MONTREAL – Taller de las DNSSEC (2 de 2)
Miércoles, 6 de noviembre de 2019 – 15:15 a 116:45 EDT
ICANN66 | Montreal, Canadá

DAN YORK: Por favor, el dueño de este USB, por favor que venga a retirarlo. Como mencionamos previamente, después de la presentación de Russ sobre la RPKI tenemos dos presentaciones más sobre este tema de seguridad de enrutamiento. Ahora Jaap nos va a contar sobre las aventuras en RPKI.

JAAP AKKERHUIS: Sí, nuevas aventuras. El tema de RPKI dice nuevas aventuras pero es un tema muy antiguo que está cobrando nueva vida. Por eso es popular. Debo decir que este trabajo lo hicimos en el NLNetLabs. Yo soy solo una voz. Hay otros que hicieron el trabajo real. Lo tengo que decir aquí en este público porque esa persona está aquí presente. ¿Hace clic? Sí. Enrutamiento en realidad es seguridad del enrutamiento. Muchas partes de la Internet hacen seguridad. Todo esto lo hemos visto en Netflix, que lo llama de una forma. Hay otros que lo llaman de otra. A pesar de que hace tiempo que está, jamás lo abordamos en detalle por falta de dinero, gente y energía. Veamos rápidamente de qué se trata. La infraestructura de clave pública de recursos está estandarizada en el RFC 6480-6493 y tiene como propósito hacer que el enrutamiento de la Internet sea más seguro. No totalmente seguro sino más seguro. Proporciona ahora validación de origen de la ruta que es parte de lo que sería hacer validación

completa de la ruta. Validar el transporte del paquete. La validación del origen de la ruta ya se trató.

RUSS MUNDY: No en detalle.

JAAP AKKERHUIS: Okey. Ahora lo veremos de un modo distinto. Tiene que ver con el enrutamiento por BGP, con determinar de dónde viene el enrutamiento. Los operadores, las partes de confianza descargan y verifican estas autorizaciones ROA y las decisiones se basan en el resultado de esta validación del ROA. La pregunta es si esta originación de la ruta por BGP ha sido autorizada por el titular legítimo del espacio de la dirección IP porque algún otro puede publicitar o anunciar una ruta y suceder otras cosas. Así se ve. El espacio es delegado. En este caso AS199664, el sistema autónomo. Está todo firmado. Es nuestro AS en nuestra base de datos.

Todos conocen las regiones. Avancemos. Cada una de ellas tiene su propia parte del espacio de los datos que firman. Cada uno de los registros regionales se dirige a los miembros y los miembros hacen el envío a los clientes. La RPKI alojada es aquella donde los recursos están contenidos como un servicio. Los certificados, las claves y los productos firmados se mantienen y publican en su infraestructura. Es un cliente. La otra manera de hacer RPKI es tener el propio certificado y vincularlo con los bloques que uno usa. He firmado por el registro pero uno es titular de la propia certificación de autoridad. Así uno

puede emitir certificados a los propios clientes y publicarlos uno mismo. Esa es la otra manera de hacerlo.

La RPKI alojada, todos los RIR lo ofrecen desde el 2011. Ya les decía que era tecnología antigua. Es fácil de comenzar y de usar porque en realidad no hay que hacer nada. Es muy bueno para adquirir experiencia operativa con la tecnología. No tiene ningún costo de energía porque uno ya es miembro en la RPKI. No hay que preocuparse por el tiempo de actividad ni la disponibilidad, al menos no directamente. Quizá indirectamente pero ese es un detalle menor. Aquí ven cómo funciona. Esto es para RIPE NCC. Tenemos el cliente NLNetLabs. Hay dos anuncios de BGP. Dos para IPv6 y uno para IPv4. No hay problemas. Todo muy bonito.

RPKI alojada. Ahí entramos en algunos problemas, en especial cuando estamos hablando de una entidad grande. Hay distintos tipos de niveles. Hay que tener interfaces propias con distintas funcionalidades, con distintos sistemas de renovación de las ROA. Se puede usar la base de datos para distintos propósitos. Hay distintos niveles de actualización de las publicaciones. Luego la interfaz de programa de aplicación puede ser distinta y también distintos niveles de soporte.

Esto hace que sea difícil si se maneja una gran base, brindar el mismo producto porque cada uno lo puede hacer un poquito distinto. En la RPKI delegada, uno lo maneja solo. Uno maneja la propia certificación como entidad hija del registro. Se instala y se mantiene el software directamente. El software era difícil de instalar al comienzo pero ahora

es distinto. Para hacerlo hay que manejar los propios certificados y hacerlos firmar por la entidad padre. Uno publica los objetos firmados y la gente puede ver los objetos ya sea a través de la autoridad de certificación que uno puede hacerlo directamente o contratar a otro. Esto significa que uno es operativamente independiente del RIR. En especial se puede trabajar un solo sistema sin necesidad de mantener las ROA en cinco interfaces distintas. Uno puede controlar los intervalos de publicación de las ROA y delegarlo como servicio a los clientes.

Estas son las ventajas y desventajas a considerar. Qué pasa si hay un problema, si se rompe, si la cadena de autorización se rompe. No es como en el DNSSEC. Esto no significa que la zona no va a estar ya disponible porque RPKI da una afirmación positiva de una intención de enrutamiento. Si se perdió la clave, si hay un fallo de hardware, si el servidor de publicación recibe un ataque DDoS, todo esto pasa al estado de no encontrado. Como si nunca hubiera existido la RPKI.

