ICANN83 | Foro sobre políticas – Sesión conjunta: ALAC y SSAC
Martes, 10 de junio de 2025 – 9:00 a 10:15 CEST

YEŞIM SAĞLAM: Hola y bienvenidos a esta sesión conjunta de ALAC y el SSAC, soy Yeşim Sağlam y soy la coordinadora de participación remota para esta sesión. Tengan en cuenta que esta sesión está siendo grabada y sigue los estándares de comportamiento esperados de la ICANN, así como las políticas antiacoso de la ICANN.

Durante esta sesión las preguntas y los comentarios se van a leer en voz alta si se presentan en el recuadro de preguntas y respuestas, tendremos interpretación en inglés, español y francés y en esta sesión. Si quieren hablar levanten la mano en Zoom y una vez que mencionen sus nombres los participantes remotos tendrán permiso para activar su micrófono en Zoom, los participantes en persona utilizarán un micrófono físico.

Por favor, digan su nombre para los registros, el idioma en el que hablarán, si es que no hablan inglés, y hablen a una velocidad razonable. Gracias a todos por participar y ahora le voy a dar la palabra a Jonathan Zuck y a Ram Mohan, presidente del SSAC.

JONATHAN ZUCK: Gracias, Yeşim. Gracias a todos por estar aquí, siempre tenemos una muy buena colaboración con SSAC, lo que queremos es ver qué han estado investigando y poder encontrar maneras de que

nosotros podamos entenderlos y luego ayudar a nuestros grupos a que también lo entiendan. Gracias y bienvenidos.

RAM MOHAN

Siempre es un placer estar con ALAC, en el pasado era un grupo donde uno tenía que explicar la tecnología y ahora no hay que explicarla, sino que se trata de ver cómo explicársela a las otras personas porque aquí hay gente con mucha experiencia y podemos utilizar toda la jerga sin tener que explicarlo mucho, de todos modos, es un placer siempre estar aquí.

En particular analizamos aquí la colaboración con ALAC como una parte esencial de lo que está haciendo SSAC y buena parte de esto es porque nos damos cuenta en SSAC que se trata de algo muy importante para nosotros hacer este trabajo y poder hacer investigación y dar asesoramiento, pero el verdadero valor es, ¿cómo lo hacemos de un modo que resulte comprensible, digerible y que esté en las manos de aquellos que lo necesitan más?

Evolucionamos entonces de un lugar en el que nos dábamos palmaditas en la espalda y decíamos: “Hicimos un buen trabajo”, describir este informe y decir: “Así comienza…”

[Error del audio 00:03:40 – 00:04:24]

JONATHAN ZUCK

Con respecto al curso de pesca que estamos haciendo de phishing, parte de lo que resulta muy singular de nuestra

comunidad, es que es una gran comunidad de At-Large que incluye las organizaciones At-Large, las estructuras, los miembros individuales y crea una cierta cobertura en el mundo que no se compara dentro de la comunidad de la ICANN, hacemos entonces muchos experimentos para poder así entender cómo hacerlo en asociación con ustedes.

RAM MOHAN Es fantástico esto. El ecosistema más allá de ALAC en sí es una verdadera ventaja para nosotros porque tenemos muchas ideas, Jonathan, con respecto a las maneras en las que podemos hacer que el material sea más accesible.

Algo que hacemos también para muchos documentos de SSAC es que les pedimos a los miembros que nos den un resumen ejecutivo de 500 palabras que pueda capturar en esencia qué es todo esto y lo que nos gusta hacer es trabajar con ustedes para establecer cómo animarlo, es decir, a ser discernible, hacerlo accesible para todo tipo de audiencias.

JONATHAN ZUCK Es como una danza interpretada todo esto, ¿no?

RAM MOHAN El primer tema en SSAC es que hace unas semanas hemos publicado un documento que es el SSAC127 sobre el bloqueo de DNS y uno de los copresidentes estuvo aquí para presentarles a ustedes cuáles son los hallazgos principales y algunas de las cosas

que pensamos sobre esto, se trata de un área que recibe mucha atención en SSAC, estamos trabajando con ustedes y vamos a hablar también con el GAC y con otros porque, como todos saben, reunimos a los gobiernos, a los formuladores de políticas que vemos que cada vez bloquean más el DNS y lo hacen por distintas razones.

Entonces aquí estamos para echar un poco de luz y también para dar cierta precaución.

WARREN KUMARI Voy a saludar con el sombrero para que vean la próxima diapositiva que es muy bonita, tiene una linda imagen de Praga, tenemos muchas diapositivas por ver, así que, vamos a tratar de ir rápido.

¿De qué se trata todo esto? En 2011 y 2012 SSAC publicó la SAC50/SAC56 que habló del bloqueo del DNS, el internet ha cambiado bastante en los últimos 12 o 13 años y por eso hemos decidido que era momento de actualizar el documento y dar asesoramiento especialmente en lo que se refiere al bloqueo del DNS.

El objetivo del documento es dar asesoramiento a los funcionarios sobre lo efectivo que puede ser el bloque del DNS, pero también ver cuáles pueden ser los peligros, el daño colateral que puede haber, etc.

¿Qué es el bloqueo del DNS del que hablamos? Básicamente es

una manera de bloquear el acceso al contenido de internet al realizar algún tipo de bloqueo en los resolutores recursivos, es bloquear el contenido, pero lo importante es que, si solamente afecta a los usuarios que están utilizando un resolutor recursivo, ahí es donde ocurre el bloqueo.

