ICANN82 | Foro de la comunidad – Sesión conjunta: ALAC y SSAC
Domingo, 9 de marzo de 2025 – 13:15 a 14:30 PST

JONATHAN ZUCK: Venimos desde la oscuridad. Quisiera repetir lo que acaba de decir Michelle. Este es un grupo muy heterogéneo en la comunidad de At-Large, entonces les recomiendo que, por favor, saquen los auriculares, elijan su idioma para que la gente pueda hacer una transición rápida cuando decida tomar la palabra y también pueden hacerlo desde Zoom.

En el interín vamos a hablar un poquitín de ALAC y SSAC, estamos encontrándonos alineados en una serie de distintos temas, es muy bueno y fructífero, le hemos escrito a la Junta y veremos la respuesta, estamos trabajando juntos en la educación de phishing a través de la campaña correspondiente, hemos terminado el curso, ya empezamos el proceso de traducción para poder dictar estos cursos.

Estamos entusiasmados con lo que vamos a hablar y ambos vamos a centrarnos en el uso indebido del DNS, encontrar respuestas, no sé si se comparten la frustración con el webinar e INFERMAL, encontramos estas correlaciones y parece que no hubiera que hacer nada al respecto, lo que es un comentario extraño, así que, me gustaría hablar y saber qué les parece este tema.

Nuevamente, gracias por estar aquí, bienvenidos. Usted está sustituyéndolo, así que, preséntese por favor.

JEFFREY BEDSER Estoy reemplazando a Mohan. Soy del equipo líder de SSAC, vamos a hablar de los hallazgos de INFERMAL y el uso indebido del DNS, yo soy el líder del tema y voy a tomar esa categoría en esta conversación.

JONATHAN ZUCK En el temario pusimos un poco de cómo es este curso, cómo está funcionando, entonces podemos ingresar a Zoom y voy a compartir mi pantalla, voy a reemplazar la imagen. Esto es más o menos de lo que vamos a hablar, es de alto contraste, es un poquito más colorido que esto, pero bueno.

Esto nos da algunos números de alto nivel desde el inicio sobre cómo sigue creciendo este problema y habla de los distintos tipos de ciberdelito y phishing, es en lo que nos vamos a centrar, en primer lugar, en este curso. Ver lo que es, cómo identificamos los intentos y cómo tratamos de evitarlo, si uno se siente altruista debe informarlo, denunciarlo, para que no afecte a los demás.

Vamos a hablar de qué se trata el phishing, cuáles son los pasos, cómo se ubica al usuario. Hay un sitio del que se recopila información a través de pharming, una pantalla de ingreso, se dirige al servidor de pharming, en lugar de la persona que uno estaba pensando que es la persona que uno conoce; y este es el

círculo que uno conoce, o quizás uno recibe un email, puede llegar a pensar que viene del Banco de América y uno al ingresar se encuentra en el sitio del Banco de América, uno ingresa la información al sitio y, si son inteligentes, lo mandarían al Banco de América.

Uno sigue recibiendo el dinero, no sabes que la información fue capturada y uno cree que se hizo la transacción prevista. Tenemos distintos tipos de phishing, este puede ser divertido, hice una clase para organizaciones de ALAC regionales de Norte América sobre phishing y se hizo algo investigando sobre una escuela, el nombre del quarterback, el año en el que estuvo y después mandó una carta para conseguir fondos desde el quarterback, apuntando a un sitio que parecía el sitio de los egresados de la escuela. Entonces todos estaban muy sorprendidos de la cantidad de información que estaba disponible sobre él, en este caso, el quarterback.

El phishing lo agregamos hace poco, a pedido de Ram, es cada vez más relevante todo esto. Este es el orden de las cosas, ya hablamos de los correos electrónicos y cómo se construyen, tenemos un remitente sospechoso, información sospechosa y después algunos mensajes de phishing para demostrar las distintas posibilidades y aspectos que aparecen en los emails. Creo que vamos a hacer más de esto y en distintos idiomas a medida que va evolucionando.

Hablamos un poco del malware o software malicioso, los números de llamadas telefónicas gratuitas, hablamos fundamentalmente de phishing, pero tratamos de ser un poquito más abarcatorios.

Estos son los representantes de atención al cliente, las cosas que no hay que hacer, la URL; cómo recuperarlas, para verificar si realmente están apuntando a este tipo de cosas, lo que subyace en estos mensajes, tenemos algunos ejemplos, algunas sugerencias.

Luego quizás estén familiarizados con que Google en algún momento armó un crucigrama en múltiples idiomas listos para utilizar, muy abarcatorio, sobre ciberdelito, entonces lo subimos para que la gente lo probara, hablamos de los distintos tipos, el phishing, las cosas que podemos hacer para evitarlo y para informarlo; para que tengan una idea, también voy a compartir esto con ustedes.

Ya compartimos una versión anterior, pero creo que esta es más profunda, así que, sería bueno volverla a ver. Tenemos un resumen y al final algunas URL, los códigos QR van a llegar a los lugares donde se denuncian las cosas y eso es lo que hablamos ayer.

Tenemos una localización, en este caso, para comunicarse con la FTC, llegado el caso, pero eso es básicamente el curso resumido y tenemos que divulgarlo en la infraestructura a las organizaciones regionales de At-Large y sus miembros, la mitad son capítulos de ISOC y algunas son organizaciones de interés para las actividades de la ICANN, y muestran algo de interés en participar en las cosas que venimos haciendo, por ejemplo, en la Aceptación Universal y otras cosas.

Tenemos algunas relaciones que estamos iniciando, por ejemplo, con la Organización Internacional de Bibliotecas para llegar a sus

comunidades, también para utilizarlo en los centros comunitarios y en las bibliotecas, así que, estaban muy contentos de ver cursos multilingües y es bueno compartirlo con ellos.

