System Security Research @ University of Birmingham, UK

Marco Cova
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, …

System Security

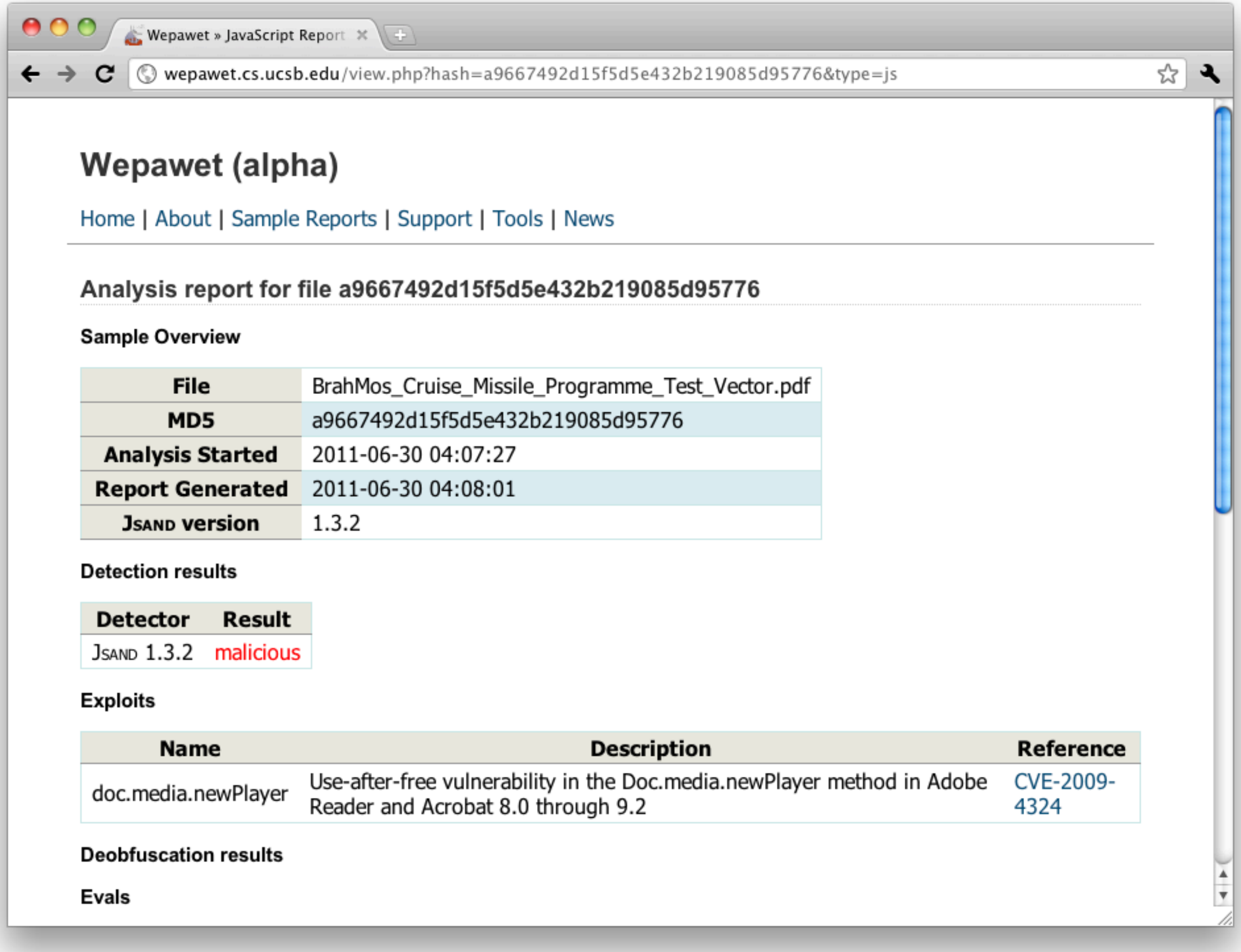
- Web-based malware
- Web application security
- Botnets

Mark Ryan

Tom Chotia

Marco Cova

Web malware detection



Wepawet » JavaScript Report
wepawet.cs.ucsb.edu/view.php?hash=a9667492d15f5d5e432b219085d95776&type=js

Wepawet (alpha)

