

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



CSIRT

foundry

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

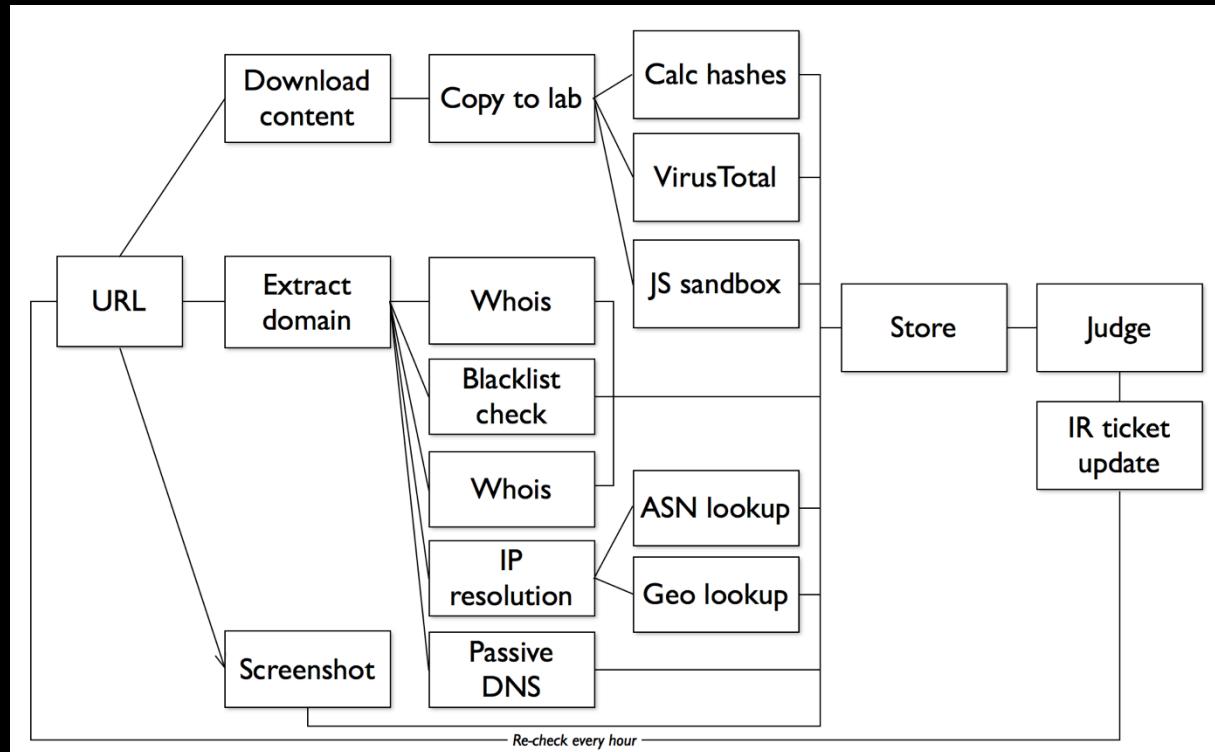
If you verify, look up the URL one by one...

Expect half day to complete...

Then another half day to notify owners or operators one by one...



