RS4Ly

Prologo 3
Desde la vista de un analista de ciberseguridad: 3
Desde la vista de un usuario casual: 3
Objetivos 4
Introducción: 5
Conceptos Básicos 5
¿Qué es un ataque informático? 5
¿Cómo podrían estos ingresar a nuestro dispositivo? 5
Definición junto a conceptos de virus y Ataques informáticos 6
Como un usuario casual puede evitar ser víctima de uno de estos ataques 8
Conceptos de informática, ciberseguridad y redes a nivel básico 9
Cómo funciona la herramienta 12
Como le ayudara la herramienta en su rutina diaria 13
Análisis de IP 13
Análisis de subnet (Redes) 14
Análisis de archivos 15
Continuación 15
Uso 15
Análisis de url 16
Porque es necesario tener tantas keys personales 17
Detalle de la información recolectada de cada fuente y como se combinan (próximamente) 17
Primeros pasos 18
1) Obtener sus keys personales 18
- Virus Total 18
- IP Abuse DB 18
- IP Quality Score 18
- IP Abstract 18

2) Ingresar sus keys personales en la herramienta 19
3) Comprobar que todo este correcto 20
Información y resultados que se obtendrán al realizar una búsqueda (Próximamente) 21

Funcionamiento a nivel de programación (Próximamente).....21
Fuentes de información:.....22
Versiones actuales y futuras mejoras.....23
Próximas mejoras.....23
0.2.0 - Actual.....23
0.1.0.....24

Prologo

Antes de entrar en tema quisiera decir que su servidor Elias Ramirez con el Nick RamirezS4, aunque pueda parecer simple todo el funcionamiento me siento muy bien de poner en practica estos nuevos conocimientos adquiridos sobre programación a disposición de la comunidad en general para fines de hacer el bien y aportar mi granito de arena.

Lo que he llegado a aprender en el transcurso de desarrollar este proyecto ha sido increíble, agradezco a todos los que colaboraron de una forma u otra dándome algún consejo, doy gracias a las fuentes de información que se encuentran en internet, a las personas que se dedican a hacer videos, dar clases a todos ustedes que desinteresadamente por transmitir sus conocimientos sacan el tiempo y le ponen mucha dedicación.

Desde la vista de un analista de ciberseguridad:

Actualmente es una tarea tediosa hasta para un analista de ciberseguridad obtener información de manera centralizada de diferentes fuentes de inteligencia de amenazas (threat intelligence), esto hace que, al momento de intentar obtener información sobre alguna ip, hash de un archivo, url, subnet (Redes), debamos buscar la misma de manera individual en cada fuente y analizar los resultados para luego compararlos, esto supone un gasto de recursos como lo son energía eléctrica, energía vital, entre otros, destacando el más importante “el tiempo”. El tiempo con el que cuenta un analista para dar respuesta a una alerta de seguridad es limitado y más bien escaso si el número de estas es considerable.

Desde la vista de un usuario casual:

En el justo momento que decidimos tener conexión a internet ya sea para entrar a nuestras redes sociales, navegar por internet en general y otras tareas estamos expuestos a un sin número de amenazas que intentaremos definir, explicar y dar ejemplo más adelante.

Estas amenazas intentan: obtener sus datos personales (documentos de identidad, tarjetas electrónicas, entre otros), obtener acceso a sus dispositivos como teléfono, Tablet, computadoras. Obtener acceso a sus redes sociales para hacerse pasar por usted o con cualquier otro fin, entre un sin número de objetivos que podría tener. Todos tenemos información que consideramos importante como lo podrían ser fotos familiares, videos personales, documentos de nuestros trabajos u otra información sensible que no queremos divulgar. Mantener los mismos seguros es en parte nuestra responsabilidad y esta responsabilidad crece mucho más cuando tenemos algún niñ@, adolecente u otra persona con poca información sobre los peligros de navegar en internet, entrando a diferentes sitios sin conocer su reputación, descargando archivos de juegos modificados o en páginas de dudosa procedencia, pero no se preocupe ahora tendrá una ayuda con esto.

