Informe preparado para la ICANN

Revisión del sistema de dominios Abuso Activity Reporting (DAAR) y la metodología

Por: Marcus J. Ranum, consultor

Resumen ejecutivo

He realizado una revisión rigurosa del sistema DAAR y su metodología, con especial atención pagado a la metodología de DAAR para combinar los datos existentes de nivel superior genéricos-dominio (gTLD) los registros y los registradores acreditados por ICANN con 3rd datos de reputación del partido. Una preocupación principal es que el DAAR sistema de forma precisa y creíble mide amenazas a la seguridad de los datos compuestos y puede ser se ve con confianza. Desde DAAR es un histórico enrollable de fuentes de datos - metadatos DNS más 3rd fiesta datos de clasificación. Su precisión será tan bueno como aquellas fuentes de datos; Sin embargo, esas fuentes son aceptadas con alta confianza en la industria ya y que son los que hacen la función de Internet DNS correctamente. Los datos compuestos en DAAR es una publicación útil: referencia histórica de calidad para el comunitarios, investigadores y registradores. La recopilación y compilación metodología es bien DAAR explicado y documentado.

Una segunda cuestión es si el DAAR estudia un conjunto significativo de datos que son dignos de estudio: si dominios de spam son una amenaza a la seguridad de la comunidad de usuarios de Internet. Son. Además de la colocación de una carga masiva innecesaria, sin valor en la infraestructura de DNS, dominios de spam tienen importantes papeles en despliegues de infraestructura de spam que son vehículos populares para los ataques. documentación DAAR explica esto, pero pierde la oportunidad de explicar que las corrientes masivas de spam basado en importancia ataques proporcionan camuflaje para ataques más específicos y significativos. Seguridad y la estabilidad de la ICANN Comité Asesor (SNCC) es correcta para identificar el spam como una parte importante del ecosistema de registro esto es digno de estudio. El cuerpo de este informe contendrá extensa discusión del problema del spam.

En conclusión: el sistema DAAR es una aplicación directa de una buena idea. Asimismo, ayudará a la formulación de políticas fabricantes e investigadores que desean estudiar y abuso de Internet dominio de un diario, periódico, o perspectiva historica.

El resto de este informe se verá en sub-temas con más detalle y concluirá con una relativamente pocos sugerencias técnicas menores y el razonamiento detrás de ellos.

Alcance y propósito de esta revisión

Me han encargado con la validación de los principios de funcionamiento DAAR, diseño de sistemas, documentación, y salidas, para evaluar si cumplen con las normas / comunidad de la industria para la fiabilidad. Mi proceso de revisión tiene sido examinar el sistema a través de la interfaz de su operador, documentación, preguntas frecuentes existente, y documentos técnicos industriales y de investigación sobre el ecosistema de correo no deseado. Desde la interfaz del operador no es destinado a ser hecho accesible al público, que no examinó su aplicación para la seguridad del software cuestiones; mi análisis era estrictamente en los datos, fuentes de datos, métodos de compilación, y la descripción de la sistema y su funcionamiento.

Soy un practicante de la seguridad informática con más de 25 años de experiencia en consultoría de diseño del sistema y implementación; Soy titular de un premio a la trayectoria de la AISS y soy un compañero de ISSA. El proceso que utilizada para esta revisión es típico para este tipo de proyectos; He realizado aplicación similar y Revisiones de diseño para una serie de productos de seguridad significativos, utilizando esta metodología.

Método

El método de la DAAR es sonido: las fuentes, método de recogida, combinación y métodos de recuento son bien pensado. La combinación de múltiples fuentes de datos en general, provoca una cuestión de normalización - cómo calibrar los incrementos en las múltiples fuentes - pero DAAR evita ese problema no se intentar resolverlo. Las listas de bloqueo que DAAR se emparejan contra pueden tener potencialmente sutil diferencias en su puntuación, sino porque DAAR está informando de datos a gran escala, las diferencias sutiles

son, literalmente, va a perderse en el ruido. Si alguien fuera a decidir resolver una sola entrada en DAAR
que sólo sería capaz de aprender los diversos proveedores de RBL que han anotado. Ninguna queja sobre la
RBL puntuación no son problema de la ICANN; que son los proveedores de RBL, o los registradores. A partir de una
punto de vista metodológico, DAAR se basa en metodologías de la RBL - Eso es bueno desde el punto de vista
tanto de la gestión de base de conocimientos y determinación del alcance del dominio del problema: si hay alguna queja,
que será sobre las RBL, no DAAR. Los mantenedores RBL tienen fuertes incentivos para asegurar su
las clasificaciones son tan precisos como pueden ser y tener un sistema creíble en su lugar para la corrección / reparación;
habrá ocasionales clasificaciones erróneas, sino que será corregido y las correcciones se
transparente para el sistema DAAR. Del mismo modo, la información y los datos de la zona de TLD recogieron de la
registradores será tan precisa como lo puede ser; es meta-datos sobre cómo funciona el DNS y si hay
ningún problema con ella los distribuidores autorizados específicos fijarán de forma transparente para el sistema DAAR.