Manual incident handling workflow



CSIRT foundry

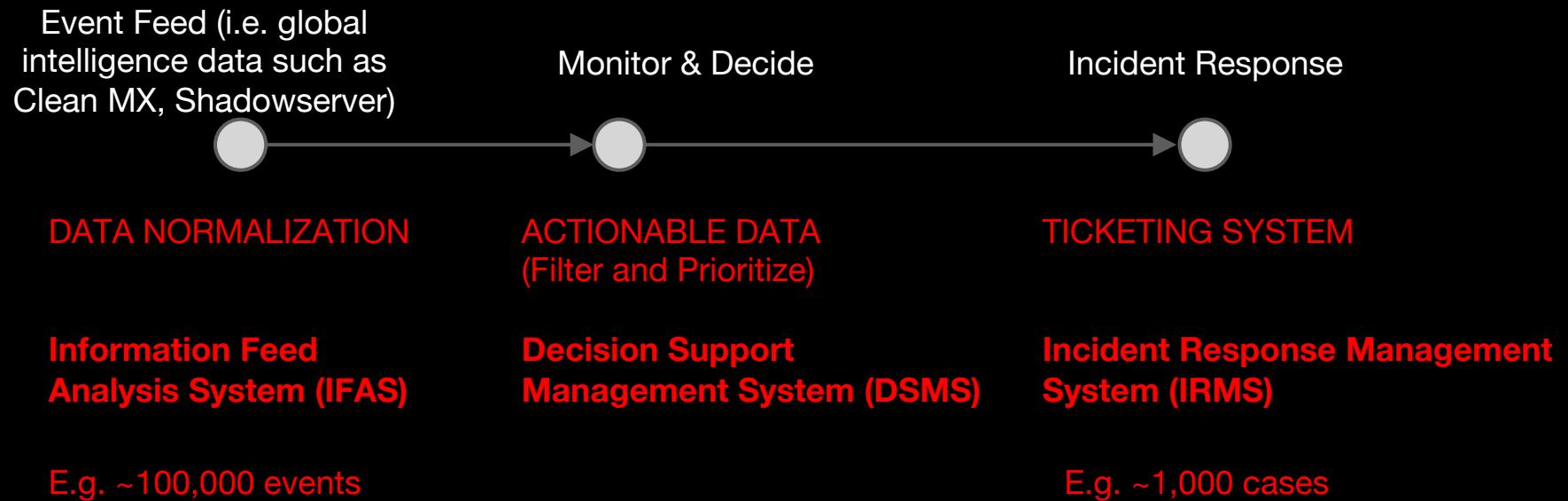
Manual IR workflow

Issue of manual processing	How it can be improved with automation
<ul style="list-style-type: none"><input type="checkbox"/> Repeated, manual re-checking of targets with many steps<input type="checkbox"/> Storage inconsistent, tedious	
<ul style="list-style-type: none"><input type="checkbox"/> Manual decision making on targets: malicious or not?<input type="checkbox"/> Results can take a long time to arrive (e.g. external sandboxes)	<p>Let the robot (i.e. DSMS) do it for you!</p>
<ul style="list-style-type: none"><input type="checkbox"/> Unsafe handling of malicious files<input type="checkbox"/> May be identified by attackers based on IP, metadata	



