

Keeping Eyes on Malicious Websites “ChkDeface” against Fraudulent Sites

Hiroshi KOBAYASHI, Takayuki UCHIYAMA
Japan Computer Emergency Response Team
Coordination Center (JPCERT/CC)

Agenda

■ Background

—Increase and changes in website defacements

■ Internal operations when a defacement is discovered

Hiroshi KOBAYASHI

koba is a Information Security Analyst at JPCERT Coordination Center, National CSIRT in Japan.

He is in charge of incident response.

■ System Development

—chkdeface

Takayuki UCHIYAMA

Taki is a Information Security Analyst at JPCERT Coordination Center, National CSIRT in Japan.

He is in charge of handling vulnerability reports.

■ Going Forward

BACKGROUND

Reasons for Defacing a Website

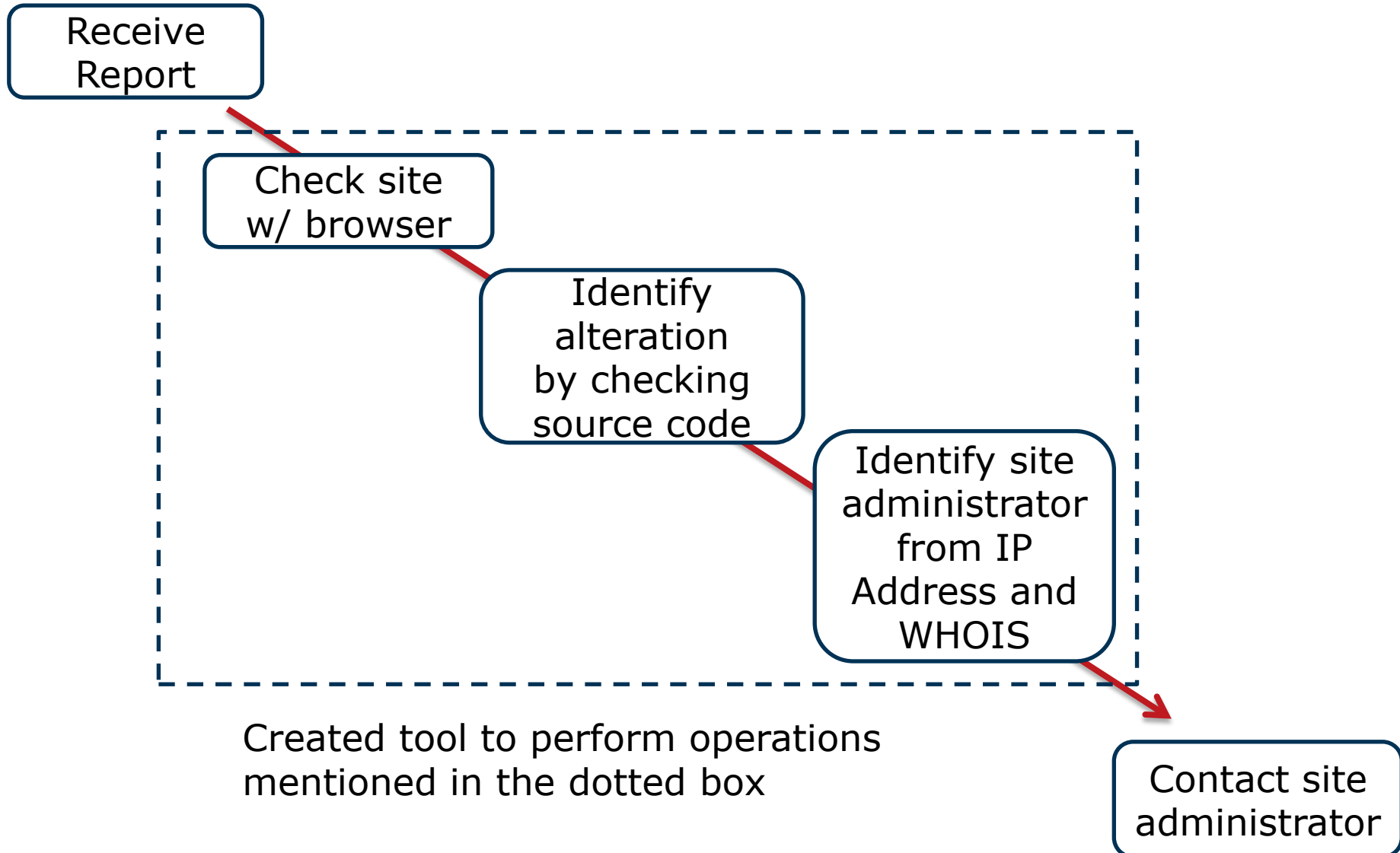
- To infect with malware
 - “Guide” to an Exploit Kit
- "Guide" to a fake shopping site (Spamvertising)
 - Pharmacy, Supplements
 - Selling fake products, etc.
- To use for SEO poisoning
- Exhibit power or make a political stand
 - Hacked by / Pwned by
 - Display country flag or organization log
- To leverage in DDoS attacks

