ICANN84 | Reunión General Anual – ccNSO: sesión conjunta del día de la tecnología y del uso indebido del DNS
Lunes, 27 de octubre de 2025 – 15:00 a 16:00 IST

CLAUDIA RUÍZ

Hola y bienvenidos a esta sesión de la jornada técnica de la ccNSO, soy Claudia Ruíz y junto con mi colega Andrea Glandon somos las coordinadoras de participación de esta sesión. Esta sesión se está grabando y se rige por los estándares de comportamiento esperados de la ICANN, el código de conducta de participantes y la política antiacoso de la comunidad de la ICANN.

Estas son las guías a seguir en esta sesión, las pautas a seguir también las voy a presentar en el chat para que ustedes las puedan consultar. Durante esta sesión las preguntas y comentarios se leerán en voz alta si se presentan en el formato correcto, como se describe en el chat.

En esta sesión habrá interpretación en inglés español y francés, si quieren tomar la palabra durante la sesión, por favor, levanten la mano en Zoom, cuando digan su nombre los participantes virtuales podrán activar su micrófono en Zoom y los participantes presenciales utilizarán el micrófono físico para tomar la palabra.

Por favor, digan su nombre para los registros y el idioma en el que hablarán; si no es inglés, hablen a una velocidad razonable para que la interpretación pueda ser precisa. Muchas gracias y dicho esto, le doy la palabra a Nick Wenban-Smith, presidente de DASC.

NICK WENBAN-SMITH

Gracias, Claudia. Bienvenidos todos a esta tarde, es feriado en Dublín, así que, muchas gracias por tomar su día libre para venir a esta sesión, creo que, va a ser una sesión muy interesante. La primera instrucción es que hablemos lentamente y con claridad, creo que, esto va dirigido específicamente a mí, así que, debo recordar que debo hablar de manera lenta y clara.

Por favor, siéntanse libres de participar a través de Zoom, hay una ventana de chat para enviar comentarios y preguntas, vamos a ir viendo qué escriben allí. Si tienen algún problema con el audio, los auriculares ayudan mucho a escuchar con claridad lo que todo el mundo dice y si quieren hablar en otro idioma, por favor, empiecen su intervención diciendo en qué idioma van a hablar para que los intérpretes se puedan preparar.

Muchas gracias a los organizadores de la jornada técnica por darnos una hora esta tarde, el tema de esta sesión tiene que ver específicamente con el uso creciente de la Inteligencia Artificial para combatir el uso indebido del DNS. Para darles un poco de contexto, a quienes no sabían, hacemos una encuesta cada dos años entres los ccTLD y en 2022 se utilizaba cero la Inteligencia Artificial, se llegó a utilizar en el 23% en 2024 y, creo que, cuando lo repitamos en 2026 más del 50% utilizarán la Inteligencia Artificial, así que, creo que, es una tendencia muy importante y creciente.

Es un placer estar aquí con tres ccTLD, que nos van a dar un poco de información sobre la adopción de la Inteligencia Artificial en tres

ccTLD, así que, les voy a dar a los presentadores la posibilidad de presentarse, para que entendamos el formato de esta sesión.

Habrá tres presentaciones de 12 minutos y tiempo para preguntas específicas sobre esas presentaciones, así que, por favor, que las preguntas sean sucintas y que tengan que ver con la presentación en cuestión, después hay un tiempo al final para que la comunidad debata a través de este proceso de relacionamiento y participación, para escuchar ideas de otras personas que todavía no pudieron decir lo que creen que pasará en el futuro con la Inteligencia Artificial.

Ahora le voy a dar la posibilidad a los ponentes que se presenten.

PHILIP STRUYF: Buenas tardes a todos, soy Philip Struyf y a principio de año me incorporé como gerente de programa para la prevención del uso indebido.

JAKE VINCET: Yo soy Jake Vincet, gerente de políticas de registro y me ocupo de la política de uso indebido del DNS.

CRYSTAL PETERSON: Soy Crystal Peterson, directora Sénior de cuentas, claves y operaciones para el registro GoDaddy.

NICK WENBAN-SMITH

Muchas gracias. Quiero recordarles a los oradores que, por favor, hablen de manera lenta y con claridad en beneficios de los que no son hablantes nativos de inglés y para los intérpretes, así que, tengo algunas instrucciones aquí.

Esto es un resumen del mandato de DASC, lo que está en nuestros términos de referencia, no es para definir políticas, sino que, tenemos que crear consciencia, promover el diálogo constructivo y ayudar a los ccTLD en su trabajo de mitigación del uso indebido del DNS para ayudar a toda la comunidad, especialmente esto está dirigido a los ccTLD más pequeños que tienen menos recursos y a los que les viene bien aprender de nuestra experiencia.

¿Qué hicimos en el pasado y cuáles son los recursos disponibles? Todas nuestras sesiones se graban, así que, no es información sobre herramientas y mediciones, tenemos información sobre la forma de denunciar casos de uso indebido, hay información sobre datos de registración, hay información sobre cómo prevenir los delitos financieros y el fraude en línea. Toda esa información está en nuestros registros, la tenemos registrada y está en nuestros archivos. Ahora le doy la palabra al siguiente orador.