BARRY LEIBA

Estuvo hablando del aspecto personalizado y el correo electrónico con el idioma coloquial. En el último mes estuve en el grupo de anti uso indebido y el simposio de seguridad distribuida del DNS, hubo debates de algo que habíamos visto mucho últimamente con la hiper personalización de los mensajes en una escala que no se podía hacer antes a través de la IA, recopilando información sobre todos y personalizando los mensajes que solían ser solamente prácticos para mandar al presidente de una empresa, pero se lo pueden mandar a Jonathan, a Matthias o a mí.

Recibes mensajes donde saben en dónde vives, saben dónde trabajas, lo que haces, cuáles son tus pasatiempos… Es muy difícil distinguirlos de los mensajes reales, así que, quizás quieran encarar ese tema para ver la gravedad del problema, incluso la gente lúcida en cuanto a esto también se ve engañada.

JONATHAN ZUCK

Si tiene ejemplos que quiera compartir sería muy bueno, me siento un poco mal porque no he recibido un mensaje altamente personalizado, pero bueno, usted y yo no, me da lástima francamente.

Yo puedo comprar Bitcoin, ¿por qué me dejan afuera? Entonces me encantaría ver alguno, solamente he escuchado hablar de ellos y yo creé uno, tal como les dije, desde cero con mi propia débil inteligencia.

BARRY LEIBA: Voy a ver si encuentro algún ejemplo.

MATTHIAS HUDOBNIK: Dos cosas. Mi primera pregunta sería, ¿hay alguna planificación después de cada capítulo? Hacer una evaluación para verificar si se entendió, por ejemplo, si se seleccionó tal cosa, después un par de preguntas para verificar el conocimiento y también se espera que ICANN Learn esté disponible para que su amplia audiencia pueda tomar estos ejemplos.

JONATHAN ZUCK: Excelente idea. Tenía varias evaluaciones en una versión anterior y pensé que el crucigrama lo abarcaba, pero quizás es mejor tener evaluaciones verbales con un seminario especializado, así que, puedo revisarlo y agregarlo, nuevamente.

Hablando de ICANN Learn, una clase no necesariamente tendría que ser como esto, pero, en general, las clases de ICANN Learn parecen libros de texto de los años 70', pero me he enterado de esto por la ley estadounidense con capacidades diferentes y había lectores de pantallas. Yo soy disléxico, entonces me daban 30 páginas de texto, eso afectaba mi capacidad, pero sería algo válido

para hacer y tenemos que investigar a ver cómo podría terminar siendo esto, así que, es una buena sugerencia.

Ya me perdí con el orden, ¿quién sigue?

LAYAL JEBRAN

Vi que presentó MFA, entonces dada esa parte como la autenticación, que es muy vulnerable, ¿consideraría también incluir claves de acceso? A mí me parece que es muy útil. Gracias.

JONATHAN ZUCK

¿Te refieres a las aplicaciones de autenticación? La tensión aquí es tratar de ubicar la audiencia a la que nos queremos dirigir y nos queremos concentrar, por ejemplo, por un lado, Sébastien hizo una prueba con las versiones anteriores con mujeres de una mayor edad, las que estaban a punto de jubilarse o jubiladas, y les pareció que era bastante abrumador, o sea no sé a qué grupo te estarías refiriendo, tal vez tenemos que concentrarnos en el objetivo, según el público al que estamos apuntando.

LAYAL JEBRAN

Por ejemplo, las claves de acceso se implementan ahora por defecto en Google y se necesita autenticación, ¿no es cierto?

TARA WHALEN

Me parece muy importante ubicar nuestros objetivos y ver cuál es el público al que apuntamos y, en general, la expectativa es que puedan reconocer las URL cuando son URL incorrectas, se pone

mucho esfuerzo en el individuo para que pueda identificar los URL correctos y eso puede ser muy difícil, entonces pueden poner identificaciones de multifactor, contraseñas, o lo que sea necesario para poder tener estas opciones.

(Hay un dialogo entre Jonathan Zuck y la oradora).

Ninguna de estas opciones es perfecta, la dificultad, es decir: “Le dijimos toda la información, está todo allí, el usuario lo puede descifrar por sí solo”, y no están así. Es bastante difícil.

JONATHAN ZUCK: En los 90’ el 80% de las contraseñas, en general, se obtenían y las podían hackear a través del teléfono.

BARRY LEIBA: La audiencia ya está viendo solicitudes de las aplicaciones de los sitios web que solicitan el cambio de contraseña, se les alienta a hacer esto.

SÉBASTIEN BACHOLLET: Voy a hablar en francés, si me lo permiten. Aprovechando la primera versión del curso de Jonathan traté de utilizarlo y presentarlo, básicamente con estas mujeres en edad de jubilación lo entiendo porque es nuestro trabajo tratar de ser lo más abarcativo posible, lo más completo posible, pero hay que ver cómo lo vamos a presentar, cuáles son los ejemplos que vamos a tomar en cada uno de los idiomas y de cada uno de los países en el

que lo vamos a dirigir, y eso lleva mucho tiempo, va a ser una gran parte de la tarea ver si podemos tener una presentación que sea en varias etapas.

Por ejemplo, en la escuela y el grado siguiente, pero esto también demanda mucho tiempo, mucho trabajo, entonces me parece que, en primer lugar, no hay que agregar demasiado por el momento, sino usar lo que ya tenemos y ver cuál puede ser la retroalimentación que podemos obtener para ver las cosas que se pueden mejorar y que vengan estos feedback de parte de la gente que lo necesita.

Yo vivo en Francia en un lugar muy alejado y explicar este tipo de cosas es complejo cuando tenemos que explicar lo que sucede en un teléfono celular, o en una computadora portátil; según la marca de computadora, y demás, todo esto lleva mucho tiempo, entonces me parece que tenemos que tomar todo en cuenta en un momento u otro, como dije antes, ya todo lo que se hizo está muy bien.

JONATHAN ZUCK Creo que con la aclaración estamos agregando cosas para alentar este enfoque y abordar estos temas, no hay que aprender tanto sobre la tecnología subyacente, tal vez eso es algo fácil de agregar.

