OPERACIONES DE RECONOCIMIENTO

DOXING

USERNAME

REDBIRD

OPERACIONES DE RECONOCIMIENTO

DOXING

USERNAME

Tabla de contenido

Introducción

En esta oportunidad evaluaremos los riesgos y amenazas que representan los nombres de usuario desde la perspectiva de la ciberseguridad y como operadores RedTeam pueden emplearlos para explotar vulnerabilidades y realizar labores de reconocimiento. Por otro lado, exploraremos las técnicas y herramientas empleadas por operadores de ciberinteligencia durante investigaciones.

Los username o nickname son los nombres de usuario o apodos empleados por los usuarios con la finalidad de poder identificarse en algún medio digital, como foros, redes sociales, en una red informática, en internet, etc. Estos nombres suelen ser creados por los usuarios o generados por el propio sistema y pueden ser cualquier combinación de letras, números o caracteres especiales.

Los “buenos” y los “malos” han explotado con éxito los nombres de usuario con diversos fines, algunos casos han sido empleados para obtener las direcciones de email y con ello ejecutar campañas de phishing, otros han creado comunidades sobre Doxing, cuyo único objetivo es recopilar y exponer información de los usuarios.

¿Qué es el Doxing?

El doxing es una práctica en la que se recopila y se divulga información personal de una persona sin su consentimiento. Esta información suele incluir detalles como el nombre real, la dirección, números de teléfono, correos electrónicos y perfiles en redes sociales. El objetivo principal del doxing es exponer y avergonzar a la persona afectada.

Mediante un conjunto de técnicas y el uso de herramientas empleadas para la recopilación de información o datos de un usuario en Internet, partiendo de sitios web, como lo son redes sociales, blogs, foros, etc.

La información que se recopila y posteriormente es divulgada, se puede clasificar en tres grupos:

1. **Información de identificación personal (IIP)**. Son todos aquellos datos que identifican a un individuo, registros de nacimiento, números de seguro social, pasaportes, licencias, etc.
2. **Información de contacto.** Son todos los datos que permiten establecer algún medio de comunicación, como email, numero de teléfono, redes sociales, dirección, ubicación, etc.
3. **Información personal o intima.** Este tipo de información comprende todas las relaciones personales de una persona, como la información familiar (padres, hermanos, sobrinos, etc.) y la información intima donde destacan las relaciones de amistad, noviazgo, pareja sentimental. Por otro lado, se incluye la información en relación a los gustos y preferencias del individuo en todos los ámbitos, ya sean personales o profesionales, tales como deportes, música, colores, partidos políticos, marcas comerciales, etc.

Obtención de información

La forma en la que se obtiene esta información es muy variada, ya que se suelen usar técnicas o tácticas intrusivas o pasivas mediante herramientas especializadas o haciendo uso de campañas maliciosas de ingeniería social.

Métodos generales de obtención de información de un objetivo.

1. **Métodos intrusivos.** Los métodos intrusivos son todos aquellos en donde un atacante comprometerá sistemas informáticos para acceder a la información de un objetivo. Estas intrusiones contemplan: sistemas informáticos, redes sociales, dispositivos inteligentes, etc.
2. **Campañas de ingeniería social.** Las campañas de ingeniería social (SIOPS) son todo un conjunto de actividades planificadas empleadas para influir en la toma de decisiones de un objetivo y que este comparta información personal.
3. **Ciberinteligencia.** Las operaciones de ciberinteligencia o cibervigilancia, son ampliamente empleadas por un atacante para obtener información de objetivo. Un ejemplo de ello, son las operaciones de inteligencia de redes sociales (SOCMINT) o las operaciones de inteligencia de imágenes (IMINT). También se consideran las operaciones de inteligencia de fuentes humanas (HUMINT) pero en un medio digital (CyberHUMINT).

Doxing y operaciones de inteligencia

En el ámbito de las operaciones de ciberinteligencia, el doxing puede tener implicaciones graves. Los actores malintencionados pueden utilizar la información recopilada a través del doxing para llevar a cabo acciones como el acoso, la extorsión, el robo de identidad o incluso el chantaje. Además, en el contexto de la ciberinteligencia, el doxing también puede ser utilizado como una táctica para obtener información sobre un objetivo o para llevar a cabo campañas de desinformación.

Legalidad del Doxing

Es importante tener en cuenta que el doxing es una actividad ilegal en muchos países. La divulgación no autorizada de información personal sin el consentimiento de la persona afectada viola la privacidad y puede tener consecuencias legales graves. Es fundamental respetar la privacidad y no participar en actividades de doxing. Las leyes pueden variar según el país y la jurisdicción. El doxing se considera una violación de la privacidad y puede estar sujeto a sanciones legales.

En el caso particular de México existe la Ley Federal de Protección de Datos Personales en Posesión de Particulares[1] y en el Código Penal Federal, en el articulo 210 establece como delito de invasión a la privacidad cuando se difunde información privada de una persona sin su consentimiento[2].

En resumen, el doxing es una práctica peligrosa que puede tener graves consecuencias tanto a nivel personal como legal. Es esencial respetar la privacidad de los demás y abstenerse de participar en actividades de doxing. La ética y la legalidad deben guiar nuestras acciones en el ámbito de la ciberinteligencia y la recopilación de información personal.

---

[1] Ley Federal de Protección de Datos Personales en Posesión de los Particulares (diputados.gob.mx)
[2] Código Penal Federal (diputados.gob.mx)

Nombres de Usuario (Nickname/UserName)

Los nombres de usuario también conocidos como Nickname y Username son nombres o apodos empleados por las personas para identificarse en el mundo digital, como redes sociales o foros, al igual que se emplean para sistemas informáticos.

Estos son creados por los propios usuarios o generados automáticamente por un sistema, tienden a ser la combinación de números, letras y de ser posible caracteres especiales. Esta combinación puede estar representada por fechas especiales como día de nacimiento, aniversarios, días festivos, etc. En cuanto a la otra parte, podemos encontrarnos con nombres invertidos, una combinación de las iniciales de su nombre, un apodo o sobre nombre.

Por ejemplo

- Luis1995
- Vict0r95
- Claudia1234

Los nombres de usuario también pueden representar sus ideologías sociales, su fanatismo o que pertenecen a grupos que realizan ciertas actividades legales o no.

Algunas organizaciones de gobierno, empresas, instituciones educacionales y demás, asignan nombres de usuario predefinidos a sus trabajadores o estudiantes con el fin de poder ser identificados en sus servicios digitales. Por ejemplo, en el gobierno, tenemos al usuario Carlos López, su identificador como trabajador de gobierno es: CLGOB11234 con este id el trabajador se identifica, dentro de las plataformas digitales con las cuales puede incluso iniciar sesión en ciertas plataformas.