Causes that allow for defacements

- Account information for servers are stolen
 - By brute force
 - Use account information stolen from a PC by malware
- Leveraging a web application vulnerability
 - CMS(WordPress(plugin),Joomla!,Movable Type,...)
 - Custom PHP (written from scratch)
- Leveraging a server management software vulnerability
 - Plesk, cPanel, etc.
- Leveraging a middleware vulnerability
 - GNU Bash, Struts, etc.

INTERNAL OPERATIONS WHEN A DEFACEMENT IS DISCOVERED

Flow for Checking Website Defacements



Things to keep in mind when checking Website defacements

- Check websites with an environment that will not be affected by malicious contents
- Conserve the website contents
 - Data for contents that make up the site (html, images, CSS, JS)
 - Screenshot of the website
- Record website information
 - IP address of the site
 - WHOIS information on the IP address and domain

SYSTEM DEVELOPMENT

Requirements

- Obtain contents and a screenshot in one access attempt
 - Some sites change behavior when accessed again
- Does not get infected when obtaining source code
 - Both the checker and tool
- Record the time of the check
 - Investigative organizations ask for this information
- Relatively easy to troubleshoot when there is an overload or an issue
- Importance on 'real-time'

Become more efficient by using a tool

- Developed a Django based Web application
 - Chkdeface

- Main operations
 1. Register the website URL
 - Handles HTTP,HTTPS,FTP
 - Handles PROXY
 - Handles both Referer and user-agent

 2. Contents for the registered website are obtained
 - Source code for the webpage that is displayed in the browser
 - Contents that make up the webpage
 - Screenshot of the webpage

