OARC 24 (Buenos Aires)

Report of Contributions

Contribution ID : **1** Type : **not specified**

Knot DNS Resolver

Friday, 1 April 2016 09:00 (30)

Knot DNS Resolver is a new CZ.NIC project that builds a fully DNSSEC-validating DNS resolver. But it's more it's a powerful platform for building resolver service due its extensibility via modules and configuration in Lua.

Summary

Primary author(s) : Mr. SURY, Ondrej (CZ.NIC)

Presenter(s) : Mr. SURY, Ondrej (CZ.NIC)

Session Classification : Public Workshop: Tools & Measurements

Track Classification : Public Workshop

Contribution ID : **2** Type : **not specified**

State of the ”DNS privacy” project: running code

Thursday, 31 March 2016 16:00 (30)

The “DNS privacy” project started at the IETF meeting in Vancouver a few months after the Snowden revelations. What is its current state? A problem statement has been published, RFC 7626. Two directions are followed: QNAME minimisation, to decrease the amount of data sent to the name servers. And encryption, to prevent a sniffer to get the data.

This talk will present the state of standardisation (it is possible that all the RFC are published before the meeting) and will demo the running code: QNAME minimisation in Unbound and Knot, and how does it work with broken name servers (such as those sending NXDOMAIN for an ENT), and DNS over TLS.

Summary

Primary author(s) : Mr. BORTZMEYER, Stéphane (AFNIC)

Presenter(s) : Mr. BORTZMEYER, Stéphane (AFNIC)

Session Classification : Public Workshop: Privacy

Track Classification : Public Workshop

Contribution ID : **3** Type : **not specified**

Rolling the Root Key

Friday, 1 April 2016 16:00 (30)

This is a report of one member's perspectives on the work of the Root Key Roll Design Team, looking at the various operational tradeoffs that were involved in preparing the plan to roll the root key. I would also like to make some comments on the state of standards and implementations of resolvers and the lack of clear standard specifications about how to signal a key roll. Where possible I will illustrate the considerations with measurement data about the behaviour of resolvers that query authoritative name servers.

Summary

report on the Root Key Roll Design Team study.

Primary author(s) : Mr. HUSTON, Geoff (APNIC)

Presenter(s) : Mr. HUSTON, Geoff (APNIC)

Session Classification : Public Workshop: DNSSEC Algorithm Rollover

Track Classification : Public Workshop

Contribution ID : **4** Type : **not specified**

ECDSA - Reviewed

Friday, 1 April 2016 14:50 (15)

This is intended to be an update to an earlier presentation on the extent to which DNS resolvers are able to performance validation on ECDSA-signed data

Summary

Update on ECDA support

Primary author(s) : Mr. HUSTON, Geoff (APNIC)

Presenter(s) : Mr. HUSTON, Geoff (APNIC)

Session Classification : Public Workshop

Track Classification : Lightning Presentations

Contribution ID : **5** Type : **not specified**

DNS Secondary service for customers, evolution and ”meta-slave”

Friday, 1 April 2016 14:30 (20)

NIC Chile, .CL ccTLD registry, started to offer a secondary name service to its customers as a way to improve the overall internet robustness in Chile more than 10 years ago. We are going to show the evolution of a free of charge service from an unicast ip server to an anycast cloud, and using a sort of “meta-slave” daemon for provisioning the nodes.

Summary

Primary author(s) : Mr. MARCO, Diaz (NIC Chile)

Presenter(s) : Mr. MARCO, Diaz (NIC Chile)

Session Classification : Public Workshop

Track Classification : Public Workshop

Contribution ID : **6** Type : **not specified**

Multi-vantage point DNS Diagnostics and Measurement

Friday, 1 April 2016 10:00 (30)

The ability to measure network and server behaviors from different network vantage points is important for understanding the general health of a network ecosystem. There are various platforms, frameworks, and APIs designed and built to accommodate this need. In this talk we discuss a new DNS looking glass framework designed for low-overhead deployment and great flexibility, and available for use with the DNSViz measurement tool. Recursive and authoritative inspection are both supported, via direct, client-based, or HTTP-proxy-based looking glass perspectives.

