefe (Android), Tinba.
Information	<https://www.govcert.ch/blog/the-retefe-saga/> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf>

Last change to this card: 22 May 2020

Download this actor card in PDF or JSON format