Lo que debe lograr es esto, es decir, si ustedes están utilizando uno de los resolutores recursivos donde se implemente el DNS, no van a poder acceder al contenido que está bloqueado, pero como dije antes, esto es efectivo parcialmente y solo se aplica en la parte en la que el bloqueo está realizado.

El bloqueo de DNS es solo una herramienta, al igual que con cualquier otra herramienta tiene ciertas fortalezas y ciertas debilidades, entender cómo funciona la herramienta es importante porque si no podemos tener inconvenientes, es potencialmente una herramienta muy poderosa y como tal esto quiere decir que, si no lo hacemos bien, el resultado puede ser muy malo.

El bloqueo de DNS, además, no remueve el contenido de internet, lo que hace es lograr que quede inaccesible a un conjunto específico de usuarios, esta es una alternativa más limitada a suspender el dominio y también en algunos casos es más apropiado o la única opción que tenemos para una comunidad específica o un conjunto de usuarios específicos.

Como ya he dicho, no es 100% efectivo, hay varias maneras de poder circunvalar el bloqueo de DNS y veremos esto en breve.

¿Cómo se logra entonces el bloque de DNS? Aquí tenemos un panorama de la resolución de DNS y con el bloqueo en el servidor de DNS recursivo que es el que está en medio, hay un filtro que se aplica.

Cuando un usuario hace una consulta de DNS, esa consulta accede al servidor recursivo y si ese dominio no está en lista de bloqueo, entonces ocurre la resolución de DNS normalmente y el usuario puede acceder al contenido.

Si ese dominio sí está en una lista de bloqueo, en lugar de poder acceder a la información, hay otra cosa que ocurre con la consulta y el usuario no puede acceder. Cuando digo que sucede “otra cosa” son distintas cosas que pueden suceder, la más común y que potencialmente es menos dañina para el usuario es que el resolutor dice: “Este nombre de dominio no existe”.

Si probamos con un sitio web que está en la lista de bloqueo, el resolutor dice que este nombre no existe, entonces el usuario no puede acceder a esta web. Otra cosa que puede hacer el resolutor es modificar la respuesta del resolutor autoritativo y puede retornar una dirección IP distinta que la que el resolutor autoritativo tenía la intención de hacer.

Esto se denomina redirección y es lo que vemos que ocurre con bastante frecuencia, una de las opciones menos buenas me parece que es está porque tiene resultados de seguridad muy malos que veremos en breve.

Una tercera opción que para muchos suena como la mejor es que, el resolutor recursivo elige ignorar la consulta, si miramos un sitio web el servidor puede ignorar la solicitud y no responderla. La desventaja de esto es que las computadoras tienen muchos resolutores recursivos listados y si el primero no responde, la máquina simplemente accederá al segundo, al tercero o al cuarto.

Si ese resolutor no realiza el bloqueo, el usuario va a poder resolver el nombre y va a poder ver el contenido que supuestamente está bloqueado, eso solamente afecta a resolutores recursivos donde sucede el bloqueo, si se utiliza otro resolutor no va a ser efectivo el bloqueo.

El bloque de nombres de alguna manera es similar y a la vez muy diferente a la suspensión de dominios o el ataque del dominio, estamos hablando de un conjunto específico de resolutores en la suspensión mientras que el seizure que es el bloqueo no permite que nadie pueda acceder a internet.

Entonces este embargo del dominio se utiliza para cuando existen casos de phishing o cuando la información se actualiza entre el servidor de DNS autoritativo, el registro y el registratario. Es una especie de operación global, es algo más amplio porque afecta a todos los que utilizan el nombre de dominio y esa opción es la única que está disponible a veces para alguien, por ejemplo, una violación de marca registrada que puede hacer que este dominio embargado pueda suspenderse.

Voy a tratar de apurarme un poquito para respetar el tiempo que

se me ha asignado.

JONATHAN ZUCK ¿El Firewall de China está haciendo lo que usted sugiere? ¿Va todo en camino?

WARREN KUMARI Este Firewall de China básicamente lo que hace es supervisar las consultas de DNS que pasan a través de él, es decir, no es lo que llamamos tradicionalmente bloqueo de DNS, no es exactamente eso, no está operando en el recursivo.

¿Por qué las personas hacen esto? Vamos a ver algunas ejemplos. Hay algunas razones, por ejemplo, la menos controvertida es que los operadores de la red hacen un bloqueo de DNS en los resolutores recursivos.

Entonces un número significativo de recursores resolutivos ya están haciendo esto, es un lugar donde se retiene el malware o donde hay una especie de comando de control o botnets, por ejemplo, CloudFlare que ejecuta el 1.1.1.1 y también tiene una segunda dirección IP que ejecuta el 1.1.1.2 que luego se puede configurar en su máquina y va a bloquear el acceso a los sitios de malware conocidos.

Muchas empresas tienen políticas corporativas que dicen que los empleados no deberían entrar a Facebook desde sus máquinas corporativas o en horas de trabajo, entonces pueden implementar una especie de bloqueo suscribiendo a lista de bloqueo de DNS e

incluirlo en sus resolutores recursivos o en sus Firewall.

Y si deciden, por ejemplo, bloquear Facebook o usar un resolutor para esto, el resolutor puede bloquear esa resolución. Hay algunas organizaciones como las escuelas o las bibliotecas que tienen un acceso bloqueado al contenido inapropiado, por ejemplo, apuestas o contenido adulto no apropiado.

