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 😱

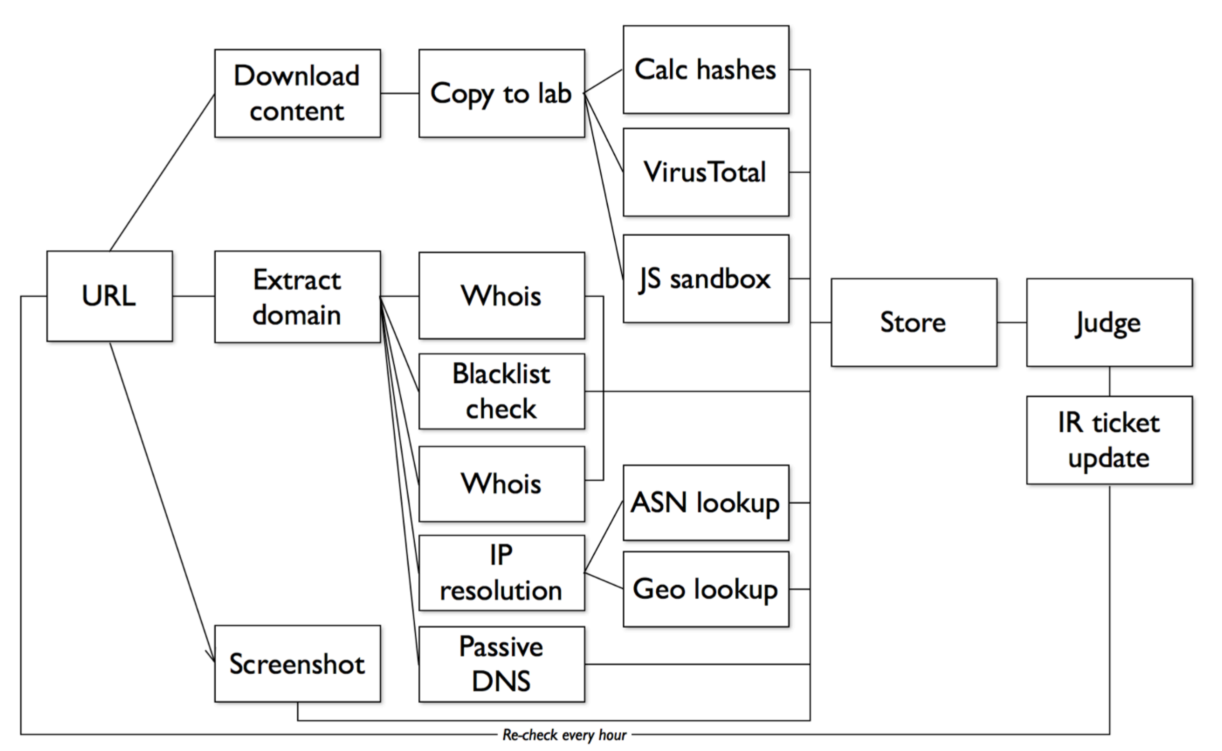
Use case: phishing campaign

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...

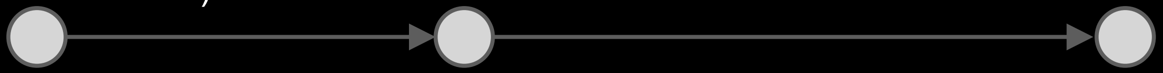
Manual incident handling workflow



Manual IR workflow

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

Automated IR workflow



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

Monitor & Decide

Incident Response

DATA NORMALIZATION

Information Feed Analysis System (IFAS)

E.g. ~100,000 events

ACTIONABLE DATA
(Filter and Prioritize)

Decision Support Management System (DSMS)

TICKETING SYSTEM

Incident Response Management System (IRMS)