Siempre se necesitaron herramientas para mejorar el enrutamiento y la Internet pero hay dos problemas. Tenemos código abierto y a veces el problema en este ambiente es que no se puede solicitar nada y no se encuentra gente. Hay gente que está dispuesta a financiar el trabajo existente que estamos haciendo para avanzar. Aquí están. Son DigitalOcean, el ccTLD de Brasil, NIC .BR. RIPE ahora tiene un fondo para proyectos de comunidad que trabaja desde hace un tiempo. Juniper y Cisco, Mozilla, Nokia y el Centro de Ciberseguridad de los Países Bajos. Con ellos se pudo acelerar por dos propósitos. El primer propósito es Krill. Uno de sus desarrolladores trabaja en las ciencias

biológicas. Por eso se llama así. Tiene un Doctorado en Biología. El kril son estas pequeñas cositas que hacen que el resto del mundo funcione. Esta es la parte de la certificación del producto. Uno puede ser titular de los propios certificados con API, CLI e interfaz de usuario. Pueden crearse objetos RPKI. Hay un servidor de publicaciones RFC y también tiene anclaje de confianza incorporado para simular pruebas y operar en modo remoto. Hay soporte multimaestro y soporte HSM si uno quiere hacerlo. Está todo esto disponible. Es la versión reciente de hace dos semanas. Es para pruebas.

Será lanzado a producción con nuestros amigos brasileños en diciembre de 2019. Parece prometedor. Casi listo a la fecha. Ahora está en prueba y ahí estará disponible para todos. Si ustedes quieren pueden bajarlo de nuestro sitio, hacer pruebas y luego enviar los informes. En este estado permite hacer operación de prueba y otras cosas. La documentación es un poquito escasa pero hay un sitio web que tiene toda la documentación detallada.

El otro componente es el Routinator que es para hacer el trabajo con los RIR. Es un producto que ya se usa en varios lugares del mundo. Qué hace. Nuevamente tenemos los RIR y los [sub-RIR] y los [N-RIR] y probablemente se unan más. Hay una parte de confianza que recopila toda la información de los ROA y ahí se toman decisiones de enrutamiento. Ahí es donde entró CISCO porque ellos tienen forma de descargar esto en los enrutadores pero no es parte de nuestro software. Es de ellos.

El estado de despliegue en general, ahora se está comenzando a convertir en un ecosistema saludable con siete implementaciones distintas de validador de RPKI. Algunos primitivos y otros muy sofisticados. Aparentemente, todos se inspiraron ya. Como dije, los brasileños tendrán los certificados en producción en diciembre y la validación estricta tiene lugar en todos los PoP de Cloudflare. Hay gente que está incorporándose como AT&T, Nordunet, KPN y Telia, que rechazaron inválidos en sus sesiones de EBGP. Hay filtrado de servidores de rutas en puntos de intercambio de Internet como los que ven aquí y se unirán más. La documentación la pueden encontrar en RPKI.readthedocs.io con todos los detalles de cómo usar las herramientas, en especial Krill y Routinator. Aquí algunos sitios web vinculados. ¿Alguna pregunta?

DAN YORK: ¿Alguien tiene alguna pregunta? ¿Nadie tiene ninguna pregunta para Jaap? No puede ser. Alguien tiene que tener alguna pregunta.

JACQUES LATOUR: Es una pregunta de un novato, supongo. Si usted puede tener su RPKI alojada o delegada o donde sea, ¿dónde se ubica la firma y dónde está el registro de la RPKI?

JAAP AKKERHUIS: ¿Su propio registro de la RPKI? Si la RPKI está alojada…

JACQUES LATOUR: Tengo un registro. ¿Dónde está ese registro? ¿Cómo hace alguien para encontrarlo? Disculpen, no leí lo suficiente. Es una pregunta de un novato.

RUSS MUNDY: Voy a tratar de reformular la pregunta de Jacques y también la respuesta de Jaap. Los certificados de verificación de ROA en el caso de la RPKI alojada, cuando usted trabaja con su RIR, eso está en la memoria caché del RIR. Cuando usted utiliza o hace su propia validación con Routinator, el Routinator genera sus propios conjuntos de datos a partir de lo que le brindan los cinco RIR. En un enrutador la información que usted obtiene proviene de su instancia local. Usted valida a nivel local pero tiene que buscar la información desde otro sitio.

JACQUES LATOUR: Ahora sí soy un experto. Gracias.

JAAP AKKERHUIS: Es como una gran memoria caché del DNS básicamente. El Routinator envía la información en distintos formatos y en distintas versiones. Esto se hace automáticamente con todos los RIR, incluso si usted ha dado autorización para la firma de zonas. Eso ya es un problema político.

RUSS MUNDY: Algo que para mí es una diferencia significativa entre las especificaciones para las DNSSEC y para la RPKI y la validación correspondiente es lo siguiente. En el caso de las DNSSEC, las especificaciones originales dicen que si alguien no realiza la validación exitosamente, entonces no envió una respuesta y eso implica una falla. El software de la RPKI le deja a usted un rango de maniobra para ver qué va a hacer con la validación. Esa decisión política se hace a nivel local. Usted puede aceptar rutas o vías de enrutamiento no validadas si usted así lo decide. Warren, tiene la palabra.

WARREN KUMARI: Creo que en la especificación se indica lo siguiente. Usted tiene que tomar la instancia de validación y decidir la política de enrutamiento con su comunidad. Creo que actualmente algunas personas prefieren algo validado en lugar de no validado pero no hay muchas personas que elijan otra vía de acción. Algunas personas lo están haciendo en Sudamérica y en Ecuador, algunos IXP. No se da una recomendación específica porque eso depende del operador.

RUSS MUNDY: En mi opinión, esto facilita la implementación en comparación a las especificaciones de las DNSSEC. Es decir, que la política quede en manos del operador local es un cambio muy significativo.

DAN YORK: Warren, no entendí bien lo que usted dijo. Disculpe. Muy bien. Ya quedó claro. ¿Hay alguien que tenga otra pregunta? ¿Alguna otra

pregunta para Jaap? Gracias, Jaap, por su trabajo, por mostrarnos esta tarea de NLNetLabs. Muchas gracias.

Ahora me voy a quedar de pie para dar mi presentación. Nosotros hablamos de la seguridad de BGP y de la RPKI. Me dijeron que tenía que preparar una diapositiva más contundente o impactante para hablar sobre este tema. ¿Cuántos conocen esta iniciativa MANRS? ¿Cuántos son miembros de la iniciativa MANRS? Muy bien. ¿Cuántos están en el observatorio MANRS? Buenísimo. Vamos a ayudar a los demás participantes a que entiendan de qué se trata esto.