- Nombre del trabajador: Carlos López
- Puesto/Sección: Gobierno (GOB)
- Fecha de nacimiento: Primero de diciembre del 2003 (1123)
- ID de trabajo: CLGOB1123

Y qué tal si el gobierno o su dependencia se comunica con él por medio de e-mail, en este caso puede que el mismo gobierno le asigne algún tipo de correo para ello, o utilice servicios ya sean de Gmail.

- Clgob1123@gobmx.com
- ClgoB1123@gmail.com

Algunas universidades, utilizan plataformas online, para mostrarle a sus alumnos, las calificaciones de sus materias, y para esto, puede que ellos también tengan su propio ID para identificar al alumno como un usuario de dicha plataforma.

Riesgos del uso de un (Nickname/Username)

Riesgos respecto a la ciberseguridad

El uso de username o nickname puede plantear algunos riesgos en términos de ciberseguridad. Algunos de estos riesgos incluyen:

1. **Exposición de información personal**: Si un username o nickname está vinculado a información personal identificable, como el nombre real, la ubicación o la fecha de nacimiento, podría permitir que los ciberdelincuentes recopilen información sobre una persona de manera más fácil.
2. **Suplantación de identidad**: Si un username o nickname es fácil de adivinar o se utiliza en múltiples plataformas, los ciberdelincuentes podrían intentar suplantar la identidad de una persona y realizar actividades fraudulentas en su nombre.
3. **Ataques de fuerza bruta**: Algunas plataformas permiten a los atacantes realizar ataques de fuerza bruta para adivinar usernames o nicknames junto con contraseñas débiles. Si un username o nickname es predecible o fácil de adivinar, podría facilitar estos ataques.
4. **Rastreo de actividades en línea**: Si un username o nickname se utiliza en varias plataformas en línea, los ciberdelincuentes podrían recopilar información sobre las actividades en línea de una persona y utilizarla para fines maliciosos, como el robo de identidad o el phishing.

Es importante tener precaución al elegir un username o nickname y evitar revelar información personal o sensible a través de ellos. Además, se recomienda utilizar contraseñas fuertes y únicas para cada plataforma y considerar el uso de medidas de seguridad adicionales, como la autenticación de dos factores, para proteger aún más la identidad en línea.

Operaciones de Inteligencia con nombres de usuario

Las "operaciones de inteligencia con nombres de usuario" se refieren a actividades específicas en el ámbito de la inteligencia en las cuales se realiza una recopilación, análisis y seguimiento de información relacionada con usuarios específicos en plataformas en línea o sistemas. Estas operaciones pueden tener varios propósitos, como la identificación de amenazas, la obtención de información estratégica, o la investigación en el contexto de ciberseguridad, entre otros.

Aquí hay algunos ejemplos de situaciones en las cuales las operaciones de inteligencia con nombres de usuario pueden ser relevantes:

1. Investigaciones de Seguridad Digital
Rastreo y análisis de actividades en línea asociadas con un nombre de usuario específico para identificar posibles amenazas a la seguridad de una organización.

2. Ciberseguridad y Hacking Ético
Uso de nombres de usuario para realizar pruebas de penetración, evaluar la seguridad de sistemas y aplicaciones, y verificar la presencia de vulnerabilidades.

3. Inteligencia de Amenazas
Seguimiento de nombres de usuario en foros oscuros, redes sociales u otras plataformas en línea para identificar actividades relacionadas con amenazas cibernéticas, como la planificación de ataques.

4. Prevención de Fraudes en Línea
Investigación de actividades sospechosas asociadas con nombres de usuario para prevenir o detectar fraudes en línea, tales como estafas, robo de identidad o phishing.

5. Análisis de Redes Sociales
Seguimiento de perfiles de usuarios en redes sociales para recopilar información sobre conexiones, actividades, y posiblemente identificar tendencias o patrones relevantes.

6. Contrainteligencia
Monitoreo de nombres de usuario para detectar posibles infiltraciones o intentos de obtener información clasificada o sensible. Así como distribuir información falsa, para entorpecer las investigaciones.

7. Investigaciones Forenses Digitales
Utilización de nombres de usuario en investigaciones forenses para rastrear la actividad digital de un individuo en dispositivos o sistemas específicos.

8. Gestión de Riesgos en Línea
Evaluación de la exposición y el riesgo asociado con nombres de usuario en plataformas en línea, especialmente en entornos donde la privacidad y la seguridad son críticas.

Estas operaciones de inteligencia con nombres de usuario requieren el uso de diversas herramientas y técnicas para recopilar, analizar y presentar la información de manera efectiva. Además, es fundamental que estas operaciones se lleven a cabo de manera ética y legal, respetando la privacidad y cumpliendo con las regulaciones pertinentes.

Consideraciones sobre la investigación de nombres de usuario

Las investigaciones de nombres de usuario son fundamentales en diversas áreas, desde la ciberseguridad hasta la inteligencia de amenazas y las investigaciones forenses digitales. Sin embargo, es esencial tener en cuenta varias consideraciones éticas, legales y técnicas al realizar estas investigaciones. Aquí hay algunas consideraciones importantes:

1. Legalidad y Ética

Cumplimiento Normativo: Es crucial realizar investigaciones de nombres de usuario de manera ética y respetar la legalidad. Asegúrate de cumplir con todas las leyes y regulaciones locales e internacionales relacionadas con la privacidad y la protección de datos.

2. Consentimiento y Privacidad

Consentimiento Informado: Si es posible, obtén el consentimiento informado de los usuarios antes de realizar investigaciones que involucren sus nombres de usuario. Respeta la privacidad y protege la información personal.

3. Propósito Legítimo

Propósito Justificado: Asegúrate de que tus investigaciones tengan un propósito legítimo y justificado. Evita la obtención de información para actividades ilegítimas o que puedan infringir la privacidad.

4. Metodologías Transparentes

Transparencia: Si estás llevando a cabo investigaciones como parte de un equipo o una organización, asegúrate de que las metodologías utilizadas sean transparentes y comprensibles. Esto ayuda a mantener la confianza en el proceso.

5. Validación de Datos

Verificación Rigurosa: Valida rigurosamente los datos obtenidos de las investigaciones. La información basada en nombres de usuario debe ser precisa y confiable para evitar errores o falsos positivos.

6. Uso Responsable de Herramientas

Herramientas Éticas: Al emplear herramientas automatizadas, asegúrate de que sean éticas y respeten las normativas de privacidad. Evita el uso de técnicas invasivas que puedan comprometer la integridad de la investigación.