Summary

Primary author(s) : Dr. DECCIO, Casey (Verisign Labs)

Presenter(s) : Dr. DECCIO, Casey (Verisign Labs)

Session Classification : Public Workshop: Tools & Measurements

Track Classification : Public Workshop

Contribution ID : **7** Type : **not specified**

Review and analysis of attack traffic against A-root and J-root on November 30 and December 1, 2015

Friday, 1 April 2016 11:00 (30)

On November 30 and December 1, 2015, some of the Internet's Domain Name System (DNS) root name servers received large amounts of anomalous traffic. The twelve root operators jointly published a report of the incident (http://www.root-servers.org/news/events-of-20151130.txt). The event also generated spirited discussion and speculation on public mailing lists, website forums, and blog postings.

This presentation will specifically cover Verisign's observations and analysis of the attack in operating both A-root and J-root. Topics to be discussed include:

- A recap of the attack, including an exact timeline of the event along with some specifics of the traffic itself.
- A brief discussion about any perceivable impact on A-root and J-root, and the root as a whole.
- Actions taken before, during, and after the attack. What worked well? What could of been done better?
- A video that visualizes the attack as a Hilbert Curve representation. This analysis clearly suggests that the source addresses were spoofed.
- Assumptions regarding the purpose of the attack (Hint: the attacker was not specifically targeting the root servers)

Summary

Primary author(s) : WESSELS, Duane (Verisign); Mr. WEINBERG, Matt (Verisign)

Presenter(s) : WESSELS, Duane (Verisign); Mr. WEINBERG, Matt (Verisign)

Session Classification : Public Workshop: Research

Track Classification : Public Workshop

Contribution ID : **9** Type : **not specified**

AAAA Deep Dive: DNS Resolution Anomalies and Performance across a Huge Data Set

Thursday, 31 March 2016 13:30 (30)

Much has been written about IPv6 adoption and its performance. One thing that has not been explored is how IPv6 DNS resolution contributes to overall user experience. What impact does transport, authoritative server configuration and other factors have on the "long tail" of domains queried over IPv6? This talk will present experimental results using a data set of approximately 35 million unique names and query types, extracted from production resolvers around the world. This data will feed dnsperf, a widely used utility for evaluating DNS performance, to query resolvers set up in the following ways: IPv4 only, IPv6 only, & prefer IPv6, all with EDNS0 on by default, along with a control server with EDNS0 off. Differences in resolution performance will be evaluated and presented for each of the resolvers.

Summary

Primary author(s) : Mr. WEBER, Ralf (Nominum Inc)

Presenter(s) : Mr. WEBER, Ralf (Nominum Inc)

Session Classification : Public Workshop: Data Analysis

Track Classification : Public Workshop

Contribution ID : **12** Type : **not specified**

Deckard – Integration Testing of DNS Servers

Friday, 1 April 2016 14:00 (30)

A generic testing framework was produced as a part of developing the Knot Resolver. This framework is written in python and can use UNIX domain sockets to bypass the underlying physical network and fake time using libfaketime. Apart from short introduction I will show the audience some real-life scenarios for testing the recursive and authoritative DNS servers and how to integrate Deckard into your own testing platform - this is important both for vendors and for people deploying new versions of servers into production.

Summary

Primary author(s) : Mr. SURY, Ondrej (CZ.NIC)

Presenter(s) : Mr. SURY, Ondrej (CZ.NIC)

Session Classification : Public Workshop

Track Classification : Public Workshop

Contribution ID : **14** Type : **not specified**

Increasing the Root Zone ZSK Size

Friday, 1 April 2016 12:00 (30)

Verisign, in its role as Root Zone Maintainer, plans to increase the size of the root zone Zone Signing Key (ZSK) in 2016. The ZSK has been a 1024-bit RSASHA256 key since the initial deployment of DNSSEC to the root zone in 2010. In the latter half of 2016, the ZSK size will be increased to 2048-bits.