Entonces como dije antes, CloudFlare tiene 1.1.1.2 que bloquea el acceso al malware y luego brinda el 1.1.1.3 que bloquea el acceso al malware y al contenido adulto. Entonces somos como padres, queremos evitar que nuestros hijos accedan a ese contenido, se configuran las máquinas locales para utilizar 1.1.1.3, por ejemplo.

Esto es algo que surge mucho más en la prensa y es un poco más controvertido que es cuando el bloqueo está ordenado por el gobierno o por un tribunal de justicias donde un gobierno o un tribunal es el que da la orden de utilizar estos operadores recursivos dentro de su jurisdicción para bloquear el acceso a ciertos nombres de dominios, esto tiene que ver con mecanismos de censura, también con contenido que es subversivo o desestabilizante a nivel político, un gobierno puede ordenar que estos proveedores de servicios estén bloqueados en su país. Esto es solo un resumen.

El SSAC trata de ser bien técnico en este documento y no estamos tratando de tomar partido en lo que implica una censura, sino en la legalidad de ciertos casos específicos, les pedimos que lean el

documento.

Como dije, el bloqueo de DNS es parcialmente efectivo, al final de esta diapositiva vemos una resolución de DNS normal, el usuario envía la conducta al resolutor, si no está en la lista de bloqueo funciona normalmente y si sí está, el resolutor no funciona o se redirecciona a otro.

JONATHAN ZUCK

Tengo una pregunta. En el ejemplo tenemos una fecha donde no vemos nada que vaya a través de ese filtro, ¿verdad?

WARREN KUMARI

No estoy seguro de haber respondido tu pregunta, pero el gráfico siento que puede ser un poquito confuso y, en realidad, puede ser el resultado de la decisión y no a dónde lleva al usuario. Esto se aplica a la consulta del usuario que tiene que ver con el ISP y el resolutor de filtro, si el usuario envía su consulta a otro resolutor, entonces el bloqueo no va a ser efectivo.

¿Cómo sucede esto? Podemos elegir un servidor de DNS alternativo, no el que se brinda en el país o por el proveedor de internet, hay distintas formas de hacerlo, hay algunos resolutores recursivos públicos, tenemos algunos como el DNS público de Google conocido como 8.8.8.8, CloudFlare o Quad9, algunos están patrocinados por el gobierno, tenemos también el DNS4EU que se denomina Arab Springtime, que es uno relativamente conocido. Hay varios bloqueos de DNS que ocurren en ciertos países, por

ejemplo, en Egipto donde se ha bloqueado un acceso de internet, se pueden actualizar los resolutores recursivos a 8.8.8.8.

Esto es algo bastante simple de implementar sobre todo para los usuarios no técnicos. Jeff Houston en APNIC nos muestra que aproximadamente el 21% de los usuarios del mundo utilizan algunos resolutores recursivos públicos bastante conocidos. Próxima diapositiva, por favor.

Si observan cualquier contenido de streaming verán que hay anuncios para servicios de VPN y esos están diseñados para aumentar la privacidad y la anonimización de los usuarios, pero también dejan muy en claro que brindan un medio para pasar restricciones geográficas o eludirlas.

Si estamos viajando y queremos ver videos que solamente están disponibles en nuestro país de origen, se puede instalar un VPN y ahora el contenido que está geolocalizado está disponible. Otro ejemplo común es que si queremos ver contenido que no está disponible en nuestro país se puede instalar un VPN, es como si estuviéramos localizados en otro país para acceder a este contenido.

Esto significa que si hay bloqueos de DNS o filtros de DNS donde nos ubicamos se puede instalar una VPN y eludir esto. Esto es cada vez más fácil de hacer, hay anuncios en casi todos los servicios de streaming o si estamos en línea también se brinda una VPN en cualquier equipo para los usuarios o cualquier teléfono inteligente, por ejemplo, el Apple Private Relay, es algo

muy simple de manejar y nos permite tener el dispositivo como si estuviéramos en otro lugar.

También tenemos servicios CloudFlare que brinda un servicio gratuito de VPN para aumentar la privacidad y también proveen un DNS alternativo. Relativo a esto tenemos servidores como Tor para que los periodistas puedan salir de forma segura de su país y puedan envolver sus datos de usuario en muchas capas de protección para que no quede tan claro quién es el usuario y dónde proviene, funciona muy bien, pero también es otra forma de eludir los filtros de DNS porque se puede utilizar resolutores que no están en nuestro país.

Otra cosa que tenemos que tener en cuenta es que tenemos cosas como la validación del DNSSEC que está diseñado especialmente para detectar y mitigar potencialmente a las personas que intentan modificar las respuestas del DNS, esto es lo que hace el bloqueo del DNS, cambia la respuesta del DNS por parte del servidor autoritativo.

Lo que estamos haciendo es que tenemos sistemas operativos y usuarios que tienen resolutorios de validación, hay varios distribuciones como Linux que vienen con resolutores de validación de DNSSEC y el bloqueo se aplica en una serie de resolutorios primarios de los usuarios y el DNSSEC va a detectar que algo malo está sucediendo, el resolutorio va a funcionar mal y el usuario va a poder utilizar el próximo resolutorio en la cadena si eso no tiene un filtro de DNS. Eso sería básicamente eludir el filtro.

El éxito o la eficacia del bloqueo del DNS tiene que ver con distintas medidas, por así decirlo, no es un mecanismo a prueba de todo y lo que hace es tratar de asegurar que unos usuarios específicos utilicen resolutores recursivos para bloquear su resolución, pero es relativamente fácil instalar un VPN, cambiar los resolutorios, etc.

