DAAR Informe de Validación

Por

John Bambenek, Presidente

Bambenek Consulting LTD

Tabla de contenido

Resumen ejecutivo

Este informe es el producto final del análisis de Bambenek Consulting LTD en la propuesta proyecto de abuso de dominio Actividad de Información (DAAR) en ICANN. Específicamente, se deseaba analizar el sistema a la luz de las siguientes preguntas:

- Validar la recogida y tratamiento de datos de la zona, los datos de registro de dominios y datos de abuso, o documento de cualquier problema o defectos.
- Confirmar o concurso que las fuentes de datos abuso que ICANN ha seleccionado la industria se reúnen o criterios académicos para la fiabilidad, precisión, baja tasa de falsos positivos y falsos positivos remediación. En el caso de que el SME refuta las fuentes, indican que las fuentes y por qué.
- Validar el medio por el cual el sistema DAAR atribuye dominios de abuso a TLDs o documentar cualesquiera problemas o deficiencias.
- Confirman o concurso que las afirmaciones que hacen que el spam es una amenaza a la seguridad. Pedimos que el SME correcta o ampliar afirmaciones, si es necesario. Si es posible, complementar la ya existente lista de las citas de investigación académicas o comerciales.
- Validar la generación de estadísticas o documentar cualquier problema o defectos.
- Confirmar que la descripción del sistema DAAR es suficientemente completa para otras partes en reproducir resultados similares usando los mismos datos de acceso público o comercialmente accesibles.

En términos generales, el siguiente análisis es generalmente de apoyo de este enfoque. Mediante el cálculo de lo es, en efecto, una puntuación “per cápita” de abuso por parte de TLD y registro se hace posible hacer realidad El análisis relativo en donde el abuso ocurre con más frecuencia y para llevar a cabo el seguimiento en el análisis

sobre por qué ciertos TLD o registros están siendo favorecidos. No todos los abusos directamente se puede atribuir a decisiones tomadas por los registros o registradores. Sin embargo, hay algo para “alguien” para hacer frente. Que alguien podría ser un CERT nacional si ciertas regiones están teniendo más problemas que otros, que podría ser la comunidad de seguridad en general en la búsqueda de lo que se están explotando vulnerabilidades. Estos datos son inmensamente útil, y, irónicamente, sigue un enfoque similar este analista es usando actualmente en la investigación académica e independientemente de este proyecto.

En la revisión de una ventana de un día de los datos, se observó algunos falsos positivos fueron de buena fe presentes en los datos. Estos dominios serían considerados perjudiciales si se ponen en una lista de bloques en un entorno empresarial y aumentar artificialmente una puntuación de riesgo de un dominio de nivel superior o de registro. Ese Dicho esto, el uso de análisis de “per cápita” ayuda a mitigar esto como es lógico pensar que, en términos , los falsos positivos grandes serán relativamente distribuyen a través de dominios de nivel superior y los registros en tales casos. Más discusión sobre este tema es continuación en la sección “Reconocimiento a Dominios”.

Sin embargo, la presencia de algunos de estos dominios obviamente benignos (si esos dominios están consideró erróneamente que ser maliciosa registrada o porque hay algo que se consideran abusivo en ellos, como Google Drive) se anotaron negativa podría llevar a algunos a cuestionar la validez del enfoque. Un dominio de verdad maliciosamente registrada ata más fuertemente el abuso a una espacio de nombres que la presencia de un archivo malicioso en un sistema de almacenamiento de archivos gratuito lo hace. Desafortunadamente hacer determinaciones de una manera programática de si un indicador específico es realmente dañino, comprometida, o simplemente un proveedor de servicios será utilizado por un criminal es mucho más allá del alcance de DAAR. Estos incidentes deben ser monitoreados y estrategias para mitigar su inclusión deben ser desarrollado.

En lo que respecta a la cuestión de si el spam debe ser incluido como una amenaza a la seguridad, este analista violentamente de acuerdo en que debe ser. El mayor mecanismo de entrega de malware es spam, correo no deseado (o por lo menos de correo electrónico comercial no solicitado) está prohibida o fuertemente regulada en casi todas las jurisdicciones, y gran parte de la discusión dentro de ICANN pasando actualmente en lo que respecta a la privacidad del registrante los datos apuntan a la opinión casi universal de que el spam es una amenaza a la seguridad y el abuso. Lo especifico alimentaciones elegido para enumerar dominios utilizados en esta actividad en gran medida a mitigar los falsos positivos y perfeccionar en el que la infraestructura que es verdaderamente abusiva opuesta a la simple cuestionable. La forma en que estos proveedores generan sus alimentos se basan en las características de suministro y no el contenido de los mensajes.

Este análisis apoya en gran medida el enfoque de la recopilación de datos propuesto en el documento técnico previsto en la presente Declaración. La una omisión que se observó en el Libro Blanco fue como “errores” serían procesados cuando las distintas alimentaciones de datos abuso no pudieron ser recuperados. Debería será posible manejar esas situaciones de una manera similar en cuanto a cuando los datos CZDS no está disponible, es decir, mantener la recolección y análisis de hacer tanto como sea posible. En el caso de datos de alimentación, es generada con mayor frecuencia por lo que el impacto de los “errores” individuales es más mínimo. Lo único cambio recomendado es hacer que sea obvio en qué días tales condiciones de error se producen de manera que cuando los individuos analizar estos datos después del hecho, es evidente a partir de la interfaz de usuario el cual los datos que deberían ser sospechoso de los datos devueltos. En conversaciones con el desarrollador de DAAR, tales gestión de errores sí existe, pero no se refleja en el Libro Blanco.

Por último, la descripción del sistema es sólido y deja claro que no sólo lo que se trató de mostrarse pero una persona con conocimiento probablemente podría reproducirse un estudio similar sin demasiado conjeturas. Las opciones de los datos son claros y se corresponden con las decisiones de uno probablemente haría en un costo entorno restringido. Sin duda hay otros alimentos que podrían ser utilizados para DNS basan

indicadores y que pueden ejecutar más de $ 100.000 por año. Algunos otros de código abierto se alimenta de los datos relacionados con el dominio se incluyen en “Fuentes de Abuso de datos” más adelante, pero que los datos tiene que ser templado con un poco de poda para asegurar la mayor reducción en la información de falsos positivos como posible. Hay poca superposición entre las distintas alimentaciones de inteligencia de fuente abierta y de bajo costo por ahí, por lo que más datos conducirían a una mejor visibilidad.

En conclusión, la perspectiva de tener un sistema de este tipo para analizar los datos de abuso a un nivel per cápita de TLD y registradores es emocionante. Aunque no todos los abusos revierta directa a la negligencia o malversación de un registrador o registro, teniendo dichos datos comparativos disponibles ayudará a plomo mejor comprensión del ecosistema criminal cibernético y ayudar a la ICANN, registros y registradores, CERT nacionales y la comunidad de seguridad más amplio para mejor las acciones a medida para ayudar a asegurar la Internet en general. Estoy deseando ver a este sistema lanzado a la comunidad en general y estoy dispuesto a ser de ayuda en todo lo que pueda para ayudar.

Los cambios recomendados

Los cambios recomendados se incluyen a continuación en forma de bala, ya que son relativamente trivial promulgar. El proceso general es el sonido sino para aumentar la aceptación y facilidad de uso, algunos ajustes debería ser considerado.

- Crear un documento actualizado (Libro Blanco o un documento separado) que precisa refleja lo que se incluye en DAAR. El Libro Blanco, como en la actualidad por escrito, no está actualizado y el desarrollador ha hecho cambios significativos.
- La eliminación del Mozilla Firefox AdBlock RSS. (Nota: esto fue mencionado en el White El papel como fuente, pero las conversaciones con el desarrollador de DAAR han demostrado que esto era Nunca incluidos.)