No veo la lista de participantes, permítanme un segundo. Tenemos a Robert que desea hacer uso de la palabra, pero, primero, tenemos a Jeff.

JEFFREY BEDSER

Una de las cosas que deberían considerarse es que hay una tendencia creciente, que se llama los fake shop o lugares donde se compran falsos, la percepción es exactamente como el phishing, pero el mecanismo es diferente. En el mundo de la ICANN este fake shop significa esto, no es una tienda que venda cosas falsas, sino que el sitio en sí es falso y va a robarnos nuestros datos personales y de tarjeta de crédito, es el mismo fraude que el phishing, pero con otro mecanismo.

Esto es algo que me parece que tenemos que agregar, por ejemplo, si vemos que el precio no parece correcto y se vende tras una plataforma de redes sociales y nos lleva a otra plataforma, hay que desconfiar de esa plataforma, puede ser básicamente un phishing a través de las redes sociales.

JONATHAN ZUCK

La verdad es que lo podemos resumir como que el mundo allá afuera es muy peligroso, da un poco de miedo.

NABIL BENAMAR

Con la introducción de la Inteligencia Artificial todo puede cambiar o ha cambiado drásticamente, sobre todo el uso del phishing a través del email.

Hemos empezado a hablar sobre este tema recientemente en SSAC, basándonos en esto le he pedido a uno de mis estudiantes que hiciera un sondeo sobre distintos enfoques para combatir este

tipo de ataques y encontramos un gran número de personas que hablan ya de este tema, que han hecho publicaciones al respecto, es algo urgente, necesitamos repensar nuestro enfoque para combatir los ataques de phishing utilizando la Inteligencia Artificial, estos ataques generados a través de la Inteligencia Artificial, afortunadamente la Inteligencia Artificial también puede detectar estos ataques hasta cierto punto.

JONATHAN ZUCK Sí, es verdad que hay muchos cambios con la Inteligencia Artificial. Robert, adelante.

ROBERT GUERRA Soy del SSAC. Creo que estamos escuchando mucho sobre cómo mejorar los cursos, las capacitaciones, hacer cuestionarios y demás, algo importante que no estoy escuchando es que hay una necesidad de hacer esto más que nunca antes, el entorno en el que los activistas y otros se encuentran, aquí en Estados Unidos y en otros países las amenazas son mayores que nunca.

Entonces no tenemos que esperar a que esté perfecto, sino que tiene que hacerse, es mejor hecho que perfecto. Hay que traducir a distintos idiomas, transmitirlo a las personas y quiero decir, sobre todo en cuanto al phishing, que hay que incluir cosas nuevas, no perdamos tiempo con un solo mercado, tenemos que difundirlo lo antes posible porque hay una verdadera necesidad. Eso quería decir, gracias.

JONATHAN ZUCK Gracias, Robert. Hadia.

HADIA ELMINIAWI Quisiera comentar sobre lo que mencionó Sébastien. Durante la pandemia hice algunos seminarios web sobre la seguridad y el fraude en línea, fue en árabe e incluí SMS, y también los factores de doble autenticación, cómo mitigar esto y cómo protegernos.

Los seminarios web estaban dirigidos a un grupo de mujeres no profesionales, la mayoría estaban jubiladas, diría de más de 70 años, fue muy bien recibido y sí entendieron de qué se trataba lo que se les estaba presentando, y estaban muy interesadas en tener más información.

Entonces la percepción de que si alguien es una persona mayor y no tiene una formación profesional no va a poder comprender lo que se les está explicando, me parece que no es un concepto correcto porque si uno está en línea aprecia mucho la información que puede recibir para poder protegerse en línea, incluso a través de los SMS, también podemos ser víctimas de phishing a través de los mensajes de textos que recibimos. Muchas gracias.

JONATHAN ZUCK Adelante, por favor.

MATTHIAS HUDOBNIK

Hay guías en línea muy buenas, por ejemplo, de Privacy International, Tactical Tech, también security in a box, o sea para distintos públicos y sobre distintos temas, cómo crear autenticación multifactor, contraseñas, usar distintas direcciones de email, cómo defenderse en el mundo digital; y creo que esto es muy útil cuando usamos distintos buscadores, cómo hacer rastreo de las cookie y demás. Creo que esto ha sido probado en muchos públicos diferentes y es realmente muy puntual.

ADRIAN SCHMIDT

En mi trabajo todos tenemos un trabajo, salvo que estemos felizmente jubilados. Soy director de IT para una asociación sin fines de lucro y este año decidimos presentar concientización acerca de la seguridad en internet y tuvo muy buena recepción.

Lo otro que me parece que tenemos que tener es una estrategia y difundirlo a las personas, por ejemplo, mi papá, que falleció hace un mes tenía 92 años, y me preguntaba siempre cómo podía ayudarlo para que no le roben a través de la tecnología, al mismo tiempo, que estamos tratando de evitar estos casos de phishing. Tenemos que pensar en cómo queremos que sea el nuevo internet, sobre todo pensar en generaciones de mayor edad que percibe las cosas de otra forma que las nuevas generaciones que nacieron con la tecnología y confían más en la tecnología, que la generación de las personas más mayores donde viéramos el mal de la tecnología.

Entonces necesitamos encontrar estos enfoques más creativos e innovadores para tratar de crear una forma de tecnología

diferente, donde el enlace débil sea solamente la persona, necesitamos tener una tecnología mucho más resiliente.

JONATHAN ZUCK Le damos la palabra a Amrita.

AMRITA CHOUDHURY Creo que, como ha dicho Roberto, phishing es un tema que todo el mundo está viendo actualmente y entendiendo, creo que, como ICANN, nos remetimos a los nombres de dominios, pero está sucediendo también en la fase de contenido, tenemos que verlo en su totalidad, hay muchos mensajes, pero si pensamos en los países en desarrollo tal vez las personas no estén leyendo el tema o haya personas que puedan acceder a ciertos mensajes de video, o que tal vez son analfabetas y no tienen acceso a ciertos contenidos, hay muchos videos para explicar, incluso en las instituciones bancarias, por ejemplo.

