DSMS: Automating Decision Support and Monitoring Workflow for Incident Response

Chris HORSLEY (CSIRT Foundry)
SC LEUNG (HKCERT)
Wally Wong (HKCERT)
Agenda

1. What are our challenges?
2. How we run IR → how DSMS can help us
3. Design and technical details
4. Future plans
5. Q & A
IR team challenges
Data rules!

Ripple effect
- Internet + programming + exploit kit + ...
- Crooks automate attacks (i.e. faster, more)
- ‘Upstream’ (e.g. security researcher, CERT) *forced* to automate response
- Your CERT receives too much data → no choice, also *forced* to automate
Data rules!

Conclusion:

- You have NO choice! Automate! Automate! Automate!
- Before automating anything, re-visit our workflow
Use case: phishing campaign

EMAIL SHOCK: On Monday morning, you saw 100 phishing reports in your email inbox 😨
Use case: phishing campaign

If you verify, look up the URL one by one...

Expect half day to complete...

Then another half day to notify owners or operators one by one...
Manual incident handling workflow
Manual IR workflow

<table>
<thead>
<tr>
<th>Issue of manual processing</th>
<th>How it can be improved with automation</th>
</tr>
</thead>
<tbody>
<tr>
<td>❏ Repeated, manual re-checking of targets with many steps</td>
<td>Let the robot (i.e. DSMS) do it for you!</td>
</tr>
<tr>
<td>❏ Storage inconsistent, tedious</td>
<td></td>
</tr>
<tr>
<td>❏ Manual decision making on targets: malicious or not?</td>
<td></td>
</tr>
<tr>
<td>❏ Results can take a long time to arrive (e.g. external sandboxes)</td>
<td></td>
</tr>
<tr>
<td>❏ Unsafe handling of malicious files</td>
<td></td>
</tr>
<tr>
<td>❏ May be identified by attackers based on IP, metadata</td>
<td></td>
</tr>
</tbody>
</table>
Automated IR workflow

Event Feed (i.e. global intelligence data such as Clean MX, Shadowserver)

Monitor & Decide

Incident Response

DATA NORMALIZATION

ACTIONABLE DATA (Filter and Prioritize)

TICKETING SYSTEM

Information Feed Analysis System (IFAS)

Decision Support Management System (DSMS)

Incident Response Management System (IRMS)

E.g. ~100,000 events

E.g. ~1,000 cases
How can DSMS help you?
What is DSMS actually?

- A system using open source libraries with pluggable distributed agents making use of Internet services (e.g. lookup, malware analysis, reputation) to perform analysis of URL/IP/malware etc.
- DSMS is self hosted, and stores and aggregates the analysis results.
How can DSMS help you?

- DSMS can help you:
  - Automate IR → become more efficient
  - Do something very difficult or even impossible (from human sense), e.g. track threat lifecycle
Be More Efficient

- Transform human process (sequential) into scalable machine processes (parallel)

- Use algorithm to make decision for you
Do Something Difficult (for human)

- Aggregation/Correlation
- Multi-geographical monitoring
- Round the clock monitoring
Use case: phishing campaign

With DSMS:
- Just submit the 100 URLs
- Have a cup of coffee
- Wait for results
- Review all lookup results (e.g. WHOIS, IP, VirusTotal) on one page
- Action on selected data
DSMS in action
DSMS design goals

- High automation
- Repeated monitoring with custom schedules
- Historical archive
- Consistent analysis methods
- Consistent storage of artifacts (Git)
- Non-attributable monitoring
- Distributed, geographically diverse monitoring
- API to receive threat data (URLs, domains, files) from other systems
- API to publish threat status to other systems
- Custom analysis workflows
- Identify priority targets based on gathered data
## Latest targets