Objetivos

El motivo de crear esta herramienta es brindar a los usuarios comunes, analistas de seguridad y cualquier otro interesado una forma rápida y confiable de obtener acceso a algunas de las fuentes de inteligencia de amenazas más grandes y usadas a nivel mundial por los profesionales de ciberseguridad con el objetivo de sacarle el mayor provecho posible para mantener nuestras redes y dispositivos seguros.

Teniendo en cuenta que mantener segura la integridad de una red o dispositivo no es una tarea fácil, pero el conjunto de pequeñas buenas prácticas y concientización es una excelente forma de iniciar.

Introducción:

Como esta herramienta está diseñada para todo tipo de público y por ende algunos necesitaran una guía más exhaustiva con el fin de entender como esta herramienta podría ayudarles en el día a día, antes de explicar cómo funciona definiremos algunos conceptos básicos de ciberseguridad.

La herramienta cuando esté completada tendrá funcionalidades como lo son análisis de IP, análisis de archivos, análisis de url, análisis de subnet (Redes), entre otras funciones. Si usted no tiene claro alguno de estos conceptos no se asuste, en breve comenzaremos a definir que son cada uno de estos, como usted interactúa día a día con ellos y ejemplos.

Conceptos Básicos

¿Qué es un ataque informático?

De manera clara y simple podemos definir un ataque informático como un intento de obtener acceso a un sistema o dispositivo el cual puede ser una computadora, teléfono, Tablet, servidor, cámara u otro. Mediante el uso de diversas formas como lo pueden ser virus, malware, ingeniería social u otro método con el objetivo final de alterar el funcionamiento del mismo, causar daños, bloquear su uso, robar/vender/comercializar la información obtenida de los mismos.

Los ataques informáticos son un intento organizado e intencionado que busca explotar alguna vulnerabilidad o debilidad en las redes o sistemas informáticos tanto en software o hardware, con el objetivo de obtener algún beneficio económico o simplemente por anarquía.

¿Cómo podrían estos ingresar a nuestro dispositivo?

Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por **desconocimiento del usuario**. El código del virus queda residente (alojado) en la memoria de la computadora, incluso cuando el programa que lo contenía ya esté cerrado o no este visible para nosotros. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

Una segunda forma seria que entremos a algún sitio web para ver una película o buscar una tarea y hagamos clics en algún enlace externos que nos dirige a descargar algún archivo, documento con cualquier tipo de excusa como lo son estos mensajes de que “su dispositivo tiene algún tipo de error o virus”, “alguna oferta increíble” u otro tipo de anuncio falso.

Una tercera forma seria que recibamos algún correo electrónico con un enlace diciéndonos que debemos ingresar a nuestra cuenta de banco porque la misma fue víctima de algún bloqueo, sin saberlo entramos en una página falsa que el ataquante realizo para que creamos que es la oficial del banco, sin saberlo ponemos nuestros datos y como si fuera magia nosotros le pasamos toda nuestra información a un ciber delincuente que puede hacer con esta lo que desee.

Definición junto a conceptos de virus y Ataques informáticos

- **Malware**: Esto es un concepto general con el cual nos referimos a cualquier software (programa) malicioso que tiene por objetivo introducirse en el sistema de un dispositivo para causar daño o robar información.
- **Ransomware**: Lo que hace es secuestrar datos (encriptándolos) y pedir un rescate por ellos. Normalmente, se solicita una transferencia en criptomonedas, para evitar el rastreo y localización de la transferencia. Este tipo de ciberataque va en aumento y debido a sus recientes variaciones es uno de los más temidos en la actualidad.
- **Spyware**: es un programa espía, cuyo objetivo principal es obtener información. Su trabajo suele ser también silencioso, sin dar muestras de su funcionamiento, para que puedan recolectar información sobre nuestro equipo sin despertar nuestra preocupación, e incluso instalar otros programas sin que nos demos cuenta de ello.
- **Recycler**: Este tipo de virus aun en la actualidad es muy común en computadoras antiguas utilizadas para poner música u otra función este lo que hace es crear accesos directos de programas y archivos, eliminando a nuestra vista el archivo original entonces cuando intentamos copiar estos, no podemos reproducirlos o abrirlos fuera del computador que los tiene.
- **Troyano**: Lo que buscan es abrir una puerta trasera para favorecer la entrada de otros programas maliciosos. Su nombre es alusivo al “Caballo de Troya” porque su misión es precisamente, pasar desapercibido e ingresar a los sistemas sin que sea detectado como una amenaza potencial. No se propagan a sí mismos y suelen estar integrados en archivos ejecutables aparentemente inofensivos.
- **Doxing**: Es un término utilizado para describir la práctica en Internet de investigación y publicación de información privada sobre un individuo o una organización, generalmente con el propósito de intimidar, humillar o amenazar.
- **Pishing**: Es uno de los ataques más habituales dirigidos a todo tipo de público de manera personalizada o general, todos alguna vez hemos visto o recibido el mensaje del príncipe nigeriano que espera que le mandemos dinero. Los medios más utilizados son el correo

