idapatchwork — Bitbucket

Published: 2014-11-04 · Archived: 2026-04-05 13:17:16 UTC

Patchwork: Stitching against malware families with IDA Pro (tool for the talk at Spring9, https://spring2014.gdata.de/spring2014/programm.html)

This repository contains the (unfinished) code for a tool I called patchwork.

In essence, I use a somewhat fixed / refurbished version of PyEmu along IDA to demonstrate deobfuscation of the different patterns found in the malware family Nymaim.

All credits and a big thank you for the original PyEmu go to Cody Pierce

- https://code.google.com/p/pyemu/
- https://github.com/codypierce/pyemu

Changes vs. the original PyEmu:

- partially fixed the memory management of PyEmu to work more robustly, especially in IDA.
- fixed some of the opcode handling that would break when encountering "rare" x86 instructions.
- recompiled pydasm with Python 2.7 to have it out of the box compatible with the version found in the last couple versions of IDA.

Setup (deobfuscation proof of concept)

- Copy the repo into some folder reachable from IDA.
- Set the variable PYEMU_PATH in $idapatchwork/patchwork/config.py to the appropriate value.
- Load $idapatchwork/patchwork/INFECTED/nymaim_2f3d6becf1e42614445816302a50d8e2.unp into IDA.
- Execute $idapatchwork/run.py.

If you just want to benefit from my changes to PyEmu, take the first steps and then you probably want to check out the modified $idapatchwork/idapyemu.py and find your way on from there. Enjoy.