In this presentation we will outline the schedule for the change, describe various technical and non-technical details for implementing the change, describe how the change will affect root zone response sizes, and our plans for emergency fallback to a 1024-bit in the unlikely event it should be necessary.

Summary

Primary author(s) : WESSELS, Duane (Verisign)

Presenter(s) : WESSELS, Duane (Verisign)

Session Classification : Public Workshop: Research

Track Classification : Public Workshop

Contribution ID : **16** Type : **not specified**

QNAME minimisation in Unbound

Thursday, 31 March 2016 16:30 (30)

Data stored in the DNS is publicly visible. DNS transactions, on the other hand, contain privacy sensitive information. The Snowden revelations about pervasive monitoring are seen as a wake up call for the internet community to increase the focus on privacy protection. One of the privacy threat mitigation methods mentioned in RFC6973, is the principle of data minimisation[0]. The RFC states that: “Reducing the amount of data exchanged reduces the amount of data that can be misused or leaked.”.

One of the new features in Unbound 1.5.7 is the support of QNAME minimisation1. QNAME minimisation is a technique to improve DNS privacy by limiting the amount of privacy sensitive data exposed to authoritative nameservers. This is done by limiting the number of labels in the QNAME sent to nameservers and by setting the QTYPE to NS in order to hide the original QTYPE where possible.

Although the proposed minimisation of the QNAME and using the NS QTYPE are not strictly forbidden in the original DNS RFC, not all nameservers handle these queries the way they should. Common wrong responses are NXDOMAIN on empty-non-terminals and refusing queries with QTYPE=NS. Resolving when using QNAME minimisation will fail on these broken nameservers. We suspect that operators will not adopt QNAME minimisation when it is implemented according to the specification. Unbound is shipped with an implementation that will resolve queries “as usual” when broken nameservers are detected.

QNAME minimisation can increase the number of queries sent to nameservers. This is most notable when resolving in the ip6.arpa name space. To limit the number of queries for reverse IPv6 lookups, unbound increments the minimised QNAME with 8 labels on each iteration when the original QNAME is a subdomain of ip6.arpa.

An uncovered topic in the specification is QNAME minimisation and forwarders. Because of the “best effort” approach, there is no privacy enhancement when minimising queries to forwarders. Unbound does not minimise queries sent to forwarders.

The most important reason to enable QNAME minimisation is the improved privacy. There are, however, some other benefits. One of them is that querying all intermediate domain names will result in a more precise negative cache. This improves both performance and privacy. Although using a completely different technique, QNAME minimisation can lead to the same result as described in draft-wkumari-dnsop-cheese-shop-00[2]. Namely reducing the amount of traffic to the root servers.

[0] - https://tools.ietf.org/html/rfc6973#section-6.1

1 - https://tools.ietf.org/html/draft-ietf-dnsop-qname-minimisation-09.

[2] - https://tools.ietf.org/html/draft-wkumari-dnsop-cheese-shop-00

Summary

Primary author(s) : DOLMANS, Ralph (NLnet Labs)

Presenter(s) : DOLMANS, Ralph (NLnet Labs)

Session Classification : Public Workshop: Privacy

Track Classification : Public Workshop

Contribution ID : **17** Type : **not specified**

Real-Time Analytics of DNS packets

Thursday, 31 March 2016 11:30 (30)

In OARC 22 (Amsterdam) we gave a lightning talk about the possibilities and prospects of using Apache Storm for real-time analytics of DNS packets.

