Proyecto Quad9

uso del DNS para proteger sin monetizar los datos

ESNOG21
Barcelona, 9-10 Abril 2018

Gael Hernandez
Interconnection Policy, PCH
gael@pch.net

AGENDA

- El sistema DNS, el rol de los resolvers recursivos y las debilidades del modelo actual
- El proyecto Quad9: motivación, funcionalidades del sistema y modelo de colaboración IBM & GCA & PCH
- Arquitectura del sistema Quad9
- Progreso del proyecto y lineas de trabajo actuales
- Q&A

QUE ES EL DNS?

- DNS es el Sistema de Nombres de Dominio - la manera en la que maquinas (“hostnames”), como por ejemplo “www.example.com”, están enlazadas con una dirección IP, servicios de email, y otros registros mas profundos que permiten comunicación machine-to-machine (M2M).
- DNS no solo se utiliza para localizar estos mapeos, sino también para validar que son correctos y genuinos (“DNSSEC”)
- DNS es casi siempre el primer paso en el establecimiento de conexiones a sistemas remotos, independientemente de si son creíbles o maliciosos.

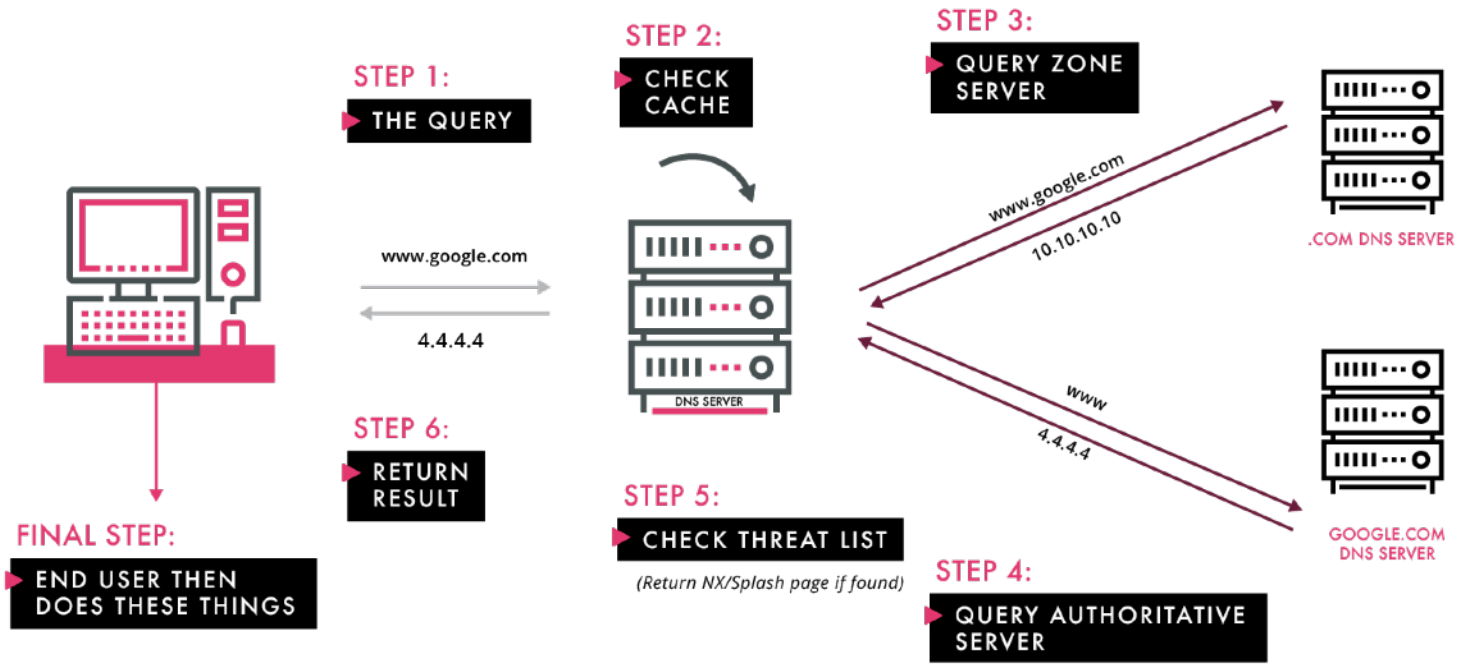
QUE ES UN RESOLVER RECURSIVO DNS?

- Ordenadores, dispositivos movies y dispositivos IoT tienen configurados un servidor DNS recursivo. Estos servidores hacen búsquedas de DNS en tu nombre, pero generalmente con pocas pautas de seguridad o privacidad en torno a su operación.
- Los resolvers recursivos solo saben como consultar resolvers autoritativos u otros resolvers recursivos - en realidad no tienen ninguna respuesta sobre el mapeo de nombre a servicio por si mismos.
- Tu resolver recursivo es normalmente el gateway/firewall/router en la oficina, o el que te proporciona tu ISP.
- La configuration del resolver recursivo se hace típicamente via DHCP, pero se puede hacer manualmente.

WHAT IS Quad9?

- Quad9 es un servicio de DNS recursivo:
  - una block-list integrado de maquinas maliciosas
  - con un diseño de alto rendimiento y baja latencia
  - preserva la privacidad y evita cualquier monetización de los datos (conforme con la regulación GDPR)
  - redundancia anycast
  - posibilidad de integrarse con cualquier dispositivo de red que use la familia de estándares DNS
  - sin coste, contratos, o contacto con una empresa de venta

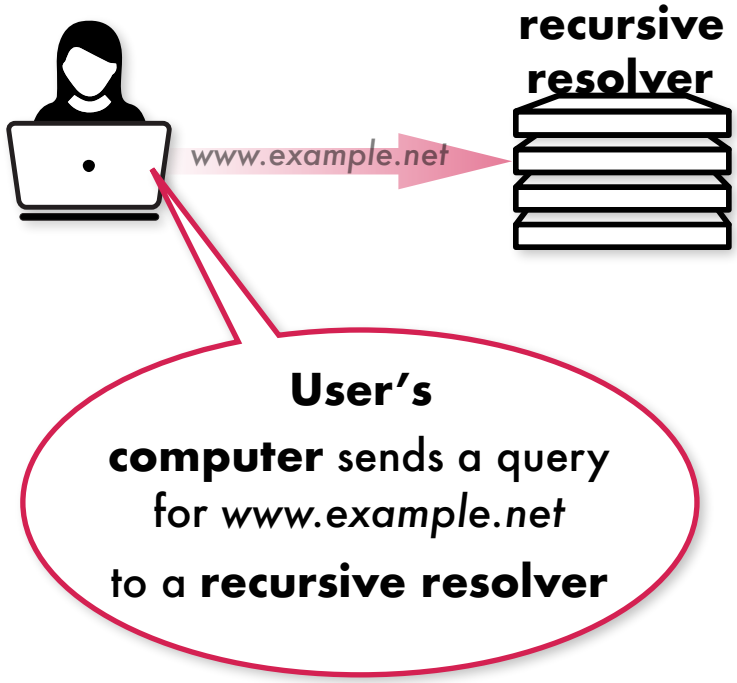
Quad9: A DNS Public Recursive Resolver



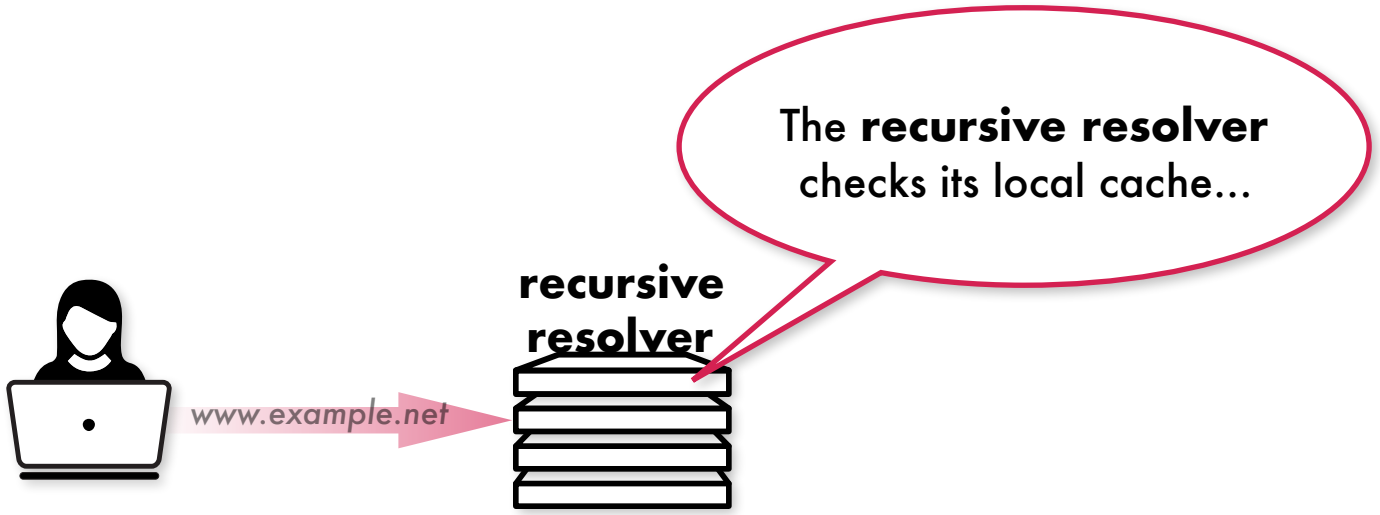
- Global open recursive DNS platform
- Populated by data crowd-sourced from the security industry
- Strong privacy controls built in (not even we know the source of requests)
- Core/root DNS level reliability on infrastructure
- NO INDIVIDUAL REPORTING OF BLOCKS!