Estamos satisfechos de que existen incentivos para asegurar la precisión de los datos que sirven de base DAAR.
Debido a que los datos se han extraído de los sistemas dinámicos, habrá cambios y correcciones en el tiempo, pero
Actualmente los datos son lo suficientemente precisos para realizar la función de DNS y productos comerciales anti-spam
eficazmente; que seguirá siendo, al menos, que precisa en el futuro. El diseño DAAR permitiría
RBLs adicionales que se añadirán si se dispusiera de otros nuevos o se ha caído uno debe ser determinada
como inexacta o de mantenimiento.

La colección de preguntas frecuentes proyecto DAAR hace un buen trabajo de explicar la relación entre los datos de DAAR
fuentes y su método de construcción de los datos. A partir de la descripción del sistema DAAR, una
constructor de sistemas con experiencia podría construir de forma independiente su propia versión idéntica funcionamiento, siempre que
quería. Es de importancia crítica para enmarcar alguna pregunta sobre DAAR correctamente, ya que es inevitable
que algunas organizaciones examinarán críticamente: están diciendo cosas desagradables sobre nosotros? ¿La gente
sacar conclusiones de estos datos que no nos gusta? La forma se describe DAAR es bueno; es muy neutral,
informativo, y no amenazante.

Amenazas de correlación de datos

Siempre que los datos se presentan basa en la combinación con otros datos, hay una amenaza potencial que alguien va a “restar” los datos adicionales y ser capaz de extraer el conjunto de datos original. DAAR evita este problema de diseño: ninguno de los datos que se utiliza es secreta, y la forma en que se compila puede ser realizado por cualquier persona. Por lo tanto, no hay datos secretos dentro DAAR que corre el riesgo de ser expuestos.

Siempre hay un potencial cuando se expone datos, para que los datos que se combina con algunos otros datos en de una manera que es problemático. La experiencia reciente con Strava haciendo su calor mapas disponibles, lo que resulta en las instalaciones de anuncios gubernamentales de Estados Unidos han dado a conocer, es un ejemplo de ese tipo de público incipiente desastre de relaciones. En el caso de los datos DAAR, no parece haber ningún problema de este tipo - en su mayoría porque los datos son de colección públicamente (con más esfuerzo) ya.

Calidad de Correlacionales feeds

El RBL alimenta DAAR que se correlaciona en contra son los mejores que están disponibles. Hay una epistemológico desafío que puede ser levantado en contra de la RBL alimenta, pero no los resultados de combinar los alimentos con Registro o registrador de datos - si hay cargos de inexactitud, que son desviados hacia los mantenedores y los productores de las listas negras. El documento de preguntas frecuentes y DAAR libro blanco DAAR proporcionan un buen explicación de la relación entre la RBL alimenta. datos Whois y zona DNS; no hay una significativa amenaza que no sea “puede haber algunas quejas” de las organizaciones que no han logrado quejándose a los mantenedores de RBL.

Los mantenedores RBL constantemente reciben quejas que son inexactos. A veces, son - para ejemplo mi servidor de correo electrónico personal estaba en la RBL por un tiempo porque he heredado una dirección IP que tenía ha utilizado para el envío de spam. Tenía que usar un sistema de recurso para obtener mi dirección elimina de la lista. Algunos podrían considerar que una queja de que la lista estaba mal, pero considero que es “cómo listas de reputación trabajo.”El consumidor de los datos de una RBL lo hace por el deseo de proteger sus sistemas mediante el bloqueo de correo no deseado

- incluso en un caso como el de mi dominio, la RBL está funcionando correctamente, proporcionando filtrado de correo basura del cliente

sistema de información de asesoramiento sobre la historia y la reputación de cualquier servidor que en contacto con ellos. Dentro los productos comerciales de bloqueo de spam que utilizan RBL, las RBL son sólo una parte de una puntuación global proceso que se utiliza para decidir si un mensaje dado consigue a través. Las personas que se quejan listas de reputación son por lo general las personas que constantemente se están puntuados como abusadores - porque, son abusadores. Es normal, en otras palabras, para que haya un poco de quejarse de RBL. Si no son los spammers quejarse de ellos, que no están funcionando correctamente. Nada de esto es un problema de la ICANN - se trata de un diálogo entre los spammers y los mantenedores de RBL.

