ICANN69 | Reunión general anual virtual – Cambios del WHOIS bajo el GDPR: impacto en los usuarios finales y la seguridad pública
Miércoles, 21 de octubre de 2020 - 10:30 a 12:00 CEST

OZAN SAHIN: Vamos a comenzar con la sesión. Hola y bienvenidos a la sesión: Cambios de WHOIS en virtud de GDPR: Impacto sobre los usuarios finales y la seguridad pública. Yo soy Ozan Sahin. Soy gerente de participación remota para esta sesión. Por favor, tengan en cuenta que esta sesión está siendo grabada y cumple con los estándares de comportamiento esperado de la ICANN. Durante esta sesión, las preguntas y los comentarios solo podrán darse en voz alta si se presentan en inglés en el espacio de preguntas y respuestas. Se puede acceder a esta funcionalidad en la barra de herramientas de Zoom. Yo leeré las preguntas y comentarios durante el tiempo asignado por el moderador para este tema.

La sesión incluye transcripción en tiempo real e interpretación simultánea. Para acceder a la transcripción, por favor, haga clic en la tecla de subtitulado que está en la barra de herramientas de Zoom. La interpretación para esta sesión incluye árabe, chino, inglés, francés, ruso y español. Se llevará a cabo utilizando tanto Zoom como la plataforma de interpretación simultánea remota operada por Congress Rental Network. Los participantes podrán descargar la aplicación de CRN de acuerdo con las instrucciones que figuran en el

chat de Zoom o en el documento con los detalles de la reunión que está disponible en el sitio web de la reunión.

Si desean hablar, por favor, levanten la mano en la sala de Zoom y una vez que el facilitador de la sesión lo llame por su nombre, nuestro equipo de apoyo técnico le permitirá habilitar el audio de su micrófono. Por favor, diga su nombre para los registros y el idioma en el que va a hablar si es que no va a hablar en inglés. Al hablar, por favor, silencie todos los demás dispositivos, incluida la aplicación de Congress Rental Network. Por favor, hable claramente y a una velocidad razonable para permitir una correcta interpretación. Quisiera subrayar el hecho de que los participantes remotos no pueden hacer clic en la tecla del micrófono y habilitar su propio audio durante esta reunión sin asistencia del equipo de apoyo técnico.

Para todos los participantes de la sesión, podrán hacer comentarios en la ventana de chat. Para ello, por favor, utilicen el menú desplegable que está en el espacio de chat y elijan “Responder a todos los panelistas y participantes”. Esto permitirá que todos puedan leer sus comentarios. Tengan en cuenta que los chats privados solo son posibles entre los panelistas en el formato de webinar. Cualquier mensaje enviado a un panelista o de un participante a otro participante también será visto por los anfitriones, coanfitriones de la sesión y otros panelistas. Habiendo dicho esto, le voy a dar la palabra a Jonathan Zuck.

JONATHAN ZUCK: Muchas gracias. Soy Jonathan Zuck, vicepresidente del comité asesor At-Large. Tal como muchos de ustedes saben, At-Large está encargado de ocuparse del uso indebido de DNS y de otros temas relacionados como tema de campaña del año. Creo que muchas de estas conversaciones han sido bastante repetitivas y no nos han llevado a ningún lugar específico. En parte se debe a la falta de datos. Hay muchas conversaciones en todas partes que hacen que un debate racional sobre este tema sea bastante complejo y difícil.

Con frecuencia hemos visto dentro del contexto de la ICANN que a veces se hacen predicciones en el fragor de la batalla acerca de una nueva política y que finalmente no se cumplen y ocurre otro resultado. Por ejemplo, cuando se propuso el programa de nuevo gTLD, alguien sugirió que Sony iba a invertir 12 millones de dólares en registraciones defensivas. Finalmente, no hicieron esto. Encontraron otra forma de proteger sus marcas comerciales en los gTLD.

Lo mismo ocurrió con el cumplimiento del GDPR y el llamado que despertó a toda la comunidad de la ICANN. Esto llevó a la implementación de la especificación temporaria, a la formación de un grupo de trabajo EPDP para ver cómo la ICANN iba a cumplir con la reglamentación del GDPR. En consecuencia, se produjo un cambio significativo en los datos disponibles para el público en el sistema de WHOIS. Se implementó una nueva clase de sistema en el que la gente tenía que solicitarle información a las partes contratadas.

Durante el curso del proceso del EPDP para bien o para mal se llevaron a cabo distintos pasos por parte de los que solicitaban los datos y los

encargados de gestionar los datos. Hubo diferentes opiniones en este debate. La idea de esta plenaria es reunir a todas las partes y hablar acerca de lo que realmente está pasando en este periodo intermedio. Es decir, cuáles son las solicitudes de datos que se están haciendo, cómo se las está manejando. Con frecuencia nos sorprende el hecho de que las cantidades son menores de lo que pensamos. No hubo tantas solicitudes. No hubo tantos pedidos. Empezar desde el punto de partida, desde los hechos nos parece que es un buen lugar para empezar a hablar acerca de los datos de los registratarios, del uso indebido. Podría ocurrir que las partes que en un principio estaban preocupadas acerca del acceso a los datos de los registratarios encontraron formas alternativas de acceder a esa información para poder hacer cumplir con los derechos de marcas comerciales, para el cumplimiento de la ley, protección de los consumidores. El objetivo entonces es entender dónde estamos hoy, un par de años después en términos de esos datos, la necesidad de la disponibilidad, la eficiencia con la que se puede acceder a los datos a través de las partes contratadas, etc.

Ese es el tipo de debate que esperamos tener en esta plenaria. El objetivo es ver cuáles son los hechos, en qué punto estamos hoy. Esperamos poder tener un debate ideológico mínimo y maximizar nuestro intercambio de ideas acerca de datos y hechos relacionados con el statu quo.

Para comenzar con la conversación vamos a hablar y obtener la perspectiva de una de las comunidades de los solicitantes, por así

llamarla, que son los organismos de cumplimiento de la ley y protección de los consumidores. Le voy a dar 10 minutos a Laureen Kapin, del FTC, de la Comisión Federal de Comercio, y a Gabriel Andrews, quien va a hablar acerca de la perspectiva de los organismos de cumplimiento de la ley, alternativas, cuál ha sido el proceso a lo largo de los últimos dos años. Laureen y Gabriel van a ocuparse de este tema. Laureen, le doy la palabra. Debe habilitar su audio.

LAUREEN KAPIN: Es demasiado temprano para mí. Bienvenidos a todos los que están en una hora difícil del día. Soy Laureen Kapin y estoy aquí para darles la perspectiva del usuario final acerca de cómo el público usa WHOIS. Pasemos a la próxima diapositiva, por favor. Yo soy abogada de la Comisión Federal de Comercio. Estoy en la oficina de asuntos internacionales y protección del consumidor. Me dedico a estos temas al igual que mi agencia desde hace muchos años. De todas formas, mis comentarios son propios y no reflejan la posición oficial de la FTC. Voy a hablar en mi propio nombre como abogada que trabaja en la Comisión Federal de Comercio. Es mi perspectiva personal.

La Comisión Federal de Comercio cuenta con un recurso fantástico al que pueden recurrir los consumidores y el público, no solamente en Estados Unidos sino en todo el mundo. Pueden presentar algún reclamo cuando han sido víctimas o cuando les preocupa alguna práctica engañosa, fraude, spam. Se llama la base de datos centinela de consumidores. Esta base de datos recopila cientos de miles de reclamos todos los años. Ha recibido datos de contribuyentes de todo

el mundo. No resulta sorprendente entonces saber que cuando analizamos esos reclamos podemos tener una especie de instantánea de cómo el público que se conecta online para comprar cosas, para reunirse con gente, para acceder a información, cómo este público usa WHOIS. Las referencias a WHOIS están incluidas en esos reclamos.