PHILIP STRUYF

Buenos días o buenas tardes, hoy voy a hablar sobre la detección del uso indebido utilizando Inteligencia Artificial, voy a dar una introducción y voy a explicar nuestros desafíos, qué es lo que

estamos haciendo, por qué decidimos utilizar Inteligencia Artificial y el aprendizaje automático.

Después voy a hablar de nuestra implementación actual del sistema de predicciones y les voy a explicar lo que hicimos, cómo avanzamos ofreciendo funcionalidades a comunidades de registros y después voy a responder todas las preguntas que puedan tener.

A principios de este año me incorporé a .EU como gerente de programa para prevención del uso indebido de ID, estamos buscando lograr dominios de alto nivel seguros para apoyar al mercado único digital europeo. Nuestro foco central para lograr este objetivo es la calidad de los datos y colaboramos con los registradores y registratarios para asegurarnos de que los datos, en nuestra base de datos de registros, sean exactos y precisos, esto es una prioridad y también una obligación legal para ID.

En este gráfico vemos la evolución de la cantidad de dominios sospechosos identificados desde que lanzamos EURid, es el sistema interno de calidad de datos, lo utilizamos como evento principal en nuestro análisis del uso indebido y utilizamos también procesos de verificación.

Entonces el objetivo está claro, pero no es fácil lograrlo, como ustedes saben, el uso indebido del DNS es una amenaza, a pesar de que la definición de uso indebido de DNS se ha debatido mucho y nunca será perfecto, en general, trato de tener en cuenta las

categorías y las definiciones que nos da el Comité Asesor de Seguridad y Estabilidad de la ICANN.

No debo explicar esto en detalle para este público, seguramente aquí veremos el programa de mitigación de amenazas, y aquí vemos que el spam se considera que es uso indebido de DNS cuando se utiliza con mecanismos para llevar a cabo otras amenazas, se considera un elemento clave.

Esto valida nuestro foco inicial en cuanto a detectar patrones en los datos de registración de nombres de dominios utilizados para spam, bueno, al principio lo hacemos en forma manual, como pueden imaginar, era algo muy lento, requerían muchísimo trabajo y no era efectivo porque los spams aparecían y desaparecían rápidamente, sin embargo, establece las bases para el desarrollo inicial de nuestro sistema de predicción.

Y después de muchos ajustes, el foco estaba en limitar la cantidad de falsos positivos. Finalmente, se implementó el sistema en forma gradual y también pasamos a medidas proactivas que, en ese momento, incluían la delegación demorada de nombres de dominios.

Actualmente estamos totalmente integrados con la plataforma de registración de .EU, nuestro sistema lleva ahora a la suspensión inmediata de dominios sospechosos y esto se hace junto con nuestro sistema interno de control de calidad. También queremos mejorar el sistema viendo a otros registros para que se puedan

beneficiar y contribuir al modelo, pero después voy a hablar de esto.

Prevención del uso indebido. Sistema de alerta temprana que nos da en tiempo real predicciones de posible uso indebido, fue desarrollado junto con la Universidad Católica de Lovaina y hay algunas publicaciones científicas sobre este tema en nuestro sitio web, está patentado y ha demostrado ser efectivo durante muchos años, en cómo analiza el sistema de predicciones, analiza los nombres antes de la delegación y; según el modelo de predicción, toma en cuenta los datos de registración, es decir, los datos que nos dan a los registradores y los metadatos de registración; que son datos que tomamos de los datos de registración. Por ejemplo, hacemos una verificación de dirección o calculamos la reputación de los servidores de nombres asociados con la registración del nombre de dominio.

En este momento tenemos tres modelos predictivos, tenemos un modelo de clasificación basado en reputación, un modelo de clustering basado en similitudes; que vemos en pantalla, y tenemos un tercer modelo naive, que se centra en otro tipo de registraciones. Los modelos son entrenados en forma continua utilizando fuentes externas y un bucle de feedback interno y los resultados van a un control de predicción único, que es administrado por EURid y por un servicio de administración de reputación, que es lo que vemos aquí.

¿Dónde estamos ahora? La configuración actual incluye la parte de aprendizaje automático, como dije antes, hay una serie de reglas que verifican y detectan patrones y paradas claves donde no se utiliza el aprendizaje innecesario, así que, el sistema hace una serie de verificaciones y asigna ponderaciones.

Cuando se llega a un cierto umbral la predicción pasa a malicioso y esta combinación, y la configuración de los componentes permite un ajuste sencillo, por ejemplo, podemos buscar fácilmente palabras claves relacionadas con la pandemia de COVID-19 o la guerra de Ucrania, según lo pidió la Comisión Europea, y esto sin desperdiciar esfuerzos de cálculo y de procesamiento.

Como vemos en el gráfico, el sistema fue implementado en forma gradual, hace varios años que está vigente, pero es solamente un elemento en el amplio panorama de prevención del abuso, trabajamos en colaboración con terceros para ampliar nuestro alcance.