Entonces, ¿cómo podemos hacer que las cosas sean más interactivas para que más gente tenga acceso a esta información? Creo que hay muchas formas de publicarlo, lo podemos ir mejorando, pero tenemos que pensar en cómo abordar estos aspectos del phishing que vienen del contenido y no solamente a nivel del nombre de dominio, creo que esto es muy importante.

JONATHAN ZUCK Todo es cierto, es un gran problema, por eso seguimos trabajando con la cámara de partes contratadas y ustedes defienden algunas

soluciones orientadas a la tecnología, estamos tratando de hacer lo que podamos para hacer un aporte a la mitigación de estas circunstancias, no hay una solución sencilla.

Creo que hemos visto todas las manos. Puedo ir a Natálie, primero.

NATÁLIE TERČOVÁ

Gracias. Es un comentario rápido porque me estaba centrando en los últimos cuatro años como parte de mi doctorado en las capacidades y alfabetización digital de los jóvenes y niños.

Estoy muy feliz de que la gente anciana sea solo el grupo más vulnerable, pero la felicidad es respecto a los niños que son nativos digitales, nacidos después del año 2000 con todas las capacidades necesarias para protegerse, para no tener que centrarnos tanto en ellos, sin embargo, esto no es totalmente cierto y viendo este tema desde mi perspectiva, en la región europea donde hay muchos países, hemos visto que cuando informan sus capacidades sobreestiman su conocimiento porque les da vergüenza, probablemente, no saber cómo se protegen, pero si le dan alguna tarea verán que les falta conocimiento crítico y también necesitan ayuda.

Quería resaltar ese tema que todavía está aquí y necesita nuestra ayuda. Vemos también que la gente mayor tiene las capacidades críticas del mundo fuera de línea y que se puede transferir al mundo en línea con facilidad, y son los jóvenes los que no la tienen, así que, no tenemos que olvidarnos de ellos.

Suelo recibir muchas invitaciones a conferencias siendo una académica y normalmente tengo un poquito de ayuda, tiene que ver con cómo está escrito antes, si había errores era IA, pero ahora ha cambiado, muchos colegas rechazan correos pensando, “esto probablemente es un fraude porque es un horror”, pero era el humano que estaba sentado en la computadora que no estaba tan avanzado como la IA.

Entonces la mentalidad es, ¿cómo podemos detectar los fraudes o un intento de phishing? Esto está cambiando con rapidez, entonces es algo que tenemos que considerar. Muchas gracias.

JONATHAN ZUCK

Totalmente de acuerdo, desde mi experiencia, los jóvenes ni siquiera saben hacerse un huevo duro, así que, estaría de acuerdo. Pero recuerdo cuando hablaban de los principios de Nigeria y los correos estaban llenos de errores gramáticos, me acuerdo que se decía que era intencional porque uno era lo suficientemente educado para reconocer los errores, esto era un juego de volumen, e iban a eliminarlos porque los que no veían los errores gramaticales eran los más susceptibles a aceptarlo y esto solamente empeoró con la IA.

EMILIA ZALEWSKA-CZAJCZYŃSKA

Quería resaltar lo que dijo Natálie y también algunos otros grupos vulnerables. En la Unión Europea, por ejemplo, hay leyes sobre IA y hay otras con algunos grupos que son especialmente vulnerables a

distintos tipos de manipulación, también los ancianos, los niños, las personas con capacidades diferentes, también la gente en circunstancias económicas complejas y distintas minorías.

Así que, creo que también vale la pena considerar que estos son los grupos que normalmente hablan de alfabetización digital, los ancianos, los niños o jóvenes, pero también hay grupos como las personas con capacidades diferentes, que son vulnerables, y para ellos quizás tengan necesidades distintas en términos de creación de capacidad, no solamente por las capacidades diferentes que puedan afectar sus capacidades, sino también en términos de phishing y otros tipos de delitos que puedan querer explotar sus dificultades.

Por ejemplo, las personas que tienen o pertenecen a minorías y también lo que se habló aquí de la IA, que ayuda a recopilar datos para apuntar a esta gente, para segmentarlo. Por ejemplo, en Polonia hace un par de años… Esta es una historia un poco distinta, pero algunos casos tienen similitudes.

Hubo una publicación redactada por personas que son profesionales con publicaciones sobre cómo fácilmente ven de determinada forma si en estas publicaciones había enlaces o links. De pronto si yo quiero vender un departamento de dos dormitorios, uno seleccionaba el enlace, tenía que ingresar el correo electrónico y se le mandaba a la persona que había emitido la publicación. Gracias a eso recopilaron datos del estado financiero de personas que querían vender sus departamentos,

que tenían deudas, que tenían préstamos y los segmentaban con sus necesidades.

La IA facilita mucho esto, nuestros datos están en internet, es sencillo recopilar y ver quién es de qué grupo vulnerable, por lo cual esto es algo a considerar; más allá de aquellos que nos vienen a la mente cuando pensamos en vulnerabilidades, sino considerar estas nuevas maneras sobre cómo se puede segmentar estos grupos. Gracias.

JONATHAN ZUCK Muchas gracias. Esto es tan deprimente, pero es bueno siempre hablar de todas estas cosas. Respecto de lo que dijo Robert, creo que vamos a tratar de avanzar y utilizar estas cosas, ver cómo reacciona la gente, dejar que crezca, que se desarrolle y que se pruebe en distintos ambientes.

Si necesitamos diversificar a los distintos grupos, lo haremos, pero en este punto creo que no tenemos que excluir a ninguno, por lo cual vamos a tratar de llegar a distintas personas con distintas alianzas, estoy muy entusiasmado con el tema de las bibliotecas y los distintos grupos que tenemos siempre en el radar, vamos a ver cómo funciona esto.

Esperamos algunas noticias buenas sobre su último trabajo porque creo que ya terminamos con todo lo demás. Muchas gracias.

JEFFREY BEDSER

Creo que vamos a hablar de INFERMAL, les ruego que me disculpen, no van a ser buenas noticias, pero sí va a facilitar algo de conversaciones hacia adelante.