Lo que yo hice fue analizar una parte de estos reclamos, especialmente después de los cambios realizados en el sistema WHOIS. Cuando hablo de cambios, me refiero a los cambios que afectan a la información especialmente a la información de contacto del registratario. Lo que encontré es lo siguiente. Los usuarios finales usan WHOIS con diferentes fines. Básicamente buscan un índice de confiabilidad. Quieren ver los registros de WHOIS para hacer diligencia debida y seguimiento de conductas sospechosas o maliciosas. Quieren ver quién es responsable. A veces quieren tratar de contactar a esas personas. A veces, a partir de leer estos reclamos, he visto que investigan algunas cosas. Tratan de entender y de ver si lo que les están haciendo es un engaño o no. Ingresan para analizar datos acerca del dominio del que están recibiendo información.

Los consumidores observaron a través de estos cambios de WHOIS que hay información que falta o que está oculta en los registros. Quizá supongan que la empresa no es honesta porque falta información. Ese supuesto puede ser correcto o no. Dicho sea de paso, la FTC recibe estos reclamos. No los verifica. Simplemente los recibe y los utiliza como datos.

La gente observó que a veces faltan algunos detalles y que eso interfiere con su proyecto de diligencia debida. Por ejemplo, hay alguien que dijo que no había datos sobre una empresa de servicios públicos. Podrán ver aquí las palabras, los términos que utilizan las diferentes personas. Esos son términos que yo encontré incluidos en los reclamos que analicé.

Esto les da una idea porque tengo poco tiempo para hablar. En la próxima diapositiva podrán entender el tipo de ideas para las cuales la gente utiliza WHOIS. Productos falsificados, scam de mascotas. No se imaginarán cuántos hay con respecto a las mascotas. Engaños para mascotas, virus, phishing, engaños con respecto a información publicada por el gobierno. Toda una gran variedad de cosas.

Quiero resaltar también el hecho de que la gente no utiliza solamente esa información que está en los registros de WHOIS. Tenemos la suerte de que la información de WHOIS también sea información útil y que nos sirva para saber dónde se creó y cuándo se creó cierto tipo de información. Esto es para que tengan una idea de la forma en la que los usuarios finales utilizan los datos de WHOIS para protegerse. Hay cierta frustración que se observa en estos reclamos con respecto a que hay cierta información que no está disponible con este fin. Le voy a dar la palabra a mi colega ahora.

GABRIEL ANDREWS: La siguiente diapositiva, por favor. Yo hablo en nombre propio. Quiero decir que es difícil obtener información acerca de los organismos de

cumplimiento de la ley en relación con este tema. Aquí reunimos varios temas, ya sea GDPR o la ley de privacidad para el consumidor de California o los servicios de privacidad y representación. En última instancia, lo que nos importa como organismos de cumplimiento de la ley es que no se pueda acceder a los datos. Estamos hablando de todo esto. La próxima diapositiva, por favor.

Quisiera hablar acerca de cuánto tiempo lleva acceder a los datos. Hay diferentes duraciones, hay diferentes plazos dependiendo de las circunstancias. Antes uno podía hacer una búsqueda en una fuente pública y obtener información sobre los registratarios en 10 segundos. Esto es lo que se hacía y se lograba últimamente pero en general hay muchos que ni siquiera tienen en cuenta que hace falta acceder a un registrador para acceder a estos datos. Si no existe un servicio de privacidad y de representación, y si saben que pueden acceder, las respuestas han sido muy variadas. Algunos registradores van a responder directamente a una solicitud de un organismo de cumplimiento de la ley y van a dar la información oculta y esto lo agradecemos. Algunos solo van a responder frente a organismos locales que están en el mismo lugar donde está el organismo de cumplimiento de la ley. Algunos van a pedir algún tipo de proceso legal. A los fines de los intérpretes, cuando hablo de proceso legal me refiero a una orden judicial, ese tipo de cosas.

El plazo en este caso aumenta como cabe esperar. Si un registrador pide algo, quizá ya no sean 10 segundos sino horas, días. Si hablamos de un proceso judicial estamos hablando de días a dos semanas en

promedio. Esto es lo que cabe esperar para obtener y recibir una respuesta cuando hay un proceso judicial en curso. Si no estamos en la misma jurisdicción y pedimos un proceso judicial, en ese caso probablemente no tengamos suerte. Si no somos firmantes del tratado de asistencia legal mutua podemos presentar una solicitud y obtener datos en seis meses. La próxima diapositiva, por favor.

Cuando hablamos de impacto quiero hablar acerca de uno de los procesos que más se han visto afectados o una de las responsabilidades que tenemos que más se han visto afectadas que es la notificación de las víctimas. Aquí vemos un ejemplo de un email empresarial que se vio afectado. Esto es lo que más ocurre en Internet hoy en día. Tenemos 23.000 millones de dólares estimados como pérdidas debido a esto el año pasado. Los números parecerían duplicarse cada año. No me sorprendería llegar a los 30.000 millones este año. En este ejemplo vemos que el mal actor se hace pasar por el CEO, ceo@example.com. Este es un dominio que se hace pasar por otro y que apunta específicamente a una víctima. Esta persona crea una cuenta de correo electrónico y se hace pasar por otra persona. Así es como funcionan estas cosas. Nosotros como investigadores antes hacíamos una búsqueda reversa de DNS para acceder al registratario de ese dominio malo y ver si registró otros dominios. Probablemente podamos deducir a partir de eso quiénes fueron porque todos esos dominios se parecen. Si esto se puede hacer rápidamente, si podemos actuar muy rápidamente, quizá podamos hacer otras consultas de DNS de las víctimas. Si tengo información de contacto, les aviso que en ese

momento hay malos actores que están apuntando directamente a ellos.

Aun si es una demora muy pequeña, lleva tiempo esa búsqueda porque se llevan a cabo múltiples búsquedas en ese proceso y esto afecta negativamente la capacidad para llevar a cabo esas notificaciones de forma tal que creo que a veces no llegan a hacerse, no porque no lo intentemos sino porque el primer paso que es obtener todos estos dominios potenciales requiere ciertos pasos jurídicos que llevan días o semanas. Yo quiero subrayar que esto es lo que ocurre en el mundo real. Hay demoras relativamente pequeñas que van desde segundos hasta días o semanas. Esto tiene consecuencias muy importantes. El tiempo es muy valioso. Voy a pasar al próximo panelista.

JONATHAN ZUCK: Gracias, Gabriel. Ahora le vamos a dar la palabra al Centro de Investigación en Ciberseguridad, a Greg Aaron y Lyman Chapin. Les damos la palabra.

GREG AARON: Hola. Buen día. La próxima diapositiva, por favor. Bien. Lyman y yo recientemente hicimos investigaciones sobre el tema de phishing para tratar de capturar información sobre cuánto phishing hay, dónde se está dando, etc.

Los intérpretes pedimos disculpas pero no estamos recibiendo al orador. Tenemos un problema de sonido. Les pedimos disculpas. No se escucha al orador.

Los intérpretes pedimos disculpas pero se cortó la transmisión del lado del orador.

Google, por ejemplo, está interesado en estas mediciones porque ellos pueden ver cuánto phishing están bloqueando en sus navegadores con Chrome. Es una medición interesante. Esta diapositiva del programa de browsing seguro y en rojo ven la cantidad de sitios de phishing que bloquearon. Es interesante porque tienen este método que utilizan desde hace bastante tiempo. Ven que el phishing está subiendo. Al mismo tiempo, el malware ha estado cayendo. No necesariamente es algo extraño esto. La cantidad de ciberdelitos y hacia dónde tienden a desplazarse y cómo cambian con el tiempo. Malware está bajando porque hubo algunos botnets que fueron dados de baja y porque los delincuentes están menos interesados en utilizar malware bancario. Han pasado otros tipos de delito como por ejemplo el compromiso de emails corporativos que ya se describieron. Cuando tratamos de entender la cantidad de ciberdelitos que se dan, hay que ver qué medimos y cómo lo medimos. También tenemos que ver el panorama general. Si no miden algunas cosas, no se van a enterar de que existen. La próxima diapositiva, por favor.

