ICANN71 | Foro virtual de la comunidad – Sesión plenaria: Comprensión de las listas de bloqueo de reputación
Jueves, 17 de junio de 2021 – 10:30 a 12:00 CEST

BRENDA BREWER: Comienza la sesión. Por favor, inicien la grabación. Hola y bienvenidos a la sesión plenaria de la ICANN71: Conocimiento de las listas de bloqueo de reputación. Yo soy Brenda Brewer y coordinaré la participación remota durante esta sesión. Tengan presente que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN. En esta sesión solo se leerán las preguntas y comentarios en voz alta si se presentan en el espacio de preguntas y respuestas. Leeré cuando el presidente o moderador de la sesión me lo indique.

Esta sesión tendrá interpretación simultánea en inglés, chino, francés, español, ruso y árabe. Haga clic en el icono de interpretación en Zoom y seleccione el idioma que desea escuchar durante la sesión. Para tomar la palabra, levante la mano en la sala de Zoom. Cuando el facilitador de la sesión diga su nombre, el equipo técnico habilitará su micrófono. Antes de tomar la palabra, asegúrese de seleccionar el idioma que utilizará en la interpretación. Por favor, indique el idioma que utilizará si no es el inglés. Asegúrese de silenciar todos sus dispositivos y notificaciones. Por favor, hable en forma clara y a velocidad razonable para una interpretación correcta.

Todos los participantes de la sesión pueden hacer comentarios en el chat. Por favor, utilice el menú desplegable del chat y seleccione

responder a todos los panelistas y participantes. Esto permitirá que todos vean sus comentarios. Por favor, tengan en cuenta que los chats privados solo están permitidos entre panelistas en el formato de seminario web de Zoom. Los mensajes enviados por un panelista o un participante a otro participante estándar también serán vistos por los anfitriones, coanfitriones y otros panelistas. Para ver la transcripción en tiempo real, haga clic en el botón de subtitulado Closed Caption en la barra de Zoom. Con esto le paso la palabra a LG Forsberg. Gracias.

LG FORSBERG: Gracias, Brenda. Yo soy LG Forsberg. Seré moderador en esta sesión plenaria que se llama: "Entender las listas de bloqueo de reputación". Para quienes no me conocen, tengo experiencia en el área de nombres de dominio. Soy gerente técnico, coordinador de enlace con el registro en distintos roles. Actualmente soy el director técnico de iQ, un proveedor de servicios técnicos de la industria de nombres de dominio tales como el iQ Abuse Manager y analítica de dominios. Cuando no me dedico a esto, también hago servicios de consulta para registros y me ocupo de temas técnicos y de política. Por último, soy el curador de la base de nombres nórdica de la conferencia que está esperando una reunión presencial lo antes posible.

Durante la sesión de hoy vamos a relacionarnos con varias personas. Hemos preparado tres preguntas para que el público responda. Dos les serán presentadas en este momento y la última aparecerá justo en el último segmento de la agenda de hoy. Pido que por favor se presenten las preguntas de la encuesta.

BRENDA BREWER: Gracias. En pantalla deberían ver la primera pregunta. ¿Está familiarizado con los siguientes tipos de amenazas a la seguridad? Por favor, marque todas las secciones aplicables. Las opciones son: Spam, suplantación de identidad, malware, farming, botnets y otros. Nuevamente la pregunta: ¿Está familiarizado con los siguientes tipos de amenazas a la seguridad? Marque todas las opciones aplicables: Spam, suplantación de identidad, malware, farming, botnets y otros. Vamos a cerrar la encuesta en unos cinco segundos. Gracias. ¿Podemos cerrar la encuesta, por favor?

¿Podemos pasar a la pregunta dos? La pregunta de la encuesta número dos es: ¿El nombre de dominio que usted administra alguna vez experimentó estas amenazas a la seguridad? Las respuestas posibles son: Sí, no, no sabe o no administra dominios. Aquí tienen que elegir una. Nuevamente: ¿El nombre de dominio que usted administra ha experimentado alguna vez alguna amenaza a la seguridad? Sí, no, no sabe o no administro nombres de dominio. Vamos a permitir unos cinco segundos más. Muchas gracias. Podemos cerrar la encuesta. LG, adelante, por favor.

LG FORSBERG: Gracias, Brenda. Voy a continuar con una breve introducción del tema antes de pasar a la sección siguiente. Hoy tenemos varias partes aquí que nos acompañan asociadas con las listas de bloqueo de reputación de diferentes maneras. Estas partes son la ICANN, que proporciona las estadísticas a través de DAAR y el uso de las RBL y también requieren

que los gTLD por lo menos hagan un monitoreo. Luego tenemos partes contratadas, los registros y registradores, que pueden utilizar una o varias listas de bloqueo de reputación para monitorear sus nombres de dominio en el caso de los registradores.

Luego tenemos proveedores de servicios como las compañías de alojamiento que pueden utilizar las listas para que los correos electrónicos de sus clientes estén libres de spam o asegurarse de que los sitios web que ellos alojan no tengan ningún inconveniente. Luego usuarios finales, que en este caso es aquel que puede ser un registratario o el operador de un nombre de dominio o sitio web que es aquel grupo que seguramente en este caso no tendría relación con una lista de bloqueo de reputación.

Lista de bloqueo de reputación puede significar varias cosas según el grupo. Para la ICANN, un registrador o un registro puede ser una herramienta que se usa para prevenir desastres, para evitar que un correo electrónico termine en la carpeta de basura. Además, como el tema quizá se lo indique, la lista de bloqueo de reputación es algo integral del uso indebido del DNS pero aquí no vamos a hablar durante 90 minutos sobre qué es el uso indebido del DNS sino para conocer un poquito más de qué manera las listas de bloqueo de reputación trabajan y cómo las partes contratadas, los usuarios finales y las distintas partes, como los proveedores de servicio, pueden trabajar con ellas.

Se ha hablado mucho de estas listas RBL pero digamos que un repaso general no puede perjudicar a nadie. Es una recolección de

indicaciones o informes que ayudan a identificar comportamientos abusivos de una u otra manera. La parte de reputación del nombre a menudo significa que hay algunas maneras de determinar si un nombre de dominio tiene que estar incluido en la lista pero a menudo la respuesta no es tan sencilla. No es sí o no.