Los desarrolladores de DAAR eran aconsejable evitar tomar sobre el problema de habilitación o la ponderación de las RBL, lo que equivaldría a hacer un juicio que uno RBL era más o menos precisa o ha tenido una mejor proceso de reparación. Evitar el “problema de la reparación” de la manera que lo hace DAAR - dejándolo en un problema para los mantenedores RBL - es también una buena estrategia. Dado que los RBLs son ampliamente utilizados operacionalmente y en productos, que son lo suficientemente precisos. Por lo tanto, los datos demográficos correlacionados con los datos RBL es también lo suficientemente precisa. Dado que los datos está cambiando día durante días, “exacta” significa “correctamente recogido y compilado “.

Hace DAAR “nombrar y avergonzar”?

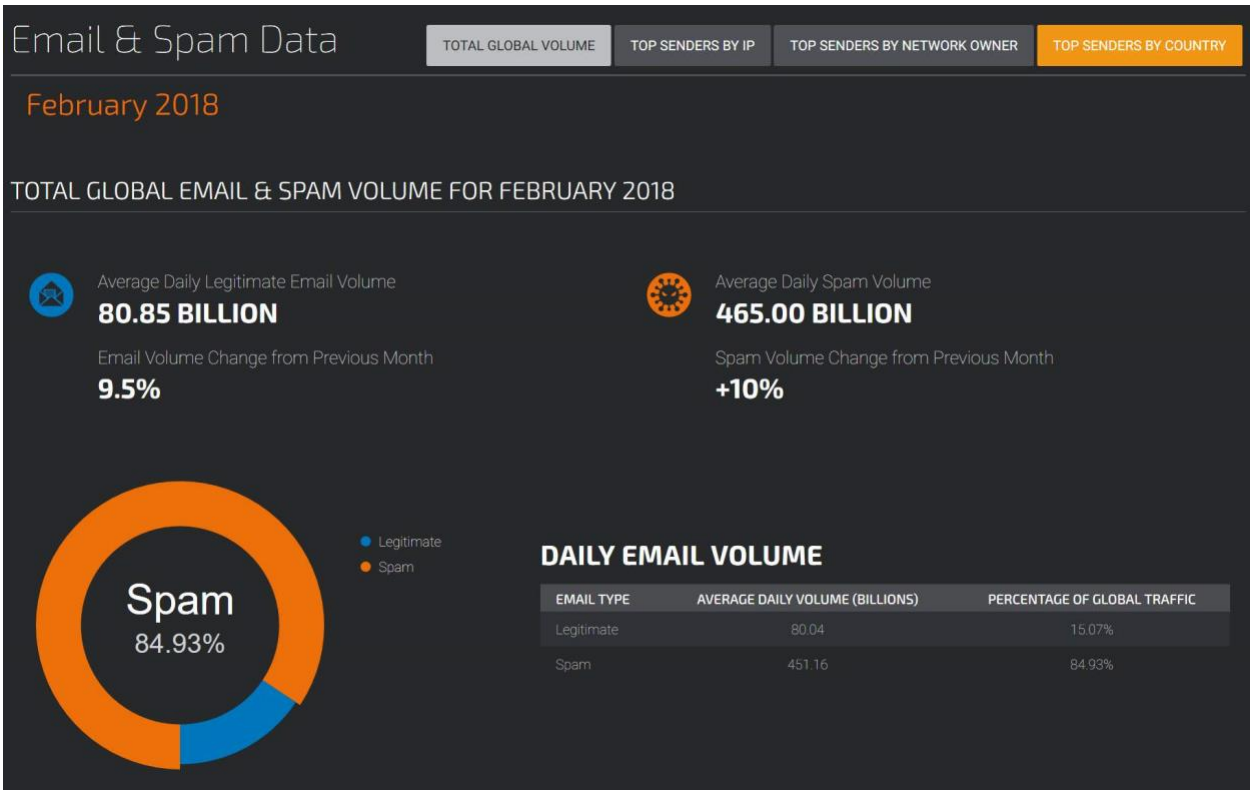
dominios de spam se nombran de manera explícita en los conjuntos de datos RBL; así es como funcionan las RBL. el DNS funciones para asignar nombres a direcciones y viceversa. Por lo tanto, siempre será posible asignar un RBL entrada a un registrador o una dirección - DAAR no es “nombrar y avergonzar” a nadie cuando el sistema hace los nombres de los registradores o dominios disponibles, es decir la información que ya está en la RBL, DAAR es sólo reunir en un solo lugar y presentarlo como un conjunto de datos unificada.