La implementación en las instalaciones que tenemos, todo eso, está integrado con la plataforma europea y esto crea dependencia, tenemos un sistema de intermediarios, pero obviamente eso también limita el bucle de feedback que tenemos a los datos de registración de nombres de dominios EU, por eso exploramos formas de ampliar el sistema abriéndolo a otros registros, permitiéndoles beneficiarse de esto y hacer sus aportes.

Entonces desarrollamos recientemente una prueba de concepto para APEWS como servicio, utilizamos tres partes, en primer lugar,

queremos una implementación contenerizada trabajando con un proveedor de servicio europeo. El segundo punto de foco era uso de API REST para simplificar la integración. Y el tercer punto en el que nos enfocamos era la anonimización de datos para almacenar los elementos de aprendizaje automático para garantizar la integridad de los datos.

Esto llevó al diseño de alto nivel que vemos aquí, la idea principal es tener un sistema APEWS compartido, este sistema debe estar albergado en la nube europea y los registros pueden buscar un dominio, incorporar datos de capacitación y todo se trabaja a partir de una API REST segura, y el objetivo final es mejorar la precisión de la detección de casos de uso indebido.

Con respecto a la hoja de ruta de APEWS como servicio, una vez que tengamos todos los modelos listos vamos a eliminar los componentes específicos complejos y reemplazarlos por API REST, también tendremos la anonimización de datos, ahora debemos abrir nuestra prueba a los registros interesados para pedirles información y comentarios sobre las características que piensan que faltan. También tenemos algunas funciones que queremos incluir en el futuro como en las interfaces webs, pero queremos escuchar las prioridades que tienen otros registros en cuanto a una estimación de costos.

El costo para integrarse con APEWS por el nivel que queremos lograr y la arquitectura técnica del sistema… Sin embargo, tenemos tres escenarios posibles, pero no voy a entrar en detalles

porque no hay tiempo ahora, pero mis colegas y yo estaremos aquí para contarles un poco más sobre esto si les interesa.

Eso concluye mi presentación y si les interesa escriban o pueden pedir acceso a la documentación y al sistema que es la prueba de concepto hacia una protección europea con IA contra el uso indebido del nombre de dominio.

NICK WENBAN-SMITH APEWS.EU nos identifica, es una sigla favorita de la ICANN. Hay un par de preguntas, entiendo. Luc Seufer, ¿quiere tomar la palabra?

LUC SEUFER Claudia tiene mejor voz que yo. Quisiera saber sobre la identidad del proveedor de nube europeo, ¿dónde se guardan los datos? ¿se puede divulgar la identidad? Si es un proveedor fuera de la EU dentro de los llamados de la EU.

PHILIP STRUYF No, no. Está basado en la Unión Europea, todavía tenemos que ver la selección, tenemos relaciones con proveedores y tenemos que seleccionar uno, pero para producción vamos a tener una licitación específica.

NICK WENBAN-SMITH Hay otra pregunta de Andrei. Adelante.

ANDREI KOLESNIKOV ¿Qué red neural se utilizó y se entrenó para lograr umbrales positivos máximos? ¿Qué plataforma usaron?

PHILIP STRUYF Es básicamente estadísticas mejoradas, no es…

ANDREI KOLESNIKOV ¿La red neural? No.

NICK WENBAN-SMITH Hay varias manos levantadas.

MACIEK PIASECKI Soy fellow de la ICANN. ¿qué hacen con los falsos positivos y los falsos negativos? ¿Hay algún sistema de apelación?

PHILIP STRUYF Se realiza una prueba para los falsos positivos, lo que se llama dry run, se suspende el nombre de dominio de inmediato si no está seguro, si es falso positivo o no. La situación actual es que pedimos a los registratarios del nombre de dominio suspendido que se identifiquen para verificar y mejorar la calidad de los datos, si es muy alto el número de falsos positivos también.

SAKSHAM JAIN	Soy NextGen. Puede hablar un poco sobre las cláusulas post delegación en .EU, especialmente que tiene un sitio durante varios años, ¿qué piensa la EU sobre esto?
PHILIP STRUYF	Trabajamos con terceros y hacemos crawling en la prueba de los sitios, como les decía, está integrado en los datos en su plataforma de calidad, cosa de que hay un disparador en la fase post delegación dado que la API es un disparador pre delegación en el programa de calidad de datos, se solicita un proceso de KYC.
SAKSHAM JAIN	¿El proceso actual es automático o manual?
PHILIP STRUYF	Tengo que dar una respuesta un poco mixta. Los tres feeds se manejan manualmente y el crawling es automático.
NICK WENBAN-SMITH	Una pregunta más y cerramos.
SAMANEH TAJALIZADEHKHOOB	Se mencionó que se maximizó el modelo para el objetivo, ¿para qué se maximizó? ¿Precisión? ¿Menos falsos positivos? ¿Hay un par de métricas para maximizar el modelo?

PHILIP STRUYF Tratamos de minimizar la cantidad de falsos positivos, es la meta principal antes de pasar a medidas correctivas.

NICK WENBAN-SMITH Muchas gracias por estar, nuevamente, con nosotros. Una última pregunta.