Qué vamos a hacer, para qué necesitamos la información de WHOIS. Necesitamos esta información porque queremos averiguar cuando se registra un nombre de dominio y los registradores con los que se

registró, esa es la información que no es información sensible. La fecha no es tan importante. Uno de los problemas que encontramos es el Rate Limiting, la limitación de la cantidad de solicitudes que se pueden procesar. Los registros y registradores solo permiten un cierto número de consultas dentro de un periodo determinado. Tenemos un documento publicado por SSAC. Esto nos impide obtener la información no sensible que nos permitiría saber y detectar más ataques de phishing.

Las personas además que están tratando de luchar contra estos problemas buscaban la información de contacto en el registro de registración. Esto era importante porque los delincuentes con frecuencia, como imaginamos, falsifican su información. No dan información de contacto precisa y es posible verificar todo esto. Si no es precisa la información, podemos decir que hay mala fe por parte del registratario. Además, también nos permite ver si una cierta parte ha registrado más de un nombre de dominio. Se puede buscar esto y comparar la información también.

Esto ya no es tan útil en la actualidad en el mundo post-GDPR. Lo que vimos en nuestro informe confirma algo que ya sabemos desde hace mucho tiempo. Cuando los delincuentes registran un dominio, en general registran varios al mismo tiempo. En general esos lotes o esa enorme cantidad de dominios no se detectan. A veces vemos largas secuencias de nombres de dominio y algunos se detectaron y se pusieron en la lista negra pero hay otros que no se encontraron, no se detectaron. La próxima diapositiva, por favor.

Lo que también analizamos es cuánto dura un ataque de phishing. Estos son datos muy interesantes preparados por un grupo que trabaja en PayPal, Google y en la Universidad Estatal de Arizona. Fue realmente un estudio muy interesante que se hizo este año. Estas empresas pueden ver dónde se hace clic. Pueden hacer un seguimiento desde la primera vista en un sitio de phishing específico hasta la última visita y después, si hubo phishing que involucró a PayPal, PayPal puede ver cómo se atacó a las personas y cuánto dinero perdieron de sus cuentas, etc. Estos datos confirman los datos de otros estudios que realicé yo pero vemos que los ataques de phishing son de corta duración. En el momento en que se recibe la primera visita hasta que se detecta el phishing pasan ocho horas aproximadamente. Un ataque de phishing en general tiene como duración 17 o 18 horas. En cuanto se detecta un ataque de phishing, la mayoría del daño ya se causó. La mayor parte de las víctimas ya fueron al sitio y aquellos que pierden dinero por este fraude ya fueron víctimas del fraude. La próxima diapositiva, por favor.

Otra cosa que encontramos es que el 60% de los dominios utilizados en ataques de phishing fueron registrados por los que realizan el phishing. Estos dominios están en dos categorías. Número uno, utilizan nombres de dominios específicos para lanzar sus sitios. Los phishers también utilizan nombres de dominio en los cuales entraron en forma ilegal a través del hosting. Hacen phishing a través del nombre de dominio de un tercero. Lo que queremos hacer como respuesta es lograr que estos sitios sean dados de baja por el proveedor de hosting, que se mantenga el resto del contenido y se

eviten daños colaterales para ese registratario. Sin embargo, los nombres de dominio que son registrados por los delincuentes o phishers pueden ser dados de baja directamente sin ningún otro daño colateral.

Hemos visto a través de nuestra metodología que el 60% de los nombres de dominio entran en esta categoría de registros maliciosos. Un estudio de SIDN y de AFNIC, que son los operadores de registros .NL y .FR, crearon un sistema independiente que se superpone un poco en cuanto a sus metodologías pero crearon un sistema muy elaborado y encontraron que esta cifra es del 57%. Los porcentajes se parecen bastante y también hicieron un muy buen trabajo que creo que es sumamente interesante. La próxima diapositiva, por favor.

Podríamos decir que algunos de los mensajes clave serían los siguientes. Lo que estamos viendo es que gran parte de estas registraciones son difíciles de encontrar en la actualidad. Uno de los motivos es que no tenemos algunos de los datos que antes estaban disponibles y esto obviamente es una conclusión clara, obvia. A veces los datos de contacto no distinguen un nombre de dominio de otro y esto indica que hay mala fe. Además, obviamente, saber quién registró o quién se supone que registró un sitio también es una información sumamente importante.

La buena noticia, si es que hay una buena noticia, es que los registradores y los operadores de registro todavía tienen acceso a esos datos. Ellos sí pueden ver esos datos aunque todos los demás no los puedan ver. Debido a que gran parte de las actividades de phishing son

los phishers, los que registran estos nombres de dominio, aquí hay una oportunidad para los registradores y los operadores de registros para que aprovechen estos datos. Podemos ver que hay actividades de phishing continuas, una y otra vez en ciertos TLD y en ciertos registradores.

En cuanto al EPDP, uno de los resultados fue que ahora tenemos un tiempo máximo para responder una solicitud de datos. Las solicitudes de ciberseguridad en el caso de phishing, por ejemplo, eso se establece en el GDPR. Estos plazos se establecen en el GDPR y hay que presentar por supuesto un interés legítimo para solicitar estos datos. Sin embargo, estos cinco días de plazo, que quizá pasen a 10, en general no van a ser efectivos porque los ataques de phishing duran menos de un día. Estamos viendo que los datos a través del sistema SSAD, sistema estandarizado de acceso y divulgación, quizá lleguen en forma rápida o lenta. Si llegan en forma lenta, esto no nos va a ayudar a resolver el problema.

El phishing es un candidato excelente, es un caso de prueba excelente para probar la automatización. El equipo de implementación deberá analizar esto y si se puede automatizar entonces el sistema de SSAD realmente podría darnos información útil para responder a los ataques de phishing y reducir los daños a las víctimas. Muchísimas gracias.

JONATHAN ZUCK: Gracias, Greg. Supongo que Mark no está aquí todavía. Mark no se incorporó a esta sesión. ¿Es así? ¿Me puede confirmar esto, por favor, Greg?

ORADOR DESCONOCIDO: Es correcto.

JONATHAN ZUCK: Entonces avanzamos y le damos la palabra a Milton para poder llegar después a la sesión de preguntas y respuestas, que creo que va a ser muy interesante. Sigamos entonces con las presentaciones y después vamos a las preguntas y respuestas. Milton, le damos la palabra.

MILTON MUELLER: Hola a todos. Soy Milton Mueller. Soy profesor en los Estados Unidos. Quiero decirles que todos los que estamos en este panel somos de los Estados Unidos. ¿No es interesante esto? De hecho, el debate sobre WHOIS ha sido un debate que se centró básicamente en estas diferencias entre Europa y los Estados Unidos en cuanto a las leyes de privacidad. La próxima diapositiva, por favor.

Algo que todavía no se mencionó mucho es por qué estoy en este panel. En realidad estoy hablando de los derechos y los intereses de los registratarios. Las personas que registran un nombre de dominio. No debería ser demasiado difícil entender por qué las personas que registran los dominios están interesados en todo esto y están interesados en expurgar cierta información personal sensible. Según

muchas leyes de privacidad, tienen el derecho legal y además el interés de proteger esos datos. De hecho, nuestra Comisión Federal de Comercio para la cual trabaja Laureen, tiene mucha información. Hay cierta información como la dirección de correo electrónico, la información de identificación personal y el número de teléfono. No deberían estar disponibles en línea, donde pueden ser copiados y utilizados por todo el mundo.

Nosotros con la aplicación del GDPR y WHOIS, el objetivo es utilizar esa idea de sentido común de que los delincuentes y los que hacen un uso indebido pueden usar de manera indebida la información e identificación personal disponible y que no es buena idea tener toda la información personal disponible para todo el mundo en Internet. A pesar de esto, en el sistema WHOIS todavía hay mucha información: el nombre del registratario, su país, en algunos casos incluso el estado y la ciudad. Esperamos que podamos crear métodos eficientes para divulgar datos expurgados de manera más rápida.