electrónico, mensajería o llamadas telefónicas, mediante el cual el atacante se hace pasar por alguna entidad u organización conocida, solicitando datos confidenciales, para posteriormente utilizar esos datos en beneficio propio.

- **AdWare**: La función principal del adware es la de mostrar publicidad de forma invasiva. Aunque su intención no es la de dañar equipos, es considerado por algunos una clase de spyware, ya que puede llegar a recopilar y transmitir datos para estudiar el comportamiento de los usuarios y orientar mejor el tipo de publicidad.
- **Gusano**: Un gusano es un programa que, una vez infectado el equipo, realiza copias de sí mismo y las difunde por la red. A diferencia del virus, no necesita nuestra intervención, ni de un medio de respaldo, ya que pueden transmitirse utilizando las redes o el correo electrónico.
- **Hoax** (**fake news**): Esta es una categoría relativamente nueva trata la cual ha visto un crecimiento masivo durante y después de la pandemia la cual consiste en noticias, mensajes u otras informaciones falsas que se difunden de manera masiva y buscan que los usuarios a los cuales llegue lo tomen como real.
- **Keylogger**: Se encarga de registrar cada tecla o clics realizado en nuestros dispositivos (Tablet, teléfonos, computadoras), se utilizan para robar contraseñas, cuentas bancarias, entre otros datos.
- **Virus Hijackers**: Los hijackers alteran las páginas iniciales del navegador e impide que el usuario pueda cambiarla, muestra publicidad en pops ups. Instala nuevas herramientas en la barra del navegador y a veces impiden al usuario acceder a ciertas páginas web. Para los que tenemos tiempo usando diversos dispositivos en tiempos pasados lo abrimos visto de manera más común que en la actualidad.

Como un usuario casual puede evitar ser víctima de uno de estos ataques

Entre las posibles formas de mantener nuestras redes y dispositivos seguros podemos mencionar:

- Analizar los archivos que va a descargar antes de hacerlo
- Verificar los links (url) a los que ingresa antes de hacerlo.
- Mantener nuestros sistemas actualizados.
- Tener un buen antivirus.
- Tener controles parentales a los dispositivos de los niños y educar a los más miembros más cercanos o en la adultez sobre los peligros que existen al navegar en internet.
- No descargas archivos sin comprobar que esté limpio.
- No navegar en sitios de dudosa procedencia.
- No hacer clics en enlaces que nos envíen por algún correo electrónico, mensaje o cualquier medio sin antes comprobar que el mismo este limpio.

Conceptos de informática, ciberseguridad y redes a nivel básico

En este apartado mencionaremos los conceptos principales para entender como esta herramienta le ayudara, dando ejemplos prácticos del uso de la misma.

¿Qué es **ciberseguridad**? La ciberseguridad se refiere a la protección de los dispositivos conectados a Internet, como computadoras, dispositivos móviles y electrónicos, servidores, redes y datos, de los ataques cibernéticos.

¿**Qué es una red**? Es un conjunto de dispositivos como lo son computadoras, Tablet, servidores, router, entre otros equipos, conectados entre sí, con la finalidad de intercambiar y compartir información, compartir recursos o servicios, entre otras funciones disponibles. Tenemos diversos ejemplos de redes como la de su hogar que está formada por los dispositivos que usted y su familia en dado caso poseen todos estos al estar conectados al router forman una red la cual se denomina **red privada**. Entonces internet es una red **pública** formado por un sin número de dispositivos los cuales interactúan entre sí.

Dispositivos, Aparatos tecnológicos con los que interactuamos, como nuestro ordenador, el móvil, la Tablet, la impresora, el smartwatch, y un gran número de objetos inteligentes.