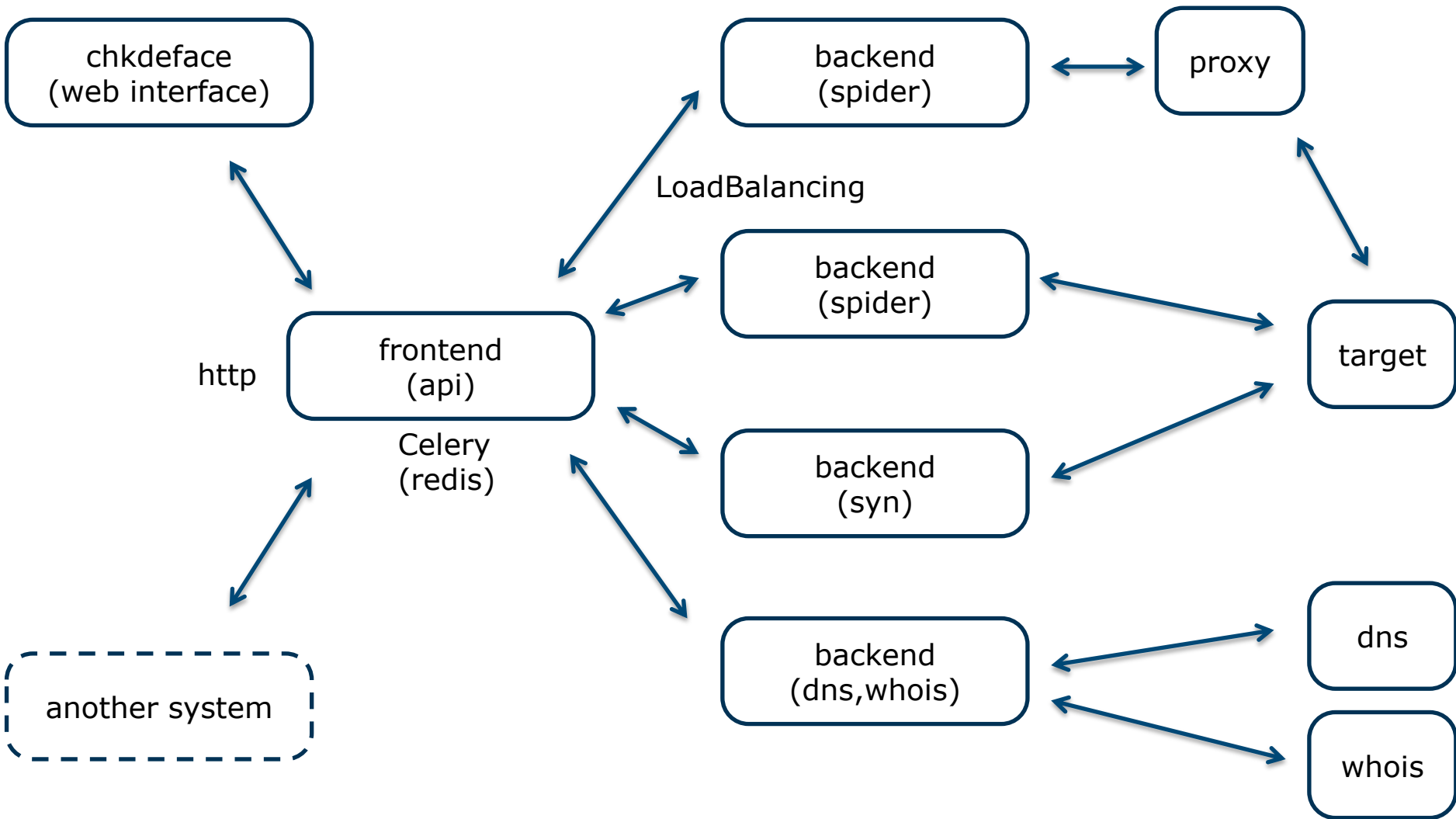
Improving efficiency by developing and using a tool

3. Using jsunpack-n, check if the signature matches with any existing signatures
 - Used a custom set of previously collected signatures

4. Record various data on the site
 - http_status
 - content_type
 - http_erver
 - wappalyzer

5. Record information on the website
 - IP address
 - WHOIS information (domain, IP address)

Structure



Main Modules

- Ghost.py
- Django
- Celery
 - redis
- jsunpack-n
 - Yara
- wappalyzer

Going Forward

- Would like to open source
 - Plan to put on github.com/JPCERTCC
- Using this system, would like to collaborate with domestic community on incident response
 - Would like to provide feedback on results at next year's FIRST Conference

APPENDIX

Screen Image (top page)

Chkdeface Search Syn Banner DNS Whois

User: kobayashi [log out](#)

New Query

Urls:

Proxy:

Referer:

User agent:

Post data:

Additional header:

Shared:

Stats

Query	1404
Job	2392
Page	1906
Resource	42063
Hostname	2343
Domain	1469
IP	3556
Hostname(Detail)	6723
Domain(Detail)	4649
IP(Detail)	6452

Search

Strings: Hidden: Item: Date from: Date to:

Query Detail Search

Page 1 of 281. [next](#)

id	created_date	url	registered_by	shared	category	period	counter
1407	2015年5月16日 14:11:01	http://bluearrows.org/1702	ir	None	-	0	0
1406	2015年5月16日 14:10:21	http://sbxp8nj9.douga-ya.net/image/s/wik.html	ir	None	-	0	0
1405	2015年5月16日 14:09:22	http://galcole.jp/optt.html	ir	None	-	0	0
1404	2015年5月15日 17:33:03	http://sockbuddy.com.au/wp-include/s/ID3/Sichern/Sie/Ihre/Online-Banking-Konto/sp	ir	None	-	0	0
1403	2015年5月15日 17:33:03	http://sockbuddy.com.au/wp-admin/css/colors/ocean/Sichern/Sie/Ihre/Online-Bankin	ir	None	-	0	0