Un ejemplo es la implementación que hizo Spamhaus de la reputación. Cada nombre que comienza con cero tiene puntos negativos por hacer cosas positivas y puntos positivos por hacer cosas negativas. Un ejemplo. Si el dominio tiene 10 puntos, está listado. De alguna manera, esto rinde tributo a los proveedores cuando se implementaron en los servidores, los firewalls para impedir el spam y el tráfico indebido. Esta lista solía bloquear las cuestiones perjudiciales.

La mitigación del uso indebido quizá no sea el único caso de uso o a veces ni siquiera el uso primario. Algunas listas de bloqueo de reputación ofrecen una lista de información completa acerca de cómo un mal recurso fue descubierto o da una indicación de que algo malo ha ocurrido con un nombre de dominio en particular. Algo que muchas listas tienen en común es entender lo que hacen, cómo lo hacen y de qué manera los datos contribuyen pero esto no siempre es sencillo, en especial si uno es un usuario final que no tiene conexión con este tipo de recursos.

Para tratar de llegar al fondo de la forma en que las listas de bloqueo de reputación recopilan los datos, categorizan los contenidos y cómo esta máquina procesa los datos y da una nueva lista y hace otros procesos, hemos reunido varios representantes de estas listas hoy aquí

y también un grupo de representantes de las partes que antes mencioné, quienes hablarán de sus experiencias con las listas de bloqueo de reputación. Habiendo dicho esto entonces, si me permiten voy a presentar a nuestro primer participante hoy. Le voy a dar la oportunidad a él para que se presente y a su empresa. Por favor, señor Carel Bitter, de Spamhaus.

CAREL BITTER: Buenos días a todos. Soy Carel Bitter. Trabajo para Spamhaus y aquí estoy para hablar de lo que hacemos en relación con la reputación sobre todo. Nosotros trabajamos con múltiples conjuntos de datos pero hoy hablaremos de lo que hacemos en reputación. Hace ya 10 años que trabajo y he estado en relación con otros participantes en distintas sesiones de la ICANN y estoy aquí para ayudar y responder las preguntas que deseen formular.

LG FORSBERG: Gracias, Carel. Por favor, señor Roman Huessy, si se puede presentar.

ROMAN HUESSY: Soy Roman Huessy. Soy fundador de abuse.ch, que es una organización de la Universidad de Berna, de la Facultad de Ciencias Aplicadas. Trabajamos en la recopilación de información sobre botnets, malware y publicamos la información de manera gratuita a disposición de todos.

LG FORSBERG: Gracias, Roman. Nuestro último participante de listas de bloqueo de reputación es el señor Ben Coon, de WMC Global. Por favor.

BEN COON: Muchas gracias. Soy Ben Coon, de WMC Global. Es una plataforma sobre todo de phishing. Nosotros damos listas de bloqueo sobre URL para phishing, firewalls y personas que son atacadas en sus credenciales de phishing. Aquí estoy a disposición de ustedes para responder las preguntas que tengan.

LG FORSBERG: Gracias, Ben. Para continuar con nuestra conversación voy a presentar a las partes. Samaneh Tajalizadehkhoob. Le voy a dar la oportunidad de que se presente y nos cuente si tiene algún punto principal que desee plantear en esta discusión.

SAMANEH TAJALIZADEHKHOOB: Hola a todos. Trabajo en la Oficina del Director de Tecnología de la ICANN en el grupo de seguridad, estabilidad y flexibilidad. Soy líder en el proyecto DAAR y tengo trabajo previo en el área académica en feeds de reputación. Hoy voy a hablar de cuál es la visión de la ICANN sobre estos feeds de reputación y los distintos proyectos relacionados.

LG FORSBERG: Gracias. Ahora voy a presentar al señor Matthew Thomas, de VeriSign. Por favor, preséntese y cuéntenos un poquito de qué va a hablar.

MATT THOMAS: Hola. Soy Matt Thomas. Trabajo en VeriSign en el departamento de estrategia de ciberseguridad e investigación. Soy ingeniero y también soy miembro del SSAC. Actualmente me desempeño como vicepresidente para el directorio del grupo M3AAWG. Aquí estoy a su disposición.

LG FORSBERG: Gracias, Matthew. Del lado de los registradores tenemos con nosotros a Reg Levy, de Tucows. Por favor, preséntese y cuéntenos de qué va a hablar.

REG LEVY: Hola. Trabajo en Tucows como jefe de cumplimiento. También estoy en el grupo de registradores de uso indebido. Soy copresidente del grupo sobre uso indebido. Buenos días. Disculpas. Todavía debo despertar. Estoy muy contenta de estar aquí.

LG FORSBERG: Gracias, Reg. Por último, pero no menos importante, de la comunidad At-Large tenemos a Joanna Kulesza. Por favor, haga su introducción y presentación.

JOANNA KULESZA: Gracias, LG. Gracias por invitarme y darme la oportunidad de hablar en nombre de los usuarios finales. Yo soy copresidenta del Comité Asesor

At-Large y me ocupo principalmente de la creación de capacidades. Creo que este panel que hablará de las listas de reputación es un punto importante según muestra la encuesta. No es cierto que los usuarios finales no tengan interés en este tema. Intentaré dar nuestro punto de vista. Es un placer estar en este panel.

LG FORSBERG: Gracias, Joanna. Pasaremos de la sección de introducción de esta sesión a la próxima sección donde hablaremos de las listas de bloqueo de reputación y trataremos de aumentar nuestro conocimiento acerca de cómo funcionan. Voy a comenzar la sección preguntándole a Carel de qué manera definen ustedes qué es una lista de bloqueo de reputación.

CAREL BITTER: Muchísimas gracias por esta pregunta. Vamos a comenzar con la parte que corresponde al bloqueo, que en muchos casos no es solamente un bloqueo de usuarios. Si lo vemos desde la perspectiva de los registros y registradores vemos que los registradores están mirando los datos para encontrar clientes o nombres de dominio que sean problemáticos y en realidad no están involucrados en ningún bloqueo de por sí. Más que nada es una observación, es un caso de uso de ese tipo.