7. Protección de Datos Sensibles

Seguridad de la Información: Asegura la protección de datos sensibles obtenidos durante las investigaciones. Adopta medidas de seguridad para prevenir el acceso no autorizado y la divulgación indebida de información.

8. Colaboración con Expertos

Consultas con Expertos Legales: Siempre es recomendable contar con la asesoría de expertos legales al llevar a cabo investigaciones que involucren nombres de usuario. Esto ayuda a garantizar que se respeten los derechos legales y éticos.

9. Límites en la Recopilación de Datos

Límites Claros: Establece límites claros en la recopilación de datos. Evita obtener información más allá de lo necesario y asegúrate de que la recopilación sea proporcionada al propósito de la investigación.

10. Actualización de Conocimientos
Evolución Tecnológica: Mantente actualizado sobre las evoluciones tecnológicas y legales en el ámbito de la investigación digital. La tecnología y las leyes cambian, y es esencial adaptarse a estos cambios.

Al considerar estos aspectos, las investigaciones de nombres de usuario pueden realizarse de manera efectiva y ética, garantizando la integridad y la legalidad de los procesos.

Falsos Positivos

Cuando nosotros realizamos una investigación partiendo de un nombre de usuario, podemos encontrarnos con falsos positivos, es decir, puede que encontremos información de nuestro objetivo y que, al momento de analizar con más detalle, esta información sea falsa, incorrecta o pertenezca a otra persona.

En el contexto de procesos de inteligencia o investigaciones, los "falsos positivos" se refieren a situaciones en las cuales una herramienta, sistema o proceso indica incorrectamente la presencia de una amenaza, entidad o evento que, en realidad, no existe o no es relevante para la investigación. En otras palabras, se trata de resultados incorrectos que indican erróneamente la existencia de algo que no es verdadero.

Ejemplos de falsos positivos en diferentes contextos podrían incluir:

1. Seguridad Informática
Un sistema de detección de intrusiones que genera una alerta indicando actividad maliciosa cuando, de hecho, la actividad es legítima y no representa una amenaza.

2. Inteligencia de Amenazas
Un indicador que se considera un signo de una amenaza potencial, pero después de una investigación más profunda, resulta ser una actividad normal sin relación con amenazas.

3. Análisis de Riesgos
Identificación incorrecta de un riesgo significativo en un proyecto o proceso que, después de una revisión detallada, se determina que es menos preocupante de lo inicialmente pensado.

4. Detección de Fraudes
Un sistema de detección de fraudes que señala una transacción como sospechosa cuando, de hecho, es legítima y no involucra actividad fraudulenta.

5. OSINT (Inteligencia de Fuentes Abiertas)
La obtención de información errónea de fuentes abiertas que lleva a conclusiones incorrectas durante una investigación de inteligencia.

La presencia de falsos positivos puede tener varios impactos negativos, como distracciones innecesarias, pérdida de tiempo y recursos, y la posibilidad de que se pasen por alto amenazas reales debido a una percepción errónea de la situación. Por lo tanto, minimizar la tasa de falsos positivos es un objetivo importante en la mejora de la precisión y la efectividad de los procesos de inteligencia y seguridad.

Verificación de información

En operaciones de inteligencia, verificar la información es una parte crítica del proceso para garantizar la precisión y la confiabilidad de los datos recopilados. Aquí hay un proceso general que se puede seguir para verificar la información en operaciones de inteligencia:

1. Evaluación de la Fuente

Autenticidad de la Fuente: Verificar la autenticidad y credibilidad de la fuente de información. Evaluar la reputación, la historia pasada de la fuente y su conexión con la información proporcionada.

2. Cross-Referencia con Fuentes Independientes

Diversificación de Fuentes: Buscar información similar o contradictoria de fuentes independientes y diversas. La convergencia de múltiples fuentes puede aumentar la confianza en la información.

3. Validación de Datos Objetivos

Datos Objetivos y Verificables: Priorizar la verificación de datos objetivos y verificables, como registros oficiales, documentos gubernamentales, imágenes o videos que puedan ser autenticados.

4. Análisis de Consistencia

Consistencia Interna: Analizar la consistencia interna de la información. Identificar discrepancias o inconsistencias dentro del conjunto de datos que puedan indicar posibles problemas.

5. Entrevistas y Contacto Directo

Contacto con Fuentes: Realizar entrevistas o contactar directamente con las fuentes cuando sea posible. Obtener clarificaciones y detalles adicionales para validar la información.

6. Validación Técnica

Verificación Técnica: Utilizar herramientas técnicas para verificar aspectos específicos. Esto podría incluir análisis forense, verificación de firmas digitales o la aplicación de técnicas de análisis de imágenes.

7. Revisión de Historial y Contexto

Historial y Contexto: Revisar el historial de la fuente y la información proporcionada. Considerar el contexto más amplio para comprender mejor la veracidad de los datos.

8. Análisis de Contrainteligencia

Contrainteligencia: Considerar la posibilidad de desinformación o manipulación. Evaluar si la información puede ser parte de una estrategia de contrainteligencia.

9. Colaboración con Expertos

Consulta con Expertos: Consultar con expertos en el campo relevante. La colaboración con profesionales que tienen experiencia en el tema puede proporcionar una perspectiva valiosa.

10. Seguimiento Continuo
Monitoreo Continuo: Establecer un sistema de monitoreo continuo para actualizar y verificar la información a medida que evoluciona la situación.

11. Registro de Decisiones
Documentación: Registrar todas las decisiones tomadas durante el proceso de verificación. Esto es esencial para la rendición de cuentas y el aprendizaje continuo.

12. Reevaluación Periódica
Reevaluación Regular: Establecer un proceso de reevaluación periódica de la información a medida que se obtienen más datos o cambian las circunstancias.

El proceso de verificación de información en operaciones de inteligencia es dinámico y requiere un enfoque meticuloso para garantizar la confiabilidad de los datos utilizados en la toma de decisiones estratégicas.

Metodología de investigación

La metodología de investigación de nombres de usuario implica un enfoque estructurado para recopilar, analizar y validar información asociada con identificadores en línea. A continuación, se presenta una metodología general junto con algunas fuentes que pueden ser útiles en cada etapa:

1. Definición de objetivos y alcance.

- **Establece objetivos claros.**
    - Identifica plenamente los nombres de usuario que serán investigados.
    - Establece el propósito de la investigación (por ejemplo, inteligencia de amenazas, análisis de perfiles, prevención de fraudes, investigación de delitos, etc.).
    - Establece límites operativos, es decir, por cuanto tiempo se desarrollará la investigación, teniendo en cuenta el tiempo, costos y recursos disponibles
- **Consideraciones Legales**
    - Previo a comenzar con la investigación, ten presente las limitaciones legales de la investigación.