Now, after a year of work, we are glad to present RaTA-DNS, our modular system for realtime analytics. RaTA-DNS was designed as a set of self-contained modules aiming to an easy integration with existing systems such as DSC and Hedgehog, and new systems such as SIDN Lab's ENTRADA.

The main components of our system are three: Fievel, a packet monitor responsible for capturing network traffic and perform a preliminary processing (for reducing the data rate in order to be transmitted to aggregators); Gopher, which is responsible for aggregate the captured data received from multiple servers (Gopher was developed in Go language instead using the Apache Storm framework for modularity reasons); and Remy, the dashboard (data visualisations), which is connected to several Gopher modules to provide real time displays.

The idea is to provide a programmable framework for real-time monitoring of DNS. Thus, Fievel has been developed as a scriptable module, where preprocessing is programmable and adaptable to the needs of different users, producing a monitoring system fully customisable.

Additionally, as Fievel provides the tcp-replay function and Remy the play-pause-rewind functions, RaTA-DNS can be also seen as a very useful tool for forensic analysis of DNS traces.
Actually, RaTA-DNS is connected to 2 NIC Chile DNS servers, processing in a normal operations day around 1200 (queries-responses)/sec per server, and aggregating statistical information such as queries/sec, non-rfc-conformant queries (queries using underscores), top-K queries by source, destiny, and geolocation. Further information can be seen in http://ratadns.niclabs.cl

Summary

Primary author(s) : Dr. BUSTOS-JIMÉNEZ, Javier (NIC Chile Research Labs (NICLabs). Universidad de Chile)

Co-author(s) : Mr. CIFUENTES, Francisco (NIC Chile Research Labs)

Presenter(s) : Dr. BUSTOS-JIMÉNEZ, Javier (NIC Chile Research Labs (NICLabs). Universidad de Chile)

Session Classification : Public Workshop: First Session

Track Classification : Public Workshop

Contribution ID : **18** Type : **not specified**

Threshold-Cryptography Distributed HSM

Friday, 1 April 2016 09:30 (30)

In the 20th DNS-OARC workshop, we showed a virtual HSM based on threshold cryptography. This system has the purpose to be used with OpenDNSSEC in order to provide a low cost solution to DNS record signing automation. But that system had a single point of failure: the key manager. Single points of failure are undesirable, even more in a fault tolerant distributed system. After a reengineering during the last year, we solved this problem by implementing the whole protocol within the PKCS #11 API. The communication now is done directly between the application that uses the system and the nodes, without the need of any centralised subsystem. This reengineering not only help us to have a really fault tolerant system but to improve the performance by reducing the latency of the operations.

In this presentation, we will walk through the main features of the system, how simple is to integrate it with currently working systems, and how the system might help to improve the number of deployed DNSSEC systems when a secure low-cost cryptographic solution is needed.

Summary

Primary author(s) : Mr. CIFUENTES, Francisco (NIC Chile Research Labs)

Co-author(s) : Dr. HEVIA, Alejandro (Computer Science Department (DCC), Universidad de Chile); Dr. BUSTOS-JIMÉNEZ, Javier (NIC Chile Research Labs (NICLabs). Universidad de Chile)

Presenter(s) : Mr. CIFUENTES, Francisco (NIC Chile Research Labs)

Session Classification : Public Workshop: Tools & Measurements

Track Classification : Public Workshop

Contribution ID : **19** Type : **not specified**

How we are developing a next generation DNS API for applications

Thursday, 31 March 2016 11:00 (30)

Many new and developing DNS features have emerged in recent years to improve both the security and privacy of DNS (e.g. DNSSEC/DANE and DNS-over-TCP/TLS). A major reason for the lack of uptake and deployment of these features by applications is that existing DNS APIs either do not support the features or do not provide an application friendly interface. To solve this problem the getdns API was developed with the main goals of:

- Ease of use by application developers across a variety of languages
- DNS capabilities that most application developers might want now or in the next few years

We present an implementation of the getdns API (verging on production release) and discuss how it has evolved through close involvement with application developers and standards developments. This collaborative development model has also helped to identify practical and implementation specific roadblocks to real-world deployment particularly for DANE and DNSSEC. As a result the API has been refined and the implementation provides easy access to DNS data both directly in C and via a range of bindings including Python, nodejs and Java.