Personalmente, nosotros hablamos de conjuntos de datos y no de listas de bloqueo de reputación o RBL. Creo que esto es muy importante destacarlo y tenerlo en cuenta. Cuando empezamos a trabajar con cualquier conjunto de datos, ¿qué es lo que significan y

cuál es el propósito? ¿Para qué se usan? ¿Cuál es la intención? Los queremos usar de manera que fueron diseñados o, de lo contrario, no estoy diciendo que no se puede utilizar algo que tiene el propósito de hacer una cosa para otro fin pero hay que ser conscientes de que el caso de uso puede ser un poco diferente para volver a lo que decíamos antes. Cómo trabajan nuestros sistemas con los nombres de dominio. Cuanta mayor puntuación le podemos dar a un dominio en nuestro caso, más seguridad tenemos de que hay una actividad maliciosa que se está desarrollando. Esto permite que las personas actúen de distintas maneras con distintos grados de puntuación.

Tenemos que entender los datos con los que estamos trabajando. De lo contrario, tenemos que hablar con quienes crearon los datos y decirles que no se entiende. Estamos tratando de hacer esto con los datos. ¿Es una idea inteligente, hacerlo así? A veces hay bloqueos en el contexto de los correos electrónicos pero no a nivel del DNS. Un buen ejemplo serían los shorteners. Son muy conocidos como correo electrónico problemático y un email legítimo no incluye los abreviadores, los shorteners. A nivel del DNS probablemente tengan un tratamiento un poco más agresivo.

LG FORSBERG: Muchísimas gracias, Carel. Ahora quisiera hacer dos preguntas vinculadas que tienen que ver específicamente con Spamhaus. ¿Cuáles son los tipos de pruebas típicas que considera Spamhaus para poder incluir algo en una lista de bloqueo de reputación? ¿Esto cómo impacta en los adoptantes de esos conjuntos de datos?

CAREL BITTER: En nuestro caso no siempre es fácil compartir la evidencia porque muchos de los datos que obtenemos provienen de ISP, de redes donde tenemos un acuerdo donde ellos pueden compartir datos con nosotros pero nosotros no podemos hacerlo. En caso de una duda, siempre estamos dispuestos a hacer preguntas. Desde el punto de vista de los registros y registradores y los casos de uso que usamos, hay mucho apoyo. A veces decimos: "Bueno, vemos esto en la lista y no entendemos qué es lo que está pasando aquí". Tal vez sea un falso positivo. Siempre podemos verlo de esa manera y compartirlo pero no es que lo compartamos por defecto, como que tenemos una lista de 100 dominios malos. No quiere decir que esto contenga 100 muestras de spam o 100 binarios de malware. Básicamente tenemos que ir viéndolo en cada caso en particular, qué podemos compartir y qué no.

LG FORSBERG: Gracias, Carel. Roman, ¿cuál es la diferencia en este tema con abuse.ch?

ROMAN HUESSY: ¿Me podrían repetir la pregunta? Estaba respondiendo una pregunta en la ventana de preguntas y respuestas.

LG FORSBERG: Sí, no hay problema. ¿Cuál es la evidencia típica de uso indebido que ustedes considerarían con seriedad para bloquear un nombre de dominio en su conjunto de datos, dentro de abuse.ch?

ROMAN HUESSY: Normalmente tenemos en cuenta malware que está enviado a través de sitios web comprometidos, nombres de dominio que han sido registrados por alguien con fines maliciosos. El sistema verifica toda la presentación de datos, si hay una carga maliciosa. Si esto es así, la evidencia se publica en el sitio web del proyecto para que todo el mundo la pueda utilizar y se evita que esa información llegue al destinatario y se envía la información a la empresa de alojamiento. El proyecto es bastante transparente. Está todo publicado en el sitio web. Todo el mundo puede verificar por qué algo aparece en una lista de bloqueo.

LG FORSBERG: Gracias, Roman. Para poder entender un conjunto de datos, ¿podría describir cómo es el ciclo de vida de un informe genérico en el caso de ustedes con software malicioso, con malware? Desde la primera vez que les llega a ustedes hasta que desaparece.

ROMAN HUESSY: Sí, por supuesto. Si hablamos de malware, este es un tema un poco más sencillo a diferencia de los dominios de spam o de phishing. Yo espero una determinada respuesta de un host remoto. Eso significa que yo puedo hacer una verificación de manera automática para ver si

ese sitio web está entregando contenido malicioso. Lo puedo hacer de manera automática. Una vez que ese contenido malicioso desaparece, el sitio web o el nombre de dominio queda marcado como que está fuera de línea en forma automática. Eso significa que ese nombre de dominio o esa URL desaparece automáticamente de la lista de bloqueo que nosotros proveemos. Debido a ello, lo bueno es que la URL solamente queda dentro de la lista por el tiempo que muestra una amenaza. Esta verificación de la amenaza se hace varias veces por hora. Normalmente cada 10 minutos.

Una vez que un usuario final resuelve esa amenaza, el nombre de dominio o la URL automáticamente desaparece de la lista de bloqueo al cabo de una hora normalmente. Por otra parte, esto significa también que el problema en realidad no fue resuelto. El contenido malicioso tal vez ha sido eliminado pero la causa raíz no ha sido resuelta. Significa que ese actor malicioso vuelve a cargar ese contenido. El sistema automáticamente va a verificar si el contenido malicioso está allí de nuevo y, de ser así, vuelve a aparecer en la lista.

LG FORSBERG: Gracias, Roman. Ben, ¿lo que Carel y Roman acaban de decir aquí difiere de manera considerable de lo que ustedes hacen en WMC Global y lo que ven en cuanto a los informes de phishing, el ciclo de vida y la evidencia de phishing?