Les voy a contar acerca del BGP. Ya hablamos acerca de BGP, de este protocolo. Vamos a seguir adelante. Todos sabemos acerca de los incidentes de enrutamiento. En respuesta a qué sucede cuando tenemos un incidente de gravedad, en 2014 algunos operadores de red se reunieron para ponerse de acuerdo acerca de las medidas para proteger sus redes y surgió este proyecto de las normas mutuamente acordadas para la seguridad de enrutamiento o MANRS. Ustedes pueden ir a nuestro sitio web y ver de qué se trata. Esta es una iniciativa en la comunidad de enrutamiento y en la comunidad de operadores de redes para determinar comportamientos en común de manera tal que todos tengamos un determinado nivel de seguridad de enrutamiento.

Para los operadores de redes hay cuatro acciones necesarias, cuatro acciones para ser parte de esta red MANRS. Primero la operación de filtros o filtrado. Es decir, evitar spoofing. Lo pueden ver aquí en pantalla. Evitar la propagación del enrutamiento de información

incorrecta. También llegar a la validación global que nos lleva a la RPKI. Quienes son parte del proyecto MANRS están de acuerdo en publicar sus ROA para que las otras personas también puedan actuar de la misma manera. También trabajamos con los puntos de intercambio de Internet, los IXP, de manera tal que ellos también acuerden llevar a cabo estas acciones que son un tanto distintas. Nuevamente está el tema del filtrado, el tema de promover la iniciativa MANRS entre los miembros del IXP pero básicamente ellos también tienen que acordar implementar estas acciones.

Aquí tenemos las últimas novedades en MANRS. Hemos creado un conjunto preliminar de acciones con los proveedores de servicios de CDN y de servicios de computación en la nube. En la última reunión de los operadores de red terminamos de plasmar esta iniciativa. Tienen este borrador en el sitio web de MANRS y con todo gusto vamos a recibir sus comentarios porque realmente son muy bienvenidos. Allí tienen, en nuestro sitio web, una lista de recursos también de consulta relacionados con este documento.

También tenemos a uno de los líderes aquí presentes. Uno de los líderes de esta iniciativa está presente aquí en la sala y acaba de levantar la mano para que lo identifiquen. Les acabo de dar la URL. Ustedes pueden participar. Tenemos un gran nivel de adopción. Tenemos 42 puntos de intercambio de Internet y 237 operadores de red y esto sigue en crecimiento. Nos gustaría ver que la membresía crece aún más y que más personas se van sumando a este proyecto.

Nosotros consideramos que es maravilloso cumplir con los requisitos de este proyecto MANRS. ¿Cómo podemos saber si realmente alguien está cumpliendo con estos requisitos, porque es toda una iniciativa voluntaria y cada uno informa lo que va haciendo, etc.? Pensamos en cómo medir esta información, cómo registrar el cumplimiento con el proyecto MANRS y sus acciones específicas, para ayudar a los miembros de nuestro proyecto justamente a que entiendan y conozcan su nivel de cumplimiento. Por ejemplo, si utilizan RPKI, si hacen tal o cual validación, cómo lo pueden corroborar.

Asimismo, queríamos darles un mecanismo de manera tal que se tenga una medición pública para que la gente conozca cuál es la situación en el mundo de la seguridad del enrutamiento. Presentamos un marco de medición. Primero desarrollamos este marco con distintas fuentes que nos dieron datos, entre ellos la entidad de Jaap, aquí presente, NLNetLabs. Así pudimos identificar distintas fuentes de datos, mediciones factibles. Ahora tenemos este observatorio MANRS. Si van a nuestro sitio web observatory.manrs.org pueden acceder a esta información. Tienen dos opciones. Una vista pública y una vista privada. Los miembros de MANRS pueden ingresar a la vista privada que les permite ver sus propias estadísticas y compararlas con las de otros miembros. Así se ve la información en nuestro observatorio MANRS. Tenemos algunas capturas de pantalla con los distintos incidentes de seguridad de enrutamiento. Pueden ver también la información por regiones en distintas partes del mundo. Aquí tienen los valores correspondientes. También pueden ver un historial a partir del comienzo del año 2019.

Es una herramienta muy útil que les permite ver cuántos miembros están listos para cumplir con una acción en particular del proyecto MANRS, cuántos están un poco atrasados, etc. Si entran en más detalle en el historial, pueden ver distintos cuadros y también tenemos una página comparativa en la cual podemos comparar distintos datos, estadísticas e investigaciones.

En la vista privada, cuando ya son miembros de MANRS, pueden hacer inicio de sesión y ver una parte distinta con más información. Pueden ver sus propios ASN, su nivel de cumplimiento y también ustedes pueden ubicarse en esta tabla de clasificación y ver su nivel de preparación. Es decir, esta es la información que ya está disponible y también a veces tienen algún tipo de ayuda. Por ejemplo, algún motivo posible de tal o cual situación o incidente.

Esto es lo que tenemos al día de hoy en nuestro observatorio MANRS. Nos gustaría tener una mayor cantidad de miembros porque así podemos fortalecer y asegurar la estructura de enrutamiento en Internet. Ustedes también, si se suman, van a poder interactuar con otros colegas de la comunidad. Ahora le voy a dar la palabra a Warren que seguro me quiere hacer una pregunta.

WARREN KUMARI: Warren Kumari, de Google. Muchas gracias. ¿Me puede explicar por qué hay que iniciar sesión para obtener más información acerca de una red?

DAN YORK: Durante un tiempo la información estaba abierta a todas las personas. Todos podían ver la información y darnos su opinión acerca del observatorio MANRS pero hay alguna información sensible de algunos operadores de red que no quieren que todos sus datos estén totalmente disponibles. Entonces tenemos la vista pública y luego los miembros pueden iniciar sesión. Probablemente a futuro toda la información sea de acceso abierto.