Router Dispositivo que nos permite conectarnos a una red la cual puede o no tener acceso a Internet como en nuestro hogar. Con este podemos conectar nuestros dispositivos a Internet a través de un cable de red o mediante la conexión wifi.

ISP: Es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías. Ejemplo: Altice, TMobile, Orange.

IP: Una dirección **IP** es una cadena de números separados por puntos. Las direcciones **IP** se expresan como un conjunto de cuatro números, por **ejemplo**, 192.158.1.38. Cada número del conjunto puede variar de 0 a 255. Por lo tanto, el rango completo de direcciones **IP** va desde 0.0.0.0 hasta 255.255.255.255.

Dirección IP: Permite identificar junto a otros elementos un dispositivo especifico en una red. Son conocidas como el mecanismo con el que los dispositivos y sitios web se comunican entre ellos y el que permite que la información que busca sepa dónde encontrarle.

Dirección **ip publica**: Es una dirección a la que se puede acceder directamente desde Internet y que su proveedor de servicios de Internet (ISP) asigna a su router de red, es la dirección que ven los otros dispositivos cuando usted navega en internet.

Dirección **ip privada**: Es una dirección creada solo para usarse en una red interna es decir en la red de su hogar, esto le permite al router poder identificar su dispositivo entre los demás conectados.

Wi-Fi Conexión inalámbrica que permite conectar nuestros dispositivos a Internet.

Información sensible o privada, Información que contiene datos privados o confidenciales: nombre, apellidos, fecha de nacimiento, ubicación, datos bancarios, número de tarjeta de crédito, etc.

Antivirus, Programa que detecta cualquier amenaza, como los virus, y la elimina de nuestro dispositivo. Es necesario mantenerlo actualizado para que nos proteja correctamente, incluso de los virus más nuevos.

Actualización Todos los dispositivos y programas instalados evolucionan y se actualizan a nuevas versiones. Con la actualización se solucionan errores y problemas de seguridad y rendimiento, por lo que debemos asegurarnos de actualizarlos siempre.

Software Programas informáticos que sirven para realizar tareas específicas. Cualquier herramienta que instalemos o utilicemos en nuestro ordenador es un ejemplo de software, como el navegador, el correo electrónico, un juego o cualquier otra aplicación que ofrezca alguna funcionalidad concreta.

Software pirata Un programa descargado de una página web que no sea la del desarrollador, fabricante o un repositorio oficial de aplicaciones, como pueden ser Google Play o Apple Store, se considera un software pirata y puede ser una gran amenaza para nuestro equipo, ya que puede contener virus u otras amenazas (malware).

Spam Correo de tipo publicitario o malicioso no deseado que llega a nuestra bandeja de entrada con el único propósito de vendernos un producto, hacernos caer en algún fraude o infectar nuestros dispositivos.

Ingeniería social Estrategia de engaño que utilizan los ciberdelincuentes para ganarse nuestra confianza y conseguir que compartamos nuestros datos con ellos, como contraseñas o datos de nuestra tarjeta, o que les demos acceso a nuestros dispositivos.

Phishing Técnica donde los ciberdelincuentes se hacen pasar por otra persona o entidad a través del correo electrónico, como puede ser el banco, una red social o incluso un servicio

público, para engañarnos y que realicemos alguna acción bajo cualquier excusa, generalmente acceder a una página fraudulenta o descargar un fichero infectado.

Archivo adjunto Fichero o documento que viene junto a un correo electrónico y que podemos descargar. Si la persona que nos envió el correo es desconocida o el contenido del mensaje nos resulta raro, no debemos descargarlo hasta saber que no estamos ante un fraude.

Correo electrónico Servicio que nos permite enviar y recibir mensajes mediante Internet. Para utilizarlo necesitamos un gestor de correo (Gmail, Outlook/Hotmail, Yahoo!, etc.).

URL Cadena de caracteres que permite acceder a una página web o contenido alojado en Internet. Se compone de varias partes: el protocolo, que puede ser “http” o “https”, y el domino, que es el nombre o dirección de la página web concreta. Ejemplos de URL: https://www.osi.es y https://www.incibe.es

Permisos es la autorización que tiene o necesita un software para realizar ciertas tareas o acceder a ciertos recursos de nuestros dispositivos como modificar archivos, leer archivos, instalar aplicaciones, acceder a nuestra cámara o micrófono entre otros.