Es curioso pensar por qué en At-Large no se han interesado tanto en los derechos de los registratarios de los nombres de dominio. Supongo que representan a los usuarios y por lo tanto quisiera saber en realidad cuál es la posición de las estructuras de At-Large de Europa con respecto a esto porque no escuchamos que apoyaran el tema de los reclamos en relación al GDPR. ALAC no dijo nada al respecto durante el proceso de EPDP. La próxima diapositiva, por favor.

Realmente me gustó la introducción que hizo Jonathan cuando presentó este panel. La pregunta es si podemos hablar de hechos. No

es fácil encontrar información concluyente sobre lo que sucedió pero debemos tener en cuenta que no estamos hablando de si el phishing es malo o cómo funciona. Estamos hablando más bien de qué pasaba con esto, cómo funcionaba esto antes y después de la expurgación de datos por el tema de que estamos cumpliendo ahora con el GDPR. Si nos fijamos en las estadísticas de Google que mostró Greg antes y vemos un periodo de 18 meses antes de que se empezaran a aceptar las ediciones de datos y vemos qué pasó después de que se implementaran estas posibilidades de expurgación, vemos que en el caso del malware los números cayeron antes y después a pesar de que la caída posterior obviamente fue más marcada.

Si vemos lo que pasó en términos de phishing podemos ver un aumento muy importante tanto antes como después de la implementación de la posibilidad de expurgar los datos. También vimos los datos de spam a pesar de que es difícil encontrar datos de spam a largo plazo. Otra vez no vemos ninguna relación entre la expurgación de los datos en 2018 y el tamaño y el alcance del problema. Es imposible establecer una correlación estadística entre la expurgación, edición de datos y cambios en los comportamientos y en los problemas.

En base a estos datos, si hablamos de expurgación por un lado y el problema de ciberdelito, la relación es muy débil y no es que la expurgación no ayude claramente en algunos casos para los organismos de seguridad que deben tener acceso rápido a los datos. Esto les ayuda pero además el acceso rápido también es un vector

importante que causa el problema pero además también cada vez hay más phishing y registraciones abusivas. Los delincuentes aprendieron a falsificar la información. Han encontrado formas muy inteligentes de utilizar referencias cruzadas y dar información falsa sobre sus identidades sin que se los detecte fácilmente, sin que los detecten los que están analizando los datos de WHOIS.

Finalmente, con respecto al problema de phishing, quisiera decir que cuando doy clases sobre ciberdelincuencia hacemos un ejercicio en el cual hay grupos de cinco alumnos que preparan un mail con phishing, lo mandan a los instructores y se fijan qué sucede. Lo que encontraron los alumnos es que los dominios de phishing en general son detectados por diferentes algoritmos de empresas de hosting, de empresas de servicios web, los fabricantes de navegadores, utilizando información con respecto a la velocidad en la que se registra un dominio, el uso de ciertas cadenas de caracteres y los alumnos descubrieron que su dominio de phishing fue bloqueado incluso antes de que pudieran terminar su actividad y presentármela a mí como profesor. La próxima diapositiva, por favor.

Una vez más, no es que no tengamos acceso a la información. Sí, claramente tenemos en este nuevo proceso de políticas un método centralizado y estandarizado para presentar las solicitudes de información. No podemos ignorar esto. Estamos hablando de cumplimiento aquí, cumplimiento contractual. Esto no es opcional, señoras y señores. Debemos cumplir con la ley. Lo que hicimos a través de un gran trabajo en el EPDP es encontrar un mecanismo de

divulgación de la información que cumpla con el GDPR. Es decir, muchas solicitudes simplemente deberán ser reanalizadas para definir si hay un interés legítimo y si el solicitante es legítimo, etc. Aquí termina mi presentación. Espero ansiosamente un intercambio de ideas muy interesante con el resto de los panelistas y con el público. Gracias.

JONATHAN ZUCK: Quiero repetir algo que dijo el orador anterior. Esto es algo que pasó y que tiene que ver con el cumplimiento de la ley. Cuando hablemos de este temo creo que tenemos que considerar cómo es el mundo en virtud de esta ley y no repetir si la ley fue buena o no sino, por el contrario, ver cuál es la relación con respecto al flujo de datos entre los solicitantes y los que conservan los datos. Esa es la idea. No volver a hablar nuevamente acerca del PDP y de lo que ocurrió hace dos años sino simplemente ver cómo han sido los procesos desde entonces y cómo es esa relación hoy en día.

Para hablar sobre este tema creo que Owen es el orador ideal ya que preparó un informe sobre solicitudes recientes de datos. No recuerdo cuándo fue. Hubo un seminario web sobre este tema. Owen va a hablar sobre este tema y nos va a dar un poco de información sobre este tema. Se va a referir a este tema desde el punto de vista de los que tienen los datos y cómo han cambiado las cosas desde la implementación de las especificaciones y cómo han sido los últimos dos años. Owen, le doy la palabra.

OWEN SMIGELSKI: Gracias, Jonathan. No sé si estoy en pantalla. ¿Ustedes me ven? No puedo ver si mi video funciona.

JONATHAN ZUCK: Sí, lo vemos.

OWEN SMIGELSKI: Perfecto entonces. Antes me veía pero ahora no me estoy viendo. La próxima diapositiva, por favor. Soy Owen Smigelski. Trabajo en el equipo de registradores y también en el grupo de partes interesadas de registradores. Voy a hablar acerca de un trabajo que llevaron a cabo los registros y registradores en septiembre. Aquí tienen el vínculo a la presentación, al seminario web y también a las grabaciones que están en el calendario de la GNSO. Puse el vínculo aquí para que todos lo puedan ver. Los aliento a que accedan, a que revisen esta información. Hay mucha información. Yo participé en ese seminario web junto con otros tres colegas que incluyen información sobre la que yo no voy a hablar. Alan Woods, de Donuts, de los registros; Beth Bacon, de PIR, y Sarah Wild, del registrador Tucows. Quiero agradecerles por la información y el material que nos suministraron. La próxima diapositiva entonces.

Cuando hablamos de este tema tenemos que tener en cuenta que el GDPR y la protección de datos no es algo nuevo. Todo esto se remonta a fines de la Segunda Guerra Mundial. En ese periodo, la preocupación

era que la información personal de las personas fuera utilizada para identificar perfiles y actuar sobre diferentes estados y actores. Esto incluía nombres, religiones, etnicidad, factores de orientación sexual. En ese momento el interés era proteger los datos personales y la privacidad y era algo muy importante. Esto ha continuado hasta el día de hoy. Es por eso que la protección de datos y el titular de los datos y la protección del titular de los datos es algo tan importante. Es algo que no podemos dejar de lado. Esto se relaciona con los derechos universales. Hablamos de tratados, acuerdos. En Suecia, en 1963, ya fue incluido en una declaración universal. Luego en Europa, antes de la creación de la ICANN en 1998. La siguiente diapositiva, por favor.

Hay siete principios presentes en todas las leyes de protección de datos de Europa. Deberían leerse teniendo en cuenta que el beneficiario de la protección es el titular de los datos. No voy a entrar en detalle pero para acceder a esta información hay que tener un propósito limitado. No podemos acceder a más datos de los necesarios. Tenemos que asegurarnos de que tengamos los datos durante un periodo determinado, que trabajemos de forma segura y también tiene que haber responsabilidad con respecto a esos datos. Antes de la fecha efectiva del GDPR, el acceso ilimitado a los datos de registración, el WHOIS, violaba muchos de estos principios. La siguiente diapositiva, por favor.