AFTAB SIDDIQUI: Nosotros comenzamos teniendo datos con acceso abierto pero los participantes decidieron que mientras estuviéramos en la etapa de mejoramiento de datos sería una buena idea dividir el acceso a estos datos. Nosotros utilizamos datos de terceros. A veces esto podría generar un problema para los grandes operadores. Estamos trabajando para que esto sea lo más transparente posible pero por el momento hay que hacer inicio de sesión para acceder a determinados datos. Aun así, tienen una vista global que les da un buen pantallazo de lo que está sucediendo.

DAN YORK: Adelante, Warren. Tiene la palabra.

WARREN KUMARI: La ventaja de tener una vista abierta para todos no es ver a quién le va mal y a quién le va bien sino que nos permite ver que la gente está realmente haciendo lo que debería hacer, que cumple con lo que tiene que hacer y también nos permite ver quién está preparado para

implementar determinadas actividades y quién está preparado efectivamente. Entiendo que esto genera cierto debate.

ORADOR DESCONOCIDO: Sí, claro. Por eso quisimos abrir la información pero esta es una iniciativa impulsada por los miembros. Queremos darle el mayor apoyo posible. Los miembros nos han dicho esto. Esto es lo que acordamos con la mayoría de los miembros. Usted es uno de ellos. A la larga vamos a compartir toda la información.

DAN YORK: Nosotros queremos ayudar desde Internet con este proyecto pero por supuesto que depende de la comunidad de MANRS. Nosotros estamos facilitando esto. Toma la palabra Dave.

DAVE: Yo quería decir justamente esto, que no estaba en su presentación. La entidad Internet Society realmente fue de gran ayuda en la coordinación de este proyecto, en impulsar este proyecto. No vi que estaba el logo de la ISOC en ninguna parte. Esto es algo que agradecemos. De todas maneras, Internet Society merece nuestro reconocimiento por impulsar este proyecto.

DAN YORK: Sí, claro. Yo trabajo en el equipo de comunicaciones de la ISOC y siempre utilizo el logo pero esta es una de las excepciones.

WARREN KUMARI: Creo que este es un proyecto de mucha utilidad y le agradezco mucho a la ISOC también. No quise ser impertinente o incomodarlo con mi pregunta.

DAN YORK: También agradecemos a los miembros de este proyecto porque son ustedes quienes lo han llevado adelante. En algunos casos hubo periodistas que se interesaron en ver estos datos, la infraestructura de enrutamiento, qué pasa con toda esta situación, porque siempre escuchamos acerca de estas novedades. También los funcionarios públicos y del gobierno quieren ver qué pasa en sus propios países con toda la seguridad de enrutamiento.

¿Alguien más tiene alguna pregunta o algún comentario? ¿No tienen ninguna pregunta difícil? Si todavía no se sumaron al proyecto MANRS y si están haciendo algunas de estas actividades, si tienen un número del sistema autónomo pueden unirse al proyecto MANRS. Los invitamos a que se sumen para que juntos sigamos fortaleciendo la seguridad de la capa de enrutamiento de Internet. El sitio web observatory.manrs.org es abierto. Estamos abiertos a recibir sus comentarios. Queremos saber qué les viene bien, qué cosa no entienden, en qué caso necesitan una explicación, etc. Los invitamos a ver el sitio web. Pueden hablar conmigo o con mi colega del equipo de MANRS y también estar en contacto con nosotros más adelante. Gracias. Ahora vamos a hacer algo que tampoco está relacionado directamente con DNSSEC. Aquí estamos.

MARC VAN WESEMAEL: Soy Marc Van Wesemael, el CEO de EURid. Buenas tardes. Fuimos invitados para hablar acerca de lo que hacemos para luchar contra el uso indebido en el espacio de .EU. Comenzó hace unos años, como una idea de reducir el impacto de registraciones posiblemente abusivas. Por un lado es un gran impacto de la reputación del TLD si pasan cosas muy malas y llegan a la prensa. Además, puede ser una gran responsabilidad si el dominio está activo y se suprime mal o en un momento incorrecto. Esto puede tener un impacto financiero.

Comenzamos con una pregunta. ¿No sería posible suprimir o bloquear el nombre de dominio, impedir que sea activo, si tenemos la certeza de que está cometiendo uso indebido? Fuimos a la Universidad de Laverne e hicimos esta pregunta, si existía alguna posibilidad de hacer este tipo de trabajo. El siguiente orador, Lieven Desmet, nos va a contar un poquito qué hicimos y qué no hicimos para cumplir con este objetivo.

Antes, un par de palabras más de mi parte. Esto forma parte de una estrategia más extensa para el espacio de confianza de .EU que tiene que ver con parte prevención y parte de habilitación o empoderamiento, darle herramientas a la gente para encontrar usos indebidos, para ayudarnos a encontrarlos. Cuando los encontramos, porque no pudimos prevenirlos, remediarlos de manera sencilla y rápida.

Esta parte es la parte superior, la de la prevención. Hablamos de una delegación demorada. El caso es que cuando vemos una registración

potencialmente inapropiada demoramos la delegación del nombre de dominio que ya ha sido registrado. No entra en el archivo de la zona y se inicia un proceso manual donde solicitamos prueba de identidad al usuario y si hay una mala intención no permitimos que el dominio entre en actividad y se previene el perjuicio. Ahora le doy la palabra a Lieven, que nos dará una explicación más técnica.

LIEVEN DESMET: Gracias, Marc. Para relacionarme con lo que hicimos en la sesión de la mañana sobre uso indebido, quiero dar en los próximos 15-20 minutos una explicación de cómo entender un poquito mejor cómo funciona este comportamiento de uso indebido. Qué es lo que podemos hacer y qué no podemos hacer para prevenirlo. Somos académicos. Esto hace tiempo que lo estudiamos de manera profunda y lo primero que quiero mostrarles es lo que surgió del estudio de 14 meses de TLD .EU, que se presentó en el 2017. Aquí lo que intentamos es capturar el comportamiento de los malos actores en el dominio TLD .EU. Cada línea representa un actor individual y la intensidad del punto es el número de registraciones indebidas que aparecen en listas negras como SURBL y otras.