- Asegurarse de forma rutinaria que “contenido”, basada alimentos no entran en esta lista (es decir, adultos páginas web, dominios publicidad / seguimiento de anuncios, etc.).
- Indicación en la interfaz de usuario cuando los datos CZDS no estaba completamente accesible (en Además de “no trazado” de datos).
- Indicación en la interfaz de usuario cuando algunas de las alimentaciones de inteligencia de origen no eran accesible por un período “largo” de tiempo (por ejemplo 24 horas).
- Algunos ajustes para aquellas situaciones en las que los registradores tienen un pequeño número de dominios bajo gestión (es decir, menos de 500) donde unos pocos dominios maliciosos pueden tener una enorme impacto a su puntuación de riesgo.
- Consistentemente volver a determinar si existen fuentes de datos de código abierto que pueden ser valiosos para este esfuerzo para aumentar la visibilidad en cierto abuso que puede atribuirse inequívocamente a los dominios.
- Podar las URL de los feeds Adware o eliminarlos por completo de la consideración.
- Continuará monitoreando la presencia de datos de “falsos positivos”, lo que da lugar a su inclusión, y lo que, en todo caso, se debe hacer para evitar que sea considerado en la puntuación.
- Asegúrese de que el matiz apropiado se comunica a los usuarios finales de este sistema o productos que puede producir. No todos los dominios en una lista de abusos se deben a cuestiones que pueden ser atribuida a la acción o falta de acción por parte de un registrador / de registro (malvertizing, dominios comprometidas, etc. discuten más abajo).
- Examinar la viabilidad de la adición de “ponderación” para los dominios que existen en períodos más largos de tiempo.
- Monitor para la tasa de dominios que no puede ser atribuido apropiadamente a un registrador debido a problemas de acceso (whois o problemas con cualquier sistema sucesor pueden ser puestos en marcha).
- La revisión continua de la adición de nueva amenaza se alimenta como relevantes para su esfuerzo.

Antecedentes de Analista

John Bambenek llevó a cabo el análisis en este proyecto. Además de ser Presidente de Bambenek Consulting, LTD, se desempeña como vicepresidente de Investigación de Seguridad e Inteligencia en ThreatSTOP y es un profesor de la Universidad de Illinois en la enseñanza 5 cursos de seguridad cibernética. Él tiene 18 años de experiencia en seguridad cibernética y ha hablado en conferencias en todo el mundo.

Lo que es más relevante para este análisis, es que se ha producido y desarrollado dos de los más grandes inteligencia de amenazas de código abierto alimentos usados por miles de organizaciones en todo el mundo. los primera alimentación se basa en algoritmos de generación de dominio (DGA) que rastrea más de un millón actualmente dominios DGA activos y se puede encontrar en http://osint.bambenekconsulting.com/feeds . los la segunda es la base de datos de configuración de malware Barncat que tiene casi 400.000 programas maliciosos configuraciones de malos-muestras conocidas visto en la naturaleza.

Al mismo tiempo e independiente de este esfuerzo, que lidera un equipo de 10 estudiantes graduados utilizando información de fuente abierta para crear un análisis representativo a nivel mundial en TLDs, registradores, y Los proveedores de alojamiento que utiliza una metodología relativamente similares (aunque centrándose en diferentes los resultados y las entidades).

El núcleo de su trabajo profesional gira en torno a la creación, conservación, y puesta en marcha de los datos de análisis de riesgos para proteger a las empresas de todo el mundo.

Enfoque

Este análisis ha tomado varias medidas para analizar DAAR para proporcionar información que se espera conducir a un sistema robusto. Como parte de este esfuerzo, una ventana de un día de un subconjunto de los datos (es decir, del Malware Patrol) se examinó para “falsos positivos” y otros puntos de datos que podrían conducir a resultados que podrían ser cuestionada. En esos casos, una cierta discusión es necesaria sobre el diferencias entre lo que la industria consideraría falsos positivos y lo que sería un falso positivo en este caso. Para una discusión sobre los “falsos positivos”, por favor ver que la sección de cómo este analista definiría ese término en este caso. En general, el enfoque de lo que la industria utilizaría en el estudio de los datos es el análisis aquí, pero en los puntos clave que hay más análisis en profundidad de por qué puede y debe haber diferencias en la forma en que la ICANN y la industria debe buscar en los mismos datos y alimenta.

Algunos datos errante fue identificado en este análisis, otros elementos son cuestionables. Para esos casos, por lo menos para los ejemplos utilizados para este informe, consultando a otros servicios de terceros se hizo para tomar una determinación. En general, los datos son de sonido, pero hay tonos de gris y en algunos Se realizó casos de prueba, resolviendo el gris a blanco o negro.

Para cada uno de los alimentos que se hace referencia en el Libro Blanco, se llevó a cabo la investigación para determinar cómo el se recogieron los datos y el contexto en el que aparece en la alimentación. En algunos casos, el White El papel no era lo suficientemente específica para tomar una determinación directa. En otros casos, algunos de los datos de no se utilizó en última instancia, el Libro Blanco. Sin embargo, al examinar los datos directamente, más fuerte conclusiones han sido capaces de realizar. En general, esos alimentos que se centran en el contenido basado en decisiones (es decir, los dominios de seguimiento ad) mencionados en el Libro Blanco fueron llamados como no aptos

para este enfoque. En algunos casos, las alimentaciones Malware Patrol no pudieron determinarse exactamente cómo se recogieron los datos, incluso con acceso directo a los datos. En esos casos, “el mejor adivinar”se hicieron determinaciones.

En un análisis en profundidad de los diversos motivos un dominio o nombre de host encontrar su camino en listas de bloqueo era realizaron como que es relevante en la medida tal presencia se puede atribuir al abuso de dominio y puede llevar a algunos a tener preguntas acerca de los datos y el análisis.

Recopilación y procesamiento de datos de zona

Como cuestión inicial, el uso de whois para reunir el patrocinio de la información de registro puede ser problemática basada en el trabajo en curso con el RDS proceso PDP-Generaciones Siguiente. Como parte de el cumplimiento continuo de GDPR y otros temas, el acceso a los datos whois está cambiando. Tarifa-limitación de los datos ungated, por ejemplo, podría limitar la capacidad de utilizar este tipo de sistema. En algunos casos, las entidades han dado a entender que whois se apagan por completo. Dicho esto, es probable que el sistema de cambiando “pronto” que puede requerir un ajuste en la cantidad de datos de registro está siendo recopilada.

La colección inicial de los datos de CZDS u otro proceso de registro es patrocinado sonido, ya que es el método utiliza todos primaria y tiene acceso a. Idealmente, la inclusión de las zonas de ccTLD sería una buena adición a esto, pero eso depende de los distintos ccTLD acuerdan enviar los datos.

En general, el método es bastante sencillo. Recopilar datos CZDS, recopilar datos de abuso, enriquecer con datos whois para información de registro y realizar operaciones matemáticas. Esto hace que el sistema DAAR fácil entender y reproducir para verificar los hallazgos según sea necesario.

El sistema de información era bastante fácil de usar y muy fácil de derivar rápidamente los datos de esta análisis. Los detalles de la validez de las estadísticas se cubre en la sección de abajo.

Procesamiento de error y el fracaso

Una de las omisiones en el Libro Blanco en condiciones de error discuten fue como el falta de disponibilidad (es decir, limitante de la velocidad) de Whois podría ser manejado. La cuestión fue llamado a salir, pero a diferencia de la falta de datos de zona TLD o datos de alimentación, la ausencia de estos datos puede causar algunos problemas

particularmente en el cálculo de las puntuaciones de abuso de registradores. Es posible tal falta de disponibilidad podría causar una sesgar en los datos de tal manera que algunos registradores tienen puntuaciones artificialmente bajos mientras que otros registradores son “Totalmente calculado” debido a que los servidores Whois sus dominios pueden estar a favor y son disponibles.

Esto es algo mitigado por el hecho de que los registradores para un dominio dado no cambian “a menudo” lo que sólo una recuperación necesita para tener éxito.

