

# System Security Research @ University of Birmingham, UK

Marco Cova

[m.cova@cs.bham.ac.uk](mailto:m.cova@cs.bham.ac.uk)

# Security group

## Formal verification

- Techniques: information flow, applied pi-calculus, protocol analysis, ...
- Applications: Trusted Platform Module (TPM), e-voting, e-passport, ...



Mark Ryan



Tom Chotia

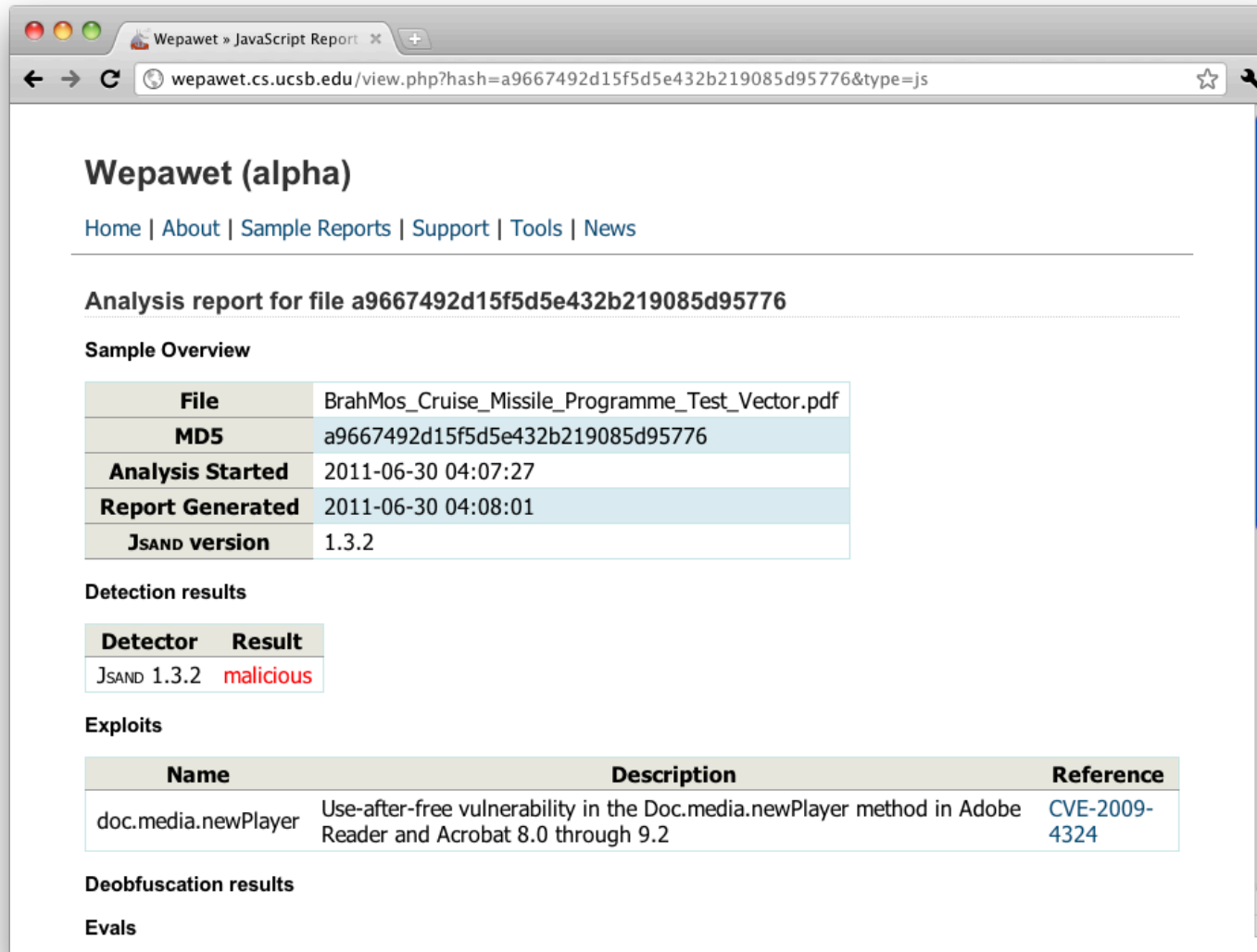
## System Security

- Web-based malware
- Web application security
- Botnets



Marco Cova

# Web malware detection



The screenshot shows a web browser window with the title "Wepawet » JavaScript Report". The address bar displays the URL "wepawet.cs.ucsb.edu/view.php?hash=a9667492d15f5d5e432b219085d95776&type=js". The page content includes a header for "Wepawet (alpha)" with navigation links: Home | About | Sample Reports | Support | Tools | News. Below this is a section titled "Analysis report for file a9667492d15f5d5e432b219085d95776". Under "Sample Overview", a table lists file details. Under "Detection results", a table shows the detector "JSAND 1.3.2" with a "malicious" result. Under "Exploits", a table lists a vulnerability in Adobe's Doc.media.newPlayer method. The page also has sections for "Deobfuscation results" and "Evals".