Descripción general del Sistema de Nombre de Dominios

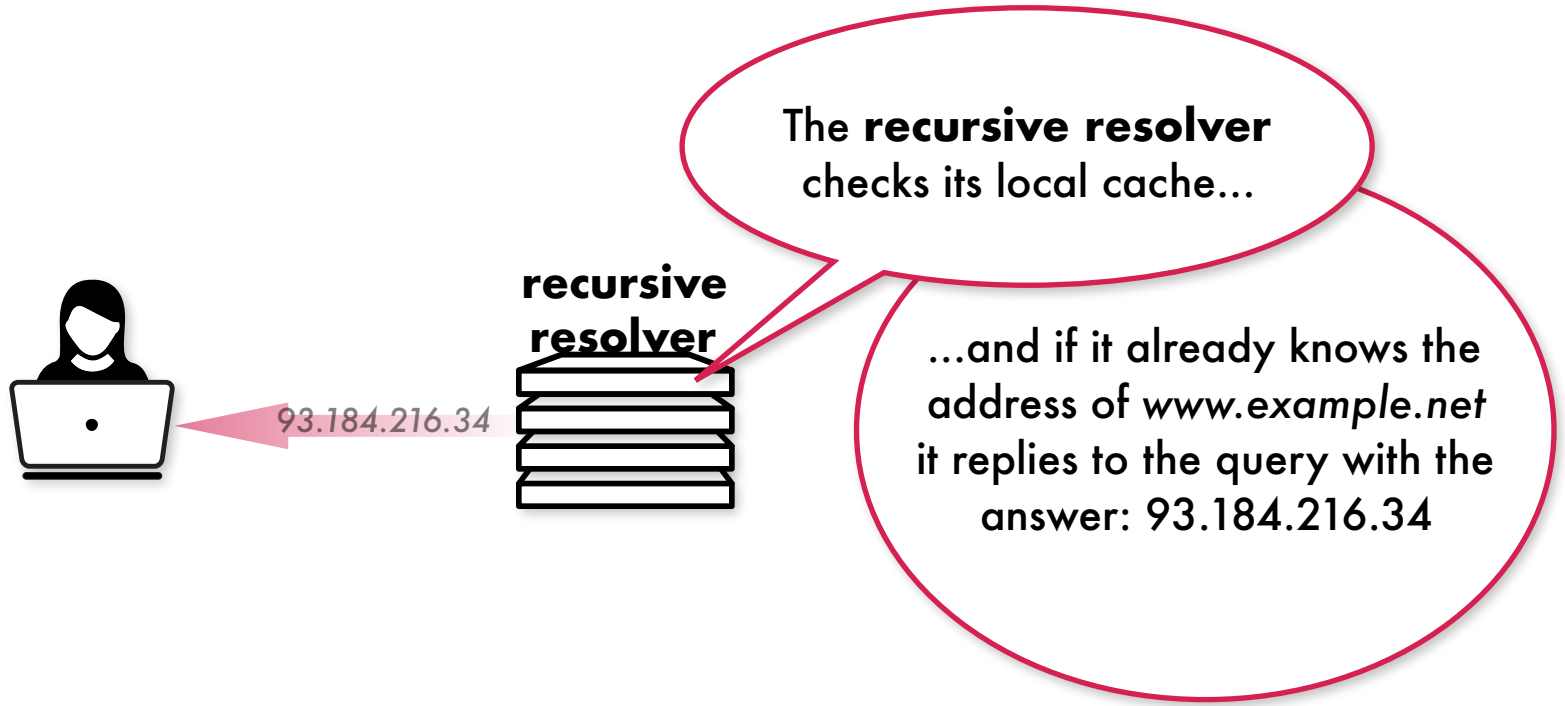
Descripción general del Sistema de Nombre de Dominios



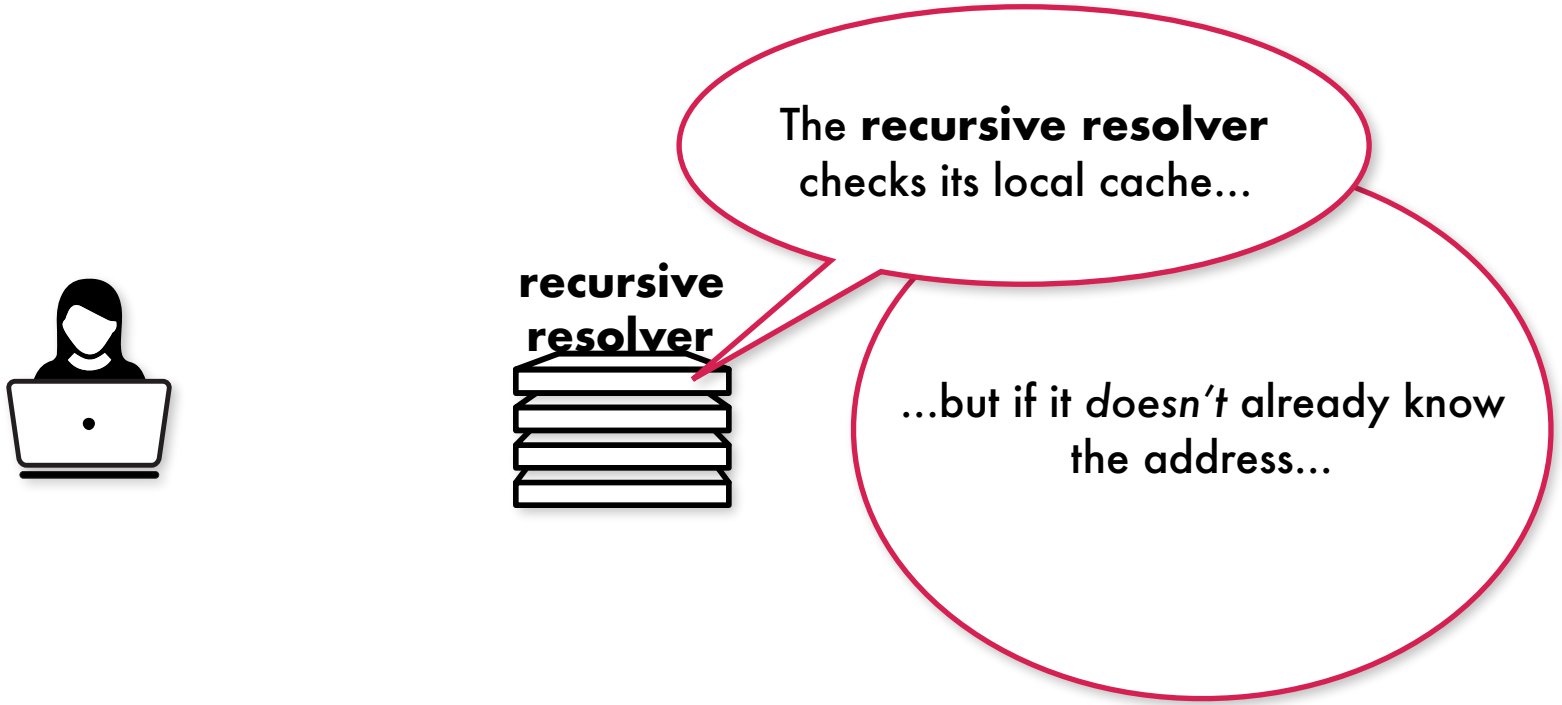
Descripción general del Sistema de Nombre de Dominios