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

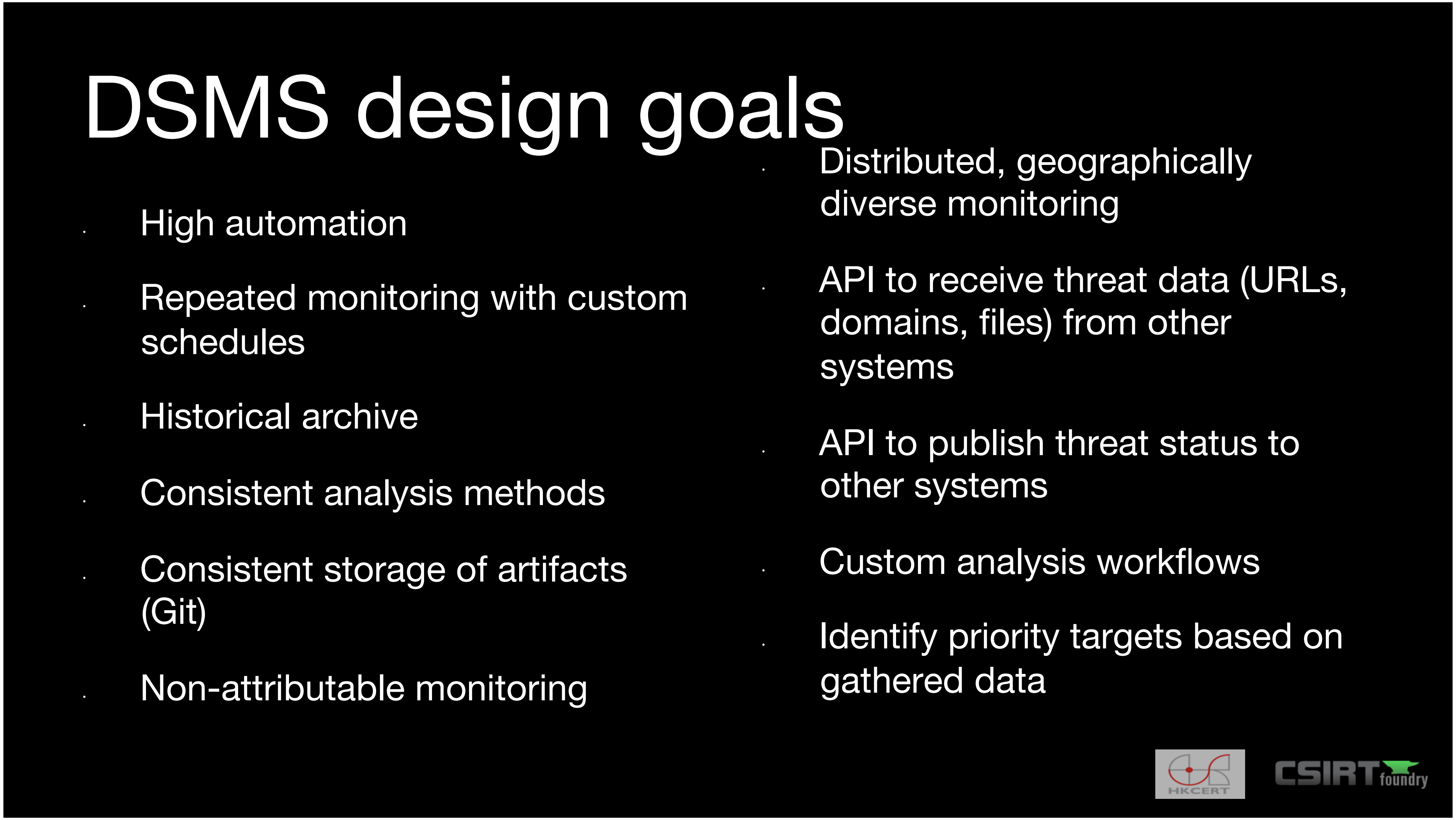
❑ Have a cup of coffee

❑ Wait for results

❑ Review all lookup results (e.g. WHOIS, IP, VirusTotal) on one page

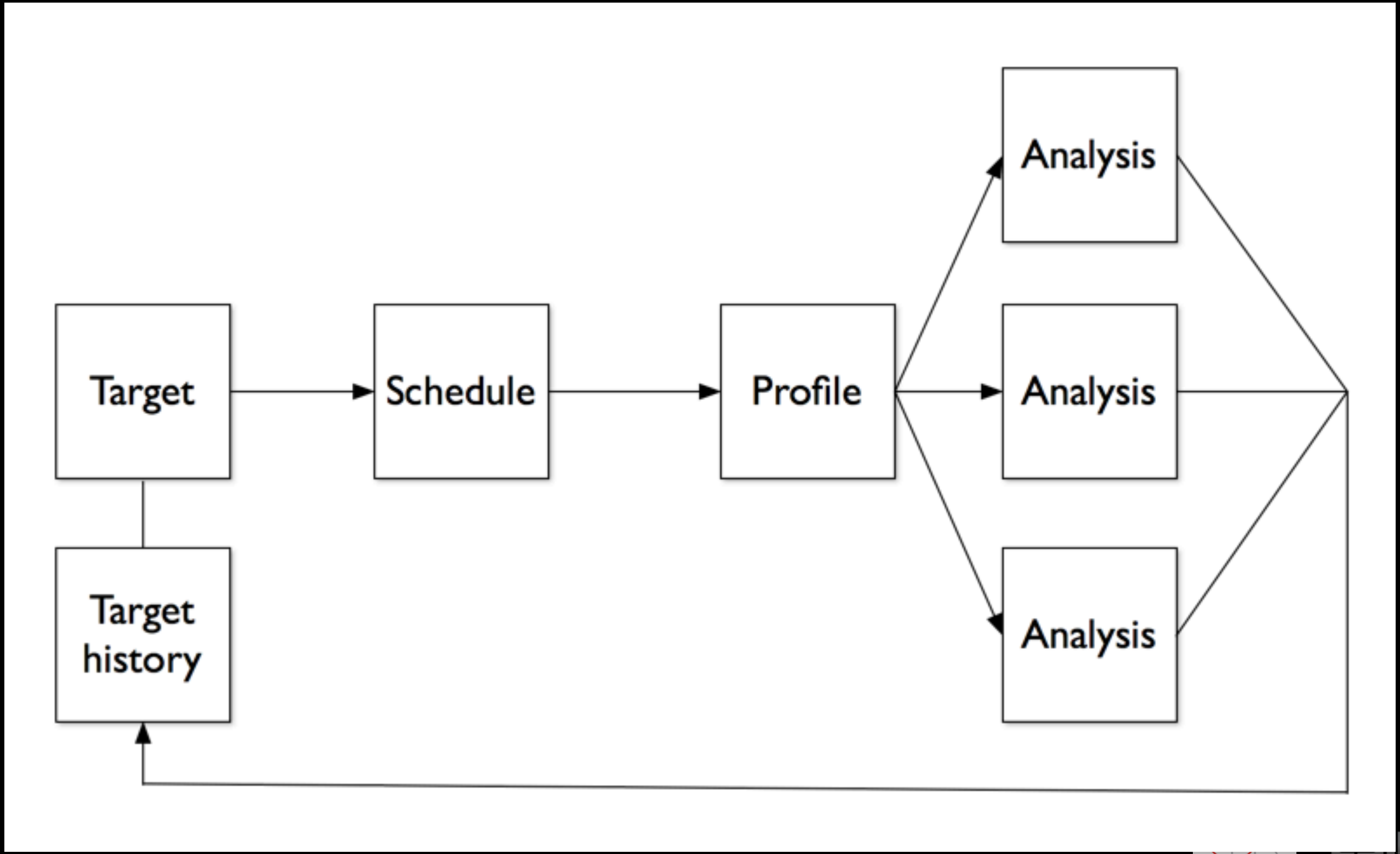
❑ Action on selected data

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



Target

Schedule

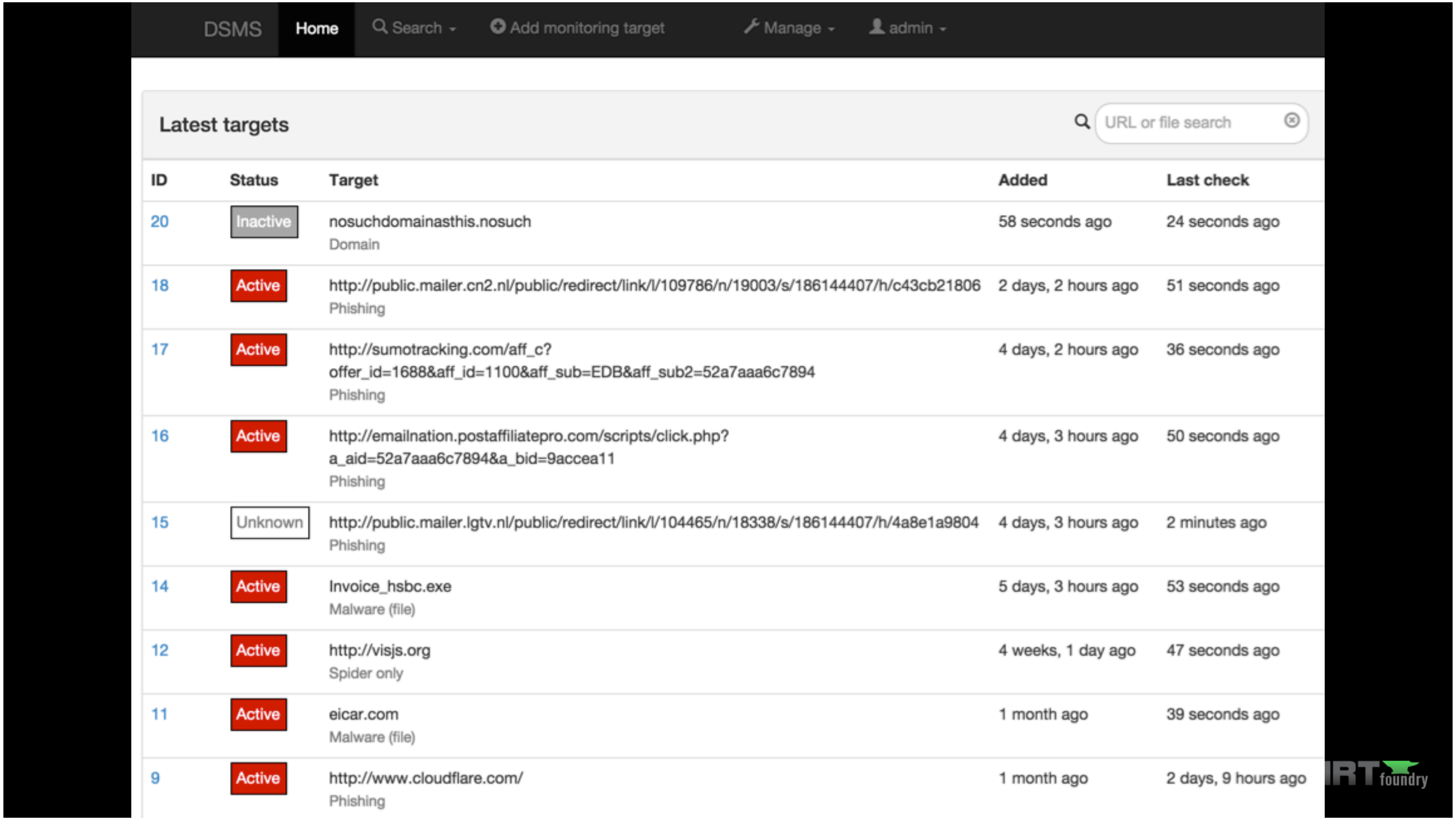
Profile

Analysis

Analysis

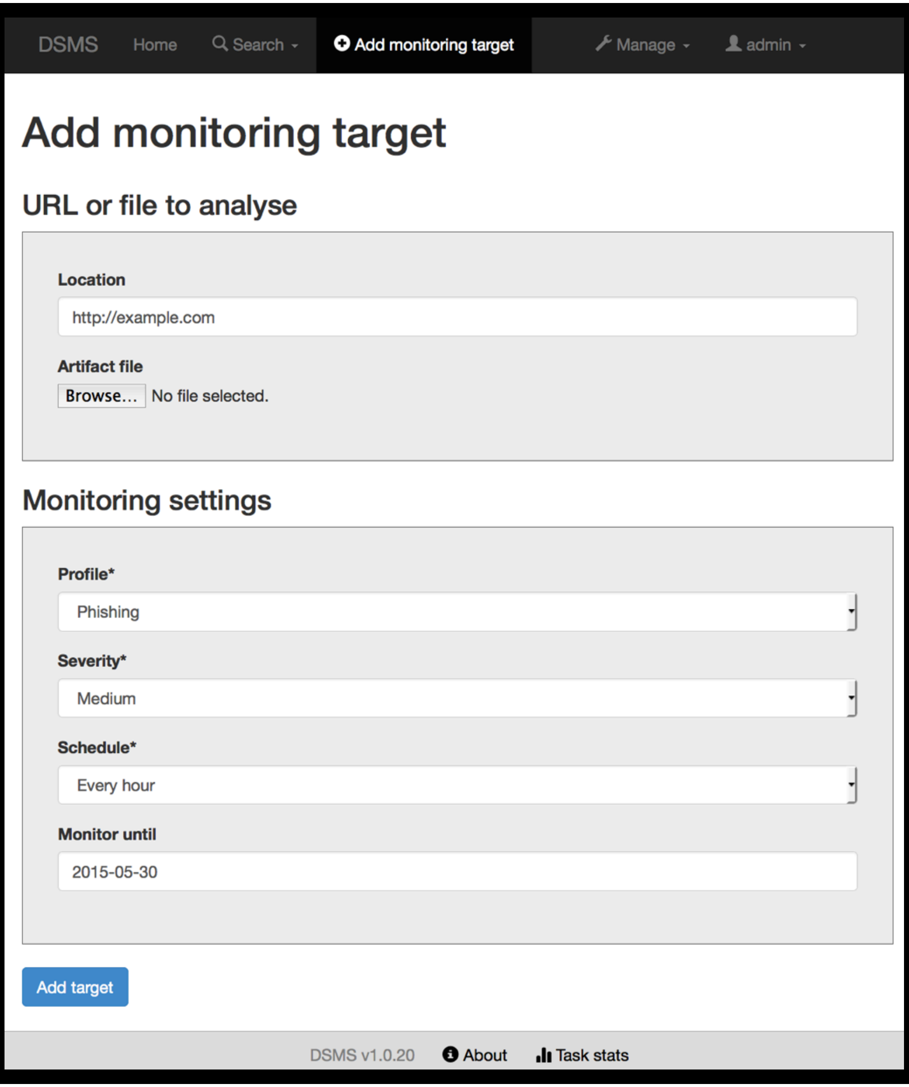
Analysis

Target history



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



Add monitoring target