Aquí tenemos una descripción general. Aquí subrayé algunos puntos, algunas cuestiones. El GDPR no es algo nuevo. Se hicieron algunos cambios para aumentar la responsabilidad pero lo que está incluido

en GDPR ya existía en Europa y en otros países y tratados desde hace muchas décadas. WHOIS nunca fue algo oscuro. Sigue estando allí. Sigue cumpliendo con la ley. Sé que se ha dicho varias veces en este seminario web, que los datos de WHOIS apuntan a detener los informes. Esta no es la forma de hacerlo. Lo mejor es informar estos datos a través de las partes contratadas y los proveedores de hosting. Esta es la forma de hacerlo. Luego se hizo un análisis para ver quién hizo qué, cómo evitarlo pero es necesario detener los ataques, los informes y las presentaciones no hacen nada para resolver el problema. Tenemos que poder tomar alguna medida y, una vez más, todos estos modelos de protección de datos incluyendo la CCPA en California, Brasil también tiene una ley, otros países tienen leyes que apuntan a proteger los titulares de los datos pero no les dan acceso a terceros ni tampoco crean obligaciones de divulgar los datos.

Con respecto a los datos omitidos en el WHOIS, antes, la comunidad de la ICANN había estado ocupándose de este tema desde hacía 10 años. Secuestro de dominios, spam, phishing, engaños telefónicos. Todos los temas de los que venimos hablando desde hace más de una década son cosas que pueden resolverse detectando y protegiendo los datos de registración y el acceso completo por parte de todos. Una vez más, tal como ya escuchamos varias veces, el uso indebido de los nombres de dominio no está subiendo. Está bajando. No hubo un aumento durante la pandemia del COVID-19.

Incluyo esto aquí como información general para aquellos a los que les interesa acceder a datos de solicitudes. Estos son pedidos que se

pueden hacer a un registro, a un registrador. Cuando se pide divulgación de datos básicamente son requerimientos descritos en el informe final del EPDP fase dos así como las mejores prácticas detalladas para los registros y registradores. Aquí tienen los datos para acceder al sitio web. Aquí tenemos información mínima básica que necesitan las partes contratadas para llevar a cabo una verificación y ver si se divulgan los datos. Sin esta información, esto demoraría el proceso. Los registros y registradores reciben reclamos sin un nombre de dominio y sin que el solicitante indique cuáles son los datos que necesita y esto demora el proceso. Por lo tanto, es necesario mejorar esta situación para que los registros y los registradores puedan cooperar y tomar una decisión con respecto a la divulgación de los datos. Próxima diapositiva, por favor.

Esta es una descripción general de información recopilada para la presentación que hicimos con datos suministrados de manera voluntaria por registros y registradores. Representa registrados y registradores pequeños, medianos y grandes en diferentes regiones geográficas del mundo. Hay una amplia variedad de datos. Algunos registradores informaron 30 y otros 3.400 solicitudes. Los números iniciales después de GDPR fueron más bajos pero fueron aumentando con el tiempo.

Algunos mensajes clave son que menos del 1% de los dominios totales gestionados están sujetos a solicitudes de divulgación de datos. Los índices varían significativamente debido a diferentes reglas de omisión de datos y cuándo se aplica esta ley. También quisiera subrayar que en

función de SSAD se necesitarán muchos más indicadores. La ICANN requerirá muchos más indicadores para ICANN y para la comunidad, para poder saber qué tipo de solicitudes de divulgación ingresan, quién las hace, cuáles son los resultados, etc. Próxima diapositiva, por favor.

Aquí tenemos algunos resultados que observamos. Pueden ver los registros, las solicitudes rechazadas o redirigidas. Aquí pueden ver los porcentajes. Redirigidos significa que un registro dice: "Por favor, contacte al registrador. Por algún requerimiento legal no podemos ocuparnos nosotros de este tema". Hay otras razones que pueden ser un dominio protegido por un servicio de privacidad o el dominio no está registrado o no está registrado con ese registro o registrador. En la próxima diapositiva vemos cuáles son las clases de datos suministrados. Un tercio de las veces eran datos de registratarios y dos tercios eran datos técnicos. Cuando los datos no se divulgaron, la práctica era explicar por qué no se suministraban los datos. Con frecuencia, cuando hay un servicio de privacidad y representación hacer una solicitud de divulgación de datos no es el camino adecuado a seguir ya que los servicios de privacidad y representación tienen procesos específicos para poder hacer esto. La próxima diapositiva, por favor.

Algunos registradores recibieron ciertas apelaciones para rechazar las solicitudes de divulgación, los registros no. Aquí vemos que los valores para registradores son muy bajo. Con frecuencia las apelaciones vienen a través del mecanismo equivocado. Esto genera un trabajo de

difusión y de capacitación para explicar por qué este fue el caso. La forma en que se recibieron las apelaciones no afectaron las decisiones de divulgación.

Aquí tenemos información acerca de la clase de solicitudes. Aquí pueden ver que tres cuartos provenían eran solicitudes de IP. Un 15%, organismos de aplicación de la ley y el resto eran otros que incluyen investigadores de seguridad, solicitudes para conocer al titular de un nombre de dominio o solicitudes que no incluyen un dominio y otro tipo de solicitudes. Esperamos ver en esta diapositiva que hay un solicitante por cada cuatro solicitudes. Es decir, hay muchos solicitantes que vuelven a presentar solicitudes. De hecho, hay un solicitante en particular que fue fuente del 45%. Una gran parte del volumen de solicitudes. Una diapositiva más, por favor.

Este es el tiempo de respuesta típico. Menos de tres días en general. Los registros respondieron más rápidamente que los registradores porque en general un registro deriva la solicitud a un registrador que está en mejores condiciones de evaluar los datos o tomar esa decisión con respecto a la divulgación de la información. Este es el fin de mi presentación. Me apuré un poco pero quería asegurarme de que hubiera tiempo suficiente para el intercambio.

JONATHAN ZUCK: Gracias. Realmente cubrió muchos temas en muy poco tiempo.

OWEN SMIGELSKI: Por favor, visiten ese webinar de septiembre porque hay mucho más material. Duró una hora y media. Pueden ver más información allí. Yo lo resumí en este tiempo que me asignaron.

JONATHAN ZUCK: Le pedimos al personal si por favor pueden buscar esta información y ponerla en el chat. Creo que es muy buena información para esta conversación. Realmente les agradezco. Ahora vamos a retroceder un poco. Le vamos a pedir al personal que le dé la palabra a Mark. Le vamos a dar la oportunidad de presentar brevemente su tema. Mark Svancarek, le damos la palabra.

MARK SVANCAREK: Buenos días. ¿Me escuchan?

JONATHAN ZUCK: Sí.

MARK SVANCAREK: Les pido disculpas. Tuve un problema con mi despertador. Ahora vamos a empezar. Hola. Yo soy Mark Svancarek, de Microsoft. Voy a darles la perspectiva de cómo vemos la ciberdelincuencia en Microsoft y qué es lo que está pasando con WHOIS y el GDPR. Voy a tratar de hablar rápidamente para que tengamos tiempo para intercambiar ideas posteriormente. Estoy escribiendo algo en el chat.

Este es el nuevo informe de defensa digital de Microsoft. Es muy completo. Explica cuál es nuestra opinión con respecto a la situación actual del ciberdelito. Se está hablando mucho sobre si la ciberdelincuencia aumentó o se redujo últimamente. No estoy seguro de por qué estamos hablando de esto. Los números están subiendo. Por lo tanto, la defensa contra el ciberdelito sigue siendo una prioridad importante. Estamos dedicando mucho trabajo a esto. El WHOIS es una de las herramientas que utilizamos para resolver todos los tipos de delitos, fraude para los consumidores, problemas antipiratería, evaluaciones generales de seguridad y otros. Hay más cosas aquí, en esta lista. Les pido disculpas pero no envié diapositivas anteriormente. Les pido disculpas. Cuando las di antes, creo que Milton ya había mencionado algunos de esos temas en sus diapositivas. Por lo tanto, yo no envié diapositivas.