El spam es una amenaza de seguridad

El libro blanco DAAR FAQ y ambos hacen la afirmación de que el spam es una amenaza a la seguridad. Esto es evidente en las reacciones de la comunidad de seguridad informática académica, el mercado de productos de seguridad, y en el poner fin a las prácticas de los clientes. Por ejemplo, lo primero que daba clases un día de duración en el bloqueo de spam para el USENIX

conferencia en Atlanta en 2004. Antes de eso, y desde entonces, ha habido un interés académico en el spam técnicas de bloqueo, incluyendo algunos muy gran investigación académica fundamental en los métodos estadísticos para la clasificación de correo no deseado. El artículo de Paul Graham 2002 " *Un plan para el spam* "Es un ejemplo - Graham rompió abrir todo el campo de la utilización de técnicas de aprendizaje automático para la clasificación de correo no deseado y el bloqueo. Mientras tanto, en el frente comercial, el proveedor de tecnología de correo no deseado bloqueador Barracuda Networks fue adquirido por $ 1.6 mil millones en 2017 y Google adquirió el servicio de correo de bloqueo de spam Postini para $ 625 millones en 2007. Los investigadores y las empresas están poniendo ese nivel de valor de bloqueo de spam: es una *problema.*

Alguien que dice que "el spam no es una amenaza a la seguridad" sería hacer un recelo auto-servicio argumento dado que una gran cantidad de actividad de las amenazas se basa en exactamente ese principio. Por ejemplo, "Centro de detección de amenazas" Talos de Cisco trata específicamente de spam como una *amenaza* no una molestia, como lo hace servicio Gmail de Google.



(Cisco Talos)

En los 465 mil millones de mensajes de spam que Cisco está midiendo en este momento, hay un porcentaje de spam

mensajes que llevan adjuntos PDF con código de explotación / ataque en ellos. De hecho, el ruso piratería

ataques durante las elecciones estadounidenses de 2016 se basó en dos ataques por correo dirigidos y ataques de correo electrónico de spam - más de

100.000 piezas de correo no deseado llevar documentos adjuntos con malware, en una sola campaña de ataques.

securelist informes:

- 40% de los correos electrónicos no deseados eran menos de 2 KB de tamaño.
- La familia de malware más común encontrado en el tráfico de correo fue **Trojan-Downloader.JS.Sload**
- El sistema anti-phishing se desencadenó 246,231,645 veces.

descargadores de malware como Trojan-Downloader.JS.Sload son piezas de código javascript, incrustados en

correos electrónicos no deseados, que dirigen cliente de correo del lector para recuperar el código de ataque de un sitio de ensayo; el ataque

código, a continuación se hace cargo de la computadora de los lectores e instala una puerta trasera. Los 246 millones de veces securelist

detectado Trojan-Downloader.JS.Sload son sólo uno de los miles de vectores de ataque basados en spam.

En la comunidad de seguridad, hacemos un seguimiento de malware basado en correo no deseado con el fin de derrotarlo. Pero también mantenemos

estadísticas históricas sobre la cantidad de malware basado en correo no deseado nos ocupamos, con el fin de comprender y

comunicar acerca de la magnitud e importancia del problema. DAAR es otro histórico Data-

ver en los roles que tienen los nombres de dominio en los ataques de spam y el abuso de correo electrónico; que será valioso para el

comunidad de seguridad.

Hay argumentos extremos “libertad de expresión” que se han hecho en favor de correo no deseado (si uno está discutiendo

en contra bloqueo de spam, uno está discutiendo *para* correo no deseado) y actualmente esos argumentos están trabajando su camino

a través del sistema judicial en Georgia, Maryland, Washington y Virginia. La cuestión no es “es spam

molesto?”sino más bien‘no correo basura constituye una amenaza a la seguridad?’Para eso, la comunidad de seguridad da

un inequívoco “sí” por dos razones: 1) el spam se utiliza como vehículo de ataques en masa y 2) masivas

cantidades de correo no deseado proporcionan ocultar el ruido de los ataques dirigidos.

La primera generación de amenazas a la seguridad basados en spam dependía de los errores de software en clientes de correo electrónico. por ejemplo, Microsoft Outlook utiliza para traer y mostrar imágenes que estaban vinculados a una forma automática mensaje. Un atacante podría crear una imagen que explota un error de software en una versión específica de la Perspectiva y que a continuación, poner en marcha una campaña de spam entrega de ese mensaje a millones de usuarios de correo electrónico. Un significante porcentaje de los usuarios de correo electrónico estaría funcionando versiones vulnerables de Outlook y tendría su sistema asumida. Las únicas defensas contra este tipo de ataque están en constante actualización de un navegador y el cliente de correo electrónico y el uso de un sistema de bloqueo de spam en el borde de la red o en frente del correo electrónico cliente.