URL or file to analyse

Location

http://example.com

Artifact file

Browse… No file selected.

Monitoring settings

Profile*

Phishing

Severity*

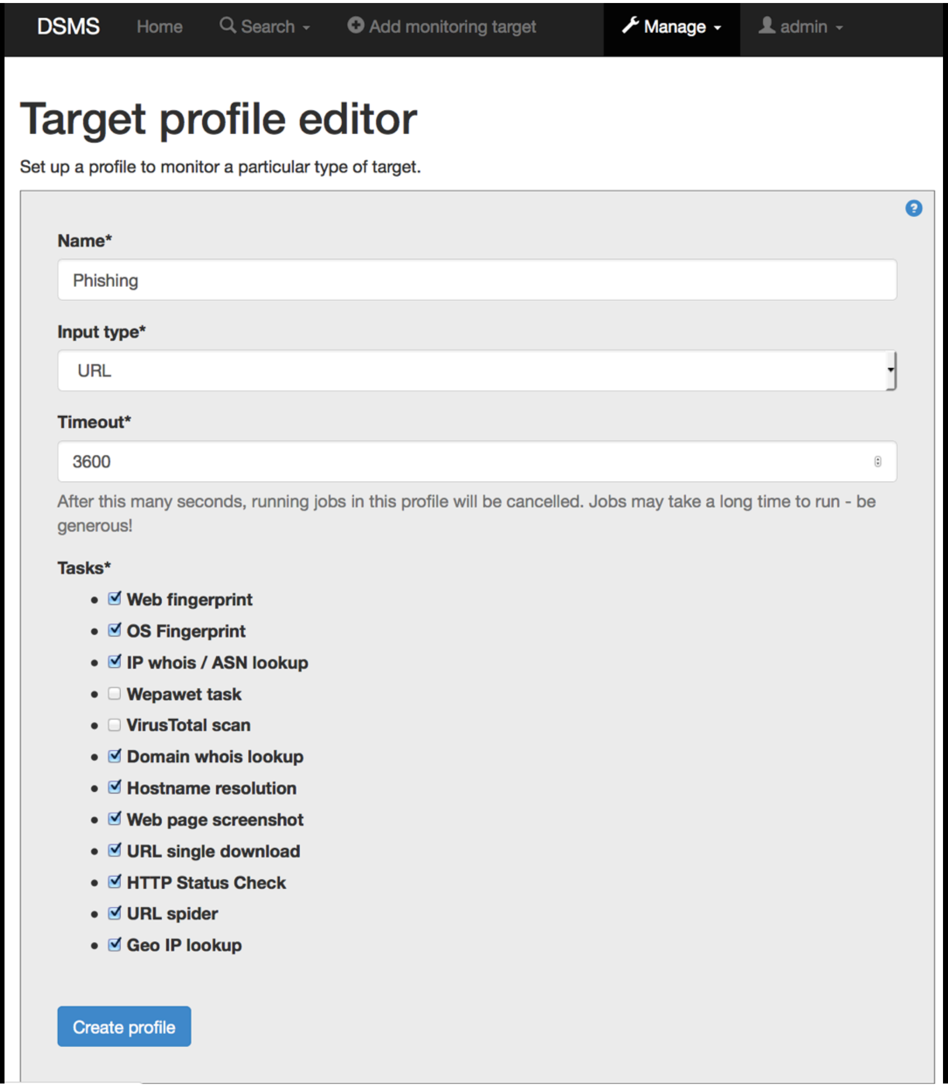
Medium

Schedule*

Every hour

Monitor until

2015-05-30



Target profile editor

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

Name*

Phishing

Input type*

URL

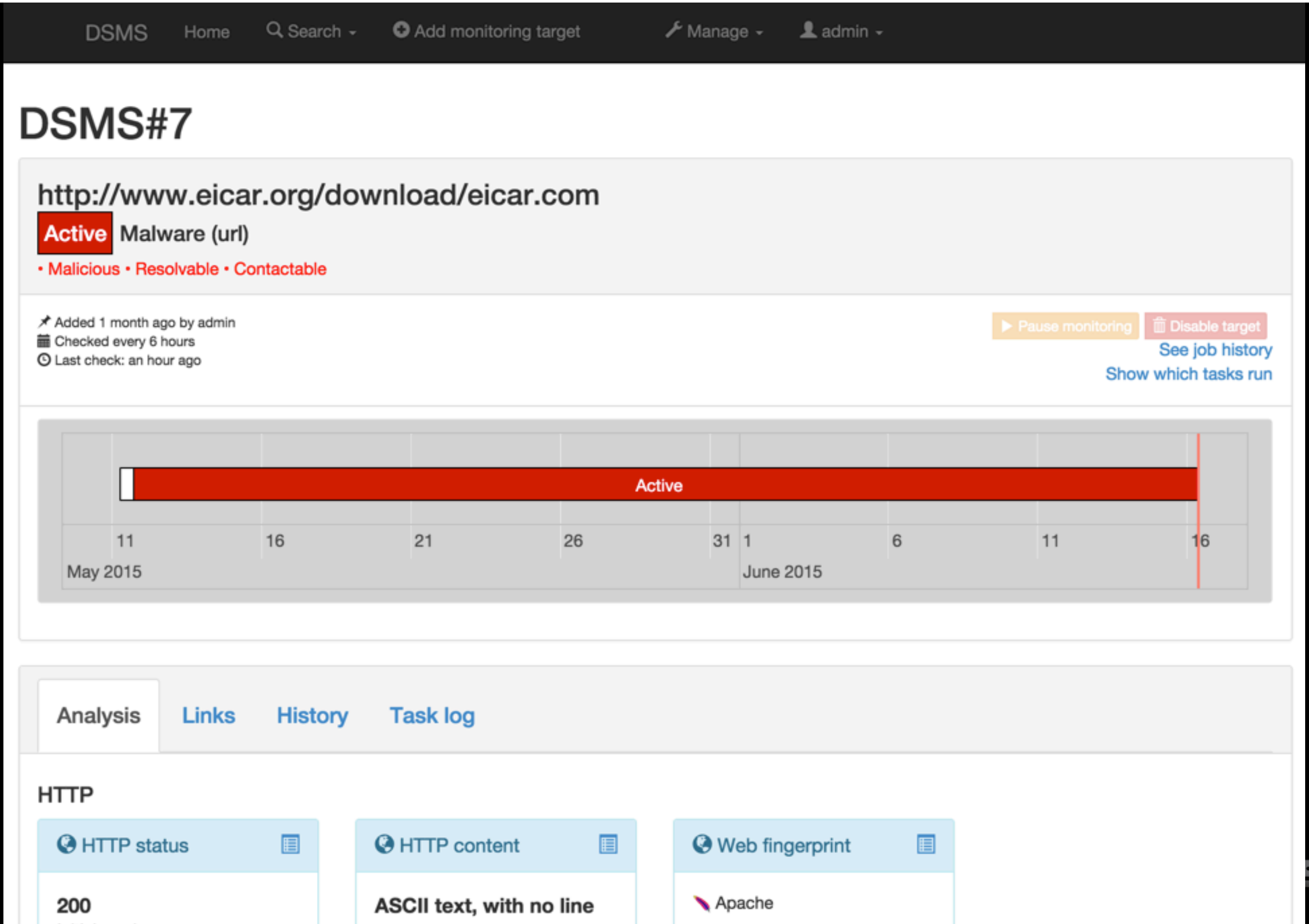
Timeout*

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



DSMS#7

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

Active Malware (url)