El DNS ha sido una de las tecnologías que probablemente filtra la privacidad que más vimos en los últimos años, capacitamos a nuestros usuarios cada vez más para utilizar sitios HTTPS y datos encriptados, pero el DNS sigue filtrando a los usuarios.

Para poder mitigar esto el IETF y otros grupos están tratando de proteger al DNS, una forma de hacer esto es encriptar las búsquedas de DNS y las respuestas de DNS. Tenemos DNS mediante TLS, DNS mediante HTTPS y DNS mediante QUIC, pero las consultas y las respuestas de DNS están encriptadas, en general, no pueden extinguirse de cualquier otro dato de búsqueda o de internet, es decir, que los usuarios pueden actualizar su sistema de resolución para utilizar resolutorios recursivos en otros lugares que no va a ser detectable.

Es decir, que básicamente puede eludir el bloqueo, también existe el error extendido del DNS, este es el RFC8914 que ha sido redactado para resolver distintos casos de uso, uno tiene que ver con bloqueo de DNS y tradicionalmente el DNS no brinda información de error útil, si la resolución de dominio no funciona, en general, obtendríamos un dominio NX o una falla de servidor

que básicamente nos dice lo que salió mal, pero no es el caso.

Tenemos el código de error extendido 16 y si hay un nombre en la lista de bloqueo de DNS, el resolutor recursivo puede decir que este dominio no existe y lo digo porque esto puede estar en una lista de bloqueo a la que hemos optado, por ejemplo, si tenemos un filtro como 1.1.1.3 y alguien quiere ir a adult content, podría optar por este tipo de filtro.

Como dije, el bloqueo del DNS es una herramienta, tenemos que entender sus consecuencias, si hacemos un bloqueo en forma incorrecta puede haber consecuencias que no esperábamos, por ejemplo, si tratamos de bloquear un sitio como FOO.BAR.COM y accidentalmente bloqueamos todo el TLD .COM, eso no es algo bueno.

También puede haber daños colaterales si utilizamos la infraestructura incorrecta para hacer el bloqueo, si tratamos de bloquear un sitio web y nos damos cuenta de que se encuentra Akamai y colocamos los nombres de servidores de Akamai, esto va a bloquear todos los servicios que utiliza Akamai y esto puede ser un gran número de servicios. Les ruego que consulten el documento.

También hablamos sobre los distintos tipos de respuestas a los bloqueos, se puede intentar redireccionar al usuario a otro lugar o directamente no funcionar. Redireccionar al usuario a otro lugar es algo que vemos que los resolutores recursivos a veces se ven obligados a hacer y esto, creo que, es una de las opciones más

peligrosas en mi opinión.

Si alguien trata buscar FOO.BAR.COM, en general, los redirige a otro tipo de dirección IP donde está el servidor web. El peligro de hacer esto es que, por definición donde se redirige el nombre de dominio no va a tener un certificado de TLS, es decir, que el usuario va a recibir un mensaje de pop up diciendo que se pueden intentar robar su información si desea continuar.

Si el usuario accede, esto puede mitigar la seguridad, es decir, que hemos entrenado a los usuarios para utilizar solamente sitios HTTPS y no hacer clic en ningún otro sitio. Para respetar el tiempo asignado vamos a pasar directamente a las recomendaciones.

El documento contiene tres recomendaciones. Uno, si ustedes van a implementar un bloqueo de DNS asegúrense de entender cuáles son las implicaciones de todo esto, las fortalezas y debilidades de la herramienta y cómo hacerlo de una manera que no cause daño colateral.

La recomendación dos tiene subpuntos. Antes de hacer bloqueos de DNS se debe entender las implicaciones, debe haber también una política clara de qué bloquear, cuándo, potencialmente revisar las decisiones y, en todo caso, desbloquear.

Si se implementa el bloqueo de DNS se debe minimizar el daño colateral o el bloqueo excesivo, es decir, bloquear solamente lo necesario para eliminar el contenido y si se implementa un bloqueo de DNS solo se debe hacer a los cuatro usuarios que

están dentro del control.

Y si los operadores de DNS recursivos están retornando una respuesta bloqueada se debe utilizar esta extensión de errores para anotar y explicar por qué el acceso no pudo ocurrir, si se confunden y tratan de cambiar cosas aleatoriamente se puede cambiar el resolutor a uno que no sea confiable o que tenga una conexión de información y teníamos una diapositiva con un QR vinculado al documento, pero desapareció, solo tengo dos o tres minutos para preguntas. Adelante, si tienen preguntas.

JONATHAN ZUCK Estoy pensando en cuando iniciamos esta conversación en cuanto a lo que se refiere a cómo sacar la información hacia afuera, si la audiencia es la que opera desde servidores, ¿tendría sentido que nos concentremos en cosas que tienen implicaciones para el usuario o que puede generar cambios? Como usted planteó.

WARREN KUMARI Depende de a quién nos referimos, una de las audiencias principales para ALAC son las cuestiones como las empresas que obligan a los bloqueos, si usted tiene una empresa y está sugiriendo el bloqueo de DNS para garantizar que los empleados no accedan a Facebook estas son las cosas que se deben tener en cuenta para asegurarnos que la empresa utiliza el resolutor. Si se está haciendo el bloqueo, probablemente, no se debe re direccionar a los usuarios a otro lado porque los empleados

ignorarían las advertencias TLS.

