PeekabooAV - Cuckoo Sandbox Scanner for Amavis

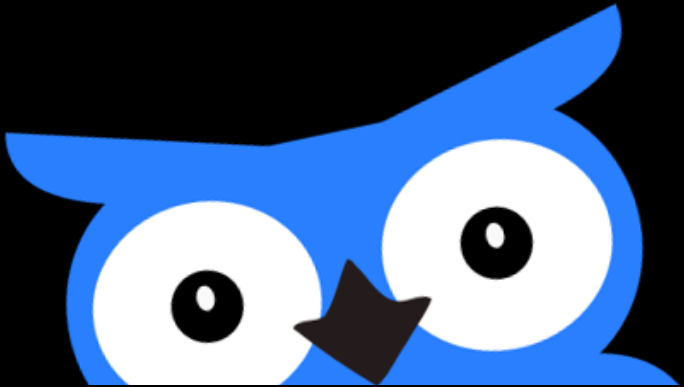
Open Source Behavior Analysis of Email Attachments

Felix Bauer

December 27, 2017

felix@ai4me.de

Hey
I'm Peekaboo

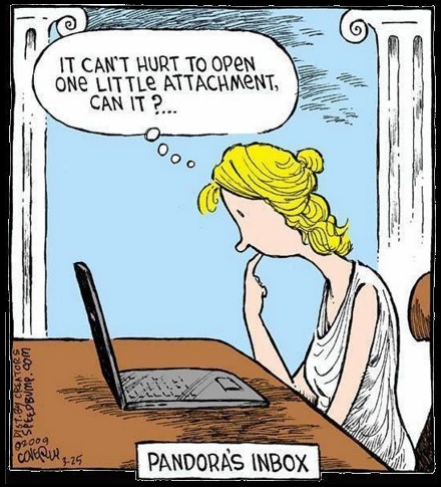


PeekabooAV turns Cuckoo Sandbox into an AV

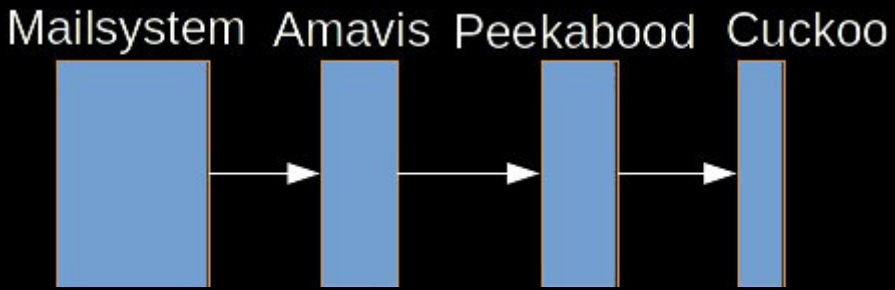
It's the connection between mail system and behavior analysis

Peekaboo queues, schedules, checks, interprets and makes a decision

Cyber is Dangerous



PeekabooAVs Place



Amavis

- Amavis with its policy banks
- It dissects email
- Passes a directory for each email
- Over a file socket connection

We need a patch for Amavis to preserve the original filename (which I would like to see upstream)

What everyone likes most!

PeekabooAV is licensed under GPLv3

The project was started 1.5 years ago and is OpenSource since May this year

Recently we won the OSBAR OpenSouce Award

Setup

`[ubuntu, postfix, amavis, virtualbox, python, cuckoo]`

there is also an installer

More

- Sample database to recognise already analysed samples
- and cache results
- In active use on the internet
- Can itself run inside a VM
- It can scan files as well
- plans to scan from web proxy, bro, ...

Goal

The goal is to go unnoticed unless you need it

Best Vulnerabilites So Far

Issue#3
Avoid detection - same file with different file extensions

Issue#4
Test in whitelist rule allows to bypass analysis

Thanks

Lots of thanks to CuckooSandbox and the CuckooSandbox Community

Thanks for listening looking forward to hearing from you

Twitter: @peekabooav
Github: scvenus/peekabooav
Youtube: https://youtu.be/Vjd1JeACz70 1h talk (German)