# GitHub - itsreallynick/office-crackros: Crack your macros like the math pros.

By Nick Carr

Archived: 2026-04-06 01:10:38 UTC

## OfficeCrackros

**Crack your macros like the math pros.**

This is a substitution cipher detector & decoder plugin for Microsoft Office documents. Essentially, this is Sigpedia for Macros. What I'm trying to say is I think you'll find this helpful if you can navigate all the trolling. **Feb 2017 Update:** This now supports PointsToInches character encoding (new FIN8 technique)!

## How To Use It

### 1. download teh scripts

### 2. run against suspect documents

**Usage:** `python oledump.py -p plugin_officecrackros <path/to/file.doc>`

### 3. let me know what you think

- Please understand that, like all good hacked together tools, I stopped as soon as it worked - with much room for improvement
- If you found the tool helpful, let me know @itsreallynick

## Requirements

- oledump
  - Didier Stevens, who is awesome, created this tool
    - oledump has been included in this repository
    - https://github.com/DidierStevens/DidierStevensSuite/blob/master/oledump.py
  - oledump requires olefile python library: `easy_install olefile`
- Malicious Microsoft Office Document using encoded macros
  - Specifically: macros substitution noise used by FIN8; also seen for Nymaim ransomware delivery
  - Try it yourself:
    - https://www.virustotal.com/en/file/cba63594f28e69405b5075013624075ef1a538be40a7c2402f84d33f9f6c2927/ar

## To Do List:

- ~~CRUSH IT.~~
- Remove extraneous text in multiple line matches (improve regular expressions)
- Add back in substitution / dropchar detection based on character histogramming

---