BEN COON: En WMC Global básicamente seguimos el mismo modelo que acaban de presentar los colegas. Nosotros detectamos el contenido malicioso en los sitios antes de que aparezcan en la lista. Normalmente, cuando proveemos una lista de bloqueo, la usamos en las últimas 24 horas porque ese sitio de phishing va a desaparecer. Ya no va a estar más en línea. Volvemos a ponerlo en una lista si vuelve a aparecer. Hacemos controles automáticos y vemos durante cuánto tiempo esa URL está activa. Otra cosa que ofrecemos con la lista de bloqueo, no ponemos en la lista el dominio sino la URL completa para poder identificar dónde está la mayor parte del contenido malicioso. Una vez que sale de línea ese contenido, vuelve a estar activo y sale de esa lista.

LG FORSBERG: Muchas gracias, Ben. Volvemos a Carel. Mencionó anteriormente que una lista de bloqueo de reputación tiene que tener un fin y el usuario tiene que saber cuál es el propuesta de esa lista, qué es lo que usan en Spamhaus, cuál es el usuario principal al que está tratando de brindarle un servicio. ¿Ha cambiado esto en los últimos 10 años?

CAREL BITTER: Obviamente tenemos spam como parte del nombre de nuestra empresa. Nos ocupamos de todo lo que tiene que ver con el correo electrónico. Es un poquito más complicado. Los conjuntos de datos que nosotros publicamos, la lista de bloqueo de dominios son una visión de lo que creemos que tiene mala reputación. Mayormente se aplica al correo electrónico pero también en todo el contenido de phishing o aquellos nombres de dominio que nosotros consideramos

maliciosos. Hacemos una distinción en ese caso, en ese archivo tan grande a través de los códigos de DNS. Podemos segmentar la parte que corresponde a correo electrónico y la parte que corresponde a phishing específicamente pero lo que hacemos es proporcionar datos. Tenemos poco control con respecto a cómo los usan las personas. Por ejemplo, esto puede ser a través de una versión gratuita que todo el mundo puede utilizar y es un formato que se usa más que nada con los servidores de correo electrónico. Hay una consulta con el DNS y hay una respuesta y se trabaja sobre la base de esa respuesta, dependiendo de las políticas que uno tenga establecidas.

Hay algunas versiones que están disponibles que se ajustan a amenazas específicas y casos de uso específicos. Hay distintos subconjuntos de datos para ser utilizados. Por ejemplo, a nivel de los resolutores del DNS. Hay otros que se utilizan a nivel de registradores y registros para que hagan investigación y reparación. ¿Cuál es el caso de uso primario? Supongo que aquellas personas que quieren tomar decisiones en términos de reputación sobre la base de un nombre de dominio. Tal vez ahora las cosas han cambiado un poco en relación con lo que tenemos en el pasado. Roman les va a decir que hay muchos nombres de dominio que se usan para botnets o malware. Nunca se van a encontrar en un correo electrónico. Pueden verificar pero nunca van a ver esos correos.

Hay distintos niveles en los que una computadora infectada puede establecer el contacto a través del malware. El lugar donde se buscan esos nombres de dominio no es un servidor de correo electrónico sino a nivel de resolutor del DNS o IDS o algo por el estilo. El propósito

dependerá del tipo de problema que están tratando de resolver. Como dijo Ben, en el caso de verificar SMS, por ejemplo. Muchos de los dominios que vemos, que se utilizan en los acortadores o en SMS no los vemos en el correo electrónico. Va más allá del correo electrónico. Hay conjuntos de datos que producimos nosotros o que produce Ben o Roman que pueden ser útiles para resolver los problemas de seguridad que uno pueda tener y para uno tener conocimiento de las cosas que van ocurriendo.

LG FORSBERG: Gracias, Carel. Ahora tengo una pregunta para los tres proveedores de listas de bloqueo de reputación. Todos ustedes hablaron un poco acerca de cómo reciben informes o indicaciones de estas situaciones. Mayormente estamos hablando de informes basados en la detección automática que buscan correos a los que tienen acceso. ¿Ustedes dirían que hay una forma de investigación humana? ¿Puede haber un componente humano en sus listas de bloqueo de reputación dentro de sus empresas? Comencemos por Ben.

BEN COON: Sí. Nosotros utilizamos cazadores de amenazas que van a detectar gran parte del phishing de credenciales que observamos. También nos aseguramos de ver aquellos dominios que no tienen un puntaje tan alto como para quedar automáticamente dentro de la lista de bloqueo de reputación antes de colocarlo allí. Cuando tenemos un falso positivo, recurrimos al equipo. El equipo hace una investigación y lo

agrega en forma manual o lo retira de la lista en forma manual pero diría que tenemos bastante intervención humana en nuestro caso.

LG FORSBERG: Gracias, Ben. Roman.

ROMAN HUESSY: Hablando de URLhaus, que busca sitios de malware, aquí tenemos un proyecto comunitario. Es decir, que los conjuntos de datos que nosotros producimos son solamente una parte de todos los datos. A su vez, hay otra parte generada por la comunidad. Cuando hablamos de comunidad, es importante destacar que hay dos tipos de notificadores. Uno, los notificadores extraños. Es decir, usuarios que yo no conozco, en los que no confío y cada vez que notifican algo al proyecto en general tenemos que verificarlo de forma manual.

Después, por otra parte, tenemos los notificadores confiables a los que conocemos. El sitio automáticamente va a pasar a la lista a partir de esos informes. Por supuesto, tenemos que verificar si hay contenido malicioso o no en ese sitio pero la URL va a ir directamente a la base de datos. Ahora, si lo utilizamos con un abordaje de lista de bloqueo que es un caso de uso para los conjuntos de datos, el nombre de dominio solamente va a aparecer en la lista de bloqueo cuando haya un contenido malicioso que se está propagando. En respuesta a su pregunta, la respuesta breve, tenemos una combinación de URL o nombres de dominio vetados manualmente y también otros que son automáticamente vetados por una máquina.

LG FORSBERG: Gracias, Roman. Carel.

CAREL BITTER: En nuestro caso también es una combinación de automatización y a su vez investigación por parte de humanos. Si queremos asignar una reputación a todo nombre de dominio que exista en el planeta, obviamente van a necesitar automatización porque hay demasiados nombres de dominio y hay muchos nuevos que surgen todos los días y los seres humanos no pueden analizar todo e investigar todo. Por eso hay una parte automatizada. Sin duda también hay un componente humano con investigadores que observan aquellas cosas que parecen sospechosas o que tienen un puntaje lo suficientemente alto. Siempre es una combinación del hombre y de la máquina.

