

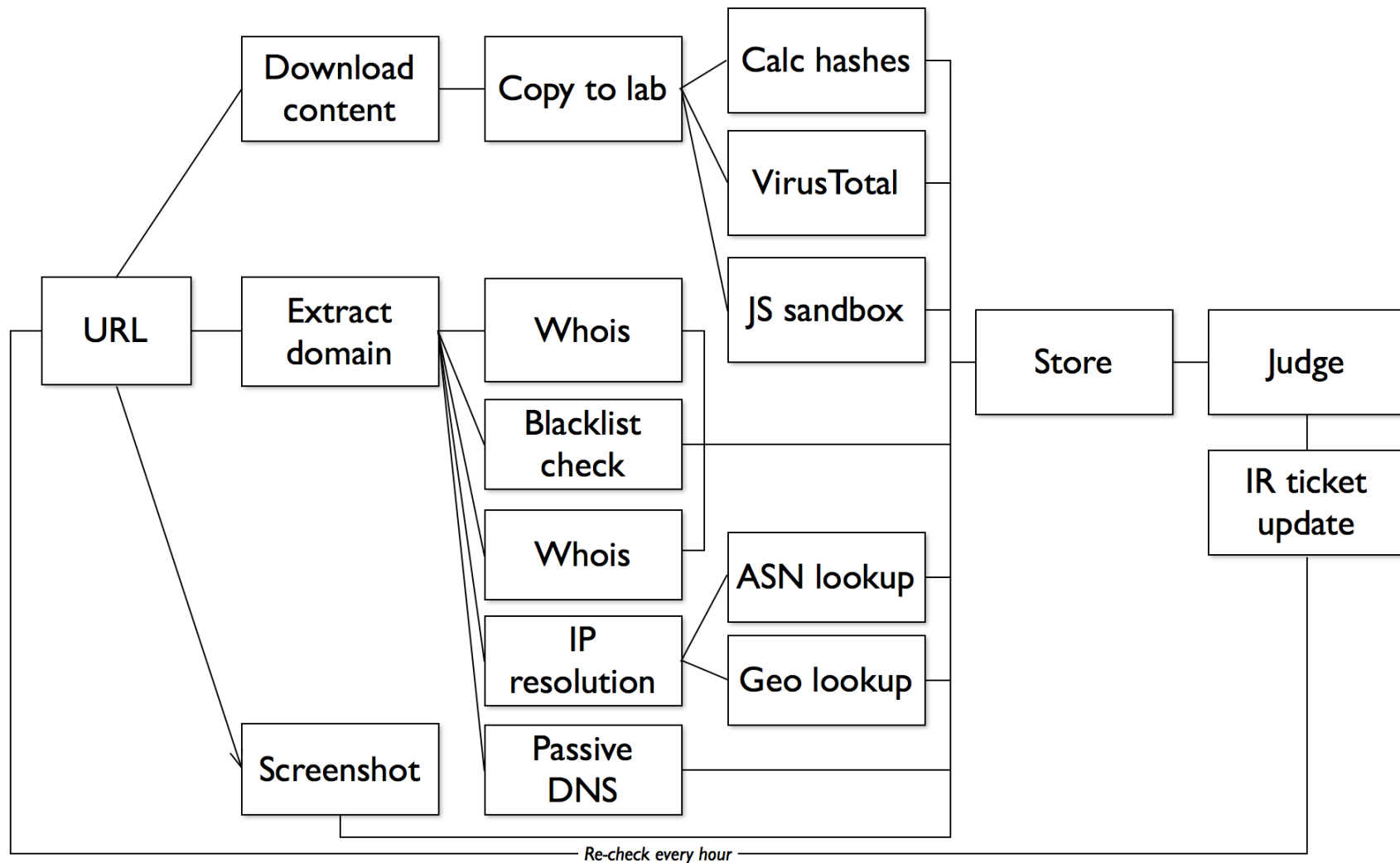
DSMS

Decision Support Monitoring System

- Automate incident response workflows
- Track threat life cycles
- Open source

IR team challenges

Typical IR workflows



Many steps

Unsafe handling of malicious files

May be identified by attackers based on IP, metadata

Storage inconsistent, tedious

Repeated, manual re-checking of targets time-consuming

Manual decision making on targets: malicious or not?