<table>
<thead>
<tr>
<th>ID</th>
<th>Status</th>
<th>Target</th>
<th>Added</th>
<th>Last check</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Inactive</td>
<td>nosuchdomainasthis.nosuch Domain</td>
<td>58 seconds ago</td>
<td>24 seconds ago</td>
</tr>
<tr>
<td>18</td>
<td>Active</td>
<td><a href="http://public.mailer.cn2.nl/public/redirect/link/!/109786/r/n/19003/s/186144407/h/o43cb21806">http://public.mailer.cn2.nl/public/redirect/link/!/109786/r/n/19003/s/186144407/h/o43cb21806</a> Phishing</td>
<td>2 days, 2 hours ago</td>
<td>51 seconds ago</td>
</tr>
<tr>
<td>17</td>
<td>Active</td>
<td><a href="http://sumotracking.com/aff_c?offer_id=1888&amp;aff_id=1100&amp;aff_sub=EDB&amp;aff_sub2=52a7aa6c7894">http://sumotracking.com/aff_c?offer_id=1888&amp;aff_id=1100&amp;aff_sub=EDB&amp;aff_sub2=52a7aa6c7894</a> Phishing</td>
<td>4 days, 2 hours ago</td>
<td>36 seconds ago</td>
</tr>
<tr>
<td>16</td>
<td>Active</td>
<td><a href="http://emailnation.postaffiliatepro.com/scripts/click.php">http://emailnation.postaffiliatepro.com/scripts/click.php</a>? a_aid=52a7aa6c7894&amp;a_bid=99ceaf11 Phishing</td>
<td>4 days, 3 hours ago</td>
<td>50 seconds ago</td>
</tr>
<tr>
<td>15</td>
<td>Unknown</td>
<td><a href="http://public.mailer.lgtv.nl/public/redirect/link/!/104465/n/18338/s/186144407/h/4a8e1a9804">http://public.mailer.lgtv.nl/public/redirect/link/!/104465/n/18338/s/186144407/h/4a8e1a9804</a> Phishing</td>
<td>4 days, 3 hours ago</td>
<td>2 minutes ago</td>
</tr>
<tr>
<td>14</td>
<td>Active</td>
<td>Invoice_hsbc.exe Malware (file)</td>
<td>5 days, 3 hours ago</td>
<td>53 seconds ago</td>
</tr>
<tr>
<td>12</td>
<td>Active</td>
<td><a href="http://visjs.org">http://visjs.org</a> Spider only</td>
<td>4 weeks, 1 day ago</td>
<td>47 seconds ago</td>
</tr>
<tr>
<td>11</td>
<td>Active</td>
<td>eicar.com Malware (file)</td>
<td>1 month ago</td>
<td>39 seconds ago</td>
</tr>
<tr>
<td>9</td>
<td>Active</td>
<td><a href="http://www.cloudflare.com/">http://www.cloudflare.com/</a> Phishing</td>
<td>1 month ago</td>
<td>2 days, 9 hours ago</td>
</tr>
</tbody>
</table>
Add monitoring target

URL or file to analyse

Location
http://example.com

Artifact file
Browse... No file selected.

Monitoring settings

Profile*
Phishing

Severity*
Medium

Schedule*
Every hour

Monitor until
2015-05-30

Add target
Target profile editor

Set up a profile to monitor a particular type of target.

Name*
Phishing

Input type*
URL

Timeout*
3600

After this many seconds, running jobs in this profile will be cancelled. Jobs may take a long time to run - be generous!