## Wepawet (alpha)

[Home](#) | [About](#) | [Sample Reports](#) | [Support](#) | [Tools](#) | [News](#)

---

### Analysis report for file a9667492d15f5d5e432b219085d95776

---

#### Sample Overview

<b>File</b>	BrahMos_Cruise_Missile_Programme_Test_Vector.pdf
<b>MD5</b>	a9667492d15f5d5e432b219085d95776
<b>Analysis Started</b>	2011-06-30 04:07:27
<b>Report Generated</b>	2011-06-30 04:08:01
<b>JSAND version</b>	1.3.2

#### Detection results

Detector	Result
JSAND 1.3.2	malicious

#### Exploits

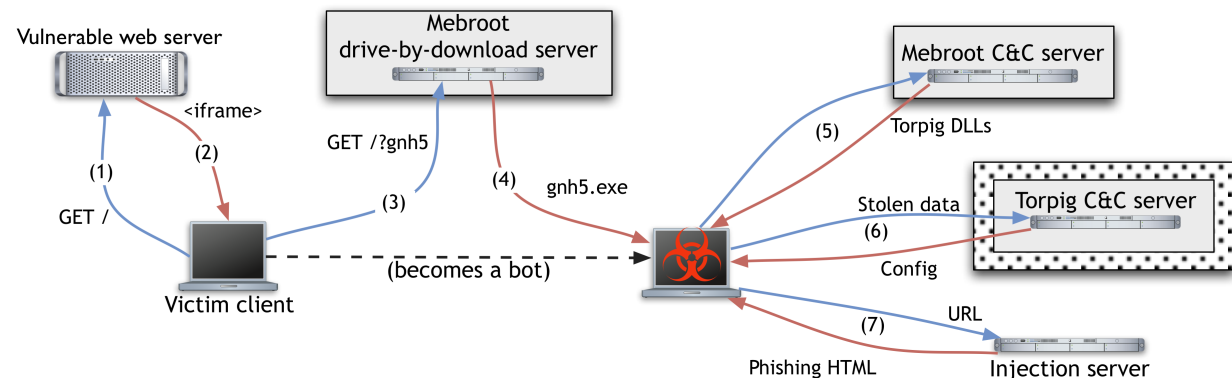
Name	Description	Reference
doc.media.newPlayer	Use-after-free vulnerability in the Doc.media.newPlayer method in Adobe Reader and Acrobat 8.0 through 9.2	<a href="#">CVE-2009-4324</a>

#### Deobfuscation results

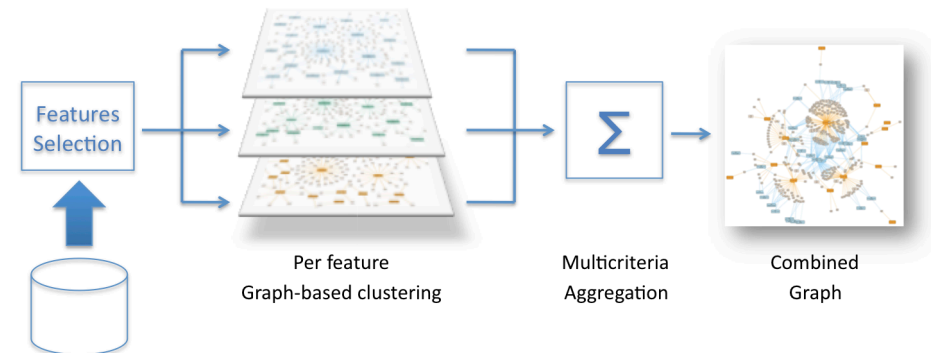
#### Evals

# Measuring the malicious web

- Botnets: Mebroot/Torpig studies

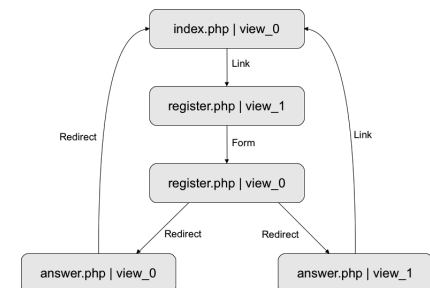
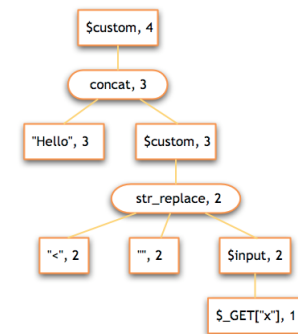
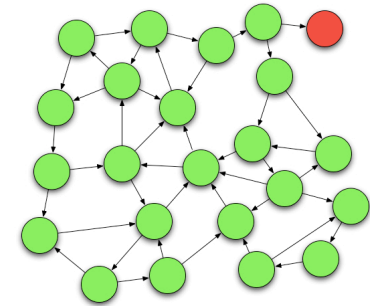


- Phishing: (backdoored) phishing kits
- Rogue AV campaigns



# Webapp security

- Swaddler: detecting workflow violation attacks via anomaly detection and invariant learning
- Saner: identify weak sanitization in web applications (SQL injection, XSS) via static string analysis
- MiMoSa: detect multi-step input validation vulnerabilities (e.g., stored SQL injection)



# Future work

- Detection techniques
  - More classes of malicious content (e.g., rogue AV, spam pages)
  - Smarter crawling: focus on “toxic” areas of Web
  - Address evasion attempts
  - Better analysis techniques (patterns in malicious code, organization of malicious activity, attackers techniques)
- Prevention techniques
  - Web application frameworks that assure the absence of certain vulnerabilities
- Malware
  - Machines do get infected and still used for sensitive activity; then what?
- Privacy
  - Social networks, cloud, smartphones