# More Obvious Web-malware Repository

...

MOWR

RMLL Security Track

July 6th, 2016

# Agenda

- Who are we ?
- One year ago...
- Design
- Several softwares
- User friendly
- Collaborative
- Demo

# Who are we ?

We’re hosting websites, mostly e-commerce but not only

Our CerberHost hosting platform aims to provide a secure environment for web applications

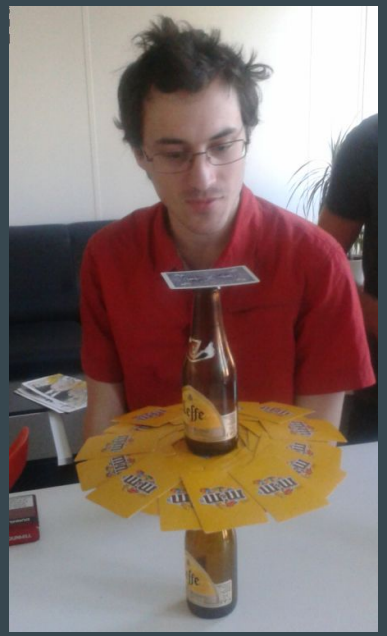
And, last but not least, we’re opensource supporters : PMF, Naxsi, mapster and now MOWR are opensource projects developped at NBS System


# Last year

We introduced you a tool to detect malware on Linux webservers, coded by Julien Voisin during his internship :

PHP Malware Finder

He was so skilled we hired him. Then, we had an idea : sharing the malwares we found.



# A wild Antide appears !

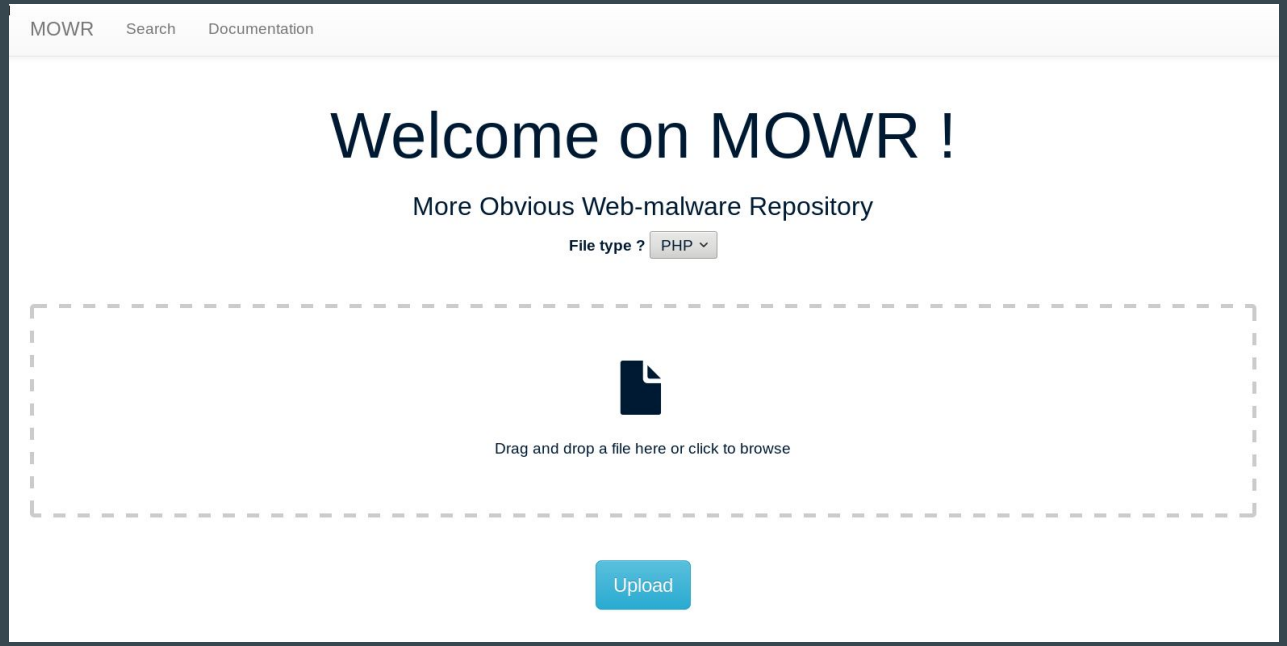
Here comes a new challenger^Wintern !