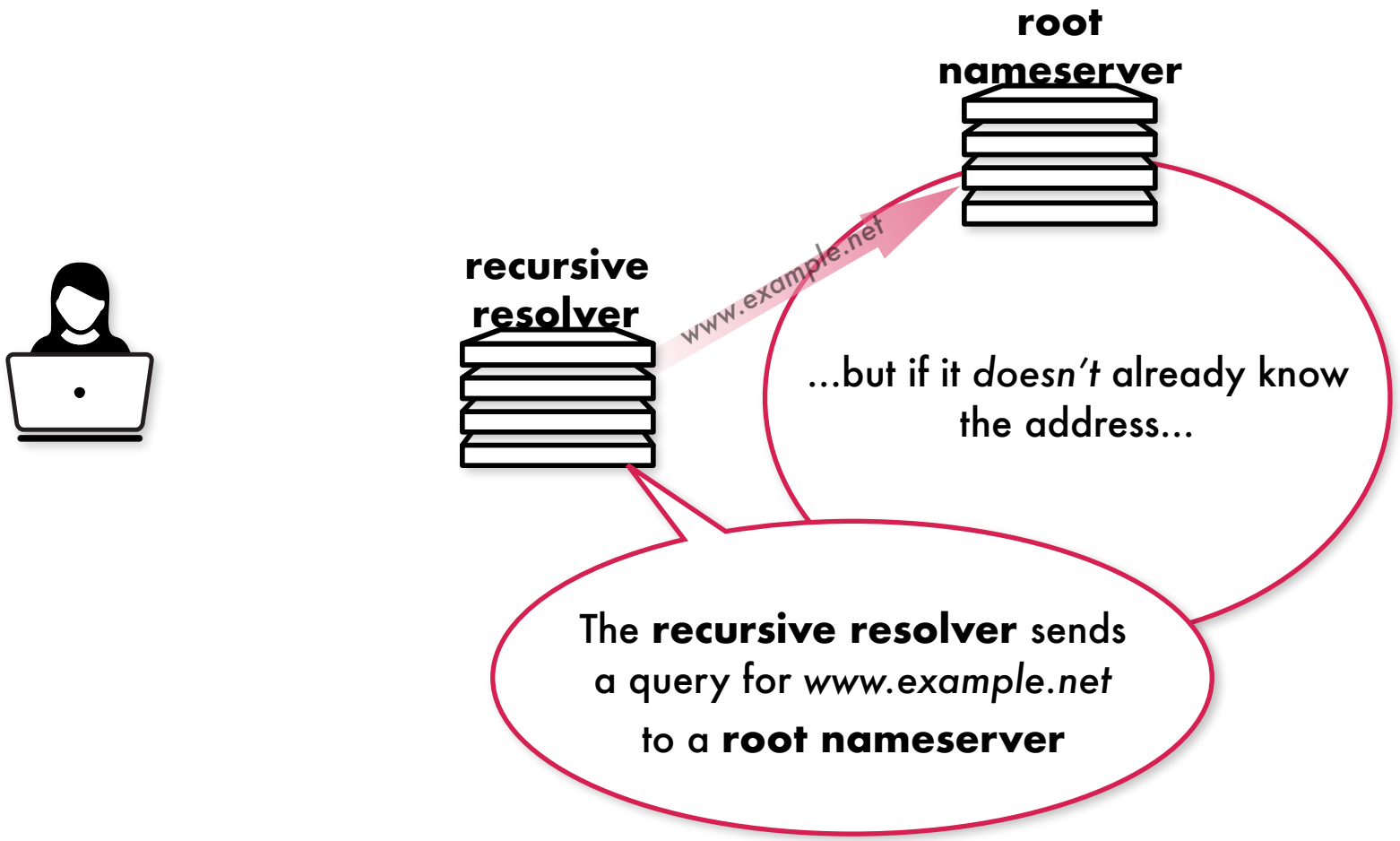
Descripción general del Sistema de Nombre de Dominios



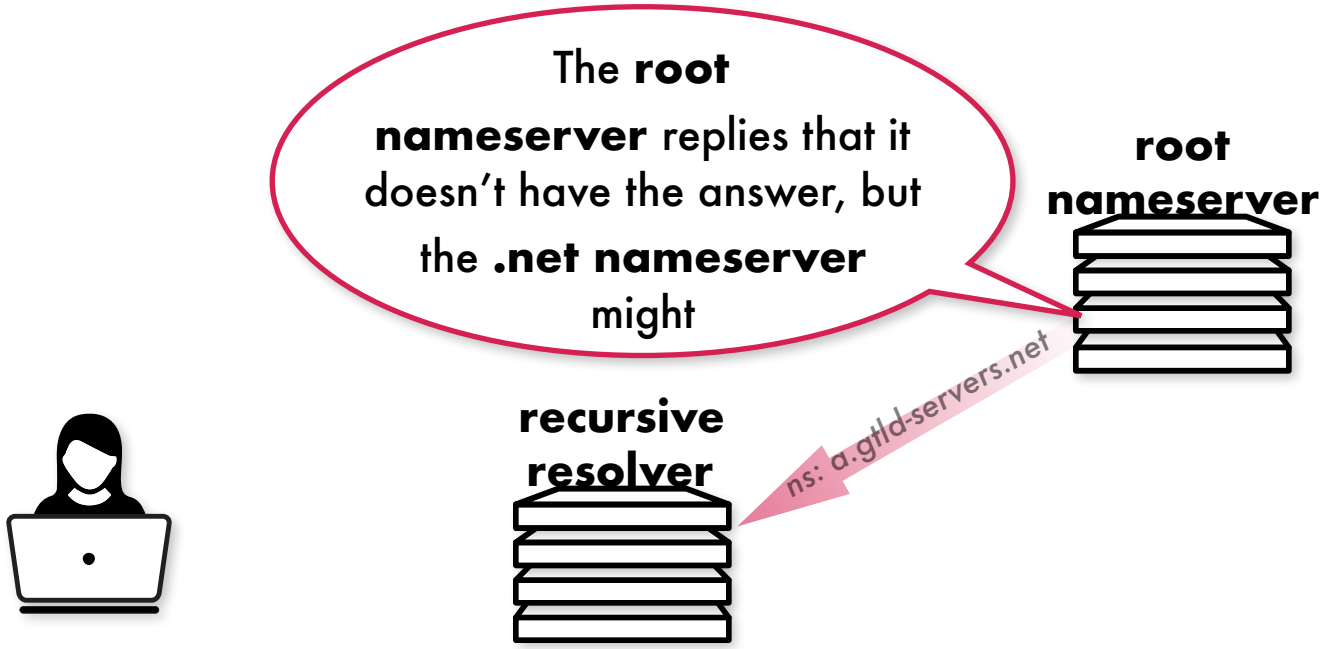
Descripción general del Sistema de Nombre de Dominios



