TERRI AGNEW: Buenos días, buenas tardes y buenas noches. Bienvenidos al programa de generación de capacidad de At-Large 2016. Este es el noveno webinar sobre el tema: Las tendencias de seguridad actuales que impactan en los registratarios y en los usuarios. Este webinar ocurre el 19 de octubre de 2016 a las 21:00 UTC. No vamos a hacer una llamada de asistencia porque se trata de un seminario web pero sí quiero recordarles a todos que pongan en silencio sus micrófonos y sus parlantes y que digan su nombre cuando tomen la palabra, no solo para la transcripción sino también para permitirles a nuestros intérpretes que los identifiquen. Hoy tenemos inglés, español y francés. Ahora le voy a pasar la palabra a nuestro moderador, Tijani Ben Jemaa, presidente del grupo de generación de capacidad.

TIJANI BEN JEMAA: Buenos días, buenas tardes y buenas noches a todos. Gracias, Terri. Este es el noveno seminario web de este año 2016 para el grupo de trabajo de generación de capacidad. Hoy vamos a hablar sobre las tendencias actuales que impactan en los registratarios y en los usuarios finales. Este tema ha sido elegido por nuestra especialista Julie Hammer, que también es participante de SSAC. Primero le voy a dar al personal la palabra para que nos cuenten las reglas de esta llamada y luego vamos a continuar.

TERRI AGNEW: Quiero recordarles algunos temas antes de empezar. Si quieren hacer una pregunta durante el seminario web de hoy, por favor, escríbanla a la

izquierda del Adobe Connect. Escríbanla allí y nuestro presentador o alguien del personal les va a leer la pregunta. Luego vamos a tener un cuestionario rápido al finalizar la llamada. Esas preguntas son siete preguntas de evaluación. Para las preguntas de evaluación, el recuadro va a aparecer en la parte inferior de su pantalla. Quiero recordarles a todos los participantes que completen la encuesta de At-Large. Seguramente ustedes saben que estamos realizando una revisión independiente y les pedimos a todos que participen. La encuesta está disponible en inglés, español y francés. Se trata de mejorar la efectividad de la comunidad de At-Large. Pueden hacer clic en el link en el pod que está a la izquierda de la pantalla. Con esto le voy a dar la palabra a Julie.

JULIE HAMMER: Muchas gracias, Terri. Es un placer presentar a Rod, quien nos va a hablar esta mañana. Rod es vicepresidente de una empresa que es muy reconocida en el sistema de nombres de dominio. Rod cofundó la empresa IID que se ocupa de la respuesta a los ciberincidentes y la información que se comparte. Rod también ha sido un participante muy activo en general en roles de liderazgo en la industria y en otras organizaciones globales que se ocupan de los temas de ciberseguridad que nos aquejan hoy. Rod también es copresidente del grupo de antiphishing del Internet Policy Committee y también es enlace en la industria. En este rol, he trabaja muy de cerca con ICANN, y también es miembro del SSAC y un miembro muy activo.

Rod también es miembro del comité de la alianza Trust y también es miembro del Consejo de Confiabilidad e Interoperabilidad. También es un participante muy activo en el grupo antimalware y antiabuso y es

representante de IID para los equipos de respuesta ante incidentes. Es decir, como vemos, tiene muchos roles internacionales. Rod es un participante bastante regular en los comités de OARC, esto incluye a las organizaciones de los principales operadores de DNS y las partes interesadas. Rod tiene unas credenciales muy adecuadas para hablarnos sobre este tema y es un gran placer presentarlo. Muchas gracias, Rod.

ROD RASMUSSEN: Muchas gracias, Julie. Gracias a todos los que están en la llamada hoy. Esta es una oportunidad para ponerlos al día sobre muchos de los temas, especialmente el DNS y el abuso que se está viendo en este panorama, en este escenario. Es algo muy importante para mí. Sin más, vamos a pasar a la diapositiva siguiente. Básicamente, aquí vamos a hablar del DNS. Es un tema que es bastante amplio. Le he dedicado mucho tiempo a muchos de los temas de la ciberseguridad que están ocurriendo. En este momento en Sídney se están discutiendo muchas de estas cuestiones, incluso hoy. Muchas de las cuestiones principales que estoy escuchando en las noticias o que deberíamos estar conociendo, involucran al DNS como parte de la ecuación.

El DNS, como ustedes saben, es una parte fundamental de prácticamente todo lo que uno hace en Internet, ya sea que se trate del email o la navegación web o cualquier otra cosa que hagan con Internet. En algún punto siempre se toca el DNS. Vamos a hablar entonces de qué son estas cosas, dónde se encuentra el ecosistema del DNS, dónde hay abuso en el ecosistema del DNS y cuál es el rol de la ICANN, al menos en cierta medida, en cuanto a las disposiciones del DNS que se hacen a través de registros y registradores, por supuesto también dentro del

alcance de la misión del ICANN. Luego vamos a hablar de algunas cosas que tienen que ver con enfrentar todos estos temas, cómo me protejo, cómo protejo a mi empresa o a mi organización o a la gente que a mí me importa de todos estos temas. ¿Cómo los voy a proteger? Algunas de las cosas que se pueden tener en cuenta tienen que ver con las implicancias de política en el entorno en el que todos trabajamos.

Esta es la agenda entonces para el día de hoy. Esto es lo que hice y lo que hago. Todas son cuestiones de trabajo. Voy a entrar directamente en la estrategia. Típicamente en estas reuniones, cuando vamos a una sesión donde hablamos de abusos, nos metemos en el corazón de cómo se involucran las comunidades de registros y registradores, qué es lo que está ocurriendo. Creo que tendríamos que dar un paso hacia atrás y ver cuáles son las personas que interactúan con la organización. Si entramos más en detalle, cuando hablamos del efecto neto de las características de las reuniones, ¿cómo es ese efecto realmente? Me parece que hay mucha información que las personas que se ocupan de esto conocen. En algunas conversaciones sobre política y cuáles son las actividades hay una suposición que está ahí y esa suposición podría ocurrir de hecho en cualquier campo.