El estado actual de la técnica de una campaña de spam es combinar anuncio (de bienes o inexistente productos) *y* un ataque en un solo mensaje. El receptor se presenta con un anuncio de un poco de chatarra, con un enlace a “comprar ahora!” y un enlace a “darse de baja de estos correos electrónicos.” Si hacen clic en “Comprar ahora” consiguen vectorialmente a un carrito de la compra en alguna parte; si hacen clic en “darse de baja” su navegador se dirige a un drive-by gotero malware.

La URL construida en este correo no deseado está destinado a derrotar filtrado de URL; “Flagelo-cadáver” parece ser una inauspicious nombre generada de forma aleatoria. En el ecosistema de software malicioso nombres al azar generado y URL son un intento común de derrotar a los sistemas de seguridad de red que intentan poner en lista negra o dominios URL que se albergan programas maliciosos. Un navegador vulnerables intentar recuperar esa URL vuelve una carga de JavaScript que intenta generar un mensaje emergente que engañosa para un “anti-malware de Windows . Limpio”drive-by goteros de malware son particularmente pernicioso: identifican el navegador del usuario, mapa la versión con una lista de vulnerabilidades y exploits, inicie la explotación, e instalar persistente puertas traseras en el sistema del usuario. Una nueva tendencia en la unidad por el malware es dirigir a un usuario a una URL con el código de

que realiza la minería bitcoin; que no es muy eficiente, pero el spammer puede hacer algo de dinero, y ellos no les importa porque no están pagando por la electricidad. En el punto en el que alguien está tratando de dirigir un usuario a una URL que se ejecuta el código de ataque, el spam es una amenaza a la seguridad.

Muchas empresas despliegan de spam bloqueadores específicamente para evitar que sus usuarios se encuentren con URLs peligrosas y malware drive-by. dominios de spam a menudo se utilizan para alojar dichos sitios, así como falsa copias de los sitios reales que se utilizan para nombres de usuario y contraseñas de los usuarios de cosecha - no es una técnica de ataque llamado “Typosquatting” en el que un hacker registra un nombre de dominio abuso basado en un error común, por ejemplo: “microsft.com” o spam fuera mensajes de “0racle.com” donde el 'O' es un cero. algunos pareja los bloqueadores de spam a los filtros de URL en firewalls o proxies web; estos sistemas también utilizan RBLs junto con otras técnicas de detección. Es el mismo que utiliza los datos DAAR, y se igualó y se evalúa la misma camino; la diferencia es que el bloqueador de spam realiza una acción basada en políticas en el partido de RBL, mientras DAAR mantiene un registro histórico que una dirección en particular estaba en una lista en particular en un momento determinado.

El hecho de que los spammers están generando automáticamente las direcciones URL de ataque y registrar muchos abusan dominios en respuesta a la técnica de bloqueo es una prueba de que ellos saben que están tratando de evitar el seguridad de terminales de usuario; saben que están atacando los sistemas.

Un punto sutil en relación con el spam como un problema de seguridad es que la gran cascada de correo no deseado inofensiva sirve como cubrir de ataques de correo electrónico dirigidos. Debido a que las organizaciones de filtrar el spam, los usuarios que reciben dirigidos e-electrónico (phishing) son ataques *Más* probable que se abra un mensaje que se hace a mano para que no parezca spam. Incluso aunque los ataques de correo electrónico dirigidos son más pequeños que una campaña en toda regla correo no deseado, que a menudo son 10.000-100.000 mensajes a la vez. Por ejemplo, un típico ataque de suplantación de identidad podría ser como un mensaje de una departamento de servicio al cliente del banco, dirigiendo a los usuarios iniciar sesión y actualizar su cuenta; el destino nombre de dominio puede ser un dominio de abuso como *mybigbank-support-desk.com* donde el dominio real es *mybigbank.com*. No todos los ataques de phishing utilizan dominios de abuso, pero los más exitosos hacen.

Los ataques de phishing son parte innegable del spam / ecosistema anti-spam y de los usuarios finales y corporativos

respuestas a ellos tienen que salir.