Results can take a long time to arrive (e.g. external sandboxes)

DSMS 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

DSMS in action

Add monitoring target

URL or file to analyse

Location**Artifact file** No file selected.

Monitoring settings

Profile***Severity*****Schedule*****Monitor until**

Target profile editor

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

Name***Input type*****Timeout***

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 16 minutes ago by admin

📅 Checked every 10 mins

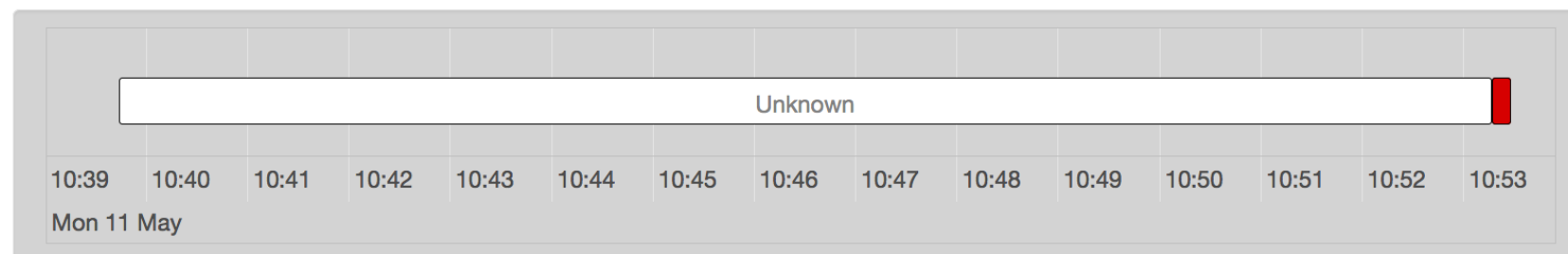
🕒 Last check: 2 minutes ago

▶ Pause monitoring

🗑 Disable target

[See job history](#)

[Show which tasks run](#)



Analysis

[Links](#)

[History](#)

[Task log](#)

HTTP

🌐 HTTP status



200

Initial version

🕒 Last update 16 minutes ago

🌐 HTTP content



ASCII text, with no line terminators

68 bytes

Initial version

🕒 Last update 16 minutes ago

🌐 Web fingerprint



🎨 Apache

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

200

Initial version

Last update 16 minutes ago

ASCII text, with no line terminators

68 bytes

Apache

Malware a

VirusTotal

DOS.Eir
(Bkav)

53/56 AV e

Scan statu

Initial vers

Last up
ago

Network

IPs

1 IP: 188



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.



Analysis

Links

History

Task log

HTTP

HTTP st

200

11 updates

Last update

Network

Whois

Corporate
Company
Ltd

Initial version




Last update
ago

OS




OS fingerprint

Netgear DG
Western Dig
player

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
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, 20 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, 20 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,

DSMS#3

http://fa

Active Ph

• Resolvable •

✦ Added 4 days,

☑ Checked every

🕒 Last check: 47

May 2015

Analysis

HTTP

🌐 HTTP st

301

Redirects to

https://faceb

2 updates

🕒 Last upda

ago

Network

May 8, 2015, 1:33 p.m.

facebook

Email or Phone

Password

Log In

☐ Keep me logged in

Forgot your password?

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

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

Create a Page for a celebrity, band or business.

English (US) 中文(简体) 한국어 日本語 Français (France) Español Deutsch Italiano Português (Brasil) العربية ...