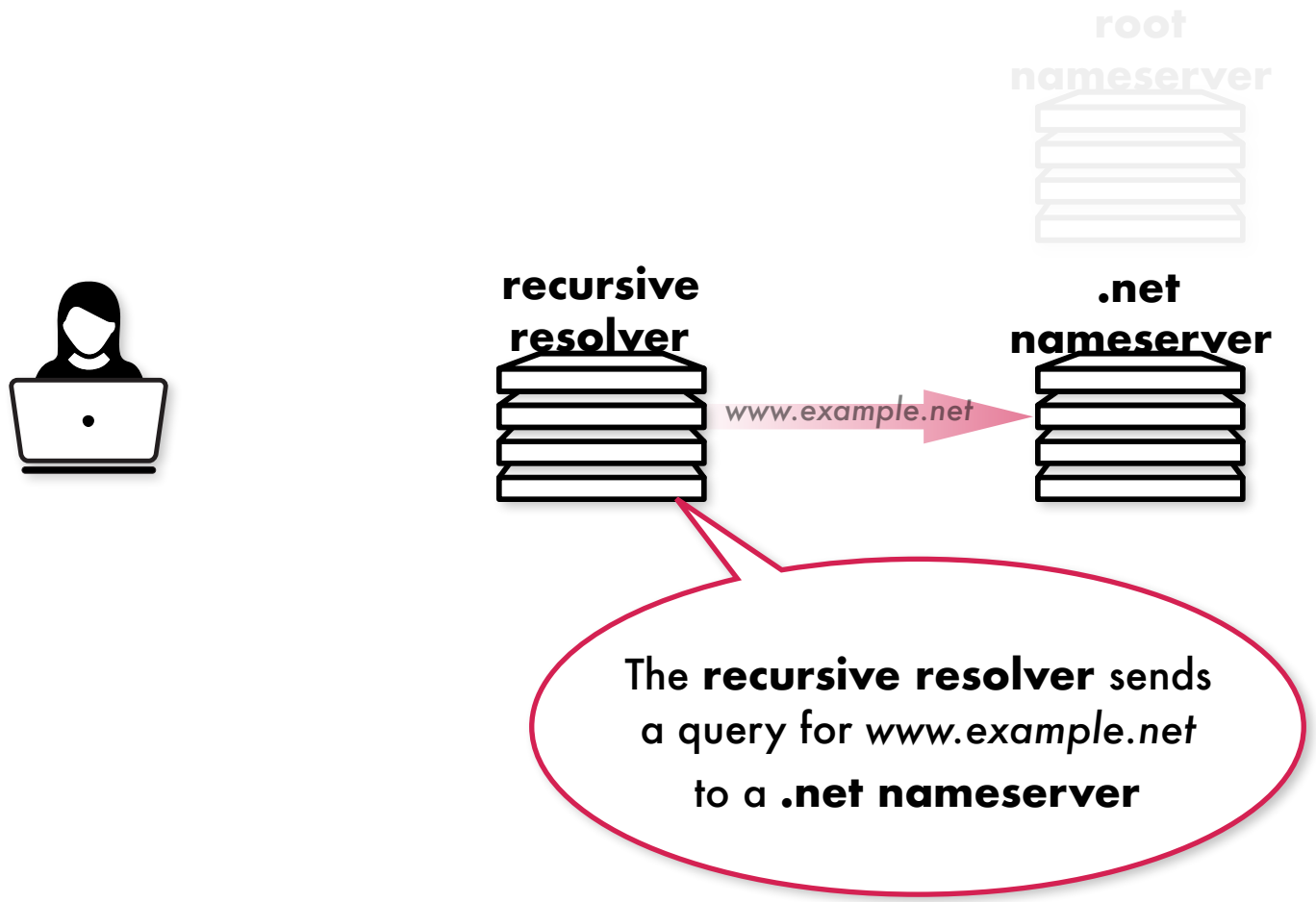
Descripción general del Sistema de Nombre de Dominios



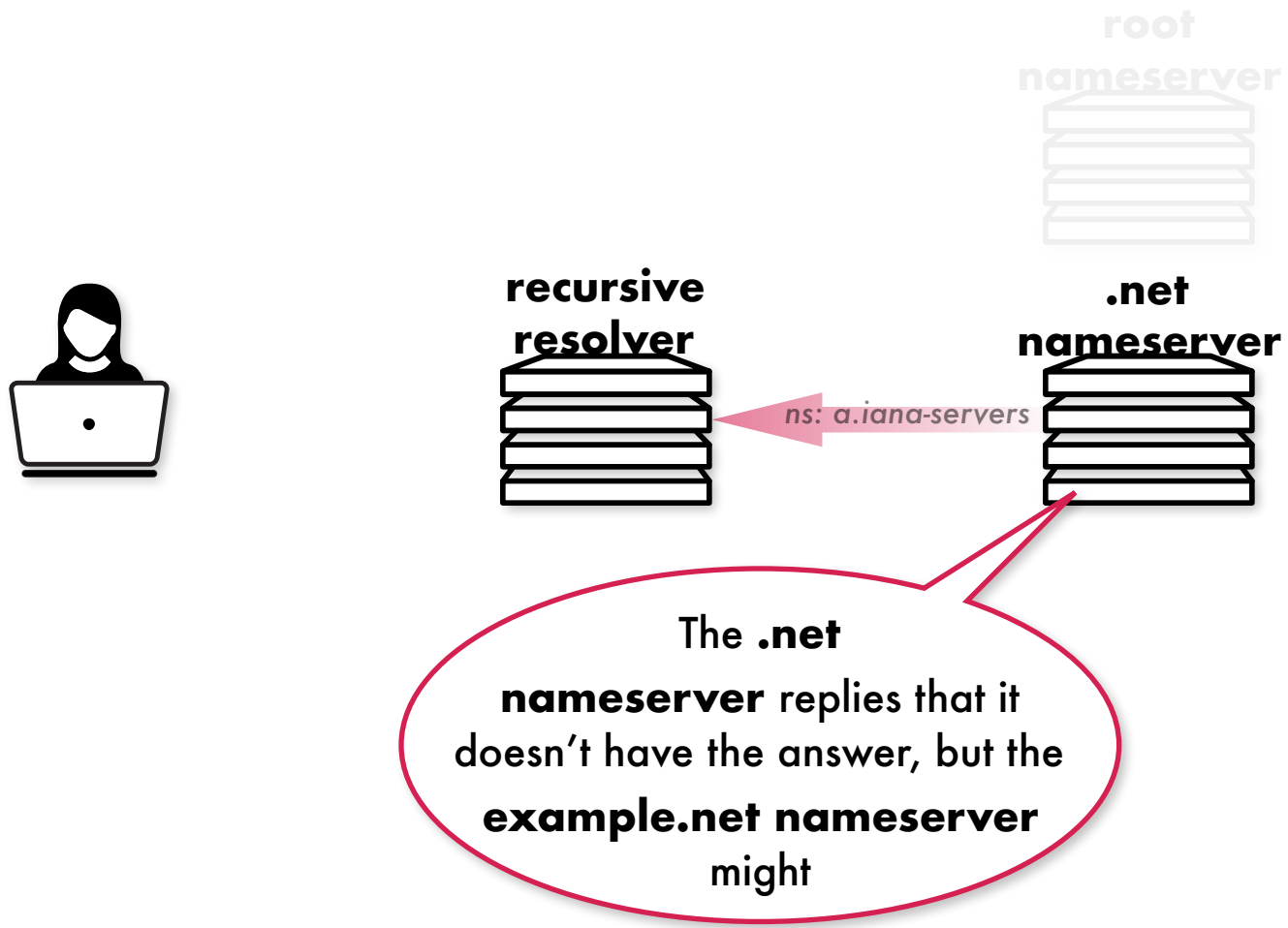
Descripción general del Sistema de Nombre de Dominios



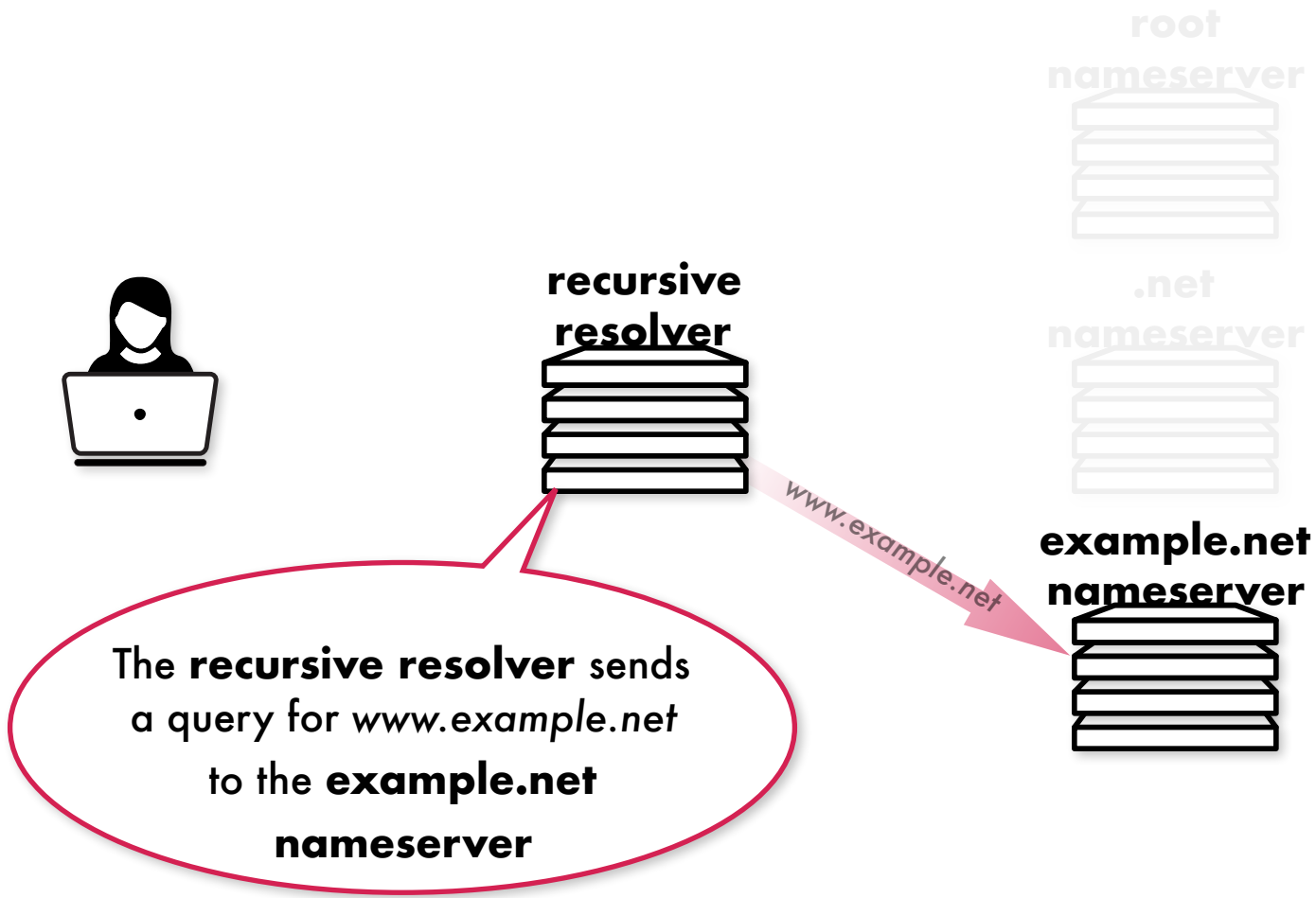
Descripción general del Sistema de Nombre de Dominios