Participation by the development team in multiple international hackathons has also demonstrated how the API enables rapid development of prototype implementations (including many DNS privacy related IETF drafts) with getdns proving a powerful research tool in these areas.

Integration of getdns into operating systems is also discussed, as it the fact that by enabling new DNS features for client applications the API will create demand for upstream services which is of consideration to operators.

Summary

Primary author(s) : DICKINSON, Sara (Sinodun IT)

Co-author(s) : Mr. TOOROP, Willem (NLnet Labs)

Presenter(s) : DICKINSON, Sara (Sinodun IT); Mr. TOOROP, Willem (NLnet Labs)

Session Classification : Public Workshop: First Session

Track Classification : Public Workshop

Contribution ID : **25** Type : **not specified**

Testing Most Authoritative Servers for Conformance

Thursday, 31 March 2016 15:30 (30)

ICANN has recently begun testing live authoritative servers for conformance to the DNS protocols, particularly for TCP and EDNS(0) compliance. We do this by collecting registered names from the zone files of all gTLDs, as well as a representative sampling of names registered in the ccTLDs. This paper shows the test methodology, the levels of compliance found, and suggests avenues for further testing.

Summary

Earlier research has tested DNS conformance on small samples of authoritative servers. In order to assess how well earlier research matches the real world, we have mapped all names registered in gTLDs to their authoritative nameservers in order to have one or more names that can be queried in our tests. In addition, we use a few non-invasive techniques to estimate how many names registered in ccTLDs are associated with nameservers not in the gTLD data. We then run representative tests, give results, and ask for suggestions about further tests that might be valuable to the DNS operations community in deciding which features of the DNS are reliably implemented.

Primary author(s) : HOFFMAN, Paul (ICANN)

Presenter(s) : HOFFMAN, Paul (ICANN)

Session Classification : Public Workshop: Privacy

Contribution ID : **26** Type : **not specified**

ENTRADA: The Impact of a TTL Change at the TLD-level

Thursday, 31 March 2016 14:00 (30)

SIDN, the registry for the .nl ccTLD, managing 5,6 million .nl domain names, has recently made significant changes to its zone file publication policy:

- A new zone file is now available every hour, instead of every 2 hours.
- The delegation TTL value has been decreased to match the new publishing interval.
- The SOA minimum TTL value has been decreased from 900 to 600 seconds.

We used ENTRADA to analyse the impact of these changes on:

- Overall DNS traffic
- Specific query types
- Specific domain name types (popular, unpopular, nxdomain)

This presentation will show the results of this work.
We are also pleased to announce that ENTRADA is now available as open source project.

ENTRADA

ENTRADA (ENhanced Top-level Domain Resilience through Advanced Data Analysis) is a DNS big data platform built on top of Hadoop, we use it at SIDN Labs for analysing over 100 billion DNS queries. Each day ~400 million new queries are added.

Summary

Primary author(s) : Mr. WULLINK, M (SIDN)

Presenter(s) : Mr. WULLINK, M (SIDN)

Session Classification : Public Workshop: Data Analysis

Track Classification : Public Workshop

Contribution ID : **27** Type : **not specified**

The Quest for the Missing Keytags

Friday, 1 April 2016 11:30 (30)

In an effort to create all possible 64K keytags for a DNSSEC signing key, an anomaly surfaced that caused 75% of the possible keytags to never appear.

This effort to generate certain cryptographic keys became an adventure in itself that included beautiful discrete math, flawed functions, carefully crafted primes, multiple cryptographic libraries, and some brilliant people.

The result of this effort shows that using an ancient checksum function to identify cryptographic keys is not optimal.