CSIRT foundry

Automated IR workflow



CSIRT foundry

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



CSIRT foundry

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

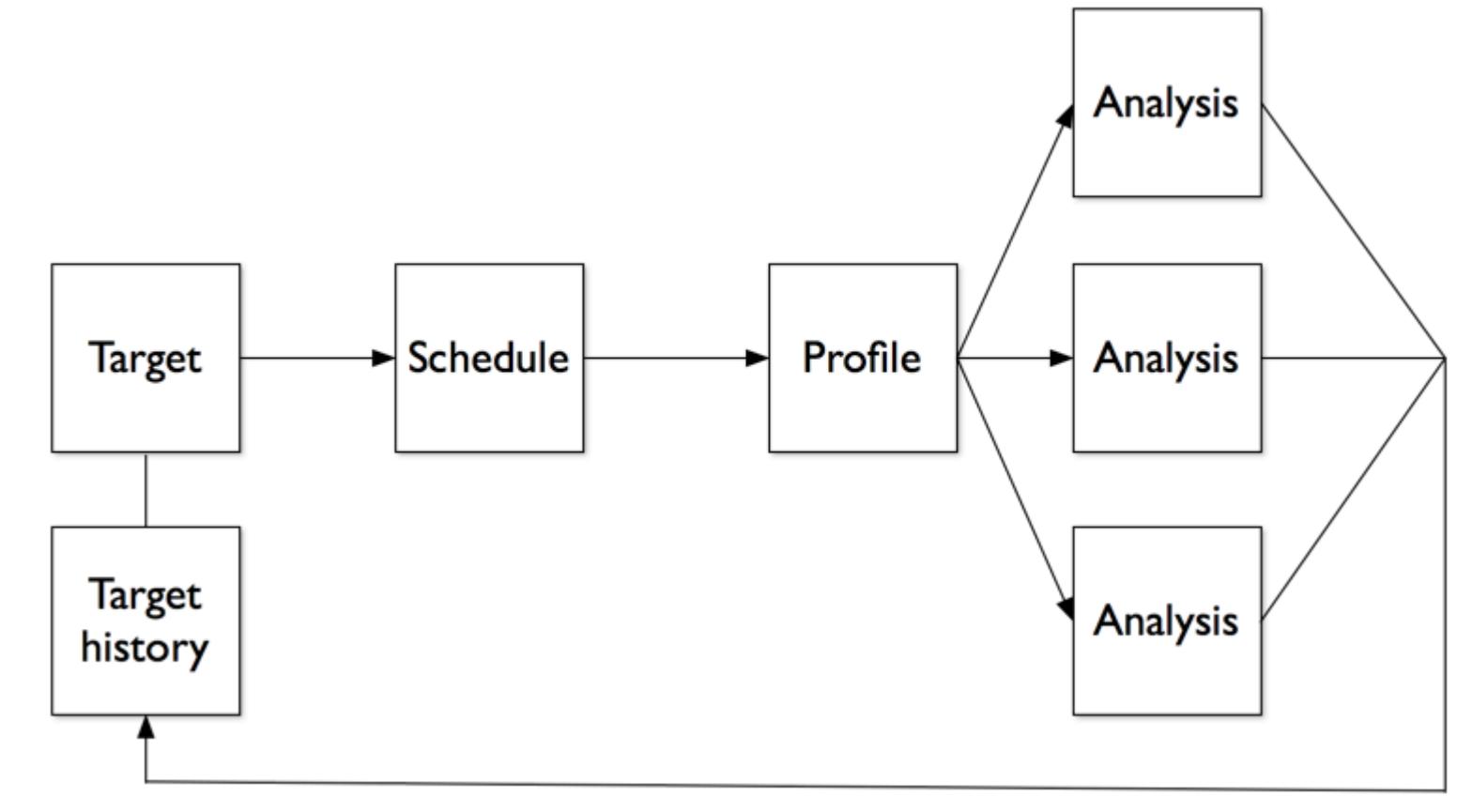


CSIRT foundry

DSMS in action

DSMS design goals

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



DSMS Home Search Add monitoring target Manage admin

Latest targets

ID	Status	Target	Added	Last check
20	Inactive	nosuchdomainasthis.nosuch Domain	58 seconds ago	24 seconds ago
18	Active	http://public.mailer.cn2.nl/public/redirect/link/l/109786/n/19003/s/186144407/h/c43cb21806 Phishing	2 days, 2 hours ago	51 seconds ago
17	Active	http://sumotracking.com/aff_c?offer_id=1688&aff_id=1100&aff_sub=EDB&aff_sub2=52a7aaa6c7894 Phishing	4 days, 2 hours ago	36 seconds ago
16	Active	http://emailnation.postaffiliatepro.com/scripts/click.php?a_aid=52a7aaa6c7894&a_bid=9accea11 Phishing	4 days, 3 hours ago	50 seconds ago
15	Unknown	http://public.mailer.lgtv.nl/public/redirect/link/l/104465/n/18338/s/186144407/h/4a8e1a9804 Phishing	4 days, 3 hours ago	2 minutes ago
14	Active	Invoice_hsbc.exe Malware (file)	5 days, 3 hours ago	53 seconds ago
12	Active	http://visjs.org Spider only	4 weeks, 1 day ago	47 seconds ago
11	Active	eicar.com Malware (file)	1 month ago	39 seconds ago
9	Active	http://www.cloudflare.com/ Phishing	1 month ago	2 days, 9 hours ago

URL or file search

IRT foundry

DSMS Home Q Search Add monitoring target Manage admin

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

DSMS v1.0.20 About Task stats



DSMS Home Search Add monitoring target Manage admin

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 Home Search Add monitoring target Manage admin

DSMS#7

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

Active Malware (url)
• Malicious • Resolvable • Contactable

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

▶ Pause monitoring ⚡ Disable target
See job history
Show which tasks run

11 16 21 26 31 1 6 11 16
May 2015 June 2015

Analysis Links History Task log

HTTP

HTTP status 200	HTTP content ASCII text, with no line	Web fingerprint Apache
--------------------	--	---------------------------

