KeyMac

Guía Completa

Versión: 2.4.4

Generado 22 septiembre 2020
Actualizado 20 octubre 2020

Creador: MacKey-255

Índice

Capítulo 1

Instalación de Servidores

Vincular el TINServer

Empezando con el KeyMac podemos observar que está muy ligado al Steam, por lo cual podemos vincularlo con el TINServer fácilmente.
En el panel de configuración del Servidor KeyMac podemos observar estas opciones:

- Vincular con TINServer
- Auto-Start TINServer
- Ruta del Servidor Principal/TINServer

Una vez leído el Tutorial básico del KeyMac, sabrás para que funciona cada opción. La primera permite vincular el TINServer anclado en la Ruta especificada, por lo cual el KeyMac podrá manejar los datos de las bases de datos del propio TINServer, ya sea leer datos y crear usuarios.
También tenemos el Auto-Start que nos mantendrá ejecutado el TINServer, aunque el mismo este apagado en ese momento. Para asegurarnos de que todo funciona correctamente revisamos la configuración del TINServer, el parámetro users debe quedar así: **users=TINserver.users.db3** con esto aseguramos la base de datos de usuario que el KeyMac utilizará. Y ya estaría lista la vinculación con el TINServer.

Servidores Independientes

Una vez vinculado o no el TINServer al KeyMac, podemos anclar nuestro Servicio al KeyMac. Tenemos varias opciones:

1. Anclarlo junto con el TINServer.
2. Anclarlo independiente.
3. Que el KeyMac gestione todo.

En la primera debemos buscar los puertos del servidor y su respectivo puerto de query (Puerto que permite ver el servidor desde el Steam). Estos puertos los agregamos a la lista de puertos y ya estaría anclado.

La segunda debemos darle como Ruta del Servidor Principal la de nuestro servicio. Ya que el KeyMac utilizará este ejecutable para crear una regla en el Firewall justa para el acceso completo al servicio. Si es necesario, se puede agregar algunos puertos que se escapan del ejecutable o extras que son requeridos.

La tercera opción es la más cómoda, pues el KeyMac no tendrá ni Ruta del Servidor Principal ni Puertos asociados. Debido al funcionamiento del KeyMac, cuando no se especifica ningún puerto, este crea una regla capaz de acaparar todos los puertos, permitiendo el acceso completo mientras se este usando el KeyMac. Entonces si posees X cantidad de servicios podrás darle acceso a todo sin necesidad de especificar la ruta del servicio, el puerto de los demás servicios, etc.…

Múltiples Servidores

Cuando tenemos muchos servicios montados en un Servidor, cuesta mucho anclarlos todos al KeyMac, debido al gran volumen de estos. Para poder vincular más de un servicio al KeyMac debemos anclar uno primero en la Ruta del Servidor Principal, normalmente en esta opción se coloca el TINServer o algún Servicio Primario. Luego procedemos a agregar todos los puertos correspondientes a los servicios extra que poseemos.
Si no queremos complicarnos tanto podemos simplemente dejar un servidor Principal como es el TINServer y dejar en blanco la lista de Puertos para que el KeyMac abarque todos los puertos, permitiendo el acceso a todos los servicios una vez accedes al KeyMac.

Otros Servicios no relacionados

Como bien sabemos, el firewall en nuestro servidor estará activado por lo que otros servicios extra pueden quedar bloqueados. Para solucionar este inconveniente podemos crear reglas en el Firewall a este servicio para que cualquier pueda acceder a él.

Ejemplo:

1. Tenemos el RCON activo en el Rust y necesitamos acceder con un Panel de Administración al RCON, pero el puerto esta bloqueado. Agregamos el puerto en el firewall como permitido el acceso y ya podremos acceder sin problema alguno.

2. Tenemos un Hosting Web y no podemos acceder debido al Firewall. Agregamos el puerto del servicio en el firewall para permitir el acceso.