KAREN ROSE Muchas gracias por la presentación. El sistema funciona con solicitudes internacionales y llegado el caso, ¿hay una diferencia en desempeño?

PHILIP STRUYF Utilizamos IDN, otras cadenas de caracteres y otros códigos de escritura, los que están en otros códigos de escritura son muy limitados, el resultamos es, cuanto más datos hay, se va mejorando.

NICK WENBAN-SMITH Esta pregunta surgió en otras reuniones también. El siguiente orador, por favor.

JAKE VINCET Vamos a hablar de Domain Watch, una de las herramientas que tenemos para el uso indebido del DNS combinado. No es mío el desarrollo.

Domain Watch viene funcionando desde hace unos siete años, lo hemos probado muchas veces, es una iniciativa anti-phishing para incrementar más la seguridad de .UK, también para identificar dominios inmediatamente después de la registración que claramente son engañosos, es una mezcla de reglas y modelos de aprendizaje automáticos que buscan combinaciones de errores de tipeo o palabras claves, la idea es resolverlos con rapidez.

Pensemos en qué podemos ver un ejemplo, se contralan contra los modelos, tengo algunos ejemplos en pantalla, vemos en rosa con un umbral, eso es 9.1, fijan los falsos positivos y se optimizan varias veces.

En este momento tenemos 20 dominios por día con un 50% de suspensión, un ejemplo sería un investigador security researcher y se hace un ejercicio de phishing para ver quiénes son y el acceso que utilizan. En este ejemplo se puede ver que el PAYPAN.UK es muy similar a PayPal, esto queda marcado y se envía a los analistas.

Del mismo modo de la parte inferior tenemos TAX-GOV.UK, esto es un dominio de segundo nivel, esto es engañoso si lo consideramos contra la autoridad fiscal de Reino Unido. Refinamos la calificación, tenemos un concepto de una cola de incidentes que no llegan a este umbral del que les hablé y lo evaluamos así.

Hay múltiples feeds, hay de phishing buscando cadenas de caracteres aleatorias con distintas calificaciones bastante altas, pero algunos no llegan al umbral, uno de los desafíos está en tener

datos confiables respecto de uso indebido y venimos pensando con el uso de IA se puede utilizar para que generar conjuntos de datos grandes, especialmente en campañas y utilizándolo para aprobar los modelos.

Vamos a ver un poco el proceso de Domain Watch. Tenemos una interacción, se registra el dominio, se califica inmediatamente por Domain Watch, si el umbral se infringe se manda un analista para revisión, ven los datos del registratario y si lo ponen como seguro, BAU se delega.

De lo contrario, se suspende el dominio y se envía una notificación al registratario, tenemos un proceso de verificación de ID para entender el usuario y después se toma la decisión sobre si se puede registrar el dominio o no.

Vamos a ver algunas cifras de alto nivel, es una herramienta muy buena, seguimos trabajando para refinarla aún más, en un año suspendimos más de 4.000 dominios con Domain Watch y hay categorías interesantes de datos, algunas respecto a las páginas de ingreso.

Por ejemplo, vimos que Barclays Bank había sido un objetivo y HMRC que es la autoridad fiscal del Reino Unido, esto es Domain Watch a alto nivel, pero hablemos de una nueva herramienta que venimos utilizando que se llama Genie.

Genie es una característica con asistencia de IA, el producto se llama Databricks, es una plataforma de analítica, usamos esta

herramienta que está en su infancia, estamos viendo los casos de uso y tenemos que traducir las preguntas de negocios en consultas analíticas permitiendo a los usuarios de negocios hacer consultas de datos que normalmente necesitarían conocimiento de SQL o acceso a la base de datos.

Genie es del estilo de ChatGPT, podemos encontrar la información en otros lados, pero aquí es con gran rapidez y sin necesidad de trabajo de desarrollo. Pensando en el uso básico de Genie se le puede preguntar, "muéstreme los dominios que se han suspendido repetidamente", y nos muestra los resultados.

Vemos el código, veo la consulta generada, podemos ver claramente la cantidad de dominios suspendido unas 11 veces y se puede preguntar por qué hubo tantas suspensiones. También podemos preguntarle las características de dominios suspendidos y podemos entrenar a Domain Watch en base a estos resultados.

Vamos a ver algunos casos de uso más avanzados, si hay registros más altos respecto del promedio. Tenemos una lista de los registros diarios de un registrador específico que están en más de 1.000 y normalmente tiene menos de 150, eso no significa que hay uso indebido, pero amerita que investiguemos, también pensando cómo podemos utilizarlo para

Cómo podemos utilizarlo para ver los datos del registrador para hacer verificaciones. Como les dije antes, es un caso de uso que está en su infancia, pero venimos haciendo buenas preguntas,

tenemos resultados interesantes que nos permite hacer investigaciones.