Intentamos entender mejor cómo se genera la lógica de creación de estos nombres. Tienen distintas características. Una campaña muy sencilla, c-14. Utilizan un único registratario falso. Lo usa solo 41 días y en total lograron casi mil nombres de dominio en la lista negra que eran casi todos dominios registrados durante este periodo. Esto es

muy sencillo. Es un solo registratario que va probando hasta que se ve bloqueado.

Una campaña más avanzada, más creativa, en este caso el actor utiliza combinaciones de dos cuentas de email, tres números de teléfono y cuatro direcciones postales. Las combina y usa a los registratarios durante un periodo de ocho meses para registrar unos 1.300 nombres de dominio. La iteración es mucho mejor. Solo el 50% de las registraciones fueron a la lista negra. En total, 2.500 registraciones de este actor.

Otro ejemplo, para darles una idea de una campaña más avanzada. En aquella época en que estudiábamos este conjunto de datos la definimos como la más avanzada. Aquí tenemos casi 100 en un periodo de ocho meses que generaron las registraciones con una herramienta que se llama Laravel Faker. Los nombres de dominio estaban compuestos por palabras en holandés de dos o tres caracteres distintos. Fui interesante ver que lo hacían a diario. Utilizaban lotes de 8, 16, 24 o 32 registraciones. Esta fue la campaña más avanzada en ese periodo.

Vinculando esto con lo que vimos antes, una de las conclusiones a las que arribamos es que en estos 14 meses de registraciones solo pocos actores, casi 20, representan el 80% de las registraciones maliciosas en .EU. En el ecosistema, si los identificamos y podemos hacerles la vida difícil a estos 20 tendríamos un impacto positivo en el TLD. En estos datos vimos que las campañas estaban relacionadas entre sí. En este periodo de 40 meses hubo unos 50 actores. Cuando se registra un

nombre de dominio, se usan facilitadores: servidores de nombres, dirección de mail, proveedor de mail como registratario, un registrador para registrar el número, un número telefónico. Vimos la reputación de estos facilitadores en nuestro dataset. Por ejemplo, los registradores 3, 5 y 7 en nuestro conjunto de datos, aquí podemos ver el nivel de popularidad en los datos. El primero, el 5, tenía más o menos 10.000 en la lista negra. El tres, 3.000 y el 7, 2.000.

Aquí lo importante es que para el registrador 5 representaba casi la mitad de los nombres de dominio en la lista negra. En términos de toxicidad, una de cada tres registraciones de este registratario en .EU estaba en la lista negra. Puede ser un registrador pero también puede ser otra parte en el ecosistema.

En el caso de los proveedores de email es más complicado. Gmail, Yahoo y AOL son los proveedores más populares. Es muy obvio que hay otros que permiten crear cuentas gratuitas. Las cuentas Gmail representan el 20% de las registraciones maliciosas pero la toxicidad es del 2%. En nuestro conjunto de datos es por debajo del promedio. Tener un proveedor de mail muy popular, Gmail, no necesariamente significa que la cuenta será maliciosa.

En comparación con AOL, que solo tiene el 10% de la contribución de las registraciones maliciosas, aquí vemos que su toxicidad era de casi el 46%. Una de cada dos registraciones es un registratario con una dirección AOL que era maliciosa en nuestro conjunto de datos. Al interpretar los datos tenemos que tener en cuenta el sesgo. Por

ejemplo, en Europa, AOL ya no es tan popular o ya no es en general popular pero los atacantes lo pueden usar para sus sistemas.

Otros datos. No voy a darles detalles de todas las conclusiones a las que llegamos. Algunas voy a mencionar. Otro es que la mayoría de los dominios en lista negra estaban relacionados con spam. También vimos que la lista negra se produce después de la registración. Tres de cuatro son incluidos en la lista después de los primeros cinco días.

Por último, vemos que los actores exhiben conductas humanas o lo que podríamos definir así. Vemos que las campañas en general son manuales en un horario de 9 a 5. Se toman vacaciones de verano, de invierno. A veces tienen errores tipográficos. Por distintas razones cambian sus estrategias con el tiempo.

Con esto espero haberles dado una idea de cómo se hacen estas campañas para registrar nombres en .EU. Ahora qué podemos hacer al respecto. Esto está publicado en PREMADOMA, que se presentó en diciembre en Puerto Rico. Aquí es ver cómo utilizar el sistema de aprendizaje por máquina con un sistema que pueda detectar o prevenir conductas maliciosas. Comenzamos con una máquina típica que tomó todas las registraciones previas de .EU. Combinamos con el etiquetado de Spamhaus de la navegación por Google. Se hizo un modelo de predicción que permite así que toda nueva registración en el momento de la registración, antes de entrar al archivo de la zona se hace predicción y se define si hay o no intención maliciosa. Sobre esa base se toman distintas acciones. Puede ser demorar la activación antes de llevarlo al archivo de la zona.

Estas técnicas de aprendizaje por máquina, y lo pueden leer en el documento en más detalle, hay dos tipos de algoritmos. El primero es la similitud. En estas campañas hay mucha similitud en la creación de los nombres. Esa similitud permite mapear las registraciones entrantes en grupos de registraciones maliciosas en comparación con nuestro conjunto de datos.

El segundo abordaje es la clasificación típica de aprendizaje por máquina. Esto se combina con características de reputación de los facilitadores. Los proveedores de email, los registradores de mail, los teléfonos y demás. Con esto se logran muy buenos resultados de predicción. En el sistema en .EU combinamos los dos sistemas.