Quiero dividir eso en tres áreas en cuanto al DNS. La primera es ataques en la infraestructura en sí del DNS. Es decir, aprovechar el uso de las víctimas del DNS y utilizarlo contra ellas. Luego hablar del DNS como infraestructura, que es como debe utilizarse en el protocolo. Como ustedes saben, los malos usan el DNS igual que los buenos y ellos quieren tratar de asegurarse de que la infraestructura que están utilizando sea la adecuada. Vamos a hablar entonces de cómo se puede usar parte de esto de algún modo normal en Internet. Luego, el DNS

cómo se utiliza como un vector de ataque en sí, de modos no intencionados. Quizá en el sentido de mover los datos. Es un modo de hacer funcionar el DNS. Vamos a hablar ahora de las metas y las motivaciones, y por qué estamos diciendo todo esto.

TERRI AGNEW: Perdón, Rod, por interrumpirlo. ¿Es posible quizá que ajuste un poco el micrófono? Nuestros intérpretes están teniendo un poco de problema para poder escuchar todo lo que usted está diciendo. No se está escuchando muy bien.

ROD RASMUSSEN: Vamos a hablar de los ataques al DNS y a las operaciones, etc. Estoy intentando de nuevo.

TERRI AGNEW: Lo lamentamos pero no lo estamos escuchando bien, Rod. Algunos lo estamos escuchando un poco fuerte. Lamentablemente no está funcionando muy bien. ¿Hay algún número de teléfono donde quizá lo pudiéramos llamar? Quizá pueda ser usted el que llame.

ROD RASMUSSEN: Tengo un número australiano. Quizá me puedan llamar ahí.

CHERYL LANGDON-ORR: Estaría sorprendida si pasa algo de esto.

TERRI AGNEW: Pedimos disculpas a todos por la interrupción. Estamos esperando a poder ajustar todo esto. Continuamos esperando que se conecte Rod para poder continuar con la llamada.

ROD RASMUSSEN: Ahora sí conectado. La idea entonces es hablar sobre las distintas cosas que suceden en el DNS y explicar por qué. De algún modo, son todas las cuestiones que ocurren con el ataque del DNS, los DDOS o utilizar todo esto para reflejar lo que ocurre en el DNS y lo que sucede. Por ejemplo, en general con el DNS, la gente que bloquea el DNS, etc. También estamos tratando de ver lo que ocurre con los ataques y cómo hacemos con las consultas al DNS. Todo esto luego se termina traduciendo en DNSSEC. Es exactamente el tipo de cosa que sucede, tratar de enviarle la información incorrecta, etc., el recurso del DNS. Por ejemplo, cuando hay una intrusión en una computadora. Vamos a poder entonces ver lo que está ocurriendo y de algún modo vamos a poder incluir información de WHOIS y todo lo que ocurre por lo menos con los gTLD. Es decir, ver qué es lo que puede llegar a ocurrir con el spam o quién puede estar enviando un ataque de phishing personalmente. Esto particularmente refleja lo que está ocurriendo en este tipo de ataques y en el acceso a los nombres de dominio de los registratarios. Lamentablemente, este es un caso bastante común.

Esta es una sección bastante rápida sobre cómo la gente puede acceder y atacar el DNS en los dominios que uno gestiona o de los cuales es propietario. Lo que ocurre con el DNS, con los distintos contenidos o servicios, ya sea servicio web, email o alguna otra actividad como Adobe Connect, en los distintos servicios, este tipo de actividad va desde las

ofertas y cosas como las cosas que pueden ser ilegales en algunas jurisdicciones u otras para que haya actividades criminales. Están por ejemplo intentando robar dinero o datos o activos que son muy valiosos. Luego, por supuesto, cosas que hacen otros actores para tratar de robar datos. Casi siempre eso involucra el DNS en alguna parte de esta actividad.

Yo ya mencioné también por qué la gente lo quiere utilizar, por la misma razón que la gente quiere utilizar el DNS en primer lugar. Esto también se aplica a los malos. Es decir, se aplica tanto a los buenos como a los malos. Esa es la idea que quería expresar. Vamos a ver si podemos hacer que ustedes puedan entender esto un poco mejor. Gran parte de estas operaciones de gran escala como estos dominios complicados o dodgy. Digo dodgy o complicados porque dependen de la jurisdicción en la que se encuentran para ver si son legales o ilegales, o si son grises, por ejemplo. Una de las cuestiones principales con este tipo de registro, cuando hay estos registros de dominios dudosos, hay algunas técnicas que se utilizan para engañar a servicios en base a la reputación del dominio para poder tomar decisiones sobre cómo tratarlo. Cosas como las inserciones más altas o más bajas o si se trata de enviar emails en base a lo que nosotros consideramos spam a partir de un dominio o no, o si se permite o no algo como servicios. ¿Qué debo hacer yo con eso?

Uno de los impulsores principales de la registración en alto dominio de este tipo de cosas es el hecho de que este tipo de servicios generan una reputación para los nombres de dominio y ahí especificamos qué ocurre con las distintas actividades. Esto lleva a que continúen dando este tipo de recursos. Hay registros del nombre de dominio, etc. Parte de lo que impulsa la actividad en un registro, en un país, versus un área contra la

otra es que se establecen nombres de dominio, por ejemplo .PHARMACY en Estados Unidos. Tenemos cooperación con otros países sobre eso pero hay otros países donde se establece que esto no es legal. Yo tengo mi registración por ejemplo en otra jurisdicción legal y puedo llegar a ser una víctima de nuestra jurisdicción para que se haga algo porque no hay nada que se pueda hacer con los registradores en los registros que los estén afectando.

Aquí es donde vemos estos problemas con los que nos estamos enfrentando desde hace mucho tiempo. Sé que estamos tratando de resolverlos. Es un problema sin resolver en realidad. Estamos tratando de encontrar alguna mitigación. La cuestión por ejemplo del derecho local y el derecho de que existan recursos globales, cuál es la jurisdicción que se aplicaría. Creo que este es un buen ejemplo de por qué la gente va a un lugar o a otro para conseguir recursos de DNS.