LG FORSBERG: Gracias, Roman. Nos estamos quedando sin tiempo para este segmento de la sesión. Sin embargo, hay una pregunta que es muy popular y es la que quiero traerles aquí al panel. Cuán probable dirían que es que un indicio o un reporte sea un falso positivo. ¿Cuál es el motivo más común por el cual encuentran falsos positivos? Vamos a comenzar por Ben.

BEN COON: Yo diría que dentro de los datos que nosotros observamos y que son notificados en las listas de bloqueo siempre hay algún falso positivo.

Nuestro impulso tiende a ser llevarlo a un nivel lo más bajo posible a ese falso positivo. El motivo principal por el que tenemos falsos positivos es por la falta de comprensión de lo que es malicioso y lo que no lo es. Tal vez hay personas que reciben algo que no les gusta y lo reportan como malicioso cuando en realidad no lo es.

LG FORSBERG: Gracias, Ben. Roman.

ROMAN HUESSY: Por supuesto, hay falsos positivos. Siempre ocurre. Pueden ser notificados por todos. Si un notificador confiable empieza a reportar datos que no son malware de sitios de phishing o spam, simplemente va a ser bloqueado y va a ser excluido del proyecto. Yo creo que el flujo de datos es relativamente bueno.

LG FORSBERG: Por último, Carel.

CAREL BITTER: Los falsos positivos siempre van a existir. Como dijo Ben, es nuestra función asegurarnos de que el número sea lo más bajo posible. Con respecto a lo que se notifica, hace muchos años, cuando empezamos a tener botnets y spammers en los proveedores de correo electrónico, una de las cosas que se solían notificar y que no era spam o malicioso eran simplemente correos que no les gustaban, como una factura

como una factura que no querían pagar, por ejemplo, o una carta de rechazo para una solicitud de empleo.

En ese caso, el sistema funciona de manera tal que si hay una masa crítica lo suficientemente grande para notificar algo, entonces allí hay una asignación de una mala reputación a un nombre de dominio o a un IP o un proveedor. Existe la posibilidad de que si los informes de usuarios son parte de la función que uno desarrolla, que algunos notifiquen aquellas cosas que no les gustan simplemente. Tal vez no sean spam, no sea contenido malicioso ni phishing pero para muchas personas la distinción entre el botón para eliminar el spam o eliminar todo el contenido, básicamente no es diferente. Siempre hay una preocupación en ese sentido.

Obviamente, si uno lo piensa con cuidado, y creo que esto también se aplica a Roman y a Ben, todo falso positivo que podemos tener en nuestro conjunto de datos y siempre va a haber algún inconveniente, puede haber una semana en la que no tengamos ningún problema y después en otra tengamos tres o cuatro incidentes pero lo importante es ver cómo lo manejamos, cómo nos aseguramos de que aparezcan en la lista cuando deben, que todo se administre de la manera correcta pero obviamente, como proveedores de datos y creadores de los datos, nosotros también estamos interesados en que los datos sean lo mejor posible. Si no son buenos, la gente no los va a usar. Entonces cuál es el sentido de existir para los creadores de los datos.

Sobre todo Roman estará de acuerdo con lo que voy a decir. Los datos empiezan a ser más poderosos y más potentes cuanta más gente los

use. Si hay un nombre de dominio que está siendo utilizado para una situación de mando y control de botnet, por ejemplo, cuanto más rápido ese nombre de dominio es dado de baja o cuantas más personas lo bloqueen, más segura va a ser Internet. Si Roman lo notifica y muchos dicen: "Estas notificaciones no son buenas", entonces eso nos desvía de la misión que tenemos que cumplir. Nosotros queremos producir datos y que esos datos sean usados ampliamente, que las notificaciones, los informes sean lo mejor posible y que la Internet sea un lugar seguro.

Creo que los tres estamos tras este objetivo. Roman también. Nosotros estamos tratando de resolver problemas de seguridad para las redes, los registros, los registradores, los usuarios finales en última instancia porque ese es el objetivo último, proteger al usuario final. Cuantos más usuarios finales estén protegidos y no usen los datos si los datos no son buenos, mejor.

Esto es algo sumamente importante que siempre queremos tener en cuenta. Hay infinitas maneras de avanzar y ser agresivos y decir: "Si hacen esto, bloqueo más o voy a detectar más situaciones maliciosas". Hay muchas situaciones diferentes en las que siempre hay alguien en algún lugar que está haciendo siempre exactamente lo mismo que es que tiene fines maliciosos con el alojamiento de nombres raros de dominios.

Tal vez hay 100 informes que son malos y el último no lo es. Es como que siempre hay que estar buscando el equilibrio. Tratar de ser lo más eficientes posible, tener un buen proceso para manejar cualquier

situación que pueda presentarse. En una de las preguntas que hicieron aquí, por ejemplo, en nuestro caso, cualquier persona puede ingresar y retirar un nombre de dominio. No es necesario completar formularios extensos para hacerlo ni tener un contacto telefónico. Es simplemente un botón que hay que presionar. Esa es una ventaja para asegurarnos de que el proceso para lidiar con los falsos positivos fluya de la mejor manera posible para quien sea la víctima de ese falso positivo.

LG FORSBERG: Gracias, Roman. Estamos en el segmento de preguntas ahora. Quiero tomar una antes de pasar al siguiente segmento de la sesión. Quiero preguntarle a Roman si las listas de bloqueo de reputación o los feeds de inteligencia de amenazas tienen datos originales que cooperan entre sí. Por ejemplo, el uso de abuse.ch le puede dar a Spamhaus datos sobre falsos positivos o notificaciones importantes que pueden tener.

ROMAN HUESSY: Sí. La pregunta apareció en el chat también. Hay procesos por supuesto donde se comparte información con las amenazas actuales, con proveedores u otras partes y algunos de estos procesos que son bilaterales y existen por ejemplo con Spamhaus o Safe Browsing u otros proveedores de RBL pero en abuse.ch los datos están a disposición de todos. Cualquiera puede consumirlos. Hay una gran parte de proveedores comerciales de datos que consumen estos feeds y hacen con ellos lo que desean. Como no hay ninguna registración requerida, eso es una cuestión de nuestra parte que es que nosotros

no sabemos quiénes usan la información porque son de dominio público.