Para las audiencias más globales apuntábamos a reguladores de gobiernos y a formuladores de políticas que pueden decidir crear censura o bloquear las marcas en el país y esto es lo que deben entonces tener en cuenta, son distintas audiencias para distintos conjuntos de personas, creo que, la de ALAC los usuarios tienen que entender que, si la resolución de DNS no funciona, tienen que ver qué es lo que lo causa y si se trata de un operador de ISP; que está obligado a hacer el bloqueo, anote las respuestas del bloqueo, ver qué es lo que los usuarios entienden, si es un ISP que también lo está haciendo voluntariamente se debe tener en cuenta que solo se debe bloquear lo que uno necesita.

RAM MOHAN Si puede ir a la diapositiva que está mencionando Warren, de entrenar a los usuarios a circunvalar la seguridad, creo que, hay un punto relevante aquí.

WARREN KUMARI Vamos a la siguiente. Si re direccionamos al usuario y vamos a FOO.BAR.COM, el resolutor nos da una dirección IP diferente y nos envía a una dirección IP que no está afiliado con BAR.COM o FOO.BAR.COM el servidor web que está en esa dirección IP no va a poder tener un certificado TLS para esa dirección web, los TLS están diseñados específicamente para prevenir este tipo de ataque, el usuario va a recibir un popup en su navegador y

posiblemente se va a confundir, y va a hacer clic en el mensaje.

RAM MOHAN ¿Es una experiencia normal que en muchos WiFi abiertos en aeropuertos que son públicos y que están en áreas públicas tengan cierto nivel de bloqueo o cosas que sucedan que también provoquen errores como este?

JONATHAN ZUCK Ciertamente esto ocurre en aviones.

WARREN KUMARI Cuando uno va a un hotel o a un café lo que trata de hacer es conectarse a su red y hay unos términos de servicios, o una política que uno tiene que aceptar haciendo clic, normalmente esto se hace cuando uno… Es decir, cuando uno se conecta ellos tienen sus propios resolutores recursivos y tratan de enviarlos a un sitio web que está bajo su control, que dice: “Ustedes están usando el WiFi de Starbucks, hagan clic aquí para aceptar la política”. Esto era un problema mucho más importante que está siendo mitigado estos días y que no es completamente efectivo.

En general, cuando mi teléfono o mi laptop se une a una nueva red de WiFi la red puede enviar una respuesta y decir: “Aquí es donde está el servidor web que uno debe contactar”, y para el dispositivo que se conecta, cuando abre este tipo de conexiones, aparece un sandbox. Esto sigue ocurriendo porque sigue habiendo portales cautivos, básicamente entonces lo que este

portal cautivo hace en este punto es básicamente un ataque de redirección de DNS que, potencialmente, es más razonable.

RAM MOHAN Sí, respondió.

JOHN LEVINE Voy a tratar de hacer esta pregunta breve. Las organizaciones en Estados Unidos, al menos, siempre han tenido recomendaciones de DNS y la nueva revisión es distinta de las anteriores, nos dice que configuremos el servidor para que la gente no lo pueda hackear, ahora se dice que las empresas tienen que usar DNS con un Firewall y quizás es malo para los usuarios. No están equivocados honestamente, lo que dicen ellos es distinto de lo que decimos nosotros y es que depende mucho del entorno, si tenemos una red en una empresa y estamos dando facilidades a los empleados, está bien para la empresa, y si ellos hacen difícil que entren a sitios web y compren cosas, ellos dicen que deberían hacerlo en su teléfono en el horario del almuerzo.

Por eso es importante entender que nuestro asesoramiento a los gobiernos es que van a bloquear cosas en el país y deben ser súper conservadores en ese sentido, en una organización el bloqueo tiene que coincidir con las leyes de la organización. Si entramos en el 9999 y hay un bloqueo, luego está 991010 donde también hay bloqueos esto no es amigable con la familia, tenemos que poder equilibrar el no bloquear porque hay cosas

buenas también que la gente debería poder ver y, por el otro lado, decir: “Ningún tipo de bloqueo hace que uno esté fuera de tono”.

WARREN KUMARI

La cuestión es si el usuario optó por el bloqueo, o no, si uno trabaja para una empresa y tienen restricciones sobre lo que uno puede hacer, uno portó por ese conjunto de restricciones. También en una empresa o en una red hogareña los dispositivos están gestionados, en un entorno corporativo si uno trae la laptop y la empresa nos ha obligado a un conjunto de resolutor y no lo podemos cambiar.

RAM MOHAN

Parece que hay tres preguntas.

LUTZ DONNERHACKE

Primero, gracias por el informe, gracias en el sentido de que esto lleva a la atención de los gobiernos al DNS y no a los métodos de bloqueo, no hacen un daño al acceso a los usuarios de internet como podrían y eso está muy bien, esto podría ser una forma intrusiva de implementar un bloqueo que está bien, lamentablemente en este momento la mayor parte de los resolutores recursivos no pueden hacer las denuncias, los reportes y esperamos que esto pueda ir cambiando a lo largo del año.

Gracias por no decir cómo hacer un verdadero bloqueo y espero

que nunca lo haga.

RAM MOHAN Robert.

ROBERT GUERRA Quería responder a la pregunta de Jonathan en cuanto al asesoramiento que hicimos en cuanto al bloqueo. Hay dos cuestiones, una para los formuladores de política, ya sea en Estados Unidos o en otros lados también, cada vez más el tipo de contenido que se desea bloquear o remover de internet ocurre de un modo que no es tranparente, entonces si se hace a través del bloqueo de DNS mi punto de vista; y creo que la de SSAC también, es que hay que ser transparente, si lo van a hacer, ¿cuáles son las consecuencias? ¿Cómo vamos a impactar en el sistema? Eso es parte del informe que hicimos, en la actualización, dado el uso de internet estas son las consecuencias si ustedes bloquean.