Vamos a pasar un poco a algo más divertido, por lo menos lo que yo considero como divertido o no divertido, que tiene que ver con el malware y cómo se utiliza en el DNS. El 91% de las personas que lo han estado utilizando está más cercano ahora creo yo al 99% pero estos son simplemente números. El malware utiliza el DNS con el objetivo principal de establecer un canal de dominio y control. Es decir, se pide que busque instrucciones de un recurso central. Le dice qué hacer, le dice si tiene que mandar un ataque DDOS o atacar una red o quizá intentar redireccionar cierto tráfico a través de un ataque de este tipo. Se le redirecciona a otro lado. Este tipo de cosas que se utilizan y todo este control se hace con el DNS porque es difícil bloquearlo con un firewall. No se logra fácilmente. Se ataca quizá una dirección IP. Estas son las actividades que en general vemos y que se emitían mucho más

fácilmente al controlar la dirección IP. Tenemos que ir moviendo todos estos recursos. Hay algunas técnicas de las que vamos a hablar en un segundo.

A pesar de esto, la ironía es que en el mundo actual hay muy pocas organizaciones que están analizando lo que ocurre con el DNS y cuáles son las actividades. Estamos empezando a ver más gente que lo hace pero hay un agujero muy grande en el mundo de la seguridad que existe desde hace unos cuantos años en este sentido. Hay, de hecho, aquí algunas cifras que les puedo mostrar donde se va a ver por qué esto es tan importante. Ya lo hemos estado escuchando desde hace tiempo y a veces puede ser difícil mitigarlo y entender por qué los proveedores de servicio hacen todo esto. Creo que este es un buen ejemplo que seguramente ustedes habrán escuchado. En este punto estamos hablando del ransomware. Es un tipo de malware muy particular que existe desde el 2016. Un ejemplo de esto es que el DNS se utiliza en todas las etapas de un delito.

La idea con el ransomware entonces es que voy a poner un malware en una computadora después de haber visto dónde está. Hay distintas maneras de infectar la máquina con un adjunto en un mail, un vínculo en el que te pido que hagas clic. Incluso se puede encriptar y denegar el acceso y decir: “Acabas de ser hackeado. Esta dirección de email ha sido hackeada para instrucciones”. Básicamente lo que hace el ransomware es que toma los datos y los secuestra de algún modo. Es decir, uno deja de tener ya acceso a sus datos. Lo que ocurre con esto es que los malos saben cuál es la meta en base al tipo de víctima que tiene y qué es lo que está ocurriendo con los distintos negocios profesionalmente. Ellos tienen los datos en esa computadora y son quienes pueden pagar un

rescate más alto. Estamos hablando a veces de problemas con una cantidad de dinero muy alta y al parecer esto va a ir ocurriendo incluso más. Ni siquiera en este caso estoy contando las pérdidas que se van básicamente con la información que ya es irrecuperable.

Todo el mundo tiene que ser consciente de todo esto. Hay una falta de consciencia de lo que ocurre. En estas encuestas hay un 50% o 60% de los empleados de una organización que no sabían. Se trata entonces de algo que nos asusta mucho y que es muy activo y que deberíamos tenerlo en cuenta. Lamentablemente, la utilización del DNS está en todos los aspectos de esa operación desde los dominios registrados para que tengan un lugar al que pueden ir, incluso poner un Bitcoin de información que se puede pagar y que se puede hacer.

Vamos a hablar ahora del phishing. Es realmente una actividad muy importante, muy popular, y está creciendo. Hay actualmente entre 2.000 y 5.000 sitios que se detectan diariamente. Tiene que ver con el acceso a las credenciales básicamente. Ahí vemos algunas cifras con respecto al costo. El objetivo principal del phishing son las bases de datos, como pueden imaginar. El efecto que esto tiene en los usuarios ahora está cambiando porque ahora se utilizan las credenciales para ingresar a los servidores y cometer actividades delictivas.

Luego tenemos el spear phishing que es otro tipo de delito. Esto implica ir a la búsqueda de individuos particulares o de un grupo en particular de individuos. Esto se enfoca más en la demografía. Lo importante a tener en cuenta es que aquí hablamos de correos electrónicos que se ven comprometidos, hay estafas mediante correo electrónico o quizá correos electrónicos de directores ejecutivos que se ven comprometidos

y que tienen acceso a este tipo de correos electrónicos a través de un funcionario de alto rango, un presidente o director ejecutivo de una compañía por ejemplo o alguien que tiene el control de las finanzas. Por ejemplo, se envía un correo electrónico que dice algo así como: Me encuentro en un avión. Me encuentro en viaje. Por favor, necesito una transferencia a la cuenta de tal persona por determinada cuestión y hay muchísima actividad en este sentido. Hay muchos correos electrónicos de este estilo. Afecta a muchas compañías y a muchos negocios.

Otra cuestión a tener en cuenta tiene que ver con los nombres de dominio y con los dominios que son engañosos para el envío de correos electrónicos. Un problema tiene que ver con la falta de autenticación de los correos electrónicos. A veces parece que las direcciones de correo electrónico son similares pero esto compromete a la cuenta de correo electrónico. Estas son las cuestiones implicadas en el spear phishing. Aquí vemos algunas cifras. En el segundo trimestre de este año vemos las cifras de la actividad detectada. Este es un informe hecho por el grupo de EPWG. Se puede ver un crecimiento bastante importante en los últimos años. Esta otra diapositiva muestra otro tipo de información. Aquí vemos los sectores industriales divididos. Hay una gran proporción que apunta a los servicios pero básicamente el objetivo de la actividad de phishing es el sector financiero o los bancos porque se intentan irrumpir en cuentas bancarias o en información financiera.

El DNS raramente es monitoreado y a menudo está disponible. Hay que trabajar en el uso de Internet. Esto no se ve en realidad como un vector de amenaza tradicional. Además de la capacidad o de la habilidad de amenazar o de engañar a las personas, también se señalizan o se tunelizan datos. Ahora voy a explicar a qué me refiero con estos ataques

de tunelización del DNS. Es una forma en la cual el malware se puede implementar, a través por ejemplo del uso de tarjetas de crédito. Por ejemplo, se utiliza el DNS para transferir los datos de la tarjeta de crédito por fuera, es decir, a los delincuentes a través de un malware y cada vez esto es parte de la práctica cibernética delictiva común.