Home | About | Sample Reports | Support | Tools | News

Analysis report for file a9667492d15f5d5e432b219085d95776

Sample Overview

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

Detection results

Detector	Result
JSAND 1.3.2	malicious

Exploits

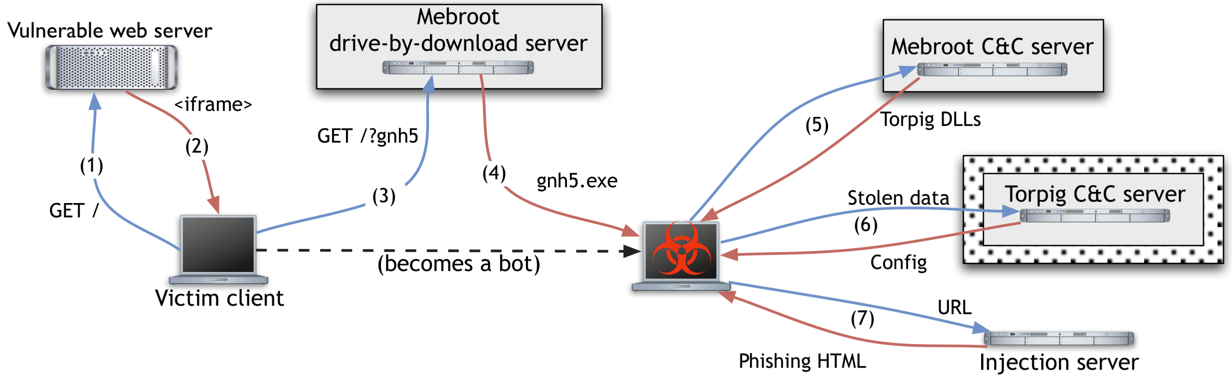
Name	Description	Reference
doc.media.newPlayer	Use-after-free vulnerability in the Doc.media.newPlayer method in Adobe Reader and Acrobat 8.0 through 9.2	CVE-2009-4324

Deobfuscation results

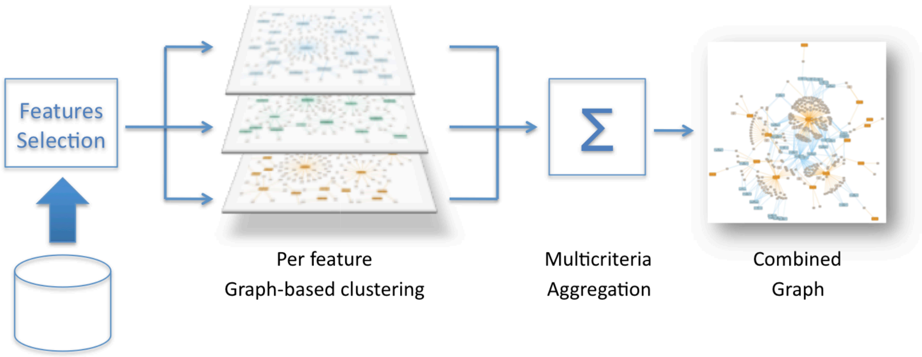
Evals

Measuring the malicious web

- Botnets: Mebroot/Torpig studies

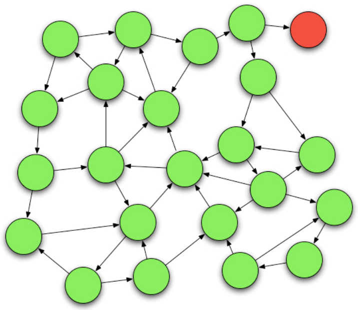


- Phishing: (backdoored) phishing kits
- Rogue AV campaigns

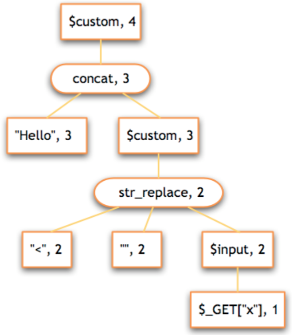


Webapp security

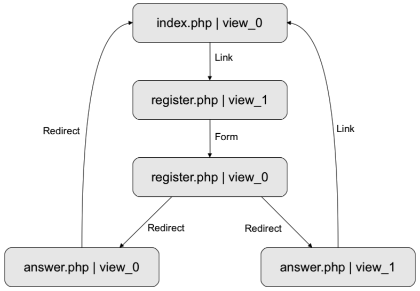
- Swaddler: detecting workflow violation attacks via anomaly detection and invariant learning



- 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