Finalmente, tenemos un lindo caso de estudio también tratando de explicarnos el uso indebido del DNS, que recopila informes de una serie de fuentes con MISP para recopilar datos fundamentales utilizando Genie para analizar los reportes, extraer datos en escala y producir hallazgos en un formato que pueda ser consumible por humanos. Para nosotros está en la infancia y estamos viendo los datos subyacentes para entrenarla y espero poderles dar algo más en el futuro para contarles cómo vienen las cosas.

¿Alguien tiene alguna pregunta?

NICK WENBAN-SMITH: Uno, dos, tres… Y no hay ninguna pregunta en el chat ahora.

MACIEK PIASECKI: Yo soy becario de la ICANN. Quiero saber cuando pasan a la parte de ID, ¿lo comparan con qué? ¿Con qué base de datos? Especialmente con ID exteriores y si hay un procedimiento de apelación es una forma de tomar algunas medidas quizás, o algunas acciones judiciales. Si hacemos unas verificaciones, ¿eso lo hacemos a través de un tercero? ¿Tenemos un proceso de apelaciones?

NICK WENBAN-SMITH: Allí hay otra persona que levantó la mano.

FURKAN ÇOLHAK

Gracias por la presentación. Soy becario y tengo una pregunta acerca de la protección de datos, usted dijo que están utilizando alguna herramienta para estas operaciones, ¿ustedes comparten el archivo de zona? Y, creo que, falta algo con respecto a la protección de datos porque usted dijo que no se puede utilizar modelos de lenguaje grande para hacer esto, porque tiene un tema de capacidad y procesamiento. Muchas gracias por su presentación, una vez más.

NICK WENBAN-SMITH

Yo soy encargado de protección de datos de Nominet y, creo que, usted allí levantó la mano. Luc.

LUC SEUFER

¿Podría ampliar un poco el rol de la revisión del análisis en el proceso? Porque hay algunos abogados que están haciendo un bypass del DRS, ¿están dejando de trabajar con abogados o están trabajando simplemente con otro tipo de personas?

JAKE VINCET

Este es un proceso DRS, tenemos a un grupo de analistas de uso indebido del DNS interno, entonces cuando ellos revisan los casos se fijan quién es el registratario, cuáles son los datos del registratario, si ya estuvo en contacto con la comunidad de seguridad anteriormente, etc., ¿responde a tu pregunta?

LUC SEUFER No me da mucha certeza, pero sí.

NICK WENBAN-SMITH No veo ningún comentario en el chat ni ninguna pregunta. Pasemos a la tercera presentación, estamos cumpliendo muy bien con el horario, así que, muchas gracias a los presentadores por cumplir con el tiempo asignado. Le doy la palabra a Crystal.

CRYSTAL PETERSON Nuevamente, soy Crystal Peterson, trabajo con GoDaddy para .US y voy a hablar ahora acerca de nuestros abordajes proactivos para la prevención del uso indebido del DNS.

Para contarles la situación actual de los dominios, estamos hablando de 2.5 millones de nombres de dominios, tenemos un 57% de tasa de renovación en el año anterior. Para combatir el uso indebido del DNS, bueno, antes de que empiece el abuso todos sabemos que el uso indebido es una amenaza continua y persistente, con respecto a los abordajes reactivos tradicionales creemos que ya no son suficientes y queríamos ampliar nuestro sistema de gestión de amenazas para incluir un modelo proactivo utilizando la Inteligencia Artificial y reconocimiento de patrones entre TLD.

Entonces con la detección reactiva lo que tenemos es que el uso indebido se mitiga después de que ya se produjo un daño, los atacantes pueden explotar brechas en TLD y nuestra solución

consiste en detectar patrones de amenazas y bloquear temporalmente las etiquetas que podrían ser maliciosas, antes de que se registren para impedir que se desarrolle un ataque antes de que llegue a los gTLD.

¿Qué queremos hacer? Queremos tener un sistema de múltiples capas que incluya una integración de alertas históricas, información en tiempo real de amenazas provenientes de múltiples fuentes, análisis de Inteligencia Artificial, creación de agentes y después una plataforma de bloqueo. Esto nos permite actuar antes de que el uso indebido llegue y afecte a los usuarios de internet.

Entonces uno de los objetivos que queremos lograr con esta herramienta proactiva, que utiliza Inteligencia Artificial, es buscar un 20% de reducción en las registraciones maliciosas, queremos tener menos de un 5% de falsos positivos y también queremos acelerar el tiempo de respuesta en un 75%, en el caso de abusos. ¿Qué queremos hacer? Vamos a utilizar un abordaje de tres fases para implementación, ahora estamos haciendo la prueba de concepto y queremos poder implementar esto en .US centrándonos, en primer lugar, en la detección de phishing o detectando las diferentes definiciones de uso indebido del DNS. Después queremos pasar a los otros tipos de uso indebido.

También buscamos establecer métricas iniciales teniendo en cuenta los objetivos que mencioné y buscamos desarrollar un proceso de apelaciones para lo que vayamos a bloquear. Después

pasaríamos a la fase 2, que es optimización de lo que ya tenemos y nuestro objetivo final es poder ampliar y llevar esto a otras cantidades de TLD que son administradas, estoy hablando de gTLD y ccTLD, y queremos poder compartir inteligencia entre diferentes plataformas y con diferentes socios.