Hablemos ahora un poco sobre las técnicas del uso indebido del DNS. Obviamente, hay varias formas de usar el DNS pero una de esas es a través de los nombres de dominio. Lo mismo lo hacen los delincuentes. Lo que hacen es utilizar credenciales o utilizar datos. Por ejemplo, hablamos de las Bitcoins. En este caso, para obtener los recursos del DNS se pueden comprar y algunos son gratuitos. A veces la actividad delictiva apunta a las credenciales, cuentas o tarjetas de crédito para obtener más recursos. Otra manera es comprometer una cuenta cuando hay una tarjeta de crédito asociada. Hay otros recursos que no utilizan los revendedores sino que son parte de la actividad delictiva como por ejemplo robar los recursos del DNS. En este caso se comprometen los sitios web. Esta sería una actividad de hackeo tradicional. También se puede comprometer el operador del DNS. Hay gente que puede irrumpir en los servicios de DNS. Esa sería básicamente una situación que enfrentaría un ISP.

Se puede comprometer también la cuenta de un registrador cuando se utilizan contraseñas que son débiles o cuando hay problemas en la gestión de contraseñas débiles. Es decir, se puede irrumpir en la cuenta porque utilizan la misma contraseña o porque hay una violación de las cuentas o porque se obtiene cierta información. Raramente se ve, lo cual es bueno, que haya ataques directamente a la infraestructura del registrador que no sea por logins o ingresos forzados. Ahora estoy

escuchando algo de música de fondo, que por cierto es muy linda la música.

TERRI AGNEW: Perdón, pido disculpas nuevamente. Vamos a identificar de donde viene ese sonido, esa música.

ROD RASMUSSEN: Bien. Este gráfico entonces describe el circuito donde se explica la anatomía del spear phishing pero vamos a avanzar rápidamente para que podamos tener tiempo para las preguntas. Bien. Ahora quiero hablar de algunas cuestiones técnicas que se utilizan dentro del DNS. Lo interesante es que hay ciertas características que son únicas y les voy a indicar cuál es el valor de esto. Tenemos el fast flux. Hace unos años teníamos una política de vast flux y la idea era tener un recurso que permitiera que las computadoras no estuviesen comprometidas. Aquí se hablaba de la reputación por ejemplo de IP. Estos flux cambiaron rápidamente dentro de los registros del DNS y esta política permite que los nombres de dominio funcionen correctamente sin ser cancelados o dados de baja.

A veces se trata de hacer un fluxeo a los nombres de dominio o también se utilizan otras técnicas que pueden ser mecanismos estáticos de protección. El problema con el fast flux es que a menudo utiliza la misma técnica básica para los contenidos, para diferentes actividades. Por ejemplo, uno tipea el nombre de dominio y retorna una página distinta. Hay algunas diferencias. Tenemos una descripción de una anatomía de un ataque de fast flux. Se lo voy a explicar rápidamente, así lo ven

graficado. Quisiera comentarles un poco. Por ejemplo, aquí están los botnets. Tenemos un registro. Un registrador de nombres de dominio cambia un registro rápidamente. Hay un correo electrónico que sufre phishing y esto termina afectando al cliente, independientemente del sitio web que exista. Esto es parte de un mapa o de una fórmula. Hay muchas formas mediante las cuales se puede detectar este tipo de ataque. Por ejemplo, observando el contenido que se envía. Es bastante sencillo.

Hablemos ahora de los algoritmos de generación de dominios, los DTA. Estos son recursos. Pensemos por ejemplo que si yo tengo un control del malware o se ha detectado la existencia de un malware, esto puede dar como resultado el cierre o el bloqueo de un nombre de dominio, entonces yo me quiero proteger de que esto suceda, de estas actividades y lo quiero hacer a través de una práctica. Lo que hacen la mayoría de los malware es utilizar los algoritmos de generación de dominio. Esto genera una lista de dominios y lo que hace es, al azar, elegir un nombre de dominio. El malware lo que hace es tomar uno de esos nombres de dominio y tratar de ver cuál es el servidor que le corresponde. Esto tiene cierta flexibilidad a lo largo del tiempo pero resulta ser un dolor de cabeza que termina dando como resultado el cierre o la cancelación de un nombre de dominio. Cuando hay que cambiar los datos en cada oportunidad, resulta bastante complicado.

Si uno está monitoreando la red y el DNS, puede ver este tipo de actividades. Las puede detectar. Cuando una máquina llega a un dominio que no existe, da una respuesta recursiva y dice que la respuesta es que ese nombre no existe. Si uno puede detectar el malware, puede también aplicar una ingeniería de reversión y solucionar el problema. Aquí

tenemos algo de contexto sobre el DTA. Esto comenzó allá por el 2008. Hubo un malware llamado Conficker y la idea era hacer un cierre generalizado de los nombres. Esto había afectado a muchos nombres de dominio y se creó un grupo de trabajo con los registros que trabajaban sobre esto. Como ustedes imaginarán, esto se transformó en un problema realmente serio. Por supuesto, fue un tema muy importante en ese entonces y se cambiaron alguno de los estándares a partir de ese momento.

Hay cientos y cientos de ataques de diferentes formas de malware y muchas veces con el mismo malware se pueden tener DTA. Hay muchísima información que se está generando. Hoy por hoy, lo que se está haciendo es compartir cómo son estos algoritmos para poder establecer un patrón y para poder detectarlos. Esta diapositiva, por ejemplo, muestra cómo se vería un nombre de dominio. Son muy fáciles de ver una vez que uno los puede identificar porque están encriptados. Hay técnicas para ubicar este tipo de cuestiones. Lo que sucede es que cuando se identifican, lo que se hace es utilizar diccionarios. Se crea un diccionario para poder rastrear este tipo de algoritmos. Este es el diccionario que utiliza. Lo que sucede es que el malware toma varias palabras, lo hace en forma de diccionario y esto a menudo perjudica. Lo importante es que muchas veces el nombre de dominio coincide con estas palabras o estos nombres de diccionario que fueron generados por el DTA.

Lo que hace el malware es tratar de llegar al nombre de dominio y tomar el control y esto da lugar a un ataque y como resultado, el dominio se ve afectado y puede causar serios problemas. Este tipo de DTA puede afectar porque puede causar una colisión de nombres, por ejemplo.

¿Cuál es la mejor manera de detectar un DTA? Haciendo un análisis y utilizar ciertas técnicas para poder identificarlos fácilmente. Aquí tenemos algo de ingeniería o algunos recursos para poder utilizar y encontrar un DTA. Prometo que no voy a explicarlos todos.