Para los usuarios Warren mencionó un portal cautivo y tenemos que saber cómo ocurre el bloqueo, y esto es un recurso educativo también, por eso es importante. Lo que se debe reconocer, especialmente en algunas partes del mundo, es que el contenido desaparece, por eso es muy importante que los usuarios puedan saber qué se debe hacer, si lo quieren acceder en otra herramienta, entonces es educativo, está escrito en un lenguaje que no es solo para expertos técnicos y se debe poder informar de las consecuencias colaterales, si vamos a bloquear, ¿cuáles son

los problemas y qué es lo que debe ocurrir para que haya un flujo libre de la información?

RAM MOHAN Matthias, ultimo comentario.

MATTHIAS HUDOBNIK Quería preguntarle a Warren si nos puede dar dos o tres puntos prácticos para los usuarios finales, ¿qué pueden hacer? Yo sé que depende del tipo de bloqueo y de la técnica del bloqueo, pero aquí no tenemos una audiencia técnica, ¿cuáles son dos o tres puntos que ustedes recomendarían o qué les parece que es significativo?

WARREN KUMARI Lo primero es decidir si queremos un bloqueo específico, si quieren que se bloquee el malware hay que actualizar el resolutor recursivo, pero si se trata de un usuario que está sujeto al bloqueo, que quiere evitar, lo que se puede hacer es actualizar el resolutor para que sea uno de los resolutores públicos o también se puede incluir una VPN y derivar el tráfico. Depende, de nuevo, de las leyes locales y de cuánto quiere uno hacer, con una VPN el tráfico puede aparecer en otro lado y si el tráfico pasa por la VPN se debe poder dar un tráfico confiable, pero el tráfico de la navegación también va a ser más lento, es decir, que hay que cambiar el resolutor y la VPN.

RAM MOHAN

Gracias. Vamos a nuestra próxima actualización, Maarten está aquí, él es uno de los presidentes del grupo de trabajo de software libre. Dentro de SSAC estamos trabajando en un informe, que todavía no está finalizado, pero tiene que ver con el software gratuito y de código abierto en la infraestructura de la registración de nombres de dominios, la motivación es que algunos de nosotros nos hemos dado cuenta que en los Procesos de Desarrollo de Políticas, en cuanto a regular el software o regular la infraestructura el uso del software de código abierto y gratuito, nos permitía saber que esto se usaba ampliamente y que, si bien buscábamos algunos sitios, veíamos que estaban libres.

Este documento trata de documentar el uso del software de código abierto y gratuito en el DNS y también documenta sus características, la idea entonces es que sea visible y que pueda resultar un recurso para los formuladores de políticas para que hagan políticas sin considerar esta influencia. Para quienes no están muy familiarizados con el software de código abierto y gratuito, este es el software que permite que toda persona lo pueda utilizar y también que pueda modificarlo y distribuirlo.

Esto termina estando muy alineado con la cultura de internet y para el software de DNS. Estamos investigando cuatro áreas en este informe, dos de ellas son actividades de investigación y otras dos tienen más que ver con el análisis y las consideraciones de política. Las primeras dos mapean el uso del software de código

abierto en la infraestructura, la primera es la infraestructura vinculada con los dominios, que la audiencia está muy familiarizada, y específicamente considera los registros. La segunda parte es el DNS, donde analizamos el uso de resolutores y nombres falsos.

La segunda parte es la encuesta de las características del software de código abierto, entonces, ¿cómo es diferente de lo físico? Porque, aparentemente, es muy diferente. Luego hicimos un contraste de este tipo de software a nivel general con el software de código abierto, que es muy abierto en el espacio de DNS. La tercera y la cuarta pretenden clarificar las suposiciones comunes que la gente hace al pensar en esto y poder aclarar que están equivocadas.

El cuarto es documentar los factores de riesgo que consideramos relevantes al hacer o regular la política, se aplica a los desarrolladores y a las operaciones de este software, y también a los procesos regulatorios. No les voy a dar aquí respuestas porque básicamente estoy presentando aquello con lo que estamos trabajando, pero van a tener una presentación completa en Muscat, que va a incluir algunas directrices.

De cara al futuro tenemos que seguir utilizando estas fortalezas, pero hay riesgos y vamos a expresar nuestro punto de vista sobre este tema. Esto es todo lo que diré, salvo que tengamos más tiempo y pueda entrar en cada uno de estos gráficos.

RAM MOHAN Vamos a hacer una pausa para las preguntas y vamos a tratar de continuar.

EUNICE PÉREZ Gracias, mi nombre es Eunice Pérez y voy a hablar en español. Mi pregunta es con respecto a este software, ¿funciona con cualquier sistema operativo o sobre cualquier sistema operativo?

MAARTEN AERTSEN Gracias, les pido disculpas por no saber cómo utilizar el dispositivo de traducción. Sí es para cualquier sistema operativo. Bien, la mayor parte del software está disponible para varios sistemas operativos, los operadores suelen utilizar ciertos sistemas operativos y este software está disponible para todos, así que, puedo decir que sí está disponible para todos, pero para los que lo usan en la práctica está personalizado para ellos.

En general, la mayoría analiza la capa superior, la aplicación que provee el sistema del DNS, pero nunca solemos ir más profundo, pero sí hay muchísimos datos al respecto. Gracias.