Continuando, estamos preparándonos. Les pido disculpas. De todos modos, el desafío que enfrentamos con WHOIS y el GDPR en este momento es que realmente no desarrollamos un sistema que nos permita acceder a los datos en la forma completa en que se debería poder hacerlo según las normativas. Creo que es interesante debatir esto en el grupo pero en realidad lo importante es que presentamos una cierta cantidad de información y en nuestro grupo no llegamos a un consenso con respecto a cuál era la información que había que presentar o no. Estamos hablando de precisión, necesidad, etc. en cuanto al requerimiento de los datos, al pedido de los datos.

Creo que si visitan y escuchan este seminario web de septiembre, y van al minuto 34, allí van a ver que hay algunas pruebas y análisis que se hicieron y esto se diferencia un poco de los comentarios que recibimos de algún otro grupo. El tema es qué significa necesario. Hablamos de esto. Tengo parte de esa información aquí, si la pueden ver. Estoy tratando de compartir esta información. Les pido disculpas. No tengo preparados los vínculos. Creí que estaban listos para compartir.

Les pido disculpas una vez más. Les pido muchísimas disculpas. Voy a incluir esta información en la ventana de chat. Básicamente el tema es la definición de necesario. Tengo que ver si puedo corregir esto para seguir adelante. Les pido disculpas. Mientras se copia el vínculo, quiero decirles que se habló por ejemplo de la existencia del sistema uniforme de resolución de disputas que dice que nunca sería lícito dar información según WHOIS. Así es como funcionaría en principio.

JONATHAN ZUCK: Mark.

MARK SVANCAREK: Voy a volver a conectarme en unos minutos.

JONATHAN ZUCK: Siga adelante. No hace falta tener los vínculos y compartirlos. Simplemente mencione los puntos más importantes que quería compartir con nosotros y así podemos pasar a la sesión de preguntas y respuestas.

MARK SVANCAREK: Sigan adelante ustedes, que voy a encontrar los links. Se dijeron muchísimas cosas, que SSAD solo se podría desarrollar de una manera por los comentarios legales que recibimos y no es así la cosa. La realidad es que teníamos otras opciones y elegimos no ir por esos caminos.

JONATHAN ZUCK: Gracias. En esta sesión no queremos hablar específicamente de eso sino que queremos ver cuáles son las solicitudes, los plazos, etc. Por eso esos datos serán muy útiles. Sé que David preparó ciertos datos del lado del solicitante pero supongo que lo que estamos tratando de hacer es que, dado que el GDPR es una realidad, y que la aplicación del mismo es una realidad y la implementación de las recomendaciones del EPDP es una realidad, ¿hay canales de comunicación entre los que solicitan datos y los que tienen o poseen esos datos? Creo que lo que tenemos que tratar de debatir es cómo debe ser ese intercambio, cómo fue y cómo debería ser. Por eso la información que compartamos puede ser muy útil. Por ejemplo, una de las cosas que surgieron en otras presentaciones anteriores, y creo que Gabriel lo mencionó, es que cuando se identifica un caso de phishing ya terminó. La respuesta no es lo suficientemente rápida. Las partes contratadas llegan tarde, una vez que se presenta un reclamo. Por lo tanto, la idea es hablar sobre qué sería realista en términos de cómo podría ser este intercambio de datos e información.

Veamos ahora. Una de las conversaciones que surgió muchas veces es que los datos de DAAR sugieren que el uso indebido del DNS cayó en términos generales. Hay otros tipos de fraudes que subieron o subieron de otra manera. No sé si alguien quiere tomar esta idea. Hay alguien que preguntó esto en las preguntas y respuestas. ¿Por qué hay esta dicotomía entre dos conjuntos de datos? ¿Por qué no tenemos una respuesta final en cuanto a saber en qué medida cambian el uso indebido del DNS, si sube o si baja?

GREG AARON: ¿Puedo hablar de esto? Yo diseñé y creé el sistema DAAR. Lo que hace DAAR es analizar los datos de diferentes listas de bloques que tienen nombres de dominio y analiza las listas de bloques que incluyen ciertas categorías de fenómenos como por ejemplo phishing o malware. Lo que normalmente esperamos es ver una tendencia a lo largo del tiempo. Quizá caen los números y después suben. Eso es lo que normalmente vemos. Eso es estándar. Se miden cosas muy específicas provenientes de fuentes específicas. Lo que vemos por ejemplo es que hay nuevas técnicas de evasión que quizá reduzcan la cantidad de dominios que vemos. No sabemos cuál es el efecto de tener menos información de WHOIS disponible, qué consecuencias tiene esto en relación a la eficiencia de poner ciertos dominios en las listas negras. En algunos casos se midió y hay una publicación que demuestra que si es más difícil encontrar a los malos actores, habrá menos dominios que pasen a la lista negra. Esta es una de las posibles consecuencias.

Esto no significa que las cifras de ciberdelincuencia cayeron. Simplemente que encontramos menos dominios con problemas y hay menos que están en las listas negras. Cuando alguien dice que el número total de uso indebido de dominios está cayendo, eso puede ser según una fuente, según una métrica. Sin embargo, no importa cómo lo midamos, los número siguen siendo altos. Debemos recordar que la cantidad de nombres de dominio en una lista determinada no nos indica el daño que se causó ni cuál es el riesgo involucrado. En el compromiso de email corporativo, la cantidad de dinero que se pierde a través de cada uno de esos fraudes ha estado subiendo. Por lo tanto, si tenemos el mismo número de nombres de dominio, los daños son mucho mayores. Por lo tanto, yo creo que depende de lo que estamos midiendo, cómo lo estamos midiendo. Hay otros indicadores que dicen que los números están subiendo. DAAR está midiendo algo de una manera determinada y no creo que esto indique qué pasa en la totalidad del ecosistema. Muchísimas gracias.

JONATHAN ZUCK: Muchas gracias, Greg. Theo Geurts preguntó: ¿Cuál es la calidad de los datos cuando los registradores comparten datos? ¿Son útiles para las investigaciones? Algunas personas dijeron que estos datos carecen de precisión o que hay servicios de privacidad y representación en el medio. Creo que Milton preguntó: ¿Realmente las dificultades que enfrentamos se deben a los cambios que surgieron como consecuencia del cumplimiento del GDPR? Creo que esta es una

pregunta para la gente de organismos de seguridad e investigación en ciberseguridad.

GABRIEL ANDREWS: Si puedo tratar de responder a esto. Creo que la calidad de las respuestas varía obviamente. El único momento en que las respuestas no sirven es cuando vuelven a un servicio de privacidad y representación, porque allí no sirven. Incluso si los delincuentes mienten con respecto a la información que presentaron, estos son diferentes puntos de datos. Nunca sabemos qué punto de datos servirá para iniciar una investigación. Creo que incluso los datos fraudulentos demuestran algo. Habría que ver en qué medida los datos son reales o no. Cuanta más información tengamos, mejor podremos hacer las investigaciones.

JONATHAN ZUCK: Gracias, Gabriel. Stephanie tiene una pregunta. ¿Tenemos estadísticas sobre la frecuencia con que se roban los datos válidos y son remplazados por datos de delincuentes? Históricamente los datos ya han sido limpiados. Otros siguen siendo válidos.

GREG AARON: Puedo responder a esta pregunta. Hola, Stephanie. Yo analicé los datos de contactos de millones de nombres de dominio utilizados en forma indebida a lo largo del tiempo y lo que veo es que los delincuentes en general no toman los datos de otros y los usan. En

general simplemente inventan los datos. Algunos hacen esto mejor que otros pero es poco común en mi experiencia ver que toman datos de terceros los delincuentes.

JONATHAN ZUCK: Gracias. Quisiera pedirle si por favor puede activar el vídeo cuando habla, ya que estamos tratando de vernos las caras en estas reuniones online. Cuando respondan a las preguntas les agradecería que por favor activen el vídeo para que la gente los pueda ver. Volker mencionó que Greg al parecer dice que no hay ninguno beneficio en cuanto a dar de baja nombres de dominio cuando se recibe un informe dado que el daño ya fue causado. ¿Es esa la idea? Parece ser contradictorio.