Hablemos ahora un poco sobre la exfiltración de datos, sobre las consultas al DNS. La idea es hablar de la exfiltración de datos a las consultas del DNS. Uno tiene por ejemplo una máquina y tiene información sensible o confidencial en esa máquina que quiere guardar o que quiere archivar. Uno ingresa el malware y el malware decide tomar esa información, por ejemplo, números de seguridad, nombres, información que tiene que ver con licencias, lo que sea. Lo que se hace es hacer consultas al DNS.

Por ejemplo, uno quiere buscar una información en particular. Entonces envía la consulta al servidor del DNS y el servidor del DNS no sabe qué es. Esta pregunta se efectúa nuevamente al servidor principal, lo cual significa que si yo estoy administrando un servidor de nombres, cada vez que aparezca una consulta de ese estilo, se va a transmitir. En cada oportunidad, el servidor de nombres va a responder diciendo: “Esta información o este dato pertenece a tal persona” o “Pertenece a Juan”, por ejemplo. Así se obtiene información de las direcciones de IP y una dirección de IP implica también que se pueda acceder a registros de texto con rapidez. Esta es una forma muy rápida. Es importante que monitoreen de cerca el DNS para saber cuáles son las consultas que se hacen al DNS. Esto se puede hacer a través de servidores, servidores de control entre otras cuestiones.

Lo último que quería cubrir es algo que tiene que ver con los propietarios de los dominios y esto tiene que ver con el shadowing de dominios. Durante los últimos 18 meses esto empezó a tomar vuelo. Existe en realidad hace unos cuantos años pero ahora se convirtió en algo mucho más común y hablamos de servicios o paquetes. Este es un buen ejemplo de eso. Lo que ellos hacen es que para poder continuar con una reputación, ellos van a hacer un abuso de esa reputación. Lo que hacen es que lo convierten en un sitio de phishing o algo parecido.

Lo que están haciendo ahora es que entran en el registrador, el registrador es el que da el servicio de DNS que tiene un panel de control automatizado y que lo hace más fácil para él. Entonces agregan varios alojamientos a ese nombre de dominio como fubar.goodguy.com, dejan el nombre de dominio www.goodguy.com solo y lo utilizan con objetivos criminales. Es decir, tienen subdominios. No hace falta registrar un dominio. Utilizan un dominio que tiene ya una reputación y muchos servicios hablan a nivel del nombre de dominio, no a nivel más específico. Podría ocurrir que haya medidas y contramedidas.

Esto se utiliza particularmente en algo que se llama [inaudible] que también se convirtió en algo muy común. Lo que eso hace es que mantiene actualizadas las vulnerabilidades de los [inaudible] y la gente entra en el sitio web y utiliza las mismas técnicas de las que estuvimos hablando. Esos sitios web cuando tienen algunos visitantes lo que hacen es que llevan a estos exploit kits e incluyen una lista de los no explotados contra el navegador y lo vuelven a incluir. Esta es la razón por la que uno no hace clic en los links. Hay exploit kits que pueden incluso ser utilizados. Tienen esos kits explotados y son los que ellos permiten que se utilicen.

Este es el shadowing de dominios. Este shadowing de dominios es algo difícil porque es una especie de discusión. Hay que tomar una idea de dónde surge. Hay cosas que van saliendo nuevas, hay redes de avisos donde uno ve estos posibles problemas y si uno las va encontrando, si las tiene que enfrentar, obviamente tiene que notificar a la persona que tiene al registrador para que desde un punto de vista de mitigación no se lo bloquee. Esto ocurre con empresas medianas y pequeñas y lo que ellos quieren es en realidad tomar a los que más dificultades tienen. Este es el problema.

Vamos a hablar ahora del Spamhaus. Hay algunas organizaciones que ustedes seguramente conocen. Spamhaus es la que aparece con bastante regularidad. Ellos son grupos líderes, una autoridad sobre el spam, que tienen muchos ISP que están suscritos a sus listas para que lo malo quede por fuera de la red. Spamhaus entonces tiene algunas listas, especialmente para nuestras comunidades. Nosotros podemos de hecho ir a verlas. Podemos ver cuáles son los primeros 10 registros y registradores que tienen problemas, o por lo menos los registros en cierto nivel. Para ser justo con cosas como el .COM, donde hay distintos dominios en el mundo, ustedes se pueden imaginar que hay muchos problemas con el .COM. Ellos han creado entonces esta fórmula que lo que hace es normalizar para el tamaño del dominio total. Cuando digo los dominios que están ahí me refiero a una metodología que tiene Spamhaus.

Ellos básicamente toman los dominios que están viendo y tienen esta capacidad de que en ciertos lugares, en tres o cuatro lugares, uno obviamente es el email, ellos ven estos dominios que se utilizan en el DNS. Tienen una replicación que se llama passive DNS y tienen puntos

de observación para múltiples servidores de dominios como ISP o ciertas universidades, empresas. Están entonces teniendo en cuenta la consulta y cómo ocurre esta consulta. Se fijan en quién hace la pregunta. Lo que sí saben es qué es lo que se pregunta y cuál es la respuesta que se va a dar. Ellos toman esto que se clasifica como malo y el nombre que utilizan. De hecho, así es como se va explicando lo que está sucediendo.

La próxima diapositiva aquí nos muestra dónde están los problemas. De acuerdo con esta métrica, estos son los TLD. Fíjense qué interesante que hay una especie de TLD legado. Todo lo demás son nuevos gTLD. Estos números reflejan algunas fuentes. Hay una superposición de fuentes. Ahí es donde empiezan a aparecer los problemas. En los nuevos gTLD definitivamente están teniendo problemas con el abuso en esos TLD y por el tamaño podemos ver el .TOP que tiene más de 300.000 dominios malos. Así los clasifica al menos Spamhaus. Hay cosas interesantes que están empezando a ocurrir cuando uno mira lo que ocurre. GDN significa Generic Domain Name, nombre de dominio genérico. Nos dimos cuenta porque vimos que todo el malware estaba apareciendo en .GDN. Vimos internamente que Spamhaus está viendo lo mismo. Eso es lo que significa entonces GDN.