En esta discusión, me he centrado exclusivamente en el spam de correo electrónico. Hay otras formas de spam y

todos ellos son, también, las amenazas de seguridad. Foro de comentarios spam se puede utilizar para saltar a los espectadores a drive-by

descargas de malware. correo no deseado redes sociales también se puede utilizar para los espectadores directos a sitios de malware cuentagotas -

esto era parte del arsenal de técnicas utilizadas por los hackers rusos para influir en la elección 2016 -

usuarios estarían dirigidos a sitios falsos, sus cuentas asumidas, y luego utilizarse para el voto seleccionado hacia arriba

artículos. Texto de spam de mensajes / SMS también se utiliza para los usuarios directos para descargar aplicaciones que contienen puertas traseras,

o a sitios web que contienen los cuentagotas de malware. Todas las variedades de correo no deseado se han convertido en arma de

hackers y spammers y que responden frente a estos ataques ha habido un enorme gasto para el

software y seguridad de la industria: todos los clientes de correo electrónico, todos los navegadores, cada foro de discusión - todos deben estar

cuidadosamente codificado y actualizado para evitar que constantemente se utilizan como vectores de ataque por

los spammers. El costo de mantenimiento de mantener el software resistentes contra ataques basados en datos desemboca en el

cientos de millones de dólares, al año. Si se añade en el costo para el usuario final, de nueva imagen

sistemas comprometidos, y la actualización constante de su software, ataques de spam entregadas representan una

masiva “impuesto” global de software que se ejecuta en los mil millones de dólares anualmente.

El spam es un problema de seguridad. La medición del empleo de los dominios de abuso en los ataques de spam es la investigación de mérito.

El valor de los datos históricos

Hay muchos aspectos del crecimiento de Internet que no fueron medidos y registrados cuando se

empezado. En algunos casos, se ha hecho un gran esfuerzo para volver a obtener esa información (por ejemplo: las tasas de mensajes de correo electrónico

enviados, documentos públicos, publicado dominios registrados, la demografía página web). Visiones históricas son útiles

en muchos caminos, los cuales pueden ser utilizados para evaluar las tendencias a largo plazo, apoyar la investigación académica sobre Internet

el uso y el crecimiento, o para identificar el crecimiento de las áreas problemáticas. Estos puntos de vista históricos son de particular

interés con respecto a la piratería de Internet, el correo basura, denegación de servicio, y otras formas de alto impacto

abuso incluyendo el abuso de nombres de dominio. Los datos históricos es la única manera en que podemos responder a la pregunta "¿es esto

en particular un problema cada vez mejor o peor?"DAAR será de gran valor, ya que ofrece una visión de la actividad abuso

a través del tiempo.

Colección, Reconocimiento y Cartografía

El enfoque de DAAR para la recogida de sus datos y de la asociación de dominios de nivel superior con los registradores se basa en

¿Cómo funciona el DNS en sí; es tan bueno como se *poder* ser.

No hay ninguna otra fuente de meta-datos para los dominios de nivel superior que pueden ser verificaron de forma cruzada contra, y

el DNS no podría funcionar correctamente si la meta-datos no fue lo suficientemente correcta para su uso. Hay un

potencial que algunas entradas podrían ser el cambio entre intervalos de sondeo, pero eso es aceptable porque

el sistema DAAR está destinado a proporcionar una vista de resumen, no resultados de la consulta en tiempo real - si alguien quiere

En tiempo real de consulta sobre los resultados de un dominio particular, que utilizarían las operaciones normales de DNS' en lugar de

DAAR.

El libro blanco DAAR FAQ y claramente la posición DAAR como fuente para la investigación, histórica y

Resumen de datos de exploración; que no intenta suplantar herramientas operativas existentes, de modo que no hay

probabilidad de que alguien va a intentar usarlo de esa manera.

los RBLs

La lista de RBLs DAAR utiliza representa el estado combinado de la técnica en la puntuación reputación; no hay

que tenga que buscar otras adicionales (sin embargo, si una nueva, mejor, RBL emerge, no hay ninguna razón por la que

no pudo ser añadido). Muchos productos comerciales dependen con éxito en uno o más de los elegidos

RBL, por lo que no parece probable que nadie pondrá a prueba su precisión *mientras que se reflejan en DAAR.*

Alguien puede estar en desacuerdo con anotaciones de cualquier RBL particular para un dominio particular, sino que es un problema entre ellos y el mantenedor de RBL.

DAAR es aconsejable haber evitado tratar de aplicar cualquier ponderación adicional o asignación en la parte superior de las RBL; eso sería abrir el sistema a las acusaciones de favoritismo.

ICANN podría publicar un contacto de los nuevos RBLs que deseen ser identificado en DAAR. Ese contacto probablemente ocurrir a través de las copias de los canales de todos modos - pero que tengan un punto de contacto oficial elimina la posibilidad de queja. La iniciativa Datos de libre cubre suficientemente este punto; cualquier organización que quiere proporcionar información o acceso a la información tiene una vía para participar en esa discusión.