2. Identificación de plataformas relevantes y criterios de investigación

- **Consideraciones preveías sobre la identificación de plataformas relevantes.**
    - Considerado el objetivo y el enfoque de la investigación, se deben identificar las plataformas y herramientas relevantes para realizar la investigación.
- **Selección de Plataformas**
    - Identifica las plataformas sociales más relevantes para tu investigación, como lo pueden ser; redes sociales, blogs, foros, sitios de noticias, comunidades online, etc.
    - Considera la popularidad y el enfoque del usuario objetivo.
        - Existen plataformas/sitios populares entre las actividades o intereses del usuario objetivo, como lo son sitios de política, programación, deportes, hacking, etc.

3. Recopilación de Nombres de Usuario

- **Fuentes Abiertas:**
    - Utiliza los motores de búsqueda para buscar el nombre de usuario en distintos sitios o plataformas en las que este registrado.
    - Utiliza recursos online de investigación OSINT o SOCMINT que faciliten el trabajo y automaticen procesos.
    - Emplea herramientas o script de investigación, disponibles en GitHub o plataformas como OSINT Framework.

4. Análisis de Perfiles Sociales

- **Consideraciones sobre el análisis de perfiles en redes sociales.**
    - El análisis manual de perfiles en redes sociales permite identificar potenciales falsos positivos.
    - Considera emplear herramientas que permitan analizar y resumir el perfil de un usuario.
- **Extracción de Datos:**
    - Examina perfiles en redes sociales relevantes.
    - Identifica detalles como biografías, fotos de perfil, ubicaciones, conexiones y publicaciones.

5. Búsqueda de Enlaces entre Perfiles

- **Análisis de Conexiones:**
    - Investiga conexiones entre diferentes perfiles.
    - Observa patrones de interacción y posibles relaciones.

6. Extracción de Metadatos

- **Obtención de Información Técnica:**
    - Utiliza herramientas que extraigan metadatos de imágenes y archivos compartidos.
    - Analiza fechas, ubicaciones y detalles técnicos.

7. Análisis de Actividad y Publicaciones

- **Estudio de Publicaciones:**
    - Examina el contenido compartido, incluyendo texto, imágenes y videos.
    - Analiza la frecuencia y el tipo de publicaciones.

8. Validación Cruzada de Datos

- **Comparación de Información:**
    - Contrasta datos obtenidos de diferentes plataformas.
    - Verifica la coherencia de la información.

9. Herramientas de OSINT Específicas:

- **Aplicación de Herramientas:**
    - Emplea herramientas de OSINT como Maltego para facilitar la recopilación de datos.

10. Análisis de Sentimientos y Tonos:

- **Evaluación de Comentarios y Publicaciones**
  - Analiza el tono general de las publicaciones y comentarios.
  - Identifica posibles cambios en el comportamiento.

11. Monitorización Continua:

- **Seguimiento de Cambios**
  - Establece un sistema de monitoreo para seguir cambios en los perfiles y actividad.
  - Actualiza la información de manera periódica.

12. Colaboración y Consulta Legal

- **Consulta con Profesionales Legales**
  - Busca asesoramiento legal sobre la recopilación y el uso de información obtenida.
  - Asegúrate de cumplir con las leyes de privacidad y regulaciones locales.

13. Documentación y Reporte

- **Registro Detallado**
  - Documenta cada paso de la investigación.
  - Genera informes detallados que puedan ser comprendidos por otros analistas o profesionales.

14. Protección de Datos y Privacidad

- **Garantía de Privacidad**
  - Asegúrate de manejar la información de manera ética y respetuosa con la privacidad.
  - Adopta medidas para proteger la información sensible.

15. Actualización Periódica de Conocimientos

- **Evolución Tecnológica**
  - Mantente actualizado sobre nuevas plataformas y cambios en las existentes.
  - Adapta tu metodología según la evolución tecnológica.

Recuerda que la legalidad y ética son fundamentales en todo el proceso. Esta metodología proporciona una guía general y puede adaptarse según las necesidades específicas de la investigación y el contexto legal en el que se lleve a cabo.

SOCMINT Nombres de Usuario

SOCMINT, acrónimo de Social Media Intelligence, es el conjunto de técnicas y herramientas que permiten la recopilación y análisis de información proveniente de redes sociales. Esta información puede ser utilizada para una variedad de propósitos, como la inteligencia, la seguridad, los negocios y el análisis social.

Las investigaciones de nombre de usuario en redes sociales son una forma de SOCMINT que se centra en la recopilación y análisis de información sobre un individuo o grupo específico a través de sus nombres de usuario en las redes sociales.

Esta información puede ser utilizada para una variedad de propósitos, como:

- **Identificación**: Las investigaciones de nombre de usuario pueden ayudar a identificar a individuos o grupos que no son conocidos por las autoridades.
- **Seguimiento**: Las investigaciones de nombre de usuario pueden ayudar a rastrear las actividades de individuos o grupos sospechosos.
- **Análisis**: Las investigaciones de nombre de usuario pueden ayudar a comprender las motivaciones y objetivos de individuos o grupos.