Esta es una métrica bastante buena, bastante decente que nos muestra lo que está pasando. Estos son los registradores. Se utiliza la misma fórmula. Spamhaus está observando los problemas en estos registradores. La mayoría de ellos están en la región del Asia-Pacífico. China y Corea, si recuerdo bien. Hay algunos más como Moniker que tienen algunos otros inconvenientes diferentes. Fíjense en el número de índice con esto, comparado con el número de índice de los TLD. Estamos teniendo un campo que se está reduciendo mucho. Aquí es donde

empezamos a ver los cuatro o cinco principales que tienen los problemas más profundos. Allí es donde estamos viendo una gran cantidad de cuestiones. Hay muchas discusiones con un registrador en particular y sus operaciones. Ese es el problema principal que está ocurriendo en el mundo de ICANN. Out names es el que tiene todos estos problemas.

Sé que el departamento de cumplimiento está trabajando en esto pero no sé cuál ha sido el resultado hasta ahora. Ya tuvimos problemas como estos antes y, dicho sea de paso, el número dos y el número tres de esta lista son propiedad de la misma empresa. Son pequeños y son propiedad de la misma empresa.

Vamos al [inaudible]. Según Spamhaus, ellos tienen distintas metodologías, distintas personas y en su sitio web ellos describen esta lista que es como cruda de algún modo. Ahí uno lo divide por TLD y, como uno seguramente esperaría, .COM es el TLD con más cantidad de abusos. Hay medio millón de dominios que representan un porcentaje de la cantidad total. El que sigue a .COM es .TOP que es uno preferido. Como ustedes ven, los TLD legados aparecen porque son por supuesto mucho más grandes que todos los demás. Estamos viendo una gran cantidad de abusos en estos TLD. Hay sin embargo dos ccTLD. Tenemos .US, .RU, que tradicionalmente también tienen muchos ataques y que están fundamentalmente impulsados por el malware. Estos números no reflejan necesariamente lo que está pasando.

El cronograma que tenemos aquí es el que está en esta lista. Esto se generó hace unos días y de este modo les da una idea de lo que está pasando. Ellos básicamente van a listar qué es lo que ocurre si el dominio desaparece de la web o si no está disponible durante 30 o 60

días. Por lo tanto, si hay un informe incorrecto, seguramente lo van a quitar.

Vamos a contarles algunas anécdotas sobre las observaciones [inaudible] y poder darles alguna realimentación. Uno de los problemas más consistentes es .TOP. Un problema que también tenemos es el .INFO en oposición al .XYZ. Es el mismo registrador. Lo que ocurre con .INFO es que tiene un programa antiabuso muy agresivo que aparece en muchos TLD. Con .XYZ, lo que sé es que tienen un programa pero no sé si es muy efectivo. Ciertamente estamos viendo mucho abuso en ese sentido. El precio también es un tema aquí. Una muy buena anécdota aquí es que hubo una promoción sobre el .WORK que costaba 50 centavos. Ese era el precio de GoDaddy. Eso era cuando uno se registra con tarjeta de crédito. Después el precio puede ir subiendo hasta cuatro dólares. El abuso desapareció cuando se levantó el precio. Es decir, se redujo bastante. Por lo tanto, ese es un indicador de que los delincuentes no quieren pagar un precio caro. Yo sé que a veces, si uno paga muy poco, como se imaginan, hay registraciones malas. A ellos sí les importa. A pesar de que estos contenidos son difíciles y lo que ocurre por ejemplo con .XXX y .PORN es que muy pocas veces vemos lo que sucede. Estos TLD cuestan 40 o 60 dólares para el TLD por año. Son bastante caros.

Los últimos números que vamos a ver, si ustedes van a la encuesta de phishing global de APWG, estos son datos que ya fueron presentados en Helsinki. Son datos de APWG. En el DNS en este caso, yo no sé muy bien cuándo lo vamos a publicar pero seguramente vamos a tener todos los gráficos. Allí vamos a poder saber qué es lo que ocurre. De todos modos, la idea es tener en cuenta el phishing. Es un buen indicador de lo que

está sucediendo. Vamos a ver los números totales. Estos son ataques verificados. Son ataques que nosotros podemos monitorear. La tendencia, de hecho, tengo algunos datos para mostrarles… Los TLD utilizados para phishing son 355. Luego tenemos el total de TLD con registraciones maliciosas que representan 135 y de nuevo estos son los criminales que entran y utilizan los recursos con sus metodologías. Es decir, no hay técnicas diferentes.

Algunas de las cosas que vimos con los dominios. Tenemos un registro electrónico. Aquí tenemos el 20% de los dominios involucrados en el phishing que registraron los delincuentes. Esto no ha subido. Con los nuevos gTLD hay algunos problemas. Les voy a mostrar algunos datos sobre eso. El precio indica que con los más baratos hay más problemas. De nuevo, tenemos problemas en Bitly o en Google. Si miran los operadores que están por detrás de estos TLD van a ver que son los mismos operadores que donde el propietario del TLD. Los problemas vuelven en general al mismo propietario del TLD. Tiene que ver más bien con una implementación de la política. Vamos a ir año por año, de derecha a izquierda. El último año es el que está del otro lado. Básicamente aquí se puede ver que esto bajó un poquito en el 2015. Yo sé que volvió a subir en el 2016 pero a pesar de que los ataques bajaron, la cantidad de los botnets fue subiendo. De estos cientos de miles de dominios que vemos, solamente algunos son los que son registrados.

Bien, vamos ahora a ver algunos de los puntajes o escalas. Al igual que sucede con el spam o correo basura, en este caso lo que hicimos fue tomar la cantidad de nombres de dominio y dividirla por la cantidad real de dominios y registradores. Tenemos estas cifras y esto es importante para la gestión de los TLD. Son a veces cifras estimativas pero siempre

las terminamos publicando. Como pueden ver, la mayor cantidad de ataques o ataques individuales se ve en el TLD .LY. Hay una razón para esto. La razón es que los operadores de registros de Bitly tienen que saber quién se registra en su TLD. Muchas veces hay mucha información que no se registra. Esto lo que hace es que aumenten estos puntajes o estas cifras significativamente en relación a la cantidad de ataques debido a la naturaleza de la información. Es algo interesante que notamos con este caso en particular.

Es realmente importante tener en cuenta estos datos, estos puntajes de los nombres de dominio que tienen mayor actividad de phishing. En realidad tenemos que hacer una diferencia entre los nombres de dominio que se utilizan para hacer phishing en relación a los ataques de phishing que se producen. Hay nombres de dominio individuales que se utilizan y que producen varios ataques. Realmente no interesa si con ese nombre de dominio se hace un solo ataque o se hacen varios porque casi todo, por ejemplo, en el dominio .LY fue tomado como información.