Capítulo 2

Manejo del KeyMac

En este capítulo principalmente nos referiremos a las secciones no tocadas en la Documentación Básica del KeyMac. Una forma de ampliar la vista del funcionamiento del KeyMac y toda su mecánica en profundidad.

Configuración Básica

El KeyMac es una herramienta fácil y a la vez compleja que proporciona muchas opciones según el entorno del usuario final. Empecemos por su sistema de configuración el cual como habrás notado no tiene guardar ni ningún tipo de función similar. Esto es básicamente porque contiene un auto guardado y ajustado al instante del cambio, por lo cual no es necesario cerrarlo para efectuar los cambios, sino que se realizan en el momento. Hay veces que el propio KeyMac cierra el Server porque estas configurando algo que implica el mismo, pero es parte del sistema para evitar el problema de no aplicar los cambios.

Consola y Registros

El KeyMac posee un complejo sistema el cual registra y muestra todo su funcionamiento para que el administrador capte toda la información que el KeyMac es capaz de brindar sobre el usuario y los procesos que realiza. Por eso podemos observar información "rara", o, mejor dicho, desconocida para el administrador. Bueno, toda esta información que principalmente esta estructura es muy simple de leer en las circunstancias correctas. A continuación, les mostraremos varias estructuras y cuando es que deben aparecer:

- Avisos y Baneados

Cuando un usuario posee un proceso sospechoso es enviado al servidor como un aviso, si esta recién abriendo el KeyMac, o como baneado directamente. Posee la siguiente estructura más que obvia:

ProductName | FilePath | FileOriginalName | WindowsTitle | FileDescription | FileVersion | CompanyName | FileSize | LastModified | LegalCopyright | Checksum | Detected

- Agregados a la lista blanca

Una vez agregado a la lista blanca podemos ver varios dispositivos separados por el símbolo | el cual es el separador de información del KeyMac. Cuando un usuario accede al KeyMac salen todos los dispositivos HID que tiene conectado separados por ese símbolo.

- Hacker detectado

Un sistema creado para detectar anomalías en la comunicación con los clientes, detecta estas anomalías y avisa de las mismas en la consola y los registros del servidor.

- Información extraída del usuario

Muchos sabrán que la información recibida del usuario se almacena en una carpeta en la raíz del KeyMac con una estructura simple y fácil de leer. Los archivos grandes con mucha información se almacenan como documento Excel (CSV), separados por el símbolo ya mencionado para una mayor lectura. También se incluyen capturas de pantallas.

Los archivos son varios:

  - data_mouse

    Contiene todos los dispositivos HID separados por | como símbolo.

  - data_process

    Contiene todos los procesos que el usuario tiene ejecutados.

  - programs_executed

    Contiene los programas que ejecutó el usuario hace un X tiempo.

  - programs_installed

    Contiene la lista de todos los programas instalados del cliente.

Excepciones de la Whitelist/Blacklist

Como has podido observar el corazón del KeyMac es este sistema y es de vital importancia no tocarlo mucho. Aquí podrás especificar que programas o mouse son maliciosos o no. Debido a que el KeyMac busca código malicioso en los procesos es necesario filtrar los procesos que dieron como maliciosos. Para ello existen dos formas de agregar fácilmente los procesos o mouses.

La primera es cuando el cliente envía un aviso de que el proceso o mouse es detectado como sospechoso, en este punto puedes agregarlo o no como seguros en la Whitelist.

La segunda es cuando el usuario es baneado por utilizar ese proceso cuando esta conectado al KeyMac, también se puede agregar y de paso desbanear al usuario implicado.

Una vez tengamos claro como trabajar con los procesos podemos agregar y banear de forma correcta muchos de ellos. Con el mouse viene lo mas complejo ya que como no tenemos forma de saber si un mouse es Bloody o tiene alguna ventaja sobre los demás, separamos el problema en empresa y producto. Funciona con estos datos:

- VID

  Este valor contiene que empresa ha creado el dispositivo, suele ser de 4 caracteres y puedes investigar mediante internet que empresa es. Solemos banear las empresas que creen dispositivos Bloody o similares para evitar que los jugadores los utilicen.