Basándonos en los datos históricos, en los 14 meses de datos, el sistema está funcionando muy bien. Pudimos así capturar dos de tres registraciones con una precisión del 84%. Estos resultados tienen una tasa de falsos positivos de 0.3%. La mayoría de las campañas pueden manejarse por estas técnicas. Queríamos ver cómo esto opera en tiempo real con nuevos datos entrantes en el espacio .EU. Este es un gráfico de julio de 2017 a enero de 2019. En verde vemos las registraciones maliciosas en .EU. Por lo menos las que están en los servicios de lista negra. La superficie en verde es el número de registraciones de este grupo malicioso que pudimos predecir. Como ven, pudimos predecir una gran fracción aunque todavía no tenemos información sobre la registración. Solo hora y fecha. Vemos que el volumen de registraciones maliciosas bajó radicalmente desde enero de 2018 porque informamos o reportamos al equipo jurídico todas estas informaciones que atemorizaron y dejaron de actuar desde julio

de 2018. El volumen de registraciones maliciosas a partir de entonces es muy bajo. Como resultado final, se suspendieron estos dominios.

Veamos las estadísticas de los 18 meses presentados. Tuvimos un 85% de predicción del sistema con una precisión mucho más baja que la que tuvimos en la condición inicial. Aquí la predicción es del 72%. Si queremos explicar estas dos cifras y la diferencia de las condiciones anteriores, el primero es que tuvimos campañas muy grandes de octubre de 2017 a marzo de 2018. Estas grandes campañas fueron muy fáciles de detectar y por eso tuvimos un índice de suspensión muy alto. Si el mismo registratario registra dos nombres de dominio en los mismos 10 segundos, la lista negra solo captura una fracción de esos nombres de dominio. Esa es también la razón por la cual hicimos un tercer estudio que es el análisis de la verdad de base para evaluar la efectividad de las listas negras a la hora de predecir si un nombre de dominio es malicioso o no.

Cuáles fueron las preguntas que nos hicimos. Un nombre de dominio aun no termina en una lista negra pero viene del mismo actor malicioso, ¿por qué sucede esto? Porque el nombre de dominio no es registrado por los servicios de lista negra entonces no lo detectaron o es porque el nombre de dominio nunca estuvo activo, nunca fue malicioso, por eso no tiene que estar en la lista negra. Nos interesaron los que no estuvieron en la lista en nuestro conjunto de datos ya sea porque los pasamos por alto o porque no se usaron.

Estudiamos los cinco registratarios más grandes con nombres maliciosos en el archivo de zona en el primer y segundo trimestre de

2018 y después de la registración estudiamos el patrón de actividad entrante en el servidor del TLD .EU. Utilizamos queries y DNS de log pasivo. De los que estaban en la lista negra vimos la gran mayoría de estos nombres que indican que estuvieron activos en el periodo con picos, por lo general spam y un pequeño porcentaje no estuvo activo o por lo menos en los servidores de TLD .EU que investigamos.

El caso es un poco distinto para los que no estuvieron en la lista. Ahí tenemos una división 50-50 entre los que estuvieron activos y los latentes. En este sentido hay ambas hipótesis válidas. O bien pasamos por alto la actividad o los que registraron los nombres de dominio no los usaron activamente. Nosotros asumimos que hay dos ecosistemas que impulsan esta situación. Uno que en forma regular registra nombres de dominio y un segundo ecosistema que compra los dominios para actividad maliciosa y con distintos patrones.

¿Cuáles son los mensajes a rescatar de aquí? Vimos que en la zona .EU hay solo un pequeño grupo de actores que causa mucho daño. Hasta 20 campañas fueron responsables del 80% de todas las registraciones maliciosas. También hubo dos facilitadores primordiales. Uno, la mitad, a través de un proveedor y otro, un proveedor de email con mucha toxicidad.

Luego vimos que es factible hacer detección y prevención de registraciones. Usamos dos modelos de predicción. Uno basado en reputación y otro en similitud. Pudimos capturar la mayoría de las registraciones maliciosas con el sistema que tenemos ahora y también vimos que hay un aspecto que no quedó completo. Es interesante

entonces saber cómo esto impactará la situación general de seguridad porque queremos ver cómo se comportan estos actores si se combinan distintos TLD en este proyecto. Con esto no me resta más que agradecer y saber si tienen preguntas.

DAN YORK: Muchas gracias. Muy interesante. Veo que Jacques está listo para hacer una pregunta.

JACQUES LATOUR: Sí, usted dijo entonces que quiere hacer crecer este ecosistema. ¿Hay software de código abierto? ¿Cómo podemos participar?

LIEVEN DESMET: Lo que queremos hacer en los próximos seis meses es incorporar otros TLD. Uno o dos primero para ver la factibilidad y para tener una tendencia de monitoreo centralizada la idea es tener gente que solicite nombres de dominio con información de contexto, marginal o no, y usar esos datos para entrenar al sistema. Ahí podríamos conseguir por lo menos hipotéticamente mejores resultados.

JACQUES LATOUR: Por las campañas que nos mostró vemos algo similar en .CA. Si pudiéramos ser proactivos, porque nosotros vemos algo similar, podríamos ser más eficientes. Me gusta mucho esto.

MARK: ¿Cuánto tiempo le llevó entrenar el sistema para la detección?

LIEVEN DESMET: El entrenamiento lleva una media hora pero si uno quiere pasar por alto el sistema o eludirlo creo que eso lleva tiempo para entrar a dominios. Si se pone open-source obviamente lo puede probar solo para ver cómo eludirlo. Puede eludirse, por supuesto. Cualquier máquina puede ser eludida pero lleva tiempo, lleva trabajo de administración.

MARK: ¿Ellos pagaron por las registraciones no exitosas aun cuando no las usaron y no les rembolsan si no se responde al query? Es una manera de consumir recursos. ¿Consideraron ir al registro que fue la fuente de las registraciones maliciosas para ver en qué otras zonas se registraban a través del mismo registrador?

LIEVEN DESMET: Esa información no la tengo porque no tengo información de todas las zonas.

MARC VAN WESEMAEL: Si la pregunta es si contactamos al registrador porque son los mismos registradores los que tienen gran parte de la actividad maliciosa, sí lo hicimos, pero la mayoría de estos registradores trabajan con revendedores. Es un revendedor el responsable. No se puede castigar al registrador por un único revendedor.