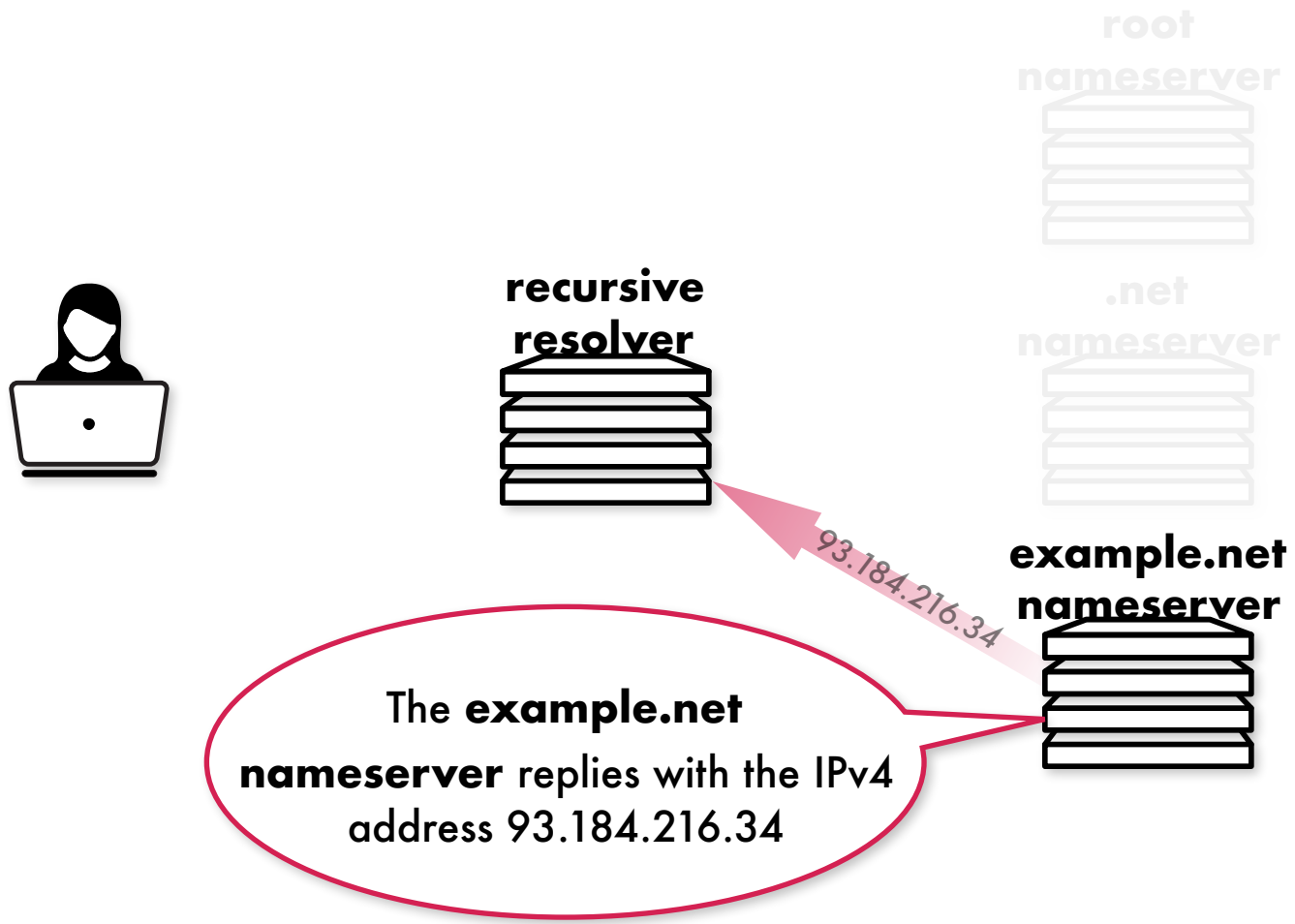
Descripción general del Sistema de Nombre de Dominios



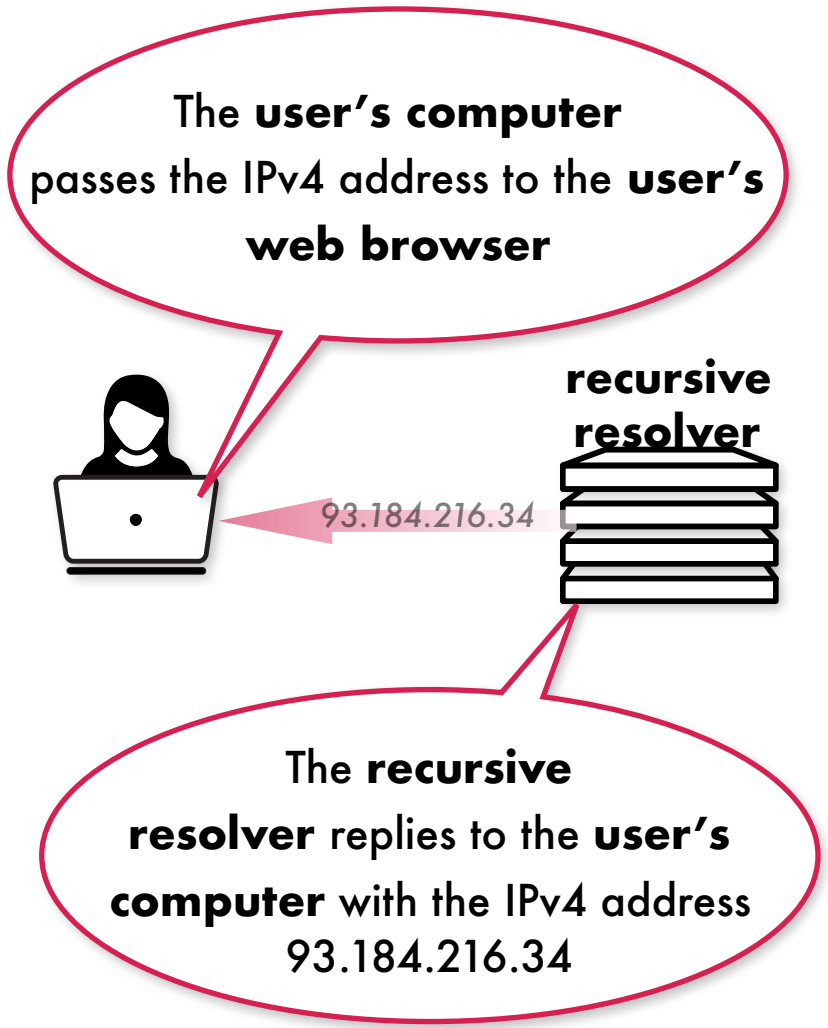
Descripción general del Sistema de Nombre de Dominios



Descripción general del Sistema de Nombre de Dominios



Descripción general del Sistema de Nombre de Dominios



Descripción general del Sistema de Nombre de Dominios

¿Cuales son las debilidades de este sistema?