SIRT foundry

Malware analysis

 VirusTotal



**DOS.EiracA.Trojan
(Bkav)**

53/56 AV engines detect
Scan status: Scan complete
Initial version
 Last update 2 minutes ago

 Wepawet



Scan status: Analysis queued
Initial version
 Last update

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

terminators

last update 16 minutes

68 bytes

VirusTotal history

<http://www.eicar.org/download/eicar.com>
(275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f)

Submitted to VirusTotal: May 11, 2015, 11:39 a.m.
Results updated: May 11, 2015, 11:53 a.m.
Scan status: Scan complete
[See full report on VirusTotal](#)

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.
Alibaba		
ALYac	Misc.Eicar-Test-File	May 11, 2015, 11:53 a.m.
Antiy-AVL	Test[:not-a-virus]/Win32.EICAR	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.

188

  **CSIRT** foundry

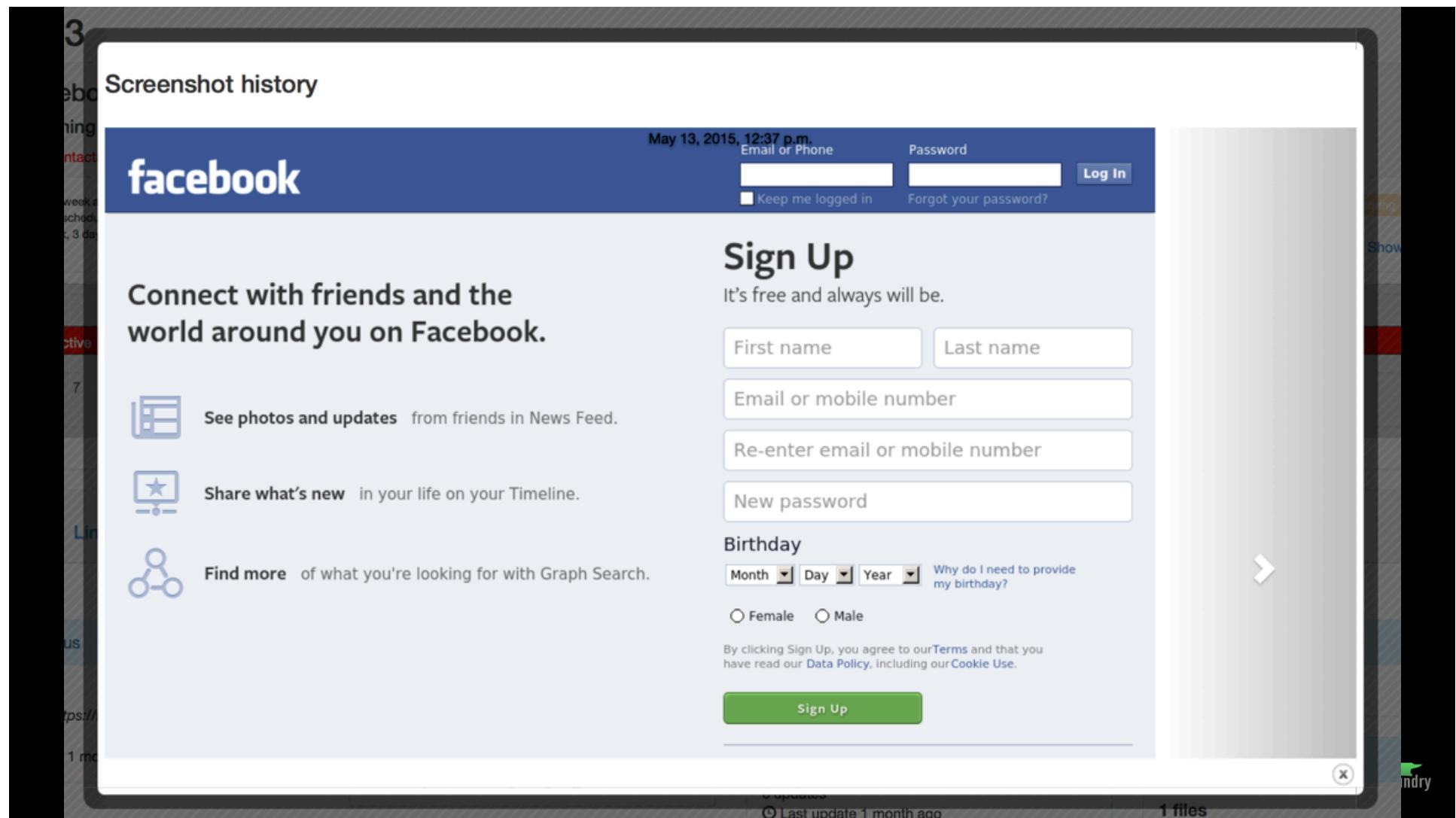
IP timeline

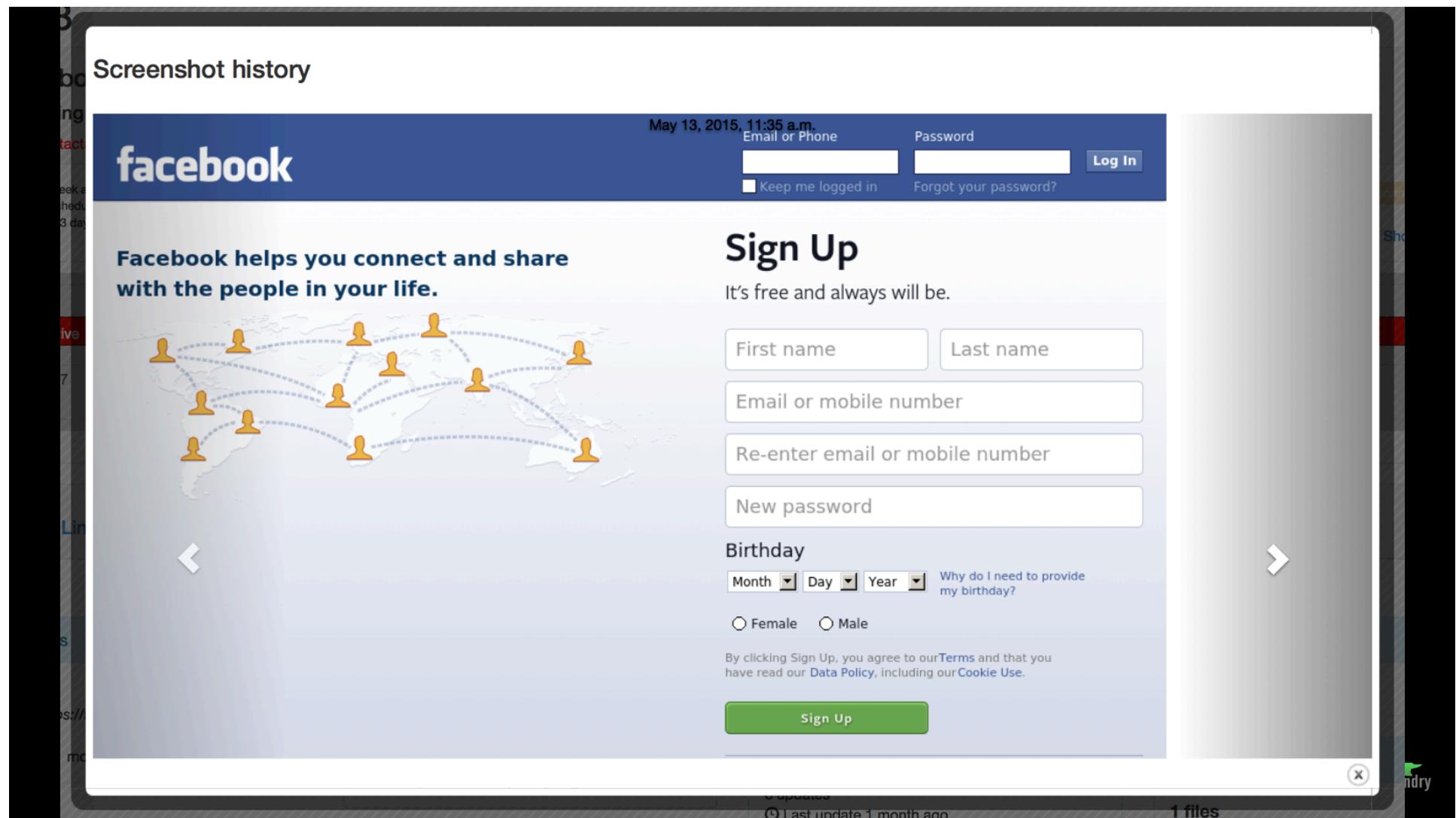
184.28.9.203	Akamai Technologies, Inc.
23.4.171.56	Akamai Technologies, Inc.
23.9.227.171	Akamai Technologies, Inc.