Con respecto a la pregunta del intercambio de información sobre falsos positivos, creo que este es un tema muy importante. Por lo que yo conozco, los mecanismos para reportarlos no existen por ahora. Cuando algo es marcado como falso positivo, por supuesto, sale de los feeds y otros proveedores de RBL u otros proveedores de información de amenazas lo conocen pero, por supuesto, nosotros no tenemos ninguna influencia al respecto. Es un tema que necesita tener una plataforma por ejemplo de intercambio donde se anuncien quizá los falsos positivos y se compartan con otros proveedores.

LG FORSBERG: Gracias, Roman. Bien. Hemos llegado al momento de la presentación por parte de la ICANN de esta sesión así que le doy la palabra a Samaneh.

SAMANEH TAJALIZADEHKHOOB: Hola a todos. Soy Samaneh Tajalizadehkhoob. Represento a la oficina del Departamento de Tecnología de la ICANN. Hoy hablaré sobre nuestra visión acerca de las listas de bloqueo de reputación. Gracias. Próxima diapositiva. Hasta ahora hemos tenido muy buenas discusiones. Ya se han formulado algunos de los puntos de la presentación. Ya fueron cubiertas en las presentaciones y en las respuestas.

Quería comenzar por la base, hablando de qué es una lista de bloqueo de reputación. Pueden ser listas de bloqueo de direcciones IP o de nombres de dominio de host. Lo que generalmente representan son entidades que están identificadas como maliciosas o que simplemente tienen una mala reputación. Yo he listado algunos de los casos de uso que existen en la industria o en el mundo académico de la investigación que la gente utiliza para alimentar firewalls de DNS para prevenir el tráfico malicioso, el tráfico no deseado, típicamente spam o phishing. Usan los CDN para entregar contenidos a las redes. Hoy se usa como paso también en los procesos de los organismos de aplicación de la ley o de respuesta a incidentes para identificar ataques.

Pueden compartirse a través de distintos mecanismos. Están los de código abierto pero también los comerciales, ya sea disponibles a través de un mecanismo con limitación de velocidad, con licencia o pago por uso y que normalmente lo mantienen compañías que tienen fines de lucro que se especializan en esto. Hay algunos de código abierto que normalmente los utilizan los académicos y también otras partes. Algunos ejemplos son Spamhaus, abuse.ch, Phish Tank, que son los que yo conozco pero hay otros.

También pueden ser específicos de determinadas amenazas. Es decir, que se centran en algunas. Por ejemplo, abuse.ch, que Roman mantiene. Tienen distintas feed sobre botnets, ransomware o pueden ser más generales y contener todo tipo de amenazas. Un ejemplo es SURBL. Siguiente diapositiva.

Esto ya lo hemos discutido extensamente. Son las características y las desventajas de las listas. Quería centrarme en ambos aspectos porque lo que para un investigador puede ser una característica, para otra parte puede ser una desventaja. El propósito de usar una RBL en nuestra perspectiva es para entender lo que uno hace pero más importante para entender la metodología detrás de una RBL que representa cómo puede usarse.

Algunas de las características son que algunas listas pueden estar excesivamente especializadas, como estar dirigidas a un propósito específico. Una persona que desee usarlas tiene que entender cuál es este propósito y si cumple su interés. Hablo de este tema como investigadora. Ahora en general tienen una cobertura limitada y puntos de visión que se superponen y son limitados. Los proveedores de los datos están ubicados en determinadas localizaciones geográficas. Quizá tengan una representación inferior de determinadas localizaciones geográficas.

Con el tiempo, por mi experiencia ya hace siete u ocho años que trabajo aquí, la mayoría de las listas han venido mejorando con respecto a la cobertura pero es importante tener esto en cuenta cuando se hacen anuncios en las listas. Esta idea de considerar la calidad y las distintas métricas de confiabilidad de las listas no es una idea nueva. Ya ha sido algo sometido a investigación desde hace algunos años.

En la presentación yo pongo una lista de las distintas investigaciones académicas y de la industria que se han hecho pero me pueden

contactar si desean más información. Hay otra cuestión o característica de las RBL. En general, hay una limitada documentación sobre los métodos internos. Por lo que entiendo de las conversaciones personales que he tenido con los proveedores, no es algo directo documentar todo el proceso. Puede ser un proceso ad hoc o un proceso muy detallado o reactivo. Es difícil mantener documentación en tiempo real que represente todo lo que un proveedor de una RBL hace con un feed específico.

Además, como hay tantos proveedores de RBL, es de esperar que exista mucha variedad en las metodologías con respecto a la recopilación de datos o curación, mantenimiento de las listas. Esto genera distintos efectos con respecto a la cobertura, la confiabilidad, la efectividad y la velocidad de los anuncios. Es importante entender que esto no necesariamente es malo. Puede ser bueno. La diversidad aporta más información en tanto el usuario comprenda la diversidad y la maneje correctamente. La siguiente, por favor.

Esto ya lo dije. ¿Por qué es importante conocer estas desventajas o características? En primer lugar, es importante para que cada tipo de usuario como operadores, investigadores y empresas de seguridad conozca las diferencias que existen entre las listas y las desventajas. También que sepan cuáles son para diseñar defensas y métodos de curación más efectivos, además de que esto permite tener resultados más exactos en los reportes.

En la comunidad de la ICANN solemos decir que hay una investigación que muestra tendencias de phishing en aumento. ¿Por qué no

compararlo con otra investigación que hace la persona B sobre el tema? Este es el punto exactamente que intento transmitir. Creo que es el mensaje principal de la diapositiva. Dependiendo de qué conjunto de datos se utilice, dependiendo de qué tipo de periodo se esté utilizando, qué proceso de etiquetado para el conjunto de datos, cómo se adquiere, la tendencia puede cambiar. No existe una tendencia absoluta en los feeds. Al menos en mi experiencia no hay ningún informe que pueda decir: "Esta es una tendencia absoluta". Siempre es parcial. Dependerá del feed y, como Roman y los demás señalaron, es nuestra visión de la RBL. Siempre parcial y siempre depende de la metodología. Siguiente, por favor.

