

Injecting Malware into Dating Sims

By Dennis Goodlett

How it starts



How it ends

- Obfuscated python pickle malware
  - Breaking decompilers
  - Breaking Disassemblers
  - Bypassing protections
  - Pickle Schizophrenia
  - Pickles all the way down
- Reversing pickles
- Patching pickles

$ whoami -really

- Newest Doyensec Employee!
- NOT a part of visual novel community
- Not really even a gamer anymore…
- Radare2 contributor
- Created Eval Villain
- Collect random hobbies
  - Magic, math, DDR, yo-yos…

DDLC


Monika
"That's right, you usually like to write about cute things, don't you, Natsuki?"
History
Skip
Auto
Save
Load
Settings

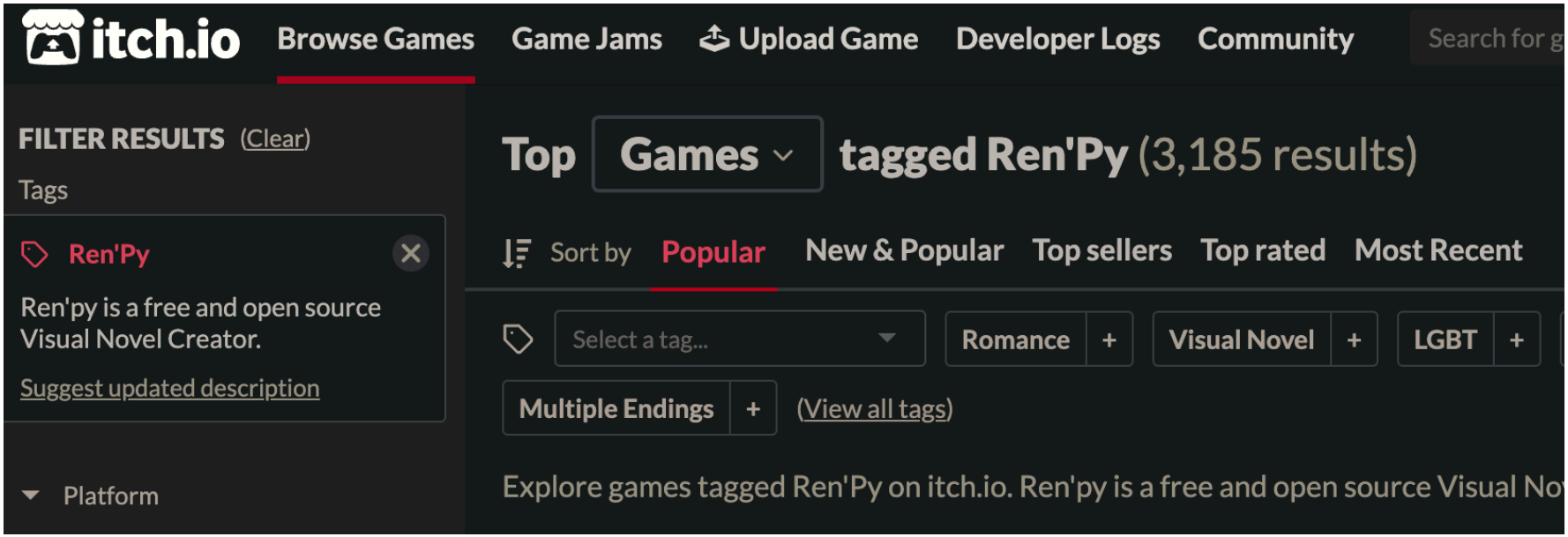
Doki Doki Literature Club

- Aka DDLC
- Free game
- Mac, Windows and Linux
- 147k followers, 96% positive on steam
- /r/ddlc has 241k followers
- DDLC+ sold 1M+ copies
- Psychological Horror
  - I am not suggesting you play it
  - Take warnings seriously

Ren'Py

- Visual Novel Engine
- Free
- Open source
- Mac, Linux, Windows, Web, Android, iOS
- Has its own language of the same name
- **Very low barrier for entry**
- More then 3 thousand games
- Built on **pygame**
- A save system that **just works**