¿Cuales son las debilidades de este sistema?

The connection between the user and the recursive resolver exposes the IP address of the user, which is considered regulated Personally Identifiable Information (PII) in many jurisdictions.

The domain names that the user's computer is querying for constitute a rich "click trail" of information about the user's browsing history, email, all of the software on their computer that's checking for updates, and all of the malicious software that's infected their machine.

¿Cuales son las debilidades de este sistema?

If the recursive resolver is a single machine, or a cluster of machines that share common fate, simple power or network outages can leave large communities of users unable to utilize their Internet connections.

Even when users are already using recursive resolvers that are broadly anycast, the failure of a local node often results in users' queries being backhauled to other continents.

¿Cuales son las debilidades de este sistema?

The maximum performance a user can receive is limited by the distance between the user and the recursive resolver: the further away, the slower the user's performance will be.

Also, the further away the recursive resolver is, the more surveillance regimes the user's traffic is likely to be exposed to in transit.

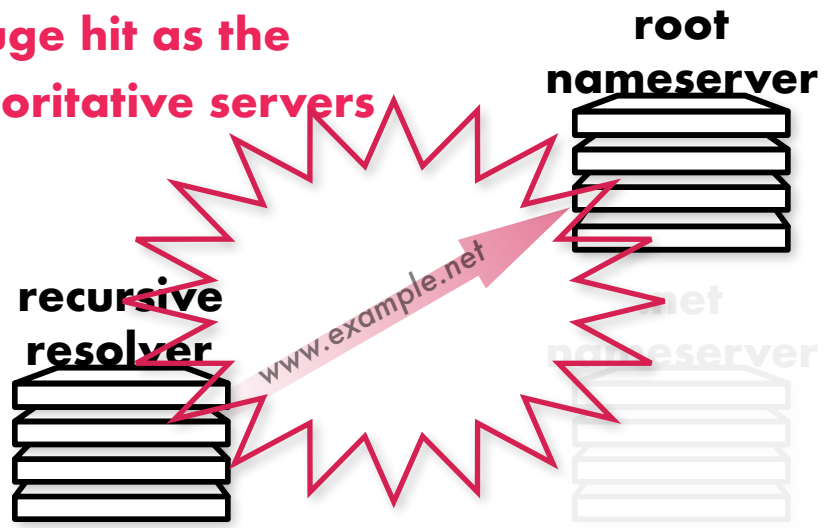
¿Cuales son las debilidades de este sistema?

A malicious computer posing as a recursive resolver can provide inauthentic answers, compromising the user's computer or online transactions.

And even a correct recursive resolver can be tricked into providing inauthentic answers to the user.

¿Cuales son las debilidades de este sistema?

When a recursive resolver has a "cache miss" performance takes another huge hit as the resolver begins querying authoritative servers that are far away and potentially slow to respond.



Many commercial recursive resolver operators intentionally pass user IP address information onward to authoritative server operators.

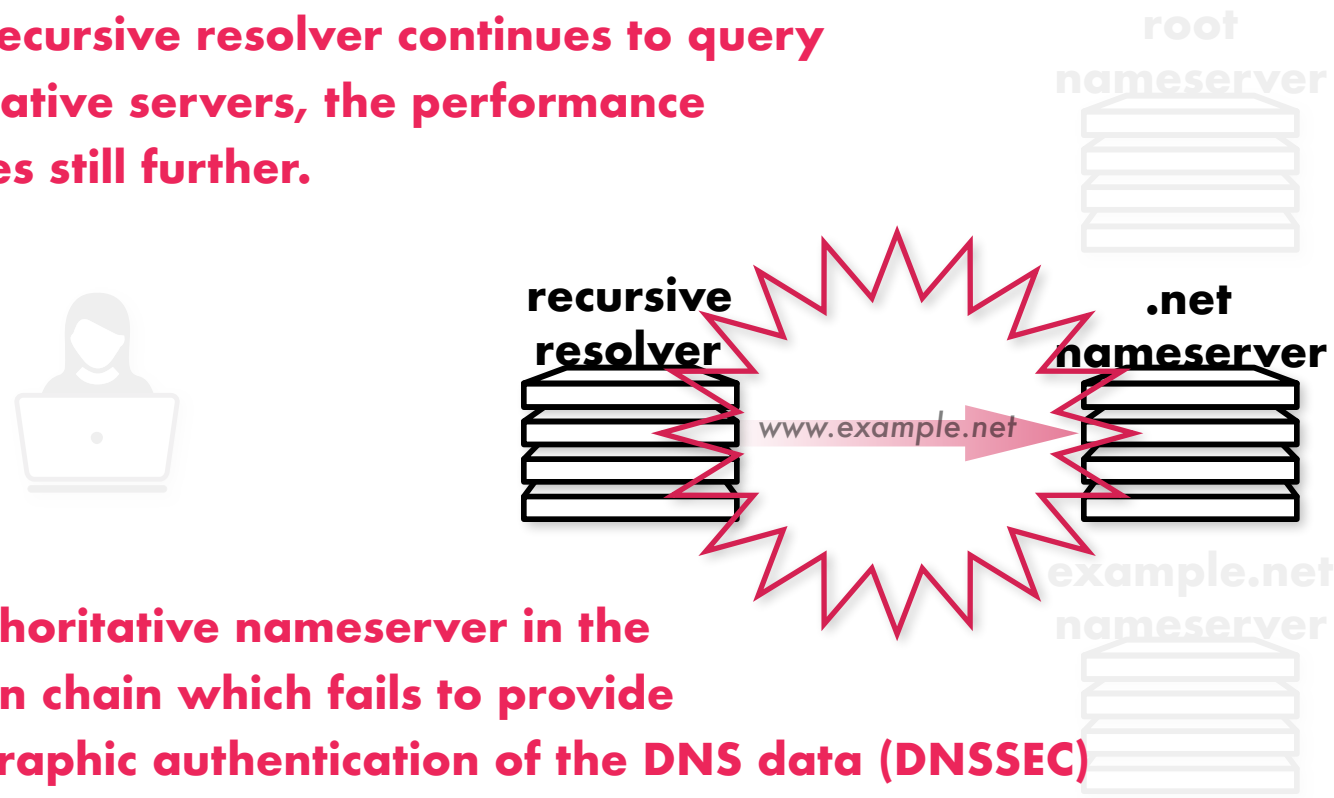
¿Cuales son las debilidades de este sistema?

Recursive resolvers leak far more information to authoritative servers than is necessary to answer queries. In this example, a query to a root nameserver need not include the "www.example" portion of the domain name.

Many authoritative nameserver operators monetize click-trail information by collecting and selling recordings of network traffic collected between the recursive servers and their authoritative servers.

¿Cuales son las debilidades de este sistema?

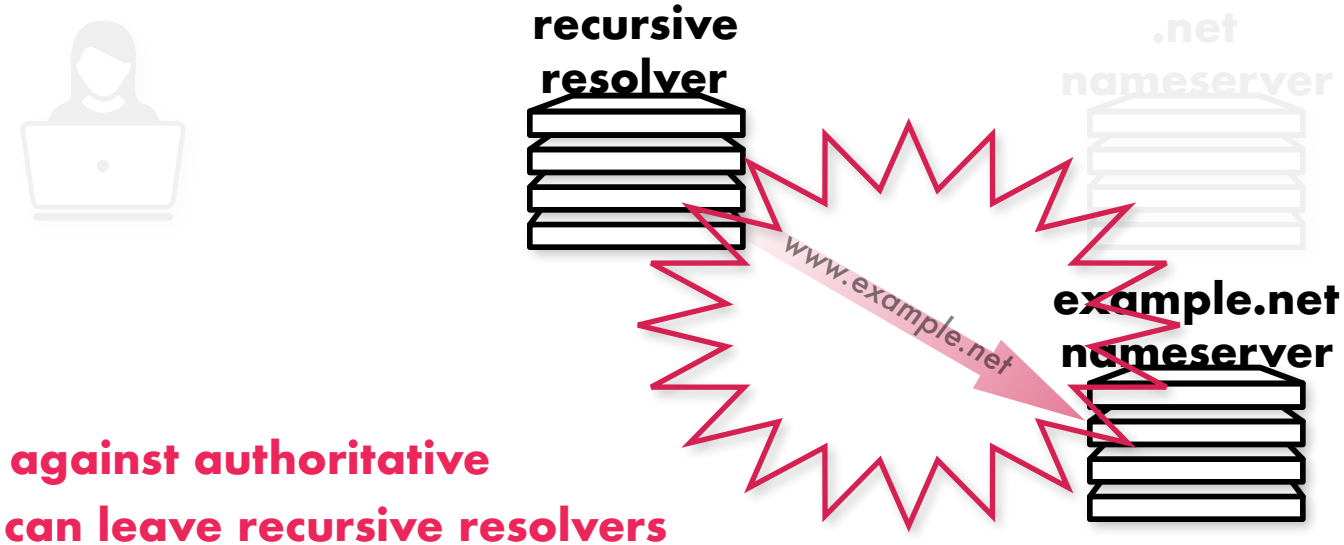
As the recursive resolver continues to query authoritative servers, the performance degrades still further.