En general, el manejo de la falta de datos CZDS error parece estar en buen estado. Es ambigua en el Libro Blanco de que si un solo archivo de zona TLD es inaccesible que los cálculos para ese día no lo haría que hacer para todas las zonas o simplemente la que nos ocupa. Hay pros y los contras de ambos. Si el DAAR sistema sólo estaba calculando las tasas de abuso de dominio de nivel superior, no calcular para cualquier zona sobre la base de un único error sería extrema. Registradores, sin embargo, pueden operar a través de varios dominios de primer nivel tan pequeñas interrupciones puede tener un impacto descomunal. Errar en el lado de no calcular los datos es probablemente la más “segura” enfoque en este caso. El Libro Blanco no llamar específicamente, pero algunos reintentos se debe hacer para recuperar datos de la zona si el error subyacente es meramente de naturaleza transitoria.

Las conversaciones con el desarrollador de DAAR indican que hay múltiples intentos para obtener datos CZDS y la validación de los datos recibidos, que minimiza en gran medida cualquier posibilidad de errores. En el caso pasa un día sin ser capaz de recuperar los datos, realizar los cálculos en base a la última los datos del día es una buena solución para este problema ya que el número de dominios en un dominio de nivel superior (o bajo gestión por un registrador) no cambiaría significativamente durante un día determinado por lo que la puntuación de abuso Todavía debe estar en buen estado.

Manejo del error para cuando se producen errores en el abuso alimenta es relativamente buena. A medida que se generan los alimentos de forma más rutinaria, varios intentos se pueden hacer durante un día determinado (y en algunos casos,

ya están hechos en el procesamiento), por lo que los errores transitorios son manejados por sí. La única área de preocupación es que la mayoría de los alimentos usados para DAAR se abstraen a través Malware Patrol. Qué esto significa es que las fuentes individuales de Malware Patrulla podrían tener “fallos silenciosos” sin embargo, la propio pienso Patrulla de malware aún está trabajando. A corto plazo, tal impacto es mínimo, pero en el largo plazo sesgo puede resultar. Se recomienda que hay algún seguimiento interno de Indicador de cuenta en los alimentos en consulta a tiempo, así que las cosas pueden ser marcados para su revisión humana (es decir, si el número de indicadores para un cambio de fuente individual en una cantidad significativa).

Fuentes de Abuso de Datos

De los cinco principales fuentes incluidas en DAAR (SURBL, Spamhaus, PhishTank, APWG, y Ransomware Rastreador), todos ellos son ampliamente utilizados y aceptados en trabajos académicos y profesionales. La única preocupación con PhishTank es que cualquier persona puede enviar URL y una validación de ese datos deben llevarse a cabo antes de la inclusión. En este caso, la metodología DAAR sólo toma dominios marcados “verificado” que mitiga este problema, por lo que su inclusión es aceptable con que filtrar.

Las alimentaciones restantes son proporcionados a través de Malware Patrol. En algunos casos, no hubo externa referencia, además de la página web de Malware Patrulla de qué es exactamente la alimentación, lo que era la metodología empleado para poblarlo, o cómo manejan remediación falso positivo. Algunos de los alimentos se menciona en el Libro Blanco son ya sea parcial o totalmente basado en el contenido que no debería estar atribuido al abuso. Al hablar con el desarrollador de DAAR, la única área de preocupación es el adware / potencialmente los datos de aplicación no deseadas.

Para este análisis, un valor de día de datos de alimentación de Malware Patrol fue examinado por lo que era posible “Trabajar hacia atrás” para identificar las entradas potencialmente problemáticas y algunas estrategias para mitigar ellos. En general, éstos fueron causados por adware y que serán tratados más adelante.

Una de las alimentaciones de la Patrulla malware que fue seleccionado de acuerdo con el Libro Blanco es el “Mozilla Firefox AdBlock”. Si bien hay casos de uso para las personas (y empresas) para bloquear publicidad y otros ámbitos relacionados ad-tracking, que no se asignan a una categoría de abuso seleccionada para este esfuerzo. De un modo similar, la alimentación es otro llamado “Calamar lista de bloques de proxy Web”, que

implica la inclusión de proxies web abiertas. Las empresas se quieren bloquear estos, ya que a menudo son correlacionados con los usuarios que buscan abusivas para anonimizar sí mismos, pero que podría no ser apropiada para este esfuerzo.

La alimentación DansGuardian (referenciado en el Libro Blanco) incluye una variedad de datos que pueden ser seleccionados por los usuarios y algunos de los datos es puramente basado en contenido. Por ejemplo, una de las DansGuardian “sub-feeds” es para sitios web para adultos. Muchas empresas y organizaciones bloquearían tal contenido, pero su inclusión aquí no se asigna directamente a una categoría de abuso en ausencia de otros detalles (Que no es desconocida para los sitios web para adultos que intentan también para infectar a sus visitantes, y en ese momento incluyendo el dominio tendría sentido. Discusión con el desarrollador ha puesto de manifiesto estos datos eran no incluido una vez que desarrollaron el sistema.

En concreto, el Libro Blanco llama a no usar el algoritmo prima para la generación de Dominio (DGA) del Malware Patrol. A menudo, cuando las personas crean listas de bloques DGA, que incluyen todos los dominios que podría ser generada por un DGA sin respecto a si un dominio está realmente registrado. Esto es un enfoque de protección válida, pero incluiría dominios no registrados en las estadísticas si DAAR incluidos aquí. Una fuente DGA puede ser útil para incluir (y se enumeran en el Apéndice 1 abajo). Este analista produce varios alimentos basados en DGA disponibles como osint.bambenekconsulting.com/feeds. Dos de las alimentaciones (DGA-feed.txt y DGA-feed-high.txt) son los listados de todos los dominios de la DGA válido, pero no hace ningún intento para ver si están registrados. Aquellos no debe ser considerado aquí. Hay otras dos alimentaciones (C2-dommasterlist.txt y C2-dommasterlist-high.txt) que enumeran todos los dominios DGA válidos que están resolviendo actualmente (y por tanto registrada) en las últimas 3 horas (alimentación generado por hora) y proporciona algunos rudimentario

listas blancas para los sumideros conocidos y para los dominios que están asociados a la infraestructura que nunca debe ser bloqueado (los servidores DNS raíz, 8.8.8.8, etc.). La alimentación “alta” elimina DGA que generan dominios cortos o listas de uso de la palabra para su generación como aquellos DGA a menudo “colisionar” con dominios de otra manera benignos y registrados de forma independiente. c2-dommasterlist-high.txt puede ser una buen candidato para su inclusión.

Como punto final, hay un cierto sesgo de los datos en los piensos utilizados para este esfuerzo que existe en una gran parte dado que algunos vectores de abuso no tienen alimenta consiguiente peligro. Discutido más adelante en detalle (y en un grado en el Libro Blanco), correo no deseado tiene una variedad de mecanismos de entrega para llegar víctimas. SURBL y SpamHaus se centran en el spam basado en el correo electrónico y que rastrean bien. No hay buenas alimentaciones de medios de comunicación social o indicadores relacionados con la mensajería instantánea de correo no deseado, incluso aunque siguen siendo populares vectores para llegar al consumidor.

A medida que más consumidores de todo el mundo se mueven de su uso de Internet para plataformas móviles, que se tener un gran impacto en los patrones de DNS y abuso. Hasta la fecha, no hay alimentación real para móviles basados en amenazas (malware, el spam de SMS, etc.). De acuerdo con un informe reciente, el porcentaje de internet **el tráfico procedente de dispositivos móviles es más del 50% de todo el tráfico de Internet** [1]. **Eso significa que hay un potencial de** un gran sesgo de los datos frente a los patrones de tráfico típicos de los usuarios de Internet. Allí no se recomienda solución para ese problema en el contexto de DAAR pero es un área de interés para esta investigación analista y potencialmente habrá alimenta de estos datos en el futuro que puede ser digno de inclusión.

[1] https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/

A medida que más alimentaciones estén disponibles para su inclusión en DAAR, cuando se añade se puede sesgar artificialmente los datos en comparación con las tasas históricas. Por ejemplo, el malware móvil puede favorecer a un conjunto diferente de TLD que el malware o spam convencional y que pueden dar lugar a cambios en las tendencias discordante. Esta no debe disuadir a nadie de la adición de los alimentos, como la visibilidad más completa en el panorama de amenazas dará lugar a mejores resultados de las políticas. Se recomienda, sin embargo, si hay adiciones de datos de alimentación (o sustracciones de feeds, si alguna vez relevante), hay alguna indicación obvia de cuando tales cambios ocurren de modo que las grandes oscilaciones de datos pueden ser fácilmente explicado.