Vamos a ver un par de sitios para informarnos sobre INFERMAL, este es un informe de la oficina de los científicos de datos respondiendo a algunas preguntas claves desde algún punto en el tiempo sobre algunos temas, el phishing y uso indebido del DNS.

La conclusión del informe es que están los incentivos económicos y la verificación proactiva en estas concentraciones donde suceden los usos indebidos, en cuanto a las partes que proveen dominios a los registradores, pero nada ofrece soluciones a los problemas, básicamente valida lo que se viene diciendo desde los últimos 10 años, ¿los precios bajos facilitan las compras a granel de dominios y también lo facilitan? La respuesta, por supuesto, en base a los estudios hay concentraciones del problema en volumen y en el lugar donde los precios son menos generosos se pueden adquirir volúmenes más rápidos y más grandes. Siguiente, por favor.

Entonces en algunos de los hallazgos claves, las cuotas de registros más bajos, servicios gratuitos, por supuesto, los descuentos obviamente, las restricciones más estrictas pueden reducir el uso indebido agregando más fricción al sistema para evitar la facilidad del acceso con fines de uso indebido del DNS. El acceso a las API cuenta con más del 401% de elevación en los dominios maliciosos, pero hay una salvedad en base a ciertos tipos de usos indebidos y las prácticas de verificación que, nuevamente, puede ser un punto

de fricción como activa o proactiva en cuanto a la adquisición de dominios para uso indebido. Siguiente.

Las medidas reactivas, los tiempos de mitigación. Este es uno de los hallazgos que hablamos en los puntos que vamos a tocar al final de la presentación, el punto de spear phishing que nos comentó Jonathan, también es una víctima a la que se segmenta para el phishing, la cantidad de víctimas que puede haber en un segundo si hay una distribución en masa versus cuántas en 10 segundos y cuántas se detectan en 48 horas, y la comparación entre ambas.

La práctica de registradores, por supuesto, con ciertos TLD en base a las prácticas comerciales, los menores precios y los servicios gratuitos. Siguiente.

Los precios y la facilidad de acceso son puntos fundamentales para la economía, la gente va al lugar donde el precio es inferior, por eso en Norte América particularmente con estos lugares, tales como Walmart, sus segmentos ofrecen muchos precios bajos y permite comprar grandes cantidades.

No creo que ninguno aquí esté sorprendido con la concentración que se ve cuando los precios son más bajos, sin embargo, ustedes vieron las cifras que mostró Jonathan y vemos un incremento de un trillón a 10 trillones, y esto es un tema para debate, pero es un debate que no vamos a tener ahora porque añadir un cero al trillón son trillones de pérdidas de ciberdelitos relacionadas con los dominios y está mal, por supuesto.

Pero ¿a qué precio? Con un dominio la pérdida promedio por víctima globalmente es de 138, no parece tanto, pero en Estados Unidos es $3.520, si estos son los montos que se ganan en un dominio por parte del delincuente, ¿a qué precio van a comprar un dominio con fines criminales? Podemos apuntar al primer GDP o al segundo GDP, depende si es un trillón o 10 trillones, la realidad de la concentración de precios bajos creo que es un hecho que todos reconocemos. Si tenemos un precio muy alto por dominio, no sé cómo funcionaría eso, pero no creo que sea una solución el tema del precio porque siempre vamos a ir al precio más bajo.

Siguiente, por favor. Procesos de verificación, hay varios TLD de códigos de país con procesos muy estrictos de verificación, pero en su mayoría son manuales, dado que la capacidad de crear identidades digitales que no solamente puedan crear una persona falsa completamente, pero que se pueden utilizar para usar la identidad o crear la identidad con la cara de otro, está muy bien hecho y son las generadas de IA, son significativamente mejores que las que se hacía originalmente, entonces uno no sabe cómo son las fotos o la identificación del estado de Pensilvania, se podría parecer a mí el registro de conductor.

Entonces el proceso de verificación está en riesgo en base a la evolución de la tecnología, sí se puede hacer, básicamente insistir que hay que hablar con una persona cada vez que se registra un dominio, pero creo que la practicidad del volumen del registro es algo cuestionable respecto de la manera de usar el sistema.

Los índices de detección, delegación y mitigación es una medición valida, diría que hablando de uso indebido del DNS todos los informes públicos de terceros y los informes anuales, o trimestrales, de los volúmenes de uso indebido de la ICANN, de InterRail, de Spamhaus, todos ven los datos públicos, para mí es la punta del iceberg cada una de las partes a las que apuntan este tipo de delitos, tienen muchos mitigados que nunca aparecen en esa lista, pero hay informes de uso indebido porque alguien lo detectó y alguien lo denunció.

Todos podemos adivinar cuántos han aquí eliminado phishing y no lo informaron, si no lo han hecho, por favor, háganlo, el volumen no está denunciado, no vemos esas cifras, por lo cual, para mí, tiene que ver con el tiempo de la delegación a la mitigación, es un factor clave. Si podemos detectarlo lo antes posible entre la delegación y mitigarlo en segundos, quizás haya 10 víctimas en ese período de 2 o 10 segundos, pero, a la vez, reducimos la victimización, que es la meta. Con esta meta, con la capacitación de ALAC y demás, desarrollar esto y eliminarlo; en lugar de pararlo, porque hay un incentivo financiero y siempre tratan, y consiguen, la mejor manera de lograrlo, hay que denunciarlo, detectarlo y eliminarlo.

Y creo que la otra pregunta sería medir la cantidad de víctimas por dominio es una métrica más útil, podemos entender el tamaño, el costo de las pérdidas y dónde están las víctimas. Siguiente, por favor.

Bien, uno de los puntos sobre la imagen anterior era un aumento del 401% cuando había una API disponible para los registros de dominios, sin embargo, este algoritmo de generación de dominios, o DGA, tenemos que pensar en qué punto es apropiado restringir la compra de un mayor número de dominios, sé que en un sentido corporativo cuando alguien lanza una nueva marca o un nuevo producto van a tratar de comprar una marca o un nombre en varios TLD, entonces tenemos que pensar, ¿cómo podemos distinguirlos? Si hay alguno que es delictivo.