Una de las cosas que buscamos, o que sabemos, es que esta iniciativa cambia totalmente la mitigación de abusos, pero ayuda a mejorar la reputación de la industria para los gTLD, ayuda a reducir costos y también ayuda a fortalecer la protección de las marcas que están utilizando nuestros TLD. También creemos que esto ayuda al cumplimiento regulatorio y mejora la colaboración entre los TLD y la comunidad.

Dicho esto, muchas gracias y con gusto voy a responder las preguntas que puedan tener.

NICK WENBAN-SMITH Gracias, Crystal. ¿Hay alguna pregunta para Crystal?

FURKAN ÇOLHAK Soy un becario. Usted habló de eficiencia, hay que mejorar la eficiencia y hay que mejorar nuestra competitividad, por supuesto, tenemos muchos competidores y las soluciones proactivas pueden ser perfectas, pero el problema es que los que hacen phishing cuando registran un nombre de dominio quizás lo registren con nombres o temas que no tienen nada que ver. Ahora, si mejoramos

la eficiencia en general, pregunto: ¿Por qué necesitamos esto que usted menciona? Igualmente muchas gracias por su presentación.

CRYSTAL PETERSON Lo que queremos hacer con este sistema de aprendizaje automático con Inteligencia Artificial es que vimos patrones en los TLD y la idea es ayudar a resolver los problemas que puedan surgir y queremos después llevarlos a otros campos, pero este experimento busca ver cómo podemos detectar rápidamente patrones que pasan de un TLD a otro y para evitar que todo esto llegue a nuestro TLD.

NICK WENBAN-SMITH Yo tengo una pregunta para usted, Crystal. Seguramente identifican cadenas de alto riesgo, después las bloquean y no permiten que sean registradas, ahora, ¿tienen una lista? ¿O qué se hace con esta lista? ¿Cuán larga es esta lista?

CRYSTAL PETERSON Esta lista puede ser muy larga o muy corta, si hubo un ataque y este ataque causó muchos problemas y tiene algunos patrones este ataque, que tiene una serie de caracteres y utilizan letras o números orquestados en forma aleatoria, esto puede entrar en un set o en un conjunto mayor, pero esto no es necesariamente donde las marcas nos piden que actuemos, por eso lo bloqueamos en forma temporaria, pero estamos buscando un proceso de apelaciones porque si una persona piensa que su nombre ideal de

dominio está dentro de este conjunto bloqueado puede apelar y pedirlo.

NICK WENBAN-SMITH Si yo quiero registrar un nombre de dominio y soy inocente y entro a la plataforma de un registrador como GoDaddy, por ejemplo, trato de registrarlo y no funciona, ¿cómo se conectan con los registradores para decirles cuáles dominios están disponibles o no? Para ser registrados porque hay un bloqueo aquí, se bloquea algo por una amenaza.

CRYSTAL PETERSON Buena pregunta. Todavía estamos analizando y desarrollando los mensajes y cómo mostramos esto en un EPP cuando se bloquea, por ejemplo, para los nombres reservados por el registro hay una respuesta uniforme pre-preparada que indicaría que esto está reservado, por supuesto, debemos actualizar nuestras respuestas para otros casos, para poder decir: “Bueno, esto está bloqueado porque podría ser una amenaza”, estamos haciendo esto y queremos demostrarles a los delincuentes que estamos detectando lo que están haciendo, y esto quizás lo lleve a buscar otras soluciones, no queremos que sigan intentándolo.

NICK WENBAN-SMITH Muchas gracias. Y ahora tenemos 15 preguntas para una conversación más general u otros temas, son temas generales, el uso de Inteligencia Artificial para prevenir el uso indebido y

detectar el uso indebido del DNS, yo tengo varias preguntas, ya hicimos preguntas a los tres presentadores, pero ahora con mucho gusto podemos tomar preguntas más generales sobre el uso de la Inteligencia Artificial para detectar amenazas.

MACIEK PIASECKI Yo soy becario de la ICANN y tengo una pregunta para todos ustedes. Yo sé que la ICANN no maneja los contenidos, se mantiene alejada de los contenidos, pero ¿ustedes utilizan o conservan los contenidos en el proceso de aprendizaje, o cuando van a suspender un dominio? Porque si un sitio web utiliza un logo de Facebook o de un banco yo diría que podría ser un caso de uso indebido, si no pertenece a ese banco.

PHILIP STRUYF Utilizamos capturas de pantalla y contenido en los feeds de amenazas, pero por el momento no lo utilizamos para educar a los modelos predictivos.

JAKE VINCET Si, lo mismo hacemos nosotros, buscamos capturas de pantalla, evidencias de uso indebido, pero nada más.

CRYSTAL PETERSON Hacemos lo mismo, partes de nuestras actividades de mitigación utilizan capturas de pantalla de las personas que trabajan con nosotros y de revisiones que hacen los investigadores, pero en

cuanto a esta herramienta utilizamos alertas pasadas confirmadas y también los feeds, no estamos utilizando el contenido en este momento.