Tasks*
- [ ] Web fingerprint
- [ ] OS Fingerprint
- [ ] IP whois / ASN lookup
- [ ] Wepawet task
- [ ] VirusTotal scan
- [ ] Domain whois lookup
- [ ] Hostname resolution
- [ ] Web page screenshot
- [ ] URL single download
- [ ] HTTP Status Check
- [ ] URL spider
- [ ] Geo IP lookup

Create profile
DSMS#7

http://www.eicar.org/download/eicar.com

**Active** Malware (url)
- Malicious
- Resolvable
- Contactable

- Added 1 month ago by admin
- Cracked every 6 hours
- Last check: an hour ago

---

Analysis

**HTTP**

- **HTTP status**: 200
- **HTTP content**: ASCII text, with no line
- **Web fingerprint**: Apache
**Malware analysis**

- **DOS.EiracA.Trojan (Bkav)**
  - 53/56 AV engines detect
  - Scan status: Analysis queued
  - Initial version
  - Last update 2 minutes ago

**Network**

- **IPs**
  - 1 IP: 188.40.238.250

- **Whois**
  - Corehub, S.R.L (R23-LROR)
  - Registered 17 years, 1 month ago
  - Initial version
  - Last update 16 minutes ago

**OS**

- **OS fingerprint**
  - Linux 2.6.32
## VirusTotal history

http://www.eicar.org/download/eicar.com
(275a021bbf6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f)

- **Submitted to VirusTotal:** May 11, 2015, 11:39 a.m.
- **Results updated:** May 11, 2015, 11:53 a.m.
- **Scan status:** Scan complete

### AV engine | Detected as | First reported
--- | --- | ---
Ad-Aware | EICAR-Test-File (not a virus) | May 11, 2015, 11:53 a.m.
AegisLab | EICAR-AV-Test | May 11, 2015, 11:53 a.m.
Agnitum | EICAR_test_file | May 11, 2015, 11:53 a.m.
AhnLab-V3 | EICAR_Test_File | May 11, 2015, 11:53 a.m.
Aliaba |  |  
ALYac | Misc.Eicar-Test-File | May 11, 2015, 11:53 a.m.
Avast | EICAR Test-NOT virus!!! | May 11, 2015, 11:53 a.m.
AVG | EICAR_Test | May 11, 2015, 11:53 a.m.
AVware | EICAR (v) | May 11, 2015, 11:53 a.m.
### IP timeline

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>184.28.9.203</td>
<td>Akamai Technologies, Inc.</td>
</tr>
<tr>
<td>23.4.171.56</td>
<td>Akamai Technologies, Inc.</td>
</tr>
<tr>
<td>23.9.227.171</td>
<td>Akamai Technologies, Inc.</td>
</tr>
</tbody>
</table>

### IP details

<table>
<thead>
<tr>
<th>Country</th>
<th>ASN</th>
<th>AS name</th>
<th>AS CIDR</th>
<th>Net</th>
<th>Net desc</th>
<th>Net CIDR</th>
<th>Abuse contact</th>
<th>Address</th>
<th>First seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>20940</td>
<td>AKAMAI-ASN1</td>
<td>23.4.160.0/20</td>
<td>AKAMAI</td>
<td>Akamai Technologies, Inc.</td>
<td>23.0.0.0/12</td>
<td><a href="mailto:ip-admin@akamai.com">ip-admin@akamai.com</a></td>
<td>Cambridge Center</td>
<td>2019-08-23 00:40:16</td>
</tr>
<tr>
<td>US</td>
<td>20940</td>
<td>AKAMAI-ASN1</td>
<td>184.28.8.0/23</td>
<td>AKAMAI</td>
<td>Akamai Technologies, Inc.</td>
<td>184.24.0.0/13</td>
<td><a href="mailto:ip-admin@akamai.com">ip-admin@akamai.com</a></td>
<td>Cambridge Center</td>
<td>2019-08-23 00:40:16</td>
</tr>
<tr>
<td>US</td>
<td>4739</td>
<td>INTERNODE-AS</td>
<td>23.9.224.0/20</td>
<td>AKAMAI</td>
<td>Akamai Technologies, Inc.</td>
<td>23.0.0.0/12</td>
<td><a href="mailto:ip-admin@akamai.com">ip-admin@akamai.com</a></td>
<td>Cambridge</td>
<td>2019-08-23 00:40:16</td>
</tr>
</tbody>
</table>
Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Find more of what you're looking for with Graph Search.