Los datos de un día proporcionados no informa de las cuales pertenecen a los indicadores de qué fuentes, por lo El análisis detallado de alimentación por alimentación es difícil de combinar con el hecho de que muchos no tienen ningún pública Descripción detallada. A continuación se muestra un análisis del mejor esfuerzo de los alimentos Malware Patrol (como se indica en el Libro Blanco) en la que guardar, podar o eliminar.

SpamAssassin: lista de direcciones URL de malware	Mantener
Dominios de carbono malicioso Negro	Mantener
Postfix MTA	Mantener
blocklist proxy squid Web	retirar
Symantec Email Security para SMTP	Mantener
Seguridad Web de Symantec	Mantener
Firekeeper	Mantener
DansGuardian	Filtrar (asegurarse de que no hay elementos basados en el contenido)
ClamAV Virus Blocklist	Mantener
Mozilla Firefox AdBlock	retirar
smoothwall	Filtrar (asegurarse de que no hay elementos basados en el contenido)
MailWasher	Mantener

Tabla 1. Malware Patrulla alimenta con disposición recomendada (basada en lo que se enumeran en

Libro Blanco, en algunos casos, desarrollador DAAR ya ha eliminado)

Por último, hay otros alimentos de código abierto que pueden ser útiles para su inclusión para ayudar a aumentar la

la visibilidad en el paisaje abuso. Los que se incluyen al final de este informe en el Apéndice I.

Además de la de código abierto y libre de amenaza se alimenta en el apéndice, puede ser comercial

alimentos que son beneficiosos para tener en cuenta para este proyecto. Kasperksy y CrowdStrike, por ejemplo,

tiene amenaza de piensos basados en su propia investigación sobre el malware. ¿En qué medida se proporcionarían

un acceso razonable a un precio asequible para este caso de uso no es algo que este análisis tiene

investigado. Dicho esto, puede haber valor en examinar lo que otros alimentos están ahí fuera y

lo que, en su caso, pueden ser adquiridos a bajo costo / sin costo, siempre y cuando no se está compartiendo los datos específicos

echarse atrás con los demás. Hay otros grupos de intercambio de inteligencia que comparten datos de forma gratuita que

podría conducir a estar disponible algunos conjuntos de datos interesantes, pero tomaría post-procesamiento adicional

o normalización de los datos para hacer accesible. Ciertamente hay otras ofertas comerciales de alimentación

que los datos única oferta de alta calidad, pero su integración en este caso sería objeto de financiera

restricciones a las que este analista no pueden hablar.

Por ejemplo, los barcos PSIM varios conjuntos de datos de código abierto como parte de la construcción y por defecto es

relativamente fácil unirse a algunas comunidades de intercambio de PSIM (OTAN, CIRCL, etc.) lo cual produciría

nombres de host adicionales o nombres de dominio que podrían ser útiles para su inclusión. Sin embargo, en esos casos,

requeriría la creación de hardware adicional y que puede haber más allá del alcance de lo que es

se va a hacer en este caso.

Una nota importante, es que muchos alimentos serán intrínsecamente tienen sesgos geográficos no intencionales para una

amplia variedad de razones. Es difícil por razones innecesarias a entrar aquí para crear un nivel mundial

colección representativa de sensores para recibir y procesar datos. patrones de ataque seguirá

patrones geográficos y los sesgos en los alimentos puede conducir a puntos ciegos. oportunista buscando

para diversos alimentos geográficas debe ser intentado, pero esto es básicamente un problema no resuelto de

proveedores de inteligencia también. Se está mencionado aquí como un potencial brecha de datos de abuso, pero

Desafortunadamente no hay solución específica se puede ofrecer, excepto para supervisar la adición de nuevo

específicamente no occidental alimenta estén disponibles.

Las complicaciones de la inclusión a base de Adware

Desde el día de “saneadas” malware URL Patrulla previstas para este análisis, hubo aproximadamente 146.000 URLs diferentes en la alimentación. De ellos, unos 48.000 fueron marcados como publicidad no deseada. los dificultad con Adware es que hay muchos tonos de gris de los sabores simplemente nocivos de Adware a versiones maliciosas. Con la inclusión de esta categoría sin filtración adicional, algunos claramente los datos erróneos pueden ser incluidos. Se observó, por ejemplo, que estaba en el mapquest.com Patrulla de datos de malware. Aquí está la entrada específica:

MBL # 25613 20060326211802 http% 3A% 2F% 2Fcdn.mapquest.com% 2Fmqtoolbarv2 9cec62b72dc705de952e28a021bff1f074a422f0ebb71683d8c3f057c428c9671830dae9 AdWare.Win32.MegaSearch.m 1668 AOL-ATDn - AOL tránsito de datos Ne cdn.mapquest.com exe

VirusTotal detecta este archivo con 38 de 64 motores en su mayoría dentro de la categoría de Adware (o programas potencialmente no deseados / aplicaciones). Adware es generalmente molesto y muchos antivirus herramientas detectarán, ya que en última instancia se comporta de software que es difícil de distinguir de comportamiento malicioso (pop-ups, inyectando intersticiales, el seguimiento del comportamiento del usuario). algunos Adware programas probablemente probablemente podrían estar correctamente etiquetados como malware, pero no todos.

Windows.net también fue visto con algunas anotaciones fuera de blob.core.windows.net con varios Adware detecciones. La inclusión de dichos dominios de recuento como datos de abuso podría ser utilizado para intentar desacreditar DAAR. Cualquiera de post-filtrado de manera específica para eliminar dichas entradas de consideración o la eliminación de la categoría de Adware en su totalidad serían apropiadas para manejar esto situación. Es la recomendación de eliminar esta categoría en su totalidad para ser conservador y para ayudar a reforzar la credibilidad de DAAR.

Atribución de abuso a Dominios

La cuestión clave en el proyecto DAAR y este análisis es que lo presencia medida en una amenaza

de alimentación puede ser atribuida a un dominio, y por extensión a un TLD y registrador. Esto también es probable

ser el área más grande de retroceso de las diversas partes interesadas.

Desde la perspectiva de cómo las empresas utilizan listas de bloqueo, la siguiente discusión importa menos.

Empresas bloquean los proveedores, los dominios de primer nivel, sitios web comprometidos y / o proveedores de alojamiento compartido

si las amenazas se enfrentan a partir de esos lugares es mayor que el daño que sufrirán la de tener una

bloquear en su lugar. En su caso, es totalmente circunstancial, ya que el coste será asumido por la entidad

poner el bloque en su lugar.

En el presente caso, la ICANN es la creación de un sistema para analizar las estadísticas relativas para el abuso de dominios

entre los gTLD y los registradores y que el cambio en el contexto tiene algún impacto en su caso

análisis de los datos resultantes. Se describen varios aspectos de esta a continuación, pero la principal diferencia

es que las empresas tienen una amplia variedad de acciones que pueden tomar sobre la base de listas de bloques.

Por ejemplo, las diversas correo no deseado alimenta generalmente tienen alguna forma de una advertencia diciendo que la

idoneidad de sus alimentos se adapta en la aplicación de las listas de bloqueo para proteger los servidores de correo

y potencialmente proxies web (para atrapar a los usuarios hacer clic en correo no deseado). Aplicándolos a la frontera

firewall puede ser una aplicación excesivamente amplia. En el caso de DAAR, la única opción es la de cualquiera

aplicar una puntuación basada en un indicador o no. Hay un cierto matiz en términos de lo que esto significa para

el presente análisis, y que se discute a continuación, específicamente para los falsos positivos, comprometida

infraestructura, proveedores de servicios, malvertizing, consideraciones geográficas y estadística

consideraciones.