- PID

3. Este valor es el Producto especifico de la empresa que lo creo, o sea un identificador único que identifica a ese producto. Normalmente buscamos la empresa y dado el PID sacamos el modelo del Mouse. Hay páginas en internet que, dado estos datos, podemos saber que mouse es ya que poseen bases de datos enormes con todos los modelos registrados.

Agregar Procesos Protegidos

Primero que todo, ¿Qué son los procesos protegidos? Son los procesos conocidos que están protegidos por el KeyMac, de forma tal que es necesario tener el cliente original de este proceso. También incluye la protección de memoria y otras mejoras como obligar al usuario a solo poder abrirlos cuando esté conectado al servidor, de lo contrario se cerrará de forma inmediata. Usualmente, cuando el usuario posea el proceso abierto, antes de una previa conexión al servidor, se cerrará automáticamente para prevenir la inyección o modificación del cliente. Cuando ocurra una pérdida de la conexión, el usuario tendrá 30 segundos para reconectarse, sino se cerrará el proceso protegido.

Para poder agregar un proceso protegido basta con abrir el proceso a proteger (Si es un juego les recomiendo entrar en el servidor antes para tener todos los módulos cargados previamente) y abrimos la nueva herramienta llamada: "KeyMac Tool", la cual te proporciona una lista de procesos; buscas el proceso correspondiente y luego escoges la carpeta donde está el ejecutable de tu proceso. Toda esta operación genera en la carpeta de tu "KeyMac Tool" un archivo .json el cual contiene la información necesaria que entenderá el KeyMac. Vas a la pestaña de Procesos en el KeyMac Server y agregas este .json y ya estaría agregado un proceso protegido al KeyMac.

Capítulo 3

Errores Comunes

Corta fuegos (Firewall)

En muchas ocasiones no podemos acceder de forma correcta al servicio que tenemos montado en el KeyMac, principalmente porque no tenemos correctamente configurado el mismo. A veces nos puede faltar algún puerto por agregar; revisemos bien los puertos que utiliza nuestro servicio para poder acceder a él correctamente.

A menudo cuando iniciamos un programa, el Firewall lo añade como permitido o denegado por tener habilitado las notificaciones del Firewall, por lo cual podemos o no acceder al servicio sin tener abierto o no el KeyMac. Compruebe bien las reglas de entrada en el Firewall para solucionar este error.

El KeyMac ya tiene incorporado una funciona para solucionar el tema de las notificaciones del Firewall, deshabilitándolas en cuanto el KeyMac inicia. No obstante, verifíquelo todo en el Firewall de Windows.

Whitelist/Blacklist

Este componente es uno de los más importante y sensibles que hay en el KeyMac, ya que es el corazón de la detección de posibles procesos o mouses sospechosos. Muchas veces el KeyMac no detecta los procesos o mouses maliciosos ya que se comete el error de agregar algún mouse o proceso en la Whitelist permitiendo el uso de este, siendo realmente malicioso. Para evitar este problema les recomiendo no confiar mucho en los usuarios y estar verificando que dispositivos HID son considerados como Bloody o permiten ventajas sobre los demás jugadores. Para ello existen en

internet muchas bases de datos que dado el PID y VID les muestran que producto es el que el usuario realmente este usando.

Vinculación con el TINServer

Cuando estas en el proceso de vincular el TINServer es necesario saber que debemos tener bien configurado el servidor de Steam para que el KeyMac pueda acoplarse a él. Debes asegurarte de que la carpeta "data" sea la de configuraciones del Steam, que la base de datos de "users" sea: **users=TINserver.users.db3** y que en la carpeta "data" tenga la base de datos: **TINServer.cmserver.db3** sino durante la ejecución del KeyMac abran errores desconocidos.

Verifica que tengas todas las herramientas del TINServer para poder trabajar cómodamente con él. Una vez hecho todos estos pasos y comprobando el buen funcionamiento de tu servidor de Steam puedes revisar el Capitulo 1 de nuevo de como **Vincular el TINServer**.