Sign Up

Locations

About

Messenger

Create Ad

Mobile

Create Page

Find Friends

Developers

Badges

Careers

People

Privacy

Pages

Cookies

Places

Ad Choices

Games

Terms

Help

Facebook © 2015

Disable target

See job history
which tasks run

📄

🕒 Last update 2 days, 23 hours ago

<http://www>

- Resolvable •

⌚ Last check: 20 m

May 2015

Analysis

HTTP

 HTTP st

200

11 updates

⌚ Last update

13 updates

🕒 Last update 3 hours ago

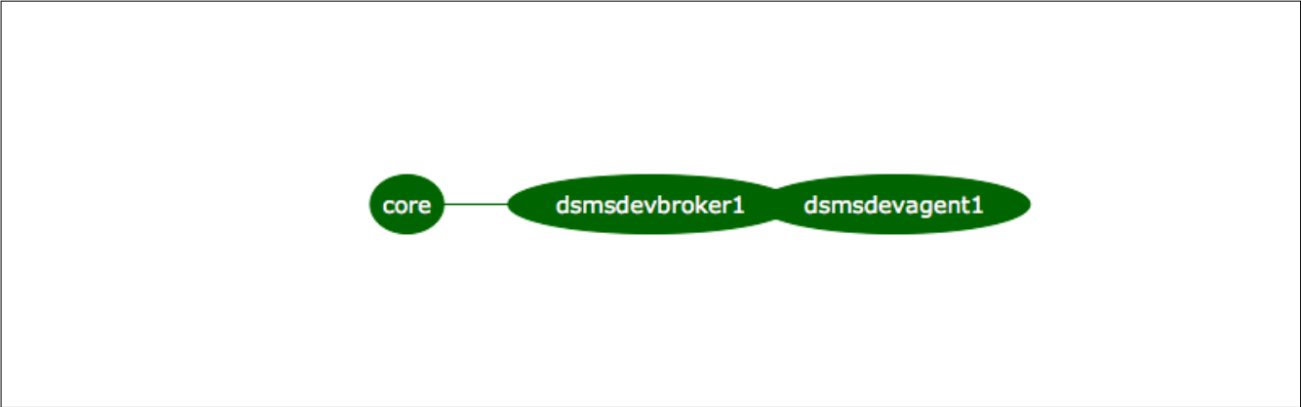
It updates

🕒 Last update 2 hours ago

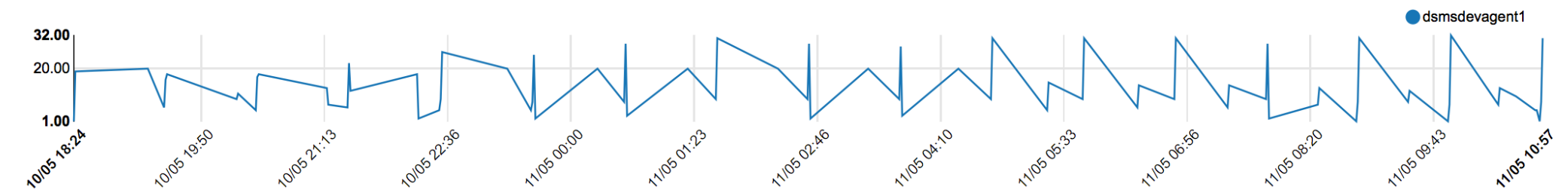
Network

Task statistics (last 1000 task results)

Node status




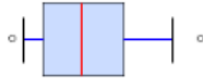


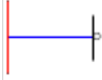
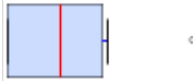



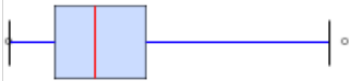


Tasks by agent over time



Task performance times

Task	Task stats	Median
	0s	62s
VirusTotal scan		Median: 3.992s Max: 5.303s

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

Filtered target results (ip_cc:de)