IP details

Country	ASN	AS name	AS CIDR	Net	Net desc	Net CIDR	Abuse contact	Address	F
23.4.171.56									
	US 20940	AKAMAI-ASN1	23.4.160.0/20	AKAMAI	Akamai Technologies, Inc.	23.0.0.0/12	ip-admin@akamai.com	8 Cambridge Center	M 9, 201: a.
184.28.9.203									
	US 20940	AKAMAI-ASN1	184.28.8.0/23	AKAMAI	Akamai Technologies, Inc.	184.24.0.0/13	ip-admin@akamai.com	8 Cambridge Center	M 8, 2012 p.
23.9.227.171									
	US 4739	INTERNODE-AS	23.9.224.0/20	AKAMAI	Akamai Technologies, Inc.	23.0.0.0/12	ip-admin@akamai.com	8 Cambridge	M 8,







S#6

p.m.	p.m.	terminators		Diff
May 10, 2015, 1:09 p.m.	to May 10, 2015, 5:11 p.m.	4 hours, 2 minutes	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators	text/html 55.3 KB Text view / Markup view / Diff
May 10, 2015, 10:02 a.m.	to May 10, 2015, 1:09 p.m.	3 hours, 6 minutes	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators	text/html 53.9 KB Text view / Markup view / Diff

[See inline diff](#)

```
@@ -100,7 +100,7 @@

    <meta name="channel" content="channel:content:to:define!" />

    <title>Optus - Mobile Phones, Broadband Internet, TV, Home Phone, Tablets</title>
-     <link rel="canonical" href="/?gclsrc=aw.ds&gclsrc=aw.ds&gclid=Cj0KEQjw4LaqBRD60pfSn43Z
+LQBEiQAJv5FLJQugxRyAEnaFpDJQkyYUP5fiHi8eUYRiUqivB-ONNkaAiPk8P8HAQ&gclid=Cj0KEQjw4LaqBRD60pfSn43ZwLQB
EiQAJv5FLJQugxRyAEnaFpDJQkyYUP5fiHi8eUYRiUqivB-ONNkaAiPk8P8HAQ&dclid=CNj6xuHdtMUCFcd6vQodhSIALQ&dclid
=CNj6xuHdtMUCFcd6vQodhSIALQ&ppc=1&ppc=1" />
+     <link rel="canonical" href="/" />
        <meta name="description" content="Shop the latest mobile phones & tablets. Find awesome value broadband internet, home phone & TV entertainment packages at Optus. Learn more." />

        <script type="text/javascript" src="//smb.optus.com.au/opfiles/v11720/cc/static/assets/common/js/globals.js"></script>

@@ -1457,7 +1457,7 @@

<!--[BEGIN "patternWrapper.tag" [-->
    <div class="row">

-     <div class="large-3 medium-6 columns">
+     <div class="large-30 medium-60 columns">
```

13 updates 11 updates Last update 2 hours ago



DSMS Home Q Search Add monitoring target Manage admin

Filtered target results (ip_cc:de)				
ID	Status	Target	Added	Last check
7	Active	http://www.eicar.org/download/eicar.com Malware (url) <i>Matching fields:</i> IP geo: DE	an hour ago	25 minutes ago



CSIRT foundry

DSMS Home Search Add monitoring target Log in

Task statistics (last 1000 task results)

Node status

```
graph TD; core((core)) --- broker((dsmsdevbroker1)); broker --- agent((dsmsdevagent1))
```