RAM MOHAN ¿Hay alguna otra pregunta? Bien, no escuchamos ninguna otra pregunta, entonces podemos seguir con el resto de nuestra presentación y si hay otra pregunta le podemos hacer la pregunta a Maarten o a cualquier orador que hizo su presentación. Pasemos

a la próxima diapositiva, por favor, o, mejor dicho, la próxima presentación.

Muchas gracias. El SSAC ha comenzado un grupo de trabajo que está analizando la integración responsable al ecosistema del DNS, ya sea los identificadores de Blockchain, entre otros, y el impacto que pueden tener en el ecosistema del DNS. Vemos en la diapositiva que estamos intentando hacer un trabajo de base sobre qué significa la integración y luego, ¿cuáles son los riesgos cuando probamos esas integraciones? Porque es de código abierto actualmente y hay distintos operadores que definen la integración a su manera.

En algunos casos están haciendo promesas o están afirmando ciertos tipos de comportamiento que pueden, o no, ser garantizados o algo que es entregable en una forma consistente, entonces un nombre de espacio no es un DNS y si uno quiere integrar ese nombre de espacio no DNS en el nombre de espacio DNS, bueno, tiene que haber una vinculación o alguna gestión entre uno y otro, y es probable que haya problemas.

Lo subyacente de esto lo hemos mencionado en varias plenarias y en otros foros dentro de la ICANN con anterioridad, lo fundamental es que, como toda tecnología, va evolucionando, los nombres de espacios evolucionan. Ese no es un problema, el problema es que si analizamos el nombre de espacio de dominios o el espacio de nombres de dominios a ciertas nomenclaturas y nombres que tienen un cierto comportamiento esperado y hay un

cierto nivel de confianza, y esto se ha establecido durante cierto tiempo.

Entonces si hay nuevos espacios vamos a tener que ver esta confianza e incluso si no es un resolutor del DNS lo llamamos “un nombre de dominio”, entonces se deben utilizar las palabras de otra forma porque tienen un significado y una confianza, los usuarios finales lo conocen, las empresas también. Uno de los riesgos es que cuando le damos otro significado no solamente a los nombres, sino también cuando tomamos partes de las funcionalidades, que sabemos que funcionan en el espacio de DNS, y lo asociamos a otras funcionalidades, que son únicas a otros espacios de nombres, ahí empezamos a establecer una base para una confusión finalmente.

¿Cuál es la identidad? ¿Cuál es el nombre de dominio? ¿Por qué esto no funciona en mi buscador? ¿Puedo mandarle un email o no? Todas las cosas y comportamientos que esperamos que funcionen en un nombre de espacio queremos asegurarnos de que esté claro, entre otras cosas, pero estamos en las etapas iniciales.

Actualmente, mientras tenemos este foco a largo plazo, en el corto plazo estamos muy concentrados en el impacto para la próxima ronda de nuevos gTLD, notamos que ya se ha publicado la guía para el solicitante y el SSAC publicó el análisis de la colisión de nombres con una serie de recomendaciones, vemos con beneplácito que estas recomendaciones han sido adoptadas

por la Junta y que la organización de la ICANN está implementando estas recomendaciones como parte de la próxima ronda, pero estamos intentando que se aplique nuestro marco analítico a la próxima ronda porque creemos que hay una posibilidad de que haya un daño para los usuarios, que tiene que ver con la colisión con sistemas de nombres alternativos.

Esto ya lo hemos abordado en nuestro informe anterior. En esto nos estamos concentrando, el grupo de trabajo tendrá una sesión que tendrá lugar en esta reunión de la ICANN y vamos a hablar con mayor profundidad de estos temas, aquellos que estén interesados, por favor, los invitamos a participar de estos debates en el SSAC. ¿Hay alguna pregunta?

JONATHAN ZUCK Tengo una pregunta breve. En primer lugar, la colisión de nombres es algo que importa muchísimo a la comunidad de At-Large, creo que, es una de las primeras colaboraciones entre nosotros que justamente nos ha llamado la atención, por así decirlo, cuando tenemos un… Es algo, como dije, que es importante para nosotros, ¿piensan que van a llegar a tiempo con una metodología recomendada al respecto o va a ser algo con lo que tenemos que tener cuidado? Porque puede suceder esto y aquello, ¿o ya va a haber algo establecido? Porque hay algunas promesas sobre que se va a hacer una integración que va a fluir muy bien, que va a haber una evaluación por parte de la comunidad.

Me gustaría saber si va a haber algo establecido claramente, como el camino a seguir o no.

WARREN KUMARI

Un comentario personal. Creo que, lo primero que hay que tener en claro es que hay un plan en curso durante la primera ronda no había un proceso previo en el tiempo, entonces ahora queremos asegurarnos de que estamos preparados para cuando esto suceda, que todo el mundo entienda cuál es el proceso, cuáles son las políticas que van a implementarse y que todo el mundo esté informado, y que si hay múltiples aplicaciones que vienen de distintos proveedores de Blockchain, si hay alguna prioridad, si tenemos que tener en cuenta que hay un conjunto de usuarios existentes o si explícitamente tenemos que asegurarnos de que los procesos están comprendidos y que estamos preparados antes de tiempo.

RAM MOHAN

Creo que, es poco probable que digamos: “Esto está bien” o “esto está mal”, creo que, es mucho más probable que digamos: “Va a haber peligro”.

JONATHAN ZUCK

Sí porque la próxima ronda ya está muy cerca.