Como pueden ver en esta diapositiva, Venezuela y muchos de los ccTLD, si ustedes conocen el contexto, siempre hay algunas cuestiones con el DNS. Por ejemplo, las unidades y los gobiernos, muchas veces son administrados por grupos de ingenieros. Cuando se producen los ataques, cuando se tienen cosas como .CF o .GQ que son administrados por ejemplo como ccTLD de publicidad o de marketing y no utilizan un código de país, hay muchas de estas actividades que se llevan a cabo aquí, como ustedes pueden imaginar. Dado que son gratuitos o que tienen un costo muy bajo, la actividad es fomentada de esta manera.

No recuerdo bien pero creo que un ejemplo era .CO. En realidad corté y pegué esta información así que quizá no está del todo completa o detallada. El continente americano, Venezuela por ejemplo, es un ejemplo dentro de esta lista. Esto nos lleva también a hablar de las registraciones maliciosas. Es decir, son registraciones realizadas por lo que serían los chicos malos o los delincuentes. Se registran nombres de dominio maliciosos. Esta es la cantidad de nombres de dominio registrados en el 2015. La idea es mostrar algunos ejemplos como por ejemplo .CF, .PW o por ejemplo .ML. Todos tienen un formato, por ejemplo .PARTY o .FIESTA, también es un nuevo gTLD. Es interesante que por ejemplo .COM tenga 2.7 en el puntaje para las registraciones maliciosas. Todo lo que está por debajo de estas cifras probablemente sea algo poco positivo, sea malo. Al menos esto es lo que se refiere al phishing.

Creo que lo que está en esta diapositiva ya ha sido abordado en la mayor parte de la presentación. Por ejemplo, dominios de bajo costo o sin costo son los que más sufren abusos. Por ejemplo, también hay registradores en diferentes partes del mundo que interactúan con organizaciones o con algunas organizaciones que no se encuentran dentro de la misma geografía. También hay revendedores que hacen un uso indebido. Por ejemplo, si un revendedor toma un nombre de dominio y lo comercializa con otro nombre. Muchos de los nuevos gTLD funcionan bastante bien. No veo que haya demasiado uso indebido con relación a un nuevo gTLD pero también hay otros problemas con los TLD.

Para resumir algunos conceptos de la presentación, aquí tenemos algunos puntos importantes. Si uno es dueño de un nombre de dominio, lo tiene que bloquear. Si no quiere sufrir un secuestro o sufrir algún uso

indebido, tiene que utilizar autenticación de correo electrónico en el DNS para poder evitar phishing o actividades similares. Hay estándares a implementar. Es decir, todas son herramientas que están ya disponibles por parte de los registradores para poder proteger un nombre de dominio. También es una buena idea implementar el DNSSEC si se tiene una empresa, por ejemplo. Luego utilizar tecnología y servicios que lo protejan de los nombres de dominio que son para uso indebido. Por ejemplo, la extrapolación de datos. Es algo que no siempre se hace. Hay que estar al tanto de estas herramientas en los mercados, especialmente en relación al malware y ver qué es lo que se puede hacer. También hay programas dedicados, exclusivos.

En el pasado había bastante escepticismo al respecto pero ahora ya no. En cuanto a las personas físicas o los individuos, pueden utilizar filtros en los buscadores o bloqueadores. Pueden también abrir servidores de DNS y limpiarlos para garantizar que no se introduzca un malware. Esto también ayuda a mejorar el DNS. Si quieren evitar este tipo de cuestiones, probablemente los ISP también puedan contribuir en esta actividad. También tienen que utilizar un programa o software antispam. La idea siempre es detenerse, pensar y conectarse. Si a ustedes por ejemplo les parece que hay un mensaje que viene de un origen dudoso o es un correo electrónico raro, antes de hacer algo con el correo electrónico tienen que pensar y analizarlo. Por eso puse este último punto que es detenerse, pensar y conectarse.

Hoy hablamos de la IANA, de varias cuestiones pero hay mucha información que no está publicada todavía y que probablemente cuando se publique va a ayudar a que las personas hagan un mejor uso de estos recursos. También, por supuesto, van a tener acceso a esta

presentación. La última diapositiva tiene que ver con cuestiones de política a considerar. Son cosas en las que habría que pensar. No estoy tratando de imponer una línea de pensamiento. Por ejemplo, ¿estamos realmente midiendo, rastreando e informando el uso indebido de una manera coherente? Hay diferencias en los métodos, categorías, observaciones. Son decisiones que hay que tomar. Lo más importante es si estamos recabando información estadística para poder hacer los análisis que correspondan. Para poder determinar una estadística hay que investigar. Hay mucha información, muchos informes sobre por ejemplo determinar información. La ICANN hace sus propios informes. Por ejemplo, informes sobre cómo reportar quejas.

También cuáles son los mecanismos de protección que implementamos. Hace un tiempo se hablaba del SSAC 40 y el SSAC 44. Son mecanismos de protección para los registrantes de nombres de dominio. ¿Dónde nos encontramos en este sentido? Hay algunas medidas que ya han sido plenamente implementadas por los registradores y otras que todavía no. Aquí tenemos también algunas cuestiones a tener en cuenta. Otra pregunta que nos podemos hacer es si tenemos las políticas adecuadas para dar una respuesta gradual. Siempre hay personas en la industria que aprenden de las prácticas y de lo que han visto. Por ejemplo, se puede decidir que una determinada metodología que se utiliza en alguna parte es adecuada para un registrador o no, o para obtener información de todos los registradores.

También tenemos que analizar si hay formas de brindar una forma más coherente o más consistente de registrar la información y de compartir información sobre los diferentes patrones de uso indebido. Hay datos que están disponibles, los aportes o los comentarios que hace la gente

que sufre este tipo de cuestiones, información que brindan los ISP. Los ISP deben hacer estos informes. Esto es importante. Es de utilidad para poder tomar acciones y para poder actuar de manera más rápida y de mejor manera porque es información importante. Esto es todo de mi parte. Gracias a todos por tener paciencia mientras solucionamos las cuestiones de comunicación al principio de nuestra presentación. Con gusto voy a responder las preguntas que tengan.