GREG AARON: No. Creo que no entendió correctamente. Una de las cosas que vimos es que si damos de baja un nombre de dominio vamos a tener un beneficio incremental. Phishing, además, es uno de los delitos cibernéticos que menos dura. Hay otros problemas en los que podemos obtener mayores beneficios si damos de baja un nombre de dominio. En esos casos resulta muy útil. La pregunta sin duda indica que hay una diferencia entre la prevención y la solución. Lo que hemos visto a partir de los datos es que hay algunos lugares donde los delincuentes van, registran nombres de dominio, luego se cancelan esos nombres de dominio y registran otros más. Ahí tenemos un problema con actividad repetitiva y sería bueno que se pudiera interrumpir, evitar y detener esa actividad repetitiva de manera

temprana. Sugerir que dar de baja nombres de dominio no vale nada no es correcto. Creo que sí vale la pena. El objetivo es proteger a las personas que son víctimas de estos engaños.

MILTON MUELLER: ¿Podría agregar algo, Jonathan?

JONATHAN ZUCK: Adelante.

MILTON MUELLER: Creo que tenemos que centrarnos en la omisión de los datos pre y post-WHOIS. Creo que es relevante decir que phishing es un problema pero ya todos lo sabemos. La pregunta es: ¿La batalla contra el phishing o contra otro tipo de delitos cibernéticos depende mucho del acceso abierto a datos de WHOIS? Creo que los delincuentes lograron generar métodos muy sólidos para evitar la detección y la mayoría de las violaciones en el caso de phishing también son detectadas. Hay algoritmos que detectan patrones y que rápidamente bloquean estos intentos pero no me queda claro que la presencia o ausencia de datos de WHOIS tenga algo que ver con esto. Una vez más, no vemos una correlación estadística entre los problemas pre y post-WHOIS. No creo que podamos decir simplemente: “Nos gustaba tener acceso”. Cuando teníamos acceso abierto e indiscriminado a los datos el phishing era un problema también y crecía más rápidamente que ahora. Centrémonos una vez más en causa y efecto, si esto fuera posible.

JONATHAN ZUCK: Un excelente punto. ¿Alguien quiere hacer algún comentario? ¿Desde el punto de vista de ciberseguridad o organismo de cumplimiento de la ley?

GABRIEL ANDREWS: Yo podría agregar un comentario. Las investigaciones se ven afectadas negativamente por la falta de datos. Hay muchas razones que explican esto pero eso forma parte de un debate más amplio. Yo quisiera decir en este panel que nuestras obligaciones no incluyen solamente el lado de la atribución. También a veces involucran la notificación a las víctimas potenciales. Este es un ejemplo del mundo real donde utilizamos no solamente identificadores de titulares dentro del sistema sino también identificadores asociados con víctimas a las que se está apuntando. En teoría, son datos válidos pero si no están disponibles rápidamente, entonces la conversación importante tendrá lugar en forma telefónica con alguien cuyos datos se están viendo afectados ese día o al día siguiente. Esto nos permite tener estas conversaciones. Si no podemos hacerlo, entonces estas conversaciones no podrán tener lugar.

JONATHAN ZUCK: ¿Usted sugiere entonces que el uso de los datos es más valioso para conectarse con los inocentes, con las víctimas que tratar de rastrear a los delincuentes?

GABRIEL ANDREWS: No estoy haciendo una evaluación. Solo digo que se puede utilizar en ambos casos. Me resulta difícil hacer una declaración muy amplia acerca de lo que está pasando simplemente porque yo traté de recabar datos y he visto lo difícil que es acceder a los datos. Yo traté 82 veces de acceder a información y tuve éxito 42 veces. No se hace un seguimiento de las fallas, de los fracasos. Es muy difícil informar sobre estos hechos que sé que serían sumamente útiles. Lo que digo es que al recabar estos datos anecdóticos, esto es lo que más me sorprende. La frustración que sienten algunos investigadores que están tratando de hacer lo correcto y de tratar de identificar a las personas que podrían verse afectadas y se sienten frustrados al ver que no pueden hacerlo. No digo que no podamos explorar otras posibilidades. Solo digo que este es un método que antes funcionaba para ellos y ahora no. Por eso es un tema que quería plantear. Les doy a ustedes entonces la palabra para que respondan al respecto.

JONATHAN ZUCK: Gracias, Gabriel. Sé que parte de la presentación que tuvo lugar recientemente en la cámara de partes contratadas con respecto al acceso a los datos estableció las bases para la mejor forma de establecer el formato de las solicitudes para acelerarlas, etc. ¿Hay algún ejemplo o datos asociados con los solicitantes de datos que trabajan de esa forma? ¿Hay alguna correlación con la mayor probabilidad de que se les den los datos más rápidamente?

OWEN SMIGELSKI: Gracias, Jonathan. En realidad no puedo llegar a ninguna conclusión. Lo que hicimos fue trabajar con un conjunto de datos limitado pero la experiencia de la cámara de partes contratadas fue que cuando tenían una solicitud de información adicional la pudieron procesar más rápidamente. Pudieron hacer las verificaciones más rápidamente. El hecho de que brindemos toda la información no significa que va a poder ser verificada, simplemente estamos hablando de la diferencia en cuanto a acceder a los datos. Sin duda acelera el proceso, nos permite llegar a una conclusión y la mayoría de los datos mostraron que la mayoría de las solicitudes son solicitudes de violación de marcas comerciales. Esto no necesariamente son los casos más urgentes. Hay otros caminos que podemos tomar más allá de los botnets como URS u otro tipo de casos para los cuales no necesitamos los datos. Es decir, alternativas menos intrusivas. Son formas menos intrusivas de acceder a esta información.

JONATHAN ZUCK: Owen, ¿piensa usted que este test de balanceo va a continuar caso por caso? Es decir, ¿habrá alguna posibilidad de que aquellos que se adhirieron al marco de uso indebido del DNS puedan llegar a alguna especie de árbol de decisiones que haga que esto sea no tanto una caja negra para aquellos que quieren acceder a esto en la cámara de partes contratadas?

OWEN SMIGELSKI: Gracias. La verdad es que no sé qué va a ocurrir en el futuro. Todavía estamos trabajando y me interesaría mucho saber qué se va a permitir o no. por el momento parecería que hay algunas cosas que no se van a poder automatizar y hay muchas incógnitas con respecto a la divulgación de datos. Yo he visto comentarios en el chat que dicen que el congreso de Estados Unidos va a tener que aprobar algo para que los datos del WHOIS estén a disposición del público pero en el caso de los registradores grandes tenemos millones de clientes en todo el mundo y en ese caso no es posible decir con 100% de certeza que esta es una persona que está fuera de nuestra jurisdicción, que no está sujeta a estas limitaciones de divulgación de datos. Hay ciertas responsabilidades legales allí. No es tan fácil. Algunos registradores quizá sean más chicos y solo se centran en una región determinada o tengan un modelo de negocios diferente y su situación sea diferente. Creo que a medida que esto vaya evolucionando con el tiempo, se modifique SSAC y cambie el proceso de políticas, sin duda la situación va a cambiar pero es difícil predecir cómo va a cambiar. Gracias.

JONATHAN ZUCK: Gracias, Owen. Lori Schuman pregunta si usted estaría dispuesto a hablar acerca de la experiencia específica de Namecheap y cómo trabajaron con la divulgación de los datos.

OWEN SMIGELSKI: No tengo acceso a esos datos en este momento. Por lo tanto no puedo hablar de ese tema.

JONATHAN ZUCK: Gracias. Vemos que en el chat se ha estado hablando de este tema. He estado tratando de seguir la ventana de chat y la de preguntas y respuestas para ver qué dice la comunidad. Mike Graham, si está conectado, usted hizo una pregunta específica acerca de un cambio específico que tuvo lugar en relación con la omisión de datos. ¿Querría activar su micrófono y compartir esta información con nosotros? Quedó bastante atrás en el chat este comentario. ¿Podría activar su audio? Quizá lo agarré sin previo aviso y no está disponible. ¿Podría activar su micrófono? ¿El personal podría habilitar el audio de Mike?

