DNSCRYPT

BRIAN HARTVIGSEN

CISCO / OPENDNS

DNSCURVE

JUNE 2009 BY DJB

DNSCURVE USES HIGH-SPEED HIGH-SECURITY ELLIPTIC-CURVE CRYPTOGRAPHY TO DRASTICALLY IMPROVE EVERY DIMENSION OF DNS SECURITY...

OPENDNS ADOPTS DNSCURVE

JULY 31, 2009

MATTHEW DEMPSKY AKA MDEMPSKY

E733205

FOREVER ALONE

OPENDNS DISABLED DNSCURVE SUPPORT

JUNE 21, 2017

ONLY BEING USED BY CR.YP.TO AND NAMESERVERS STOPPED RESPONDING TO ENCRYPTED QUERIES

DNSCURVE FORWARDER

```
<dnscrypt-query> ::= <client-magic> <client-pk> <client-nonce> <encrypted-query>
...
<encrypted-query> ::= AE(<shared-key> <client-nonce> <client-nonce-pad>,
<client-query> <client-query-pad>)
```

X25519-XSALSA20POLY1305 OR X25519-XCHACHA20POLY1305

FIRST CODE COMMIT

OCT 19, 2011

FRANK DENIS AKA JEDISCT1

17D8DD0

FIRST PUBLIC RELEASE

DECEMBER 6, 2011

DNSCRYPT-PROXY BINARY ONLY
UI FOR OSX, WINDOWS, LINUX COME LATER

FIRST ENCRYPTION IS NOT ENOUGH RESPONSE

DECEMBER 8, 2011

BEN APRIL, TREND MICRO
HTTPS://BLOG.TRENDMICRO.COM/TRENDLABS-SECURITY-INTELLIGENCE/DNSCRYPT-NOT-FUNDAMENTAL-ENOUGH/

DNSCRYPT-WRAPPER

NOVEMBER 25, 2012

INTERMEDIARY BETWEEN CLIENT AND RESOLVER TO ADD DNSCRYPT CAPABILITIES

OPENDNS ROAMING CLIENT

DECEMBER 14, 2012

OFF-NETWORK PROTECTION FOR ROAMING/REMOTE USERS

OPENDNS VIRTUAL APPLIANCE

APRIL 22, 2015

ACTIVE DIRECTORY INTEGRATION

DNSCRYPT SPECIFICATION VERSION 2

JULY 25, 2015

UPDATES INCLUDE

DNSDIST SUPPORTS DNSCRYPT

DECEMBER 21, 2015

V1.1.0

YANDEX SUPPORTS DNSCRYPT

MARCH 29, 2016

SUPPORTED IN THEIR BROWSER

INTEGRATED DNSCRYPT IN ANYCONNECT

JULY 8, 2016

REPLACING MUCH OF THE ROAMING CLIENT BASE, SAME USE CASE

UNBOUND SUPPORTS DNSCRYPT

MARCH 20, 2017

V1.9.1

CISCO SECURITY CONNECTOR

SEP 20, 2017

DNSCRYPT ON IOS

QUAD9 SUPPORTS DNSCRYPT

DECEMBER 2018

LATEST BIG PROVIDER

WHERE ARE WE?

40 PROVIDERS

- YANDEX
- OPENNIC
- QUAD9
- SECUREDNS
- ADGUARD
- CLEANBROWSING
- SCALEWAY
- DNSCRYPT.(NL|EU|ORG|UK|ME|CA)

>3M OPENDNS ENDPOINTS

~15% OPENDNS TRAFFIC

WHAT ABOUT DOT/DOH?

COUGH**DNSSEC**COUGH

QUESTIONS?