Algunas listas de bloqueo (no incluidas en el presente estudio) se utilizan con frecuencia por las empresas para

bloqueando el tráfico malicioso o sospechoso. Por ejemplo, las organizaciones bloquear direcciones IP que

el anfitrión de servicios UDP abiertos como DNS o LDAP que se pueden utilizar para la denegación de servicio distribuida

ataques. Las alimentaciones de spam a menudo bloquear direcciones IP observadas golpear sus sumideros como las

Las direcciones IP están en peligro y por lo tanto pueden ser utilizados para enviar correos electrónicos no deseados. En el presente estudio,

sólo se consideran los nombres de host y dominios de lo que los riesgos de los anteriores se reducen al mínimo, pero es

importante tener en cuenta que es una fuente de información utilizada a menudo por las listas de bloqueo y puede ser planteada por

aquellos que quieran más información sobre DAAR.

Además, algunos de los alimentos que se ingieren en DAAR vienen en forma de URL.

Las empresas pueden utilizar esos datos en formas adaptadas para minimizar los daños colaterales. Por ejemplo, las direcciones URL

podría ser colocado en un proxy web para que una URL específica se bloquea, pero no el dominio y todos

otros recursos en él. Esta opción no está disponible aquí, por lo que algunos matices en cuanto a lo que los datos

se dice es útil discutir en detalle a continuación.

Sin embargo, puede haber algunos registradores que atienden activamente a las audiencias penales y DAAR

puede ayudar a identificar dichos proveedores. Sin embargo, el análisis adicional *Debe ser hecho* Antes de realizar dicha

una afirmación que está fuera del alcance de lo que DAAR puede proporcionar directamente. El valor de DAAR

en la mente de este analista es ayudar de forma importante las preguntas que necesitan más investigaciones para llegar a

la respuesta y no hay otra herramienta disponible actualmente para ayudar a llenar este vacío muy específico de

abuso de dominio información de tendencias.

Falsos positivos

Desde una perspectiva de los datos, el término “falso positivo” parece ambigua. En la práctica para las empresas

y este esfuerzo, hay una gran cantidad de matices en lo que la gente entiende por falsos positivos y cómo

que son tratados por los que generan los alimentos y los que los consumen para la empresa

proteccion. Para los fines de este análisis, la definición de falso positivo de este analista es

sugerido que “los dominios indicados como dominios de abuso cuando no hay tal abuso está ocurriendo en realidad

en el dominio”, pero hay que señalar que esto no iba a utilizar la misma definición es la industria.

En general, cuando las empresas y las compañías de seguridad hablan de falsos positivos, lo que realmente

quieren decir es “falsas alarmas” (es decir, algún sistema que indica un problema de seguridad cuando no lo hay), el cual

es la combinación de dos eventos: “datos incorrectos” en una alimentación, y una observación en su propio

la red de ese indicador. Por ejemplo, si una dirección IP para un consumidor business-to-compartida

proveedor de alojamiento está incluido en una amenaza de alimentación (es decir, wordpress.com), la mayoría de las veces que no lo haría

ser considerado como un falso positivo debido a la probabilidad del uso legítimo de un hosting compartido, tales

sitio por un usuario de la empresa es pequeña y puede en realidad nunca ser visto.

El análisis de las direcciones URL, y compararlas con detecciones de malware parece un buen enfoque a

determinar la malicia de un URL dada, pero la abstracción de una URL en un nombre de host, y luego en una

Dominio y hacer una determinación de que el dominio debe ser anotado como el abuso podría ser visto como

problemático por algunos. En algunos casos, los datos se incluye que probablemente no ser puntuado como

abuso (ver la discusión de mapquest.com arriba). Los casos específicos de los proveedores de servicios, infraestructura comprometida, y malvertizing se discuten en detalle a continuación.

En el presente caso, los falsos positivos (o mejor aún, datos incorrectos) serán contados en las estadísticas y si es lo suficientemente frecuentes, podrían sesgar algunos dominios de nivel superior o registradores como aparecer a ser utilizado más como abuso lo que realmente son. Esto se discute a continuación bajo consideraciones estadísticas. Adicionalmente, basado en los sesgos geográficos de los registradores y algunos gTLD, es lógico pensar que las diferencias en la base de usuarios puede dar lugar a diferencias relativas entre las estadísticas. Por ejemplo, es lógico razón por la que algunas partes del mundo tienen más usuarios a la seguridad inteligente, más herramientas para ayudar a permitir la seguridad, los CERT nacionales que hacen a mejores puestos de trabajo notificación a la víctima, etc., que podrían dar lugar a sesgando de los datos basados en la distribución geográfica de los usuarios constituyentes. Algunos de esos consideraciones se discuten en consideraciones geográficas de abajo. Un beneficio importante de este sistema es que tales diferencias geográficas pueden encontrar (si existen) para entender mejor la ecosistema abuso.

En última instancia, una cosa que es difícil de discernir de este enfoque es en qué medida siendo un dominio en una alimentación de abuso debe atribuirse al dominio, y por extensión, el abuso a continuación, ser atribuido a la TLD y Registrador. Cabe señalar, que las empresas están haciendo esta atribución de todos modos porque no les importa las razones subyacentes de los abusos, lo que quieren es bloquearlo. Sin embargo, los productores de alimentos de URL maliciosas es probable empáticamente sugieren que el uso de muy datos estrechas (una URL específica) para sugerir el abuso en un espacio de nombres amplio dado (un TLD específico) no sería un uso adecuado de sus propios datos.

Dicho esto, la cuestión de si un dominio debe aparecer es una decisión subjetiva basada en datos que no está fácilmente disponible. Algunos dominios están registrados para su uso exclusivo penal, otros el uso de DNS es incidental al ataque. Ese es el mayor de la que “el debate” podría dar lugar a en esta implementación de DAAR. Dicho esto, DAAR está diseñado para determinar ciertas cosas y debería conducir a una investigación específica de seguimiento para determinar qué datos está mostrando lo que es.

Este debate se mitiga porque los indicadores individuales no parecen estar disponibles para los usuarios finales y que los patrones agregado es, sin embargo, datos útiles para estimular una mayor investigación. Si por ejemplo, 2 millones de nuevos .com dominios maliciosos se registraron, el registrador / TLD (o distribuidor) puede estar completamente libre de culpa para ese evento. No obstante, ese evento y el patrón es de datos útiles a conducir a alguien a preguntar: “¿por qué el ecosistema penal tomar esa decisión?” y responder a esa pregunta con la investigación de seguimiento es de inmenso valor para las buenas decisiones de política, tanto en el ICANN y el Internet en general y las comunidades gubernamentales.

Un caso específico de méritos positivos falsos separar la discusión y que es el registro de dominios como sumideros. Un sumidero es un dominio de otro modo malicioso que van a recibir datos desde víctimas sino que está bajo el control activo de un “partido benevolente” (gobierno, la seguridad vendedor / investigador, sin ánimo de lucro). Estos dominios suelen permanecer en un canal de abuso en casi todos los casos (excepto por la DGA se alimenta de Bambenek Consulting) porque a pesar de la dominio es ahora “segura”, equipos de las víctimas de balizamiento a ese dominio todavía indica compromiso ... sólo un compromiso que es potencialmente utilizable por el atacante. Hay que atienden a los registradores operadores sumidero que tendrán puntuaciones artificialmente altos de abuso usando este método. En particular, el Registrador de último recurso que existe casi para el uso exclusivo de sinkholing. En algunos casos,

sinkholed dominios fueron una vez “malo”; en otros casos, un dominio sinkholed nunca fue registrado por una entidad criminal. Debido a la naturaleza del trabajo de sinkholing, estimaciones específicas del tamaño de este son difíciles de obtener.

No hay una buena manera de descubrir a qué dominios son sumideros frente malicioso o cuando una de lo contrario dominio malicioso se “tomó” o “transferido” a un operador benévola. Para esto razón, estos dominios persisten en los alimentos durante largos períodos de tiempo. Para complicar aún más este es que algunos sumidero opera tomar medidas significativas para no parece ser un sumidero. La red resultado es que algunos registradores de otra forma participan en el “buen comportamiento” pueden parecer artificialmente para ser peores de lo que son simplemente porque están haciendo un “buen trabajo” en la mitigación de abusos al permitir operadores de sumidero a utilizar sus servicios. Este caso de uso debe evitarse específicamente de la degradación por el uso de estos datos. Mientras registros utilizan la ICANN ERSR, este problema debe ser mitigado con eficacia.