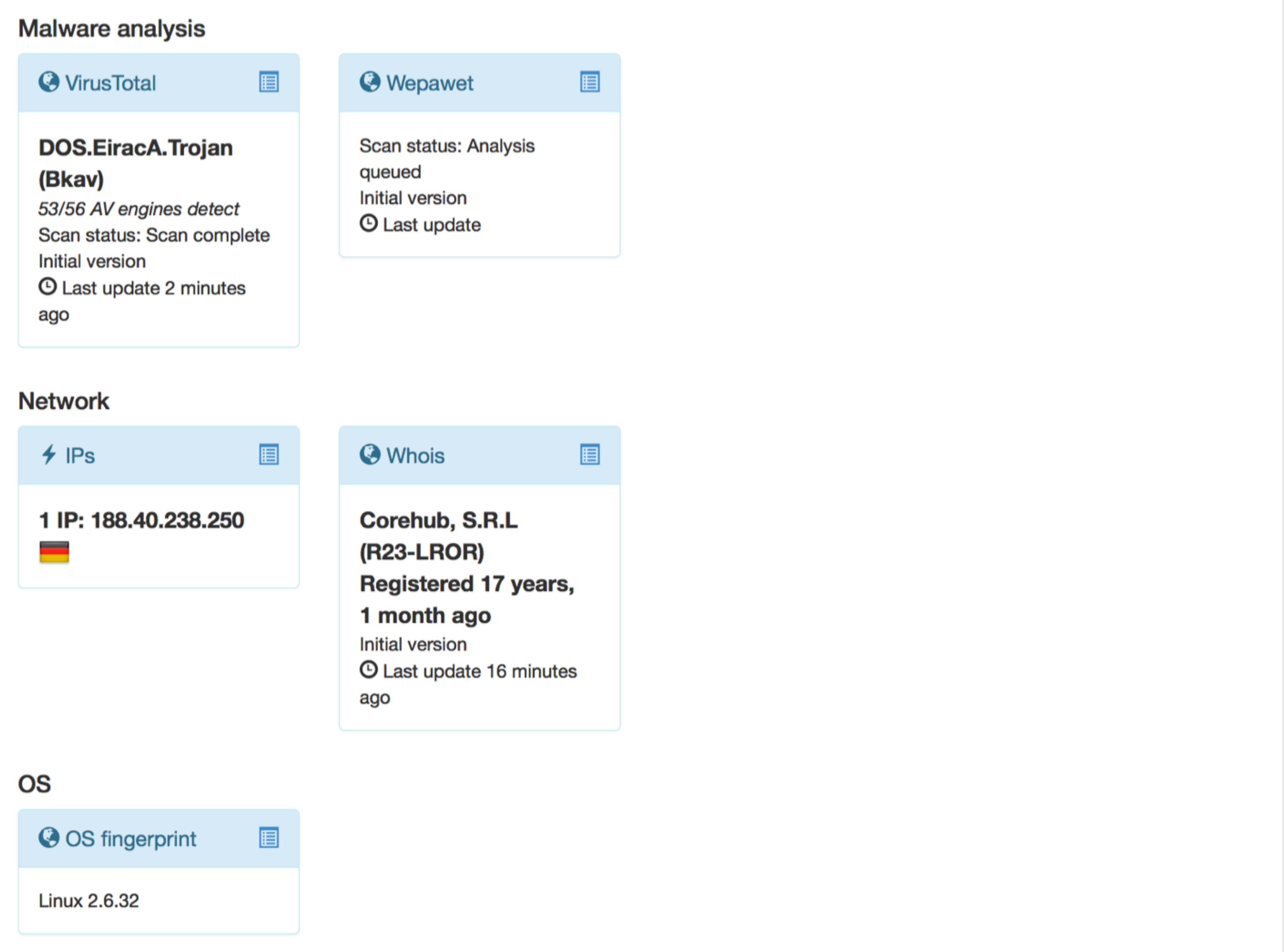
• Malicious • Resolvable • Contactable

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

HTTP

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

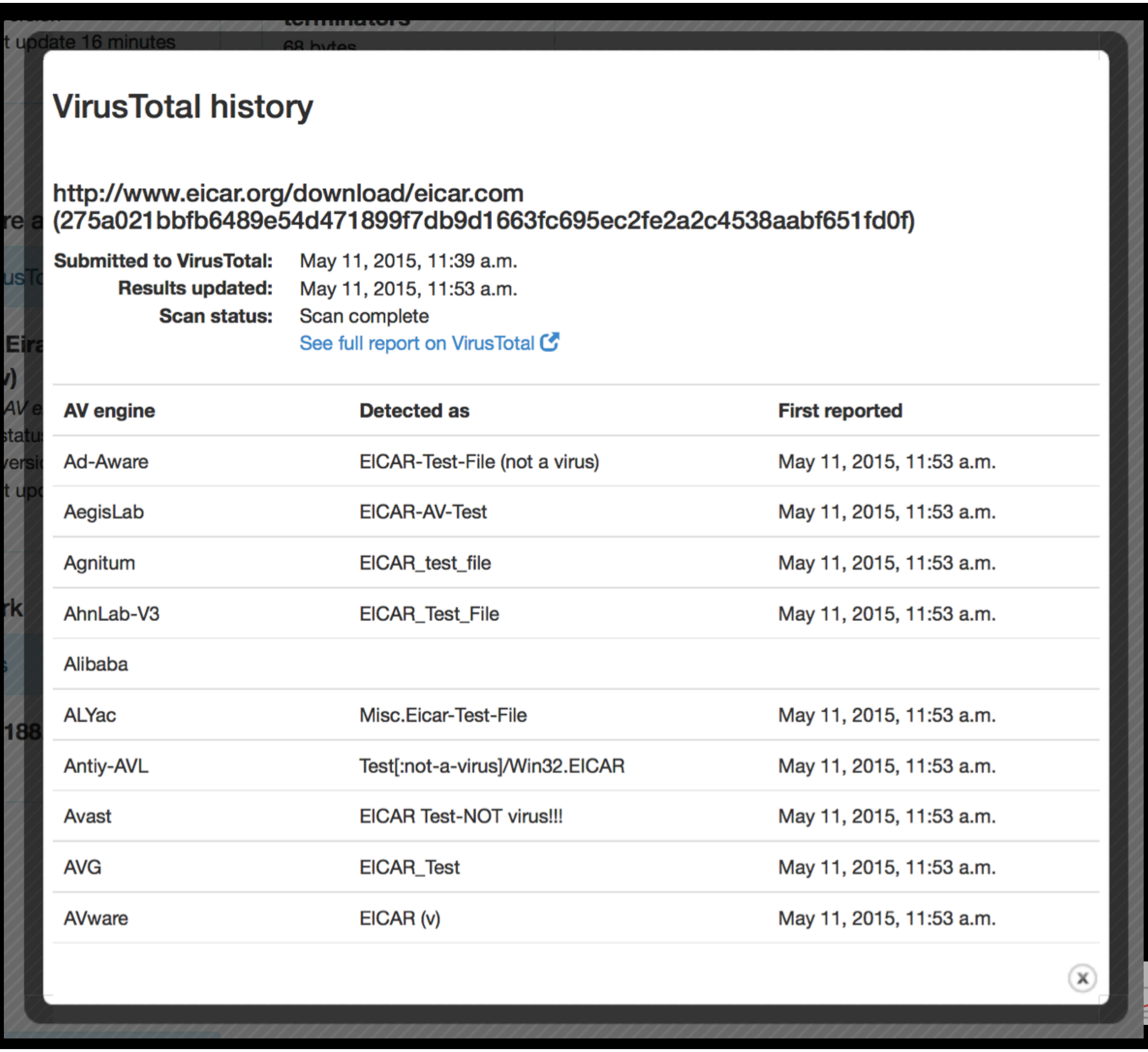
Initial version

Last update 16 minutes ago

OS

OS fingerprint

Linux 2.6.32

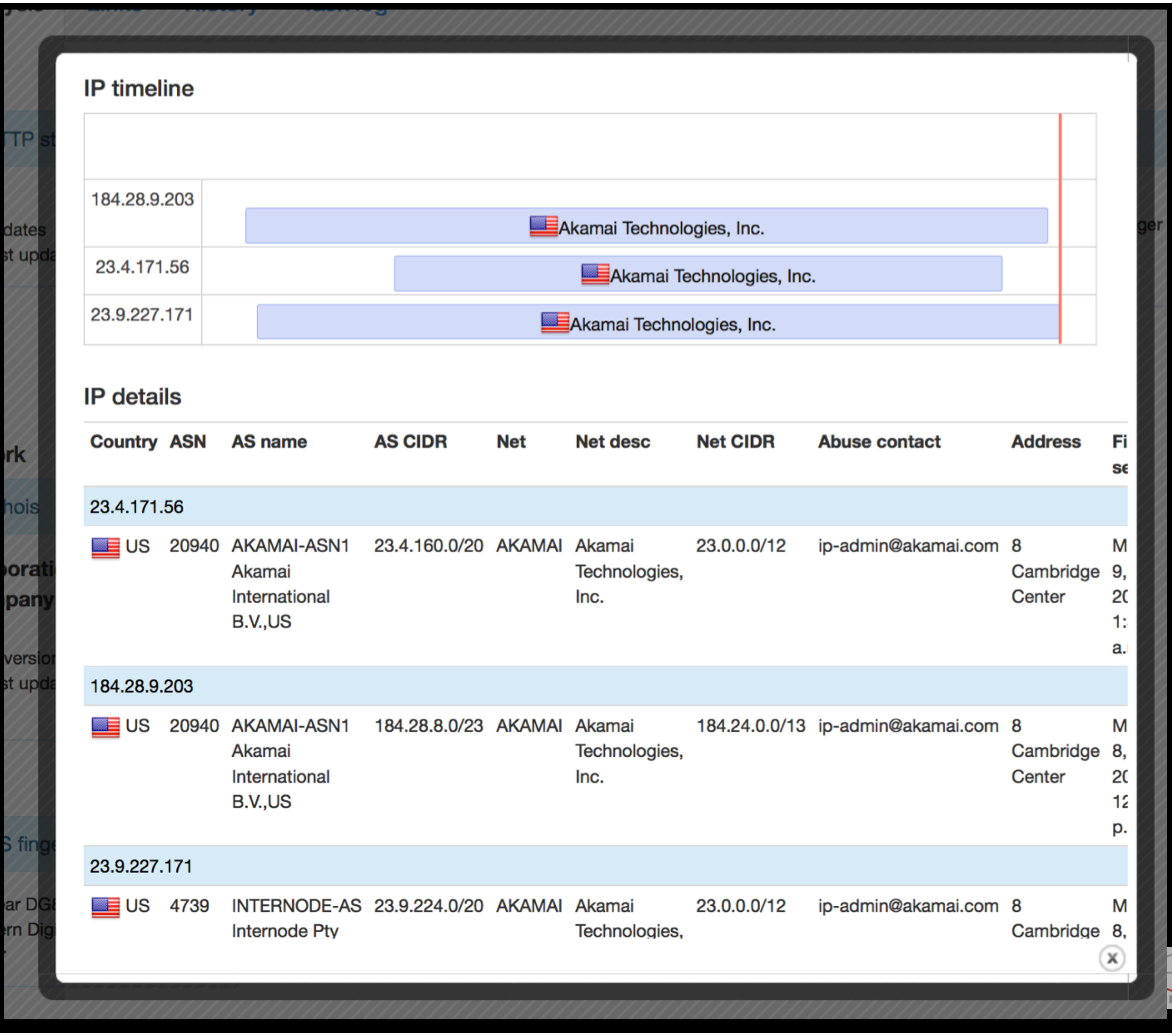


VirusTotal history

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.

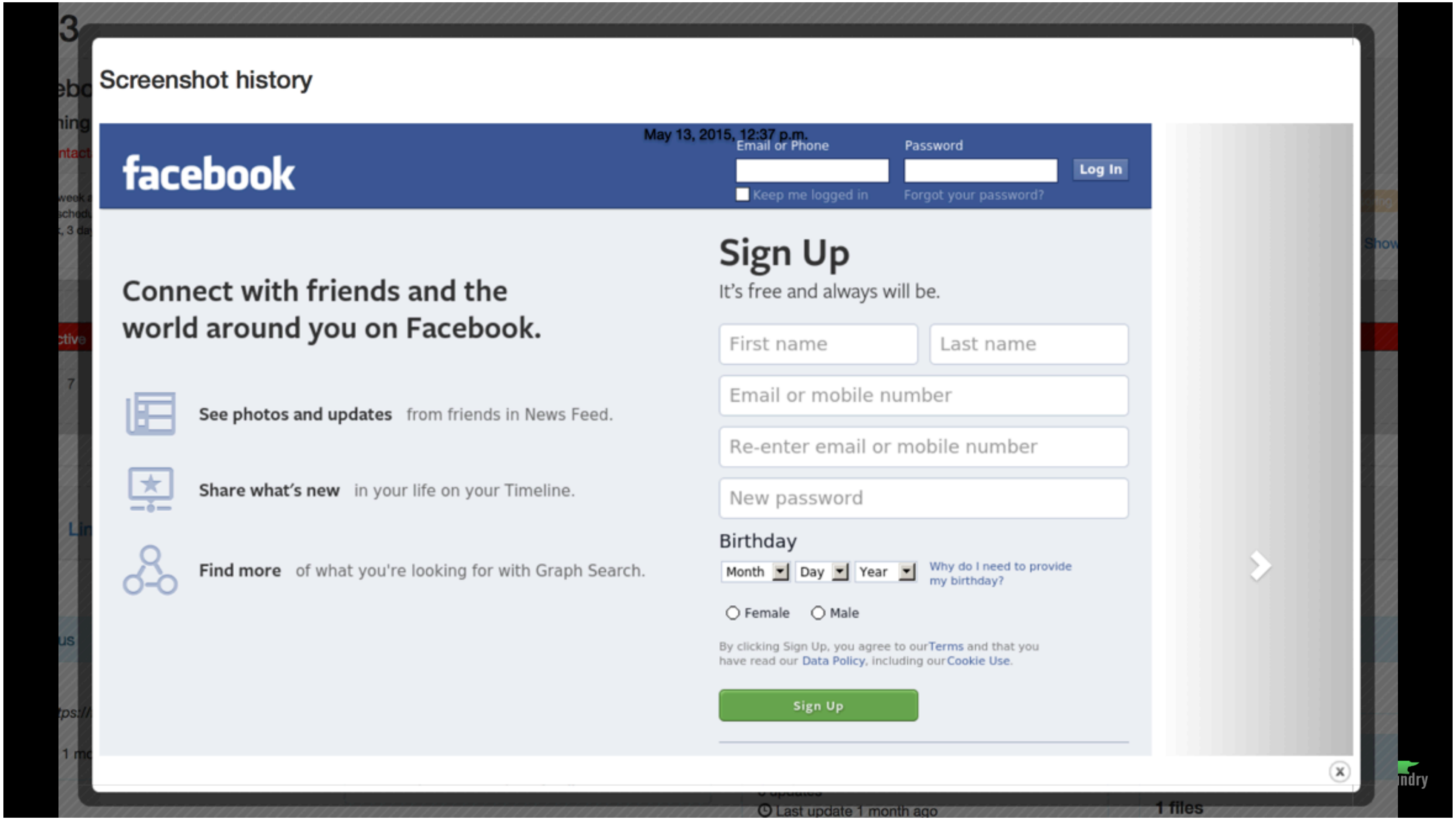


IP timeline

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	Fi se
23.4.171.56									
🇺🇸 US	20940	AKAMAI-ASN1 Akamai International B.V.,US	23.4.160.0/20	AKAMAI	Akamai Technologies, Inc.	23.0.0.0/12	ip-admin@akamai.com	8 Cambridge Center	M 9, 2(1: a.
184.28.9.203									
🇺🇸 US	20940	AKAMAI-ASN1 Akamai International B.V.,US	184.28.8.0/23	AKAMAI	Akamai Technologies, Inc.	184.24.0.0/13	ip-admin@akamai.com	8 Cambridge Center	M 8, 2(12 p.
23.9.227.171									
🇺🇸 US	4739	INTERNODE-AS Internode Pty	23.9.224.0/20	AKAMAI	Akamai Technologies,	23.0.0.0/12	ip-admin@akamai.com	8 Cambridge	M 8,



Screenshot history

May 13, 2015, 12:37 p.m.