JUSTINE CHEW

Creo que, esto es algo muy interesante y, creo que, es algo

totalmente necesario, les puedo contar desde mi experiencia al haber participado en el foro de DNS APAC, que algunos han estado presentes, tuvimos expresiones claras de interés y de confidencia de que estos actores van a obtener los nombres que deseen, independientemente de cuáles sean las reglas. Esa es la conclusión que saqué de este foro y, creo que, esto es algo de muchísima preocupación, probablemente van a utilizar las bases que ya hayan utilizado de esa cadena de caracteres en ese espacio de nombres como base para obtener su cadena de caracteres, independientemente de lo que se aplique para esa cadena de caracteres.

Creo que, esto es algo que va surgiendo, incluso antes de que comience la ronda de solicitudes y que, creo que, la Junta Directiva tiene que tener en cuenta. Y las tácticas que estos actores de Web3 estén utilizando es que hay muchísima jerga que la gente no suele entender y, creo que, la Web2 tiene que aprender de la Web3.

Y mucha gente se pregunta, ¿qué es la Web2 y qué es la Web3? Hay muchas cosas que la Web3 prescribe, que no son muy prácticas para internet en su conjunto, nadie entiende muy bien de qué se trata, entonces, creo que, es de una gran preocupación este tema.

RAM MOHAN Sabemos que se nos está acabando el tiempo, que la próxima ronda está muy cerca y por eso el grupo de trabajo está

reorientando su foco para trabajar específicamente en la guía para el solicitante y en brindar asesoramiento específico, o al menos comentarios, que luego puedan ser considerados por la organización de la ICANN para revisar esta guía del solicitante, teniendo en cuenta los comentarios públicos.

Concluimos nuestro trabajo con la colisión de nombres y nos dimos cuenta de que esta parte era un elemento que estaba como pendiente. Próxima diapositiva, por favor.

Vayamos a la última parte del trabajo de nuestro grupo de trabajo, aquí tenemos algunas consideraciones operativas de DNSSEC, el tema fundamental que estamos tratando de resolver o abordar con este grupo de trabajo es que el DNSSEC, como saben, ha existido desde hace mucho tiempo, pero todavía tenemos que seguir trabajando en pos de su éxito y preguntarnos por qué no se utiliza más.

Identificar cuáles son los desafíos que existen y otras soluciones prácticas que tal vez deberían desarrollarse o que ya existen y que no se han comprendido correctamente, o lo suficiente. Este es el trabajo de alto nivel que estamos intentando hacer, este grupo de trabajo también se está reuniendo aquí en esta reunión de la ICANN, está en el cronograma de las reuniones y pueden también venir a participar de nuestros debates, escuchar nuestros debates.

Esto nos lleva a la próxima diapositiva. Jonathan, hablamos de esto en la última reunión y en las reuniones anteriores también…

Si podemos volver a la diapositiva anterior, por favor.

La campaña de ciberseguridad es algo que ya es parte del currículo, que se difunde en todos lados y esto es muy alentador, queríamos comenzar este diálogo y seguirlo a futuro, y que este espacio de ciberseguridad es algo muy importante, estamos pensando que puede haber una variedad de temas en los que podríamos trabajar y queremos abrir esto a debate justamente aquí en la sala y en línea las cosas que les parecen pertinentes, interesantes, oportunas para sus audiencias.

Para los dos primeros temas tenemos un par de documentos redactados que no están destinados directamente a los usuarios finales, pero que pueden ser muy interesantes para ellos, SAC40 y SAC115 son documentos de donde se puede derivar material para estos dos primeros temas propuestos, pero hay otros documentos redactados, que son informes sólidos que podrían aprovecharse.

Entonces lo dejo como un tema abierto a discusión, de cuáles son los temas que les interesan y cómo podemos, tal vez, avanzar aún más.

JONATHAN ZUCK

La primera reacción es positiva, estos grupos de ACES que Amrita preside, creo que, va a ser el conducto para estos debates o estas conversaciones y tenemos algunos espías de SSAC que pueden colaborar con estos temas, me parece que es muy interesante poder obtener esta información, construir estas alianzas con las

ALS, con las bibliotecas, creo que, no hay motivo para que esto no sea información que circule por todos estos canales y poder ver cómo difundir esta información, podemos enviar algunas animaciones o encontrar financiación y ver cómo podemos hacer para difundir esta información, ver también el programa de subvenciones como mecanismo para que el trabajo increíble que el SSAC está haciendo poder redistribuirlo, por así decirlo, en forma más accesible.

Tenemos que tener esta conversación, que no podemos tener ahora en estos dos minutos que nos quedan, pero que, creo que, es una excelente idea. No sé si hay preguntas o comentarios al respecto, ¿alguno de nuestros participantes en línea? Me parece que ya nos estamos quedando sin tiempo. Bien, la verdad pasamos un muy buen momento aquí entre los miembros de ALAC y SSAC, pero nos quedamos sin tiempo.

Me gustaría mucho que organicemos una especie de retiro, por así decirlo, donde tengamos tres días para poder hablar sobre esto en detalle para ver cómo podemos hacer que los usuarios estén más seguros en línea, bueno, vamos a analizar todas estas propuestas a ver cuáles son los presupuestos disponibles, pero, una vez más, muchas gracias por estar aquí con nosotros, siempre disfrutamos de su compañía, siempre aprendemos mucho, así que, como dijimos, sigamos esta comunicación entre las distintas sesiones, que siempre funciona tan bien. Muchísimas gracias.

[FIN DE LA TRANSCRIPCIÓN]