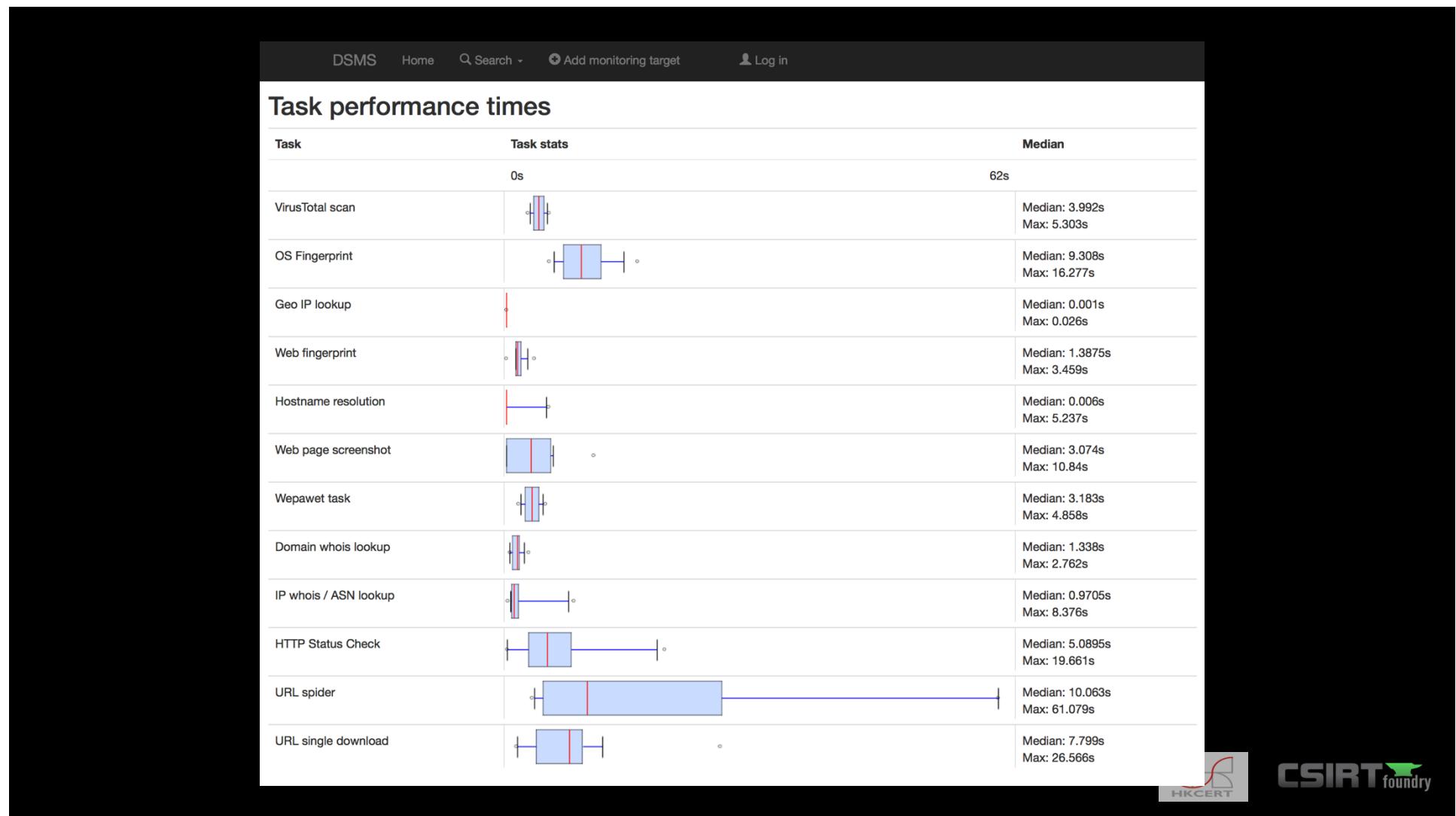
Tasks by agent over time

A line chart showing the number of tasks (Y-axis, 1.00 to 20.00) over time (X-axis, dates from 14/06 15:13 to 15/06 09:48). The chart shows a highly volatile line with several sharp peaks, indicating high task activity at various intervals. A blue dot on the line marks the specific agent being tracked.