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.

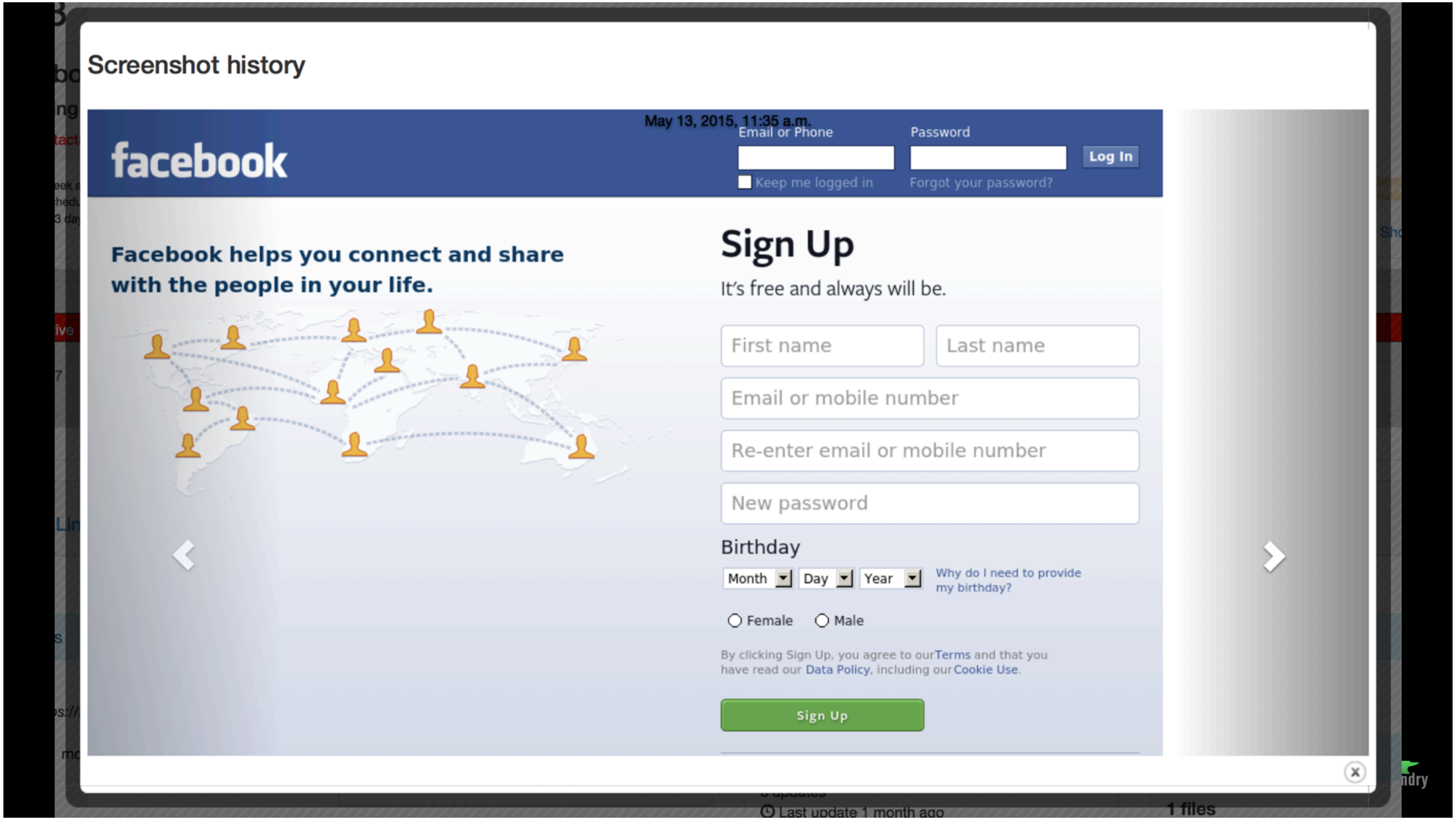
Birthday

○ Female ○ Male

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

Last update 1 month ago

1 files



Screenshot history

May 13, 2015, 11:35 a.m.

facebook

Email or Phone

Password

Log In

□ Keep me logged in

Forgot your password?

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?