ip_cc:de



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

Technical details

Platform / technologies

Python

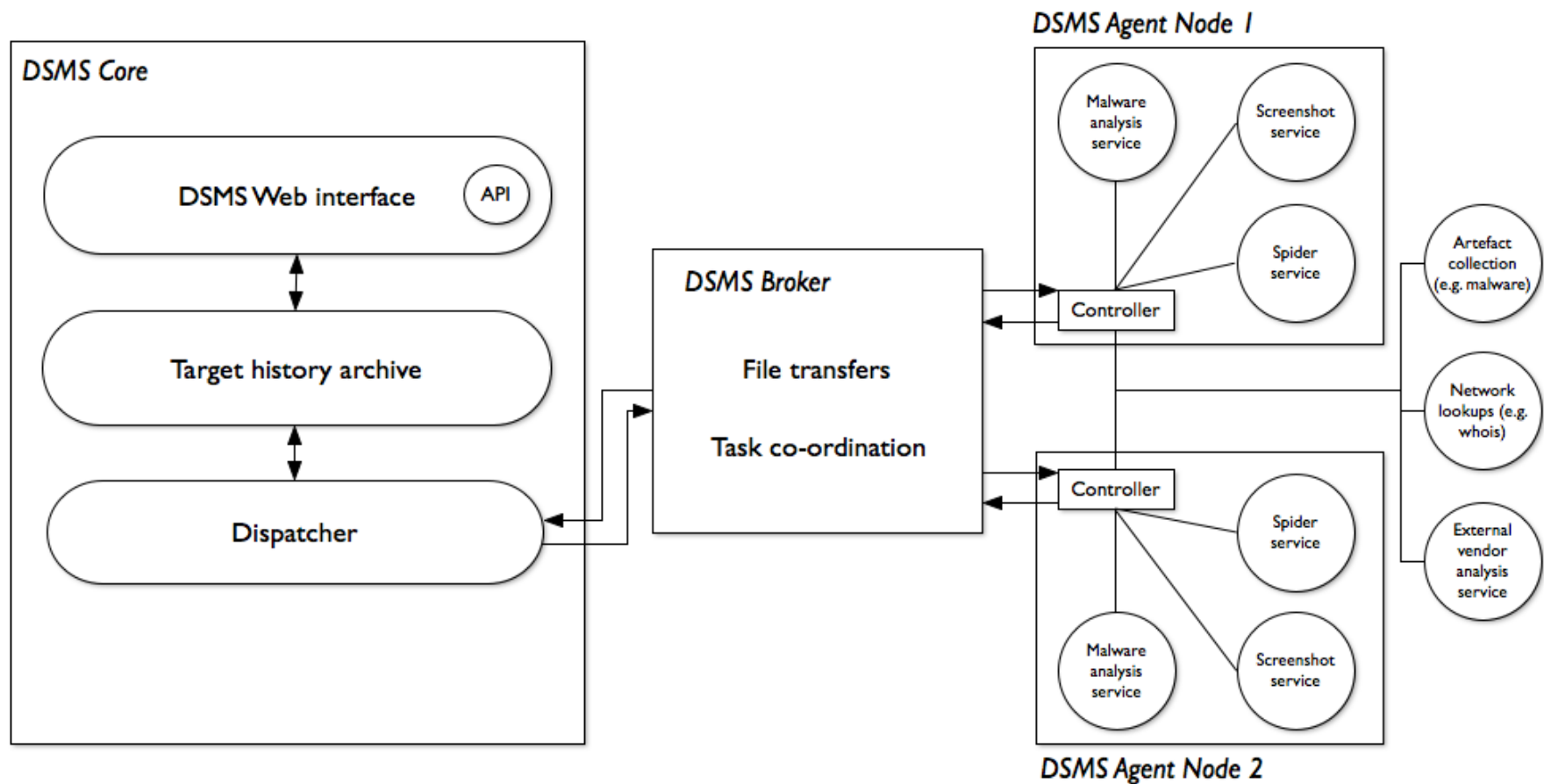
Django

Celery (distributed task execution)

RabbitMQ

Ubuntu 14.04 (current supported OS)

Architecture



Hosting

Core: internal (Postgres + file repo + Django + dispatcher)

Broker: DMZ or external (RabbitMQ + SFTP server)

Agents: external (Celery task execution, data collection)

Current modules

HTTP status

HTTP spidering

URL screenshot

IP resolution

ASN /ISP lookup

WHOIS lookup and parsing

OS fingerprinting

Web site fingerprinting

VirusTotal analysis

CWSandbox analysis

Future features

Tagging targets for analyst notes

Classification and prioritisation of targets

Android binary analysis

Further HTML / Javascript analysis with Thug

Passive DNS

TLS certificate analysis

Bitcoin wallet monitoring

Email address analysis

Artifact similarity analysis

Collaboration

Open source (Apache) licence

Currently available by invitation to trusted CSIRTs

Feature requests and patches highly encouraged!

Commercial support available

Thank you

Questions and enquiries welcome: chris.horsley@csirtfoundry.com