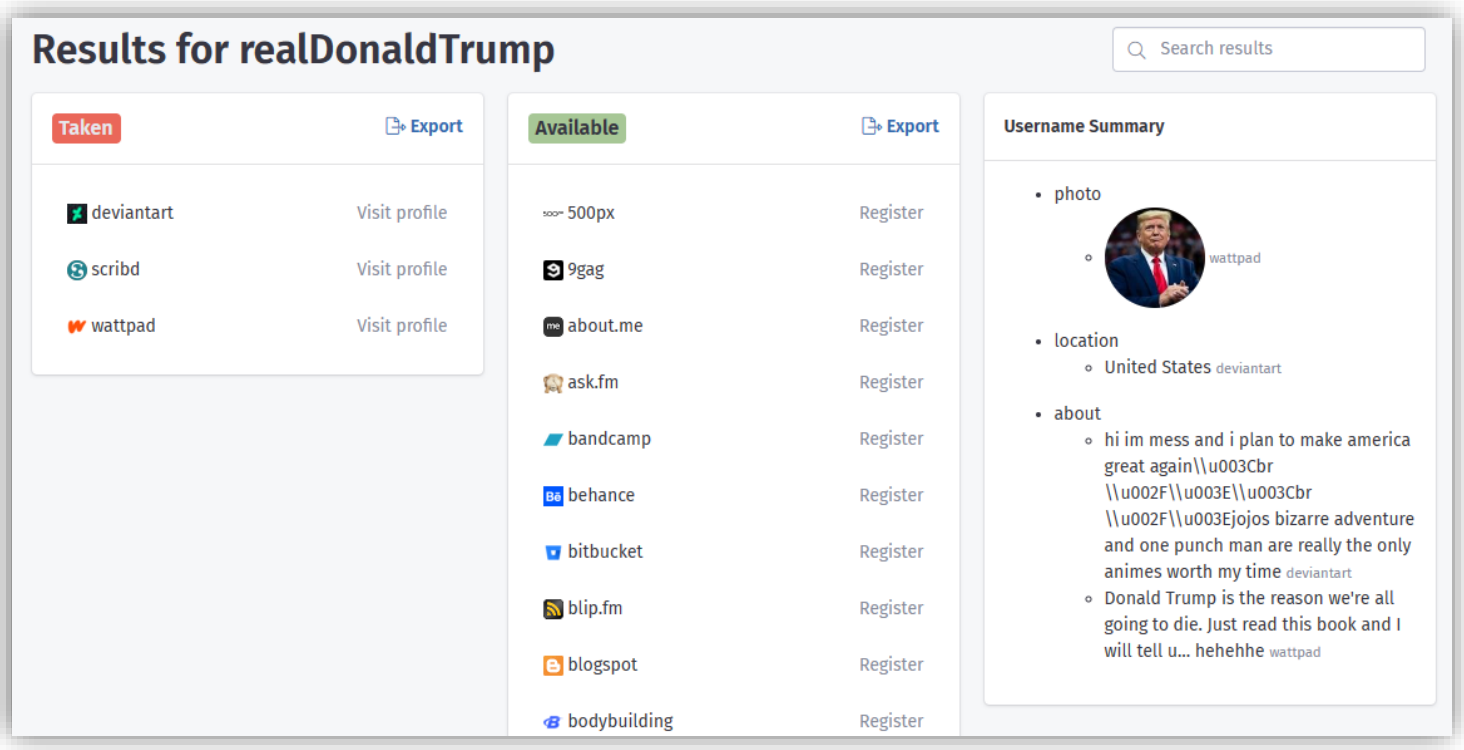
Las investigaciones de nombre de usuario pueden realizarse utilizando una variedad de técnicas, como:

- **Búsquedas en línea**: Las búsquedas en línea pueden ayudar a identificar cuentas de redes sociales que utilizan un nombre de usuario específico.
- **Análisis de datos**: El análisis de datos puede ayudar a identificar patrones y tendencias en las actividades de las cuentas de redes sociales.
- **Investigación humana**: La investigación humana, o de fuentes humanas (HUMINT) como el contacto con personas que conocen al individuo o grupo objetivo, puede ayudar a proporcionar información adicional.

Las investigaciones de nombre de usuario pueden ser una herramienta valiosa para una variedad de propósitos. Sin embargo, es importante tener en cuenta los límites legales de esta práctica. En muchos países, es ilegal recopilar información sobre individuos sin su consentimiento.

1.0 Identificación de cuentas en redes sociales y sitios

Una vez identificado el nombre de usuario, podemos verificar si el usuario esta registrado en otros sitios o redes sociales, haciendo uso del mismo nombre de usuario. Para ejemplo práctico usaremos el nombre de usuario del expresidente Donald Trump (`realDonaldTrump`). Para identificar si un usuario esta registrado con el mismo nombre de usuarios podemos hacer uso de herramientas online conocidas como “Checkers UserNames”.[3]



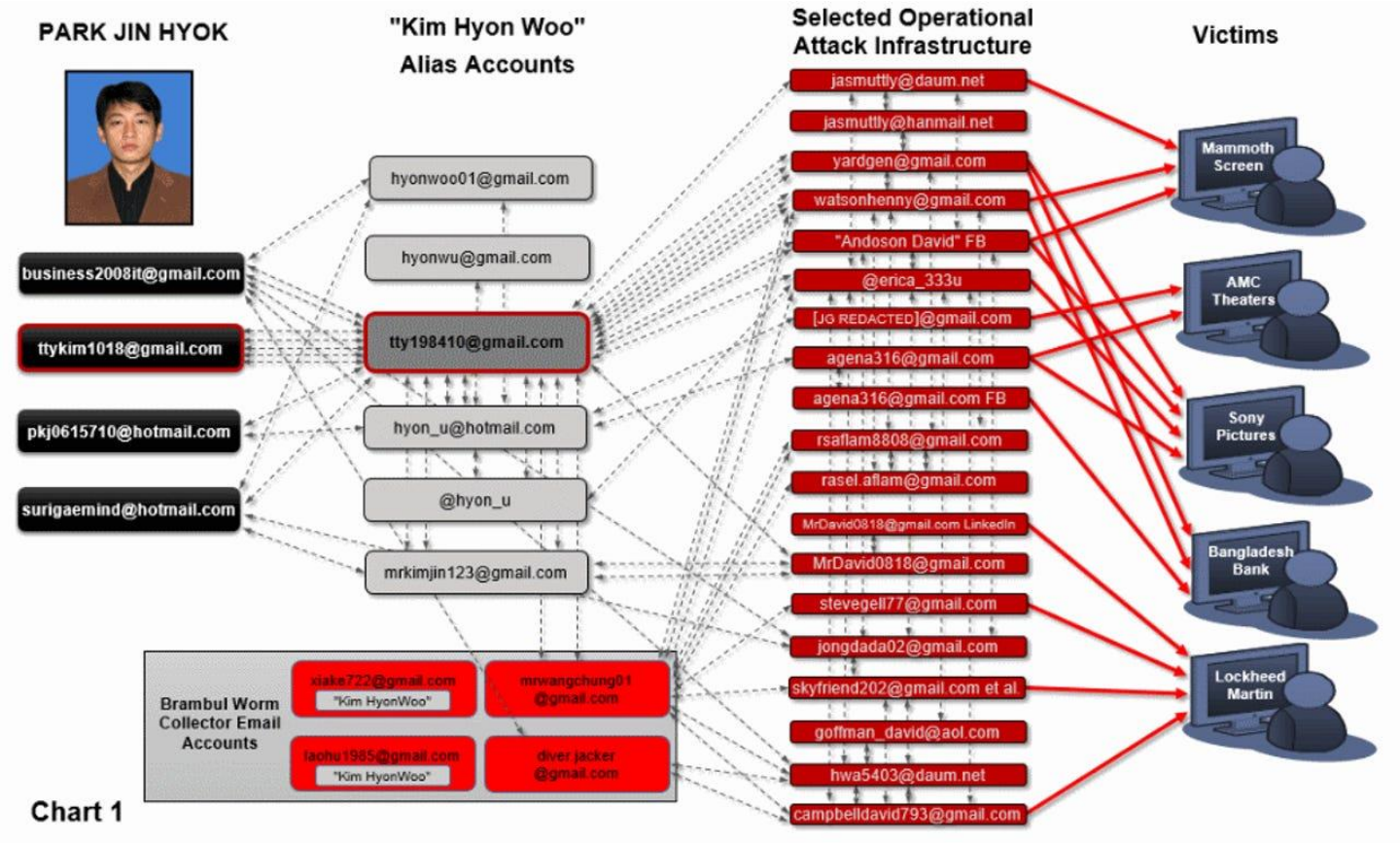
En la imagen anterior podemos ver un ejemplo de este tipo de herramientas, sin embargo, se insiste, independientemente de los resultados, se realicen verificaciones manuales, pues podemos estar frente a varios falsos positivos (leer: *Falsos Positivos*).