En las próximas diapositivas quisiera referirme a alguno de los casos de uso en la ICANN. Es decir, cómo nosotros usamos las listas. El DAAR, el informe de actividad de uso indebido de nombres de dominio, es un proyecto que utiliza, seguramente lo conocen, las RBL. No voy a dar los detalles de lo que hace el DAAR pero, en resumen, digamos que el sistema toma nombres de dominio de los archivos de zona de los registros de TLD, nombres de dominio de un conjunto preseleccionado de feeds para phishing, malware, comando y control de botnets y spam como vector de entrega y luego es una superposición entre los nombres de dominio y las RBL y procesa y calcula y genera métricas diarias mensuales para distintos tipos de análisis que ustedes pueden conocer. Han leído en los informes mensuales del DAAR que se están publicados en los sitios web de la ICANN. Muestra tendencias de dónde se concentran las amenazas a la seguridad a lo largo del tiempo y cómo va cambiando con el tiempo. Este sistema, por supuesto, hace

un proceso extenso de limpieza y procesamiento de los feeds y los datos están listados en el documento de metodología del proyecto. La siguiente, por favor.

BRENDA BREWER: Disculpas. Antes de continuar, si usted es tan gentil, nos solicitan que hable un poquito más despacio para beneficio de los intérpretes.

SAMANEH TAJALIZADEHKHOOB: Sí, por supuesto. Okey. También hicimos un proyecto en el grupo de investigación para el área de cumplimiento de la ICANN en el cual creamos métricas e instantáneas de los registros. Este fue un proyecto de única vez hasta ahora por lo menos. Hicimos algo parecido al DAAR pero solo para los registradores. En este caso nos concentramos en el phishing y malware de un periodo específico. Un determinado número de meses y calculamos métricas para familias de registradores y registradores individuales, mostrando la concentración en un punto en el tiempo y a lo largo del tiempo. Para este proyecto específico tuvimos acceso a BRDA porque es lo único que pudimos hacer por razones de cumplimiento. La siguiente, por favor.

Otros proyectos de investigación en este momento en la oficina del director de Tecnología, utilizamos las RBL para modelos de predicción a fin de predecir cuándo un nombre de dominio se tornará malicioso y también para extraer patrones para caracterizar los dominios maliciosos. También planeamos emplear un método similar que el que usó el estudio COMAR, que fue presentado en el Tech Day de la última

reunión de la ICANN para identificar como uno de los inputs un subconjunto de RBL basados en dominios para hacer esta distinción. La próxima, por favor.

¿De qué forma actualmente o en la mayoría de los proyectos mencionados antes, de qué manera evaluamos o qué evaluación hicimos en la selección de las RBL? Monitoreamos los feeds durante un tiempo determinado como parte de la investigación. Lo que hicimos básicamente fue seleccionar las listas de mejor reputación dentro del mundo académico, de la industria, según las publicaciones, basándonos en las publicaciones porque esto puede ser subjetivo y optamos por aquellas que tienen mejor documentación y una mejor calidad de los datos y que registran los procesos de remoción y cumplen con el conjunto existente con respecto a la cobertura. Siguiente, por favor.

Sin embargo, estamos planeando adaptar a futuro criterios de evaluación más sólidos. Es un trabajo en curso. Quiero hacer énfasis aquí en que la evaluación de las RBL no es algo nuevo. Lo hemos hecho. Aquí lo que estamos haciendo es hacerlo más completo, más relevante para los feeds actuales. Estamos trabajando en el desarrollo de métricas para lo que nosotros llamamos pureza, que es un análisis manual de falsos positivos y falsos negativos. Debo decir que estas no son métricas directas. Tenemos datos de verdad básica que es cuando la etiqueta no es directa, la interpretación. Esta es el primer tema que trata cualquier investigador que se ocupa de RBL.

Estamos trabajando para estimar la cobertura de las listas, la tasa de respuesta, la exactitud, es decir, el nivel de detalle que tiene la información en el feed, cuán estables son a lo largo del tiempo y de qué manera están activas, cuántos de los nombres de dominio siguen siendo positivos y activos cuando aparecen en un feed. Esto todavía no está cerrado. Seguimos trabajando para ver si podemos conseguir resultados confiables. Estamos trabajando en el proyecto de investigación. Puede cambiar pero les vamos a mantener informados. Por ahora es un trabajo en curso. Siguiente diapositiva, por favor.

Aquí ven las referencias que yo utilicé para preparar mi presentación. La presentación ya concluyó pero antes quiero decir que en la oficina del OCTO estamos haciendo varios proyectos de prueba, utilizando RBL, en especial para los registros y registradores, para obtener más información sobre las amenazas a la seguridad.

Alguna de las razones por las cuales el desarrollo de estas métricas es necesario. Hemos hablado en la comunidad que esto no es directo, que no queremos publicar algo que no es confiable. Eso es precisamente de lo que estamos hablando hoy. Por ejemplo, hemos hablado del tiempo activo, el uptime, el tiempo que les lleva a los operadores reaccionar ante un determinado uso indebido.

Hablando en relación con lo que dijeron los miembros del panel y también en mi presentación, ya hemos hablado de las diferentes de metodología que tiene cada lista. Esto nos permite notar que si tomamos varias listas y tratamos de crear una métrica para que un operador represente su tiempo de actividad, estaríamos utilizando

distintas metodologías. La métrica no representaría algo que es confiable para el operador. También depende de la metodología del proveedor de RBL.

Estos son ejemplos de las dificultades que enfrentamos en nuestro proyecto, que estamos tratando de resolver pero es bueno plantearlas ante la comunidad. Esta ha sido una buena oportunidad. Muchas gracias a todos. Aquí estoy a disposición para responder sus preguntas. No sé cómo vamos con el tiempo.