Any authoritative nameserver in the recursion chain which fails to provide cryptographic authentication of the DNS data (DNSSEC) precludes the authentication of any domain names further downstream.

¿Cuales son las debilidades de este sistema?

Every additional authoritative server in the chain is another potential weak link which could be compromised and caused to provide malicious data to the end user.



Attacks against authoritative servers can leave recursive resolvers unable to obtain answers on users' behalf.

Motivación del Proyecto Quad9

- Ante el incremento del uso de DNS recursivos abiertos por ISPs, mejorar las opciones existentes en el mercado
- Ofrecer un servicio abierto y gratuito con bloqueo de dominios maliciosos centrado en seguridad, privacidad y rendimiento del DNS
- Demostrar la viabilidad de proporcionar un servicio de DNS recursivo sin monetizar la información de los usuarios
- Proyecto estructurado como organización sin animo de lucro c501(c)3 para evitar modelos de negocio basados en el uso y la venta de datos a terceras partes
- Proteger a la mayor gente posible posible con el apoyo de la industria, promocionando una Internet mas estable y segura

Quad9: Organización y Patrocinadores

Quad9

IBM | GLOBAL CYBER ALLIANCE | PCH Packet Clearing House

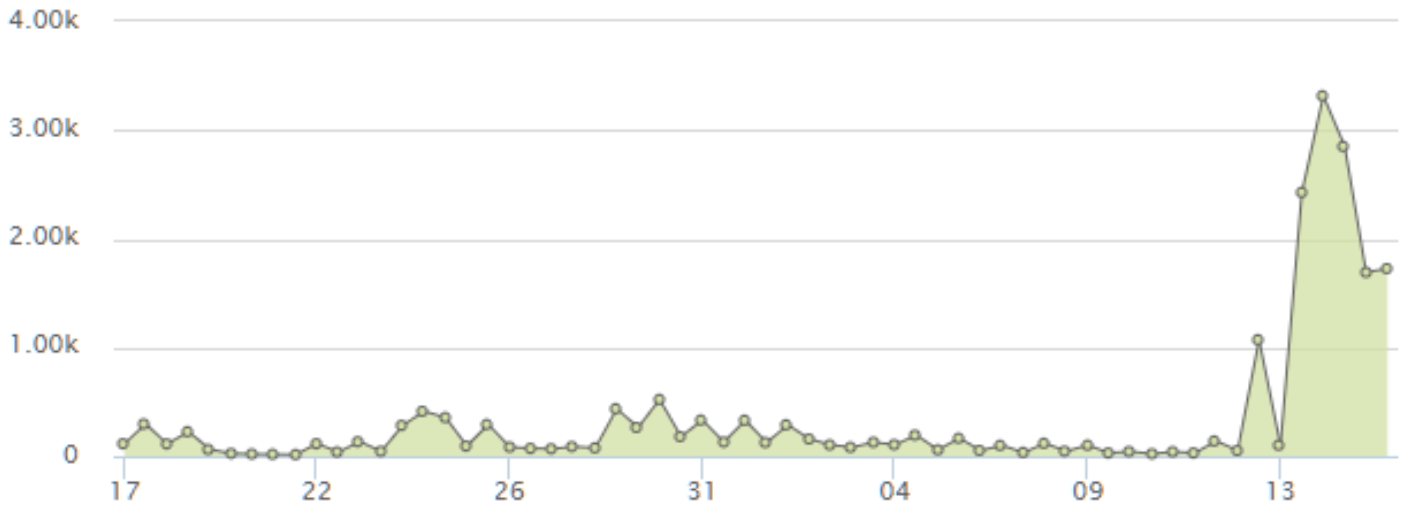
Mas información en https://quad9.net/quad9-yourdata/

SECURITY & THE BLOCKLIST

- Bloqueo de conexiones maliciosas a hosts: protección de los datos DNS usando cualquier método de cifrado técnicamente viable
- 19 proveedores de inteligencia anti-amenazas (TI): muchas perspectivas crean una blocklist efectiva y con una diversidad única:
  - Domain Generation Algorithms (DGA) lists
  - Malware lists
  - Phishing lists
  - Command-and-Control lists
  - Exfiltration destinations
  - Unexpected use (e.g.: mining)

SEGURIDAD & LA "BLOCKLIST"

- Reducción de eventos sospechosos: la desconexión accidental de Quad9 incrementó en un 2200% los eventos maliciosos/ sospechosos. Dicho de otro modo, Quad9 redujo dichos eventos en un 95.5%



BENEFICIOS PARA LOS TI PROVIDERS

FEEDBACK A INTEL PROVIDERS

Quad9 devuelve datos a los proveedores de inteligencia contra amenazas en la forma de datos genéricos para ayudarlos a mejorar sus modelos, mejorando así el sistema para todos. Resumen de datos “hit” de dominios bloqueados devueltos via una API en casi tiempo real.

DATOS DE DOMINIOS GENERALIZADOS

Quad9 puede proporcionar información sobre los dominios de destino a los patrocinadores: ataques o fallos DNSSEC, distribución geográfica aproximada de los orígenes de las consultas, latencia de resolución hacia autoritativos por POP y resolución "backdoor" hacia autoritativos en condiciones de DDoS.

CIFRADO, VALIDACION & SEGURIDAD

- Quad9 soporta DNS-over-TLS a día de hoy, cifrando peticiones entre clientes y nuestros servidores.
- DNS-over-HTTPS sera soportado pronto (en desarrollo).
- Quad9 hace validación “estricta” DNSSEC, eso significa que intentamos prevenir que se entreguen datos de dominio falseados (spoofing). Si tu organización no utiliza todavía DNSSEC en sus dominios, averigua como funcionaría y pasa a implementarlo.
- Los servidores de Quad9 están típicamente ubicados adyacentes a dos servidores DNS raíz, así como a servidores DNS que albergan >500 dominios de primer nivel (TLDs), haciendo el spoofing difícil

PRIVACIDAD

- Quad9 nunca hace escrituras a disco o transmite datos privados fuera del POP(*) y no se usan sistemas cloud o externos para tratamiento de datos
- Diseñado originalmente para cumplir con las especificaciones GDPR
- Transparencia en la estructura organizacional a través de requisitos debido al estatuto de sin animo de lucro
- Transparencia en trafico de datos (abierto para la auditoría de gestión de datos)
- En conversaciones con países de la UE y organismos de estandarización para la auditoría de la privacidad

(*) private data = IP address associated with DNS queries. Exceptions exist for security events of extremely limited scope and duration.