NICK WENBAN-SMITH Muy interesante. ¿Hay alguna otra pregunta de los participantes? Tengo a Hilde y después a Michaela. Hilde, primero y después Michaela.

HILDE THUNEM Gracias. Soy Hilde Thunem del registro de Noruega. Muchas gracias por sus presentaciones, yo sé que esta es la jornada técnica y voy a hacer una pregunta sobre cuestiones legales, así que, quizás no sea fácil responder, pero conociendo que están utilizando Inteligencia Artificial sospecho que ya consideraron la ley de Inteligencia Artificial y cómo esto se relaciona con la norma europea sobre el uso de la Inteligencia Artificial para tomar decisiones, ¿podrían decir algo al respecto? Si llegaron a alguna conclusión.

NICK WENBAN-SMITH Creo que, después del Brexit hay solamente un ccTLD aquí en la Unión Europea, pero sí todavía tengo PTSD, como usted sabe, sobre todas estas cosas. Philip.

PHILIP STRUYF Hemos considerado esto, todavía estamos realizando el análisis final, pero, como dije, hicimos mucho para anonimizar los datos

que se almacenan después de capacitar a los modelos, entonces sí queremos hacer una predicción, los datos que deben ser almacenados para facilitar la capacitación y educación del sistema pueden ser almacenados en forma anónima, teniendo en cuenta lo que dice el GDPR, etc.

NICK WENBAN-SMITH Gracias. La última, pero no menos importante, Michaela, puede tomar el resto del tiempo, es tan divertido.

MICHAELA SHAPIRO Gracias por permitirme cerrar la sesión. Esto toca las distintas empresas, seguramente, pero tengo curiosidad, si prevén este tipo de herramientas para recopilar datos adicionales, considerando que todo se basa en datos a los que ya tiene acceso, quizás se puede tomar por separado, pero me interesan las herramientas de anonimización que utilizan. Eso podría ser después de la sesión.

CRYSTAL PETERSON La anonimización y ver si hay puntos de datos adicionales recolectados también. La primera, puntos adicionales, lo que estamos analizando en este momento son alertas confirmadas históricas pasadas en nuestros agentes, pero también feeds de amenazas actuales y no habría puntos de datos adicionales a recopilar, el registro tiene punto de datos propios, pero en lo que estamos tratando de derivar se basan en patrones y también

donde vemos uso indebido confirmado en otros TLD, vemos si está protegido el TLD.

La respuesta es larga para decir "no", pero el registro per se sí tiene otros puntos de datos y los datos anonimizados dentro de los feeds de datos, que son públicos, que se pueden adquirir, algunos son gratuitos, en base a los feeds que hay… Vienen a nosotros, fundamentalmente ya están anonimizados desde esas fuentes y los comparamos con los TLD que piden apoyo contra los datos internos, pero para los que no operamos son anonimizados en base a lo que nos envían y podemos también trabajar en búsqueda de otras zonas.

JAKE VINCET Tenemos los datos del registratario, pero lo buscan en la lista manualmente en la cadena específica.

PHILIP STRUYF Además de adicionar los datos de registratarios, hacemos cálculos, por ejemplo, la reputación del servicio en los últimos 15, 30 o 60 días hacemos una serie de cálculos, pero todo empieza con los datos que nos llegan de los registratarios.

NICK WENBAN-SMITH Iba a preguntar si alguien pensó en las implicancias a nivel de Derechos Humanos y el efecto de esto. Kristian, primero, y después Luc.

KRISTIAN ØRMEN Gracias. Soy Kristian Ørmen de .SE. Para la EU, creo que, el sistema AP es muy interesante y vi en el sitio que pueden tratar o probar el concepto de prueba, esta es una pregunta técnica. Como vamos a sacar de nuestros registros las dos direcciones vi que uno de los puntos de datos que están utilizando sería probar el sistema sin utilizar esos puntos datos, ¿o requeriría el conjunto de datos para hacer la prueba?

PHILIP STRUYF El sistema tomaría el punto de datos que se entregue, pero tiene que ver con el uso también.

NICK WENBAN-SMITH Hay una pregunta en el chat de John McCormack. “Datos de precios sería un buen aporte, a menudo, los hoppers ofrecen descuentos, los nombres de dominios registrados como parte de un descuento pueden tener un riesgo más alto, independientemente de las registraciones con credenciales hurtadas o malas. Con las herramientas analíticas que tenemos, ¿se puede superponer con las promociones de precios y los descuentos a nivel registrador?

JAKE VINCET Qué buen punto. Hay que ver si lo movemos a otro nivel, no lo consideramos todavía, pero sí es algo a pensar.

CRYSTAL PETERSON Para la detección de patrones y otras tendencias de uso indebido los datos de precios no constituye algo que se está ingresando, sin embargo, habiendo dicho esto, los datos de precios contra las alertas y la actividad confirmada constituyen algo que tendemos a considerar, pero no necesariamente en el sistema IA proactivo que estamos trabajando, pero al tener alertas confirmadas sí es parte de lo que hacemos y lo que analizamos.

NICK WENBAN-SMITH ¿Alguna otra pregunta en el chat o de la sala? Primero, usted Sr.