Vishing Ataque basado en ingeniería social, donde el atacante se hace pasar por una persona que no es, llamándonos por teléfono e intentando que le facilitemos información personal, accedamos a una página web fraudulenta o instalemos algún programa para tomar el control de nuestro dispositivo. Frecuentemente se hacen pasar por el servicio técnico del sistema operativo de nuestros dispositivos.

Smishing Ataque basado en ingeniería social, donde los atacantes se hacen pasar por otras personas o entidades de confianza, a través de mensajes de texto o SMS, con el fin de engañarnos para que realicemos un pago, nos descarguemos un archivo infectado o hagamos clic en un enlace malicioso.

Cómo funciona la herramienta

Con los conceptos antes definidos podemos detallar cuales son las funciones de la herramienta RS4Ly.

RS4Ly tiene integrada 4 Apis una Api (interfaz de programación de aplicaciones) en pocas palabras esto es un conjunto de funciones, subrutinas y procedimientos que ofrece una biblioteca, en este caso son 4 fuentes de inteligencia de amenazas las cuales atreves de estas Apis permiten que nosotros de manera gratuita o pagada para obtener más funciones, obtengamos información de manera rápida y precisa, pudiendo integrar las mismas a las herramientas que nosotros creemos.

Un ejemplo de esto en la vida real puede ser que una biblioteca común intégrese a sus servicios el delivery o mensajero y que el requisito para usar el servicio sea tener una tarjeta de usuario común de la biblioteca, entonces nosotros sin tener que ir a la biblioteca física a atreves del mensajero podemos solicitar información sobre libros, revistas entre otros recursos que tenga la biblioteca de manera rápida y precisa usando nuestra tarjeta de usuario, la biblioteca es la que se encarga de tener almacenada la información, actualizarla y dar respuesta a las solicitudes que realizamos.

Continuando Entonces con estas 4 Apis de las plataformas: Ip abuse db, ip Quality score, Ip abstract y virus total:

1) se extrae información de lo que usted quiera analizar permitiendo así obtener información sobre direcciones ip públicas, redes públicas, archivos, url (links).
2) Luego se procesa la información comparando los diversos datos con la finalidad de obtener confirmaciones de los mismos.
3) Se muestra la información procesada y analizada al usuario.
4) El usuario puede si desea guardar la información en un archivo o tomar una captura de pantalla para compartirla con quien desee hacerlo.

Como le ayudara la herramienta en su rutina diaria

Ya sabiendo todo lo que puede hacer la herramienta comenzamos a listarlos uno por uno y daremos un ejemplo del mismo:

Análisis de IP

Esta función le servirá a usted en dado caso de ser un analista de seguridad si recibe algún tipo de alerta de una conexión maliciosa permitida, algún tipo de trafico sospechoso en su red poder analizar la ip que desconoce de una manera rápida logrando obtener datos como lo son:

- Nivel de riesgo general e individual según las fuentes de información.
- número de usuarios y los reportes totales que tiene esta ip por comportamiento malicioso.
- El ISP actual, el nombre del dominio y del host e información geográfica.
- Le puede informar si se trata de una conexión tipo: proxy, vpn, o un nodo tor.
- El tipo de uso de la misma.
- Si presenta tráfico no humano (bots)
- Le da información individual según la fuente con niveles de riesgo del 1 al 10 y escala de colores.
- Le muestra el número de cambios de nombres registrados y los dos últimos sin incluir el actual.
- Le informa si existen Url reportadas como maliciosas con esta IP
- Le muestra si está en algún IOC reportado.

Análisis de subnet (Redes)

Esta función le servirá a usted en dado caso de ser un analista de seguridad o un apasionado de la misma para poder obtener información de manera rápida y precisa sobre un conjunto de IPs que pertenezcan a un mismo segmento de red (Mínimo /24), esto es realmente útil al momento que analizamos un incidente para trabajar de manera proactiva y adelantarnos a los ataquante.