Task performance times

Task	Task stats	Median
VirusTotal scan	0s	29s
		Median: 2.6455s

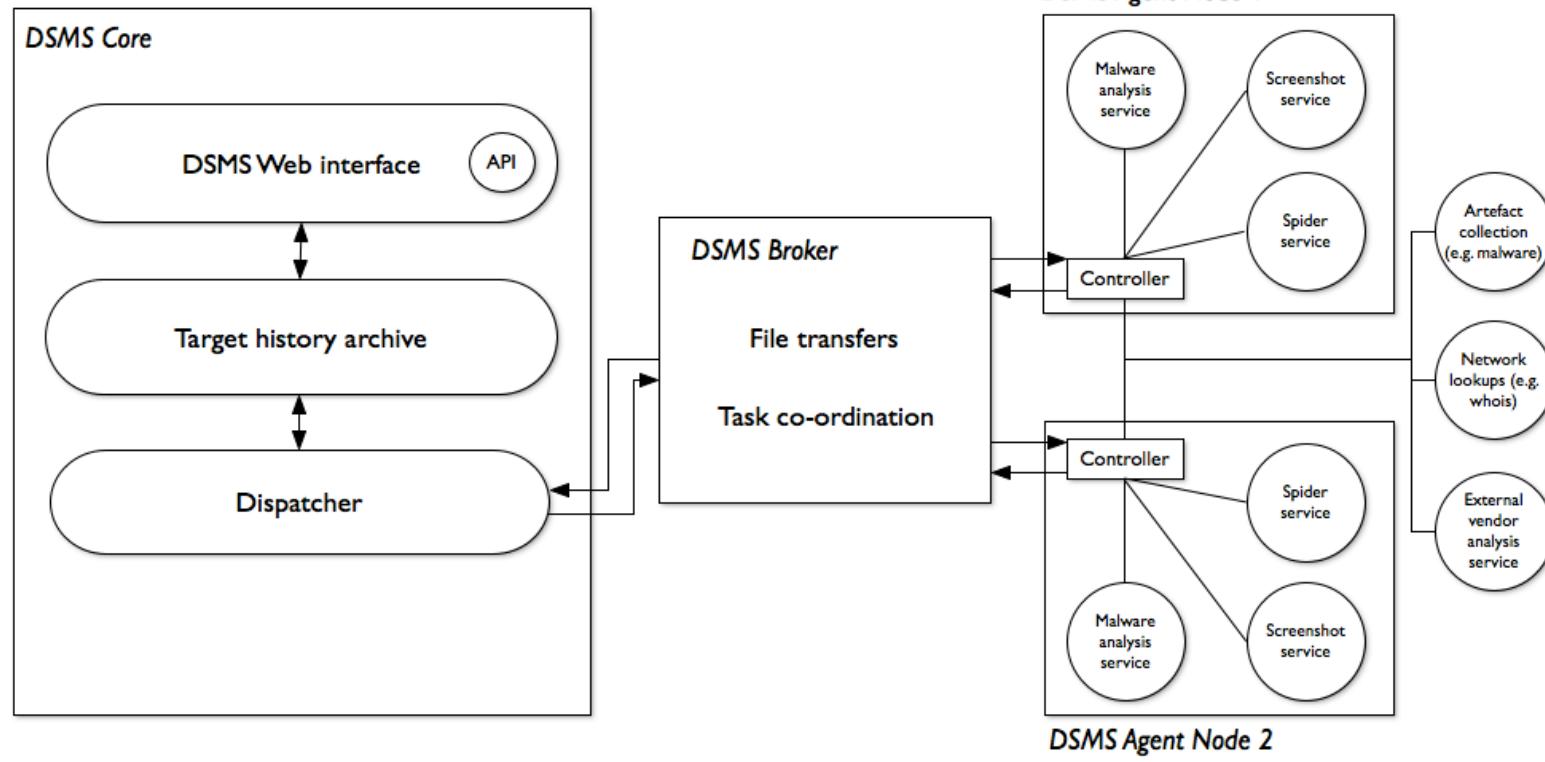
CSIRT foundry



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