Desafortunadamente, no hay una buena manera de mitigar por completo estos datos desde la inclusión. Es posible utilizar el servicio sinkdb.abuse.ch para identificar las direcciones IP que pertenecen a los sumideros, el uso artefactos de servidor de nombres para identificarlos, o pedir a los registradores sí mismos (en algunos casos) a identificarlos. Sin embargo, no existe ninguna manera integral conocido para identificar un dominio como un sumidero como una técnica de este tipo podría también ser utilizado por un criminal para mitigar las operaciones sinkholing. Esto es siendo mencionado matiz tan apropiado puede ser añadido al hacer conclusiones únicamente por Datos estadísticos. En un mundo ideal, los dominios sinkholed no deben ser incluidos porque no son que se utiliza en el abuso. Las compañías todavía pueden bloquear el tráfico de sumidero para una variedad de razones, pero si el intención es medir el abuso en espacios de nombres dados, tratando de reducir la inclusión de los dominios que

no se están utilizando en el abuso (y no puede ser de nuevo, al menos en el corto plazo) es una pena

esfuerzo.

Infraestructura comprometida

Dominios registrados para su uso exclusivo penal que se incluyen en los informes estadísticos DAAR

es probable que no controversial. Hay una amplia variedad de formas en las empresas hacer frente a esa situación y

Un enfoque actual es la de simplemente bloquear todos los “nuevos dominios” (es decir dominios recién registrados) y

“dominios recién observadas” (es decir, cuando los dominios primero empiezan resolver en DNS) bajo el

La teoría relativamente sólida que la mayoría de la gente no operativizar inmediatamente un dominio y que el

ya un dominio permanece “vivo”, es más probable que sea seguro. Dominios inmediatamente siendo utilizado (ya sea

después de haber sido registrado o después del primer resolver en DNS) es probable porque los criminales quieren participar

de la delincuencia y no obtienen ninguna ventaja para sentarse en la infraestructura sin usar (aunque ciertamente existen

grupos que registran dominios y no los utilizan por algún tiempo más tarde para evitar el bloqueo

mencionado anteriormente).

Como resultado, los delincuentes utilizarán a menudo dominios comprometida (es decir, aquellos dominios que son primaria

utilizadas para los usos legítimos, pero que han sido comprometidos por un delincuente que luego usarlos en

algún método para atacar a otros) en la cadena de ataques. Estos sitios tienen otra manera “buena

reputación”, ya que son, de hecho, dominios legítimos. A menudo los usuarios se despliegan software que es

vulnerables a los ataques, por lo que los delincuentes sólo pueden subir archivos y utilizar un sitio web comprometido para

entrega de malware y de lo contrario dejan la funcionalidad del sitio web víctima ileso. Algunos

sitios web tienen los scripts vulnerables “anuncio publicitario” que pueden permitir a los abusadores a utilizar una infraestructura víctima

enviar correo no deseado. En algunos casos, los delincuentes podrían comprometer las credenciales de cualquier propia administración

DNS para un dominio y crear un registros de otro modo no utilizados por la víctima, pero se puede aprovechar por el atacante. Hay una amplia variedad de escenarios por los que los sitios legítimos de lo contrario pueden ser utilizados por los atacantes, pero que en última instancia se reducen a dos casos de alto nivel: las deficiencias de herramientas REGISTRAR-proporcionado (aquellos bajo el control administrativo del registrador) o debilidades en herramientas de consumo-instalado (aquellos instalado y administrado por el usuario final). Ambas situaciones serán discutido aquí.

Algunos registradores tienen bastante oferta “escueto” y se centran principalmente en la conducción de una dominio a un solicitante de registro. Otros le ofrecen alojamiento web, alojamiento de correo electrónico, y una amplia variedad de valor agregar servicios. Todo lo que es accesible por Internet, teóricamente, puede ser explotado. En general, se puede ser una elección más segura para el usuario “sofisticada” para utilizar servicios de registro proporcionada como que, en efecto, subcontrata la seguridad de una organización más grande y es de esperar más seguridad inteligente.

La realidad es que no puede haber vulnerabilidades en herramientas Registrador proporcionado (o una vulnerabilidad que permite el acceso a granel para hacer cambios de DNS para las zonas que tienen el registrador como la autorizada resolver). Una vulnerabilidad en esas herramientas podría conducir a cambios repentinos en la cantidad de abuso dominios atribuidos a un registrador dado (y potencialmente un TLD). En este caso, el abuso no lo haría necesariamente por “el fallo” del registrador, pero no es una causa-registrador específico que debe estar descubierto y remediado. El informe estadístico en este caso es valiosa para ayudar a determinar si este hurón no se detecta otro modo por el registrador sin esta herramienta.

En el segundo caso, una herramienta-desplegado usuario o debilidad conduce a compromiso generalizada de que es a continuación, utilizado por los delincuentes para propósitos abusivos. Por ejemplo, no es reciente presentación de informes sobre

"Drupalgeddon 2.0" en una vulnerabilidad que potencialmente podría afectar a más de un millón de sitios web [2], aunque presumiblemente un número menor de dominios. En este caso, podría haber sesgado a gran escala de los datos en función de los delincuentes que explotan en realidad estos sitios web de una manera que los sufran enumerados en el abuso alimenta. El sesgo podría variar en función de la base de usuarios del software o vulnerables las preferencias de orientación del atacante. Registradores y TLD serían justamente ser correcta para tomar problema con este tipo de listados de abuso que se les atribuye. Eso no significa, sin embargo, que informar sobre los datos abuso es inútil.

Si existen sesgos geográficos en la infraestructura comprometida, estas estadísticas pueden ayudar nacional CERT a tomar medidas específicas para sus representados. Podría ayudar a identificar de forma proactiva en masa compromiso eventos y algunos atributos de los mismos (se atacantes sólo se dirigen a los TLD específicos o registradores específicos). Consideraciones estadísticas y geográficas se discuten a continuación, pero los datos se sin embargo valiosa incluso para dominios comprometidos. Si los patrones se pueden discernir por cuánto atacantes objetivo de la infraestructura comprometida, ciertas acciones por parte de ICANN, la comunidad de registradores, o que otros podrían ser desarrollados para ayudar a mitigar eso. atribución directa de la frecuencia del abuso dominios como la falla de un registrador o registro en estos casos es "injusta", pero, no obstante, representa importantes datos de tendencia, siempre y cuando suficientes matices se utiliza para analizar los datos.

Proveedores de servicio

En este caso, "proveedores de servicios" se refiere a los proveedores no registrador / TLD que ofrecen algún servicio que podría ser útil para un criminal y que podría dar lugar a que el servicio termina en un abuso alimentar. Hay una amplia variedad de clases de proveedores de servicios en este sentido: los proveedores de alojamiento,

[2] https://www.securityweek.com/drupalgeddon-critical-flaw-exposes-million-drupal-websites-attacks

sistemas de almacenamiento de archivos en la nube, sistemas de intercambio de archivos, plataformas de mensajería, proveedores de DNS dinámico, mitigación de DDoS o redes de distribución de contenidos, etc. El caso específico de malvertizing es discutido por separado a continuación.

Por ejemplo, hay una variedad de programas maliciosos almacenados en Google Drive porque es la disponibilidad de seudónimo compartir archivos de manera indiscriminada con Internet. Los atacantes pueden enviar a cualquiera el malware a las víctimas directa o necesita ser acogido “en algún lugar” y alguna técnica empleada para conseguir que el usuario del ordenador de la víctima para descargarlo. En muchos casos, las combinaciones de ambos son involucrado. sitios web comprometidos son una herramienta útil para tener malware distribuido a las víctimas. Google Drive y Dropbox también son utilizados de vez en cuando.

Muchos abuso alimenta, en concreto los que utilizan las direcciones URL, a menudo aparecerá una lista de URL específicas a software malicioso almacenada en estos servicios. La presencia, sin embargo, de google.com (por drive.google.com) o dropbox.com en el abuso de las alimentaciones sería considerado por las empresas para ser un falso positivo en casi todos los casos. Al considerar el malware móvil, los mayores dominios para la distribución de la el malware son “tiendas de aplicaciones” ellos mismos. Su inclusión en las listas de bloqueo en una empresa sería imprudente. Se alimenta genera en base a aplicaciones donde se habla de que sería valioso, pero no existe tal alimentación.