Page Detail Search


Page 1 of 381. [next](#)

id	created_date	url	ip - country	status	capture
41959	2015年5月16日 14:21:52	https://www.first.org/conference/2015	166.78.29.118	200	
41958	2015年5月16日 14:20:48	https://www.first.org/conference/2015	166.78.29.118	200	
41912	2015年5月16日 14:20:31	https://www.first.org/conference/2015	166.78.29.118	200	
41911	2015年5月16日 14:18:57	https://www.first.org/conference/2015	166.78.29.118	200	
41881	2015年5月16日 14:11:15	http://bluearrows.org/1702	210.172.183.49	200	







Screen Image (Check in progress)

Chkdeface Search Syn Banner DNS Whois

User: kobayashi [log out](#)

Status: Loading 

Job			
id	date	url	status
2397	2015年5月16日 14:25:39	https://www.first.org/conference/2015	Completed
2398	2015年5月16日 14:25:09	https://www.first.org/conference/2015	Page Created
2399	2015年5月16日 14:25:34	https://www.first.org/conference/2015	Completed

Page			
page	ip	capture	
job_id 2397	166.78.29.118 		
url https://www.first.org/conference/2015			
status 200			
length 11855			
job_id 2398	166.78.29.118 		
url https://www.first.org/conference/2015			
status 200			
length 11456			
job_id 2399	166.78.29.118 		
url https://www.first.org/conference/2015			
status 200			
length 11855			

Screen Image (Check Result)

Query [previous](#) [next](#)

query_id 746
url https://www.first.org/conference/2015
created_date 2015年4月28日 12:53:23
modified_date 2015年4月28日 12:53:23
registered_by ir
tag

Status

Incident category:

Tracking interval:

Counter:
[set]

Shared:

Hidden:

Edit Tag

Job (Total:10)

Page 1 of 1.

id	date	status
2399	2015年5月16日 14:24:38	Completed
2398	2015年5月16日 14:24:38	Page Created
2397	2015年5月16日 14:24:38	Completed
2394	2015年5月16日 14:20:02	Completed
2393	2015年5月16日 14:20:02	Completed
2392	2015年5月16日	Completed

Page

[page](#) [source](#) [resource](#)



job_id 2399
page_id 42069
created_date 2015年5月16日 14:25:20
url https://www.first.org/conference/2015
domain first.org
hostname www.first.org
ipaddress 166.78.29.118 [sympa.first.org](#) [Rackspace Cloud Servers](#)
status 200
server nginx
content_type text/html
content_length 11855
content_file static/content/2015/05/16/www.first.org/1431753919/www.first.org/264c64c0105336ff97b954e4bcd5a2eb
content_md5 264c64c0105336ff97b954e4bcd5a2eb
content_ssdeep 192:cIAzQ/AeGt2NkdE4ivmZMLsP3bVBksVVITU6ry8vZHW:cf/roqfML83Rrrgu6ry8vZHW

Screen Image (Screenshot)

chkdeface Search Syn Banner DNS Whois User: kobayashi log out

NAVIGATE TO:

Facebook Twitter LinkedIn Email

FIRST
Improving Security Together

27th ANNUAL **FIRST BERLIN** CONFERENCE 14-19 JUNE 2015

Conference News

WED, 15 APR 2015
Germany's Federal Government Commissioner for Information Technology opens 27th Annual FIRST conference in Berlin (20:42 +0100)

WED, 18 MAR 2015
FIRST Welcomes Two New Gold Sponsors – NC4 and AIRBUS (16:58 +0100)
FIRST would like to welcome two new sponsors of the annual conference – NC4 and AIRBUS Defense & Space. Both organizations are joining the sponsorship team at the Gold level.