Summary

The presentation will go through the quest of uncovering the anomaly that caused the limitation in keytags generation.

Primary author(s) : ARENDS, Roy (ICANN)

Presenter(s) : ARENDS, Roy (ICANN)

Session Classification : Public Workshop: Research

Track Classification : Public Workshop

Contribution ID : **28** Type : **not specified**

Continuous Data-driven Analysis of Root Server System Stability

Thursday, 31 March 2016 14:30 (30)

At the end of 2015 the Continuous Data-driven Analysis of Root Server System Stability (CDAR)1 study was started by the consortium partners NLnet Labs, SIDN and TNO. The objective of the CDAR study is to analyze the technical impact of the introduction of New gTLDs in the root zone on the stability and security of the root server system.

With this in mind, we engaged in the collection and analyses of a large variety of measurement data sets (RIPE Atlas measurements, RIPE DNSMON, RSSAC002, DITL, and others). The projects aims at answering the question if the growth on the root zone files impact, in any measurable way, the operational stability of the root DNS system.

In this presentation, the CDAR team will discuss with the community our first results on the analysis of the measurement data, as well the data collection and analysis methods used to observe the technical impact of New gTLD program. In specific, we will present a (i) characterization of the Root DNS traffic, an (ii) analysis of RSSAC002 data and TLD domain statistic to describe the impact of new gTLDs, and (iii) the impact of fluctuations in the query rates at the Root on DNS stability. (For the latter, we can use data of the late root DDoS attacks [2] and analyse the combined data of RIPE Atlas, DNSSMON and RSSAC002 data.)

A second type of assessments focusses on the correctness of DNS data and its impact on the Root stability and security. Results will be presented from continuous, valid/broken DNSSEC chain validations between the Root and (New g)TLDs, amongst others.

By sharing the current CDAR results we contribute to building on previous results from the DNS-OARC community and we enable the community to reflect on the study results.

1 http://cdar.nl
[2] http://root-servers.org/news/events-of-20151130.txt

Summary

Primary author(s) : Mr. GIJSEN, Bart (TNO)

Presenter(s) : Mr. GIJSEN, Bart (TNO)

Session Classification : Public Workshop: Data Analysis

Track Classification : Public Workshop

Contribution ID : **30** Type : **not specified**

Algorithm roll-over experiences

Friday, 1 April 2016 16:30 (30)

Algorithm roll-overs are part of any security system, because older algorithms lose their strength, and stronger and newer algorithms come along. At the RIPE NCC we recently rolled our algorithm from SHA1 and to SHA256. We had some interesting issues, and I'd like to talk about them, especially as more people may want to consider rolling their algorithms now.

Amongst these issues were things like software support, testing, planning of the roll-over and timing issues.

Summary

The RIPE NCC's experiences with rolling DNSSEC signature algorithm from SHA1 to SHA256.

Primary author(s) : BUDDHDEV, Anand (RIPE NCC)

Presenter(s) : BUDDHDEV, Anand (RIPE NCC)

Session Classification : Public Workshop: DNSSEC Algorithm Rollover

Track Classification : Lightning Presentations

Contribution ID : **31** Type : **not specified**

Recent DDoS attacks against RIPE NCC's DNS servers

Thursday, 31 March 2016 10:35 (15)

In the last several weeks, the RIPE NCC's DNS infrastructure has experienced some DDoS events. In this presentation, I would like to talk about what we experienced, and how we tried to mitigate the attacks. I will talk about the nature of the attacks, and specifically what kind of methods and tools we used to try and defence our infrastructure.

Summary

A talk about the recent DDoS attacks against RIPE NCC DNS servers, and how we defended against them.