[3] What’s wrong with namecheckers? Last time I took a look at username checking tools... | by Soxoj | Medium

2.0 Generando variantes de nombre de usuario

Durante el proceso de investigación, podemos tener varios falsos positivos, los cuales pueden entorpecer nuestra investigación, ya sea consumiendo recursos limitados, como tiempo o dinero. Estos falsos positivos pueden ser cuentas en redes sociales, que hagan uso del nombre de usuario que estamos investigando, pero que no pertenezcan a nuestro usuario objetivo.

O viceversa, pueden existir cuentas en redes sociales, las cuales en principio no concuerden o coincidan con el nombre de usuario principal, dado que son variantes, un ejemplo de esto, es el caso del cibercriminal Park Jin Hyok y su red de cuentas de correo electrónico.

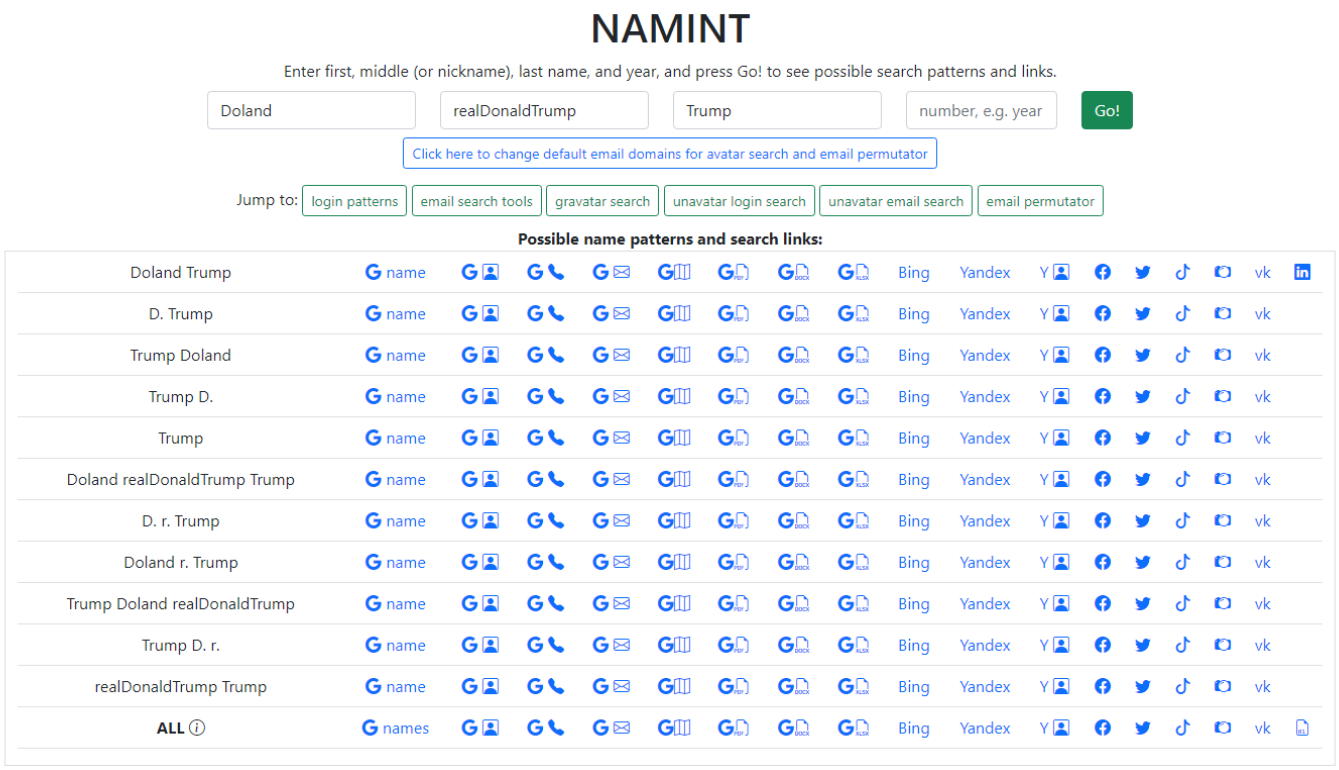


En la imagen anterior se puede apreciar las cuentas de email del cibercriminal, uno de los puntos de interés, para nosotros, son las variantes de su nombre de usuario. Para poder abordar este problema durante la investigación es importante usar herramientas que nos permitan generar variantes de nombres de usuario, para nuestras investigaciones.[4]

[4] Similar usernames generation guide | by Soxoj | Medium

2.1 Herramientas para generar variaciones de nombres de usuario

Para generar variantes de nombre de usuario, podemos hacer uso de la herramienta NAMINT[5] la cual nos permite generar variantes para nombre de usuario, direcciones de email, credenciales de inicio de sesión (username y password) y hacer búsquedas directamente desde la herramienta.