MON, 16 MAR 2015
Hotel Early Bird Rate Extended to Coincide with Registration Early Bird – April 10th (18:47 +0100)
We are happy to announce that the InterContinental Berlin has kindly extended the Early Bird hotel rate offer from April 1st to April 10th to coincide with our registration Early Bird offer. Please visit the Hotel Information page for more information and to book your lodging.

Tweets about "#firstcon15 OR @FIRSTdotOrg"

CONTACT US

id	date	status
2399	2015年5月16日 14:24:38	Completed
2398	2015年5月16日 14:24:38	Page Created
2397	2015年5月16日 14:24:38	Completed
2396	2015年5月16日 14:20:02	error: No Data from A
2395	2015年5月16日 14:20:02	error: No Data from A
2394	2015年5月16日 14:20:02	Completed

Screen Image (Source code)

Query [previous](#) [next](#)

query_id	746
url	https://www.first.org/conference/2015
created_date	2015年4月28日 12:53:23
modified_date	2015年4月28日 12:53:23
registered_by	ir
tag	

Status

Incident category:

Tracking interval:

Counter:
[set]

Shared:

Hidden:

Edit Tag

Job (Total:10)

Page 1 of 1.

id	date	status
2399	2015年5月16日 14:24:38	Completed
2398	2015年5月16日 14:24:38	Page Created
2397	2015年5月16日 14:24:38	Completed
2396	2015年5月16日 14:20:02	error: No Data from API
2395	2015年5月16日 14:20:02	error: No Data from API
2394	2015年5月16日	Completed

Page

[page](#) [source](#) [resource](#)

Header

```
Content-Encoding: gzip
Transfer-Encoding: chunked
Strict-Transport-Security: max-age=15768000
Server: nginx
5. Connection: keep-alive
Cache-Control: public, max-age=1800, s-maxage=1800
Date: Sat, 16 May 2015 05:24:49 GMT
Content-Type: text/html
```

Source

```
<!--?xml version="1.0" encoding="UTF-8"?--><!DOCTYPE html><html class=" js flexbox touch cssgradients video"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="title" content="FIRST.org / 27th Annual FIRST Conference">
<title>FIRST.org / 27th Annual FIRST Conference</title>
<meta name="viewport" content="initial-scale=1,maximum-scale=1.0,user-scalable=no"><link
rel="alternate" type="application/rss+xml" title="FIRST Annual Conference" href="/newsroom
/news/conference.xml"><link rel="stylesheet" type="text/css" media="screen" href="/_styles
/conf2015.css?20150515182531"></head>
<body class="index" data-twttr-rendered="true">
<header><div id="header"><div class="relative"><p id="first-logo"><a href="/"><span>FIRST</span>
</a></p><p id="socialmedia"><li class="facebook"><a href="http://facebook.com/firstcon"
target="_blank"><span>Facebook</span></a></li><li class="twitter"><a href="http://twitter.com
/firstdotorg" target="_blank"><span>Twitter</span></a></li><li class="linkedin"><a
href="http://linkedin.com/groups?gid=2585&amp;trk=myg_ugrp_ovr" target="_blank"><span>LinkedIn</span>
</a></li><li class="email"><a href="mailto:first-2015@first.org" target="_blank"><span>E-mail</span>
</a></li></ul></div></header>
<div class="lcol">
<h2 class="label gray light"><a href="/conference/2015">27th Annual FIRST Conference</a></h2>
<nav><div id="nav"><ul><li><a class="current ancestor" href="/conference/2015">Home</a></li><li><a
href="/conference/2015/about">The Conference</a></li><li><a href="/conference/2015/program">Conference
Overview</a></li><li><a href="/conference">Conference Archive</a></li></ul></li><li><a href="/conference
/2015/hotel">Hotel Information</a></li><li><a href="/conference/2015/registration">Registration</a>
<ul><li><a href="/conference/2015/registration">Registration Fees</a></li><li><a
href="https://registration.first.org/registration/2015/berlin">Register Today!</a></li><li><a
href="/conference/2015/terms-conditions">Terms &amp; Conditions</a></li></ul></li><li><a
href="/conference/2015/program">Program</a><ul><li><a href="/conference/2015/program">Conference
Program</a></li><li><a href="https://cfp.first.org/event/5/overview">Call for Speakers</a></li></ul>
</li><li><a href="/conference/2015/berlin">Berlin</a><ul><li><a href="/conference/2015/berlin">About
Berlin</a></li><li><a href="/conference/2015/traveling-to-berlin">Travelling to Berlin</a></li><li><a
href="/conference/2015/things-to-do">Things to Do</a></li><li><a href="/conference/2015/quick-
facts">Quick Facts</a></li></ul></li><li><a href="/conference/2015/sponsorship">Sponsorship</a>
```