TIJANI BEN JEMAA: Muchísimas gracias, Rod, por la presentación. Nos quedan seis minutos antes de terminar el seminario web. Por favor, si tienen alguna pregunta para Rod, por favor, levanten la mano ahora. No veo a nadie. Le voy a pedir a Terri entonces que coloque en pantalla el pop quiz.

OLIVIER CRÉPIN-LEBLOND: Yo tengo una pregunta.

TIJANI BEN JEMAA: Perdón, no lo vi, Olivier. Adelante, por favor.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias, Tijani. Yo levanté la mano para decir lo siguiente. Gracias, Rod, por la presentación. Fue muy interesante. Quería preguntarle algo con respecto a los informes. Como ustedes saben, ¿han tomado la información de ciertas organizaciones, de Architelos, por ejemplo? ¿Están utilizando esa información?

ROD RASMUSSEN: Bueno, en realidad mi colega está trabajando con el APWG. Mi compañía brinda también información para los informes pero estamos tomando en realidad la información de múltiples fuentes. Los informes que se emiten se dan como un servicio a la comunidad y la idea es trabajar con el APWG. Por supuesto, también se trata de una organización voluntaria y trabajamos con voluntarias, ustedes ya conocen esto, están más que acostumbrados. Afortunadamente, la idea es poder compilar los datos, hacer un buen trabajo y también ver la información que están recopilando las compañías de seguridad en materia de datos.

TIJANI BEN JEMAA: Olivier, tiene la mano levantada.

OLIVIER CRÉPIN-LEBLOND: Gracias, Tijani. Yo tengo dos preguntas más. La primera pregunta tiene que ver con los datos que ustedes presentaron. ¿Pudimos hacer uso de esto? Hasta la última reunión de la ICANN, yo tuve gente de las partes contratadas e incluso gente de la junta que vino y me dijo que no hay ninguna prueba de que pueda haber algún malware en los nuevos gTLD que sea peor en los nuevos gTLD que en los TLD legados. Lo que estamos viendo en esta presentación, salvo que yo esté alucinando, es que efectivamente sí hay problemas con los nuevos gTLD. En segundo lugar, veo en el chat que hay una pregunta de Ricardo Holmquist de ISOC Venezuela y .VE está muy calificada en la lista de malware. Habría que ver si lo podemos mostrar al TLD local para que ISOC Venezuela pueda abordar estos temas.

ROD RASMUSSEN: Sí. Voy a responder a las dos preguntas. Yo ya respondí en realidad a las preguntas en el chat pero quiero ser muy rápido con los números de Venezuela. Les pido que lo usen con la gente de ISOC Venezuela. Los números no publicados de APWG, todo el mundo tiene acceso a eso. Son los números finales. Yo soy el autor así que les digo que los utilicen. En cuanto a Spamhaus, esto es público. Todos esos datos están listos para ser usados.

TIJANI BEN JEMAA: Muchas gracias. Si no hay más preguntas, quiero pedirle a Terri que vayamos a los puntos siguientes.

TERRI AGNEW: Tenemos dos preguntas. Queremos ver si todos estaban prestando atención. Pregunta uno: ¿Qué es el shadowing de dominios? Voten, por favor, ahora. Nuevamente, la pregunta tiene que aparecer a la derecha de su pantalla, en el recuadro derecho vertical. Rod, voy a mostrar los resultados. Si pudieras resolverlo, por favor.

ROD RASMUSSEN: La respuesta correcta es B. Veo que hay algunos que no lo han entendido bien. B es que está comprometido con la adición de dominios.

TERRI AGNEW: Vamos a la pregunta dos. Los datos muestran que el abuso de nombres de dominio tiende a correlacionarse con los precios bajos para los nombres de dominio con ciertas excepciones. ¿Esto es verdadero o falso? Voten por favor ahora. Voy a mostrar ahora los resultados.

ROD RASMUSSEN: La respuesta correcta es verdadero. Al menos con los datos que tenemos en esta presentación, esto es lo que se ve. Para la única persona que dice que es falso, bueno, hay que darle algunos datos más a esta persona.

TERRI AGNEW: Gracias. Tijani, ¿vamos entonces a la evaluación o tiene algún comentario?

TIJANI BEN JEMAA: Adelante.

TERRI AGNEW: Vamos ahora sí a la evaluación del webinar de hoy. Nuevamente, les queremos pedir que se queden algunos momentos más para recolectar algunos datos. Les agradecemos a todos por su tiempo. Pregunta de evaluación uno: ¿Qué les pareció el horario de este webinar? Por favor, seleccionen ahora. Pregunta de evaluación número dos: ¿En qué región vive usted en este momento? Por favor, seleccione ahora. Pregunta número tres: ¿Cuántos años de experiencia tiene usted en la comunidad de la ICANN? Por favor, seleccione ahora. Pregunta número cuatro: ¿Cómo es la tecnología utilizada para el seminario web? Por ejemplo: audio, vídeo, puente telefónico. Pregunta número cinco: ¿El orador demostró conocimiento del tema?

Dos preguntas más todavía y les agradecemos por su tiempo. ¿Está satisfecho usted con el seminario? Una pregunta final y luego la dejo en

la pantalla. Tómense su tiempo para responder. ¿Qué tema le gustaría que cubramos para futuros seminarios en línea? Esta es una pregunta abierta y pueden tipear en ese recuadro. De nuevo, quiero aprovechar para agradecerles. Les quiero pedir que desconecten sus líneas y que tengan un buen día. Esta llamada finaliza aquí.

JULIE HAMMER: Antes de desconectarnos todos, quería reconocer el esfuerzo de Rod para preparar y presentar este seminario web y extenderle nuestros agradecimientos porque se ha portado muy bien con nosotros. Muchas gracias, Rod.

ROD RASMUSSEN: Es un placer.

TIJANI BEN JEMAA: Gracias, Rod. Gracias, Julie. Gracias a nuestros intérpretes y al personal. Gracias a todos. Hasta luego.

TERRI AGNEW: Esta reunión ahora sí ha finalizado aquí. Muchas gracias a todos por participar. Por favor, recuerden desconectar todas las líneas. Que tengan un buen día.

[FIN DE LA TRANSCRIPCIÓN]