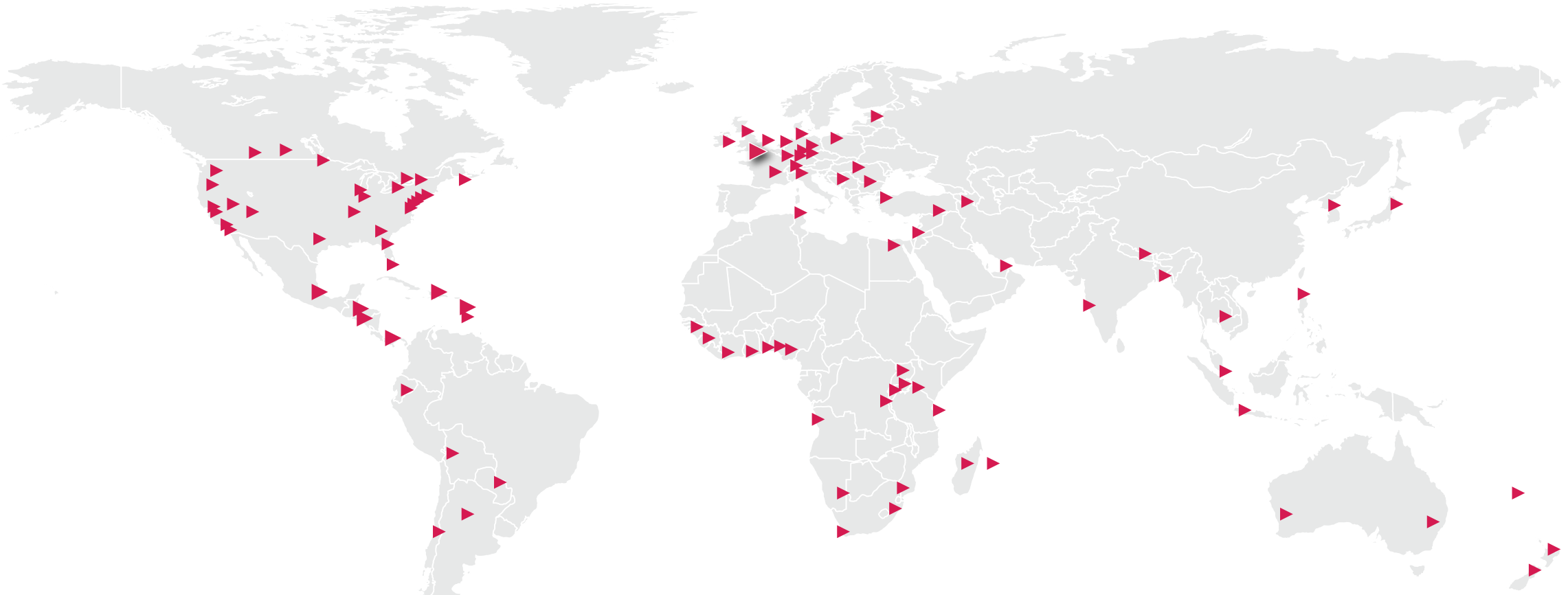
RENDIMIENTO/ SITUACION ACTUAL

- Principalmente ubicados en puntos neutros (IXPs) - menores latencias a una mayoría de ASNs
- Cuantos mas usuarios en el sistema, el sistema se vuelve mas rápido (efecto de red)
- Actualmente 114 ubicaciones y objectivo de 150 al final de 2018
- Millones de usuarios ahora mismo - divididos entre usuarios finales y caching resolvers
- Universidades, ISPs, organismos gubernamentales, gobiernos y grandes empresas como usuarios del sistema
- Tasas de crecimiento iniciales de ~2% al día comienzan a ralentizarse
- ~1.5 - 2.0 millions de eventos bloqueados al día
- 100% uptime durante ~2 anos de operación

Arquitectura del sistema Quad9

- Nodos construidos sobre servidores Cisco UCS
- Cada nodo contiene una instancia de telemetría y tres instancias de resolvers DNS
- Balanceado de carga con dnsdist
- Redundancia DNS con servidores PowerDNS y Unbound
- Servidores Root y TLDs “back-to-back” en el mismo nodo
- Enrutamiento a través del ASN propio Quad9 (AS19281) y el ASN de PCH (AS42)
- Conexiones de Nx10Gbps y Nx1Gbps según tamaño del nodo

Mapa de despliegue nodos Quad9 (March 2018)



114 ubicaciones Anycast en 73 países

Y desde España, donde queda Quad9?

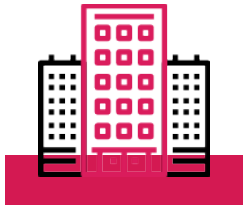
```
➜  ~ traceroute -a 9.9.9.9
traceroute to 9.9.9.9 (9.9.9.9), 64 hops max, 52 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  [AS5511] ae101-24.bartr1.barcelona.opentransit.net (193.251.251.229)  6.474 ms  3.308 ms  2.929 ms
 6  [AS5511] hundredgige0-6-0-0.barcr4.barcelona.opentransit.net (193.251.132.17)  6.375 ms
    [AS5511] hundredgige0-7-0-1.barcr4.barcelona.opentransit.net (193.251.132.25)  11.109 ms  9.804 ms
 7  [AS5511] hundredgige0-7-0-1.madtr3.madrid.opentransit.net (193.251.128.104)  11.771 ms  !Z  12.201 ms
 8  [AS0] 81.52.188.30 (81.52.188.30)  13.320 ms  12.518 ms  13.314 ms
 9  [AS2914] ae-7.r24.londen12.uk.bb.gin.ntt.net (129.250.4.137)  32.364 ms  32.645 ms  31.882 ms
10  [AS2914] ae-21.r00.londen10.uk.bb.gin.ntt.net (129.250.4.24)  33.623 ms  31.636 ms  30.393 ms
11  [AS2914] 83.231.233.182 (83.231.233.182)  34.041 ms  31.659 ms  48.488 ms
12  [AS19281] dns.quad9.net (9.9.9.9)  156.151 ms !Z  30.327 ms !Z  136.804 ms !Z
```

Matriz de sabores Quad9

- Por defecto: 9.9.9.9 o 2620:fe::fe
- Sin bloqueo (insegura): 9.9.9.10 o 2620:fe::ff
- CDN-Friendly: 9.9.9.11
- IoT-Friendly: 9.9.9.12

Name	IP	Blocklist	NXDOMAIN only	Send EDNS Subnet	DNSSEC Validation
Default	9.9.9.9	x			x
Non-secure	9.9.9.10			x	
CDN-Friendly	9.9.9.11	x		x	x
IOT-Friendly	9.9.9.12	x	x		x

Ejemplos de Casos de Uso para Quad9



ENTERPRISE

Additional layer in a full-spectrum cyber-defense. No contract or cost & near-zero implementation effort.

ISP

Provide differentiation to customer base; outsource DNS recursive resolver costs and privacy issues.

EDUCATIONAL

Protect students & staff in “BYOD” environments which are typical for .edu. Devices can’t be controlled closely, but where they connect can be controlled.

Integración con infraestructura DNS

IMPLEMENTATION

- Standalone:
  - Change DHCP DNS resolver IP to 9.9.9.9
- Forwarder - compatible with:
  - Microsoft DNS servers of all types
  - Open source resolvers like ISC BIND, PowerDNS, Unbound, Knot, etc.
  - Hardware-based firewall/gateway systems such as Barracuda, Juniper, pfSense, etc.
  - Any system that is DNS RFC-compatible should work with Quad9. If not, we'd like to hear about it.

Lineas de trabajo actuales

- Colaboración con fabricantes de dispositivos IoT
- Optimización del enrutamiento para mantener el trafico lo mas local posible
- Especialización en los proveedores de inteligencia anti-amenaza añadidos durante 2018:
  - Financial services providers
  - Cryptocurrency domain attack data
  - Specific API-based service attack data
  - Mobile device platforms at high risk

Lineas de trabajo actuales

- Implementación de DNS-over-TLS en el código fuente de Android
- Implementación de la opción Extended Client Subnet (ECS) para mitigar el impacto negativo al usar CDNs
  - Colaboración con CDNs en el mapeo exacto de los nodos
- Integración de Quad9 dentro de proveedores de servicio
- Expansion del numero de POPs (150 ciudades en 2018)
- Uso de Quad9 en programas de cyber seguridad para países en desarrollo

RESUMIENDO

- DNS is vital to almost every Internet transaction; Quad9 can block desktop, mobile, and IoT threats with the same model
- DNS security is often weak; Quad9 provides DNSSEC and encryption capabilities
- DNS resolution speed is important for fast services; Quad9 is located at >114 IX locations for low-latency and high redundancy
- DNS privacy is critical; Quad9 has strict data anti-harvesting guidelines and no profit motive
- DNS blocklists are effective only when comprehensive; Quad9 integrates 19 different threat providers into a single interface
- Network security is often complex; Quad9 is a single configuration - just change your DNS resolver IP addresses
- DNS commercial services require contracts and friction; Quad9 doesn't even ask for your email address

Quad9

9.9.9.9
2620:fe::fe

Gael Hernandez - PCH
gael@pch.net

https://www.quad9.net/

WHAT IS Quad9 NOT?

Quad9 is not:

- a complete security solution - it is a part of a layered security model
- a content policing tool - Quad9 only targets malicious hosts
- a customizable filter - there are only two flavors: “on” and “off”
- a reporting tool - privacy precludes storing report data on IPs
- an antivirus program - Quad9 only stops connections to hosts, not programs
- profit-driven - the goal is to protect as many people as possible with support given by industry to promote a more stable Internet