Screen Image (List contents)

Chkdeface Search Syn Banner DNS Whois

User: kobayashi [log out](#)

Query [previous](#) [next](#)

query_id	746
url	https://www.first.org/conference/2015
created_date	2015年4月28日 12:53:23
modified_date	2015年4月28日 12:53:23
registered_by	ir
tag	

Status

Incident category:

Tracking interval:

Counter: [set]

Shared:

Hidden:

Edit Tag

Job (Total:10)

Page 1 of 1.

id	date	status
2399	2015年5月16日 14:24:38	Completed
2398	2015年5月16日 14:24:38	Page Created
2397	2015年5月16日 14:24:38	Completed
2396	2015年5月16日 14:20:02	error: No Data from API
2395	2015年5月16日 14:20:02	error: No Data from API
2394	2015年5月16日	Completed

Page

[page](#) [source](#) [resource](#)

Resource - Total: 45

id	url	ip - country	status	content_type	length
42069	https://www.first.org/conference/2015	166.78.29.118	200	text/html	11855
42070	https://www.first.org/conference/2015	166.78.29.118	200	text/html	9896
42071	https://www.first.org/_styles/conf2015.css?20150515182531	166.78.29.118	200	text/css	28359
42072	https://www.first.org/_images/conf2015/index-1.jpg	166.78.29.118	200	image/jpeg	41424
42073	https://www.first.org/_images/conf2015/index-3.jpg	166.78.29.118	200	image/jpeg	55635
42074	https://www.first.org/_scripts/conf2015.js?201403	166.78.29.118	200	application/x-javascript	116304
42075	https://www.first.org/_styles/type/open-sans-noblack.css	166.78.29.118	200	text/css	5153
42077	https://www.first.org/_images/conf2015/index-5.jpg	166.78.29.118	200	image/jpeg	41994
42078	https://www.first.org/_images/conf2015/index-2.jpg	166.78.29.118	200	image/jpeg	66829
42082	https://www.first.org/_images/conf2015/index-4.jpg	166.78.29.118	200	image/jpeg	76469
42083	https://platform.twitter.com/widgets.js	199.96.57.6	200	application/javascript; charset=utf-8	109039
42084	https://www.first.org/_images/conf2015/first-logo.png	166.78.29.118	200	image/png	5372
42085	https://www.first.org/_images/conf2015/menu-icon.png	166.78.29.118	200	image/png	961
42086	https://www.first.org/_images/conf2015/h3-bull	166.78.29.118	200	image/gif	1108

Screen Image (Search)

Query Search

Url:

Incident category:

Brand:

Tag:

Tracking interval:

Date from:
[clear]

Date to:
[clear]

Hidden:

Items per page:

Query total:1402

Page 1 of 281. [next](#)

<input type="checkbox"/>	id	created_date	url	group	shared	incident	period	counter	hidden
<input type="checkbox"/>	1407	2015年5月16日 14:11:01	http://bluearrows.org/1702	ir	None	-	0	0	False
<input type="checkbox"/>	1406	2015年5月16日 14:10:21	http://sbxp8nj9.douga-ya.net/images/wik.html	ir	None	-	0	0	False
<input type="checkbox"/>	1405	2015年5月16日 14:09:22	http://galcole.jp/opt.html	ir	None	-	0	0	False
<input type="checkbox"/>	1404	2015年5月15日 17:33:03	http://sockbuddy.com.au/wp-includes/D3/Sichern/Sie/Ihre/Online-Banking-Konto/sp	ir	None	-	0	0	False
<input type="checkbox"/>	1403	2015年5月15日 17:33:03	http://sockbuddy.com.au/wp-admin/css/colors/ocean/Sichern/Sie/Ihre/Online-Bankin	ir	None	-	0	0	False