We talked to Antide about a virustotal-like website dedicated to malwares.

MOWR was born.


# Where to find MOWR ?

https://github.com/nbs-system/mowr/ (You can add some stars if you like it)



# Design

- Can handle multiple analyzers
- User friendly
- Collaborative

- Flask (Python)
- Bootstrap
- PostgreSQL

# Several analyzers

- For now only 2 scanners are used (PMF and ClamAV)
- YOU can help us to find a few MOWR !

# User friendly

If you know ***how to drag and drop a file*** OR ***browse your file system***, then you can use it !


He knows how to use it

# Collaborative

- Anyone can upload a file and view other analyzes
- You can give your opinion about a sample (not much more than “clean”/” malicious”)
- You can assign pre-defined tags
- If your file is very similar to another one, then MOWR informs you
  - ex: P.A.S. webshell generation website with on the fly password protection
- TODO: Multiple account system which can download samples (only one today)

It’s **MOWR** than just a web application !

# Installation

Requirements:

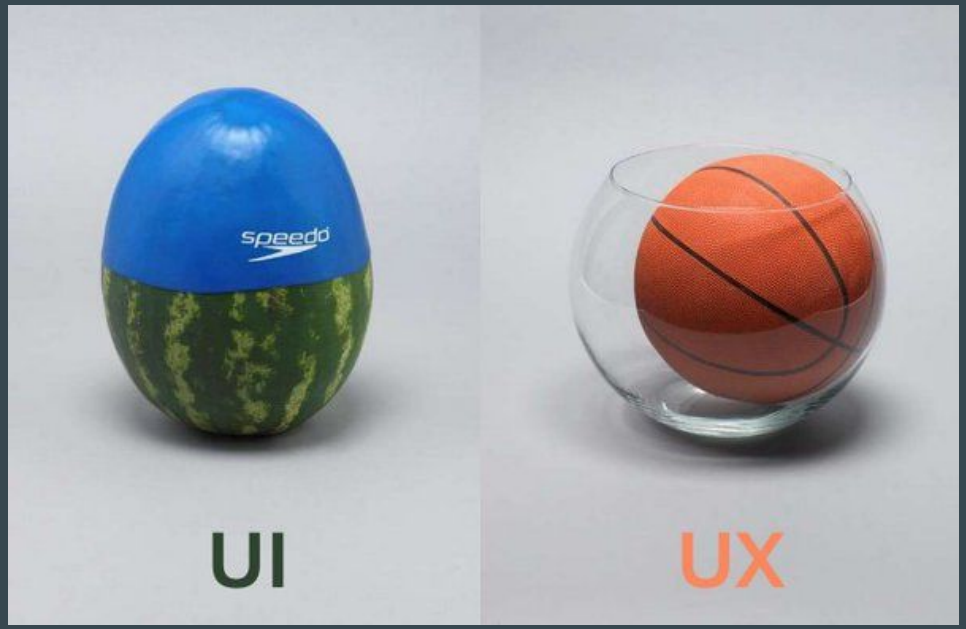
- Python 2.7 or Python 3.5
- PostgreSQL with fuzzystrmatch extension
- pip

Installation:

- Clone repository
- pip install -r requirements.txt
- python mowr-server.py

# Usage

Best UI and UX you'll ever see !



MOWR Search Documentation

# Analysis:


| sample informations | |
|---|---|
| Name(s) | cipher_design.php |
| MD5 | 42c8ce3feb1a91a769f15977070573ff |
| Sha1 | 9e6c03eef27338c11db7e6b2dbcea7cb5402e366 |
| Sha256 | 62af3fadae7589d30890b2538c2e8177abc894b8639afbbbb8a43d68074a0e45 |
| SSDeep | 48:Y6zyhTLI6cu94+4+Q4PYgTJOEzGwiQjwBmPdZtB6KIEC06RA0160T:Y6GTcr+qR+OWGwiQkBKdPB6KIz06RZ1R |
| Entropy | 5.87156627095534 |
| MIME | text/x-php |
| Dates | |
| First analysis | 2016-07-05 13:46:21.731750 UTC |
| Last analysis | 2016-07-05 13:46:21.731873 UTC |
| Tags | Obfuscated |
| Neighbours | |
| Sample analysis | |
| PMF | ObfuscatedPhp DodgyPhp |

Upload a new sample


KEEP
CALM
IT IS
DEMO
TIME

# Any MOWR Questions ?