Entonces estas son las preguntas en las que nos tenemos que concentrar, las métricas de dominios han confirmado algo y es la concentración alrededor del incentivo económico de obtener algo al menor precio posible, entonces para los que se dedican al ciberdelito tienen mucho más beneficio que el costo del sistema en sí, tenemos que informar, detectar y aumentar la mitigación para evitar la victimización, para asegurarnos de que haya una ventana muy pequeña en la que puede haber este uso indebido y que ya no sea interesante para los criminales poder utilizar este método para victimizar a las personas.

RAM MOHAN Roberts, adelante. Satish.

SATISH BABU Muchas gracias, Ram. Esto tiene que ver con la sección anterior, pero me parece que es pertinente. Solo este mes el Banco Central

en India emitió una circular que introduce dos subdominios exclusivos, .BANK.IN y .FIN.IN, que los bancos y las instituciones financieras en India tienen la obligación de usar. Lo estoy mencionando, pero no estoy seguro de cuánto éxito va a tener, pero prueba de que hay un punto de control que las personas no pueden registrar una gran cantidad de nombres de dominios.

RAM MOHAN Muchas gracias, Satish. Jonathan, por favor.

JONATHAN ZUCK Gracias, Satish. Sí, creo que, lo que has dicho es algo similar a la restricción de dominios y la menor concentración de uso indebido, entonces se está tratando de fomentar esto, el GAC está trabajando en esto desde hace bastante tiempo para que las instituciones financieras, los médicos, los abogados tengan TLD restringidos que ayuden a las personas a buscar estos subgrupos más pequeños de dominios.

Y, creo que, nos tenemos que preguntar, ¿qué es lo que tenemos que hacer para alentar a las partes contratadas y a los registradores en particular para que lleven a cabo algunos debates o negociaciones? Que podamos hablar con ellos para ver qué es lo que podrían hacer y lo que no, no sé si tal vez la verificación o alguna otra medida que valga la pena implementar porque, de lo contrario, el debate es… ¿Cómo decirlo? Como un anhelo en vez de una acción concreta. Esa era mi pregunta.

JEFFREY BEDSER

Creo que uno de los problemas y es lo que surgió del SAC115, que tiene que ver con la interoperabilidad y la gestión del uso indebido del DNS, se necesita que cada parte contratada verifique cada informe para que pueda actuar al respecto y si el informe establece las pruebas la acción es más simple porque si necesitamos que una persona investigue sobre cada phishing que se informa estamos hablando de una demora de muchos días y de muchas personas trabajando en esto.

Entonces creo que una de las cosas importantes y que tenemos que agregar al componente de capacitación, no solamente saber qué es el phishing, sino también cómo se informa un caso de phishing para que la gente sepa cómo informarlo porque hace unos seis o siete años se informaba y no pasaba nada en un caso de estos, algunas partes lo informaban y otras no, pero había tanto esfuerzo en validarlo que ya no se informaba porque no pasaba nada al informarse.

Y justamente eso es lo que queremos cambiar, tener un componente de formación donde no solamente no seamos víctimas de este tipo de delitos, sino que, también cuando lo identifiquemos podamos informarlo y para cuando se informe también con esa evidencia se pueda mitigar.

JONATHAN ZUCK

Hemos hecho algo de investigación por nuestra parte, tener herramientas y mi frustración principal es que, con la herramienta NetBeacon, necesitamos formar parte del proceso de informe y que sería muy bueno si hubiera una herramienta donde solamente hubiera que reenviar algún email sin tener que hacer mucho más.

JEFFREY BEDSER

Se podría tratar de resolver esto con un DNS que done software para NetBeacon con este propósito, es un punto válido el que mencionas y podemos hablar con Graeme para tratar de solucionar esto.

RAM MOHAN

Olivier.

OLIVIER CRÉPIN-LEBLOND

Hablando sobre este informe INFERMAL, que fue publicado en noviembre, si entiendo bien, como tenemos un nuevo gobierno en los Estados Unidos y el mundo ha cambiado bastante desde entonces, hay muchas cosas que están cambiando y viendo esto me pregunto, ¿qué ha sucedido desde entonces? Han pasado cuatro meses, ¿hay alguna acción? O algo que surja de esta ronda para educar a las personas, no sé si habrá algún cambio en este espacio, para ver si hay algunas acciones más sólidas al respecto o si vamos a continuar diciendo: “Estamos condenados, estamos en problemas…” ¿Y vamos a seguir haciendo informes sobre qué mal

está la situación? No sé si me explico, mi pregunta es más sobre lo que podemos hacer.

RAM MOHAN Podemos volver a la diapositiva anterior, por favor Jeff, no sé si quiere tomar el micrófono.

JEFFREY BEDSER Sí. Bueno, no estás equivocado, en un foro público no sé si podemos hablar honestamente de esto, podemos hablarlo luego en privado, pero creo que el problema principal que tenemos es que estamos lidiando con la punta del iceberg y necesitamos hacernos la idea de que las partes contratadas han hecho un gran paso al proponerse a tomar más medidas y esto se puede justamente facilitar o llevar a cabo haciendo más informes.

Entonces no sé qué otros mecanismos puedan existir hoy para identificar este uso indebido y tenemos que justamente mejorar, tenemos que ver cómo pasar de esperar a que exista una víctima y que haya pérdidas a poder detenerlo, detener este concepto del pre-delito, ¿no? Como la película Minority Report, tenemos que pensar en que los criminales usan las mismas estructuras una y otra vez porque la infraestructura es costosa y podemos ver cuáles son los patrones para determinar si el dominio se utiliza para un solo individuo o no.

Así que, mi frustración, en realidad, son los informes constantes sobre las mismas fuentes de datos y eso es lo que me asusta, me

pregunto, ¿cuán grande es el iceberg? Si solo estamos viendo la punta.