El acceso al tablero de instrumentos

El sistema DAAR se presenta como una colección de datos y la agregación, pero llegará a ser visto por su los usuarios en términos de su interfaz de usuario. Por lo general con conjuntos de datos como DAAR, se encuentra una mezcla de los usuarios que quieren explorar gráficamente, y los usuarios que desea descargar un subconjunto y analizar un artículo específico que se descubierto durante el proceso de exploración. Para construir ese ciclo explore-> Analyze> explorar, los usuarios querrán la interfaz de usuario bastante (y la interfaz de usuario de DAAR *es* bonita!) porque es más fácil, y que va a traer problemas de sistema de consulta de carga, si los usuarios van a sentarse allí machacando el botón en la misma consulta una y más, los datos de raspado, etc. Por lo tanto, recomendamos dos cosas:

Continuar con el plan para limitar el acceso a la interfaz administrativa DAAR.

Dado que los datos DAAR se actualiza a diario, producir un tablero estático de salidas gráficas a las preguntas básicas - almacenar en caché los resultados a continuación, generar automáticamente un índice para ellos, con imágenes en miniatura, etc., utilizando un naming- estática esquema en el caso de que alguien desea un enlace profundo a un gráfico dado para un momento dado. Dado que las actualizaciones son diarias, y las imágenes serían de tamaño moderado, no daría lugar a una gran acumulación de datos a través de tiempo: 365 entradas / veces el año número de cartas producidas. personas que dan acceso a los datos “cocinados” en el forma de una imagen simplificaría enormemente la cuestión de si alguien necesita credenciales para utilizar el

interfaz administrativa; dando un acceso ajeno a la interfaz administrativa trae en el software cuestiones de seguridad, como si no sería posible llevar a cabo un ataque en contra de la inyección interfaz, etc. La mejor forma de resolver ese problema es evitar por completo.

casos extremos

DAAR será utilizado para realizar comparaciones, por lo que de borde casos van a ser un problema; supongamos que hay un registrador que sólo registra un único dominio y las RBL marcar ese dominio no abusiva - el registrador parece ser “100% libre de abuso-” cuando, de hecho, es irrelevante. En estadística, de borde son casos suelen tratarse con el uso de puntos de corte: simplemente no tienen en cuenta los valores pequeños que causarán gran movimientos porcentuales. DAAR no debe informar sobre los registradores que tienen menos de 1.000 dominios; Si que corte resulta ser demasiado baja se puede ajustar más tarde. Puntos de corte deben ser documentados como: “(no reportadas: registradores de apoyo menos de 1.000 dominios)”Eso no sería evitar que alguien registro de dominios de conseguir por encima de la línea de corte; sólo les costó algo de dinero y no hay mucho punto en el intento de jugar con el sistema de esa manera. No vale la pena el esfuerzo. Supongamos que un registrador decidido iniciar una campaña de marketing a “venir a utilizar, estamos 100% libre de abuso!”; eso sería un auto corregir un problema si la campaña de marketing atrajo a un gran número de los spammers. En otras palabras, las estructuras de incentivos no parecen alentar a los intentos de jugar con el sistema de esta manera.

Alguien podría decidir para recorrer el sistema - tratar de manipular a un porcentaje por el mero hecho de ser capaz de decir, “manipulé el porcentaje!”, pero, ¿y qué? El FAQ DAAR hace que sea muy clara donde el valor de los datos es, y no es, y ningún sistema puede controlar en contra de lo que a cantidad insustancial reclamaciones.

Resumen de resultados

DAAR es un sistema preciso y útil que ofrecerá una visión histórica valiosa en un título significativo problema que afecta a Internet. Utiliza métodos válidos para compilar predecible datos de fuentes que son exactos dentro de su ciclo diario. Los datos recopilados por DAAR se mantiene por terceros y la ICANN no tiene ninguna responsabilidad por la corrección de cualquier queja sobre los datos subyacentes. No existen elementos de datos sensibles en su compilación que corren el riesgo de ser revelados. La documentación (papel blanco, FAQ) es minuciosa y proporciona una explicación detallada y precisa de la lógica y el método del sistema, y el sistema como obras implementado como se describe en la documentación. El spam es una investigación significativa tema y es una zona de fuerte actividad comercial debido a que el spam es una amenaza a la seguridad; no es una mera molestia.

Apéndice A: Recomendaciones Específicas

Estos son los detalles que no encajan en ninguna otra parte, o no merecen una discusión más profunda.