MARK: No sugería castigar sino estudiarlo porque ese es el punto de entrada que probablemente sigan usando los mismos malos actores no en .EU ahora sino en otras partes.

LIEVEN DESMET: Nos estamos concentrando solamente en el registrador. Si combinamos más datos de más TLD vamos a identificar patrones de cómo las cosas se están moviendo entre los TLD.

DAN YORK: ¿Alguna otra pregunta?

ORADOR DESCONOCIDO: [inaudible], de Spamhaus. Muy buena investigación, en mi opinión. Hace años que tratamos de decir que hay muchas cosas que los registros pueden hacer para prevenir que haya nombres maliciosos activos. Ustedes tienen muy buenos datos de registración, a los cuales no estamos expuestos. No es necesario cancelar un dominio. Hay otras cosas que se pueden hacer. Como ustedes decían, suspenderlo o demorarlo, rondas de recertificación. Podemos ser creativos. En relación con lo que dijo Mark, es un buen uso de nuestro tiempo combinar los recursos.

A ver, qué iba a decir. Es muy bueno esto de salir de .EU. No puedo decir con certeza que las mismas personas se fueron a otro TLD. Quizá fueron a otro lugar donde los precios, las comisiones son adecuadas y

donde están las herramientas pero se fueron a otra parte. Esto funciona muy bien para que la casa esté limpia pero imagínense si toda la industria lo hiciera. Sería un gran avance.

LIEVEN DESMET: Es cierto pero es un juego entre atacantes y defensores, pero ese es nuestro juego.

DAN YORK: Otra pregunta.

YOSHIRO YONEYA: Perdón. No pude estar presente en la presentación. Mi pregunta es sobre el título. Ustedes dicen uso indebido de nombre de dominio no de DNS. Quería saber por qué hacen referencia en el título a uso indebido de nombre de dominio.

MARC VAN WESEMAEL: Fue un error. Lo pasé por alto. Si lo hubiera preparado antes, hubiera salido mejor.

ORADOR DESCONOCIDO: ¿Puede volver a la diapositiva donde muestra que disminuye la cantidad de registraciones maliciosas de nombres de dominio? En esta diapositiva vemos que la cantidad de registraciones maliciosas de nombres de dominio disminuye pero en cuanto a la proporción entre julio y enero vemos que ese propósito aumentó.

LIEVEN DESMET: Los que se registraron en ese momento eran una registración por única vez, una registración maliciosa por única vez y si se combina con la campaña entonces vemos que da este resultado. Luego relanzamos la campaña y volvimos a captar a estos sitios maliciosos. La idea es que las campañas sean tan buenas que no sigamos registrando estas actividades maliciosas. La idea es que el sistema luego los detecte automáticamente y los elimine. El sistema no puede captar los de única registración.

ORADOR DESCONOCIDO: ¿Qué pasa con los falsos negativos?

LIEVEN DESMET: Los rastreamos, registramos los falsos negativos. Sobre todo eso lo hace nuestro equipo de abogados.

ORADOR DESCONOCIDO: ¿Cuál es la tendencia en falsos negativos en este periodo?

LIEVEN DESMET: Yo diría que tuvimos un 80% que pudimos detectar. Hay un 20% de falsos negativos.

ORADOR DESCONOCIDO: ¿Sigue todo estable, la tendencia?

LIEVEN DESMET: Sí. Sigue estable.

DAN YORK: ¿Alguna otra pregunta o comentario? Cuando yo veía el tema del aprendizaje automatizado me preguntaba si vieron la presentación el lunes. Yoshiro dio una presentación que tiene algunas similitudes con esta presentación y con algunos estudios sobre nombres de dominio. Muchas gracias. Gracias por esta presentación.

Tengo una pregunta para quienes están aquí presentes en nombre de los organizadores del programa. Hoy tuvimos algunas presentaciones. Hablamos acerca de los resolutores de DNS. Russ nos habló acerca de RPKI. Kim habló del traspaso de la KSK. Yoshiro presentó su investigación sobre fallas de validación de DNSSEC. Jaap acerca de RPKI. Yo les hablé del proyecto MANRS.

El comité que organiza este programa tiene la siguiente pregunta. Hoy nos desviamos un poquito del tema de las DNSSEC. Tratamos otros temas también. ¿Qué les parece este nuevo programa? ¿Les gusta? ¿Quieren volver a tratar exclusivamente DNS y DNSSEC? Es decir, queremos escuchar sus comentarios, qué les pareció esta combinación de temas. ¿Les pareció de utilidad? ¿Qué les parece? ¿Hay alguien que me mira? Wes, tiene la palabra. ¿No? ¿Sí? Muy bien. Para los participantes remotos, Wes levantó el pulgar, lo cual no es de demasiada utilidad. Bueno, Warren también levanta el pulgar. Mark, tiene la palabra.

MARK: Creo que fue una buena combinación de temas. Fueron temas muy relevantes. Estuvieron muy bien seleccionados.

DAN YORK: Wes, tiene la palabra.

WES HARDAKER: Creo que hay una serie de tecnologías que impactan sobre las redes y sobre la ICANN. Por ejemplo, el enrutamiento es una de ellas. Todas estas presentaciones fueron muy buenas. Me gustaría a futuro ver presentaciones sobre una diversidad de temas. Así como ustedes clasifican las presentaciones por colores, según el grado de dificultad, me gustaría ver también esa clasificación en esta nueva variedad de temáticas. Me gustaría ver temas a nivel introductorio y también temas más avanzados. Realmente me pareció una buena combinación. Muchas gracias.

DANIEL: Creo que no hay que atacarse siempre en el mismo tema. Hay que evolucionar. Es muy bueno ver que se trataron otros temas en este día, en este taller.

DAN YORK: Alguien solicita la palabra.

ORADOR DESCONOCIDO: Quería decir que estoy de acuerdo con la variedad de los temas pero creo que faltó ver cuál fue el funcionamiento operativo, ver qué pasa con la implementación de las tecnologías de seguridad y ver una estadística un poco más reciente. Eso estaría faltando en el programa.