RAM MOHAN Alan.

ALAN GREENBERG Me llegó un SMS de phishing y lo informé, unos días después todavía seguía activo y estaba en el mismo vuelo que Graeme el otro día y le pregunté, ¿cuán rápido las personas suelen responder? Y me dijo que algunos registradores muy rápido y otros no contestan. Es verdad que hay obligaciones, pero no necesariamente se cumplen.

Creo que nuestra opción actual es concentrarnos en lo que podemos hacer, las registraciones en masa es una cosa a la que podemos prestar atención, preguntar quiénes están autorizados a utilizar las API y quiénes no, y que lo justifiquen, que tengan que pedir una solicitud o una autorización y justificarlo. Y si tienen dominios que se dan de baja por uso indebido, bueno, que ya no se puedan utilizar más.

Creo que algunas de estas cosas son fáciles de implementar y tenemos que hacer que se implementen.

RAM MOHAN Tiene razón, dentro de nuestro entorno lo primero que tenemos que hacer es publicar buenas prácticas, cuáles son las prácticas

razonables con sentido común que pueden utilizarse dentro del entorno de desarrollo de políticas, el Proceso de Desarrollo de Políticas porque para cuando ya tengamos el resultado todas las recomendaciones que se han hecho ya van a ser obsoletas por motivos obvios, ¿verdad?

Entonces, como dijo Jeff, cada vez más partes en este entorno están tomando la iniciativa para tratar de mitigar y reducir la incidencia de este tipo de problemas, no es algo uniforme, pero creo que a lo que deberíamos apuntar como medida, tal vez, no es a uniformidad, sino tratar de tener la mayor cantidad de partes involucradas, por un lado, y, por otro lado, creo que es algo que ALAC y SSAC van a estar muy contentos en contribuir y colaborar para tener cada vez más capacitación sobre no solamente cómo reconocer el phishing o si se nos está queriendo tener como víctimas de phishing, sino cómo informarlo, no solo identificarlo, sino también cómo informarlo.

Una vez que tenemos esa información vamos a tener un conjunto de datos que podemos analizar y podemos señalar a aquellos que deberían actuar o hacer algo al respecto y decirles: “Bueno, tienen tantos informes que han recibido, ¿y cómo van a responder a eso?” Y ahí sí tenemos algo concreto sobre lo que podemos actuar y podemos presionar un poco.

Actualmente como que cada uno tiene que hacer lo que es moralmente correcto y eso a veces está en conflicto con los

intereses económicos, si me lo permiten, lamentablemente estas obligaciones o estos intereses económicos.

ALAN GREENBERG Tienen que ver con estos… Tenemos personas en esta sala que estarían dispuestos a interactuar con nosotros, no solamente como líneas.

JEFFREY BEDSER Ni el registrador ni el registro hacen dinero el primer año, entonces no están dispuestos a uso indebido, el dinero se hace con las remuneraciones y la mayoría del uso indebido con algunas excepciones, estos outliers no van más allá de los 365 días, si van al día 364 no van a repetir el pago, entonces la economía y los incentivos…

Y también hay delitos con las tarjetas de crédito, entonces la idea es que se quedan solamente si hay crecimiento económico. Quisiera recordarles a todos, y probablemente estoy hablando desde el coro, como así se dice, los ciberdelincuentes están mirándonos, están mirando lo que hablamos en el foro público para ver qué van a hacer, por ejemplo, sé que hay registradores, si tienen problemas con los clientes legítimos que compran cuentas, las crean, las financian, compran dominios y después venden toda la cuenta a alguna otra persona que la utiliza para delito.

Entonces, ¿cómo va el registrador a atraparlo? Yo solía pensar que ellos sabían de estos y que básicamente compraban y vendían

cuentas a un revendedor no autorizado, este es el punto, no se trata de restringir el acceso a los dominios, sino ver cómo atraparlos y pararlos, en lugar de tratar de poner restricciones que nos den cinco o 10 pasos por delante para ver cómo pueden ellos evitar tal cantidad de bloqueos.

JONATHAN ZUCK: INFERMAL tiene razón.

JEFFREY BEDSER: Bien dicho.

RAM MOHAN: Muy bien, esta es la parte linda del tema. Esta parte es para iniciar un diálogo con ustedes, pero también para compartir con ustedes las áreas principales, las cinco en las que se centra SSAC… Yo lo llamaba temas de estado quieto, pero ya no lo hago.

En estos cinco pasos que hablamos con ustedes de muchas maneras fundamentalmente el primero sobre el uso indebido del DNS, esto tiene efecto directo sobre los usuarios y tiene puntos tangibles, vamos a seguir trabajando con ustedes porque la seguridad no termina en esta campaña, lo que venimos haciendo juntos; y creo que lo que hemos hecho, es excelente como punto de partida, pero tenemos 125 documentos adicionales que hemos elaborado con hallazgos, recomendaciones y cosas de ese tipo, que consideramos también, no todos, pero muchos de ellos tienen

efectos prácticos en la vida real, algunos son para divertirse nada más, algunos son de la transición de la IANA que ya no usamos.

Queremos trabajar con ustedes en estos aspectos, lo que hace falta de ustedes, lo que les pedimos y podemos tener una sesión con ustedes para tratar de resolver estos temas, ¿cuáles de estos temas principales que tenemos tienen la mayor resonancia y necesidad de las audiencias a las que ustedes apuntan? Porque una cosa es tener una plétora de información, pero la meta, propiamente dicha, es tomarla, darle forma para que la información se pueda utilizar de manera adecuada.

En el uso indebido del DNS en particular sospecho, Jonathan, que tenemos 30 o 40 documentos elaborados sobre el punto, esto es una vena profunda en la mina para explotar. En los nuevos gTLD, para refrescar la memoria, venimos trabajando, opinando, comentando y asesorando sobre los nuevos gTLD desde hace tiempo, lo más reciente que hemos hecho es el análisis de colisión de nombres y una serie de recomendaciones sobre cómo evitar, cuando un nuevo gTLD se presenta, no solamente la confusión, sino la colisión, propiamente dicha, con los nombres que ya se han resuelto o que ya se han solicitado hoy por hoy en internet.