- **las imágenes almacenadas en caché** - tener en cuenta la producción de imágenes generadas automáticamente cacheables de alto nivel resultados de la consulta.
- **Ajuste de escala en el eje x** - Cuando se generan los gráficos, el eje X por defecto a escala automática. Es decir razonables, excepto que los resultados en las apariencias engañosas si alguien está comparando visualmente el imágenes, es decir: si se toma dos imágenes de las estadísticas de dos registradores diferentes, que podrían ser que uno se escala 1-50, y el otro se escala 1-5,000,000 pero el histograma se ve la mismo. Auto-escalamiento gráficos cantidades a la amplificación del ruido. No tiene nada de malo, porque a veces (si usted está buscando en un solo registro) desea que los datos sean auto-escala con el alcance, por lo que la tabla no es una pequeña línea en la parte inferior. Si estás imágenes de dos de corte registradores y compararlas visualmente, sin embargo, que realmente los necesitan estar en el mismo escala. Considerar la adición de una opción de escala fija - dejar que la entrada del usuario final del X eje superior valor.
- **Registrar y evaluar las consultas en uso** - crear un registro de las consultas que generalmente se hacen a través de la interfaz de usuario; que es un buen candidato para el conjunto de “la mayoría de las consultas comunes” y se puede utilizar para construir imágenes estáticas.
- **“Curación” vs “Compilación”** En el documento DAAR, el término “curación” se utiliza para describir la proceso de combinar las puntuaciones RBL con los datos de Registradores de la ICANN. En la AYUDA el término “compilar” es usado. Elegir el término correcto para el proceso es importante, ya que es la principal cosa que la gente son propensos a quejarse de DAAR respecto. Desde “curación” es un proceso estético en el que una el arte del trabajo se mantiene y se presentó para un efecto específico, parece ser mejor evitar, como terminología. “Compilar” (un proceso automatizado) implica una combinación predecible de dos cosas y es técnicamente más precisa, menos propensos a hacer preguntas, y más fácil de entender.

Apéndice B: Breve Bio de Marcus Ranum

Marcus Ranum ha estado activo en el establecimiento de una red UNIX y comunidad de seguridad desde 1989, cuando asumió la responsabilidad de operar una de Digital Equipment Corporation tres gateways de Internet y lo convirtió en el primer producto de cortafuegos de Internet con éxito, el sello-DIC-.

Desde entonces se ha celebrado cada puesto de trabajo en la computadora de seguridad de nueva creación: codificador, proyecto gerente, gerente de producto, estratega de marketing, soporte de ventas, atención al cliente, VP de ingeniería, director de tecnología, fundador, CEO y miembro del Consejo de Administración. En 1997 y 1998 fue en el equipo de Oferta Pública de V-One Corporation y estaba en el consejo de administración de una sociedad anónima abierta, Red Uno. Intercalados entre todo eso, Marcus ha escrito libros, documentos técnicos, blogs, enseñado, y consultado. Él es un popular conferenciante y ha dio el tono mayoría de las conferencias de seguridad informática en un momento u otro. Como consultor, Marcus ha trabajado para los gobiernos nacionales, Fortune 10 firmas, y la abuela de la calle cuya computadora tiene software malicioso.

Sus proyectos de consultoría se han extendido de ayudar a las políticas de seguridad de diseño a nivel nacional y enmarcando la legislación a los controladores de dispositivos y software de escritura de depuración. Él es igual de cómodo trabajando en todos los niveles en la organización de una sociedad anónima. Él ha hecho una cantidad considerable de trabajar en el ámbito de auditoría de seguridad, así como la realización de los servicios discretos de respuesta a incidentes, incluyendo en varios incidentes mayores que recibieron la atención a nivel nacional.

Más recientemente, Marcus ha estado hablando y consultoría para IANS, así como consultar en estrategia / tecnología de seguridad para una gran empresa de medios en Los Ángeles. Antes de eso, era un experto no testificar en un litigio de patentes tecnología de firewall y fue importante en su cliente de ganar un asentamiento de más de $ 100 millones. Antes de eso se desempeñó como director de seguridad para Tenable Network Security, Inc., donde era responsable de las operaciones de seguridad interna, diseño del ciclo de vida del producto, y el despliegue del cliente final doctrinas -, así como el diseño de la

programa de formación del usuario final que todavía se utiliza para enseñar cómo Nessus y el Centro de seguridad han de ser usado.

Marcus es un miembro de la AISS y posee un Premio a la Trayectoria de la AISS. Él escribe una bi-columna mensual para SearchSecurity.