Si usted analiza cierta dirección ip que es claramente usada para fines maliciosos usted puede tomarse los segundos extras de investigar esta misma ip con el /24 así podrá analizar un segmento de red que contiene 254 dirección las cuales podrían de igual manera ser usada para los mismos fines maliciosos permitiendo recomendar o usted tomar la iniciativa de bloquear el segmento completo de red con la finalidad de que la misma no se pueda conectar con sus equipos en el futuro y ahorrarse en un futuro tener que analizar nuevamente un incidente relacionado con este segmento.

Los datos que muestra este apartado, son similares al de anterior pero aquí se añaden:

- El número total de reportes que tiene la red
- El numero usuarios que han reportado la red
- Un porcentaje de las IPs maliciosas dentro del segmento insertado.
- La recomendación general de si es o no conveniente bloquear el segmento completo.
- Fecha del último reporte que se le realizo a cada ip de manera individual

Análisis de archivos

Esta función ayuda tanto al usuario casual como al usuario más especializado explicaremos como y luego un detalle de la información que se mostrara:

Algunos conceptos que cabe remarcar antes de iniciar seria el concepto de **Hash,** en resumen, se encarga de convertir un valor en otro a través de algoritmos matemáticos. Entiendo por valor como un texto, contraseña, archivos, documentos, archivos de música, videos, entre otros. Teniendo en cuenta que el valor final es único a cualquier otro según lo que introduzcamos, por ejemplo, usando la función hash SHA256:

La palabra "Hola" es equivalente a e633f4fc79badea1dc5db970cf397c8248bac47cc3acf9915ba60b5d76b0e88f

La palabra "hola" es equivalente a b221d9dbb083a7f33428d7c2a3c3198ae925614d70210e28716ccaa7cd4ddb79

Una simple Mayúscula o minúscula cambia el código totalmente.

Continuación

Esto permite que un libro de más de 500 páginas sea identificable con un código hash pequeño de por ejemplo en 56 caracteres como el ejemplo anterior. Tome de ejemplo esta parte del texto en negritas su longitud hasta este punto es de 236 caracteres con espacios.

Esto es útil debido a que con estos códigos hash podemos realizar una "verificación de integridad", es decir verificar que una entrada como lo que mencionamos arriba haya o no recibido alguna modificado no autorizada o que no sea la versión segura que estamos buscando y en cambio sea la versión modificada para causar daño de algún ataquante o ciber delincuente.

Uso

Para un usuario común: Usted y los suyos antes de ejecutar un archivo, aplicación o documento descargado podrá obtener un hash de identificación y al introducirlo en la misma herramienta podrá saber si el mismo está registrado como malicioso en nuestras fuentes de inteligencia de amenazas esto es útil con los niños o si estamos involucrados en labores que requieran estar constantemente descargando, archivos, documentos, imágenes entre otros. Analizar los mismos antes de ejecutarlos.

Para un usuario más especializado al recibir algún tipo de alerta de una descarga maliciosa podrá tomar el código hash identificado e ingresarlo en la herramienta así obtendrá más información sobre el mismo y si en realidad se trata de un evento importante o si es un falso positivo.

Análisis de url

Esta función ayuda tanto al usuario casual como al usuario más especializado.

Cuantas veces le ha pasado que atreves de algún grupo de WhatsApp, Telegram o en alguna red social ve que alguien comparte un link de una oferta con un descuento atractivo, o que le llega un mensaje del banco a su correo diciendo que su cuenta fue bloqueada, o de que está buscando registrarse a alguna página de internet para obtener acceso a alguna función que anuncia. ¿Se ha preguntado usted cuantas de estas podrían ser trampas hechas por ciber delincuentes para obtener sus datos? La probabilidad es alta de caer en una estafa del tipo pishing para evitar esto tiene esta función.

Con este apartado puede copiar la url(link) e ingresarlo de manera rápida, luego de manera precisa y concisa se investigará de la misma, se procesará y presentará la información diciéndole si la misma es maliciosa, si ha sido utilizada para malware y virus o pishing, de esta forma podrá tener una certera elevada a la hora de navegar por internet de que los sitios web que visite sean seguro para usted y los suyos.