LG FORSBERG: [inaudible]

REG LEVY: [inaudible]

LG FORSBERG: [inaudible]

MATT THOMAS: [inaudible]

LG FORSBERG: [inaudible]

REG LEVY: [inaudible]

LG FORSBERG: [inaudible]

MATT THOMAS: [inaudible]

LG FORSBERG: [inaudible]

REG LEVY: [inaudible]

REG LEVY: [inaudible]

LG FORSBERG: [inaudible]

JOANNA KULESZA: [inaudible]

LG FORSBERG: [inaudible]

CAREL BITTER: [inaudible]

LG FORSBERG: [inaudible]

BEN COON: [inaudible] También vemos específicamente lo que se está haciendo. Cuando informamos algo a los proveedores o a los registradores, ellos nos ponen mucha presión. Nosotros lo vemos, lo analizamos con mucha seriedad para asegurarnos de que lo que aparece en la lista realmente corresponda a un caso legítimo malicioso o de phishing. De lo contrario lo retiramos de inmediato. Como decía Carel, al cabo de unos minutos.

LG FORSBERG: Gracias, Ben. Queda claro por lo hablado hasta ahora que no existe un loop de retroalimentación claro para reportar una indicación de uso indebido como algo que ha sido resuelto o falso positivo. Roman, ¿considera usted que estarían dispuesto trabajar de una manera estandarizada para recibir la información de múltiples fuentes? ¿Qué piensa usted que sería necesario para facilitarlo y que sea confiable?

ROMAN HUESSY: Es interesante este punto. Por supuesto, no tengo una respuesta directa que dar pero creo que sería una buena forma de facilitar y generar confianza en la comunidad tener algo así. Sin duda es algo en lo cual se puede trabajar. Qué sería el paraguas de una cosa de este

tipo es quizá un tema que podría tratar la ICANN o que deba resolver la industria.

LG FORSBERG: Gracias, Roman. Joanna, quiero volver a usted y hacerle una pregunta. No se refiere directamente a las listas de bloqueo de reputación pero qué medidas de seguridad piensa usted que se necesitan para que los registradores y registros no actúen más allá de los mandatos estipulados para ellos e inhabilitan nombres de dominio.

JOANNA KULESZA: Tiene que ver, como decía Matt, con transparencia. Cuanto más claros son los datos y cuanto más abiertos estén los proveedores de RBL a discutir los criterios que se aplican más sencillo será para que el usuario final promedio entienda los procesos y pueda ser oído. Yo creo firmemente que es aquí donde At-Large puede ayudar a definir las expectativas. Las respuestas pueden ser regionales. Esto ya lo hablamos. At-Large está trabajando en una campaña de creación de capacidades sobre el uso indebido del DNS que comience regionalmente y estas respuestas podrían ser regionales, podría haber distintas respuestas en los distintos países, en las distintas RALO. Hemos tenido una sesión al respecto. Pueden surgir distintas respuestas pero esto sería en beneficio del modelo de múltiples partes interesadas en mi opinión. Reiterando, tiene que ver con la transparencia de los procesos, con comprender cómo funcionan y, como ha venido haciendo desde siempre la comunidad de la ICANN, actuar con buena fe para avanzar positivamente. Gracias.

LG FORSBERG: Gracias, Joanna. Voy a tomar una pregunta del público que pregunta Volker. ¿Por qué tantas listas de bloqueo de reputación no proporcionan prueba en los informes? Sin prueba de acciones de referencia específica, ¿cómo se puede tomar una decisión? Esta pregunta se la voy a pasar a Carel.

CAREL BITTER: Sí. Voy a hablar del aspecto de spam, que es el que más conozco. Los informes de spam vienen de corporaciones con grandes ISP donde comparten características con nosotros. Los spammers trabajan muy bien a la hora de hacer un seguimiento de los detalles y vincularlos con URL o con correos electrónicos. La escala a la que recibimos toda esta información nos hace imposible garantizar que las pruebas hayan sido provistas de manera adecuada. Es un punto que hay que decidir, la protección de las fuentes.

Estamos siempre dispuestos a título individual, en cada caso individual, a darles a las personas la evidencia que requieren pero de manera automatizada no es posible para darles una idea. Cada serie de honeypots que nosotros operamos, recibe 2.000, 3.000 correos por segundo. No hay manera de manejar o garantizar que los datos estén limpios sin identificar las fuentes. Como decía, si las personas que trabajan en remediación necesitan pruebas específicas, saben dónde contactarnos, dónde está la gente que trabaja con los datos y ahí podrán obtener los detalles cuando es posible.

LG FORSBERG: Gracias, Carel. Lamentablemente con esto ha concluido la sesión de hoy porque nos hemos quedado sin tiempo pero viendo las respuestas de la encuesta yo diría que el público ha sido bastante amplio. Hay personas que no han oído hablar demasiado acerca de los distintos tipos de uso indebido y otras que sí claramente los conocen. Personas que nunca han tenido que involucrarse en mitigación y otras que sí. Muchos de nosotros hemos aprendido mucho de esta discusión. Esperamos poder aplicarlo a nuestro trabajo en este tema.

Quiero agradecer a todos los panelistas por su tiempo y participación, al personal de la ICANN por su apoyo y, por último, pero no menos importante, al público que ha apartado su tiempo para estar en esta sesión, en esta ocupada semana. Entender las listas de bloqueo de reputación, su propósito, cómo se usan o cómo contactarlas para corregir errores es un paso muy importante para desarrollar maneras de trabajar con ellas y en el uso indebido del DNS. Es largo el camino que debemos atravesar pero espero que hoy hayamos avanzado un poco. Nuevamente, gracias a todos por participar.

BRENDA BREWER: Tenemos la última pregunta de la encuesta. La vamos a abrir. Un segundo. La pregunta debe estar en pantalla. ¿Tienen conocimiento de cómo reportar una amenaza de seguridad o cómo tomar otras medidas para mitigar estas amenazas? Por favor, respondan por sí o por no. Repito la pregunta. Si tienen conocimiento de cómo se puede reportar una amenaza a la seguridad o cómo tomar otras medidas

para mitigar esas amenazas. Por favor, respondan por sí o por no. Gracias. Voy a cerrar la encuesta y compartir los resultados. Muchas gracias por su participación hoy. Concluye la sesión.

[FIN DE LA TRANSCRIPCIÓN]