DAN YORK: No sé si Andrew está aquí. Andrew no está aquí. Andrew McConachie es quien recopiló las diapositivas para esta presentación inicialmente. Nosotros consideramos que es importante hablar acerca del éxito o no de nuestras actividades y nuestras iniciativas. Nosotros ya llevamos alrededor de 10 años haciendo estos talleres en distintos foros así que es válido lo que usted dice. Recibiremos más comentarios, por supuesto. Nosotros justamente decidimos ampliar la temática de nuestros talleres. Por ejemplo, incluir RPKI. Esto fue algo nuevo. Lo hicimos deliberadamente. ¿Van a volver si hacemos un taller de este estilo? Veo que sí, que asienten con la cabeza y que levantan los pulgares. Muy bien.

RUSS MUNDY: Yo soy miembro del comité organizador de este taller. Me gustaría también que propongan más temas que les gustaría tratar en nuestros próximos talleres. Pueden ser temas similares o puede ser algo totalmente nuevo o completamente distinto. Por ejemplo, investigaciones sobre nuevas tecnologías para mejorar la seguridad en el espacio del DNS.

DAN YORK: También tuvimos en otras oportunidades demostraciones de distintos sistemas, nuevas tecnologías, herramientas. Si ustedes quieren mostrarnos sus nuevos sistemas siempre y cuando no vengan a hacer una promoción comercial, por supuesto, ustedes son más que bienvenidos a hacer una demostración. Tenemos la capacidad técnica para hacer una demostración. No vimos cómo Kathy puede pasar de una ventana a la otra en la participación remota pero sabemos que lo puede hacer.

YOSHIRO YONEYA: Yo soy miembro del comité organizador también y tengo una pregunta. Generalmente nosotros invitamos a los participantes a través de nuestra lista de correo electrónico de operación en el DNS. Si queremos tener más propuestas de temas de la comunidad sería bueno enviar una convocatoria a participantes de otra manera. ¿Cómo podemos emitir la convocatoria a participación más allá de toda esta comunidad del DNS? todos venimos de la comunidad del DNS, por supuesto, pero todas las ideas son bienvenidas.

ROD RASMUSSEN: Hay muchísimas listas de correo electrónico con muchos participantes sobre distintos temas. Seguramente hay listas por ejemplo de correo electrónico para la comunidad de seguridad en el enrutamiento que pueden también colaborar con distinta temática de uso indebido, etc. Tendríamos que ver cuáles son los temas que queremos tratar y luego ver cómo emitir la convocatoria en las listas de correo electrónico

correspondientes. También podemos trabajar con otras organizaciones.

DAN YORK: Claro. También hay personas que quieren presentar determinados temas y tenemos que ver cómo pueden viajar a la reunión de la ICANN porque nosotros no brindamos apoyo financiero para viajes. Cada uno tiene que poder venir por sus propios medios a la reunión. A veces, aunque no sea lo ideal, tenemos presentadores que participan en forma remota.

JACQUES LATOUR: Tengo un comentario. Tenemos que ver cuál es la diferencia claramente entre la jornada técnica de la ICANN, el Tech Day, y estos talleres de las DNSSEC. Es decir, tenemos que marcar claramente esta diferencia de manera tal que colaboremos con el comité que organiza las jornadas técnicas, el Tech Day.

DAN YORK: Bueno, Jacques, usted está en los dos comités organizadores. Usted nos puede ayudar.

JACQUES LATOUR: Sí, claro. Con todo gusto pero no pude estar en todas las presentaciones. De todas maneras, podemos seguir hablando al respecto. Varios de nosotros nos perdimos algunas de las presentaciones.

DAN YORK: ¿Se pueden poner de pie los miembros del comité organizador para que la gente los identifique? Muy bien. Aquí tenemos algunos miembros del comité organizador. Otros no están presentes en la sala pero los pueden conocer. Muy bien. Dicho esto, estamos llegando… Perdón, alguien más solicita la palabra.

ROD RASMUSSEN: El SSAC tiene cierta responsabilidad con respecto al horario de este taller. Esta es una de las primeras veces en las cuales lo hacemos durante la tarde. Mañana los líderes de las SO y los AC se van a reunir para hablar acerca de los horarios de las sesiones. Quisiera saber qué prefieren si prefieren sesiones a la mañana, sesiones a la tarde, sesiones después del almuerzo. ¿Cuál es la preferencia?

DAN YORK: ¿Quién quiere volver a las sesiones por la mañana? Levanten la mano. ¿Quién quiere hacer las sesiones por la tarde? Levanten la mano. ¿A quién le da lo mismo? Muy bien. Yo diría lo siguiente. A mí me gusta la sesión por la mañana porque tenemos el almuerzo también y eso nos permite socializar, generar contactos y a lo largo de los años surgieron muy buenos contactos en esos almuerzos. Creo que tenemos muchos auspiciantes y deberíamos agradecer a Steve Crocker. Si ven a Steve Crocker, denle las gracias porque todos sabemos que, por lo general, teníamos tres o cuatro auspiciantes y yo los convocaba y los invitaba a renovar su compromiso. Aquí está Christian, que es uno de los

auspiciantes de larga data de Afilias. También CERA, Jacques. Muchas gracias. Steve se hizo cargo de los auspiciantes y terminamos con 11, 13, no sé cuántos auspiciantes. Es maravilloso contar con estos auspiciantes. Supongo que algunos de ellos van a continuar apoyándonos. Tenemos apoyo para hacer nuestro almuerzo. Ese sería mi comentario.

ROD RASMUSSEN: Vamos a ver qué es lo que podemos hacer. Voy a continuar luchando para que esto siga adelante.

DAN YORK: Muchas gracias a Rod y al SSAC por patrocinar esto desde la ICANN. Gracias a Kathy, por su maravillosa coordinación junto con el resto del personal que nos brinda su apoyo. Por favor, cuando vean la convocatoria a participación en los próximos talleres piensen en temas que les gustaría tratar para nuestro taller en Cancún. Muchas gracias a todos.

[FIN DE LA TRANSCRIPCIÓN]