Un buen ejemplo en la ronda previa eran los solicitantes de .HOME, .CORP, .MAIL los solicitaban, pero no eran conscientes de que esos tres gTLD tenían nombres que ya se habían utilizado en internet durante muchos años, inclusive décadas, previamente, o sea había ya mucho tráfico en internet que utilizaba el .HOME o el .CORP, hay

mucho trabajo escrito sobre el tema, pero a la ICANN y a la Junta les dimos algunas guías y recomendaciones claras sobre cómo evitar o, al menos, cómo mitigar ese tipo de colisiones en la próxima ronda.

Sobre DNSSEC hace tiempo ya, casi dos décadas, desde su implementación estamos empezando en todo este tiempo transcurrido en la ejecución operativa sucedida, ¿cuáles son las observaciones que podemos hacer? Una de ellas a nivel anecdótico o imperativo inclusive, es que en algún nivel de fragilidad adicional aparece y se puede utilizar cuando se trata de implementar DNSSEC. Los TLD, en general, los pequeños y los grandes, los que tienen buenos recursos y los que no tienen buenos recursos, encuentran problemas ante estas circunstancias, estamos en el proceso de considerar una carta orgánica para algo de trabajo en esta área, no empezamos todavía el trabajo, pero eso es lo que quisiéramos hacer.

En cuanto a los espacios de nombres alternativos y dentro de este mundo de la ICANN, que se ha expresado inicialmente como las muchas iniciativas expuestas disponibles sobre cadena de bloques, o Blockchain, nombres de espacios, interacción, integración con el espacio de nombres de dominios del DNS, hemos encargado a un grupo de trabajo que se ocupe de la integración responsable de estos espacios de trabajo dentro del DNS, sus aspectos, sus características y vamos a integrar estos espacios de nombres dentro de los del DNS, ¿cómo lo haríamos?

De manera responsable para mantener la seguridad y la estabilidad, y sus parámetros.

Entonces estamos recién empezando el trabajo al respecto y vamos a volverles a informar a ustedes cómo van yendo las cosas, algo subyacente en cuanto a esto es que dentro de SSAC el enfoque en cuanto a Blockchain, como ejemplo, y los nombres en Blockchain y otros espacios, no es algo reflexivo, no es que sea malo y que de pronto hay que bloquearlo en tal caso.

Lo que estamos haciendo es considerar las motivaciones detrás de las innovaciones centrándonos fundamentalmente en innovaciones, desarrollos, cómo afectan la integridad, la estabilidad y seguridad de los espacios de nombres de los que dependemos todos nosotros. Ese es el foco claro, hay trabajo que está pesando en esta área.

Y, finalmente, Olivier estaba hablando de un par de cambios que se están desarrollando a nivel mundial y no nos centramos demasiado en la geopolítica de estas cosas, sin embargo, les prestamos atención a los aspectos de SSR.

Nuestro enfoque general en el área consiste en tratar de brindar una clave práctica de la vida real sobre cómo funciona el DNS, si uno es un regulador o elabora políticas, o trabaja en el interés de la seguridad nacional vamos a redactar una ley sobre cómo se tiene que bloquear el DNS. Nuestro enfoque es no opinar respecto del bloqueo en sí, si es bueno o malo, sino brindar aclaraciones, de pronto, sobre: “Estas son las consecuencias no previstas

potenciales que puede haber si uno le da con un martillo a un chiche o a un pequeño clavo".

Entonces este es el enfoque que tenemos, ayer me informaron que, aparentemente, hay trabajo que está avanzando en la Unión Europea en la luz de recientes desarrollos sobre algún tipo de mecanismo de seguridad de los resolutores de DNS para forzarlo, en los resolutores europeos de DNS. Lo miré y pensé: "!Wow! Eso no es ingeniería, eso es alucinación en la vida real", no diría esto a quien se ocupa de elaborar políticas, probablemente les diríamos: "Brinde los detalles técnicos sobre cómo funciona la resolución…" Y ese tipo de cosas.

En esta parte, en realidad, lo que quiero decir aquí es que SSAC, en general, consiste en escépticos completos que son optimistas sobre el futuro para donde puede llegar a ir, pero también somos realistas en el sentido de que hay mucha fuerza, hay mucha gente que trata de beneficiarse a partir de una cultura básica que dice que uno puede confiar al otro lado de una transacción porque esa era la cultura que empezó toda esto.

Los miembros de SSAC, en general, tienen esa mentalidad, pero, a la vez, son conscientes de que eso es exactamente lo que buscan los que están del otro lado de la cerca para comprometer, erosionar, degradar y actuar en contra. Ese es el panorama en alto nivel de las áreas principales que estamos considerando y quisiera darles la palabra a colegas de ALAC y otros del SSAC.

JONATHAN ZUCK

Necesitamos no esperar hasta la próxima reunión de la ICANN para implementar algunas de estas conversaciones, quizás armar como un equipo pequeño y ver algunas cosas en las que compatibilizamos, ver algunas cosas que se conecta un poco con nuestro mandato y ver cómo podemos ser útiles para lograr algún resultado y llevar esto a una audiencia más amplia.

Estamos llegando ya al final, tenemos que permitirles a los intérpretes que descansen un poquito, así que, comprometámonos a no esperar tres meses porque la próxima reunión está como en 14 días, pero reunámonos, nuevamente, por Zoom y veamos algunos de estos temas de a uno y resolvámoslo, estamos muy contentos de recibirlos, pero nunca alcanza el tiempo cuando nos juntamos, hay mucho más pro hablar, tenemos tanto en común en cuanto a nuestra visión del mundo, así que, sigamos trabajando juntos. Muchas gracias a todos y disculpas, vamos a ver cómo seguimos adelante y gracias a los intérpretes.

[FIN DE LA TRANSCRIPCIÓN]