Bulk Update

Incident category: Restrict: Hidden:

Screen Image (Search)

Page Search

Url:

Ip:

Ip org:

Country code:

Header:

Server:

Content payload:

Content md5:

Brand:

Domain whois:

Ip whois:

Wappalyzer:

Date from:

Date to:

Hidden:

Items per page:

Page total:1909

Page 1 of 382. [next](#)

id	query	created_date	url	ip	status	size	capture
42076	746	2015年5月16日 14:25:23	https://www.first.org/conference/2015	166.78.29.118 	200	11855	
42069	746	2015年5月16日 14:25:20	https://www.first.org/conference/2015	166.78.29.118 	200	11855	
42068	746	2015年5月16日 14:25:09	https://www.first.org/conference/2015	166.78.29.118 	200	11456	
41959	746	2015年5月16日 14:21:52	https://www.first.org/conference/2015	166.78.29.118 	200	11457	
41958	746	2015年5月16日 14:20:46	https://www.first.org/conference/2015	166.78.29.118 	200	11456	

Screen Image (Search)

[Search](#) [Query](#) [Page](#) [Resource](#)

Resource Search

Url:

Ip:

Ip org:


Country code:

Header:

Server:

Content payload:

Content md5:

Brand: 

Domain whois:

Ip whois:

Wappalyzer:

Date from:

[\[clear\]](#)

Date to:






[\[clear\]](#)

Hidden: 

Items per page: 

Resource total:42155

Page 1 of 8431. [next](#)

id	query	created_date	url	ip	status	size
42159	746	2015年5月16日 14:25:39	https://platform.twitter.com/embed/timeline.bb90bc33d9656b090e6a0f0247348a85.default.css	199.96.57.6 	200	38226
42158	746	2015年5月16日 14:25:39	https://www.first.org/_styles/type/OpenSans-Bo ld-webfont.ttf	166.78.29.118 	200	38452
42157	746	2015年5月16日 14:25:38	https://www.first.org/_styles/type/OpenSans-Se mibold-webfont.ttf	166.78.29.118 	200	39476
42156	746	2015年5月16日 14:25:38	https://www.first.org/_scripts/conf2015.js?2014 03	166.78.29.118 	200	149072
42155	746	2015年5月16日 14:25:38	https://www.first.org/_styles/type/OpenSans-Lig ht-webfont.ttf	166.78.29.118 	200	37336

Screen Image (WHOIS)

Chkdeface Search Syn Banner DNS Whois

User: kobayashi [log out](#)

Whois

Query:

Result

id	date	query	result
----	------	-------	--------

9194	2015年5月16日 14:25:22	166.78.29.118	
------	------------------------	---------------	--

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
5. # If you see inaccuracies in the results, please report at
# http://www.arin.net/public/whoisinaccuracy/index.xhtml
#
10. #
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=166.78.29.118?showDetails=true&showARIN=false&
showNonArinTopLevelNet=false&ext=netref2
#
15.
# start

NetRange: 166.78.0.0 - 166.78.255.255
CIDR: 166.78.0.0/16
20. NetName: RACKS-8-NET-11
NetHandle: NET-166-78-0-0-1
Parent: NET166 (NET-166-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS19994
25. Organization: Rackspace Hosting (RACKS-8)
RegDate: 2012-10-17
Updated: 2012-10-17
Ref: http://whois.arin.net/rest/net/NET-166-78-0-0-1