Primary author(s) : BUDDHDEV, Anand (RIPE NCC)

Presenter(s) : BUDDHDEV, Anand (RIPE NCC)

Session Classification : Members Session

Track Classification : Member Business

Contribution ID : **32** Type : **not specified**

Panel: DNSSEC algorithm flexibility

Friday, 1 April 2016 17:00 (45)

This is a proposal to have a discussion panel with DNS vendors (ISC, NlNetLabs, PowerDNS, CZ.NIC, Nominum,
Microsoft) and people from operating systems and Linux distros (Microsoft, Debian, Ubuntu, RedHat, SuSE) to come and discuss challenges of introducing new and deprecating old DNS(SEC) algorithms.

The proposed moderators are Dan York and Olaf Kolkman as neutral moderators. Also invited to participate are large scale DNS resolver like Google DNS, and reaching for other operators as well.

The initial ideas to discuss are:

1. The life cycles of upstream (DNS vendors);
2. The life cycle of downstream (linux distros' releases, windows releases, etc.);
3. Experiences with customers' deployments, etc.
4. Other ideas

We are expecting a 45 to 60 minute slot to have enough time for discussion.

Summary

Primary author(s) : Mr. SURY, Ondrej (CZ.NIC)

Presenter(s) : Dr. OVEREINDER, Benno (NLnet Labs); YORK, Dan (Internet Society); HUNT, Evan (ISC); VČELÁK, Jan (CZ.NIC); Mr. SURY, Ondrej (CZ.NIC); WOUTERS, Paul (Redhat); Mr. WEBER, Ralf (Nominum Inc)

Session Classification : Public Workshop: DNSSEC Algorithm Rollover

Track Classification : Public Workshop

Contribution ID : **33** Type : **not specified**

OARC Status Update

Thursday, 31 March 2016 10:10 (25)

It has been another busy 6 months for the OARC Team. In particular, we're well down the path of executing a plan which will re-locate our primary infrastructure hosting site to multiple new locations. We also have a new staff member recently joined as Software Engineer, and are gearing up for our DITL2016 data gathering exercise shortly after the workshop.

This presentation will update OARC Members and the audience on these developments and OARC's 2016 budget and fees.

Summary

Presenter(s) : Mr. MITCHELL, Keith (DNS-OARC)

Session Classification : Members Session

Contribution ID : **34** Type : **not specified**

Welcoming Remarks

Thursday, 31 March 2016 10:00 (10)

Summary

Presenter(s) : Mr. FILIP, Ondrej (CZ.NIC)

Session Classification : Members Session

Contribution ID : **35** Type : **not specified**

PGP Signing Session

Summary

Primary author(s) : Mr. SURY, Ondrej (CZ.NIC)

Presenter(s) : Mr. SURY, Ondrej (CZ.NIC)

Contribution ID : **36** Type : **not specified**

DNS-Stats Collector Project

Friday, 1 April 2016 15:15 (5)

Summary

Presenter(s) : DICKINSON, Sara (Sinodun IT)

Session Classification : Public Workshop: Lightning Talks

Contribution ID : **37** Type : **not specified**

RIPE Atlas and DNS

Friday, 1 April 2016 15:25 (5)

Summary

Presenter(s) : Mr. BORTZMEYER, Stéphane (AFNIC)

Session Classification : Public Workshop: Lightning Talks

Contribution ID : **38** Type : **not specified**

EDNS Compliance

Friday, 1 April 2016 15:20 (5)

Summary

Presenter(s) : Mr. ANDREWS, Mark (ISC)

Session Classification : Public Workshop: Lightning Talks

Contribution ID : **39** Type : **not specified**

Zombies

Friday, 1 April 2016 15:10 (5)

Summary

Presenter(s) : Mr. HUSTON, Geoff (APNIC)

Session Classification : Public Workshop: Lightning Talks

Contribution ID : **40** Type : **not specified**

COM/Net Anycast Changes

Friday, 1 April 2016 15:25 (5)

Summary

Presenter(s) : Mr. WEINBERG, Matt (Verisign)

Session Classification : Public Workshop: Lightning Talks