SAKSHAM JAIN Hola, soy Saksham Jain de NextGen. No sé quién quiere responder esto, pero muchos de los sistemas hablan del tiempo de registración o pre-registración, ¿se está trabajando en post registración? Por ejemplo, si un dominio es agregado y se ve afectado por uso indebido del DNS, ¿están haciendo algo para que ese proceso sea más rápido para la restauración del dominio?

JAKE VINCET No sé bien qué quiere decir “restaurar”, sí, pero no con IA. Creo que, respondí.

NICK WENBAN-SMITH Luc.

LUC SEUFER Para Crystal, cuando mencionó la lista, ¿tiene alguna salvaguarda a considerar para que no afecte la libertad de expresión? O que no esté bloqueando los nombres de dominios, por ejemplo, sé que la administración actual quizás no quiera que se registre algún nombre de dominio.

CRYSTAL PETERSON Qué buena pregunta. Esto es para detectar patrones, pero también para detectar y considerar lo que se utiliza y/o se registra como uso indebido ya hecho que, quizás ya sea a otro TLD, suceda en nuestro TLD. Si hay alguna confirmación de actividad de uso indebido ese es el patrón que buscamos, en lugar de buscar nombres de dominios desde la perspectiva de eliminar a alguien que registra un nombre de dominio, que no necesariamente constituya un patrón. ¿Respondí?

LUC SEUFER El de uso indebido del DNS definido por el agente.

NICK WENBAN-SMITH Nos quedan un par de minutos disponibles. Se dedica mucho tiempo en la comunidad de la ICANN en la argumentación doctrinaria de la definición del uso indebido, todo el mundo habla de phishing, que es un uso indebido predominante. Por simplicidad, hablando del uso indebido del DNS, se puede hablar del phishing, entonces la pregunta es: ¿Cómo medimos el éxito de

estas iniciativas? Particularmente Estados Unidos tiene un objetivo en términos de reducción numérica, ¿tienen algún benchmarking o alguna referencia? ¿O cómo funcionan las cosas? Para medir, si tienen un problema, una intervención, para ver si hay algún cambio sobre eso o estamos perdiendo la carrera contra los malos actores que realizan estas campañas de phishing, ¿alguna idea al respecto?

CRYSTAL PETERSON Desde la primera pregunta sobre si tenemos que hablar de phishing, en comparación con otros, como mencionó, phishing es uno de los más prevalentes, por eso queremos comenzar ahí porque consideramos que es algo que se puede resolver más fácilmente, pero también ampliarlo hacia las otras definiciones, phishing y después poder considerar si hay algún otro patrón o malware, o CNC y bots, pero phishing es un buen lugar para comenzar.

La segunda pregunta… Ah, la medición del éxito, y si estamos ganando o no. Con la medición del éxito son nuestras metas y seguimos en las etapas de infancia tratando de recopilar, empezar el bloqueo, el análisis y no tenemos todavía datos suficientes para ver el resultado de lo que estamos haciendo.

NICK WENBAN-SMITH Es como la prueba ácida.

CRYSTAL PETERSON

Lo que estamos viendo es si lo estamos previniendo o no, es info checks, si los vemos contra esas cadenas de caracteres y vemos que salta ese valor u otras áreas que podemos ver también dentro de los feeds y los datos, vemos un salto que no sucede quizás en Estados Unidos, pero que sí puede llegar a estar sucediendo al otro lado, que no se mitiga, pero quizás se bloquea. Son áreas que evaluamos.

¿Estamos cumpliendo la meta? Porque vemos una reducción, porque no vino en el primer lugar, sí.

NICK WENBAN-SMITH

¿Algún otro comentario? Muy bien, adelante, Samaneh.

SAMANEH TAJALIZADEHKHOOB

Soy de ICANN Org. Hay una gran investigación sobre los datos y los modelos, y lo que se especula en base a los resultados de los datos, básicamente el uso del modelo de LLM puesto sobre la mesa muestran lo que quiere decir este plan. Escucho que hay un par de registros que adoptaron el LLM en sus servicios, como se les ha aprobado, si la interpretación es que van a estar en línea con lo que muestran los datos, sabiendo que un plan puede llegar a tener múltiples interpretaciones.

NICK WENBAN-SMITH	¿La organización está hablando del trabajo de LLM? Le pido una respuesta a posteriori. Es una negativa, ¿quiere contarnos un poco sobre la organización? Si lo están adoptando.
SAMANEH TAJALIZADEHKHOOB	Todavía no lo estamos adoptando ni está planificado, estamos utilizando modelos para predecir esto como parte del trabajo de EURid, pero no más allá de eso.
NICK WENBAN-SMITH	Creo que, vamos a ir cerrando, pero un comentario final. Muchas gracias a los panelistas por contarnos sus conocimientos profundos, por responder a las preguntas y mi conclusión es citar a T.S. Eliot, IA es más un golpecito que un golpe grande en la adopción de ccTLD. Un aplauso para los panelistas, por favor.

[FIN DE LA TRANSCRIPCIÓN]