Es lógico pensar que los proveedores de servicios pueden ser relativamente distribuidas de manera uniforme entre los dominios de nivel superior (en una base per cápita) o registradores con un fuerte a favor de .com. El factor atenuante en este caso es que a pesar de que el abuso se alimenta puede tener muchas entradas para Google Drive, sólo un dominio en última instancia, ser contados y, que por lo menos en términos de impacto per cápita en .com, el impacto puntuación es mínimo. El mayor riesgo es para los pequeños dominios de nivel superior o registradores, pero no es probable que esto va a ser un gran

un problema, pero esto no se puede decir definitivamente. Una vez que el sistema está en su lugar, puede ser digno de

el examen de este problema específico para ver en qué medida se distorsiona artificialmente puntuaciones de abuso

Malvertizing

De una manera similar a los proveedores de servicio, un subconjunto de los delincuentes se utilizan de alguna manera legítima

redes de publicidad para distribuir contenido malicioso para intentar conseguir más víctimas. Para complicar

que importa es que las redes de seguimiento de anuncios suelen utilizar técnicas similares ya que los operadores de malware con

respecto a DNS. Por ejemplo, hay dos, grandes “grupos de usuarios” de DGA, operadores de malware

y las redes de seguimiento de anuncios. Ambos utilizan DGA por razones similares. La inclusión de las redes de seguimiento de anuncios,

Sin embargo, no se asigna a una categoría de abuso, que deben considerarse en DAAR.

Dado que las redes de publicidad proporcionan la capacidad de terceros para comunicar el contenido a los demás,

criminales utilizarán esta comunicarse estafas, fraude o hazañas reales a los usuarios finales. El fin

resultado es que los artefactos de redes de publicidad de otro modo legítimos se abren camino en el abuso

se alimenta de vez en cuando. Por ejemplo, el elemento de datos MapQuest anterior parece haber hecho

en un canal de abuso debido a que está vinculado en un anuncio (que después se descarga la barra de herramientas

y vio que sea adware que lo consiguió en la lista). La eliminación de la categoría de Adware desde el malware

alimentación Patrulla probablemente ayudará a mitigar este problema.

Dicho esto, la publicidad maliciosa *objetivos (* en contraposición a las redes de distribución de legítimos

ellos mismos) deben contarse como abuso; ya sea porque es un dominio comprometida entregando

malware o Es un dominio registrado para su uso exclusivo penal.

Consideraciones geográficas

límites jurisdiccionales desempeñan un papel en los patrones de ataque, y por extensión, el uso de DNS atacantes. Por ejemplo, los ciberdelincuentes rusos a menudo no dirigir su propio país por temor a enjuiciamiento. Los criminales han comenzado a reducir el uso de ransomware contra las víctimas de la mundo desarrollado a favor de diversas formas de malware minera criptomoneda. Algunas herramientas son Sólo popular en ciertas áreas geográficas. Una amplia variedad de factores dará lugar a la geográfica sesgo de los datos que se refleja parcialmente en gTLD y las tasas de abuso de registrador. Esto es especialmente cierto cuando se consideran las tasas de abuso de ccTLD, pero ya que no está disponible a DAAR en este punto, no se está considerando aquí.

Además, algunos gTLD son geográfica en la naturaleza (es decir gTLD referencia a nombres específicos de la ciudad) y algunos registradores tienen geográfica específica dirigida a su base de clientes. Es lógico que la postura de seguridad relativa de usuarios específicos en zonas geográficas específicas varían ampliamente y esto finalmente se refleja en las puntuaciones de abuso de uno respecto al otro. Es lógico, muchos la gente va a mirar simplemente filas de abuso relativos y hacer que “snap” juicios, tener algún datos adicionales podrían llevar a mejores y más matizadas decisiones de política.

Desde un punto de vista puramente de investigación, que podría ser útil para determinar el país de los principales IP dirección para el registro de dominio y el mapa que en los datos con una importante advertencia. La presencia de una dirección IP en un determinado país es, a lo sumo, marginalmente conectado a las que el usuario vive en realidad. Uno puede comprar un servidor privado virtual en casi todos los países del mundo, independientemente de dónde se En realidad vivir. Sin embargo, la integración de la información geográfica, además de Registrador / TLD información podría proporcionar algunas ideas interesantes en cuanto a los patrones de ataque y abuso. Tambien es

es verdad, esto puede “saturar el análisis” de DAAR. Este analista estaría muy interesado en el

El análisis estadístico de los tres puntos de datos (TLD, Secretario, código de país de la dirección IP del dominio)

juntos, pero en última instancia, que podría no ser en el ámbito de DAAR. Su mencionado aquí simplemente como

algo a considerar como cuestiones geográficas pueden proporcionar una cierta penetración en cuanto a las diferencias relativas en

puntajes de abuso entre los dominios de nivel superior y / o registradores.

Consideraciones estadísticas

Generalmente, después de la discusión de las consideraciones anteriores, las estadísticas DAAR genera es valioso.

La inclusión de otros datos (específicamente en los países) podría conducir a conclusiones más ricos o al menos

líneas más específicas en la investigación. Como muchos usuarios simplemente mirar Top X resultado de abuso, algún tipo de atención

debe tenerse que hay algún matiz en la interpretación. La presencia de muy pequeña

registradores con grandes puntuaciones de abuso (mencionado anteriormente) es un ejemplo de vistas cómo superficiales de

los datos pueden conducir a decisiones infundadas.

Puede valer la pena tener en cuenta las puntuaciones diferenciales (Top X mejora TLD / o registradores Top

X disminuyendo TLD / registradores) para tener una idea de movimiento relativo con el tiempo. Consideración de

ponderación basado en dominios que están en una alimentación y no suspendida por el registrador podría ser ambos

útil y excesivamente complica a la simplicidad de los cálculos DAAR.

En general, la fuerza de DAAR es la simplicidad y la solidez de cómo son las cosas. los

preocupaciones expresadas anteriormente giran en torno a los matices de cómo deberían y podrían utilizarse esos datos.

Correo no deseado como una amenaza a la seguridad

Correo no deseado se ubica como una de las principales preocupaciones de los consumidores, empresas y gobiernos como una de las más formas evidentes de abuso que es inmediatamente visible para los consumidores. Toda una industria ha surgido para luchar contra el spam en cuenta la fuerza, el vigor y la unanimidad en su inconveniencia. Algunos de los más grandes de alimentos de inteligencia de amenazas son casi todos exclusiva a base de spam, ya que cuenta con la mayor conjuntos de datos. La mayoría de correo electrónico que transita por Internet es spam; Talos Lab de Cisco muestra que el 85% de mensajes de correo electrónico en Marzo 2018 eran spam. [3]

Debe tenerse en cuenta todos los países de la UE han adoptado una ley contra el correo no deseado en toda la UE como tener docenas de otros países que regulan el spam en diversos grados. Un reciente acusación del nacional rusa Peter Levashov en los Estados Unidos en relación a su funcionamiento de la botnet Kelihos específicamente habían cargos relacionados con spam de correo electrónico como criminal procesable (Count 6 y 7). [4]

Como una nota interesante, todos los servidores de correo electrónico tienen protecciones “fuera de la caja” contra correo no deseado, como lo hacen todos los servicios de correo electrónico privadas. Esto puede no parecer sorprendente, pero los navegadores web tienen sólo algunos una función de protección contra los sitios de phishing (y sólo recientemente ha sido ampliamente desplegado como parte del navegador) o el navegador ataques, sistemas operativos casi universalmente tienen ningún software malicioso proteccion. La amenaza del spam es tan grave y ampliamente aceptadas que no sólo son sus opciones en las propias aplicaciones para proteger en contra de ella, el valor predeterminado es proporcionar realidad esa protección.