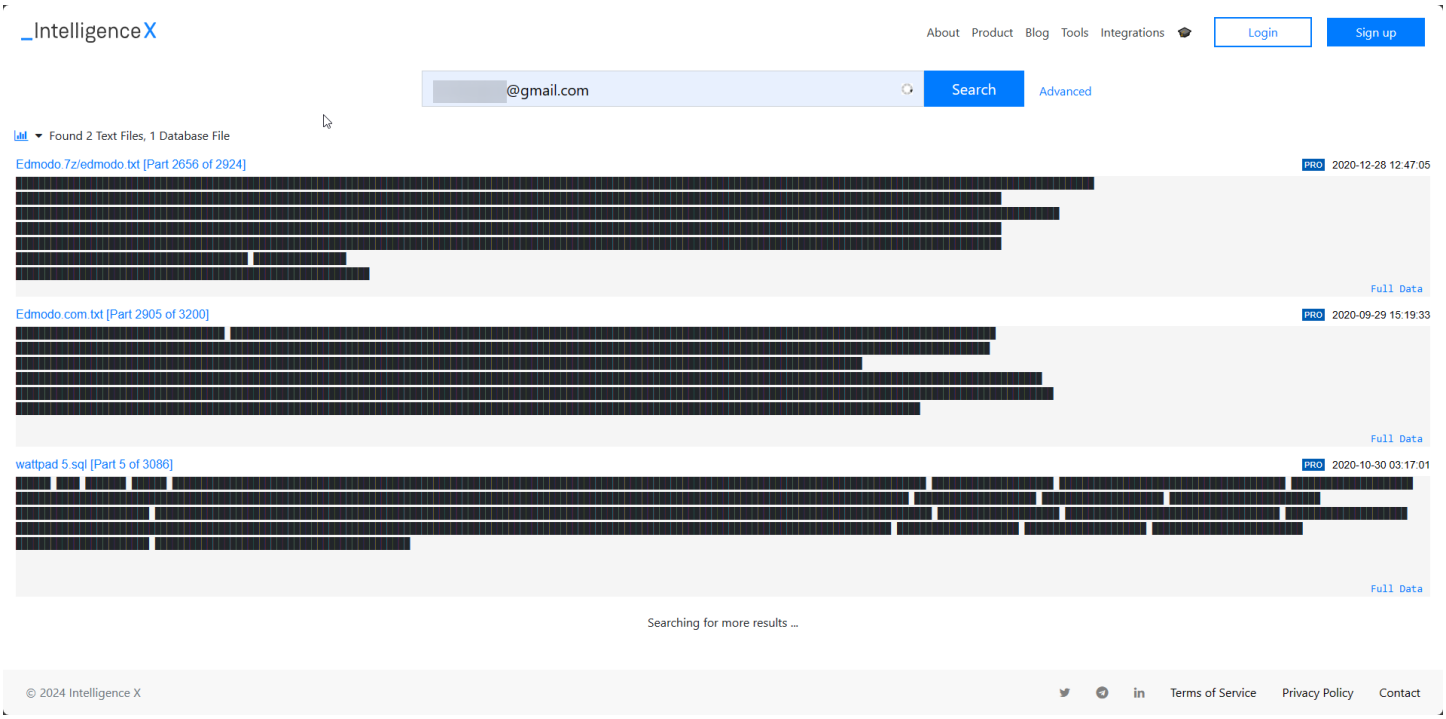
[5] NAMINT (seintpl.github.io)

3.0 Nombres de usuario en Dataleaks

El uso de información filtrada puede ser un tema delicado y potencialmente ilegal, dependiendo del contexto y la jurisdicción. En muchos casos, el uso de información obtenida ilegalmente puede violar las leyes de privacidad y propiedad intelectual. Además, si la información filtrada se refiere a datos personales no públicos, su uso podría infringir las leyes de protección de datos.

Existen herramientas que nos permiten realizar búsquedas en filtraciones de información como lo es Dehashed[6] o HaveIBeenPwned[7].

Una de las mejores herramientas con un basto registro de información filtrada es IntelligenceX[8] incluyendo sus herramientas de investigación de nombres de usuario[9] sin embargo, al igual que muchas herramientas de esta índole, se debe realizar un pago, ya sea una suscripción o comprar una cantidad de búsquedas.



[6] https://dehashed.com
[7] Have I Been Pwned: Check if your email has been compromised in a data breach
[8] https://intelx.io/
[9] Tools - Intelligence X (intelx.io)

Toolkit

Herramientas o recursos de investigación para nombres de usuario.

<table>
<tr><th>Búsqueda de sitios donde se registró el objetivo con el mismo nombre de usuario</th><th>Scripts para la investigación de nombres de usuario</th></tr>
<tr><td>

WhatsMyName Web
Username Checker (analyzeid.com)
Find User Profiles | UserSearch
Instant Username Search
https://www.peekyou.com/
Search POF by Username
CheckUsernames - by KnowEm
KnowEm Username Search
Username Checker - (checkuser.org)
Home | Usersearch Premium
Username Checer - Namevine
Username Checker (bloggingehow.com)
IntelTechniques Search Tool

</td><td>

GitHub - sherlock-project/sherlock
GitHub - soxoj/maigret
GitHub - qeeqbox/social-analyzer
GitHub - thewhiteh4t/nexfil
GitHub - WebBreacher/WhatsMyName
GitHub - snooppr/snoop: Snoop
GitHub - WebBreacher/WhatsMyName.
GitHub - wishihab/userrecon
GitHub - restanse/NicknameFinder
GitHub - YouVBeenHacked/gideon
GitHub - AlexC-ux/Arina-OSINT.
GitHub - rahulrajpl/netizenship.
GitHub - meanii/Search4.
GitHub - iojw/socialscan
GitHub - mesuutt/sherlock
GitHub - tdh8316/Investigo.
GitHub - lanmaster53/recon-ng.
GitHub - woj-ciech/SocialPath
GitHub - CYB3R-G0D/SPY
GitHub - soxoj/marple

</td></tr>
<tr><th colspan="2">Herramientas de investigación OSINT/SOCMINT con características para la investigación de nombres de usuario,</th></tr>
<tr><td>

GitHub - C0MPL3XDEV/E4GL30S1NT
GitHub - arxhr007/Aliens_eye
GitHub - novitae/sterraxcyl
GitHub - oryon-osint/querytool
Lullar.com - Search People Profile

</td><td>

Homepage - Maltego
Global Scammer Database
Username search (aware-online.com)
OSINT Toolkit (one-plus.github.io)
Tools - Intelligence X (intelx.io)

</td></tr>
<tr><th colspan="2">Recursos de interés o complementarios</th></tr>
<tr><td colspan="2">

GitHub - kkrypt0nn/wordlists
NAMINT (seintpl.github.io)

</td></tr>
</table>

Búsquedas Avanzadas en Google

Las búsquedas avanzadas en Google, son un medio por el cual podemos especificar los resultados en nuestras búsquedas, con lo cual acercarnos más al resultado esperado, para realizar este tipo de búsquedas tenemos una variedad de opciones, para mejorar nuestros resultados, un ejemplo de esto es el formulario de búsqueda avanzada de imágenes[10], y de igual forma, existe un formulario para búsquedas avanzadas[11].

Para realizar estas búsquedas avanzadas, tenemos que definir con exactitud la búsqueda[12], es decir comprender que vamos a buscar para posteriormente realizar la búsqueda[13]. Entre todas estas opciones, encontramos los parámetros especiales de búsqueda de Google, o PEBAG (Parámetros Especiales de Búsqueda Avanzada de Google).

Parámetros Especiales de Búsqueda Avanzada de Google (PEBAG)

Google nos ofrece una gran cantidad de parámetros los cuales son implementados en búsquedas avanzadas de información para lograr tener resultados más precisitos, con estos parámetros podemos reducir la cantidad de resultados "basura", por ejemplo, de hacer una búsqueda la cual nos arroje 10,000,000 de resultados podemos reducir esta cantidad significativamente, incluso a 100.