3,185 Ren’Py games on itch.io



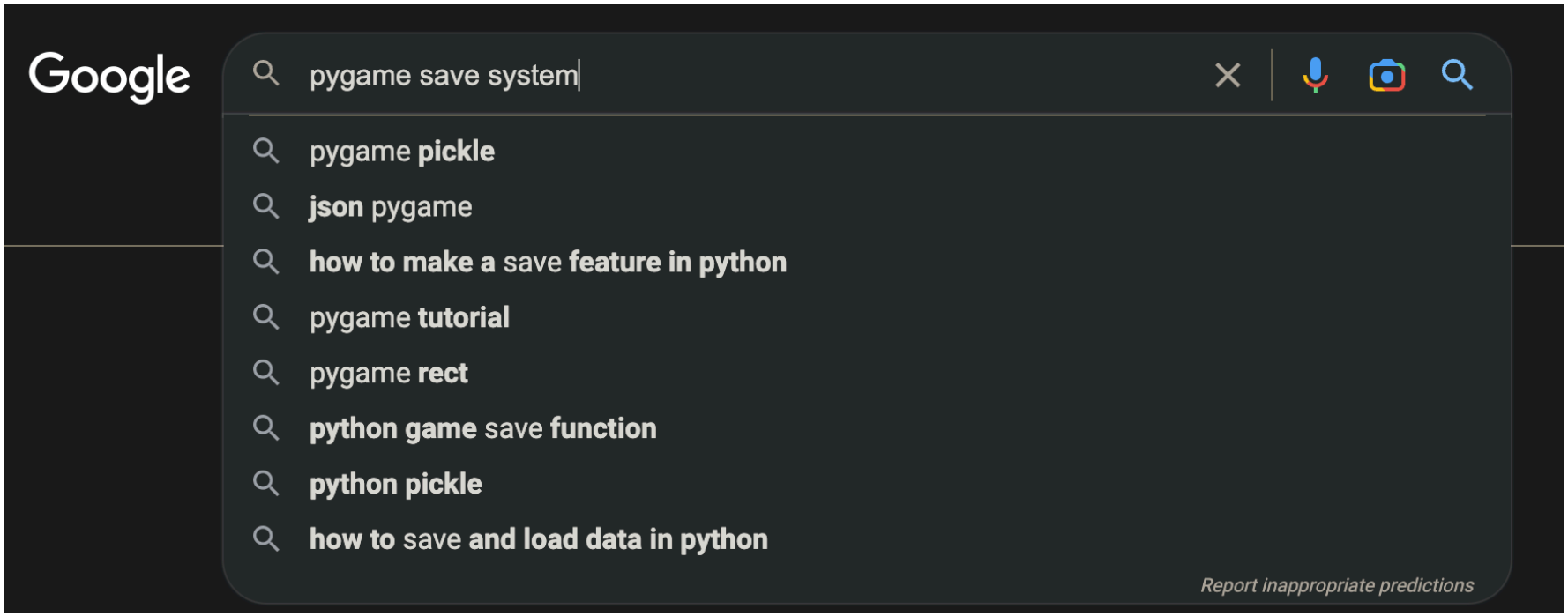
Games on Everything



No Hate, Ren'Py is cool



Pygames Save systems



Python Pickles Documentation

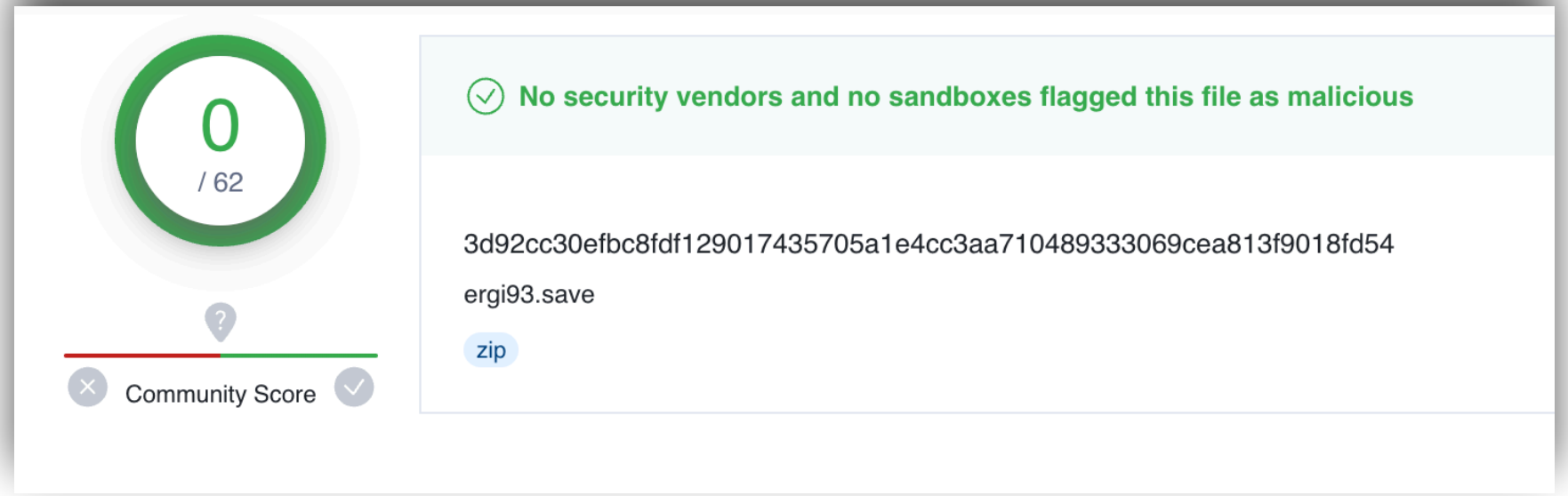
Warning: The `pickle` module **is not secure**. Only unpickle data you trust.

It is possible to construct malicious pickle data which will **execute arbitrary code during unpickling**. Never unpickle data that could have come from an untrusted source, or that could have been tampered with.

Consider signing data with `hmac` if you need to ensure that it has not been tampered with.

Safer serialization formats such as `json` may be more appropriate if you are processing untrusted data. See Comparison with json.

Is it safe?


0
/ 62
Community Score
No security vendors and no sandboxes flagged this file as malicious
3d92cc30efbc8fdf129017435705a1e4cc3aa710489333069cea813f9018fd54
ergi93.save
zip

Pickles ASM Primer

- Stack machine
- Simple, small language
- Create and assemble objects (has setattr)
- No opcodes to de-construct (no getattr)
- Can import ANYTHING
- Python2 supported
- No magic bytes
- No control flow

Pickle Tooling

- pickle
- pickletools
- picklescan
- fickling
- Radare2
- r2pickledec

Pickles all the way down

- Inspired by Russ Cox's "Zip all the way down"
- https://research.swtch.com/zip

Pickle Schizophrenia

- Inspired By Ange Albertini's Funky File Formats talk
- https://media.ccc.de/v/31c3_-_5930_-_en_-_saal_6_-_201412291400_-_funky_file_formats_-_ange_albertini

Questions?

- Twitter: @bemodtwz
- My Git: swoops
- r2pickledec: github.com/doyensec/r2pickledec
- Blog (soon): blog.doyensec.com
- Radare2: githib.com/radareorg/radare2