[3] https://www.talosintelligence.com/reputation_center/email_rep
[4] https://www.justice.gov/opa/press-release/file/1030976/download

Hay dos formas principales en que el malware encuentra su camino en los ordenadores victima o en el interior organizaciones: correo electrónico y Web basados en paquetes de exploits. De ellos, el correo electrónico es mucho más frecuente. los ataques contra la elección presidencial de 2016 Estados Unidos y la elección presidencial francesa 2017 eran habilitado por mensajes de correo electrónico malintencionados.

El sistema DAAR está utilizando diversas alimentaciones amenaza para poblar su modelo para encontrar dominio relacionada abuso. Cabe señalar que todo el concepto de amenaza alimenta y lo que finalmente se convirtió en inteligencia de amenazas que se estaba haciendo por las organizaciones anti-spam durante una década antes de que comenzara a ser utilizado por las compañías de seguridad cibernética en general. SURBL, por ejemplo, se creó en 2004. El toda noción de listas de amenaza fue creado por la necesidad y el deseo de evitar el spam.

En última instancia el concepto de abuso es una construcción social, y el consenso en casi todo el mundo es que el spam es una amenaza abusos en que el costo de la víctima es mucho mayor que el coste al remitente. Cualquier actividad que hace que el receptor gastar más recursos que el remitente es inherentemente abusivo.

Técnicamente, el protocolo SMTP permite a las personas enviar mensajes de correo electrónico, simplemente mediante el uso de IP direcciones, por convención, esto es casi universalmente bloqueadas y requiere remitentes (malicioso y de otro modo) para tener los nombres de dominio para enviar mensajes, tienen registros MX en el DNS, y por otra parte tienen características de DNS habilitado para permitir la entrega y la transmisión de correo no deseado. Con el excepción de la infraestructura comprometida, la mayor parte de lo que queda se puede considerar dominio-abuso relacionado como el spammer necesita sus dominios y DNS para trabajar con el fin de operar y con frecuencia registrará dominios para uso malicioso exclusiva.

Al centrarse en los registros de dominio para este análisis, hay una gran cantidad de mitigación contra la falsa positivos. Por ejemplo, un sitio web comprometido con un script PHP podría ser utilizado por un criminal a enviar una gran cantidad de correo no deseado, pero los datos en la alimentación sólo se reconocerían el nombre de host del sitio comprometido. Ese sitio puede sentarse en un servidor compartido con un millón de otros sitios, pero la forma en que el los datos se recogen impediría aquellos dominios de ser implicado. Esto no necesariamente por cómo las organizaciones protegería a sí mismos en este caso, pero para este análisis, este tratamiento de los datos es el sonido.

Debe tenerse en cuenta que el correo no deseado alimentaciones elegido confiar en spamtraps. Se trata fundamentalmente de “falsa cuentas de correo electrónico”que nunca debe recibir todo el correo electrónico, ya que no están en uso por los usuarios legítimos. Esta evita los problemas de interpretación que a veces los usuarios pueden creer que un mensaje es spam porque que no les gusta el contenido o una variedad de otras razones. En este caso, no hay un “humano en el Mix”y el análisis y categorización se automatizado basado en el correo electrónico ir a lugares que sería Nunca ir orgánicamente en un caso legítimo.

El Libro Blanco hace discutir correo no deseado a través de mecanismos distintos de correo electrónico (medios de comunicación social, instantánea mensajería, etc.) y las que sería válida para incluir en este esfuerzo. Dicho esto, ninguna de las alimentaciones parte de DAAR sería probable que obtenga la información de una manera sustancial como las fuentes de los alimentos en general, no son los mensajes o las plataformas de medios sociales.

En resumen, correo no deseado debe ser considerado una amenaza abuso y su inclusión en DAAR es vigorosamente soportado. En la medida en que los alimentos o fuentes de datos pueden ser identificados por falta de spam de correo electrónico, los deben integrarse.

Validación de Estadísticas

A menudo, cuando las organizaciones intentan asignar abuso por parte de dominios de nivel superior y / o registradores, que operan en crudo números porque es más simple para generar (especialmente en el caso de los registradores en los que no es sencillo para obtener una lista completa de los dominios de registro). La conversión de esto en un porcentaje permite la posibilidad de hacer verdaderas comparaciones manzanas con las manzanas entre dominios de nivel superior y los registradores.

El método es simple, sencillo, y difícil de debatir su solidez. Es exactamente cómo este el analista puede y de hecho su propio análisis sobre temas similares cuando se mira en los datos de abuso de DNS.

Puede ser posible aumentar la ponderación o crear otra anotación para ilustrar cuánto tiempo abusiva dominios permanecen operativos. Puramente dominios criminales contra meramente comprometida tienen diferentes ciclos de vida. Si es posible, algún mecanismo para analizar la ventana de tiempo de cuánto tiempo malicioso dominios siguen existiendo y comparando ese gTLD de ancho y registradores podrían conducir a una cierta análisis útil y la investigación.

Un punto final sobre las estadísticas, a partir de este escrito actual, el 7 ◦ hasta el 10 de ◦ Secretario superior clasificado abuso tienen cada uno menos de 20 dominios total bajo gestión.

7	Everest 30, LLC	3048	15	2	13.33 0		0	0	2
8	Una empresa de tecnología, Inc.	53	8	1	12.50 0		0	0	1
9	Everest 35, LLC	3053	8	1	12.50 0		0	0	1
10	Camelot 12, LLC	2930	18	2	11.11 0		0	0	2

Tabla 2. Informe DAAR Registrador del 4 de abril ◦, 2018 (lista parcial)

Lo que esto puede conducir a sin matiz es que los registradores con un pequeño número de dominios pueden ser excesivamente afectada en sus clasificaciones y estadísticas por un único dominio abusivo de los cuales tienen poco o ningún control sobre.

Por las razones expuestas en los apartados anteriores, el valor de estas estadísticas es ayudar a la piedra de afilar “lo preguntas que debe hacer”para entender mejor el uso de los dominios en el abuso. Conclusiones basadas únicamente fuera probablemente será menos bien fundada estos datos (es decir, desde el Everest 30, LCC es el # 7, es una “de balas prueba de registro”sería infundada en ausencia de otros datos). Si se realiza correctamente, este los datos pueden ayudar a la actividad medida para hacer frente a la amenaza. X se TLD altamente clasificado ya que en realidad intencionalmente proporciona servicios a los criminales, algunas de las características de su negocio son atractivos para divulgación criminales, son herramientas proporcionadas por el registrador vulnerables de alguna manera, está ahí dirigidos que se podría hacer para los consumidores porque están usando herramientas inseguros (es decir, CMS vulnerabilidades), etc. Esto tiene el potencial de aumentar dramactically la seguridad de la Internet dado correcta y adecuadamente matizada de seguimiento sobre la base de lo que las estadísticas son diciendo.

Descripción del sistema

El Libro Blanco DAAR en las páginas 4-9 cubre la descripción del sistema y su enfoque de el problema. La descripción es exhaustiva y completa, por lo que otra persona podría reproducir el los resultados para proporcionar la verificación de las salidas de DAAR. En el caso de este analista, en profundidad conocimiento de cómo podría funcionar esto ya era conocido. Dicho esto, un moderadamente informado persona con suficientes recursos podría reproducir un sistema similar al DAAR para verificar los resultados.

Apéndice 1 - Feeds adicionales para su consideración

La siguiente es una lista no exhaustiva de los alimentos para su consideración para la inclusión.

https://www.alienvault.com/open-threat-exchange (Requiere curación)

https://hosts-file.net/?s=Download (No se deben incluir todos los canales)

https://isc.sans.edu/feeds/suspiciousdomains_Medium.txt

http://malc0de.com/database/

http://www.malwaredomainlist.com/

http://mirror1.malwaredomains.com/files/ (Es decir 20180404.txt)

http://osint.bambenekconsulting.com/feeds/c2-dommasterlist-high.txt

https://openphish.com/feed.txt

Además, a través de la Microsoft Virus Information Alliance, puede ser posible obtener acceso a

la alimentación Bing orugas malicioso URL que proporcionaría datos sobre más de 25 millones de URLs diaria

(A pesar de todo puede que no sea digna de ser incluida.