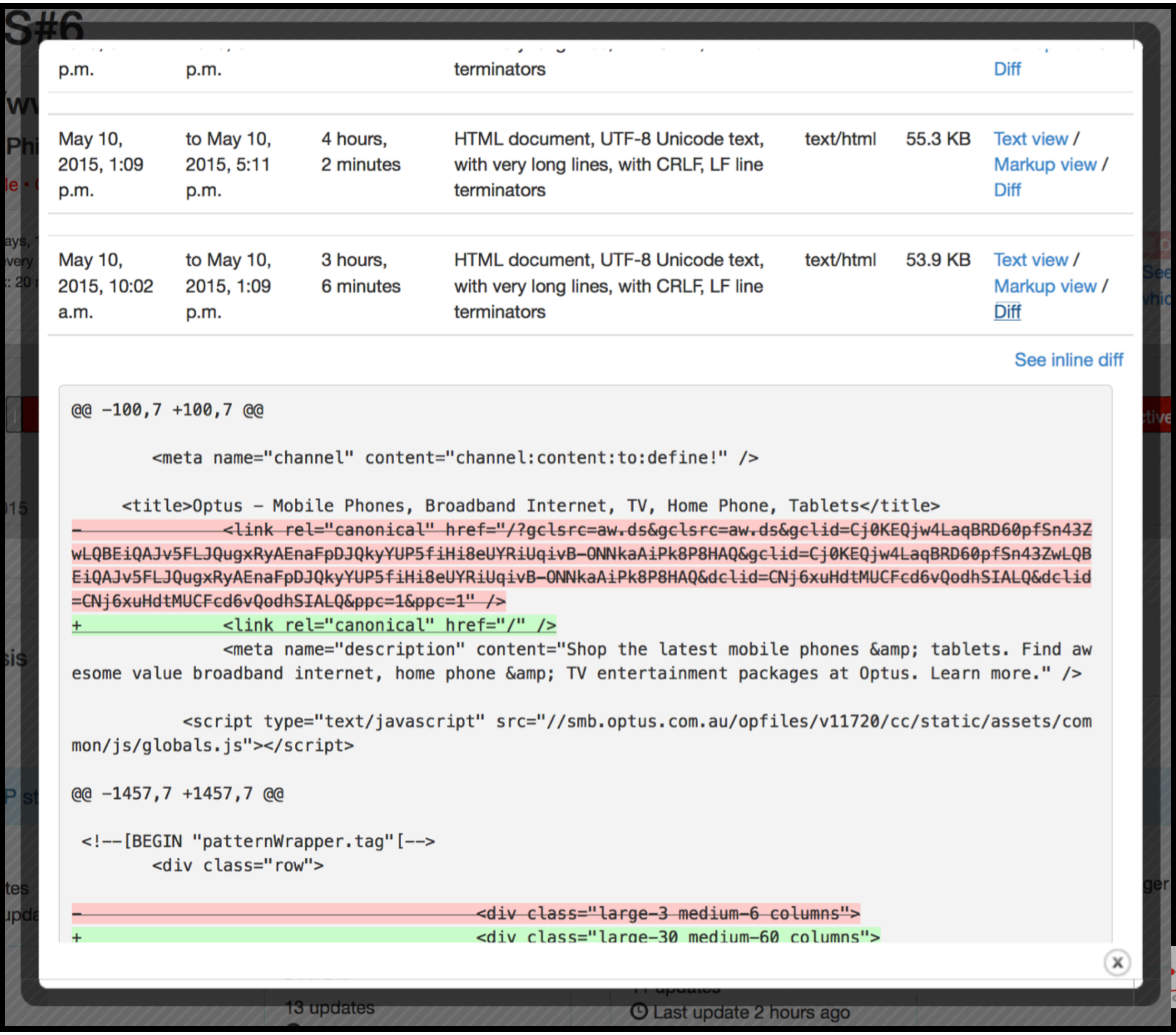
○ Female ○ Male

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

Sign Up

Last update 1 month ago

1 files



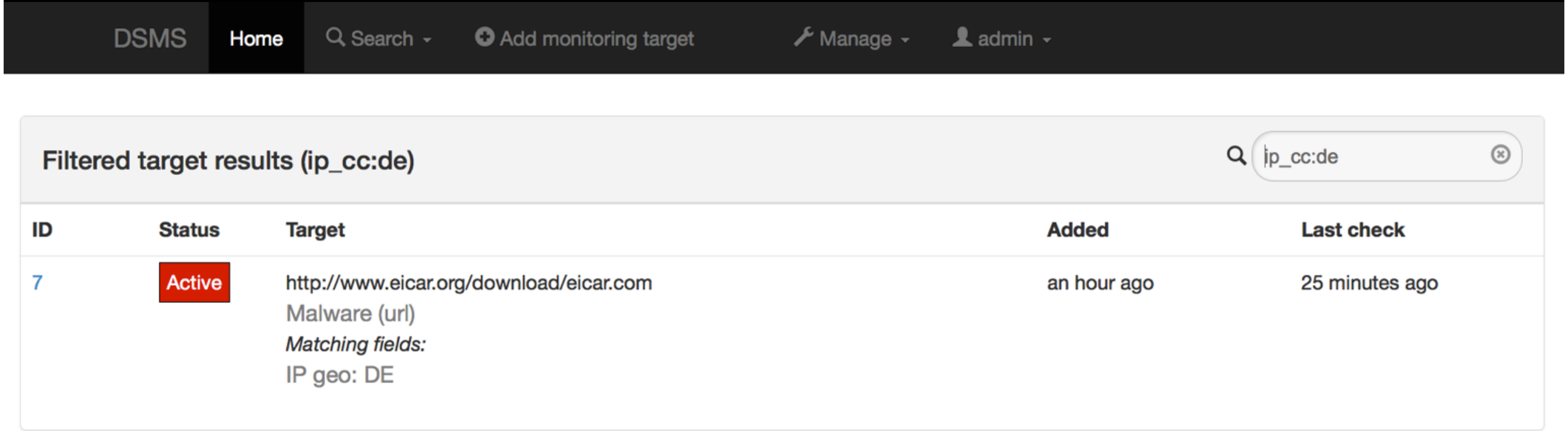
p.m.	p.m.		terminators			Diff
May 10, 2015, 1:09 p.m.	to May 10, 2015, 5:11 p.m.	4 hours, 2 minutes	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators	text/html	55.3 KB	Text view / Markup view / Diff
May 10, 2015, 10:02 a.m.	to May 10, 2015, 1:09 p.m.	3 hours, 6 minutes	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
wLQBEiQAJv5FLJQugxRyAEnaFpDJQkyYUP5fiHi8eUYRiUqivB-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 &amp; tablets. Find aw
esome value broadband internet, home phone &amp; TV entertainment packages at Optus. Learn more." />

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

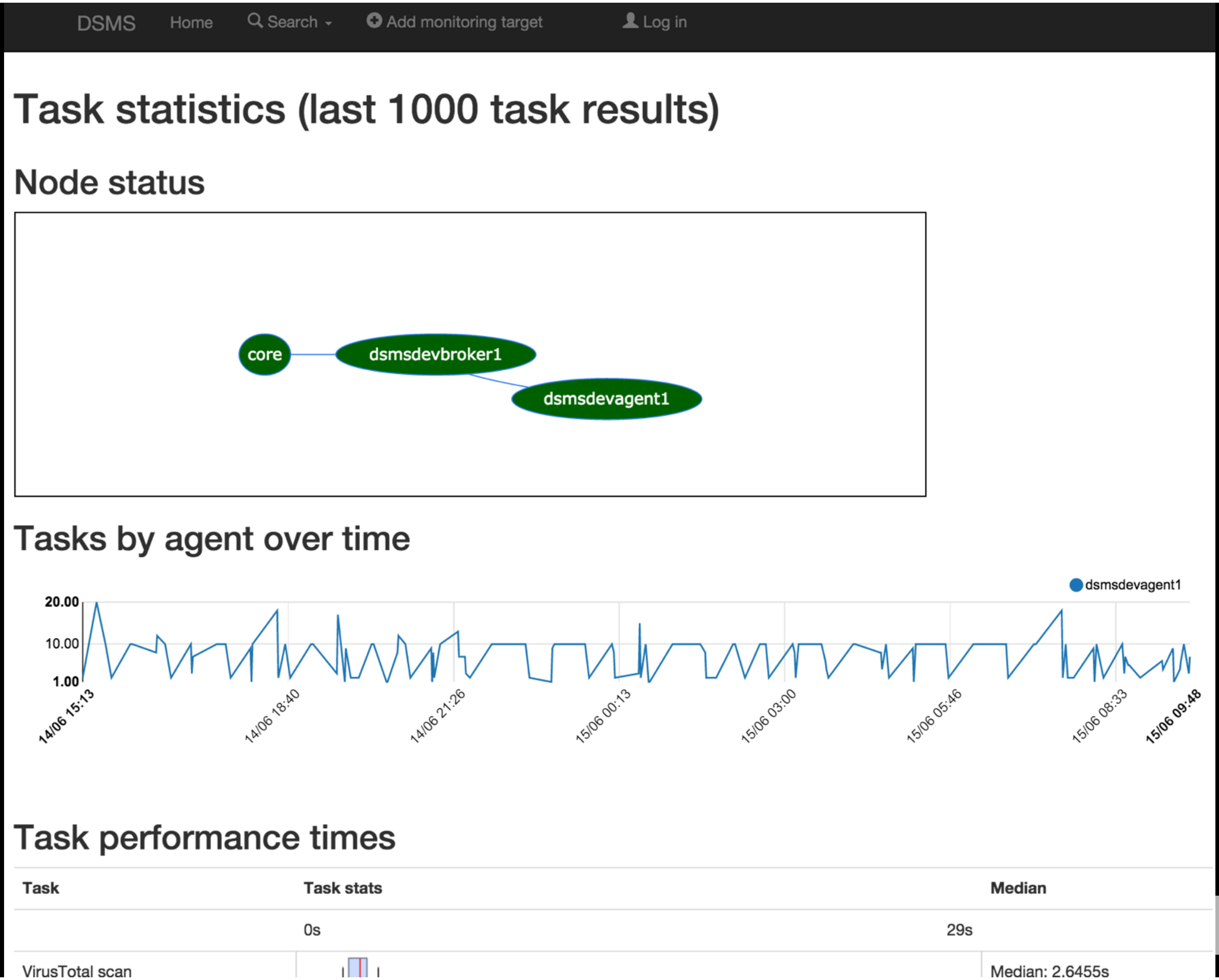
13 updates

Last update 2 hours ago



Filtered target results (ip_cc:de)

ID	Status	Target	Added	Last check
7	Active	http://www.eicar.org/download/eicar.com Malware (url) *Matching fields:* IP geo: DE	an hour ago	25 minutes ago