Sign Up
It's free and always will be.

First name
Last name
Email or mobile number
Re-enter email or mobile number
New password
Birthday
Month
Day
Year
Why do I need to provide my birthday?

Female
Male

By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.

Sign Up
Facebook helps you connect and share with the people in your life.

Sign Up
It’s free and always will be.

First name
Last name
Email or mobile number
Re-enter email or mobile number
New password

Birthday
Month Day Year
Why do I need to provide my birthday?

Female Male

By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.

Sign Up
### Filtered target results (ip_cc:de)

<table>
<thead>
<tr>
<th>ID</th>
<th>Status</th>
<th>Target</th>
<th>Added</th>
<th>Last check</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Active</td>
<td><a href="http://www.eicar.org/download/eicar.com">http://www.eicar.org/download/eicar.com</a></td>
<td>an hour ago</td>
<td>25 minutes ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malware (url)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matching fields:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP geo: DE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Matching fields:*
- IP geo: DE
Task statistics (last 1000 task results)

Node status

![Node status diagram]

Tasks by agent over time

![Tasks by agent over time graph]

Task performance times

<table>
<thead>
<tr>
<th>Task</th>
<th>Task stats</th>
<th>Median</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirusTotal scan</td>
<td>0s</td>
<td>20s</td>
</tr>
<tr>
<td></td>
<td>Median: 2.6455s</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Task stats</td>
<td>Median</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>VirusTotal scan</td>
<td></td>
<td>Median: 3.999s</td>
</tr>
<tr>
<td>OS Fingerprint</td>
<td></td>
<td>Median: 9.308s</td>
</tr>
<tr>
<td>Geo IP lookup</td>
<td></td>
<td>Median: 0.001s</td>
</tr>
<tr>
<td>Web fingerprint</td>
<td></td>
<td>Median: 1.3875s</td>
</tr>
<tr>
<td>Hostname resolution</td>
<td></td>
<td>Median: 0.000s</td>
</tr>
<tr>
<td>Web page screenshot</td>
<td></td>
<td>Median: 3.074s</td>
</tr>
<tr>
<td>Wepewet task</td>
<td></td>
<td>Median: 3.183s</td>
</tr>
<tr>
<td>Domain whois lookup</td>
<td></td>
<td>Median: 1.338s</td>
</tr>
<tr>
<td>IP whois / ASN lookup</td>
<td></td>
<td>Median: 0.970s</td>
</tr>
<tr>
<td>HTTP Status Check</td>
<td></td>
<td>Median: 5.0895s</td>
</tr>
<tr>
<td>URL spider</td>
<td></td>
<td>Median: 10.062s</td>
</tr>
<tr>
<td>URL single download</td>
<td></td>
<td>Median: 7.799s</td>
</tr>
</tbody>
</table>
Technical details
Platform / technologies

- Python
- Django
- Celery (distributed task execution)
- RabbitMQ
- Ubuntu 14.04 (current supported OS)
Current modules

- HTTP status
- HTTP spidering
- URL screenshot
- IP resolution
- ASN / geo IP lookup
- WHOIS lookup and parsing
- OS fingerprinting
- Web site fingerprinting
- VirusTotal analysis
- Wepawet analysis
Future features

• Tagging targets for analyst notes
• Classification and prioritisation of targets
• Android binary analysis
• Further HTML / Javascript analysis with Thug
• Passive DNS
• Bitcoin wallet monitoring
• Email address analysis
• Artifact similarity analysis
Future plans
We need more...

Some proposed features to make automation by DSMS more complete:
- Data exchange among various systems.
- Normalize data from email.
- Find useful contact, not only from WHOIS.
- Let user choose different views of report.
Collaboration

• Closed pilot for now
• Open source (Apache) licence
• Currently available to interested co-developers and contributors
• Feature requests and patches highly encouraged!
Thank you

• Questions and enquiries welcome: dsms@hkcert.org