Google Hacking es una técnica infalible de reconocimiento pasivo la cual bien implementada nos permite obtener datos sensibles de personas, empresas (públicas o privadas) y entidades de gobierno[14].

La información que podemos conseguir aplicando de manera eficiente las búsquedas avanzadas puede ser:

- Datos de configuración de aplicaciones web, sistemas y redes
- Datos de acceso a bases de datos
- Usuario y contraseña
- Mensajes y Advertencias de errores de programación
- Datos sensibles de alguna compañía
- Búsquedas aleatorias de sistemas o aplicaciones vulnerables
- Números y claves de tarjetas de crédito
- NIP
- Número de tarjeta bancaria
- Acceso a archivos .log
- Redes Sociales
- Correos Electrónicos
- Bases de Datos
- Nombres de usuario
- Información de servidores
- Información de Sistemas Operativos
- BackUp en texto plano
- Mensajes
- Archivos multimedia
- Paneles de Administración de aplicaciones web, sistemas o redes
- Dispositivos mal configurados o dispositivos IoT vulnerables
- Cámaras de seguridad
- Impresoras
- Cámaras Web
- Lámparas
- Dispositivos de refrigeración
- Alarmas
- Cajas registradoras

[10] Búsqueda avanzada de imágenes de Google
[11] Búsqueda avanzada de Google
[12] Cómo definir mejor las búsquedas de Google - Ayuda de Búsqueda web de Google
[13] Cómo realizar una Búsqueda avanzada en Google - Computadora - Ayuda de Búsqueda web de Google
[14] Google Hacking - Wikipedia, la enciclopedia libre

Todo este tipo de información y dispositivos podemos encontrar gracias a Google Hacking y sus PEBAG, pero ¿Y los usuarios? Realizando prácticamente las mismas búsquedas, pero con un objetivo distinto podemos encontrar información de usuarios como:

- Nombres de usuario (Nickname/Username).
- Correo electrónico.
- Contraseñas
- Sitios donde está registrado (Blogs, redes sociales, foros, etc).
- Direcciones fisicas
- Número de Teléfono
- Fotografías
- Otras cuentas

La información disponible a la que se puede acceder, depende de una variedad de factores entre los que destacan principalmente es la cantidad de información que el usuario ha expuesto en internet a lo largo del tiempo, por otro lado, acceder a esta información depende de nuestras habilidades y recursos disponibles, pues en algunos casos es necesario pagar para acceder a información privilegiada.

OPERADOR	DESCRIPCION
INURL	Busca una palabra en la URL de un sitio o de todos en general
AUTHOR	Busca al autor de post, comentarios, etc.
SITE	Podemos especificar búsquedas en X sitio
INTEXT	Busca una pablara indicada en el texto de la página con variaciones en mayúsculas y minúsculas
ALLINTEXT	Busca varias palabras en el texto de la pagina
INACHOR	Busca palabras en las descripciones de los enlaces
“”	Especifica que buscamos únicamente el texto dentro de las comillas
-	Ayuda a excluir términos

NOTA: No son todos los operadores existentes para poder realizar el Google Hacking, sin embargo, podemos decir que son los básicos para poder encontrar información de un usuario, ya que los demás están destinados para contra otro tipo de información.

Suponiendo que un usuario, del cual solo conocemos su nombre de usuario (carlos666) por ejemplo, es nuestro objetivo, podemos implementar los parámetros para realizar una búsqueda basándonos en su nombre de usuario.

PEBAG	DESCRIPCIÓN
Inurl: carlos666	Buscará en las URL el nickname.
Autor: carlos666	Buscará comentarios, publicaciones, con el nickname.
Site: sitioejemplo.com carlos666	Buscará en el sitio sitioejemplo.com el nickname.
Intext: carlos666	Buscará en páginas el nickname.
Allintext: carlos666	Buscará carlos666 en el texto de alguna página, puede ser dentro de un comentario.
Inachor: carlos666	Buscará el nickname en la descripción de enlaces
“carlos666”	Buscará de manera precisa el nickname

Como mencionamos anteriormente cada uno de los parámetros por si solo puede buscar datos de manera efectiva, sin embargo, podemos mejorar la precisión de esta búsqueda combinando los parámetros y formar un Dork.

Ya conocimos algunos de los Parámetros Especiales de Búsqueda Avanzada de Google y como los podemos implantar para hacer búsquedas avanzadas y Google Hacking.

DORKS

Un Dork es un conjunto de parámetros PEBAG el cual tiene como función precisar nuestra búsqueda, dándonos resultados más precisos. Por ejemplo:

- Dork para encontrar usuarios y contraseñas de aplicaciones web

```
ext:pwd inurl:(service | authors | administrators | users) “# -FrontPage-“
```

- BackUp de bases de datos

```
filetype:sql “# dumping data for table” “`PASSWORD` varchar”.

filetype:sql “# dumping data for table” “`PASSWORD` varchar”
```

Búsqueda de nombres de usuario en un sitio especifico

Para buscar el nombre de usuario en un sitio especifico usamos dos parámetros especiales, SITE y las comillas dobles “”. Con este dork, indicamos a Google que estamos buscando exactamente la información contenida en las comillas en un sitio web especifico.

- `Site:ejemplo.com “username”`
- `Site:Facebook.com “drok3r”`

Búsqueda general de nombre de usuario

Si buscamos un nombre de usuario exacto, lo que podemos hacer es hacer uso de las comillas dobles.

- `“nombre de usuario”`
- `“realDonaldTrump”`

Buscamos un correo electrónico:

- ”@gmail.com” “Drok3r”

Buscamos sus publicaciones o comentarios en foros

- Autor:”drok3r”

También podemos especificar el sitio en el cual creemos ha hecho comentarios o publicado post, por ejemplo:

- site:hackingpublico.net autor:”Drok3r”

También podemos indicar a Google que nos muestre las URL que contenga mi nickname, por ejemplo:

- Inurl:”drok3r”
- Inurl:”drok3r” intext:drok3r
- Site:twitter.com inurl:”drok3r” | intext:drok3r

Búsqueda de nombres de usuario en archivos

Podemos buscar el nombre de usuario, en el contenido de algunos archivos públicos en internet, como lo son archivos de la suite de office, archivos .txt, .pdf, .rtf, etc. Existen casos particulares en donde podemos encontrar los nombres de usuario en los títulos multimedia de archivos .mp3 o .mp4.

- Intext:”username” filetype:pdf
- Intext:”username” filetype:txt