Esta función usando le permitirá al usuario:

- Detección de URL de phishing: detecte las URL maliciosas utilizadas para campañas de phishing y publicidad engañosa.
- Escaneo de URL maliciosas: identifique las URL utilizadas para malware y virus con fuentes de inteligencia de amenazas en vivo que detectan enlaces de phishing de día cero y comportamiento sospechoso.

Porque es necesario tener tantas keys personales

Entiendo que puede sonar tedioso tener que registrarse en 4 plataformas para obtener sus keys personales y utilizar la herramienta por eso considero pertinente explicar porque usamos 4 diferentes y no solo una:

1) Obtener una visión general: Usando diversas fuentes de información tenemos la oportunidad de ver un panorama general de la dirección a investigar, debido a que cada fuente brinda un dato, información o campo especial que las otras no.
2) Confirmar informaciones: Al tener diversas fuentes podemos comparar los resultados así confirmar o no algunos campos importantes para dar más veracidad.

Detalle de la información recolectada de cada fuente y como se combinan (próximamente)

Primeros pasos

Para comenzar a usar la herramienta los pasos a seguir son los siguientes:

1) Obtener sus keys personales

Antes de iniciar la herramienta deberá registrarse en las 4 plataformas para obtener su keys personales para usar las Apis de las mismas, explicaremos paso a paso lo que debe hacer según la plataforma:

- Virus Total
  a) El enlace para registrarse es https://www.virustotal.com/gui/join-us
  b) Una vez este registrado abre el enlace **https://www.virustotal.com/gui/user/Su-usuario/apikey** para ver su clave api y registros de uso, reemplaza el texto en verde por su usuario.

- IP Abuse DB
  a) En enlace para registrarse es https://www.abuseipdb.com/register?plan=free
  b) Después de registrarse debe ir al enlace https://www.abuseipdb.com/account/api
  c) Una vez dentro de la página deberá ir al apartado "**API**"
  d) Busque la opción "**Create Key**" e ingrésele el nombre que guste para identificarla
  e) Copie solamente el "**Key**".

- IP Quality Score
  a) El enlace para registrarse es https://www.ipqualityscore.com/create-account
  b) Después de creada su cuenta debe ir al enlace https://www.ipqualityscore.com/documentation/proxy-detection/overview
  c) Luego que la pagina cargue debe presionar "**Ctrl + F**" esto abrirá la herramienta de búsqueda
  d) Ya abierta la herramienta de búsqueda ingrese "**Prívate Key**"
  e) Esto le mostrara el apartado donde se encuentra su Key personal.
  f) Copie su keys personal.

- IP Abstract
  a) El enlace para registrarse es https://app.abstractapi.com/users/signup
  b) Para encontrar su Key debe ir al link https://app.abstractapi.com/api/ip-geolocation/documentation
  c) Una vez en documentación en la parte superior vera un mensaje que dice "**This is your private API keys, specific to this API.**", Seguido de este mensaje esta su Key.
  d) Ir al apartado de "**Documentation**"

2) Ingresar sus keys personales en la herramienta

Ya registrado y con sus keys personales listas para ser introducidas en la herramienta, debe ir al módulo "**RS4LyAPIKEYS02**":

Vera que las líneas con valores son las 2,4,6 y 8. Tendrán en común el texto "Key-Personal" después del signo de "=", lo que haremos en pocas palabras es reemplazar el texto por nuestra keys personal igual que como indica el mensaje.

a) Identificación:

I. En la línea 2 vera "ApiKey_Virus_Total=", aquí debe ir su keys de Virus Total.
II. En la línea 4 vera "ApiKey_IP_Abuse_DB=", aquí debe ir su keys de IP abuse db.
III. En la línea 6 vera "ApiKey_IP_Quality_Score=", aquí debe ir su keys de Ip Quality Score.
IV. En la línea 8 vera "ApiKey_IP_AbstractApi=", aquí debe ir su keys de IP Abstract.

b) Ejemplo:

I. Dado el caso imaginemos que su keys de virus total es: "9b7368f7a54fe5b41821988f47basdadasdadascda1f14465".
II. Como hemos mencionado de forma anterior en el apartado a, se va a línea 2 en la cual tendrá: ApiKey_Virus_Total="Key-Personal"
III. Usted dentro de las comillas eliminara el mensaje Key-Personal y pondrá su keys en este caso quedaría:

ApiKey_Virus_Total="9b7368f7a54fe5b41821988f47basdadasdadascda1f14465"

IV. Repite este paso con las otras keys personales.

3) Comprobar que todo este correcto

Ya que usted haya ingresado sus keys personales en la herramienta procederemos a realizar una prueba o varias pruebas de conexión para verificar que los datos ingresados sean correctos

En el menú principal el apartado correspondiente a este tema se encuentra en la opción 5 con el nombre (Verificar conexiones y keys personales), usted presiona el número 5 y luego “enter” en su teclado, esto abrirá el menú de este apartado. En este caso tendrá 3 opciones disponibles:

1-**Basica (Conexiones a las Apis):** Esta opción realizara un ping a las 4 plataformas que estamos usando para comprobar que podemos entablar una conexión con las mismas. Se recomienda utilizarla siempre que se inicie la herramienta.

2-Intermedia (Revisa Que las Key Personales estén funcionando): Esta opción se encarga de verificar que las keys personales que usted ingreso estén funcionando correctamente. Se recomienda usarla la primera vez que usted ingresa sus keys personales.

3-Completa (Verifica la conexión y las keys personales): Esta opción es una combinación de la opción 1 y 2. Se recomienda ejecutarla la primera vez que introduzcamos nuestras keys personales.

Información y resultados que se obtendrán al realizar una búsqueda (Próximamente)

Funcionamiento a nivel de programación (Próximamente)

Fuentes de información:

https://es.wikipedia.org/wiki/Virus_inform%C3%A1tico#Tipos_de_virus

https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/

https://www.docusign.mx/blog/amenazas-la-ciberseguridad

https://www.osi.es/es/actualidad/blog/2021/06/28/conceptos-basicos-de-ciberseguridad-que-debes-conocer

https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

https://www.caser.es/glosario-seguros/comercio/ataque-informatico

https://www.madrid.es/UnidadesDescentralizadas/UDCObservEconomico/015%20Cl%C3%BAsteres/Ficheros/002%20CIBERSEGURIDAD/An%C3%A1lisisTalentoCiberseguridadMayo-Julio2020.pdf

https://www.nephosit.com/diferencia-entre-ciberseguridad-y-seguridad-en-la-nube/

https://www.redeszone.net/tutoriales/seguridad/comprobar-integridad-archivos-hash/#:~:text=Para%20la%20verificaci%C3%B3n%20del%20hash,archivo%20o%20generar%20el%20hash.

https://www.redeszone.net/tutoriales/seguridad/comprobar-integridad-archivos-hash/

Versiones actuales y futuras mejoras

Próximas mejoras

- Activar análisis de Url
- Activar análisis de Archivos
- Activar análisis de subnet (Redes)
- Guardar información en un documento
- Entre otras mejoras de funcionamiento general.

0.2.0 - Actual

- Reescritura general de todo el código para ser más entendible, mejorar el consumo de recursos, entre otros aspectos.
- Se creó el módulo APIKEYS para que sea más fácil ubicar las keys necesarias además contienen los links de registro, uso de solicitudes, y donde encontrar su api keys.
- Se cambió el nombre del módulo análisis de datos a análisis de condiciones.
- Se creó el modulo opciones del menú sacando este apartado del menú principal.
- Se creó el modulo análisis de ip publica solo se activa si la ip insertada es pública.
- Se mejoró el proceso de consulta y toma de data para bajar el consumo de datos en caso de error y no gastar las consultas disponibles de cada api.
- Se añadió el api de AbstractApi.
- Se creó el modulo Verificación de datos el cual compara los datos traídos de diferentes fuentes.
- Se creó el modulo Extras el cual contiene las opciones para modificar el color del texto y fondo de la herramienta, entre otras.
- Se creó el modulo Manual de uso para ofrecer ayuda al usuario al momento de usar la herramienta.
- Se creó el modulo Conexiones el cual se encargará de verificar que en primer lugar pueda conectarse al link de las Apis, en segundo lugar, que no tenga el valor por defecto en las keys personales, estas dos funciones se ejecutaran al abrir la herramienta y en tercer lugar que las keys ingresadas sean correctas, esta es una opción que se activara manual y hará una consulta de prueba a todas las Apis.

0.1.0

- Primer lanzamiento