30.
OrgName: Rackspace Hosting
OrgId: RACKS-8
Address: 5000 Walzem Road
City: San Antonio
35. StateProv: TX
PostalCode: 78218
Country: US
RegDate: 2010-03-29
Updated: 2011-11-30
40. Ref: http://whois.arin.net/rest/org/RACKS-8
```

Screen Image (WHOIS)

Whois

Query:

Result

id	date	query	result
5622	2015年4月28日 12:53:33	first.org	<pre>Domain Name: FIRST.ORG Domain ID: D766817-LROR Creation Date: 1991-12-17T05:00:00Z Updated Date: 2014-09-03T20:20:49Z 5. Registry Expiry Date: 2015-12-16T05:00:00Z Sponsoring Registrar: Network Solutions, LLC (R63-LROR) Sponsoring Registrar IANA ID: 2 WHOIS Server: Referral URL: 10. Domain Status: clientTransferProhibited -- http://www.icann.org/epp#clientTransferProhibited Registrant ID: 31737549-NSI Registrant Name: FIRST.ORG, Inc. Registrant Organization: FIRST.ORG, Inc. Registrant Street: PO Box 1187 15. Registrant Street: 650 Castro Street, Suite 120 Registrant City: Morrisville Registrant State/Province: NC Registrant Postal Code: 27560-1187 Registrant Country: US 20. Registrant Phone: +1.5712476345 Registrant Phone Ext: Registrant Fax: +1.9999999999 Registrant Fax Ext: Registrant Email: first-sec@first.org 25. Admin ID: 43570176-NSI Admin Name: Nora Duhig Admin Organization: FIRST.org, Inc Admin Street: PO Box 1187 Admin City: Morrisville 30. Admin State/Province: NC Admin Postal Code: 27560-1187 Admin Country: US Admin Phone: +1.15712476345 Admin Phone Ext: 35. Admin Fax: +1.9999999999 Admin Fax Ext: Admin Email: first-sec@first.org Tech ID: 38705262-NSI Tech Name: FIRST Secretariat Tech Organization: FIRST.Org, Inc. Tech Street: PME 349 Tech Street: 650 Castro Street, Suite 120 Tech City: Mountain View Tech State/Province: CA</pre>

Screen Image (DNS)

Chkdeface Search Syn Banner DNS Whois

User: kobayashi [log out](#)

DNS Query

Query: Resolver:

Result

id	date	query	resolver	md5	result
8523	2015年5月16日 14:48:44	www.first.org	8.8.8.8	39bce2506847d8bedfd29d14f76045bd	<input type="text" value="www.first.org. 599 IN A 166.78.29.118"/>

History

Query: Resolver: Item: Date from: Date to:

Page 1 of 2. [next](#)

id	date	query	resolver	md5	result
8523	2015年5月16日 14:48:44	www.first.org	8.8.8.8	39bce2506847d8bedfd29d14f76045bd	<input type="text" value="www.first.org. 599 IN A 166.78.29.118"/>
8521	2015年5月16日 14:46:18	www.first.org	None	fd91a6515c483d57b558a50fa49d1b05	<input type="text" value="www.first.org. 600 IN A 166.78.29.118"/>
8519	2015年5月16日 14:25:21	www.first.org	None	487142f58618bd811e8a1af648da38ba	<input type="text" value="www.first.org. 188 IN A 166.78.29.118"/>
8516	2015年5月16日 14:21:50	www.first.org	None	087b044f6f18b2e3cd7901ef5a9bb42e	<input type="text" value="www.first.org. 398 IN A 166.78.29.118"/>
8512	2015年5月16日 14:18:55	www.first.org	None	f975fa139be39d46eb8422ecb00e14f9	<input type="text" value="www.first.org. 574 IN A 166.78.29.118"/>

Screen Image (syn)

Send Syn Packet

Src port:

Dst ip:

Dst port:

Timeout:

History

Strings: Hidden: Item: Date from: Date to:

Page 1 of 1.

id	date	src_port	dst_ip	dst_port	syn/ack	error_code	error_message
4	2015年4月23日 20:05:25	49802	210.148.223.7	25	False	11	接続がタイムアウトしました。
3	2015年4月23日 19:17:10	55845	210.148.223.7	80	True	0	
2	2015年4月21日 13:13:03	12684	210.148.223.7	80	True	0	
1	2015年4月21日 13:13:03	16132	210.148.223.7	80	True	0	