MICHAEL GRAHAM: ¿Funciona?

JONATHAN ZUCK: Sí, muchas gracias.

MICHAEL GRAHAM: Les pido disculpas. Solo puedo compartir parte de la información con ustedes. En términos de esfuerzo y costos hay dos formas diferentes en las que esto tuvo un impacto. Por un lado, necesitamos acceder a la información para poder determinar si un nombre de dominio en particular se ha registrado de manera fraudulenta y se ha utilizado de manera fraudulenta o quizá fue registrado por alguien que tiene algún tipo de vínculo con una empresa. Simplemente sin querer está haciendo squatting. En muchos casos nosotros entendemos que hay

muchas personas que trabajan en Internet, que no tienen tantos conocimientos y quizá ocasionan algún perjuicio a nuestra capacidad de llegar a los consumidores y a su propia capacidad para hacerlo pero son buenos ciudadanos de Internet.

En términos de la investigación y el costo para las empresas, es un gasto enorme, un gasto adicional enorme acceder a esa información y en cuanto al uso indebido real y me refiero a uso indebido de phishing en nuestro caso y falsificación que tiene lugar en Internet, el costo de la investigación ha aumentado enormemente y en cierto punto es un costo que tenemos que pagar no solamente nosotros sino también los consumidores, tanto en forma financiera como en cuanto a su confianza que se ve afectada. Tenemos que tratar de no caer en uno de estos sistemas o esquemas que al parecer aparecen todos los días.

JONATHAN ZUCK: El tema de costo es un tema muy complejo porque obviamente aquellos que están en la comunidad de solicitantes de datos no siempre tienen en cuenta el costo de las partes contratadas cuando implementan algunas de las cosas que nos solicitan. Si cumplir con la ley es el costo de operar, de estar en el mercado, entonces creo que ese va a ser un tema complejo también.

MILTON MUELLER: ¿Podría hacer un comentario al respecto?

JONATHAN ZUCK: Sí, adelante.

MILTON MUELLER: Sí. El costo en realidad es el tema. Durante 20 años, los solicitantes no solamente podían acceder de manera gratuita sino que estaban subsidiados por el sistema de la ICANN. Básicamente les dábamos a los registratarios de nombres de dominio una adhesión al contrato que decía: "Si usted quiere un nombre de dominio, para eso sin su consentimiento, sin que usted diga nada, debe poner a disposición del público su identificación personal identificable". Esto implicaba costo para los registratarios y se subsidiaba el acceso de la gente. Algunos utilizaban y ganaban dinero con esta información. Creo que lo que hemos hecho con SSAD fue decir que tenemos que equilibrar el costo para que sea más justo y más eficiente. Si usted es un gran solicitante, y todos podemos pensar seguramente en un par de empresas que generan la mayor parte de las solicitudes, lo que dijo Owen fue muy útil en relación con este tema, ustedes son los que están generando el costo para el sistema. Ustedes son los que ocasionan estos costos y por lo tanto tienen que pagar a más, ya sea a través de algún arancel o a través de algún sistema de acreditación que cubra el costo de poner estos datos a disposición.

Si estos datos van a estar disponibles tan rápidamente como algunos quieren, esto implica un gran costo para las partes contratadas que tienen que evaluar estas solicitudes y, una vez más, podemos evitar estos costos automatizando pero la automatización también puede ser ilegal dependiendo de la naturaleza de las solicitudes. Sin duda es

un equilibrio muy complejo, Jonathan, como usted dijo. En cuanto a los fines de este panel, creo que sería bueno ser más conscientes con respecto a la distribución del costo. Es necesario que se equilibren los costos entre los distintos grupos de partes interesadas.

JONATHAN ZUCK: Gracias, Milton. Natalie pregunta: La mayoría de los registros europeos ofrecen servicios de divulgación de datos cumpliendo con GDPR. Si un solicitante puede proporcionar evidencias de una registración de marcas comerciales. ¿Se sabe si los gTLD y otros ccTLD están pensando en adoptar un modelo similar? Esto serviría muchísimo para los esfuerzos de los organismos de cumplimiento de la ley. ¿Quién quiere responder a esta pregunta aun cuando no tengan la respuesta?

OWEN SMIGELSKI: Perdón. ¿Cuál fue la pregunta?

JONATHAN ZUCK: Natalie Leroy. Está al final de todas las preguntas que figuran en la ventana de preguntas y respuestas. Es la última.

OWEN SMIGELSKI: Gracias. No estoy seguro de si hay otros gTLD o ccTLD que estén adoptando modelos similares pero a medida que avanzamos, a medida que trabajamos con SSAD, quizá encontremos una forma de establecer credenciales para los usuarios que estén con gTLD o ccTLD.

Quizá el informe del EPDP fase dos sea un punto de partida. Hubo muchos participantes dentro y fuera de este grupo. Hay muchos que quieren hacer algo más rápidamente. Hicimos todo lo posible para trabajar dentro de la información que tenía pero creo que es una sugerencia posible para el futuro en caso de que vaya evolucionando. Si es algo en lo que todos estamos de acuerdo, si cumplimos con la ley, sin duda podríamos tenerlo en cuenta. Gracias.

JONATHAN ZUCK: Gracias, Owen. Espero que esto ayude a responder en parte la pregunta aunque la pregunta es mucho más amplia. Laureen pidió tener la posibilidad de responderle a Milton. ¿Le pueden dar la palabra a Laureen?

LAUREEN KAPIN: Muchas gracias. Quería estar de acuerdo con algunas de las cosas que mencionó Milton acerca de la información que es una espada de dos filos. Puede usarse para cosas buenas y para cosas malas. Por otro lado, el DNS es un recurso público y Milton utilizó el ejemplo de las cosas que se utilizan para fines maliciosos. Eso es algo ilegal. Estamos de acuerdo con esto pero el GDPR no protege los datos de las entidades legales, personas jurídicas. Viendo lo que se está haciendo en el PDP, es importante tenerlo en cuenta porque el público tiene derecho a conocer la información sobre las personas jurídicas y haciendo este cambio, permitiendo a los usuarios averiguar quién está tras un nombre de dominio que no es una entidad individualmente,

eso ayudaría muchísimo a la población y a los organismos de seguridad en sus investigaciones y en sus actividades de due diligence. Se necesita dar cierta información para el uso de los recursos públicos, ya sea un registro de conductor o una utilización para una operación comercial. Esto es información se pone a disposición en forma pública. Esta información legal se debe brindar, también relacionada con las entidades o personas jurídicas.

JONATHAN ZUCK: Gracias, Laureen. Hay más preguntas. Por lo tanto, el personal va a juntar todas estas preguntas y vamos a tratar de escribirles la respuesta. Lamentablemente se nos acabó el tiempo. Ha sido un debate muy interesante. Traté en lo posible de mantenernos centrados en el tema que nos convoca pero para responder la pregunta de Jeff, cuál es el objetivo de una plenaria, no estoy seguro pero la idea es que cuanto mejor entendemos cuál es la situación, lo que pasó antes y después de un cambio en las políticas, cuanta más información tengamos sobre los pasos que hay que tomar, mejor. Más preparados estaremos. Ese es el objetivo de este intercambio de ideas. Ver cómo cambió el statu quo y qué pasó en relación al flujo de datos y la disponibilidad de información necesaria para proteger a los consumidores y para las investigaciones en términos de ciberseguridad. Esta es una misión de búsqueda de hechos y búsqueda de información. Hay muchas preguntas que no pudimos responder pero se nos acabó el tiempo hoy.

Son las 3:00 de la madrugada para mí. Creo que ya no tengo nada más inteligente para decirles. Solamente quiero agradecer a todos los presentadores y a todos los que participaron de esta sesión, debatiendo, los que estuvieron leyendo el chat. Vamos a utilizar esto para seguir hablando del tema. Muchísimas gracias a todos. Con esto terminamos la sesión.

[FIN DE LA TRANSCRIPCIÓN]