Lectura de la Consola

A medida que vamos trabajando con el KeyMac podemos ver muchas cosas en la consola y principalmente la que nos llama mucho la atención es la de: "Hacker Detected" el cual hace referencia a un dato mal enviado o alguna anomalía en la comunicación con el servidor KeyMac. Esto te advierte de los posibles clientes falsos que la comunidad pudo haber desarrollado para violar el sistema del KeyMac o de clientes viejos.

También podemos darnos cuenta de una estructura rara en los datos que el KeyMac presenta separados por el símbolo | que a cualquiera dejará pensando en que orden esta ordenado cada dato. Bueno aquí te dejaré el orden para poder leerlo:

ProductName | FilePath | FileOriginalName | WindowsTitle | FileDescription | FileVersion | CompanyName | FileSize | LastModified | LegalCopyright | Checksum | Detection

Si traduces bien los datos te darás cuenta que son cada uno ya que son muy evidentes y te permitirán ver toda la información de un proceso.

Conexión y consumo de red

Si eres un administrador de redes experimentado podrás notar el alto consumo de red cuando hay varias opciones del KeyMac activas. El KeyMac tiene una opción muy interesante que envía cada un tiempo diferente información del Cliente por lo cual la red se dispara y los diferentes filtros de red pueden hacer que el Usuario sea baneado o expulsado durante un tiempo del servidor. Si posee una buena infraestructura de red podrá dejar esta opción activa y puede recibir toda esta información para monitorear al usuario. Sino deshabilítalo y revise de forma manual al usuario pidiendo la información del mismo. Todo depende de su infraestructura y los Mikrotik con sus límites de copia demasiado estrictos pueden afectar mucho al servicio.

Errores del KeyMac

En muchas ocasiones el KeyMac no funciona del todo bien y este expulsa un registro con los errores que pudo ocasionarse. Intenta enviárselos al creador para poderle dar mayor seguimiento al error. También puedes sugerir cambios y mejoras en el producto, intenta ponerte en comunicación con el mediante correo o en la propia SNET.

Capítulo 4

Desarrollo e Integración

Nuevas características y desarrollo

Cada cierto tiempo el KeyMac lanza nuevas características y arreglos a los fallos que sus versiones posteriores presentan. El creador desarrolla este producto con el único objetivo de solucionar un problema real que presentan muchos servicios. Este proyecto es libre y no busca robar, aprovechar o lucrarse con el mismo, simplemente busca cumplir su objetivo: Una red más justa y libre de individuos lleno de complejos y manías capaces de utilizar cualquier tipo de ventaja sobre los demás jugadores, arruinando el servicio por completo.

Eres libre de confiar o no en el proyecto, el creador es lo más explícito y transparente posible en todos los cambios y ajustes que realiza, Siendo desarrollado por una única persona sin ánimo de lucro y con las mejores intenciones del mundo.

Debido al poco presupuesto (inexistente) que posee el creador, irá sacando versiones poco a poco según su ritmo y sus condiciones. Si desea aportar en el proyecto eres libre de ello, contacte con: MacKey-255 vía correo o por la SNET.

Integración con un API

Suele suceder de que posees un servicio ya estructurado con su sistema y necesitas vincularlo con el KeyMac y su compleja estructura. El KeyMac tiene la solución, un sistema de integración vía API. Para desarrollar la integración con el mismo debes leer el README_API el cual posee todo lo necesario para crear el API con todas las especificaciones y medidas de seguridad requeridas.

Nuevas características

Dado que la demanda aumenta y la diversidad de ambientes también, puedes proponer nuevas mejoras y cambios importantes al KeyMac.

Como has podido apreciar, en la documentación básica, hay una pagina web dentro del KeyMac. Puedes acceder a ella y realizar bastantes operaciones útiles sin necesidad de acceder al servidor. Si posee algún prototipo o mejora para el mismo, puedes comunicárselo al creador, estará encantado de recibir retroalimentación por porta de los administradores y personas, que al igual que él, luchan por el mismo objetivo.