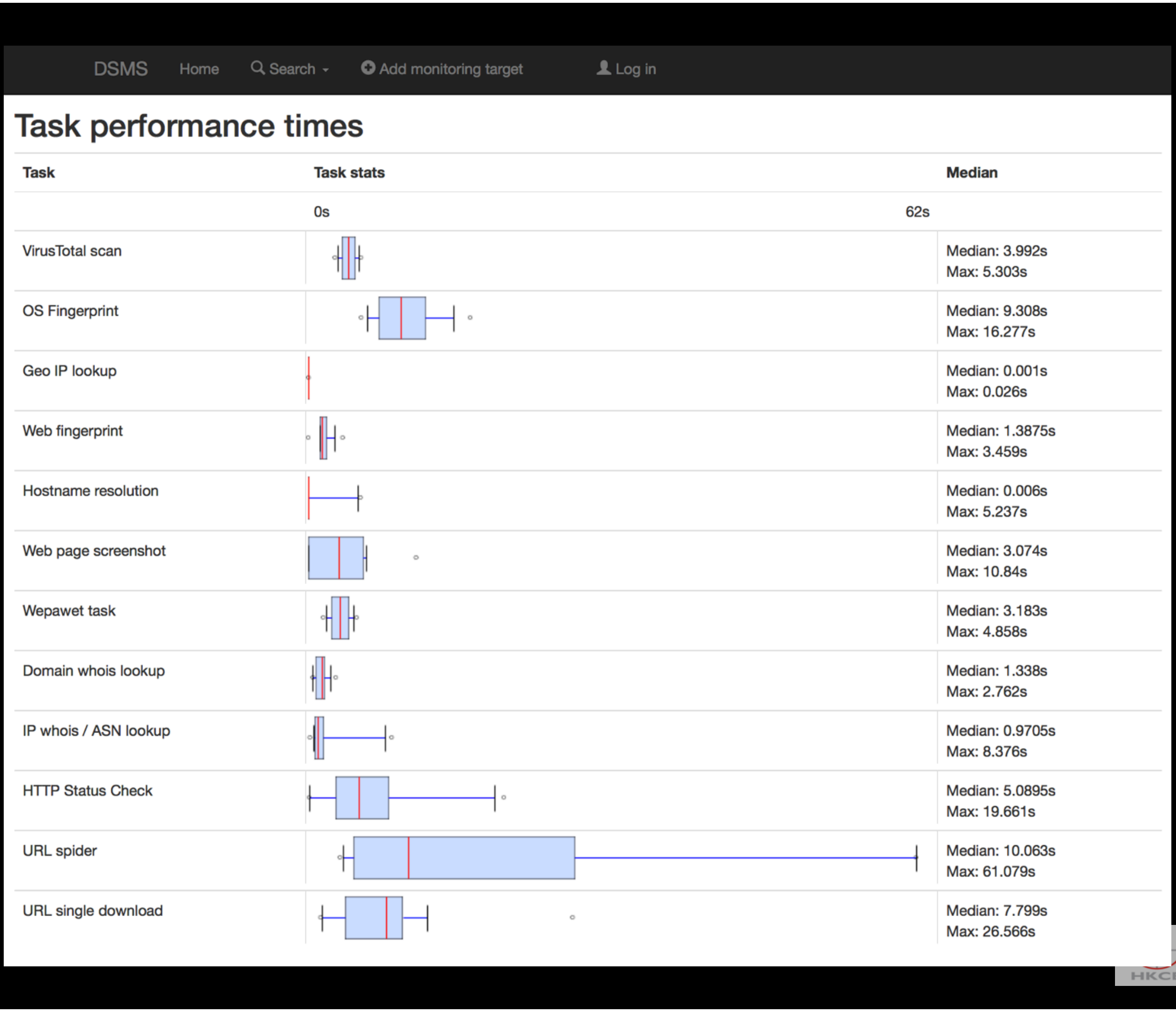
Task statistics (last 1000 task results)

Node status

Tasks by agent over time

Task performance times

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



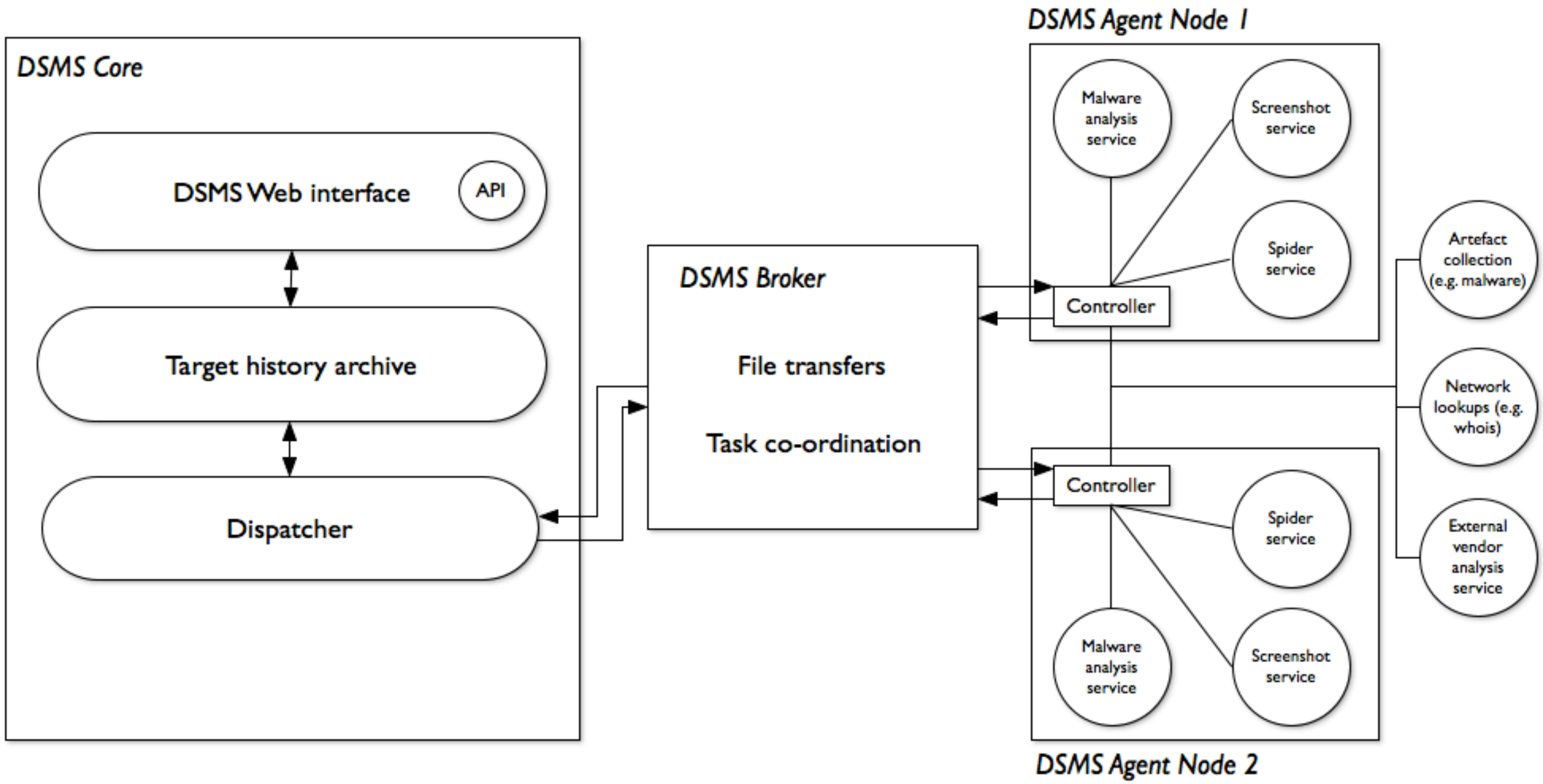
Task performance times

Task	Task stats	Median
	0s 62s	
VirusTotal scan		Median: 3.992s Max: 5.303s
OS Fingerprint		Median: 9.308s Max: 16.277s
Geo IP lookup		Median: 0.001s Max: 0.026s
Web fingerprint		Median: 1.3875s Max: 3.459s
Hostname resolution		Median: 0.006s Max: 5.237s
Web page screenshot		Median: 3.074s Max: 10.84s
Wepawet task		Median: 3.183s Max: 4.858s
Domain whois lookup		Median: 1.338s Max: 2.762s
IP whois / ASN lookup		Median: 0.9705s Max: 8.376s
HTTP Status Check		Median: 5.0895s Max: 19.661s
URL spider		Median: 10.063s Max: 61.079s
URL single download		Median: 7.799s Max: 26.566s

Technical details

Platform / technologies

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



DSMS Core

DSMS Web interface

API

Target history archive

Dispatcher

DSMS Broker

File transfers

Task co-ordination

DSMS Agent Node 1

Malware analysis service

Screenshot service

Spider service

Controller

DSMS Agent Node 2

Controller

Spider service

Malware analysis service

Screenshot service

Artefact collection (e.g. malware)

Network lookups (e.g. whois)

External vendor analysis service

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